CYBER THREAT INTELLIGENCE REPORT

The Iranian Cyber War Intensifies (Part 2)

31 Days Dark. 200,000+ Devices Wiped. Cloud Infrastructure Under Kinetic Fire.

Iranian Cyber Operations Escalation & Multi-State Exploitation in the US-Israel-Iran Conflict

Date: April 1st, 2026

Prepared by: HiveForce Labs - Hive Pro's Threat Intelligence

Period: March 5 - 31, 2026

Classification: TLP:AMBER

Executive Summary

TLP:AMBER

The three weeks following our initial report (March 5–31, 2026) have witnessed a phase transition: from retaliatory cyber mobilization to sustained, industrialized cyber warfare. Despite 31 consecutive days of near-total domestic internet blackout, Iranian offensive operations have not only persisted — they have intensified. The Stryker MDM wiper attack, IRGC drone strikes on AWS data centers, and confirmation of MuddyWater pre-positioning inside US critical infrastructure mark a fundamental escalation in both capability and intent.

$100+/bbl	200,000+	31+ Days
BRENT CRUDE SURGE	DEVICES WIPED (STRYKER)	IRAN NEAR-ZERO CONNECTIVITY

Three Headline Developments

CRITICAL

Stryker MDM Wiper Attack : First Destructive Attack on a Major US Company

Handala (Void Manticore) weaponized Microsoft Intune to wipe ~200,000+ devices across 79 countries in 3 hours. No malware deployed — all actions were legitimate admin commands, completely bypassing EDR. Emergency medical services in Maryland disrupted; ~5,500 employees in Ireland sent home.

CRITICAL

IRGC Drone Strikes on AWS Data Centers : First Military Strike on Hyperscale Cloud

Shahed-136 drones struck three AWS facilities (two in UAE, one in Bahrain) on March 1, with a second wave on March 24. Two availability zones knocked offline; regional banking, payments, ride-hailing, and enterprise data disrupted. Fars News Agency claimed deliberate targeting of cloud infrastructure supporting allied military activities.

HIGH

MuddyWater Pre-Positioned in US Networks : Bank, Airport, Defense Contractor

Confirmed embedded inside a US bank, US airport, and defense/aerospace software company with Israeli operations. 9+ new malware families deployed in March alone. Now collaborating with Agonizing Serpens to deploy MultiLayer and BFG Agonizer wiper modules at scale.

What Changed Since Last Report?

TLP:AMBER

Every escalation trajectory predicted in Report 1 has materialized within 22 days. The following delta summary maps the acceleration across six critical dimensions:

DIMENSION	REPORT 1 (FEB 26–MAR 5)	FOLLOW-UP (MAR 5–31)
Attack Surface	VPN edge, ICS/OT, phishing	+ MDM weaponization, cloud kinetic strikes, IP camera exploitation, CI/CD supply chain
Most Impactful Event	Kinetic strikes + cyber mobilization	Stryker wiper: 200,000+ devices, 79 countries, 3 hours, zero malware
Threat Actors	6 Iranian APTs	10+ Iranian APTs + 3 China-nexus +1 cloud-native (TeamPCP)+ Russia + Hamas + Pakistan + Belarus actors
Malware Families	5 families (GhostFetch, CHAR, HTTP_VIP, WezRat, Sicarii)	20+ families: + 9 MuddyWater, MultiLayer, BFG Agonizer, CanisterWorm
Law Enforcement	No actions reported	FBI/DOJ seized 4 MOIS domains (Mar 19); $10M Rewards for Justice; Handala restored domains in 24h. Additionally, Handala breached FBI Director Kash Patel's personal email (Mar 27), leaking historical emails from 2010–2019.
Report 1 Predictions	Transborder spillover, AI warfare, civilian targeting	ALL THREE materialized: Stryker (transborder), Op Olalampo expansion (AI), RedAlert/prayer app (civilian)

Adversary Profiles & Attributions — Updated

TLP:AMBER

The Iranian cyber ecosystem has expanded from six to ten tracked APT groups during this period. Three new actors identified: ShroudedSnooper (telecom pre-positioning), UNK_CraftyCamel (aerospace/ maritime) and Dust Specter (Iraqi government).

