IRANIAN APT THREAT INTELLIGENCE REPORT

HORIZON3.ai

Iranian Advanced Persistent Threats

Comprehensive TTP Analysis, Exploit Inventory & NodeZero Cross-Mapping

Threat Research | Horizon3.ai

March 2026 | TLP: WHITE

OSINT-Based Threat Intelligence Report

Table of Contents

Executive Summary

This report provides a comprehensive deep-dive into Iranian Advanced Persistent Threat (APT) groups active from 2023 through early 2026. Based on open-source intelligence (OSINT) from CISA advisories, Microsoft Threat Intelligence, Google Mandiant, Palo Alto Unit42, CrowdStrike, and other leading threat research organizations, this document profiles the primary Iranian state-sponsored threat actors, their documented Tactics, Techniques, and Procedures (TTPs), specific CVEs actively weaponized, and the types of devices and infrastructure they target.

A critical component of this report is a cross-mapping between Iranian APT exploitation techniques and NodeZero's autonomous penetration testing capabilities — enabling Horizon3.ai customers to understand which Iranian TTPs NodeZero can actively validate within their environments.

Key findings:

- Iran operates at least 10 distinct APT groups under IRGC and MOIS direction, each with differentiated targeting mandates and TTPs.
- Iranian APTs have weaponized over 20 distinct CVEs across VPN appliances, Windows kernel, web platforms, and industrial control systems — often within days of public disclosure.
- Primary targeted device classes: edge network devices (Fortinet, Citrix, Ivanti/Pulse Secure, F5 BIG-IP, Palo Alto PAN-OS), industrial PLCs/HMIs (Unitronics), Microsoft Exchange/AD, and MikroTik routers.
- Post-October 7, 2023, Iranian cyber operations increased 2.5x in volume and expanded geographically to target US, European, and Gulf state organizations.
- NodeZero maps strongly to Iranian APT TTPs — particularly VPN exploitation, credential attacks, Active Directory abuse, and lateral movement. ICS/OT and social engineering fall outside NodeZero's scope.

Organizational Attribution:

- IRGC (Islamic Revolutionary Guard Corps): APT33, APT35, APT42, Fox Kitten, CyberAv3ngers, Cotton Sandstorm, Void Manticore, Tortoiseshell/UNC1549
- MOIS (Ministry of Intelligence and Security): OilRig/APT34, MuddyWater/Seedworm

Iranian APT Group Profiles

The following profiles detail major Iranian APT groups active in 2023–2026, including organizational affiliation, primary targets, tooling, and documented TTPs mapped to MITRE ATT&CK.

1. OilRig / APT34 (MOIS)

Also known as: Earth Simnavaz, Helix Kitten, Hazel Sandstorm, EUROPIUM, Crambus, TA452, COBALT GYPSY

Affiliation: Ministry of Intelligence and Security (MOIS) | Active Since: 2014

Primary Targets: Energy, finance, government, chemical, telecom; Middle East, US, Europe, India, Iraq

Notable Campaigns (2023–2025):

- CVE-2024-30088 Exploitation — Windows Kernel TOCTOU race condition (CVSS 7.0) exploited to gain SYSTEM privileges; deployed STEALHOOK backdoor via Microsoft Exchange servers against UAE and Gulf governments. Confirmed by Hacker News (Oct 2024).
- Iraqi Government Networks (2024) — elaborate campaign using MOIS-associated installer logos targeting Iraq's Prime Minister's Office and Foreign Ministry (Check Point Research).
- Earth Simnavaz / Gulf Campaign (2023–2024) — targeting UAE and Gulf governments; used ngrok tunneling, password filter DLLs for credential harvesting, and custom web shells.
- Israeli/Emirati Defense Companies (2024) — M365 credential harvesting via compromised Microsoft 365 infrastructure and PowerShell loaders.

Key Malware & Tools:

- Backdoors: SideTwist, Menorah (evolved SideTwist), STEALHOOK, Helminth, SaitamaAgent, AgentDrable, QUADAGENT, ISMAgent
- Web Shells: TwoFace, HyperShell, HighShell, RunningBee, IntrudingDivisor (deployed on Exchange/IIS)
- Credential Tools: ValueVault (browser credential harvester), Pickpocket (LSASS dumper), custom password filter DLLs, Mimikatz, LaZagne
- C2 & Tunneling: DNS tunneling (T1071.004), HTTP exfiltration, Plink (SSH tunneling), ngrok

MITRE ATT&CK TTPs:

Technique ID	Technique Name	Description / Evidence
T1566.001	Spearphishing Attachment	Malicious Office docs exploiting CVE-2017-11882

T1059.001	PowerShell	Obfuscated PS scripts (Invoke-Obfuscation) for C2 and credential ops
T1505.003	Web Shell	TwoFace, HyperShell, HighShell, RunningBee on Exchange/IIS
T1003.001	LSASS Memory Dump	Pickpocket/Mimikatz for credential harvesting
T1114.002	Remote Email Collection	Exchange credential extraction, M365 access abuse
T1071.004	DNS for C2	DNS tunneling for persistent C2 communications
T1567	Exfil Over Web Service	HTTP/FTP exfiltration via compromised email accounts
T1068	Exploitation for Priv Esc	CVE-2024-30088 (Windows Kernel TOCTOU) → SYSTEM access
T1053.005	Scheduled Task	Persistence via Windows scheduled tasks

Key CVEs Used:

