ZEROFOX INTELLIGENCE

Assessment

Q1 2026 MEA Cyber Threat Activity Wrap-Up

A-2026-04-24a

Classification: TLP:CLEAR

Criticality: Low

Intelligence Requirements: Ransomware, Data Breach, Threat Actor

April 24, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 7:00 AM (EDT) on April 24, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Assessment | Q1 2026 MEA Cyber Threat Activity Wrap-Up

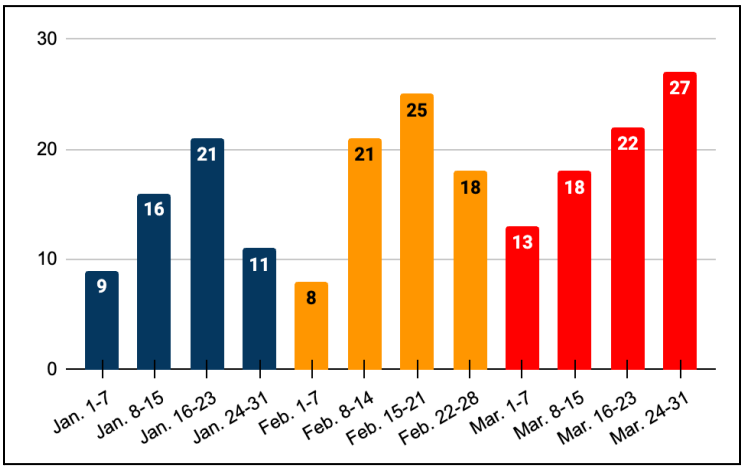
Key Findings

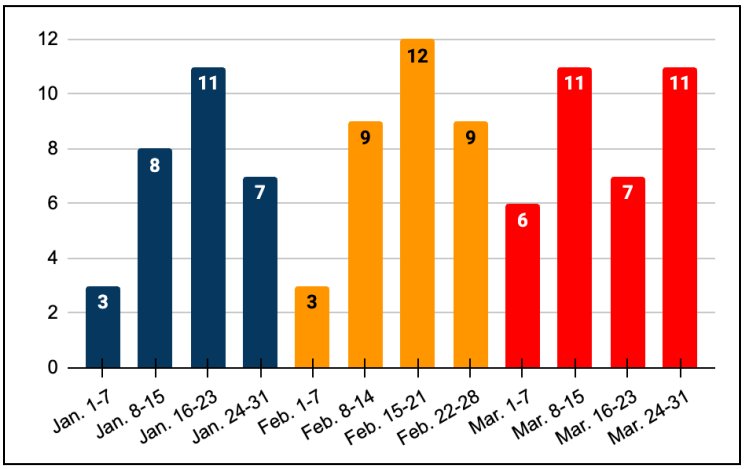
- ZeroFox observed at least 209 separate cyber threat incidents in Q1 2026 targeting Middle East and Africa (MEA)-based entities, an increase of roughly 5 percent from Q4 2025, which accounted for at least 196 incidents; and an increase of nearly 64 percent from Q1 2025 which saw at least 126 incidents.
- Notably, Iranian authorities imposed a nation-wide internet blackout on January 8, 2026, and later following the U.S. and Israeli-led strikes in Iran, the regime further restricted internet access in the nation. This very likely impacted cyber threat incident volume, especially those coming from or targeting Iran and contributed to less incidents than anticipated for Q1 2026.
- In Q1 2026, government organizations continued to represent the most targeted victims for threat actors in MEA. This sustained targeting is likely driven by factors such as regional and international geopolitical tensions and conflict. MEA is the only region where government organizations are the most targeted industry.
- ZeroFox observed that the five most active threat collectives in Q1 2026 for MEA were almost certainly The Gentlemen, Handala Hack, TENGU, LockBit and INC Ransom—with Handala likely to continue to serve as a key instrument for Iranian state-sponsored cyberattacks.

Q1 2026 Overview

ZeroFox observed at least 209 separate cyber threat incidents in Q1 2026 targeting MEA-based entities, an increase of roughly 5 percent from Q4 2025, which accounted for at least 196 incidents; and an increase of nearly 64 percent from Q1 2025 which saw at least 126 incidents. Globally, ZeroFox observed at least 3,039 separate cyber incidents in Q1 2026, notably MEA represents approximately 7 percent of all regional targeting.

