Horizon3.ai Issues Guidance on Emerging Iranian Cyber Threats and Defensive Measures for Organisations

Thursday 19 March, 2026

London -
Horizon3.ai, a leader in offensive
security, today released guidance outlining the evolving Iranian cyber threat landscape and recommended actions for organisations to enhance their cyber resilience. As geopolitical tensions intensify, this guidance aims to equip security leaders with actionable insights to anticipate and mitigate risks from nation-state actors.

Recent U.S. and Israeli strikes on Iranian infrastructure, including banks and oil facilities, have prompted declarations from Iran of retaliatory actions against equivalent Western targets. With Iranian military leadership disrupted but expected to regroup into a decentralised structure, experts anticipate a shift toward "cyber guerrilla warfare." This approach is likely to focus on eroding U.S. strike capabilities through attacks on the Defense Industrial Base (DIB), disrupting domestic support via impacts on banking, telecommunications, public utilities, and manufacturing, and targeting oil and gas infrastructure to induce market panic and elevate prices.

Early indicators of this escalation include attacks on AWS data centres in the UAE and Bahrain, as well as Stryker Medical and UK hospital systems. Observed activities encompass destructive data wipers (e.g., Stryker variants), unauthorised access to CCTV systems like Hikvision cameras to aid physical targeting, and false claims on social media to sow panic.

Looking ahead, security analysts expect intensified operations in the coming weeks, including:

? Disruptions to DIB manufacturing, production, and repair capacities

? Oil and gas attacks reminiscent of the Colonial Pipeline incident

? Financial system interference to halt commerce and trigger market volatility

? Cloud provider targeting to interrupt digital services

? Disrupting healthcare services causing risk to patients

? Impacts on state, local, and education entities to degrade citizen services

To defend against these threats, Horizon3.ai emphasises securing initial attack surfaces such as VPNs and edge devices vulnerable to CISA Known Exploited Vulnerabilities (KEVs), including Fortinet, Ivanti, and Citrix NetScaler; Active Directory and compromised credentials; and Remote Management Tools (RMMs) with known KEVs.

Related Sectors:

Computing & Telecoms ::

Related Keywords:

Iranian Cyber Threats ::

Scan Me:

Key recommended actions for immediate implementation include:

1. Assessing, identifying, and rapidly remediating attack surfaces exploitable by Iranian tactics, techniques, and procedures (TTPs)

2. Deploying decoys across networks, particularly in Active Directory, to enhance detection and speed incident response

3. Evaluating and strengthening critical Security Operations Center (SOC) controls, such as Endpoint Detection and Response (EDR) and Security Information and Event Management (SIEM)

4. Rehearsing incident response, containment, and eradication workflows

5. Locating and protecting critical data while practicing backup and recovery procedures

“Right now we need to rally as practitioners and work together to plug security holes, build confidence that SOC tools are working, and create muscle memory for how to respond to attacks. It’s about training like we fight so we know exactly what to do when things go awry,” said Snehal Antani, CEO and co-founder of Horizon3.ai.

As a service to our customers, Horizon3.ai surged attack research capacity to maximise coverage of known Iranian techniques, tactics, and procedures (TTPs) within NodeZero®, as well as temporarily enabling Iranian Threat Actor Intelligence for all NodeZero® customers. This capability helps defenders identify the exploitable vulnerabilities most likely to be targeted in Iranian cyber campaigns.

“This is a fluid situation that changes daily. We can’t control what the adversary will do, we can only control our readiness and ability to defend the enterprise,” Snehal explained.

Horizon3.ai encourages security professionals to operate with urgency and integrate these recommendations into their cyber resilience plans.

About Horizon3.ai

Horizon3.ai’s NodeZero® platform is trusted by over 40% of the Fortune 10, the world’s largest banks, top global pharmaceutical and semiconductor manufacturers, critical infrastructure operators around the globe, and the U.S. Defense Industrial Base to proactively find, fix, and verify exploitable vulnerabilities to continuously fortify cyber defences and improve cyber resilience. The fastest-growing cybersecurity company in America (Inc. 5000, Deloitte Fast 500), Horizon3.ai was founded by a mix of U.S. Special Operations veterans and industry experts and is headquartered in San Francisco.

Follow Horizon3.ai on LinkedIn and X.

Contact:
Horizon3.AI Europe GmbH, Prielmayerstraße 3, 80335
Munich, Germany
www.horizon3.ai

Pr Agency: euromarcom public relations GmbH, www.euromarcom.de,
team@euromarcom.de

Company Contact:

_

news aktuell

E. desk@newsaktuell.de
W. https://www.newsaktuell.de/

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.newsaktuell.pressat.co.uk