- CVE-2024-30088 — Windows Kernel TOCTOU Race Condition, EoP to SYSTEM (CVSS 7.0) — active exploitation confirmed Q3/Q4 2024
- CVE-2017-11882 — Microsoft Office Equation Editor memory corruption RCE
- CVE-2019-0604 — Microsoft SharePoint RCE
- CVE-2020-0688 — Microsoft Exchange Server EoP
- CVE-2021-26855 — Microsoft Exchange Server SSRF (ProxyLogon) — part of web shell deployment chain

2. MuddyWater / Seedworm (MOIS)

Also known as: Static Kitten, MERCURY, Earth Vetala, Mango Sandstorm, TA450, TEMP.Zagros

Affiliation: Ministry of Intelligence and Security (MOIS) | Active Since: 2017

Primary Targets: Government, defense, telecom, oil/gas; Middle East, Central Asia, Europe, US, Israel

Notable Campaigns (2023–2025):

- DarkBeatC2 Framework (Early 2024) — evolved C2 infrastructure replacing PhonyC2/MuddyC2Go, identified in Operation Diplomatic Specter analysis.
- BugSleep / MuddyRot Backdoor (May 2024+) — new phishing campaigns targeting Israel and regional targets; improved evasion vs. prior tooling.

- MuddyViper + Fooder Uploader (2024–2025) — modular implant family; MuddyViper impersonates Veeam, AnyDesk, Xerox, and OneDrive updater processes (VAXOne).
- Fortinet Mass Exploitation — CVE-2024-55591 (CVSS 9.8), CVE-2024-23113 (CVSS 9.8), CVE-2022-42475 for edge device RCE.
- N-able N-central Exploitation (2025) — CVE-2025-9316 mass exploitation against Managed Service Providers (MSPs).
- ChromeStealer (2025) — custom Chromium-based credential stealer targeting Chrome, Opera, Brave, and Edge; decrypts login data from Local State encrypted keys.

Key Malware & Tools:

- Backdoors/Implants: BugSleep/MuddyRot, MuddyViper, VAXOne, PowGoop, Mori, Covicli, POWERSTATS, Small Sieve, Canopy/SloughRAT
- Credential Stealers: ChromeStealer, CE-Notes, Blub, LP-Notes
- RMM Abuse: Atera Agent, ConnectWise ScreenConnect, SimpleHelp, N-able, MeshCentral (used for legitimate-looking C2)
- Open-Source Tools: LaZagne, Chisel, PLink, FRP (Fast Reverse Proxy), Ligolo

MITRE ATT&CK TTPs:

Technique ID	Technique Name	Description / Evidence
T1566.001/002	Spearphishing	Malicious attachments/links; conflict-themed lures
T1219	Remote Access Software	Atera, ConnectWise ScreenConnect, SimpleHelp RMM abuse for C2
T1059.001	PowerShell	PowerShell-based backdoors, loaders, and C2 comms
T1547.004	Winlogon Helper DLL	Persistence via Winlogon registry modifications
T1218.005	Mshta	HTA file execution for initial payload delivery
T1105	Ingress Tool Transfer	Tools dropped via legitimate RMM channels
T1003.001	Credential Dumping	LaZagne, ChromeStealer for post-exploitation credential collection
T1190	Exploit Public-Facing App	Fortinet CVEs, N-able N-central; fast weaponization of KEV CVEs

Key CVEs Used:

- CVE-2024-55591 — Fortinet FortiOS/FortiProxy authentication bypass → RCE (CVSS 9.8) — exploited 2025
- CVE-2024-23113 — Fortinet FortiOS format string vulnerability, RCE (CVSS 9.8) — exploited 2024
- CVE-2025-9316 — N-able N-central RCE — mass exploitation against MSPs in 2025
- CVE-2023-27350 — PaperCut NG/MF unauthenticated RCE (CVSS 9.8) — exploited 2023
- CVE-2022-42475 — Fortinet FortiOS SSL-VPN buffer overflow RCE (CVSS 9.3)
- CVE-2020-1472 — Zerologon, Windows Netlogon EoP to domain compromise (CVSS 10.0)

3. APT33 / Peach Sandstorm (IRGC)

Also known as: Elfin, Refined Kitten, MAGNALLIUM, Holmium

Affiliation: Islamic Revolutionary Guard Corps (IRGC) | Active Since: 2013

Primary Targets: Aerospace, defense, petrochemical, satellite, government; US, Middle East, Europe, South Korea

Notable Campaigns (2023–2025):

- **Password Spray Campaigns (2023) —** large-scale targeting of US defense industrial base (DIB) organizations; authenticated with valid accounts before deploying implants.
- **FalseFont Backdoor (Late 2023) —** custom backdoor deployed against DIB targets following password spray compromise; signed executable disguised as legitimate software.
- **Tickler Backdoor (2024) —** multi-stage C/C++ backdoor in ZIP archives using double-extension masquerading (e.g., .pdf.exe). Uses PEB traversal to locate kernel32.dll and resolve APIs dynamically, bypassing EDR API hook inspection. Persists via Run registry key as 'SharePoint.exe'. C2 hosted on attacker-controlled Azure subscriptions to blend with legitimate Microsoft traffic.

