مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

UAE Cyber Threat Landscape Analysis

January 2026

"**Disclaimer** :This report is provided by Mastercard solely for informational purposes and is based on publicly available information. Mastercard makes no representations or warranties regarding the accuracy, completeness, or suitability of the information contained in this report.

Any references to cyber threat actors or groups are based solely on publicly available information and should not be interpreted as independent attribution by Mastercard. This report does not constitute legal, regulatory, compliance, or attribution advice and should not be used as the basis for actions such as sanctions, blacklisting, enforcement decisions, or any other governmental or commercial determinations.

To the fullest extent permitted by law, Mastercard disclaims all liability arising from any use or misuse of the information contained in this report.

All rights, title, and interest in the content of this report remain the exclusive property of Mastercard and/or its affiliates. No part of this report may be used, reproduced, distributed, or published except as expressly authorised by Mastercard and in compliance with applicable laws.

This report shall be governed by and construed in accordance with the laws of the United Arab Emirates, and any disputes arising from or in connection with it shall be subject to the exclusive jurisdiction of the competent UAE courts."

This report looks at the evolving cyber threat landscape of the UAE, threat actors and methods used to target organizations and highlights the work being undertaken by the government to strengthen cyber resilience while reinforcing the need for continued investment in cybersecurity.

Key Observations

Expanding attack surface

The UAE's rapid digitalization has strengthened its position as a global innovation hub—currently hosting approximately **223,800*** digital assets—but this growth has also significantly increased its exposure to cyber threats, particularly across government, financial, and technology sectors.

Multitude of different types of attacks targeting organizations

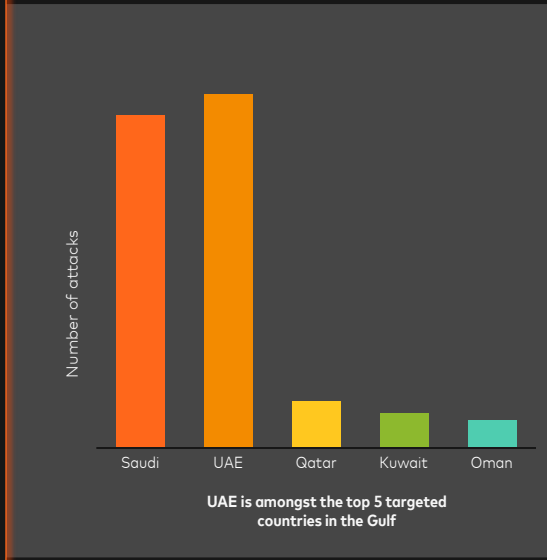
In 2025, the UAE faced over **17,000*** cyberattacks. **Ransomware** and **phishing** were the most common methods, often used in multi-stage campaigns for extortion and network infiltration.

Variety of actors and motivation

State-affiliated groups, **ransomware gangs**, and **ideologically driven actors** targeted UAE entities, creating a complex and fast-evolving threat landscape.

Cybersecurity Council (CSC) of the UAE continues to lead the charge on cyber resilience

To address these challenges, the Cyber Security Council (CSC) has implemented **a national cybersecurity strategy**, enhanced AI-powered threat detection and incident response via **National SOC** and launched awareness and capacity-building programs to strengthen national cyber resilience.



UAE is amongst the top 5 targeted countries in the Gulf

Source: Mastercard Cyber Insights Data (Jan–Dec 2025), *State of the UAE Cybersecurity Report 2025

A national blueprint for cyber resilience

To address evolving cyber threats, the UAE Cybersecurity Council has launched the National Cybersecurity Strategy 2025–2031. It is anchored on five strategic pillars to secure the nation's digital future.

Strategic Pillars

GOVERN

Establishing updated laws, standards, and regulatory frameworks to safeguard digital infrastructure.

Initiatives

- National cyber security governance framework
- Cybersecurity baseline standards for all sectors
- National cyber accreditation program
- Regulatory sandboxes for emerging technologies

PROTECT

Enhancing detection and response capabilities through advanced SOCs, incident response frameworks, and sector-level readiness.

- National Security Operations Center (NSOC)
- National Vulnerability Disclosure Program
- Cyber Crystal Ball
- Secure supply chain program
- Cyber Protective Shield
- Cyber Pulse
- Cyber Sniper

INNOVATE

Positioning the UAE as a testbed for cybersecurity innovation, piloting new technologies and creating ecosystems that attract R&D and startups.

- Cybersecurity Centre of Excellence
- OT and IIOT center of excellence
- Quantum Secure Program
- Secure-by-design frameworks for emerging technology

BUILD

Developing national capacity and resilience through workforce development, research programs, and cyber-awareness campaigns.

