CYBER THREAT INTELLIGENCE

CRITICAL**START**® Security Advisory

TLP CLEAR // [CS-SA-26-0301] Security Advisory on Escalating Iranian Conflicts

Executive Summary

On February 28, 2026, the United States and Israel initiated coordinated airstrikes across Iran under Operation Epic Fury, targeting defense infrastructure, and senior leadership including Supreme Leader Ali Khamenei. This attack represents a significant escalation with implications for near-term cyber risk. Based on historical Iran-aligned cyber behavior during periods of geopolitical escalation, and current public reporting, organizations should anticipate opportunistic and potentially disruptive cyber activity in the immediate-to-short term (days to weeks) as retaliatory moves by Iran and affiliates.

Observed and anticipated cyber threat activity associated with Iran-aligned actors frequently includes credential-driven attacks, phishing, exploitation of vulnerable internet-facing systems, and disruptive 'hack-and-leak' or wiper operations conducted directly or via proxy personas. The Critical Start Cyber Research Unit (CRU) assesses with medium to high confidence that Iranian state-directed APT groups will intensify targeted intrusions and disruptive attacks against U.S. and allied organizations in the near term. Organizations in critical U.S. sectors are advised to prepare for retaliatory cyberattacks and elevate monitoring.

Introduction

In the wake of heightened geopolitical tensions following Operation Epic Fury, organizations face a rapidly evolving cyber threat environment. Iran-aligned actors have historically exploited such periods to conduct opportunistic and targeted attacks, leveraging phishing, credential-based access, and disruptive malware campaigns. Iranian cyber forces operate through both the Ministry of Intelligence and Security (MOIS) and the Islamic Revolutionary Guard Corps (IRGC), and their activities span espionage, influence campaigns, and disruptive operations against foreign governments, critical infrastructure, and private sectors. Critical Start published a Security Advisory on "Iranian Cyber Threat Activity on U.S. Financial Institutions" more details for additional reference. This advisory provides context and outlines prioritized mitigation strategies designed to help organizations reduce exposure, detect suspicious activity early, and maintain operational resilience during this elevated threat period.

Historical Context

Iran has a well-documented pattern of responding to geopolitical escalation with cyber operations. Key prior campaigns targeting U.S. interests include:

- **Operation Ababil (2012-2014):** Sustained DDoS campaigns targeting U.S. banking portals.
- **Las Vegas Sands Corporation (2014):** Destructive wiper malware deployed in retaliation for statements by the casino's owner.
- **Boston Children's Hospital (2014):** Thwarted intrusion attempt targeting healthcare critical infrastructure.
- **Municipal Ransomware (2016-present):** Iranian nationals have been charged with ransomware attacks crippling U.S. city services.
- **June 2025 (12-Day War):** Cyberattacks against Israel surged within 48 hours of Israeli military strikes on Iran.

The consistent thread across each episode: Iranian cyber retaliation is not immediate, it is staged. Actors conduct reconnaissance and pre-positioning first, then execute.

Top Iranian Threat Groups

This section highlights the most active and notable Iranian-aligned threat groups currently posing significant cyber risks. Understanding their tactics, techniques, procedures (TTPs) and targets is crucial for anticipating potential attacks and strengthening defensive measures against their evolving operations.

MuddyWater (Primary Threat)

Affiliation	Iranian Ministry of Intelligence and Security (MOIS)
Also Known As	Seedworm, MERCURY, Earth Vetala, TA450, Boggy Serpens, Static Kitten
Primary Targets	Government, Energy, Telecommunications, Critical Infrastructure
Key Tradecraft	Spear-phishing with macro-enabled documents, RMM tool abuse (ScreenConnect, Atera), password spraying, MFA fatigue, custom backdoors (BugSleep, LiteInject)

PIONEER KITTEN (Secondary Threat)

Affiliation	Islamic Revolutionary Guard Corps (IRGC)
Also Known As	Fox Kitten, UNC757, Parisite
Primary Targets	Technology, Government, Defense, Healthcare, Energy
Key Tradecraft	Exploitation of internet-facing VPNs and network appliances, SSH tunneling via Ngrok/SSHMinion, web shell deployment, hands-on-keyboard via RDP

