MONTHLY THREAT BRIEF

March 2026

THIS MONTH IN CYBER

Key Developments shaping operational risk in March 2026

At a Glance

Geopolitical Cyber Activity

Supply Chain & Third-Party Risk

Operational & Infrastructure Risk

Cyber Activity Becoming More Visible

Cyber operations tied to geopolitical tensions are becoming more visible, with threat actors increasingly using data leaks, targeted messaging, and public disclosure to amplify impact beyond initial access and influence broader audiences.

What To Do

- Monitor for credential exposure and targeted phishing
- Reinforce protections for high-profile users
- Prepare response plans for public-facing incidents

Cisco SD-WAN Exploitation & Edge Risk

An advisory from NSA and partners highlights sustained exploitation of Cisco SD-WAN devices, reinforcing the importance of securing externally exposed infrastructure and monitoring for long-term access.

What To Do

- Audit exposed infrastructure and apply patches
- Hunt for unusual SD-WAN activity
- Review segmentation and access controls

Brief

Energy Sector Targeting Signals

Ransomware groups and threat actors continue to signal interest in energy and utility environments, reinforcing the importance of visibility across operational and infrastructure systems.

New U.S. Cyber Strategy Released

A new national cybersecurity strategy emphasizes protecting critical infrastructure, securing supply chains, and strengthening resilience across public and private sectors.

Platform and Identity Abuse Increasing

Threat actors are increasingly leveraging valid accounts, common platforms, and identity-based access to support intrusion activity and persistence.

CONTINUED ON NEXT PAGE »

EMERGING THREAT SURFACE

Infrastructure, supply chain, and operational exposure developments

Threat Activity Aligning with Strategic and Geopolitical Interests

Threat activity is increasingly aligned with geopolitical objectives, targeting organizations and sectors where impact can extend beyond initial access to influence and disruption.

What To Do

- Monitor targeting patterns across industries and regions
- Strengthen protections for high-profile and sensitive users
- Secure and continuously monitor externally exposed systems
- Prepare for incidents with potential reputational impact

Supply Chain & Third-Party Access Risk

Threat actors are increasingly using trusted third-party access as an entry point. Vendor and partner connections can create indirect pathways into environments that often lack the same level of visibility and control.

What To Do

- Review and validate third-party access
- Enforce least privilege for vendor accounts
- Monitor external connections for anomalies
- Define and enforce security requirements

Operational Disruption as a Strategic Objective

Recent activity shows a shift toward disruption as a primary objective, with attackers targeting systems where impact affects operations, safety, or public perception.

What To Do

- Align cyber and business response teams
- Test escalation and communication plans
- Strengthen business continuity planning

Living-off-the-Land Techniques Increasing

Attackers are increasingly using built-in system tools to carry out activity, allowing them to blend into normal operations and avoid detection while maintaining access over time.

What To Do

- Monitor use of administrative tools
- Establish baselines for normal activity
- Investigate unusual command execution
- Limit unnecessary administrative privileges

CONTINUED ON NEXT PAGE »

STRATEGIC TAKEAWAYS

March 2026

Across this month's developments, several consistent themes are emerging for security and IT teams. Rather than focusing on individual incidents, these signals highlight where organizations should be directing attention as risk continues to evolve.

Operational Impact Is Extending Beyond the Network

Recent activity highlights how cyber incidents are increasingly designed to create impact beyond internal systems. Whether through public data exposure, disruption, or reputational effects, organizations must be prepared for incidents that extend into customer trust, public perception, and broader operational consequences.

Externally Exposed Systems Require Continuous Validation

Infrastructure that sits at the edge of the network continues to be a reliable entry point for attackers. These systems should not be treated as "set and forget" assets, but instead require ongoing validation, monitoring, and review to ensure they remain secure as configurations and threat activity evolve.

Credential-Based Access Is Replacing Traditional Exploitation

Attackers are increasingly relying on valid credentials and session-based access rather than exploiting vulnerabilities directly. This shift makes detection more challenging and reinforces the need for organizations to focus on identity monitoring, access control, and behavioral visibility across environments.

Threat Activity Is Becoming More Coordinated and Visible

Cyber operations are no longer always quiet or isolated. Many campaigns now involve coordination across groups, public messaging, and visible indicators of compromise. This trend requires organizations to be prepared not only for technical response, but also for communication and broader organizational coordination.

Resilience Depends on Speed and Coordination

As attack timelines continue to shorten, the ability to respond quickly becomes a defining factor in limiting impact. Organizations should prioritize coordination across teams, clear escalation paths, and the ability to act quickly when indicators of compromise are identified.

CONTINUED ON NEXT PAGE »

THREAT INTELLIGENGE SOURCES

VMware VCSP Termination: A Forced Architecture Decision, Not a Licensing Event

Our latest blog analysis explores how infrastructure decisions are increasingly being driven by security, visibility, and long-term operational control, and what organizations should consider as these shifts continue.

Read the Full Analysis

Sources & Further Reading

Infrastructure, Policy & Strategy

- NSA Issues Advisory on Cisco SD-WAN Exploitation
- President's Cyber Strategy for America Outlines National Security Priorities
- Dpt. of Energy Prepares First Cybersecurity Strategy for Energy Sector

Threat Intelligence & Activity

- Iranian Cyber Activity Expands with Targeted Operations
- MuddyWater Activity and Evolving Attack Chain Observed in Active Campaigns
- Handala Hackers Leveraging Telegram for Malware Delivery

Stay Connected

Follow us on social media for the latest updates: