

V1.1

APT WIKI.



THREATRADAR
By HADESS

WWW.THREATRADAR.NET

INTRODUCTION

In the digital era, the landscape of cybersecurity is constantly reshaped by the emergence of sophisticated threats. Among these, Advanced Persistent Threats (APTs) represent a new frontier of cyber warfare, characterized by their stealth, persistence, and complexity. This introduction sets the stage for a deep dive into the world of APTs, offering a comprehensive overview of their methodologies, the software they employ, and the advanced techniques that make them a formidable force in the cyber realm.

Defining Advanced Persistent Threats APTs are not just typical cyber threats; they are highly coordinated attacks orchestrated by entities with significant resources, such as nation-states or organized criminal groups. These attacks target specific entities with the intent to steal, spy, or disrupt. This paragraph elaborates on the defining characteristics of APTs, differentiating them from other forms of cyber attacks and highlighting their targeted, prolonged, and sophisticated nature.

Historical Context and Evolution Tracing the roots of APTs provides critical insights into their evolution. From early instances in the late 1990s and early 2000s to the highly complex operations of today, APTs have evolved in tandem with technological advancements. This part discusses notable historical APT campaigns and how they have shaped the current threat landscape.

The Motivations Behind APT Attacks Understanding what drives APT groups is key to comprehending their operations. This section delves into the various motivations behind APT attacks, which range from political espionage and intellectual property theft to financial gain and geopolitical domination.

An Arsenal of Tools and Software APTs use a wide array of tools and software, some custom-built and others repurposed from the cybercriminal ecosystem. This paragraph introduces the types of malware (like ransomware, spyware, and Trojans), exploitation tools, and other software commonly deployed in APT campaigns, setting the stage for a more detailed exploration in subsequent chapters.

Sophisticated Techniques and Strategies APTs are known for their sophisticated attack techniques. This section briefly touches upon the various strategies employed by these groups, including initial access methods like spear-phishing, moving laterally within networks, maintaining persistence, and evading detection.

Real-World Impact and Notable Incidents The real-world impact of APTs is far-reaching, affecting governments, corporations, and individuals alike. This part provides an overview of some of the most impactful APT incidents in recent history, illustrating the scale and seriousness of these threats.

Navigating the Chapters Ahead Concluding the introduction, this paragraph outlines the structure of the book, guiding the reader through the upcoming chapters that delve deeper into each aspect of APTs - from their organizational structure, specific case studies, analysis of their tools and techniques, to defense strategies and future trends in APT activities.







To be the vanguard of cybersecurity, HadeSS envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish HadeSS as a symbol of trust, resilience, and retribution in the fight against cyber threats.

At HadeSS, our mission is twofold: to unleash the power of white hat hacking in punishing black hat hackers and to fortify the digital defenses of our clients. We are committed to employing our elite team of expert cybersecurity professionals to identify, neutralize, and bring to justice those who seek to exploit vulnerabilities. Simultaneously, we provide comprehensive solutions and services to protect our client's digital assets, ensuring their resilience against cyber attacks. With an unwavering focus on integrity, innovation, and client satisfaction, we strive to be the guardian of trust and security in the digital realm.

ACKNOWLEDGMENT

- Negin Nourbakhsh(<https://www.linkedin.com/in/negin-nourbakhsh/>)
- Ali RahimDabagh(<https://ir.linkedin.com/in/cyberlynx>)
- Hasti Alikhani(<https://ir.linkedin.com/in/hasti-alikhani-989462221>)

Table of Content

- [Admin@338 - Group Overview](#) 
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Ajax Security Team - Group Overview](#) 
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed Activities:](#)
- [ALLANITE - Group Overview](#) 
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
 - [**Tools Used:**](#)
- [Andariel - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
 - [Tools Used:](#)
 - [**Techniques Used by Andariel:**](#)
- [Angin Dragon: A Suspected Chinese Cyber Espionage Threat Group](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
 - [Tools Used:](#)
 - [** Description: **](#)
 - [** Motivation: **](#)
 - [** Names: **](#)
 - [**Techniques Used by APT.C-36**](#)
 - [**APT3 \(Advanced Persistent Threat3\)**](#) 
 - [** Description: **](#)

- ** Motivation: **
- ** Names: **
- ** Location: **
- ** First Seen: **
- ** Observed: **
- **Techniques and Software Used by APT1**
 - ** Techniques Used by APT1: **
- **APT12 (IXESHE, Numbered Panda, Group 22)**
 - ** Description **
 - ** Motivation **
 - ** Names **
 - ** Location **
 - ** First Seen **
 - ** Observed Activities **
- **APT12 (IXESHE, Numbered Panda, Group 22) Techniques and Software**
 - ** Techniques Used **
- **APT16: Overview and Activities**
 - ** Description **
 - ** Motivation **
 - ** Names: - **
 - ** Location **
 - ** First Seen: - **
 - ** Observed Activities **
- **APT17 Overview**
 - ** Description **
 - ** Motivation **
 - ** Names **
- **APT17 Techniques and Software Used**
 - ** Techniques Used by APT17 **
- **APT18: Overview and Details**
 - ** Description **
 - ** Motivation **
 - ** Names **
- **APT18 Techniques and Software Used**
 - ** Techniques Used by APT18 **
 - ** Description **
 - ** Motivation **
 - ** Names **
- **APT28 (Fancy Bear)**
 - ** Description **
 - ** Motivation **
 - ** Names **
- **Description of APT3**
- **Motivation:**
- **Names:**
- **Location:**
- **First Seen:**
- **Observed:**
 - ** Techniques Used by APT3: **
- **Description of APT 30 (Override Panda)**
- **Motivation**

- ****Names****
- ****Location****
- ****First Seen****
- ****Observed Activities****
- ****Techniques Used by APT 30****
- ****Description of APT32****
- ****Motivation****
- ****Names****
- ****Location****
- ****First Seen****
- ****Observed Activities****
- ****APT33: Overview and Activities****
 - **** Techniques Used by APT33 ****
- ****APT37 (Reaper)****
 - **** Description ****
 - **** Motivation ****
 - **** Names ****
 - **** Location ****
 - **** First Seen ****
 - **** Observed ****
- ****Techniques Used by APT37****
- ****APT38 Threat Actor Profile****
 - **** Description ****
 - **** Motivation ****
 - **** Names ****
 - **** Location ****
 - **** First Seen ****
 - **** Observed Activities ****
- ****Techniques Used by APT38****
- ****APT39: Overview and Activities****
 - **** Description ****
 - **** Motivation ****
 - **** Location and Observed Activities ****
- ****APT39 (Chefer): Overview and Activities****
 - **** Description ****
 - **** Motivation ****
 - **** Names and Affiliations ****
- ****APT41 - Group Overview****
 - **** Description: ****
 - **** Motivation: ****
 - **** Names: ****
 - **** Location: ****
 - **** First Seen: ****
 - **** Observed: ****
- ****Description****
- ****Motivation****
- ****Names****
- ****Location****
- ****First Seen****
- ****Observed****
- ****Description****

- [**Motivation**](#)
- [**Names**](#)
- [**Location**](#)
- [**First Seen**](#)
- [**Observed**](#)
- [**Backdoor Diplomacy: Overview and Activities**](#)
- [**BITTER APT Group**](#)
- [**BlackOasis APT Group**](#)
- [**BlackTech \(Circuit Panda, Radio Panda\)**](#)
- [**Blue Mockingbird - Cyber Threat Group**](#)
 - [**_Description_**](#)
 - [**_Motivation_**](#)
 - [**_Names_**](#)
 - [**_Location_**](#)
 - [**_First Seen_**](#)
 - [**_Observed Activities_**](#)
- [**Description**](#)
- [Description:](#) 📄
- [Motivation:](#) 📍
- [Names:](#) 📋
- [Location:](#) 📍
- [First Seen:](#) 📅
- [Observed:](#) 📅
- [Techniques Used in all tactics](#)
- [Software Used by Chimera](#)
- [🗡️ Cleaver - Group Overview 🇸🇰](#)
 - [📄 Description:](#)
 - [📍 Motivation:](#)
 - [📋 Names:](#)
 - [📍 Location:](#)
 - [📅 First Seen:](#)
 - [📅 Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Cleaver](#)
- [🇷🇺 Cobalt Group - Group Overview 🇸🇰](#)
 - [📄 Description:](#)
 - [📍 Motivation:](#)
 - [📋 Names:](#)
 - [📍 Location:](#)
 - [📅 First Seen:](#)
 - [📅 Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Cobalt Group](#)
- [🇨🇳 Confucius - Group Overview 🇸🇰](#)
 - [📄 Description:](#)
 - [📍 Motivation:](#)
 - [📋 Names:](#)
 - [📍 Location:](#)
 - [📅 First Seen:](#)
 - [📅 Observed:](#)
- [Techniques Used in all tactics](#)

- [Software Used by Confucius](#)
- [Copy Kittens - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Copy Kittens](#)
- [CURILUM - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by CURILUM](#)
- [Dark Caracal - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Dark Caracal](#)
- [Darkhotel - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Darkhotel](#)
- [DarkHydruS - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by DarkHydruS](#)
- [DarkVishwa - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)

- [📄 First Seen:](#)
- [🕒 Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by DarkVishnya](#)
- [🐼 Deep Panda - Group Overview 🇸🇰](#)
 - [📄 Description:](#)
 - [👤 Motivation:](#)
 - [👥 Names:](#)
 - [📍 Location:](#)
 - [📄 First Seen:](#)
 - [🕒 Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Deep Panda](#)
- [🐉 Dragonfly - Group Overview 🇸🇰](#)
 - [📄 Description:](#)
 - [👤 Motivation:](#)
 - [👥 Names:](#)
 - [📍 Location:](#)
 - [📄 First Seen:](#)
 - [🕒 Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Dragonfly](#)
- [🐉 DragonOK - Group Overview 🇸🇰](#)
 - [📄 Description:](#)
 - [👤 Motivation:](#)
 - [👥 Names:](#)
 - [📍 Location:](#)
 - [📄 First Seen:](#)
 - [🕒 Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by DragonOK](#)
- [🌍 Earth Lusca - Group Overview 🇸🇰](#)
 - [📄 Description:](#)
 - [👤 Motivation:](#)
 - [👥 Names:](#)
 - [📍 Location:](#)
 - [📄 First Seen:](#)
 - [🕒 Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Earth Lusca](#)
- [🌲 Elderwood - Group Overview 🇸🇰](#)
 - [📄 Description:](#)
 - [👤 Motivation:](#)
 - [👥 Names:](#)
 - [📍 Location:](#)
 - [📄 First Seen:](#)
 - [🕒 Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Elderwood](#)
- [🔥 Ember Bear - Group Overview 🇸🇰](#)
 - [📄 Description:](#)

- [📍 Motivation:](#)
- [👤 Names:](#)
- [📍 Location:](#)
- [📅 First Seen:](#)
- [👁️ Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Ember Bear](#)
- [👤 Equation - Group Overview 👤](#)
 - [📄 Description:](#)
 - [📍 Motivation:](#)
 - [👤 Names:](#)
 - [📍 Location:](#)
 - [📅 First Seen:](#)
 - [👁️ Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Equation](#)
- [EXOTIC LILY - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by EXOTIC LILY](#)
- [Ferocious Kitten - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Ferocious Kitten](#)
- [FIN10 - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by FIN10](#)
- [FIN13 - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)

- [Software Used by FIN13](#)
- [FIN4 – Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by FIN4](#)
- [FIN5 – Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by FIN5](#)
- [FIN6 – Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by FIN6](#)
- [FIN7 – Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by FIN7](#)
- [FIN8 – Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by FIN8](#)
- [Fox Kitten – Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)

- [First Seen:](#)
- [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Fox-Kitten](#)
- [GALLIUM - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by GALLIUM](#)
- [Ballmaker - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Ballmaker](#)
- [Gamaredon Group - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Gamaredon Group](#)
- [GCMAN - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by GCMAN](#)
- [GOLD SOUTHERFIELD - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by GOLD SOUTHERFIELD](#)
- [Gordon Group - Group Overview](#)

- [Motivation:](#)
- [Names:](#)
- [Location:](#)
- [First Seen:](#)
- [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Gorgon Group](#)
- [Group5 - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Group5](#)
- [HAENILIM - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by HAENILIM](#)
- [HEXANE - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by HEXANE](#)
- [Higala - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Higala](#)
- [Inception - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)

- [Software Used by Inception](#)
- [IndigoZebra - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by IndigoZebra](#)
- [Indrik Spider - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Indrik Spider](#)
- [Ke3chang - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Ke3chang](#)
- [Kimsuky - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by Kimsuky](#)
- [LAPSUS\\$ - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics](#)
- [Software Used by LAPSUS\\$](#)
- [Lazarus Group - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)

- [Location:](#)
- [First Seen:](#)
- [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Lazarus Group](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by LazyScloter](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Leafminer](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Leviathan](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Lotus Blossom](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Machete](#)
- [APT - Group Overview](#)

- [Description:](#)
- [Motivation:](#)
- [Names:](#)
- [Location:](#)
- [First Seen:](#)
- [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Magic Hound](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by manuPass](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Matador](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Moafee](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Mofang](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)

- [Techniques Used in all Tactics](#)
- [Software Used by Molerats](#)
- [APT - Group Overview](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Moses Staff](#)
- [APT - Group Overview: MuddyWater](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by MuddyWater:](#)
- [APT - Group Overview: Mustang Panda](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Mustang Panda:](#)
- [APT - Group Overview: Naikon](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Naikon:](#)
- [APT - Group Overview: NEODYMIUM](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by NEODYMIUM:](#)
- [APT - Group Overview: Nomadic Optopus](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)

- [Location:](#)
- [First Seen:](#)
- [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Nemadric Octopus:](#)
- [APT - Group Overview: OllRig](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by OllRig:](#)
- [APT - Group Overview: Orangeworm](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Orangeworm:](#)
- [APT - Group Overview: Patchwork](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Patchwork:](#)
- [APT - Group Overview: PlityTiger](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by PlityTiger:](#)
- [APT - Group Overview: PLATINUM](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by PLATINUM:](#)
- [APT - Group Overview: POLONIUM](#)

- [Description:](#)
- [Motivation:](#)
- [Names:](#)
- [Location:](#)
- [First Seen:](#)
- [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by POLONIUM:](#)
- [APT - Group Overview: Poseidon Group](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [APT - Group Overview: PROMETHIUM](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by PROMETHIUM:](#)
- [APT - Group Overview: Putter Panda](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Putter Panda:](#)
- [APT - Group Overview: Rancor](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Rancor:](#)
- [APT - Group Overview: Rocks](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)

- [Software Used by Rocks:](#)
- [APT - Group Overview: RTM](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by RTM:](#)
- [APT - Group Overview: Sandworm Team](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Sandworm Team:](#)
- [APT - Group Overview: Scarlet Mimic](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Scarlet Mimic:](#)
- [APT - Group Overview: Scattered Spider](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Scattered Spider:](#)
- [APT - Group Overview: SideCopy](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by SideCopy:](#)
- [APT - Group Overview: Sidewinder](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)

- [First Seen:](#)
- [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Silewindar:](#)
- [APT - Group Overview: Silence](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Silence:](#)
- [APT - Group Overview: Silent Librarian](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Silent Librarian:](#)
- [APT - Group Overview: SilverTerror](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by SilverTerror:](#)
- [APT - Group Overview: Sowbug](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Sowbug:](#)
- [APT - Group Overview: Stealth Falcon](#)
 - [Description:](#)
 - [Motivation:](#)
 - [Names:](#)
 - [Location:](#)
 - [First Seen:](#)
 - [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Stealth Falcon:](#)
- [APT - Group Overview: Strider \(Associated with ProjectSauron\)](#)
 - [Description:](#)

- [Motivation:](#)
- [Names:](#)
- [Location:](#)
- [First Seen:](#)
- [Observed:](#)
- [Techniques Used in all tactics:](#)
- [Software Used by Strider \(Associated with ProjectSauron\):](#)
- [APT - Group Overview: Suckfly](#)

- [Description:](#)
- [Motivation:](#)
- [Names:](#)
- [Location:](#)
- [First Seen:](#)
- [Observed:](#)

- [Techniques Used in all tactics:](#)
- [Software Used by Suckfly:](#)

- [Description:](#)
- [Motivation:](#)
- [Names:](#)
- [Location:](#)
- [First Seen:](#)
- [Observed:](#)

- [Techniques Used in all tactics:](#)
- [Software Used by TA2541:](#)
- [APT - Group Overview: TA459](#)

- [Description:](#)
- [Motivation:](#)
- [Names:](#)
- [Location:](#)
- [First Seen:](#)
- [Observed:](#)

- [Techniques Used in all tactics:](#)
- [Software Used by TA459:](#)
- [Techniques Used in all Tactics](#)
- [Software Used by TA506](#)

- [Matrices Group Overview](#)
- [Techniques Used in all Tactics](#)
- [Software Used by Matrices](#)
- [TeamTNT - Group Overview](#)

- [Techniques Used in All Tactics](#)
- [Software Used by TeamTNT](#)
- [TEMPVales - Group Overview](#)
- [Techniques Used in All Tactics](#)

- [Software Used by TEMPVales](#)
- [The White Company - Group Overview](#)
- [Techniques Used in All Tactics](#)
- [Software Used by The White Company](#)

- [Threat Group-1314 - Group Overview](#)
- [Techniques Used in All Tactics](#)
- [Software Used by Threat Group-1314](#)
- [Thris - Group Overview](#)





- [Techniques Used in All Tactics](#)
- [Software Used by Thrip](#)
- [Toronto Team - Group Overview](#)
- [Techniques Used in All Tactics](#)
- [Software Used by Toronto Team](#)
- [Transparent Tribe - Group Overview](#)
- [Techniques Used in All Tactics](#)
- [Software Used by Transparent Tribe](#)
- [Tropic Trooper - Group Overview](#)
- [Techniques Used in All Tactics](#)
- [Software Used by Tropic Trooper](#)
- [Tulia - Group Overview](#)
- [Techniques Used in all tactics](#)
- [Software and Tools Used](#)
- [Volatile Cedar - Group Overview](#)
- [Techniques Used in all tactics](#)
- [Software Used by Volatile Cedar](#)
- [Volt Typhoon - Group Overview](#)
- [Techniques Used in all tactics](#)
- [Software Used by Volt Typhoon](#)

Admin@338 - Group Overview

Description:

Admin@338, also known as Temper Panda, is a China-based cyber threat group. This APT group has been active since at least 2014 and is primarily involved in information theft and espionage . They have a history of using newsworthy events as lures to deliver malware . Their targets have largely been organizations involved in financial , economic , and trade policy . The group has shown a particular interest in political and economic issues in Hong Kong  and China , targeting Hong Kong media companies  and pro-democracy movements .

Motivation:

The primary motivation of Admin@338 appears to be espionage , with a focus on collecting sensitive information  from targeted organizations . Their activities suggest an intent to gather intelligence related to financial, economic, and trade policies, as well as political movements , especially those related to Hong Kong's pro-democracy activities.

Names:








Admin@338 is known by several aliases , including Temper Panda , Team338, and Magnesium. These names have been attributed to the group by various cybersecurity organizations and researchers.

Location:

First Seen:

Admin@338 was first observed in 2014 .

Observed:

The group has been observed targeting sectors such as Defense , Financial , Government , Media , and Think Tanks . Geographically, their activities have been primarily focused on Hong Kong  and the USA .

Tools Used:

Admin@338 has used a variety of tools in their operations, including but not limited to:

- Bozok
- BUBBLEWRAP
- LOWBALL
- Poison Ivy
- Techniques for 'Living off the Land' (utilizing existing software or system tools to conduct malicious activities)

Their use of these tools demonstrates a capability to employ both publicly available RATs and sophisticated, non-public backdoors for their operations.

The Admin@338 APT group, identified on the MITRE ATT&CK framework as G0018, employs a range of sophisticated techniques in their cyber operations. Here's a detailed look at some of the key techniques used by this group:

- **Account Discovery (T1087.001):** Admin@338 actors have used commands following the exploitation of a machine with LOWBALL malware to enumerate user accounts. This includes commands like `net user >> %temp%\download` and `net user /domain >> %temp%\download`, which help them gather information about local and domain accounts on the compromised system.
- **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** After exploiting a machine with LOWBALL malware, the actors create a file containing a list of commands to be executed on the compromised computer. This technique allows them to perform various actions using the Windows command shell.
- **Exploitation for Client Execution (T1203):** Admin@338 has exploited client software vulnerabilities for execution, such as Microsoft Word CVE-2012-0158. This involves taking advantage of software vulnerabilities to execute arbitrary code.
- **File and Directory Discovery (T1083):** The group uses commands to obtain information about files and directories after exploiting a machine. This includes commands like `dir c:\ >> %temp%\download` and similar commands for other directories, which helps them understand the file system layout and locate files of interest.
- **Masquerading: Match Legitimate Name or Location (T1036.005):** Admin@338 actors have used commands to rename one of their tools to a benign file name, such as `ren "%temp%\upload" audiodg.exe`. This technique helps them evade detection by making their malicious tools appear legitimate.
- **Permission Groups Discovery: Local Groups (T1069.001):** They use commands like `net localgroup administrator >> %temp%\download` following the exploitation of a machine with LOWBALL malware to list local groups. This helps them identify administrative groups and other permission sets on the compromised system.
- **Phishing: Spearphishing Attachment (T1566.001):** Admin@338 has sent emails with

malicious Microsoft Office documents attached. This spearphishing technique is a common method for initial access, tricking users into opening malicious attachments.

- **System Information Discovery (T1082):** The actors use commands to obtain information about the operating system after exploiting a machine, such as `ver >> %temp%\download` and `systeminfo >> %temp%\download`. This provides them with detailed information about the compromised system.
- **System Network Configuration Discovery (T1016):** They acquire information about local networks using commands like `ipconfig /all >> %temp%\download` after exploiting a machine.
- **System Network Connections Discovery (T1049):** Admin@338 uses commands to display network connections, such as `netstat -ano >> %temp%\download`, which helps them understand the network environment of the compromised system.
- **System Service Discovery (T1007):** They use commands like `net start >> %temp%\download` to obtain information about services running on the system.
- **User Execution: Malicious File (T1204.002):** The group attempts to get victims to launch malicious Microsoft Word attachments delivered via spearphishing emails, a tactic that relies on user interaction to execute the malicious payload.

The Admin@338 APT group, as identified in the MITRE ATT&CK framework, uses a variety of software tools in their cyber operations. Here's a summary of the key software tools and the associated techniques they employ:

- **BUBBLEWRAP (S0043):**
 - Techniques: Application Layer Protocol: Web Protocols, Non-Application Layer Protocol, System Information Discovery.
 - BUBBLEWRAP is a multifunctional tool used for various purposes, including web protocol communication and system information gathering.
- ******
 - Technique: System Network Configuration Discovery.
 - This common Windows utility is used by Admin@338 to discover network configuration details on compromised systems.
- **LOWBALL (S0042):**
 - Techniques: Application Layer Protocol: Web Protocols, Ingress Tool Transfer, Web Service: Bidirectional Communication.
 - LOWBALL is a malware tool used for establishing web-based communication channels and transferring tools onto targeted systems.
- **Net (S0039):**
 - Techniques: Account Discovery (Domain and Local Account), Create Account (Local and Domain Account), Indicator Removal (Network Share Connection Removal), Network Share Discovery, Password Policy Discovery, Permission Groups Discovery (Domain and Local Groups), Remote Services (SMB/Windows Admin Shares), Remote System Discovery, System Network Connections Discovery, System Service Discovery, System Services (Service Execution), System Time Discovery.
 - The Net utility is used extensively for a range of activities from account discovery to system service manipulation.
- **netstat (S0104):**
 - Technique: System Network Connections Discovery.
 - Admin@338 uses netstat to discover network connections on compromised systems, aiding in their reconnaissance efforts.
- **PoisonIvy (S0012):**
 - Techniques: Application Window Discovery, Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder, Active Setup), Command and Scripting Interpreter (Windows Command Shell), Create or Modify System Process (Windows Service), Data from Local System, Data Staged (Local Data Staging), Encrypted Channel (Symmetric

Obfuscated Files or Information, Process Injection (Dynamic-link Library Injection), Rootkit.

- PoisonIvy is a well-known Remote Access Trojan (RAT) used for a wide range of malicious activities, from data theft to system manipulation.
- **SystemInfo (S0096):**
 - Technique: System Information Discovery.
 - This tool is used to gather detailed information about the operating system and hardware configurations of compromised systems.

In summary, Admin@338 is a sophisticated cyber espionage group, primarily focusing on political and economic intelligence gathering, with a strategic emphasis on targets in Hong Kong and the United States. Their operations, marked by a diverse array of cyber tools and techniques, underscore their significant role in the realm of cyber threats and espionage. Demonstrating a highly sophisticated approach, Admin@338 leverages various methods to infiltrate, explore, and extract valuable information from their targets, showcasing their adeptness in navigating and exploiting digital environments for espionage purposes.

🌐 Ajax Security Team - Group Overview 🇮🇷

📄 Description:

Ajax Security Team (AST), active since at least 2010, is a cyber threat group believed to be operating out of Iran 🇮🇷. Initially known for website defacement operations, by 2014, AST transitioned to malware-based cyber espionage campaigns 🕵️. Their primary targets have been the US defense industrial base 🏢 and Iranian users of anti-censorship technologies 🌐. The group is notably associated with Operation Saffron Rose.

💡 Motivation:

Ajax Security Team's shift from website defacement to cyber espionage indicates a strategic evolution in their objectives 📄. Their focus on the US defense industry 🏢 and anti-censorship users in Iran 🇮🇷 suggests motivations rooted in political and strategic espionage, likely aimed at gaining intelligence 🕵️ and exerting control over information flow 🌐.

🔥 Names:

Apart from Ajax Security Team, the group is associated with several other names 🏢, including Operation Woolen-Goldfish, AjaxTM, Rocket Kitten, Flying Kitten, and Operation Saffron Rose. These aliases reflect the diverse nature of their operations and campaigns.

🌐 Location:

The group is believed to be based in Iran 🇮🇷, aligning with their targeting patterns and the geopolitical interests reflected in their activities 🌐.

📅 First Seen:

AST's activities date back to at least 2010 📅, marking over a decade of their presence in the

Observed Activities:

Ajax Security Team has conducted operations against the US defense industry 🇺🇸 and energy sectors of Middle Eastern countries 🇸🇦, including corporations like Saudi Aramco and Qatar's RasGas. Their shift to more sophisticated cyber espionage tactics marks a significant evolution in their operational capabilities 📈.

Tools Used:

- **Stealer:** Developed by AST, Stealer is a powerful spyware capable of stealing sensitive information, including keystrokes and screenshots. It stores the data on the victim's computer before sending it to a command and control (C2) server.
- **Havij:** An automated SQL injection tool distributed by ITSecTeam, an Iranian security company. Released in 2010, Havij is known for its high success injection rate of over 95%. It offers both free and commercial editions and is considered a forerunner of automated SQL injection tools.

Techniques Used by Ajax Security Team:

- **Credentials from Password Stores: Credentials from Web Browsers (T1555.003):**
 - The group has used FireMalv, a custom-developed malware, to collect passwords from the Firefox browser storage. This technique involves accessing and extracting stored credentials from web browsers.
- **Ingress Tool Transfer (T1105):**
 - Ajax Security Team has utilized Wrapper/Gholee, another custom-developed malware, which is capable of downloading additional malware onto the infected system. This technique is crucial for establishing a foothold and expanding control within the target system.
- **Input Capture: Keylogging (T1056.001):**
 - The group has deployed CWoogler and MPK, custom-developed malware, to record all keystrokes on an infected system. Keylogging is a common method for capturing sensitive information, including passwords and other confidential data.
- **Phishing: Spearphishing Attachment (T1566.001):**
 - Personalized spearphishing attachments have been used by Ajax Security Team. This method involves sending targeted emails with malicious attachments to trick victims into compromising their systems.
- **Phishing: Spearphishing via Service (T1566.003):**
 - The group has employed various social media channels to spearfish victims, using these platforms to deliver targeted phishing messages.
- **User Execution: Malicious File (T1204.002):**
 - Victims have been lured by Ajax Security Team into executing malicious files. This technique relies on social engineering to convince users to run files that compromise their systems.

Software Used by Ajax Security Team:








- **Havij (S0224):**
 - **Techniques:** Exploit Public-Facing Application.
 - Havij is an automated SQL injection tool known for its high success rate in exploiting vulnerabilities in web applications. It's used to gain unauthorized access to databases through SQL injection.
- **sqlmap (S0225):**
 - **Techniques:** Exploit Public-Facing Application.
 - Similar to Havij, sqlmap is another tool for automating the process of detecting and

exploiting SQL injection flaws. It is used to compromise databases and extract data from them.



In summary, the Ajax Security Team employs a combination of custom-developed malware and well-known exploitation tools to conduct their cyber espionage activities. Their techniques range from sophisticated phishing operations to keylogging and exploiting web application vulnerabilities, demonstrating their capability to adapt and employ various methods for intelligence gathering and system compromise.

ALLANITE - Group Overview


Description:

ALLANITE, also known as Palmetto Fusion, is a cyber espionage group that focuses on accessing business and industrial control (ICS) networks . The group conducts reconnaissance  and gathers intelligence, particularly in the United States  and United Kingdom  electric utility sectors . ALLANITE's operations are characterized by their focus on understanding operational environments and developing capabilities that could potentially disrupt electric utilities. However, their activities have so far been limited to information gathering without demonstrating any disruptive or damaging capabilities. The group is known for conducting malware-less operations , primarily leveraging legitimate and available tools in the Windows operating system .

Motivation:

The primary motivation of ALLANITE appears to be espionage , with a specific interest in the electric utility sector . Their activities suggest an intent to understand and potentially develop capabilities to disrupt operations in this sector. The group's focus on maintaining access to ICS networks indicates a strategic interest in the operational aspects of electric utilities.


Names:

ALLANITE is also known as Palmetto Fusion .




Location:

ALLANITE is a suspected Russian  cyber espionage group.

First Seen:

ALLANITE has been active at least since May 2017 , as reported by the industrial cybersecurity firm Dragos.

Observed:

ALLANITE has primarily targeted the electric utility sector within the United States  and the United Kingdom . Their tactics and techniques are reportedly similar to those of the Dragonfly group .

Tools Used:

ALLANITE uses email phishing campaigns and compromised websites, known as watering holes, to steal credentials and gain access to target networks. This includes collecting and distributing screenshots of industrial control systems. The group conducts operations without relying on traditional malware, instead using legitimate tools available in the Windows operating system. There are no specific malware families currently associated with ALLANITE.

techniques used by ALLANITE:

- **Drive-by Compromise (ICS T0817):**
 - ALLANITE leverages watering hole attacks as a method to gain access to electric utilities. In these attacks, the group compromises websites frequently visited by their target audience. When users visit these infected sites, malware is silently downloaded onto their systems, providing ALLANITE with unauthorized access.
- **Screen Capture (ICS T0852):**
 - The group has been identified collecting and distributing screenshots of ICS systems, such as Human-Machine Interfaces (HMIs). This technique allows them to visually capture and analyze information displayed on screens within the targeted industrial control systems, providing insights into operational details and potentially sensitive data.
- **Spearphishing Attachment (ICS T0865):**
 - ALLANITE has utilized spearphishing emails to gain access to environments within the energy sector. These emails contain malicious attachments that, when opened, can install malware or provide backdoor access to the attackers. Spearphishing is a targeted approach, often using social engineering to trick specific individuals into compromising their systems.
- **Valid Accounts (ICS T0859):**
 - The group also uses credentials collected through phishing and watering hole attacks. By obtaining legitimate user credentials, ALLANITE can gain unauthorized access to systems and networks while appearing as a legitimate user. This technique reduces the likelihood of detection and allows for deeper penetration into the targeted infrastructure.

These techniques demonstrate ALLANITE's sophisticated approach to cyber espionage, focusing on stealth and the effective use of social engineering and legitimate credentials to infiltrate and gather intelligence from critical infrastructure sectors. Their methods underscore the importance of robust cybersecurity measures in protecting against such advanced threat actors.

Andariel - Group Overview

Description:

Andariel is a North Korean state-sponsored threat group that has been active since at least 2009. The group is primarily focused on conducting destructive attacks against South Korean government agencies 🏛️, military organizations ⚔️, and various domestic companies 🏢. Additionally, Andariel has engaged in cyber financial operations targeting ATMs 🏧, banks 🏦, and cryptocurrency exchanges 📈. Their notable activities include Operation Black Mine, Operation GoldenAxe, and Campaign Rifle. Andariel is considered a subset of the Lazarus Group 🇰🇷 and is attributed to North Korea's Reconnaissance General Bureau 🏢. It's important to note that North

Korean group definitions often overlap, and some security researchers report on North Korean state-sponsored cyber activity under the name Lazarus Group instead of tracking individual clusters or subgroups.

💡 Motivation:

Andariel's operations are motivated by both political and financial objectives. Their attacks against South Korean entities are likely driven by geopolitical tensions between North and South Korea 🌐. The cyber financial operations suggest a motive of financial gain 💰, particularly through attacks on financial institutions and cryptocurrency platforms.

🔥 Names:

Andariel is primarily known by this name but is also recognized as a subset of the Lazarus Group 📄.

🌐 Location:

Andariel is a North Korean state-sponsored group 🇰🇵.

📅 First Seen:

The group has been active since at least 2009 📅.

👁️ Observed:

Andariel has been observed targeting South Korean government agencies, military organizations, domestic companies, ATMs, banks, and cryptocurrency exchanges 🏦🏢🏦🏦🏦. Their operations have included both destructive attacks and cyber financial crimes.

🔧 Tools Used:

Specific tools used by Andariel were not detailed in the provided source. However, given their affiliation with the Lazarus Group and the nature of their operations, it is likely that they use a range of sophisticated cyber tools and techniques for both destructive attacks and financial theft 📡.

Techniques Used by Andariel:

- Data from Local System (T1005): Andariel has been known to collect a large number of files from compromised network systems for later extraction.
- Drive-by Compromise (T1189): The group uses watering hole attacks, often with zero-day exploits, to gain initial access to victims within specific IP ranges.
- Exploitation for Client Execution (T1203): Andariel exploits numerous ActiveX vulnerabilities, including zero-days, for executing malicious code on victim systems.
- Gather Victim Host Information: Software (T1592.002): They insert malicious scripts within compromised websites to collect information such as browser type, system language, Flash Player version, and more.

- **Gather Victim Network Information: IP Addresses (T1590.005):** The group's watering hole attacks are tailored to specific IP address ranges.
- **Ingress Tool Transfer (T1105):** Andariel downloads additional tools and malware onto compromised hosts.
- **Obfuscated Files or Information: Steganography (T1027.003):** The group has hidden malicious executables within PNG files.
- **Obtain Capabilities: Malware (T1568.001):** They use a variety of publicly available remote access Trojans (RATs) for their operations.
- **Phishing: Spearphishing Attachment (T1566.001):** Andariel conducts spearphishing campaigns with malicious Word or Excel attachments.
- **Process Discovery (T1057):** The group uses the tasklist command to enumerate processes and find specific strings.
- **System Network Connections Discovery (T1049):** Andariel uses the netstat -naop tcp command to display TCP connections on a victim's machine.
- **User Execution: Malicious File (T1204.002):** They attempt to lure victims into enabling malicious macros within email attachments.

Software Used by Andariel:

- **gh0st RAT (S0032):**
 - **Techniques:** This RAT is used for a range of activities including boot or logon autostart execution, command and scripting interpreter, creating or modifying system processes, data encoding, deobfuscating/decoding information, dynamic resolution, encrypted channels, hijack execution flow, indicator removal, ingress tool transfer, input capture, process discovery, process injection, query registry, screen capture, shared modules, system information discovery, and more.
- **Rifdoor (S0433):**
 - **Techniques:** Rifdoor is employed for boot or logon autostart execution, encrypted channels, obfuscated files or information, phishing via spearphishing attachments, system information discovery, system network configuration discovery, system owner/user discovery, and user execution of malicious files.

In summary, Andariel's cyber operations are characterized by a diverse range of sophisticated techniques and software tools. These include exploiting vulnerabilities, conducting spearphishing campaigns, using steganography for obfuscation, and employing RATs like gh0st RAT and Rifdoor. Their approach demonstrates a high level of sophistication and adaptability in executing cyber espionage and cyber warfare activities.

Aoqin Dragon: A Suspected Chinese Cyber Espionage Threat Group

Description:

Aoqin Dragon is a cyber espionage group suspected to be of Chinese origin 🇨🇳. Active since at least 2013, they have primarily targeted government 🏛️, education 🎓, and telecommunication organizations 📡 in Australia 🇦🇺, Cambodia 🇰🇲, Hong Kong 🇭🇰, Singapore 🇸🇬, and Vietnam 🇻🇳. The group is known for its sophisticated cyber operations, focusing on espionage 🕵️ and information theft 📁. Aoqin Dragon is noted for its use of document exploits 📄 and fake removable devices, such as USB drives 🗑️, for initial access into target systems.

Motivation:

The primary motivation of Aeqin Dragon appears to be espionage 🕵️, with a focus on collecting sensitive information 📁 from targeted organizations. Their activities suggest an intent to gather intelligence related to government, education, and telecommunication sectors 🏢🎓📶 in Southeast Asia and Australia.

🏠 Names:

Aeqin Dragon is also potentially associated with UNC94, based on similarities in malware, infrastructure, and targets 🏢.

🌐 Location:

The group is believed to be based in China 🇨🇳.

📅 First Seen:

Aeqin Dragon has been active since at least 2013 📅.

👁️ Observed:

The group has targeted a variety of sectors, with a particular focus on government, education, and telecommunication organizations 🏢🎓📶 in Southeast Asia and Australia. Their operations are characterized by the use of sophisticated cyber techniques and tools 🛠️.

🔧 Tools Used:

Aeqin Dragon employs a range of tools in their operations, including document exploits 📄 and fake removable devices like USB drives 🗂️. These tools are used for initial access and subsequent operations within the target networks 🏢🔒.

Aeqin Dragon: Techniques and Software

Techniques Used by Aeqin Dragon:

- Develop Capabilities: Malware (T1587.001): Aeqin Dragon has developed custom malware, including Mongall and Heyoka Backdoor, for their cyber operations.
- Exploitation for Client Execution (T1203): The group has exploited vulnerabilities like CVE-2012-0158 and CVE-2010-3333 to execute code on targeted systems.
- File and Directory Discovery (T1083): They have utilized scripts to identify specific file formats, including Microsoft Word documents, within target networks.
- Lateral Tool Transfer (T1570): Aeqin Dragon spreads malware across target networks by copying modules into folders disguised as removable devices.
- Masquerading: Match Legitimate Name or Location (T1036.005): The group has used fake icons, such as antivirus and external drive symbols, to disguise malicious payloads.
- Obfuscated Files or Information: Software Packing (T1027.002): They have employed the Themida packer to obfuscate their malicious payloads, making detection more difficult.
- Obtain Capabilities: Tool (T1588.002): Aeqin Dragon obtained and modified the Heyoka open-source exfiltration tool for their operations.
- Replication Through Removable Media (T1091): The group has used a dropper that employs a worm infection strategy, using removable devices to penetrate secure network environments.

- User Execution: Malicious File (T1204.002): They have tricked victims into opening weaponized documents and fake external drives or antivirus software to execute malicious payloads.

Software Used by Aojin Dragon:

- Heyoka Backdoor (S1027):
 - Techniques: Application Layer Protocol: DNS, Boot or Logon Autostart Execution, Deobfuscate/Decode Files or Information, File and Directory Discovery, Indicator Removal, Masquerading, Obfuscated Files or Information, Peripheral Device Discovery, Process Discovery, Process Injection, Protocol Tunneling, System Binary Proxy Execution, System Information Discovery, System Service Discovery, User Execution.
 - Heyoka Backdoor is a sophisticated tool used for various malicious activities, including data exfiltration and system information discovery.
- Mongall (S1026):
 - Techniques: Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution, Data Encoding, Data from Local System, Deobfuscate/Decode Files or Information, Encrypted Channel, Exfiltration Over C2 Channel, Ingress Tool Transfer, Obfuscated Files or Information, Peripheral Device Discovery, Process Injection, System Binary Proxy Execution, System Information Discovery, User Execution.
 - Mongall is a multifunctional malware used for data theft, system information discovery, and maintaining persistent access in compromised systems.

Aojin Dragon's use of these techniques and software tools demonstrates their sophisticated approach to cyber espionage. They leverage a variety of methods to infiltrate, explore, and extract valuable information from their targets, showcasing their adeptness in navigating and exploiting digital environments for espionage purposes.

Description:

APT-C-36, also known as Blind Eagle, is an Advanced Persistent Threat (APT) group suspected to originate from South America. Since April 2018, they have been actively targeting Colombian government institutions and significant corporations in the financial sector, petroleum industry, professional manufacturing, and others.

Motivation:

The primary motivation of APT-C-36 appears to be espionage and intelligence gathering, focusing on government and corporate entities. Their consistent targeting of specific sectors suggests a strategic intent to collect sensitive information for political or economic advantage.

Names:

- APT-C-36
- Blind Eagle

Location:

The group is suspected to be based in South America.

First Seen:

APT-C-36's activities were first observed in April 2018.

Observed:

The group has targeted Colombian government institutions and major corporations across

various sectors, including finance, petroleum, and manufacturing.

Tools Used:

APT-C-36 has used a variety of tools in their campaigns, including:

- Imminent Monitor RAT
- LimeRAT

Techniques Used by APT-C-36:

- Command and Scripting Interpreter: Visual Basic (T1059.005): Embedding VBScript within malicious Word documents that execute upon opening.
- Ingress Tool Transfer (T1105): Downloading binary data from a specified domain after opening a malicious document.
- Masquerading: Masquerade Task or Service (T1036.004): Disguising scheduled tasks as those used by Google.
- Non-Standard Port (T1571): Using port 4050 for C2 communications.
- Obfuscated Files or Information (T1027): Using ConfuserEx to obfuscate variants of Imminent Monitor, compress payloads, and password-protect email attachments for evasion.
- Obtain Capabilities: Tool (T1588.002): Utilizing a modified variant of Imminent Monitor.
- Phishing: Spearphishing Attachment (T1566.001): Employing spearphishing emails with password-protected RAR attachments.
- Scheduled Task/Job: Scheduled Task (T1053.005): Using macro functions to set scheduled tasks, disguised as those used by Google.
- User Execution: Malicious File (T1204.002): Prompting victims to accept macros to execute the payload.

Software Used by APT-C-36 (Blind Eagle)

Imminent Monitor (ID: S0434)

Imminent Monitor is a sophisticated Remote Access Trojan (RAT) used by APT-C-36 in their cyber operations. This tool exhibits a wide array of capabilities, making it a versatile choice for the group's espionage activities. The key techniques associated with Imminent Monitor include:

- Audio Capture: Ability to record audio from the compromised system's microphone.
- Command and Scripting Interpreter: Executing commands and scripts for various malicious purposes.
- Credentials from Password Stores: Credentials from Web Browsers: Extracting stored credentials from web browsers.
- Deobfuscate/Decode Files or Information: Unraveling obfuscated data or files to reveal their true content.
- Exfiltration Over C2 Channel: Transmitting stolen data back to the command and control (C2) server.
- File and Directory Discovery: Scanning the compromised system to locate files and directories of interest.
- Hide Artifacts: Hidden Files and Directories: Concealing files and directories to evade detection.
- Impair Defenses: Disable or Modify Tools: Disabling or altering security tools to prevent detection.
- Indicator Removal: File Deletion: Deleting files to remove evidence of the intrusion.
- Input Capture: Keylogging: Recording keystrokes to capture sensitive information like passwords and other credentials.
- Native API: Using native system application programming interfaces for various malicious activities.
- Obfuscated Files or Information: Employing techniques to make files or information difficult to analyze.

- Process Discovery: Identifying and analyzing running processes on the compromised system.
- Remote Services: Remote Desktop Protocol: Utilizing RDP for remote access and control over the compromised system.
- Resource Hijacking: Misusing system resources for malicious purposes, such as cryptocurrency mining.
- Video Capture: Recording video from the compromised system's camera.

Imminent Monitor's diverse functionalities enable APT-C-36 to conduct comprehensive espionage operations, ranging from data theft to surveillance. Its ability to remain undetected and manipulate system processes makes it a potent tool for cyber espionage campaigns.

APT1 (Advanced Persistent Threat 1) 🇺🇸

Description:

APT1, also known as Comment Crew or Comment Group, is a cyber espionage group believed to be associated with the Chinese military. This group is known for its sophisticated cyber operations and has been implicated in numerous cyber espionage campaigns targeting a wide range of industries and government entities around the world. 🇨🇳🇺🇸🇩🇪🇬🇧

Motivation:

APT1's primary motivation appears to be cyber espionage, with a focus on intellectual property theft and gaining strategic advantages in various industries. Their activities suggest an intent to gather sensitive information for economic and political gain. 🇨🇳🇺🇸🇩🇪🇬🇧🏛️

Names:

APT1 is also known as Comment Crew or Comment Group. These names have been attributed to the group by various cybersecurity organizations and researchers. 🇨🇳🇺🇸

Location:

The group is believed to be based in China. 🇨🇳

First Seen:

APT1 has been active for several years, but their activities gained significant attention in 2013 following a detailed report by Mandiant, a cybersecurity firm. 🇨🇳🇺🇸

Observed:

APT1 has targeted a broad range of corporations and government entities around the world, with a particular focus on English-speaking countries. Their targets span various industries, including information technology, telecommunications, aerospace, public administration, and others. 🇨🇳🇺🇸🇩🇪🇬🇧🏛️

Techniques Used by APT1:

- Account Discovery (T1067.001): APT1 used commands like net localgroup, net user, and net group to find accounts on the system.
- Acquire Infrastructure: Domains (T1583.001): They registered hundreds of domains for use in operations.
- Archive Collected Data: Archive via Utility (T1560.001): APT1 used RAR to compress files before moving them outside of the victim network.
- Automated Collection (T1119): They employed a batch script to perform discovery techniques and save results to a text file.
- Command and Scripting Interpreter: Windows Command Shell (T1059.003): The group used the Windows command shell for command execution and batch scripting for automation.
- Compromise Infrastructure: Domains (T1584.001): APT1 hijacked FQDNs associated with legitimate websites hosted by hop points.
- Data from Local System (T1005): They collected files from local victim systems.
- Email Collection (T1114.001 and T1114.002): APT1 used GETMAIL and MAPIGET utilities to steal emails from Outlook .pst files and Exchange servers.
- Establish Accounts: Email Accounts (T1585.002): They created email accounts for social engineering, phishing, and domain registration.
- Masquerading: Match Legitimate Name or Location (T1036.005): Malware was named after legitimate processes like AcroRD32.exe to evade detection.
- Network Share Discovery (T1135): APT1 listed connected network shares.
- Obtain Capabilities: Malware and Tool (T1588.001 and T1588.002): They used publicly available malware and open-source tools for privilege escalation.
- OS Credential Dumping: LSASS Memory (T1003.001): APT1 used Mimikatz for credential dumping.
- Phishing: Spearphishing Attachment and Link (T1566.001 and T1566.002): They conducted spearphishing campaigns with malicious attachments and links.
- Process Discovery (T1057): APT1 gathered a list of running processes using tasklist /v.
- Remote Services: Remote Desktop Protocol (T1021.001): They used RDP during operations.
- System Network Configuration Discovery (T1016): APT1 used ipconfig /all to gather network configuration information.
- System Network Connections Discovery (T1049): They used net use to get a listing of network connections.
- System Service Discovery (T1007): APT1 used net start and tasklist to list services on the system.
- Use Alternate Authentication Material: Pass the Hash (T1550.002): They used pass the hash techniques.

Software Used by APT1:

- BISCUIT: Used for command execution, screen capture, keylogging, and other functions.
- Cachedump: For dumping cached domain credentials.
- CALENDAR: Employed for bidirectional communication.
- GLOOXMAIL: Used for web-based bidirectional communication.
- gsecdump: For dumping SAM and LSA secrets.
- Ipconfig: To discover network configuration.
- Lsass: For dumping LSASS memory.
- Mimikatz: A versatile tool for credential dumping and manipulation.
- Net: Used for account discovery, network share discovery, and more.

- Pass-the-Hash Toolkit: Employed for pass-the-hash attacks.
- PoisonIvy: A RAT used for data exfiltration and command execution.
- PsExec: For lateral movement and remote service execution.
- pwdump: For dumping SAM credentials.
- Seasalt: Used for web protocol communication and other functions.
- Tasklist: For process and service discovery.
- WEBC2: Employed for command execution and data transfer.
- xCmd: Used for service execution.

In summary, APT1 utilized a wide array of techniques and software tools, ranging from basic command-line utilities to sophisticated malware and credential dumping tools. Their operations demonstrate a high level of sophistication and a broad capability to infiltrate, explore, and exfiltrate data from targeted systems.

APT12 (IXESHE, Numbered Panda, Group 22) 🇨🇳

Description

APT12, also known as IXESHE, Numbered Panda, and Group 22, is a threat actor primarily targeting organizations in Japan, Taiwan, and other parts of East Asia. Their activities mainly focus on espionage and have been directed towards electronics manufacturers and telecommunications companies. 🌐🔍📡

Motivation

The primary motivation of APT12 is espionage. They have been involved in extensive cyber espionage campaigns, targeting sensitive information from various organizations. 🕵️🔍📡

Names

APT12 is known by several aliases:

- IXESHE
- Numbered Panda
- Group 22
- BeeBus
- DynCalc
- Calc Team
- DNSCalc
- Crimson Iron
- BRONZE GLOBE

Location

APT12 is believed to be based in China. 🇨🇳

First Seen

The group has been active for several years, with notable activity traced back to at least 2012.

Observed Activities

APT12 has conducted numerous spear-phishing attacks and has been associated with various malware families, including:

- win.etumbot
- win.rapid_stealer
- win.threebyte
- win.waterspout

APT12 (IXESHE, Numbered Panda, Group 22) Techniques and Software

Techniques Used

- **Dynamic Resolution: DNS Calculation (T1568.003)**
 - APT12 has employed DNS Calculation techniques, manipulating IP address octets to determine command and control (C2) port numbers.
- **Exploitation for Client Execution (T1203)**
 - The group exploited various vulnerabilities in Microsoft Office (CVE-2009-3129, CVE-2012-0158), Adobe Reader, and Flash (CVE-2009-4324, CVE-2009-0927, CVE-2011-0609, CVE-2011-0611) for execution.
- **Phishing: Spearphishing Attachment (T1566.001)**
 - APT12 sent emails with malicious attachments, including Microsoft Office documents and PDFs, as part of spearphishing campaigns.
- **User Execution: Malicious File (T1204.002)**
 - They attempted to trick victims into opening malicious Microsoft Word and PDF attachments sent via spearphishing.
- **Web Service: Bidirectional Communication (T1102.002)**
 - The group used blogs and WordPress platforms for their C2 infrastructure.

Software Used

- HTRAN (S0040)
 - Techniques: Process Injection, Proxy, Rootkit.
 - HTRAN is used to obscure the location of their C2 servers.
- Ixeshe (S0015)
 - Techniques: Various, including Application Layer Protocol: Web Protocols, Data Encoding, File and Directory Discovery, Indicator Removal, and System Information Discovery.
 - Ixeshe is a malware family associated with APT12, known for its versatility and capability to perform a wide range of functions.
- RIPTIDE (S0003)
 - Techniques: Application Layer Protocol: Web Protocols, Encrypted Channel: Symmetric Cryptography.
 - RIPTIDE is another malware tool used by APT12, known for its encrypted communication capabilities.

APT12's use of diverse techniques and sophisticated software highlights their capability to conduct complex cyber espionage operations. Their methods include exploiting software vulnerabilities, spearphishing, and utilizing advanced malware, all aimed at infiltrating target

APT16: Overview and Activities

Description

APT16 is a China-based threat group known for spearphishing campaigns targeting organizations primarily in Japan and Taiwan. The group's activities focus on government, financial services, media, and high technology industry sectors. APT16 is believed to be closely aligned with Chinese nation-state activities.

Motivation

The primary motivation of APT16 appears to be espionage, gathering intelligence from targeted sectors and organizations that align with the interests of the Chinese state.

Names: -

Location

APT16 is based in China.

First Seen: -

Observed Activities

APT16 has been responsible for:

- Spear phishing attacks.
- Using compromised legitimate sites as staging servers for second-stage payloads.
- Delivering malware-laden Microsoft Word documents exploiting vulnerabilities like CVE-2015-1701.

APT16: Techniques and Software Used

Techniques Used by APT16

- Compromise Infrastructure: Server (Enterprise T1584.004)
 - Use: APT16 has demonstrated the capability to compromise legitimate websites, using them as staging servers for hosting their second-stage payloads. This technique involves breaching the security of a web server and then using it to store and distribute malware or other malicious tools. By leveraging legitimate infrastructure, APT16 can evade detection and increase the success rate of their attacks.

Software Used by APT16

- ELMER Backdoor (Software ID: S0064)
 - Techniques:
 - Application Layer Protocol: Web Protocols: ELMER uses standard web protocols for communication, which helps it blend in with normal traffic and avoid detection.
 - File and Stream: Disguise: The backdoor is capable of operating through files

and directories on the compromised system, allowing APT16 to locate and exfiltrate sensitive information.

- **Process Discovery:** ELMER can enumerate running processes on the infected system, providing insights into the operational environment and potentially identifying security tools that need to be evaded or disabled.

Summary

APT16, a group with suspected ties to China, employs sophisticated techniques and custom software to conduct espionage-focused cyber operations. Their use of compromised legitimate websites for staging attacks highlights their ability to adapt and mask their activities within normal network traffic. The ELMER backdoor, a key tool in their arsenal, provides them with capabilities essential for reconnaissance and data exfiltration within targeted networks.

APT17 Overview

Description

APT17, also known as Deputy Dog and Axiom, is a Chinese-based threat actor group. It is sponsored by the Chinese Ministry of State Security and has conducted malicious attacks against government and industry within the United States. APT17 targets various industry sectors, including mining, legal, information technology, and the defense industry. The group is known for using sophisticated techniques, including leveraging Microsoft's TechNet blog for command-and-control operations by creating bogus profiles and posting encoded CNC within technical forums. This method, known as "hiding in plain sight," helps obfuscate their identity and makes detection less likely.

Motivation

APT17 primarily engages in espionage activities. They target U.S. government entities, the defense industrial base, law firms, information technology companies, resource extraction companies, and non-governmental organizations. Their operations are believed to be carried out on-demand for the Jinan bureau of the Chinese Ministry of State Security.

Names

- APT17
- Deputy Dog
- Axiom

Location

The group is believed to be operating out of China, specifically as contractors for the Jinan bureau of the Chinese Ministry of State Security.

First Seen: -

Observed

APT17 has been observed targeting a wide range of sectors in the United States, focusing on espionage.

APT17 Techniques and Software Used

Techniques Used by APT17

- **Acquire Infrastructure: Web Services (T1583.006)**
 - **Usage:** APT17 created profile pages on Microsoft TechNet, which were utilized as command-and-control (C2) infrastructure. This innovative approach allowed them to hide their C2 communications in plain sight, blending in with legitimate traffic and making detection more challenging.
- **Establish Accounts (T1585)**
 - **Usage:** The group meticulously crafted and maintained profile pages on Microsoft TechNet. To enhance the credibility of these pages, APT17 added detailed biographical sections and actively participated in forum threads. This activity was part of their strategy to establish a legitimate-looking online presence, which was crucial for their C2 operations and for maintaining a low profile.

