Latest Cyber Threat Intelligence & Security Insights

Archived: 2026-04-29 02:06:22 UTC

The geopolitical landscape of 2026 has been fundamentally reshaped by the convergence of kinetic military operations and systemic digital suppression, a phenomenon most acutely visible in the ongoing tensions between the Islamic Republic of Iran, Israel, and the United States. In the wake of Operation Epic Fury—the coordinated U.S.-Israeli airstrikes on Iranian infrastructure in early 2026—the global community has observed a peculiar divergence in the prominence of cyber warfare. While the conflicts in Ukraine and the Gaza Strip have featured highly visible, destructive, and persistent cyber campaigns that dominate international headlines, Iran’s cyber response has often appeared muted or recessed into a state of "digital isolation". This perceived lack of prominence is not a reflection of diminished capability—Iran remains a top-tier global cyber power—but is rather the result of a deliberate strategic doctrine centered on the National Information Network (NIN) and the systemic use of internet blackouts to insulate the regime from external digital and psychological pressure.

The Mechanics of Digital Sovereignty: Iran’s National Information Network

The centerpiece of Iran’s defensive cyber strategy is the National Information Network (NIN), a multi-layered domestic infrastructure designed to achieve what the regime terms "digital sovereignty". Unlike standard internet filtering, the NIN is a comprehensive re-engineering of the nation’s telecommunications gateways, allowing the state to decouple domestic traffic from the global World Wide Web while maintaining the functionality of essential internal services. During the heightened conflict of June 2025, often referred to as the "Twelve-Day War," the Iranian government enacted its most comprehensive internet disruption to date, shifting the entire country toward a full reliance on the NIN. This transition is achieved through a sophisticated array of technical maneuvers, including DNS injection, BGP (Border Gateway Protocol) manipulation, and the nationwide suppression of specific transport layer protocols.

The technical execution of these blackouts follows a regimented, three-stage implementation process designed to minimize the surface area for external cyberattacks and domestic dissent. In the initial phase, authorities utilize Deep Packet Inspection (DPI) to perform "soft throttling," deliberately slowing connectivity to external platforms while monitoring traffic patterns for signs of coordinated opposition. As tensions escalate, the state moves to protocol suppression, specifically targeting secure and speed-optimized protocols such as HTTP/3 and IPv6. These protocols are often blocked nationwide because their encryption and advanced header structures make them difficult for state sensors to intercept and analyze. By forcing traffic back to legacy protocols like HTTP/1.x, the regime ensures that all digital communication remains traceable and manageable within the borders of the NIN.

Technical Layer of NIN	Controlled Mechanism	Strategic Outcome
Routing Layer	BGP Hijacking and National Gateway Sealing	Complete severance of international data paths; enforcement of internal-only routing.
DNS Layer	DNS Injection and Recursive Resolver Hijacking	Redirection of users to state-sanctioned mirrors; prevention of external IP resolution.
Protocol Layer	Suppression of HTTP/3 and IPv6; Legacy Rollback	Enhanced traceability for state monitoring; reduction of "blind spots" in encrypted traffic.
Application Layer	DPI-based Throttling and White-Listing	Prioritization of domestic banking, religious, and government apps over foreign platforms.

The resilience of the NIN is complicated by "hardware decay" and the regime's forced reliance on gray-market equipment. Due to international sanctions, Iranian network administrators frequently use second-hand or smuggled hardware, which leads to an unstable architecture characterized by erratic speeds and frequent DNS resolution failures even when the network is technically operational. This fragility creates a paradox: while the NIN acts as a "digital redoubt" that protects the state from external cyber intrusions, it also degrades the regime's own ability to coordinate sophisticated offensive operations from within its borders. During the March 2026 blackouts, nationwide connectivity dropped to between 1 and 4 percent of normal levels, a move intended to control the internal flow of information but which simultaneously hindered the agility of state-aligned cyber units.

