مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

State of the UAE CYBERSECURITY Report

2025

Table of Contents

1. Foreword

The UAE has long recognized the critical role of cybersecurity in safeguarding our national security, economic stability, and digital future. Through proactive measures, such as the establishment of the National Cybersecurity Strategy and key partnerships with international stakeholders, we have laid a strong foundation for a safer digital ecosystem.

2024 was a milestone year for the UAE—we ranked at the top of the "Pioneering Model" category in the Global Cybersecurity Index (GCI). This recognition is a testament to our forward-thinking strategies, robust policies, and the collaboration of public and private sectors in protecting our digital infrastructure.

Last year, the **State of the UAE Cybersecurity Report 2024** highlighted the rising security threats faced by organizations across the UAE. The report spurred swift action, prompting significant advancements across various fronts.

Today, I am proud to say we have made significant strides. From launching key national initiatives to fostering a culture of cybersecurity awareness, our progress reflects our resilience and determination. However, as we stand on the cusp of a new era powered by emerging technologies, we recognize that the journey is far from over. The rise in AI-driven attacks and widening cyber capabilities demands stricter vigilance and innovation to secure the future.

This year's report takes a deeper dive into the evolving threat landscape, providing a comprehensive analysis of the UAE threat landscape and recommendations. As we look ahead, our priorities include harnessing advanced technologies, fostering greater public-private collaboration, and ensuring that cybersecurity becomes an intrinsic part of every digital initiative.

The path forward requires collective efforts, innovation, and commitment. Together, we will continue building a secure and prosperous digital UAE—one where innovation flourishes, opportunities thrive, and our systems remain resilient in the face of any challenge.

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

2. Message from the CEO

Hadi Anwar

Chief Executive Officer, CPX

As we move forward in an era of rapid digital innovation, cybersecurity has become a critical priority for every organization and nation. While the digital world offers incredible opportunities for growth and transformation, it also presents evolving threats that require immediate action, careful planning, and strong collaboration.

At CPX, our mission is to empower organizations with the knowledge, tools, and strategies they need to navigate these challenges effectively. By strengthening defenses, fostering public-private partnerships, and embracing innovation, we aim to help businesses and governments build a more secure future.

This report offers a comprehensive view of the UAE's cybersecurity landscape. It delves into the strategies, policies, and innovations that are shaping the nation's digital transformation while addressing the complexities of protecting critical infrastructure and sensitive data. The UAE's remarkable progress in cybersecurity reflects a commitment to creating a secure environment where digital advancements and national resilience go hand in hand.

Whether you're a business leader, policymaker, or technology enthusiast, this report provides valuable insights into the UAE's cybersecurity landscape and offers actionable recommendations to prepare for the future.

I would like to express my sincere gratitude to the UAE government, the Cyber Security Council, and the dedicated teams at CPX for their collaborative efforts in advancing our shared vision for a secure digital ecosystem.

With confidence in the path ahead, we remain committed to building a resilient and innovative digital UAE. Together, let us rise to the challenge, united in purpose and vision, and create a future that generations can trust and thrive in.

3. Executive Summary

The UAE's cyber landscape is evolving rapidly, but a concerning statistic highlights the urgent need for stronger cybersecurity: the nation hosts **~223,800 digital assets** and half of the top vulnerabilities are over five years old. These outdated vulnerabilities are increasingly being exploited by threat actors, emphasizing the need for robust cyber defenses in a country that is at the forefront of technological progress and geopolitical importance.

As the UAE continues to embrace innovative technologies like artificial intelligence (AI), it's also becoming a more appealing target for cyber threats. This report offers an in-depth examination of the top cyber threats that surfaced in 2024, focusing on emerging trends, the most active threat actors, key incidents, and the strategies attackers are using to exploit vulnerabilities.

CPX made a notable discovery this year regarding the Iranian-affiliated group APT39 engaging in cyber espionage activities targeting the UAE. Additionally, significant Iranian activity was observed by other groups such as Pulsar Kitten and Muddy Water, highlighting the nation's complex and challenging security environment.

eCrime remains a significant threat, in terms of the number of confirmed incidents, with ransomware gangs such as LockBit, DarkVault, and RansomHub being the most prevalent attacking organizations. However, the number of overall ransomware groups active in the UAE increased by 58 percent in 2024. This has been supported by a strong network of affiliates who help to service the ransomware-as-a-service (RaaS) model used by most major groups. Additionally, a rise in the use of infostealers such as RedLine, Lumma, and META available cheaply on the deep and dark web, has helped to facilitate the activities of such ransomware gangs and their affiliates.

While the overall number of Distributed Denial of Service (DDoS) declined significantly in 2024 when compared with 2023, there is a noticeable pattern of hacktivist groups utilizing DDoS attacks in a highly targeted manner against UAE-based organizations. However, this activity declined in the fourth quarter of 2024, largely due to a combination of law enforcement and stricter social media usage policies.

The use of publicly available AI technology became more widespread throughout 2024, streamlining workflows and processes with greater efficiency. However, this technological leap also brought significant challenges as cyber threat actors began leveraging AI for malicious activities.

AI-generated malware and deepfake technology were reported in attacks targeting UAE-based entities. Additionally, state-sponsored threat actors used AI-driven tools to map organizational vulnerabilities for the purposes of reconnaissance. As such attacks are likely to increase in the coming years, organizations must prioritize the advancement of cyber detection tools. The development of adaptive AI-powered defenses will be critical to stay ahead of emerging threats.

The report advocates for robust cyber defense capabilities through stronger threat intelligence, continuous security monitoring, proactive threat hunting, increased awareness of cybersecurity issues, and timely updates to software and systems.

Organizations and governments need to adopt a strategic and forward-thinking approach to cybersecurity. This includes understanding the latest threats, adjusting defenses as needed, and working together to strengthen the nation's overall cybersecurity. By fostering a culture of awareness and resilience, UAE businesses can stay one step ahead of cybercriminals and continue to thrive in a digital-first world.

This report offers actionable insights to help navigate these challenges and build stronger defenses, ensuring a safer and more secure future for everyone.

4. Top Threat Trends

The cyber threat landscape in the UAE remained varied throughout 2024, with several key trends highlighting specific threats that pose significant risks to the nation.

Ransomware

- **Increase in ransomware groups:** The number of ransomware groups operating in the UAE grew significantly from 2023 to 2024 (refer to Figure 1), with new groups like DarkVault, Qilin, RansomEXX, and KillSec emerging in 2024.

- **Shift in dominance: Lockbit3** remained a prominent ransomware group, though its percentage share decreased from 31 percent in 2023 to 16 percent in 2024, reflecting diversification in threat actors.
RansomHub emerged as a top ransomware group in 2024, accounting for 13 percent ransomware activity in 2024, indicating its growing influence in the UAE's cybersecurity landscape.
The **Clop** ransomware group, which had a 12 percent share in 2023, did not appear in the data for 2024, indicating a decline in its operations or presence in the UAE.

- **Landscape changes:** Several ransomware groups active in 2023 in the UAE like Alphv, Dragonforce, Mallox, Medusa, NoEscape, RansomHouse, Snatch, and Vice Society were not reported in 2024, indicating significant changes in the ransomware ecosystem.

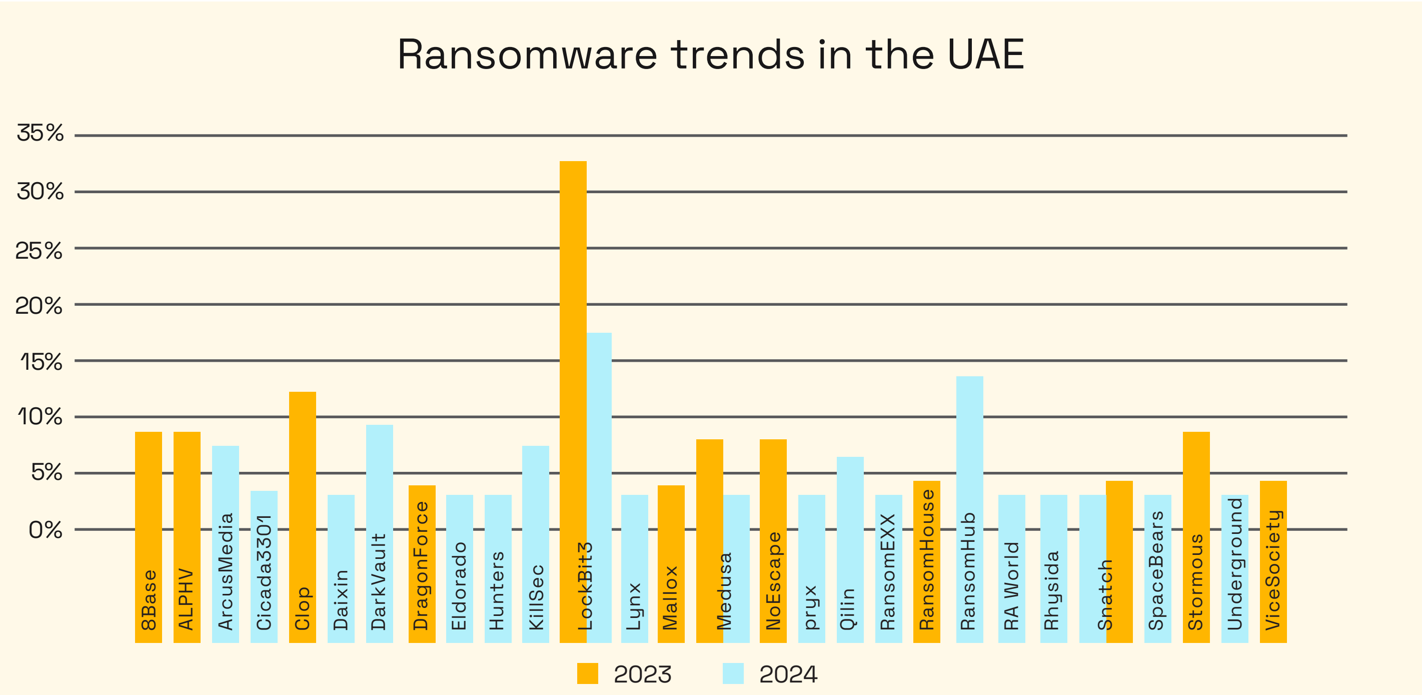

Ransomware trends in the UAE

Figure 1: Active ransomware groups in the UAE in 2023 and 2024[1]

Data Breach Costs

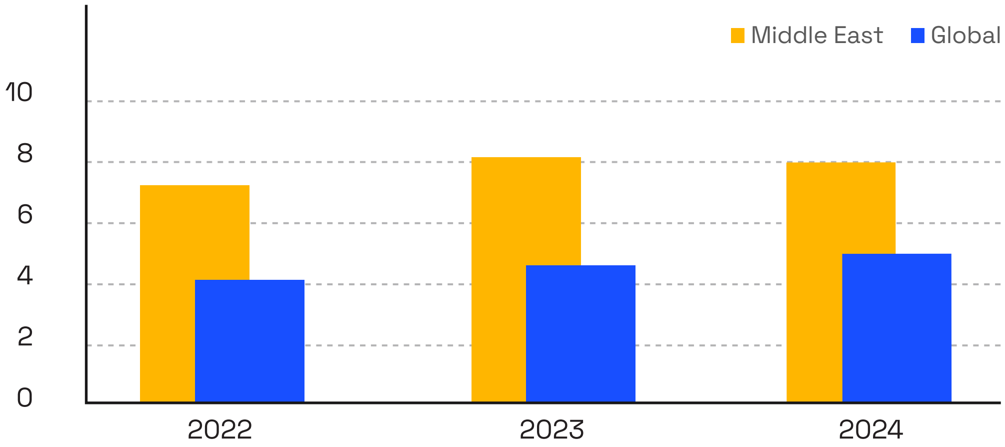
In 2024, the financial implications of data breaches in the Middle East, including the UAE, continued to rise, with the region recording the second-highest data breach costs globally.

The average cost of a data breach reached US$4.88 million globally, driven by factors such as lost business, customer response costs, and data visibility gaps.

Organizations extensively using AI and automation saw significant cost savings, while those with understaffed security teams faced higher breach costs. This trend reflects the economic prosperity of Gulf economies and cyber threat actors exploiting this wealth.

Data breach costs

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



Distributed Denial of Service (DDoS) Attacks

From the first half of 2023 to the first half of 2024, the UAE experienced a drastic decrease in DDoS attacks, with a reduction of approximately 96.09 percent, dropping from 58,538 attacks to just 2,301.

Total DDoS Attacks	• **2,301 (UAE)** • 7.96 million (Globally)
Max Bandwidth	• **85.92 Gbps peak volume (UAE)** • 960.397 Gbps peak volume (Globally)
Average Attack Duration	• **18.53 minutes (UAE)** • Varies, with longest attack lasting 60 minutes (Globally)
Top Targeted Industries	• **Wired telecommunications carriers (UAE)** • Wired telecommunications carriers (Global)

Figure 3: DDoS attack statistics (first half of 2024) – Global vs. UAE[3]

The maximum bandwidth recorded during attacks decreased by 67.7 percent, falling from 266.9 Gbps to 85.92 Gbps. The average attack duration also saw a decline of 26.9 percent, decreasing from 25 minutes to 18.53 minutes.

In contrast, globally, the total number of DDoS attacks increased slightly by 0.8 percent, rising from 7,900,000 to 7,962,491. The maximum bandwidth for global attacks experienced a significant increase of 58.7 percent, going from 605 Gbps to 960.397 Gbps. Notably, wired telecommunications carriers were the most targeted industries in both the UAE and globally during the first half of 2024.

Overall, while the UAE saw substantial decreases in both the frequency and intensity of DDoS attacks, the global landscape reflected a slight uptick in attack numbers and a notable rise in bandwidth.

5. UAE Attack Surface

The attack surface of the UAE refers to the extent of vulnerabilities and potential entry points within the technology infrastructure of organizations operating within the country. It encompasses weaknesses that could be exploited by cyber attackers at an individual, sectoral, or national levels. This section delves into the combined attack surface of UAE organizations, highlighting the risks inherent in their networks.