Software Used by APT17

- **BLACKCOFFEE (S0069)**
 - **Techniques:**
 - **Command and Scripting Interpreter: Windows Command Shell:** BLACKCOFFEE used the Windows Command Shell for executing commands.
 - **File and Directory Discovery:** The malware could discover files and directories on the infected system.
 - **Indicator Removal: File Deletion:** BLACKCOFFEE had capabilities to delete files, helping to cover its tracks.
 - **Multi-Stage Channels:** It utilized multi-stage channels for communication, adding complexity to its operations.
 - **Process Discovery:** The malware could discover processes running on the system.
 - **Web Service: Dead Drop Resolver:** BLACKCOFFEE used web services as a means to resolve dead drops.
 - **Web Service: Bidirectional Communication:** It was capable of bidirectional communication over web services, enhancing its ability to control compromised systems and exfiltrate data.

Additional Insights

- APT17's use of Microsoft TechNet for C2 infrastructure is a notable example of their innovative tactics. By embedding encoded command-and-control IP addresses in valid Microsoft TechNet profile pages and forum threads, they effectively masked their malicious activities.
- The BLACKCOFFEE malware's diverse capabilities, including command execution, file and process discovery, and sophisticated communication methods, highlight APT17's technical proficiency and the advanced nature of their operations.

These techniques and tools reflect APT17's sophisticated approach to cyber espionage, emphasizing stealth and long-term access to targeted networks.

APT18: Overview and Details

Description

APT18, also known as Dynamite Panda, Threat Group-0416, Wexby, and Scandium, is a Chinese nation-state-aligned threat group. It has been active since approximately 2009 and is believed to be directly supported by the Chinese People's Liberation Navy. APT18 has targeted a broad

mix of industry sectors, including manufacturing, technology, government, healthcare, defense, telecommunications, and human rights groups, primarily focusing on organizations in North America, especially the United States.

Motivation

The primary motivation of APT18 appears to be espionage and information theft. They have been involved in medical espionage, exfiltrating patient data from medical device databases, and stealing intellectual property rights, including advanced proprietary designs. Their activities seem to be aimed at advancing China's industries at the expense of U.S. industries.

Names

- Dynamite Panda
- Threat Group-0416
- Wekby
- Scandium

Location

APT18 primarily targets organizations in North America, with a specific focus on the United States.

First Seen

The group has been active since approximately 2009.

Observed Activities

APT18 has been very visible in attacks on the healthcare sector, including a significant data breach in a community health systems campaign, resulting in the theft of over 4.5 million patients' medical data. They have exploited vulnerabilities in various software, including a zero-day vulnerability (CVE-2015-5119), and launched phishing campaigns against multiple industry sectors.

APT18 Techniques and Software Used

Techniques Used by APT18

- Application Layer Protocol: Web Protocols (T1071.001): APT18 uses HTTP for command and control (C2) communications.
- Application Layer Protocol: DNS (T1071.004): They also utilize DNS for C2 communications.
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001): APT18 establishes persistence via the HKCU\Software\Microsoft\Windows\CurrentVersion\Run key.
- Command and Scripting Interpreter: Windows Command Shell (T1059.003): They use cmd.exe to execute commands on the victim's machine.
- External Remote Services (T1133): APT18 leverages legitimate credentials to log into external remote services.
- File and Directory Discovery (T1083): They can list file information for specific directories.
- Indicator Removal: File Deletion (T1070.004): APT18 deletes tools and batch files from victim systems.
- Ingress Tool Transfer (T1105): They can upload files to the victim's machine.
- Obfuscated Files or Information (T1027): APT18 obfuscates strings in their payloads.
- Scheduled Task/Job: At (T1053.002): They use the native at Windows task scheduler tool for execution on victim networks.

- System Information Discovery (T1082): APT18 collects system information from the victim's machine.
- Valid Accounts (T1078): They leverage legitimate credentials for logging into external remote services.

Software Used by APT18

- cmd (S0106): Used for command execution, file and directory discovery, file deletion, and system information discovery.
- gh0st RAT (S0032): A remote access trojan used for a variety of purposes including keylogging, screen capture, and process discovery.
- hcdLoader (S0071): Utilized for creating or modifying system processes.
- HTTPBrowser (S0070): A tool for DNS and web protocol communication, file and directory discovery, and obfuscating files.
- Pisloder (S0124): Used for DNS communication, file and directory discovery, and system information discovery.

APT18's techniques and software reflect a sophisticated approach to cyber espionage, leveraging a mix of custom tools and common administrative tools to maintain stealth and effectiveness in their operations.

APT19:

Description

APT19, also known as Deep Panda, KungFu Kittens, and PinkPanther, is a cyber espionage group believed to be operating out of China. The group is known for its sophisticated cyber attacks targeting a variety of sectors, including government, defense, financial, and telecommunications.

Motivation

APT19's primary motivation appears to be intelligence gathering and espionage, often targeting information that aligns with the Chinese government's interests. This includes sensitive political, economic, and military information.

Names

- Deep Panda
- KungFu Kittens
- PinkPanther

Location

APT19 is believed to be based in China.

First Seen:-

Observed

APT19 has been observed conducting cyber espionage campaigns against a range of targets, including government entities, defense contractors, and financial institutions.

APT19: Techniques and Software Used

Techniques Used by APT19

- Application Layer Protocol: Web Protocols (T1071.001): APT19 used HTTP for command and control (C2) communications and an HTTP malware variant for this purpose.
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001): They

established persistence by setting the Registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Windows Debug Tools-%LOCALAPPDATA%.

- Command and Scripting Interpreter (T1059): APT19 downloaded and launched code within SCT files.
- PowerShell (T1059.001): They used PowerShell commands to execute payloads.
- Create or Modify System Process: Windows Service (T1543.003): An APT19 Port 22 malware variant registers itself as a service.
- Data Encoding: Standard Encoding (T1132.001): An HTTP malware variant used Base64 to encode communications to the C2 server.
- Deobfuscate/Decode Files or Information (T1140): The HTTP malware variant decrypts strings using single-byte XOR keys.
- Drive-by Compromise (T1189): APT19 performed a watering hole attack on forbes.com in 2014.
- Hide Artifacts: Hidden Window (T1564.003): They used -W Hidden to conceal PowerShell windows.
- Hijack Execution Flow: DLL Side-Loading (T1574.002): They launched malware variants using legitimate executables that loaded malicious DLLs.
- Modify Registry (T1112): A Port 22 malware variant was used to modify several Registry keys.
- Obfuscated Files or Information (T1027): Base64 was used to obfuscate payloads and executed commands.
- Obtain Capabilities: Tool (T1588.002): APT19 obtained and used publicly-available tools like Empire.
- Phishing: Spearphishing Attachment (T1566.001): They sent spearphishing emails with malicious RTF and XLSM attachments.
- System Binary Proxy Execution: Regsvr32 (T1218.010) and Rundll32 (T1218.011): APT19 used these techniques for payload injection and to bypass application control techniques.
- System Information Discovery (T1082): They collected system architecture information using malware variants.
- System Network Configuration Discovery (T1016): The malware variants were used to collect MAC and IP addresses.
- System Owner/User Discovery (T1033): They used malware variants to collect the victim's username.
- User Execution: Malicious File (T1204.002): APT19 attempted to get users to launch malicious attachments delivered via spearphishing emails.

Software Used by APT19

- Cobalt Strike (S0154): A tool used for exploitation and post-exploitation tasks in victim networks. It includes capabilities like command execution, keylogging, file transfer, SOCKS proxying, privilege escalation, and more.
- Empire (S0363): A post-exploitation framework that provides a range of tools for system penetration, including PowerShell and Python capabilities, lateral movement, and various exploitation techniques.

APT19's operations demonstrate a high level of sophistication and a focus on stealth and persistence. Their use of a variety of techniques and software tools underscores their capability to conduct advanced cyber espionage campaigns.

APT28 (Fancy Bear)

Description

APT28, also known as Fancy Bear, is a sophisticated and well-resourced cyber espionage group. It is believed to be associated with the Russian military intelligence agency GRU. This group has been active since at least the mid-2000s and is known for its advanced cyber capabilities.

Motivation

APT28 primarily focuses on collecting intelligence in support of Russian political and military interests. The group has been involved in numerous high-profile cyber espionage campaigns, targeting government, military, security organizations, and other entities perceived as threats or of interest to the Russian government.

Names

- Fancy Bear
- Sofacy
- Sednit
- STRONTIUM
- Pawn Storm

Location

APT28 is believed to be based in Russia.

First Seen

The group has been active since at least the mid-2000s.

Observed

APT28 has been observed targeting a wide range of entities, including government and military organizations, security firms, media outlets, and political figures, particularly in countries that are geopolitically significant to Russia.

Techniques and Software Used by APT28 (Fancy Bear)

APT28, a highly sophisticated cyber espionage group, employs a wide array of techniques and software tools in its operations. Below is a detailed overview of some key techniques and software they have used:

Techniques

- Access Token Manipulation (T1134.001): APT28 exploited CVE-2015-1701 to access and copy the SYSTEM token for privilege escalation.
- Account Manipulation (T1098.002): They used PowerShell cmdlets to grant additional permissions to compromised accounts.
- Acquire Infrastructure (T1583): The group registered domains imitating various organizations and used Blogspot pages for credential harvesting.
- Active Scanning (T1595.002): APT28 performed large-scale scans to find vulnerable servers.
- Application Layer Protocol (T1071): They used protocols like HTTP, HTTPS, IMAP, POP3, and SMTP for communication in various implants.
- Archive Collected Data (T1560): APT28 used tools like WinRAR to archive and password-protect collected data.
- Boot or Logon Autostart Execution (T1547.001): They deployed malware that copied itself to the startup directory for persistence.
- Brute Force (T1110): APT28 performed brute force and password spraying attacks to obtain credentials.
- Command and Scripting Interpreter (T1059): The group used PowerShell scripts and Windows Command Shell for executing payloads.

- Data from information repositories (T1213): They collected files from Microsoft SharePoint services within target networks.
- Exploitation for Privilege Escalation (T1068): APT28 exploited various vulnerabilities like CVE-2014-4076 and CVE-2015-1701 for escalating privileges.
- Obfuscated Files or Information (T1027): The group encrypted and obfuscated payloads to avoid detection.
- Phishing (T1566): APT28 used spearphishing with malicious attachments or links to compromise targets.
- Remote Services (T1021.002): They used SMB/Windows Admin Shares for remote operations.
- System Binary Proxy Execution (T1218.011): APT28 executed payloads using commands like rundll32.

Software

- ADVSTORESHELL (S0045): A multifunctional toolkit used for various purposes including data staging and encrypted communication.
- Cannon (S0351): A tool used for tasks like screen capture and file discovery.
- CHOPSTICK (S0023): A sophisticated backdoor used for keylogging, screen capture, and proxying.
- CORESHELL (S0137): A backdoor used for encrypted communication and data encoding.
- Drovorub (S0502): A Linux-based malware used for data exfiltration and rootkit capabilities.
- JHUHUGIT (S0044): A backdoor used for clipboard data capture, screen capture, and process injection.
- Koadic (S0250): An advanced RAT (Remote Access Trojan) used for credential dumping and command execution.
- Mimikatz (S0002): A well-known tool used for credential dumping and pass-the-hash attacks.
- XTunnel (S0117): A network tunneling tool used for encrypted communication and proxying.
- Zebrocy (S0251): A malware toolkit used for data collection, screen capture, and network discovery.

APT28's arsenal of techniques and software demonstrates their capability to conduct sophisticated cyber espionage operations. Their methods range from exploiting system vulnerabilities to sophisticated social engineering attacks, underlining the need for robust cybersecurity measures.

Description of APT3:

APT3, also known as UPS Team, Buckeye, Gothic Panda, and TG-0110, is a sophisticated cyber espionage group believed to be based in China. This group has been active since at least 2009 and is known for its advanced persistent threats (APT) targeting a variety of sectors worldwide, including government, defense, technology, and telecommunications.

Motivation:

APT3's primary motivation appears to be espionage, likely driven by national and economic interests. Their activities suggest an intent to gather intelligence and potentially steal intellectual property or sensitive government and military information.

Names:

APT3 is known by various aliases, including UPS Team, Buckeye, Gothic Panda, and TG-0110.

Location:

APT3 is believed to be operating out of China.

First Seen:

APT3 has been active since at least 2009.

Observed:

APT3 has targeted a wide range of sectors, including government, defense, technology, and telecommunications, with a global focus. Their operations have been observed in multiple countries, indicating a broad and diverse set of targets.

APT3: Techniques and Software

Below is a detailed overview of the techniques and software used by APT3:

Techniques Used by APT3:

- Account Discovery (T1087.001): APT3 uses tools to gather information about local and global group users, power users, and administrators.
- Account Manipulation (T1098): The group adds created accounts to local admin groups to maintain elevated access.
- Archive Collected Data (T1560.001): APT3 compresses data before exfiltrating it.
- Boot or Logon Autostart Execution (T1547.001): Scripts are placed in the startup folder for persistence.
- Brute Force: Password Cracking (T1110.002): The group is known to brute force password hashes.
- Command and Scripting Interpreter (T1059): APT3 uses PowerShell and Windows Command Shell for various malicious activities.
- Create Account: Local Account (T1136.001): Known for creating or enabling accounts for access.
- Create or Modify System Process (T1543.003): The group creates new services for persistence.
- Credentials from Password Stores (T1555.003): APT3 dumps passwords from browsers.
- Data from Local System (T1005): Identifies Microsoft Office documents for exfiltration.
- Data Staged: Local Data Staging (T1074.001): Stages files for exfiltration in a single location.
- Event Triggered Execution (T1546.008): Replaces accessibility features binaries for persistence.
- Exfiltration Over C2 Channel (T1041): Uses tools that exfiltrate data over the C2 channel.
- Exploitation for Client Execution (T1203): Exploits vulnerabilities in Adobe Flash Player and Internet Explorer.
- File and Directory Discovery (T1083): Looks for files and directories on the local file system.
- Hide Artifacts: Hidden Window (T1564.003): Conceals PowerShell windows.
- Hijack Execution Flow: DLL Side-Loading (T1574.002): Known to side-load DLLs.
- Indicator Removal: File Deletion (T1070.004): Deletes files to remove traces.

- Input Capture: Keylogging (T1056.001): Records keystrokes in encrypted files.
- Multi-Stage Channels (T1104): Establishes SOCKS5 connections for C2.
- Non-Application Layer Protocol (T1095): Uses SOCKS5 for initial C2.
- Obfuscated Files or Information (T1027): Obfuscates files to evade detection.
- OS Credential Dumping (T1003.001): Dumps credentials from LSASS memory.
- Permission Groups Discovery (T1069): Enumerates permissions of Windows groups.
- Phishing: Spearphishing Link (T1566.002): Sends spearphishing emails with malicious links.
- Process Discovery (T1057): Lists currently running processes.
- Proxy: External Proxy (T1090.002): Establishes external proxy connections.
- Remote Services (T1021): Enables and uses Remote Desktop Protocol and SMB/Windows Admin Shares.
- Remote System Discovery (T1018): Detects the existence of remote systems.
- Scheduled Task/Job: Scheduled Task (T1053.005): Creates scheduled tasks for persistence.
- System Binary Proxy Execution: Rundll32 (T1218.011): Runs DLLs for execution.
- System Information Discovery (T1082): Gathers information about the local system.
- System Network Configuration Discovery (T1016): Gathers network information.
- System Network Connections Discovery (T1049): Enumerates current network connections.
- System Owner/User Discovery (T1033): Determines the system owner or user.
- Unsecured Credentials: Credentials In Files (T1552.001): Locates credentials in files.
- User Execution: Malicious Link (T1204.001): Lures victims into clicking malicious links.
- Valid Accounts: Domain Accounts (T1078.002): Leverages valid accounts for domain access.

Software Used by APT3:

- LaZagne (S0349): Used for various credential dumping techniques.
- OSInfo (S0165): A tool for account discovery, system information discovery, and more.
- PlugX (S0013): A multifunctional tool used for command execution, data exfiltration, and more.
- RemoteCMD (S0166): Facilitates remote command execution.
- schtasks (S0111): Used for creating scheduled tasks.
- SHOTPUT (S0063): A custom backdoor used for account discovery and other functions.

In summary, APT3 is a highly sophisticated group employing a wide range of techniques and custom software to conduct espionage and cyber operations. Their tactics demonstrate advanced capabilities in maintaining persistence, evading detection, and extracting sensitive information.

Description of APT 30 (Override Panda)

APT 30, also known as Override Panda, is a cyber espionage group suspected to be associated with the Chinese government. This group has been active since at least 2005 and is known for its decade-long operation focused predominantly on entities in Southeast Asia and India. APT 30 is notable for its sustained activity and regional focus, as well as its success in espionage despite maintaining relatively consistent tools, tactics, and infrastructure over a long period.

Motivation

The primary objective of APT 30 appears to be data theft, particularly targeting government and commercial entities holding key political, economic, and military information about the region. Unlike many cyber threat groups, APT 30 does not seem to be motivated by financial gain, as they have not been observed targeting data that can be readily monetized, such as credit card

sets of bank transfer credentials. Instead, their tools are designed to identify and steal documents, showing an interest in documents that may be stored on air-gapped networks.

Names

APT 30 is also known as Override Panda. The group has been identified under different names by various cybersecurity organizations.

Location

APT 30 is suspected to be associated with the Chinese government, indicating that their operations are likely based in China.

First Seen

APT 30 has been active since at least 2005, engaging in cyber espionage activities for over a decade.

Observed Activities

APT 30 has shown a distinct interest in organizations and governments associated with the Association of Southeast Asian Nations (ASEAN), especially around the time of official ASEAN meetings. Their decoy documents often relate to Southeast Asia, India, border areas, and broader security and diplomatic issues. In addition to their focus on Southeast Asia and India, APT 30 has also targeted journalists reporting on issues considered focal points for the Chinese Communist Party, such as corruption, the economy, and human rights.

Techniques Used by APT 30

- **Phishing: Spearphishing Attachment (T1566.001):** APT30 has utilized spearphishing emails with malicious DOC attachments. This technique involves sending targeted emails that contain malicious attachments to trick recipients into opening them, thereby compromising their systems.
- **User Execution: Malicious File (T1204.002):** The group relies on users executing malicious file attachments delivered via spearphishing emails. This tactic depends on user interaction to initiate the execution of the malicious payload.

Software Tools Used by APT 30

- **BACKSPACE (S0031):**
 - **Techniques:** Application Layer Protocol: Web Protocols, Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder, Shortcut Modification), Command and Scripting Interpreter (Windows Command Shell), Data Encoding (Non-Standard Encoding), Exfiltration Over C2 Channel, File and Directory Discovery, Impair Defenses (Disable or Modify System Firewall), Modify Registry, Multi-Stage Channels, Process Discovery, Proxy (Internal Proxy), Query Registry, System Information Discovery.
 - **Usage:** BACKSPACE is a multifunctional tool used for various purposes, including communication over web protocols, data encoding, and exfiltration.
- **FLASHFLOOD (S0036):**
 - **Techniques:** Archive Collected Data (Archive via Custom Method), Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder), Data from Local System, Data

- Techniques: Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder), File and Directory Discovery, Exfiltration Over Physical Medium (Exfiltration over USB), File and Directory Discovery.
- Usage: FLASHFLOOD is employed for data collection and staging, including archiving data using custom methods and extracting data from local and removable media.
- NETEAGLE (S0034):
 - Techniques: Application Layer Protocol, Web Protocols, Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder), Command and Scripting Interpreter (Windows Command Shell), Dynamic Resolution, Encrypted Channel (Symmetric Cryptography), Exfiltration Over C2 Channel, Fallback Channels, File and Directory Discovery, Non-Application Layer Protocol, Process Discovery.
 - Usage: NETEAGLE is a sophisticated tool used for encrypted communication, dynamic resolution, and data exfiltration.
- SHIPSHAPE (S0028):
 - Techniques: Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder, Shortcut Modification), Replication Through Removable Media.
 - Usage: SHIPSHAPE is used for persistence and replication, particularly through the use of removable media.
- SPACESHIP (S0035):
 - Techniques: Archive Collected Data (Archive via Custom Method), Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder, Shortcut Modification), Data Staged (Local Data Staging), Exfiltration Over Physical Medium (Exfiltration over USB), File and Directory Discovery.
 - Usage: SPACESHIP focuses on data archiving, staging, and exfiltration, particularly over physical mediums like USB.

These techniques and tools demonstrate APT 30's capabilities in conducting targeted cyber espionage operations, particularly focused on information gathering, document theft, and exploiting user interactions to compromise systems.

Description of APT32

APT32, also known as the OceanLotus Group, is a Vietnam-based threat group. It was founded in 2014 and has primarily targeted journalists, dissidents, large private enterprises, and government organizations in Southeast Asia. The group's activities have been concentrated within Vietnam, the Philippines, Cambodia, and Laos. APT32's operations often align with Vietnamese state interests, raising questions about potential nation-state sponsorship.

Motivation

APT32's motivations appear to be closely aligned with Vietnamese state interests. They have targeted foreign corporations in key commercial sectors such as manufacturing, hospitality, and consumer products, which are significant to Vietnam's economy. Additionally, they have targeted network security and technology corporations, as well as dissidents and journalists, indicating a focus on both economic and political espionage.

Names

APT32 is also known as the OceanLotus Group.

Location

APT32 is based in Vietnam.

First Seen

APT32 was first identified in 2014.

Observed Activities

APT32 has been involved in various cyber espionage activities, including:

- Targeting and compromising a European corporation involved in building manufacturing facilities in Vietnam (2014).
- Compromising Vietnamese and foreign corporations in network security, technology infrastructure, media, and banking (2016).
- Targeting a large hospitality industry company expanding operations into Vietnam (2016).
- Targeting U.S. and Philippine consumer products corporations with operations in Vietnam for spyware and data exfiltration activities.
- Conducting spyware attacks on Vietnam-based and non-profit human rights organizations.

Techniques Used by APT32

- Account Discovery: Local Account (T1087.001): APT32 used commands like net localgroup administrators to enumerate administrative users.
- Acquire Infrastructure: Domains (T1583.001) and Web Services (T1583.006): APT32 set up websites for information gathering and malware delivery, and used services like Dropbox, Amazon S3, and Google Drive for hosting malicious downloads.
- Application Layer Protocol (T1071): They used JavaScript for communication over HTTP/HTTPS to attacker-controlled domains and downloaded encrypted payloads.
- Archive Collected Data (T1560): APT32's backdoor utilized LZMA compression and RC4 encryption before data exfiltration.
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001): They established persistence using Registry Run keys for executing scripts and their backdoor.
- Command and Scripting Interpreter (T1059): APT32 used various scripting methods including PowerShell, cmd.exe, Visual Basic, and JavaScript for execution and C2 communications.
- Create or Modify System Process: Windows Service (T1543.003): They modified Windows Services for loading scripts and establishing persistence.
- Drive-by Compromise (T1169): Victims were infected by visiting compromised websites.
- Exploitation for Client Execution (T1203) and Privilege Escalation (T1068): APT32 exploited vulnerabilities like CVE-2017-11882 and CVE-2016-7255.
- File and Directory Discovery (T1083): Their backdoor could list files and directories on infected machines.
- Gather Victim Identity Information (T1589): APT32 targeted activists and bloggers for surveillance.
- Hide Artifacts (T1564): They used various methods to hide their activities, including hidden files, windows, and NTFS file attributes.
- Hijack Execution Flow: DLL Side-Loading (T1574.002): APT32 used legitimately-signed executables to load malicious DLLs.
- Indicator Removal (T1070): They cleared event logs, deleted files, and used timestomping to hide their tracks.
- Ingress Tool Transfer (T1105): APT32 added JavaScript to websites for downloading additional frameworks.
- Input Capture: Keylogging (T1056.001): They monitored and captured account password changes.

Lateral Tool Transfer (T1576): Tools were deployed using administrative accounts and moving laterally.

- Masquerading (T1036): APT32 disguised their tools and activities, including renaming utilities and using hidden characters.
- Modify Registry (T1112): Their backdoor modified the Windows Registry for storing configuration.
- Network Service Discovery (T1046) and Network Share Discovery (T1135): APT32 performed network scanning and discovered network shares.
- Non-Standard Port (T1571): Their backdoor used HTTP over non-standard TCP ports.
- Obfuscated Files or Information (T1027): APT32 used various obfuscation techniques including Base64 encoding and code obfuscation frameworks.
- Obtain Capabilities: Tool (T1588.002): They obtained and used tools like Mimikatz and Cobalt Strike.
- Office Application Startup (T1137): APT32 replaced Microsoft Outlook's VbaProject.OTM file for installing a backdoor.
- OS Credential Dumping (T1003): They used tools like Mimikatz for harvesting credentials.
- Phishing: Spearphishing Attachment (T1566.001) and Link (T1566.002): APT32 sent spearphishing emails with malicious attachments and links.
- Process Injection (T1055): Their malware injected a Cobalt Strike beacon into Rundll32.exe.
- Query Registry (T1012): The backdoor queried the Windows Registry for system information.
- Remote Services: SMB/Windows Admin Shares (T1021.002): APT32 used hidden network shares for copying tools to remote machines.
- Remote System Discovery (T1018): They enumerated domain controllers and used the ping command for discovery.
- Scheduled Task/Job: Scheduled Task (T1053.005): APT32 used scheduled tasks for persistence.
- Server Software Component: Web Shell (T1505.003): They used Web shells for maintaining access to victim websites.
- Software Deployment Tools (T1072): APT32 compromised software deployment tools for lateral movement.
- Stage Capabilities (T1608): They hosted malicious payloads in cloud storage services.
- System Binary Proxy Execution (T1218): APT32 used various system binaries like mshta.exe and regsvr32.exe for execution.
- System Information Discovery (T1082): They collected information about the OS version, computer name, and other system details.
- System Network Configuration Discovery (T1016): APT32 used the ipconfig command for gathering IP addresses.
- System Network Connections Discovery (T1049): They used netstat to display TCP connections.
- System Owner/User Discovery (T1033): APT32 collected usernames and executed the whoami command.
- System Script Proxy Execution: PubPrn (T1216.001): They used PubPrn.vbs within execution scripts.
- System Services: Service Execution (T1569.002): Their backdoor used Windows services for executing payloads.
- Unsecured Credentials: Credentials in Registry (T1552.002): APT32 harvested credentials stored in the Windows registry.
- Use Alternate Authentication Material: Pass the Hash (T1550.002) and Pass the Ticket (T1550.003): They used techniques like pass the hash and pass the ticket for lateral movement.
- User Execution: Malicious Link (T1204.001) and File (T1204.002): APT32 lured targets to download malicious payloads through spearphishing.
- Valid Accounts: Local Accounts (T1078.003): They used legitimate local admin account

- Web Service (T1102): APT32 used cloud storage services for hosting malicious downloads.
- Windows Management Instrumentation (T1047): They used WMI for deploying tools and gathering information.

Software Used by APT32

- Arp (S0099): Used for remote system discovery and network configuration discovery.
- Cobalt Strike (S0154): A versatile tool used for a wide range of activities including command execution, data exfiltration, and credential dumping.
- Denis (S0354): Used for various purposes including command execution, data encoding, and obfuscation.
- Goopy (S0477): Employed for DNS communication, data exfiltration, and DLL side-loading.
- ipconfig (S0100): Used for system network configuration discovery.
- Kerndown (S0585): Utilized for command execution, data obfuscation, and phishing.
- KOMPROGO (S0156): Used for command execution and system information discovery.
- Mimikatz (S0002): A well-known tool for credential dumping and manipulation.
- Net (S0039): Used for account discovery, remote services, and system discovery.
- netsh (S0108): Employed for event-triggered execution and impairing defenses.
- OSX_OCEANLOTUS.D (S0352): A macOS backdoor used for data exfiltration and system process modification.
- PHOREAL (S0158): Used for command execution and registry modification.
- RotaJakiro (S1078): A tool for automated collection and boot or logon autostart execution.
- SOUNDBITE (S0157): Employed for DNS communication and system information discovery.
- WINDSHIELD (S0155): Used for indicator removal, query registry, and system information discovery.

APT32's use of a wide range of sophisticated techniques and software demonstrates their capability to conduct complex cyber espionage operations. Their methods are diverse, covering everything from initial access and persistence to data exfiltration and covering their tracks.

APT33: Overview and Activities

Description:

APT33, a cyber espionage group, is known for its sophisticated cyber operations targeting a variety of sectors. Their activities primarily focus on espionage and data exfiltration, often targeting organizations in the aviation, energy, and government sectors. APT33 is recognized for its advanced techniques and persistent approach in cyber operations.

Motivation:

The primary motivation of APT33 appears to be espionage, with a strong focus on gathering sensitive information and intellectual property from targeted industries and government entities. Their activities suggest an intent to support national strategic objectives, likely for a state-sponsored purpose.

Names:

APT33 is also known by other monikers such as Elfin, MAGNALLIUM, Refined Kitten, HOLMIUM, COBALT TRINITY, G0064, ATK35. These aliases have been used by various cybersecurity organizations to describe the group's activities and operations.

Location:

APT33 is believed to be operating out of Iran.

First Seen:

The group has been active since at least 2013, engaging in numerous sophisticated cyber espionage campaigns.

Observed Activities:

APT33 has been observed targeting a wide range of sectors, including but not limited to aviation, energy, and government organizations. Their activities have been primarily focused on espionage and intellectual property theft.

APT33 Techniques and Software

Techniques Used by APT33

- Application Layer Protocol: Web Protocols (T1071.001): APT33 used HTTP for command and control.
- Archive Collected Data: Archive via Utility (T1560.001): Utilized WinRAR to compress data before exfiltration.
- Boot or Logon Autostart Execution (T1547.001): Deployed DarkComet to the Startup folder and used Registry run keys for persistence.
- Brute Force: Password Spraying (T1110.003): Employed password spraying to access target systems.
- Command and Scripting Interpreter: PowerShell (T1059.001): Used PowerShell for downloading files and running scripts from the C2 server.
- Command and Scripting Interpreter: Visual Basic (T1059.005): Initiated payload delivery using VBScript.
- Credentials from Password Stores (T1555): Harvested credentials using tools like LaZagne.
- Data Encoding: Standard Encoding (T1132.001): Encoded command and control traffic using base64.
- Encrypted Channel: Symmetric Cryptography (T1573.001): Utilized AES encryption for command and control traffic.
- Event Triggered Execution: Windows Management Instrumentation Event Subscription (T1546.003): Attempted to establish persistence using WMI event subscriptions.
- Exfiltration Over Alternative Protocol (T1048.003): Exfiltrated files using FTP, separate from the C2 channel.
- Exploitation for Client Execution (T1203): Exploited vulnerabilities in WinRAR and attempted remote code execution via security bypass.
- Exploitation for Privilege Escalation (T1068): Used a public exploit for CVE-2017-0213 for local privilege escalation.
- Ingress Tool Transfer (T1105): Downloaded additional files and programs from the C2 server.
- Network Sniffing (T1040): Employed SniffPass for credential collection via network traffic sniffing.
- Non-Standard Port (T1571): Used HTTP over TCP ports 808 and 880 for command and control.
- Obfuscated Files or Information (T1027): Employed base64 encoding for payload obfuscation.
- Obtain Capabilities: Tool (T1588.002): Leveraged publicly-available tools for early intrusion activities.
- OS Credential Dumping (T1003): Utilized tools like LaZagne, Mimikatz, and ProcDump for credential dumping.
- Phishing: Spearphishing Attachment (T1566.001): Sent spearphishing emails with archive attachments.
- Phishing: Spearphishing Link (T1566.002): Distributed spearphishing emails containing links to .hta files.

- Scheduled Task/Job: Scheduled Task (T1053.005): Created scheduled tasks for executing .vbe files.
- Unsecured Credentials (T1552): Gathered credentials using tools like LaZagne and Gpppassword.
- User Execution: Malicious Link (T1204.001): Lured users to click malicious links in spearphishing emails.
- User Execution: Malicious File (T1204.002): Used malicious email attachments to execute malware.
- Valid Accounts (T1078): Utilized valid accounts for initial access and privilege escalation.
- Cloud Accounts (T1078.004): Compromised Office 365 accounts in conjunction with Ruler for endpoint control.
- Screen Capture (ICS T0852): Utilized backdoors for capturing screenshots.
- Scripting (ICS T0853): Employed PowerShell scripts for command and control and file execution.
- Spearphishing Attachment (ICS T0865): Conducted targeted spearphishing campaigns with HTML application files embedded with malicious code.

Software Used by APT33

- Autolt backdoor (S0129): Used for various malicious activities including PowerShell execution and data encoding.
- Empire (S0363): A versatile framework used for a wide range of malicious activities, from account discovery to exfiltration.
- ftp (S0095): Used for file exfiltration and tool transfer.
- LaZagne (S0349): Employed for credential harvesting from various sources.
- Mimikatz (S0002): A well-known tool for dumping credentials and manipulating access tokens.
- NanoCore (S0336): Used for audio capture, command execution, and credential theft.
- Net (S0039): Utilized for account discovery and network share access.
- NETWIRE (S0198): A multi-functional remote access tool used for data collection and system control.
- PoshC2 (S0378): A PowerShell C2 framework used for a variety of tasks including token manipulation and data exfiltration.
- PowerSploit (S0194): A collection of PowerShell modules used for various stages of exploitation and post-exploitation.
- POWERTON (S0371): Utilized for command and control activities and credential dumping.
- Pupy (S0192): A remote administration and post-exploitation tool.
- Ruler (S0358): Used in conjunction with compromised email accounts for endpoint control.
- StoneDrill (S0380): Employed for data destruction and system information discovery.
- TURNEDUP (S0199): Used for system information discovery and screen capture.

APT33's techniques and software usage demonstrate a sophisticated and versatile approach to cyber espionage, leveraging a mix of custom tools and publicly available utilities to achieve their objectives.

APT37 (Reaper)

Description

APT37, also known as Reaper, is a cyber espionage group believed to be operating out of North Korea. It has been active since at least 2012, primarily targeting the public and private sectors in South Korea. By 2017, APT37 expanded its operations to include Japan, Vietnam, and the Middle East, focusing on a range of industries such as chemicals, electronics, manufacturing,

Motivation

APT37's activities are primarily driven by espionage objectives, likely in support of North Korean state interests. Their operations are characterized by a focus on gathering intelligence and potentially disrupting targets that are of strategic importance to North Korea.

Names

APT37 is known by various aliases including Group 123, InkySquid, Operation Daybreak, Operation Erebus, Reaper Group, Red Eyes, Ricochet Chollima, ScarCruft, Venus 121, ATK4, G0067, and Moldy Pisces.

Location

APT37 is believed to be based in North Korea.

First Seen

The group has likely been active since at least 2012.

Observed

APT37 has expanded its targeting beyond the Korean peninsula since 2017, including Japan, Vietnam, and the Middle East.

Techniques Used by APT37

- Abuse Elevation Control Mechanism (T1548.002): APT37 uses methods to bypass Windows User Account Control (UAC), allowing the execution of payloads with higher privileges.
- Application Layer Protocol (T1071.001): The group uses HTTPS to conceal command and control (C2) communications, making detection more challenging.
- Audio Capture (T1123): APT37 employs SOUNDWAVE, an audio capturing utility, to record microphone input, likely for surveillance purposes.
- Boot or Logon Autostart Execution (T1547.001): They achieve persistence by adding entries in the Registry key HKCU\Software\Microsoft\CurrentVersion\Run.
- Command and Scripting Interpreter (T1059): The group uses various scripting languages like Ruby, Python, and Visual Basic to execute payloads and perform malicious activities.
- Credentials from Password Stores (T1555.003): APT37 uses ZUMKONG, a credential stealer, to harvest usernames and passwords from web browsers.
- Data from Local System (T1005): The group collects sensitive data from victims' local systems.
- Disk Wipe (T1561.002): They have access to destructive malware capable of overwriting the Master Boot Record (MBR), potentially rendering the infected systems inoperable.
- Drive-by Compromise (T1189): APT37 uses compromised websites, especially South Korean sites, and torrent file-sharing sites to distribute malware.
- Exploitation for Client Execution (T1203): The group exploits vulnerabilities in popular software like Flash Player, Word, Internet Explorer, and Microsoft Edge for execution.

- Ingress Tool Transfer (T1105): APT37 downloads second-stage malware from compromised websites.
- Inter-Process Communication (T1559.002): The group uses Windows DDE for command execution and malicious scripting.
- Masquerading (T1036.001): They sign their malware with invalid digital certificates to appear legitimate.
- Native API (T1106): APT37 leverages Windows API calls for process injection.
- Obfuscated Files or Information (T1027): The group obfuscates strings and payloads to evade detection.
- Peripheral Device Discovery (T1120): APT37 uses a Bluetooth device harvester to find information on connected Bluetooth devices.
- Phishing (T1566.001): They deliver malware using spearphishing emails with malicious attachments.
- Process Discovery (T1057): The group's Freenki malware lists running processes using the Windows API.
- Process Injection (T1055): APT37 injects its ROKRAT malware into the cmd.exe process for stealthy execution.
- Scheduled Task/Job (T1053.005): They create scheduled tasks to run malicious scripts on compromised hosts.
- System Information Discovery (T1082): APT37 collects detailed system information like computer name and BIOS model.
- System Owner/User Discovery (T1033): The group identifies the victim's username.
- System Shutdown/Reboot (T1529): APT37 uses malware that can reboot a system after wiping its MBR.
- User Execution (T1204.002): The group sends spearphishing attachments to trick users into executing malicious files.
- Web Service (T1102.002): APT37 uses social networking sites and cloud platforms for C2 communications.

Software Used by APT37

- BLUELIGHT: A multifunctional malware tool used for data exfiltration, screen capture, and information gathering.
- Cobalt Strike: A commercial penetration testing tool repurposed for malicious activities, including command and control.
- CORALDECK: A tool used for data exfiltration and file discovery.
- DOGCALL: A multifunctional tool capable of audio capture, keylogging, screen capture, and bidirectional communication.
- Final1stspy: A tool used for information gathering and obfuscation.
- HAPPYWORK: A tool for system information discovery and data transfer.
- KARAE: Used in drive-by compromises and for system information discovery.
- NavRAT: A tool for command execution, keylogging, and data staging.
- POORAIM: Used for screen capture, information gathering, and web service communication.
- ROKRAT: A sophisticated malware variant used for a wide range of activities including audio capture, data exfiltration, and process injection.
- SHUTTERSPEED: A tool primarily used for screen capture and system information gathering.
- SLOWDRIFT: A tool for system information discovery and web service communication.
- WINERACK: A tool used for command execution and system information discovery.

APT37's diverse range of techniques and software tools highlights their capability to conduct sophisticated cyber espionage operations. Their focus on stealth and persistence, coupled with the use of custom tools, makes them a significant threat to their targets.

Description

APT38 is a North Korean state-sponsored threat actor primarily targeting banks and financial institutions. It is believed to be directed by or part of the North Korean Reconnaissance General Bureau (RGB), an intelligence agency responsible for the state's covert operations. APT38 has targeted financial institutions, cryptocurrency entities, SWIFT system users and endpoints, and ATMs in over 35 countries.

Motivation

APT38's primary motivation appears to be financial gain, specifically through sophisticated attacks on banks and financial systems worldwide. Their operations include large-scale heists, such as the \$81 million theft from the Bank of Bangladesh in 2016.

Names

APT38 is the primary name used to identify this group.

Location

APT38 is associated with North Korea, operating under the guidance or part of the RGB.

First Seen

The group has been active for several years, with notable attacks dating back to at least 2016.

Observed Activities

APT38's activities include a wide range of cyberattacks against financial institutions. They have been responsible for significant financial thefts, including the Bank of Bangladesh heist in 2016 and attacks on Bancomext and Banco de Chile in 2018. Their methods involve sophisticated multi-stage attacks, including initial research, compromising targets through various means (like watering holes and exploiting vulnerabilities), conducting reconnaissance within the network, impacting SWIFT servers, exfiltrating funds, and covering their tracks by wiping disks and destroying logs.

Techniques Used by APT38

- Application Layer Protocol (T1071.001): APT38 used QUICKRIDE backdoor for C2 communication over HTTP and HTTPS.
- Browser Information Discovery (T1217): They collected browser bookmarks to learn about compromised hosts and users.
- Brute Force (T1110): Employed brute force techniques for account access.
- Clipboard Data (T1115): Used KEYLIME Trojan to collect clipboard data.
- Command and Scripting Interpreter (T1059): Utilized PowerShell, VBScript, and a command-line tunneler, NACHOCHEESE, for various operational tasks.
- Control as Modified System Processes (T1543.002): Installed new Windows processes for

persistence.

- Data Destruction (T1485): Implemented custom secure delete functions.
- Data Encrypted for Impact (T1486): Used Hermes ransomware for file encryption.
- Data Manipulation (T1565): Employed DYEPACK for manipulating SWIFT transactions and data.
- Disk Wipe (T1561.002): Used BOOTWRECK to render systems inoperable.
- Drive-by Compromise (T1189): Conducted watering hole schemes for initial access.
- File and Directory Discovery (T1083): Enumerated files and directories on compromised hosts.
- Impair Defenses (T1562): Disabled or modified system firewalls and command history logging.
- Indicator Removal (T1070): Cleared Windows Event logs and used CLOSESHAVE for file deletion.
- Ingress Tool Transfer (T1105): Used NESTEGG backdoor for file transfers.
- Input Capture (T1056.001): Captured keystrokes using KEYLIME Trojan.
- Modify Registry (T1112): Utilized CLEANTOAD tool for registry modifications.
- Native API (T1106): Executed code using Windows API.
- Network Share Discovery (T1135): Enumerated network shares.
- Obfuscated Files or Information (T1027.002): Used various code packing methods.
- Obtain Capabilities (T1588.002): Acquired and used tools like Mimikatz.
- Phishing (T1566.001): Spearphishing campaigns with malicious attachments.
- Process Discovery (T1057): Leveraged Sysmon for process and service discovery.
- Scheduled Task/Job (T1053): Used cron and Task Scheduler for persistence.
- Server Software Component (T1505.003): Employed web shells for access and persistence.
- Software Discovery (T1518.001): Identified security software on compromised systems.
- System Binary Proxy Execution (T1218): Used CHM files and rundll32.exe for concealed payload execution.
- System Information Discovery (T1082): Gathered detailed information about compromised hosts.
- System Network Connections Discovery (T1049): Installed MAPMAKER for monitoring TCP connections.
- System Owner/User Discovery (T1033): Identified primary and current users.
- System Services (T1569.002): Created or modified services for execution.
- System Shutdown/Reboot (T1529): Used BOOTWRECK for system reboots.
- User Execution (T1204.002): Lured victims to enable malicious macros.

Software Used by APT38

- DarkComet (S0334): A multifunctional tool used for various purposes including data collection and system manipulation.
- ECCENTRICBANDWAGON (S0593): Employed for command execution, data staging, and information removal.
- HOPLIGHT (S0376): A versatile tool used for data encoding, firewall impairment, and system information discovery.
- KillDisk (S0607): Used for data destruction and system disruption.
- Mimikatz (S0002): A well-known tool for credential dumping and authentication manipulation.
- Net (S0039): Utilized for account discovery, network share discovery, and remote system discovery.

APT38's sophisticated use of these techniques and software tools highlights their capability to conduct complex cyber operations, ranging from data theft and manipulation to system disruption and destruction.

APT39: Overview and Activities

APT39, also known as Chafer, Remix Kitten, Cobalt Hickman, TA454, and ITG07, is a cyber espionage group believed to be connected to the Iranian government. This group has been active since at least 2014 and is known for its focus on information theft and espionage. APT39's activities are primarily concentrated in the Middle East, but its targeting scope is global.

Description

APT39 was created to consolidate previous activities and methods used by this actor. Its activities largely align with those publicly referred to as "Chafer." The group leverages backdoors like SEAWEED and CACHEMONEY, along with a specific variant of the POWBAT backdoor. APT39's focus on the telecommunications and travel industries suggests an intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes, and create additional accesses and vectors to facilitate future campaigns. Government entity targeting implies a potential secondary intent to collect geopolitical data beneficial for nation-state decision-making.

Motivation

The primary mission of APT39 appears to be tracking or monitoring targets of interest, collecting personal information, including travel itineraries, and gathering customer data from telecommunications firms.

Location and Observed Activities

APT39 is based in Iran and has been observed targeting various sectors, including Aviation, Engineering, Government, High-Tech, IT, Shipping and Logistics, Telecommunications, and Transportation. The countries targeted include Israel, Jordan, Kuwait, Saudi Arabia, Spain, Turkey, the UAE, the USA, and other parts of the Middle East.

APT39 (Chafer): Overview and Activities

Description

APT39, also known as Chafer, Remix Kitten, Cobalt Hickman, TA454, and ITG07, is a cyber espionage group believed to be connected to the Iranian government. It was first seen in 2014 and has been primarily active in the Middle East, targeting various sectors including aviation, engineering, government, high-tech, IT, shipping and logistics, telecommunications, and transportation. The group's activities are concentrated in the Middle East but have a global scope.

APT39's operations are characterized by the use of a variety of tools and techniques, focusing on information theft and espionage. The group has shown a particular interest in the telecommunications sector, as well as the travel industry and IT firms supporting it, and the high-tech industry. Their activities suggest an intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data, and create accesses for future campaigns.

APT39's primary motivation appears to be tracking or monitoring targets of interest, collecting personal information, including travel itineraries, and gathering customer data from telecommunications firms. The targeting of government entities suggests a secondary intent to collect geopolitical data that may benefit nation-state decision-making.

Names and Affiliations

- Names: Chafer, APT 39, Remix Kitten, Cobalt Hickman, TA454, ITG07
- Affiliations: Believed to be connected to the Iranian government.

Location and First Seen

- Location: Iran
- First Seen: 2014

Observed Activities

- Sectors Targeted: Aviation, Engineering, Government, High-Tech, IT, Shipping and Logistics, Telecommunications, Transportation.
- Countries Targeted: Israel, Jordan, Kuwait, Saudi Arabia, Spain, Turkey, UAE, USA, and others in the Middle East.

Techniques Used by APT39

- Application Layer Protocol: APT39 has utilized HTTP and DNS in communications with their command and control (C2) servers.
- Archive Collected Data: They have used WinRAR and 7-Zip for compressing and archiving stolen data.
- BITS Jobs: The group has exploited the BITS protocol to exfiltrate data from compromised hosts.
- Boot or Logon Autostart Execution: APT39 maintained persistence using the startup folder and by modifying LNK shortcuts.
- Brute Force: Tools like Ncrack were used to reveal credentials.
- Clipboard Data: They have employed tools capable of stealing clipboard contents.
- Command and Scripting Interpreter: APT39 used AutoIt, PowerShell, Visual Basic, and Python for executing malicious scripts.
- Create Account: They created local accounts on compromised hosts for network activities.
- Credentials from Password Stores: Tools like Smartftp Password Decryptor were used to decrypt FTP passwords.
- Data from Local System: Various tools were used to steal files from compromised systems.
- Deobfuscate/Decode Files or Information: Malware was used to decrypt encrypted files.
- Event Triggered Execution: Malware was used to establish persistence via AppInit DLLs.
- Exfiltration Over C2 Channel: Stolen data was exfiltrated through C2 communications.
- Exploit Public-Facing Application: SQL injection was used for initial compromises.
- File and Directory Discovery: Tools were employed to search for files on compromised hosts.
- Indicator Removal: Malware was used to delete files post-deployment.
- Ingress Tool Transfer: Tools were downloaded to compromised hosts.
- Input Capture: Tools were used to capture mouse movements and keystrokes.
- Masquerading: Malware was disguised as legitimate software like Mozilla Firefox.
- Network Service Discovery: Tools like CrackMapExec and BLUETORCH were used for network scanning.
- Obfuscated Files or Information: Malware dropped encrypted files and used software packing techniques.

- Obtain Capabilities: Modified versions of publicly available tools like FLINK and Mimikatz were used.
- OS Credential Dumping: Various versions of Mimikatz were used to dump credentials.
- Phishing: Spearphishing emails with malicious attachments and links were used for initial compromises.
- Proxy: Custom tools were used to create internal and external proxies.
- Query Registry: Malware strains were used to query the Registry.
- Remote Services: RDP, SMB, and SSH were used for lateral movement and persistence.
- Remote System Discovery: Tools like NBTscan were used to discover remote systems.
- Scheduled Task/Job: Scheduled tasks were created for persistence.
- Screen Capture: Tools were used to take screenshots on compromised hosts.
- Server Software Component: Web shells like ANTAK and ASPXSPY were installed.
- Subvert Trust Controls: Malware was used to modify code signing policies.
- System Owner/User Discovery: Tools like Remexi were used to collect usernames.
- System Services: Post-exploitation tools were used for process execution.
- User Execution: Spearphishing emails were sent to lure users into clicking malicious links or files.
- Valid Accounts: Stolen credentials were used to compromise Outlook Web Access (OWA).
- Web Service: C2 communications were conducted through services like DropBox.

Software Used by APT39

- ASPXSpy: Used for web shell operations.
- Cadelspy: Employed for various espionage activities including audio capture and keylogging.
- CrackMapExec: Used for account discovery, credential dumping, and network reconnaissance.
- Mimikatz: A key tool for credential dumping and various other malicious activities.
- NBTscan: Utilized for network service discovery and system reconnaissance.
- PsExec: Employed for lateral movement and system service execution.
- pwdump: Used for dumping security account manager credentials.
- Remexi: A versatile tool used for data exfiltration, screen capture, and more.
- Windows Credential Editor: Another tool for credential dumping, particularly LSASS memory.

APT39's operations demonstrate a high level of sophistication and a wide range of capabilities in cyber espionage, reflecting their advanced skill set in conducting complex cyber operations.

APT41 - Group Overview

Description:

APT41, a highly sophisticated cyber threat group, is known for its dual espionage and cybercrime operations. This group, active since at least 2012, has been involved in a range of activities from intellectual property theft to financial gain. APT41's operations are characterized by their complexity and precision, often targeting healthcare, high-tech, telecommunications, higher education, video game, and travel industries.

Motivation:

The primary motivation of APT41 appears to be a combination of state-sponsored espionage activities and financially motivated operations. This dual intent is somewhat unique among threat groups, as they engage in espionage to collect intelligence beneficial to the Chinese state while simultaneously pursuing personal financial interests.

Names:

APT41 is also known by other aliases, including Barium, Winnti, Wicked Panda, and Wicked Spider. These names reflect the diverse nature of their operations and the various sectors they target.

Location:

APT41 is believed to be based in China, with its activities aligning with Chinese state interests.

First Seen:

The group has been active since at least 2012, demonstrating a long history of sophisticated cyber operations.

Observed:

APT41's operations have been observed worldwide, with a focus on industries that align with China's Five-Year economic development plans. They have targeted organizations globally, including those in the United States, United Kingdom, Germany, Japan, South Korea, and more.

Aquatic Panda

Description

Aquatic Panda is a cyber threat group known for its sophisticated cyber operations. The group has been observed using a variety of techniques and tools to infiltrate and compromise target systems, often focusing on vulnerability scanning and data exfiltration.

Motivation

The primary motivation of Aquatic Panda appears to be espionage, with activities aimed at acquiring sensitive information from targeted organizations. Their operations suggest a focus on intelligence gathering, which is typical of state-sponsored or state-affiliated cyber espionage groups.

Names

Aquatic Panda is the primary name used to identify this group. However, like many cyber threat groups, they may operate under different aliases or be identified differently by various cybersecurity organizations.

Location

The specific location of Aquatic Panda is not clearly stated in the available data. However, many cyber espionage groups operate from countries with significant state-sponsored cyber capabilities.

First Seen

The exact date when Aquatic Panda was first observed is not provided in the MITRE ATT&CK database.

Observed

Aquatic Panda has been observed employing a range of cyber techniques, including active scanning for vulnerabilities, using PowerShell for command execution, and attempting to disable or modify endpoint detection and response (EDR) tools.

The Axiom cyber espionage group, also known as Group G0001, is a sophisticated and long-standing threat actor. Here is a detailed overview based on the information from the MITRE ATT&CK framework:

Description:

Axiom is a highly skilled and persistent cyber espionage group. They are known for their advanced techniques and have been involved in numerous high-profile cyber espionage campaigns. The group is adept at using a combination of custom-developed malware and publicly available tools to achieve their objectives.

Motivation:

The primary motivation of Axiom appears to be cyber espionage. Their activities are typically focused on stealing sensitive information from a variety of targets, which often include government, technology, and media sectors. The nature of their operations suggests a strong interest in gathering intelligence and conducting surveillance.

Names:

Axiom is known by several aliases, including Group G0001. They have been identified and tracked under this designation by various cybersecurity organizations.

Location:

The exact location of Axiom is not clearly defined, but they are believed to operate out of China.

First Seen:

The exact date of when Axiom was first observed is not specified in the available data.

Observed:

Axiom has been involved in a wide range of activities, including acquiring infrastructure like DNS servers and virtual private servers, compressing and encrypting data before exfiltration, and

using botnets. They have also been known to collect data from local systems and use steganography for hiding C2 communications.

BackdoorDiplomacy: Overview and Activities

Description:

BackdoorDiplomacy is a cyber espionage group known for its sophisticated cyber operations targeting diplomatic entities and telecommunication companies. The group is adept at exploiting public-facing applications and leveraging various sophisticated techniques to infiltrate and maintain presence in victim networks.

Motivation:

The primary motivation of BackdoorDiplomacy appears to be espionage, focusing on gathering sensitive information from diplomatic and telecommunication entities. Their activities are characterized by stealth and persistence, indicating a strategic interest in long-term intelligence gathering.

Names:

BackdoorDiplomacy is the primary name associated with this group. However, it's common for such groups to operate under multiple aliases or to be identified differently by various cybersecurity organizations.

Location:

The specific location of BackdoorDiplomacy is not clearly defined, but their targets often include entities in the Middle East and Africa, suggesting a possible regional focus.

First Seen:

The exact date of when BackdoorDiplomacy first emerged is not specified in the provided sources. However, their activities have been observed over several years, indicating a long-term operation.

Observed Activities:

BackdoorDiplomacy has been observed targeting diplomatic entities and telecommunication companies, exploiting vulnerabilities in public-facing applications, and conducting sophisticated cyber espionage operations.

BITTER APT Group

Description:

BITTER is an advanced persistent threat (APT) group known for its targeted cyber espionage campaigns. The group is noted for its sophisticated use of malware and phishing techniques to infiltrate and compromise high-value targets.

Motivation:

The primary motivation of BITTER appears to be espionage, focusing on acquiring sensitive information from targeted organizations and individuals. Their activities suggest an intent to gather intelligence that could be of strategic or political value.

Names:

The group is primarily known as BITTER. However, like many APT groups, it may operate under

different aliases or be referred to by different names in cybersecurity reports.

Location:

The specific location of BITTER is not clearly defined in the available information. APT groups often operate across international borders, making it challenging to pinpoint a precise location.

First Seen:

The exact date of when BITTER was first observed is not provided in the available sources. APT groups often operate for some time before being detected.