Comparative Prominence: The Doctrine of Asymmetric Obscurity

A recurring theme in threat intelligence analysis is the comparison between Iran’s cyber activities and those observed in the Russia-Ukraine and Israel-Palestine crises. The consensus among researchers is that while Russia and Ukraine engage in high-visibility "total cyber war," Iran operates within a framework of "asymmetric obscurity". In Ukraine, cyber warfare is utilized as a precursor and supplement to kinetic invasion, with Russian units like Sandworm targeting electric grids, satellite communications, and government databases to cause immediate, observable chaos. Similarly, the conflict between Israel and Hamas features highly synchronized digital-kinetic strikes, where cyber operations are used to disrupt real-time communications and sensors ahead of airstrikes.

In contrast, Iran’s cyber doctrine is shaped by its lack of symmetric conventional options. Because the Iranian regime cannot match the conventional military power of the United States or Israel, it utilizes cyber as a tool of "managed escalation" and plausible deniability. The perceived lack of prominence in Iranian cyber warfare is a byproduct of three primary factors:

1. **Defensive Prioritization:** Iran views the internet primarily as a vector for "soft war" (psychological operations) aimed at regime change. Consequently, its first instinct during a crisis is to shut down the network rather than project power through it.

2. **Devolved Proxy Ecosystem:** To maintain operations during domestic blackouts, Iran relies on a dispersed network of proxies and hacktivist personas who operate from outside the country. These actors provide a layer of

insulation, making their activities appear as grassroots activism rather than state-sponsored warfare.

3. **Strategic Timing:** Unlike the constant barrage of Russian wiper malware in Ukraine, Iranian actors like MuddyWater or OilRig often prioritize long-term espionage and "pre-positioning" in critical infrastructure. Their attacks are timed for maximum psychological impact rather than tactical military gain, leading to long periods of apparent inactivity followed by sudden, highly publicized leaks.

The "Twelve-Day War" of 2025 showcased this doctrine in practice. While Israel and pro-Israeli groups like Predatory Sparrow hit Iranian targets such as the Nobitex crypto exchange and Bank Sepah, Iran’s response focused on large-scale DDoS attacks and disinformation campaigns designed to create mass anxiety and portray the regime as a victim of Western aggression. This focus on psychological effects over kinetic-like destruction further contributes to the narrative that Iran’s cyber warfare is "less prominent" than the infrastructure-level destruction seen in Eastern Europe.

Mapping the Iranian State-Sponsored Apparatus

The Iranian cyber ecosystem is a bureaucratized military and intelligence apparatus divided primarily between the Ministry of Intelligence and Security (MOIS) and the Islamic Revolutionary Guard Corps (IRGC). Each entity manages a distinct cluster of Advanced Persistent Threat (APT) groups, each with specialized TTPs and targeting mandates.

The Ministry of Intelligence and Security (MOIS): The Espionage Experts

The MOIS operates under the civil executive branch and focuses primarily on long-term intelligence collection, regional surveillance, and the targeting of dissidents. Its most active and sophisticated clusters include MuddyWater and the "Prince of Persia" (Infy) group.

MuddyWater (Static Kitten, MERCURY)

MuddyWater is one of Iran’s most prolific actors, characterized by its agility and its ability to maintain operations even during national internet blackouts. In late 2025 and early 2026, the group was observed utilizing commercial satellite internet (Starlink) to maintain Command-and-Control (C2) after the regime severed national fiber-optic connectivity. This shift highlights a strategic maturation where MOIS units have decoupled their operational infrastructure from the domestic telecom network.

Latest TTPs (2025-2026):

- **Phishing via Compromised Accounts:** The group has moved away from generic lures to using compromised legitimate mailboxes within target organizations to send internal spearphishing emails, a technique that boasts a notably high success rate.
- **Infrastructure Masking:** MuddyWater leverages NordVPN exit nodes, specifically in France, to access and distribute phishing emails, thereby masking the origin of the attack.
- **Living off the Land (LotL):** The group integrates commercial RMM (Remote Monitoring and Management) tools like ScreenConnect, Action1, and PDQ to maintain persistent access without deploying traditional malware.