Nimbus Manticore (Emerging Threat)

Affiliation	IRGC-aligned
Also Known As	Related to Educated Manticore cluster
Primary Targets	Aerospace, Telecommunications, Defense
Key Tradecraft	Fake recruiter personas and fraudulent career portals, multi-stage DLL sideloading into legitimate Windows executables, custom backdoors (Minibike, MiniJunk, MiniBrowse), cloud C2 via Azure/Cloudflare

While MuddyWater, Pioneer Kitten, and Nimbus Manticore are highlighted, other actors also contribute to the broader cyber threat activity linked to Iran. These include APT42, APT33 (also known as Elfin, MAGNALLIUM, Refined Kitten, HOLMIUM), Curium (UNC1549, IMPERIAL KITTEN, Tortoiseshell), MalKamak, Storm-1084 (DEV-1084), GreenCharlie, and Ferocious Kitten. Many of these groups share tradecraft and collaborate operationally, so attribution should be approached carefully. Collectively, they employ a wide range of espionage and disruptive tactics, emphasizing the need for comprehensive defense strategies.

Tactics, Techniques, and Procedures

The table below consolidates the known TTPs of MuddyWater, Pioneer Kitten and other Iran-affiliated cyber threat actors to help frame how Iranian-aligned groups typically operate. This is not an exhaustive list of all methods employed by Iranian-aligned threat actors but a starting point.

Tactic	Technique ID	Technique Name	Actor
Resource Development	T1583.001	Acquire Infrastructure: Domains	MuddyWater, APT35
Resource Development	T1587.001	Develop Capabilities: Malware	MuddyWater
Reconnaissance	T1595.002	Active Scanning: Vulnerability Scanning	PIONEER KITTEN
Initial Access	T1566.001	Phishing: Spearphishing Attachment	MuddyWater, APT35
Initial Access	T1190	Exploit Public-Facing Application	PIONEER KITTEN
Initial Access	T1078	Valid Accounts (Credential Abuse)	MuddyWater, PIONEER KITTEN
Execution	T1059.001	Command and Scripting: PowerShell	MuddyWater, APT35
Execution	T1204.002	User Execution: Malicious Macro	MuddyWater
Persistence	T1547.001	Boot/Logon: Registry Run Keys	MuddyWater
Persistence	T1505.003	Server Software Component: Web Shell	PIONEER KITTEN
Defense Evasion	T1055	Process Injection	MuddyWater
Defense Evasion	T1078.002	Valid Accounts: Domain Accounts	PIONEER KITTEN
Credential Access	T1110.003	Brute Force: Password Spraying	MuddyWater
Credential Access	T1621	Multi-Factor Authentication Request Gen.	MuddyWater
Collection	T1114	Email Collection (HYPERSCRAPE)	APT35
Command & Control	T1219	Remote Access Software (RMM Tools)	MuddyWater
Command & Control	T1090	Proxy: External Proxy (Ngrok/SSHMinion)	PIONEER KITTEN
Command & Control	T1071.001	Application Layer Protocol: Web Protocols	PIONEER KITTEN
Exfiltration	T1041	Exfiltration Over C2 Channel	MuddyWater
Exfiltration	T1005	Data from Local System	IRGC-affiliated actors
Impact	T1485	Data Destruction (Wiper Malware)	IRGC-affiliated actors
Impact	T1498	Network Denial of Service (DDoS)	Handala Hack, proxies

While the named actors have distinct labels, they often share tradecraft and operational methods, so historical behaviors, such as spear-phishing, credential harvesting, exploitation of unpatched services, and custom malware deployment, are useful for understanding likely adversary actions.

What to Watch For

The following activities reflect the types of operations Iranian-aligned threat actors are likely to pursue in the current environment. Organizations should monitor these behaviors closely to identify potential threats early and guide defensive actions:

Pre-Positioning and Reconnaissance Activity

Elevated scanning of internet-facing infrastructure, VPN appliances, and network edge devices for vulnerabilities is expected. Threat actors are identifying targets of opportunity prior to executing more disruptive operations. Unusual authentication attempts, abnormal MFA push activity, and attempts to exploit known CVEs should be treated as precursors.

