Green Cyber Consulting

GREEN CYBER CONSULTING | FLASH UPDATE

Iranian Cyber Threat Surge Executive Brief (2 March 2026)

What's changing, who's at risk, and what we're doing next

March 2026 | Prepared by: Green Cyber Coonsulting

Executive Summary

Three facts your leadership team needs to absorb in Thirty Seconds.

Identity-Led Intrusions

Heightened likelihood of credential-abuse campaigns, password spraying and targeted phishing against privileged accounts across government and enterprise environments.

Critical Infrastructure at Risk

Elevated concern for operational technology (OT) and industrial control system (ICS) disruption scenarios, including energy, water and transport sectors.

72-Hour Hardening Sprint

We are executing an immediate hardening sprint paired with targeted threat hunts aligned to published government advisories and known Iranian TTPs.

Briefing context: Multiple allied agencies have issued credible warnings. The risk is manageable with rapid, prioritised controls. Our posture is proactive, not reactive, this brief exists to align leadership behind swift, measured action.

What Government Partners Are Warning About

Allied intelligence and cyber-security agencies across the Five Eyes have converged on a consistent set of threat indicators, tactics, techniques and procedures (TTPs), and recommended mitigations. The alignment across jurisdictions reinforces credibility and urgency.

Key Messages

Increased vigilance

Iran-linked cyber activity is trending upward, correlated with geopolitical escalation in the Middle East and retaliatory posturing.

Critical infrastructure targeting

Energy, water, transport and telecommunications sectors are explicitly cited as priority targets by state-affiliated groups.

Credential abuse dominant

Brute force and password-spraying campaigns remain the primary initial-access vector, often targeting legacy authentication protocols.

OT/ICS environments at risk

Advisories explicitly warn of attempts to traverse from IT networks into operational technology environments where safety consequences are highest.

Sources

- **CISA / NSA / FBI / DC3:** Joint fact sheet and advisories on Iranian cyber actors
- **ACSC (Australia):** Joint advisory on credential access and brute-force techniques
- **UK NCSC:** Phishing warning and sector-specific guidance

All sources are public government advisories and major vendor reporting. Full reference list available in appendix.

Briefing context: The significance here is convergence; when CISA, ACSC and NCSC all point to the same TTPs and mitigations within the same window, the signal is strong. This is not speculative; it is intelligence-led guidance from our closest allies.

Threat Model: What We Expect to See

Iranian cyber operations historically span three distinct lanes. Understanding these lanes helps us differentiate signal from noise; because hacktivism can serve as a smokescreen for deeper, more consequential activity beneath the surface.

Espionage

- Theft of sensitive data, intellectual property and strategic intelligence
- Long-dwell reconnaissance of government networks and defence supply chains
- Credential harvesting for persistent access to email and cloud platforms

Disruption

- DDoS attacks against public-facing services
- Website defacement and data-wiper deployment
- OT/ICS manipulation targeting safety and availability

Criminal Enablement

- Sale of harvested access to ransomware affiliates
- Ransomware deployment under false-flag personas
- Monetisation of stolen data through underground markets

> **Noise vs signal:** Hacktivist DDoS campaigns generate headlines but may mask the real objective, persistent access to high-value networks for espionage or pre-positioning for destructive operations.

Briefing context: When you see a surge of hacktivist claims, resist the urge to treat them as the main event. They are often the distraction. The substantive risk lies in the quieter espionage and pre-positioning activity that uses the same window of elevated tension to advance deeper objectives.

Who Is Most at Risk…. Our Environment

Not every asset carries equal risk. The following tiered assessment reflects where a credential compromise or initial foothold would yield the highest adversary return on investment within our specific environment.

