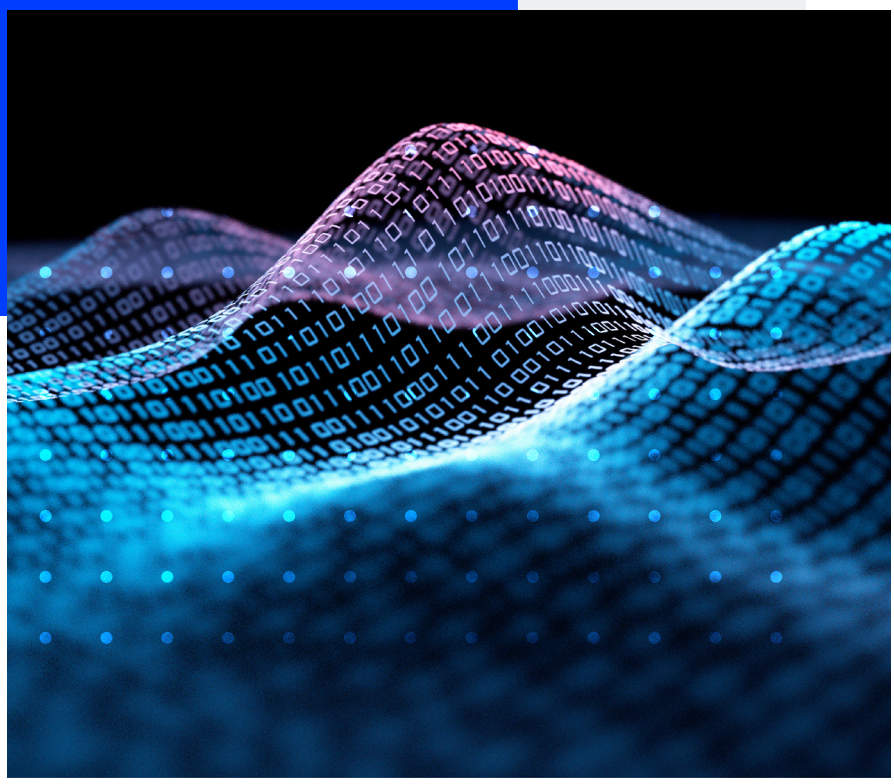
State of the UAE CYBERSECURITY Report

2024

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Table of Contents



1. Foreword

As we step into 2024, the question of whether the cybersecurity landscape will shift significantly from previous years remains prevalent among our stakeholders.

The expansion of Attack Surfaces is a trend set to persist, driven by the increasing complexity and interconnectivity of technologies like cloud computing, operational technology (OT), and artificial intelligence (AI). This evolution offers threat actors more opportunities to infiltrate systems illegally.

Ransomware attacks will continue to make headlines, with the UAE and the broader Middle East region being prime targets. Additionally, we are witnessing a rise in Distributed Denial of Service (DDoS) attacks against UAE organizations, particularly against our critical infrastructure, amid a challenging geopolitical climate that amplifies cyber threats.

It is against this backdrop that I am proud to introduce the State of the UAE Cybersecurity Report. This document offers a comprehensive and accurate analysis of our Nation's cyber threat environment, providing actionable insights and recommendations. With cyber attacks on the rise, it is imperative for the entire ecosystem to engage proactively in reducing the Nation's vulnerability to these threats.

This report not only explores the UAE's cyber attack landscape, common vulnerabilities, and incidents but also delves into the predominant threat trends, groups and their tactics within our borders.

The UAE Cyber Security Council is committed to enhancing societal awareness about the importance and impact of digital threats. Our goal is to foster a robust cyber culture, heighten vigilance against suspicious digital activities, and establish effective deterrence, response, and cybersecurity measures.

Cybersecurity is a concern that transcends local, regional and global boundaries and demands a unified and coordinated response. By remaining vigilant, we collectively form the first line of defence in safeguarding our Nation.

I invite you to engage with this report, which serves as a testament to our dedication to strengthening the UAE's cyber resilience.

Sincerely,

H.E. DR. MOHAMED AL KUWAITI
Head of Cyber Security for the UAE Government

2. Executive Summary

In the dynamic cyber landscape of the United Arab Emirates (UAE), a startling statistic serves as a clarion call to action: the Nation currently hosts at least

155,000 vulnerable assets

with more than

40% of the top vulnerabilities being over five years old.

These vulnerabilities are further exacerbated by threat actors increasingly exploiting such weaknesses remotely, with **Remote Access Technologies** implicated in 23% of these exploitations. This stark reality underlines the urgent need for robust cyber defences in a country at the nexus of technological advancement and geopolitical significance.

As the UAE continues to flourish, integrating cutting-edge technologies such as AI asserting its prominence in regional and international arenas, it becomes an ever-more attractive target for cyber threat actors. This report provides a comprehensive overview of the cyber threats that emerged in 2023, detailing the major trends observed, the primary threat actors involved, the UAE's cyber attack surface, common incidents, and the tactics employed by adversaries to infiltrate organizations.

A significant development in 2023 was the detection by CPX of the North Korean-linked **Lazarus Group** actively engaging in cyber espionage within the UAE. This activity challenges the prevailing belief that the Nation is only targeted by regional adversaries, highlighting the global scale of threats the UAE faces. Additionally, the rise in **Distributed Denial of Service (DDoS)** attacks, driven by groups with political motives such as Anonymous Sudan and Sylhet Gang, signals a trend likely to continue, fueled by the ongoing regional conflicts.

The **Government, Energy, and Information Technology sectors** emerged as the most targeted by cyber threat actors. Despite the evolving threat landscape, traditional attack vectors such as **Business Email Compromise (BEC) and Phishing** remain prevalent, posing a continuous threat. These methods are likely to become more sophisticated with the integration of AI tools, enhancing social engineering efforts, phishing lures, and the deployment of deep-fake technology to deceive victims.

The shift in attack vectors is notable, with a nearly 30% increase in **Insider Threat**-related incidents and an 18% increase in **Drive-by-Downloads,** largely driven by a rise in the use of **Infostealing Malware and Spyware** to acquire organizational credentials. This trend is corroborated by the high occurrence of **malicious code,** accounting for 22% of all cyber incidents in the UAE.

The report emphasizes that while the cyber threat landscape presents a formidable challenge, effective cyber defences based on core cybersecurity principles can mitigate these risks. It advocates for enhanced cyber defensive capabilities through comprehensive threat intelligence, security monitoring, threat hunting, cybersecurity awareness, and timely patch management.

To navigate and mitigate the evolving cyber threats, organizations in the UAE must adopt a strategic, proactive approach to cybersecurity, fostering a culture of vigilance and adaptability. The path forward involves understanding this modern threat, adapting defences accordingly, and collectively strengthening the Nation's cyber defences.

3. Threat Trends

The cyber threat landscape in the UAE remained varied throughout 2023, yet a number of key trends emerged, underscoring specific threats that pose significant risks to the Nation.

Ransomware

Ransomware remains a critical concern in the UAE, with major global ransomware groups intensifying their focus on the region. Notably, CPX identified Lockbit 3.0, Cl0p, and Alphv (also known as Blackcat) as the primary actors, responsible for 51% of the ransomware incidents in the UAE.

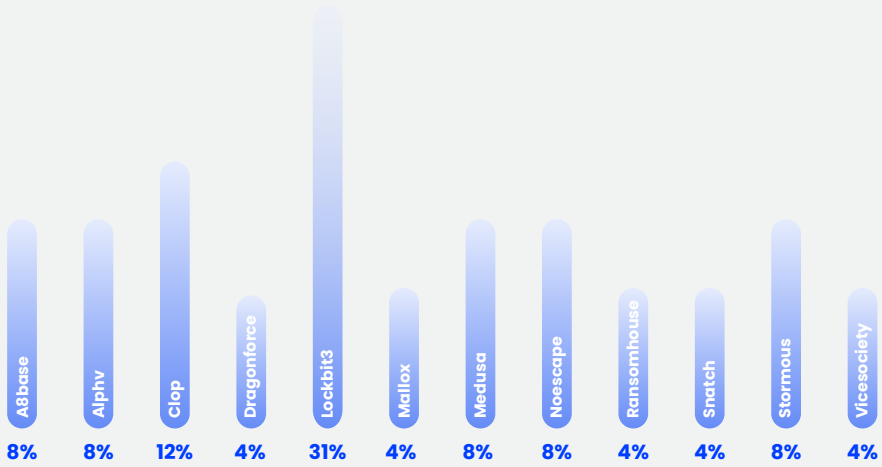


Figure 1: Top Ransomware threat actors – Responsible for Ransomware Incidents – UAE [1]

Data Breach Costs

The financial implications of data breaches in the Middle East, including the UAE, are escalating, with the region recording the second-highest data breach costs globally. A year-on-year increase of 600,000 USD (see Figure 2) highlights the growing economic impact, contrasting with the relatively stable global cost of data breaches. This trend likely reflects the economic prosperity of Gulf economies and the consequent targeting by cyber threat actors aiming to exploit this wealth through data compromise.