MITRE ATT&CK TTPs:

- **T1078.004 —** Cloud Accounts: Attacker-controlled Azure subscriptions for Tickler C2
- **T1110.003 —** Password Spray: Large-scale valid account compromise against DIB organizations
- **T1059.001 —** PowerShell: Malicious scripts for payload execution
- **T1547.001 —** Registry Run Keys: Tickler persists as 'SharePoint.exe' in Run key
- **T1036.005 —** Match Legitimate Name: Tickler masquerades as Microsoft SharePoint process
- **T1027 —** Obfuscated Files: PEB traversal to bypass EDR API hooks

Key CVEs Used:

- **CVE-2017-11774 —** Microsoft Outlook home page property RCE (persistence mechanism)
- **CVE-2018-20250 —** WinRAR ACE archive code execution

4. APT35 / Charming Kitten / Mint Sandstorm (IRGC)

Also known as: Phosphorus, Newscaster, TA453, Cobalt Illusion, Magic Hound, ITG18, Damselfly

Affiliation: Islamic Revolutionary Guard Corps (IRGC) | Active Since: 2011

Primary Targets: Academics, policy experts, journalists, nuclear experts, government officials, presidential campaigns; US, Israel, UK, France, Belgium, Gaza

Notable Campaigns (2023–2025):

- **Nuclear Security Expert Targeting (July 2023) —** US-based think tank researcher targeted using tailored social engineering.
- **Israel Sector Attacks (Nov 2023) —** transportation, logistics, and technology sectors; conflict-themed phishing lures.
- **Multi-Country Academia Campaign (Jan 2024) —** universities and research organizations across Belgium, France, Gaza, Israel, UK, US; Israel-Hamas conflict themes used to build rapport before credential harvesting.
- **US Presidential Campaign Targeting (2024) —** confirmed by Microsoft MSTIC; campaign staff of a presidential candidate targeted alongside Israeli military and political personnel.
- **NICECURL & TAMECAT Backdoors —** VBScript (NICECURL) and PowerShell (TAMECAT) implants used for intelligence collection from high-value targets.

MITRE ATT&CK TTPs:

- **T1598.003 —** Spearphishing Link: Sophisticated social engineering, conflict-themed lures, often multi-stage
- **T1534 —** Internal Spearphishing: Using compromised trusted accounts to reach additional targets
- **T1566.003 —** Spearphishing via Service: LinkedIn, WhatsApp, Signal social engineering personas
- **T1185 —** Browser Session Hijacking: Stealing authentication cookies and session tokens
- **T1059.001/005 —** PowerShell/VBScript: TAMECAT (PS) and NICECURL (VBS) backdoors
- **T1056.001 —** Keylogging: Intelligence collection on targeted workstations

5. APT42 (IRGC)

Also known as: Charming Kitten (variant), UNC788, TA453 (overlap with APT35 in some reporting)

Affiliation: Islamic Revolutionary Guard Corps (IRGC) | Active Since: 2015

Primary Targets: Journalists, activists, civil society, policymakers, diaspora; US, EU, Middle East, Israel, Iran dissidents

Notable Campaigns (2023–2025):

- **Journalist/Researcher Impersonation —** elaborate social engineering using fabricated journalist/researcher personas to build trust before delivering credential-harvesting links.
- **TAMECAT Backdoor —** PowerShell-based remote access tool for intelligence collection from targeted endpoints.
- **NICECURL Backdoor —** VBScript implant for initial access operations and data collection.
- **Post-October 7 Operations (Nov 2023) —** phishing campaigns targeting US and Israeli government officials, diplomats, and US-Israel policy experts. Confirmed by Google GTIC.
- **Operational Records Leak (December 2025) —** internal spreadsheets exposed tracking domain registrations, European VPS providers, and cryptocurrency payments routed through Bitcoin wallets and the Cryptomus payment processor. Provided rare insight into IRGC cyber program administration.

MITRE ATT&CK TTPs:

- **T1656 —** Impersonation: Fabricated journalist/researcher personas for trust establishment
- **T1566.002 —** Spearphishing Link: Links to credential-harvesting infrastructure
- **T1539 —** Steal Web Session Cookie: OAuth token theft for account takeover
- **T1059.005 —** VBScript: NICECURL implant delivery
- **T1059.001 —** PowerShell: TAMECAT for C2 and collection

6. Fox Kitten / Pioneer Kitten (IRGC)

Also known as: UNC757, Parisite, RUBIDIUM, Lemon Sandstorm, Br0k3r, xplfinder

Affiliation: Islamic Revolutionary Guard Corps (IRGC); cover company: Danesh Novin Sahand | Active Since: 2017

Primary Targets: Defense, aerospace, oil and gas, water, electric, healthcare, education; US, Middle East, Europe, Australia

Notable Campaigns (2023–2025):

- **Extended CNI Compromise (May 2023 – Feb 2025) —** documented 21-month persistent access campaign against Middle East critical national infrastructure via VPN exploitation and web shell deployment.
- **Ransomware Collaboration (2024) —** FBI/CISA/DC3 joint advisory AA24-241A (Aug 2024) confirmed collaboration with BlackCat/AlphV and NoEscape ransomware affiliates; Fox Kitten provides network access and ransomware deployment assistance in exchange for a share of ransom proceeds.

- **Br0k3r/xplfinder Rebrand (2024) —** rebranded from Br0k3r as an initial access broker selling network access on dark web forums.
- **RUBIDIUM / Lemon Sandstorm Operations —** continued CNI targeting in UAE, Saudi Arabia, and Kuwait through 2025.

