

Iran's Cyber Paradox: Degraded APTs, Empowered Proxies, and the Rise of Bootkit Wipers

 anomali.com/blog/irans-cyber-paradox-degraded-apt-empowered-proxies-and-the-rise-of-bootkit-wipers

Anomali Threat Research

May 29, 2026



Threat Assessment Level: HIGH

Maintained from prior cycle. While no single event triggered escalation to CRITICAL, the convergence of confirmed kinetic strikes on cloud infrastructure, novel bootkit-wiper capabilities from unattributed Iran-nexus actors, and active ICS/OT exploitation of Rockwell PLCs collectively sustains HIGH threat posture for defense, critical infrastructure, and government sectors.

Introduction

Ninety days into the Iran conflict that began on 28 February 2026, the cyber battlefield is defying conventional expectations. Rather than a sustained surge from Iran's well-known APT groups — many of which are degraded by regime-imposed internet restrictions — we are witnessing something potentially more dangerous: **the transfer of advanced destructive capabilities to proxy actors operating outside Iran's borders with less oversight and more aggressive mandates.**

This week's intelligence confirms three developments that demand immediate executive attention:

- 1. **Bootkit-style wipers** — a capability previously exclusive to Russian state actors — have appeared in the hands of unattributed Iran-nexus groups
- 2. **Iran has physically struck cloud data centers** in the Gulf, validating the kinetic-cyber hybrid threat model
- 3. **HYDRO KITTEN (Cyber Av3ngers)** has expanded its exploitation arsenal to seven additional CVEs while actively compromising Rockwell Allen-Bradley PLCs

If your organization operates ICS/OT systems, hosts workloads in Gulf-region cloud availability zones, or sits in the defense industrial base supply chain, this report requires your immediate attention.

What Changed

Development	Significance
ESET confirms two new unattributed destructive clusters (Rusty Boots, MoKhargosh) with bootkit-wiper capability	First documented bootkit-level persistence in Iranian-nexus operations — attacks can survive OS reinstallation
Amazon cloud facility in Bahrain confirmed struck kinetically by Iran; Oracle/Dubai strike alleged	Physical destruction of cloud infrastructure hosting government/military workloads — a new threat category
HYDRO KITTEN CVE arsenal expanded to include CVE-2024-47575, CVE-2024-55591, CVE-2024-53704, CVE-2025-0282, CVE-2024-0012, CVE-2024-9474, CVE-2024-6387	IRGC-CEC unit actively exploiting network edge devices (PAN-OS, Ivanti, FortiGate, SonicWall, OpenSSH)
UNC6446 deploys DUSTYPROXY + ERIESNAKE.GO against Turkey and Saudi Arabia	New Iran-nexus espionage tooling with cross-platform (Golang) capability targeting Middle East defense entities

Development	Significance
Nimbus Manticore/UNC1549 conducts three MiniFast backdoor waves against US aviation (February–April 2026)	Sustained Iran-nexus espionage campaign against aviation sector using AI-assisted SEO poisoning
Fox Kitten/Pioneer Kitten enters 69-day operational silence during active conflict	Prolonged silence consistent with pre-positioned access awaiting activation — high-risk pre-positioning indicator
CISA alerts on Nx Console / GitHub supply chain compromise	CI/CD pipeline attacks intensifying; technique transferable to Iran-nexus actors with demonstrated supply chain capability
UAE defense company compromised via SmartOffice CRM	Defense industrial base supply chain exploitation via customer-facing applications

Conflict & Threat Timeline

Date	Event	Category
28 Feb 2026	Operation Epic Fury initiated; Iran conflict begins	Kinetic/Cyber
Feb–Apr 2026	Nimbus Manticore/UNC1549 conducts three MiniFast backdoor waves against US aviation	Espionage
Late Feb 2026	HYDRO KITTEN exploits CVE-2021-22681 against Rockwell Allen-Bradley PLCs	ICS/OT Destruction