Tier	Asset Category	Risk Rationale
Tier 1: Critical	Identity systems, email platforms, remote access gateways, admin tooling	Compromise here enables lateral movement, privilege escalation and persistence across the entire estate. These are the keys to the kingdom.
Tier 2: High	OT gateways/jump hosts, vendor remote access, internet-facing services	Direct pathways into operational technology or externally exposed surfaces that adversaries actively scan and exploit.
Tier 3: Moderate	End-user endpoints	Initial compromise vector via phishing; risk escalates when combined with privilege escalation or lateral movement techniques.

> **Targeting amplifier:** Organisations with defence, research, or Middle East-linked work face elevated targeting likelihood. If your unit touches any of these domains, assume you are a priority target.

Briefing context: Make it relatable for leadership, "If they get one set of privileged credentials, the game changes entirely. That single credential can unlock access to identity infrastructure, email, cloud admin consoles and from there, the path to OT environments becomes viable."

Common Entry Paths

What attackers actually do….and every one of these is preventable.

Password Spraying / Brute Force

Automated campaigns testing common passwords against large numbers of accounts. Targets legacy authentication endpoints that lack rate limiting or modern MFA enforcement. The most frequently observed Iranian TTP in current advisories.

Spear-Phishing

Highly targeted emails crafted using open-source intelligence, often impersonating trusted colleagues or partner organisations. AI-generated lures are increasing both quality and volume of these campaigns significantly.

MFA Fatigue / Push Bombing

Repeated MFA push notifications sent to a target until they approve one out of frustration or confusion. Effective against push-based MFA without number matching or additional context.

Exploited Edge Devices

Unpatched VPN concentrators, firewalls and other internet-facing appliances provide direct network access. Known vulnerabilities in these devices are actively exploited within hours of disclosure.

Trusted Third Parties / Suppliers

Compromise of a supplier with legitimate access to your environment. Supply-chain intrusions are harder to detect because the traffic originates from a trusted source with valid credentials and connectivity.

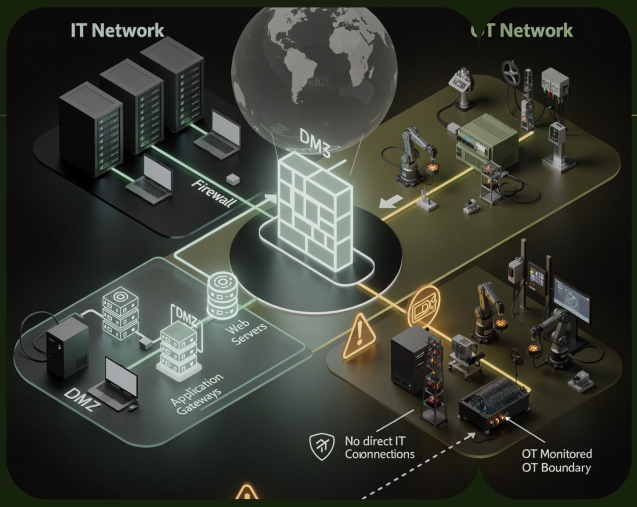
Briefing context: Reinforce that every one of these paths is addressable with strong identity controls, aggressive patching, and robust monitoring. The adversary doesn't need a zero-day, they need one weak password or one unpatched appliance.

OT / Critical Infrastructure Risk

High consequence, limited tolerance……this is where disruption becomes physical.

Segmented Architecture

IT → DMZ/Firewall → OT with monitored boundary



Flat Network

IT → OT direct path — Unacceptable risk

The diagram above illustrates the critical difference between a properly segmented architecture and a flat network. IRGC-affiliated personas have historically targeted industrial control systems, and the consequence of OT compromise extends beyond data loss into physical safety, environmental harm, and service disruption affecting populations.

Remove Internet Exposure

No OT device or management interface should be directly reachable from the internet. Audit and eliminate any residual exposure immediately.

Tight Remote Access + Monitoring

All remote access to OT must traverse a monitored jump host with MFA, session recording, and time-limited access windows. No exceptions.

Change Control & Recovery Readiness

Maintain validated backups of OT configurations. Test recovery procedures including scenarios where IT-to-OT connectivity is severed.