Malware / Tool	Function	Latest IOC / File Artifact
Phoenix Backdoor (v4)	Primary C2 and data exfiltration	sysprocupdate.exe (Mutex and dropper)
Chromium_Stealer	Browser credential extraction	chromium_stealer_user.exe (Disguised as calculator)
DCHSpy	Android surveillance and WhatsApp theft	Malicious Starlink-themed VPN apps on Telegram
FakeUpdate Injector	Initial payload delivery	VBA Macros with "Enable Content" lures

Prince of Persia (Infy / Sarafraz)

The actor cluster known as "Prince of Persia" has been active for nearly two decades, specializing in high-value intelligence collection and monitoring dissidents. Recent research in 2025 revealed that the group's activity is far more expansive than previously thought, with multiple malware variants—Foudre and Tonnerre—operating in parallel.

- **Foudre (First-Stage Reconnaissance):** Version 34, identified in 2025, transitioned from macro-enabled files to Microsoft Excel documents with embedded executables. It drops a loader (Conf8830.dll) and utilizes a DLL disguised as a camouflage MP4 file to deceive users.
- **Tonnerre (Second-Stage Exploitation):** Version 50, detected in September 2025, utilizes the Telegram API for its C2 infrastructure, effectively bypassing traditional network-based monitoring. The use of a Persian username (@ehsan8999100) within the Telegram C2 group provided rare attribution clues back to the Iranian operators.

The Islamic Revolutionary Guard Corps (IRGC): The Offensive Vanguard

The IRGC units are the most aggressive in the Iranian apparatus, focusing on critical infrastructure, military capability assessment, and high-impact influence operations. The primary groups in this category are OilRig (APT34) and Charming Kitten (APT35).

APT34 (OilRig, Earth Simnavaz)

OilRig is characterized by its disciplined, long-term approach to cyber espionage, focusing heavily on energy, telecommunications, and government sectors in the Middle East. By 2025, the group had transitioned into a "highly mature threat actor," moving away from simple malware to modular development and hybrid cloud-based intrusions.

Latest IOAs and TTPs (2025):

- **Cloud Credential Abuse:** OilRig has shifted its focus to the persistent use of hacked Microsoft 365 sites and compromised Azure accounts to maintain access within target networks.
- **DNS Tunneling:** The group continues to use encrypted HTTPS traffic and DNS tunneling to bypass perimeter security, allowing their C2 traffic to blend with normal network activity.
- **Modular Malware Arsenal:** The group utilizes a suite of specialized tools, including **Tonedeaf** (HTTP-based backdoor), **Helminth** (PowerShell implant), and **Karkoff** (lightweight backdoor for command execution).

APT35 (Charming Kitten, Phosphorus, Mint Sandstorm)

A massive internal leak in late 2025 provided an unprecedented look at Charming Kitten's operations, revealing it to be a regimented, quota-driven unit within the IRGC Intelligence Organization. The leaked documents show a bureaucratized intelligence apparatus with specialized teams for reconnaissance, exploitation, and influence.

Technical Findings from the 2025 Leak:

- **Custom Frameworks:** The group developed custom phishing frameworks (e.g., HERV) and specialized Firefox add-ons to steal and replay session cookies, allowing them to bypass MFA on services like Gmail. * **Vulnerability Specialization:** Charming Kitten operators utilize detailed playbooks for exploiting specific CVEs, with a recent focus on **ConnectWise ScreenConnect (CVE-2024-1709)** and **Ivanti Connect Secure (CVE-2024-21893)**.
- **KPI-Driven Operations:** The leak included "Daily Operational Bookkeeping" and "MJD Campaign Reports," showing that operators are ranked based on lures sent, credentials captured, and mailbox "dwell times".

Vulnerability (CVE)	Affected Product	Exploitation Method
CVE-2024-1709	ConnectWise ScreenConnect	Unauthorized admin account creation via /SetupWizard.aspx.
CVE-2024-21893	Ivanti Connect Secure	Malicious XML requests to execute reverse shell Python payloads.
CVE-2012-1823	PHP-CGI (Legacy)	RCE on applications using old PHP versions; used in Jordan campaigns.
CVE-2017-11317	Telerik UI for ASP.NET	Insecure deserialization flaws used for RCE via DLL upload.