Date	Event	Category
Mar 2026	Fox Kitten/Pioneer Kitten goes operationally silent (69+ days) — assessed pre-positioned	Pre-positioning
13 May 2026	Iran kinetically strikes Amazon cloud facility in Bahrain; claims Oracle/Dubai strike	Kinetic-Cyber Hybrid
25 May 2026	HYDRO KITTEN destroys food production facility compressors via PLC setpoint manipulation — no malware used	ICS/OT Destruction
27 May 2026	UNC5858/Black Shadow IOC activity confirmed in Rafael defense impersonation campaign	Espionage
28 May 2026	CISA issues supply chain alert for Nx Console / GitHub repository compromises	Supply Chain
29 May 2026	ESET publishes Q4'25–Q1'26 APT report confirming Rusty Boots/MoKhargosh bootkit-wipers; UNC6446 DUSTYPROXY/ERIESNAKE.GO bulletin updated	Destructive/Espionage

Key Threat Analysis

1. The Proxy Paradox: Rusty Boots & MoKhargosh

ESET's Q4 2025–Q1 2026 APT Activity Report reveals a counterintuitive dynamic: Iran's internet restrictions, imposed to control domestic dissent, have **degraded established APT groups** (APT33, APT42, MuddyWater) while simultaneously creating operational space for **less-controlled proxy actors** operating from outside Iran.

Two newly identified clusters — **Rusty Boots** and **MoKhargosh** — possess both espionage and destructive capabilities. Most alarming: Rusty Boots employs a **bootkit-style wiper**

(ATT&CK T1542.003), a technique previously associated exclusively with Russian GRU operations (Sandworm). This means:

- Destructive payloads can **survive OS reinstallation and disk formatting**
- Standard incident response procedures (reimage and restore) are insufficient
- Firmware-level integrity monitoring becomes a defensive requirement

These actors remain **unattributed** — suspected IRGC proxy but not confirmed. The attribution gap means we cannot predict their targeting with the same confidence as named groups.

2. HYDRO KITTEN: ICS/OT Destruction at Scale

HYDRO KITTEN (Cyber Av3ngers), the IRGC Cyber-Electronic Command's (IRGC-CEC) Shahid Kaveh sub-unit, continues to represent the most immediate destructive threat to critical infrastructure. Key updates:

- **Confirmed exploitation of CVE-2021-22681** (Rockwell RSLogix 5000 authentication bypass) targeting Allen-Bradley PLCs
- **25 May 2026** : Destroyed compressors at a food production facility using only valid credentials — **no malware deployed** , making detection extremely difficult
- **Expanded CVE arsenal** : CVE-2024-47575 (FortiManager), CVE-2024-55591 (FortiOS), CVE-2024-53704 (SonicWall), CVE-2025-0282 (Ivanti), CVE-2024-0012/CVE-2024-9474 (PAN-OS), CVE-2024-6387 (OpenSSH)
- **Wiper sharing confirmed** with IMPERIAL KITTEN — indicating operational coordination across IRGC units
- Custom malware: **IOControl** backdoor, **Crucio** ransomware, C++/Golang wipers

The "living off the land" approach (valid credentials, no malware) used in the May 25 attack represents a detection nightmare for traditional security tools.

3. UNC6446: Custom Espionage Tooling Against Middle East Defense

Iran-nexus cluster UNC6446 has deployed a sophisticated custom toolkit against defense and government entities in Turkey and Saudi Arabia:

- **DUSTYPROXY** — C# proxy client using ConfuserEx obfuscation, persists via Registry Run key (T1547.001)
- **ERIESNAKE.GO** — Golang backdoor with shell/PowerShell execution, file transfer, REST API C2 over **unencrypted HTTP on port 443** (a highly anomalous and detectable behavior)

- **NEATSNAKE** — Host data exfiltration backdoor

The use of Golang indicates cross-platform ambitions, and the unencrypted-HTTP-over-443 technique is both a detection opportunity and an indicator of operational confidence.