- Observed cyber threat incidents include ransomware and digital extortion (R&DE), initial access broker (IAB) sales, data leaks and data breaches.
- The MEA region was disproportionately targeted by ransomware—which accounted for at least 97 incidents, and constituted approximately 46 percent of all incidents in Q1 2026.
- Notably, Iranian authorities imposed a nation-wide internet blackout on January 8, 2026, and later following the U.S. and Israeli-led strikes in Iran, the regime further restricted internet access in the nation. This very likely impacted cyber threat incident volume, especially those coming from or targeting Iran and contributed to less incidents than anticipated for Q1 2026.

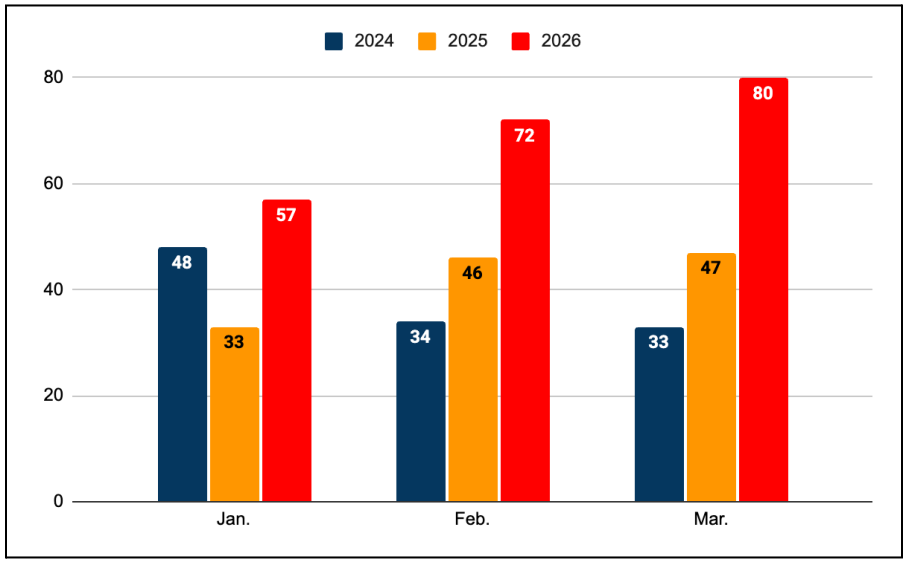




Q1 2026 total (left) and R&DE specific (right) MEA-based cyber incidents by week

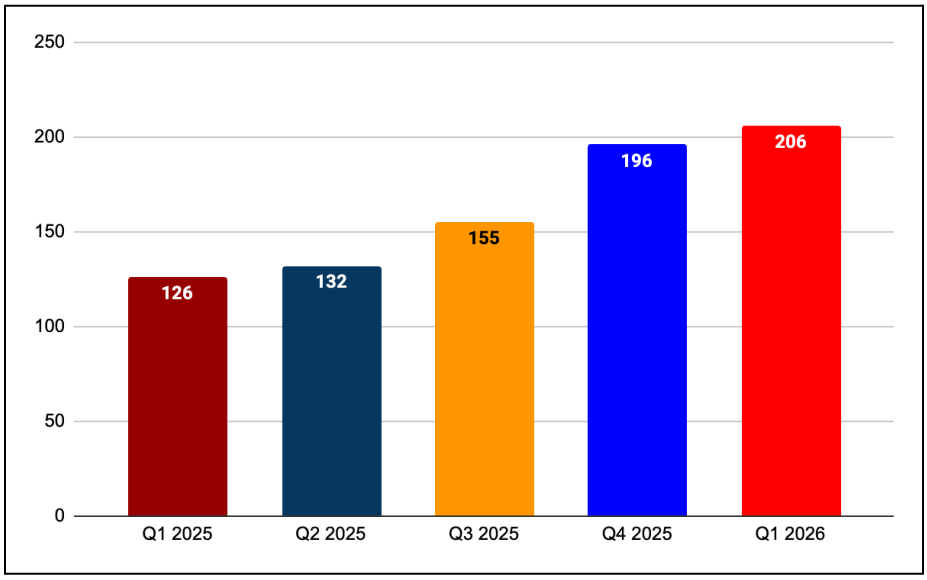
Source: ZeroFox Intelligence

Cyber-related attacks targeting MEA-based victims in Q1 witnessed a slight increase from 2024 to 2025, accounting for at least 115 to 126, respectively. However, there was a significant increase in Q1 2026, which accounted for at least 209 incidents—representing approximately a 64 percent increase from Q1 2025. Comparatively, there was only an increase of approximately 6 percent of attacks globally from Q1 2025 to Q1 2026—accounting for at least 2,870 and 3,039 incidents respectively.



