OPERATION LION SURGE

THREAT INTELLIGENCE RESEARCH PAPER

Iranian Regime Cyber Operations: Attack Taxonomy, Active TTPs, and Threat Actor Profiles

CLASSIFICATION	PUBLICATION DATE	AUTHOR	AFFILIATION
TLP:CLEAR — Public Release	March 2026	KayVon Nejad, CISSP	Vijilan Security, LLC

This research paper provides a comprehensive, referenced taxonomy of Iranian state-sponsored and proxy cyber operations — documenting attack categories, active threat actors, tactics, techniques, and procedures (TTPs), and the critical infrastructure sectors currently at elevated risk. It is published in support of Operation Lion Surge, Vijilan Security's active initiative providing free managed remediation to qualifying MSP and MSSP partners.

1. Executive Summary

Iran's offensive cyber capability is among the most mature, diverse, and operationally active of any nation-state adversary. Operating through two primary intelligence organs — the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS) — Tehran has built a layered cyber ecosystem comprising state-sponsored advanced persistent threat (APT) groups, contractor networks, and state-deputized hacktivist proxy collectives.
Historically, Iranian cyber operations were characterized by destructive wiper attacks and long-dwell espionage campaigns. Between 2023 and 2026, the threat model evolved significantly: Iranian actors began masquerading as criminal ransomware operators, blurring the line between state sabotage and financially motivated cybercrime, while dramatically expanding the role of hacktivist proxies for plausible deniability at scale.

In February 2026, the US–Israel joint offensive codenamed Operation Epic Fury (US) / Operation Roaring Lion (Israel) disrupted Iranian command-and-control infrastructure and reduced Iranian internet connectivity to 1–4%. In the immediate aftermath, Palo Alto Unit 42 and Halcyon observed a paradoxical dynamic: sophisticated state-directed APT activity decreased in the near term due to connectivity and C2 degradation, while hacktivist proxy activity surged — with an estimated 60 active pro-Iranian groups and a newly formed Electronic Operations Room coordinating retaliatory campaigns as of February 28, 2026.
This paper documents the full spectrum of Iranian cyber attack types, the actors behind them, and the specific tactics currently being observed by Vijilan's SOC and major threat intelligence providers including CISA, Palo Alto Unit 42, Check Point Research, Trellix, Halcyon, and the Canadian Centre for Cyber Security.

2. Iranian Cyber Threat Actor Landscape

Iran's offensive cyber capability is among the most mature, diverse, and operationally active of any nation-state adversary. Operating through two primary intelligence organs — the Islamic Revolutionary Guard Corps (IRGC) and the Ministry of Intelligence and Security (MOIS) — Tehran has built a layered cyber ecosystem comprising state-sponsored advanced persistent threat (APT) groups, contractor networks, and state-deputized hacktivist proxy collectives.
Historically, Iranian cyber operations were characterized by destructive wiper attacks and long-dwell espionage campaigns. Between 2023 and 2026, the threat model evolved significantly: Iranian actors began masquerading as criminal ransomware operators, blurring the line between state sabotage and financially motivated cybercrime, while dramatically expanding the role of hacktivist proxies for plausible deniability at scale.

In February 2026, the US–Israel joint offensive codenamed Operation Epic Fury (US) / Operation Roaring Lion (Israel) disrupted Iranian command-and-control infrastructure and reduced Iranian internet connectivity to 1–4%. In the immediate aftermath, Palo Alto Unit 42 and Halcyon observed a paradoxical dynamic: sophisticated state-directed APT activity decreased in the near term due to connectivity and C2 degradation, while hacktivist proxy activity surged — with an estimated 60 active pro-Iranian groups and a newly formed Electronic Operations Room coordinating retaliatory campaigns as of February 28, 2026.
This paper documents the full spectrum of Iranian cyber attack types, the actors behind them, and the specific tactics currently being observed by Vijilan's SOC and major threat intelligence providers including CISA, Palo Alto Unit 42, Check Point Research, Trellix, Halcyon, and the Canadian Centre for Cyber Security.

2.1 IRGC-Controlled Actors

APT33 (ELFIN / REFINED KITTEN / PEACH SANDSTORM)

STATUS	ACTIVE — RETOOLING POST-FEBRUARY 2026 STRIKES

APT33 is one of Iran's most capable offensive units, operating under IRGC direction with a primary focus on the energy, aviation, and petrochemical sectors. Active since at least 2013, the group is distinguished by its deployment of custom destructive malware alongside long-dwell reconnaissance campaigns designed to pre-position for future disruption operations.