Briefing context: IRGC-affiliated actors have demonstrated both intent and capability to target programmable logic controllers (PLCs). The consequence is why we prioritise OT. A compromised identity system is serious; a compromised water treatment plant is a public safety event. OT stands for Operational Technology and ICS for Industrial Control Systems, the hardware and software that run physical processes.

Hacktivist Surge & Information Operations

Geopolitical escalation reliably triggers a surge in hacktivist activity……some genuine, much of it performative or state-encouraged. The challenge is maintaining perspective: not every claimed attack is real, and not every real attack is what it appears.

Geopolitical Escalation

Tensions rise between nation states, triggering retaliatory posturing across cyber domains.

Surge in Claimed Attacks

DDoS, defacement and data-leak claims multiply rapidly…..many exaggerated or fabricated.

Hacktivist Mobilisation

Persona-driven groups claim targets, recruit volunteers, and amplify messaging on social media platforms.

Potential Cover for Deeper Intrusion

Noise from hacktivism may mask more sophisticated state-sponsored operations pursuing persistent access.

Expect DDoS, Defacement & Leaks

These are the most visible and most common hacktivist tools. They create headlines but rarely cause lasting operational damage. Prepare public-facing teams for potential incidents.

Verify Claims — Don't Amplify

Many hacktivist claims are exaggerated or entirely fabricated. Verify every claim internally before issuing any statement. Communications discipline is essential during this window.