The Handala Hack: Psychological Performance vs. Tactical Reality

The hacktivist persona known as "Handala" represents a new generation of ideologically motivated cyber actors that function as a bridge between decentralized hacktivism and state-sponsored information warfare. Since its emergence in late 2023, Handala has focused almost exclusively on Israeli organizations and individuals, pairing its operations with overt pro-Iranian and pro-Palestinian messaging. However, technical analysis by firms like KELA and ESET reveals a significant gap between the group’s social media "dramatics" and its actual technical effectiveness.

The Strategy of Narrative Amplification

Handala’s operations are designed for maximum visibility rather than stealth. Every defaced website or leaked dataset serves as a message rather than a covert intelligence operation, operating on the principle that "Visibility = Power".

- **Symbolic Targeting:** The group times its operations to coincide with global media narratives or symbolic dates (e.g., Nakba Day), ensuring that even minor attacks receive international coverage.

- **Information Exaggeration:** A hallmark of Handala's strategy is the use of coordinated posts, hashtags, and "victory messages" that frequently exaggerate the magnitude of their attacks. This tactic is designed to erode public trust in institutions and instill constant digital unrest.

Debunking the Technical Claims: The Case of the "iPhone Hacks"

The most prominent example of Handala's dramatic exaggeration occurred in late 2025, when the group claimed to have fully compromised the iPhones of senior Israeli officials, including former Prime Minister Naftali Bennett and Tzachi Braverman.

- **The Technical Reality:** Investigative analysis revealed that the breach was restricted to Telegram account access only, likely achieved through **SIM swapping** or the exploitation of **SS7 signaling weaknesses** to intercept one-time passwords (OTPs).
- **The Data Mirage:** While Handala claimed to have accessed thousands of conversations and intimate photos, the leaked materials consisted mostly of empty contact cards automatically generated during Telegram synchronization. Only approximately 40 conversations contained actual messages, many of which were of limited intelligence value.
- **WordPress Vulnerabilities:** Despite their claims of high sophistication, Handala's own operational security was found to be lacking. Their primary leak site ran on WordPress and, at times, left administrative login pages exposed, revealing the user account "vie6c" as a primary operator.

Correlation with Iranian State Interests

While Handala presents itself as an independent collective, multiple indicators point to deep ties with the Iranian Ministry of Intelligence (MOIS).

- **Overlapping Brands:** Reporting associates Handala with several other Iranian-linked "front" brands, such as **Banished Kitten**, **Karma Below**, and **Homeland Justice**, all of which are used to leak data and amplify psychological impact.
- **Coordinated Campaigns:** In July 2025, Handala targeted five journalists from Iran International, an internationally-based news outlet critical of the Iranian regime. The operation, which leaked government IDs and intimate content, was further amplified by Iranian state news websites and AI chatbots, highlighting a coordinated "hack-and-leak" ecosystem.

Handala Operational Phase	Narrative Projection	Technical Reality / IOA
Initial Access	Advanced zero-day exploits on iOS	Phishing, SIM swapping, and OTP harvesting.
Data Exfiltration	Terabytes of "classified" blueprints	Recycled data and "empty" Telegram contact cards.
Ransom Phase	"Political" ransom for policy change	Psychological pressure via Telegram and BreachForums.
Attribution	Independent Palestinian hackers	MOIS-linked persona (Banished Kitten cluster).

The 2026 Shift: Geographic Expansion and OT Targeting

As the conflict between Israel and Iran transitioned into early 2026, the patterns of Iranian-aligned cyber activity underwent a significant shift. No longer confined to the immediate Israel-Iran axis, operations expanded into the Gulf states, and the focus shifted from symbolic web disruptions toward the targeting of Operational Technology (OT) and critical infrastructure.