Observed:

BITTER has been observed using a variety of sophisticated techniques and tools in their operations. They have targeted organizations through spearphishing campaigns and have exploited vulnerabilities in software for initial access and escalation of privileges.

BlackOasis APT Group

Description:

BlackOasis is a Middle Eastern threat group, believed to be a customer of Gamma Group. The group has shown interest in prominent figures in the United Nations, as well as opposition bloggers, activists, regional news correspondents, and think tanks. BlackOasis is associated with operations of a group known by Microsoft as Neodymium, although it's not confirmed if these names refer to the same group.

Motivation:

The primary motivation of BlackOasis is information theft and espionage.

Names:

BlackOasis is the name given by Kaspersky. There is a possible association with Neodymium, as identified by Microsoft, but it's not confirmed if these are aliases for the same group.

Location:

BlackOasis is based in the Middle East.

First Seen:

The group was first observed in 2015.

Observed Activities:

BlackOasis has targeted sectors including Media, Think Tanks, activists, and the UN. Geographically, their activities span across various countries including Afghanistan, Angola, Bahrain, Iran, Iraq, Jordan, Libya, Netherlands, Nigeria, Russia, Saudi Arabia, Tunisia, the UK, and others.

BlackTech (Circuit Panda, Radio Panda)

Description:

BlackTech is a suspected Chinese cyber espionage group that has been active since at least 2013. They primarily target organizations in East Asia, particularly Taiwan, Japan, and Hong Kong, as well as the United States. BlackTech employs a combination of custom malware, dual-use tools, and blurs off the land tactics to compromise networked hardware systems, including

media, construction, engineering, electronics, and finance.

Motivation:

The group's primary motivation appears to be information theft and espionage. Their activities are focused on stealing technology and sensitive information from their targets.

Names:

- BlackTech (Trend Micro)
- Circuit Panda (CrowdStrike)
- Radio Panda (CrowdStrike)
- Palmerworm (Symantec)
- TEMP.Overboard (FireEye)
- T-APT-03 (Tencent)

Location:

China

First Seen:

2010

Observed:

BlackTech has been observed targeting sectors such as Construction, Financial, Government, Healthcare, Media, and Technology. Geographically, their activities have been focused on China, Hong Kong, Japan, Taiwan, and the USA.

Blue Mockingbird - Cyber Threat Group

Description:

Blue Mockingbird is a cyber threat group known for exploiting public-facing applications to gain initial access to victim networks. They have been observed using various techniques such as access token manipulation, command and scripting interpreter, and exploiting vulnerabilities in web applications.

Motivation:

The primary motivation of Blue Mockingbird appears to be resource hijacking, specifically for cryptocurrency mining. They use tools like XMRIG to mine cryptocurrency on victim systems.

Names:

The group is commonly referred to as Blue Mockingbird.

Location:

The specific location of Blue Mockingbird is not clearly identified in the available sources.

First Seen:

The exact date of when Blue Mockingbird was first observed is not provided in the available information.

Observed Activities:

Blue Mockingbird has been observed engaging in various malicious activities, including:

- Exploiting CVE-2019-18935, a vulnerability in Telerik UI for ASP.NET AJAX.
- Using PowerShell and batch script files for command execution.
- Establishing persistence through methods like Windows Service and WMI Event Subscription.
- Hijacking execution flow and masquerading their payloads.
- Using tools like Mimikatz for credential dumping.
- Establishing proxy connections and using remote services for file transfer.
- Resource hijacking for cryptocurrency mining.

Bouncing Golf

Bouncing Golf, also known as Domestic Kitten, APT-C-50, and by its MITRE ATT&CK designation G0097, is a cyberespionage campaign primarily targeting Middle Eastern countries. This campaign is believed to be state-sponsored and originates from Iran. It has been active since at least 2016 and is known for its focus on information theft and espionage.

Description

- **Bouncing Golf/Domestic Kitten:** This campaign is notable for its use of mobile applications loaded with spyware to collect sensitive information. The attackers use fake decoy content to entice victims to download these applications, which then enable the collection of a wide range of data, including contact lists, call records, SMS messages, browser history, geo-location, photos, voice recordings, and more.

Motivation

- **Information Theft and Espionage:** The primary motivation behind Bouncing Golf is to gather sensitive information, particularly from Kurdish and Turkish natives, ISIS supporters, and Iranian citizens. This data is likely used for further actions against these groups.

Names

- **Aliases:** Domestic Kitten (Check Point), APT-C-50 (Check Point), Bouncing Golf (Trend Micro).

Location

- **Country:** Iran.

First Seen

- **Initial Activity:** The campaign was first observed in 2016.

Observed Activities

- **Target Regions:** Afghanistan, Iran, Iraq, Pakistan, Turkey, the UK, the USA, and Uzbekistan.
- **Notable Operations:**
 - June 2019: Mobile Campaign 'Bouncing Golf' Affects the Middle East.
 - November 2020: Over 1,200 individuals targeted, with more than 600 successful infections across 10 unique campaigns.
 - October 2022: Domestic Kitten campaign using new FurBall malware to spy on Iranian

Chimera - Group Overview 🧙🌐

Description: 📄

Chimera is a suspected China-based threat group 🇨🇳 that has been active since at least 2018 📅. This group is known for targeting the semiconductor industry in Taiwan 🇹🇼 as well as obtaining data from the airline industry ✈️.

Motivation: 💬

While the specific motivations of Chimera are not detailed in the provided text, their targeting of the semiconductor 🧑🔬 and airline industries ✈️ suggests a focus on industrial espionage 🕵️ and possibly intellectual property theft 📄.

Names: 🗨️

The group is primarily known as Chimera 🐉.

Location: 🌐

Chimera is suspected to be based in China 🇨🇳.

First Seen: 🕒

The group has been active since at least 2018 📅.

Observed: 🔍

Chimera has been observed engaging in sophisticated cyber espionage activities 🖥️, particularly targeting the semiconductor industry in Taiwan 🇹🇼 and the airline industry ✈️ for data exfiltration and possibly intellectual property theft 📄.

Techniques Used in all tactics

No.	Technique	Description
1	Account Discovery	Used net user for local and domain account discovery.
2	Application Layer Protocol	Utilized HTTPS and DNS for C2 communications.
3	Archive Collected Data	Employed gzip and modified RAR software for archiving data.
4	Automated Collection	Used custom DLLs for continuous data retrieval.
5	Browser Information Discovery	Executed commands for bookmark discovery.
		Exploited in-memory execution and credential

6	Brute Force	stuffing attacks.
7	Command and Scripting Interpreter	Used PowerShell scripts and Windows Command Shell for execution.
8	Data from Information Repositories	Collected documents from SharePoint.
9	Data from Network Shared Drive	Retrieved data from network shares.
10	Data Staged	Staged stolen data locally and remotely.
11	Domain Trust Discovery	Used nltest to identify domain trust relationships.
12	Email Collection	Harvested data from local and remote email collections.
13	Exfiltration Over C2 Channel	Used Cobalt Strike C2 beacons for data exfiltration.
14	Exfiltration Over Web Service	Exfiltrated data to OneDrive accounts.
15	External Remote Services	Accessed external VPN, Citrix, SSH, and other services.
16	File and Directory Discovery	Identified data of interest in file and directory listings.
17	Gather Victim Identity Information	Collected credentials from previous breaches.
18	Hijack Execution Flow	Employed DLL side-loading.
19	Indicator Removal	Cleared event logs, performed file deletion, and used timestomp.
20	Ingress Tool Transfer	Remotely copied tools and malware onto targeted systems.
21	Lateral Tool Transfer	Copied tools between compromised hosts using SMB.
22	Masquerading	Renamed malware to mimic legitimate applications.
23	Modify Authentication Process	Altered NTLM authentication on domain controllers.
24	Multi-Factor Authentication Interception	Registered alternate phone numbers for 2FA interception.
25	Native API	Used direct Windows system calls.

Software Used by Chimera

No.	Software Used
1	BloodHound
2	Cobalt Strike
3	esentuti
4	Mimikatz
5	Net
6	PsExec

Chimera's use of these software tools demonstrates their capabilities in conducting sophisticated cyber espionage operations, including credential theft, lateral movement, and data exfiltration.



Description:

Cleaver is a formidable threat group attributed to Iranian actors, responsible for the activities tracked as Operation Cleaver. The group is known for its sophisticated cyber operations and has been linked to Threat Group 2889 (TG-2889).

Motivation:

While the specific motivations of Cleaver are not detailed in the provided text, their advanced cyber operations suggest objectives aligned with state-sponsored espionage or intelligence gathering.

Names:

Cleaver is also associated with Threat Group 2889 (TG-2889).




Location:

Cleaver is attributed to Iranian actors.

First Seen:

Unfortunately, the specific date of their inaugural activity remains shrouded in mystery within the provided text.

Observed:

Cleaver has been keenly observed employing a range of sophisticated techniques and tools for cyber operations, including ARP cache poisoning, creating customized tools and payloads, and establishing fake social media accounts.   

Techniques Used in all tactics

No.	Tactic/Technique	Description
1	Adversary-in-the-Middle: ARP Cache Poisoning	Cleaver has used custom tools for ARP cache poisoning.
2	Develop Capabilities: Malware	Created customized tools and payloads for various functions including encryption, credential dumping, and network interface sniffing.
3	Establish Accounts: Social Media Accounts	Created fake LinkedIn profiles with detailed information and connections.
4	Obtain Capabilities: Tool	Obtained and used open-source tools like PsExec, Windows Credential Editor, and Mimikatz.
5	OS Credential Dumping: LSASS Memory	Known for dumping credentials using Mimikatz and Windows Credential Editor.

Software Used by Cleaver

1. **Mimikatz** - Used for various purposes including access token manipulation, credential dumping, and account manipulation.
2. **Net Crawler** - Employed for password cracking, OS credential dumping, and accessing remote services.
3. **PSEXEC** - Utilized for creating accounts, modifying system processes, lateral tool transfer, and executing system services.
4. **TinyZBot** - Used for autostart execution, clipboard data capture, command execution, impairing defenses, input capture, and screen capture.

Cleaver's use of these software tools demonstrates their capabilities in conducting complex cyber operations, including credential theft, lateral movement, and maintaining access within targeted networks.

📁 Cobalt Group - Group Overview 📁

📄 Description:

The Cobalt Group 🏢 is a financially motivated threat group that has been primarily targeting financial institutions since at least 2016. The group is known for conducting intrusions to steal money 💰 by targeting ATM systems 🏧, card processing 📠, payment systems 💳, and SWIFT systems 🌐. Cobalt Group has mainly targeted banks 🏦 in Eastern Europe 🌍, Central Asia 🏢, and Southeast Asia 🌏.

💡 Motivation:

The primary motivation of the Cobalt Group is financial gain 💰, achieved through sophisticated cyber intrusions into banking systems 🏦 and financial infrastructure 🏢.

👤 Names:

Cobalt Group is also known as GOLD KINGSWOOD 🏰, Cobalt Gang 🦂, and Cobalt Spider 🕷️.

🌐 Location:

The specific location of the Cobalt Group is not mentioned 🌐, but they have targeted banks 🏦 in Eastern Europe 🌍, Central Asia 🏢, and Southeast Asia 🌏.

📅 First Seen:

Cobalt Group has been active since at least 2016 📅.

👁️ Observed:

The group has been observed conducting sophisticated cyberattacks on financial institutions, including ATM systems 🏧 and SWIFT systems 🌐. Despite the arrest of one of its alleged leaders in October 2019, the group remains active.

Techniques Used in all tactics

No.	Technique	Description
1	Abuse Elevation Control Mechanism: Bypass User Account Control	Cobalt Group has bypassed UAC.
2	Application Layer Protocol: Web Protocols, DNS	Used HTTPS and DNS tunneling for C2.
3	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Used Registry Run keys and Startup path for persistence.
4	Boot or Logon Initialization Scripts: Logon Script (Windows)	Added persistence via HKCU\Environment\UserInitMprLogonScript.
5	Command and Scripting Interpreter: PowerShell, Windows Command Shell, Visual Basic, JavaScript	Executed various scripting languages for malicious activities.
6	Create or Modify System Process: Windows Service	Created new services for persistence.
7	Encrypted Channel: Asymmetric Cryptography	Used PLink utility for SSH tunnels.
8	Exploitation for Client Execution	Exploited multiple vulnerabilities for execution.
9	Exploitation for Privilege Escalation	Used exploits to increase privileges.
10	Indicator Removal: File Deletion	Deleted DLL dropper to cover tracks.
11	Ingress Tool Transfer	Used public sites to upload and download files.
12	Inter-Process Communication: Dynamic Data Exchange	Sent malicious Word OLE compound documents.
13	Network Service Discovery	Leveraged SoftPerfect Network Scanner for scanning.
14	Obfuscated Files or Information: Command Obfuscation	Obfuscated scriptlets and code.
15	Obtain Capabilities: Tool	Obtained and used tools like Mimikatz, PsExec, Cobalt Strike, and SDelete.
16	Phishing: Spearphishing Attachment, Spearphishing Link	Sent spearphishing emails with various attachments and links.
17	Process Injection	Injected code into trusted processes.
18	Protocol Tunneling	Used PLink utility for SSH tunnels.
19	Remote Access Software	Used Ammyy Admin and TeamViewer for remote access.
20	Remote Services: Remote Desktop Protocol	Used RDP for lateral movement.
21	Scheduled Task/Job: Scheduled Task	Created Windows tasks for persistence.
22	Software Discovery: Security Software Discovery	Collected list of security solutions installed.
23	Supply Chain Compromise: Compromise Software Supply Chain	Compromised legitimate web browser updates.
24	System Binary Proxy Execution: Windows System Binary	Used various system binaries for proxy execution.

25	User Execution: Malicious Link, Malicious File	Sent emails with malicious links and files.
26	XSL Script Processing	Used msxsl.exe to bypass AppLocker.

Software Used by Cobalt Group

No.	Tool	Purpose
1	Cobalt Strike	Used for a variety of purposes including network discovery, process injection, and data exfiltration.
2	Mimikatz	Utilized for credential dumping and access token manipulation.
3	More_eggs	Employed for web protocol communication, command execution, and information discovery.
4	PSEXEC	Used for creating accounts, modifying system processes, and executing system services.
5	SDelete	Used for data destruction and file deletion.
6	SpicyOmelette	Utilized for command execution, phishing, and software discovery.

Cobalt Group's use of these software tools demonstrates their focus on financial theft, maintaining access, privilege escalation, and lateral movement within targeted financial networks.

👤 Confucius - Group Overview 🌐

📖 Description:

Confucius is a cyber espionage group primarily targeting military personnel 🧑, high-profile personalities 🌟, business persons 💼, and government organizations 🏛️ in South Asia 🌏 since at least 2013. The group is known for its custom malware code 📄 and targets, with noted similarities to the Patchwork group 🌿.

💡 Motivation:

The primary motivation of Confucius appears to be espionage 🕵️, focusing on gathering sensitive information 📁 from military 🧑, governmental 🏛️, and high-profile targets 🌟 in South Asia 🌏.

🔥 Names:

Confucius is also referred to as Confucius APT 🇮🇳.





🌐 Location:

Confucius primarily targets entities in South Asia 🌏.

📅 First Seen:

The group has been active since at least 2013 .

Observed:

Confucius has been observed engaging in sophisticated cyber espionage activities, utilizing custom malware  and various techniques  to infiltrate and extract information  from its targets .

Techniques Used in all tactics

No.	Technique	Description
1	Acquire Infrastructure: Web Services	Obtained cloud storage service accounts to host stolen data.
2	Application Layer Protocol: Web Protocols	Used HTTP for C2 communications.
3	Automated Collection	Employed a file stealer to steal documents and images.
4	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Dropped malicious files into the startup folder for persistence.
5	Command and Scripting Interpreter: PowerShell, Visual Basic	Executed PowerShell and VBScript for malicious activities.
6	Exfiltration Over C2 Channel	Exfiltrated stolen files to its C2 server.
7	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Exfiltrated data to cloud storage service accounts.
8	Exploitation for Client Execution	Exploited Microsoft Office vulnerabilities for execution.
9	File and Directory Discovery	Used a file stealer to check specific folders for documents and images.
10	Ingress Tool Transfer	Downloaded additional files and payloads onto compromised hosts.
11	Phishing: Spearphishing Attachment, Spearphishing Link	Crafted and sent malicious attachments and links to gain initial access.
12	Scheduled Task/Job: Scheduled Task	Created scheduled tasks for persistence.
13	System Binary Proxy Execution: Mshta	Used mshta.exe to execute malicious VBScript.
14	System Information Discovery	Examined system drives for information.
15	Template Injection	Used weaponized Microsoft Word documents with embedded RTF exploits.
16	User Execution: Malicious Link, Malicious File	Lured victims to click on malicious links or execute malicious attachments.

Software Used by Confucius

No.	Software	Purpose
1	Hornbill	Used for various purposes including audio capture, data exfiltration, and screen capture.
2	Sunbird	Employed for audio capture, data exfiltration, and location tracking.
3	WarzoneRAT	Utilized for command execution, credential theft, and process injection.

Confucius's use of these software tools demonstrates their capabilities in conducting targeted cyber espionage operations, including data theft, surveillance, and maintaining access within targeted networks.

🐱 CopyKittens - Group Overview 🌐

📖 Description:

CopyKittens is an Iranian cyber espionage group that has been operating since at least 2013. The group has targeted various countries, including Israel 🇮🇱, Saudi Arabia 🇸🇦, Turkey 🇹🇷, the U.S. 🇺🇸, Jordan 🇯🇴, and Germany 🇩🇪. It is responsible for the campaign known as Operation Wilted Tulip 🌷.

💡 Motivation:

The primary motivation of CopyKittens appears to be espionage 🕵️, focusing on gathering sensitive information 📁 from a range of international targets 🌐.

🔥 Names:

CopyKittens is the primary name used to identify this group 🏷️.

🌐 Location:

CopyKittens is an Iranian group 🇮🇷, targeting entities in countries such as Israel 🇮🇱, Saudi Arabia 🇸🇦, Turkey 🇹🇷, the U.S. 🇺🇸, Jordan 🇯🇴, and Germany 🇩🇪.

📅 First Seen:

The group has been active since at least 2013 📅.

👁️ Observed:

CopyKittens has been observed conducting cyber espionage activities 🕵️, utilizing various techniques 🛠️ and tools 🖥️ to infiltrate and extract information 📁 from its targets 🎯.

Techniques Used in all tactics

No.	Technique	Description
1	Archive Collected Data: Archive via Utility, Archive via Custom Method	Used ZPP to compress files with ZIP and encrypted data with a substitute cipher.
2	Command and Scripting Interpreter: PowerShell	Utilized PowerShell Empire for execution.
3	Hide Artifacts: Hidden Window	Concealed PowerShell windows using hidden flags.

4	Obtain Capabilities: Tool	Used tools such as Metasploit, Empire, and AirVPN.
6	Proxy	Employed the AirVPN service for operational activity.
6	Subvert Trust Controls: Code Signing	Digitally signed an executable with a stolen certificate.
7	System Binary Proxy Execution: Rundll32	Used rundll32 to load various tools, including lateral movement tools and Cobalt Strike.

Software Used by CopyKittens

No.	Software	Purpose
1	Cobalt Strike	Employed for a variety of purposes including network discovery, process injection, and data exfiltration.
2	Empire	Utilized for command execution, credential dumping, and lateral movement.
3	Matryoshka	Used for DNS communication, keylogging, and screen capture.
4	TDTESS	Employed for command execution, process creation, and indicator removal.

CopyKittens' use of these software tools demonstrates their capabilities in conducting targeted cyber espionage operations, including data theft, surveillance, and maintaining access within targeted networks.

🇮🇷 CURIUM - Group Overview

📖 Description:

CURIUM is an Iranian threat group first reported in November 2021. The group is known for its unique approach of investing time to build relationships with potential targets via social media 📱 over several months. This method is used to establish trust and confidence before sending malware 🦋. CURIUM demonstrates great patience and persistence, engaging in daily chats 💬 with potential targets and sending benign files 📁 to lower their security consciousness.

💡 Motivation:

While the specific motivations of CURIUM are not detailed in the provided text, their methodical approach to targeting individuals suggests objectives aligned with espionage 🕵️ or intelligence gathering 🕒.

🏠 Names:

CURIUM is the primary name used to identify this group 🏷️.

🌐 Location:

CURIUM is identified as an Iranian threat group 🇮🇷.

📅 First Seen:

The group was first reported in November 2021 📅.

👁 Observed:

CURIUM has been observed using social engineering tactics 🧑, particularly through social media 📱, to engage with and eventually compromise targets. Their approach indicates a focus on individual targets rather than broad, indiscriminate campaigns 🎯.

Techniques Used in all tactics

No.	Tactic/Technique	Description
1	Data from Local System	CURIUM has exfiltrated data from compromised machines.
2	Establish Accounts: Social Media Accounts	Established fictitious social media accounts, including on Facebook and LinkedIn, to build relationships with victims, often posing as an attractive woman.
3	Phishing: Spearphishing via Service	Used social media to deliver malicious files to victims.
4	User Execution: Malicious File	Lured users into opening malicious files delivered via social media.

Software Used by CURIUM

The specific software tools used by CURIUM are not detailed in the provided text. However, their tactics suggest the use of custom malware and social engineering tools designed to engage targets and deliver malicious payloads through social media platforms.

CURIUM's approach, focusing on establishing trust through social media interactions before deploying malicious payloads, highlights their methodical and patient strategy in cyber espionage operations.

🗡 Dark Caracal - Group Overview 🇸🇦

📄 Description:

Dark Caracal is a threat group attributed to the Lebanese General Directorate of General Security (GDGS). It has been operational since at least 2012 and is known for its global cyber-espionage campaigns 🕵.

💡 Motivation:

While the specific motivations of Dark Caracal are not detailed in the provided text, the group's activities suggest a focus on espionage 🕵, likely driven by national security 🛡 or political interests 🗳.

🇸🇦 Names:

Dark Caracal is the primary name used to identify this group 🇸🇦.

🌐 Location:

Dark Caracal is attributed to the Lebanese General Directorate of General Security (GDGS) 🇸🇦.

📅 First Seen:

The group has been active since at least 2012 🇸🇦.

👁️ Observed:

Dark Caracal has been observed conducting cyber-espionage activities 🇸🇦, utilizing various techniques 🔧 to infiltrate systems, collect data 🇸🇦, and maintain persistence 🇸🇦.

Techniques Used in all tactics

No.	Technique	Description
1	Application Layer Protocol: Web Protocols	Used HTTP for C2 communications with Base64 encoded payloads.
2	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Added a registry key for persistence.
3	Command and Scripting Interpreter: Windows Command Shell	Used macros in Word documents to download a second stage.
4	Data from Local System	Collected contents of the 'Pictures' folder from compromised Windows systems.
5	Drive-by Compromise	Leveraged a watering hole to serve up malicious code.
6	File and Directory Discovery	Collected file listings of all default Windows directories.
7	Obfuscated Files or Information	Obfuscated strings in Bandook.
8	Phishing: Spearphishing via Service	Spearphished victims via Facebook and Whatsapp.
9	Screen Capture	Took screenshots using their Windows malware.
10	System Binary Proxy Execution: Compiled HTML File	Leveraged a compiled HTML file to download and run an executable.
11	User Execution: Malicious File	Made malware appear like common file types to entice user interaction.

Software Used by Dark Caracal







No.	Software	Purpose
1	Bandook	Used for various purposes including audio capture, data exfiltration, and screen capture.
2	CrossPAT	Employed for file and directory discovery and screen capture.

3	FinFisher	Utilized for privilege escalation, file discovery, and input capture.
4	Pallas	Used for audio capture, location tracking, and data exfiltration.





Dark Caracal's use of these software tools demonstrates their capabilities in conducting sophisticated cyber espionage operations, including data theft, surveillance, and maintaining access within targeted networks.

Darkhotel - Group Overview


Description:

Darkhotel is a suspected South Korean threat group that has been active since at least 2004. The group is known for its cyber espionage operations  conducted via hotel Internet networks  against traveling executives  and other select guests . Darkhotel has also engaged in spearphishing campaigns  and infected victims through peer-to-peer and file-sharing networks .



Motivation:

While the specific motivations of Darkhotel are not detailed in the provided text, their targeting of executives  and use of espionage tactics  suggest motivations related to intelligence gathering , possibly for economic  or political  advantage.


Names:

Darkhotel is also associated with the name DUBNIUM .

Location:

Darkhotel is suspected to be based in South Korea  and primarily targets victims in East Asia .

First Seen:

The group has been operational since at least 2004 .

Observed:

Darkhotel has been observed conducting sophisticated cyber espionage activities , utilizing various techniques  to infiltrate systems, collect data , and maintain persistence .

Techniques Used in all tactics

No.	Technique	Description
1	Boot or Logon Autostart Execution:	Established persistence by adding

	Registry: Run Keys; Startup; Local programs to download; Registry Key	
2	Command and Scripting Interpreter: Windows Command Shell	Dropped a shell script to download and execute files.
3	Deobfuscate/Decode Files or Information	Decrypted strings and imports using RC4, XOR, and RSA.
4	Drive-by Compromise	Used embedded iframes on hotel login portals for malware distribution.
5	Encrypted Channel: Symmetric Cryptography	Used AES-256 and 3DES for C2 communications.
6	Exploitation for Client Execution	Exploited Adobe Flash vulnerability for execution.
7	File and Directory Discovery	Searched for files with specific patterns.
8	Ingress Tool Transfer	Downloaded additional malware from C2 servers.
9	Input Capture: Keylogging	Employed keyloggers.
10	Masquerading: Match Legitimate Name or Location	Disguised malware as an SSH tool.
11	Obfuscated Files or Information	Obfuscated code using RC4, XOR, and RSA.
12	Phishing: Spearphishing Attachment	Sent spearphishing emails with malicious attachments.
13	Process Discovery	Collected a list of running processes.
14	Replication Through Removable Media	Modified executables on removable media for spreading.
15	Software Discovery: Security Software Discovery	Searched for anti-malware strings and processes.
16	Subvert Trust Controls: Code Signing	Used stolen or forged code-signing certificates.
17	System Information Discovery	Collected system information from compromised hosts.
18	System Network Configuration Discovery	Gathered IP address and network adapter information.
19	System Time Discovery	Obtained system time from compromised hosts.
20	Taint Shared Content	Propagated by infecting executables on shared drives.
21	User Execution: Malicious File	Lured users into clicking on malicious attachments.
22	Virtualization/Sandbox Evasion	Employed just-in-time decryption and system checks to evade detection.






Software Used by Darkhotel

No.	Software	Purpose
1	Bandook	Used for various purposes including audio capture, data exfiltration, and screen capture.
2	CrossRAT	Employed for file and directory discovery and screen capture.
3	FinFisher	Utilized for privilege escalation, file discovery, and input capture.
4	Pallas	Used for audio capture, location tracking, and data exfiltration.







Darkhotel's use of these software tools demonstrates their capabilities in conducting targeted cyber campaigns, operations, including data theft, surveillance, and malware deployment within

DarkHydrus - Group Overview

Description:

DarkHydrus is a threat group that has been actively targeting government agencies  and educational institutions  in the Middle East  since at least 2016. The group is known for heavily leveraging open-source tools  and custom payloads  to carry out its attacks.

Motivation:

While the specific motivations of DarkHydrus are not detailed in the provided text, their targeting of government  and educational institutions  suggests objectives related to espionage  or intelligence gathering , possibly for political  or strategic  purposes.

Names:

DarkHydrus is the primary name used to identify this group .







Location:

DarkHydrus primarily targets entities in the Middle East .

First Seen:

The group has been active since at least 2016 .

Observed:

DarkHydrus has been observed using a variety of techniques  to infiltrate systems , execute commands , and exfiltrate data , focusing on government agencies  and educational institutions .

Techniques Used in all tactics

No.	Technique	Description
1	Command and Scripting Interpreter: PowerShell	Leveraged PowerShell to download and execute additional scripts.
2	Forced Authentication	Used Template Injection to launch an authentication window for credential harvesting.
3	Hide Artifacts: Hidden Window	Concealed PowerShell windows.
4	Obtain Capabilities: Tool	Obtained and used tools like Mimikatz, Empire, and Cobalt Strike.

5	Phishing: Spearphishing Attachment	Sent spearphishing emails with malicious attachments, including password-protected RAR archives and Microsoft Office documents.
6	Template Injection	Used Phishery to inject malicious remote template URLs into Word documents.
7	User Execution: Malicious File	Required users to enable execution in Microsoft Excel for .iqy file download.

Software Used by DarkHydrus

No.	Software	Purpose
1	Cobalt Strike	Used for various purposes including command execution, data encoding, and process injection.
2	Mimikatz	Employed for credential dumping and access token manipulation.
3	RogueRobin	Utilized for command execution, data encoding, and screen capture.

DarkHydrus's use of these software tools demonstrates their capabilities in conducting sophisticated cyber espionage operations, including credential theft, surveillance, and maintaining access within targeted networks.

💰 DarkVishnya - Group Overview 🏠

📖 Description:

DarkVishnya is a financially motivated threat actor known for targeting financial institutions 🏦 in Eastern Europe 🌍. The group has been active in conducting sophisticated cyberattacks 🕒 against at least eight banks 🏦 in the region during 2017-2018.

💡 Motivation:

The primary motivation of DarkVishnya appears to be financial gain 💰, as evidenced by their focus on attacking financial institutions 🏦.

🔥 Names:

The group is known as DarkVishnya 🏠.

🌍 Location:

DarkVishnya has primarily targeted financial institutions 🏦 in Eastern Europe 🌍.

📅 First Seen:

The group's activities were first reported in 2017 📅.

👁️ Observed:

DarkVishnya has been observed using a variety of techniques 🛠️ to infiltrate financial institutions 🏦, execute commands 🖱️, and potentially exfiltrate sensitive financial data 📡.

Techniques Used in all tactics

No.	Technique	Description
1	Brute Force (T1110)	DarkVishnya used brute-force attacks to obtain login data.
2	Command and Scripting Interpreter: PowerShell (T1059.001)	Utilized PowerShell to create shellcode loaders.
3	Create or Modify System Process: Windows Service (T1543.003)	Created new services for distributing shellcode loaders.
4	Hardware Additions (T1200)	Employed devices like Bash Bunny, Raspberry Pi, netbooks, or inexpensive laptops to connect to local networks.
5	Network Service Discovery (T1046)	Performed port scanning to identify active services.
6	Network Share Discovery (T1135)	Scanned for public shared folders on the network.
7	Network Sniffing (T1040)	Used network sniffing techniques to obtain login data.
8	Non-Standard Port (T1571)	Utilized ports 5190, 7900, 4444, 4445, and 31337 for shellcode listeners and C2 communications.
9	Obtain Capabilities: Tool (T1588.002)	Acquired and used tools like Impacket, Winexe, and PsExec.
10	Remote Access Software (T1219)	Employed DameWare Mini Remote Control for lateral movement within networks.

Software Used by DarkVishnya

No.	Software	Purpose
1	PsExec	Used for creating accounts, modifying system processes, lateral tool transfer, and executing system services.
2	Winexe	Utilized for executing system services.

DarkVishnya's tactics and tools indicate a high level of sophistication in conducting targeted attacks against financial institutions, with a clear focus on gaining unauthorized access, conducting surveillance, and potentially facilitating financial fraud or theft.

🐼 Deep Panda - Group Overview 🇨🇳

📄 Description:

Deep Panda is a sophisticated and suspected Chinese threat group 🇨🇳 known for targeting a wide range of industries, including government 🏛️, defense 🛡️, financial 🏦, and telecommunications 📡 sectors. The group has been active for several years 📅 and is known for

its advanced cyber espionage tactics 🕵️.

💡 Motivation:

Deep Panda's primary motivation appears to be cyber espionage 🕵️, gathering intelligence 📁 and sensitive information 📁 from targeted organizations 🏢 and government entities 🏛️.

🔥 Names:

Deep Panda is also known by several other names 🏷️, including Shell Crew 🐚, WebMasters 🌐, KungFu Kittens 🐱, PinkPanther 🐼, and Black Vine 🌿.

🌍 Location:

While the specific location of Deep Panda is not explicitly mentioned 🌐, it is suspected to be based in China 🇨🇳.

📅 First Seen:

Deep Panda's activities have been observed for several years 📅, with significant operations noted as early as 2014.

👁️ Observed:

Deep Panda has been observed targeting a variety of sectors 🏢 with sophisticated cyber espionage campaigns 🕵️. The group's intrusion into the healthcare company Anthem 🏥 is one of its most notable operations.

Techniques Used in all tactics

No.	Technique	Description
1	Command and Scripting Interpreter: PowerShell (T1059.001)	Used PowerShell scripts for downloading and executing programs in memory.
2	Event Triggered Execution: Accessibility Features (T1546.008)	Utilized the sticky-keys technique to bypass RDP login screens.
3	Hide Artifacts: Hidden Window (T1564.003)	Concealed PowerShell windows using the -w hidden parameter.
4	Obfuscated Files or Information: Indicator Removal from Tools (T1027.005)	Updated and modified malware to evade detection.
5	Process Discovery (T1057)	Employed Microsoft Tasklist utility for listing running processes.
6	Remote Services: SMB/Windows Admin Shares (T1021.002)	Used net.exe for connecting to network shares.
7	Remote System Discovery (T1018)	Utilized ping for identifying other machines of interest.
8	Server Software Component: Web Shell (T1505.003)	Deployed Web shells on public web servers.
	System Binary Proxy Execution: Powershell (T1059.001)	Executed server variant of Powershell using

9	(T1218.010)	regsvr32.exe.
10	Windows Management Instrumentation (T1047)	Used WMI for lateral movement.

Software Used by Deep Panda

No.	Software	Purpose
1	Derusbi	A multifunctional malware toolkit used for various malicious activities.
2	Mivast	Employed for autostart execution and credential dumping.
3	Net	Utilized for account discovery, network share discovery, and remote services.
4	Ping	Used for remote system discovery.
5	Sakula	A backdoor used for gaining persistent access and executing malicious activities.
6	StreamEx	Employed for command execution, registry modification, and information gathering.
7	Tasklist	Used for process and software discovery.

Deep Panda's operations demonstrate a high level of sophistication and focus on long-term intelligence gathering. The group's use of advanced techniques and custom malware indicates a well-resourced and skilled adversary capable of conducting significant cyber espionage campaigns.

🦋 Dragonfly - Group Overview 🇷🇺

📖 Description:

Dragonfly is a cyber espionage group attributed to Russia's Federal Security Service (FSB) Center 16 🇷🇺. Active since at least 2010, Dragonfly has targeted defense 🛡️ and aviation ✈️ companies, government entities 🏛️, companies related to industrial control systems 🏭, and critical infrastructure sectors 🌐🌍 worldwide. The group employs supply chain attacks 📦, spearphishing 📧, and drive-by compromise attacks 🚗 in its operations.

💡 Motivation:

Dragonfly's primary motivation appears to be cyber espionage 🕵️, focusing on gathering intelligence 📁 and compromising critical infrastructure 🏭 for strategic advantage 🌐.

🔥 Names:

Dragonfly is also known by various aliases 🏷️, including TEMP.Isotope, DYMALLOY, Berserk Bear, TG-4192, Crouching Yeti, IRON LIBERTY, and Energetic Bear.

🌐 Location:

Dragonfly is believed to be operating out of Russia 🇷🇺.

17 First Seen:

The group has been active since at least 2010 📅.

👁 Observed:

Dragonfly has been observed conducting sophisticated cyber espionage campaigns 🕵 targeting a wide range of sectors 🏢, particularly those related to national security 🛡 and critical infrastructure 🏗.

Techniques Used in all tactics

No.	Technique	Description
1	Account Discovery (T1087.002)	Used batch scripts for user enumeration on domain controllers.
2	Account Manipulation (T1098)	Added new accounts to administrators group for elevated access.
3	Acquire Infrastructure (T1583.001 & .003)	Registered domains and acquired VPS infrastructure for campaigns.
4	Active Scanning (T1595.002)	Scanned systems for vulnerable services.
5	Application Layer Protocol (T1071.002)	Used SMB for command and control (C2) communications.
6	Archive Collected Data (T1560)	Compressed data into .zip files for exfiltration.
7	Boot or Logon Autostart Execution (T1547.001)	Established persistence via Registry Run keys.
8	Brute Force (T1110 & .002)	Attempted to brute force credentials and used password cracking tools.
9	Command and Scripting Interpreter (T1059 & sub-techniques)	Utilized various scripting methods, including PowerShell, batch scripts, and Python for execution.
10	Compromise Infrastructure (T1584.004)	Compromised legitimate websites for C2 and malware hosting.
11	Create Account (T1136.001)	Created local accounts on victims.
12	Data from Local System (T1005)	Collected data from local systems.
13	Data Staged (T1074.001)	Staged data in specific directories for exfiltration.
14	Drive-by Compromise (T1189)	Used strategic web compromise with exploit kits.
15	Email Collection (T1114.002)	Accessed email accounts using Outlook Web Access.
16	Exploit Public-Facing Application (T1190)	Exploited vulnerabilities in public-facing applications.
17	Exploitation for Client Execution (T1203)	Exploited Adobe Flash Player vulnerability for execution.
18	Exploitation of Remote Services (T1210)	Exploited Windows Netlogon vulnerability.
19	External Remote Services (T1133)	Used VPNs and OWA for persistent access.
20	File and Directory Discovery (T1083)	Gathered file and folder names from hosts.
21	Forced Authentication (T1187)	Collected hashed credentials via spearphishing and .LNK file modifications.





22	Gather Victim Org Information (T1591.002)	Collected open-source information for targeting.
23	Hide Artifacts (T1564.002)	Modified Registry to hide user accounts.
24	Impair Defenses (T1562.004)	Disabled host-based firewalls and opened specific ports.
25	Indicator Removal (T1070.001 & .004)	Cleared event logs and deleted files used in operations.
26	Ingress Tool Transfer (T1105)	Transferred tools for operations within victim environments.
27	Masquerading (T1036)	Created accounts disguised as legitimate service accounts.
28	Modify Registry (T1112)	Used Reg for various techniques.
29	Network Share Discovery (T1135)	Identified and browsed file servers in victim networks.
30	Obtain Capabilities (T1588.002)	Used tools like Mimikatz, CrackMapExec, and PsExec.
31	OS Credential Dumping (T1003 & sub-techniques)	Used tools to dump password hashes and credentials.

Software Used by Dragonfly




No.	Software	Purpose
1	Backdoor.Oldrea	A multifunctional backdoor used for various malicious activities.
2	CrackMapExec	A tool used for network reconnaissance and credential dumping.
3	Impacket	A collection of Python classes for working with network protocols.
4	MCMD	A malware used for command execution and data exfiltration.
5	Mimikatz	A tool used for credential dumping and lateral movement.
6	Net	A Windows command-line tool used for network reconnaissance and remote access.
7	netsh	A command-line scripting utility used to modify network configurations.
8	PsExec	A tool for executing processes on remote systems.
9	Reg	A command-line tool for modifying the Windows Registry.

DragonOK - Group Overview



Description:

DragonOK is a cyber threat group known for targeting Japanese organizations  through phishing emails . The group's activities are characterized by the use of a variety of malware  and sophisticated techniques .



Motivation:

The primary motivation of DragonOK appears to be cyber espionage , focusing on obtaining sensitive information  from Japanese entities .

Names:

DragonOK is the primary name used to identify this group . It is also thought to have a direct or indirect relationship with the threat group Moafée .




Location:

The specific location of DragonOK is not clearly identified , but its targeting of Japanese organizations suggests a focus in East Asia .

First Seen:

The group was first identified in reports dating back to at least 2014 .

Observed:

DragonOK has been observed conducting targeted phishing campaigns  and deploying a range of custom malware  against Japanese targets .

Techniques Used in all tactics

DragonOK employs various techniques across different tactics, including but not limited to:

No.	Technique	Description
1	Application Layer Protocol	Utilizes web protocols and DNS for communication.
2	Boot or Logon Autostart Execution	Adds programs to the Registry Run keys and Startup folder for persistence.
3	Command and Scripting Interpreter	Uses Windows Command Shell for execution.
4	Create or Modify System Process	Creates Windows services for its malicious processes.
5	Deobfuscate/Decode Files or Information	Employs techniques to decode or deobfuscate files.
6	Encrypted Channel	Uses symmetric cryptography for secure communication.
7	File and Directory Discovery	Searches for files and directories of interest on the victim's machine.
8	Hide Artifacts	Hides files and directories to evade detection.
9	Hijack Execution Flow	Employs DLL side-loading and DLL search order hijacking.
10	Ingress Tool Transfer	Transfers additional tools or payloads into the victim's environment.
11	Input Capture	Uses keylogging to capture user input.
12	Masquerading	Disguises tasks or services and matches legitimate names or locations to blend in.
13	Modify Registry	Alters the Windows Registry for various purposes.
14	Native API	Uses native API calls for various malicious activities.
15	Network Share Discovery	Searches for network shares in the victim

16	Non-Application Layer Protocol	Utilizes non-standard protocols for communication.
17	Obfuscated Files or Information	Obfuscates files to evade detection.
18	Process Discovery	Identifies processes running on the victim's system.
19	Query Registry	Queries the Windows Registry to gather information.
20	Screen Capture	Captures screenshots of the victim's screen.
21	System Network Connections Discovery	Discovers network connections and related information.
22	Trusted Developer Utilities Proxy Execution	Uses MSBuild for proxy execution.
23	Virtualization/Sandbox Evasion	Employs checks to evade detection in virtualized or sandboxed environments.
24	Web Service	Uses dead drop resolvers for communication.

Software Used by DragonOK

No.	Software	Purpose
1	PlugX (S0013)	A multifunctional backdoor used for remote control and data exfiltration.
2	PoisonIvy (S0012)	A well-known remote access tool with capabilities like keylogging, screen capture, and process injection.

🌐 Earth Lusca - Group Overview 🇨🇳

📖 Description:

Earth Lusca is a suspected China-based cyber espionage group 🇨🇳, active since at least April 2019 📅. The group is known for targeting a wide range of organizations globally 🌐, including government institutions 🏛️, news media 📰, gambling companies 🎰, educational institutions 🎓, COVID-19 research organizations 🦠, telecommunications 📶, religious movements banned in China 🚫, and cryptocurrency trading platforms 💰. Some of Earth Lusca's operations appear to be financially motivated 💰.

💡 Motivation:

The primary motivation of Earth Lusca seems to be cyber espionage 🕵️, with a focus on gathering sensitive information 📁. The group's targeting of a diverse set of sectors indicates a broad set of interests, possibly extending beyond traditional espionage to include financial gains 💰.

🔥 Names:

Earth Lusca is the primary name for the group 🏠. It is also associated with TAG-22.

🌐 Location:

While the group is suspected to be based in China 🇨🇳, its operations are global 🌐, affecting countries across multiple continents 🌍.

📺 First Seen:

Earth Lusca's activities were first observed in April 2019 📅.

👁 Observed:

The group has been observed conducting sophisticated cyber espionage campaigns 🕵 targeting a wide range of sectors worldwide 🌐.

Techniques Used in all tactics

Earth Lusca employs a variety of techniques, including but not limited to:

No.	Technique	Description
1	Abuse Elevation Control Mechanism	Utilizes the Fodhelper UAC bypass technique.
2	Account Manipulation	Drops SSH-authorized keys for server access.
3	Acquire Infrastructure	Registers domains and acquires servers and web services for operations.
4	Active Scanning	Scans for vulnerabilities in public-facing servers.
5	Archive Collected Data	Uses WinRAR for data compression before exfiltration.
6	Boot or Logon Autostart Execution	Adds keys to the Registry for persistence.
7	Command and Scripting Interpreter	Employs PowerShell, Visual Basic, Python, and JavaScript for various tasks.
8	Compromise Infrastructure	Compromises web servers and web services.
9	Create or Modify System Process	Creates Windows services for persistence.
10	Deobfuscate/Decode Files or Information	Uses certutil for decoding.
11	Domain Trust Discovery	Utilizes Nltest for domain controller information.
12	Drive-by Compromise	Conducts watering hole attacks.
13	Exfiltration Over Web Service	Utilizes cloud storage for data exfiltration.
14	Exploit Public-Facing Application	Exploits vulnerabilities in servers like Microsoft Exchange and Oracle GlassFish.
15	Exploitation of Remote Services	Uses Mimikatz for exploiting domain controllers.
16	Hijack Execution Flow	Employs DLL side-loading techniques.
17	Masquerading	Matches legitimate names or locations for disguising activities.
18	Modify Registry	Alters the Registry for various purposes.
19	Obfuscated Files or Information	Uses Base64 encoding and steganography.
20	Obtain Capabilities	Acquires malware and tools for operations.
21	OS Credential Dumping	Uses tools like ProcDump and Mimikatz for credential dumping.







22	Phishing	Sends spearphishing emails with malicious links.
23	Process Discovery	Utilizes Tasklist for process information.
24	Proxy	Adopts Cloudflare for proxying compromised servers.
25	Remote System Discovery	Uses PowerShell and scanning tools for system discovery.
26	Scheduled Task/Job	Creates scheduled tasks for persistence.
27	Stage Capabilities	Stages malware on compromised servers and web services.
28	System Binary Proxy Execution	Uses mshta.exe for executing scripts.
29	System Network Configuration Discovery	Employs ipconfig for network information.
30	System Network Connections Discovery	Uses scripts and netstat for network connection info.
31	System Owner/User Discovery	Collects user account information.

Software Used by Earth Lusca




No.	Software	Description
1	certutil (S0160)	Used for data archiving and decoding.
2	Cobalt Strike (S0154)	A sophisticated exploitation tool used for network reconnaissance and data exfiltration.
3	Mimikatz (S0002)	A well-known tool used for credential dumping.
4	NBTscan (S0590)	Utilized for network service discovery.
5	Nltest (S0359)	Employed for domain trust discovery.
6	PowerSploit (S0194)	A collection of Microsoft PowerShell modules used for various tasks in a network attack.
7	ShadowPad (S0596)	Malware used for network infiltration and data extraction.
8	Tasklist (S0057)	Used for process discovery.
9	Winnti for Linux (S0430)	A Linux variant of the Winnti malware, used for persistent access and data exfiltration.

Elderwood - Group Overview

Description:

Elderwood is a cyber espionage group, suspected to be based in China , known for its involvement in the 2009 Google intrusion, dubbed Operation Aurora. The group has targeted a diverse array of entities , including defense organizations , supply chain manufacturers , human rights and nongovernmental organizations (NGOs) , and IT service providers .

Motivation:

Elderwood's primary motivation appears to be espionage , with a focus on stealing sensitive information  from a variety of high-value targets that align with strategic interests .

🔥 Names:

The group is known as Elderwood 🇨🇳, and it has been associated with other names 🇨🇳 including Elderwood Gang, Beijing Group, and Sneaky Panda.

🌐 Location:

Elderwood is suspected to be operating out of China 🇨🇳.

📺 First Seen:

The group's activities were notably recognized during the Operation Aurora in 2009 🇨🇳.

👁️ Observed:

Elderwood has been observed conducting sophisticated cyber espionage campaigns 🌐 targeting a wide range of sectors globally 🌐.

Techniques Used in all tactics

Elderwood employs various techniques, including:

Technique	Description
Drive-by Compromise	Injecting malicious code into public web pages visited by targets.
Exploitation for Client Execution	Using endpoint software vulnerabilities and zero-day exploits.
Ingress Tool Transfer	Utilizing the Ritsol backdoor trojan to download files onto compromised hosts.
Obfuscated Files or Information	Encrypting documents and executables.
Software Packing	Packing malware payloads before delivery.
Phishing	Spearphishing with attachments and links to deliver exploits and malware.
User Execution	Leveraging spearphishing to get users to open links and attachments.

Software Used by Elderwood

Elderwood has used a range of software tools, including:

Software	Description
Bribe (S0204)	Utilizes various techniques for execution and persistence.
Hydraq (S0203)	A sophisticated backdoor with data exfiltration and process discovery capabilities.
Linfo (S0211)	Capable of command execution, data collection, and scheduled data transfer.
Naid (S0205)	Used for service creation and network information gathering.

Nerex (S0210)	Employs code signing to subvert trust controls.
Pasam (S0208)	Collects data from local systems and performs file and directory discovery.
PoisonIvy (S0012)	A well-known backdoor with keylogging and data exfiltration capabilities.
Vasport (S0207)	Used for proxying and data ingress.
Wiarp (S0206)	Executes commands and injects processes.

🔥 Ember Bear - Group Overview 🇷🇺

📖 Description:

Ember Bear is a cyber espionage group suspected to be sponsored by the Russian state 🇷🇺. Active since at least March 2021 📅, the group has primarily focused on operations against Ukraine 🇺🇦 and Georgia 🇧🇪. They have also targeted Western European 🌐 and North American 🌐 foreign ministries 🏛️, pharmaceutical companies 💊, and financial sector organizations 💰. Ember Bear is believed to have conducted the WhisperGate destructive wiper attacks 🗑️ against Ukraine in early 2022.

💡 Motivation:

The primary motivation of Ember Bear appears to be state-sponsored espionage 🕵️, with a focus on geopolitical intelligence gathering 🌐 and potentially causing disruption in targeted regions 🌐.

🔥 Names:

Ember Bear is also known as Saint Bear 🐻, UNC2589, UAC-0056, Lorec53, Lorec Bear, and Bleeding Bear 🩸.

🌐 Location:

The group is suspected to be based in Russia 🇷🇺.

📅 First Seen:

Ember Bear's activities were first identified in March 2021 📅.

👁️ Observed:

The group has been observed targeting a range of entities in Ukraine 🇺🇦, Georgia 🇧🇪, Western Europe 🌐, North America 🌐, and other regions 🌐, with a focus on government 🏛️, pharmaceutical 💊, and financial sectors 💰.

Techniques Used in all tactics

Ember Bear employs various techniques, including:

Technique	Description
Command and Scripting Interpreter	Using PowerShell, Windows Command Shell, and JavaScript for execution.
Exploitation for Client Execution	Exploiting Microsoft Office vulnerabilities.
Impair Defenses	Disabling Windows Defender and other security tools.
Ingress Tool Transfer	Downloading malicious code.
Modify Registry	Altering registry keys for persistence and evasion.
Obfuscated Files or Information	Employing binary padding, software packing, and command obfuscation.
Phishing	Spearphishing with attachments and links.
Subvert Trust Controls	Using stolen certificates for payload signing.
System Binary Proxy Execution	Leveraging control panel files for execution.
User Execution	Luring users to click on malicious links or files.
Web Service	Using Discord's CDN for malware delivery.

Software Used by Ember Bear

Ember Bear utilizes various software tools, including:

1. **OutSteel (S1017)**: A document stealer and phishing tool.
2. **Saint Bot (S1018)**: A downloader with capabilities like UAC bypass and process injection.
3. **WhisperGate (S0689)**: A destructive wiper tool used in attacks against Ukraine.

Equation - Group Overview

Description:

Equation is a highly sophisticated cyber threat group known for its advanced techniques and capabilities 🛠️. The group is particularly notable for its use of zero-day exploits 🚫 and its unique ability to overwrite the firmware of hard disk drives 🗑️, making their attacks extremely stealthy and persistent 🕵️.


Motivation:

While the specific motivations of Equation are not explicitly detailed in the available information 🤔, their advanced capabilities and the nature of their operations suggest a focus on cyber espionage 🕵️ and intelligence gathering 🌐.

Names:

The group is primarily known as Equation 📄.



Location:

The specific location of Equation is not publicly disclosed or identified in the available sources .

First Seen:

Equation's activities were first identified and reported by Kaspersky Lab's Global Research and Analysis Team in February 2015 .

Observed:

Equation has been observed employing sophisticated techniques and tools , targeting a range of systems and devices with advanced malware .

Techniques Used in all tactics

Equation employs a variety of advanced techniques, including:

1. **Execution Guardrails: Environmental Keying (T1480.001)**: Utilizing environmental keying in payload delivery to ensure that their malware executes only in specific environments.
2. **Hide Artifacts: Hidden File System (T1564.005)**: Using an encrypted virtual file system stored in the Windows Registry for stealth.
3. **Peripheral Device Discovery (T1120)**: Searching for specific information about attached hard drives, potentially to identify and overwrite firmware.
4. **Pre-OS Boot: Component Firmware (T1542.002)**: Demonstrating the capability to overwrite the firmware on hard drives from certain manufacturers.

Software Used by Equation

While specific software tools used by Equation are not detailed in the provided information, their known capabilities suggest the use of highly sophisticated malware, including:

- Malware capable of firmware manipulation.
- Tools for environmental keying and hidden file systems.
- Advanced malware leveraging zero-day exploits.

EXOTIC LILY - Group Overview

Description:

EXOTIC LILY is a financially motivated cyber threat group, closely associated with Wizard Spider. The group is known for deploying ransomware, including Conti and Diabol. EXOTIC LILY is believed to act as an initial access broker for other malicious actors. Since at least September 2021, they have targeted various industries, including IT, cybersecurity, and healthcare.

Motivation:

The primary motivation of EXOTIC LILY appears to be financial gain. Their activities suggest a

focus on ransomware deployment and possibly selling access to compromised systems to other threat actors.

Names:

The group is primarily known as EXOTIC LILY.

Location:

EXOTIC LILY's specific location is not mentioned, but they have targeted organizations globally.

First Seen:

Their activities were first observed in September 2021.

Observed:

EXOTIC LILY has been observed using sophisticated phishing techniques, exploiting vulnerabilities, and leveraging various tools for initial access and payload delivery.

Techniques Used in all tactics

EXOTIC LILY employs a range of techniques, including:

1. **Acquire Infrastructure: Domains (T1583.001)**: Registering domains to spoof targeted organizations.
2. **Establish Accounts: Social Media and Email Accounts (T1585.001, .002)**: Creating social media profiles and email accounts for impersonation.
3. **Exploitation for Client Execution (T1203)**: Using malicious documents with exploits.
4. **Gather Victim Identity Information: Email Addresses (T1589.002)**: Collecting email addresses through open-source research.
5. **Phishing: Spearphishing Attachment and Link (T1566.001, .002)**: Conducting email campaigns with malicious attachments and links.
6. **Search Closed Sources and Open Websites/Domains (T1597, T1593.001)**: Utilizing business databases and social media for information gathering.
7. **Stage Capabilities: Upload Malware (T1608.001)**: Uploading malicious payloads to file-sharing services.
8. **User Execution: Malicious Link and File (T1204.001, .002)**: Luring users to execute malicious payloads.
9. **Web Service (T1102)**: Using file-sharing services for payload delivery.

Software Used by EXOTIC LILY

EXOTIC LILY is known to use several software tools, including:

1. **Bazar (S0534)**: A backdoor used for various malicious activities, including data exfiltration and command execution.
2. **Bumblebee (S1039)**: A loader and backdoor capable of bypassing user account control and

Ferocious Kitten - Group Overview

Description:

Ferocious Kitten is a cyber threat group known for its covert surveillance activities targeting Persian-speaking individuals in Iran. The group has been active since at least 2015 and is noted for its use of sophisticated cyber espionage tactics.

Motivation:

The primary motivation of Ferocious Kitten appears to be intelligence gathering and surveillance, particularly focusing on individuals within Iran.

Names:

The group is primarily known as Ferocious Kitten.

Location:

While the specific location of Ferocious Kitten is not detailed, their primary target region is Iran.