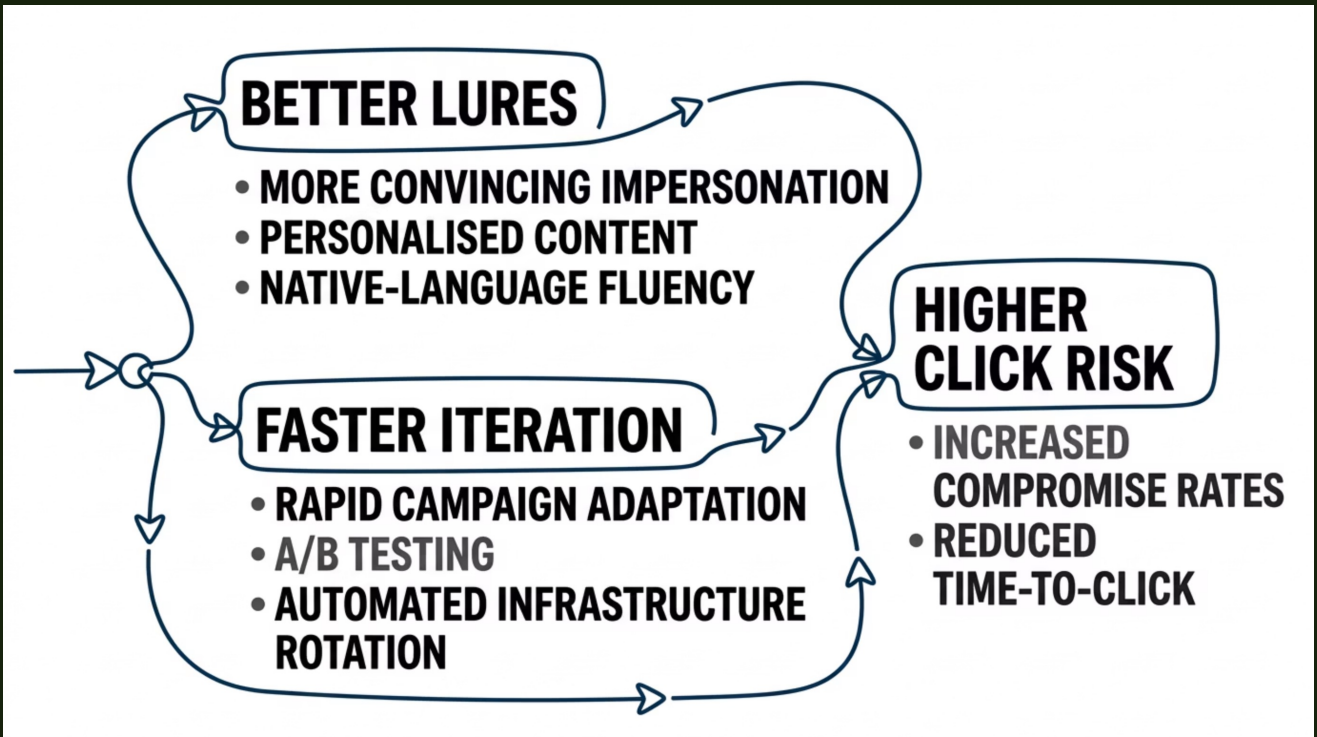
Treat as Potential Cover

The most dangerous scenario is a hacktivist distraction masking a deeper, quieter intrusion by a state-sponsored group. Ensure detection teams are not drawn entirely to the noise.

Briefing context: Stress communications discipline above all. A premature public statement about a "breach" that turns out to be a minor DDoS amplifies the adversary's objective for free. Verify first, communicate second.

AI Increases Phishing Quality and Scale

Artificial intelligence has fundamentally shifted the economics of social engineering. What previously required skilled human operators crafting individual lures can now be automated at scale with significantly higher quality. This is not theoretical, Microsoft's 2025 Digital Defense Report documents the trend in operational campaigns.



More Convincing Impersonation

AI-generated lures now mimic writing style, tone and organisational context with alarming accuracy. Generative models can scrape publicly available information to craft personalised messages that bypass the "does this look right?" instinct that traditional security awareness training relies upon. Multi-language capability means non-English-speaking targets are no longer protected by the language barrier that once made many phishing attempts obvious.

Faster Campaign Iteration

Threat actors use AI to rapidly test and refine lure variants, rotating infrastructure and adapting messaging within hours rather than days. This compresses the defender's detection window and increases the probability that at least one variant will reach an inbox and elicit a click. The volume-quality combination is what makes this evolution particularly dangerous for organisations relying solely on perimeter controls.

Briefing context: Tie this directly to Microsoft's 2025 reporting on AI's role in modern threat scaling. The key message is that our existing phishing defences were calibrated for a lower-quality, lower-volume threat. We need to recalibrate; stronger technical controls, adaptive detection, and updated awareness training that reflects AI-quality lures.

What We're Doing: 0–72 Hours

Immediate hardening sprint: controlled, measurable, owner-assigned.

The following actions are underway now. Each has a designated owner and a completion target within the 72-hour window. Progress is being tracked centrally and will be reported to leadership at the next briefing.

01

Identity Lockdown

Owner: Identity & Access Management Enforce phishing-resistant MFA across all privileged accounts. Disable legacy authentication protocols. Review and tighten conditional access policies. Revoke stale sessions and force re-authentication for administrative roles.

02

External Exposure Review

Owner: Vulnerability Management Complete external attack surface scan. Patch or mitigate all critical and high-severity vulnerabilities on internet-facing assets within 72 hours. Confirm no OT management interfaces are externally reachable.

03

EDR & Logging Verification

Owner: Security Operations Validate endpoint detection and response (EDR) coverage across all in-scope endpoints. Confirm critical log sources are flowing to SIEM. Address any gaps in telemetry that would impair detection or investigation capability.

04

OT Access Review & Segmentation Checks

Owner: OT Security / Infrastructure Audit all remote access pathways into OT environments. Verify segmentation controls between IT and OT. Confirm jump host configurations and ensure session monitoring is active.

05

Threat Hunting Against Advisory TTPs

Owner: Threat Intelligence / Hunt Team Execute targeted hunts using indicators and behavioural signatures from CISA, ACSC and NCSC advisories. Focus on credential-abuse patterns, anomalous authentication events, and lateral movement indicators.