The Expansion into the Gulf

Groups like **DieNet**, **Keymous**, and **APT IRAN** began a systematic campaign against Gulf states perceived as politically aligned with Israel or the United States, specifically **Jordan, Saudi Arabia, Bahrain, and Kuwait**.

- **Jordan as a Primary Target:** In March 2026, APT IRAN claimed a month-long intrusion into Jordanian critical infrastructure, allegedly manipulating power plant controls to reduce electricity output. DieNet expanded this campaign to include the utility and civilian sectors, sharing imagery of accessed industrial control interfaces.
- **Strategic Escalation:** Keymous declared daily targets across Kuwait and Saudi Arabia, claiming compromises of ministries of Finance, Oil, and Education. These attacks are part of a broader "multi-vector escalation" designed to demonstrate that the regional allies of the U.S. and Israel are equally vulnerable to Iranian cyber retaliation.

The Move Toward OT and Ransomware

A concerning development in 2026 is the convergence of hacktivist personas and destructive capabilities. Groups that previously focused on website defacements are now claiming access to **PLC (Programmable Logic Controller)** interfaces and energy monitoring dashboards.

- **Cyber Islamic Resistance:** This group shared screenshots allegedly showing access to VeroPoint industrial control systems, marking a significant escalation from previous campaigns.
- **Political Ransomware: INC Ransomware** and **Tarnished Scorpius** have listed Israeli entities on their leak sites, claiming "political" attacks where the goal is data destruction and reputational damage rather than financial profit.

Conclusion: The New Frontier of Digital Redoubts

The landscape of Iranian cyber warfare in 2026 is defined by a strategic paradox: a nation that has achieved world-class offensive capabilities while simultaneously embracing a doctrine of digital isolation. The National Information Network has successfully transitioned from a domestic censorship tool to a "digital redoubt" that provides the regime with a unique form of asymmetric protection during kinetic crises. While this strategy results in a perceived lack of "prominence" compared to the overt campaigns of Russia or Israel, it allows Iran to maintain a persistent, low-intensity presence on the global digital battlefield through its network of proxies and dispersed MOIS/IRGC units.

The prominence of personas like Handala serves a vital function within this doctrine, providing the "social media dramatics" required to project power to a domestic and regional audience, even when the underlying technical successes are limited. For international organizations and regional governments, the 2026 outlook is clear: the threat from Iran is no longer just about espionage, but about the targeting of critical infrastructure across the Gulf

and the sophisticated use of "hack-and-leak" operations to influence global narratives. As Iran continues to adapt its infrastructure—utilizing Starlink and cloud-based C2 to bypass its own domestic blackouts—the challenge for the international community will be to distinguish between the noise of hacktivist dramatics and the silent, modular persistence of a maturing cyber power.

Works cited

1. How Will Cyber Warfare Shape the U.S.-Israel Conflict with Iran?, https://www.csis.org/analysis/how-will-cyber-warfare-shape-us-israel-conflict-iran

2. Iran's Cyber Retaliation Clock Is Ticking: What CISOs Need to Know Right Now - Anomali, https://www.anomali.com/blog/the-cyber-front-of-operation-epic-fury-what-cisos-need-to-know-right-now

3. The Cyber Wars That Weren't | Small Wars Journal by Arizona State University, https://smallwarsjournal.com/2026/01/07/the-cyber-wars-that-werent/

4. Iran's internet shutdown signals a new stage of digital isolation | Chatham House, https://www.chathamhouse.org/2026/01/irans-internet-shutdown-signals-new-stage-digital-isolation

5. The Iranian Cyber Threat | INSS, https://www.inss.org.il/publication/iranian-cyber/

6. From .com to .gov: The internet's inevitable nationalist turn | Internet ..., https://policyreview.info/articles/analysis/internets-inevitable-nationalist-turn

7. Understanding the Israel-Iran Cyber Conflict - University of Hawai‘i–West O‘ahu, https://westoahu.hawaii.edu/cyber/global-weekly-exec-summary/understanding-the-israel-iran-cyber-conflict/