Figure 2: Data breach cost (USD) by region – Middle East vs. Global [2]

Distributed Denial of Service (DDoS) Attacks

Distributed denial of service (DDoS) attacks persist as a significant threat to UAE organizations, with an uptick in incidents driven by politically motivated regional hacktivist groups such as Anonymous Sudan. Although the UAE represents only a small fraction (close to 1%[3]) of global DDoS attacks, the characteristics of these attacks—such as their bandwidth and duration—tend to be less severe compared to global averages. This discrepancy suggests a nuanced threat landscape where the intensity of attacks may not always align with global trends.

Total DDoS Attacks	• **58,538 attacks (UAE)** • 7.9 million attacks (Globally)
Max Bandwidth	• **266.9 Gbps peak volume (UAE)** • 605 Gbps peak volume Globally
Average Attack Duration	• **25 minutes (UAE)** • Varies, with longest attack lasting 7 days (Globally)
Top Targeted Industries	• **Telecommunications, Computer Services, (UAE)** • Telecommunications , data hosting (Global)

Figure 3: Distributed Denial of Service statistics – Global vs. UAE [4]

A DDoS attack involved flooding a server with internet traffic to block users from accessing connected online services and sites. [5]

4. UAE Attack Surface

The UAE's attack surface is based on the composition of technologies that comprise the networks of all organizations and networks based within that geographical location. It encompasses all vulnerabilities, entry points, and potential exposures across an organization's network, reflecting the total area or components susceptible to cyber attacks. The concept applies to individual organizations, industrial sectors, or the national level. This section focuses on the collective attack surface of UAE-based organizations.

4.1 UAE Attack Surface Exposure

The UAE hosts nearly **155,000 vulnerable assets** with a significant concentration in Dubai (69.9%), followed by Fujairah (16.6%), Abu Dhabi (9.7%), and Sharjah (2.7%). The remaining 1% are in Ajman (0.6%), Ras al Khaimah (0.3%) and Umm Al Quwain (0.1%)[6]. This distribution underscores the geographical variance in cyber vulnerability within the country.

Top 10 Vulnerable Technology

Remote access and **network vulnerabilities** are prime targets for cyber threat actors, facilitating unauthorized system access without physical network presence. Remote technologies, essential for IT remote system monitoring, managed service providers, IT help desks, and software-as-a-service (SaaS) providers[6], remain a high risk in 2024. Network vulnerabilities, on the other hand, are particularly susceptible to malware attacks, social engineering, and potential misconfiguration[7].

Remote Access 23%	Network Administration 18%	Network Device 15%	File Sharing 10%
Login Page 9%	Network Device Firewall 6%	jQuery 5%	Email 3%
Database 2%	Bootstrap 2%	Other 7%	

Figure 4: Distribution of vulnerabilities recorded in the UAE - 2023[8]

Remote access services, constituting **23%** of attack surface exposures in the UAE, enable attackers to infiltrate an organization's network or systems, potentially leading to financial losses and reputational damage. In addition, Remote Desktop Protocol (RDP) has been shown to be a leading vector for business interruption via ransomware[9].

4. UAE Attack Surface

IT and networking infrastructure exposures, accounting for

39%

of exposures, encompassing application layer protocols and internet-accessible administrative interfaces of routers, firewalls, VPNs, and other core networking and security devices. The compromise of these critical assets can lead to substantial consequences for organizations, including the disruption of core business operations and potential data breaches.

File sharing exposures,

accounting for

10%

of exposures, pose significant risks to organizations, including data breaches. Such compromises allow attackers to access both stored on and future data transmitted through these systems.

Database vulnerabilities,

making up

2%

of exposures, pose a substantial risk when sensitive information is exposed directly to the internet, significantly heightening the likelihood of a data breach with organizations.

Top Vulnerability Types Affecting UAE Organizations

SSL certificate issues dominate the vulnerability types, making up the largest portion at 42% collectively. This typically involves mismatched or misconfigured SSL certificates, facilitating information interception or alteration[10]. Exposed login pages and Oracle forms vulnerabilities are also prevalent, offering unauthenticated access to threat actors[11].

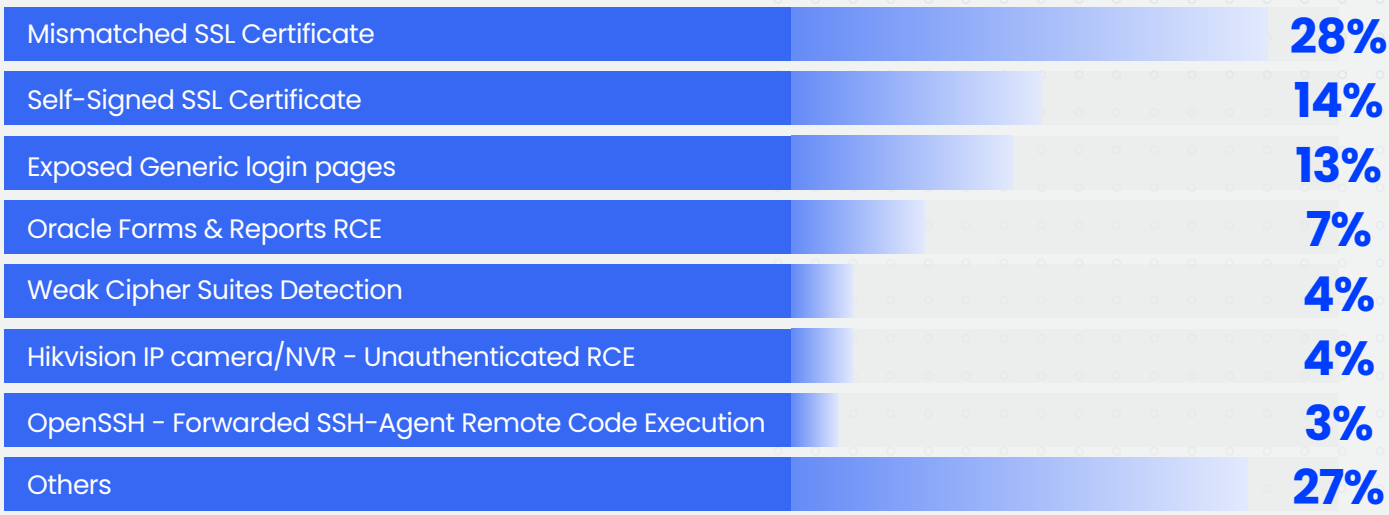


Figure 5: UAE's top observed vulnerabilities by type - 2023[12]

4. UAE Attack Surface

Top 10 Critical Common Vulnerabilities and Exposures (CVEs)

A significant portion of exploited vulnerabilities in the UAE are historic, with many being over five years old. This indicates that vulnerability patch management within UAE-based organizations may not be as up to date as necessary, posing a substantial risk to in-country networks. Notably, 53% of the vulnerabilities identified pertain to an Oracle Form vulnerability, CVE-2021-3153, chosen for its ease of exploitation, which enables an authenticated attacker to extract valuable information from servers, facilitating network reconnaissance. The other predominant vulnerabilities are primarily high-severity remote access issues, granting attackers direct network access. Effective and timely patch management can significantly reduce the risk posed by these vulnerabilities.