First Seen:

Their activities were first observed in 2015.

Observed:

Ferocious Kitten has been observed employing various cyber espionage techniques, including spearphishing, domain masquerading, and the use of open-source tools for malicious purposes.

Techniques Used in all tactics

Ferocious Kitten employs a range of techniques, including:

1. **Acquire Infrastructure: Domains (T1583.001):** Acquiring domains that imitate legitimate sites.
2. **Masquerading: Right-to-Left Override (T1036.002):** Using right-to-left override to disguise executable file names.
3. **Masquerading: Match Legitimate Name or Location (T1036.005):** Naming malicious files as `update.exe` and placing them in common folders.
4. **Obtain Capabilities: Tool (T1588.002):** Utilizing open-source tools like JsonCPP and Psiphon.
5. **Phishing: Spearphishing Attachment (T1566.001):** Conducting spearphishing campaigns with malicious document attachments.

5. User Execution: Malicious File (11204.002): Convincing victims to enable malicious content within spearphishing emails.

Software Used by Ferocious Kitten

Ferocious Kitten is known to use several software tools, including:

1. **BITSAAdmin (S0190)**: Utilizing BITS jobs for various purposes, including exfiltration and tool transfer.
2. **MarkiRAT (S0652)**: A RAT with capabilities like capturing clipboard data, keylogging, screen capture, and more.

FIN10 - Group Overview

Description:

FIN10 is a financially motivated threat group that has been active since at least 2013, primarily targeting organizations in North America. The group is known for using stolen data exfiltrated from victims to extort organizations.

Motivation:

FIN10's primary motivation appears to be financial gain, achieved through cyber extortion and other financially motivated cybercrimes.

Names:

The group is commonly referred to as FIN10.

Location:

While specific details about the group's location are not provided, their primary targets have been organizations in North America.

First Seen:

FIN10's activities were first observed in 2013.

Observed:

FIN10 has been observed employing a variety of techniques for extortion, data theft, and maintaining access to victim networks.

Techniques Used in all tactics

1. **Boot or Log / Autostart Execution: Registry Run Keys / Startup Folder (T1547.001):** FIN10 has used the Registry option in PowerShell Empire to add a Run key for persistence.
2. **Command and Scripting Interpreter: PowerShell (T1059.001):** The group uses PowerShell for execution and to establish persistence with PowerShell Empire.
3. **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** Execution of malicious .bat files containing PowerShell commands.
4. **Indicator Removal: File Deletion (T1070.004):** Use of batch scripts and scheduled tasks to delete critical system files.
5. **Lateral Tool Transfer (T1570):** Deployment of Meterpreter stagers and SplinterRAT after moving laterally.
6. **Obtain Capabilities: Tool (T1588.002):** Reliance on publicly-available software for initial footholds and persistence.
7. **Remote Services: Remote Desktop Protocol (T1021.001):** Use of RDP for lateral movement.
8. **Scheduled Task/Job: Scheduled Task (T1053.005):** Establishing persistence using S4U tasks and Scheduled Task option in PowerShell Empire.
9. **System Owner/User Discovery (T1033):** Enumeration of users on remote systems using Meterpreter.
10. **Valid Accounts (T1078):** Use of stolen credentials for remote access and lateral movement.

Software Used by FIN10

- **Empire (S0363):** A post-exploitation framework used for various purposes, including persistence, privilege escalation, and lateral movement.

FIN13 - Group Overview

Description:

FIN13 is a financially motivated cyber threat group that has been active since at least 2016. The group primarily targets the financial, retail, and hospitality industries in Mexico and Latin America. FIN13 is known for stealing intellectual property, financial data, mergers and acquisition information, or personally identifiable information (PII).

Motivation:

The primary motivation of FIN13 is financial gain, achieved through intellectual property theft, financial data exfiltration, and potentially other forms of cybercrime.

Names:

FIN13 is also associated with the name Elephant Beetle.

Location:

While specific details about the group's location are not provided, their primary targets have been organizations in Mexico and Latin America.

First Seen:

FIN13's activities were first observed in 2016.

Observed:

FIN13 has been observed employing a variety of techniques for data theft, maintaining access to victim networks, and conducting financial theft.

Techniques Used in all tactics

1. **Access Token Manipulation: Make and Impersonate Token (T1134.003):** Utilizing tools like Incognito V2 for token manipulation.
2. **Account Discovery (T1087):** Enumerating users and roles from victim systems.
3. **Account Manipulation (T1098):** Assigning sysadmin roles to new accounts for persistence.
4. **Application Layer Protocol: Web Protocols (T1071.001):** Using HTTP requests for web shell chaining and C2 communication.
5. **Archive Collected Data: Archive via Utility (T1560.001):** Compressing stolen credentials using 7zip.
6. **Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001):** Using Windows Registry run keys for persistence.
7. **Command and Scripting Interpreter: PowerShell (T1059.001):** Executing PowerShell commands for DNS data extraction.
8. **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** Leveraging cmd.exe and Windows Script Host for command execution.
9. **Create Account: Local Account (T1136.001):** Creating local MS-SQL accounts in compromised networks.
10. **Data from Local System (T1005):** Gathering stolen credentials and sensitive data for exfiltration.
11. **Data Manipulation (T1565):** Injecting fraudulent transactions to siphon off money.
12. **Data Staged: Local Data Staging (T1074.001):** Using temporary folders on compromised systems for staging data.
13. **Deobfuscate/Decode Files or Information (T1140):** Using certutil to decode base64 encoded malware.
14. **Develop Capabilities: Malware (T1587.001):** Utilizing custom malware for persistence.
15. **Exploit Public-Facing Application (T1190):** Exploiting known vulnerabilities for initial access.
16. **External Remote Services (T1133):** Gaining access via corporate VPNs.
17. **File and Directory Discovery (T1083):** Enumerating files and directories using Windows dir command.
18. **Financial Theft (T1657):** Observing victim's software and infrastructure for fraudulent transactions.
19. **Gather Victim Identity Information (T1589):** Researching employees for social engineering attacks.
20. **Gather Victim Network Information: Network Topology (T1590.004):** Searching for remote access infrastructure.
21. **Hide Artifacts: Hidden Files and Directories (T1564.001):** Creating hidden files and folders for stealth.
22. **Hijack Execution Flow: DLL Side-Loading (T1574.002):** Using side-loading techniques for malicious DLL execution.

23. **Ingress Tool Transfer (T1105)**: Downloading additional tools and malware.
24. **Input Capture: Keylogging (T1056.001)**: Logging keystrokes for privilege escalation.
26. **Masquerading (T1036)**: Using various masquerading techniques for stealth.
26. **Modify Authentication Process (T1556)**: Replacing legitimate binaries with trojanized versions.
27. **Network Service Discovery (T1046)**: Using tools like nmap for reconnaissance.
28. **Network Share Discovery (T1135)**: Executing net view commands for share enumeration.
29. **Obtain Capabilities: Tool (T1588.002)**: Utilizing publicly available tools like Mimikatz and Impacket.
30. **OS Credential Dumping (T1003)**: Dumping credentials from LSASS memory and NTDS.DIT file.
31. **Permission Groups Discovery (T1069)**: Enumerating users and roles from victim systems.
32. **Protocol Tunneling (T1572)**: Using web shells and Java tools for tunneling.
33. **Proxy: Internal Proxy (T1090.001)**: Utilizing internal proxy tools for communication.
34. **Remote Services: Remote Desktop Protocol (T1021.001)**: Accessing environments via RDP for lateral movement.
35. **Scheduled Task/Job: Scheduled Task (T1053.005)**: Creating scheduled tasks for persistence.
36. **Server Software Component: Web Shell (T1505.003)**: Utilizing web shells for remote code execution.
37. **System Information Discovery (T1082)**: Collecting host and network information.
38. **System Network Configuration Discovery (T1016)**: Using nslookup and ipconfig for network reconnaissance.
39. **Unsecured Credentials: Credentials In Files (T1552.001)**: Obtaining credentials from local files.
40. **Use Alternate Authentication Material: Pass the Hash (T1550.002)**: Executing pass the hash for lateral movement.
41. **Valid Accounts: Default Accounts (T1078.001)**: Leveraging default credentials for initial access.
42. **Windows Management Instrumentation (T1047)**: Using WMI for command execution and lateral movement.

Software Used by FIN13

- **certutil (S0160)**: Used for various purposes including data archiving and decoding.
- **Empire (S0363)**: A post-exploitation framework used for various purposes, including persistence, privilege escalation, and lateral movement.
- **Impacket (S0357)**: A collection of Python classes for working with network protocols.
- **Mimikatz (S0002)**: A tool to extract plaintext passwords, hash, PIN code, and kerberos tickets from memory.

FIN4 - Group Overview

Description:

FIN4 is a financially-motivated threat group known for targeting confidential information related to the public financial market. Active since at least 2013, their primary focus has been on healthcare and pharmaceutical companies. Unlike many cyber threat groups, FIN4 does not typically use persistent malware; instead, they concentrate on capturing credentials authorized to access email and other non-malware communications.

Motivation:

FIN4's primary motivation appears to be financial gain, achieved through the acquisition of sensitive information related to the stock market, particularly in the healthcare and pharmaceutical sectors.

Names:

FIN4 is the primary name associated with this threat group.

Location:

The specific location of FIN4 is not detailed in the available information.

First Seen:

FIN4's activities have been observed since at least 2013.

Observed:

FIN4 has been observed employing various techniques to capture sensitive information and credentials, often focusing on email hijacking and credential theft rather than deploying traditional malware.

Techniques Used in all tactics

1. **Application Layer Protocol: Web Protocols (T1071.001):** FIN4 has used HTTP POST requests to transmit data.
2. **Command and Scripting Interpreter: Visual Basic (T1059.005):** Utilization of VBA macros to display dialog boxes and collect credentials.
3. **Email Collection: Remote Email Collection (T1114.002):** Accessing and hijacking online email communications using stolen credentials.
4. **Hide Artifacts: Email Hiding Rules (T1564.008):** Creating rules in Outlook accounts to automatically delete emails containing certain keywords.
5. **Input Capture: Keylogging (T1056.001):** Capturing credentials via fake login pages and a .NET-based keylogger.
6. **Input Capture: GUI Input Capture (T1056.002):** Presenting spoofed Windows Authentication prompts to collect credentials.
7. **Phishing: Spearphishing Attachment (T1566.001):** Using spearphishing emails with attachments containing malicious macros.
8. **Phishing: Spearphishing Link (T1566.002):** Sending spearphishing emails containing malicious links.
9. **Proxy: Multi-hop Proxy (T1090.003):** Using Tor to log into victims' email accounts.
10. **User Execution: Malicious Link (T1204.001):** Luring victims to click malicious links in spearphishing emails.
11. **User Execution: Malicious File (T1204.002):** Encouraging victims to launch malicious attachments in spearphishing emails.

Software Used by FIN4

FIN4 primarily uses custom tools and techniques tailored to their specific method of operation, focusing on credential theft and email hijacking. Specific software names are not mentioned in the provided information, but their tactics involve the use of VBA macros, .NET-based keyloggers, and possibly other custom-developed tools for credential capture and email manipulation.

FIN5 - Group Overview

Description:

FIN5 is a financially motivated threat group known for targeting personally identifiable information (PII) and payment card information. Active since at least 2008, FIN5 has primarily targeted industries such as restaurants, gaming, and hotels. The group consists of actors who likely speak Russian.

Motivation:

FIN5's primary motivation is financial gain, achieved through the theft of sensitive personal and financial data.

Names:

FIN5 is the primary name associated with this threat group.

Location:

The specific location of FIN5 is not detailed in the available information, but the group is believed to comprise Russian-speaking actors.

First Seen:

FIN5's activities have been observed since at least 2008.

Observed:

FIN5 has been observed employing various techniques to capture sensitive information, focusing on automated collection, brute force attacks, and the use of external remote services.

Techniques Used in all tactics

1. **Automated Data Collection (T1115):** FIN5 uses scripts to scan processes on all systems in the environment and automate data collection.
2. **Brute Force (T1110):** Utilization of tools like GET2 Penetrator to search for remote login and hard-coded credentials.
3. **Command and Scripting Interpreter (T1059):** Execution of automated scripts for scanning processes.
4. **Data Staged: Local Data Staging (T1074.001):** Scripts save memory dump data in specific directories on hosts.
5. **External Remote Services (T1133):** Use of legitimate VPN, Citrix, or VNC credentials for access.
6. **Indicator Removal: Clear Windows Event Logs (T1070.001) and File Deletion (T1070.004):** Clearing event logs and using SDelete for cleanup.
7. **Obtain Capabilities: Tool (T1588.002):** Acquisition and use of tools like a customized PsExec, pwdump, SDelete, and Windows Credential Editor.
8. **Proxy: External Proxy (T1090.002):** Maintaining access via FLIPSIDE to create a proxy for backup RDP tunnel.
9. **Remote System Discovery (T1018):** Using tools like Essential NetTools for network mapping.
10. **Valid Accounts (T1078):** Using legitimate credentials for maintained access.

Software Used by FIN5

1. **FLIPSIDE:** Used for protocol tunneling.
2. **PsExec:** A customized version for creating accounts, modifying system processes, and lateral movement.
3. **pwdump:** For dumping OS credentials.
4. **RawPOS:** Employed for data collection, staging, and masquerading tasks.
5. **SDelete:** Used for data destruction and indicator removal.
6. **Windows Credential Editor:** For dumping credentials from LSASS memory.

FIN6 - Group Overview

Description:

FIN6 is a cybercrime group known for stealing payment card data and selling it on underground marketplaces. They have aggressively targeted and compromised Point of Sale (PoS) systems, predominantly in the hospitality and retail sectors.

Motivation:

FIN6 is financially motivated, focusing on the theft and sale of payment card data for profit.

Names:

- FIN6
- Associated Groups: Magecart Group 6, ITG08, Skeleton Spider

Locations:

The specific location of FIN6 is not detailed in the available information.

First Seen:

FIN6's activities have been observed since at least 2016.

Observed:

FIN6 has been noted for its aggressive tactics in compromising PoS systems and its sophisticated methods of data exfiltration and sale.

Techniques Used in all tactics

1. **Access Token Manipulation (T1134):** Used Metasploit's named-pipe impersonation for privilege escalation.
2. **Account Discovery: Domain Account (T1087.002):** Employed Metasploit's PsExec NTDSGRAB module for Active Directory database access.
3. **Archive Collected Data (T1560):** Compressed log files into ZIP archives before staging and exfiltration.
4. **Automated Collection (T1119):** Scripted iteration through compromised PoS systems for data collection.
5. **Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001):** Established persistence for downloader tools.
6. **Brute Force: Password Cracking (T1110.002):** Extracted password hashes for offline cracking.
7. **Command and Scripting Interpreter (T1059):** Used for executing scripts on compromised systems.
8. **Credentials from Password Stores (T1555):** Employed Stealer One credential stealer for targeting email and FTP utilities.
9. **Data from Information Repositories (T1213):** Collected schemas and user accounts from SQL Server systems.
10. **Data from Local System (T1005):** Gathered and exfiltrated payment card data.
11. **Data Staged: Remote Data Staging (T1074.002):** Compressed data from remote systems for staging.
12. **Encrypted Channel: Asymmetric Cryptography (T1573.002):** Used Plink for SSH tunnel creation.
13. **Exploitation for Privilege Escalation (T1068):** Exploited Windows vulnerabilities for privilege escalation.
14. **Impair Defenses: Disable or Modify Tools (T1562.001):** Deployed scripts to disable anti-virus.
15. **Indicator Removal: File Deletion (T1070.004):** Removed files from victim machines.
16. **Masquerading: Masquerade Task or Service (T1036.004):** Renamed services to masquerade as legitimate.
17. **Network Service Discovery (T1046):** Used tools for internal network mapping and reconnaissance.
18. **Obfuscated Files or Information: Command Obfuscation (T1027.010):** Encoded PowerShell commands.
19. **Obtain Capabilities: Tool (T1588.002):** Acquired tools like MimiKatz and Cobalt Strike.
20. **OS Credential Dumping (T1003):** Used Windows Credential Editor for LSASS memory.

dumping.

21. **Phishing: Spearphishing Attachment (T1566.001):** Targeted victims with malicious email attachments.
22. **Protocol Tunneling (T1572):** Created SSH tunnels using Plink.
23. **Remote Services: Remote Desktop Protocol (T1021.001):** Used RDP for lateral movement.
24. **Scheduled Task/Job: Scheduled Task (T1053.005):** Established persistence for malware.
25. **Subvert Trust Controls: Code Signing (T1553.002):** Used Comodo code-signing certificates.
26. **System Services: Service Execution (T1569.002):** Created services for executing encoded commands.
27. **User Execution: Malicious File (T1204.002):** Lured victims to execute malicious files.
28. **Valid Accounts (T1078):** Used stolen credentials for lateral movement.
29. **Web Service (T1102):** Utilized Pastebin and Google Storage for hosting operations.
30. **Windows Management Instrumentation (T1047):** Automated remote execution of scripts.

Software Used by FIN6

1. AdFind
2. Cobalt Strike
3. FlawedAmmyy
4. FrameworkPOS
5. GrimAgent
6. LockerGoga
7. Maze
8. Mimikatz
9. More_eggs
10. PsExec
11. Ryuk
12. Windows Credential Editor

FIN7 - Group Overview

Description:

FIN7 is a financially-motivated threat group that has been active since 2013. Known for targeting a wide range of industries including retail, restaurant, hospitality, and more, FIN7 is notorious for its use of point-of-sale malware and sophisticated cyber attacks. They have been linked to the use of REvil ransomware and their own Ransomware as a Service (RaaS), Darkside.

Motivation:

FIN7's primary motivation is financial gain, achieved through cyber attacks targeting sensitive financial data.

Names:

- FIN7

- Associated Groups: GOLD NIAGARA, ITG14, Carbon Spider

Location:

The specific location of FIN7 is not detailed in the available information.

First Seen:

FIN7's activities have been observed since at least 2013.

Observed:

FIN7 has been noted for its diverse targeting across various industries and its shift to big game hunting (BGH) tactics, including the use of ransomware.

Techniques Used in all tactics

1. **Acquire Infrastructure: Domains (T1583.001)**: Registered look-alike domains for phishing.
2. **Application Layer Protocol: DNS (T1071.004)**: Performed C2 using DNS.
3. **Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)**: Created Registry Run and RunOnce keys for persistence.
4. **Command and Scripting Interpreter (T1059)**: Used various scripting languages for tasks execution.
5. **Create or Modify System Process: Windows Service (T1543.003)**: Created new Windows services for persistence.
6. **Data Encrypted for Impact (T1486)**: Employed Darkside ransomware for data encryption.
7. **Develop Capabilities: Malware (T1587.001)**: Developed malware, including infected removable media.
8. **Event Triggered Execution: Application Shimming (T1546.011)**: Used application shim databases for persistence.
9. **Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)**: Exfiltrated data to MEGA file sharing site.
10. **Exploitation of Remote Services (T1210)**: Exploited ZeroLogon vulnerability.
11. **Ingress Tool Transfer (T1105)**: Downloaded additional malware for execution.
12. **Inter-Process Communication: Dynamic Data Exchange (T1559.002)**: Used DDE in spear phishing campaigns.
13. **Masquerading: Masquerade Task or Service (T1036.004)**: Created tasks like "AdobeFlashSync" for persistence.
14. **Non-Standard Port (T1571)**: Used port-protocol mismatches for C2.
15. **Obfuscated Files or Information: Command Obfuscation (T1027.010)**: Employed various obfuscation techniques.
16. **Obtain Capabilities: Tool (T1588.002)**: Utilized tools like Cobalt Strike and PowerSploit.
17. **Phishing: Spearphishing Attachment (T1566.001)**: Sent spearphishing emails with malicious attachments.
18. **Remote Access Software (T1219)**: Used remote management tools like Atera.
19. **Remote Services: RDP, SSH, VNC (T1021)**: Used various remote services for lateral movement.
20. **Replication Through Removable Media (T1091)**: Mailed USB drives containing malware.
21. **Scheduled Task/Job: Scheduled Task (T1053.005)**: Created tasks for malware

- persistence.
- 22. **Screen Capture (T1113):** Captured screenshots and desktop recordings.
 - 23. **Stage Capabilities: Upload Malware (T1608.001):** Staged trojanized software on Amazon S3.
 - 24. **Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003):** Used Kerberoasting for credential access.
 - 25. **Subvert Trust Controls: Code Signing (T1553.002):** Digitally signed payloads and tools.
 - 26. **Supply Chain Compromise: Compromise Software Supply Chain (T1195.002):** Gained access via software supply chain compromise.
 - 27. **System Binary Proxy Execution: Mshta, Rundll32 (T1218.005, .011):** Used system binaries for execution.
 - 28. **System Owner/User Discovery (T1033):** Collected user session information.
 - 29. **User Execution: Malicious Link/File (T1204.001, .002):** Lured victims to execute malicious content.
 - 30. **Valid Accounts (T1078):** Harvested valid credentials for lateral movement.
 - 31. **Video Capture (T1125):** Created custom video recording capabilities.
 - 32. **Virtualization/Sandbox Evasion: User Activity Based Checks (T1497.002):** Used embedded images in documents for evasion.
 - 33. **Web Service: Bidirectional Communication (T1102.002):** Used services like Google Docs for C2.
 - 34. **Windows Management Instrumentation (T1047):** Installed malware using WMI.

Software Used by FIN7

- 1. AdFind
- 2. BOOSTWRITE
- 3. Carbanak
- 4. Cobalt Strike
- 5. CrackMapExec
- 6. GRIFFON
- 7. HALFBAKED
- 8. JSS Loader
- 9. Lizar
- 10. Mimikatz
- 11. Pillowmint
- 12. POWERSOURCE
- 13. PowerSploit
- 14. RDFSNIFFER
- 15. REvil
- 16. SQLRat
- 17. TEXTMATE

FIN8 - Group Overview

Description:

FIN8 is a financially motivated threat group, active since at least January 2016. They are known for targeting various sectors including hospitality, retail, entertainment, insurance, technology, chemical, and financial. Notably, in June 2021, FIN8 shifted focus from targeting point-of-sale

Motivation:

FIN8's primary motivation is financial gain, achieved through sophisticated cyber attacks targeting sensitive financial data and systems.

Names:

- FIN8
- Associated Groups: Syssphinx

Location:

The specific location of FIN8 is not detailed in the available information.

First Seen:

FIN8's activities have been observed since at least January 2016.

Observed:

FIN8 has been noted for its diverse targeting across various industries and its shift from POS device targeting to ransomware distribution.

Techniques Used in all tactics

1. **Access Token Manipulation: Token Impersonation/Theft (T1134.001):** Used a malicious framework for impersonation.
2. **Application Layer Protocol: Web Protocols (T1071.001):** Used HTTPS for command and control.
3. **Archive Collected Data: Archive via Utility (T1560.001):** Used RAR for data compression before exfiltration.
4. **Command and Scripting Interpreter: PowerShell (T1059.001):** Executed payloads and used for lateral movement and credential access.
5. **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** Automated post-compromise activities and executed remote commands.
6. **Data Encrypted for Impact (T1486):** Deployed ransomware like Ragnar Locker and White Rabbit.
7. **Data Staged: Remote Data Staging (T1074.002):** Aggregated staged data from a network.
8. **Domain Trust Discovery (T1482):** Retrieved a list of trusted domains.
9. **Encrypted Channel: Asymmetric Cryptography (T1573.002):** Used Plink utility for tunneling RDP.
10. **Event Triggered Execution: Windows Management Instrumentation Event Subscription (T1546.003):** Used for persistence.
11. **Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003):** Used FTP for data exfiltration.
12. **Exploitation for Privilege Escalation (T1068):** Exploited CVE-2016-0167

13. **Indicator Removal: Clear Windows Event Logs (T1070.001):** Cleared logs during post-compromise activities.
14. **Indicator Removal: File Deletion (T1070.004):** Deleted temporary and prefetch files.
15. **Ingress Tool Transfer (T1105):** Downloaded subsequent payloads.
16. **Modify Registry (T1112):** Deleted registry keys during cleanup.
17. **Obfuscated Files or Information: Command Obfuscation (T1027.010):** Used various methods for command-line obfuscation.
18. **Obtain Capabilities: Tool (T1588.002):** Utilized tools like Impacket.
19. **OS Credential Dumping: LSASS Memory (T1003.001):** Harvested credentials using tools like Invoke-Mimikatz.
20. **Phishing: Spearphishing Attachment (T1566.001):** Distributed targeted emails with malicious documents.
21. **Process Injection: Asynchronous Procedure Call (T1055.004):** Injected code into processes.
22. **Remote Services: Remote Desktop Protocol (T1021.001):** Used RDP for lateral movement.
23. **Remote Services: SMB/Windows Admin Shares (T1021.002):** Used for lateral movement and mapping.
24. **Remote System Discovery (T1018):** Used Active Directory utilities for host enumeration.
25. **Scheduled Task/Job: Scheduled Task (T1053.005):** Maintained RDP backdoors.
26. **Software Discovery: Security Software Discovery (T1518.001):** Detected and avoided potential sandboxes.
27. **System Information Discovery (T1082):** Checked architecture before selecting malware versions.
28. **System Network Configuration Discovery: Internet Connection Discovery (T1016.001):** Checked connectivity to C2 servers.
29. **System Owner/User Discovery (T1033):** Displayed session details of compromised machines.
30. **User Execution: Malicious Link/File (T1204.001, .002):** Lured victims to install malware.
31. **Valid Accounts (T1078):** Used for persistence and lateral movement.
32. **Web Service (T1102):** Used services like sslip.io for traffic encryption.
33. **Windows Management Instrumentation (T1047):** Launched malware and executed commands.

Software Used by FIN8

1. BADHATCH
2. dsquery
3. Impacket
4. Net
5. Nltest
6. Ping
7. PsExec
8. PUNCHBUGGY
9. PUNCHTRACK
10. Ragnar Locker
11. Sardonic

Fox Kitten - Group Overview

Description:

Fox Kitten is a threat actor with suspected ties to the Iranian government, active since at least 2017. They have targeted a wide range of entities across the Middle East, North Africa, Europe, Australia, and North America. Fox Kitten's operations span multiple industrial verticals, including oil and gas, technology, government, defense, healthcare, manufacturing, and engineering.

Motivation:

Fox Kitten's primary motivation appears to be espionage and intelligence gathering, likely in support of national interests aligned with the Iranian government.

Names:

- Fox Kitten
- Associated Groups: UNC757, Parisite, Pioneer Kitten

Location:

While specific operational locations are not detailed, Fox Kitten is believed to have a nexus to the Iranian government.

First Seen:

Fox Kitten's activities have been observed since at least 2017.

Observed:

Fox Kitten has been noted for its broad targeting scope and sophisticated cyber operations across various industries and geographical regions.

Techniques Used in all tactics

1. **Account Discovery (T1087):** Accessed local and domain accounts.
2. **Archive Collected Data: Archive via Utility (T1560.001):** Used 7-Zip for data archiving.
3. **Browser Information Discovery (T1217):** Utilized Google Chrome bookmarks.
4. **Brute Force (T1110):** Brute-forced RDP credentials.
5. **Command and Scripting Interpreter (T1059):** Used Perl reverse shell, PowerShell scripts, and cmd.exe.
6. **Create Account: Local Account (T1136.001):** Created local user accounts with administrative privileges.
7. **Credentials from Password Stores: Password Managers (T1555.005):** Accessed KeePass database.
8. **Data from Cloud Storage (T1530):** Obtained files from cloud storage.
9. **Data from Information Repositories (T1213):** Accessed security and IT environments, Microsoft Teams.
10. **Data from Local System (T1005):** Searched local system resources.

11. Data from Network Shared Drive (T1039): Searched network shares.
12. Establish Accounts (T1585): Created KeyBase and social media accounts.
13. Event Triggered Execution: Accessibility Features (T1546.008): Used sticky keys.
14. Exploit Public-Facing Application (T1190): Exploited vulnerabilities in VPN appliances.
15. Exploitation of Remote Services (T1210): Exploited vulnerabilities in remote services.
16. File and Directory Discovery (T1083): Used WizTree for file and directory listings.
17. Ingress Tool Transfer (T1105): Downloaded tools like PsExec.
18. Masquerading (T1036): Named tasks and binaries to appear legitimate.
19. Network Service Discovery (T1046): Used tools like NMAP for scanning.
20. Obfuscated Files or Information (T1027): Base64 encoded payloads and scripts.
21. OS Credential Dumping (T1003): Used prodump and Volume Shadow Copy.
22. Protocol Tunneling (T1572): Used tunneling for communication and RDP.
23. Proxy (T1090): Utilized reverse proxy tools.
24. Query Registry (T1012): Accessed Registry hives.
25. Remote Services (T1021): Used RDP, SMB, SSH, and VNC for lateral movement.
26. Remote System Discovery (T1018): Used Angry IP Scanner.
27. Scheduled Task/Job: Scheduled Task (T1053.005): Used for persistence and execution.
28. Server Software Component: Web Shell (T1505.003): Installed web shells.
29. Unsecured Credentials: Credentials in Files (T1552.001): Accessed files for credentials.
30. Valid Accounts (T1078): Used valid credentials for lateral movement.
31. Web Service (T1102): Used AWS for hosting C2.

Software Used by Fox Kitten

1. China Chopper (S0020): Web shell used for various malicious activities.
2. ngrok (S0508): Used for dynamic resolution, exfiltration, and proxy.
3. Pay2Key (S0556): Ransomware used for data encryption and impact.
4. PsExec (S0029): Tool for system process creation and lateral movement.

GALLIUM - Group Overview

Description:

GALLIUM is a cyberespionage group active since at least 2012, primarily targeting telecommunications companies, financial institutions, and government entities. Their activities have been observed in various countries including Afghanistan, Australia, Belgium, Cambodia, Malaysia, Mozambique, the Philippines, Russia, and Vietnam. GALLIUM is identified as a likely Chinese state-sponsored group, based on their tools and tactics, techniques, and procedures (TTPs) commonly associated with Chinese threat actors.

Motivation:

GALLIUM's primary motivation appears to be espionage, likely driven by state-sponsored objectives to gather intelligence from targeted countries and industries.

Names:

- Associated Groups: Operation Soft Cell

Location:

While specific operational locations are not detailed, GALLIUM is believed to be based in China.

First Seen:

GALLIUM's activities have been observed since at least 2012.

Observed:

GALLIUM has been noted for its sophisticated cyber operations targeting a range of sectors and geographical regions, indicative of a broad intelligence-gathering mission.

Techniques Used in all tactics

1. **Acquire Infrastructure: Server (T1583.004):** Used Taiwan-based servers exclusive to GALLIUM.
2. **Archive Collected Data: Archive via Utility (T1560.001):** Employed WinRAR for data compression and encryption.
3. **Command and Scripting Interpreter: PowerShell (T1059.001):** Utilized PowerShell for execution, lateral movement, and credential dumping.
4. **Create Account: Domain Account (T1136.002):** Created high-privileged domain user accounts.
5. **Data from Local System (T1005):** Collected data including password hashes.
6. **Data Staged: Local Data Staging (T1074.001):** Compressed and staged files in the Recycle Bin.
7. **Exfiltration Over C2 Channel (T1041):** Used Web shells and HTRAN for data exfiltration.
8. **Exploit Public-Facing Application (T1190):** Exploited vulnerabilities in servers and VPN appliances.
9. **External Remote Services (T1133):** Utilized VPN services for access and persistence.
10. **Hijack Execution Flow: DLL Side-Loading (T1574.002):** Employed DLL side-loading techniques.
11. **Ingress Tool Transfer (T1105):** Dropped additional tools including PsExec.
12. **Lateral Tool Transfer (T1570):** Used PsExec for lateral movement.
13. **Masquerading: Rename System Utilities (T1036.003):** Renamed cmd.exe for evasion.
14. **Obfuscated Files or Information (T1027):** Obfuscated payloads and scripts.
15. **Obtain Capabilities: Tool (T1588.002):** Used a variety of tools, some modified.
16. **OS Credential Dumping: LSASS Memory (T1003.001):** Employed Mimikatz for credential dumping.
17. **Proxy: External Proxy (T1090.002):** Used HTRAN for connection redirection.
18. **Remote System Discovery (T1018):** Utilized NBTscan and ping for system discovery.
19. **Scheduled Task/Job: Scheduled Task (T1053.005):** Established persistence via scheduled tasks.
20. **Server Software Component: Web Shell (T1505.003):** Installed web shells for persistence.
21. **Subvert Trust Controls: Code Signing (T1553.002):** Used stolen certificates for tool signing.

- 22. **System Network Configuration Discovery (T1010):** Gathered network configuration data.
- 23. **System Network Connections Discovery (T1049):** Used netstat for network connections information.
- 24. **System Owner/User Discovery (T1033):** Employed whoami and query user.
- 25. **Use Alternate Authentication Material: Pass the Hash (T1550.002):** Authenticated via pass the hash.
- 26. **Valid Accounts (T1078):** Leveraged valid accounts for network access.
- 27. **Windows Management Instrumentation (T1047):** Used WMI for execution and tool installation.

Software Used by GALLIUM

- 1. **at (S0110):** Scheduled tasks.
- 2. **BlackMould (S0564):** Various malicious activities.
- 3. **China Chopper (S0020):** Web shell for command execution and data collection.
- 4. **cmd (S0106):** Command execution and system information gathering.
- 5. **HTRAN (S0040):** Connection redirection and proxy.
- 6. **ipconfig (S0100):** Network configuration discovery.
- 7. **Mimikatz (S0002):** Credential dumping.
- 8. **NBTscan (S0590):** Network service and system discovery.
- 9. **Net (S0039):** Account discovery and network share access.
- 10. **Ping (S0097):** Remote system discovery.
- 11. **PingPull (S1031):** Various malicious activities including data exfiltration.
- 12. **PlugX (S0013):** Command execution, data collection, and persistence.
- 13. **PoisonIvy (S0012):** Command execution, data collection, and persistence.
- 14. **Psexec (S0029):** Lateral movement and system process creation.
- 15. **Reg (S0075):** Registry query and modification.
- 16. **Windows Credential Editor (S0005):** Credential dumping.

Gallmaker - Group Overview

Description:

Gallmaker is a cyberespionage group known for targeting entities in the Middle East, particularly in the defense, military, and government sectors. Active since at least December 2017, Gallmaker is noted for its use of "living off the land" tactics, relying on tools that are already present on the victim's system rather than deploying their own malware.

Motivation:

The primary motivation of Gallmaker appears to be espionage, with a focus on gathering intelligence from defense, military, and government sectors.

Names:

- Gallmaker

Location:

While specific operational locations are not detailed, Gallmaker's activities have predominantly targeted entities in the Middle East.

First Seen:

Gallmaker's activities have been observed since at least December 2017.

Observed:

Gallmaker has been noted for its sophisticated cyber operations targeting specific sectors, indicative of a targeted intelligence-gathering mission.

Techniques Used in all tactics

1. **Archive Collected Data: Archive via Utility (T1560.001)**: Gallmaker has utilized WinZip, likely for archiving data prior to exfiltration.
2. **Command and Scripting Interpreter: PowerShell (T1059.001)**: Used PowerShell to download additional payloads and for execution.
3. **Inter-Process Communication: Dynamic Data Exchange (T1559.002)**: Attempted to exploit Microsoft's DDE protocol for access and execution.
4. **Obfuscated Files or Information (T1027)**: Employed obfuscation techniques for shellcode used during execution.
5. **Phishing: Spearphishing Attachment (T1566.001)**: Sent emails with malicious Microsoft Office documents attached.
6. **User Execution: Malicious File (T1204.002)**: Distributed lure documents prompting victims to "enable content" for execution.

Software Used by Gallmaker

Gallmaker's approach of 'living off the land' suggests a reliance on pre-existing software and system tools rather than deploying custom malware. This strategy involves the use of legitimate system tools for malicious purposes, making detection more challenging. Specific software or tools used by Gallmaker, as per the provided information, include:

1. **WinZip**: For archiving collected data.
2. **PowerShell**: For downloading payloads and execution.
3. **Microsoft Office**: Utilized for crafting malicious documents used in spearphishing attacks.

Gamaredon Group - Group Overview

Description:

Gamaredon Group is a cyber espionage threat group suspected to be linked to Russia's Federal Security Service (FSB). Active since at least 2013, the group primarily targets military, NGO, judiciary, law enforcement, and non-profit organizations in Ukraine. The group's name, "Gamaredon," is derived from a combination of "Gamma" and "Redon," referring to the chemical element radon.

Motivation:

The group's activities suggest a focus on intelligence gathering, likely for geopolitical purposes, given its targeting of Ukrainian entities and attribution to Russian state interests.

Names:

- Gamaredon Group
- IRON TILDEN
- Primitive Bear
- ACTINIUM
- Armageddon
- Shuckworm
- DEV-0157

Location:

While the group's exact location is not specified, it is attributed to Russia's FSB, indicating a potential base of operations in Russia.

First Seen:

Gamaredon Group's activities have been documented since at least 2013.

Observed:

The group has been observed conducting sophisticated cyber espionage operations, primarily targeting Ukrainian entities across various sectors.

Techniques Used in all tactics

1. **Acquire Infrastructure: Domains (T1583.001):** Used multiple domains for payload staging and C2.
2. **Application Layer Protocol: Web Protocols (T1071.001):** Employed HTTP and HTTPS for C2 communications.
3. **Automated Collection (T1119):** Deployed scripts for automatic scanning of documents.
4. **Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001):** Registered Run keys for persistence.
5. **Command and Scripting Interpreter: PowerShell, Windows Command Shell, Visual Basic (T1059):** Utilized various scripting methods for execution and C2.
6. **Data Destruction (T1485):** Used tools to delete files and folders.
7. **Exfiltration Over C2 Channel (T1041):** Transferred collected files to C2 servers.
8. **File and Directory Discovery (T1083):** Scanned for Microsoft Office files to inject with malicious macros.
9. **Hide Artifacts: Hidden Window (T1564.003):** Used hidcon for hidden batch file execution.
10. **Impair Defenses: Disable or Modify Tools (T1562.001):** Tampered with Microsoft Office

security settings.

11. **Indicator Removal: File Deletion (T1070.004)**: Deleted files used during operations.
12. **Inter-Process Communication: Component Object Model (T1559.001)**: Inserted malicious macros using Microsoft.Office.Interop object.
13. **Internal Spearphishing (T1534)**: Sent phishing emails with malicious attachments internally.
14. **Masquerading: Match Legitimate Name or Location (T1036.005)**: Used legitimate process names to hide malware.
15. **Modify Registry (T1112)**: Altered registry values for VBA macro execution.
16. **Obfuscated Files or Information (T1027)**: Delivered obfuscated scripts and payloads.
17. **Office Application Startup (T1137)**: Inserted malicious macros for persistence.
18. **Phishing: Spearphishing Attachment (T1566.001)**: Delivered spearphishing emails with malicious attachments.
19. **Process Discovery (T1057)**: Used tools to enumerate processes.
20. **Remote Services: VNC (T1021.005)**: Employed VNC tools for remote interaction.
21. **Scheduled Task/Job: Scheduled Task (T1053.005)**: Created scheduled tasks for execution.
22. **Screen Capture (T1113)**: Captured screenshots of compromised computers.
23. **Stage Capabilities: Upload Malware (T1608.001)**: Registered domains for payload staging.
24. **System Binary Proxy Execution: Mshta, Rundll32 (T1218)**: Used system binaries for execution.
25. **System Information Discovery (T1082)**: Gathered information about compromised systems.
26. **User Execution: Malicious File (T1204.002)**: Encouraged users to execute malicious files.
27. **Web Service (T1102)**: Used web services like Git-hub for downloader retrieval.

Software Used by Gamaredon Group

1. **Ping (S0097)**: For remote system discovery.
2. **PowerPunch (S0685)**: A PowerShell-based tool.
3. **Pteranodon (S0147)**: A backdoor malware.
4. **QuietSieve (S0686)**: Used for data collection and screen capture.

GCMAN – Group Overview

Description:

GCMAN is a cyber threat group known for targeting banks with the primary goal of transferring money to e-currency services. The group's activities involve sophisticated cyber attacks against financial institutions.

Motivation:

GCMAN's primary motivation appears to be financial gain, achieved through unauthorized bank transfers to e-currency services.

Names:

- GCMAN

Location:

The specific location of GCMAN is not detailed in the available information.

First Seen:

The group's activities were first reported in 2016.

Observed:

GCMAN has been observed conducting targeted attacks against banks, focusing on the illicit transfer of funds.

Techniques Used in all tactics

1. **Remote Services: SSH (T1021.004):** GCMAN has utilized SSH (Secure Shell) for lateral movement within a network. This technique involves using SSH to access and control systems remotely, often as part of an effort to move laterally to different areas of a network.
2. **Remote Services: VNC (T1021.005):** The group has employed VNC (Virtual Network Computing) for lateral movement. VNC is a graphical desktop-sharing system that allows remote control of another computer, which can be used for malicious purposes in a cyber attack.

Software Used by GCMAN

- **Putty:** A free and open-source terminal emulator, serial console, and network file transfer application. GCMAN uses Putty for lateral movement, leveraging its capabilities to remotely access and control systems within the target network.
- **VNC:** A graphical desktop-sharing system that uses the Remote Frame Buffer protocol to remotely control another computer. GCMAN employs VNC for lateral movement, utilizing it to gain control over systems within the target's network.

GOLD SOUTHFIELD - Group Overview

Description:

GOLD SOUTHFIELD is a financially motivated threat group known for operating the REvil Ransomware-as-a-Service (RaaS). Active since at least 2018, the group provides backend infrastructure for affiliates recruited on underground forums to carry out high-value ransomware deployments. In early 2020, GOLD SOUTHFIELD began stealing data and extorting victims to pay for their data to prevent public leaks.

Motivation:

The primary motivation of GOLD SOUTHFIELD is financial gain, achieved through ransomware attacks and data extortion.

Names:

- GOLD SOUTHFIELD
- Associated with Pinchy Spider

Location:

The specific location of GOLD SOUTHFIELD is not detailed in the available information.

First Seen:

The group's activities were first reported in 2018.

Observed:

GOLD SOUTHFIELD has been observed targeting a wide range of sectors, including exploiting public-facing applications and conducting phishing campaigns.

Techniques Used in all tactics

1. **Command and Scripting Interpreter: PowerShell (T1059.001):** GOLD SOUTHFIELD has executed PowerShell scripts on compromised hosts for staging and execution.
2. **Exploit Public-Facing Application (T1190):** The group has exploited vulnerabilities in Oracle WebLogic for initial compromise.
3. **External Remote Services (T1133):** Utilized publicly-accessible RDP and remote management and monitoring (RMM) servers for access.
4. **Obfuscated Files or Information: Command Obfuscation (T1027.010):** Executed base64 encoded PowerShell scripts on compromised hosts.
5. **Phishing (T1566):** Conducted malicious spam campaigns for access.
6. **Remote Access Software (T1219):** Used "ConnectWise Control" for deploying REvil ransomware.
7. **Screen Capture (T1113):** Employed ConnectWise to obtain screen captures from victim machines.
8. **Supply Chain Compromise: Compromise Software Supply Chain (T1195.002):** Distributed ransomware by backdooring software installers.
9. **Trusted Relationship (T1199):** Breached Managed Service Providers (MSPs) to deliver malware.

Software Used by GOLD SOUTHFIELD

- **ConnectWise (S0591):** Used for PowerShell command execution, screen capture, and video capture.
- **REvil Ransomware (S0496):** Employed for various malicious activities including data encryption, destruction, and exfiltration.

Gorgon Group - Group Overview

Description:

Gorgon Group is a threat actor suspected to have connections to Pakistan. The group has engaged in a mix of criminal and targeted attacks, including campaigns against government organizations in the United Kingdom, Spain, Russia, and the United States.

Motivation:

The Gorgon Group's activities suggest a combination of criminal financial motives and targeted attacks, possibly for espionage.

Names:

- Gorgon Group

Location:

The group is suspected to be Pakistan-based or have connections to Pakistan.

First Seen:

The specific date of the group's first activities is not provided in the available information.

Observed:

Gorgon Group has been observed targeting a variety of sectors, including government organizations in several countries.

Techniques Used in all tactics

1. **Boot or Logon Autostart Execution (T1547.001 & .009):** Creating .lnk files and adding Registry Run keys for persistence.
2. **Command and Scripting Interpreter (T1059.001, .003, .005):** Using PowerShell, cmd.exe, and VBScripts for execution and payload download.
3. **Deobfuscate/Decode Files or Information (T1140):** Decoding Base64 encoded payloads.
4. **Hide Artifacts: Hidden Window (T1564.003):** Concealing PowerShell windows.
5. **Impair Defenses: Disable or Modify Tools (T1562.001):** Disabling security features in Microsoft Office and Windows Defender.
6. **Ingress Tool Transfer (T1105):** Downloading additional files from C2 servers.
7. **Modify Registry (T1112):** Deactivating security mechanisms in Microsoft Office.
8. **Native API (T1106):** Leveraging Windows API for execution.
9. **Obtain Capabilities: Tool (T1588.002):** Using tools like QuasarRAT and Remcos.

10. **Phishing: Spearphishing Attachment (T1566.001):** Sending emails with malicious Microsoft Office documents.
11. **Process Injection (T1055.002 & .012):** Using portable executable injection and process hollowing.
12. **User Execution: Malicious File (T1204.002):** Encouraging users to launch malicious attachments.

Software Used by Gorgon Group

- **NanoCore (S0336):** A remote access tool with various capabilities including audio and video capture.
- **njRAT (S0385):** A remote access trojan used for command execution, data theft, and surveillance.
- **QuasarRAT (S0262):** A remote access tool used for system information discovery, keylogging, and remote control.
- **Remcos (S0332):** A comprehensive remote control tool with capabilities like keylogging, screen capture, and process injection.

Group5 - Group Overview

Description:

Group5 is a threat group with suspected ties to Iran, although this attribution is not definitive. The group has primarily targeted individuals connected to the Syrian opposition, employing spearphishing and watering hole attacks. Their campaigns often revolve around Syrian and Iranian themes.

Motivation:

The group's activities suggest a focus on espionage, particularly targeting opposition groups and individuals, likely for political intelligence gathering.

Names:

- Group5

Location:

The group is suspected to have an Iranian nexus.

First Seen:

The specific date of the group's first activities is not detailed in the provided information.

Observed:

Group5 has been observed targeting individuals connected to the Syrian opposition, using themes relevant to Syrian and Iranian interests.

Techniques Used in all tactics

1. **Indicator Removal: File Deletion (T1070.004)**: The malware used by Group5 can remotely delete files from victims' systems.
2. **Input Capture: Keylogging (T1056.001)**: Group5's malware has keylogging capabilities to capture keystrokes.
3. **Obfuscated Files or Information (T1027)**: The group disguises its malicious binaries with multiple layers of obfuscation, including encryption.
4. **Screen Capture (T1113)**: Group5's malware can capture screenshots, allowing the group to monitor victims' screens.

Software Used by Group5

- **NanoCore (S0336)**: A remote access tool with capabilities like audio capture, keylogging, and system network configuration discovery.
- **njRAT (S0385)**: A remote access trojan used for a variety of purposes, including command execution, data theft, and surveillance.

HAFNIUM - Group Overview

Description:

HAFNIUM is a cyber espionage group believed to be state-sponsored and operating out of China. Active since at least January 2021, HAFNIUM primarily targets a wide range of entities in the United States, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.

Motivation:

The group's activities suggest a focus on intelligence gathering, likely for strategic national interests.

Names:

- HAFNIUM
- Operation Exchange Marauder (Associated Group)

Location:

HAFNIUM is believed to operate out of China.

First Seen:

The group has been active since at least January 2021.

Observed:

HAFNIUM has been observed targeting a diverse set of sectors in the United States, indicating a broad intelligence collection mandate.

Techniques Used in all tactics

1. **Account Manipulation (T1098):** HAFNIUM has been known to grant privileges to domain accounts.
2. **Acquire Infrastructure (T1583.003 & .006):** The group operates from leased virtual private servers in the United States and acquires web services for C2 and exfiltration.
3. **Application Layer Protocol (T1071.001):** Utilization of open-source C2 frameworks like Covenant.
4. **Archive Collected Data (T1560.001):** Use of 7-Zip and WinRAR to compress stolen files for exfiltration.
5. **Command and Scripting Interpreter (T1059.001 & .003):** Execution of PowerShell scripts and commands via cmd.exe.
6. **Create Account: Domain Account (T1136.002):** Creation of domain accounts for operations.
7. **Data Encoding (T1132.001):** ASCII encoding used for C2 traffic.
8. **Email Collection: Remote Email Collection (T1114.002):** Use of web shells to export mailbox data.
9. **Exfiltration Over Web Service (T1567.002):** Data exfiltration to cloud storage services like MEGA.
10. **Exploit Public-Facing Application (T1190):** Exploitation of vulnerabilities in Microsoft Exchange Server.
11. **File and Directory Discovery (T1083):** Searching file contents on compromised hosts.
12. **Gather Victim Network Information (T1590):** Gathering FQDNs and IP addresses of Exchange servers.
13. **Hide Artifacts: Hidden Files and Directories (T1564.001):** Concealing files on compromised hosts.
14. **Ingress Tool Transfer (T1105):** Downloading tools like Nishang and PowerCat onto compromised hosts.
15. **OS Credential Dumping (T1003.001 & .003):** Dumping LSASS process memory and stealing Active Directory databases.
16. **Process Discovery (T1057):** Using tasklist to enumerate processes.
17. **Remote System Discovery (T1018):** Enumerating domain controllers.
18. **Server Software Component: Web Shell (T1505.003):** Deployment of multiple web shells.
19. **System Binary Proxy Execution: Rundll32 (T1218.011):** Using rundll32 to load malicious DLLs.
20. **System Network Configuration Discovery (T1016):** Collecting IP information and checking network connectivity.
21. **System Owner/User Discovery (T1033):** Gathering user information with whoami.
22. **Valid Accounts: Local Accounts (T1078.003):** Using the NT AUTHORITY\SYSTEM account for operations.

Software Used by HAFNIUM

- **ASPXSpy (S0073)**: A web shell used for server software component manipulation.
- **China Chopper (S0020)**: A web shell known for its small size and powerful capabilities.
- **Impacket (S0357)**: A collection of Python classes for working with network protocols.
- **PsExec (S0029)**: A tool for executing processes on other systems.
- **Tarrask (S1011)**: Malware used for token impersonation, command execution, and scheduled tasks.

HEXANE - Group Overview

Description:

HEXANE is a cyber espionage threat group that has been active since at least 2017. The group primarily targets organizations in the oil & gas, telecommunications, aviation, and internet service provider sectors. Their activities have predominantly focused on entities located in the Middle East and Africa, including Israel, Saudi Arabia, Kuwait, Morocco, and Tunisia. HEXANE's tactics, techniques, and procedures (TTPs) bear similarities to APT33 and OilRig, but due to differences in victims and tools, it is tracked as a separate entity.

Motivation:

The group's activities suggest a focus on espionage, likely aimed at gathering strategic intelligence in the energy and telecommunications sectors.

Names:

- HEXANE
- Associated Groups: Lyceum, Siamesekitten, Spirlin

Location:

HEXANE's operations have primarily targeted the Middle East and Africa.

First Seen:

The group has been active since at least 2017.

Observed:

HEXANE has been observed targeting a variety of sectors, with a focus on oil & gas, telecommunications, aviation, and internet service providers.

Techniques Used in all tactics

1. **Acquire Infrastructure (T1583.001 & .002)**: Registering domains and setting up custom

- DNS servers for command and control.
2. **Application Window Discovery (T1010)**: Using a PowerShell-based keylogging tool to capture window titles.
 3. **Brute Force (T1110 & .003)**: Employing brute force and password spraying attacks to compromise credentials.
 4. **Command and Scripting Interpreter (T1059.001 & .005)**: Utilizing PowerShell-based tools and scripts, and a VisualBasic script for execution.
 5. **Compromise Accounts (T1586.002)**: Compromising email accounts for spearphishing.
 6. **Credentials from Password Stores (T1555 & .003)**: Using tools to identify and steal stored credentials and passwords from web browsers.
 7. **Establish Accounts (T1585.001 & .002)**: Creating fraudulent social media and email accounts for targeting.
 8. **Exfiltration Over Web Service (T1567.002)**: Using cloud services like OneDrive for data exfiltration.
 9. **Gather Victim Identity Information (T1589 & .002)**: Identifying specific potential victims and collecting email addresses.
 10. **Ingress Tool Transfer (T1105)**: Downloading additional payloads and scripts onto compromised hosts.
 11. **Input Capture: Keylogging (T1056.001)**: Employing a PowerShell-based keylogger.
 12. **Internal Spearphishing (T1534)**: Conducting spearphishing attacks against internal targets.
 13. **Obfuscated Files or Information (T1027.010)**: Using Base64-encoded scripts.
 14. **Obtain Capabilities: Tool (T1588.002)**: Acquiring and customizing tools like Mimikatz and Empire.
 15. **Permission Groups Discovery: Local Groups (T1069.001)**: Enumerating local groups on compromised systems.
 16. **Process Discovery (T1057)**: Enumerating processes on targeted systems.
 17. **Remote Services: Remote Desktop Protocol (T1021.001)**: Using RDP for lateral movement.
 18. **Remote System Discovery (T1018)**: Enumerating domain machines.
 19. **Scheduled Task/Job: Scheduled Task (T1053.005)**: Establishing persistence for keyloggers.
 20. **Software Discovery (T1518)**: Enumerating installed programs.
 21. **Stage Capabilities: Upload Malware (T1608.001)**: Staging malware on fraudulent websites.
 22. **System Information Discovery (T1082)**: Collecting hostname information.
 23. **System Network Configuration Discovery (T1016 & .001)**: Using tools for network discovery and internet connectivity checks.
 24. **System Network Connections Discovery (T1049)**: Monitoring connections using netstat.
 25. **System Owner/User Discovery (T1033)**: Identifying the current user with whoami.
 26. **User Execution: Malicious File (T1204.002)**: Relying on victims executing malicious file attachments.
 27. **Web Service: Bidirectional Communication (T1102.002)**: Using cloud services for command and control.

Software Used by HEXANE

- **BITSAdmin (S0190)**: Used for BITS jobs and exfiltration.
- **DanBot (S1014), DnsSystem (S1021), Kevin (S1020), Milan (S1015), Shark (S1019)**: Various custom tools for command execution, data exfiltration, and C2 communication.
- **Empire (S0363)**: A post-exploitation framework.
- **Mimikatz (S0002)**: A tool for credential dumping and manipulation.
- **PoshC2 (S0378)**: A remote administration and post-exploitation framework.

Description:

Higaisa is a cyber threat group suspected to have origins in South Korea. The group has been active in targeting government, public, and trade organizations primarily in North Korea, but their activities have also extended to China, Japan, Russia, Poland, and other nations. Higaisa's operations include a mix of cyber espionage and targeted attacks, and the group has been active since at least 2009, with its activities first disclosed in early 2019.

Motivation:

Higaisa's activities suggest a focus on espionage and intelligence gathering, particularly targeting entities related to government and trade.

Names:

- Higaisa

Location:

The group has targeted entities primarily in North Korea, with additional activities in China, Japan, Russia, Poland, and other countries.