Primary sectors targeted: Energy infrastructure, aviation, aerospace, petrochemical, defense supply chain

Signature malware: StoneDrill wiper, Shamoon variants, DROPSHOT dropper, TURNEDUP backdoor

Key TTPs: Spear-phishing with credential harvesting pages; PowerShell-based LOTL techniques; destructive payload deployment after extended dwell periods

APT42 (CHARMING KITTEN / MINT SANDSTORM / TA453)

STATUS	ACTIVE — EXPANDED 2026 CAMPAIGNS TARGETING NGOS, HEALTHCARE, DIASPORA

APT42 is the IRGC Intelligence Organization's primary social engineering and credential harvesting unit. The group is distinctive for its relationship-based targeting methodology: operators cultivate sustained personal engagement with high-value targets before attempting compromise, often posing as journalists, conference organizers, or researchers.

Primary sectors targeted: Healthcare, defense contractors, think tanks, NGOs, journalists, human rights advocates, Iranian diaspora communities

Signature malware: NICECURL and TAMECAT backdoors; credential harvesters hosted on Cloudflare Workers, OneDrive, Firebase

Key TTPs: Multi-platform social engineering (LinkedIn, email, phone); watering hole attacks; cloud platform abuse for C2 traffic obfuscation; keylogging, screen capture, browser credential theft, session cookie exfiltration

A December 2025 leak of internal operational records exposed APT42's bureaucratic infrastructure, including structured spreadsheets tracking domain registrations, European VPS hosting, and cryptocurrency payments — and confirmed direct overlap with the Moses Staff operation, formally connecting previously distinct personas into a single coordinated state effort.

APT35 (PHOSPHORUS / COBALT ILLUSION / YELLOW GARUDA)

STATUS	ACTIVE — PASSWORD-SPRAY CAMPAIGNS AGAINST M365 AND EXCHANGE ENVIRONMENTS

APT35 focuses primarily on nuclear policy researchers, government officials, and defense sector personnel. The group is known for sustained multi-persona social engineering and systematic password-spray campaigns against Microsoft cloud environments.

Primary sectors targeted: Nuclear policy, government agencies, defense sector, academic institutions

Key TTPs: Password spraying against Microsoft Exchange and Office 365/M365; multi-persona LinkedIn social engineering; MFA push-bombing; credential harvesting via fake login portals

TORTOISESHELL (IMPERIAL KITTEN / YELLOW LIDERC)

STATUS	ASSESSED — REPOSITIONING FOR 2026 OPERATIONS AFTER 2025 SUPPLY CHAIN CAMPAIGNS

Tortoiseshell is an IRGC-directed group specializing in supply chain compromise and fake LinkedIn recruitment attacks. The group deploys the MiniBike custom backdoor via DLL sideloading and has demonstrated consistent targeting of aerospace and defense supplier networks.

Primary sectors targeted: Aerospace, defense industrial base (DIB), IT supply chain

Key TTPs: Watering hole attacks; LinkedIn fake recruiter personas; DLL sideloading for backdoor deployment; supply chain compromise through trusted vendor relationships

CYBERAV3NGERS (CYBERAVENG3RS)

STATUS	ACTIVE — ONGOING EXPLOITATION OF INTERNET-FACING PLCS IN WATER, ENERGY, AND INDUSTRIAL SECTORS

CyberAv3ngers is an IRGC-affiliated cyber persona responsible for some of the most consequential attacks on US operational technology (OT) infrastructure. The group targets programmable logic controllers (PLCs) and human-machine interfaces (HMIs) across water and wastewater systems, energy infrastructure, and other critical sectors. Their method is frequently the exploitation of default credentials on internet-facing OT devices — a low-sophistication initial access vector with potentially catastrophic physical consequences.

CISA, FBI, NSA, EPA, and the UK NCSC issued a joint advisory in December 2024 specifically addressing CyberAv3ngers TTPs, mapping them to MITRE ATT&CK v16 and documenting newly observed techniques targeting OT/ICS systems in the US, UK, and Israel.