4.1 UAE Attack Surface Exposure

The UAE hosts about

223,800 assets

with a significant concentration across key emirates:

Dubai **65%**

Abu Dhabi **13%**

Fujairah **11%**

Sharjah **7%**

Ajman **3%**

Ras al Khaimah **1%**

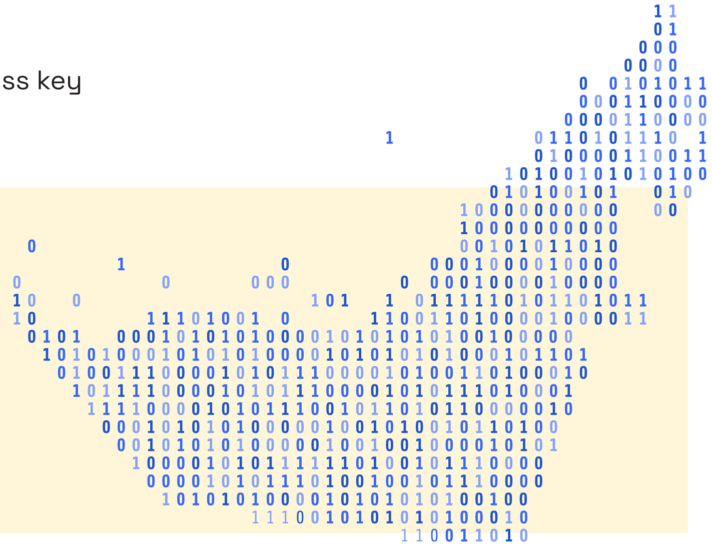


Figure 4: Assets hosted in the UAE - breakdown by emirate

This distribution underscores the geographical variance in digital assets that could potentially be targets for cyber-attacks.[4]

Top 10 Critical Common Vulnerabilities and Exposures (CVEs)

In 2024, OpenSSH vulnerabilities* remained a significant concern for cybersecurity professionals, with several high-severity vulnerabilities identified.

CVE-2023-38408: This is the most prevalent vulnerability. It involves Forwarded SSH-Agent Remote Code Execution and has a high CVSS score* of 9.8 and a high percentage of affected devices existing at 33.3 percent. It allows attackers to execute code remotely, posing a serious threat to network security.

CVE-2024-6387: Known as "regreSSHion", this vulnerability involves Unauthenticated Code Execution in glibc-based Linux systems. With a CVSS score of 8.1 and affected systems existence at 16.7 percent, this vulnerability highlights the importance of ensuring proper authentication measures.

Denial of service vulnerabilities: Threats such as CVE-2021-28041 and CVE-2016-6515 underscore the need for organizations to address not only remote code execution issues but also threats that can disrupt network availability. Prioritizing patch management and implementing security best practices can help mitigate the risks posed by these vulnerabilities.

*OpenSSH vulnerability refers to a security flaw in OpenSSH, a popular open-source implementation of the SSH (Secure Shell) protocol. This vulnerability can allow malicious actors to exploit weaknesses in the software to gain unauthorized access to a system, execute arbitrary code, or perform other malicious activities.

*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[5]

CVE	Description	Category	CVSS Score	Public Exploit Exists	Affected Systems (%)
CVE-2023-38408	OpenSSH - Forwarded SSH-Agent Remote Code Execution	Remote Code Execute	9.8	✓	33
CVE-2024-6387	OpenSSH - Unauthenticated Code Execution in glibc-based Linux systems (regreSSHion)	Remote Code Execute	8.1	✓	17
CVE-2023-28531	OpenSSH - Remote Code Execution	Remote Code Execute	9.8	✓	13
CVE-2021-28041	OpenSSH - Double-free memory corruption	Denial of Service	7.1	✗	12
CVE-2019-16905	OpenSSH - Pre-Auth Integer Overflow in the XMSS Key Parsing Algorithm	Remote Code Execute	7.8	✓	4
CVE-2016-10012	OpenSSH - The shared memory manager used by pre-authentication compression support had a bounds check	Elevation of Privilege	7.8	✗	2
CVE-2016-6515	OpenSSH - Denial of Service	Denial of Service	7.5	✓	2
CVE-2016-10010	OpenSSH - Privilege Escalation	Elevation of Privilege	7.0	✓	2
CVE-2016-10009	OpenSSH - Arbitrary Library Loading	Remote Code Execute	7.3	✓	2
CVE-2024-39929	Exim - Incorrect parsing of multiline rfc2231 header filename	Security Feature Bypass	5.4	✓	2

Figure 5: UAE's top observed vulnerabilities by assigned CVE number – 2024[6, 7, 8]

Infostealer Trends

Our research shows a growing prevalence of infostealer malware in the UAE.

RedLine Stealer, at 69.9 percent, emerged as the predominant threat element posing the highest threat, and exhibiting the highest number of infected systems in the UAE.

META Stealer, identified in 13.1 percent of the records, surfaced in the rankings due to its significant occurrence.

Lumma and Vidar stealers represented 12.6 percent and 4.4 percent of the infections, respectively.

Overall, of 238,109 unique passwords leaked by infostealers, we observed that 77.04 percent of them adhered to the National Institute of Standards and Technology (NIST) password length guidelines. While a significant majority of the leaked passwords met the recommended length of at least 12 characters, the fact that these passwords were still compromised by infostealer malware highlights a critical issue—even long passwords can be vulnerable if they are exposed through malware attacks. This suggests that simply following length guidelines is not sufficient for password security.

Users may be creating long passwords, but if they are using them on compromised systems or failing to implement other security measures (like two-factor authentication), those passwords can still be stolen. Therefore, while adherence to length guidelines is a positive trend, it underscores the need for comprehensive security practices beyond just password length, including awareness of malware threats and the importance of using secure devices and networks.

Number of compromised passwords

1 to 8 characters	9 to 12 characters	Greater than 12 characters
54,655	**107,478**	**75,976**

6. Common Incident Types

In 2024, CPX's Security Operations Center (SOC) handled and analyzed a wide range of incidents across different client environments. These incidents were categorized into seven groups and evaluated on severity using the UAE's Computer Emergency Response Team (aeCERT) scale.

Misconfiguration/Tuning/Change requests emerged as the most frequent category, representing a significant 32 percent of all incidents. This underscores the importance of stringent configuration management to prevent errors that could expose systems to threats. Ensuring that systems are correctly configured is crucial for maintaining network security and mitigating risks.

Improper usage and unlawful activity accounted for 19 percent of the incidents, highlighting the ongoing challenge of ensuring compliance with organizational policies. Such activities could lead to serious security breaches if not addressed promptly. Enhancing user training and awareness programs can help mitigate these risks.

Scans/Probes/Attempted access made up 15 percent of the incidents, reflecting persistent attempts by adversaries to identify vulnerabilities within networks. These actions often precede more severe attacks and highlight the need for robust perimeter defenses and regular vulnerability assessments.

E-mail frauds/Phishing/Spoofing represented 12 percent of the total incidents. Despite being less dominant, the prevalence of these socially engineered attacks highlights the critical need for continuous user education and robust email security measures.

Malicious code was involved in 9 percent of the incidents. The continued presence of malware, including viruses, worms, and Trojan horses, underscores the importance of advanced malware detection and response mechanisms to protect systems from infections.

