BLACKSWAN CYBERSECURITY

THREAT INTELLIGENCE REPORT

Top Attributable Cyber Threats

March 6, 2026

Executive Summary

As of March 2026, the cyber threat landscape is dominated by heightened activity from Iranian-affiliated actors following the February 28, 2026 U.S./Israel-Iran escalation, with coordinated hacktivist campaigns, destructive wipers, and espionage targeting critical infrastructure and regional adversaries. Ransomware operations continue to evolve, with new groups emphasizing double extortion, cross-platform attacks, and identity-based access. Pro-Russian hacktivists like NoName057(16) remain active with DDoS campaigns. These threats feature attributable IOCs and well-documented TTPs aligned with MITRE ATT&CK, enabling proactive detection and mitigation.

Iranian-Affiliated State-Sponsored Actors

Iran-linked actors, including IRGC-affiliated groups, have escalated operations post-escalation, focusing on disruption, espionage, and wipers against Israel, Gulf states, and U.S. allies.

Key Groups and TTPs:

- **OilRig/APT34, Mint Sandstorm, Fox Kitten/Pioneer Kitten**: Exploit vulnerabilities in VPN gateways/firewalls (e.g., Pulse Secure, Fortinet, Palo Alto, F5, Citrix); use legitimate RMM tools (Atera, AnyDesk, ScreenConnect) for persistence and evasion; deploy destructive wipers; exfiltrate via Telegram; target energy/utilities/SCADA.
- **CyberAv3ngers (IRGC-linked)**: Exploit default credentials in ICS/SCADA (e.g., Unitronics PLCs); deface devices; alter configurations for disruption.

Attributable IOCs:

- **Exploited CVEs**: CVE-2024-30088 (Windows Kernel), CVE-2022-47966 (Zoho ManageEngine), CVE-2022-42475 (Fortinet FortiOS), CVE-2021-34473 (Exchange), CVE-2020-5902 (F5 BIG-IP), CVE-2019-19781 (Citrix ADC), CVE-2025-1960 (Schneider Electric).
- No specific hashes/IPs detailed in recent reports, but teams should monitor for Telegram C2 and RMM misuse.

Targets: Energy, utilities, defense, transportation, government, ICS/SCADA in Israel, Jordan, Saudi Arabia, UAE, Bahrain, Kuwait.

BLACKSWAN CYBERSECURITY

THREAT INTELLIGENCE REPORT

Top Attributable Cyber Threats

March 6, 2026

Pro-Iran Hacktivist Collectives

A surge of ~60 hacktivist groups (some pro-Russian opportunists) coordinate via an "Electronic Operations Room" for low-to-medium sophistication attacks.

Key Groups and TTPs:

- **Handala Hack** (MOIS-linked): Data exfiltration, hack-and-leak; phishing via malicious Android APKs (e.g., mimicking RedAlert app).
- **Cyber Islamic Resistance** (umbrella incl. RipperSec, Cyb3rDrag0nzz): DDoS, data-wiping, defacements; target drone/payment systems.
- **FAD Team/Fatimiyoun**: Wiper malware; unauthorized SCADA/PLC access.
- **Evil Markhors, Dark Storm Team, DieNet, 313 Team**: Credential harvesting, DDoS, ransomware with ideological symbols.

Attributable IOCs:

- **Malicious APK**: hash 83651b0589665b112687f0858bfe2832ca317ba75e700c91ac34025ee6578b72;
- **URLs**: hxxps://www.shirideitch.com/wp-content/uploads/2022/06/RedAlert.apk; hxxps://api.ra-backup.com/analytics/submit.php; hxxps://bit.ly/4tWJhQh.

Targets: Israel (defense, energy, healthcare, banks), Jordan, Saudi Arabia, UAE, Kuwait, Turkey.

Ransomware Operators

Ransomware attacks rose 47% in 2025, with declining payments driving new TTPs: DDoS bundling, insider recruitment, gig worker exploitation, and exfil-first extortion.

Notable Active Groups (2025-2026):

- **Sinobi** (Lynx ecosystem rebrand): 138 victims; credential-based access (VPN compromise), defense evasion, staged extortion; targets manufacturing/mid-large businesses.
- **NightSpire**: 92 victims; exfil-first to double extortion; multi-sector (healthcare, education, government).

BLACKSWAN CYBERSECURITY

THREAT INTELLIGENCE REPORT

Top Attributable Cyber Threats

March 6, 2026

- **Warlock**: 66 victims; exploits on-premises SharePoint; rapid ransomware delivery.
- **The Gentlemen**: 63 victims; legitimate tooling, Group Policy manipulation; targets manufacturing, healthcare, critical industries.
- Others: Devman, DireWolf, RALord/NOVA, Global, BEAST, Chaos (DDoS bundling).

Attributable IOCs (examples):

- **Sinobi**: extension .SINOBI; note README.txt; Curve-25519 + AES-128-CTR crypto.
- **Warlock**: webshell spinstall0.aspx (variants); C2 IP 65.38.121.198; ngrok domains; exploited CVEs 2025-49704/49706/53770/53771.
- **DireWolf**: hashes e.g., 27d90611f005db3a25a4211cf8f69fb46097c6c374905d7207b30e87d296e1b3; domain tor-browser.io.
- **General**: Extensions like: .DEVMAN, .RALord, .LoveYou; mutexes e.g., Global\Fxo16jmdgujs437, BEAST HERE?.

Targets: Global, heavy in the U.S., Asia, Europe; cross-platform (Windows/Linux/ESXi).

Pro-Russian Hacktivists

NoName057(16): Persistent DDoS via DDoSia project; claimed 49 attacks in late Feb-early March 2026; targeted Winter Olympics sites, Italian infrastructure.

TTPs: Large-scale DDoS; opportunistic alignment with pro-Iran efforts.

IOCs: Limited public details; monitor for DDoSia botnet indicators.

Targets: Western nations, events (e.g., Milan-Cortina Olympics).

Recommendations

Prioritize patching (e.g., VPN/ICS vulnerabilities), MFA, segmentation of critical systems, monitoring for RMM/Telegram abuse, and threat hunting for listed IOCs. Leverage MITRE ATT&CK for TTP mapping.

References and Bibliography

BLACKSWAN CYBERSECURITY

THREAT INTELLIGENCE REPORT

Top Attributable Cyber Threats

March 6, 2026

1. Unit 42 Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran. Palo Alto Networks. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/.
2. Heightened Cyber Risk Following February 2026 U.S./Israel–Iran Escalation. Arctic Wolf. https://arcticwolf.com/resources/blog/heightened-cyber-risk-following-february-2026-us-israel-iran-escalation.
3. 10 New Ransomware Groups Of 2025 & Threat Trends For 2026. Cyble. https://cyble.com/knowledge-hub/10-new-ransomware-groups-of-2025-threat-trend-2026.
4. New ransomware tactics to watch out for in 2026. Recorded Future. https://www.recordedfuture.com/blog/ransomware-tactics-2026.
5. CISA Issues Updated RESURGE Malware Analysis. CISA. https://www.cisa.gov/news-events/news/cisa-issues-updated-resurge-malware-analysis-highlighting-stealthy-active-threat.