Primary sectors targeted: Water and wastewater systems, energy infrastructure, industrial control systems (ICS), food and agriculture

Key TTPs: Default credential exploitation on internet-exposed PLCs; OT device reconnaissance; unauthorized access to SCADA/HMI systems; disruptive manipulation of industrial processes

2.2 MOIS-Controlled Actors

APT34 (OILRIG / HAZEL SANDSTORM / HELIX KITTEN)

STATUS	ACTIVE — PRE-OPERATIONAL INFRASTRUCTURE STAGING OBSERVED THROUGH APRIL 2025

APT34 is MOIS's most technically sophisticated long-horizon actor. The group is defined by meticulous pre-operational preparation: infrastructure staging campaigns involving impersonated academic and technology companies, consistent SSH key reuse, and systematic domain registration designed to support future credential harvesting — all executed before any malware is deployed. This discipline reflects a patient, intelligence-gathering orientation rather than immediate disruption.

Primary sectors targeted: Financial services, government agencies, defense sector, energy, telecommunications, oil and gas

Signature malware: POWBAT, POWRUNER, BONDUPDATER backdoors; C# malware masquerading as PDF documents; Mimikatz and LaZagne for credential theft

Key TTPs: Long-horizon pre-operational staging; credential harvesting via fake academic portals; command obfuscation and encrypted C2 channels; commands concealed in HTTP Authorization Bearer tokens; dual C2 channels combining HTTP and email-based control using compromised government accounts

MUDDYWATER (SEEDWORM / STATIC KITTEN / MANGO SANDSTORM / MERCURY)

STATUS ACTIVE — CISA-CONFIRMED TARGETING OF US BANKS, AIRPORTS, AND NON-PROFITS AS OF MARCH 2026

MuddyWater has been formally confirmed by CISA as a subordinate element within MOIS. As of March 2026, Halcyon's Ransomware Research Center identified MuddyWater conducting Operation Olalampo, a structured offensive cyber operation targeting the META (Middle East, Turkey, Africa) region with TTPs overlapping a separately tracked campaign designated RedKitten — indicating coordinated infrastructure across multiple Iranian-aligned actors.

Researchers have also identified the Tsundere Botnet (also called DinDoor), discovered in 2025 and linked to MuddyWater through infrastructure and operational patterns, using Node.js scripts to execute code on compromised systems with a Deno-based fallback method.

Primary sectors targeted: Banking and financial institutions, airports and aviation infrastructure, government, telecommunications, non-profit organizations, software companies with Israeli defense connections

Key TTPs: Spear-phishing via compromised mailboxes; Phoenix backdoor deployment; living-off-the-land (LOTL) binaries; PowerShell-based execution; botnet infrastructure for persistent access

AGRIUS (AGONIZING SERPENS / PINK SANDSTORM)

STATUS ACTIVE — WIPER AND PSEUDO-RANSOMWARE OPERATIONS; OT CAMERA SCANNING OBSERVED JUNE 2025

Agrius is MOIS's primary destructive operations unit, specializing in wiper deployments disguised as ransomware to complicate initial incident triage. The group exploits internet-facing web applications for initial access, deploys ASP.NET webshells for persistence, and uses LOTL tools for lateral movement — a methodology that provides a defensive advantage because the consistent playbook can be specifically countered.

Signature malware: Apostle wiper (evolved into functional ransomware), Fantasy wiper, BiBi wiper (Linux), Hatef wiper (.NET, Windows), Hamsa wiper (Bash, Linux), BFG Agonizer, IPsec Helper backdoor

Key TTPs: One-day vulnerability exploitation in web-facing applications; ASPX webshell deployment; data exfiltration before wiper execution; masquerading destructive attacks as ransomware; supply chain exploitation (Fantasy wiper)

EMENNET PASARGAD (COTTON SANDSTORM / HAYWIRE KITTEN)

STATUS ACTIVE — EXPANDING OPERATIONAL SCOPE; ALTOUFAN TEAM PERSONA REACTIVATED MARCH 2026

Emennet Pasargad is an IRGC-linked actor conducting cyber-enabled influence operations combined with intrusion activity. The group's consistent malware toolset includes WezRat, a custom modular infostealer delivered via spear-phishing disguised as urgent software updates. In some campaigns, intrusions were followed by WhiteLock ransomware deployment. The group reactivated the dormant Altoufan Team persona within one day of the February 2026 conflict escalation, demonstrating reactive and opportunistic operational posture.