Q1 MEA cyber incidents from 2024–2026 by month

Source: ZeroFox Intelligence



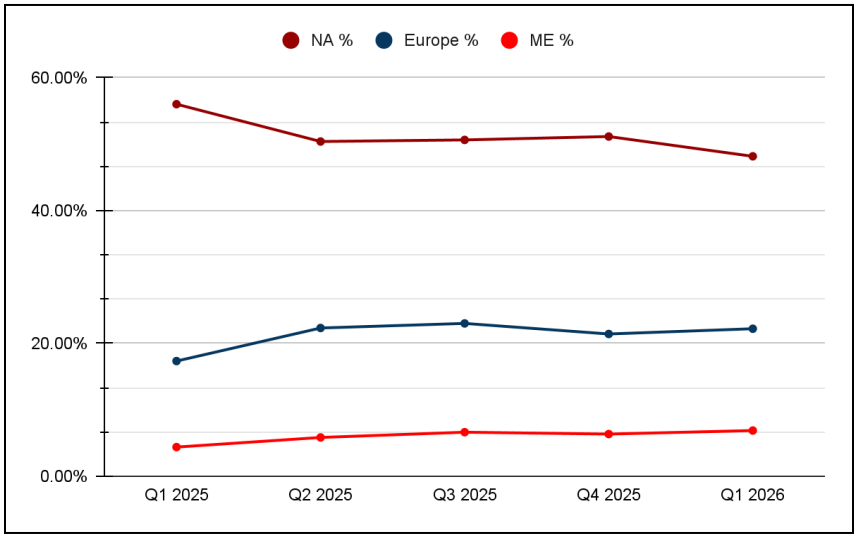
MEA incidents by quarter

Source: ZeroFox Intelligence

Regional Trends

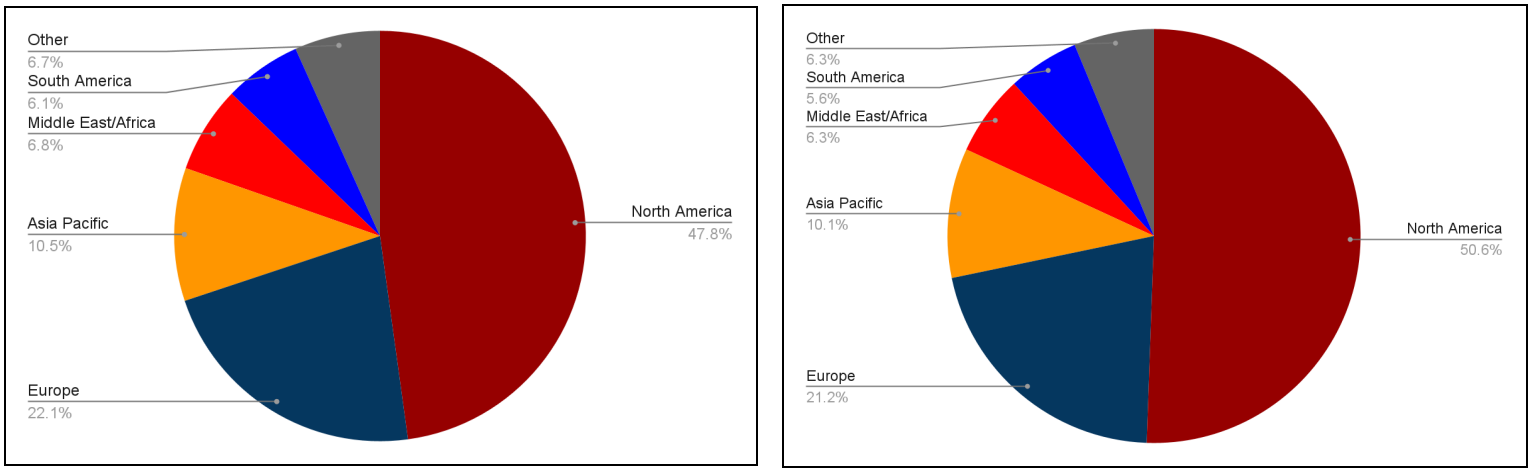
MEA has experienced significant growth in targeting volume over the last two years—from Q1 2024 to Q1 2026 MEA's volume of cyber threat incidents has increased 82 percent. Despite MEA's smaller share of approximately 4-6.8 percent cyber threat incidents since 2024; North America and Europe comparatively have maintained a steady and significant share of approximately 70-74 percent of all incidents in the same time period.