CVE	Description	Category	CVSS Score	Public Exploit Exists	
CVE-2012-3153	Oracle Forms & Reports RCE	Remote Code Execute	6.4	✓	53%
CVE-2021-36260	Hikvision IP camera/NVR - Unauthenticated RCE	Remote Code Execute	9.8	✓	32%
CVE-2023-38408	OpenSSH - Forwarded SSH-Agent Remote Code Execution	Remote Code Execute	9.8	✓	10%
CVE-2023-25690	Apache HTTP Server - HTTP Request Splitting With mod_rewrite and mod_proxy	Remote Code Execute	9.8	✓	2%
CVE-2023-28531	OpenSSH - Remote Code Execution	Remote Code Execute	9.8	✗	1%
CVE-2016-1908	OpenSSH - Mishandled untrusted X11 forwarding	Remote Code Execute	9.8	✗	1%
CVE-2020-1938	Apache Tomcat - AJP Request Injection and potential Remote Code Execution	Remote Code Execute	9.8	✓	0.4%
CVE-2023-27997	FortiGate firewalls - Remote Code Execution	Remote Code Execute	9.8	✓	0.3%
CVE-2017-18264	phpMyAdmin - Allow bypass login	Remote Code Execute	9.8	✗	0.2%
CVE-2016-6621	phpMyAdmin - Multiple vulnerabilities in setup script	Remote Code Execute	8.6	✗	0.1%

Figure 6: UAE's top observed vulnerabilities by assigned CVE number - 2023[13]

***The Common Vulnerability Scoring System (CVSS) provides a qualitative way of scoring the severity of a vulnerability and is the industry standard first developed and managed by FIRST.org*[14]**

4. UAE Attack Surface

Top 5 Most Abused Protocols

Protocols are fundamental for data transfer, with threat actors exploiting various protocols depending on their attack strategy. In the UAE, HTTP is the most abused protocol, attributed to unencrypted data transfer, allowing threat actors greater opportunities to intercept data from vulnerable servers.

HTTP	SSH	SNMP	IKE	RTSP
Instances	Instances	Instances	Instances	Instances
486,570	43,960	33,540	23,320	13,670

Figure 7: UAE's top 5 abused protocols by count - 2023[15]

5. Common Incident Types

In 2023, the Security Operations Centre (SOC) of CPX encountered a diverse array of incidents across various client environments. These incidents were classified into seven distinct categories, with their severity assessed according to the scale defined by the UAE's Computer Emergency Response Team (aeCERT).

Malicious code

Malicious code was notably prevalent, comprising 22% of all incidents. This highlights the increasing complexity of malware attacks and the critical need for advanced detection and response mechanisms. Additionally, incidents categorized as Scans/Probes/Attempted Access and Unauthorized Access together accounted for over 30% of cases, marking a significant portion of the threat landscape.

Email Fraud and Phishing

Email Fraud and Phishing though not the most dominant, made up a considerable 10% of the total incidents. This highlights the ongoing relevance of user awareness and training in mitigating such socially engineered threats. The relatively lower occurrence of Web Application Attacks may indicate the effectiveness of existing security protocols or suggest a strategic shift by attackers to exploit more susceptible vectors.

Misconfiguration

Notably, the most frequent category of incidents was **Misconfiguration**, representing 27% of the total. Misconfigurations, which involve devices being set up incorrectly, are critical to address in order to optimize network detection capabilities. While these incidents are not inherently malicious, they highlight areas where security adjustments are necessary to enhance overall protection.

5. Common Incident Types

5.1 Incidents by Type

27%

Misconfiguration
Requests to reconfigure security policies and/or rules to reduce false positives, or to tune content to realign with the objectives, fall in this category. It also includes any device configured improperly that requires remediation

22%

Malicious Code
Successful installation of malicious code—such as viruses, worms, Trojan horses, or other code-based malicious entities—that infects an operating system or application

15%

Scans/Probes/Attempted Access
Activities aimed at identifying or accessing a computer, open ports, protocols, services, or any combination thereof for later exploitation

15%

Unauthorized Access
Any incident where an individual gains logical or physical access without permission to a network, system, application, data, or other resources

10%

Email Fraud/Phishing
Includes any form of email fraud, including phishing and spoofing, whether reported by an entity or discovered by the Incident Response team

10%

Improper Usage and Unlawful Activity
Violation of organizational policies, including inappropriate and/or illegal activities

1%

Web Application Attacks
Vulnerabilities in an entity's operating systems and web applications

Figure 8: Incident breakdown by type – CPX SOC data - 2023

5.2 Incident by Severity

The classification of incidents by severity reveals a significant concentration of cases classified as critical, high, or medium, collectively accounting for **85% of all incidents.** This distribution suggests that the majority of incidents pose a significant risk to business operations, potentially impacting them for an extended period of time.

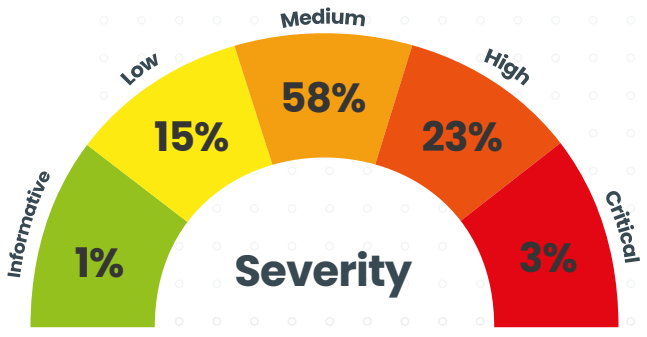


Figure 9: Incident breakdown by severity– CPX SOC data - 2023

5. Common Incident Types

5.3 Threat Hunting Insights

CPX's Threat Hunting team engages in proactive searches for hidden threats within client networks, leveraging the latest cyber threat intelligence and focusing on the most current tactics, techniques, and procedures (TTPs) of threat actors. Throughout 2023, their investigations across client environments yielded several noteworthy insights.

Incidents Observed During Threat Hunting Operations

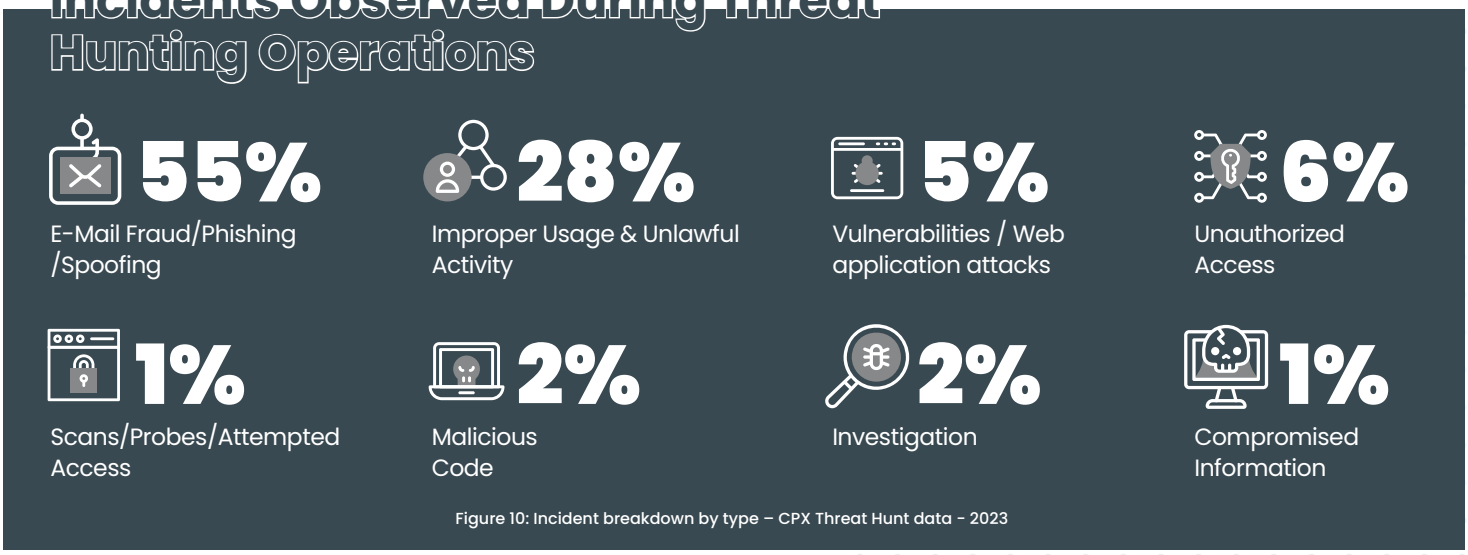


Figure 10: Incident breakdown by type – CPX Threat Hunt data - 2023

Email-based attacks, particularly phishing and business email compromise (BEC), are identified as significant threats, comprising 55% of total incidents, often involving sophisticated social engineering tactics to deceive victims into unwittingly disclosing sensitive information or credentials. CPX anticipates that such email-based attacks will continue to be prevalent in 2024, with an expected increase in the use of AI-specific tools by threat actors. These tools are likely to enhance phishing attempts and facilitate more advanced social engineering attacks, including the use of deep-fake technology.