Key TTPs: WezRat infostealer delivery via spear-phishing; WhiteLock ransomware deployment; hack-and-leak operations; influence operations combining data theft with coordinated social media amplification

2.3 State-Deputized Hacktivist Proxy Network

Iran deliberately deploys hacktivist proxy groups to conduct operations with plausible deniability. Analysis of over 250,000 Telegram messages from more than 178 hacktivist and proxy groups during the June 2025 Israel–Iran conflict demonstrated rapid mobilization coordinated with military developments. As of February 28, 2026, a newly formed Electronic Operations Room began coordinating retaliatory cyber operations.

Handala Hack (Void Manticore)
MOIS-linked. Combines data exfiltration with destructive wiper attacks. Operated through the Homeland Justice persona in the 2022 Albania campaign. Reduced public Telegram blog activity since January 2026 — historically consistent with active operational tempo. Has issued physical death threats to Iranian-American and Iranian-Canadian influencers, claiming to have shared home addresses with physical operatives.

Sicarii Ransomware
An Iranian-aligned RaaS operation that surfaced in December 2025 with a critical encryption flaw: the malware permanently discards its own keys after encrypting files, making decryption impossible for both victim and operator regardless of ransom payment. The group has publicly signaled intent to dramatically expand targeting volume. Primarily targeting META-region entities with one confirmed US victim as of March 2026.

DieNet, Dark Storm Team, FAD Team (Fatimiyoun Cyber)
DieNet specializes in DDoS attacks, claiming responsibility for disruptions against US energy, financial, healthcare, and government systems. Dark Storm Team (also DarkStorm/MRHELL112) is a pro-Palestinian/pro-Iranian collective specializing in large-scale DDoS and ransomware. The FAD Team focuses on wiper malware and permanent data destruction, claiming unauthorized access to SCADA/PLC systems in Israel and other countries.

3. Iranian Cyber Attack Taxonomy

Iranian cyber operations span six primary attack categories, often deployed in combination. The following taxonomy documents each category with associated actors, observed techniques, targeted sectors, and historical precedents.

3.1 Destructive Wiper Attacks

Wiper attacks are Iran's most strategically significant offensive capability. Unlike ransomware, wipers are designed to permanently destroy data with no possibility of recovery — often deployed after extended dwell periods during which intelligence is gathered or as a retaliatory measure coordinated with geopolitical escalation.

Historical Precedents

- Shamoon (2012): Targeted Saudi Aramco, destroying approximately 30,000 workstations. Overwritten the master boot record (MBR) using the Eldos RawDisk driver.
- Shamoon 2 & 3 (2016–2018): Redeployment against Middle Eastern energy and government entities.
- ZeroCleare & Dustman (2019–2020): Deployed against energy and industrial sectors; used modified legitimate drivers to overwrite MBR.
- ROADSWEEP & ZEROCLEAR — Albania (2022): Deployed by HomeLand Justice (Agrius) against Albanian government networks via Exchange ProxyShell/SharePoint vulnerabilities.

Current Activity (2024–2026)

- BiBi Wiper: Cross-platform (.NET for Windows, Bash for Linux) deployed by Void Manticore/Handala against Israeli and allied targets.
- Hatef & Hamsa Wipers: Next-generation cross-platform wipers representing a technical evolution to multi-OS capability.
- Sicarii Ransomware: A permanently destructive 'ransomware' variant where data recovery is impossible by design — rendering it functionally a wiper with a ransomware facade.
- FAD Team/Fatimiyoun: Wiper attacks claimed against SCADA/PLC systems in Israel and allied countries.

Defender implication: Treat all ransomware alerts in targeted sectors as potential wiper events. Preserve forensic evidence before attempting recovery. Validate data integrity before assuming criminal ransomware intent. Offline, air-gapped backups are a mandatory control against this attack category.

3.2 Credential Theft & Identity-Based Attacks

Credential theft is the most prevalent Iranian initial access technique and their most common pathway to lateral movement. CISA's joint advisory AA24-290A documents Iranian actors' systematic use of brute force, password spraying, and MFA push-bombing since at least October 2023 across healthcare, government, IT, engineering, and energy sectors.