- In Q1 2026 MEA represented roughly 6.8 percent of all cyber threat incidents observed throughout the quarter, compared to North America which represented 47.8 percent and Europe represented 22.2 percent of all incidents, respectively.
- Notably, since 2024 while North America's absolute numbers remain the utmost, its percentage share is slightly declining over quarters; whereas MEA's is gradually increasing—only having experienced a minor dip in Q4 2025.
- North America experienced a proportional 9 percent decrease in Q1 2026 from Q1 2025; which is very likely attributed to a slight targeting shift towards MEA-based entities in light of the military conflict in Iran.



Percentage share of global incidents between North America, Europe, and MEA

Source: ZeroFox Intelligence



Q1 2026 (left) and Q4 2025 (right) total cyber incidents by region

Source: ZeroFox Intelligence

In Q1 2026, there were at least 209 separate cyber threat incidents targeting the MEA region, which represents nearly 38 percent more incidents than its 2025 quarterly average of approximately 152 incidents. If the volume of incidents in Q1 2026 were to persist at the same pace, then MEA could likely experience a projected 836 incidents in 2026, compared to a total of 609 incidents in 2025. However, there is a roughly even chance that Q1 2026's pace continues throughout this year, as geopolitical events heavily influence hacktivism, and other cyber threats.

- As the U.S. and Israeli-led conflict either evolves or diminishes, this activity will likely fluctuate MEA's 2026 cyber threat incident volume.

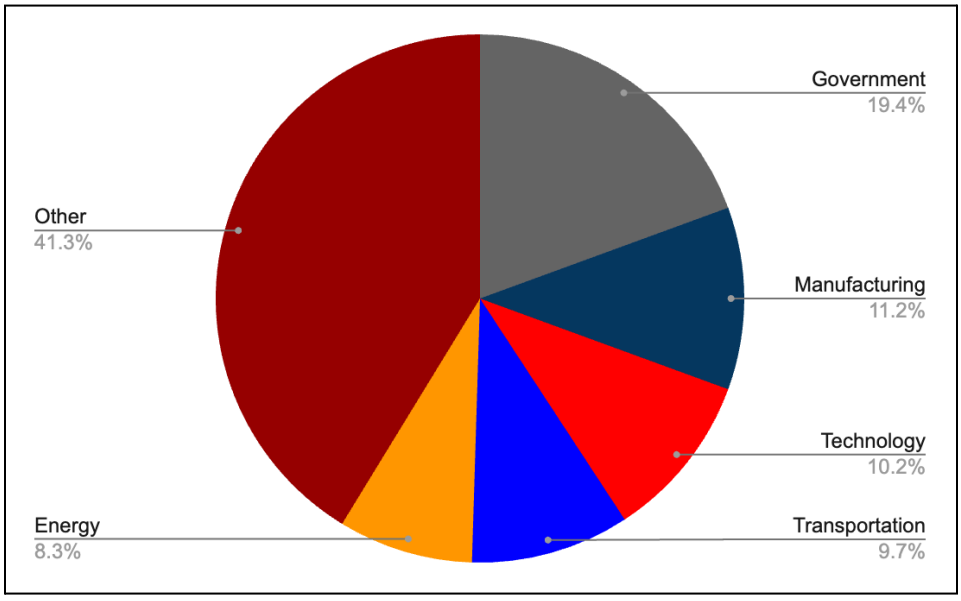
Since at least 2022, North America and Europe have dominated the cyber threat incident charts; however, as North America experiences slight decreases and with Europe's remaining steady, this likely signifies a slight structural shift or potentially an increasing shift away from disproportionate North American targeting.