First Seen:

Higaisa has been operational since at least 2009, with public disclosure of its activities occurring in early 2019.

Observed:

Higaisa has been observed targeting a variety of sectors, with a particular focus on government, public, and trade organizations.

Techniques Used in all tactics

1. **Application Layer Protocol (T1071.001)**: Higaisa used HTTP and HTTPS for data exfiltration to C2 servers.
2. **Boot or Logon Autostart Execution (T1547.001)**: Added spoofed binaries to the startup folder for persistence.
3. **Command and Scripting Interpreter (T1059.003, .005, .007)**: Utilized cmd.exe, VBScript, and JavaScript for execution.
4. **Data Obfuscation (T1001.003)**: Employed FakeTLS sessions for C2 communications.
5. **Deobfuscate/Decode Files or Information (T1140)**: Used certutil for decoding Base64 binaries and XOR for data decryption.
6. **Encrypted Channel (T1573.001)**: Utilized AES-128 encryption for C2 traffic.

7. **Exfiltration: C2 Channel (T1041)**: Exfiltrated data via C2 channels.
8. **Exploitation for Client Execution (T1203)**: Exploited CVE-2018-0798 for execution.
9. **Hide Artifacts (T1564.003)**: Created payloads that operate in hidden windows.
10. **Hijack Execution Flow (T1574.002)**: Used DLL side-loading techniques.
11. **Masquerading (T1036.004)**: Named a shellcode loader binary to mimic legitimate system processes.
12. **Native API (T1106)**: Called various OS native APIs.
13. **Obfuscated Files or Information (T1027 & .001)**: Employed Base64 encoding and binary padding.
14. **Phishing: Spearphishing Attachment (T1566.001)**: Sent spearphishing emails with malicious attachments.
15. **Process Discovery (T1057)**: Attempted to find the process ID of the current process.
16. **Proxy: Internal Proxy (T1090.001)**: Utilized system proxy settings for C2 communication.
17. **Scheduled Task/Job: Scheduled Task (T1053.005)**: Dropped and added executables to scheduled tasks for persistence.
18. **Scheduled Transfer (T1029)**: Sent system identifiers to C2 server at regular intervals.
19. **System Information Discovery (T1082)**: Collected system volume serial number, GUID, and computer name.
20. **System Network Configuration Discovery (T1016)**: Used ipconfig for network configuration information.
21. **System Time Discovery (T1124)**: Gathered current system time.
22. **User Execution: Malicious File (T1204.002)**: Relied on users executing malicious email attachments.
23. **XSL Script Processing (T1220)**: Utilized XSL files to run VBScript code.

Software Used by Higaia

- **certutil (S0160)**: Used for decoding files and information, and transferring ingress tools.
- **gh0st RAT (S0032)**: A remote access tool with various capabilities including keylogging, process injection, and screen capture.
- **PlugX (S0013)**: A malware family known for its extensive capabilities, including command execution, data exfiltration, and system information discovery.

Inception - Group Overview

Description:

Inception is a sophisticated cyber espionage group that has been active since at least 2014. This group is known for its complex and multifaceted attacks, targeting multiple industries and governmental entities primarily in Russia. However, their activities have also spanned the United States, Europe, Asia, Africa, and the Middle East.

Motivation:

The primary motivation of Inception appears to be espionage, with a focus on gathering intelligence from a wide range of global targets.

Names:

- Inception
- Inception Framework
- Cloud Atlas

Location:

Inception has targeted entities primarily in Russia but has also been active in the United States, Europe, Asia, Africa, and the Middle East.

First Seen:

The group has been operational since at least 2014.

Observed:

Inception has been observed targeting a variety of sectors, including government organizations, across multiple regions.

Techniques Used in all tactics

1. **Application Layer Protocol (T1071.001)**: Utilized HTTP, HTTPS, and WebDav for network communications.
2. **Boot or Logon Autostart Execution (T1547.001)**: Maintained persistence by modifying Registry run key values.
3. **Command and Scripting Interpreter (T1059.001, .005)**: Executed malicious commands and payloads using PowerShell and VBScript.
4. **Credentials from Password Stores (T1555.003)**: Employed a browser plugin to steal passwords and sessions from various web browsers.
5. **Data from Local System (T1005)**: Used a file hunting plugin to collect sensitive files from infected hosts.
6. **Encrypted Channel (T1573.001)**: Encrypted network communications using AES.
7. **Exploitation for Client Execution (T1203)**: Exploited various vulnerabilities for execution, including CVE-2012-0158 and CVE-2017-11882.
8. **File and Directory Discovery (T1083)**: Collected information about files and directories on local and remote drives.
9. **Obfuscated Files or Information (T1027)**: Encrypted malware payloads with AES and RC4 encryption.
10. **Obtain Capabilities: Tool (T1588.002)**: Acquired and used open-source tools like LaZagne.
11. **Permission Groups Discovery: Domain Groups (T1069.002)**: Gathered domain membership information using malware modules.
12. **Phishing: Spearphishing Attachment (T1566.001)**: Used weaponized documents in spearphishing emails for initial compromise.
13. **Process Discovery (T1057)**: Identified active processes and associated loaded modules.
14. **Proxy: Multi-hop Proxy (T1090.003)**: Utilized compromised routers to proxy C2 communications.
15. **Software Discovery (T1518)**: Enumerated installed software on compromised systems.
16. **System Binary Proxy Execution: Mshta (T1218.005)**: Executed malicious HTA files.
17. **System Binary Proxy Execution: Regsvr32 (T1218.010)**: Ensured persistence using

- 18. **System Information Discovery (T1082)**: Gathered information about the operating system and hardware.
- 19. **Template Injection (T1221)**: Used decoy documents to load malicious remote payloads.
- 20. **User Execution: Malicious File (T1204.002)**: Lured victims into executing malicious files.
- 21. **Web Service (T1102)**: Incorporated cloud service providers into their C2 infrastructure.

Software Used by Inception

- **LaZagne (S0349)**: Used for extracting credentials from various sources on the infected host.
- **PowerShower (S0441)**: A PowerShell-based tool for various malicious activities including data encoding and system information discovery.
- **VBShower (S0442)**: A Visual Basic script used for execution and indicator removal.

IndigoZebra - Group Overview

Description:

IndigoZebra is a cyber espionage group suspected to have Chinese origins. Active since at least 2014, the group primarily targets Central Asian governments, employing sophisticated cyber espionage tactics.

Motivation:

The primary motivation of IndigoZebra appears to be espionage, focusing on gathering sensitive information from government entities in Central Asia.

Names:

- IndigoZebra

Location:

The group primarily targets Central Asian governments.

First Seen:

IndigoZebra has been active since at least 2014.

Observed:

The group has been observed conducting cyber espionage activities against Central Asian governments.

Techniques Used in all tactics

1. **Acquire Infrastructure: Domains (T1583.001)**: Established domains for operations, some mimicking official government domains.
2. **Acquire Infrastructure: Web Services (T1583.006)**: Created Dropbox accounts for operations.
3. **Compromise Accounts: Email Accounts (T1586.002)**: Compromised legitimate email accounts for spearphishing operations.
4. **Ingress Tool Transfer (T1105)**: Downloaded additional files and tools from its C2 server.
5. **Obtain Capabilities: Tool (T1588.002)**: Acquired open-source tools like NBTscan and Meterpreter.
6. **Phishing: Spearphishing Attachment (T1566.001)**: Sent spearphishing emails with malicious password-protected RAR attachments.
7. **User Execution: Malicious File (T1204.002)**: Urged recipients to review modifications in files attached to spearphishing emails, triggering the attack.

Software Used by IndigoZebra

- **BoxCaon (S0651)**: Used for various purposes including data exfiltration, file discovery, and command execution.
- **PoisonIvy (S0012)**: Employed for keylogging, process injection, and data exfiltration.
- **xCaon (S0653)**: Utilized for web protocol communication, data encoding, and software discovery.

Indrik Spider - Group Overview

Description:

Indrik Spider is a Russia-based cybercriminal group, active since at least 2014. Initially known for deploying the Dridex banking Trojan, the group shifted to ransomware operations around 2017, using BitPaymer, WastedLocker, and Hades ransomware. Following U.S. sanctions and an indictment in 2019, Indrik Spider diversified their tactics and toolset.

Motivation:

The primary motivation of Indrik Spider appears to be financial gain, primarily through banking Trojans and ransomware operations.

Names:

- Indrik Spider
- Associated with Evil Corp

Location:

Based in Russia, with global targets.

First Seen:

Active since at least 2014.

Observed:

Observed conducting banking fraud and ransomware operations globally.

Techniques Used in all tactics

1. **Command and Scripting Interpreter: PowerShell (T1059.001):** Used PowerShell Empire for malware execution.
2. **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** Employed batch scripts for execution.
3. **Compromise Infrastructure: Server (T1584.004):** Served fake updates via compromised legitimate websites.
4. **Create Account (T1136):** Utilized wmic.exe to add new users to systems.
5. **Data Encrypted for Impact (T1486):** Encrypted domain-controlled systems using BitPaymer.
6. **Data Staged: Local Data Staging (T1074.001):** Stored collected data in .tmp files.
7. **Develop Capabilities: Malware (T1587.001):** Developed malware, including BitPaymer and WastedLocker.
8. **Domain Policy Modification: Group Policy Modification (T1484.001):** Used Group Policy Objects to deploy scripts.
9. **Establish Accounts: Email Accounts (T1585.002):** Created email accounts for ransomware communications.
10. **Impair Defenses: Disable or Modify Tools (T1562.001):** Leveraged Windows Defender to disable scanning and real-time monitoring.
11. **Indicator Removal: Clear Windows Event Logs (T1070.001):** Used Cobalt Strike to clear log files.
12. **Ingress Tool Transfer (T1105):** Downloaded scripts, malware, and tools onto compromised hosts.
13. **Masquerading: Match Legitimate Name or Location (T1036.005):** Used fake updates for FlashPlayer and Google Chrome.
14. **OS Credential Dumping: LSASS Memory (T1003.001):** Employed Cobalt Strike for credential dumping.
15. **Remote System Discovery (T1018):** Used PowerView for Active Directory database enumeration.
16. **Service Stop (T1489):** Stopped services prior to ransomware execution.
17. **System Service Discovery (T1007):** Retrieved a list of services using the win32_service WMI class.
18. **User Execution: Malicious File (T1204.002):** Attempted to get users to click on malicious zipped files.
19. **Valid Accounts: Domain Accounts (T1078.002):** Collected credentials, including domain accounts.
20. **Windows Management Instrumentation (T1047):** Executed commands on remote computers using WMIC.

Software Used by Indrik Spider

- **BitPaymer (S0570)**: Used for impact encryption and various other malicious activities.
- **Cobalt Strike (S0154)**: A versatile tool used for a wide range of malicious activities, including credential dumping and remote execution.
- **Donut (S0695)**: Employed for command execution and obfuscation.
- **Dridex (S0384)**: A banking Trojan used for financial fraud.
- **Empire (S0363)**: Utilized for command execution, credential dumping, and other malicious activities.
- **Mimikatz (S0002)**: Used for credential dumping and manipulation.
- **PsExec (S0029)**: Employed for lateral movement and service execution.
- **WastedLocker (S0612)**: Another ransomware tool used for encrypting victim data.

Ke3chang - Group Overview

Description:

Ke3chang, attributed to actors operating out of China, is a threat group known for targeting a variety of sectors including oil, government, diplomatic, military, and NGOs. Their activities have been observed in Central and South America, the Caribbean, Europe, and North America since at least 2010.

Motivation:

Ke3chang's primary motivation appears to be cyber espionage, targeting a wide range of international governmental and diplomatic entities.

Names:

- Ke3chang
- APT15
- Mirage
- Vixen Panda
- GREF
- Playful Dragon
- RoyalAPT
- NICKEL

Location:

Based in China, with global targeting scope.

First Seen:

Active since at least 2010.

Observed:

Techniques Used in all tactics

1. **Account Discovery (T1087)**: Used commands like `net localgroup administrators` for account discovery.
2. **Application Layer Protocol (T1071)**: Communicated over HTTP/HTTPS/DNS with C2 servers.
3. **Archive Collected Data (T1560)**: Known to compress data before exfiltration.
4. **Boot or Logon Autostart Execution (T1547.001)**: Achieved persistence by adding Run keys.
5. **Command and Scripting Interpreter (T1059)**: Utilized batch scripts and command-line interface for execution.
6. **Create or Modify System Process (T1543.003)**: Established persistence through services like RoyalDNS.
7. **Data from Information Repositories (T1213.002)**: Used tools like spwebmember for SharePoint data dumping.
8. **Data from Local System (T1005)**: Gathered information and files from local directories.
9. **Deobfuscate/Decode Files or Information (T1140)**: Deobfuscated Base64-encoded shellcode strings.
10. **Develop Capabilities: Malware (T1587.001)**: Developed custom malware for operations.
11. **Email Collection: Remote Email Collection (T1114.002)**: Dumped data from Microsoft Exchange mailboxes.
12. **Exfiltration Over C2 Channel (T1041)**: Transferred data through backdoor C2 channels.
13. **Exploit Public-Facing Application (T1190)**: Exploited vulnerable Microsoft Exchange and SharePoint servers.
14. **External Remote Services (T1133)**: Accessed networks through VPNs using compromised accounts.
15. **File and Directory Discovery (T1083)**: Searched files and directories via command-line.
16. **Ingress Tool Transfer (T1105)**: Downloaded files to compromised machines.
17. **Input Capture: Keylogging (T1056.001)**: Employed keyloggers in their operations.
18. **Masquerading (T1036)**: Used right-to-left override and legitimate software paths for masquerading.
19. **Obfuscated Files or Information (T1027)**: Utilized Base64-encoded shellcode strings.
20. **Obtain Capabilities: Tool (T1588.002)**: Acquired tools like Mimikatz for operations.
21. **OS Credential Dumping (T1003)**: Dumped credentials using tools like Mimikatz and gsecdump.
22. **Permission Groups Discovery: Domain Groups (T1069.002)**: Performed discovery of permission groups.
23. **Process Discovery (T1057)**: Conducted process discovery using tasklist commands.
24. **Remote Services: SMB/Windows Admin Shares (T1021.002)**: Copied files to network shares for lateral movement.
25. **Remote System Discovery (T1018)**: Used tools like Ping for network scanning.
26. **Steal or Forge Kerberos Tickets: Golden Ticket (T1558.001)**: Generated Kerberos golden tickets.
27. **System Information Discovery (T1082)**: Collected operating system and hardware information.
28. **System Location Discovery: System Language Discovery (T1614.001)**: Identified system language ID.
29. **System Network Configuration Discovery (T1016)**: Performed network configuration discovery.
30. **System Network Connections Discovery (T1049)**: Conducted network connection

discovery.

- 31. **System Owner/User Discovery (T1033)**: Collected signed-in username information.
- 32. **System Service Discovery (T1007)**: Discovered services using net start commands.
- 33. **System Services: Service Execution (T1569.002)**: Used tools like RemoteExec for remote execution.
- 34. **Valid Accounts (T1078)**: Utilized legitimate credentials for access.

Software Used by Ke3chang

- **ipconfig (S0100)**: Used for system network configuration discovery.
- **Mimikatz (S0002)**: Employed for credential dumping and manipulation.
- **MirageFox (S0280)**: Utilized for command execution and system information discovery.
- **Neolichor (S0691)**: Used for various malicious activities including data collection and system discovery.
- **Net (S0039)**: Applied for account discovery, remote services, and system discovery.
- **netstat (S0104)**: Used for system network connections discovery.
- **Okrum (S0439)**: Employed for command execution, data exfiltration, and system discovery.
- **Ping (S0097)**: Utilized for remote system discovery.
- **spwebmember (S0227)**: Used for SharePoint data collection.
- **Systeminfo (S0057)**: Applied for system information discovery.
- **Tasklist (S0057)**: Used for process and software discovery.

Kimsuky - Group Overview

Description:

Kimsuky is a North Korea-based cyber espionage group, active since at least 2012. The group has primarily targeted South Korean government entities, think tanks, and individuals identified as experts in various fields. Over time, Kimsuky expanded its operations to include the United States, Russia, Europe, and the UN, focusing on foreign policy and national security issues related to the Korean peninsula, nuclear policy, and sanctions.

Motivation:

Kimsuky's primary motivation appears to be gathering intelligence on foreign policy and national security issues, particularly those related to North Korea's geopolitical interests.

Names:

- Kimsuky
- STOLEN PENCIL
- Thallium
- Black Banshee
- Velvet Chollima

Location:

Based in North Korea, with global targeting scope.

First Seen:

Active since at least 2012.

Observed:

Notable campaigns include the 2014 Korea Hydro & Nuclear Power Co. compromise, Operation STOLEN PENCIL (2018), Operation Kabar Cobra (2019), and Operation Smoke Screen (2019).

Techniques Used in all tactics

1. **Account Manipulation (T1098)**: Added accounts to specific groups using `net localgroup`.
2. **Acquire Infrastructure (T1583)**: Registered domains, purchased hosting servers, and hosted content via web services.
3. **Adversary-in-the-Middle (T1557)**: Used modified versions of PHPProxy for web traffic examination.
4. **Application Layer Protocol (T1071)**: Utilized HTTP, HTTPS, FTP, and mail protocols for C2 communications.
5. **Archive Collected Data (T1560)**: Employed QuickZip and RC4 encryption for data archiving.
6. **Boot or Logon Autostart Execution (T1547.001)**: Placed scripts in the startup folder and modified Registry keys for persistence.
7. **Browser Extensions (T1176)**: Used Google Chrome extensions for infection and data theft.
8. **Command and Scripting Interpreter (T1059)**: Executed PowerShell, Windows Command Shell, Visual Basic, Python, and JavaScript scripts.
9. **Compromise Accounts (T1586)**: Compromised email accounts for spearphishing.
10. **Create Account (T1136.001)**: Created local accounts using `net user`.
11. **Create or Modify System Process (T1543.003)**: Created new services for persistence.
12. **Credentials from Password Stores (T1555.003)**: Stole passwords and cookies using browser extensions and tools.
13. **Data from Local System (T1005)**: Collected documents from victims.
14. **Data Staged (T1074.001)**: Staged data under specific directories.
15. **Deobfuscate/Decode Files or Information (T1140)**: Decoded malicious VBScripts using Base64.
16. **Develop Capabilities (T1587)**: Created mailing toolkits and developed unique malware.
17. **Email Collection (T1114)**: Used tools like MailFetch to collect emails.
18. **Establish Accounts (T1585)**: Created social media and email accounts for operations.
19. **Event Triggered Execution (T1546.001)**: Altered default program associations in the Registry.
20. **Exfiltration Over C2 Channel (T1041)**: Exfiltrated data via C2 channels.
21. **Exfiltration Over Web Service (T1567.002)**: Exfiltrated data to Blogspot accounts.
22. **Exploit Public-Facing Application (T1190)**: Exploited vulnerabilities like CVE-2020-0688.
23. **External Remote Services (T1133)**: Used RDP for persistence.
24. **File and Directory Discovery (T1083)**: Enumerated files and directories.
25. **Gather Victim Identity Information (T1589)**: Collected email addresses and employee names.

26. **Gather Victim Org Information (T1591)**: Collected organization-related information.
27. **Hide Artifacts (T1564)**: Used techniques to hide users and windows.
28. **Impair Defenses (T1562)**: Disabled security tools and system firewall.
29. **Indicator Removal (T1070)**: Deleted exfiltrated data and used timestomp.
30. **Ingress Tool Transfer (T1105)**: Downloaded additional tools and malware.
31. **Input Capture (T1056.001)**: Employed keyloggers.
32. **Internal Spearphishing (T1534)**: Sent internal spearphishing emails for lateral movement.
33. **Masquerading (T1036)**: Disguised C2 addresses and services.
34. **Modify Registry (T1112)**: Altered Registry settings for macros and persistence.
35. **Multi-Factor Authentication Interception (T1111)**: Intercepted one-time passwords.
36. **Network Sniffing (T1040)**: Used tools like SniffPass for password capture.
37. **Obfuscated Files or Information (T1027)**: Employed XOR encryption and Base64 encoding.
38. **Obtain Capabilities (T1588)**: Acquired tools like Nirsoft WebBrowserPassView and Mimikatz.
39. **OS Credential Dumping (T1003.001)**: Dumped credentials using Mimikatz and ProcDump.
40. **Phishing (T1566)**: Used spearphishing with attachments and links.
41. **Phishing for Information (T1598.003)**: Employed links in emails for information theft.
42. **Process Discovery (T1057)**: Gathered a list of running processes.
43. **Process Injection (T1055)**: Used techniques like process hollowing.
44. **Query Registry (T1012)**: Obtained Registry keys and values.
45. **Remote Access Software (T1219)**: Utilized modified TeamViewer for C2.
46. **Remote Services (T1021.001)**: Used RDP for remote access.
47. **Scheduled Task/Job (T1053.005)**: Downloaded malware via scheduled tasks.
48. **Search Open Websites/Domains (T1593)**: Used social media and search engines for reconnaissance.
49. **Search Victim-Owned Websites (T1594)**: Searched target company websites.
50. **Server Software Component (T1505.003)**: Used PHP web shells for access.
51. **Software Discovery (T1518.001)**: Checked for antivirus software.
52. **Stage Capabilities (T1608.001)**: Used Blogspot to host malicious content.
53. **Subvert Trust Controls (T1553.002)**: Signed files with fake names.
54. **System Binary Proxy Execution (T1218)**: Used mshta.exe, regsvr32s, and rundll32.exe for execution.
55. **System Information Discovery (T1082)**: Enumerated system information.
56. **System Network Configuration Discovery (T1016)**: Used ipconfig/all for network information.
57. **System Service Discovery (T1007)**: Gathered service names.
58. **Unsecured Credentials (T1552.001)**: Obtained credentials from saved mail.
59. **Use Alternate Authentication Material (T1550.002)**: Employed pass the hash technique.
60. **User Execution (T1204)**: Lured victims to click malicious links and files.
61. **Valid Accounts (T1078.003)**: Added Windows admin accounts for RDP access.
62. **Web Service (T1102.002)**: Used Blogspot pages for C2.

Software Used by Kimsuky

- **AppleSeed (S0622)**: A multifunctional tool used for various malicious activities.
- **BabyShark (S0414)**: Employed for data collection and system information discovery.
- **Brave Prince (S0252)**: Used for exfiltration and system discovery.
- **CSPY Downloader (S0527)**: A downloader used for various purposes including software packing.
- **Gold Dragon (S0249)**: Utilized for data collection and system information discovery.
- **KGH_SPY (S0526)**: A spyware used for credential theft and data collection.

- **Mimikatz (S0002)**: Employed for credential dumping and manipulation.
- **NOKKI (S0353)**: Used for data collection and system information discovery.
- **PsExec (S0029)**: Utilized for remote execution and lateral movement.
- **schtasks (S0111)**: Used for scheduling tasks and jobs.

LAPSUS\$ - Group Overview

Description:

LAPSUS\$ is a cyber criminal threat group that has been active since at least mid-2021. The group is known for its large-scale social engineering and extortion operations, including destructive attacks without the use of ransomware. LAPSUS\$ has targeted a wide range of sectors globally, including government, manufacturing, higher education, energy, healthcare, technology, telecommunications, and media.

Motivation:

The primary motivation of LAPSUS\$ appears to be financial gain through extortion and possibly disruption.

Names:

- LAPSUS\$
- DEV-0537

Location:

Not specified, but the group has targeted organizations globally.

First Seen:

Active since at least mid-2021.

Observed:

LAPSUS\$ has been involved in various high-profile attacks and extortion campaigns against major organizations across different sectors.

Techniques Used in all tactics

1. **Account Access Removal (T1531)**: Removed global admin accounts to lock organizations out of access.
2. **Account Discovery (T1087.002)**: Used AD Explorer to enumerate users on networks.
3. **Account Manipulation (T1098.003)**: Added global admin roles in cloud instances.
4. **Acquire Infrastructure (T1583.003)**: Utilized VPS hosting for infrastructure.

5. **Compromise Accounts (T1586.002)**: Paid for credentials from employees and partners.
6. **Compromise Infrastructure (T1584.002)**: Reconfigured DNS records to control domains.
7. **Create Account (T1136.003)**: Created cloud accounts for persistence.
8. **Credentials from Password Stores (T1555)**: Accessed web browsers and password managers for credentials.
9. **Data Destruction (T1485)**: Deleted systems and resources in cloud and on-premises.
10. **Data from Information Repositories (T1213)**: Searched for collaboration channels for credentials.
11. **Data from Local System (T1005)**: Uploaded sensitive files for extortion.
12. **Email Collection (T1114.003)**: Set mail transport rules in Office 365.
13. **Exploitation for Privilege Escalation (T1068)**: Exploited vulnerabilities in servers for escalation.
14. **External Remote Services (T1133)**: Accessed VPN, RDP, and VDI systems.
15. **Gather Victim Identity Information (T1589)**: Collected detailed employee information.
16. **Gather Victim Org Information (T1591)**: Acquired knowledge of organizational structures.
17. **Impersonation (T1656)**: Impersonated legitimate users for access.
18. **Modify Cloud Compute Infrastructure (T1578)**: Created and deleted cloud instances.
19. **Multi-Factor Authentication Interception (T1111)**: Replayed stolen session tokens.
20. **Multi-Factor Authentication Request Generation (T1621)**: Spammed users with MFA prompts.
21. **Obtain Capabilities (T1588)**: Acquired malware and tools like Redline and AD Explorer.
22. **OS Credential Dumping (T1003)**: Used tools to extract Active Directory database.
23. **Permission Groups Discovery (T1069.002)**: Enumerated groups using AD Explorer.
24. **Phishing for Information (T1598.004)**: Spearphishing via voice calls to help desks.
25. **Proxy (T1090)**: Used NordVPN for egress points.
26. **Search Closed Sources (T1597.002)**: Purchased technical data and credentials.
27. **Search Open Websites/Domains (T1593.003)**: Searched code repositories for credentials.
28. **Service Stop (T1489)**: Shut down virtual machines in VMware ESXi infrastructure.
29. **Trusted Relationship (T1199)**: Accessed identity providers like Azure AD and Okta.
30. **Unsecured Credentials (T1552.008)**: Targeted collaboration tools for credential hunting.
31. **User Execution (T1204)**: Recruited organization employees for system access.
32. **Valid Accounts (T1078)**: Used compromised credentials for access to VPN, VDI, RDP, and IAMs.

Software Used by LAPSUS\$

- **Mimikatz (S0002)**: Used for various credential dumping and manipulation techniques.

Lazarus Group - Group Overview

Description:

Lazarus Group is a North Korean state-sponsored cyber threat group, attributed to the Reconnaissance General Bureau. Active since at least 2009, it has been involved in high-profile cyber attacks, including the 2014 destructive wiper attack against Sony Pictures Entertainment as part of Operation Blockbuster. The group's malware has been linked to various campaigns like Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.

Motivation:

The primary motivations of the Lazarus Group include espionage, data theft, financial gain, and disruption of targeted organizations.

Names:

- Lazarus Group
- Labyrinth Chollima
- HIDDEN COBRA
- Guardians of Peace
- ZINC
- NICKEL ACADEMY

Location:

North Korea

First Seen:

Active since at least 2009.

Observed:

Lazarus Group has been involved in numerous cyber espionage and sabotage operations, targeting a wide range of industries and organizations worldwide.

Techniques Used in all tactics

1. **Access Token Manipulation (T1134.002)**: Lazarus Group's keylogger KiloAlfa obtains user tokens for execution under user context.
2. **Account Discovery (T1087.002)**: Used in Operation Dream Job for querying active directory servers.
3. **Account Manipulation (T1098)**: Malware attempts to rename administrator accounts.
4. **Acquire Infrastructure (T1583)**: Acquired domains, servers, and web services for campaigns.
5. **Adversary-in-the-Middle (T1557.001)**: Executed Responder for credential harvesting.
6. **Application Layer Protocol (T1071.001)**: Conducted C2 over HTTP/HTTPS.
7. **Application Window Discovery (T1010)**: Malware reported window titles of running processes.
8. **Archive Collected Data (T1560)**: Used RAR for data compression and encryption.
9. **Boot or Logon Autostart Execution (T1547)**: Maintained persistence via startup folder and Registry Run keys.
10. **Brute Force (T1110.003)**: Used password spraying techniques.
11. **Command and Scripting Interpreter (T1059)**: Employed PowerShell, Windows Command Shell, and Visual Basic for execution.
12. **Compromise Infrastructure (T1584)**: Compromised domains and servers for C2 infrastructure.

13. **Create or Modify System Process (T1543.003)**: Installed malware as new services.
14. **Data Destruction (T1485)**: Used custom secure delete functions.
15. **Data Encoding (T1132.001)**: Encoded data with base64.
16. **Data from Local System (T1005)**: Collected data and files from networks.
17. **Data Obfuscation (T1001.003)**: Used FakeTLS for communication encryption.
18. **Data Staged (T1074.001)**: Staged data in %TEMP% directory.
19. **Debugger Evasion (T1622)**: Employed tools to detect debuggers.
20. **Defacement (T1491.001)**: Replaced system wallpaper with threatening images.
21. **Deobfuscate/Decode Files or Information (T1140)**: Used shellcode within macros for decryption.
22. **Develop Capabilities (T1587)**: Developed custom malware and tools.
23. **Disk Wipe (T1561)**: Employed various methods for disk wiping.
24. **Drive-by Compromise (T1189)**: Delivered malware via compromised websites.
25. **Encrypted Channel (T1573.001)**: Used symmetric cryptography for C2 traffic encryption.
26. **Establish Accounts (T1585)**: Created social media and email accounts for spearphishing.
27. **Exfiltration Over Alternative Protocol (T1048.003)**: Used SMTP for data exfiltration.
28. **Exfiltration Over C2 Channel (T1041)**: Exfiltrated data over C2 channels.
29. **Exfiltration Over Web Service (T1567.002)**: Used cloud storage for data exfiltration.
30. **Exploitation for Client Execution (T1203)**: Exploited Adobe Flash vulnerability.
31. **Fallback Channels (T1008)**: Used multiple C2 servers for data transmission.
32. **File and Directory Discovery (T1083)**: Identified target files by extension.
33. **Gather Victim Identity Information (T1589.002)**: Collected email addresses for phishing campaigns.
34. **Gather Victim Org Information (T1591)**: Studied public information for spearphishing.
35. **Hide Artifacts (T1564.001)**: Used hidden files and directories.
36. **Hijack Execution Flow (T1574)**: Replaced DLLs for payload execution.
37. **Impair Defenses (T1562)**: Disabled or modified system defenses.
38. **Impersonation (T1656)**: Impersonated HR personnel for social engineering.
39. **Indicator Removal (T1070)**: Employed various methods for indicator removal.
40. **Indirect Command Execution (T1202)**: Used forfiles.exe for execution.
41. **Ingress Tool Transfer (T1105)**: Downloaded tools and malware onto hosts.
42. **Input Capture (T1056.001)**: Used keylogging functionality.
43. **Internal Spearphishing (T1534)**: Conducted spearphishing within organizations.
44. **Masquerading (T1036)**: Disguised malicious code and utilities.
45. **Multi-Stage Channels (T1104)**: Used multi-stage malware components.
46. **Native API (T1106)**: Employed various Windows API functions.
47. **Network Service Discovery (T1046)**: Used nmap for port scanning.
48. **Non-Standard Port (T1571)**: Created port-protocol mismatches.
49. **Obfuscated Files or Information (T1027)**: Used multiple encryption and encoding methods.
50. **Obtain Capabilities (T1588)**: Acquired various tools and digital certificates.
51. **Phishing (T1566)**: Used spearphishing with attachments and links.
52. **Pre-OS Boot (T1542.003)**: Modified the Master Boot Record.
53. **Process Discovery (T1057)**: Gathered a list of running processes.
54. **Process Injection (T1055.001)**: Performed DLL injection.
55. **Proxy (T1090)**: Used internal and external proxies.
56. **Query Registry (T1012)**: Checked Registry keys for specific applications.
57. **Reflective Code Loading (T1620)**: Used shellcode for process execution flow hijacking.
58. **Remote Services (T1021)**: Accessed RDP, SMB, and SSH for lateral movement.
59. **Scheduled Task/Job (T1053.005)**: Used scheduled tasks for persistence.
60. **Search Open Websites/Domains (T1593.001)**: Used social media for target identification.
61. **Server Software Component (T1505.004)**: Targeted IIS servers for C2 installation.

- 62. **Service Stop (T1485)**: Stopped services to render systems inaccessible.
- 63. **Stage Capabilities (T1608)**: Hosted malware and tools on compromised servers.
- 64. **Subvert Trust Controls (T1553.002)**: Digitally signed malware for evasion.
- 65. **System Binary Proxy Execution (T1218)**: Used system binaries for malicious execution.
- 66. **System Information Discovery (T1082)**: Collected OS type, version, and system information.
- 67. **System Location Discovery (T1614.001)**: Deployed malware with language-based execution guardrails.
- 68. **System Network Configuration Discovery (T1016)**: Obtained network configuration information.
- 69. **System Network Connections Discovery (T1049)**: Identified network connections with net use.
- 70. **System Owner/User Discovery (T1033)**: Enumerated logged-on users.
- 71. **System Shutdown/Reboot (T1529)**: Rebooted systems after destructive activities.
- 72. **System Time Discovery (T1124)**: Obtained current system time.
- 73. **Template Injection (T1221)**: Used DOCX files for malicious template retrieval.
- 74. **User Execution (T1204)**: Lured users into executing malicious links and files.
- 75. **Valid Accounts (T1078)**: Used administrator credentials for network access.
- 76. **Virtualization/Sandbox Evasion (T1497)**: Employed system checks and time-based evasion.
- 77. **Web Service (T1102.002)**: Used GitHub for bidirectional communication.
- 78. **Windows Management Instrumentation (T1047)**: Used WMIC for discovery and payload execution.
- 79. **XSL Script Processing (T1220)**: Used remote XSL scripts for downloading encoded DLLs.
- 80. **Spearphishing Attachment (ICS T0865)**: Targeted organizations with spearphishing documents.

Software Used by Lazarus Group

- **AppleJeuS (S0584)**: Used for various cyber attack techniques.
- **AuditCred (S0347)**: Employed for command execution and data collection.
- **BADCALL (S0245)**: Used for data obfuscation and system firewall impairment.
- **Bankshot (S0239)**: Utilized for token manipulation and data collection.
- **BLINDINGCAN (S0520)**: Employed for data encryption and exfiltration.
- **Cryptoistic (S0498)**: Used for data collection and network protocol manipulation.
- **DacIs (S0497)**: Utilized for data collection and masquerading.
- **DRATzarus (S0694)**: Used for monitoring drives and remote desktop connections.
- **Dtrack (S0567)**: Employed for data collection and keylogging.
- **ECCENTRICBANDWAGON (S0593)**: Used for keylogging and screen capture.
- **FALLCHILL (S0181)**: Utilized for data collection and encryption.
- **HARDRAIN (S0246)**: Employed for command execution and proxy usage.
- **HOPLIGHT (S0376)**: Used for data collection and firewall impairment.
- **HotCroissant (S0431)**: Utilized for data collection and artifact hiding.
- **KEYMARBLE (S0271)**: Employed for data collection and command execution.
- **netsh (S0108)**: Used for firewall impairment and proxy configuration.
- **Proxysvc (S0238)**: Utilized for data destruction and collection.
- **RATANKBA (S0241)**: Employed for account discovery and data collection.
- **RawDisk (S0364)**: Used for disk wiping and data destruction.
- **Responder (S0174)**: Utilized for credential harvesting and network sniffing.
- **route (S0103)**: Employed for network configuration discovery.
- **TAINTEDSCRIBE (S0586)**: Used for data collection and obfuscation.

- **ThreatNeedle (S0665)**: Utilized for data collection and registry modification.
- **Torisma (S0678)**: Employed for system monitoring and data encoding.
- **TYPEFRAME (S0263)**: Used for command execution and firewall impairment.
- **Volgmer (S0180)**: Utilized for command execution and data collection.
- **WannaCry (S0366)**: Employed for data encryption and exploitation of remote services.

APT - Group Overview

Description:

LazyScripter is a threat group that has been actively targeting the airline industry since at least 2018. This group primarily utilizes open-source toolsets in its operations.

Motivation:

The specific motivations of LazyScripter are not detailed in the provided text. However, given their targeted attacks on the airline industry, it can be inferred that their motivations could be related to espionage, data theft, or disruption of industry operations.

Names:

LazyScripter

Location:

The location of LazyScripter is not explicitly mentioned in the provided text.

First Seen:

LazyScripter has been active since at least 2018.

Observed:

LazyScripter has been observed using a variety of techniques and software, mainly focusing on open-source tools for executing their attacks.

Techniques Used in all Tactics

1. **Acquire Infrastructure**: LazyScripter has used dynamic DNS providers to create legitimate-looking subdomains for command and control (C2) and has established GitHub accounts to host its toolsets.
2. **Application Layer Protocol**: The group has leveraged dynamic DNS providers for C2 communications.
3. **Boot or Logon Autostart Execution**: Persistence is achieved via writing a PowerShell script to the autorun registry key.

4. **Command and Scripting Interpreter:** They have used PowerShell scripts, batch files, VBScript, and JavaScript to execute malicious code.
5. **Ingress Tool Transfer:** LazyScripter downloaded additional tools to compromised hosts.
6. **Masquerading:** They have disguised executables using different security software icons.
7. **Obfuscated Files or Information:** The group has used advanced batch script obfuscation and encoding techniques.
8. **Obtain Capabilities:** A variety of open-source remote access Trojans have been used.
9. **Phishing:** Spearphishing techniques involving attachment and links have been employed as initial infection vectors.
10. **Stage Capabilities:** Open-source remote access Trojans used in operations were hosted on GitHub.
11. **System Binary Proxy Execution:** They have used `mshta.exe` and `rundll32.exe` to execute Koadic stagers.
12. **User Execution:** Reliance on users clicking on malicious links or opening email attachments.
13. **Web Service:** GitHub was used to host payloads and operate spam campaigns.

Software Used by LazyScripter

1. **Empire:** A post-exploitation framework used for various malicious activities.
2. **Koadic:** Utilized for command and control capabilities.
3. **KOCTOPUS:** A tool used for various malicious purposes including obfuscation and phishing.
4. **ngrok:** Employed for tunneling and proxy services.
5. **njRAT:** A remote access Trojan used for command and control.
6. **QuasarRAT:** Another remote access Trojan with various capabilities.
7. **Remcos:** Used for command and control, along with data exfiltration.

APT - Group Overview

Description:

Leafminer is an Iranian threat group known for targeting government organizations and business entities in the Middle East. The group has been active since at least early 2017 and is known for its sophisticated cyber espionage campaigns.

Motivation:

While the specific motivations of Leafminer are not detailed in the provided text, their targeting of government and business entities suggests motivations likely include espionage, intelligence gathering, and possibly disruption of governmental and business operations.

Names:

- Leafminer
- Associated Groups: Raspite

Location:

First Seen:

Leafminer has been active since at least early 2017.

Observed:

Leafminer has been observed using a variety of cyber attack techniques and tools, focusing on espionage and data exfiltration.

Techniques Used in all Tactics

1. **Brute Force:** Used tools like Total SMB BruteForcer for internal password spraying.
2. **Command and Scripting Interpreter:** Infected victims using JavaScript code.
3. **Create Account:** Set up persistent remote access accounts using tools like Imecab.
4. **Credentials from Password Stores:** Employed tools like LaZagne for retrieving login and password information.
5. **Drive-by Compromise:** Infected victims through watering hole attacks.
6. **Email Collection:** Utilized MailSniper for searching through Exchange server mailboxes.
7. **File and Directory Discovery:** Used tools like MailSniper and Sobolsoft for searching files and extracting attachments.
8. **Network Service Discovery:** Scanned network services to find vulnerabilities.
9. **Obfuscated Files or Information:** Obfuscated scripts used on victim machines.
10. **Obtain Capabilities:** Obtained and used tools such as LaZagne, Mimikatz, PsExec, and MailSniper.
11. **OS Credential Dumping:** Employed tools for dumping credentials from various sources.
12. **Process Injection:** Used Process Doppelgänger for evading security software.
13. **Remote System Discovery:** Gathered information about remote systems using Microsoft's Sysinternals tools.
14. **Unsecured Credentials:** Retrieved login and password information from unsecured files.

Software Used by Leafminer

1. **LaZagne:** Used for extracting credentials from various sources including web browsers, Windows Credential Manager, and system files.
2. **MailSniper:** Employed for email account discovery, password spraying, and remote email collection.
3. **Mimikatz:** Utilized for various credential theft techniques, including dumping LSASS memory and manipulating authentication certificates.
4. **PsExec:** Used for creating accounts, modifying system processes, and executing services remotely.

APT - Group Overview

Description:

Leviathan is a Chinese state-sponsored cyber espionage group. It has been attributed to the Ministry of State Security's (MSS) Hainan State Security Department and an affiliated front company. Active since at least 2009, Leviathan has targeted a wide range of sectors including academia, aerospace/aviation, biomedical, defense industrial base, government, healthcare, manufacturing, maritime, and transportation across various regions including the US, Canada, Europe, the Middle East, and Southeast Asia.

Motivation:

The primary motivation of Leviathan appears to be espionage, given its state-sponsored nature and the wide range of high-value sectors it targets.

Names:

- Leviathan
- Associated Groups: MUDCARP, Kryptonite Panda, Gadolinium, BRONZE MOHAWK, TEMP.Jumper, APT40, TEMP.Periscope

Location:

China

First Seen:

The group has been active since at least 2009.

Observed:

Leviathan has been observed employing a variety of sophisticated cyber espionage techniques and tools.

Techniques Used in all Tactics

1. **Acquire Infrastructure:** Established domains impersonating legitimate entities for targeting efforts.
2. **Archive Collected Data:** Archived victim's data prior to exfiltration.
3. **BITS Jobs:** Used BITSAdmin to download additional tools.
4. **Boot or Logon Autostart Execution:** Created shortcut files in the Startup folder pointing to its main backdoor.
5. **Command and Scripting Interpreter:** Used PowerShell and VBScript for execution.
6. **Compromise Accounts:** Compromised social media and email accounts for social engineering attacks.
7. **Data Staging:** Used local and remote data staging techniques.
8. **Deobfuscate/Decode Files or Information:** Employed a DLL known as SeDll for decrypting and executing JavaScript backdoors.
9. **Drive-by Compromise:** Infected victims using watering holes.
10. **Establish Accounts:** Created new social media and email accounts for targeting efforts.

11. **Event Triggered Execution:** Used WMI for persistence.
12. **Exfiltration Over C2 Channel:** Exfiltrated data over its C2 channel.
13. **Exfiltration Over Web Service:** Used LUNCHMONEY uploader for exfiltrating files to Dropbox.
14. **Exploitation for Client Execution:** Exploited multiple Microsoft Office and .NET vulnerabilities.
15. **External Remote Services:** Used external remote services like VPNs for initial access.
16. **Gather Victim Identity Information:** Collected compromised credentials.
17. **Ingress Tool Transfer:** Downloaded additional scripts and files from adversary-controlled servers.
18. **Inter-Process Communication:** Utilized OLE for inserting malicious content in phishing documents.
19. **Internal Spearphishing:** Conducted internal spearphishing within victim environments.
20. **Obfuscated Files or Information:** Employed base64 and gzip compression for obfuscation.
21. **OS Credential Dumping:** Used tools like HOMEFRY and ProcDump for dumping password hashes.
22. **Phishing:** Sent spearphishing emails with malicious attachments and links.
23. **Process Injection:** Utilized techniques like reflective DLL loading for backdoor access.
24. **Protocol Tunneling:** Used protocol tunneling for concealing C2 communications.
25. **Proxy:** Employed multi-hop proxies to disguise malicious traffic.
26. **Remote Services:** Targeted RDP credentials and used SSH for internal reconnaissance.
27. **Server Software Component:** Relied on web shells for initial foothold and persistence.
28. **Subvert Trust Controls:** Used stolen code signing certificates to sign malware.
29. **System Binary Proxy Execution:** Used regsvr32 for execution.
30. **User Execution:** Sent spearphishing email links and attachments.
31. **Valid Accounts:** Obtained valid accounts for initial access.
32. **Web Service:** Received C2 instructions from profiles on legitimate websites.
33. **Windows Management Instrumentation:** Used WMI for execution.

Software Used by Leviathan

1. **at:** Scheduled task/job tool.
2. **BADFLICK:** A tool with various capabilities including data collection and exfiltration.
3. **BITSAdmin:** Used for BITS jobs and data transfer.
4. **BLACKCOFFEE:** A command and scripting interpreter with multiple functionalities.
5. **China Chopper:** A web shell with various capabilities.
6. **Cobalt Strike:** A comprehensive tool for exploitation and post-exploitation.
7. **Derusbi:** A RAT with capabilities like audio capture and keylogging.
8. **Empire:** A post-exploitation framework.
9. **gh0st RAT:** A remote access tool with various capabilities.
10. **HOMEFRY:** Used for OS credential dumping.
11. **MURKYTOP:** A tool for account discovery and network reconnaissance.
12. **NanHaiShu:** A tool for application layer protocol manipulation and data exfiltration.
13. **Net:** Used for account and system discovery.
14. **Orz:** A command and scripting interpreter with various capabilities.
15. **PowerSploit:** A PowerShell-based exploitation framework.
16. **Tor:** Used for encrypted communication and proxying.
17. **Windows Credential Editor:** Employed for OS credential dumping.

APT - Group Overview

Description:

Lotus Blossom is a threat group known for targeting government and military organizations in Southeast Asia. The group is noted for its focused attacks on high-value targets within this region.

Motivation:

While the specific motivations of Lotus Blossom are not detailed in the provided text, the targeting of government and military organizations suggests motivations likely include espionage, intelligence gathering, and possibly influencing political or military decisions.

Names:

- Lotus Blossom
- Associated Groups: DRAGONFISH, Spring Dragon

Location:

The group primarily targets entities in Southeast Asia.

First Seen:

The first recorded activities of Lotus Blossom date back to at least 2015.

Observed:

Lotus Blossom has been observed employing a variety of cyber attack techniques and tools, focusing on espionage and data exfiltration.

Techniques Used in all Tactics

The specific techniques used by Lotus Blossom are not detailed in the provided text. However, given their targeting of government and military organizations, it can be inferred that they likely employ advanced persistent threat tactics including spearphishing, exploitation of vulnerabilities, and use of custom malware.

Software Used by Lotus Blossom

1. **Elise:** This software has been used by Lotus Blossom for various purposes including account discovery, application layer protocol manipulation, boot or logon autostart execution, data encoding and staging, encrypted communication, file and directory discovery, indicator removal, ingress tool transfer, masquerading, process discovery and injection, and system information discovery.
2. **Emissary:** Employed for application layer protocol manipulation, boot or logon autostart

execution, command and scripting interpreter usage, creation or modification of system processes, encrypted communication, group policy discovery, ingress tool transfer, obfuscation, permission groups discovery, process injection, and system information discovery.

APT - Group Overview

Description:

Machete is a cyber espionage group suspected to be Spanish-speaking, active since at least 2010. The group has primarily focused its operations within Latin America, particularly in Venezuela, but also has a presence in the US, Europe, Russia, and parts of Asia. Machete typically targets high-profile organizations such as government institutions, intelligence services, military units, telecommunications, and power companies.

Motivation:

While the specific motivations of Machete are not detailed in the provided text, their targeting of government, military, and critical infrastructure suggests motivations likely include espionage, intelligence gathering, political influence, and possibly disruption of critical services.

Names:

- Machete
- Associated Groups: APT-C-43, El Machete

Location:

Machete primarily operates in Latin America, with significant activities in Venezuela and additional operations in the US, Europe, Russia, and parts of Asia.

First Seen:

The group has been active since at least 2010.

Observed:

Machete has been observed employing a variety of sophisticated cyber espionage techniques and tools, focusing on espionage and data exfiltration.

Techniques Used in all Tactics

1. **Command and Scripting Interpreter:** Used batch files, Visual Basic, and Python scripts for initiating downloads and executing malicious files.
2. **Drive-by Compromise:** Distributed malware through a fake blog website.
3. **Man-in-the-middle:** The Machete MITM installer was masqueraded as a legitimate Adobe Acrobat

Reader installer.

4. **Phishing:** Delivered spearphishing emails containing zipped files with malicious contents and sent phishing emails with links to external servers.
5. **Scheduled Task/Job:** Created scheduled tasks for maintaining persistence.
6. **System Binary Proxy Execution:** Used msixexec for installing malware.
7. **User Execution:** Relied on users opening malicious links and attachments delivered through spearphishing.

Software Used by Machete

1. **Machete:** This software has been used for a wide range of activities including application layer protocol manipulation, data collection and exfiltration, audio capture, browser information discovery, clipboard data collection, command and scripting interpretation, credentials theft, file and directory discovery, indicator removal, ingress tool transfer, keylogging, masquerading, obfuscation, process discovery, scheduled tasks, screen capture, system information discovery, and network configuration discovery.

APT - Group Overview

Description:

Magic Hound is an Iranian-sponsored threat group known for conducting long-term, resource-intensive cyber espionage operations. This group is likely operating on behalf of the Islamic Revolutionary Guard Corps. Since at least 2014, Magic Hound has targeted European, U.S., and Middle Eastern government and military personnel, academics, journalists, and organizations such as the World Health Organization (WHO), using complex social engineering campaigns.

Motivation:

The primary motivation of Magic Hound appears to be espionage, likely driven by geopolitical interests, given its focus on government, military, and international organizations.

Names:

- Magic Hound
- Associated Groups: TA453, COBALT ILLUSION, Charming Kitten, ITG18, Phosphorus, Newscaster, APT35

Location:

Magic Hound primarily targets entities in Europe, the United States, and the Middle East.

First Seen:

The group has been active since at least 2014.

Observed:

Magic Hound has been observed employing a variety of sophisticated cyber espionage techniques and tools, focusing on espionage and data exfiltration.

Techniques Used in all Tactics

1. **Account Discovery:** Used PowerShell to discover email accounts.
2. **Account Manipulation:** Added users to administrative groups.
3. **Acquire Infrastructure:** Registered fraudulent domains for phishing attacks.
4. **Active Scanning:** Conducted scanning for vulnerabilities in public-facing systems.
5. **Application Layer Protocol:** Used IRC and HTTP for command and control (C2).
6. **Archive Collected Data:** Employed gzip and RAR for data archiving.
7. **Boot or Logon Autostart Execution:** Established persistence using Registry Run keys.
8. **Command and Scripting Interpreter:** Utilized PowerShell, Windows Command Shell, and Visual Basic for execution.
9. **Compromise Accounts:** Compromised email accounts using legitimate credentials.
10. **Create Account:** Created local accounts on compromised machines.
11. **Data Encrypted for Impact:** Used BitLocker and DiskCryptor for encrypting workstations.
12. **Drive-by Compromise:** Conducted watering-hole attacks.
13. **Email Collection:** Compromised email credentials to steal sensitive data.
14. **Encrypted Channel:** Used encrypted http proxy in C2 communications.
15. **Establish Accounts:** Created fake social media accounts for spearphishing.
16. **Exfiltration Over Web Service:** Utilized Telegram API for data exfiltration.
17. **Exploit Public-Facing Application:** Exploited various vulnerabilities in public-facing applications.
18. **File and Directory Discovery:** Listed logical drives and directory contents.
19. **Gather Victim Host Information:** Captured user-agent strings from phishing site visitors.
20. **Gather Victim Identity Information:** Acquired mobile phone numbers and email addresses for targeting.
21. **Hide Artifacts:** Used techniques to hide windows and remove indicators.
22. **Impair Defenses:** Disabled security tools and modified firewall settings.
23. **Ingress Tool Transfer:** Downloaded additional malicious code and files.
24. **Input Capture:** Employed keylogging capabilities.
25. **Lateral Tool Transfer:** Copied tools within compromised networks.
26. **Masquerading:** Named malicious scripts to mimic legitimate tasks.
27. **Modify Registry:** Altered Registry settings for security tools.
28. **Network Service Discovery:** Performed network scanning.
29. **Non-Standard Port:** Communicated over non-standard TCP ports.
30. **Obfuscated Files or Information:** Used base64 encoding and AES encryption.
31. **Obtain Capabilities:** Acquired and used various tools like Mimikatz and Metasploit.
32. **OS Credential Dumping:** Stole domain credentials by dumping LSASS memory.
33. **Phishing:** Sent malicious links and attachments via email and social media.
34. **Process Discovery:** Listed running processes on victim machines.
35. **Protocol Tunneling:** Used Plink for tunneling RDP over SSH.
36. **Proxy:** Employed Fast Reverse Proxy for RDP traffic.
37. **Remote Services:** Used Remote Desktop Services for access and tool transfer.
38. **Remote System Discovery:** Used Ping for network discovery.
39. **Scheduled Task/Job:** Established persistence and execution via scheduled tasks.
40. **Screen Capture:** Captured screenshots for intelligence gathering.

41. **Server Software Component:** Utilized web shells for execution.
42. **System Binary Proxy Execution:** Executed MiniDump using rundll32.exe.
43. **System Information Discovery:** Gathered system architecture, OS version, and host names.
44. **System Network Configuration Discovery:** Collected IP and MAC addresses.
45. **System Network Connections Discovery:** Identified existing RDP connections.
46. **System Owner/User Discovery:** Obtained victim usernames.
47. **User Execution:** Lured victims to open malicious links and attachments.
48. **Valid Accounts:** Enabled and used default system accounts for RDP connections.
49. **Web Service:** Used SOAP Web service for C2 communication.
50. **Windows Management Instrumentation:** Ran WMI commands for discovery.

Software Used by Magic Hound

1. **CharmPower:** Used for various activities including data encoding, file discovery, and screen capture.
2. **DownPaper:** Employed for command execution and system information discovery.
3. **Impacket:** Used for network sniffing and credential dumping.
4. **ipconfig:** Utilized for system network configuration discovery.
5. **Mimikatz:** Employed for credential dumping and token manipulation.
6. **Net:** Used for account discovery and remote system discovery.
7. **netsh:** Employed for event triggered execution and firewall manipulation.
8. **Ping:** Used for remote system discovery.
9. **PowerLess:** Utilized for data archiving and keylogging.
10. **PsExec:** Employed for system process creation and lateral tool transfer.
11. **Pupy:** Used for a wide range of activities including audio capture, file discovery, and screen capture.
12. **Systeminfo:** Utilized for system information discovery.

APT - Group Overview

Description:

menuPass, also known as APT10, is a threat group that has been active since at least 2006. This group is known for its association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and has worked for the Huaying Hantai Science and Technology Development Company. menuPass has targeted a wide range of sectors globally, including healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government, with a particular emphasis on Japanese organizations. The group has also targeted managed IT service providers (MSPs), manufacturing and mining companies, and a university.

Motivation:

The primary motivation of menuPass appears to be espionage, likely driven by geopolitical and economic interests, given its focus on a wide range of critical sectors and global targets.

Names:

- menuPass
- Associated Groups: Cicada, POTASSIUM, Stone Panda, Red Apollo, CVNX, HOGFISH

Location:

menuPass primarily targets global entities, with a significant focus on Japanese organizations.

First Seen:

The group has been active since at least 2006.

Observed:

menuPass has been observed employing a variety of sophisticated cyber espionage techniques and tools, focusing on espionage and data exfiltration.