Key CVEs Used — Fox Kitten is Iran's primary VPN/edge exploitation specialist:

- **CVE-2019-11510 —** Pulse Connect Secure arbitrary file read, pre-auth credential theft (CVSS 10.0)
- **CVE-2019-19781 —** Citrix NetScaler ADC/Gateway path traversal to RCE (CVSS 9.8)
- **CVE-2020-5902 —** F5 BIG-IP TMUI RCE (CVSS 9.8)
- **CVE-2022-1388 —** F5 BIG-IP iControl REST API authentication bypass to RCE (CVSS 9.8)
- **CVE-2023-3519 —** Citrix NetScaler ADC/Gateway unauthenticated RCE (CVSS 9.8)
- **CVE-2024-21887 —** Ivanti Connect Secure command injection (CVSS 9.1); paired with CVE-2024-21893 (SSRF, CVSS 8.2)
- **CVE-2024-3400 —** Palo Alto PAN-OS GlobalProtect OS command injection (CVSS 10.0)

MITRE ATT&CK TTPs:

- **T1190 —** Exploit Public-Facing Application: Primary initial access vector via VPN/gateway CVEs
- **T1133 —** External Remote Services: Persistence via compromised VPN/remote access footholds
- **T1505.003 —** Web Shell: Post-exploitation web shells for persistent access
- **T1078 —** Valid Accounts: Credentials harvested from VPN compromise used for lateral movement
- **T1486 —** Data Encrypted for Impact: Ransomware deployment through criminal affiliate partnerships
- **T1021.004 —** SSH: Lateral movement using SSH tunneling

7. Void Manticore / Storm-842 (IRGC)

Also known as: Scarred Manticore, DEV-0842, BANISHED KITTEN, DUNE, Handala Hack Team

Affiliation: Islamic Revolutionary Guard Corps (IRGC) | Active Since: ~2020

Primary Targets: Israeli organizations, Albanian government, critical infrastructure

Notable Campaigns (2023–2025):

- **Israel Destructive Campaign (2023–2024) —** deployed BiBi-Linux and BiBi-Windows wipers against Israeli organizations, overwriting files and MBR to render systems inoperable.

- **Albania Operations (2022–2023) —** destructive wiper attacks targeting Albanian government infrastructure, including the national e-Albania portal, in response to Albania hosting the MEK opposition group.
- **Cooperation with Scarred Manticore —** documented task-sharing: Scarred Manticore handles initial access; Void Manticore conducts destructive operations on the same target.
- **WhiteLock Ransomware (2025) —** ransomware deployment against Israeli entities causing operational disruptions.

MITRE ATT&CK TTPs:

- **T1485 —** Data Destruction: BiBi wiper family overwrites files and MBR
- **T1486 —** Data Encrypted for Impact: WhiteLock ransomware deployment
- **T1505.003 —** Web Shell: Post-exploitation persistence prior to destructive phase
- **T1041 —** Exfiltration Over C2 Channel: Data theft precedes destruction
- **T1490 —** Inhibit System Recovery: Shadow copy deletion, backup destruction

8. CyberAv3ngers / IRGC-CEC

Affiliation: IRGC Cyber-Electronic Command (IRGC-CEC) — US Treasury sanctioned 6 officials, Feb 2024 | Active Since: 2020

Primary Targets: Water/wastewater systems, fuel management, energy OT/ICS infrastructure; US, Israel, Poland, Turkey, Jordan, Gulf states

Notable Campaigns (2023–2025):

- **Unitronics PLC Campaign (Nov–Dec 2023) —** CISA Advisory AA23-335A confirmed compromise of at least 75 Unitronics Vision Series PLCs, including at least 34 in the US Water and Wastewater Systems (WWS) sector. Exploitation method: default credentials via internet-exposed TCP port 20256. Group deployed custom ladder logic files per device type.
- **Aliquippa Municipal Water Authority (Nov 2023) —** first publicly named US water facility confirmed compromised; attackers changed a display screen but operators retained manual control.
- **US Treasury Sanctions (Feb 2024) —** 6 IRGC-CEC officials sanctioned by name, definitively confirming state direction rather than independent hacktivist activity.
- **IP Camera Campaign —** expanded scope to HIKVISION and Teltonika internet-facing surveillance cameras at Israeli and US infrastructure sites.
- **ICS/OT Custom Malware (2024–2025) —** custom ICS-targeting malware deployed against expanded target set including Poland, Turkey, Jordan, and Gulf states.
- **API/Mobile Reconnaissance (Feb 2026) —** surge in reconnaissance against government APIs and mobile applications in Israel and Persian Gulf states.

MITRE ATT&CK TTPs (including ICS framework):

- **T1078.001 —** Default Accounts: Factory default credentials on Unitronics PLCs (primary exploitation method)
- **T1110 —** Brute Force: Credential attacks against internet-exposed OT device management interfaces
- **T1595 —** Active Scanning: Mass internet scanning for Unitronics, HIKVISION, and Teltonika devices
- **T0821 (ICS) —** Modify Controller Tasking: Manipulation of PLC ladder logic programs
- **T0826 (ICS) —** Loss of Availability: Disrupting water/fuel management system operations
- **T1059.006 —** Python: Custom ICS-targeting scripts

9. Cotton Sandstorm / Haywire Kitten (IRGC)

Also known as: Altoufan Team, NEPTUNIUM, Aria Sepehr Ayandehsazan (ASA)

Affiliation: Islamic Revolutionary Guard Corps (IRGC) | Active Since: ~2020

Primary Targets: Influence operations against media, critical infrastructure; Israel, US, Gulf states

Notable Campaigns (2023–2025):

- **Israeli TV Broadcast Hijacking (Dec 2023) —** interrupted streaming television services and replaced programming with an AI-generated fake news anchor delivering pro-Hamas messaging. First documented large-scale AI-generated deepfake use in Iranian IO.
- **Most Prolific Iranian IO Actor —** Microsoft and Google designate ASA as Iran's most active cyber-enabled influence operation threat actor; conducted at least 4 complex high-profile IO operations post-October 7.
- **Sockpuppet Network Deployment —** coordinated social media account networks across multiple platforms for disinformation distribution at scale.
- **2026 Escalation —** part of coordinated campaign alongside CyberAv3ngers and Cyber Islamic Resistance targeting Israel, Persian Gulf states, and US-affiliated organizations.