- CyberE71
- Cloud Security & Data Localization Standards
- Cyber 193 (The Biggest Cyber Drill)
- National Youth Cyber Awareness Program
- NAFIS program
- Women In Cybersecurity
- Cyber Defense Day (Train-the-nation)

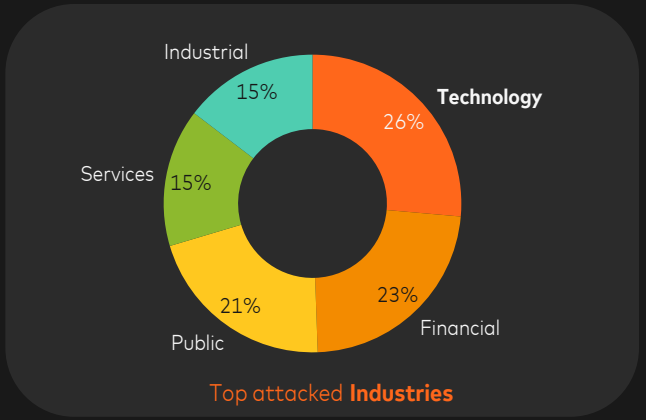
PARTNER

Expanding collaboration with global bodies such as ITU, INTERPOL, UNCCT, FIRST, and CRI, as well as fostering public–private partnerships.

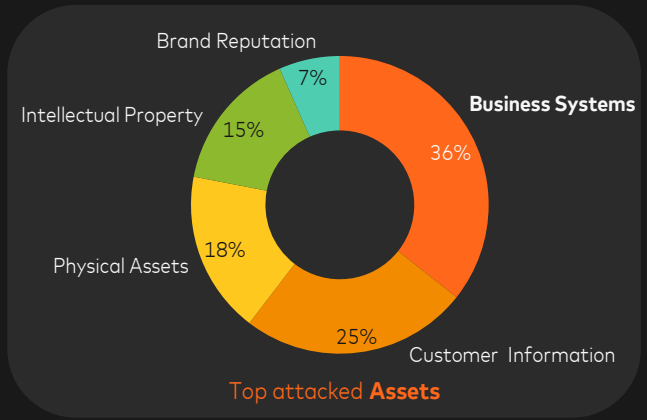
- Counter Ransomware Initiative (CRI)
- Public–private partnerships (PPP)
- International capacity-building initiatives

Table of Contents

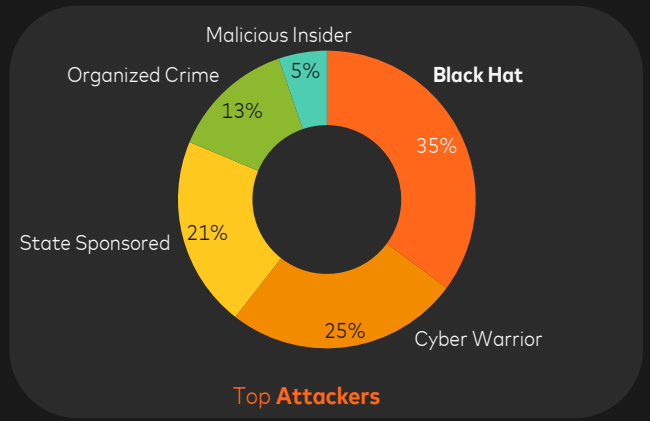
UAE threat landscape breakdown: Industries, Assets, Attackers & Methods