4. Kinetic-Cyber Convergence: Cloud as a Kinetic Target

The confirmed Iranian strike on Amazon's cloud facility in Bahrain (13 May 2026) fundamentally changes the threat model for any organization hosting workloads in Gulf-region availability zones. This is not a cyber attack — it is **physical destruction of digital infrastructure** as an act of war.

Implications:

- Cloud disaster recovery plans must now account for **kinetic destruction** of entire availability zones
- Multi-region architectures with Gulf-only redundancy are insufficient
- Military and government workloads in AWS Bahrain, Oracle Dubai, or Azure UAE face existential risk

5. Supply Chain Pressure: Three Vectors Simultaneously

Three independent supply chain compromise campaigns are active:

- **Nx Console / GitHub Actions** (CISA alert, 28 May 2026)
- **axios npm library** (Lazarus/DangerousPassword — 100M+ weekly downloads)
- **SmartOffice CRM** (UAE defense company compromise)

While not all Iran-attributed, the technique is within demonstrated Iranian capability. Defense software development pipelines face unprecedented pressure from multiple simultaneous supply chain vectors.

Predictive Analysis

Scenario	Probability	Timeframe	Basis
Ivanti EPMM CVE-2026-5786/5787/5788/7821 exploitation in the wild	60%	7 days	Pioneer Kitten/Fox Kitten historical pattern of rapid Ivanti exploitation; 69 days of operational silence suggests pre-positioned access awaiting new vectors
Additional supply chain compromise indicators from CISA Nx Console investigation	70%	7 days	Investigation ongoing; scope likely broader than initial disclosure
Rusty Boots or MoKhargosh attributed to known IRGC unit	50%	30 days	ESET typically releases IOCs in follow-up publications
Retaliatory cyber operations surface publicly post-May 13 kinetic strikes	40%	14 days	Historical pattern of cyber retaliation following kinetic escalation; absence may indicate unreported operations
Fox Kitten/Pioneer Kitten breaks 69-day silence with destructive or access-brokering operation	55%	21 days	Prolonged silence during active conflict is consistent with pre-positioned access awaiting activation signal
HYDRO KITTEN conducts additional ICS/OT destructive attack using credential-only (no malware) technique	65%	14 days	Technique proven successful on May 25; likely to be repeated

SOC Operational Guidance

Detection Priorities

Priority 1 — UNC6446 DUSTYPROXY/ERIESNAKE.GO (Active Espionage)

ATT&CK ID	Detection Logic
T1071.001	Hunt for HTTP traffic on TCP/443 that is NOT TLS-encrypted. ERIESNAKE.GO uses unencrypted HTTP REST API over port 443 — this is highly anomalous and should trigger immediate investigation
T1547.001	Monitor Registry Run key additions for unknown executables (DUSTYPROXY persistence)
T1059.001	Alert on PowerShell execution spawned by processes named winlog.exe, Pro.exe, prvservice.exe, csvserv.exe, ProxyAgent.exe, Svshost.exe, slick.exe
T1090.002	Detect proxy-relay behavior from endpoints — DUSTYPROXY acts as an external proxy client

Hunting Hypothesis: "If UNC6446 has compromised our environment, we will observe DNS queries to clothingshop[.]live, cmdhubs[.]uk, or codeteamhub[.]com, OR we will see unencrypted HTTP traffic on port 443 to IPs 91.222.173[.]6, 212.232.22[.]104, 104.238.248[.]35, 94.158.244[.]206, or 216.73.157[.]70."

Priority 2 — HYDRO KITTEN ICS/OT (Active Destruction)

ATT&CK ID	Detection Logic
T1078	Monitor for anomalous authentication to Rockwell RSLogix 5000 / Allen-Bradley PLCs — especially outside maintenance windows

ATT&CK ID	Detection Logic
T1190	Alert on exploitation attempts against CVE-2021-22681 (Rockwell auth bypass), CVE-2024-0012/CVE-2024-9474 (PAN-OS), CVE-2025-0282 (Ivanti)
T1485/T1499	Monitor PLC setpoint changes — HYDRO KITTEN's May 25 attack used only valid credentials to manipulate compressor setpoints with no malware

Hunting Hypothesis: "If HYDRO KITTEN has pre-positioned in our OT environment, we will observe PLC configuration changes outside scheduled maintenance windows, OR authentication to RSLogix 5000 from non-engineering workstations."