MITRE ATT&CK TTPs:

- **T1583 —** Acquire Infrastructure: Domain/hosting acquisition for IO campaigns and media impersonation
- **T1491.002 —** External Website Defacement: TV broadcast hijacking; media platform manipulation
- **T1059.004 —** Unix Shell: Linux-based infrastructure compromises
- **T1650 —** Acquire Access: Purchasing or stealing access to social media accounts for IO amplification

10. Tortoiseshell / UNC1549 / Crimson Sandstorm (IRGC)

Also known as: Imperial Kitten, TA456

Affiliation: Islamic Revolutionary Guard Corps (IRGC) | Active Since: 2017

Primary Targets: Defense, aerospace, telecommunications, aviation, regional government; US, Europe, Middle East

Notable Campaigns (2023–2025):

- **LinkedIn Social Engineering Campaign (2022–2025) —** sustained multi-year campaign using fake job recruitment lures on LinkedIn to establish initial footholds; compromised dozens of devices across numerous targeted organizations.
- **Western Aerospace/Defense Espionage (2024–2025) —** named 4th most active Iranian actor in H2 2025 by threat intelligence firms; documented sustained access from original June 2022 footholds through 2025.
- **Watering Hole Attacks —** compromise of aerospace/defense industry-specific websites to deliver malware to visitors.
- **LEMPO/METAJAB Custom Backdoors —** deployed post-LinkedIn compromise for persistent access and data collection.

MITRE ATT&CK TTPs:

- **T1566.003 —** Spearphishing via Service: LinkedIn-based social engineering with fake aerospace/defense job lures
- **T1189 —** Drive-by Compromise: Watering hole attacks on defense/aerospace-sector websites
- **T1505.003 —** Web Shell: Post-exploitation web shell deployment for persistent access
- **T1557 —** Adversary-in-the-Middle: Credential interception in some campaigns
- **T1583.006 —** Web Services: Abuse of legitimate web services for C2

Weaponized CVE & Exploit Inventory

CVEs actively weaponized by Iranian APT groups based on CISA KEV, FBI/CISA joint advisories, and threat research from Microsoft, Mandiant, CrowdStrike, and Palo Alto Unit42. Note on MikroTik CVE-2023-30799: this is an authenticated privilege escalation (requires admin credentials) exploited to gain root; Iranian threat actors have targeted MikroTik routers primarily to use as C2 relay infrastructure.

CVE	Affected Product	Vulnerability Type	CVSS	Attribution	CISA KEV
CVE-2025-9316	N-able N-central	Improper Input Validation	6.9	MuddyWater	No
CVE-2024-30088	Windows Kernel (TOCTOU)	EoP to SYSTEM	7.0	OilRig/APT34	No
CVE-2024-55591	Fortinet FortiOS/FortiProxy	Auth Bypass → RCE	9.8	MuddyWater	Yes
CVE-2024-23113	Fortinet FortiOS	Format String RCE	9.8	MuddyWater	Yes
CVE-2024-21887	Ivanti Connect Secure	Command Injection RCE	9.1	Fox Kitten	Yes
CVE-2024-21893	Ivanti Connect Secure	SSRF	8.2	Fox Kitten	Yes
CVE-2024-3400	Palo Alto PAN-OS	OS Cmd Injection RCE	10.0	Fox Kitten, Multiple	Yes
CVE-2023-3519	Citrix NetScaler ADC/GW	Unauthenticated RCE	9.8	Fox Kitten	Yes
CVE-2023-30799	MikroTik RouterOS	Priv Esc (auth req'd)	9.1	Multiple (C2 relay)	No
CVE-2023-27350	PaperCut NG/MF	Unauthenticated RCE	9.8	MuddyWater	Yes

CVE-2022-42475	Fortinet FortiOS SSL-VPN	Buffer Overflow RCE	9.3	MuddyWater	Yes
CVE-2022-40684	Fortinet FortiOS/FGT/FSM	Auth Bypass	9.8	Multiple	Yes
CVE-2022-1388	F5 BIG-IP iControl	Auth Bypass RCE	9.8	Fox Kitten	Yes
CVE-2021-44228	Apache Log4j (Log4Shell)	RCE via JNDI Injection	10.0	IRGC-Affiliated	Yes
CVE-2021-34473					
CVE-2021-26855	MS Exchange (ProxyLogon)	SSRF → RCE Chain	9.8	OilRig, Multiple	Yes
CVE-2020-5902	F5 BIG-IP TMUI	Unauthenticated RCE	9.8	Fox Kitten	Yes
CVE-2020-1472	Windows Netlogon (Zerologon)	EoP to Domain Compromise	10.0	MuddyWater	Yes
CVE-2020-0688	Microsoft Exchange	EoP to SYSTEM	8.8	MuddyWater	Yes
CVE-2019-11510	Pulse Connect Secure VPN	Pre-auth File Read (creds)	10.0	Fox Kitten	Yes
CVE-2019-19781	Citrix ADC / NetScaler	Path Traversal RCE	9.8	Fox Kitten	Yes
CVE-2019-0604	Microsoft Sharepoint	Unauthenticated RCE	9.8	Multiple	Yes
CVE-2018-20250	WinRAR ACE	ACE Archive Code Exec	7.8	APT33	No
CVE-2017-11882	MS Office Equation Editor	Memory Corruption RCE	7.8	OilRig, Multiple	Yes

CVE-2017-11774	Microsoft Outlook	EoP to System	7.8	OilRig, APT33	Yes

Targeted Device Types & Infrastructure

Iranian APT groups exhibit consistent, repeated patterns in device targeting. Understanding these device categories helps defenders prioritize patching, monitoring, and segmentation.