Techniques Used in all Tactics

1. **Account Discovery:** Used csvde.exe to export Active Directory data.
2. **Acquire Infrastructure:** Registered malicious domains for intrusion campaigns.
3. **Archive Collected Data:** Encrypted and compressed files before exfiltration.
4. **Automated Collection:** Used Csvde tool for collecting Active Directory files and data.
5. **Command and Scripting Interpreter:** Utilized PowerShell, Windows Command Shell, and malicious macros for execution.
6. **Data from Local System:** Collected various files from compromised computers.
7. **Data from Network Shared Drive:** Collected data from remote systems by mounting network shares.
8. **Data Staged:** Staged data in multi-part archives, often saved in the Recycle Bin.
9. **Deobfuscate/Decode Files or Information:** Used certutil for decoding base64-encoded content.
10. **Dynamic Resolution:** Employed dynamic DNS service providers for hosting malicious domains.
11. **Exploit Public-Facing Application:** Leveraged vulnerabilities in Pulse Secure VPNs.
12. **Exploitation of Remote Services:** Used tools to exploit the ZeroLogon vulnerability.
13. **File and Directory Discovery:** Searched compromised systems for folders of interest.
14. **Hijack Execution Flow:** Used DLL search order hijacking and DLL side-loading.
15. **Indicator Removal:** Removed PowerShell execution logs and deleted files after use.
16. **Ingress Tool Transfer:** Installed updates and new malware on victims.
17. **Input Capture:** Employed keyloggers for stealing usernames and passwords.
18. **Masquerading:** Used esentutil for changing file extensions.
19. **Network Service Discovery:** Used tcping.exe for probing port status.
20. **Obfuscated Files or Information:** Encoded strings with base64 and XOR obfuscation.
21. **Obtain Capabilities:** Used and modified open-source tools like Impacket and Mimikatz.
22. **OS Credential Dumping:** Dumped credentials using modified pentesting tools.
23. **Phishing:** Sent malicious Office documents and executables via email.
24. **Process Injection:** Utilized process hollowing in iexplore.exe.
25. **Proxy:** Used external IP as a proxy for C2 traffic.
26. **Remote Services:** Employed RDP and SSH for network movement.
27. **Remote System Discovery:** Used scripts and net view for information gathering.

28. **Scheduled Task/Job:** Executed commands via Task Scheduler.
29. **Subvert Trust Controls:** Resized and added data to certificate tables.
30. **System Binary Proxy Execution:** Used InstallUtil.exe for execution.
31. **System Network Configuration Discovery:** Scanned for open NetBIOS nameservers.
32. **Trusted Relationship:** Exploited access to MSPs to reach victims.
33. **User Execution:** Attempted to get victims to open malicious files.
34. **Valid Accounts:** Used valid accounts for movement between environments.
35. **Windows Management Instrumentation:** Used modified pentesting script for WMI access.

Software Used by menuPass

1. **AdFind:** Used for account and domain trust discovery.
2. **certutil:** Employed for file decoding and information deobfuscation.
3. **ChChes:** Utilized for various activities including data encoding and file discovery.
4. **cmd:** Used for command execution and file manipulation.
5. **Cobalt Strike:** Employed for a wide range of activities including exploitation and credential dumping.
6. **Ecipekac:** Used for file deobfuscation and code signing subversion.
7. **esentutil:** Employed for data extraction and file manipulation.
8. **EvilGrab:** Used for audio capture and keylogging.
9. **FYAnti:** Employed for data obfuscation and evasion.
10. **Impacket:** Used for network sniffing and credential dumping.
11. **Mimikatz:** Employed for credential dumping and token manipulation.
12. **Net:** Used for account discovery and remote system discovery.
13. **P8RAT:** Employed for data obfuscation and evasion.
14. **Ping:** Used for remote system discovery.
15. **PlugX:** Employed for command execution and file discovery.
16. **PoisonIvy:** Used for application window discovery and data extraction.
17. **PowerSploit:** Employed for token manipulation and keylogging.
18. **PsExec:** Used for system process creation and lateral tool transfer.
19. **pwdump:** Employed for credential dumping.
20. **QuasarRAT:** Used for remote access and data extraction.
21. **RedLeaves:** Employed for file discovery and screen capture.
22. **SNUGRIDE:** Used for command execution and encrypted communication.
23. **SodaMaster:** Employed for data encryption and system information discovery.
24. **UPPERCUT:** Used for command execution and screen capture.

APT - Group Overview

Description:

Metador is a suspected cyber-espionage group that emerged in September 2022. The group has primarily targeted telecommunications companies, internet service providers, and universities in the Middle East and Africa. The name "Metador" is derived from the string "I am meta" found in one of the group's malware samples and the anticipated Spanish-language responses from their command and control (C2) servers.

Motivation:

While the specific motivations of Metador are not explicitly stated, the nature of their targets suggests interests in intelligence gathering and espionage, particularly in the telecommunications and academic sectors.

Names:

- Metador

Location:

Metador's activities have been focused on entities in the Middle East and Africa.

First Seen:

The group was first reported in September 2022.

Observed:

Metador has been observed using sophisticated techniques and unique malware in their operations, indicating a high level of skill and specific targeting objectives.

Techniques Used in all Tactics

1. **Application Layer Protocol:** Used HTTP for C2 communications.
2. **Command and Scripting Interpreter:** Employed the Windows command line for executing commands.
3. **Event Triggered Execution:** Established persistence using WMI event subscription and living-off-the-land binaries like cdb.exe.
4. **Indicator Removal:** Quickly deleted cdb.exe following successful malware deployment.
5. **Ingress Tool Transfer:** Downloaded tools and malware onto compromised systems.
6. **Non-Application Layer Protocol:** Utilized TCP for C2 communications.
7. **Obfuscated Files or Information:** Encrypted their payloads to evade detection.
8. **Obtain Capabilities:** Used unique malware, including metaMain and Mafalda, and tools like Microsoft's Console Debugger.

Software Used by Metador

1. Mafalda:

- **Techniques:** Token manipulation, web protocol usage, browser information discovery, PowerShell execution, data encoding, local data staging, debugger evasion, symmetric encryption, external remote services, file and directory discovery, registry modification, screen capture, and more.
- **Capabilities:** Mafalda is a multifaceted tool capable of performing a wide range of espionage activities, including credential dumping, data exfiltration, and internal network exploration.

2. metaMain:

- **Techniques:** Web protocol usage, data staging, file and directory discovery, DLL side-loading, keylogging, reflective code loading, internal proxy usage, and more.
- **Capabilities:** metaMain is designed for extensive data collection, exfiltration, and system manipulation, demonstrating advanced capabilities in maintaining persistence and evading detection.

APT - Group Overview

Description:

Moafee is a cyber threat group believed to be operating out of the Guangdong Province in China. This group is known for its sophisticated cyber attacks and is thought to have connections with another threat group, DragonOK, due to similarities in tactics, techniques, and procedures (TTPs), including the use of custom tools.

Motivation:

While specific motivations for Moafee's activities are not detailed, the group's sophisticated nature and the overlap with other known threat groups suggest a focus on cyber espionage and intelligence gathering.

Names:

- Moafee

Location:

Moafee is believed to be operating from the Guangdong Province of China.

First Seen:

The group was first identified and reported in cybersecurity literature in 2014.

Observed:

Moafee has been observed employing advanced cyber techniques and using custom tools in its operations, indicating a high level of technical proficiency and strategic planning in its cyber espionage activities.

Techniques Used in all Tactics

1. **Obfuscated Files or Information:** Moafee has used binary padding as a method to obfuscate files and information, making it more challenging for security systems to detect their malicious activities.

Software Used by Moafée

1. PoisonIvy:

- **Techniques:** Includes application window discovery, boot or logon autostart execution, command and scripting interpreter usage, data extraction from local systems, encrypted communication channels, keylogging, registry modification, and process injection.
- **Capabilities:** PoisonIvy is a versatile remote access tool (RAT) used by Moafée for a wide range of espionage activities, including data theft, system surveillance, and maintaining persistent access to compromised systems.

APT - Group Overview

Description:

Mofang is a cyber espionage group, likely based in China, known for its sophisticated cyber operations. The group has been active since at least May 2012 and is characterized by its strategy of imitating the infrastructure of its victims. Mofang primarily targets government entities and critical infrastructure sectors in Myanmar and other countries, including military, automobile, and weapons industries.

Motivation:

Mofang's activities suggest a focus on espionage, likely driven by political and strategic interests. The group's targeting of government and critical infrastructure sectors indicates an intent to gather sensitive information and possibly disrupt operations in these areas.

Names:

- Mofang

Location:

Mofang is believed to be based in China.

First Seen:

The group was first identified and reported in cybersecurity literature in May 2012.

Observed:

Mofang has been observed conducting focused attacks against a variety of targets, employing sophisticated techniques to evade detection and successfully infiltrate target networks.

Techniques Used in all Tactics

1. **Obfuscated Files or Information:** Mofang has used compression and encryption techniques to obfuscate executable files within email attachments and payloads before downloading them to victims' systems.
2. **Phishing: Spearphishing Attachment:** The group has delivered spearphishing emails containing malicious documents, PDFs, or Excel files.
3. **Phishing: Spearphishing Link:** Mofang has also used spearphishing emails with embedded malicious links.
4. **User Execution: Malicious Link:** The group's spearphishing campaigns often require the user to click a link that leads to a compromised website.
5. **User Execution: Malicious File:** Mofang's attacks often rely on users opening malicious file attachments received via email.

Software Used by Mofang

1. ShimRat:

- **Techniques:** Includes bypassing User Account Control, using web protocols, creating Windows services, data extraction, application shimming, file and directory discovery, registry modification, and more.
- **Capabilities:** ShimRat is a sophisticated tool used by Mofang for various espionage activities, including data theft and maintaining access to compromised systems.

2. ShimRatReporter:

- **Techniques:** Account discovery, web protocols, data archiving, automated collection and exfiltration, masquerading, process discovery, and system information discovery.
- **Capabilities:** ShimRatReporter is used for gathering and transmitting sensitive information from compromised systems, enhancing Mofang's intelligence-gathering capabilities.

APT - Group Overview

Description:

Molerats, an Arabic-speaking, politically-motivated threat group, has been active since 2012. The group primarily targets entities in the Middle East, Europe, and the United States. Their operations are characterized by sophisticated cyber espionage tactics.

Motivation:

Molerats' activities suggest a focus on gathering intelligence and possibly influencing political scenarios in the targeted regions. Their consistent targeting of specific geographic areas indicates a strategic intent behind their operations.

Names:

- Molerats
- Operation Molerats
- Gaza Cybergang

Location:

The group is believed to operate from an undisclosed location, with a focus on the Middle East, Europe, and the United States.

First Seen:

Molerats was first identified in 2012.

Observed:

The group has been observed conducting cyber espionage campaigns, employing a range of sophisticated techniques to infiltrate and extract information from target networks.

Techniques Used in all Tactics

1. **Boot or Logon Autostart Execution:** Molerats used the Startup folder and Registry Run keys for persistence.
2. **Command and Scripting Interpreter:** They employed PowerShell, VBScript, and JavaScript in their implants.
3. **Credentials from Password Stores:** The group used tools like BrowserPasswordDump10 to extract saved browser passwords.
4. **Deobfuscate/Decode Files or Information:** They decompressed ZIP files on victim machines.
5. **Ingress Tool Transfer:** Executables were used to download malicious files.
6. **Obfuscated Files or Information:** Molerats delivered compressed executables within ZIP files.
7. **Phishing:** Spearphishing with attachments and links was a primary vector for initial compromise.
8. **Process Discovery:** They obtained lists of active processes for reconnaissance.
9. **Scheduled Task/Job:** Scheduled tasks were created for persistence.
10. **Subvert Trust Controls:** Forged Microsoft code-signing certificates were used on malware.
11. **System Binary Proxy Execution:** Msiexec.exe was utilized to execute MSI payloads.
12. **User Execution:** Malicious links and files were sent via email to trick users into executing them.

Software Used by Molerats

1. **DropBook:** Used for Python and Windows Command Shell scripting, information discovery, and data exfiltration.
2. **DustySky:** Employed for data collection, keylogging, screen capture, and system information discovery.
3. **MoleNet:** Utilized for system information discovery and execution via Windows Management Instrumentation.
4. **PoisonIvy:** A tool for keylogging, data extraction, and process injection.
5. **SharpStage:** Used for data staging, screen capture, and system information discovery.
6. **Spark:** Employed for data encoding, system discovery, and evasion techniques.

Description:

Moses Staff is a suspected Iranian threat group that has been active since at least September 2021. The group is known for its targeted cyber attacks against Israeli companies, aiming to cause damage by leaking sensitive data and encrypting networks without demanding a ransom.

Motivation:

Moses Staff's operations are politically motivated, with a clear focus on causing disruption and extracting sensitive information from Israeli entities. Their activities also extend to government, finance, travel, energy, manufacturing, and utility sectors in various countries, including Italy, India, Germany, Chile, Turkey, the UAE, and the US.

Names:

- Moses Staff

Location:

While the exact location is undisclosed, the group is suspected to be operating from Iran.

First Seen:

Moses Staff was first reported in September 2021.

Observed:

The group has been observed targeting a range of sectors with sophisticated cyber espionage tactics, primarily focusing on Israeli companies but also extending their operations globally.

Techniques Used in all Tactics

1. **Account Discovery:** Collected administrator usernames from compromised hosts.
2. **Develop Capabilities:** Built malware such as DCSrv and PyDCrypt for targeting victims' machines.
3. **Exploit Public-Facing Application:** Exploited vulnerabilities in Microsoft Exchange Servers.
4. **Impair Defenses:** Disabled Windows firewalls using batch scripts.
5. **Ingress Tool Transfer:** Downloaded and installed web shells.
6. **Obfuscated Files or Information:** Employed obfuscated web shells.
7. **Obtain Capabilities:** Utilized tools like DiskCryptor.
8. **Remote Services:** Enabled SMB on compromised hosts.
9. **Server Software Component:** Dropped web shells onto systems.
10. **Subvert Trust Controls:** Used signed drivers from DiskCryptor for evasion.
11. **System Information Discovery:** Collected details about infected hosts.

12. **System Network Configuration Discovery:** Gathered domain names of compromised networks.

Software Used by Moses Staff

1. **DCSrv:** Used for creating/modifying system processes, encrypting data, masquerading tasks, modifying registry, and system shutdown/reboot.
2. **PsExec:** Employed for creating accounts, modifying system processes, lateral tool transfer, and system service execution.
3. **PyDCrypt:** Utilized for command execution, impairing defenses, indicator removal, masquerading, and system discovery.
4. **StrifeWater:** Used for command execution, data exfiltration, file and directory discovery, indicator removal, masquerading, scheduled tasks, screen capture, and system information discovery.

APT - Group Overview: MuddyWater

Description:

MuddyWater is a cyber espionage group, believed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS). Active since at least 2017, MuddyWater has been involved in numerous cyber operations targeting a wide range of sectors, including telecommunications, local government, defense, and oil and natural gas organizations. Their activities span across the Middle East, Asia, Africa, Europe, and North America.

Motivation:

MuddyWater's operations are primarily driven by espionage motives, focusing on gathering sensitive information from government and private organizations. Their activities suggest a state-sponsored agenda, likely aimed at advancing Iran's national interests.

Names:

The group is also known by various aliases, including Earth Vetala, MERCURY, Static Kitten, Seedworm, and TEMP.Zagros.

Location:

MuddyWater is assessed to operate from Iran.

First Seen:

The group's activities were first identified in 2017.

Observed:

MuddyWater has been observed employing a range of sophisticated cyber tactics and techniques. They have targeted various entities across multiple regions, indicating a broad and persistent threat landscape.

Techniques Used in all tactics:

- **Abuse Elevation Control Mechanism:** Bypassing User Account Control to execute privileged operations.
- **Account Discovery:** Enumerating domain accounts using command-line tools.
- **Acquire Infrastructure:** Utilizing web services for distributing tools.
- **Application Layer Protocol:** Employing HTTP for command and control (C2) communications.
- **Archive Collected Data:** Using native tools like `makecab.exe` for compressing stolen data.
- **Boot or Logon Autostart Execution:** Establishing persistence via Registry Run keys.
- **Command and Scripting Interpreter:** Utilizing PowerShell, Windows Command Shell, VBScript, Python, and JavaScript for execution and control.
- **Credentials from Password Stores:** Dumping credentials using tools like LaZagne.
- **Data Encoding and Obfuscation:** Encoding C2 communications and obfuscating files and information.
- **Exploitation of Public-Facing Applications and Remote Services:** Leveraging known vulnerabilities for initial access and execution.
- **File and Directory Discovery:** Identifying folders and files of interest on compromised systems.
- **Hijack Execution Flow:** Employing DLL side-loading for persistence.
- **Impair Defenses:** Disabling security tools and modifying system firewall settings.
- **Ingress Tool Transfer:** Uploading additional malicious files to victims' machines.
- **Inter-Process Communication:** Executing malicious code via COM, DCOM, and Outlook.
- **Masquerading:** Disguising malicious executables and using filenames associated with legitimate Windows processes.
- **Multi-Stage Channels and Proxy:** Using various C2 channels and proxy networks to obfuscate activities.
- **Phishing:** Spearphishing with attachments and links for initial compromise.
- **Process Discovery:** Enumerating running processes on the victim's system.
- **Remote Access Software:** Utilizing legitimate applications for remote management and lateral movement.
- **Scheduled Task/Job:** Using scheduled tasks for persistence.
- **Screen Capture:** Capturing screenshots of victims' machines.
- **Software Discovery:** Identifying security software and other applications on compromised systems.
- **System Binary Proxy Execution:** Leveraging legitimate system binaries like `CMSTP.exe`, `Mshsta.exe`, and `Rundll32.exe` for execution.
- **System Information Discovery:** Collecting information about the infected host.
- **Unsecured Credentials:** Accessing credentials stored in files.

Software Used by MuddyWater:

- ConnectWise
- CrackMapExec
- Empire
- Koadic

- LaZagne
- Mimikatz
- Mori
- Out1
- PowerSploit
- POWERSTATS
- PowGoop
- RemoteUtilities
- SHARPSTATS
- Small Sieve
- STARWHALE

APT - Group Overview: Mustang Panda

Description:

Mustang Panda is a China-based cyber espionage threat actor, first observed in 2017, but potentially active since 2014. The group has targeted a diverse set of entities including government organizations, nonprofits, religious groups, and other non-governmental organizations across various countries such as the U.S., Europe, Mongolia, Myanmar, Pakistan, and Vietnam.

Motivation:

The primary motivation of Mustang Panda appears to be espionage, with a focus on gathering sensitive information from a wide range of international targets.

Names:

Mustang Panda is also known by other names including TA416, RedDelta, and BRONZE PRESIDENT.

Location:

The group is believed to be operating out of China.

First Seen:

Mustang Panda's activities were first identified in 2017.

Observed:

The group has been observed conducting cyber espionage operations against a variety of targets worldwide, indicating a broad and persistent campaign.

Techniques Used in all tactics:

- **Acquire Infrastructure:** Acquiring C2 domains prior to operations.
- **Application Layer Protocol:** Communicating with C2 via HTTP POST requests.
- **Archive Collected Data:** Using RAR for creating password-protected archives and encrypting documents with RC4.
- **Automated Collection:** Utilizing custom batch scripts for automatic data collection.
- **Boot or Logon Autostart Execution:** Creating registry keys for persistence.
- **Command and Scripting Interpreter:** Employing PowerShell, Windows Command Shell, and VBScript for execution.
- **Data Staged:** Storing collected data locally before exfiltration.
- **Encrypted Channel:** Encrypting C2 communications.
- **Establish Accounts:** Leveraging legitimate email services for phishing campaigns.
- **Event Triggered Execution:** Using WMI event subscription for persistence.
- **Exfiltration Over Physical Medium:** Employing customized PlugX variant for data exfiltration.
- **Exploitation for Client Execution:** Exploiting vulnerabilities like CVE-2017-0199.
- **File and Directory Discovery:** Searching for specific file types on targeted systems.
- **Hide Artifacts:** Creating hidden folders and using DLL side-loading.
- **Indicator Removal:** Deleting tools and files post-operation.
- **Ingress Tool Transfer:** Downloading additional executables post-infection.
- **Masquerading:** Using deceptive file names and double file extensions.
- **Obfuscated Files or Information:** Delivering payloads hidden using archives and encoding.
- **OS Credential Dumping:** Utilizing vssadmin and reg save for credential access.
- **Phishing:** Spearphishing with attachments and links.
- **Process Discovery:** Using tasklist to gather active process information.
- **Remote Access Software:** Installing TeamViewer for remote access.
- **Replication Through Removable Media:** Spreading through USB connections.
- **Scheduled Task/Job:** Creating tasks for execution and persistence.
- **Software Discovery:** Searching for specific programs and versions.
- **Stage Capabilities:** Using servers to validate tracking pixels.
- **System Binary Proxy Execution:** Utilizing InstallUtil.exe and Mshta.exe.
- **System Information Discovery:** Gathering system information.
- **System Network Configuration Discovery:** Using ipconfig and arp for network information.
- **System Network Connections Discovery:** Employing netstat for network connection details.
- **User Execution:** Sending malicious links and files requiring user interaction.
- **Web Service:** Using services like DropBox for payload delivery.
- **Windows Management Instrumentation:** Executing scripts via WMI.

Software Used by Mustang Panda:

- Cobalt Strike
- NBTscan
- PlugX
- PoisonIvy
- RCSession

APT - Group Overview: Naikon

Description:

Naikon is a state-sponsored cyber espionage group attributed to the Chinese People's Liberation Army's Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020). Active since at least 2010, Naikon has primarily targeted government, military, and civil organizations in Southeast Asia, as well as international bodies such as the United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN).

Motivation:

Naikon's primary motivation appears to be gathering intelligence and conducting espionage activities in line with state-sponsored objectives.

Names:

Naikon is also known by other identifiers, including its Military Unit Cover Designator 78020.

Location:

The group is believed to be operating out of China, specifically linked to the Chinese PLA's Chengdu Military Region.

First Seen:

Naikon's activities date back to at least 2010.

Observed:

The group has been observed conducting espionage operations against a range of targets in Southeast Asia and international organizations.

Techniques Used in all tactics:

- **Boot or Logon Autostart Execution:** Modifying Windows Run registry for persistence.
- **Hijack Execution Flow:** Using DLL side-loading techniques.
- **Masquerading:** Renaming malicious services and disguising programs as legitimate software.
- **Network Service Discovery:** Employing tools like LadonGo scanner.
- **Office Application Startup:** Utilizing RoyalRoad exploit builder for dropping loaders.
- **Phishing:** Spearphishing with email attachments.
- **Remote System Discovery:** Using netbios scanner.
- **Scheduled Task/Job:** Employing schtasks.exe for lateral movement.
- **Software Discovery:** Discovering local firewall and network interface settings.
- **System Network Configuration Discovery:** Using commands for network discovery.
- **User Execution:** Convincing victims to open malicious attachments.

- **Valid Accounts:** Using administrator credentials for lateral movement.
- **Windows Management Instrumentation:** Utilizing WMIC.exe for lateral movement.

Software Used by Naikon:

- **Aria-body:** Various techniques including data encryption, file discovery, and screen capture.
- **ftp:** Used for exfiltration and tool transfer.
- **HDoor:** Disabling or modifying tools, network service discovery.
- **Nebulae:** Employing DLL side-loading, data encryption, and file deletion.
- **Net:** Various network-related activities and system discovery.
- **netsh:** Discovering security software and modifying system firewall.
- **Ping:** Remote system discovery.
- **PsExec:** Lateral movement and system service execution.
- **RainyDay:** Various techniques including web protocols, file discovery, and screen capture.
- **RARSTONE:** File discovery and tool transfer.
- **SsIMM:** Various techniques including token manipulation and system information discovery.
- **Sys10:** Web protocols and system information discovery.
- **Systeminfo:** System information discovery.
- **Tasklist:** Process and software discovery.
- **WinMM:** Web protocols, file discovery, and system information discovery.

APT - Group Overview: NEODYMIUM

Description:

NEODYMIUM is an activity group known for its cyber campaign in May 2016, primarily targeting Turkish victims. The group displays similarities to another activity group, PROMETHIUM, due to overlapping victim profiles and campaign characteristics. NEODYMIUM is also reportedly associated with BlackOasis operations, although there is no conclusive evidence to suggest that these group names are aliases.

Motivation:

NEODYMIUM's specific motivations are not detailed in the provided information, but their targeted attacks suggest a focus on intelligence gathering, possibly for political or strategic purposes.

Names:

NEODYMIUM is the primary name used to identify this group. There are indications of a possible association with BlackOasis, but this remains unconfirmed.

Location:

The exact location of NEODYMIUM is not specified, but their targeting of Turkish victims suggests a possible interest in the region or connections to it.

First Seen:

NEODYMIUM's activities were first observed in May 2016.

Observed:

The group has been notably active in targeting individuals and entities in Europe, with a heavy focus on Turkish victims. Their operations are characterized by the use of specific malware and tactics.

Techniques Used in all tactics:

- **Boot or Logon Autostart Execution:** Utilizing LSASS Driver for persistence.
- **Create or Modify System Process:** Creating or modifying Windows services.
- **Exploitation for Privilege Escalation:** Exploiting vulnerabilities to escalate privileges.
- **Hijack Execution Flow:** Employing DLL side-loading techniques.
- **Indicator Removal:** Deleting files to remove traces of their presence.
- **Process Injection:** Injecting malicious code into processes.
- **Software Discovery:** Discovering security software on the victim's system.
- **System Information Discovery:** Gathering information about the victim's system.
- **System Services:** Executing services as part of their operation.

Software Used by NEODYMIUM:

- **Wingbird:** This malware has been used by NEODYMIUM and is associated with various techniques such as boot or logon autostart execution, creating or modifying system processes, exploitation for privilege escalation, DLL side-loading, file deletion for indicator removal, process injection, security software discovery, system information discovery, and system service execution.

APT - Group Overview: Nomadic Octopus

Description:

Nomadic Octopus is a Russian-speaking cyber espionage threat group. Active since at least 2014, they have primarily targeted Central Asia, focusing on local governments, diplomatic missions, and individuals. The group is known for its campaigns involving both Android and Windows malware, predominantly developed using the Delphi programming language. They have been observed creating custom variants for their operations.

Motivation:

While specific motivations are not detailed, the targeting of government and diplomatic entities suggests a focus on intelligence gathering, possibly for political or strategic purposes.

Names:

- **Primary:** Nomadic Octopus
- **Associated:** DustSquad

Location:

The group primarily targets Central Asia, indicating a regional focus in their operations.

First Seen:

Nomadic Octopus has been active since at least 2014.

Observed:

The group has been observed conducting espionage campaigns involving sophisticated malware targeting various entities in Central Asia.

Techniques Used in all tactics:

- **Command and Scripting Interpreter: PowerShell:** Utilizing PowerShell for execution.
- **Command and Scripting Interpreter: Windows Command Shell:** Employing cmd.exe within malicious macros.
- **Hide Artifacts: Hidden Window:** Executing PowerShell in a hidden window to avoid detection.
- **Ingress Tool Transfer:** Using malicious macros to download additional files to victims' machines.
- **Masquerading:** Attempting to disguise Octopus malware as a Telegram Messenger with a Russian interface.
- **Phishing: Spearphishing Attachment:** Targeting victims with spearphishing emails containing malicious attachments.
- **User Execution: Malicious File:** Luring victims to click on malicious attachments within spearphishing emails.

Software Used by Nomadic Octopus:

- **Octopus:** A multifunctional malware tool used by Nomadic Octopus, featuring capabilities such as:
 - Web protocol communication
 - Data archiving and staging
 - Exfiltration over C2 channels and cloud storage
 - File and directory discovery
 - Screen capture
 - System information discovery
 - Masquerading as legitimate applications
 - User execution through malicious files
 - Windows Management Instrumentation utilization

APT - Group Overview: OilRig

Description:

OilRig is a suspected Iranian threat group that has been active since at least 2014. The group has targeted a diverse range of sectors, including financial, government, energy, chemical, and telecommunications. Notably, OilRig is known for carrying out supply chain attacks, exploiting the trust relationship between organizations to reach their primary targets. The group's activities are believed to be conducted on behalf of the Iranian government, as suggested by infrastructure details referencing Iran, the use of Iranian infrastructure, and targeting that aligns with nation-state interests.

Motivation:

OilRig's operations are primarily driven by espionage, with a focus on collecting sensitive information from targeted sectors. Their activities align with the strategic interests of the Iranian state, indicating a nation-state backed cyber espionage motive.

Names:

- Primary: OilRig
- Associated: COBALT GYPSY, IRN2, APT34, Helix Kitten, Evasive Serpens

Location:

OilRig primarily targets entities in the Middle East and has international reach.

First Seen:

The group has been active since at least 2014.

Observed:

OilRig has been observed targeting a variety of sectors with sophisticated cyber espionage tactics.

Techniques Used in all tactics:

- **Account Discovery:** Using commands like `net user` for account listings.
- **Application Layer Protocol:** Utilizing HTTP and DNS for C2 communications.
- **Automated Collection:** Employing automated methods for data collection.
- **Brute Force:** Using brute force techniques for credential access.
- **Command and Scripting Interpreter:** Leveraging PowerShell, Windows Command Shell, and VBScript for execution.
- **Credentials from Password Stores:** Using tools like LaZagne for credential dumping.
- **Deobfuscate/Decode Files or Information:** Employing methods like `catcat11` for decoding.

files.

- **Encrypted Channel:** Using asymmetric cryptography for secure communication.
- **Exfiltration Over Alternative Protocol:** Exfiltrating data over FTP.
- **External Remote Services:** Utilizing remote services like VPN for persistence.
- **Fallback Channels:** Using DNS tunneling as a fallback communication method.
- **Indicator Removal:** Deleting files associated with payloads post-execution.
- **Ingress Tool Transfer:** Downloading remote files onto victims.
- **Input Capture:** Employing keylogging tools.
- **Masquerading:** Disguising malicious programs with legitimate file extensions.
- **Network Service Discovery:** Using network scanning tools for discovery.
- **Obfuscated Files or Information:** Encrypting and encoding data in malware.
- **Office Application Startup:** Abusing Outlook Home Page feature for persistence.
- **OS Credential Dumping:** Utilizing tools like Mimikatz for credential dumping.
- **Password Policy Discovery:** Discovering domain password policies.
- **Peripheral Device Discovery:** Identifying connected devices like mice.
- **Permission Groups Discovery:** Discovering local and domain group permissions.
- **Phishing:** Spearphishing with attachments and links.
- **Process Discovery:** Running `tasklist` for active process information.
- **Protocol Tunneling:** Creating tunnels to C2 servers.
- **Query Registry:** Accessing the Registry for information gathering.
- **Remote Services:** Using RDP and SSH for lateral movement.
- **Scheduled Task/Job:** Creating tasks for execution and persistence.
- **Screen Capture:** Capturing screenshots of the user's desktop.
- **Server Software Component:** Using web shells for persistent access.
- **System Binary Proxy Execution:** Utilizing CHM payloads for execution.
- **System Information Discovery:** Gathering system information using commands like `hostname`.
- **System Network Configuration Discovery:** Running `ipconfig /all` for network configuration.
- **System Network Connections Discovery:** Using `netstat -an` for network connections.
- **System Owner/User Discovery:** Running `whoami` for user information.
- **System Service Discovery:** Using `sc query` for service information.
- **Unsecured Credentials:** Stealing credentials from files.
- **User Execution:** Delivering malicious links and files for execution.
- **Valid Accounts:** Using compromised credentials for network access.
- **Virtualization/Sandbox Evasion:** Checking for connected peripherals.
- **Windows Management Instrumentation:** Using WMI for execution.

Software Used by OilRig:

- BONDUPDATER
- certutil
- ftp
- Helminth
- ipconfig
- ISMinjector
- LaZagne
- Mimikatz
- Net
- netstat

- OopsIE
- POWRUNER
- PsExec
- QUADAGENT
- Reg
- RGDoor
- SEASHARPEE
- SideTwist
- Systeminfo
- Tasklist

OilRig's sophisticated and diverse set of tactics, techniques, and procedures (TTPs) highlight its capability as a significant player in the realm of state-sponsored cyber espionage. The group's focus on Middle Eastern and international targets, along with its advanced methods of attack, demonstrate a high level of expertise and resources likely backed by a nation-state.

APT - Group Overview: Orangethreat

Description:

Orangethreat is a cyber threat group that has been actively targeting organizations in the healthcare sector across the United States, Europe, and Asia since at least 2015. The group's primary focus appears to be corporate espionage, gathering sensitive information from healthcare-related organizations.

Motivation:

The main motive of Orangethreat seems to be corporate espionage. Their consistent targeting of healthcare organizations indicates a specific interest in acquiring confidential and proprietary information related to this sector.

Names:

- Primary: Orangethreat

Location:

Orangethreat has targeted organizations in the United States, Europe, and Asia, indicating a broad geographical focus.

First Seen:

The group has been active since at least 2015.

Observed:

Orangethreat has been observed conducting targeted attacks against the healthcare sector.

likely for espionage purposes.

Techniques Used in all tactics:

- **Application Layer Protocol:** Orangeworm has utilized HTTP for Command and Control (C2) communications.
- **Remote Services:** The group has exploited SMB/Windows Admin Shares for lateral movement, copying its backdoor across open network shares.

Software Used by Orangeworm:

- **Arp:** Used for remote system discovery and system network configuration discovery.
- **cmd:** Employed for various purposes including command execution, file and directory discovery, indicator removal, ingress tool transfer, lateral tool transfer, and system information discovery.
- **ipconfig:** Utilized for system network configuration discovery.
- **Kwampirs:** A backdoor used by Orangeworm for a range of activities including account discovery, system process creation, deobfuscation of information, network share discovery, and system information gathering.
- **Net:** Used for account discovery, network share discovery, remote services access, and system service discovery.
- **netstat:** Employed for system network connections discovery.
- **route:** Utilized for system network configuration discovery.
- **Systeminfo:** Used for system information discovery.

Orangeworm's targeted approach, focusing on the healthcare sector, demonstrates a clear intent and capability to infiltrate and extract valuable information from this industry. The use of specific tools like Kwampirs further indicates a sophisticated level of technical expertise and a focused operational objective.

APT - Group Overview: Patchwork

Description:

Patchwork, also known as Hangover Group, Dropping Elephant, Chinastrats, MONSOON, and Operation Hangover, is a cyber espionage group first observed in December 2015. While definitive attribution is unclear, circumstantial evidence suggests it may be a pro-Indian or Indian entity. The group has targeted diplomatic and government agencies, and has been known for its spearphishing campaigns targeting U.S. think tanks.

Motivation:

Patchwork's activities suggest a focus on espionage, likely driven by political and strategic interests, particularly in gathering intelligence from government and diplomatic entities.

Names:

- Aliases: Hangover Group, Dropping Elephant, Chinastrats, MONSOON, Operation Hangover

Location:

Patchwork has targeted entities globally, with a focus on the Indian subcontinent and U.S. think tanks.

First Seen:

The group was first observed in December 2015.

Observed:

Patchwork has been active in conducting cyber espionage campaigns, primarily targeting diplomatic and government sectors. The group is known for its use of copied and pasted code from online forums and spearphishing techniques.

Techniques Used in all tactics:

- **Abuse Elevation Control Mechanism:** Bypassed User Access Control (UAC).
- **Archive Collected Data:** Encrypted and base64-encoded collected files' paths.
- **Automated Collection:** Developed a file stealer for specific file extensions and executed scripts for data enumeration and upload.
- **BITS Jobs:** Used for downloading malicious payloads.
- **Boot or Logon Autostart Execution:** Added malware to startup folders and Registry Run keys for persistence.
- **Command and Scripting Interpreter:** Used PowerShell, Windows Command Shell, and Visual Basic Scripts for execution.
- **Credentials from Password Stores:** Dumped credentials from web browsers.
- **Data Encoding:** Employed Base64 encoding for C2 traffic.
- **Data from Local System:** Collected and exfiltrated files from infected systems.
- **Data Staged:** Local Data Staging in a directory called 'index' for C&C upload.
- **Develop Capabilities:** Created self-signed certificates for malware signing.
- **Drive-by Compromise:** Utilized watering holes for initial victim exploitation.
- **Exploitation for Client Execution:** Used various exploits in malicious documents.
- **File and Directory Discovery:** Searched drives for files with specific extensions.
- **Hijack Execution Flow:** Employed DLL side-loading techniques.
- **Indicator Removal:** Deleted and replaced certain files.
- **Ingress Tool Transfer:** Downloaded additional files from C2 servers.
- **Inter-Process Communication:** Leveraged the DDE protocol for malware delivery.
- **Masquerading:** Disguised payloads with legitimate-sounding names.
- **Modify Registry:** Altered Registry keys for operational purposes.
- **Obfuscated Files or Information:** Used binary padding, software packing, and command obfuscation.
- **Obtain Capabilities:** Acquired and utilized open-source tools like QuasarRAT.
- **Phishing:** Spearphishing with attachments and links for initial access.
- **Phishing for Information:** Used web bugs for recipient tracking.
- **Process Injection:** Utilized process hollowing techniques.

- **Remote Services:** Attempted lateral movement using RDP.
- **Scheduled Task/Job:** Used TaskScheduler for persistence.
- **Software Discovery:** Scanned for specific security software installations.
- **Subvert Trust Controls:** Signed malware with fabricated certificates.
- **System Information Discovery:** Collected detailed system information.
- **System Owner/User Discovery:** Gathered user and admin status information.
- **User Execution:** Encouraged users to execute malicious links and files.
- **Web Service:** Used dead drop resolvers for C2 communication.

Software Used by Patchwork:

- Autolt backdoor
- BackConfig
- BADNEWS
- NDiskMonitor
- PowerSploit
- QuasarRAT
- TINYTYPHON
- Unknown Logger

Patchwork's operations demonstrate a significant focus on espionage through a variety of sophisticated techniques and tools, indicating a well-resourced and technically capable actor with specific intelligence-gathering objectives.

APT - Group Overview: PittyTiger

Description:

PittyTiger is a cyber threat group believed to be operating out of China. This group is known for using a variety of malware types to establish and maintain command and control over compromised systems.

Motivation:

While specific motivations are not detailed, the typical behavior of PittyTiger suggests objectives aligned with espionage, likely driven by political, economic, or strategic interests.

Names:

The primary name for this group is PittyTiger.

Location:

PittyTiger is believed to operate out of China, based on the nature of its attacks and tools used.

First Seen:

The exact date of PittyTiger's first observed activities is not specified in the provided information.

Observed:

PittyTiger has been observed engaging in cyber espionage activities, utilizing various types of malware for command and control operations.

Techniques Used in all tactics:

- **Obtain Capabilities: Tool:** PittyTiger has been known to obtain and use tools such as **Mimikatz** and **gsecdump** for its operations.
- **Valid Accounts:** The group attempts to obtain legitimate credentials during its operations, likely to facilitate lateral movement and maintain access.

Software Used by PittyTiger:

- **gh0st RAT:** A remote access tool with capabilities like keylogging, screen capture, and process manipulation.
- **gsecdump:** A tool used for dumping system credentials.
- **Lurid:** A malware variant used for data encryption and collection.
- **Mimikatz:** A well-known tool used for credential dumping and manipulation.
- **PoisonIvy:** A remote access tool with capabilities for keylogging, data collection, and process injection.

PittyTiger's use of a diverse set of tools and techniques indicates a focus on gaining access to systems and exfiltrating sensitive information, consistent with the objectives of a sophisticated cyber espionage group.

APT - Group Overview: PLATINUM

Description:

PLATINUM is a sophisticated cyber espionage group known for its advanced techniques and focus on targets in South and Southeast Asia. Active since at least 2009, the group has primarily targeted government entities and related organizations.

Motivation:

While specific motivations are not detailed, the group's activities suggest a focus on intelligence gathering and surveillance, likely driven by geopolitical interests.

Names:

The group is predominantly known as PLATINUM.

Location:

PLATINUM's operations primarily target regions in South and Southeast Asia.

First Seen:

The group has been active since at least 2009.

Observed:

PLATINUM has been observed conducting cyber espionage campaigns against government and related organizations in South and Southeast Asia.

Techniques Used in all tactics:

- **Drive-by Compromise:** PLATINUM has used drive-by attacks to exploit vulnerabilities in browser plugins.
- **Exploitation for Privilege Escalation:** The group has leveraged zero-day vulnerabilities for privilege escalation.
- **Ingress Tool Transfer:** PLATINUM has transferred files using Intel® Active Management Technology (AMT) Serial-over-LAN (SOL) channel.
- **Input Capture:** The group has employed various keyloggers and credential API hooking for information gathering.
- **Masquerading:** PLATINUM has renamed tools like rar.exe to avoid detection.
- **Non-Application Layer Protocol:** The group has used the Intel® AMT SOL channel for command and control.
- **OS Credential Dumping:** PLATINUM has used keyloggers capable of dumping credentials from LSASS memory.
- **Phishing:** Spearphishing emails with malicious attachments have been a primary vector for initial access.
- **Process Injection:** Various methods of process injection, including hot patching, have been used.
- **User Execution:** The group has attempted to get users to execute malicious files through spearphishing.

Software Used by PLATINUM:

- **adbuspd:** A tool used for command execution, encrypted communication, and event-triggered execution.
- **Dipsind:** A malware known for web protocol communication, symmetric encryption, and scheduled data transfer.
- **JPIN:** A multifaceted tool capable of mail protocol communication, file transfer, keylogging, process injection, and more.

PLATINUM's sophisticated use of a variety of techniques and custom software indicates a high level of expertise in conducting cyber espionage operations, with a clear focus on maintaining stealth and gathering intelligence from high-value targets in specific geographic regions.

Description:

POLONIUM is a Lebanon-based cyber espionage group known for targeting Israeli organizations, including those in critical manufacturing, information technology, and defense industries. Active since at least February 2022, the group is noted for its sophisticated operations and coordination with entities affiliated with Iran's Ministry of Intelligence and Security (MOIS).

Motivation:

POLONIUM's activities suggest a focus on gathering intelligence and possibly disrupting operations in Israeli organizations. The group's alignment with Iranian interests indicates a geopolitical motivation, likely driven by regional tensions and strategic objectives.

Names:

The group is primarily known as POLONIUM.

Location:

POLONIUM is based in Lebanon and has primarily targeted Israeli entities.

First Seen:

POLONIUM's activities were first observed in February 2022.

Observed:

The group has been observed conducting espionage campaigns against Israeli organizations, leveraging sophisticated techniques and tools.

Techniques Used in all tactics:

- **Acquire Infrastructure: Web Services:** POLONIUM created and used legitimate Microsoft OneDrive accounts for operations.
- **Exfiltration Over Web Service:** The group exfiltrated stolen data to their own OneDrive and Dropbox accounts.
- **Obtain Capabilities: Tool:** POLONIUM obtained and utilized tools like AirVPN and plink.
- **Proxy:** The group used the AirVPN service for operational activities.
- **Trusted Relationship:** POLONIUM exploited compromised credentials from an IT company to target downstream customers, including a law firm and aviation company.
- **Valid Accounts:** They used valid compromised credentials for accessing victim environments.
- **Web Service: Bidirectional Communication:** The group used OneDrive and Dropbox for command and control (C2) communications.

Software Used by POLONIUM:

- **CreepyDrive:** A tool used for web protocol communication, PowerShell scripting, data exfiltration to cloud storage, file discovery, and bidirectional communication via web services.
- **CreepySnail:** This software employs web protocols, PowerShell, standard data encoding, exfiltration over C2 channels, and discovery of network configuration and system ownership information.

POLONIUM's operations reflect a high level of sophistication and strategic focus, aligning with broader geopolitical objectives and showcasing advanced capabilities in cyber espionage. The group's use of legitimate web services for exfiltration and C2, along with its ability to exploit trusted relationships, indicates a nuanced understanding of digital environments and operational security.

APT - Group Overview: Poseidon Group

Description:

Poseidon Group is a Portuguese-speaking threat group known for its unique approach to cyber-espionage. Active since at least 2005, this group is distinctive for using information exfiltrated from victims to blackmail them into contracting the Poseidon Group as a security firm.

Motivation:

The primary motivation of the Poseidon Group appears to be financial gain through a combination of cyber-espionage and blackmail. By exfiltrating sensitive information, they coerce victim companies into hiring them under the guise of a security firm, thus monetizing their cyber-espionage activities.

Names:

The group is predominantly known as the Poseidon Group.

Location:

The Poseidon Group is a Portuguese-speaking entity, but specific geographic location details are not provided.

First Seen:

The group's activities date back to at least 2005.

Observed:

Poseidon Group has been observed engaging in targeted cyber-espionage campaigns, primarily

Techniques Used in all tactics:

- **Account Discovery:** Poseidon Group searches for administrator accounts on local machines and across networks.
- **Command and Scripting Interpreter: PowerShell:** The group's Information Gathering Tool (IGT) includes PowerShell components for executing commands and scripts.
- **Masquerading:** Poseidon Group tools attempt to spoof anti-virus processes as a means of self-defense, hiding their malicious activities.
- **OS Credential Dumping:** They focus on obtaining credentials, particularly those belonging to domain and database servers.
- **Process Discovery:** After compromising a system, the group lists all running processes to understand the environment and identify targets for further exploitation.
- **System Network Connections Discovery:** They obtain and save information about victim network interfaces and addresses.
- **System Service Discovery:** Poseidon Group discovers all running services post-compromise to further their access and control over the victim's system.

Poseidon Group's operations are marked by a blend of technical sophistication and unconventional tactics, including leveraging the stolen data for blackmail. Their focus on credential and service discovery, along with masquerading techniques, indicates a methodical approach to maintaining persistence and avoiding detection in targeted environments.

APT - Group Overview: PROMETHIUM

Description:

PROMETHIUM is an espionage-focused activity group that has been active since at least 2012. The group is known for its global operations, with a significant emphasis on targeting Turkish entities. PROMETHIUM is characterized by its use of sophisticated techniques and overlaps in victim and campaign characteristics with another activity group, NEODYMIUM.

Motivation:

The primary motivation of PROMETHIUM appears to be espionage. Their activities suggest a focus on gathering intelligence and compromising information from targeted entities, particularly in Turkey.

Names:

PROMETHIUM is also associated with the name StrongPity.

Location:

While specific geographic origins are not detailed, PROMETHIUM's targeted campaigns have a global reach, with a notable focus on Turkish targets.

First Seen:

The group's activities date back to at least 2012.

Observed:

PROMETHIUM has been observed conducting global espionage campaigns, with a particular focus on Turkish targets. Their operations are marked by the use of sophisticated techniques and tools.

Techniques Used in all tactics:

- **Boot or Logon Autostart Execution:** PROMETHIUM has used Registry run keys and created new services for persistence.
- **Develop Capabilities:** The group has created self-signed certificates for signing malicious installers and for HTTPS C2 traffic.
- **Drive-by Compromise:** They have employed watering hole attacks to deliver malicious versions of legitimate installers.
- **Masquerading:** PROMETHIUM has named services and disguised installer files to appear legitimate.
- **Subvert Trust Controls:** The group has signed code with self-signed certificates.
- **Traffic Signaling:** They used a script configuring the knockd service and firewall for accepting C2 connections only from systems using a specific sequence of knock ports.
- **User Execution:** PROMETHIUM attempted to get users to execute compromised installation files for legitimate software.
- **Valid Accounts:** The group has created admin accounts on compromised hosts.

Software Used by PROMETHIUM:

- **StrongPity:** A malware used by PROMETHIUM for various purposes including web protocols, data collection, encryption, exfiltration, and masquerading.
- **Truvasys:** Another tool used for autostart execution and masquerading as legitimate services.

PROMETHIUM's operations demonstrate a high level of technical sophistication and strategic planning. Their focus on creating and using self-signed certificates, masquerading techniques, and leveraging legitimate software installers for malicious purposes indicates a methodical approach to infiltrating and maintaining persistence in targeted environments.

APT - Group Overview: Putter Panda

Description:

Putter Panda is a Chinese threat group known for its cyber espionage activities. It has been attributed to Unit 61486 of the 12th Bureau of the PLA's 3rd General Staff Department (GSD), indicating state-sponsored operations.

Motivation:

The primary motivation of Putter Panda is likely espionage, gathering intelligence, and possibly conducting cyber warfare activities, consistent with the objectives of a state-sponsored group.

Names:

Putter Panda is also known as APT2 and MSUpdater.

Location:

The group is believed to be based in China, given its attribution to a unit of the People's Liberation Army.

First Seen:

The specific date of the group's first observed activity is not mentioned, but it has been active for several years, at least since the early 2010s.

Observed:

Putter Panda has been observed conducting cyber espionage campaigns, primarily targeting information related to satellite and aerospace sectors.

Techniques Used in all tactics:

- **Boot or Logon Autostart Execution:** Putter Panda installs itself into the ASEP Registry key for persistence.
- **Impair Defenses:** The group attempts to disable or modify defense tools, specifically targeting components of Sophos Anti-Virus.
- **Obfuscated Files or Information:** Droppers used by Putter Panda obfuscate payloads using RC4 or a 16-byte XOR key.
- **Process Injection:** The group injects DLLs into processes that normally access the network, such as Outlook Express, Outlook, Internet Explorer, and Firefox.

Software Used by Putter Panda:

- **3PARA RAT:** A remote access tool with capabilities like web protocol communication, symmetric encryption, and file discovery.
- **4H RAT:** Another RAT used for command execution, encrypted communication, and system information discovery.
- **httpclient:** A tool for web protocol communication, command execution, and encrypted communication.
- **pngdowner:** Used for web protocol communication, file deletion, and extracting unsecured credentials from files.

Putter Panda's activities demonstrate a focus on stealth and persistence, employing techniques to maintain long-term access to compromised systems and networks. The use of RATs and other

custom malware indicates a high level of sophistication and the ability to adapt tools to specific targets or objectives.

APT - Group Overview: Rancor

Description:

Rancor is a cyber threat group known for its targeted campaigns primarily against the South East Asia region. The group is notable for using politically-motivated lures to entice victims into opening malicious documents.

Motivation:

The primary motivation of Rancor appears to be espionage, likely driven by political interests, as indicated by their use of politically-themed lures.

Names:

The group is primarily known as Rancor.

Location:

While the specific location of Rancor is not detailed, their primary target region is South East Asia.

First Seen:

The exact date of Rancor's first observed activity is not provided, but they have been active at least since the report's creation date in 2018.

Observed:

Rancor has been observed conducting targeted cyber espionage campaigns, using spearphishing and other tactics to compromise victims in the South East Asia region.

Techniques Used in all tactics:

- **Application Layer Protocol (Web Protocols):** Rancor uses HTTP for command and control (C2) communications.
- **Command and Scripting Interpreter (Windows Command Shell and Visual Basic):** The group utilizes cmd.exe and VBS scripts, including embedded macros, for execution.
- **Ingress Tool Transfer:** Rancor downloads additional malware, including using tools like certutil.
- **Phishing (Spearphishing Attachment):** They attach malicious documents to emails for initial access.
- **Scheduled Task/Job:** Rancor establishes persistence by creating scheduled tasks using the

schtasks command.

- **System Binary Proxy Execution (Msiexec):** The group uses msiexec to download and execute malicious installer files over HTTP.
- **User Execution (Malicious File):** Rancor attempts to trick users into clicking on embedded macros within Microsoft Office documents to launch malware.

Software Used by Rancor:

- **certutil:** Used for tasks like data archiving, file deobfuscation, and ingress tool transfer.
- **DDKONG:** A malware that involves file and directory discovery, deobfuscation, and use of rundll32 for execution.
- **PLAINTEE:** This malware abuses elevation control mechanisms, creates registry run keys for persistence, and uses symmetric cryptography for encrypted communication.
- **Reg:** Utilized for modifying and querying the registry, and potentially accessing unsecured credentials stored within the registry.

Rancor's activities demonstrate a focus on targeted espionage using socially engineered lures and a variety of custom tools and techniques to infiltrate and maintain presence within victim networks. The group's use of scheduled tasks for persistence and system binary proxy execution methods indicates a sophisticated understanding of Windows environments and evasion techniques.

APT - Group Overview: Rocke

Description:

Rocke is an alleged Chinese-speaking cyber threat group primarily engaged in cryptojacking, which involves the unauthorized use of victim system resources for mining cryptocurrency. The group's name, "Rocke," originates from the email address "rocke@live.cn," associated with the cryptocurrency wallet they use.

Motivation:

Rocke's primary objective appears to be financial gain through cryptojacking, exploiting system resources of compromised networks to mine cryptocurrency.

Names:

The group is known as Rocke, derived from their associated email address. There are also detected overlaps with the Iron Cybercrime Group, though this attribution is not definitively confirmed.

Location:

The specific location of Rocke is not detailed, but they are described as a Chinese-speaking group.

First Seen:

The exact date of Rocke's inception is not provided, but they have been active at least since the report's creation date in 2020.

Observed:

Rocke has been observed conducting cryptojacking operations, exploiting vulnerabilities in public-facing applications, and using various techniques for persistence, defense evasion, and command and control.

Techniques Used in all tactics:

- **Application Layer Protocol:** Utilizing web protocols for command and control, including HTTP.
- **Boot or Logon Autostart Execution:** Creating UPX-packed files in the Windows Start Menu Folder for persistence.
- **Command and Scripting Interpreter:** Using Unix shell scripts and Python-based malware.
- **Create or Modify System Process:** Installing systemd service scripts for persistence.
- **Exploit Public-Facing Application:** Exploiting vulnerabilities in Apache Struts, Oracle WebLogic, and Adobe ColdFusion.
- **File and Directory Permissions Modification:** Changing file permissions to prevent modifications.
- **Hide Artifacts:** Downloading files to hide artifacts on the target system.
- **Impair Defenses:** Disabling or modifying tools and system firewalls.
- **Ingress Tool Transfer:** Downloading additional malicious files to the target system.
- **Masquerading:** Matching legitimate names or locations to disguise malicious activities.
- **Network Service Discovery:** Scanning for exposed TCP ports and SSH servers.
- **Obfuscated Files or Information:** Modifying UPX headers and using software packing.
- **Process Injection:** Injecting into Windows processes for evasion.
- **Remote Services:** Spreading coinminer via SSH.
- **Resource Hijacking:** Distributing cryptomining malware.
- **Scheduled Task/Job:** Installing cron jobs for persistence.
- **Software Discovery:** Detecting and uninstalling antivirus software.
- **System Information Discovery:** Collecting information about the infected system's kernel.
- **Unsecured Credentials:** Using SSH private keys to spread the coinminer.
- **Web Service:** Using services like Pastebin, Gitee, and GitLab for C2.

Software Used by Rocke:

- **3PARA RAT:** A remote access tool with various capabilities.
- **4H RAT:** Another RAT used by Rocke.
- **httpclient:** Used for encrypted communication and command execution.
- **pngdowner:** A tool for downloading and executing files.
- **Reg:** Utilized for registry modifications.

Rocke's operations demonstrate a focus on financial gain through the exploitation of network resources for cryptocurrency mining. Their use of various evasion techniques, exploitation of public-facing applications, and persistence mechanisms indicate a sophisticated understanding of network environments and security evasion.