Observed Techniques

- Password Spraying (T1110.003): Automated attempts of a single common password against many accounts simultaneously to avoid lockout thresholds. APT35 and MuddyWater have active campaigns targeting M365 and Exchange environments.
- MFA Push Bombing (T1621): Flooding a user's authenticator app with approval requests until they accidentally or out of fatigue accept the prompt. CISA advisory AA24-290A documents this as a primary Iranian technique.
- Credential Harvesting via Fake Login Pages: APT34 and APT42 deploy sophisticated credential harvesting infrastructure impersonating legitimate academic, government, and corporate portals — with APT34's November 2024–April 2025 campaign specifically impersonating Iraqi academic institutions and UK technology companies.
- Social Engineering via LinkedIn/Email/Phone: APT42 invests weeks or months in relationship cultivation before attempting credential theft, achieving higher success rates through social trust.
- Browser Credential & Session Cookie Theft: APT42's NICECURL/TAMECAT backdoors capture browser-stored credentials and session cookies post-compromise, enabling account takeover even where MFA is present.
- Brute Force of OT Default Credentials: CyberAv3ngers systematically exploits factory-default passwords on internet-exposed PLCs and HMIs — a technique that requires no sophisticated tooling but grants direct access to critical industrial processes.

Defender implication: Phishing-resistant MFA (FIDO2/hardware keys) is the highest-priority control against Iranian credential attacks. Password spraying and push-bombing are ineffective against FIDO2. Additionally, organizations should monitor for impossible travel events and concurrent session anomalies as indicators of stolen session cookies.

3.3 Ransomware & Pseudo-Ransomware Operations

Iran's use of ransomware has evolved from rare incidents to a core operational tactic that serves multiple strategic objectives simultaneously: generating revenue to offset sanctions, masking state attribution behind the appearance of criminal activity, and achieving destructive effects when wiper payloads are deployed after encryption.

The Ransomware-as-Cover Pattern

Agrius pioneered the pseudo-ransomware model with the Apostle malware: initially deployed as a pure wiper with a ransomware facade (no actual decryption capability), Apostle was later patched to function as genuine ransomware — complicating attribution and delaying incident response by forcing defenders to treat the event as standard cybercrime. This deliberate blurring is now a documented Iranian tradecraft feature.

Active Ransomware Operations

- Sicarii (December 2025–present): Iranian-aligned RaaS with permanent encryption — data is irrecoverably destroyed. Group has signaled intent to expand targeting volume significantly in 2026.
- WhiteLock (deployed by Emennet Pasargad/Cotton Sandstorm): Used specifically against Israeli targets following WezRat infostealer intrusions. Geographic scope assessed as expandable.
- HomeLand Justice pattern: Exfiltrate data, deploy ransomware, then leak stolen data publicly — maximizing both disruption and reputational damage.

Defender implication: Iranian 'ransomware' incidents in critical sectors should be triaged differently from criminal ransomware: assume wiper capability, preserve forensic evidence, engage law enforcement and CISA simultaneously, and do not assume payment will result in decryption.

3.4 OT/ICS & Critical Infrastructure Attacks

Iran is one of only a handful of nation-states with demonstrated willingness and capability to attack critical infrastructure operational technology (OT) and industrial control systems (ICS). This attack category carries the highest potential for kinetic physical consequences.

Water and Wastewater Systems

CyberAv3ngers gained direct unauthorized access to US water and wastewater treatment facilities through exploitation of internet-exposed Unitronics PLCs with default credentials. CISA, FBI, NSA, EPA, and the NCSC issued a joint advisory in December 2024 warning of continued and expanding activity across the water, energy, and food sectors. The technique — accessing publicly-facing industrial devices with unchanged factory passwords — represents the lowest-sophistication, highest-consequence attack vector in the Iranian arsenal.

Energy Infrastructure

APT33 maintains persistent targeting of energy sector OT through a combination of IT-side compromise followed by OT network lateral movement. StoneDrill and Shamoon wiper deployments have historically targeted the oil and gas sector's operational environment. The IRGC's strategic logic: energy infrastructure disruption creates maximum economic and societal impact with international attribution complications.

SCADA/PLC Targeting by Proxy Groups

The FAD Team (Fatimiyoun Cyber) has claimed SCADA/PLC access against Israeli and allied targets. Nozomi Networks' March 2026 analysis of Middle East vulnerability exposure found 61% of 2025-discovered flaws carry high/critical CVSS scores — versus 48% globally — with top MITRE ATT&CK TTPs including default credential abuse (T1110), valid account use (T1078), and network scanning (T1595).