Industry Trends

In Q1 2026, government organizations based in the MEA were targeted by a higher number of incidents than those in other industries, totaling at least 40 incidents (an increase from the 30 observed in Q4 2025). However, this represents a greater proportion of attacks, increasing from approximately 15 percent in Q4 2025 to approximately 19

percent in Q1 2025. Government organizations have consistently been the most targeted industry since at least 2024. Roughly 11 percent of all incidents targeted entities in the manufacturing industry in Q1 2026, which is consistent with the approximately 10 percent ZeroFox observed in Q4 2025.

- In Q1 2026, government organizations continued to represent the most targeted victims for threat actors in MEA. This sustained targeting is likely driven by factors such as regional and international geopolitical tensions and conflict. MEA is the only region where government organizations are the most targeted industry.
- Heavily targeted industries in Q1 2026 include government, manufacturing, technology, transportation, and energy; together, attacks on these industries accounted for approximately 59 percent of all incidents.
- Government, manufacturing, and technology remained the most targeted industries in Q4 2025 as in Q1 2026.



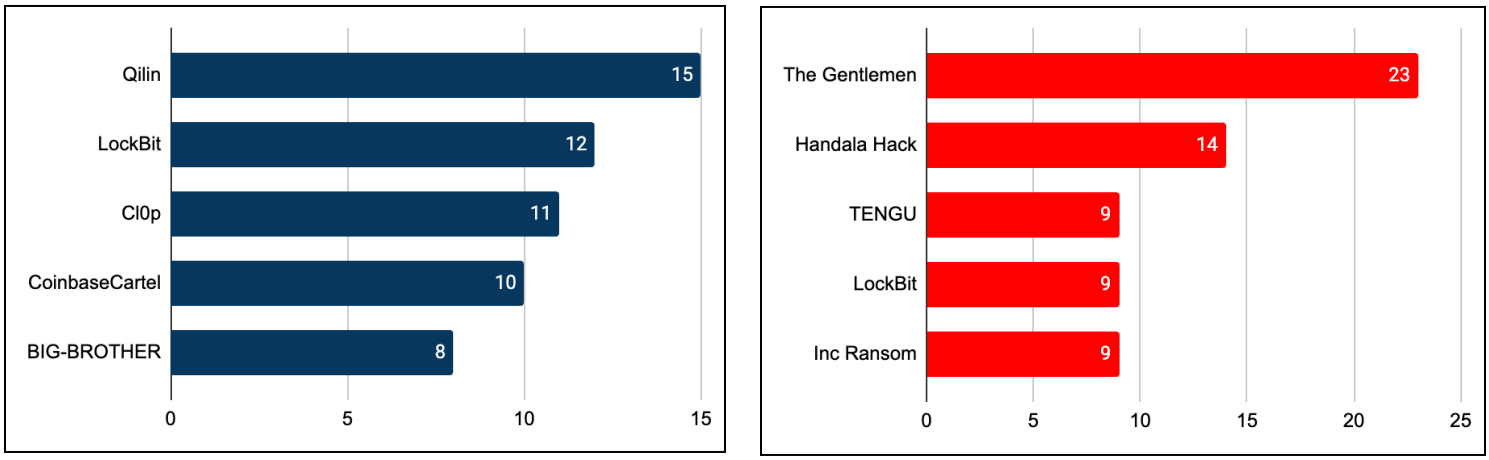
Most heavily targeted industries in MEA, Q1 2026

Source: ZeroFox Intelligence

Prominent Collectives

ZeroFox observed that the five most active threat collectives in Q1 2026 for MEA were almost certainly The Gentlemen, Handala Hack, TENGU, LockBit and INC Ransom. This is a change from Q4 2025, with only LockBit remaining in the top five from the previous quarter. These top five most prominent collectives accounted for approximately 31 percent of all attacks to MEA-based entities in Q1 2026 and were responsible for a combined total of at least 64 incidents.

- The Gentlemen was the most prominent threat collective targeting MEA-based victims in Q1 2026, accounting for at least 23 incidents-all of which were R&DE operations.