Increased Targeting of Critical Infrastructure

Energy grids, water utilities, transportation networks, telecommunications providers, and defense industrial base organizations should expect heightened targeting. Iranian actors have previously probed U.S. water utility SCADA and ICS systems. With conventional military options degraded, disrupting essential services carries high strategic value as a signaling mechanism.

Destructive Malware and Wiper Deployments

Iranian actors are known to deploy wiper malware and ransomware during periods of high escalation. Organizations should watch for indicators including rapid mass file deletion or encryption, volume shadow copy deletion, Master Boot Record (MBR) modification attempts, and lateral movement from previously dormant footholds. The goal of these operations is disruption and economic damage, not just data theft.

DDoS and Service Disruption Campaigns

Pro-Iranian hacktivist groups and botnet infrastructure (notably HydraC2 and groups associated with the Handala and Sicarii clusters) are actively mobilizing. DDoS attacks represent the most immediately available retaliatory tool across the hacktivist ecosystem. Pro-Russian groups including Noname057(16) have joined in support, expanding available botnet capacity. Customer-facing services and public-sector portals are likely targets.

Ransomware and Extortion

PIONEER KITTEN has been linked to ransomware operations in collaboration with affiliates not limited to ALPHV/BlackCat, DEV-1084, NoEscape. Post-strike, financially motivated ransomware operations against U.S. targets may serve dual purposes of revenue generation and operational disruption.

Iran-Themed Phishing Lures

Social engineering campaigns will align with the current news cycle. Watch for phishing emails using themes such as:

- Breaking news alerts about the Iran conflict prompting users to click links or open attachments.
- Fake government notifications, emergency alerts, or security warnings tied to the strikes.
- Recruitment-themed lures impersonating aerospace, defense, and government contractors.
- Credential-harvesting pages mimicking VPN portals, Microsoft 365, or corporate SSO login screens.

What Critical Start is Doing

The Critical Start CRU and Security Operations Center are operating at heightened vigilance in response to the current threat environment. Specific actions underway include:

- **Increased Monitoring:** SOC analysts are operating with an elevated monitoring posture to observe for anomalous authentication events, lateral movement patterns, unusual outbound connections, and PowerShell-based execution chains commonly associated with Iranian actor tradecraft. Alerts will be investigated according to established SLAs.
- **IOC Deployment:** Indicators of compromise are being gathered and prepared for operationalization. Threat hunts using these IOCs will be conducted in the coming days.
- **Intelligence Monitoring:** The CRU is maintaining continuous monitoring of threat intelligence sources, government advisories (CISA, FBI, CYBERCOM), and ISAC feeds for emerging indicators and actor activity updates related to this conflict.
- **Detection Uplift:** The SOC and Security Engineering teams are actively reviewing and expanding detection coverage aligned to MuddyWater, PIONEER KITTEN, and Nimbus Manticore TTPs, IOCs, and behavioral indicators documented in this advisory. The table below gives a summary:

Behavioral Layer	MITRE Techniques	Description	What We Monitor For	Typical Telemetry Sources
Pre-Compromise & Reconnaissance	T1583.001, T1587.001, T1595.002	Domain registration, malware development, and external vulnerability scanning	Malicious domain activity, scanning patterns, reconnaissance traffic, threat intel correlations	Threat intel, DNS, firewall, web server logs
Initial Access & Identity Abuse	T1566.001, T1190, T1078, T1110.003, T1621	Phishing, public-facing application exploitation, credential abuse, password spraying, MFA fatigue	Suspicious attachments, anomalous authentication attempts, MFA push abuse, web exploitation patterns	Endpoint EDR, identity provider logs, email security, WAF
Execution & Persistence	T1059.001, T1204.002, T1547.001, T1505.003	PowerShell abuse, macro execution, registry persistence, web shell deployment	Abnormal scripting activity, Office child process spawning, persistence registry changes, web shell artifacts	Endpoint EDR, OS event logs, web server logs
Defense Evasion & Privilege Abuse	T1055, T1078.002	Process injection and misuse of privileged/domain accounts	Suspicious parent-child processes, injection behavior, abnormal privileged account usage, lateral movement indicators	Endpoint EDR, AD logs, identity telemetry
Command & Control	T1219, T1090	Remote management tools and encrypted tunneling/proxy services	Unauthorized RMM tool execution, rare outbound connections, encrypted tunnel creation, anomalous DNS patterns	Endpoint EDR, DNS, firewall, proxy logs
Collection & Exfiltration	T1114, T1041	Email harvesting and data theft over command-and-control channels	Mailbox access anomalies, bulk export behavior, large outbound encrypted transfers	Email logs, cloud audit logs, proxy/firewall telemetry
Impact	T1485, T1498	Destructive malware (wipers) and denial-of-service activity	Mass file deletion, disk overwrite patterns, service disruption activity, network saturation events	Endpoint EDR, server logs, network telemetry