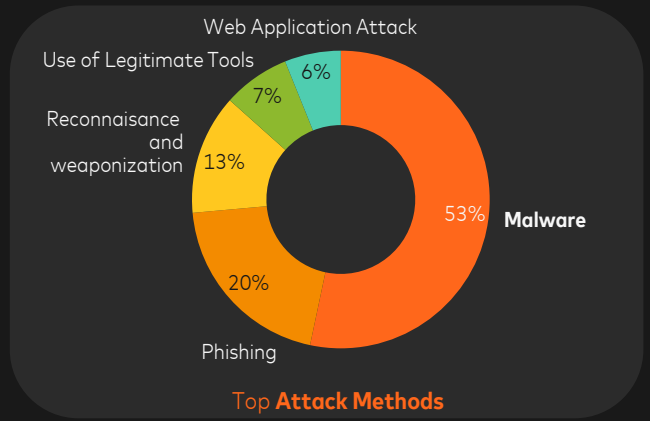
Top attacked **Industries**



Top attacked **Assets**



Top **Attackers**



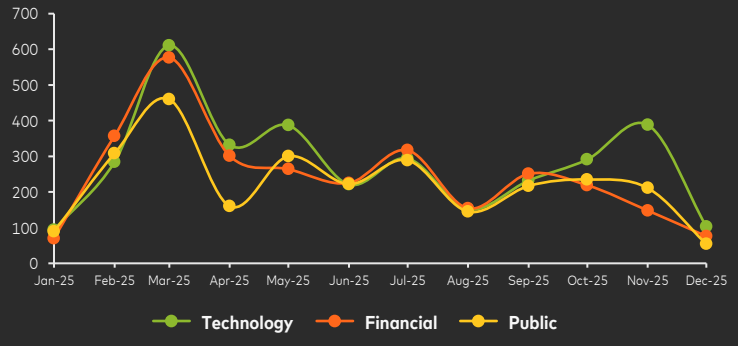
Top **Attack Methods**

KEY INSIGHTS

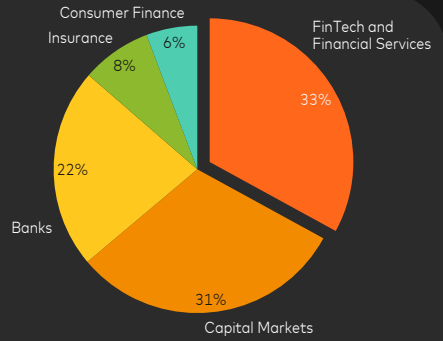
- Technology, Financial Services, and Public Sector faced 70% of the attacks in 2025. Due to the importance of these sectors and the sensitive nature of the data they hold, they are considered high-value targets by cybercriminals.
- Business systems, customer data, and physical infrastructure were the top targets, accounting for 61% of asset-focused attacks.
- Most threat actors fall into the categories of Black Hat, Cyber Warriors, State-sponsored groups, and Organized crime groups.
- To address this complex threat landscape, the UAE has stipulated standards for critical infrastructure protection, developed a National SOC and launched national awareness and compliance programs.

Source: Mastercard Cyber Insights Data (Jan–Dec 2025)

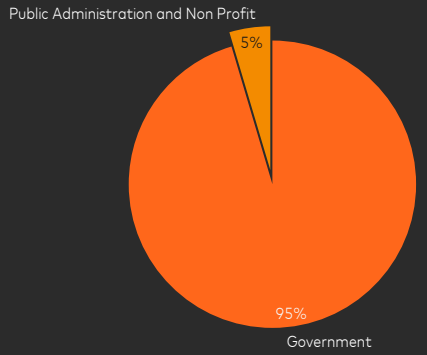
Distribution of attacks in Finance, Technology, and Public sectors



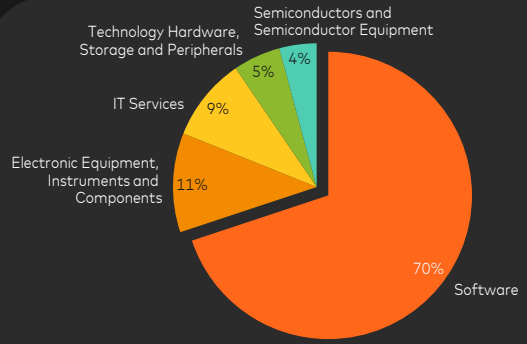
Distribution of attacks across top 3 targeted industries