Top five most prominent collectives in Q4 2025 (left) and Q1 2026 (right)

Source: ZeroFox Intelligence

Handala Hack

Handala Hack Team (Handala) is a pro-Palestinian threat collective that employs phishing, data theft, and custom wiper malware against organizations they perceive to be pro-Israel or pro-U.S. However, it is likely that the group is a state-sponsored entity linked to Iran's Ministry of Intelligence and Security (MOIS), utilizing this front to obfuscate attribution and gain notoriety.

Handala primarily claimed responsibility for targeting Israel-based entities, though prominent organizations in the U.S. and the wider Middle East have also been allegedly

compromised. The group heavily focuses on exfiltrating and leaking internal or classified information associated with the Israeli government—specifically targeting intelligence agencies like Mossad. Broadly, Handala targets high-profile entities whose compromise generates significant media attention and aligns with Iranian state interests. The group's data leaks typically include video recordings, screenshots, contact lists, and internal communications.

- Furthermore, Handala recently launched a targeted doxxing and bounty operation dubbed "Handala RedWanted," designed to expose individuals associated with the Israeli military and intelligence community. The dedicated clear-web site hosts the personal data of over 200 individuals across 19 pages, arranged in a gallery format. Each entry allegedly displays the target's identity, operational history, and professional network.

Handala Hack is likely linked to MOIS, operating alongside other alleged state-backed hacktivist fronts such as HomeLand Justice (HLJ) and Karma_Below80 (Karma). Notably, these three collectives are likely operated by or otherwise affiliated with Void Manticore, an Iranian Advanced Persistent Threat (APT) group also reportedly affiliated with MOIS.

- Significantly, while these three groups project slightly different public stances—such as HLJ targeting Albania and entities associated with the Mojahedin-e-Khalq (MEK / People's Mojahedin Organization of Iran), and Karma targeting Israel claiming that they are "Anti-Zionist Jewish Hackers"—they all consistently execute operations that align with pro-Iranian interests, primarily targeting entities or regions that oppose the regime.
- Furthermore, previous reporting indicates significant operational overlap among these groups. Karma and Handala are believed to share victim targeting profiles, while HLJ and Karma reportedly exhibit overlaps in their malware code. Ultimately, all three hacktivist personas reportedly share identical Tactics, Techniques, and Procedures (TTPs), reinforcing the assessment that they are operated by the same central MOIS-linked apparatus.

Tactics, Techniques, and Procedures:

Handala reportedly gains initial access via spear-phishing attachments and relies heavily on command interpreters—specifically AutoHotKey and AutoIT scripts—to execute payloads. To bypass security controls, the group is believed to utilize file obfuscation, time-based evasion tactics, and Bring Your Own Vulnerable Driver (BYOVD) exploits for privilege escalation.

After actively gathering victim network and identity information, the attack chain is reported to culminate in automated data exfiltration followed immediately by a destructive disk structure wipe. Because Handala and their other personas (like Karma and HLJ) are assessed to be operated by the same underlying APT, it is highly probable they share a centralized malware repository, enabling Handala to deploy shared tools such as the BiBi and Hatef wipers.

Abuse of Endpoint Management Software:

On April 7, 2026, the Cybersecurity and Infrastructure Security Agency (CISA) issued an alert regarding the group's alleged compromise of legitimate endpoint management software employed by the targeted companies.[1]

In response to this abuse of centralized administrative tools, CISA strongly recommends organizations harden their endpoint management software and identity and access management environments. To prevent the mass-deployment of wipers, security teams should immediately implement:

- Multi-Admin Approval: Mandate a second administrator's approval for high-impact actions, specifically broad configuration changes or mass device wiping.
- Strict Role-Based Access Control (RBAC): Enforce the principle of least privilege, ensuring administrative roles possess only the minimum permissions necessary for daily operations.
- Phishing-Resistant MFA: Utilize risk signals and conditional access controls to block unauthorized access to highly privileged administrative accounts.

[1] hXXps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa26-097a

Preliminary Malware Analysis:

As a primary operator of the Void Manticore malware repository, Handala reportedly deploys custom destructive payloads, most notably the Hatef wiper. Recent static malware analysis reveals that Hatef is likely designed for rapid, widespread data destruction and relies heavily on opportunistic social engineering and trust abuse to achieve execution.