Organizational Mitigation Strategies

In light of the elevated threat environment following Operation Epic Fury, organizations should implement or validate the following mitigation strategies, prioritized by recommended timeframes:

24-48 Hours

- Audit MFA configurations and disable legacy authentication protocols
- Patch the CVEs listed in the advisory and further reading links, prioritizing any internet-facing VPNs and network appliances. If you have VMS, expect an outreach from the team
- Send employee awareness communications specifically about conflict-themed phishing lures
- Validate rules of engagement (ROE) in place to allow Critical Start to take remediation actions, and ensure your notification groups are up-to-date for proper escalation

1 - Week

- Audit VPN, firewall, and appliance configurations for unauthorized access
- Block or sandbox macro-enabled attachments and validate email security controls (DMARC/DKIM/SPF)
- Audit all RMM tools (ScreenConnect, Atera, AnyDesk) for unauthorized instances. Detection opportunities exist. Feel free to reach out to CSM for customization and deployment
- Validate DDoS mitigation capabilities and upstream provider agreements

30-Days

- Implement or review network segmentation to limit lateral movement from compromised edge devices
- Conduct phishing simulations reflecting Iranian APT lure styles
- Develop and test incident response playbooks for sustained DDoS scenarios
- Review service account permissions and enforce least-privilege access broadly
- Implement or review network segmentation to limit lateral movement from compromised edge devices

Conclusion

Iranian cyber actors have a proven, consistent track record of responding to kinetic escalation with cyber operations targeting U.S. and allied critical infrastructure. Operation Epic Fury represents a significant escalation that eliminates Iran's conventional deterrence, making cyber the primary remaining tool of retaliation. The threat is active, the actors are capable, and the targeting is broad across all critical infrastructure sectors. The Critical Start CRU will continue to monitor developments and publish updates via the Intelligence Hub and CORR Bulletins. Customers with questions should feel free to engage with their Customer Success Managers.

Further Reading

1. Critical Start - Iranian Cyber Threat Activity on U.S. Financial Institutions
2. Google - Tool of First Resort: Israel-Hamas War in Cyber
3. Infosecurity Magazine – Iran: Nimbus Manticore (European targets)
4. CISA Cybersecurity Advisory AA24-290A
5. Sophos – Cyber advisory: increased cyber risk amid U.S.-Israel-Iran escalation
6. FBI IC3 CSA (220914) PDF
7. FBI – The Iran Threat
8. Microsoft - MERCURY and DEV-1084: Destructive attack on hybrid environment
9. Unit42 - Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran
10. CISA - Iran State-Sponsored Cyber Threat: Advisories
11. Washington Institute - Iran Crisis Moves Into Cyberspace