Defender implication: Remove default credentials from all internet-facing OT devices immediately. Segment OT networks from IT environments with robust firewall controls. Never connect control systems directly to the public internet. Inventory all OT assets and establish continuous monitoring baselines.

3.5 Spear-Phishing & Social Engineering

Spear-phishing is the primary initial access vector across virtually all Iranian threat actor clusters. The Canadian Centre for Cyber Security specifically identified 'targeted manipulation: Iran's social engineering and spear phishing campaigns' as a designated threat advisory category in December 2024.

Technique Variants

- Credential Harvesting Lures: Emails directing targets to sophisticated fake login pages for Microsoft 365, academic portals, or government systems. APT34's infrastructure staging campaign (November 2024–April 2025) built out fake UK technology companies and an Iraqi academic institution specifically to support this technique.
- Malicious Document Macros: Halcyon documents primary methods of initial access for APT34, APT35, APT39, and APT42 including phishing with documents exploiting macros within Microsoft Excel.
- Fake Software Updates: Emennet Pasargad/Cotton Sandstorm delivers WezRat infostealer via phishing emails disguised as urgent software update notifications — a lure with high success rates due to the appearance of legitimacy and urgency.
- Relationship-Based Long-Game Engineering: APT42 operators cultivate weeks or months of trusted engagement via LinkedIn, email, and phone before attempting compromise — impersonating conference organizers, journalists, and researchers.
- Vishing (Voice Phishing): UAE-based threat actors were observed in 2026 impersonating the Ministry of Interior in phone calls, claiming to confirm receipt of a national alert and requesting Emirates Identification Numbers for 'verification.'
- Android Spyware via Spoofed Websites: Iranian proxy groups distribute Android spyware hosted on spoofed websites via social engineering to distribute surveillance tools targeting diaspora communities and political dissidents.

3.6 DDoS & Hacktivist Disruption Operations

Iran has used DDoS attacks as a cyber-coercive tool since at least 2011, when Operation Ababil disabled US financial institution websites. The technique has scaled significantly: during the June 2025 and February 2026 conflict periods, pro-Iranian hacktivist groups launched coordinated DDoS campaigns against US military, defense, and financial targets with an estimated 60 active groups operating simultaneously.

Strategic Context

CSIS analysis of Iran's hacktivist ecosystem demonstrates that DDoS attacks serve a function beyond technical disruption: they create psychological pressure, generate news coverage, and project capability — often with exaggerated impact claims designed to shape perception and compensate for actual capability gaps. The distinction between nuisance-level DDoS and state-directed strategic disruption is increasingly difficult to draw, with Iran deliberately blurring the categories.

Active Groups & Operations

- DieNet: Claimed DDoS attacks against US energy, financial, healthcare, and government websites following US military strikes. Associated with HydraC2, a high-reputation DDoS botnet active since August 2023.
- Dark Storm Team: Large-scale DDoS campaigns against Israeli and allied targets including banks and government infrastructure.
- Electronic Operations Room (est. February 28, 2026): Coordinating retaliatory DDoS and defacement operations across Iran-aligned hacktivist groups following Operation Epic Fury.

Defender implication: DDoS protection (cloud scrubbing, rate limiting, CDN-based mitigation) is a baseline control for any organization in an Iranian APT target sector. More critically, DDoS activity may serve as a distraction or cover for concurrent, more sophisticated intrusion attempts — elevated DDoS alert should trigger full defensive posture review.

3.7 Hack-and-Leak & Influence Operations

Iran combines data exfiltration with coordinated information operations: stolen data is published on dedicated Telegram channels, leak sites, and social media to maximize reputational damage, generate media coverage, and shape domestic and international narrative. This category of operation is designed as much for psychological impact as for the technical harm of data exposure.

Operational Pattern

Handala's operational model exemplifies the hack-and-leak pattern: compromise an organization, exfiltrate sensitive data, publish on Telegram and leak site, amplify through affiliated channels. The group has targeted Israeli energy companies, a major Israeli healthcare network, and claimed access to Saudi Aramco (later assessed as likely based on previously circulating data — suggesting deliberate information operations designed to generate attention regardless of factual accuracy).

The December 2025 operational records leak against APT42's own infrastructure — exposing their domain registration spreadsheets, VPS hosting payments, and cryptocurrency wallets — provides a rare inversion of the technique, with Iranian intelligence infrastructure itself becoming the subject of a hack-and-leak operation.