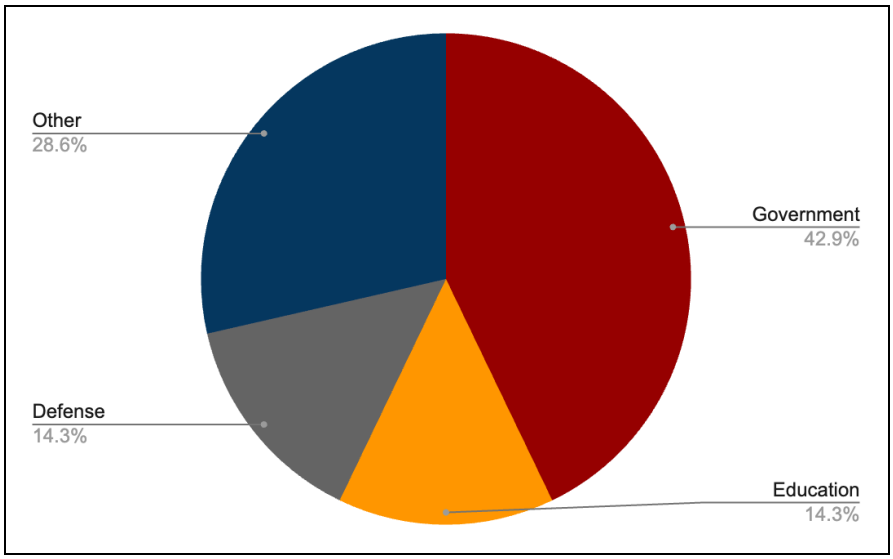
Packaging and Evasion:

- To hinder static analysis and evade signature-based detection, the core Hatef payload is typically packaged within a legitimate Nullsoft Scriptable Install System (NSIS) wrapper.
- The threat actor abuses this framework as a dropper to obfuscate the underlying wiper code, write necessary registry keys, and execute the payload seamlessly.
- Furthermore, Handala actively mimics trusted entities to bypass Endpoint Detection and Response (EDR) solutions and Windows Mark-of-the-Web (MotW) protections.
- Recent variants have been observed masquerading as critical IT patches (e.g., CrowdStrike Updater.exe) and utilizing spoofed or stolen digital certificates associated with reputable software vendors, such as VideoLAN.

Execution and Impact:

Upon execution, the malware manipulates process access tokens to grant itself high-level system permissions, specifically requesting privileges required to force system shutdowns (SeShutdownPrivilege). It subsequently enumerates all running processes, highly likely to identify and terminate security agents or database services that might place file locks on targeted data.

Because the Windows operating system protects critical files while running, Hatef queries local and attached storage capacities to map its wiping radius, then utilizes the MoveFileExW API to stage protected files for deletion during the next boot sequence. The malware then forces a system restart (ExitWindowsEx) to finalize the destructive routine, effectively rendering the host machine unbootable and the data unrecoverable.



Handala Hack's most targeted industries in MEA, Q1 2026

Source: ZeroFox Intelligence

Analyst Note:

Handala will likely continue to serve as a key instrument for Iranian state-sponsored cyberattacks. Unlike traditional ideological hacktivists who typically attempt to minimize civilian impact, Handala's operations frequently result in widespread collateral damage. For example, the group's alleged cyberattacks against Jerusalem's municipal camera networks, the Hebrew University of Jerusalem, and local water supply facilities demonstrate a pattern of mirrored retaliatory targeting, rather than the precision targeting of specific government or military entities that have direct influence over the conflict

- This calculated disregard for non-combatants further reinforces the assessment that Handala is not driven by grassroots ideology. Furthermore, the group's publication of close-up imagery from kinetic strike zones—such as the rubble associated with Ali Larijani's recent death—likely suggests direct state coordination.

Conclusion:

Crucially, while Handala frequently broadcasts highly publicized claims of compromising prominent entities, analysts have observed a consistent discrepancy between the

magnitude of these assertions and the actual volume of exfiltrated data. The relatively smaller size of their published datasets strongly suggests that the group often exaggerates the scale, depth, and occasionally the authenticity of its intrusions.

This pattern of capability inflation is a hallmark of psychological operations designed to project an outsized threat. As geopolitical tensions persist, it is very likely the group will maintain its current operational tempo—blending legitimate, albeit often shallower, intrusions with exaggerated public claims—to project power and preserve plausible deniability for the Iranian regime.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%