CVE Reference Table

CVE ID	Description	CVSS Score
CVE-2020-0688	Remote code execution vulnerability in Microsoft Exchange Server due to static validation key, allowing authenticated attackers to execute arbitrary code with SYSTEM privileges.	8.8 (High)
CVE-2018-20250	Path traversal vulnerability in WinRAR ACE format handler (UNACEV2.DLL) allowing extraction of files to arbitrary locations, enabling code execution on the next login.	7.8 (High)
CVE-2017-11882	Memory corruption vulnerability in Microsoft Office Equation Editor (EQNEDT32.EXE) allowing remote code execution via specially crafted Office documents.	7.8 (High)
CVE-2017-11774	Security feature bypass in Microsoft Outlook allowing attackers to execute arbitrary commands by convincing a user to open a specially crafted file.	7.8 (High)
CVE-2017-0199	Remote code execution vulnerability in Microsoft Office/WordPad via OLE interface, exploited via malicious RTF or HTA files delivered through phishing.	7.8 (High)
CVE-2023-3519	Unauthenticated remote code execution vulnerability in Citrix NetScaler ADC and NetScaler Gateway when configured as a gateway or AAA virtual server.	9.8 (Critical)
CVE-2022-1388	Authentication bypass vulnerability in F5 BIG-IP iControl REST API allowing unauthenticated remote code execution with root-level privileges.	9.8 (Critical)
CVE-2021-20016	SQL injection vulnerability in SonicWall SSLVPN SMA100 allowing unauthenticated attackers to access credentials and session information.	9.8 (Critical)
CVE-2018-13379	Path traversal vulnerability in Fortinet FortiOS SSL VPN web portal allowing unauthenticated attackers to download system files, including plaintext credentials.	9.8 (Critical)
CVE-2021-26855	Server-Side Request Forgery (SSRF) vulnerability in Microsoft Exchange Server allowing unauthenticated attackers to send arbitrary HTTP requests and authenticate as the Exchange server (ProxyLogon).	9.8 (Critical)
CVE-2021-34473	Pre-authentication remote code execution vulnerability in Microsoft Exchange Server via a backend URL rewrite issue, part of the ProxyShell exploit chain.	9.8 (Critical)
CVE-2021-34523	Elevation of privilege vulnerability in Microsoft Exchange Server PowerShell backend, part of the ProxyShell exploit chain enabling execution of arbitrary cmdlets.	9.8 (Critical)
CVE-2020-1472	Privilege escalation vulnerability (Zerologon) in Microsoft Netlogon Remote Protocol allowing unauthenticated attackers to establish a vulnerable Netlogon channel and take over the domain controller.	10.0 (Critical)
CVE-2019-0604	Remote code execution vulnerability in Microsoft SharePoint Server due to improper input validation, exploitable via specially crafted SharePoint application packages.	9.8 (Critical)
CVE-2021-44228	Remote code execution vulnerability in Apache Log4j 2 (Log4Shell) via JNDI lookup features; allows unauthenticated attackers to execute arbitrary code by logging a crafted string.	10.0 (Critical)
CVE-2022-26134	Object-Graph Navigation Language (OGNL) injection vulnerability in Atlassian Confluence Server and Data Center allowing unauthenticated remote code execution.	9.8 (Critical)
CVE-2023-22515	Broken access control vulnerability in Atlassian Confluence Data Center and Server allowing external attackers to create unauthorized Confluence administrator accounts.	10.0 (Critical)
CVE-2023-27350	Authentication bypass vulnerability in PaperCut MF/NG print management software allowing unauthenticated remote code execution with SYSTEM-level privileges.	9.8 (Critical)

CVE ID	Description	CVSS Score
CVE-2022-47966	Remote code execution vulnerability in multiple Zoho ManageEngine products due to use of an outdated Apache Santuario library, exploitable by unauthenticated attackers.	9.8 (Critical)
CVE-2019-19781	Path traversal vulnerability in Citrix Application Delivery Controller (ADC) and Gateway allowing unauthenticated remote code execution.	9.8 (Critical)
CVE-2019-11510	Arbitrary file read vulnerability in Pulse Connect Secure SSL VPN allowing unauthenticated attackers to retrieve sensitive files including plaintext credentials.	10.0 (Critical)
CVE-2020-5902	Remote code execution vulnerability in F5 BIG-IP Traffic Management User Interface (TMUI) allowing unauthenticated attackers to execute system commands.	9.8 (Critical)
CVE-2024-21887	Command injection vulnerability in Ivanti Connect Secure and Policy Secure web components allowing authenticated administrators to execute arbitrary commands via specially crafted requests.	9.1 (Critical)
CVE-2024-3400	Command injection vulnerability in Palo Alto Networks PAN-OS GlobalProtect Gateway allowing unauthenticated attackers to execute arbitrary code with root privileges.	10.0 (Critical)
CVE-2024-24919	Information disclosure vulnerability in Check Point Security Gateway allowing attackers to read sensitive information, including password hashes, potentially enabling further compromise.	8.6 (High)