Business Email Compromise (BEC)

The CPX Threat Hunting Team has identified several campaigns involving BEC, a sophisticated form of cyber fraud. In BEC attacks, threat actors gain access to a business email account and impersonate the account owner to defraud the company, its employees, customers, or partners. These attacks often involve sending spear-phishing emails using hijacked email threads and creating typo-squatted domains—a technique known as email thread hijacking (Mitre ATT&CK Technique: T1566)[16]. This method proves significantly more effective than broader, untargeted approaches. The CPX team observed these attacks being primarily used for cyber espionage, with a notable focus on the financial sector, indicating a targeted approach towards organizations with substantial financial assets or information.

5. Common Incident Types

Distributed Denial of Service (DDoS) Attacks

The CPX Threat Hunting team also observed a surge in DDoS attacks, particularly from the hacktivist group Anonymous Sudan. This group has launched attacks against a number of UAE-based organizations, especially within the Banking, Utilities and Government sectors. These observations align with an overall increase in regional hacktivist activity against UAE organizations, as well as a general uptick in DDoS attacks targeting entities within the country. Such attacks disrupt services and operations, posing significant threat to the stability and security of critical infrastructure and financial services, underscoring the need for enhanced defensive measures against these common cyber threats.

Attack Vector (MITRE ATT&CK) observed Network Denial of Service (T1498)[17]

Threat Actor Intent Disrupt Network Traffic

Target Industries

Banking Utilities Government

6. Key Attack Insights

The section aims to dissect the methodologies employed by threat actors to breach or infiltrate a victim's network, based on incidents handled by the CPX Incident Response Team.

6.1 Threat Vector Highlights

The year 2023 witnessed a significant shift in the tactics of threat actors, with a nearly

30%

increase in insider threat incidents.

18%

increase in drive-by-downloads.

Conversely, the exploitation of public-facing assets saw a reduction by more than half, from 44% in 2022 to 21% in 2023.

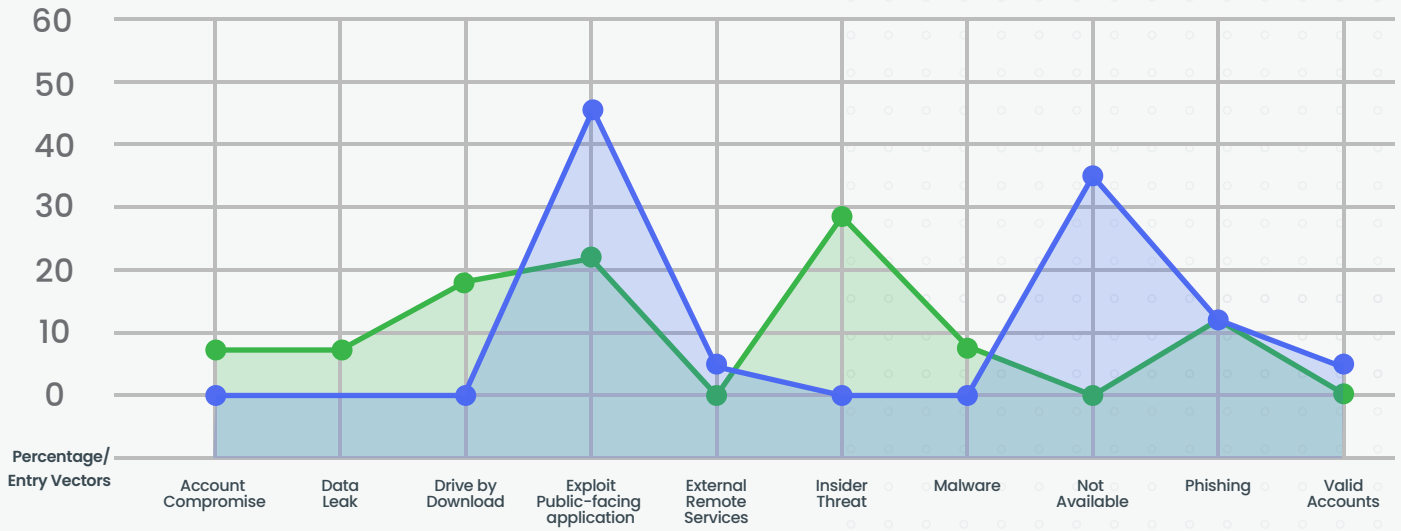


Figure 11: Observed entry vectors – CPX IR Data - 2023

In malware delivery methods, there was a notable 36% increase in malware directly installed on a victim's machine, primarily through drive-by-downloads. This occurs when a victim unknowingly downloads a malicious file through a deceptive link, application, or bundled within legitimate software. This contrasts with a 37% decrease in remote injection attacks.

Malware Delivery Vector

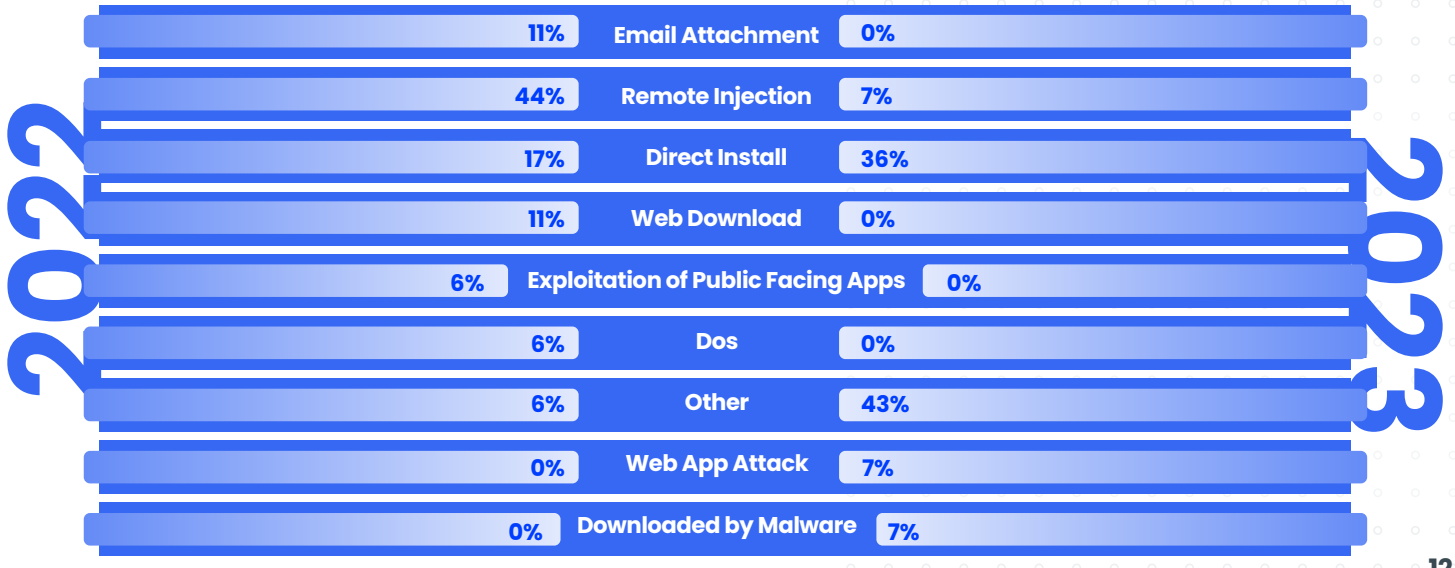


Figure 12: Malware delivery vectors – CPX IR Data - 2023

6. Key Attack Insights

Incidents by Industry

CPX's incident response activities across the UAE have revealed a targeting preference towards the Defence, Energy, Government, and Information Technology sectors.