Priority 3 — Bootkit/Wiper Detection (Emerging Threat)

ATT&CK ID	Detection Logic
T1542.003	Enable Secure Boot verification monitoring; deploy firmware integrity checks (e.g., CHIPSEC, fwupd) on critical systems
T1485	Monitor for MBR/VBR modifications; alert on raw disk write operations from userland processes

Hunting Hypothesis: "If Rusty Boots has pre-positioned bootkit-wipers in our environment, we will observe Secure Boot policy violations, unexpected firmware updates, or raw disk sector writes outside of legitimate disk management tools."

IOC Blocking Table

Deploy the following indicators to DNS sinkholes, proxy block lists, and network detection:

Type	Value	Context
Domain	clothingshop[.]live	ERIESNAKE.GO C2

Type	Value	Context
Domain	cmdhubs[.]uk	DUSTYPROXY C2
Domain	codeteamhub[.]com	DUSTYPROXY C2
URL	http://clothingshop[.]live:443/webapi/	ERIESNAKE.GO C2 endpoint
URL	http://clothingshop[.]live:443/medias/fileman/	ERIESNAKE.GO C2 endpoint
URL	http://clothingshop[.]live:443/webapi/api/	ERIESNAKE.GO C2 endpoint
URL	http://clothingshop[.]live:443/webapi/fpi/	ERIESNAKE.GO C2 endpoint
URL	http://swimmingsport2022[.]info	ERIESNAKE.GO C2
IP	91.222.173[.]6	UNC6446 C2 infrastructure
IP	212.232.22[.]104	UNC6446 C2 infrastructure
IP	104.238.248[.]35	UNC6446 C2 infrastructure
IP	94.158.244[.]206	UNC6446 C2 infrastructure
IP	216.73.157[.]70	UNC6446 C2 infrastructure
MD5	4b4cb57bc4aa1ba60cf67a065ba55151	NEATSNAKE (Neon.exe)
MD5	eed66fe72a8a8c2ea98209cd09a35b90	ERIESNAKE.GO (Pro.exe)
MD5	e275b96af7936f0c61b254bc9eed954a	ERIESNAKE.GO (winlog.exe)

Type	Value	Context
MD5	c8f168efa270f6ffbd899d9e1689c4fc	DUSTYPROXY (prvservice.exe)
MD5	06cb6f3bcf64b5c571aab4b89db5b84f	DUSTYPROXY (csvserv.exe)
MD5	d9570591f514594fd2262d53110edc0c	DUSTYPROXY (ProxyAgent.exe)
MD5	91acab55a3f04af3d105cc0053ba3f7a	DUSTYPROXY (Svshost.exe)
MD5	fc83a07c272ea3033cc23803ef37a98f	DUSTYPROXY (Svshost.exe)
MD5	f1a24a156ed792cfd21e3361d9fcd045	DUSTYPROXY (slick.exe)

Note: Six SHA-256 hashes originally included in this report were removed prior to publication after failing IOC integrity validation (incorrect hash length — 63 characters instead of the required 64). Additional verified file hashes for campaigns discussed in this report, including Rusty Boots, MoKhargosh, and HYDRO KITTEN tooling, are available through Anomali ThreatStream Next-Gen and partner feeds.