Category 1: VPN & Remote Access Appliances (Highest Priority)

Edge VPN devices are the single most targeted device category across Iranian APT operations. Fox Kitten/Pioneer Kitten has built its entire operational model around VPN exploitation for initial access, which it then monetizes through ransomware partnerships and access sales.

- Ivanti Connect Secure / Pulse Secure VPN: CVE-2019-11510, CVE-2024-21887, CVE-2024-21893. Fox Kitten weaponized CVE-2024-21887 within days of January 2024 disclosure alongside Chinese APT actors.
- Fortinet FortiGate SSL-VPN: CVE-2022-42475, CVE-2024-55591, CVE-2024-23113. MuddyWater's primary edge exploitation vector for C2 establishment.
- Citrix NetScaler ADC/Gateway: CVE-2019-19781, CVE-2023-3519. Fox Kitten targeted these extensively; CVE-2023-3519 (CitrixBleed) exposed ~900K devices globally at peak.
- Palo Alto Networks PAN-OS Firewalls: CVE-2024-3400 (CVSS 10.0). Weaponized by Iranian and other APTs within days of April 2024 disclosure.
- F5 BIG-IP: CVE-2020-5902, CVE-2022-1388. Both exploited by Fox Kitten for unauthenticated/auth-bypass RCE.

Category 2: Industrial Control Systems & OT Devices

CyberAv3ngers and IRGC-CEC represent a significant and documented Iranian OT exploitation capability, confirmed by CISA and resulting in US Treasury sanctions.

- Unitronics Vision Series PLCs: Primary target. CISA-confirmed exploitation via default credentials on TCP port 20256. At least 75 devices compromised (34 in US WWS sector). Models: Vision1040, V570, V350, V290, V130.
- Unitronics Samba/Jazz Series HMIs: Human-Machine Interfaces co-located with targeted PLCs.
- Teltonika Industrial Routers: Networking gear at industrial sites, targeted in post-PLC expansion.
- HIKVISION IP Cameras: Internet-facing surveillance cameras targeted in mass campaigns, particularly at Israeli and US infrastructure sites.

Category 3: Network Infrastructure — C2 Relay Infrastructure

Iranian APTs compromise network routing devices to use as anonymizing relay nodes, making attribution more difficult by routing malicious traffic through legitimate networks.

- MikroTik RouterOS: CVE-2023-30799 — requires authenticated admin access; escalates to root. Up to 900,000 devices exposed globally. Compromised MikroTik devices used as C2 relay hops by multiple Iranian and other threat groups. Defender note: enforce strong unique admin credentials and restrict Winbox/HTTP management interface exposure.
- SOHO Routers (various): Default credential scanning against Asus, Netgear, TP-Link, and similar consumer/SOHO devices for C2 relay infrastructure.
- Cisco IOS/IOS XE: Targeted for network pre-positioning in critical infrastructure environments.

Category 4: Microsoft Platform Infrastructure

- Microsoft Exchange Server: CVE-2021-26855 (ProxyLogon), CVE-2021-34473 (ProxyShell), CVE-2020-0688. OilRig/APT34 deploys web shells (TwoFace, HyperShell) via Exchange. Exchange is also used as a C2 and exfiltration channel.
- Windows Active Directory / Domain Controllers: Zerologon (CVE-2020-1472), LSASS dumping, Pass-the-Hash. AD is the primary lateral movement target enabling domain-wide compromise.
- Microsoft Azure Cloud Infrastructure: APT33 uses attacker-controlled Azure subscriptions for Tickler C2; blends with legitimate Microsoft traffic to evade detection.
- Microsoft 365 / Exchange Online: Credential harvesting via compromised M365 infrastructure, used against Israeli and Emirati defense companies.

Category 5: Web Application Platforms

- PaperCut NG/MF Print Management: CVE-2023-27350 — unauthenticated RCE; MuddyWater exploited in 2023.
- N-able N-central (MSP RMM): CVE-2025-9316 — mass exploitation by MuddyWater against MSPs in 2025, enabling leverage over multiple downstream organizations.
- Apache Log4j Applications: CVE-2021-44228 (Log4Shell) — IRGC-affiliated actors exploited against US government and defense contractor targets.
- Microsoft SharePoint: CVE-2019-0604 — OilRig/APT34 exploitation for initial access.

Device Targeting Summary

Device / Platform	Key CVEs / Methods	APT Groups	Priority
Ivanti/Pulse Secure VPN	CVE-2019-11510, CVE-2024-21887/21893	Fox Kitten	CRITICAL
Fortinet FortiGate SSL-VPN	CVE-2022-42475, CVE-2024-55591/23113	MuddyWater, Fox Kitten	CRITICAL
Citrix NetScaler ADC/GW	CVE-2019-19781, CVE-2023-3519	Fox Kitten	CRITICAL
Palo Alto PAN-OS	CVE-2024-3400 (CVSS 10.0)	Fox Kitten, Multiple	CRITICAL
F5 BIG-IP	CVE-2020-5902, CVE-2022-1388	Fox Kitten	HIGH
Microsoft Exchange Server	ProxyLogon, ProxyShell, CVE-2020-0688	OilRig/APT34	HIGH
Windows Domain Controllers	CVE-2020-1472 (Zerologon)	MuddyWater, Multiple	HIGH
Unitronics Vision PLCs/HMIs	Default Credentials (TCP/20256)	CyberAv3ngers	HIGH (OT)
MikroTik RouterOS	CVE-2023-30799 (auth req'd)	Multiple (C2 relay)	MEDIUM
HIKVISION IP Cameras	Default Creds, CVE-2021-36260	CyberAv3ngers	MEDIUM
PaperCut NG/MF	CVE-2023-27350	MuddyWater	MEDIUM
Apache Log4j Applications	CVE-2021-44228 (Log4Shell)	IRGC-Affiliated	HIGH
N-able N-central (MSP)	CVE-2025-9316	MuddyWater	HIGH
Azure Cloud Infrastructure	Credential theft / config abuse	APT33, OilRig	HIGH

NodeZero Cross-Mapping: Iranian APT TTPs vs. NodeZero Capabilities

This section cross-references Iranian APT exploitation techniques with NodeZero's autonomous penetration testing capabilities. Coverage ratings reflect NodeZero's documented CVE library, active exploit modules, and published Horizon3.ai Rapid Response advisories as of early 2026.