Briefing context: The intent here is to convey control. These are not aspirational actions, they are assigned, tracked, and time-bound. Leadership should feel confident that the response is structured and measurable, not ad hoc.

What We're Doing: 2–4 Weeks

Sustained hardening: Building resilience beyond the initial sprint.

After the immediate 72-hour window, we transition into a sustained hardening phase designed to deepen defences, validate resilience, and close gaps identified during the initial sprint. These actions ensure we are not simply responding to the current threat window but building durable capability improvements.

1

Targeted Hunts & Detection Engineering

Expand hunt operations beyond advisory-specific indicators to broader Iranian TTP patterns. Develop and deploy new detection rules calibrated to credential abuse, MFA bypass and lateral movement techniques. Tune existing detections to reduce false positives and improve signal fidelity.

2

Tabletop Exercise

Conduct a scenario-based tabletop exercise simulating a credential compromise escalating into an attempted OT boundary breach. Involve IT security, OT operations, incident response and executive communications teams. Identify decision-making gaps and refine playbooks.

3

Supplier Access Review

Audit all third-party and supplier access to our environment. Validate that each connection is business-justified, time-limited where appropriate, and monitored. Revoke or restrict access where controls are insufficient. Engage key suppliers on their own threat posture.

4

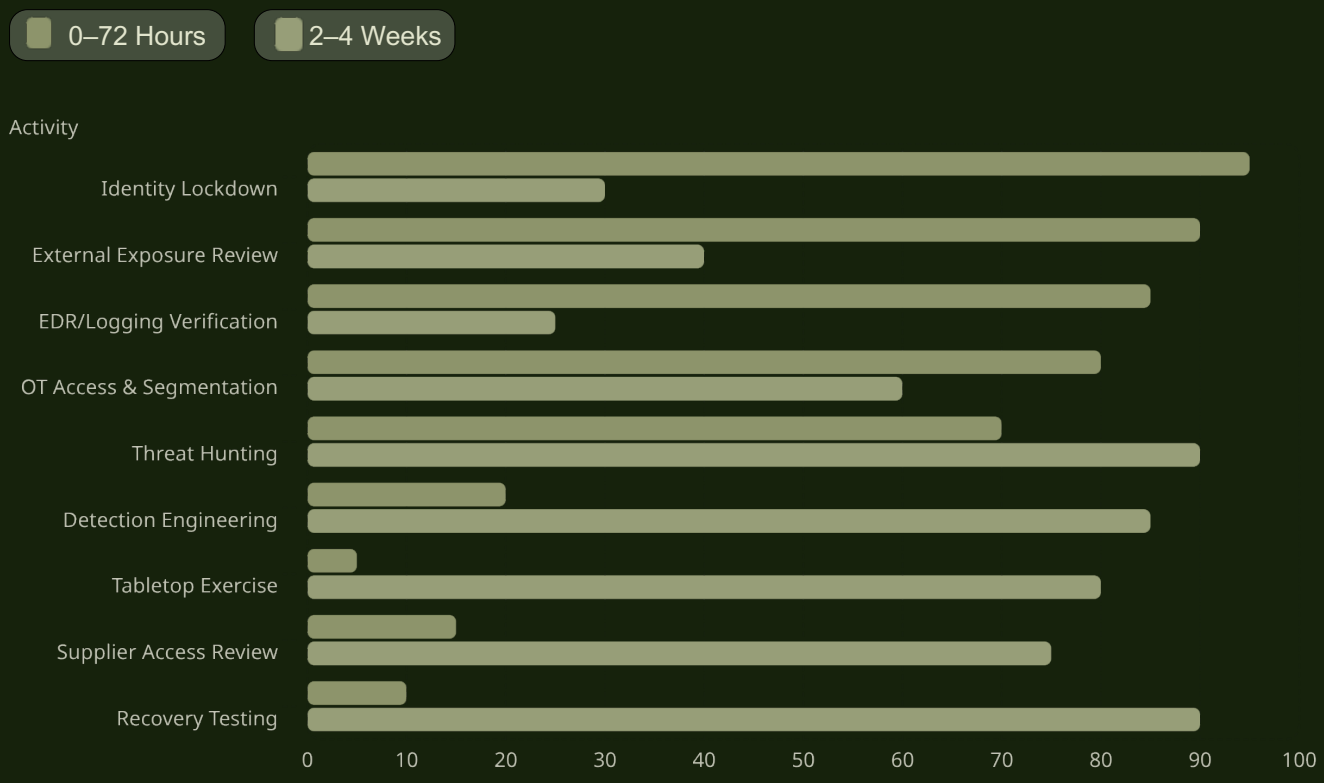
Recovery Testing

Test backup and recovery procedures for critical systems, explicitly including OT scenarios where IT connectivity may be severed. Validate recovery time objectives (RTOs) and ensure teams can execute restoration under pressure with current documentation and tooling.

Briefing context: Emphasise resilience as the theme of this phase. The 72-hour sprint addresses the immediate risk; the 2–4 week programme builds the muscle memory and structural improvements that reduce risk durably. The Tabletop Exercise is particularly important; it exposes decision-making seams that no amount of technical hardening can address on its own.

Response Timeline Overview

The following chart summarises how our response activities are distributed across the two phases; demonstrating both the urgency of the initial sprint and the sustained commitment required over the following weeks.



Values represent estimated percentage of effort allocated to each phase. The initial sprint prioritises identity, exposure and detection coverage. The sustained phase shifts emphasis toward hunting, resilience testing and supply-chain assurance……activities that require more time but deliver durable risk reduction.

LEADERSHIP ACTION REQUIRED

What is Needed From Leadership