ACTOR	ALIASES	AGENCY	SPECIALTY	MARCH TARGETS	STATUS
Void Manticore	Handala Hack	MOIS	MDM Weaponization, Wipers	Stryker, IL energy	ESCALATED
Static Kitten	MuddyWater	MOIS	AI Malware, RMM Abuse	US bank, airport, defense	ESCALATED
Cotton Sandstorm	Emennet Pasargad	IRGC	Infostealers, Influence	Political networks, media	ACTIVE
Pioneer Kitten	Fox Kitten	Contractor	Edge Exploit, Access Broker	VPN/firewall infra	ACTIVE
CyberAv3ngers	Cyber Avengers	IRGC-CEC	ICS/OT Sabotage	Water, energy (IL/JO)	HIGH RISK

Key March Developments:

Void Manticore: Stryker MDM wiper; FBI domain seizure; Handala Wiper + Rhadamanthys

Static Kitten: 9 new malware families; pre-positioned in US critical infra

Cotton Sandstorm: WezRat distribution continues; EU sanctions March 17

Pioneer Kitten: Selling access to ransomware affiliates (NoEscape, ALPHV)

Adversary Profiles — Continued

TLP:AMBER

ACTOR	ALIASES	AGENCY	SPECIALTY	MARCH TARGETS	STATUS
Charming Kitten	APT35	IRGC	Credential Phishing	US think tanks	ACTIVE
Prince of Persia	Infy / APT-C-07	Suspected MOIS	Telegram Espionage, Custom DGA Malware	Dissidents, diplomats, academics	ESCALATED
ShroudedSnooper	UNC1860	MOIS	Passive Backdoors	QA/SA/IL telecom	NEW
UNK_CraftyCamel	—	MOIS	Aerospace/Maritime	UAE sat-nav, transport	NEW
Dust Specter	—	Iran-nexus	Iraqi Govt Targeting	Iraq MoFA officials	NEW

Key March Developments:

Charming Kitten: March 8 credential phishing against US think tank

Prince of Persia: Telegram C2 rebuilt post-Iran blackout

ShroudedSnooper: LionTail/TEMPLEDOOR framework; long-dwell access

UNK_CraftyCamel: Strait of Hormuz escalation driver

Dust Specter: SPLITDROP/GHOSTFORM .NET malware; GenAI use

Case Study: The Stryker MDM Wiper Attack

TLP:AMBER

On March 11, 2026, Handala (Void Manticore/MOIS) executed the first confirmed destructive cyberattack on a major US company by weaponizing Microsoft Intune, not malware. The attack wiped approximately 200,000+ devices across 79 countries in a 3-hour window, completely bypassing all endpoint detection.

~200,000	79	3 Hours	$25B	ZERO
DEVICES WIPED	COUNTRIES AFFECTED	ATTACK WINDOW	STRYKER REVENUE	MALWARE SIGNATURES

Attack Kill Chain

PHASE	TECHNIQUE	DETAIL
1 Pre-Positioning	VPN Credential Stuffing	Compromised Entra ID admin credentials months before. “Access dated back ‘well before’ March.” -- Check Point
2 Privilege Escalation	Cloud Account Creation	Created new Global Administrator account in Microsoft Entra ID at 05:00 UTC on March 11.
3 Destruction	Intune Remote Wipe	Mass Remote Wipe commands to all enrolled devices simultaneously. ~200,000 devices wiped in 3 hours. Login screens defaced with Handala logo.
4 Collateral Impact	BYOD + Medical Disruption	Personal phones factory-reset (photos, banking, MFA destroyed). LIFENET ECG platform disrupted; Maryland EMS reverted to radio. ~5,500 Ireland employees sent home.