Sector-Specific Defensive Priorities

Financial Services

- **Primary threat:** HYDRO KITTEN's expanded CVE arsenal (CVE-2024-0012/CVE-2024-9474 PAN-OS, CVE-2024-55591 FortiOS) targets the same network edge devices protecting financial networks
- **Action:** Verify PAN-OS and FortiGate firmware is patched against all listed CVEs; implement network segmentation between internet-facing firewalls and core banking systems
- **Supply chain risk:** Audit third-party fintech integrations for SmartOffice CRM or similar customer-facing application vulnerabilities
- **Cloud risk:** If using Gulf-region availability zones for disaster recovery, develop failover procedures to non-Gulf regions

Energy

- **Primary threat:** HYDRO KITTEN is actively exploiting Rockwell Allen-Bradley PLCs (CVE-2021-22681) and has demonstrated ability to destroy physical equipment via PLC setpoint manipulation without deploying malware
- **Action:** Immediately audit all Rockwell RSLogix 5000 versions 20–38; enforce CIP Security authentication; implement PLC configuration change monitoring with alerting outside maintenance windows
- **Detection gap:** The May 25 attack used only valid credentials — traditional malware detection is blind to this technique. Behavioral monitoring of PLC setpoint changes is the only reliable detection
- **Wiper risk:** HYDRO KITTEN possesses C++/Golang wipers AND Crucio ransomware; energy sector OT networks are primary targets

Healthcare

- **Primary threat:** Supply chain compromise via CI/CD pipelines (Nx Console, GitHub Actions) affecting medical device software and health IT systems
- **Action:** Audit all GitHub Actions workflows for version-tag references (convert to pinned commit SHAs); review VS Code extensions installed on developer workstations
- **ICS/OT crossover:** Hospital building management systems (HVAC, power) using Rockwell or Schneider PLCs face the same HYDRO KITTEN threat as industrial facilities
- **Bootkit risk:** Medical imaging systems and other specialized hardware with limited firmware update capabilities are vulnerable to bootkit-wiper attacks that survive reimaging

Government

- **Primary threat:** Multi-vector espionage from UNC6446 (DUSTYPROXY/ERIESNAKE.GO targeting Turkey/Saudi government), APT42/Charming Kitten (credential harvesting), and Rusty Boots/MoKhargosh (espionage + destructive)
- **Action:** Deploy all IOCs from this report to government network monitoring; hunt for unencrypted HTTP on port 443; brief personnel on Iranian social engineering campaigns impersonating defense contractors (UNC5858/Black Shadow Rafael impersonation)
- **Cloud sovereignty:** Government workloads in AWS Bahrain or Azure UAE face kinetic destruction risk — accelerate migration to sovereign or geographically diversified cloud architectures
- **Pre-positioning concern:** Fox Kitten/Pioneer Kitten's 69-day operational silence during active conflict strongly suggests pre-positioned access in government networks awaiting activation

Aviation & Logistics

- **Primary threat:** Nimbus Manticore/UNC1549 conducted three waves of MiniFast backdoor attacks against US aviation (February–April 2026) using AI-assisted SEO poisoning
- **Action:** Hunt for MiniFast backdoor indicators in aviation IT/OT environments; review web browsing logs for SEO poisoning redirects to malicious aviation-themed content
- **Supply chain:** Aviation software development pipelines face the same Nx Console/GitHub Actions supply chain risk; audit avionics software build systems
- **Logistics disruption:** Iran's kinetic strikes on Gulf infrastructure could disrupt logistics networks dependent on Gulf-region cloud services or communications infrastructure

Prioritized Defense Recommendations

IMMEDIATE (Within 24 Hours)

Team	Action
SOC	Block all UNC6446 IOCs (domains, IPs, hashes) listed in the IOC table above at DNS, proxy, and endpoint levels
SOC	Create detection rule for unencrypted HTTP traffic on TCP/443 — this is ERIESNAKE.GO's primary C2 signature and is highly anomalous in any environment
IT Ops / OT	Verify Rockwell Allen-Bradley PLC firmware and confirm CVE-2021-22681 mitigations (authentication enforcement) are applied on all RSLogix 5000 versions 20–38
SOC / OT	Implement emergency monitoring for PLC setpoint changes outside scheduled maintenance windows — HYDRO KITTEN's latest technique uses no malware
IT Ops	Confirm PAN-OS patched against CVE-2024-0012 and CVE-2024-9474; confirm Ivanti patched against CVE-2025-0282