Three decisions that will materially accelerate defensive posture.

1 Approve Emergency Policy Changes

Executive authorization is required to implement immediate identity-tightening measures, including enforcing phishing-resistant MFA for all users (not just privileged accounts), disabling legacy authentication protocols that may impact a small number of legacy applications, and restricting conditional access policies that will temporarily reduce convenience for some remote access scenarios. These changes carry minor operational friction but dramatically reduce exposure to the primary attack vector.

2 Fast-Track Patching Windows & OT Segmentation

Standard change-management timelines are insufficient for the current threat tempo. Approval is needed for accelerated patching windows on critical internet-facing infrastructure, and authorisation to proceed with OT segmentation work that may require brief, coordinated service interruptions. Every day of delay on a known-exploited vulnerability is a day the adversary retains a viable entry point.

3 Clear Communications Authority

In the event of a disruption or claimed attack, a pre-agreed communications authority and escalation pathway is needed. This means designating who speaks externally, approving holding statements in advance, and ensuring the security team can brief the communications function rapidly without waiting for multi-layer approvals. Speed and accuracy of public messaging directly impacts reputational outcomes.

Next Steps

Next update in 7 days or sooner if indicators change. The security team will provide a written status report covering completion rates for the 72-hour sprint, any findings from initial threat hunts, and a refined risk assessment based on the evolving intelligence picture. Ad hoc updates will be issued immediately if we observe indicators of targeting against our environment or if allied agencies issue new advisories.

Confidence Statement

The threat is real and credible. Our response is structured, measured and underway. With the three leadership decisions above, we can close the most significant gaps within days, not weeks. We are not starting from zero, we are accelerating an already-capable programme to meet an elevated threat.

Briefing context: End with confidence and clarity. The ask is specific and bounded; three decisions, each with a clear rationale. Avoid leaving the room without commitments on all three. Remind leadership that the next update is calendared and the team is in control.
Sources referenced throughout this brief: CISA fact sheet on vigilance regarding Iranian cyber actors; NSA press release on joint fact sheet; ACSC joint advisory on credential access / brute force; CISA advisory on IRGC-affiliated PLC exploitation; UK NCSC phishing warning; Microsoft Digital Defense Report 2025. All cited as public government advisories and major vendor reporting.