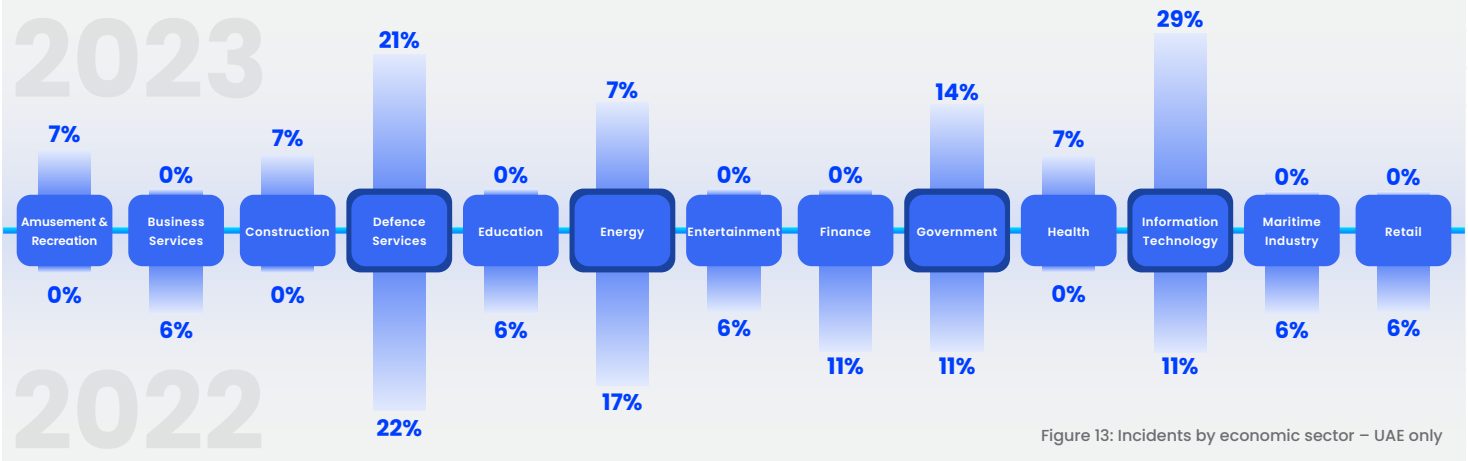


Figure 13: Incidents by economic sector – UAE only

QR Code Phishing – Social Engineering

QR Code phishing campaigns have been notably targeting UAE organizations, often impersonating Microsoft 365. This tactic has gained traction as businesses increasingly adopt cloud-based services, with stolen credentials being used to access email and VPN services with the intent to access, abuse, and exfiltrate critical data and information.

Exploitation of Public-facing Applications

There has been observed exploitation of both N-day and Zero-day vulnerabilities in public-facing applications, with attacks often commencing immediately after the disclosure of proof-of-concept (PoC) exploit code. Major vulnerabilities exploited include Confluence CVE-2023-22515, the 5-year-old Telerik UI CVE-2019-18935, and brute force attempts against exchange servers using stolen Global Address List (GAL).

Infostealers

The rise of infostealers in the UAE highlights a growing trend of trojan malware designed to harvest information from a victim's system, including usernames and passwords.

Drive-by-Download

Drive by downloads pose a significant threat, as victims inadvertently download malicious code through phishing emails or by interacting with malicious URLs. This code can trigger the download of additional executables, compromising the victim's personal or professional accounts and allowing unauthorized access to their network.

6. Key Attack Insights

6.2 Profile of Threat Actors Targeting the UAE

The UAE faces a diverse array of cyber threat actors, each with distinct motivations and methodologies. These range from nation-state threat actors, eCrime groups, to hacktivists. Nation-state actors are typically motivated by espionage or destructive purposes, investing significant time, money, and manpower to compromise specific targets. eCrime actors, on the other hand, are driven primarily by profit. These actors seek organizations with weak defences to quickly exploit and monetize data. Hacktivists are motivated by political beliefs, often targeting organizations aligned against their ideologies, though they may lack the technical knowledge to conduct sophisticated network intrusions.

29%
eCrime

36%
Unattributed

14%
Nation State

21%
Insider Threat

Figure 14: Attributed threat actors by type – CPX IR data - 2023

Time Until a Threat Actor is Discovered (Dwell Time)

Threat actors can remain within a victim's network for extended periods, seeking valuable information for later exfiltration. They often move laterally across the network undetected in search of sensitive information.

CPX's observations indicate that the majority of threat actors remain undetected for days or weeks, accounting for 93% of incidents. Notably, incidents remaining undiscovered for up to a month decreased by 33% year-on-year, suggesting improvements in detection times, likely due to enhanced detection tools and methodologies.

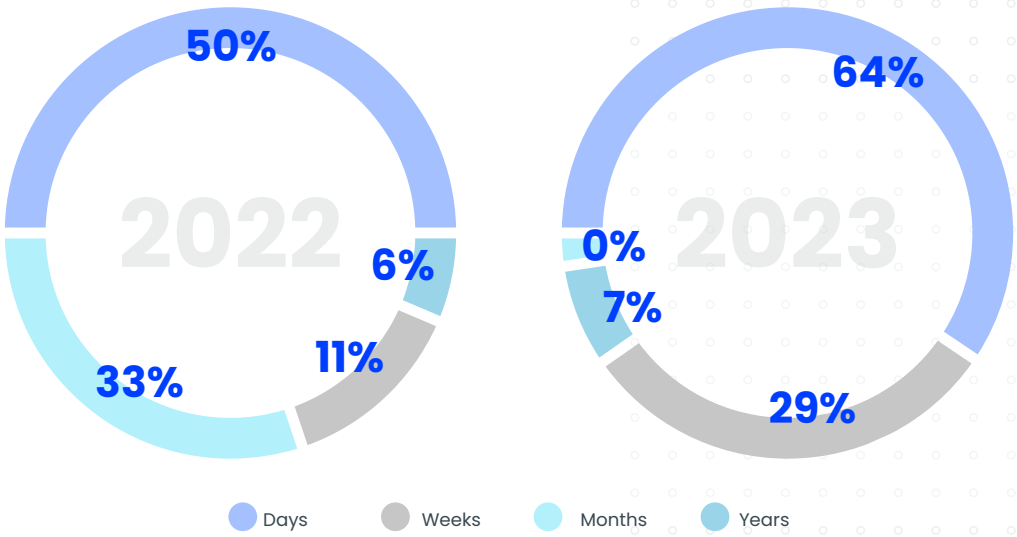


Figure 15: Dwell time – Time from initial entry to detection – CPX IR data - 2023