8. Palo Alto Networks: Iran's internet blackout is reshaping the cyber battlefield | Ctech, https://www.calcalistech.com/ctechnews/article/byqgscef11l

9. Seven Security Scenarios on Russian War in Ukraine for 2025 – 2026: - GLOBSEC, https://www.globsec.org/sites/default/files/2025-10/Seven%20Security%20Scenarios%20Ukraine%202025-2026%20WEB%20rv.pdf

10. Air Superiority in the Twenty-First Century: Lessons from Iran and Ukraine - CSIS, https://www.csis.org/analysis/air-superiority-twenty-first-century-lessons-iran-and-ukraine

11. OilRig: Iran's Persistent Espionage Arm In Cyberspace - Brandefense, https://brandefense.io/blog/oilrig-apt-2025/

12. SentinelOne Intelligence Brief: Iranian Cyber Activity Outlook, https://www.sentinelone.com/blog/sentinelone-intelligence-brief-iranian-cyber-activity-outlook/ 13. (PDF) OILRIG (APT34) Advanced Persistent Threat Analysis - ResearchGate, https://www.researchgate.net/publication/388220746_OILRIG_APT34_Advanced_Persistent_Threat_Analysis

14. Inside APT34 (OilRig): Tools, Techniques, and Global Cyber Threats - LevelBlue, https://www.levelblue.com/blogs/levelblue-blog/inside-apt34-oilrig-tools-techniques-and-global-cyber-threats

15. Iran Cyber Threat Operations | NJCCIC - NJ.gov, https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/iran-cyber-threat-operations

16. Unmasking the Evolving Iranian Prince of Persia | SafeBreach, https://www.safebreach.com/blog/prince-of-persia-a-decade-of-an-iranian-nation-state-apt-campaign-activity/

17. Unmasking MuddyWater's New Malware Toolkit Driving ... - Group-IB, https://www.group-ib.com/blog/muddywater-espionage/

18. ESET APT Activity Report Q2 2025–Q3 2025 - WeLiveSecurity, https://www.welivesecurity.com/en/eset-research/eset-apt-activity-report-q2-2025-q3-2025/

19. Critical Update: February 2026 Escalation - DSCI, https://www.dsci.in/files/content/advisory/2026/cyber_threat_advisory-middle_east_conflict.pdf 20. Dark Web Profile: APT35 - SOCRadar, https://socradar.io/blog/apt-profile-who-is-phosphorus/

21. Threat Intelligence Report: APT35 Internal Leak of Hacking Campaigns Against Lebanon, Kuwait, Turkey, Saudi Arabia, Korea, and Domestic Iranian Targets - DomainTools Investigations, https://dti.domaintools.com/research/threat-intelligence-report-apt35-internal-leak-of-hacking-campaigns-against-lebanon-kuwait-turkey-saudi-arabia-korea-and-domestic-iranian-targets

22. Data breach: the operations of “Charming Kitten” revealed ..., https://www.gatewatcher.com/en/lab/data-breach-the-operations-of-charming-kitten-revealed/

23. Handala: The Rise Of A Decentralized Pro-Palestinian Hacktivist ..., https://brandefense.io/blog/handala-apt-2025/

24. Handala Leak Shows Telegram Account Risk, Not iPhone Hacks | eSecurity Planet, https://www.esecurityplanet.com/threats/handala-leak-shows-telegram-account-risk-not-iphone-hacks/

25. Handala Hack: Telegram Breach of Israeli Officials - KELA Cyber Threat Intelligence, https://www.kelacyber.com/blog/handala-hack-telegram-breach-israeli-officials/

26. Iran-linked hacker group doxes journalists and amplifies leaked information through AI chatbots - Global Affairs Canada, https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/iran-hack-piratage-iranien.aspx?lang=eng

27. Cyber Reflections of the U.S. & Israel-Iran War - SOCRadar, https://socradar.io/blog/cyber-reflections-us-israel-iran-war/

Team FalconFeeds – Threat Research

Share Article