Distribution of attacks in the Financial sector



Distribution of attacks in the Public sector



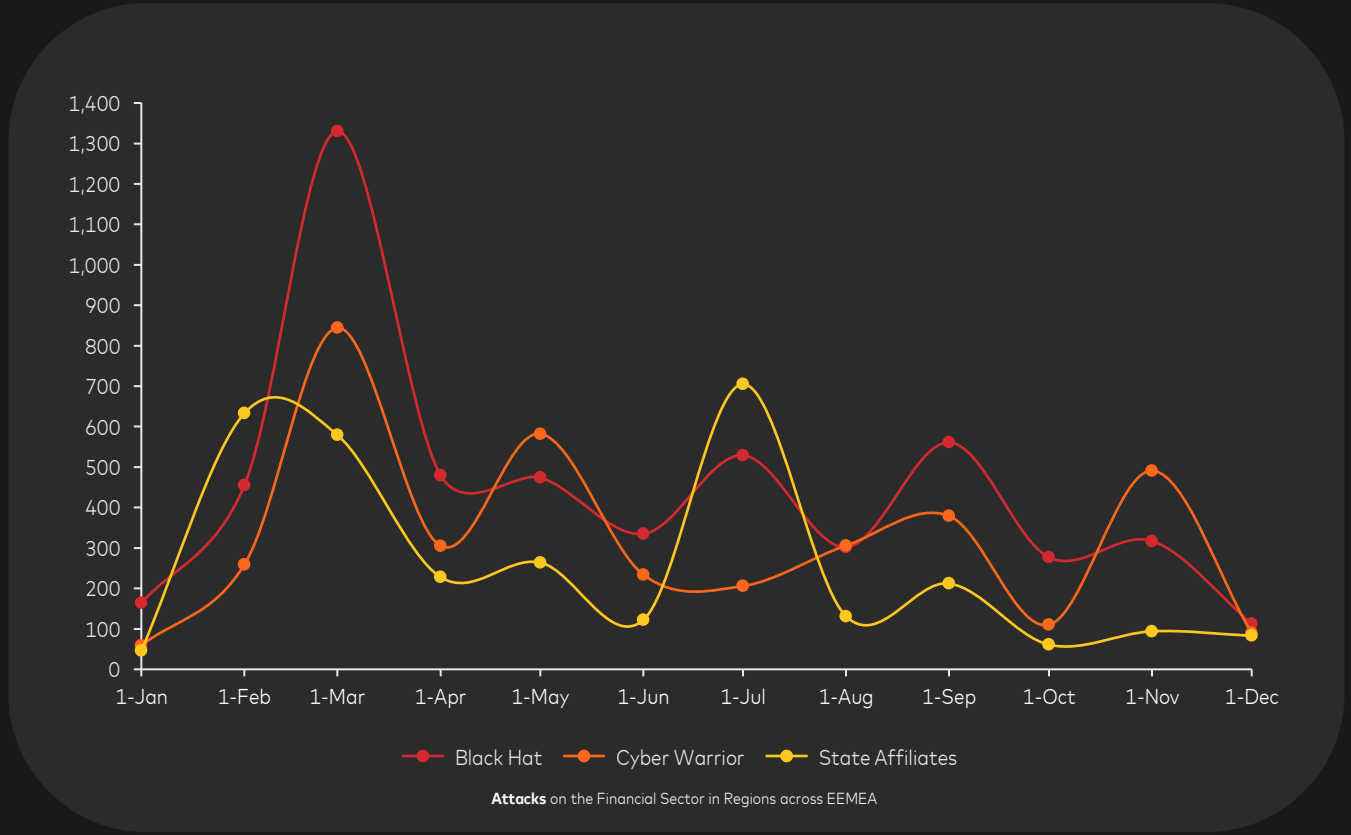
Distribution of attacks in the Technology sector

KEY INSIGHTS

- Organizations in the Technology sector were targeted most frequently, followed by those in the Financial and Public sectors. Service and Industrial sector organizations also experienced a notable share of cyberattack activity.
- In the Financial sector, attackers primarily focused on organizations in the FinTech and Capital markets.
- Most attacks in the Public sector targeted Government operations, public administration systems, and non-profit entities.
- Within the Technology sector, software companies, electronic equipment providers, and IT service firms were the most targeted.

Source: Mastercard Cyber Insights Data (Jan–Dec 2025)