Why This Attack Matters

This represents a fundamental departure from prior Iranian tradecraft. Instead of custom wiper malware, the group abused the enterprise management plane itself. EDR tools are blind to MDM-initiated wipes because the action originates from a trusted system. This technique aka System Feature is vendor-agnostic: Intune, Jamf, Workspace ONE are all vulnerable. Stryker was targeted because of its 2019 acquisition of Israeli company OrthoSpace, demonstrating that indirect Israeli business connections are sufficient to make a US company a target. Stryker holds a $450M DOD medical supply contract.

MITRE ATT&CK Mapping

- **T1078** — Valid Accounts (compromised admin credentials)
- **T1136.003** — Create Account: Cloud Account
- **T1098** — Account Manipulation (Global Admin escalation)
- **T1485** — Data Destruction (Mass device wipe)
- **T1491** — Defacement
- **T1566** — Phishing
- **T1072** — Software Deployment Tools

Kinetic-Cyber Convergence — New Frontiers

TLP:AMBER

IRGC Drone Strikes on AWS

March 1–3: Shahed-136 drones struck three AWS facilities (two UAE ME-CENTRAL-1, one Bahrain ME-SOUTH-1). The first military strike on hyperscale cloud infrastructure in history. March 24: Second wave struck Bahrain again.

Regional Cascade: Emirates NBD, ADCB, First Abu Dhabi Bank — outages lasting 24–48h. Careem — full app outage. Snowflake — elevated errors. UAE Securities Authority suspended trading for two days; Dubai benchmark fell 4.7%.

Deliberate Targeting: Fars News Agency stated the Bahrain facility was targeted to disrupt allied military/intelligence support. Tasnim published a target list of 29 locations naming AWS, Microsoft, Google, Oracle, Palantir, and Nvidia facilities across 4 countries.

IP Camera Exploitation for Military Targeting

Check Point Research documented hundreds of exploitation attempts against Hikvision and Dahua cameras across Israel, UAE, Qatar, Bahrain, Kuwait, Lebanon, and Cyprus since February 28. Attack infrastructure uses commercial VPNs (Mullvad, ProtonVPN, NordVPN, Surfshark).

Assassination Targeting: Israeli Cyber Directorate head Yossi Karadi (March 25): Iran and Hezbollah are running a joint campaign to hack security cameras to support targeted assassinations. The INCD blocked ~50 major incidents. Karadi disclosed 50 Israeli companies had been digitally erased.

Precedent: Weizmann Institute (June 2025): Iran compromised a street camera near Weizmann Institute shortly before a ballistic missile struck the building. Same targeting pattern now systematized at scale.

Poland Nuclear Sector: First European Nuclear Infrastructure Targeting

Poland's National Centre for Nuclear Research disclosed a foiled intrusion on March 12. Minister Gawkowski cited "many indications" pointing toward Iran but explicitly cautioned that these indicators may have been planted as a false flag to disguise the true origin. One of the first attempted intrusions on European nuclear infrastructure during this conflict (attribution remains unconfirmed).

Technical Analysis: Expanded Attack Mechanisms

TLP:AMBER

MuddyWater March 2026 Arsenal

Nine new malware families deployed in a single month — the most prolific period documented for any Iranian APT:

PAYLOAD	DESCRIPTION
Phoenix v4	Full-featured backdoor; C2 via screenai[.]online
BlackBeard, LampoRAT	Rust-based; HTTP status codes + Telegram API for C2. Dev username: Jacob
UDPGangster, Nuso	UDP backdoor; C2: 157.20.182[.]75:1269; mutex: xhxhxhxhxhxpp
Dindoor	Deno JS runtime backdoor. Signed cert: Amy Cherne. Linked to Tsundere botnet.
Fakeset + Stagecomp + Darkcomp	Python-based via Backblaze cloud. Linked by shared digital certificates. Exfil via Rclone to Wasabi.