Unauthorized access incidents made up 9 percent of the total, indicating potential weaknesses in access control mechanisms. Strengthening these controls and implementing multi-factor authentication can help prevent unauthorized access to sensitive resources.

Vulnerabilities/Web application attacks accounted for 4 percent of the incidents. Although lower in frequency, these attacks pose significant risks, suggesting the effectiveness of existing security measures or a strategic shift by attackers to target more vulnerable vectors.

Figure 6: UAE's top observed vulnerabilities by assigned CVE number – 2024[9]

6.1 Incidents by Type

32%

Misconfiguration/Tuning/Change requests

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

19%

Improper usage and unlawful activity

Violation of organizational policies, including inappropriate and/or illegal activities

15%

Scans/Probes/Attempted access

This category encompasses any activity aimed at accessing or identifying a federal agency's computer systems, open ports, protocols, services, or any combination thereof, for potential future exploitation

12%

E-mail fraud/Phishing/Spoofing

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

9%

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

9%

Unauthorized access

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

4%

Vulnerabilities/Web application attacks

Vulnerabilities in an entity’s operating systems and web application

Figure 7: Incident breakdown by type – CPX SOC data – 2024[10]

6.2 Incidents by Severity

A significant **77 percent of incidents** were classified as critical, high, or medium severity. This reflects the substantial risks they pose to business continuity and operations, with the potential to cause significant disruptions over an extended timeframe.

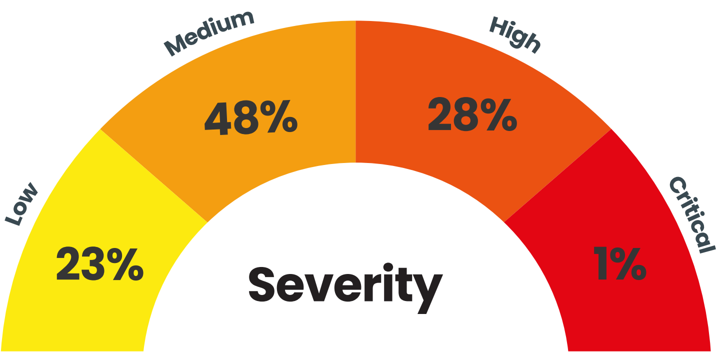


Figure 8: Incident breakdown by severity – CPX SOC data – 2024[11]

6.3 Incidents by Sector

Key sectors targeted include finance, energy, government, and defense, highlighting the need for industry-specific cybersecurity strategies to mitigate risks effectively.

Government	34.9%
Finance	21.3%
Energy	14.1%
Insurance	11.6%
Healthcare	6.7%
Defense	6.6%
IT services	4.8%

Figure 9: Incident breakdown by sector – CPX SOC data – 2024[12]

6.4 Threat Hunting Insights

The CPX Threat Hunting team observed a high number of attacks in 2024, targeting companies located in the UAE (refer to Figure 8). Most of them were related to phishing email campaigns that bypassed email security gateways.

The Threat Hunting team leveraged the CPX Intelligent Threat Detection platform to detect phishing email campaigns and stop the attack as early as possible.

Incidents observed during threat hunting operations

61%	E-Mail Fraud/Phishing /Spoofing
24%	Improper Usage & Unlawful Activity
4%	Vulnerabilities/Web Application Attacks
8%	Scans/Probes/ Attempted Access
1%	Malicious Code
1%	Investigation
1%	Compromised Information

Figure 10: Incident breakdown by type – CPX Threat Hunt data – 2024[13]

DLL Search Order Hijacking

In the first half of 2024, the CPX Threat Hunting team identified activities linked to the MINIBUS and MINBIKE backdoor, associated with an Iranian threat actor. The campaign used spear-phishing emails with fake job offer links to deliver the malicious payload. It relied on DLL search order hijacking for persistence and abused Azure infrastructure for C2 communications.

Threat actors dropped malicious DLLs in benign application folders, including Microsoft Office, VMware VGAuth, OneDrive, and Splunk Universal Forwarder, to evade detections.

Target Countries

UAE

Target Industries

- **Defense**

Attack Vector (MITRE ATT&CK)

Hijack Execution Flow (T1574)

Intent

Espionage

Malicious Tools

- **MINIBIKE**
- **MINIBUS**

Phishing Email Campaign

The CPX Threat Hunting team has observed increased phishing campaigns targeting multiple organizations in the UAE. Since phishing is a relatively simple and highly effective strategy, threat actors frequently employ this technique to steal credentials. Unlike malware and exploits, which depend on flaws in security defenses, phishing depends on human contact to trick targets.

Most of the observed phishing campaigns consisted of spear phishing links that impersonated Microsoft 365. They further used the stolen credentials to gain access to email and VPN services, with the intention of accessing, abusing, and exfiltrating critical data.

In addition, the team observed high numbers of payment card phishing campaigns impersonating multiple local organizations in the UAE, like Etisalat, DEWA, Aramex UAE, and DHL.

In May 2024, threat actors were found sending phishing emails with ZIP attachments containing an executable that installs LockBit Black ransomware.

Target Countries

UAE

Target Industries

- **Government**
- **Healthcare**
- **Energy**
- **Financial Services**
- **Maritime**
- **Defense**

Attack Vector (MITRE ATT&CK)

Phishing (T1598)

Intent

Espionage

Exploitation of Public-facing Applications

CPX continues to see exploitation of both N-days and Zero-days vulnerabilities* in public-facing applications. Most of the attacks are opportunistic and the attack starts immediately after the disclosure of proof-of-concept (PoC) exploit code. A significant portion of these scanning activities have been traced back to IP addresses associated with Linode, LLC, a cloud hosting provider. At present, no specific threat actor has been linked to the vulnerability scans.

In April 2024, CPX observed multiple exploit attempts against the OS Command Injection Vulnerability CVE-2024-3400 in GlobalProtect and there were attempts to deploy RedTail Cryptominers.

Target Countries

UAE

Target Industries

- **Government**
- **Healthcare**
- **Energy**
- **Financial Services**
- **Cultural & Tourism**
- **Maritime**
- **Defense**

Attack Vector (MITRE ATT&CK)

Exploit Public-facing Applications (T1190)

*A zero-day vulnerability is unknown to the vendor, and thus there is no patch, mitigation, or fix available to address it.

One-day vulnerabilities are known vulnerabilities for which a patch or mitigation is available but hasn't yet been applied.

Sometimes these vulnerabilities are referred to as "n-day" vulnerabilities since the period is often much longer than one day, as the average mean time to patch (MTTP) is between 60 and 150 days.[14]

InfoStealer Malware

The CPX Threat Hunting team noticed a significant increase in the number of credential leak incidents due to InfoStealer malware infections in the Windows-based personal devices. This happens when the victim synchronizes Google Password Manager in the Chrome browser installed in both the corporate and personal systems.

There are several inexpensive malware-as-a-service (MaaS) infostealers sold on the Dark Web Forums. The cybercriminals leverage these infostealer malware and sell the stolen credentials for as little as US$10.

Target Countries

UAE

Target Industries

- **Government**
- **Energy**
- **Financial Services**
- **Maritime**
- **Defense**

Attack Vector (MITRE ATT&CK)

Credentials from password stores (T1555)

7. Key Attack Insights

This section dissects the methodologies employed by threat actors to breach or infiltrate a victim's network, based on the incidents handled by the CPX THREAD (Threat Hunting Response and Active Defense) team.

7.1 Threat Vector Highlights

Major Entry Vectors Used by Threat Actors

In 2024, there was a significant shift in the initial vectors used by threat actors. While drive-by downloads remained a prevalent method, data destruction emerged as new prominent initial vectors.

Increased data destruction: Data destruction incidents rose significantly by 22 percent, highlighting a growing concern for organizations as threat actors focus on causing harm by destroying data.

Continued phishing concerns: While phishing incidents remained unchanged, the category of "unknown (possibly Phishing)" suggests a potential overlap with other vectors. This highlights the persistent relevance of phishing attacks as a common threat vector.

Web Server Compromise: A continued trend in 2024 is the appearance of web server compromise incidents, accounting for 11 percent of the total incidents. This highlights the importance of securing web servers against exploitation by threat actors.

2023 (in %)	Entry vectors	2024 (in %)
7	Account compromised	0
7	Data leak	0
18	Drive by download	11
21	Exploit public-facing application	0
29	Insider threat	0
7	Malware	0
11	Phishing	11
0	Brute force attack	12
0	Web server compromise	11
0	Data destruction	22
0	Unidentified	22
0	Vulnerability exploitation	11

Figure 11: Observed entry vectors – CPX THREAD Data – 2023–24

In 2024, malware delivery methods showed a shift towards different malware delivery methods, with a decrease in direct installs and an increase in web application attack delivery methods.

Decrease in direct install: The percentage of malware directly installed on a victim's machine decreased from 36 percent in 2023 to 11 percent in 2024, suggesting attackers are favoring indirect methods.

Emergence of web application attacks: Web application attacks accounted for 11 percent of malware delivery in 2024, indicating a focus on exploiting vulnerabilities in web applications to distribute malware.

Malware Delivery Vector

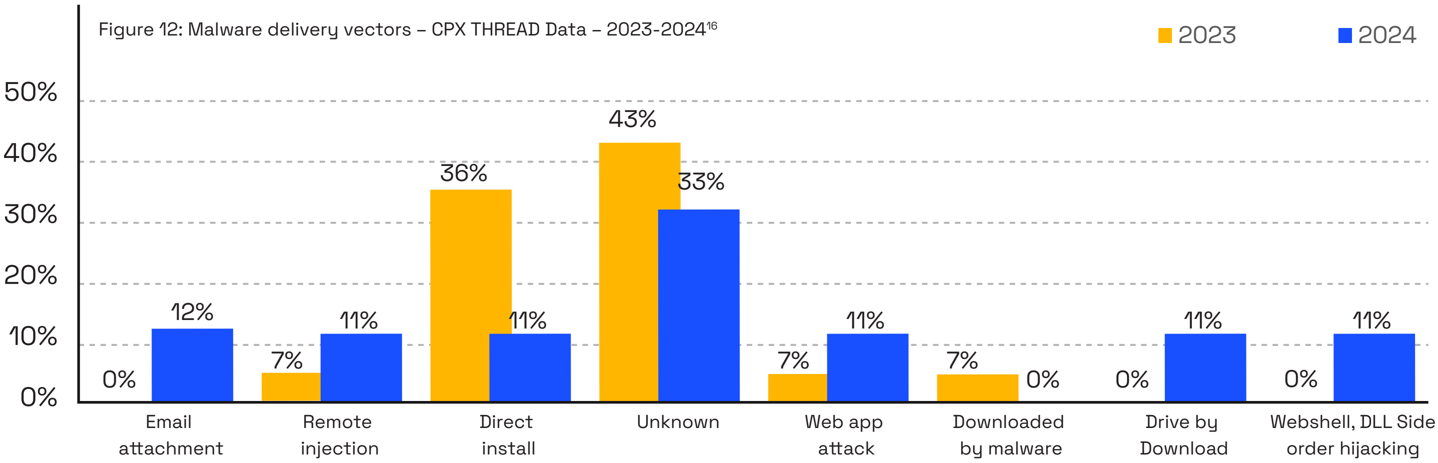
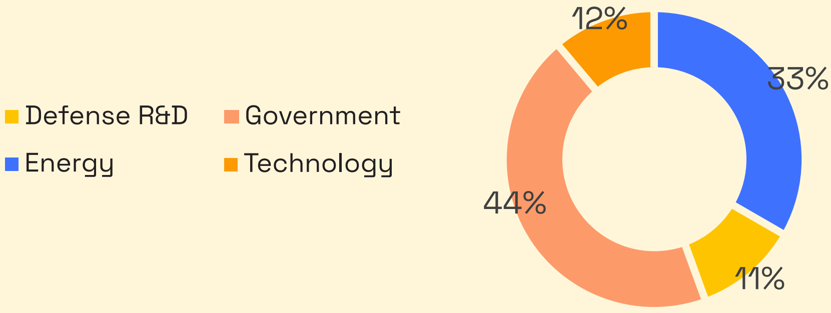


Figure 12: Malware delivery vectors – CPX THREAD Data – 2023-2024[16]

Incidents by Industry

Figure 13: Incidents by sectors 2024 – UAE only[17]



7.2 Profile of Threat Actors Targeting the UAE

In 2024, the UAE continued to encounter a varied landscape of cyber threat actors, each characterized by unique motivations and tactics.

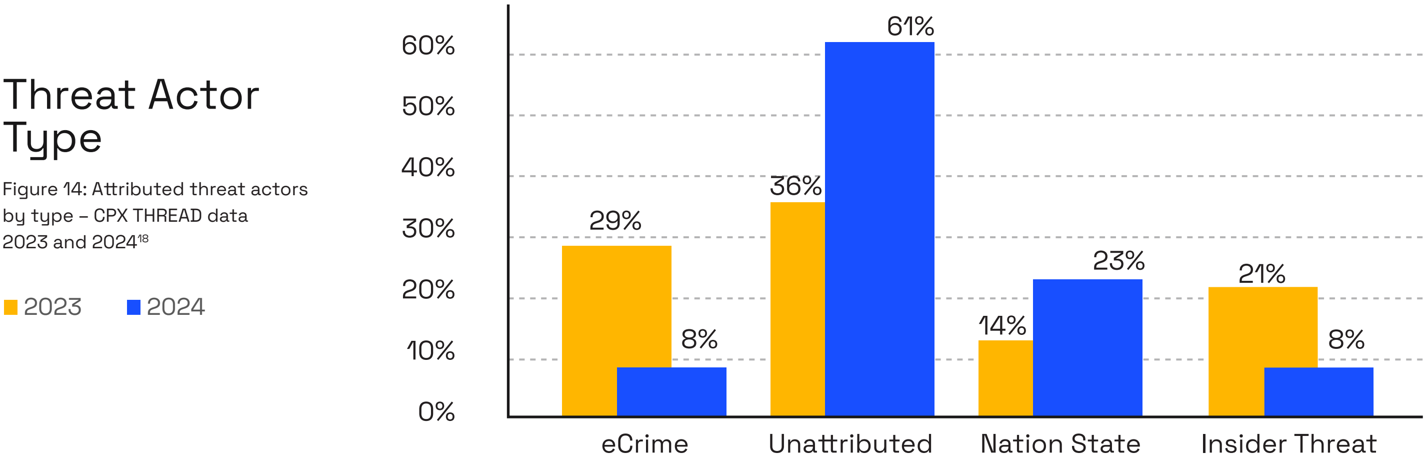
The most prominent group in 2024 was the unattributed actors, who accounted for a significant 62 percent of threats. These actors often operate anonymously, making it challenging to discern their intentions or affiliations.

Nation-state actors, representing 23 percent of the threats, typically engage in cyber activities driven by espionage or destructive goals, dedicating substantial resources to infiltrate specific targets.

eCrime groups, which have decreased to 8 percent, remain focused on financial gain, targeting organizations with vulnerabilities to swiftly exploit and monetize sensitive data.

Threat Actor Type

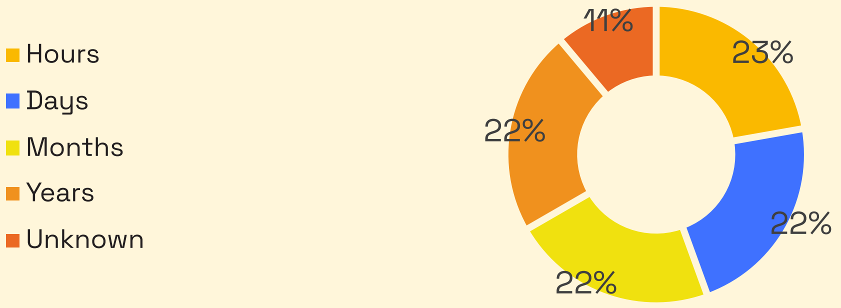
Figure 14: Attributed threat actors by type – CPX THREAD data 2023 and 2024[18]



Time Until a Threat Actor is Discovered (Dwell Time)*

Dwell Time

Figure 15: Dwell time – Time from initial entry to detection – CPX THREAD data – 2024[19]



*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.

8. Threat Groups

The CPX Threat Intelligence Centre has carefully assessed the cyber threat landscape, focusing on key trends, motivations, and the tools, techniques, and procedures (TTPs) employed by various threat actors. This research has resulted in the identification and profiling of several notable groups, including nation-state actors, ransomware operators, and hacktivists.

The purpose of this analysis is to provide organizations with practical insights that will help them bolster their security defenses against threats relevant to their particular sector.

8.1 Nation-state Threat Actors

Government-backed threat actors are typically associated with nation-states, operating under the direction and support of their respective governments. These threat actors often have close ties to military or state security organizations within their countries. They tend to have access to significant government resources, including funding, personnel, technical capabilities, and operational assistance to carry out their activities.

APT 39

Aliases

COBALT HICKMAN, Chafer, G0087, REMIX KITTEN, Radio Serpens, TA454

Motivation

Espionage[20]

Targeted sectors

Hospitality · Technology · Government · Telecommunications[21]

TTPs

- Data Encoding: Non-Standard Encoding
- Brute Force
- Valid Accounts
- Command and Scripting Interpreter: PowerShell
- Obfuscated Files or Information[22]

Muddy Water

Aliases

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

Motivation

Espionage, political influence, and circumventing international sanctions[23]

Targeted sectors

Education · Energy · Technology · Government · Telecommunications

TTPs

- Command and Scripting Interpreter: PowerShell
- Hijack Execution Flow: DLL Side-Loading
- Obfuscated Files or Information
- Data Encoding: Non-Standard Encoding
- Ingress Tool Transfer[24,25]

Lazarus

Aliases

APT38, Lazarus Group

Motivation

Financial gain and political influence for North Korea

Targeted sectors

Finance Healthcare Technology Defense Cryptocurrency

TTPs

- Brute Force
- Process Injection
- Phishing: Spearphishing Attachment
- Ingress Tool Transfer
- Valid Accounts

Pulsar Kitten

Aliases

Pulsar Kitten

Motivation

State-sponsored

Targeted sectors

Government Aerospace Technology Defense Cryptocurrency

TTPs

- Phishing
- Command and Scripting Interpreter
- Ingress Tool Transfer
- Process Injection
- Valid Accounts[26]

Salt Typhoon

Aliases

Earth Estries, Ghost Emperor, Famous Sparrow, UNC 2286

Motivation

Espionage

Targeted sectors

Government Chemical Technology Critical infrastructure Telecommunications[27]

TTPs

- Exploit Public-Facing Application
- Command and Scripting Interpreter: PowerShell
- Data Encoding: Non-Standard Encoding
- Impair Defenses: Disable or Modify Tools
- Obfuscated Files or Information[28, 29, 30]

8.2 eCrime Threat Actors

eCrime threat actors are driven mainly by the pursuit of financial gain. They frequently target organizations with weak network defenses, aiming to infiltrate systems or steal data. Their usual objectives include selling the stolen data on the Dark Web or demanding a ransom from the victim organization to return the compromised information.

LockBit

Aliases

Bitwise Spider, LockBit 3.0, LockBit Black, LockBitSupp

Motivation

Financial Gain

Targeted sectors

Finance · Healthcare · Energy · Food and Agriculture · Government[31]

TTPs

- External Remote Services
- Boot or Logon Autostart Execution
- Exfiltration
- Data Encrypted for Impact[32, 33]

RansomHub

Aliases

Cyclops, Knight

Motivation

Financial Gain

Targeted sectors

Transportation · Healthcare · Technology · Government · Critical infrastructure[34]

TTPs

- Phishing
- Command and Scripting Interpreter
- Impair Defenses: Disable or Modify Tools
- Transfer Data to Cloud Account
- Data Encrypted for Impact[35, 36, 37]

Darkvault

Aliases
DarkVault, Darkvaultransom

Motivation
Financial gain[38]

Targeted sectors

Lifestyle · Healthcare · Technology · Government · Insurance[39]

TTPs

- Phishing
- Command and Scripting Interpreter
- Ingress Tool Transfer
- Data Encrypted for Impact
- Indicator Removal[40]

8.3 Hacktivists

Hacktivists are a growing phenomenon in the digital age, representing a unique intersection of technology, politics, and social activism. These individuals or loosely organized collectives are driven by a desire to promote their political beliefs and agendas through the use of hacking and other cyber-based tactics.

Hacktivists are politically driven hackers who form loose collectives to target organizations that oppose their political ideologies.

Sylhet Gang-SG

Aliases
Sylhet Gang-SG

Targeted sectors

Finance · Education · Critical infrastructure · Government

Motivation
Religious and Political

TTPs
DDoS attacks[41], website defacement, data exfiltration[42]

SN_BLACKMETA

Aliases
SN Blackmeta

Targeted sectors

Government · Finance · Social media platforms[43,44] · Energy · Telecommunications

Motivation
Political ideology, opposition to content promoting Israel[45]

TTPs
DDoS attacks, website defacement, data exfiltration[46]

Black Maskers Army

Aliases
None

Targeted sectors

Finance · Technology · Government · Critical infrastructure[47]

Motivation
Political ideology, support for Palestine[48]

TTPs
DDoS attacks, data breaches, website defacement[49]

9. Rise of AI-powered Threats in the UAE

AI is revolutionizing industries worldwide, but its adoption by cybercriminals poses significant risks. In 2024, the UAE witnessed a surge in AI-powered threats, with adversaries leveraging machine learning (ML) and automation to enhance the scale, speed, and sophistication of their attacks. This section explores the rise of AI-powered cyber threats in the UAE and the critical role of Cyber Threat Intelligence (CTI) in addressing these challenges[50].

AI-driven Cyber Threat Landscape

AI-enhanced Phishing Attacks

Phishing campaigns have become more convincing with the use of AI tools to craft personalized and context-aware emails. These emails often evade traditional detection mechanisms, increasing their success rate. UAE-based financial institutions and multinational corporations reported a sharp rise in spear-phishing campaigns targeting high-profile executives, leading to increased credential theft and unauthorized access to sensitive systems.

AI-generated malware

Adversaries are using AI to develop malware that can adapt its behavior in real time, evading detection by traditional antivirus and endpoint security solutions. For instance, polymorphic malware capable of rewriting its code to avoid signature-based detection was used in an attack on a UAE-based energy firm. This resulted in extended dwell times and increased potential for data exfiltration. CTI plays a critical role in monitoring dark web marketplaces for AI-based malware tools and sharing indicators of compromise (IoCs) with affected sectors.

Deepfake and synthetic media exploit

Deepfake technology has been weaponized for disinformation[51], fraud, and identity theft. Attackers create convincing audio or video impersonations to manipulate victims, as seen in a UAE-based corporate scam where deepfake audio was used to trick employees into transferring funds to fraudulent accounts, leading to financial losses and reputational damage. Iranian hackers went further, interrupting UAE TV streams[52] to broadcast a deepfake newsreader reporting on the Gaza war, undermining trust in media.

AI in advanced persistent threats (APTs)

State-sponsored actors[53] are increasingly integrating AI into their attack frameworks to automate reconnaissance, exploit identification, and lateral movement within networks. An APT group used AI-driven tools to map vulnerabilities in the UAE's critical infrastructure, targeting OT environments and posing heightened risks to national security and economic stability.

UAE’s response to AI-powered threats

The UAE has taken proactive measures to address the rise of AI-driven cyber threats. Key initiatives include the adoption of AI-based cybersecurity solutions to detect and respond to evolving threats in real time, the incorporation of AI in the National Cybersecurity Strategy to strengthen national cyber resilience, and public awareness campaigns to educate the public and businesses about AI-related cyber risks, including deepfakes and phishing scams.

Crystal Ball

The Crystal Ball platform is an analytical next-generation AI information-sharing platform developed for members of over 68 Counter Ransomware Initiative (CRI) nations and partners. Designed to foster the relationships among CRI members to combat cyber threats effectively, this platform facilitates a culture of information sharing that works to attribute incidents and attacks to their origins, share intelligence globally, and deter cybercriminals from future attacks.

Future implications

AI’s dual-use nature—its role in promoting as well as preventing cyberattacks will continue to grow. To counter this, the UAE must invest in AI research to develop models for detecting and mitigating AI-powered threats, strengthen collaboration with international cybersecurity agencies to share intelligence and best practices, and enhance CTI capabilities to anticipate emerging threats and understand the tools and methods employed by attackers.

10. The CPX Safe AI Framework

The CPX Safe AI Framework provides organizations with a practical guide for implementing AI responsibly, ensuring safety, security, and ethical compliance. Designed to address regulatory complexities and promote effective AI governance, the framework offers a structured approach tailored to the evolving needs of businesses.

The framework is structured around three essential pillars:

Organizational drivers

This component assists organizations in formulating a clear AI strategy that aligns with their overarching goals, mission, and vision. We emphasize the importance of securing leadership support, integrating responsible AI principles into operations, evaluating regulatory obligations, and establishing accountability to ensure that all AI initiatives prioritize human welfare and advancement.

Model development and deployment

This pillar emphasizes a thorough approach to evaluating fairness, accountability, and transparency throughout the AI system lifecycle. It includes conducting impact assessments, defining data usage policies, and clarifying data ownership and storage practices. Additionally, it addresses the responsible training of AI models, setting standards for human oversight, and creating comprehensive testing and incident response strategies.

Security and privacy considerations

Our framework strengthens the security of AI models through robust controls, vulnerability assessments, and AI red teaming, while also ensuring compliance with privacy regulations. It offers guidance on securing AI infrastructure using zero-trust principles, maintaining a secure runtime environment, and managing risks through diligent assessments and user training.

The Safe AI Framework empowers organizations to harness the advantages of AI while fostering trust among customers, stakeholders, and regulators. As AI technology continues to advance, the frameworks and protections necessary to safeguard users, data, and society will also evolve. Our Safe AI Framework represents a proactive step toward guiding organizations in the safe and secure deployment of AI, ensuring that innovation is pursued responsibly.

11. Recommendations

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

Strategy

Establish AI governance frameworks: Develop and implement AI governance frameworks to ensure the responsible and ethical use of AI within the organization. This should include policies, processes, and controls to manage AI-related risks and ensure alignment with regulatory requirements.

Cybersecurity awareness and education initiatives: Increase awareness and education on cybersecurity best practices for government employees, businesses, and the general public.

Governance, Risk, and Compliance (GRC)

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.

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 defenses.

Security Operations Center (SOC)

Implement SOC capability: Establish a 24/7 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.

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.

Vulnerability Management: Implement regular, coordinated vulnerability assessments across critical national infrastructure sectors to identify and prioritize vulnerabilities that could impact national security. This should involve collaboration with various government agencies and private sector partners.

Use Cyber Threat Intelligence: Establish a robust cyber threat intelligence function to systematically monitor specific external threats, delivering critical insights on new and emerging risks. This capability will facilitate real-time adjustments to security postures, enhancing overall resilience.

Additionally, actively engage in intelligence-sharing communities to acquire timely and relevant threat intelligence (TI). This collaboration enables countries and organizations to implement effective controls against both current and emerging threats. By participating in these trusted networks, members gain access to TLP Red Intelligence that may not be available through commercial TI feeds, allowing them to proactively address potential risks.

This collective approach provides real-time indicators and insights, empowering organizations to effectively monitor and respond to activities within their environments.

Develop 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 AI-powered threat hunting: Leverage AI and machine learning capabilities to enhance threat hunting efforts, enabling the identification of advanced, stealthy threats that may evade traditional security controls. This can involve the use of anomaly detection, behavioral analysis, and other AI-driven techniques.

Integrate with the National Cyber Security Operations Center (NSOC): Collaborate with the NSOC 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.

12. Conclusion

As the UAE's economy continues to grow rapidly, it is also grappling with a complex and evolving cyber threat landscape. This landscape is populated by a variety of threat actors, including state-sponsored groups, cybercriminal organizations, insider threats, and politically motivated hacktivists. Despite their varied goals, these groups share a unified intent: to breach organizational networks and access confidential information.

Organizations in the UAE are facing a multitude of attack strategies, ranging from exploiting system vulnerabilities and deploying malicious software to executing ransomware and DDoS attacks. To effectively combat these threats, it is crucial for UAE organizations to not only recognize the nature of these risks but also to proactively adjust their defenses to stay ahead of the ever-changing tactics used by cyber adversaries.

In the near future, an uptick in DDoS attacks is expected, driven by ongoing regional geopolitical tensions. Additionally, the demand for compromised credentials is likely to lead to an increase in ransomware incidents, with initial access brokers using information-stealing malware to monetize unauthorized access on the dark web. The rise of AI tools is also anticipated to make spear-phishing attacks more sophisticated, alongside traditional methods of infiltrating networks through vulnerable systems and remote access technologies.

To effectively address this multifaceted threat environment, UAE organizations must develop robust cybersecurity programs that extend beyond technical measures. These programs should incorporate educational campaigns aimed at raising awareness among employees about potential cyber threats, fostering a culture of vigilance, and promoting the timely reporting of suspicious activities. The challenge of combating cyber threats is not solely a technological one; it is deeply rooted in human behavior. Cultivating a knowledgeable workforce—comprising employees, citizens, and cybersecurity experts—who can identify and mitigate threats before they escalate is vital.

By staying ahead of AI-driven cyber threats and investing in cutting-edge CTI, the UAE can secure its digital landscape and maintain its position as a global leader in technological innovation.

Ultimately, a comprehensive approach that blends technical proficiency with human awareness will be the most effective strategy for safeguarding the UAE against the diverse array of cyber threats it faces.

About Us

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, a G42 company, is a leading provider of end-to-end cyber and physical security solutions and services. Founded in 2022 and headquartered in Abu Dhabi, CPX employs over 500 cyber specialists serving enterprises, governments, and critical infrastructure sectors in the UAE and beyond. With a strong focus on delivering transformative security across the AI ecosystem, CPX empowers organizations to assess risks, protect assets, and operate with unwavering confidence.

Discover more at www.cpx.net.

References

1 hxxps[://]ransomfeed[.]it
2 hxxps[://]www[.]ibm[.]com/reports/data-breach
3 hxxps[://]www[.]netscout[.]com/threatreport/emea/united-arab-emirates
4 hxxps[://]spidersilk[.]com
5 hxxps[://]www[.]first[.]org/cvss/
6 hxxps[://]spidersilk[.]com
7 hxxps[://]vuldb[.]com/
8 hxxps[://]nvd[.]nist[.]gov/vuln/search
9 CPX-SOC 2024 Data Set
10 CPX-SOC 2024 Data Set
11 CPX-SOC 2024 Data Set
12 CPX-SOC 2024 Data Set
13 CPX-Threat Hunting Data Set
14 hxxps[://]fieldeffect[.]com/blog/1-day-0-day-vulnerabilities-explained
15 CPX-THREAD Data set
16 CPX-THREAD Data set
17 CPX-THREAD Data set
18 CPX-THREAD Data set
19 CPX-THREAD Data set
20 hxxps[://]attack[.]mitre[.]org/groups/G0087/
21 hxxps[://]attack[.]mitre[.]org/groups/G0087/
22 hxxps[://]attack[.]mitre[.]org/groups/G0087/
23 hxxps[://]www[.]infosecurity-magazine[.]com/news/iran-muddywater-new-custom-backdoor/
24 hxxps[://]www[.]infosecurity-magazine[.]com/news/iran-muddywater-new-custom-backdoor/
25 hxxps[://]www[.}www.picussecurity.com/resource/blog/ttp-ioc-used-by-muddywater-apt-group-attacks
26 hxxps[://]www[.]crowdstrike[.]com/
27 hxxps[://]eclypsium[.]com/blog/salt-typhoon/
28 hxxps[://]www[.]csoonline[.]com/article/3621674/salt-typhoon-poses-a-serious-supply-chain-risk-to-most-organizations[.]html
29 hxxps[://]eclypsium[.]com/blog/salt-typhoon/
30 hxxps[://]eclypsium[.]com/blog/salt-typhoon/
31 hxxps[://]www[.]cisa[.]gov/news-events/cybersecurity-advisories/aa23-165a
32 hxxps[://]www[.]cyber[.]gov[.]au/about-us/advisories/understanding-ransomware-threat-actors-lockbit
33 hxxps[://]www[.]cyber[.]gov[.]au/about-us/advisories/understanding-ransomware-threat-actors-lockbit
34 hxxps[://]www[.]darkreading[.]com/cyberattacks-data-breaches/ransomhub-actors-exploit-zerologon-vuln-in-recent-ransomware-attacks
35 hxxps[://]blackpointcyber[.]com/resources/threat-profile/ransomhub-ransomware/
36 hxxps[://]blackpointcyber[.]com/resources/threat-profile/ransomhub-ransomware/
37 hxxps[://]blackpointcyber[.]com/resources/threat-profile/ransomhub-ransomware/
38 hxxps[://]www[.]threatintelligence[.]com/blog/darkvault-ransomware
39 hxxps[://]www[.]threatintelligence[.]com/blog/darkvault-ransomware
40 hxxps[://]www[.]cyfirma[.]com/news/weekly-intelligence-report-15-nov-2024/
41 hxxps[://]falconfeeds[.]io/blog/post/cyber-attacks-in-the-middle-east-an-indepth-analysis-january--july-2024-405112
42 hxxps://t.me/SylhetGangsgOfficial
43 hxxps[://]thecyberexpress[.]com/sn-blackmeta-claim-snapchat-cyberattack/
44 hxxps[://]malpedia[.]caad[.]fkie[.]fraunhofer[.]de/actor/blackmeta
45 hxxps[://]thecyberexpress[.]com/sn-blackmeta-claim-snapchat-cyberattack/
46 hxxps[://]malpedia[.]caad[.]fkie[.]fraunhofer[.]de/actor/blackmeta
47 hxxps[://]www[.]helpag[.]com/top-middle-east-cyber-threats-april-16-2024/
48 hxxps[://]industrialcyber[.]co/critical-infrastructure/cyprus-critical-infrastructure-targeted-in-series-of-cyberattacks-as-authorities-stress-on-readiness/
49 hxxps[://]industrialcyber[.]co/critical-infrastructure/cyprus-critical-infrastructure-targeted-in-series-of-cyberattacks-as-authorities-stress-on-readiness/
50 hxxps[://]www[.]kaspersky[.]com/blog/cyber-defense-and-ai-kaspersky-report-2024
51 hxxps[://]www[.]zawya[.]com/en/press-release/companies-news/rising-cyber-threats-target-uaes-financial-sector-and-critical-infrastructure-in-2025-qqb6j12z
52 hxxps[://]www[.]globalcompliance-news[.]com/2024/07/04/https-insightplus-bakermckenzie-com-bm-technology-media-telecommunications_1-united-arab-emirates-deepfakes-and-the-use-of-artificial-intelligence-ai-legal-issues-and-considerations_06112024/
53 hxxps[://]www[.]theguardian[.]com/technology/2024/feb/08/iran-backed-hackers-interrupt-uae-tv-streaming-services-with-deepfake-news

Website:
cpx.net

Email:
contactus@cpx.net