Most active threat actor groups: Black Hat, Cyber Warriors and State Affiliates



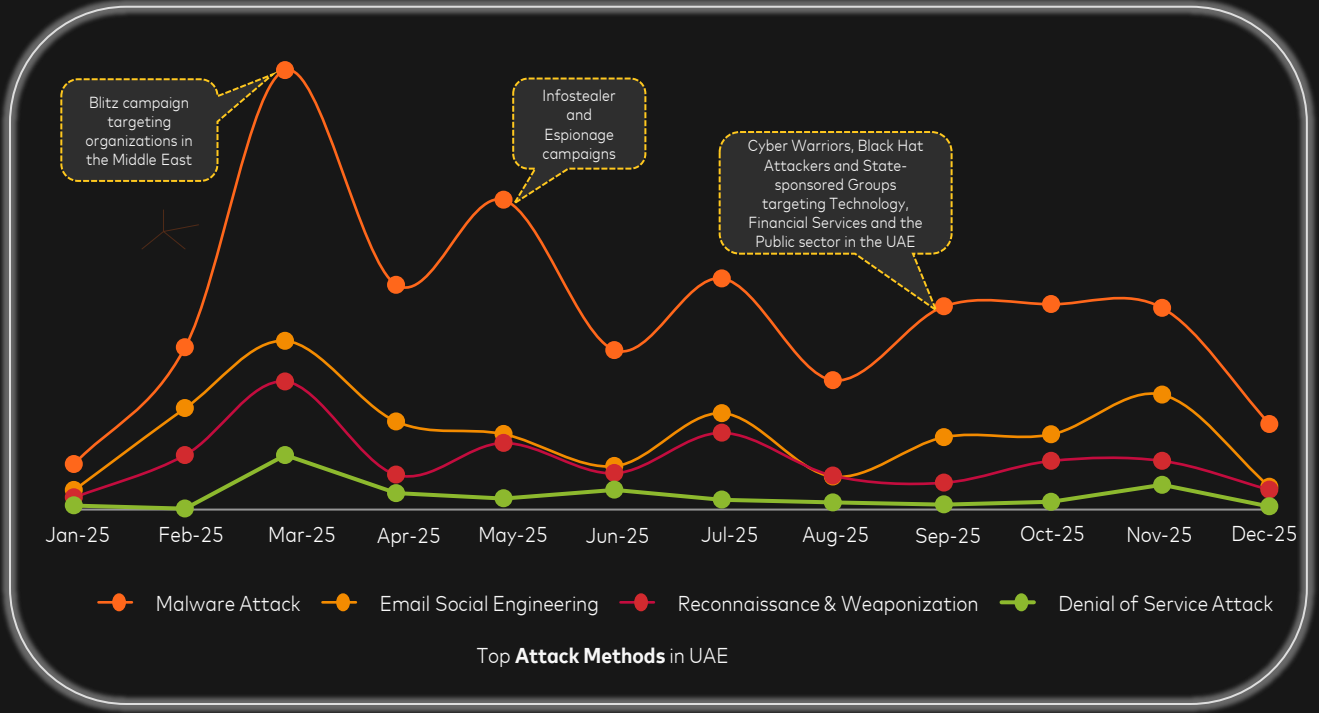
Attacks on the Financial Sector in Regions across EEMEA

KEY INSIGHTS

- Black Hat hackers, driven by financial gain, often target business systems and data-rich environments using ransomware, infostealers, and weaponized AI.
- Cyber Warriors, often ideologically motivated, focused on public-facing services and cloud infrastructure, using trojans, spyware and application vulnerability exploitation.
- State-sponsored groups pursue strategic objectives like espionage and disruption, targeting critical infrastructure with malware and social engineering.
- In response, the UAE has prioritized threat intelligence sharing, international coordination, and cyber crisis simulation exercises to improve readiness against diverse threat actors, while reinforcing national monitoring and response capabilities through NSOC.

Source: Mastercard Cyber Insights Data (Jan–Dec 2025)

Most prevalent attack methods in the UAE



Top **Attack Methods** in UAE

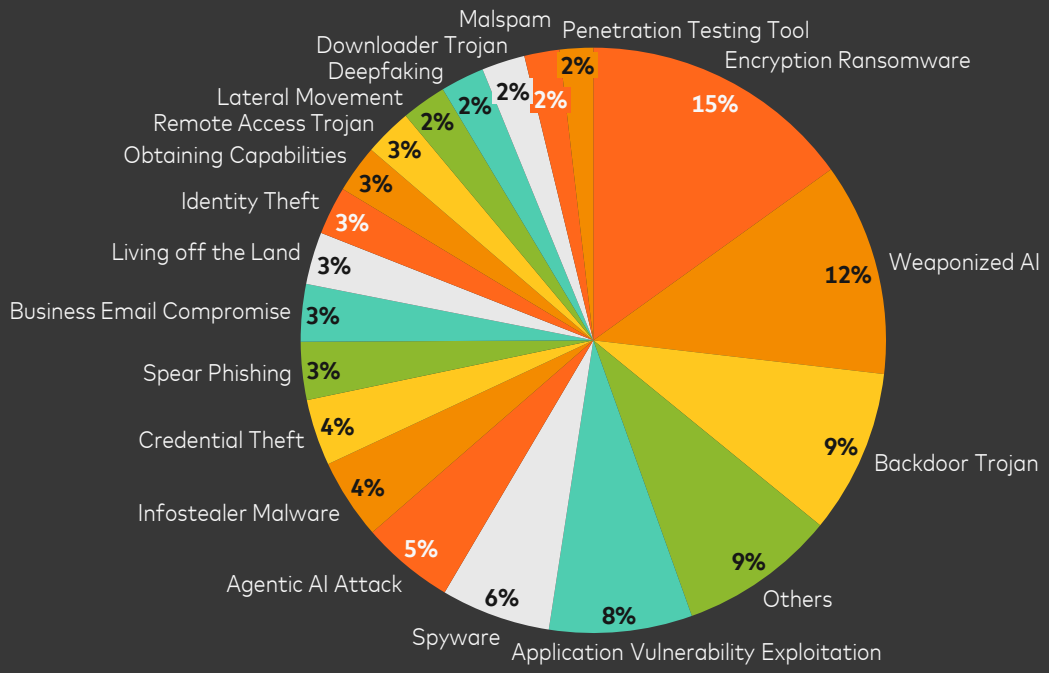
- Malware*: Malicious software designed to infiltrate, damage, or disrupt systems, often used for data theft or extortion, including forms such as ransomware, trojans, and viruses
- Email Social Engineering: Deceptive emails crafted to trick recipients into revealing sensitive information or clicking malicious links.
- Reconnaissance and Weaponization: Early-stage attacker activities involving information gathering and preparing tools or exploits for targeted attacks.
- Denial of Service (DoS) Attack: An attempt to overwhelm a system or network with excessive traffic, rendering it unavailable to users.