Wiper Arsenal Expansion (15+ families)

WIPER	DESCRIPTION
MultiLayer	MuddyWater + Agrius collaboration. .NET wiper with code overlaps with Apostle/Fantasy wipers.
BFG Agonizer	Deployed alongside MultiLayer at scale against Israeli targets
Handala Wiper	Adopted by Handala. Identity-based wiper, compromised Intune Global Admin credentials weaponized to remotely destroy endpoints

Supply Chain: TeamPCP/CanisterWorm

CVE-2026-33634 (CVSS 9.4). Cascaded from a single GitHub token across 5 ecosystems in 8 days: Trivy, npm (66+ packages), Docker Hub, Checkmarx KICS, LiteLLM (PyPI, 3.4M daily downloads). First documented use of blockchain (Internet Computer Protocol) as takedown-resistant C2. Iran-targeted wiper component that destroys clusters configured with Tehran timezone/Farsi.

Axios npm Compromise

On March 31, 2026, the npm account of the primary Axios maintainer (jasonsaayman) was hijacked; malicious axios@1.14.1 and axios@0.30.4 published with hidden RAT dropper (plain-crypto-js@4.2.1). Axios has ~100M weekly downloads and is present in ~80% of cloud and code environments. Wiz confirmed malicious version execution in 3% of affected environments.

RMM Tool Abuse

MuddyWater abuses: Atera, AnyDesk, Syncro, SimpleHelp, ScreenConnect, ConnectWise, RemoteUtilities, PDQ, Action1, NetBird. Any unrecognized RMM agent = assume compromised.

Non-Iranian Actors Exploiting the Conflict

TLP:AMBER

The conflict has become a multi-state exploitation event. China, Russia, Hamas, Belarus, and cybercriminal groups on both sides are leveraging the chaos as operational cover.

ACTOR	ALIGNMENT	TECHNIQUE	TARGETS	KEY DEVELOPMENT
NoName057(16)	Russia	DDoS	Israeli defense (Elbit Systems), Jerusalem Post	Joint targeting with Iranian hacktivists on March 2
Z-Pentest Alliance	Russia	OT/ICS Access	Israeli water supply, other industrial control systems	Published Hebrew HMI screenshots showing pump controls
UNK_InnerAmbush	China (suspected)	DLL Sideloading	ME diplomatic/government orgs	AppleChris backdoor; geofenced payload delivery via Google Drive
TA402 / Frankenstein	Hamas	Credential Harvest	ME government entities	Compromised Iraqi MFA sender; OWA phishing at iwsmailserver[.]com
TA473 / Winter Vivern	Belarus	Reconnaissance	European + ME government	First documented ME targeting; conflict-themed lures
UNK_RobotDreams	Pakistan	Spear-phishing + Rust Backdoor	India-based ME govt offices	Impersonated India MoEA; geofenced Rust backdoor via fake Adobe PDF
UNK_NightOwl	China (suspected)	Credential Harvest	ME government entities	Spoofed OneDrive + Syrian ministry email; OWA phishing at 1drvms[.]store
CL-STA-1087	China (suspected)	Malware Delivery	SE Asian defense entities	MemFun + Getpass malware; geofenced DLL sideloading
BaqiyatLock RaaS	Hezbollah	Ransomware-as-a-Service	Israeli entities (free access)	Sicarii operators redirected; consolidation of pro-Iranian ransomware
HydraC2 Botnet	Five Families	DDoS	Hospitals, aviation, defense	Indicated Iranian regime support in private channels
TeamPCP	Cybercrime/ Anti-Iran	Supply Chain Poisoning + Iran-targeted Wiper	CI/CD pipelines, security tools, AI tooling, Iranian Kubernetes clusters	Cascading 8-day supply chain blitz (Trivy→KICS→LiteLLM→Telnyx). Geotargeted wiper. LAPSUS$ extortion partnerships.

Actively Exploited Vulnerabilities: Feb–Mar 2026

TLP:AMBER

The conflict window has shifted attacker focus beyond VPN edge (covered in Report 1) to three new attack surfaces: IP camera networks for physical targeting, firewall/MDM management planes for destructive access, and software supply chains for mass credential harvest.

SURVEILLANCE & CAMERA INFRASTRUCTURE

CVE	PRODUCT	CVSS	EXPLOITATION METHOD	ACTOR
CVE-2017-7921	Hikvision IP Cameras	**10.0**	Auth bypass via crafted URL. Full admin access without credentials.	Multiple Iran-nexus
CVE-2021-36260	Hikvision IP Cameras	**9.8**	Command injection in web server. Chained with CVE-2017-7921 for full camera network takeover.	Multiple Iran-nexus
CVE-2023-6895	Hikvision IP Cameras	**9.8**	Command injection in Hikvision Intercom Broadcasting System.	Multiple Iran-nexus
CVE-2025-34067	Hikvision IP Cameras	**9.8**	Auth bypass. Hundreds of attempts logged since Feb 28 across 7 countries.	Multiple Iran-nexus
CVE-2021-33044	Dahua IP Cameras	**9.8**	Identity auth bypass. Exploited in parallel with CVE-2025-34067 for camera access.	Multiple Iran-nexus

Used for physical assassination targeting — Iran compromised a camera near Weizmann Institute before a ballistic missile struck (June 2025). Same pattern is now systematized at scale.

MANAGEMENT PLANE & FIREWALL

CVE	PRODUCT	CVSS	EXPLOITATION METHOD	ACTOR
CVE-2026-20131	Cisco Secure FMC	**10.0**	Insecure deserialization, unauth RCE as root. Zero-day exploited 36 days before disclosure.	Interlock RaaS
CVE-2026-1281	Ivanti EPMM	**9.8**	Code Injection, exploited by MuddyWater	MuddyWater
CVE-2026-1731	BeyondTrust RS& PRA	**9.9**	OS command injection, exploited by MuddyWater	MuddyWater
CVE-2025-54068	Laravel Livewire	**9.8**	Code injection. Exploited by MuddyWater in spear-phishing campaigns.	MuddyWater
CVE-2026-33017	Langflow AI Framework	**9.8**	Code injection in public flow endpoint. Exploited within 20 hrs of public disclosure.	Multiple

CVE-2026-20131 (Cisco FMC) was exploited as a zero-day for 36 days before disclosure. FMC compromise allows rewriting firewall policy across entire enterprises — like Stryker's Intune compromise, it confirms that centralized management planes are now the highest-value targets.

SUPPLY CHAIN & DEVELOPER TOOLING

CVE	PRODUCT	CVSS	EXPLOITATION METHOD	ACTOR
CVE-2026-33634	Aqua Security Trivy	**9.4**	Embedded malicious code via GitHub Action tag poisoning. 76/77 tags force-pushed. Cascaded across 5 ecosystems. KEV Mar 26.	TeamPCP
GHSA-fw8c-xr5c-95f9 (No CVE ID)	Axios (npm)	—	Maintainer account hijacked. RAT via plain-crypto-js@4.2.1. 100M+ weekly downloads, 80% cloud presence.	UNC1069

Indicators of Compromise

TLP:AMBER

For the comprehensive list of IOCs and mitigations related to this conflict, visit https://hivepro.com/threat-advisory/ and search by actor name (e.g., Handala, MuddyWater, TeamPCP, CyberAv3ngers) or keyword "Iran", advisories are updated continuously as new indicators are identified.

Novel Malwares

PAYLOAD	TYPE	ATTRIBUTION
Phoenix v4	Full-featured backdoor	MuddyWater
UDPGangster	UDP backdoor	MuddyWater
BlackBeard	Rust-based RAT	MuddyWater
Dindoor	Deno JS runtime backdoor	MuddyWater
CanisterWorm	Self-propagating worm	TeamPCP
SPLITDROP	.NET dropper	Dust Specter
GHOSTFORM	.NET RAT	Dust Specter
MultiLayer	.NET wiper	MuddyWater+Agrius
handala.exe / .bat	Wiper + defacement	Handala

Threat Forecast: Next 30–180 Days

TLP:AMBER

TIER 1: IMMEDIATE PRIORITY (0–60 DAYS)

#	THREAT	PRIORITY	KEY SIGNAL
1	**MDM/Device Management Weaponization**	HIGH	Stryker proved MDM abuse bypasses all endpoint defenses. Expect 3–5 copycat attacks within 60 days targeting healthcare, manufacturing, defense.
2	**OT/ICS Pre-Positioned Access Activation**	HIGH	CyberAv3ngers IOCONTROL implants may trigger without real-time C2. FBI confirms hospital HVAC, water, and life-safety at risk. Iran's blackout does NOT reduce this risk.
3	**Wiper Attack Escalation**	HIGH	Shift to living-off-the-land wipers (MDM/RMM abuse). MuddyWater + Agrius deploying MultiLayer/BFG Agonizer. 15+ wiper families now active.
4	**Financial Sector DDoS and Fraud**	HIGH	Hydro Kitten (IRGC) explicitly signaled financial targeting. HydraC2 botnet + 53+ hacktivist groups. IEEPA sanctions risk ($311K per violation).

TIER 2: MEDIUM TERM (60–180 DAYS)

#	THREAT	PRIORITY	KEY SIGNAL
5	**Post-Blackout Surge**	HIGH	31+ days near-zero connectivity. When restored, expect coordinated surge from reconnected state cyber units with updated targeting.
6	**Satellite & Maritime Infrastructure**	MED-HIGH	UNK_CraftyCamel targeting UAE sat-nav. Strait of Hormuz threat. 17 submarine cables in Red Sea.
7	**European/Asian Financial Institutions**	MED-HIGH	Second-order targets: banks connected to ME trade. Poland nuclear sector already probed.
8	**AI-Generated Phishing at Scale**	MED-HIGH	Op Olalampo + Dust Specter confirmed AI/LLM use. Mass-personalized spear-phishing at executive level incoming.
9	**Supply Chain & Contractor Targeting**	MEDIUM	Stryker proved indirect Israel connections sufficient. TeamPCP cascade across 5 ecosystems. Scarred Manticore handoff model.

Four Strategic Pillars for Defense

TLP:AMBER

1

Threat Informed Defense

Make a shift from reactive to proactive security, map your defenses to MITRE ATT&CK techniques aligned with sector-specific threat actors. Run adversary emulation periodically prioritizing Living-off-the-Land (LOTL) and credential abuse scenarios.

2

Industrial Control Systems Protection

Strict IT/OT segmentation with industrial DMZs and unidirectional gateways. Maintain Asset inventory and perform risk assessments across all building automation, HVAC, life-safety, water treatment, and manufacturing control systems. Hunt proactively for anomalous behaviors mapped to MITRE ATT&CK for ICS (especially T0813)

3

Malware & Data Destruction Defense

Immutable Backups: At least one copy offline/air-gapped/immutable. Validate ESXi offline copies. RMM Audit: Whitelist known agents, alert on unknown. CI/CD Pipeline Integrity: Review Trivy, KICS, LiteLLM dependencies. AI Phishing Training: Conflict-themed social engineering exercises. Binary Blocking: Deploy anti-ransomware solutions blocking unknown binary execution.

4

MDM/UEM Hardening [NEW]

Multi-Person Approval for all bulk device wipe actions (Intune, Jamf, Workspace ONE). Review and minimize Global Admin account list. Alert on new Global Admin creation, unusual policy changes, mass enrollment modifications.