4. MITRE ATT&CK Framework Mapping

The following table maps the most frequently observed Iranian TTP categories to MITRE ATT&CK Enterprise framework techniques, as documented in CISA advisories AA24-290A, AA23-335A (updated December 2024), and Unit 42 threat research.

TACTIC	ATT&CK ID	TECHNIQUE	ATTRIBUTED ACTORS
Reconnaissance	T1589	Gather Victim Identity Information	*APT34, APT42, MuddyWater*
Reconnaissance	T1595	Active Scanning	*CyberAv3ngers, Evil Markhors*
Initial Access	T1566.002	Phishing: Spear-phishing Link	*APT33, APT34, APT42, APT35*
Initial Access	T1190	Exploit Public-Facing Application	*Agrius, CyberAv3ngers, APT34*
Initial Access	T1110.003	Password Spraying	*APT35, MuddyWater, APT42*
Initial Access	T1621	MFA Request Generation (Push Bombing)	*APT35, APT42, MuddyWater*
Initial Access	T1078	Valid Accounts	*CyberAv3ngers, APT34*
Execution	T1059.001	PowerShell	*APT34, MuddyWater, APT33*
Execution	T1059.003	Windows Cmd Shell	*APT42, Agrius*
Persistence	T1505.003	Web Shell	*Agrius, APT34, HomeLand Justice*
Persistence	T1547.001	Registry Run Keys	*APT42*
Defense Evasion	T1027	Obfuscated Files or Information	*APT34, APT42, MuddyWater*
Defense Evasion	T1036	Masquerading (wiper as ransomware)	*Agrius, Sicarii, HomeLand Justice*
Credential Access	T1003	OS Credential Dumping (Mimikatz)	*APT34, APT35*
Credential Access	T1539	Steal Web Session Cookie	*APT42*
Discovery	T1082	System Information Discovery	*APT33, APT34, MuddyWater*
Lateral Movement	T1021	Remote Services	*APT34, Agrius, MuddyWater*
Collection	T1056	Input Capture (Keylogging)	*APT42*
Exfiltration	T1041	Exfiltration Over C2 Channel	*APT34, APT42, Handala*
Impact	T1561	Disk Wipe	*Agrius, Void Manticore, APT33*
Impact	T1486	Data Encrypted for Impact	*Sicarii, HomeLand Justice*
Impact	T1498	Network Denial of Service (DDoS)	*DieNet, Dark Storm Team, HydraC2*

5. Priority Target Sectors

The following sectors face the highest risk of Iranian cyber attack based on documented targeting history, active CISA advisories, and Vijilan SOC observations as of March 2026.

Critical Infrastructure (OT/ICS) — SEVERITY: CRITICAL
- Water and wastewater treatment systems (primary CyberAv3ngers target)
- Energy infrastructure: electricity generation, oil and gas pipelines, petrochemical facilities
- Food and agriculture sector: SCADA/PLC systems
- Transportation systems including aviation control systems

Financial Services — SEVERITY: HIGH
- US banking institutions (MuddyWater confirmed active targeting as of March 2026)
- FinTech and payment processing platforms
- Cryptocurrency exchanges: $90M destroyed in a June 2025 breach attributed to Iranian-aligned actors

Healthcare & Public Health — SEVERITY: HIGH
- Hospital networks and electronic health records systems (APT42, MuddyWater)
- Medical device management systems
- Healthcare data aggregators — targeted for population-scale identity data to locate dissidents

Defense Industrial Base (DIB) — SEVERITY: HIGH
- Defense contractors and subcontractors (APT33, Tortoiseshell)
- Aerospace and aviation suppliers
- Technology companies with Israeli defense connections (MuddyWater)

Government & Academic — SEVERITY: HIGH
- Federal, state, and local government agencies
- Academic institutions, particularly those involved in nuclear policy, defense research, or Middle East policy (APT34, APT35, APT42)
- Think tanks and NGOs

ISPs, Telecom & Data Aggregators — SEVERITY: MEDIUM-HIGH
- Internet service providers, telecommunications companies, and medical systems holding large individual-level data sets are targeted by APT34, APT35, APT39, and APT42 with the assessed intent of locating regime dissidents.