KEY INSIGHTS

- Attack volumes fluctuated throughout 2025, with notable spikes in February, March, May, and November, indicating campaign-driven surges rather than seasonal patterns.
- Attackers relied heavily on malware (especially ransomware), phishing, and reconnaissance as primary tactics.
- To counter these evolving threats, the UAE has enhanced real-time monitoring through the National Security Operations Center (NSOC), enabling early detection of campaign-based surges and rapid incident response across sectors. Similarly, nationwide awareness campaigns and capacity-building programs were launched to educate citizens and organizations on recognizing and preventing phishing attacks.

Source: Mastercard Cyber Insights Data (Jan–Dec 2025)

Key cyber attack vectors targeting the UAE



KEY INSIGHTS

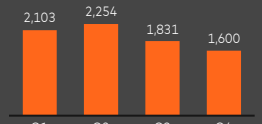
- **Encryption Ransomware accounts for the largest share of activity**. This indicates that high-impact, financially motivated ransomware operations remain a primary concern for organizations.
- **AI-enabled attack vectors are gaining prominence, with Weaponized AI forming the second-largest category.** This reflects a growing shift toward automated, adaptive, and more sophisticated offensive techniques.
- **Traditional intrusion methods continue to play a major role**, including Backdoor Trojans, application vulnerability exploitation, and spyware. These longstanding tactics remain effective and widely used by threat actors.
- **Identity and access-based threats** remain prevalent. Credential theft, spear phishing, business email compromise, and identity theft contribute a significant portion of overall activity.

Source: Mastercard Cyber Insights Data (Jan–Dec 2025)

Malware including ransomware was the most common attack method

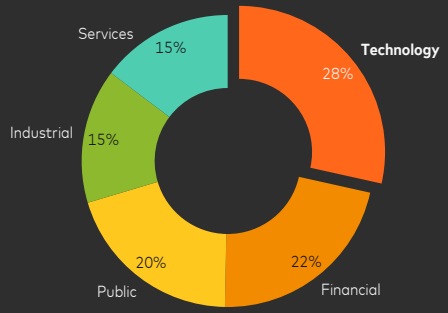
KEY INSIGHTS

Malware was the most common attack method used in the UAE, with data showing a sharp increase in attacks during March 2025.

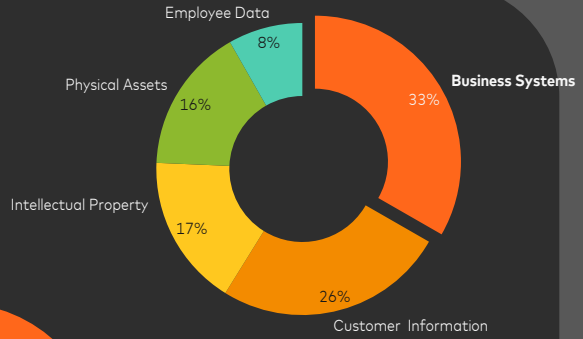


Malware attack trend in UAE

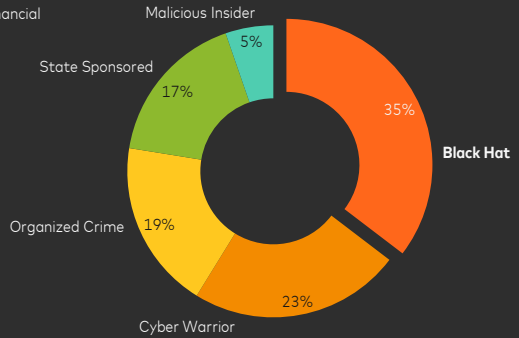
The Technology and Financial sectors remain a primary target, as Cyber Warriors and Black Hat attackers focus on compromising business-critical systems and customer information.