APT - Group Overview: RTM

Description:

RTM is a cybercriminal group active since at least 2015, primarily targeting users of remote banking systems in Russia and neighboring countries. The group is known for its use of a Trojan, also named RTM, to conduct its operations.

Motivation:

RTM's primary motivation appears to be financial, focusing on the theft of funds and financial information from users of remote banking systems.

Names:

The group is known as RTM, which is also the name of the Trojan they use for their cybercriminal activities.

Location:

RTM primarily targets Russia and neighboring countries, suggesting a focus on this geographical region.

First Seen:

The group has been active since at least 2015.

Observed:

RTM has been observed using various techniques for initial access, execution, persistence, and command and control. Their operations are characterized by the use of spearphishing, exploit kits, and remote access tools.

Techniques Used in all tactics:

- **Boot or Logon Autostart Execution:** RTM uses Registry run keys for persistence of the RTM Trojan and modified TeamViewer software.
- **Drive-by Compromise:** Distribution of malware via exploit kits like RIG and SUNDOWN, and through online advertising networks.
- **Hijack Execution Flow:** Employing DLL search order hijacking with TeamViewer.
- **Phishing:** Spearphishing attachments are used to distribute malware.
- **Remote Access Software:** Utilizing modified versions of TeamViewer and Remote Utilities.
- **User Execution:** Luring victims to open email attachments to execute malicious code.
- **Web Service:** Using an RSS feed on Livejournal for updating encrypted C2 server names.

Software Used by RTM:

- **RTM Trojan:** A multifunctional Trojan used for various malicious activities, including:
 - Bypassing User Account Control
 - Collecting clipboard data and keylogging
 - Command execution via Windows Command Shell
 - Dynamic resolution and symmetric encryption for secure communication
 - File and directory discovery
 - Indicator removal and registry modifications
 - Masquerading tasks or services
 - Peripheral device discovery
 - Process discovery and screen capture
 - Scheduled task creation for persistence
 - Subverting trust controls
 - System information discovery
 - User execution through malicious files
 - Virtualization and sandbox evasion
 - Dead drop resolver via web services

RTM's activities demonstrate a sophisticated understanding of banking systems and the financial sector, employing a range of techniques to evade detection, maintain persistence, and achieve their financial objectives. Their focus on remote banking systems in Russia and neighboring countries highlights a regional specialization in their operations.

APT - Group Overview: Sandworm Team

Description:

Sandworm Team is a destructive cyber threat group attributed to Russia's General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies (GTsST), military unit 74455. Active since at least 2009, Sandworm Team is known for its high-profile cyber operations against various international targets.

Motivation:

The primary motivation of Sandworm Team appears to be geopolitical, conducting cyber operations that align with Russian state interests. Their activities often target governmental, energy, and infrastructural sectors in various countries.

Names:

Sandworm Team is associated with several aliases, including ELECTRUM, Telebots, IRON VIKING, BlackEnergy Group, Quedagh, Voodoo Bear, and IRIDIUM.

Location:

While the group is attributed to Russia, their operations have a global impact, targeting entities

First Seen:

The group has been active since at least 2009.

Observed:

Sandworm Team has been implicated in numerous high-profile cyber operations, including attacks on Ukrainian electrical companies, the worldwide NotPetya attack, targeting the 2017 French presidential campaign, the 2018 Olympic Destroyer attack, operations against the Organisation for the Prohibition of Chemical Weapons, and attacks in Georgia.

Techniques Used in all tactics:

- **Account Discovery:** Querying Active Directory and email settings for user information.
- **Acquire Infrastructure:** Registering domain names and leasing servers for operations.
- **Active Scanning:** Scanning network infrastructure for vulnerabilities.
- **Application Layer Protocol:** Using HTTP for command and control (C2) communication.
- **Brute Force:** Attempting RPC authentication against multiple hosts.
- **Command and Scripting Interpreter:** Utilizing PowerShell, Windows Command Shell, and Visual Basic for execution.
- **Compromise Client Software Binary:** Using trojanized versions of software for persistence.
- **Create Account:** Creating privileged domain accounts for exploitation and lateral movement.
- **Data Destruction:** Employing destructive components like BlackEnergy KillDisk.
- **Exploitation for Client Execution:** Exploiting vulnerabilities in software like Microsoft PowerPoint and Word.
- **External Remote Services:** Using remote services like SSH for persistence and access.
- **File and Directory Discovery:** Enumerating files and directories on compromised hosts.
- **Impair Defenses:** Disabling event logging and modifying Internet settings.
- **Indicator Removal:** Deleting files and modifying registry settings.
- **Ingress Tool Transfer:** Pushing additional malicious tools onto infected systems.
- **Input Capture:** Employing keyloggers to capture keystrokes.
- **Lateral Tool Transfer:** Transferring tools for lateral movement within networks.
- **Masquerading:** Naming malicious binaries to appear legitimate.
- **Obfuscated Files or Information:** Using encoding and packing techniques for evasion.
- **Phishing:** Delivering malicious attachments and links via spearphishing.
- **Process Injection:** Loading malware into processes like svchost.exe.
- **Remote Access Software:** Using remote administration tools for execution and control.
- **Remote Services:** Utilizing SMB/Windows Admin Shares for lateral movement.
- **Remote System Discovery:** Discovering systems over LAN and querying Active Directory.
- **System Information Discovery:** Enumerating information about infected systems.
- **User Execution:** Tricking users into executing malicious files and links.
- **Valid Accounts:** Using legitimate credentials for access and lateral movement.
- **Web Service:** Employing web services for bidirectional communication and C2.

Software Used by Sandworm Team:

- **Bad Rabbit:** Ransomware used in various attacks.
- **BlackEnergy:** A toolkit with various capabilities, including data destruction.
- **CHEMISTGAMES:** Malicious mobile applications.
- **Cyclops Blink:** Targeting network devices.
- **Exaramel for Linux and Windows:** Backdoors for respective operating systems.
- **GreyEnergy:** Advanced persistent threat malware.
- **Impacket:** A collection of Python classes for working with network protocols.
- **Industroyer:** Targeting industrial control systems.
- **Invoke-PSImage:** Employing steganography in PowerShell scripts.
- **KillDisk:** Used for data destruction.
- **Mimikatz:** Credential harvesting tool.
- **NotPetya:** Destructive malware disguised as ransomware.
- **Olympic Destroyer:** Targeting the 2018 Winter Olympics.
- **Prestige:** Ransomware impacting organizations in Ukraine and Poland.
- **PsExec:** Tool for remote execution.
- **P.A.S. Webshell:** Webshell for maintaining access to networks.
- **Rundll32:** Used for executing DLLs.
- **Windows Management Instrumentation (WMI):** Used for remote code execution and system surveys.

Sandworm Team's operations demonstrate a sophisticated and broad range of capabilities, from destructive attacks to espionage, impacting critical infrastructure and geopolitical landscapes. Their activities are characterized by a combination of technical sophistication and strategic targeting, aligning with Russian state interests.

APT - Group Overview: Scarlet Mimic

Description:

Scarlet Mimic is a cyber threat group known for targeting minority rights activists. The group's activities have not been conclusively linked to a government source, but their motivations appear to overlap with those of the Chinese government. The group employs sophisticated cyber espionage tactics and has been active in its campaigns for several years.

Motivation:

While direct government affiliation is not established, Scarlet Mimic's operations align closely with the interests of the Chinese government, particularly in monitoring and potentially disrupting minority rights movements.

Names:

The group is primarily known as Scarlet Mimic. There is some overlap in IP addresses used by this group and Putter Panda, another known threat group, but it is unclear if they are the same entity.

Location:

The specific location of Scarlet Mimic is not disclosed, but their activities suggest an alignment with Chinese government interests.

First Seen:

Scarlet Mimic has been active since at least the early 2010s, with documented activities dating back several years.

Observed:

The group has been observed conducting cyber espionage campaigns targeting minority rights activists. Their operations are characterized by the use of sophisticated malware and spearphishing techniques.

Techniques Used in all tactics:

- **Masquerading (T1036.002):** Scarlet Mimic has utilized the right-to-left override character in file names of self-extracting RAR archive spearphishing attachments to disguise malicious files.

Software Used by Scarlet Mimic:

1. CallMe (S0077):

- Techniques: Command and Scripting Interpreter: Unix Shell, Encrypted Channel: Symmetric Cryptography, Exfiltration Over C2 Channel, Ingress Tool Transfer.

2. FakeM (S0076):

- Techniques: Data Obfuscation: Protocol Impersonation, Encrypted Channel: Symmetric Cryptography, Input Capture: Keylogging, Non-Application Layer Protocol.

3. MobileOrder (S0079):

- Techniques: Browser Information Discovery, Data from Local System, Exfiltration Over C2 Channel, File and Directory Discovery, Ingress Tool Transfer, Process Discovery, System Information Discovery.

4. Psylo (S0078):

- Techniques: Application Layer Protocol: Web Protocols, Exfiltration Over C2 Channel, File and Directory Discovery, Indicator Removal: Timestamp, Ingress Tool Transfer.

APT - Group Overview: Scattered Spider

Description:

Scattered Spider is a cybercriminal group that has been active since at least 2022. They primarily target customer relationship management (CRM) and business-process outsourcing (BPO) firms, as well as telecommunications and technology companies. The group is known for leveraging targeted social-engineering techniques and attempting to bypass popular endpoint security tools.

Motivation:

The primary motivation of Scattered Spider appears to be gaining unauthorized access to sensitive information and systems within targeted organizations. Their focus on CRM and BPO firms, as well as telecommunications and technology companies, suggests a motive aligned with economic or industrial espionage.

Names:

Scattered Spider is the primary name of the group. They are also associated with the name Roasted Oktapus.

Location:

The specific location of Scattered Spider is not disclosed in the provided information.

First Seen:

The group has been active since at least June 2022.

Observed:

Scattered Spider has been observed conducting campaigns targeting specific industries with sophisticated social engineering and technical intrusion techniques.

Techniques Used in all tactics:

- **Account Discovery:** Utilizing Azure AD for identifying email and cloud accounts.
- **Account Manipulation:** Creating additional cloud credentials and roles, and registering devices for MFA.
- **Data from Cloud Storage:** Accessing victim OneDrive environments for sensitive information.
- **Exploit Public-Facing Application:** Exploiting vulnerabilities like CVE-2021-35464 in ForgeRock OpenAM.
- **External Remote Services:** Leveraging legitimate remote management tools for persistent access.
- **Gather Victim Identity Information:** Using phishing messages to steal credentials.
- **Impersonation:** Impersonating legitimate IT personnel.
- **Ingress Tool Transfer:** Downloading tools using victim organization systems.
- **Modify Cloud Compute Infrastructure:** Creating Azure VMs.
- **Multi-Factor Authentication Request Generation:** Employing MFA fatigue tactics.
- **Network Service Discovery:** Scanning for open ports on targeted appliances.
- **Obtain Capabilities:** Acquiring tools like LINPeas, aws_console, and RustScan.
- **OS Credential Dumping:** Performing domain replication.
- **Permission Groups Discovery:** Accessing Azure AD for group member information.
- **Phishing:** Spearphishing via voice and service impersonation.
- **Protocol Tunneling:** Using SSH tunneling.
- **Proxy:** Installing reverse proxy tools.
- **Remote Access Software:** Disabling defenses to use RMM tools.

- **Remote Services:** Using compromised Azure credentials for lateral movement.
- **Subvert Trust Controls:** Utilizing self-signed and stolen certificates.
- **Valid Accounts:** Leveraging compromised cloud account credentials.
- **Web Service:** Downloading tools from various online sources.
- **Windows Management Instrumentation:** Using WMI for lateral movement.

Software Used by Scattered Spider:

- **Impacket:** Used for lateral movement and various credential dumping techniques.

APT - Group Overview: SideCopy

Description:

SideCopy is a Pakistani threat group that has been active since at least 2019. The group primarily targets South Asian countries, focusing on Indian and Afghan government personnel. SideCopy is known for its infection chain that mimics the tactics of Sidewinder, a suspected Indian threat group.

Motivation:

The primary motivation of SideCopy appears to be espionage, particularly targeting government entities in South Asia. This aligns with geopolitical interests in the region, suggesting a focus on gathering intelligence and possibly influencing regional affairs.

Names:

The group is primarily known as SideCopy.

Location:

SideCopy is believed to be based in Pakistan.

First Seen:

The group has been active since at least 2019.

Observed:

SideCopy has been observed engaging in sophisticated cyber espionage activities targeting government personnel in South Asia, particularly in India and Afghanistan.

Techniques Used in all tactics:

- **Command and Scripting Interpreter: Visual Basic:** Using malicious macros in Microsoft Office Publisher documents to execute HTA files.
- **Compromise Infrastructure: Domains:** Compromising domains for C2 and staging malware.
- **Hijack Execution Flow: DLL Side-Loading:** Utilizing a malicious loader DLL file to execute processes and side-load payloads.
- **Ingress Tool Transfer:** Delivering trojanized executables via spearphishing emails.
- **Masquerading: Match Legitimate Name or Location:** Using legitimate DLL file names to disguise malicious tools.
- **Native API:** Executing malware by calling API functions.
- **Phishing: Spearphishing Attachment:** Sending spearphishing emails with malicious HTA file attachments.
- **Phishing for Information: Spearphishing Attachment:** Crafting generic lures for spam campaigns to collect emails and credentials.
- **Software Discovery:** Collecting browser information and AV product names from infected hosts.
- **Stage Capabilities: Upload Malware:** Using compromised domains to host malicious payloads.
- **System Binary Proxy Execution: Mshta:** Utilizing mshta.exe to execute malicious HTA files.
- **System Information Discovery:** Identifying the OS version of compromised hosts.
- **System Location Discovery:** Identifying the country location of compromised hosts.
- **System Network Configuration Discovery:** Identifying the IP address of compromised hosts.
- **User Execution: Malicious File:** Luring victims to click on malicious embedded archive files.

Software Used by SideCopy:

- **Action RAT:** A remote access tool with various capabilities including data exfiltration and system information discovery.
- **AuTo Stealer:** A malware capable of stealing data, executing commands, and persisting on infected systems.

APT - Group Overview: Sidewinder

Description:

Sidewinder is a suspected Indian threat actor group that has been active since at least 2012. The group is known for targeting government, military, and business entities across Asia, with a primary focus on Pakistan, China, Nepal, and Afghanistan.

Motivation:

Sidewinder's activities suggest a motivation centered around espionage and intelligence gathering, particularly in regions and countries of strategic interest to India.

Names:

- Sidewinder
- Associated Groups: T-APT-04, Battlesnake

Location:

The group is suspected to be based in India.

First Seen:

Sidewinder has been active since at least 2012.

Observed:

The group has been observed conducting sophisticated cyber espionage campaigns targeting a range of entities in Asia, including government and military organizations.

Techniques Used in all tactics:

- **Application Layer Protocol: Web Protocols:** Using HTTP for C2 communications.
- **Automated Collection:** Collecting system and network configuration information automatically.
- **Automated Exfiltration:** Configuring tools to send collected files to attacker-controlled servers.
- **Boot or Logon Autostart Execution:** Adding executable paths in the Registry for persistence.
- **Command and Scripting Interpreter:** Using PowerShell, VBScript, and JavaScript for malware execution.
- **Data Staged:** Collecting stolen files in a temporary folder for exfiltration.
- **Exploitation for Client Execution:** Exploiting vulnerabilities like CVE-2017-11882 and CVE-2020-0674.
- **File and Directory Discovery:** Collecting information on files and directories.
- **Hijack Execution Flow:** Using DLL side-loading techniques.
- **Ingress Tool Transfer:** Using LNK files to download remote files.
- **Inter-Process Communication:** Using Dynamic Data Exchange for execution.
- **Masquerading:** Naming malicious files to resemble legitimate Windows executables.
- **Obfuscated Files or Information:** Using base64 encoding and ECDH-P256 encryption.
- **Phishing:** Spearphishing with attachments and links.
- **Process Discovery:** Identifying running processes on the victim's machine.
- **Software Discovery:** Enumerating installed software and antivirus products.
- **System Binary Proxy Execution:** Using mshta.exe for execution.
- **System Information Discovery:** Collecting detailed system information.
- **System Network Configuration Discovery:** Gathering network interface information.
- **System Owner/User Discovery:** Identifying the user of a compromised host.
- **System Time Discovery:** Obtaining the current system time.
- **User Execution:** Luring targets to click on malicious links or files.

Software Used by Sidewinder:

- **Koadic:** A remote access tool with capabilities like UAC bypass, data exfiltration, and process injection.

APT - Group Overview: Silence

Description:

Silence is a financially motivated threat actor primarily targeting financial institutions in various countries. The group has been active since June 2016, with their main targets located in Russia, Ukraine, Belarus, Azerbaijan, Poland, and Kazakhstan. They are known for compromising banking systems, including the Russian Central Bank's Automated Workstation Client, ATMs, and card processing systems.

Motivation:

Silence's primary motivation appears to be financial gain through the compromise of banking systems and financial institutions.

Names:

- Silence
- Associated Groups: Whisper Spider

Location:

The specific location of Silence is not clearly identified, but their targets are primarily in Eastern Europe and Central Asia.

First Seen:

The group was first observed in June 2016.

Observed:

Silence has been noted for its sophisticated attacks on financial institutions, compromising various banking systems and conducting operations that lead to financial theft.

Techniques Used in all tactics:

- **Boot or Logon Autostart Execution:** Using Registry Run Keys and Startup folder for persistence.
- **Command and Scripting Interpreter:** Employing PowerShell, Windows Command Shell, Visual Basic, and JavaScript for executing payloads.
- **Indicator Removal:** Deleting artifacts, including scheduled tasks and logs.
- **Ingress Tool Transfer:** Downloading additional modules and malware.
- **Masquerading:** Naming its backdoor "WINWORD.exe".
- **Modify Registry:** Creating, deleting, or modifying Registry keys or values.

- **Native API:** Leveraging Windows API for various tasks.
- **Non-Standard Port:** Using port 444 for data transmission.
- **Obfuscated Files or Information:** Employing environment variable string substitution for obfuscation.
- **Obtain Capabilities:** Acquiring and modifying tools like Empire and PsExec.
- **OS Credential Dumping:** Extracting credentials using tools like Mimikatz.
- **Phishing:** Spearphishing with various types of attachments.
- **Process Injection:** Injecting into processes like fwmain32.exe.
- **Proxy:** Using ProxyBot for traffic redirection.
- **Remote Services:** Utilizing Remote Desktop Protocol for lateral movement.
- **Remote System Discovery:** Scanning networks with tools like Nmap.
- **Scheduled Task/Job:** Using scheduled tasks for operations.
- **Screen Capture:** Capturing victim screen activity.
- **Software Deployment Tools:** Using tools like RAdmin for remote control.
- **Subvert Trust Controls:** Using valid certificates for loader signing.
- **System Binary Proxy Execution:** Weaponizing CHM files in phishing campaigns.
- **System Services:** Using Winexe for remote service installation.
- **User Execution:** Encouraging users to launch malicious attachments.
- **Valid Accounts:** Using compromised credentials for access and privilege escalation.
- **Video Capture:** Recording victim activities.

Software Used by Silence:

- **Empire:** A comprehensive framework used for various attack techniques.
- **SDelete:** A tool used for data destruction and file deletion.
- **Winexe:** A utility for remote service execution.

APT - Group Overview: Silent Librarian

Description:

Silent Librarian is a cyber threat group known for targeting research and proprietary data at universities, government agencies, and private sector companies worldwide. Active since at least 2013, the group is affiliated with the Iran-based Mabna Institute, which conducts cyber intrusions on behalf of the Iranian government, specifically the Islamic Revolutionary Guard Corps (IRGC).

Motivation:

The primary motivation of Silent Librarian appears to be intelligence gathering and accessing sensitive research and data, aligning with the strategic interests of the Iranian government.

Names:

- Silent Librarian
- Associated Groups: TA407, COBALT DICKENS

Location:

While the exact location of Silent Librarian is not specified, their affiliation with the Iran-based Mabna Institute suggests an Iranian origin.

First Seen:

The group has been active since at least 2013.

Observed:

Silent Librarian has been observed conducting extensive cyber espionage campaigns, primarily targeting academic institutions and research organizations globally.

Techniques Used in all tactics:

- **Acquire Infrastructure:** Establishing credential harvesting pages using spoofed domains.
- **Brute Force:** Employing password spraying attacks against private sector targets.
- **Email Collection:** Exfiltrating mailboxes and setting up auto-forwarding rules on compromised accounts.
- **Establish Accounts:** Creating email accounts for phishing operations.
- **Gather Victim Identity Information:** Collecting email addresses and employee names through open Internet searches.
- **Obtain Capabilities:** Using publicly available tools for cloning login pages and obtaining digital certificates.
- **Phishing for Information:** Spearphishing with links to credential harvesting websites.
- **Search Victim-Owned Websites:** Identifying interests and academic areas of targeted individuals for phishing campaigns.
- **Stage Capabilities:** Cloning victim organization login pages for credential harvesting.
- **Valid Accounts:** Utilizing compromised credentials for unauthorized access.

Software Used by Silent Librarian:

- **SingleFile and HTTrack:** Tools used to copy login pages of targeted organizations.
- **Let's Encrypt SSL certificates:** Used for phishing pages.

APT - Group Overview: SilverTerrier

Description:

SilverTerrier is a Nigerian threat group, active since 2014, known for its cybercriminal activities. The group primarily targets organizations in high technology, higher education, and manufacturing sectors.

Motivation:

SilverTerrier's primary motivation appears to be financial gain, primarily through business email compromise (BEC) campaigns.

Names:

- SilverTerrier

Location:

Based in Nigeria.

First Seen:

The group has been active since at least 2014.

Observed:

SilverTerrier has been observed engaging in sophisticated cybercriminal activities, targeting various organizations for financial theft.

Techniques Used in all tactics:

- **Application Layer Protocol:** Utilizing HTTP, FTP, and SMTP for Command and Control (C2) communications.
- **Financial Theft:** Engaging in BEC campaigns targeting high technology, higher education, and manufacturing sectors for financial gain.

Software Used by SilverTerrier:

1. **Agent Tesla:** A sophisticated malware used for account discovery, data exfiltration, and credential theft.
2. **DarkComet:** A remote access trojan used for data collection, command execution, and system monitoring.
3. **Lokibot:** A malware known for its capabilities in bypassing user account control, data exfiltration, and credential theft.
4. **NanoCore:** A remote access tool used for audio capture, system monitoring, and data exfiltration.
5. **NETWIRE:** A multi-platform remote access trojan used for data collection, system monitoring, and credential theft.

APT - Group Overview: Sowbug

Description:

Sowbug is a criminal group that has been conducting cyber espionage against organizations in South America and Southeast Asia, with a particular focus on government entities. The group has been active since at least 2015.

Motivation:

Sowbug's motivations appear to be centered around cyber espionage, with a focus on collecting sensitive information from government organizations.

Names:

- Sowbug

Location:

Sowbug primarily targets organizations in South America and Southeast Asia.

First Seen:

Sowbug's activities have been observed since at least 2015.

Observed:

Sowbug has been observed conducting cyber espionage operations, extracting sensitive documents, and engaging in various tactics to achieve its objectives.

Techniques Used in all tactics:

- **Archive Collected Data:** Sowbug extracts and archives collected documents using RAR archives.
- **Command and Scripting Interpreter:** The group uses the Windows Command Shell during its intrusions.
- **Data from Network Shared Drive:** Sowbug extracts Word documents from network shared drives.
- **File and Directory Discovery:** Identifying and extracting Word documents, searching for documents based on date ranges, and identifying installed software on victims' systems.
- **Input Capture: Keylogging:** Sowbug utilizes keylogging tools.
- **Masquerading: Match Legitimate Name or Location:** The group disguises its tools to appear as legitimate Windows or Adobe Reader software.
- **Network Share Discovery:** Sowbug lists remote shared drives accessible from victim systems.
- **OS Credential Dumping:** The group employs credential dumping tools to acquire login credentials.
- **System Information Discovery:** Gathering information about the victim's OS version and hardware configuration.

Software Used by Sowbug:

1. **Felismus:** A tool used for various purposes, including web protocol communication, command execution, data encoding, encrypted channel usage, tool transfer, masquerading, software discovery, and system information gathering.
2. **Starloader:** Utilized for deobfuscating/decoding files or information and masquerading as legitimate software.

APT - Group Overview: Stealth Falcon

Description:

Stealth Falcon is a threat group known for conducting targeted spyware attacks against Emirati journalists, activists, and dissidents since at least 2012. While there is circumstantial evidence suggesting a link between the group and the United Arab Emirates (UAE) government, this connection has not been officially confirmed.

Motivation:

Stealth Falcon's primary motivation is to conduct cyber espionage activities against individuals and entities it targets, including Emirati journalists, activists, and dissidents.

Names:

- Stealth Falcon

Location:

Stealth Falcon's operations are primarily targeted against individuals and organizations within the United Arab Emirates (UAE).

First Seen:

Stealth Falcon's activities have been observed since at least 2012.

Observed:

Stealth Falcon has been observed employing various techniques and tactics to conduct cyber espionage, gather sensitive information, and maintain persistence within victim systems.

Techniques Used in all tactics:

- **Application Layer Protocol: Web Protocols:** Stealth Falcon's malware communicates with its command and control (C2) server via HTTPS.
- **Command and Scripting Interpreter:** The group uses Windows Management Instrumentation (WMI) to script data collection and command execution on victim systems.
 - **PowerShell:** Stealth Falcon's malware leverages PowerShell commands for tasks such

as gathering system information via WMI and executing commands from its C2 server.

- **Credentials from Password Stores:** The group gathers passwords from various sources, including Windows Credential Vault, Outlook, Internet Explorer, Firefox, and Chrome.
- **Data from Local System:** Stealth Falcon's malware collects data from the local victim system.
- **Encrypted Channel: Symmetric Cryptography:** C2 traffic is encrypted using RC4 with a hard-coded key.
- **Exfiltration Over C2 Channel:** Data collected by Stealth Falcon's malware is exfiltrated over the existing C2 channel.
- **Process Discovery:** The group gathers a list of running processes on victim systems.
- **Query Registry:** Stealth Falcon's malware attempts to determine the installed version of .NET by querying the Registry.
- **Scheduled Task/Job: Scheduled Task:** The group creates a scheduled task named "IE Web Cache" to execute a malicious file hourly.
- **System Information Discovery:** Stealth Falcon's malware collects system information via WMI, including system directory, build number, serial number, version, manufacturer, model, and total physical memory.
- **System Network Configuration Discovery:** The group gathers the Address Resolution Protocol (ARP) table from victim systems.
- **System Owner/User Discovery:** Stealth Falcon's malware collects information about the registered user and primary owner name via WMI.
- **Windows Management Instrumentation:** The group leverages Windows Management Instrumentation (WMI) to gather system information.

Software Used by Stealth Falcon:

- Stealth Falcon's malware is involved in various aspects of their operations, including data communication via web protocols, data collection and execution via scripting, password theft from various sources, data collection from the local system, and encryption for C2 communication.

APT - Group Overview: Strider (Associated with ProjectSauron)

Description:

Strider is a threat group that has been active since at least 2011 and has targeted victims in Russia, China, Sweden, Belgium, Iran, and Rwanda. It is associated with ProjectSauron, which refers both to the threat group (G0041) and the malware platform (S0125) used by Strider.

Motivation:

The primary motivation of Strider is cyber espionage, and it targets victims in multiple countries, particularly those of strategic interest.

Names:

- Strider

- **Associated Group:** ProjectSauron

Location:

Strider's activities have been observed in various countries, including Russia, China, Sweden, Belgium, Iran, and Rwanda.

First Seen:

Strider's activities have been observed since at least 2011.

Observed:

Strider has been involved in various cyber espionage activities, targeting victims in different geographic regions and employing sophisticated techniques and tools.

Techniques Used in all tactics:

- **Hide Artifacts: Hidden File System:** Strider has used a hidden file system that is stored as a file on disk.
- **Modify Authentication Process: Password Filter DLL:** Strider has registered its persistence module on domain controllers as a Windows LSA (Local System Authority) password filter to acquire credentials anytime a domain, local user, or administrator logs in or changes a password.
- **Proxy: Internal Proxy:** The group has used local servers with both local network and Internet access to act as internal proxy nodes to exfiltrate data from other parts of the network without direct Internet access.

Software Used by Strider (Associated with ProjectSauron):

- **Remsec (S0125):** Strider employs the Remsec malware platform for various cyber espionage activities. This malware is involved in account discovery, application layer protocol communication (including mail and web protocols), DNS communication, data exfiltration via alternative protocols, exploitation for privilege escalation, keylogging, masquerading as legitimate software, modifying the authentication process, and more.

APT - Group Overview: Suckfly

Description:

Suckfly is a China-based threat group that has been active since at least 2014. This group is known for its cyber espionage activities and has been observed conducting targeted attacks.

Motivation:

gather intelligence and steal sensitive information.

Names:

- Suckfly

Location:

Suckfly is believed to operate from China.

First Seen:

Suckfly's activities have been observed since at least 2014.

Observed:

Suckfly has been involved in various cyber espionage campaigns, targeting organizations and individuals to gather valuable information.

Techniques Used in all tactics:

- **Command and Scripting Interpreter: Windows Command Shell:** Several tools used by Suckfly have been command-line driven, indicating their usage of Windows Command Shell for execution.
- **Network Service Discovery:** Suckfly actively scans the victim's internal network for hosts with specific ports open, including ports 8080, 5900, and 40.
- **OS Credential Dumping:** Suckfly used a signed credential-dumping tool to obtain victim account credentials, potentially for further exploitation.
- **Subvert Trust Controls: Code Signing:** Suckfly has used stolen certificates to sign its malware, enabling the malicious software to appear more legitimate.
- **Valid Accounts:** Suckfly used legitimate account credentials that they dumped to navigate the internal victim network as though they were the legitimate account owner.

Software Used by Suckfly:

- **Nidiran (S0118):** Suckfly has employed the Nidiran malware platform. This software is associated with various techniques, including creating or modifying system processes (Windows Service), ingress tool transfer, and masquerading as legitimate tasks or services.

APT - Group Overview: TA2541

Description:

TA2541 is a cybercriminal group that has been targeting the aviation, aerospace, transportation, manufacturing, and defense industries since at least 2017. Known for their high volume

campaigns, TA2541 employs various techniques and tools in their cybercriminal activities.

Motivation:

TA2541's primary motivation is financial gain through cybercriminal activities. They target industries where valuable intellectual property and sensitive information can be monetized.

Names:

- TA2541

Location:

The exact location of TA2541 is not disclosed, but their cybercriminal activities are known to target organizations globally.

First Seen:

TA2541's activities have been observed since at least 2017.

Observed:

TA2541 is known for conducting cybercriminal campaigns, particularly in the aviation, aerospace, transportation, manufacturing, and defense sectors. Their campaigns often involve the use of commodity remote access tools and various evasion techniques.

Techniques Used in all tactics:

- **Acquire Infrastructure: Domains:** TA2541 registers domains, often containing keywords like "kimjoy," "h0pe," and "grace," using various domain registrars and hosting providers to establish their infrastructure.
- **Acquire Infrastructure: Web Services:** TA2541 hosts malicious files on various online platforms, including Google Drive, OneDrive, Discord, PasteText, ShareText, and GitHub.
- **Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder:** TA2541 establishes persistence by placing VBS files in the Startup folder and using Registry run keys.
- **Command and Scripting Interpreter: PowerShell:** TA2541 leverages PowerShell to download files and inject into various Windows processes.
- **Command and Scripting Interpreter: Visual Basic:** TA2541 uses VBS files for executing or establishing persistence for additional payloads, often mimicking system functionality.
- **Dynamic Resolution:** TA2541 employs dynamic DNS services for their command and control (C2) infrastructure.
- **Encrypted Channel: Asymmetric Cryptography:** TA2541 uses TLS encrypted C2 communications, including in campaigns using AsyncRAT.
- **Impair Defenses: Disable or Modify Tools:** TA2541 attempts to disable built-in security protections, such as Windows AMSI.
- **Ingress Tool Transfer:** TA2541 utilizes malicious scripts and macros with the ability to download additional payloads.

- **Masquerading: Match Legitimate Name or Location:** TA2541 uses file names to mimic legitimate Windows files or system functionality.
- **Obfuscated Files or Information:** TA2541 employs obfuscation techniques, including compressed and char-encoded scripts.
- **Software Packing:** TA2541 uses a .NET packer to obfuscate malicious files.
- **Obtain Capabilities: Malware:** TA2541 uses multiple strains of malware available for purchase on criminal forums or in open-source repositories.
- **Obtain Capabilities: Tool:** TA2541 employs commodity remote access tools.
- **Phishing: Spearphishing Attachment:** TA2541 sends phishing emails with malicious attachments for initial access.
- **Phishing: Spearphishing Link:** TA2541 uses spearphishing emails with malicious links to deliver malware.
- **Process Injection:** TA2541 injects malicious code into legitimate .NET related processes.
- **Process Injection: Process Hollowing:** TA2541 uses process hollowing to execute CyberGate malware.
- **Scheduled Task/Job: Scheduled Task:** TA2541 uses scheduled tasks to establish persistence for installed tools.
- **Software Discovery: Security Software Discovery:** TA2541 employs tools to search victim systems for security products.
- **Stage Capabilities: Upload Malware:** TA2541 uploads malware to various platforms.
- **System Binary Proxy Execution: Mshta:** TA2541 uses mshta to execute scripts, including VBS.
- **System Information Discovery:** TA2541 collects system information before downloading malware on the targeted host.
- **System Network Configuration Discovery: Internet Connection Discovery:** TA2541 runs scripts to check internet connectivity from compromised hosts.
- **User Execution: Malicious Link:** TA2541 uses malicious links to cloud and web services to gain execution on victim machines.
- **User Execution: Malicious File:** TA2541 uses macro-enabled MS Word documents to lure victims into executing malicious payloads.
- **Windows Management Instrumentation:** TA2541 uses WMI to query targeted systems for security products.

Software Used by TA2541:

- **Agent Tesla (S0331):** Employed by TA2541 for various purposes, including account discovery, application layer protocol usage, archive collection, and more.
- **AsyncRAT (S1087):** Used by TA2541 for evasion, dynamic resolution, keylogging, and other activities.
- **Imminent Monitor (S0434):** Utilized for audio capture, command execution, and other malicious actions.
- **jRAT (S0283):** Employed by TA2541 for multiple purposes, including keylogging, remote desktop protocol usage, and screen capture.
- **NETWIRE (S0198):** Used for various activities, including web protocol usage, boot or logon autostart execution, and system information discovery.
- **njRAT (S0385):** Utilized for web protocol activities, boot or logon autostart execution, and process discovery.
- **Revenge RAT (S0379):** Employed for activities such as audio capture, system information discovery, and remote desktop protocol usage.
- **Snip3 (S1086):** Used for autostart execution, obfuscation, and spearphishing activities.
- **WarzoneRAT (S0670):** Employed for multiple purposes, including evasion, command execution, and video capture.

APT - Group Overview: TA459

Description:

TA459 is a threat group believed to operate out of China, and it has been associated with cyber-espionage activities targeting countries such as Russia, Belarus, Mongolia, and others. Their operations have involved various techniques and tools to achieve their objectives.

Motivation:

TA459's primary motivation appears to be conducting cyber-espionage activities for political, economic, or strategic gains. They focus on infiltrating and gathering sensitive information from their targeted regions.

Names:

- TA459

Location:

TA459 is believed to operate from China, although their activities extend beyond their home country to various international targets.

First Seen:

The activities of TA459 have been observed since at least April 18, 2018.

Observed:

TA459 is known for conducting cyber-espionage operations, primarily through spearphishing campaigns and exploiting vulnerabilities in Microsoft Word. They have also employed various techniques and tools to gain access to and gather information from their targets.

Techniques Used in all tactics:

- **Command and Scripting Interpreter: PowerShell:** TA459 has used PowerShell for executing payloads.
- **Command and Scripting Interpreter: Visual Basic:** TA459 utilizes VBScript for execution.
- **Exploitation for Client Execution:** TA459 has exploited Microsoft Word vulnerability CVE-2017-0199 for execution.
- **Phishing: Spearphishing Attachment:** TA459 has targeted victims using spearphishing emails with malicious Microsoft Word attachments.
- **User Execution: Malicious File:** TA459 attempts to persuade victims to open malicious Microsoft Word attachments sent via spearphishing.

Software Used by TA459:

- **gh0st RAT (S0032):** TA459 has used a Gh0st variant known as PCrat/Gh0st for various purposes, including keylogging, boot or logon autostart execution, and process discovery.
- **NetTraveler (S0033):** Employed for activities such as application window discovery and keylogging.
- **PlugX (S0013):** Used for a wide range of purposes, including web protocol usage, DNS activity, boot or logon autostart execution, and process discovery.
- **ZeroT (S0230):** Employed for activities like bypassing User Account Control, web protocol usage, and system network configuration discovery.

TA505 - Group Overview

Description: TA505 is a cyber criminal group that has been active since at least 2014. TA505 is known for frequently changing malware, driving global trends in criminal malware distribution, and ransomware campaigns involving Clop.

Motivation: TA505 primarily engages in cybercriminal activities for financial gain. They have been associated with a wide range of cyberattacks, including phishing campaigns, ransomware attacks, and the distribution of various malware families.

Names: TA505, also associated with Hive0065.

Location: The exact location of TA505's operations is unclear, but they are known to operate on a global scale, targeting victims worldwide.

First Seen: TA505 was first observed in cyber threat landscapes in 2014.

Observed: TA505 has been actively observed and analyzed by cybersecurity researchers and organizations, with various campaigns and attacks attributed to the group.

Techniques Used in all Tactics

- **Account Discovery: Email Account (T1087.003):** TA505 has used the tool EmailStealer to steal and send lists of email addresses to a remote server.
- **Acquire Infrastructure: Domains (T1583.001):** TA505 has registered domains to impersonate services such as Dropbox to distribute malware.
- **Application Layer Protocol: Web Protocols (T1071.001):** TA505 has used HTTP to communicate with command and control (C2) nodes.
- **Command and Scripting Interpreter: PowerShell (T1059.001):** TA505 has used PowerShell to download and execute malware and reconnaissance scripts.
- **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** TA505 has executed commands using cmd.exe.
- **Command and Scripting Interpreter: Visual Basic (T1059.005):** TA505 has used Visual Basic Scripting (VBS) for code execution.
- **Command and Scripting Interpreter: JavaScript (T1059.007):** TA505 has used JavaScript for code execution.
- **Credentials from Password Stores: Credentials from Web Browsers (T1555.003):** TA505 has used malware to gather credentials from Internet Explorer.
- **Data Encrypted for Impact (T1486):** TA505 has used a wide variety of ransomware, such as Clop, Locky, Jaff, Bart, Philadelphia, and GlobeImposter, to encrypt victim files and demand a ransom payment.
- **Deobfuscate/Decode Files or Information (T1140):** TA505 has decrypted packed DLLs.

with an XOR key.

- **Dynamic Resolution: Fast Flux DNS (T1568.001):** TA505 has used fast flux to mask botnets by distributing payloads across multiple IPs.
- **Impair Defenses: Disable or Modify Tools (T1562.001):** TA505 has used malware to disable Windows Defender.
- **Ingress Tool Transfer (T1105):** TA505 has downloaded additional malware to execute on victim systems.
- **Inter-Process Communication: Dynamic Data Exchange (T1559.002):** TA505 has leveraged malicious Word documents that abused DDE.
- **Modify Registry (T1112):** TA505 has used malware to disable Windows Defender through modification of the Registry.
- **Native API (T1106):** TA505 has deployed payloads that use Windows API calls on a compromised host.
- **Obfuscated Files or Information: Password-protected malicious Word documents (T1055.001):** TA505 has password-protected malicious Word documents.
- **Obfuscated Files or Information: Software Packing (T1055.002):** TA505 has used UPX to obscure malicious code.
- **Obfuscated Files or Information: Command Obfuscation (T1055.010):** TA505 has used base64 encoded PowerShell commands.
- **Obtain Capabilities: Malware (T1588.001):** TA505 has used malware such as Azorult and Cobalt Strike in their operations.
- **Obtain Capabilities: Tool (T1588.002):** TA505 has used a variety of tools in their operations, including AdFind, BloodHound, Mimikatz, and PowerSploit.
- **Permission Groups Discovery (T1069):** TA505 has used TinyMet to enumerate members of privileged groups. TA505 has also run `net group /domain`.
- **Phishing: Spearphishing Attachment (T1566.001):** TA505 has used spearphishing emails with malicious attachments to initially compromise victims.
- **Phishing: Spearphishing Link (T1566.002):** TA505 has sent spearphishing emails containing malicious links.
- **Process Injection: Dynamic-link Library Injection (T1055.001):** TA505 has been seen injecting a DLL into winword.exe.
- **Stage Capabilities: Upload Malware (T1608.001):** TA505 has staged malware on actor-controlled domains.
- **Subvert Trust Controls: Code Signing (T1552.001):** TA505 has signed payloads with code signing certificates from Thawte and Sectigo.
- **Subvert Trust Controls: Mark-of-the-Web Bypass (T1552.005):** TA505 has used .iso files to deploy malicious .lnk files.
- **System Binary Proxy Execution: Msiexec (T1218.007):** TA505 has used msiexec to download and execute malicious Windows Installer files.
- **System Binary Proxy Execution: Rundll32 (T1218.011):** TA505 has leveraged rundll32.exe to execute malicious DLLs.
- **Unsecured Credentials: Credentials in Files (T1552.001):** TA505 has used malware to gather credentials from FTP clients and Outlook.
- **User Execution: Malicious Link (T1204.001):** TA505 has used lures to get users to click links in emails and attachments.
- **User Execution: Malicious File (T1204.002):** TA505 has used lures to get users to enable content in malicious attachments and execute malicious files contained in archives.
- **Valid Accounts: Domain Accounts (T1078.002):** TA505 has used stolen domain admin accounts to compromise additional hosts.

Software Used by TA505

- **AdFind (S0552)**: Used for account discovery, domain trust discovery, permission groups discovery, remote system discovery, and system network configuration discovery.
- **Amadey (S1025)**: Used for various purposes, including application layer protocol, autostart execution, data collection, deobfuscation, exfiltration over C2 channel, and more.
- **Azorult (S0344)**: Utilized for access token manipulation, credentials from password stores, deobfuscation, encrypted channel, file and directory discovery, indicator removal, ingress tool transfer, process discovery, and more.
- **BloodHound (S0521)**: Employed for account discovery, group policy discovery, native API, password policy discovery, and various other reconnaissance activities.
- **Clop (S0611)**: Used for command and scripting execution, data encryption, deobfuscation, impairing defenses, modifying registry, native API, obfuscating files, system binary proxy execution, and more.
- **Cobalt Strike (S0154)**: Utilized for various purposes, including privilege escalation, access token manipulation, command and scripting execution, data exfiltration, and more.
- **Dridex (S0384)**: Used for application layer protocol, browser session hijacking, encrypted channel, hijacking execution flow, native API, obfuscation, proxy, remote access, scheduled tasks, and more.
- **FlawedAmmyy (S0381)**: Employed for application layer protocol, autostart execution, clipboard data, command and scripting execution, and more.
- **FlawedGrace (S0383)**: Used for obfuscation.
- **Get2 (S0460)**: Utilized for application layer protocol, command and scripting execution, process discovery, process injection, and more.
- **Mimikatz (S0002)**: Employed for various credential manipulation activities, including access token manipulation, account manipulation, OS credential dumping, rogue domain controller, and more.
- **Net (S0039)**: Used for account discovery, create account, indicator removal, network share discovery, and various network-related activities.
- **PowerSploit (S0194)**: Utilized for access token manipulation, account discovery, boot or logon autostart execution, and various scripting activities.
- **SDBbot (S0461)**: Employed for autostart execution, command and scripting execution, deobfuscation, event-triggered execution, file and directory discovery, and more.
- **ServHelper (S0382)**: Used for account manipulation, application layer protocol, autostart execution, command and scripting execution, and more.
- **TrickBot (S0266)**: Utilized for a wide range of activities, including account discovery, application layer protocol, boot or logon autostart execution, brute force, credential theft, data exfiltration, and more.

Matrices Group Overview

Description: Matrices is a financially-motivated threat group that has been active since at least 2018. The group primarily targets English, German, Italian, and Japanese speakers through email-based malware distribution campaigns.

Motivation: Matrices is primarily motivated by financial gain and conducts cyberattacks to achieve their monetary objectives.

Names: Matrices is also associated with the aliases "GOLD CABIN" and "Shathak."

Location: The exact location of Matrices' operations is not specified, but they target victims globally, with a focus on specific language groups.

First Seen: Matrices has been observed in the threat landscape since at least 2018.

Observed: Matrices' activities have been observed and analyzed by cybersecurity researchers and organizations. They are known for their use of various techniques and software in their

Techniques Used in all Tactics

- **Application Layer Protocol: Web Protocols (T1071.001):** Matrices has used HTTP for command and control (C2) communications.
- **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** Matrices has employed cmd.exe to execute commands.
- **Data Encoding: Standard Encoding (T1132.001):** Matrices has used encoded ASCII text for initial C2 communications.
- **Dynamic Resolution: Domain Generation Algorithms (T1568.002):** Matrices has used a Domain Generation Algorithm (DGA) to generate URLs from executed macros.
- **Gather Victim Identity Information: Email Addresses (T1589.002):** Matrices has used spoofed company emails acquired from email clients on previously infected hosts to target other individuals.
- **Ingress Tool Transfer (T1105):** Matrices has retrieved DLLs and installer binaries for malware execution from C2.
- **Masquerading (T1036):** Matrices has masked malware DLLs as dat and jpg files.
- **Obfuscated Files or Information: Steganography (T1027.003):** Matrices has hidden encoded data for malware DLLs in a PNG.
- **Obfuscated Files or Information: Command Obfuscation (T1055.010):** Matrices has used obfuscated variable names in a JavaScript configuration file.
- **Phishing: Spearphishing Attachment (T1566.001):** Matrices has sent spearphishing attachments with password-protected ZIP files.
- **System Binary Proxy Execution: Mshta (T1218.005):** Matrices has used mshta.exe to execute malicious payloads.
- **System Binary Proxy Execution: Regsvr32 (T1218.010):** Matrices has used regsvr32.exe to load malicious DLLs.
- **System Binary Proxy Execution: Rundll32 (T1218.011):** Matrices has used rundll32.exe to load malicious DLLs.
- **User Execution: Malicious File (T1204.002):** Matrices has prompted users to enable macros within spearphishing attachments to install malware.

Software Used by Matrices

- **IcedID (S0483):** Matrices has utilized IcedID for various purposes, including account discovery, application layer protocol, boot or logon autostart execution, browser session hijacking, command and scripting execution, encrypted channel, ingress tool transfer, native API, obfuscated files, permissions groups discovery, phishing, process injection, scheduled tasks, system binary proxy execution, system information discovery, user execution, and Windows Management Instrumentation (WMI).
- **QakBot (S0650):** Matrices has employed QakBot for multiple activities, including application layer protocol, application window discovery, boot or logon autostart execution, browser session hijacking, brute force, command and scripting execution, credentials theft, data encoding, data from local system, data staging, deobfuscation, domain trust discovery, dynamic resolution, email collection, exfiltration over C2 channel, exploitation of remote services, file and directory discovery, hiding artifacts, hijack execution flow, impairing defenses, indicator removal, ingress tool transfer, input capture, masquerading, modifying the registry, network share discovery, non-application layer protocol, obfuscated files, peripheral device discovery, phishing, process discovery, protocol tunneling, proxy, remote system discovery, replication through removable media, screen capture, system service discovery, taint shared content, virtualization/sandbox evasion, and more.

- **Ursnif (S0386):** Matrices has utilized Ursnif for various purposes, including application layer protocol, boot or logon autostart execution, browser session hijacking, command and scripting execution, creating or modifying system processes, data encoding, data from local system, data staging, deobfuscation, dynamic resolution, exfiltration over C2 channel, hiding artifacts, indicator removal, ingress tool transfer, input capture, inter-process communication, masquerading, modifying the registry, native API, obfuscated files, process discovery, process injection, proxy, query registry, replication through removable media, screen capture, system information discovery, system service discovery, taint shared content, virtualization/sandbox evasion, and Windows Management Instrumentation (WMI).
- **Valak (S0476):** Matrices has employed Valak for various purposes, including account discovery, application layer protocol, automated collection, command and scripting execution, credentials theft, data encoding, deobfuscation, email collection, exfiltration over C2 channel, fallback channels, hiding artifacts, ingress tool transfer, inter-process communication, masquerading, modifying the registry, obfuscated files, phishing, process discovery, query registry, scheduled tasks, screen capture, software discovery, system binary proxy execution, system information discovery, system network configuration discovery, system owner/user discovery, unsecured credentials, user execution, and Windows Management Instrumentation (WMI).

TeamTNT - Group Overview

Description: TeamTNT is a threat group that has been active since at least October 2019, primarily targeting cloud and containerized environments. Their main objective is to leverage cloud and container resources to deploy cryptocurrency miners in victim environments.

Motivation: The group's motivation appears to be financial gain through cryptocurrency mining activities.

Names: TeamTNT

Location: Global

First Seen: October 2019

Observed: Ongoing

Techniques Used in All Tactics

- **Account Manipulation: SSH Authorized Keys (T1098.004):** TeamTNT has added RSA keys in `authorized_keys`, potentially granting unauthorized access to victim systems.
- **Acquire Infrastructure: Domains (T1583.001):** The group has obtained domains to host their malicious payloads.
- **Active Scanning: Scanning IP Blocks (T1595.001):** TeamTNT has actively scanned specific lists of target IP addresses.
- **Active Scanning: Vulnerability Scanning (T1595.002):** Vulnerability scanning has been conducted on IoT devices and resources such as the Docker API.
- **Application Layer Protocol (T1071):** TeamTNT has utilized IRC bots for Command and Control (C2) communications.
- **Web Protocols (T1071.001):** They have used HTTP-based commands (`curl`) to send credentials and download software, along with custom user agent HTTP headers in shell scripts.
- **Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001):** Batch scripts have been added to the startup folder for automatic execution.
- **Command and Scripting Interpreter: PowerShell (T1059.001):** PowerShell commands

have been executed in batch scripts.

- **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** Batch scripts have been used to download tools and execute cryptocurrency miners.
- **Command and Scripting Interpreter: Unix Shell (T1059.004):** Shell scripts have been used for execution.
- **Command and Scripting Interpreter: Cloud API (T1059.009):** TeamTNT has leveraged the AWS CLI to enumerate cloud environments with compromised credentials.
- **Container Administration Command (T1609):** Execution of commands on running containers, including the use of kubelet API run commands.
- **Container and Resource Discovery (T1613):** Checking for running containers, inspecting container names, and searching for Kubernetes pods within local networks.
- **Create Account: Local Account (T1136.001):** Creation of local privileged users on victim machines.
- **Create or Modify System Process: Systemd Service (T1543.002):** Establishment of persistence through the creation of a cryptocurrency mining system service.
- **Create or Modify System Process: Windows Service (T1543.003):** Usage of malware to add cryptocurrency miners as services.
- **Data Staged: Local Data Staging (T1074.001):** Aggregation of collected credentials in text files before exfiltration.
- **Deobfuscate/Decode Files or Information (T1140):** Usage of scripts to decode Base64-encoded information.
- **Deploy Container (T1610):** Deployment of various container types into victim environments to facilitate execution, including transferring cryptocurrency mining software to Kubernetes clusters.
- **Develop Capabilities: Malware (T1587.001):** Development of custom malware, such as Hildegard.
- **Escape to Host (T1611):** Deployment of privileged containers that mount the victim machine's filesystem.
- **Exfiltration Over Alternative Protocol (T1048.001):** Sending locally staged files with collected credentials to C2 servers using cURL.
- **External Remote Services (T1133):** Utilization of open-source tools like Weave Scope to target exposed Docker API ports for initial access. Also, targeting exposed kubelets in Kubernetes environments.
- **File and Directory Discovery (T1083):** Searching for environment variables related to AWS in `/proc/*/environ`.
- **File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification (T1222.002):** Modifying permissions on binaries with `chattr`.
- **Impair Defenses: Disable or Modify Tools (T1562.001):** Disabling and uninstalling security tools, including Alibaba, Tencent, and BMC cloud monitoring agents on cloud-based infrastructure.
- **Impair Defenses: Disable or Modify System Firewall (T1562.004):** Disabling iptables.
- **Indicator Removal: Clear Linux or Mac System Logs (T1070.002):** Removing system logs from `/var/log/syslog`.
- **Indicator Removal: Clear Command History (T1070.003):** Clearing command history with `history -c`.
- **Indicator Removal: File Deletion (T1070.004):** Using payloads that remove themselves after running and deleting locally staged files.
- **Ingress Tool Transfer (T1105):** Utilizing commands (`curl`, `wget`) and batch scripts to download new tools.
- **Masquerading (T1036):** Disguising scripts with docker-related file names.
- **Match Legitimate Name or Location (T1036.005):** Replacing `.dockerd` and `.dockerenv` with their own scripts and cryptocurrency mining software.
- **Network Service Discovery (T1046):** Using `masscan` to search for open Docker API ports

- **Search for vulnerable services in cloud environments.**
- **Obfuscated Files or Information (T1027):** Encrypting binaries via AES and encoding files using Base64.
- **Software Packing (T1027.002):** Using UPX and Ezuri packer to pack binaries.
- **Peripheral Device Discovery (T1120):** Searching for attached VGA devices using lspci.
- **Process Discovery (T1057):** Searching for rival malware and removing it if found. Also, searching for running processes containing strings like aliyun or liyun to identify machines running Alibaba Cloud Security tools.
- **Remote Access Software (T1219):** Establishing tmate sessions for C2 communications.
- **Remote Services: SSH (T1021.004):** Using SSH to connect back to victim machines. Also, employing SSH for transferring tools and payloads onto victim hosts and executing them.
- **Resource Hijacking (T1496):** Deploying XMRig Docker images to mine cryptocurrency. Also, infecting Docker containers and Kubernetes clusters with XMRig, RainbowMiner, and lolMiner for cryptocurrency mining.
- **Rootkit (T1014):** Utilizing rootkits such as the open-source Diamorphine rootkit and custom bots to hide cryptocurrency mining activities on the machine.
- **Software Discovery: Security Software Discovery (T1518.001):** Searching for security products on infected machines.
- **Stage Capabilities: Upload Malware (T1608.001):** Uploading backdoored Docker images to Docker Hub.
- **System Information Discovery (T1082):** Searching for system version, architecture, disk partition, logical volume, and hostname information.
- **System Network Configuration Discovery (T1016):** Enumerating the host machine's IP address.
- **System Network Connections Discovery (T1049):** Running netstat -anp to search for rival malware connections. Also, using libprocesshider to modify /etc/ld.so.preload.
- **System Service Discovery (T1007):** Searching for services such as Alibaba Cloud Security's aliyun service and BMC Helix Cloud Security's bmc-agent service to disable them.
- **System Services (T1569):** Creating system services to execute cryptocurrency mining software.
- **Unsecured Credentials: Credentials In Files (T1552.001):** Searching for unsecured AWS credentials and Docker API credentials.
- **Unsecured Credentials: Private Keys (T1552.004):** Searching for unsecured SSH keys.
- **Unsecured Credentials: Cloud Instance Metadata API (T1552.005):** Querying the AWS instance metadata service for credentials.
- **User Execution: Malicious Image (T1204.003):** Relying on users to download and execute malicious Docker images.
- **Web Service (T1102):** Leveraging iplogger.org to send collected data back to C2.