6. Key Attack Insights

Size of Organizations Being Targeted

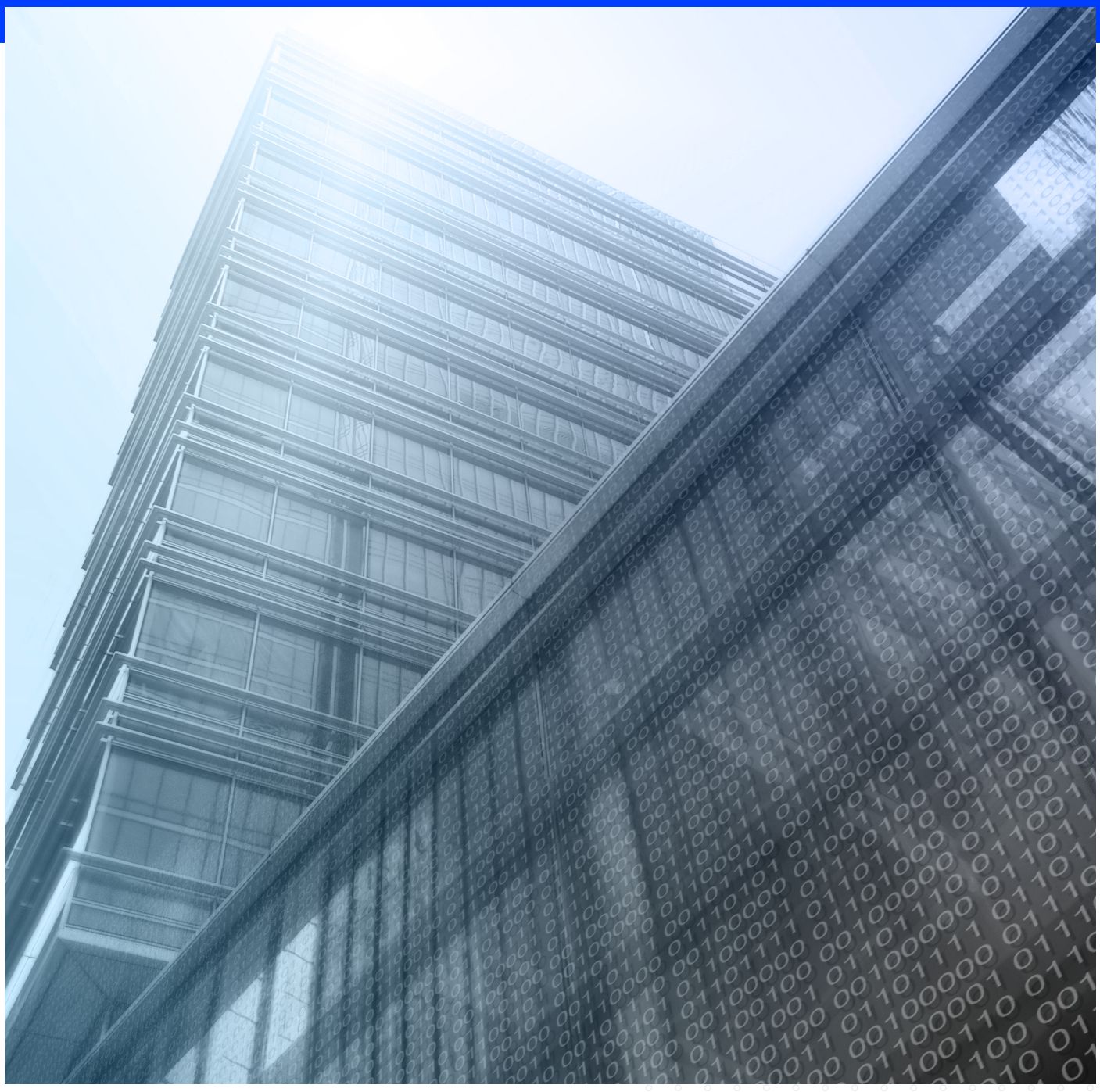
The majority of incidents, 86%, targeted large organizations within the UAE. Nation-state actors often pursue large organizations for cyber espionage, aiming to extract proprietary or politically sensitive information. Conversely, eCrime threat actors target large organizations for their perceived ability to pay ransoms or the potential market value of stolen data on the deep and dark web (DDW).

Organization Size

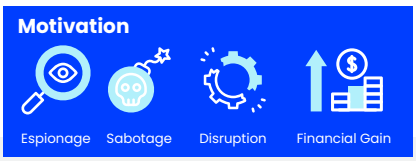
86% Large Organizations

14% Small Organizations

Figure 16: Incident victims by organization size– CPX IR data - 2023



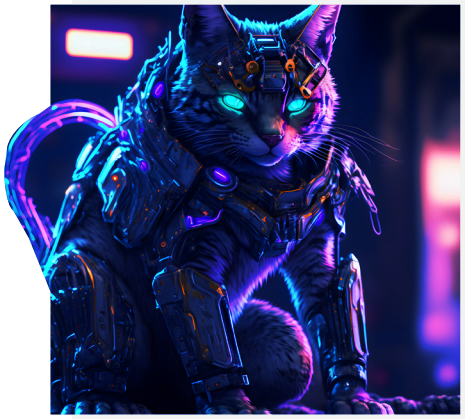
7. Threat Groups



The CPX Threat Intelligence Centre has meticulously analyzed the landscape of cyber threats, including major trends, motivations, and tools, techniques and procedures (TTPs). The investigations have led to the identification and profiling of several prominent threat actor groups, including nation-state actors, ransomware operators, and hacktivist groups. This analysis aims to provide organizations with actionable insights to enhance their security posture against threats pertinent to their specific industry.

7.1 Nation-state

Nation-state threat actors operate under the direction of their respective governments, often with ties to military or state security apparatus. They are typically supported by government funding, manpower, technical expertise, and operational assistance.



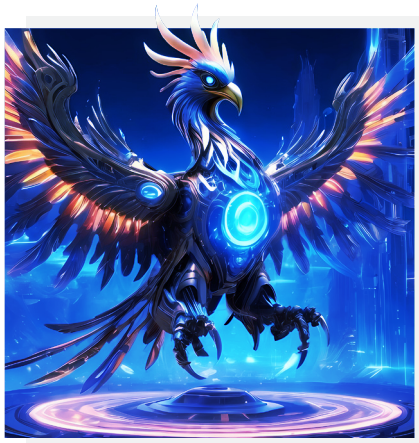
APT34

is a cyber-espionage threat actor linked to Iran, and has been active since 2014. The group primarily engages in phishing operations to advance Iranian national interests.

Aliases Oilrig, Crambus, Helix Kitten, Lyceum, Chrysene

Target Sectors

TTPs - Utilizes phishing emails, exploits known vulnerabilities, executes malicious macros to deliver payloads, and continuously updates and retools payloads to avoid detection[18]



Lazarus Group

associated with Reconnaissance General Bureau (RGB), DPRK (North Korea), and has been active since 2009. The group engages in sabotage and disruption to serve the political and national security interests of North Korea.

Aliases Hidden Cobra, TEMP.Hermit, Bluenoroff, Sapphire Sleet, LABYRINTH CHOLLIMA

Target Sectors

TTPs - Spear-phishing, supply-chain attacks, waterhole attacks, zero-day vulnerability exploitation, and maintains persistence using custom-built tools[19]

Muddy Water

is a cyber-espionage threat actor linked to the Iranian Ministry of Intelligence & Services (MOIS) and has been active since 2017. The group conducts surveillance and collects strategic information to support Iranian interests and decision-making.

Aliases Static Kitten, Earth Vetala, UNC313, Temp.Zagros, Seedworm

Target Sectors

TTPs - Initiates spear-phishing emails containing malicious documents, employs PowerShell-based malware, and uses publicly available offensive security tools and legitimate remote access software[20]

7. Threat Groups

7.2 eCrime

Motivation

Financial Gain

eCrime threat actors are primarily motivated by financial gain, often targeting organizations with vulnerable network defences to access networks or data. Their goal is typically to sell stolen data on the DDW or to ransom it back to the victim organization.

LockBit

is a cybercriminal group, possibly linked to Russia and active since September 2019. The group operates under the Ransomware-as-a-Service (RaaS) model, targeting multiple platforms including Windows, Linux, macOS and VMware.

Aliases Bitwise Spider, LockBit 3.0, LockBit Black, LockBitSupp

Target Sectors

Automobile, Oil & Gas, Healthcare, Manufacturing, Government, Law & Judiciary, Financial

TTPs – Utilizes spear-phishing, initial access brokers (IAB), insider recruitment, double extortion tactics, and maintains persistence with custom-built tools[21]

Cl0p

is a cybercriminal group, possibly linked to Russia and active since February 2019. Cl0p functions as a Ransomware-as-a-Service (RaaS).

Aliases TA505, FIN11, FIN7

Target Sectors

Construction, Financial, Logistics, Marine & Offshore services, Manufacturing

TTPs – Spear-phishing, supply-chain attacks, waterhole attacks, zero-day vulnerability exploitation, and maintains persistence using custom-built tools[22]

ALPHV

is a cybercriminal group, possibly linked to Russia and active since November 2021. The group is identified as a possible successor to REvil, BlackMatter and Darkside, operating as a Ransomware-as-a-Service (RaaS).

Aliases Blackcat, AlphaVM, NOBERUS, UNC4466

Target Sectors

Defence, Financial, Energy, Healthcare, IT Services, Construction

TTPs – Utilizes spear-phishing, exploits known vulnerabilities, gains initial access via Botnet, uses Cobalt Strike for intrusion, and employs Triple Extortion including DDoS attacks[23]

7. Threat Groups

Motivation

Religious Political

7.3 Hacktivists

Hacktivists are politically motivated hackers forming loose collectives, targeting organizations that oppose their political beliefs.

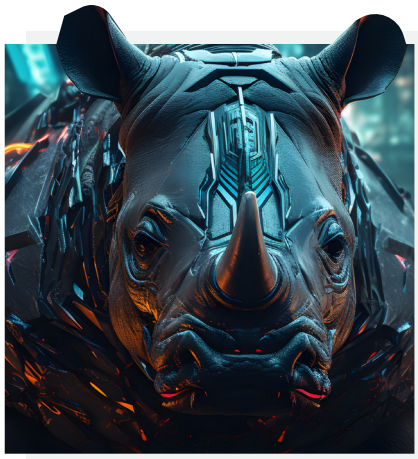
Anonymous Sudan

is a hacktivist group that has been active since early 2023. The group is motivated by religious and political beliefs, focusing on DDoS and Defacement attacks against their victims.