Top industries targeted using malware



Top assets targeted using malware



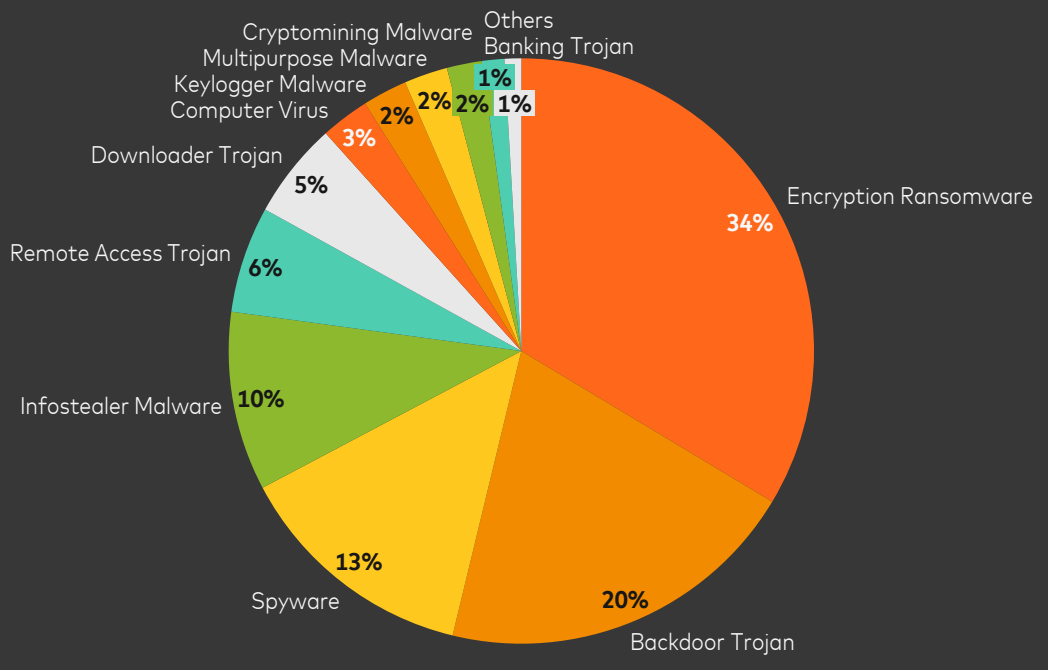
Top adversaries using malware

Source: Mastercard Cyber Insights Data (Jan–Dec 2025)

Encryption-Driven ransomware leads malware activity in the UAE

KEY INSIGHTS

- **Encryption-based ransomware** remains the dominant **malware threat**, underscoring the attackers' continued focus on high-impact, financially motivated operations. This reflects a sustained shift towards disruptive extortion tactics that directly target business-critical systems.
- The prevalence of **backdoors**, **spyware**, and **infostealers** shows that adversaries are not only seeking immediate disruption, but also long-term access, credential harvesting, and covert data exfiltration. Their combined use strengthens attacker persistence and increases the likelihood of multi-stage compromise.
- The malware landscape targeting UAE organizations continues to diversify, with multiple ransomware strains and supporting toolkits contributing to a complex and evolving threat environment. This trend points to higher operational risk, particularly for sectors with expansive digital footprints.



Distribution of types of malware

Source: Mastercard Cyber Insights Data (Jan–Dec 2025)

Key Recommendations

Based on the evolving threat landscape outlined in this report, these best practices represent key actions organizations can take to strengthen their cyber resilience. It is encouraging to see that the UAE has already launched national initiatives aligned with each of these areas — demonstrating a proactive and structured approach to securing the Country's digital ecosystem.

WHAT ORGANIZATIONS NEED TO DO

Proactive Threat Intelligence

Key Action: Establish real-time threat monitoring and intelligence sharing mechanisms.

Why It Matters: Enables early detection of ransomware, phishing, and APT campaigns before they escalate.

Incident Response Preparedness

Key Action: Develop and test incident response plans through simulations and cross-functional coordination.

Why It Matters: Timely containment and recovery are critical to minimizing the impact of ransomware and DDoS attacks.

Workforce Awareness & Training

Key Action: Conduct regular phishing simulations, cyber hygiene training, and executive-level tabletop exercises.

Why It Matters: Social engineering remains a top attack vector; human error is a leading cause of breaches.

Secure Digital Transformation

Key Action: Integrate security-by-design into digital initiatives, cloud adoption, and AI deployments.