7-DAY

Team	Action
DevOps	Pin ALL GitHub Actions to commit SHAs (not version tags); audit VS Code extensions for Nx Console or unknown publishers; review npm dependency trees for axios version anomalies
IT Ops / Cloud	Assess workload exposure in Gulf-region data centers (AWS Bahrain, Oracle Dubai, Azure UAE); develop contingency playbook for kinetic disruption of Gulf availability zones
SOC	Deploy bootkit detection: enable Secure Boot verification monitoring, implement firmware integrity checks (CHIPSEC or equivalent) on critical servers and workstations
IT Ops	Patch FortiGate (CVE-2024-55591), SonicWall (CVE-2024-53704), and OpenSSH (CVE-2024-6387) across all internet-facing assets — these are confirmed in HYDRO KITTEN's exploitation arsenal
SOC	Conduct threat hunt for Fox Kitten/Pioneer Kitten persistence indicators — 69 days of silence during active conflict is consistent with pre-positioned access

30-DAY

Team	Action
CISO	Commission assessment of all customer-facing CRM and web applications in the defense supply chain for exploitation potential (SmartOffice CRM vector)
CISO	Develop kinetic-cyber hybrid incident response playbook covering physical destruction of cloud infrastructure; include failover procedures, data sovereignty requirements, and communication plans

Team	Action
CISO	Evaluate firmware integrity monitoring solutions for deployment across critical infrastructure — bootkit-wiper capability from Rusty Boots requires detection below the OS layer
IR Team	Update incident response procedures to account for bootkit-level persistence — standard "reimage and restore" is insufficient against T1542.003 attacks
Executive	Brief board/leadership on kinetic-cyber convergence risk: Iran has demonstrated willingness to physically destroy cloud infrastructure as an act of war; this requires business continuity planning beyond traditional cyber scenarios

Bottom Line

Three findings from this reporting cycle demand board-level attention:

1. **Bootkit-wiper capability is now in Iranian-nexus hands.** Rusty Boots and MoKhargosh possess nation-state-grade destructive tools without nation-state attribution constraints. Standard incident response — reimage and restore — will not work against T1542.003 attacks. Firmware integrity monitoring is no longer optional for critical infrastructure operators.
2. **Iran has crossed the kinetic-cyber threshold.** The 13 May 2026 strike on Amazon's Bahrain facility is not a cyber event — it is physical warfare against digital infrastructure. Business continuity plans that assume cloud availability zones are immune to kinetic attack are now dangerously outdated.
3. **HYDRO KITTEN has proven it can destroy physical equipment without leaving a single malware artifact.** The May 25 food production facility attack used only valid credentials. Your EDR will not see it. Your SIEM will not alert on it. Only behavioral monitoring of PLC setpoint changes will catch it.

The most dangerous threat in this report is not what we can attribute — it is what we cannot yet see. Fox Kitten's 69-day silence during an active conflict is not inactivity; it is preparation. Act accordingly.

Closing

The Iran conflict has entered its fourth month, and the cyber dimension is evolving faster than defensive postures are adapting. The three developments in this report — bootkit wipers from unattributed proxies, kinetic destruction of cloud infrastructure, and credential-only ICS attacks — each individually warrant urgent action. Together, they represent a fundamental shift in the threat model.

The most dangerous finding is not what we see, but what we cannot yet attribute. Rusty Boots and MoKhargosh possess nation-state destructive capabilities without nation-state attribution constraints. Fox Kitten's 69-day silence screams pre-positioning. And HYDRO KITTEN has proven it can destroy physical equipment without leaving a single malware artifact for your EDR to detect.

Your firewalls are patched. Your endpoints are monitored. But is anyone watching your PLC setpoints? Your firmware integrity? Your Gulf-hosted cloud failover?

Act now. The next 14 days will determine whether your organization is prepared for what comes next.

Published 2026-05-29 by the Anomali CTI Desk. For questions, IOC feeds, or tailored briefings, contact your Anomali account team.