Aliases Anonymous Sudan Chat

Target Sectors Financial, Government, Aviation, Media, Technology, Construction

TTPs - Engages in DDoS attacks, website defacement, and DDoS-as-a-Service[24]



Sylhet Gang

is a hacktivist group possibly linked to Bangladesh, and active since 2023. Influenced by religious and political beliefs, they conduct DDoS attacks related to geopolitical events.

Aliases Sylhet Gang-SG

Target Sectors Financial, Government, Aviation, Travel, Defence, Media

TTPs - Spear-phishing, supply-chain attacks, waterhole attacks, zero-day vulnerability exploitation, and maintains persistence using custom-built tools[25]

1915 Team

is a hacktivist group, possibly linked to the Middle East region and active since January 2023. They are driven by religious and political beliefs, and conduct DDoS attacks.

Aliases N/A

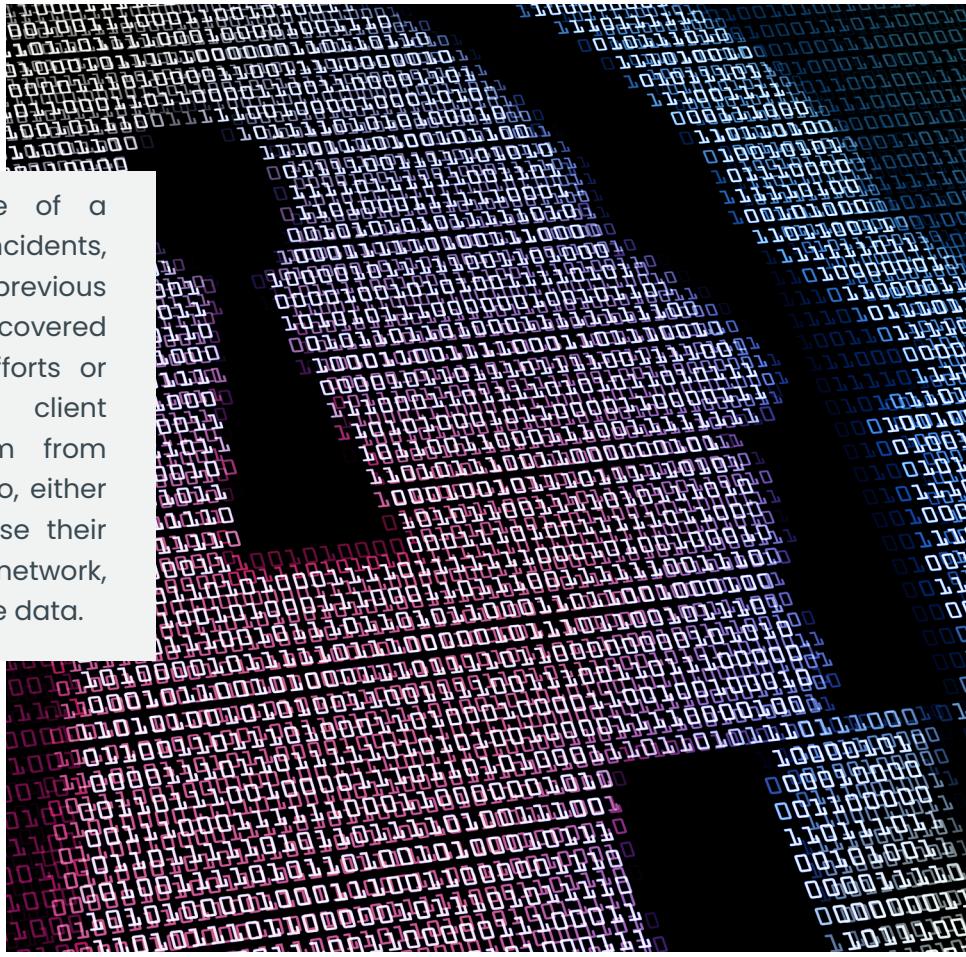
Target Sectors Government, Transport

TTPs - Conducts DDoS attacks and website defacement[26]

7. Threat Groups

7.4 Insider Threat

In 2023, observations were made of a significant increase in insider threat incidents, with a fourfold rise compared to previous years. These incidents were often uncovered through direct incident response efforts or threat hunting activities within client environments. Insider threats stem from individuals within an organization who, either through malice or negligence, misuse their access within the organization's network, leading to the compromise of sensitive data.



7.5 Threat Actor Spotlight: Lazarus Group

The Lazarus Group, linked to North Korea, conducted one of the most sophisticated attacks observed by CPX, targeting a specific client in the UAE. This attack was dubbed "Operation DreamJob," a campaign initially identified in 2019 by researchers from Japan CERT[27] , ClearSky[28] and NCC Group[29], and later observed by Kaspersky[30] in Eastern Europe, South Korea and Russia. The campaign's breadth and duration underscore Lazarus Group's strategic objectives and their focus on cyber espionage to gather intelligence and sensitive data from high-profile organizations. This effort is aimed at enhancing North Korea's technical and scientific capabilities.

Target Industries	Defence
Attack Vector (MITRE ATT&CK)	•T1059 - Command and Scripting Interpreter •T1574 – Hijack Execution Flow •T1053 - Scheduled Task/Job •T1027 - Obfuscated Files or Information •T1573 – Encrypted Channel
Intent	Espionage
Malicious Tools	Custom malware

8. Recommendations

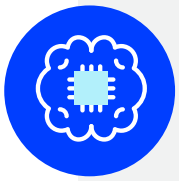
Following an extensive evaluation of digital assets in the UAE, cyber defence experts offer crucial recommendations to enhance the security posture of organizations urgently:

Implement Endpoint Detection & Response (EDR)

Deploy EDR tools to record all process-level activity on systems, enabling security analysts or threat hunters to identify compromises effectively and maintain historical process execution records.

Implement Security Operations Centre Capability

Establish a 24/7 Security Operations Centre (SOC) for continuous monitoring and analysis of the organization's security posture, focusing on networks, servers, endpoints, databases, applications, websites, and other systems for potential security incidents.



Understand Cyber Attackers Utilizing Cyber Threat Intelligence

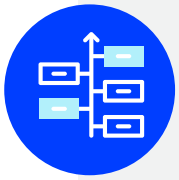
Develop an effective cyber threat intelligence function to systematically monitor specific external threats, providing vital intelligence on new and emerging threats, thereby allowing real-time security posture adjustments.

Implement Incident Response Plan and Procedures

Without fail, create and implement an incident response plan based on industry standards, supported by playbooks for a wide variety of scenarios including insider threats, ransomware, and phishing.

Implement Threat Hunting Capability

Adopt proactive threat hunting processes to search networks for threats that bypass existing security solutions, using host, network, and appliance logs. Threat hunting seeks to identify outliers within the logs collected by these systems, by identifying anomalies, validating hypotheses and improving overall detection mechanisms.



Implement Regular Cybersecurity Audits and Compliance Checks

Conduct regular cybersecurity audits and compliance checks to ensure alignment with international standards and best practices, maintaining the integrity of critical infrastructure and essential services in the UAE.

Implement the Usage of Multi Factor Authentication (MFA)

Utilize MFA for authenticating exposed services, strengthen systems and password policies, deploy a Web Application Firewall where necessary, assess cloud security configurations, and review infrastructure and development tools.

Create an Asset Inventory

Maintain comprehensive asset inventories to understand the architecture topology, applications, and active accounts in the environment. This helps to identify network anomalies and threats missed by traditional defences.

Integrate with the National Cyber Security Operations Centre (NSOC)

Collaborate with the National Cyber Security Operations Centre to leverage collective monitoring capabilities, share cyber threat intelligence, gain awareness on the latest vulnerabilities, and benefit from collective response strategies in case of significant cyber incidents.

9. Conclusion

As the UAE continues to experience rapid economic growth, it concurrently faces an escalating and diversifying cyber threat landscape. This environment is characterized by sophisticated cyber threats from a broad spectrum of actors, including nation-states, eCrime syndicates, insider threats, and politically motivated hacktivists. These adversaries, though varied in their motivations, share a common goal: to infiltrate organizational networks and compromise sensitive data.