6. Current Threat Status (March 2026)

6.1 Post-Operation Epic Fury Dynamics

Following the US–Israel joint strikes on February 28, 2026, Palo Alto Unit 42 documented a paradoxical cyber threat environment: Iran's internet connectivity dropped to 1–4%, significantly degrading the near-term capacity of state-directed APT actors for sophisticated coordinated operations. Simultaneously, Iran-aligned hacktivist proxy activity surged, with an estimated 60 groups active as of March 2026 — many operating with tactical autonomy in the absence of centralized command and control.

Unit 42 specifically warns that state-aligned cyber units may deviate from previously established patterns due to operational isolation, and that command and control degradation may lead to autonomous action by cells outside Iran. A ceasefire has been declared, but CISA, FBI, DC3, and NSA have issued a joint advisory noting that Iranian-affiliated cyber actors and hacktivist groups may still conduct malicious cyber activity despite the ceasefire — and committing to release updated threat and defense information as the situation evolves.

6.2 Active Operations Observed

- MuddyWater / Operation Olalampo: Structured offensive operation targeting META region with overlapping TTPs across RedKitten campaign infrastructure.
- Handala Hack: Operational silence since January 2026 assessed as indicative of active operations underway rather than dormancy.
- Sicarii: Permanently destructive ransomware group signaling intent to expand targeting volume dramatically.
- Electronic Operations Room: Newly formed coordination body (est. February 28, 2026) directing retaliatory cyber operations from geographically dispersed operators.
- APT42 expanded campaigns: Targeting NGOs and diaspora communities with NICECURL/TAMECAT backdoor deployments.

Threat Intelligence Providers

- Palo Alto Unit 42: Threat Brief — March 2026 Escalation of Cyber Risk Related to Iran (March 2026)
- Palo Alto Unit 42: Evolution of Iranian Cyber Threats — From MBR Wipers to Identity Weaponization (March 2026)
- Trellix: The Iranian Cyber Capability 2026
- Halcyon Ransomware Research Center: Iranian Use of Cybercriminal Tactics in Destructive Cyber Attacks — 2026 Updates
- Check Point Research: What Defenders Need to Know About Iran's Cyber Capabilities (March 2026)
- Picus Security: Iranian Threat Actors — What Defenders Need to Know (March 2026)
- Nozomi Networks: Iranian APT Groups Intensify Cyberattacks on Critical Infrastructure (March 2026)
- CSIS Strategic Technologies Blog: Beyond Hacktivism — Iran's Coordinated Cyber Threat Landscape
- Deepwatch Customer Advisory: Elevated Iranian Cyber Activity Post-US Strikes (June 2025)

ABOUT THE AUTHOR

KAYVON NEJAD

Founder & CEO, Vijilan Security | CISSP
| Author | Speaker | Cybersecurity Enthusiast

KayVon Nejad is an Iranian-American who came to the United States at the age of ten. His childhood was shaped by one of the most consequential geopolitical ruptures of the twentieth century: the Islamic Revolution of 1979. After initially settling in the US, his family was forced to return to Iran when his father — unable to sustain the family due to the economic devastation caused by the collapse of the dollar and the Iranian rial — could no longer provide for them. KayVon lived through the direct human consequences of the regime whose cyber operations he now studies and defends against.

That lived experience is not incidental to this research — it is the foundation of it. KayVon understands the Islamic Republic not as an abstract geopolitical actor but as a system he witnessed displace an entire generation of Iranians, separate families, and weaponize economic conditions as a tool of control. The regime that forced his family's return is the same regime that built the offensive cyber infrastructure documented in this paper.

He eventually returned to the United States, where he built a career at the intersection of cybersecurity, technology, and leadership. He holds a CISSP certification and advanced degrees from Carnegie Mellon University, the Wharton School of the University of Pennsylvania, and NYU. He is the Founder and CEO of Vijilan Security — a premium managed detection and response (MDR) and SIEM company serving MSP, MSSP, and enterprise channel partners globally, SOC 2 Type 2 and ISO 27001 certified, with a 24/7 global SOC presence.

Today KayVon operates at the forefront of cybersecurity in the AI era — building the next generation of AI-driven detection, response, and threat intelligence capabilities. He is an author, speaker, and practitioner whose work bridges deep technical expertise with strategic clarity. Operation Lion Surge is his direct response to a threat he has studied, lived adjacent to, and is now positioned to neutralize.

Operation Lion Surge

vijilan.com | vijilan.com/operation-lion-surge