Data point: NodeZero tested 229 unique CVEs across 50,000+ pentests in 2024, with 170 of those CVEs on the CISA KEV list. Full details: horizon3.ai/nodezero

NodeZero Coverage Matrix

Iranian APT Technique / CVE	APT Group(s)	NodeZero Coverage	Notes
Fortinet CVEs (CVE-2024-55591, CVE-2022-40684)	MuddyWater, Fox Kitten	YES — Confirmed	NodeZero has Fortinet FortiOS/FortiProxy exploit modules; Rapid Response center covers new Fortinet CVEs
Citrix NetScaler ADC/GW (CVE-2023-3519)	Fox Kitten	YES — Confirmed	Citrix NetScaler ADC/Gateway attack content documented in NodeZero module library
Ivanti Connect Secure (CVE-2024-21887/21893)	Fox Kitten	YES — Confirmed	NodeZero Ivanti Connect Secure coverage; Rapid Response for Ivanti CVEs documented
Palo Alto PAN-OS (CVE-2024-3400)	Multiple	YES — Confirmed	CVE-2024-3400 explicitly tested by NodeZero (CVSS 10.0); published in Horizon3.ai Rapid Response blog
F5 BIG-IP (CVE-2022-1388, CVE-2020-5902)	Fox Kitten	LIKELY	F5 BIG-IP in NodeZero scope; confirm specific exploit module for your BIG-IP version with Horizon3 support
Zerologon CVE-2020-1472 (DC Compromise)	MuddyWater	YES — Confirmed	NodeZero chains Zerologon into full domain compromise; demonstrated in Game of Active Directory (GOAD) completion

Iranian APT Technique / CVE	APT Group(s)	NodeZero Coverage	Notes
Active Directory Attack Paths / Domain Takeover	MuddyWater, OilRig, Multiple	YES — Core Capability	First AI to solve GOAD in 14 min; 21,592 AD domain user compromises logged in 2024 pentests
Credential Dumping / LSASS (Mimikatz-style)	OilRig, MuddyWater, Multiple	YES — Core Capability	28,866 credential dumping instances across 50K pentests; AD Password Audit module for weak/breached creds
Password Spray / Brute Force	APT33, CyberAv3ngers, Multiple	YES — Core Capability	NodeZero autonomously tests weak/default credentials; AD Password Audit covers spray patterns
Default Credentials (Network / OT Devices)	CyberAv3ngers	YES — Core Capability	Default credential testing across network devices is a core NodeZero behavior across all pentest types
MS Exchange ProxyLogon / ProxyShell	OilRig/APT34	YES — Confirmed	Exchange exploitation chains included in standard NodeZero internal pentest modules
Windows Kernel EoP (CVE-2024-30088)	OilRig/APT34	LIKELY — N-day	NodeZero tracks N-day CVEs; kernel EoP availability depends on Windows version patching; confirm via Rapid Response
Log4Shell (CVE-2021-44228)	IRGC-Affiliated	YES — Confirmed	Log4Shell is among NodeZero's core CVE coverage given prevalence across enterprise Java applications
PowerShell / LOLBins (Living off the Land)	MuddyWater, OilRig, Multiple	YES — Behavioral	NodeZero uses native OS tools in attack chains; identifies misconfigurations enabling LOLBins abuse
Azure Cloud Credential/Config Abuse	APT33	YES — Cloud Module	NodeZero Cloud Pentesting tests Azure environments for misconfiguration and credential exposure

Iranian APT Technique / CVE	APT Group(s)	NodeZero Coverage	Notes
RMM Tool Abuse (ScreenConnect, Atera, N-able)	MuddyWater	PARTIAL	NodeZero detects unauthorized RMM software presence; abuse scenario simulation requires custom pentest configuration
DNS Tunneling C2	OilRig/APT34	DETECTION SCOPE	NodeZero identifies DNS tunneling-enabling configurations; full C2 simulation requires network-specific setup
ICS/OT PLC/HMI Exploitation (Unitronics)	CyberAv3ngers	OUT OF SCOPE	Unitronics PLC exploitation is outside NodeZero's current scope. Recommend Dragos, Claroty, or Nozomi for OT testing. NodeZero can verify IT-OT network segmentation.

Coverage Summary by Category

Category	Coverage	Recommended NodeZero Action
VPN/Edge Device CVE Exploitation	HIGH (70–80%)	Run external pentests targeting your VPN/firewall perimeter stack
Active Directory / Credential Attacks	VERY HIGH (90%+)	Run internal pentests + AD Password Audit — NodeZero's strongest domain
Windows Platform CVEs	HIGH (75%+)	Include Windows workstations and DCs in internal pentest scope
Web Application TTPs	HIGH (80%+)	NodeZero Web App Pentesting covers OWASP Top 10 (XSS, SQLi, BAC, SSRF, XXE)
Cloud Infrastructure (Azure)	MEDIUM (60%)	Enable NodeZero Cloud Pentesting with Azure subscription access
ICS/OT Device Exploitation	LOW — Out of Scope	Use OT-specific tools; use NodeZero to verify IT/OT network segmentation controls

Social Engineering / Phishing	NOT IN SCOPE	Supplement with Proofpoint TAP, KnowBe4, or similar phishing simulation platforms

Recommendations for Defenders

Prioritized recommendations based on Iranian APT TTP analysis and NodeZero coverage mapping.