Software Used by TeamTNT

- **Hildegard (S0601):** Used for various purposes, including Application Layer Protocol, Command and Scripting Interpreter: Unix Shell, Container Administration Command, Container and Resource Discovery, Create Account: Local Account, Create or Modify System Process: Systemd Service, Deobfuscate/Decode Files or Information, Escape to Host, Exploitation for Privilege Escalation, External Remote Services, Hijack Execution Flow: Dynamic Linker Hijacking, Impair Defenses: Disable or Modify Tools, Indicator Removal: File Deletion, Indicator Removal: Clear Command History, Ingress Tool Transfer, Masquerading: Masquerade Task or Service, Network Service Discovery, Obfuscated Files or Information: Software Packing, Obfuscated Files or Information, Remote Access Software, Resource Hijacking, Rootkit, System Information Discovery, Unsecured Credentials: Private Keys,

Unsecured Credentials: Credentials in Files, Unsecured Credentials: Cloud Instance Metadata API, Web Service

- **LaZagne (S0349):** Used for credential theft from various sources, including Windows Credential Manager, Credentials from Web Browsers, Keychain, LSA Secrets, /etc/passwd and /etc/shadow, LSASS Memory, Cached Domain Credentials, Proc Filesystem, Credentials in Files.
- **MimiPenguin (S0179):** Utilized for OS credential dumping via the Proc Filesystem.
- **Peirates (S0683):** Employed for various cloud-related activities, including Cloud Storage Object Discovery, Container Administration Command, Container and Resource Discovery, Data from Cloud Storage, Deploy Container, Escape to Host, Network Service Discovery, Steal Application Access Token, Unsecured Credentials: Container API, Unsecured Credentials: Cloud Instance Metadata API, Use Alternate Authentication Material: Application Access Token, Valid Accounts: Cloud Accounts.

These tools and techniques provide TeamTNT with the means to infiltrate, maintain persistence, and execute cryptocurrency mining operations in cloud and containerized environments.

TEMP.Veles - Group Overview

Description: TEMP.Veles is a Russia-based threat group known for targeting critical infrastructure. They have been observed utilizing TRITON, a sophisticated malware framework designed to manipulate industrial safety systems.

Motivation: TEMP.Veles' primary motivation appears to be conducting cyber-espionage and potentially disrupting critical infrastructure operations.

Names: TEMP.Veles

Location: Russia

First Seen: April 16, 2019

Observed: Ongoing

Techniques Used in All Tactics

- **Acquire Infrastructure: Virtual Private Server (T1583.003):** TEMP.Veles has utilized Virtual Private Server (VPS) infrastructure for their operations.
- **Command and Scripting Interpreter: PowerShell (T1059.001):** The group has used publicly-available PowerShell-based tools like WMImplant and PowerShell for Timestomping.
- **Data Staged: Local Data Staging (T1074.001):** TEMP.Veles creates staging folders in directories infrequently used by legitimate users or processes.
- **Event Triggered Execution: Image File Execution Options Injection (T1546.012):** Modifications and additions within HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options are made to maintain persistence.
- **External Remote Services (T1133):** TEMP.Veles has employed VPNs to persist in victim environments.
- **Indicator Removal: File Deletion (T1070.004):** Routine deletion of tools, logs, and other files after usage.
- **Indicator Removal: Timestamp (T1070.006):** Timestomping is used to modify the \$STANDARD_INFORMATION attribute on tools.
- **Masquerading: Match Legitimate Name or Location (T1036.005):** Files are renamed to resemble legitimate files, such as Windows update files or Schneider Electric application

- **Non-Standard Port (T1571):** TEMP.Veles has used port-protocol mismatches on ports such as 443, 4444, 8531, and 50501 during Command and Control (C2).
- **Obfuscated Files or Information: Indicator Removal from Tools (T1027.005):** Modification of files based on the open-source project cryptcat to decrease antivirus detection rates.
- **Obtain Capabilities: Tool (T1588.002):** TEMP.Veles obtains and uses tools such as Mimikatz and PsExec.
- **OS Credential Dumping: LSASS Memory (T1003.001):** The group utilizes tools like Mimikatz and a custom tool, SecHack, to harvest credentials.
- **Remote Services: Remote Desktop Protocol (T1021.001):** TEMP.Veles utilizes Remote Desktop Protocol (RDP) throughout their operations.
- **Remote Services: SSH (T1021.004):** Encrypted SSH-based tunnels are relied upon for tool transfer and remote command/program execution.
- **Scheduled Task/Job: Scheduled Task (T1053.005):** TEMP.Veles has used scheduled task XML triggers.
- **Server Software Component: Web Shell (T1505.003):** Web shells have been planted on Outlook Exchange servers.
- **Valid Accounts (T1078):** TEMP.Veles has used compromised VPN accounts.

Software Used by TEMP.Veles

- **Mimikatz (S0002):** Used for various purposes, including Access Token Manipulation, SID-History Injection, Account Manipulation, Boot or Logon Autostart Execution, Credentials theft from Password Stores (Windows Credential Manager, Web Browsers, etc.), OS Credential Dumping (DCSync, Security Account Manager, LSASS Memory, LSA Secrets), Rogue Domain Controller, Steal or Forge Authentication Certificates, Steal or Forge Kerberos Tickets (Golden Ticket, Silver Ticket), Unsecured Credentials (Private Keys), Use Alternate Authentication Material (Pass the Hash, Pass the Ticket).
- **PsExec (S0029):** Utilized for various activities, including creating Domain Accounts, creating or modifying System Processes (Windows Service), lateral tool transfer, Remote Services (SMB/Windows Admin Shares), and System Services (Service Execution).
- **TRITON (S1009):** TRITON is a malware framework associated with TEMP.Veles, designed for various purposes, including changing Operating Mode, using commonly used ports, detecting Operating Mode, executing through APIs, exploiting for evasion and privilege escalation, hooking, indicator removal on the host, causing loss of safety, masquerading, modifying Controller Tasking, native API usage, program download and upload, remote system discovery, scripting, standard application layer protocol, and manipulating system firmware.

These techniques and tools enable TEMP.Veles to conduct cyber-espionage and potentially disrupt critical infrastructure by manipulating industrial safety systems, making them a significant threat to national security.

The White Company - Group Overview

Description: The White Company is a likely state-sponsored threat actor known for its advanced capabilities. From 2017 through 2018, the group conducted an espionage campaign called Operation Shaheen, primarily targeting government and military organizations in Pakistan.

Motivation: The White Company's primary motivation appears to be conducting state-sponsored cyber-espionage.

Names: The White Company

First Seen: May 2, 2019

Observed: Activities are known to have occurred until at least March 30, 2020.

Techniques Used in All Tactics

- **Exploitation for Client Execution (T1203):** The White Company exploited a known vulnerability in Microsoft Word (CVE 2012-0158) to execute code.
- **Indicator Removal: File Deletion (T1070.004):** The group possesses the capability to entirely delete its malware from the target system.
- **Obfuscated Files or Information: Software Packing (T1027.002):** The White Company obfuscates their payloads through packing.
- **Phishing: Spearphishing Attachment (T1566.001):** Phishing emails with malicious Microsoft Word attachments are used to lure victims.
- **Software Discovery: Security Software Discovery (T1518.001):** The White Company checks for specific antivirus products on the target's computer, including Kaspersky, Quick Heal, AVG, BitDefender, Avira, Sophos, Avast!, and ESET.
- **System Time Discovery (T1124):** Checking the current date on the victim system.
- **User Execution: Malicious File (T1204.002):** The White Company employs phishing lure documents that trick users into opening them, resulting in computer infections.

Software Used by The White Company

- **NETWIRE (S0198):** This software is associated with various techniques, including Application Layer Protocol, Application Window Discovery, Archive Collected Data, Automated Collection, Boot or Logon Autostart Execution, Command and Scripting Interpreter (Visual Basic, PowerShell, Unix Shell, Windows Command Shell), Create or Modify System Process, Credentials theft from Password Stores, Data Staging, Encrypted Channel, File and Directory Discovery, Hide Artifacts, Ingress Tool Transfer, Input Capture (Keylogging), Masquerading, Modify Registry, Native API usage, Non-Application Layer Protocol, Obfuscated Files or Information (Software Packing, Fileless Storage), Phishing (Spearphishing Link, Spearphishing Attachment), Process Discovery, Process Injection (Process Hollowing), Proxy, Scheduled Task/Job, Screen Capture, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, User Execution (Malicious File, Malicious Link), and Web Service.
- **Revenge RAT (S0379):** This software is associated with various techniques, including Audio Capture, Boot or Logon Autostart Execution, Command and Scripting Interpreter (Windows Command Shell, PowerShell), Data Encoding, Indirect Command Execution, Ingress Tool Transfer, Input Capture (Keylogging), OS Credential Dumping, Remote Services (Remote Desktop Protocol), Scheduled Task/Job, Screen Capture, System Binary Proxy Execution (Mshta), System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, Video Capture, and Web Service (Bidirectional Communication).

The White Company's use of advanced techniques and software indicates their involvement in state-sponsored cyber-espionage, and their campaigns have primarily targeted government and military organizations in Pakistan.

Threat Group-1314 - Group Overview

Description: Threat Group-1314 is an unattributed threat group known for using compromised

Motivation: The specific motivations and objectives of Threat Group-1314 are not detailed in the provided information.

Names: Threat Group-1314 (also associated with the abbreviation TG-1314)

Location: Unknown

First Seen: May 31, 2017

Observed: Activities are known to have occurred until at least March 19, 2020.

Techniques Used in All Tactics

- **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** Threat Group-1314 actors spawned shells on remote systems within a victim network to execute commands.
- **Remote Services: SMB/Windows Admin Shares (T1021.002):** Threat Group-1314 actors mapped network drives using the "net use" command.
- **Software Deployment Tools (T1072):** Threat Group-1314 actors utilized a victim's endpoint management platform, Altiris, for lateral movement.
- **Valid Accounts: Domain Accounts (T1078.002):** Threat Group-1314 actors used compromised domain credentials for the victim's endpoint management platform, Altiris, to move laterally.

Software Used by Threat Group-1314

- **Net (S0039):** This software is associated with various techniques, including Account Discovery (Domain Account, Local Account), Create Account (Local Account, Domain Account), Indicator Removal (Network Share Connection Removal), Network Share Discovery, Password Policy Discovery, Permission Groups Discovery (Domain Groups, Local Groups), Remote Services (SMB/Windows Admin Shares), Remote System Discovery, System Network Connections Discovery, System Service Discovery, and System Services (Service Execution).
- **Psexec (S0029):** This software is associated with various techniques, including Create Account (Domain Account), Create or Modify System Process (Windows Service), Lateral Tool Transfer, Remote Services (SMB/Windows Admin Shares), and System Services (Service Execution).

Threat Group-1314's tactics primarily involve using compromised credentials and various techniques to gain unauthorized access to remote systems and network shares, facilitating lateral movement within a victim's network. Their motivations and specific targeting information are not provided in the available data.

Thrip - Group Overview

Description: Thrip is an espionage group known for its activities targeting satellite communications, telecoms, and defense contractor companies in the United States and Southeast Asia. The group employs custom malware and "living off the land" techniques for its operations.

Motivation: Thrip's specific motivations and objectives are not provided in the available information.

Names: Thrip

Location: Not specified, but the group has targeted organizations in the U.S. and Southeast Asia.

First Seen: October 17, 2018

Observed: Thrip's activities have been observed until at least October 12, 2021.

Techniques Used in All Tactics

- **Command and Scripting Interpreter: PowerShell (T1059.001):** Thrip leveraged PowerShell to execute commands, download payloads, traverse compromised networks, and carry out reconnaissance.
- **Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol (T1048.003):** Thrip used WinSCP to exfiltrate data from targeted organizations over FTP.
- **Obtain Capabilities: Tool (T1588.002):** Thrip obtained and used tools such as Mimikatz and PsExec.
- **Remote Access Software (T1219):** Thrip used a cloud-based remote access software called LogMeIn for their attacks.

Software Used by Thrip

- **Catchamas (S0261):** This software is associated with various techniques, including Application Window Discovery, Clipboard Data, Create or Modify System Process (Windows Service), Data Staged (Local Data Staging), Input Capture (Keylogging), Masquerading (Masquerade Task or Service), Modify Registry, and System Network Configuration Discovery.
- **Mimikatz (S0002):** This software is associated with various techniques, including Access Token Manipulation (SID-History Injection), Account Manipulation, Boot or Logon Autostart Execution (Security Support Provider), Credentials from Password Stores (Credentials from Web Browsers, Windows Credential Manager), OS Credential Dumping (DCSync, Security Account Manager, LSASS Memory, LSA Secrets), Rogue Domain Controller, Steal or Forge Authentication Certificates, Steal or Forge Kerberos Tickets (Golden Ticket, Silver Ticket), Unsecured Credentials (Private Keys), and Use Alternate Authentication Material (Pass the Hash, Pass the Ticket).
- **PsExec (S0029):** Thrip used PsExec to move laterally between computers on the victim's network. This software is associated with various techniques, including Create Account (Domain Account), Create or Modify System Process (Windows Service), Lateral Tool Transfer, Remote Services (SMB/Windows Admin Shares), and System Services (Service Execution).

Thrip's tactics involve using a combination of custom malware, PowerShell, legitimate tools, and cloud-based remote access software to carry out espionage activities. Their motivations and specific targeting information remain undisclosed in the provided data.

Tonto Team - Group Overview

Description: Tonto Team is a suspected Chinese state-sponsored cyber espionage threat group known for conducting cyberattacks primarily targeting South Korea, Japan, Taiwan, and the United States since at least 2009. By 2020, the group expanded its operations to include other Asian and Eastern European countries. Tonto Team has a wide range of targets, including government, military, energy, mining, financial, education, healthcare, and technology.

organizations. Notable campaigns associated with Tonto Team include the Heartbeat Campaign (2009–2012) and Operation Bitter Biscuit (2017).

Motivation: Tonto Team's specific motivations and objectives are not provided in the available information.

Names: Tonto Team

Location: Suspected to be associated with China

First Seen: 2009

Observed: Tonto Team's activities have been observed until at least January 27, 2022.

Techniques Used in All Tactics

- **Command and Scripting Interpreter: PowerShell (T1059.001):** Tonto Team has used PowerShell to download additional payloads.
- **Command and Scripting Interpreter: Python (T1059.006):** Tonto Team has used Python-based tools for execution.
- **Exploitation for Client Execution (T1203):** Tonto Team has exploited Microsoft vulnerabilities, including CVE-2018-0798, CVE-2018-8174, CVE-2018-0802, CVE-2017-11882, CVE-2019-9489, CVE-2020-8468, and CVE-2018-0798, to enable the execution of their delivered malicious payloads.
- **Exploitation for Privilege Escalation (T1068):** Tonto Team has exploited CVE-2019-0803 and MS16-032 to escalate privileges.
- **Exploitation of Remote Services (T1210):** Tonto Team has used EternalBlue exploits for lateral movement.
- **Hijack Execution Flow: DLL Search Order Hijacking (T1574.001):** Tonto Team abuses a legitimate and signed Microsoft executable to launch a malicious DLL.
- **Ingress Tool Transfer (T1105):** Tonto Team has downloaded malicious DLLs that served as ShadowPad loaders.
- **Input Capture: Keylogging (T1056.001):** Tonto Team has used keylogging tools in their operations.
- **Network Share Discovery (T1135):** Tonto Team has used tools such as NBTscan to enumerate network shares.
- **OS Credential Dumping (T1003):** Tonto Team has used a variety of credential dumping tools.
- **Permission Groups Discovery: Local Groups (T1069.001):** Tonto Team has used the ShowLocalGroupDetails command to identify administrator, user, and guest accounts on a compromised host.
- **Phishing: Spearphishing Attachment (T1566.001):** Tonto Team has delivered payloads via spearphishing attachments.
- **Proxy: External Proxy (T1090.002):** Tonto Team has routed their traffic through an external server to obfuscate their location.
- **Server Software Component: Web Shell (T1505.003):** Tonto Team has used a first-stage web shell after compromising a vulnerable Exchange server.
- **User Execution: Malicious File (T1204.002):** Tonto Team has relied on user interaction to open their malicious RTF documents.

Software Used by Tonto Team

- **Bisonal (S0268):** Bisonal is associated with various techniques, including Application Layer

Protocol (Web Protocols), Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder), Command and Scripting Interpreter (Visual Basic, Windows Command Shell), Create or Modify System Process (Windows Service), Data Encoding (Standard Encoding), Data from Local System, Deobfuscate/Decode Files or Information, Dynamic Resolution, Encrypted Channel (Symmetric Cryptography), Exfiltration Over C2 Channel, File and Directory Discovery, Indicator Removal (File Deletion), Ingress Tool Transfer, Masquerading (Match Legitimate Name or Location), Modify Registry, Native API, Non-Application Layer Protocol, Obfuscated Files or Information (Binary Padding, Software Packing), Office Application Startup (Add-Ins), Phishing (Spearphishing Attachment), Process Discovery, Proxy, Query Registry, System Binary Proxy Execution (Rundll32), System Information Discovery, System Network Configuration Discovery, System Time Discovery, User Execution (Malicious File), Virtualization/Sandbox Evasion, Virtualization/Sandbox Evasion (Time-Based Evasion).

- **gsecdump (S0008):** Associated with OS Credential Dumping (Security Account Manager, LSA Secrets).
- **LaZagne (S0349):** Linked to Credentials from Password Stores (Windows Credential Manager, Credentials from Web Browsers, Keychain, OS Credential Dumping: LSA Secrets, /etc/passwd and /etc/shadow, LSASS Memory, Cached Domain Credentials, Proc Filesystem), OS Credential Dumping, Unsecured Credentials (Credentials in Files).
- **Mimikatz (S0002):** Mimikatz is associated with various techniques, including Access Token Manipulation (SID-History Injection, Account Manipulation), Boot or Logon Autostart Execution (Security Support Provider), Credentials from Password Stores (Credentials from Web Browsers, Windows Credential Manager), OS Credential Dumping (DCSync, Security Account Manager, LSASS Memory, LSA Secrets), Rogue Domain Controller, Steal or Forge Authentication Certificates, Steal or Forge Kerberos Tickets (Golden Ticket, Silver Ticket), Unsecured Credentials (Private Keys), Use Alternate Authentication Material (Pass the Hash, Pass the Ticket).
- **NBTscan (S0590):** Linked to Network Service Discovery, Network Sniffing, Remote System Discovery, System Network Configuration Discovery, System Owner/User Discovery.
- **ShadowPad (S0596):** ShadowPad is associated with various techniques, including Application Layer Protocol (DNS, File Transfer Protocols, Web Protocols), Data Encoding (Non-Standard Encoding), Deobfuscate/Decode Files or Information, Dynamic Resolution (Domain Generation Algorithms), Indicator Removal, Ingress Tool Transfer, Modify Registry, Non-Application Layer Protocol, Obfuscated Files or Information (Fileless Storage), Process Discovery, Process Injection, Process Injection (Dynamic-link Library Injection), Scheduled Transfer, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Time Discovery.

Tonto Team employs a diverse set of techniques and software tools to conduct cyber espionage activities, with a particular focus on exploiting vulnerabilities and conducting spearphishing campaigns. Their motivations and specific targeting information remain undisclosed in the provided data.

Transparent Tribe - Group Overview

Description: Transparent Tribe is a suspected Pakistan-based threat group known for its activities since at least 2013. The group primarily targets diplomatic, defense, and research organizations in India and Afghanistan. Transparent Tribe has been associated with various campaigns and has a history of using phishing attacks, malicious links, and weaponized documents to compromise its targets.

Motivation: Transparent Tribe's specific motivations and objectives are not provided in the available information.

Names: Transparent Tribe

Location: Suspected to be based in Pakistan

First Seen: Since at least 2013

Observed: Transparent Tribe's activities have been observed until at least July 2022.

Techniques Used in All Tactics

- **Acquire Infrastructure: Domains (T1583.001):** Transparent Tribe has registered domains to mimic file sharing, government, defense, and research websites for use in targeted campaigns. In one campaign (C0011), they registered domains designed to appear relevant to student targets in India.
- **Command and Scripting Interpreter: Visual Basic (T1059.005):** Transparent Tribe has crafted VBS-based malicious documents. In the C0011 campaign, they used malicious VBA macros within a lure document as part of the Crimson malware installation process onto a compromised host.
- **Compromise Infrastructure: Domains (T1584.001):** Transparent Tribe has compromised domains for use in targeted malicious campaigns.
- **Develop Capabilities: Digital Certificates (T1587.003):** In one campaign (C0011), Transparent Tribe established SSL certificates on typo-squatted domains registered by the group.
- **Drive-by Compromise (T1189):** Transparent Tribe has used websites with malicious hyperlinks and iframes to infect targeted victims with Crimson, njRAT, and other malicious tools.
- **Dynamic Resolution (T1568):** Transparent Tribe has used dynamic DNS services to set up Command and Control (C2) infrastructure.
- **Exploitation for Client Execution (T1203):** Transparent Tribe has crafted malicious files to exploit vulnerabilities such as CVE-2012-0158 and CVE-2010-3333 for execution.
- **Hide Artifacts: Hidden Files and Directories (T1564.001):** Transparent Tribe can hide legitimate directories and replace them with malicious copies of the same name.
- **Masquerading: Match Legitimate Name or Location (T1036.005):** Transparent Tribe can mimic legitimate Windows directories by using the same icons and names.
- **Obfuscated Files or Information (T1027):** Transparent Tribe has dropped encoded executables on compromised hosts.
- **Phishing: Spearphishing Attachment (T1566.001):** Transparent Tribe has sent spearphishing emails with attachments to deliver malicious payloads.
- **Phishing: Spearphishing Link (T1566.002):** Transparent Tribe has embedded links to malicious downloads in emails.
- **Stage Capabilities: Upload Malware (T1608.001):** In one campaign (C0011), Transparent Tribe hosted malicious documents on domains registered by the group.
- **Stage Capabilities: Drive-by Target (T1608.004):** Transparent Tribe has set up websites with malicious hyperlinks and iframes to infect targeted victims with Crimson, njRAT, and other malicious tools.
- **User Execution: Malicious Link (T1204.001):** Transparent Tribe has directed users to open URLs hosting malicious content.
- **User Execution: Malicious File (T1204.002):** Transparent Tribe has used weaponized documents in emails to compromise targeted systems.

Software Used by Transparent Tribe

- **Crimson (S0115):** Crimson is associated with various techniques, including Application Layer Protocol (Web Protocols), Audio Capture, Boot or Logon Autostart Execution (Registry

Run Keys / Startup Folder), Command and Scripting Interpreter (Windows Command Shell), Credentials from Password Stores (Credentials from Web Browsers), Data from Local System, Data from Removable Media, Deobfuscate/Decode Files or Information, Email Collection (Local Email Collection), Exfiltration Over C2 Channel, File and Directory Discovery, Indicator Removal (File Deletion), Ingress Tool Transfer, Input Capture (Keylogging), Modify Registry, Non-Application Layer Protocol, Peripheral Device Discovery, Process Discovery, Query Registry, Replication Through Removable Media, Screen Capture, Software Discovery (Security Software Discovery), System Information Discovery, System Location Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Time Discovery, Video Capture, Virtualization/Sandbox Evasion (Time-Based Evasion).

- **DarkComet (S0334):** DarkComet is associated with various techniques, including Application Layer Protocol (Web Protocols), Audio Capture, Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder), Clipboard Data, Command and Scripting Interpreter, Command and Scripting Interpreter (Windows Command Shell), Impair Defenses (Disable or Modify System Firewall, Disable or Modify Tools), Ingress Tool Transfer, Input Capture (Keylogging), Masquerading (Match Legitimate Name or Location), Modify Registry, Obfuscated Files or Information (Software Packing), Process Discovery, Remote Services (Remote Desktop Protocol), System Information Discovery, System Owner/User Discovery, Video Capture.
- **njRAT (S0385):** njRAT is associated with various techniques, including Application Layer Protocol (Web Protocols), Application Window Discovery, Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder), Command and Scripting Interpreter (PowerShell, Windows Command Shell), Credentials from Password Stores (Credentials from Web Browsers), Data Encoding (Standard Encoding), Data from Local System, Dynamic Resolution (Fast Flux DNS), Exfiltration Over C2 Channel, File and Directory Discovery, Impair Defenses (Disable or Modify System Firewall), Indicator Removal (File Deletion, Clear Persistence), Ingress Tool Transfer, Input Capture (Keylogging), Modify Registry, Native API, Non-Standard Port, Obfuscated Files or Information (Compile After Delivery), Peripheral Device Discovery, Process Discovery, Query Registry, Remote Services (Remote Desktop Protocol), Remote System Discovery, Replication Through Removable Media, Screen Capture, System Information Discovery, System Owner/User Discovery, Video Capture.
- **ObliqueRAT (S0644):** ObliqueRAT is associated with various techniques, including Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder), Data from Removable Media, Data Staged (Local Data Staging), Data Transfer Size Limits, File and Directory Discovery, Obfuscated Files or Information (Steganography), Peripheral Device Discovery, Process Discovery, Screen Capture, System Information Discovery, System Owner/User Discovery, User Execution (Malicious Link), Video Capture, Virtualization/Sandbox Evasion (System Checks).
- **Peppy (S0643):** Peppy is associated with various techniques, including Application Layer Protocol (Web Protocols), Automated Exfiltration, Command and Scripting Interpreter (Windows Command Shell), File and Directory Discovery, Ingress Tool Transfer, Input Capture (Keylogging), Screen Capture.

Transparent Tribe employs a wide range of techniques and uses multiple software tools to conduct its cyber espionage activities, with a focus on compromising targets in India and Afghanistan. Their motivations and specific targeting information remain undisclosed in the provided data.

Tropic Trooper - Group Overview

Description: Tropic Trooper is an unaffiliated threat group known for conducting targeted campaigns against entities in Taiwan, the Philippines, and Hong Kong. The group has a history of focusing on government, healthcare, transportation, and high-tech industries as its primary targets. Tropic Trooper's activities have been ongoing since 2011.

Motivation: The specific motivations and objectives of Tropic Trooper are not provided in the available information.

Names: Tropic Trooper

Location: Unknown

First Seen: Since 2011

Observed: Tropic Trooper's activities have been observed as of the last available data.

Techniques Used in All Tactics

- **Application Layer Protocol: Web Protocols (T1071.001):** Tropic Trooper has used HTTP in communication with the Command and Control (C2) servers.
- **Application Layer Protocol: DNS (T1071.004):** Tropic Trooper's backdoor has communicated with the C2 over the DNS protocol.
- **Automated Collection (T1119):** Tropic Trooper has collected information automatically using the adversary's USBferry attack.
- **Automated Exfiltration (T1020):** Tropic Trooper has used a copy function to automatically exfiltrate sensitive data from air-gapped systems using USB storage.
- **Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001):** Tropic Trooper has created shortcuts in the Startup folder to establish persistence.
- **Boot or Logon Autostart Execution: Winlogon Helper DLL (T1547.004):** Tropic Trooper has created the Registry key HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell and sets the value to establish persistence.
- **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** Tropic Trooper has used Windows command scripts.
- **Create or Modify System Process: Windows Service (T1543.003):** Tropic Trooper has installed a service pointing to a malicious DLL dropped to disk.
- **Data Encoding: Standard Encoding (T1132.001):** Tropic Trooper has used base64 encoding to hide command strings delivered from the C2.
- **Deobfuscate/Decode Files or Information (T1140):** Tropic Trooper used shellcode with an XOR algorithm to decrypt a payload. Tropic Trooper also decrypted image files which contained a payload.
- **Encrypted Channel (T1573):** Tropic Trooper has encrypted traffic with the C2 to prevent network detection.
- **Asymmetric Cryptography (T1573.002):** Tropic Trooper has used SSL to connect to C2 servers.
- **Exfiltration Over Physical Medium: Exfiltration over USB (T1052.001):** Tropic Trooper has exfiltrated data using USB storage devices.
- **Exploitation for Client Execution (T1203):** Tropic Trooper has executed commands through Microsoft security vulnerabilities, including CVE-2017-11882, CVE-2018-0802, and CVE-2012-0158.
- **File and Directory Discovery (T1083):** Tropic Trooper has monitored files' modified time.
- **Hide Artifacts: Hidden Files and Directories (T1564.001):** Tropic Trooper has created a hidden directory under C:\ProgramData\Apple\Updates\ and C:\Users\Public\Documents\Fish.
- **Hijack Execution Flow: DLL Side-Loading (T1574.002):** Tropic Trooper has been known to side-load DLLs using a valid version of a Windows Address Book and Windows Defender executable with one of their tools.
- **Indicator Removal: File Deletion (T1070.004):** Tropic Trooper has deleted dropper files on an infected system using command scripts.

additional files.

- **Masquerading: Match Legitimate Name or Location (T1036.005):** Tropic Trooper has hidden payloads in Flash directories and fake installer files.
- **Native API (T1106):** Tropic Trooper has used multiple Windows APIs including HttpInitialize, HttpCreateHttpRequest, and HttpAddUrl.
- **Network Service Discovery (T1046):** Tropic Trooper used pr and an openly available tool to scan for open ports on target systems.
- **Network Share Discovery (T1135):** Tropic Trooper used netview to scan target systems for shared resources.
- **Obfuscated Files or Information (T1027):** Tropic Trooper has encrypted configuration files.
- **Steganography (T1027.003):** Tropic Trooper has used JPG files with encrypted payloads to mask their backdoor routines and evade detection.
- **Phishing: Spearphishing Attachment (T1566.001):** Tropic Trooper sent spearphishing emails that contained malicious Microsoft Office and fake installer file attachments.
- **Process Discovery (T1057):** Tropic Trooper is capable of enumerating the running processes on the system using pslist.
- **Process Injection: Dynamic-link Library Injection (T1055.001):** Tropic Trooper has injected a DLL backdoor into dllhost.exe and svchost.exe.
- **Replication Through Removable Media (T1091):** Tropic Trooper has attempted to transfer USBferry from an infected USB device by copying an Autorun function to the target machine.
- **Server Software Component: Web Shell (T1505.003):** Tropic Trooper has started a web service in the target host and wait for the adversary to connect, acting as a web shell.
- **Software Discovery (T1518):** Tropic Trooper's backdoor could list the infected system's installed software.
- **Security Software Discovery (T1518.001):** Tropic Trooper can search for anti-virus software running on the system.
- **System Information Discovery (T1082):** Tropic Trooper has detected a target system's OS version and system volume information.
- **System Network Configuration Discovery (T1016):** Tropic Trooper has used scripts to collect the host's network topology.
- **System Network Connections Discovery (T1049):** Tropic Trooper has tested if the localhost network is available and other connection capability on an infected system using command scripts.
- **System Owner/User Discovery (T1033):** Tropic Trooper used letmein to scan for saved usernames on the target system.
- **Template Injection (T1221):** Tropic Trooper delivered malicious documents with the XLSX extension, typically used by OpenXML documents, but the file itself was actually an OLE (XLS) document.
- **User Execution: Malicious File (T1204.002):** Tropic Trooper has lured victims into executing malware via malicious email attachments.
- **Valid Accounts: Local Accounts (T1078.003):** Tropic Trooper has used known administrator account credentials to execute the backdoor directly.

Software Used by Tropic Trooper

- **BITSAAdmin (S0190):** BITSAAdmin is associated with various techniques, including BITS Jobs, Exfiltration Over Alternative Protocol (Exfiltration Over Unencrypted Non-C2 Protocol), Ingress Tool Transfer, and Lateral Tool Transfer.
- **KeyBoy (S0387):** KeyBoy is associated with various techniques, including Boot or Logon Autostart Execution (Winlogon Helper DLL), Command and Scripting Interpreter (Python, Visual Basic, PowerShell, Windows Command Shell), Create or Modify System Process

(Windows Service), Credentials from Password Stores (Credentials from Web Browsers), Data Obfuscation (Protocol Impersonation), File and Directory Discovery, Hide Artifacts (Hidden Window), Indicator Removal (Timestamp), Ingress Tool Transfer, Input Capture (Keylogging), Inter-Process Communication (Dynamic Data Exchange), Obfuscated Files or Information, Screen Capture, System Information Discovery, and System Network Configuration Discovery.

- **PoisonIvy (S0012):** PoisonIvy is associated with various techniques, including Application Window Discovery, Boot or Logon Autostart Execution (Registry Run Keys / Startup Folder, Active Setup), Command and Scripting Interpreter (Windows Command Shell), Create or Modify System Process (Windows Service), Data from Local System, Data Staged (Local Data Staging), Encrypted Channel (Symmetric Cryptography), Ingress Tool Transfer, Input Capture (Keylogging), Modify Registry, Obfuscated Files or Information, Process Injection (Dynamic-link Library Injection), and Rootkit.
- **ShadowPad (S0596):** ShadowPad is associated with various techniques, including Application Layer Protocol (DNS, File Transfer Protocols, Web Protocols), Data Encoding (Non-Standard Encoding), Deobfuscate/Decode Files or Information, Dynamic Resolution (Domain Generation Algorithms), Indicator Removal, Ingress Tool Transfer, Modify Registry, Non-Application Layer Protocol, Obfuscated Files or Information (Fileless Storage), Process Discovery, Process Injection, Process Injection (Dynamic-link Library Injection), Scheduled Transfer, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, and System Time Discovery.
- **USBferry (S0452):** USBferry is associated with various techniques, including Account Discovery (Local Account), Command and Scripting Interpreter (Windows Command Shell), Data from Local System, File and Directory Discovery, Peripheral Device Discovery, Process Discovery, Remote System Discovery, Replication Through Removable Media, System Binary Proxy Execution (Rundll32), System Network Configuration Discovery, and System Network Connections Discovery.
- **YAHOOYAH (S0388):** YAHOOYAH is associated with various techniques, including Application Layer Protocol (Web Protocols), Deobfuscate/Decode Files or Information, Ingress Tool Transfer, Obfuscated Files or Information, Software Discovery (Security Software Discovery), and System Information Discovery.

Tropic Trooper utilizes a wide array of techniques and software tools for its targeted campaigns, with a focus on various industries and regions. However, the group's specific motivations and goals are not provided in the available data.

Turla - Group Overview

Description: Turla is a sophisticated cyber espionage threat group associated with Russia's Federal Security Service (FSB). This group has been active since at least 2004 and is known for targeting various industries, including government, embassies, military, education, research, and pharmaceutical companies. Turla conducts watering hole and spearphishing campaigns and utilizes in-house tools and malware, such as Uroburos.

Motivation: Turla primarily focuses on conducting cyber espionage activities, collecting sensitive information, and advancing Russian interests on the global stage.

Names: Turla is also associated with the following groups: IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear.

Location: Turla's operations have been detected in over 50 countries worldwide.

First Seen: Turla was first identified and documented in 2004.

Observed: Turla's activities have been observed and documented up to August 2023.

Techniques Used in all tactics

- **Access Token Manipulation: Create Process with Token:** Turla leverages RPC backdoors to impersonate or steal process tokens before executing commands.
- **Account Discovery: Local Account:** Turla uses "net user" to enumerate local accounts on the system.
- **Account Discovery: Domain Account:** Turla employs "net user /domain" to enumerate domain accounts.
- **Acquire Infrastructure: Web Services:** Turla creates web accounts, including Dropbox and GitHub, for C2 (Command and Control) and document exfiltration.
- **Application Layer Protocol: Web Protocols:** Turla uses HTTP and HTTPS for C2 communications.
- **Application Layer Protocol: Mail Protocols:** Turla communicates with C2 servers via email attachments.
- **Archive Collected Data: Archive via Utility:** Turla encrypts stolen files into RAR archives before exfiltration.
- **Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder:** Turla establishes persistence by adding registry keys.
- **Boot or Logon Autostart Execution: Winlogon Helper DLL:** Turla establishes persistence by modifying Winlogon.
- **Brute Force:** Turla attempts to connect to systems within a victim's network using predefined lists of passwords.
- **Command and Scripting Interpreter: PowerShell:** Turla uses PowerShell to execute commands/scripts.
- **Command and Scripting Interpreter: Windows Command Shell:** Turla uses cmd.exe to execute commands.
- **Command and Scripting Interpreter: Visual Basic:** Turla employs VBS scripts.
- **Command and Scripting Interpreter: Python:** Turla uses IronPython scripts.
- **Command and Scripting Interpreter: JavaScript:** Turla employs various JavaScript-based backdoors.
- **Compromise Infrastructure: Virtual Private Server:** Turla leverages compromised VPS infrastructure.
- **Compromise Infrastructure: Server:** Turla uses compromised servers as infrastructure.
- **Compromise Infrastructure: Web Services:** Turla frequently uses compromised WordPress sites for C2 infrastructure.
- **Credentials from Password Stores: Windows Credential Manager:** Turla gathers credentials from the Windows Credential Manager tool.
- **Data from Information Repositories:** Turla collects documents from an organization's internal central database.
- **Data from Local System:** Turla uploads files from victim machines.
- **Data from Removable Media:** Turla collects files from USB thumb drives.
- **Deobfuscate/Decode Files or Information:** Turla uses custom decryption routines to decode payloads.
- **Develop Capabilities: Malware:** Turla develops its own unique malware.
- **Drive-by Compromise:** Turla infects victims using watering holes.
- **Event Triggered Execution: Windows Management Instrumentation Event Subscription:** Turla uses WMI event filters and consumers to establish persistence.
- **Event Triggered Execution: PowerShell Profile:** Turla uses PowerShell profiles for persistence.
- **Exfiltration Over Web Service: Exfiltration to Cloud Storage:** Turla uses WebDAV to upload stolen USB files to a cloud drive.
- **Exploitation for Privilege Escalation:** Turla exploits vulnerabilities to escalate privileges.

- **File and Directory Discovery:** Turla surveys a system to discover files in specific locations.
- **Group Policy Discovery:** Turla surveys a system to discover Group Policy details.
- **Impair Defenses: Disable or Modify Tools:** Turla uses various methods to bypass Windows antimalware products.
- **Ingress Tool Transfer:** Turla uses shellcode to download Meterpreter after compromising a victim.
- **Lateral Tool Transfer:** Turla's backdoors transfer files to/from victim machines on the local network.
- **Modify Registry:** Turla modifies Registry values to store payloads.
- **Native API:** Turla and its backdoors use APIs calls for various tasks.
- **Obfuscated Files or Information: Indicator Removal from Tools:** Turla obfuscates strings that could be used as IoCs.
- **Obfuscated Files or Information: Command Obfuscation:** Turla obfuscates PowerShell commands and payloads.
- **Obfuscated Files or Information: Fileless Storage:** Turla uses the Registry to store encrypted and encoded payloads.
- **Obtain Capabilities: Malware:** Turla obtains malware from other threat actors.
- **Obtain Capabilities: Tool:** Turla obtains and customizes publicly-available tools.
- **Password Policy Discovery:** Turla acquires password policy information.
- **Peripheral Device Discovery:** Turla lists connected drives using "fsutil fsinfo drives."
- **Permission Groups Discovery: Local Groups:** Turla enumerates local group information.
- **Permission Groups Discovery: Domain Groups:** Turla identifies domain groups on a victim system.
- **Privilege Escalation:** Turla escalates privileges by injecting code into the Winlogon process.
- **Process Discovery:** Turla uses "tasklist" to identify running processes.
- **Process Injection:** Turla injects malicious code into legitimate processes.
- **Registry Run Keys / Startup Folder:** Turla adds Registry keys for persistence.
- **Scheduled Task:** Turla adds tasks for persistence.
- **Scripting: Scheduled Task/Job:** Turla schedules scripts to execute on a victim's system.
- **Service Execution:** Turla registers malicious services.
- **Software Deployment Tools:** Turla leverages the Group Policy Object for software deployment.
- **System Network Configuration Discovery:** Turla identifies network configuration details.
- **System Owner/User Discovery:** Turla lists users via "net user" and identifies the system owner using "whoami."
- **System Service Discovery:** Turla identifies service details.
- **System Time Discovery:** Turla surveys system time.
- **Tasking Data:** Turla uses specific tasking instructions in C2 communications.
- **Traffic Signaling:** Turla uses steganography to hide C2 traffic.
- **Valid Accounts:** Turla gains access with legitimate accounts.
- **Vulnerability Scanning:** Turla uses vulnerability scanners to identify potential targets.
- **Windows Management Instrumentation Event Subscription:** Turla uses WMI subscriptions to execute arbitrary code.
- **Windows Management Instrumentation Event Trigger:** Turla triggers WMI events.
- **Windows Management Instrumentation: Windows Management Instrumentation Execution:** Turla leverages WMI to run scripts.
- **Write Registry:** Turla writes to the Registry for persistence.

Software and Tools Used

- **Compromise Infrastructure: LAMP:** Turla uses LAMP (Linux, Apache, MySQL, PHP)

- **Credential Dumping: ProcDump:** Turla uses ProcDump to dump LSASS memory.
- **Deobfuscate/Decode Files or Information: File Deletion:** Turla deletes files after use.
- **Deobfuscate/Decode Files or Information: NTFS File Attributes:** Turla extracts files from NTFS file attributes.
- **Development Tools:** Turla uses various development tools to create custom malware.
- **Execution: CMSTP:** Turla uses CMSTP for DLL side-loading.
- **Execution: PowerShell:** Turla uses PowerShell for execution.
- **Exfiltration: Exfiltration Over C2 Channel:** Turla exfiltrates data over C2 channels.
- **Exploitation for Privilege Escalation: CVE-2021-3156:** Turla exploits the sudo vulnerability.
- **Input Capture: Event Triggered Screen Capture:** Turla captures screens based on system events.
- **Input Capture: Screen Capture:** Turla captures screenshots of victim systems.
- **Persistence: DLL Side-Loading:** Turla side-loads malicious DLLs.
- **Persistence: Port Monitors:** Turla uses port monitors for persistence.
- **Privilege Escalation: Bypass User Account Control:** Turla bypasses UAC using various methods.
- **Scheduled Task:** Turla schedules tasks.
- **Service Execution: BITS Jobs:** Turla uses BITS jobs to execute files.
- **Service Execution: Named Pipes:** Turla uses named pipes to execute malicious code.
- **System Information Discovery: Bypass User Account Control:** Turla uses UAC bypass methods.
- **System Information Discovery: Software Discovery:** Turla surveys installed software.
- **System Network Configuration Discovery: Netstat:** Turla uses "netstat" to discover network information.
- **Tasking Data:** Turla uses specific tasking instructions.
- **User Execution: Command and Scripting Interpreter:** Turla uses command and scripting interpreters to execute commands.
- **Vulnerability Scanning: BlueKeep:** Turla exploits the BlueKeep vulnerability.
- **Vulnerability Scanning: CVE-2019-1040:** Turla exploits the CVE-2019-1040 vulnerability.
- **Vulnerability Scanning: CVE-2019-9670:** Turla exploits the CVE-2019-9670 vulnerability.
- **Vulnerability Scanning: CVE-2019-9710:** Turla exploits the CVE-2019-9710 vulnerability.
- **Vulnerability Scanning: CVE-2019-9832:** Turla exploits the CVE-2019-9832 vulnerability.
- **Vulnerability Scanning: CVE-2020-0688:** Turla exploits the CVE-2020-0688 vulnerability.
- **Vulnerability Scanning: CVE-2020-10189:** Turla exploits the CVE-2020-10189 vulnerability.
- **Vulnerability Scanning: CVE-2020-1350:** Turla exploits the CVE-2020-1350 vulnerability.
- **Vulnerability Scanning: CVE-2020-1472:** Turla exploits the CVE-2020-1472 vulnerability.
- **Vulnerability Scanning: CVE-2020-17144:** Turla exploits the CVE-2020-17144 vulnerability.
- **Vulnerability Scanning: CVE-2020-2021:** Turla exploits the CVE-2020-2021 vulnerability.
- **Vulnerability Scanning: CVE-2020-3153:** Turla exploits the CVE-2020-3153 vulnerability.
- **Vulnerability Scanning: CVE-2020-3396:** Turla exploits the CVE-2020-3396 vulnerability.
- **Vulnerability Scanning: CVE-2020-3433:** Turla exploits the CVE-2020-3433 vulnerability.
- **Vulnerability Scanning: CVE-2020-8616:** Turla exploits the CVE-2020-8616 vulnerability.
- **Vulnerability Scanning: CVE-2020-9054:** Turla exploits the CVE-2020-9054 vulnerability.
- **Vulnerability Scanning: CVE-2021-1527:** Turla exploits the CVE-2021-1527 vulnerability.
- **Vulnerability Scanning: CVE-2021-1732:** Turla exploits the CVE-2021-1732 vulnerability.
- **Vulnerability Scanning: CVE-2021-26411:** Turla exploits the CVE-2021-26411 vulnerability.
- **Vulnerability Scanning: CVE-2021-31166:** Turla exploits the CVE-2021-31166 vulnerability.
- **Vulnerability Scanning: CVE-2021-34473:** Turla exploits the CVE-2021-34473 vulnerability.

- **Vulnerability Scanning: CVE-2021-34484:** Turla exploits the CVE-2021-34484 vulnerability.
- **Vulnerability Scanning: CVE-2021-40444:** Turla exploits the CVE-2021-40444 vulnerability.

Volatile Cedar - Group Overview

Description: Volatile Cedar is a Lebanese threat group that has been active since 2012, targeting individuals, companies, and institutions worldwide. This group is primarily motivated by political and ideological interests.

Motivation: Volatile Cedar is motivated by political and ideological objectives, which drive its cyber activities.

Names: Volatile Cedar is also associated with the group "Lebanese Cedar."

Location: Volatile Cedar's exact location is not publicly disclosed, but it is known to operate globally.

First Seen: Volatile Cedar was first detected in cyber activities in 2012.

Observed: Volatile Cedar's activities have been observed up to April 20, 2022.

Techniques Used in all tactics

- **Active Scanning: Vulnerability Scanning (T1595.002):** Volatile Cedar performs vulnerability scans of target servers.
- **Active Scanning: Wordlist Scanning (T1595.003):** Volatile Cedar employs tools like DirBuster and GoBuster to brute force web directories and DNS subdomains.
- **Exploit Public-Facing Application (T1190):** Volatile Cedar targets publicly facing web servers, utilizing both automatic and manual vulnerability discovery.
- **Ingress Tool Transfer (T1105):** Volatile Cedar can deploy additional tools.
- **Server Software Component: Web Shell (T1505.003):** Volatile Cedar injects web shell code into servers.

Software Used by Volatile Cedar

- **Caterpillar WebShell (S0572):** This tool is associated with Volatile Cedar and is used for various purposes, including brute force attacks, data collection, exfiltration, and system discovery.
 - **Techniques:** Brute Force, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, Exfiltration Over C2 Channel, File and Directory Discovery, Ingress Tool Transfer, Modify Registry, Network Service Discovery, Permission Groups Discovery: Local Groups, Process Discovery, Rootkit, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Service Discovery.
- **Explosive (S0569):** Another tool employed by Volatile Cedar, Explosive, is used for activities such as web protocol exploitation, data collection, and system discovery.
 - **Techniques:** Application Layer Protocol: Web Protocols, Clipboard Data, Data from Removable Media, Encrypted Channel: Symmetric Cryptography, Hide Artifacts: Hidden Files and Directories, Ingress Tool Transfer, Input Capture: Keylogging, Modify Registry, Native API, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery.

Volt Typhoon - Group Overview

Description: Volt Typhoon is a state-sponsored threat actor based in the People's Republic of China (PRC), known to have been active since at least 2021. This group primarily engages in espionage and information gathering activities, with a particular focus on critical infrastructure organizations in the United States, including Guam. Volt Typhoon is characterized by its emphasis on stealth in operations, employing web shells, living-off-the-land (LOTL) binaries, hands-on-keyboard activities, and stolen credentials in its cyber operations.

Motivation: Volt Typhoon's primary motivation is to engage in espionage and gather sensitive information. The group's activities align with state-sponsored interests.

Names: Volt Typhoon is also associated with the group "BRONZE SILHOUETTE."

Location: Volt Typhoon is believed to operate from the People's Republic of China (PRC).

First Seen: The activities of Volt Typhoon were first detected in at least 2021.

Observed: Volt Typhoon's activities have been observed as of October 3, 2023.

Techniques Used in all tactics

- **Account Discovery: Domain Account (T1087.002):** Volt Typhoon performs account discovery in compromised environments using commands like `net group /dom` and `net group "Domain Admins" /dom`.
- **Archive Collected Data: Archive via Utility (T1560.001):** Volt Typhoon archives sensitive data, such as the `ntds.dit` database, as a multi-volume password-protected archive using tools like 7-Zip.
- **Command and Scripting Interpreter: PowerShell (T1059.001):** Volt Typhoon utilizes PowerShell for various purposes, including remote system discovery.
- **Command and Scripting Interpreter: Windows Command Shell (T1059.003):** Volt Typhoon employs the Windows command shell for hands-on-keyboard activities and discovery in targeted environments.
- **Compromise Infrastructure: Server (T1584.004):** Volt Typhoon utilizes compromised PRTG servers from other organizations for Command and Control (C2) purposes.
- **Compromise Infrastructure: Botnet (T1584.005):** Volt Typhoon routes traffic through compromised small office and home office (SOHO) network equipment, many of which are located in the same geographic area as the victim.
- **Credentials from Password Stores (T1555):** Volt Typhoon attempts to obtain credentials from various sources, including OpenSSH, `realvnc`, and PuTTY.
- **Data from Local System (T1005):** Volt Typhoon steals the Active Directory database from targeted environments and extracts event log information using `Wevtutil`.
- **Data Staged (T1074):** Volt Typhoon stages collected data in password-protected archives and saves stolen files locally in the `C:\Windows\Temp\` directory.
- **Encrypted Channel: Symmetric Cryptography (T1573.001):** Volt Typhoon uses an AES-encrypted version of the Awen web shell for C2 communications.
- **Exploit Public-Facing Application (T1190):** Volt Typhoon gains initial access by exploiting vulnerabilities such as CVE-2021-40539 in internet-facing ManageEngine ADSelfService Plus servers.
- **Indicator Removal: File Deletion (T1070.004):** Volt Typhoon uses the `rd /S` command to delete their working directories and files.
- **Indicator Removal: Clear Network Connection History and Configurations (T1070.007):** Volt Typhoon inspects server logs to remove their IP addresses.

- **Lateral Tool Transfer (T1570.001):** Volt Typhoon copies web shells between servers in targeted environments.
- **Log Enumeration (T1654):** Volt Typhoon uses tools like wevtutil.exe and PowerShell's Get-EventLog security to enumerate Windows logs for successful logon events.
- **Masquerading: Match Legitimate Name or Location (T1036.005):** Volt Typhoon uses legitimate-looking filenames for various activities and employs names such as cisco_up.exe, cl64.exe, vm3dservice.exe, watchdogd.exe, Win.exe, WmiPreSV.exe, and WmiPrvSE.exe for certain tools.
- **Masquerading: Masquerade File Type (T1036.008):** Volt Typhoon appends copies of the ntds.dit database with a .gif file extension.
- **Obtain Capabilities: Tool (T1588.002):** Volt Typhoon uses customized versions of open-source tools for C2.
- **OS Credential Dumping: LSASS Memory (T1003.001):** Volt Typhoon attempts to access hashed credentials from the LSASS process memory.
- **OS Credential Dumping: NTDS (T1003.003):** Volt Typhoon uses ntds.util to create domain controller installation media containing usernames and password hashes.
- **Permission Groups Discovery: Local Groups (T1074.001):** Volt Typhoon enumerates local groups in compromised environments using commands like net localgroup administrators.
- **Permission Groups Discovery: Domain Groups (T1074.002):** Volt Typhoon runs net group in compromised environments to discover domain groups.
- **Process Discovery (T1057):** Volt Typhoon enumerates running processes on targeted systems.
- **Proxy (T1090):** Volt Typhoon uses compromised devices and customized versions of open-source tools for proxying network traffic, including tools like Fast Reverse Proxy (FRP), Earthworm, and Impacket.
- **Proxy: Internal Proxy (T1090.001):** Volt Typhoon employs the built-in netsh port proxy command to create proxies on compromised systems for facilitating access.
- **Query Registry (T1012):** Volt Typhoon queries the Registry on compromised systems for information on installed software.
- **Remote System Discovery (T1018):** Volt Typhoon uses various methods, including Ping, to enumerate systems on compromised networks.
- **Server Software Component: Web Shell (T1505.003):** Volt Typhoon uses web shells, including those named AuditReport.aspx and iisstart.aspx, in compromised environments.
- **Software Discovery (T1518):** Volt Typhoon queries the Registry on compromised systems for information on installed software.
- **System Information Discovery (T1082):** Volt Typhoon discovers file system types, drive names, sizes, and free space on compromised systems.
- **System Network Configuration Discovery (T1016):** Volt Typhoon executes multiple commands to enumerate network topology and settings, including ipconfig, netsh interface firewall show all, and netsh interface portproxy show all.
- **System Network Connections Discovery (T1049):** Volt Typhoon uses netstat -ano on compromised hosts to enumerate network connections.
- **System Owner/User Discovery (T1033):** Volt Typhoon executes PowerShell commands like Get-EventLog security -instanceid 4624 to identify associated user and computer account names.
- **Valid Accounts: Domain Accounts (T1078.002):** Volt Typhoon uses compromised domain accounts to authenticate to devices on compromised networks.
- **Virtualization/Sandbox Evasion: System Checks (T1497.001):** Volt Typhoon runs system checks to determine if they are operating in a virtualized environment.
- **Windows Management Instrumentation (T1047):** Volt Typhoon leverages WMI for various purposes, including execution and remote system discovery.

Software Used by Volt Typhoon

- **certutil (S0160)**: Used for tasks such as archiving data, deobfuscating/decoding files or information, ingress tool transfer, and subverting trust controls by installing root certificates.
- **Impacket (S0357)**: Utilized for activities such as Adversary-in-the-Middle attacks, network sniffing, OS credential dumping (including NTDS and LSASS memory), stealing or forging Kerberos tickets, and Windows Management Instrumentation.
- **ipconfig (S0100)**: Employed for system network configuration discovery.
- **Mimikatz (S0002)**: Used for various purposes, including access token manipulation, credentials theft, OS credential dumping, and more.
- **Net (S0039)**: Utilized for account discovery, creating and managing accounts, indicator removal, network share operations, password policy discovery, permission groups discovery, remote services, remote system discovery, system network connections discovery, system service discovery, and system time discovery.
- **netsh (S0108)**: Used for event-triggered execution, impairing defenses, proxying, and software discovery.
- **netstat (S0104)**: Employed for system network connections discovery.
- **Nltest (S0359)**: Utilized for domain trust discovery, remote system discovery, and system network configuration discovery.
- **Ping (S0097)**: Employed for remote system discovery.
- **Systeminfo (S0096)**: Used for system information discovery.
- **Tasklist (S0057)**: Employed for process discovery, software discovery (including security software), and system service discovery.
- **Wevtutil (S0645)**: Utilized for data extraction from local systems, impairing defenses by disabling Windows Event Logging, and indicator removal by clearing Windows Event Logs.

Resources

- <https://attack.mitre.org/groups/>