The UAE is confronted with an array of attack methodologies, from exploiting vulnerabilities and deploying malware to executing ransomware and DDoS attacks. In response to these challenges, it is imperative for organizations to not only understand the nature of these threats but also adapt their defences to pre-emptively counteract the dynamic tactics employed by these threat actors.

Looking forward, it is likely that DDoS attacks will increase, fuelled by the ongoing geopolitical tensions in the region. Similarly, the market for leaked credentials is expected to trigger a rise in ransomware attacks. This rise is fuelled by access brokers monetizing unauthorized access on the DDW. Moreover, the advancement and adoption of AI-specific tools are likely to make spear-phishing attempts more sophisticated, alongside traditional methods of gaining network access through vulnerable systems and remote access technologies.

To navigate this complex threat environment, UAE organizations must establish comprehensive cybersecurity programs that extend beyond technical defences to include awareness campaigns. These initiatives should aim to educate employees on the potential cyber threats they face, encouraging vigilance and prompt reporting of suspicious activities. The battle against cyber threats is not solely technological, but profoundly human as well. The cultivation of a well-informed workforce—comprising employees, citizens, and cybersecurity professionals—equipped with the knowledge to identify and mitigate threats before they materialize, is crucial.

Ultimately, a holistic approach that combines technical acumen with human insight represents the most effective strategy for safeguarding against the multifaceted cyber threats confronting the UAE.

References

1. https://ransomfeed.it
2. https://www.ibm.com/reports/data-breach
3. https://www.netscout.com/threatreport/emea/united-arab-emirates
4. https://www.netscout.com/threatreport/emea/united-arab-emirates
5. https://www.fortinet.com/resources/cyberglossary/ddos-attack#:~:text=DDoS%20Attack%20means%20%22Distributed%20Denial,connected%20online%20services%20and%20sites.
   https://spidersilk.com/
6. https://www.cisa.gov/sites/default/files/2023-06/Guide%20to%20Securing%20Remote%20Access%20Software_clean%20Final_508c.pdf
7. https://purplesec.us/common-network-vulnerabilities/#:~:text=A%20network%20vulnerability%20is%20a,typically%20involve%20software%20or%20data.
8. Censys.io
9. https://www.paloaltonetworks.com/resources/research/2023-unit-42-attack-surface-threat-report.
10. https://www.encryptionconsulting.com/education-center/ssl-attacks/#:~:text=SSL%20Stripping%20attacks&text=Usually%2C%20the%20end%2Duser%20connects,response%20back%20to%20the%20user.
11. https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-5102/Oracle-Forms.html#:~:text=Easily%20exploitable%20vulnerability%20allows%20unauthenticated,may%20significantly%20impact%20additional%20products.
12. https://spidersilk.com/
13. https://spidersilk.com/
14. https://www.first.org/cvss/
15. https://censys.io
16. https://attack.mitre.org/techniques/T1566/
17. https://attack.mitre.org/techniques/T1498/
18. https://www.eset.com/int/about/newsroom/press-releases/research/iran-linked-oilrig-attacks-israeli-organizations-with-cloud-service-powered-downloaders-eset-research-discovers/
    https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/crambus-middle-east-government
    https://www.trendmicro.com/en_us/research/23/i/apt34-deploys-phishing-attack-with-new-malware.html
    https://nsfocusglobal.com/apt34-unleashes-new-wave-of-phishing-attack-with-variant-of-sidetwist-trojan
    https://www.darkreading.com/cyberattacks-data-breaches/iran-apt34-uae-supply-chain-attack
    https://web.archive.org/web/20230524192649/https://www.fortinet.com/blog/threat-research/operation-total-exchange-backdoor-discovered
    https://www.trendmicro.com/en_za/research/23/b/new-apt34-malware-targets-the-middle-east.html
    https://attack.mitre.org/groups/G0049/
19. https://labs.withsecure.com/publications/no-pineapple-dprk-targeting-of-medical-research-and-technology-sector
    https://www.mandiant.com/resources/blog/lightshow-north-korea-unc2970
    https://securelist.com/the-lazarus-group-deathnote-campaign/109490/
    https://asec.ahnlab.com/en/53132/
    https://mp.weixin.qq.com/s?__biz=MzUyMjk4NzExMA%3D%3D&mid=2247492789&idx=1&sn=a991e6c5ed7388515d75f02e9c33428f
    https://blog.talosintelligence.com/lazarus-quiterat/
    https://web.archive.org/web/20240107002507/https://www.welivesecurity.com/en/eset-research/lazarus-luring-employees-trojanized-coding-challenges-case-spanish-aerospace-company/
    https://asec.ahnlab.com/en/57736/
    https://www.microsoft.com/en-us/security/blog/2023/11/22/diamond-sleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/
    https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/
    https://attack.mitre.org/groups/G0032/
20. https://www.eset.com/fileadmin/ESET/INT/B2B_Resource_centrum/Reports/Q4-2022-Q1-2023_APT-Activity-Report.pdf
    https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/
    https://www.bleepingcomputer.com/news/security/microsoft-iranian-hacking-groups-join-papercut-attack-spree/
    https://www.deepinstinct.com/blog/phonyc2-revealing-a-new-malicious-command-control-framework-by-muddywater
    https://www.deepinstinct.com/blog/muddywater-en-able-spear-phishing-with-new-ttps
    https://www.deepinstinct.com/blog/muddyc2go-latest-c2-framework-used-by-iranian-apt-muddywater-spotted-in-israel
    https://attack.mitre.org/groups/G0069/
21. https://ransomfeed.it/stats.php?page=country-list&country=UAE&y=0
    https://attack.mitre.org/groups/G0092/
22. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/
    https://www.sentinelone.com/labs/cl0p-ransomware-targets-linux-systems-with-flawed-encryption-decryptor-available/
    https://thehackernews.com/2023/05/notorious-cyber-gang-fin7-returns-cl0p.html https://twitter.com/MsftSecIntel/status/1659347799442432002
    https://www.kroll.com/en/insights/publications/cyber/sysaid-vulnerability-cve-2023-47246
    https://attack.mitre.org/software/S0611/
23. https://www.mandiant.com/resources/blog/alphv-ransomware-backup
    https://www.trendmicro.com/en_se/research/23/f/malvertising-used-as-entry-vector-for-blackcat-actors-also-lever.html
    https://attack.mitre.org/groups/G0049/
    https://www.bleepingcomputer.com/news/security/alphv-ransomware-adds-data-leak-api-in-new-extortion-strategy/
    https://vulnera.com/newswire/new-blackcat-ransomware-variant-incorporates-advanced-impacket-and-remcom-tools/
    https://www.bleepingcomputer.com/news/security/blackcat-ransomware-uses-new-munchkin-linux-vm-in-stealthy-attacks/
    https://attack.mitre.org/software/S1068/
24. https://socradar.io/dark-web-profile-killnet-anonymous-sudan/
    hxxps://t.me/xAnonymousSudan
25. hxxps://t.me/SylhetGangsgOfficial
26. hxxps://t.me/z1915x
27. https://blogs.jpcert.or.jp/en/2021/01/Lazarus_malware2.html
28. https://www.clearskysec.com/operation-dream-job
29. https://research.nccgroup.com/2022/05/05/north-koreas-lazarus-and-their-initial-access-trade-craft-using-social-media-and-social-engineering/
30. https://securelist.com/the-lazarus-group-deathnote-campaign/109490/

ABOUT

The UAE Cyber Security Council
The Cabinet of the UAE formed the Cybersecurity Council in 2020 to support the UAE's commitment to achieving a safer digital transformation. It is headed by H.E. Dr. Mohamed Al Kuwaiti and comprises a variety of federal and municipal authorities in the UAE. The Council is tasked with developing legislative and regulatory frameworks that address various issues, including cybersecurity and cybercrime, as well as securing present and upcoming technologies.

Learn more at www.csc.gov.ae

CPX, headquartered in Abu Dhabi, is a leading provider of digital-first cybersecurity solutions and services. Established in 2022, CPX protects public- and private-sector organizations with customized solutions that reduce the risk of sophisticated cyberattacks. We provide clients and partners with end-to-end cybersecurity capabilities to ensure compliance with stringent cybersecurity standards and accelerate their cyber maturity.

Learn more at www.cpx.net
Contact us: contactus@cpx.net