Immediate Actions (0–30 Days)

- Patch all CISA KEV vulnerabilities, especially Fortinet, Citrix, Ivanti, F5, and Palo Alto CVEs. Iranian APTs weaponize these within days of disclosure.
- Change all default credentials on internet-facing devices — Unitronics PLCs, MikroTik routers, IP cameras, and SOHO network gear.
- Enable MFA on all VPN and remote access portals — APT33 and CyberAv3ngers use password spray specifically targeting VPN portals without MFA.
- Disable PowerShell for users who don't need it; enable Script Block Logging — MuddyWater and OilRig heavily rely on PowerShell-based implants.
- Audit RMM tool deployments — MuddyWater abuses Atera, ScreenConnect, N-able. Remove unauthorized or shadow RMM installations immediately.

Short-Term Actions (30–90 Days)

- Run NodeZero external pentests targeting your VPN/firewall perimeter — Fox Kitten and MuddyWater treat unpatched edge devices as open doors.
- Run NodeZero AD Password Audit — Iranian APTs use password spraying and credential dumping as a core lateral movement technique.
- Implement and test IT/OT network segmentation — verify OT devices are not reachable from enterprise networks using NodeZero's internal pentest.
- Deploy DNS monitoring and filtering — OilRig/APT34 uses DNS C2 tunneling extensively; alert on unusual DNS query patterns.
- Audit Microsoft Exchange and M365 configurations — OilRig deploys web shells via Exchange and abuses M365 for credential operations.

Strategic Recommendations

- Subscribe to Iranian-specific threat intelligence feeds — CISA alerts, Microsoft MSTIC, Mandiant Advantage, CrowdStrike Falcon Intelligence.
- Conduct tabletop exercises for Iranian APT intrusion scenarios — particularly for defense, energy, water, and healthcare sector organizations.
- For OT environments, deploy dedicated OT monitoring (Dragos, Claroty, Nozomi) and enforce strict network segmentation verifiable through NodeZero.
- Monitor for Fox Kitten access brokering — Fox Kitten sells network access on dark web forums. Threat intelligence subscriptions can identify whether your organization has been listed.

Sources & References

All sources publicly available as of March 2026. Click links for direct access.

Government & CISA Advisories

- CISA AA23-335A — IRGC-CEC Exploitation of PLCs in US Water and Wastewater Systems (Updated Dec 2024)
- CISA AA24-241A — Iran-Based Cyber Actors Enabling Ransomware Attacks on US Organizations (Aug 2024)
- CISA Alert — Exploitation of Unitronics PLCs Used in Water and Wastewater Systems (Nov 2023)

Microsoft Threat Intelligence

- Microsoft On the Issues — Iran Accelerates Cyber Ops Against Israel from Chaotic Start (Feb 2024)
- Microsoft Security Insider — Iran Amplifies Cyber Support for Hamas — APT42 and Influence Operations

Google / Mandiant

- Google Cloud GTIC — Uncharmed: Untangling Iran's APT42 Operations (2024)

Palo Alto Unit 42

- Unit 42 — Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran
- Unit 42 — Threat Brief: Escalation of Cyber Risk Related to Iran (Updated June 2025)

Threat Research

- SOCRadar — Dark Web Profile: OilRig (APT34)
- Picus Security — Iranian Threat Actors: What Defenders Need to Know
- Picus Security — Inside the Shadows: Understanding Active Iranian APT Groups
- Picus Security — Pioneer Kitten — CISA Alert AA24-241A Analysis
- Check Point Research — What Defenders Need to Know About Iran's Cyber Capabilities
- The Hacker News — OilRig Exploits Windows Kernel Flaw in Espionage Campaign Targeting UAE and Gulf
- SC Media — High-Severity Windows Vulnerability Leveraged in New OilRig APT Attacks
- Dark Reading — Iran's Fox Kitten Group Aids Ransomware Attacks on US Targets
- Dark Reading — Iranian APT Targets IP Cameras, Extends Attacks Beyond Israel
- Rescana — Iran's Cyberwar Has Begun: Targeted Attacks on Israeli and Unitronics ICS/OT Systems (2026)
- CSIS — Beyond Hacktivism: Iran's Coordinated Cyber Threat Landscape
- Nozomi Networks — Iranian APT Activity During Geopolitical Escalation

- PolySwarm — Cyber Strategy Under Fire: Iranian APT and Proxy Retaliation Risks
- Cyble — Middle East Conflict: Iran-US-Israel Cyber-Kinetic Crisis
- BeyondTrust — Threat Advisory: Operation Epic Fury — Iran-Aligned Cyber Actors
- Tenable — Operation Epic Fury: Potential Iranian Cyber Counteroffensive Operations

MITRE ATT&CK Group Profiles

- MITRE ATT&CK — OilRig (G0049)
- MITRE ATT&CK — MuddyWater (G0069)
- MITRE ATT&CK — APT33 (G0064)
- MITRE ATT&CK — APT35 (G0059)
- MITRE ATT&CK — APT42 (G0158)
- MITRE ATT&CK — Fox Kitten (G0117)

Horizon3.ai

- Horizon3.ai — NodeZero Platform Overview
- Horizon3.ai — NodeZero Rapid Response Center — N-Day CVE Coverage
- Horizon3.ai — NodeZero First AI to Fully Solve Game of Active Directory (GOAD)