Why It Matters: Expanding digital footprints increase the attack surface, especially in cloud and AI environments.

Key initiatives by the UAE supporting the recommendations

National Security Operations Center (NSOC)
A centralized hub for real-time cyber threat monitoring and incident response across national sectors.

Crystal Ball
A global cyber threat intelligence-sharing initiative enhancing visibility and collaboration across international partners.

Cyber Crisis Simulation Exercises
Regularly conducted exercises to test and improve cross-sectoral coordination and response to cyber incidents.

National Cybersecurity Governance Framework
Establishes structured roles and responsibilities for coordinated incident response across federal, emirate, and sectoral level.

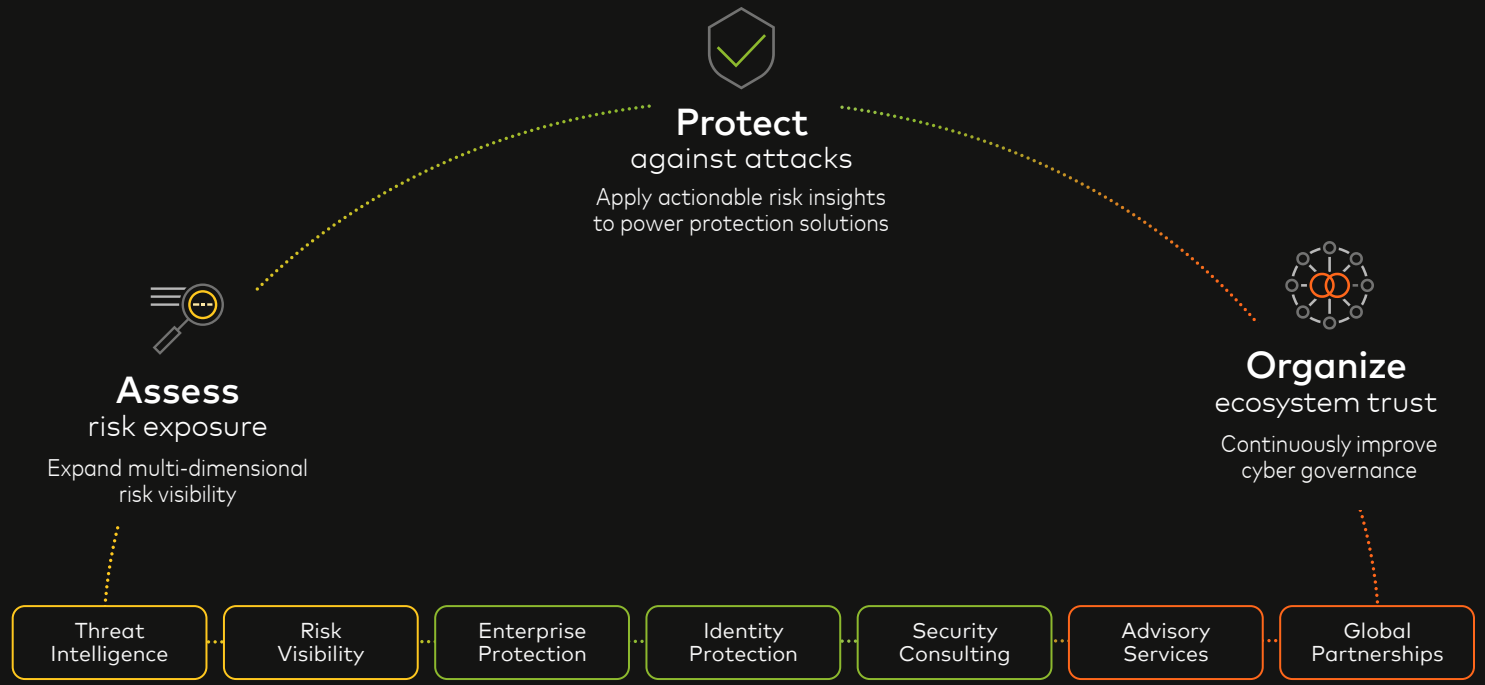
Cyber Snipers
A specialized initiative focused on building elite technical skills in areas like ethical hacking, digital forensics, and threat hunting.

Cyber Future Leaders
A national program to identify and develop cybersecurity professionals through structured learning and mentorship.

Cybersecurity Center of Excellence
Establishes national guidelines for the safe and ethical deployment of AI, OT and IIOT technologies across sectors.

Regulatory Sandboxes
Provides a controlled environment for testing emerging technologies with embedded cybersecurity requirements to ensure secure innovation.

Mastercard offers an end-to-end suite of security services across the digital ecosystem



End of the report