Leveraging Hive Pro for Threat Detection

TLP:AMBER

WORKFLOW	ACTION
Threat Actor Search	Void Manticore, MuddyWater, CyberAv3ngers, Pioneer Kitten, Cotton Sandstorm, Charming Kitten, Prince of Persia + NEW: ShroudedSnooper, UNK_CraftyCamel, Dust Specter, TeamPCP
Vulnerability Module	Hikvision: CVE-2017-7921, CVE-2021-36260, CVE-2023-6895, CVE-2025-34067, Dahua: CVE-2021-33044, Interlock: CVE-2026-20131, MuddyWater: CVE-2026-1281, CVE-2026-1731, CVE-2025-54068, Langflow: CVE-2026-33017, TeamPCP: CVE-2026-33634
Malware Library	Dindoor, Fakeset, Stagecomp, Darkcomp, LampoRAT, UDPGangster, BlackBeard, Nuso, Phoenix, Handala Wiper, MultiLayer, BFG Agonizer, CanisterWorm, SPLITDROP, GHOSTFORM
IOC Ingestion	Follow Hive Pro advisories and import all network/endpoint IOCs from them. Configure automated alerting for SIEM/EDR/firewall telemetry matches.
Attack Surface	Scan for exposed Fortinet, Ivanti, Unitronics, Hikvision, Dahua devices. Identify assets vulnerable to specific CVEs exploited by Iranian and other opportunistic actors.
Campaign Tracking	Monitor Operation Olalampo, Stryker/Handala, TeamPCP/CanisterWorm, Dust Specter campaigns. Subscribe to real-time IOC/TTP alerts.

How To Learn More

ARE YOU EXPOSED TO IRANIAN THREAT ACTORS?

Click the button below to :

Sign Up for a Free Exposure Report!

Or Scan the QR below

Works Cited

TLP:AMBER

1. https://hivepro.com/threat-advisory/void-manticore-irans-evolving-cyber-warfare-model/

2. https://hivepro.com/threat-advisory/operation-olalampo-muddywater-expanding-campaign-across-mena/

3. https://hivepro.com/threat-advisory/teampcp-automated-supply-chain-from-trivy-to-litellm-in-a-multi-ecosystem-breach/

4. https://hivepro.com/threat-advisory/iranian-mois-leverages-telegram-based-c2-in-espionage-campaign-targeting-dissidents/

5. https://hivepro.com/threat-advisory/muddywater-irans-adaptive-cyber-espionage-machine/

6. https://www.cisa.gov/news-events/alerts/2026/03/18/cisa-urges-endpoint-management-system-hardening-after-cyberattack-against-us-organization

7. https://www.cybersecuritydive.com/news/iran-hackers-target-flaws-ip-cameras/813795/

8. https://www.theregister.com/2026/03/02/amazon_outages_middle_east/

9. https://www.trellix.com/blogs/research/the-iranian-cyber-capability-2026/

10. https://www.sentinelone.com/blog/sentinelone-intelligence-brief-iranian-cyber-activity-outlook/

11. https://www.axios.com/2026/03/11/iran-war-trump-israel-ai-cyberattack

12. https://hivepro.com/threat-advisory/targeting-the-lens-iranian-cyber-operations-against-ip-cameras-in-the-middle-east/

13. https://hivepro.com/threat-advisory/cve-2026-20131-interlock-ransomware-exploits-critical-cisco-secure-fmc-flaw/

14. https://hivepro.com/threat-advisory/from-disclosure-to-exploitation-overnight-of-a-cve-2026-33017-langflow-flaw/

15. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/

16. https://www.proofpoint.com/us/blog/threat-insight/iran-conflict-drives-heightened-espionage-activity-against-middle-east-targets

17. https://unit42.paloaltonetworks.com/espionage-campaign-against-military-targets/

18. https://www.sans.org/blog/when-security-scanner-became-weapon-inside-teampcp-supply-chain-campaign

19. https://socradar.io/blog/cyber-reflections-us-israel-iran-war/

20. https://www.halcyon.ai/ransomware-alerts/iranian-use-of-cybercriminal-tactics-in-destructive-cyber-attacks-2026-updates

21. https://unit42.paloaltonetworks.com/evolution-of-iran-cyber-threats/

22. https://research.checkpoint.com/2026/interplay-between-iranian-targeting-of-ip-cameras-and-physical-warfare-in-the-middle-east/