MONTHLY THREAT BRIEF

February 2026

THIS MONTH IN CYBER

Key Developments shaping operational risk in February 2026

At a Glance

Geopolitical Cyber Escalation

SD-WAN Active Exploitation

Infrastructure & Utility Targeting

Iranian Cyber Threat Escalation

A group affiliated with the IRGC and linked to the "MuddyWater" campaign has launched operations against regional geopolitical rivals and supporting entities, employing dual-use tools and targeting VPN appliances to access networks.

What To Do

- Review and restrict VPN appliance exposure
- Enhance geopolitical and threat actor monitoring
- Plan resilience against destructive operations

Cisco SD-WAN Exploitation & Hunt Guidance

CISA and other agencies have flagged significant, active exploitation of Cisco SD-WAN vulnerabilities, urging organizations to promptly assess and secure SD-WAN devices.

What To Do

- Audit SD-WAN exposure and patch if vulnerable
- Activate threat hunting focused on SD-WAN compromise
- Monitor Cisco's latest advisories and apply guidance

Brief

Dell RecoverPoint Zero-Day

Dell disclosed a zero-day in RecoverPoint for VMs opening paths for remote code execution. Immediate patching is advised.

Supply Chain Website Hijacking

A BEC attack hijacked a vendor's website to redirect partners, highlighting risks in compromised supply chains.

AI-Assisted Attacks

Reports are emerging that generative AI is being leveraged to refine phishing campaigns and bypass traditional defense mechanisms.

ICS Advisory Spotlight

CISA issued a critical ICS advisory related to vulnerabilities in industrial control system software, recommending immediate attention.

CONTINUED ON NEXT PAGE »

EMERGING THREAT SURFACE

Infrastructure, supply chain, and operational exposure developments

Dell RecoverPoint for VMs Zero-Day

Google Cloud/Mandiant reported discovery of a Dell RecoverPoint for Virtual Machines vulnerability during investigations involving backdoor activity, describing an exploitation path tied to hard-coded default credentials for an admin user and deployment of a malicious WAR file via Tomcat Manager.

What To Do

- Identify any RecoverPoint for VMs footprint and confirm vendor remediation status.
- Review Tomcat Manager access patterns and look for suspicious requests to /manager and WAR deployment activity as described in the investigative notes.

Supply-Chain Style Web Compromise

Recorded Future reported on activity it describes as “GrayCharlie” hijacking law firm sites in what it frames as a suspected supply-chain style event.

What To Do

- Review CMS plugins and third-party scripts.
- Monitor web assets for unauthorized changes.
- Restrict and secure admin access.
- Confirm vendor incident notification procedures.

Critical Infrastructure: Physical Threats

A power substation was targeted near Boulder City, reinforcing the need for blended resilience planning.

What To Do

- Confirm IR plan accounts for physical scenarios
- Review monitoring & access for operational sites
- Validate after hours response paths

AI Misuse

A recent report described how a hacker used a generative AI chatbot to assist with attacks targeting Mexican government agencies, helping generate scripts and accelerate parts of the intrusion process.

What To Do

- Emphasize phishing resilience
- Review login patterns & credential misuse
- Confirm incident notification paths and access controls

CONTINUED ON NEXT PAGE »

STRATEGIC TAKEAWAYS

February 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.

Edge Infrastructure Is Becoming a Primary Entry Point

Networking appliances, edge devices, and externally exposed infrastructure continue to be attractive targets for attackers seeking durable access. Organizations should treat these systems as critical security boundaries and ensure they are included in ongoing risk reviews and monitoring strategies.

Operational Platforms Are High-Impact Targets

Backup platforms, operational technology, and infrastructure management systems increasingly represent valuable control points for attackers. Security teams should evaluate how these systems are monitored, who has access to them, and how compromise of these platforms would affect business continuity.

Third-Party Ecosystems Expand the Risk Surface

Web platforms, service providers, and external vendors remain an extension of an organization's attack surface. Maintaining visibility into vendor dependencies and third-party access paths is essential for understanding where risk may originate outside the traditional network perimeter.

Cyber and Physical Resilience Are Converging

Recent events highlight how infrastructure disruption can occur through both cyber intrusion and physical interference. Organizations should continue strengthening resilience planning that accounts for operational disruption across both domains.

Speed Is Increasing Across the Threat Landscape

Automation and AI-assisted workflows are accelerating how quickly attackers can research targets, develop tools, and execute campaigns. Security teams should focus on reducing detection and response timelines to keep pace with this evolving environment.

CONTINUED ON NEXT PAGE »

THREAT INTELLIGENGE SOURCES

Geopolitical Volatility and the Iranian Cyber Threat: What Defenders Need to Know Now

Our latest blog analysis explores how Iranian cyber actors respond during geopolitical escalation.

Read the Full Analysis

Sources & Further Reading

Government Advisories

- Canadian Cyber Threat Bulletin
- NSA/ASD/ACSC SD-WAN Alert
- ICS Advisory—CVE-2026-1670

Threat Intelligence Reports

- Cisco Talos—SD-WAN Exploitation
- Google Cloud/Mandiant-Dell RecoverPoint Investigation
- Recorded Future – GrayCharlie Law Firm Website Compromise

Stay Connected

Follow us on social media for the latest updates: