CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** March 30th, 2026 - April 10th, 2026
Distribution: Public Sector Partners, Local Governments, IT Department *Volume 2 Issue 6*

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Microsoft Windows Defender Zero-Day	General	A security researcher publicly released exploit code affecting Windows Defender where an attacker can trick Defender into writing attacker-controlled content to an arbitrary path as SYSTEM, via its own update mechanism.	Monitor Microsoft Security Response Center (MSRC) advisories for emergency patches.
Chromium Dawn WebGPU Exploit	General	Use-after-free vulnerability in Google Chrome's WebGPU Dawn implementation allows remote attackers who have compromised the renderer process to execute arbitrary code via crafted HTML pages.	Update Chromium to version 146.0.7680.177 (Linux), 146.0.7680.177/178 (Windows/ macOS) immediately.
Fortinet FortiClient Improper Access Control	Enterprise Infrastructure, Finance, Government	Critical improper access control vulnerability in FortiClient Endpoint Management Server (EMS) versions 7.4.5 and 7.4.6 allows unauthenticated attackers to execute arbitrary code or commands. No authentication or user interaction is required.	Apply emergency hotfix for FortiClient EMS to 7.4.5 and 7.4.6 immediately. Conduct forensic review of all access logs from February onwards.
Sapphire Sleet Attacker Group	Software Development	A North Korean supply chain attack campaign is currently being carried out. Compromised HTTP client library 'Axios' via npm supply chain attack. 2 new npm package version for v5.x updates were trojanized with C2 redirection.	Review all package-lock.json files for Axios versions released March 31, 2026. Remain vigilant for unexpected outbound C2 connections from build servers and workstations.
MuddyWater Espionage Group	General	Iran's Minitry of Intelligence and Security (MOIS) has been utilizing a cyber espionage group named MuddyWater. MuddyWater has carried out a myriad of attacks since 2017, with increased activity as of early 2026.	Monitor emails for Farsi content from external addresses spoofing trusted domains.

CERIAC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** CISA Known Exploited Vulnerabilities Catalog Update - *CISA updated its Known Exploited Vulnerabilities (KEV) Catalog in April 2026, adding multiple critical vulnerabilities requiring urgent remediation, including flaws in Chrome, TrueConf, and FortiClient EMS, along with several ICS advisories.*
- **CISA ICS Medical Advisory:** Health ISAC Monthly Update - *The Health ISAC has published their monthly Cybersecurity newsletter which contains several announcements. Among the announcements, key highlights include a Massachusetts hospital cyberattack forcing ambulances to divert, and an update on the Stryker cyberattack from last month.*

Security Awareness Theme

April Focus: Social Engineering Tactics

Social Engineering is the art of manipulating people into divulging confidential information or performing actions that compromise security. Unlike traditional technical hacks that target software or networks, social engineers target human psychology by exploiting their trust through fear, urgency, or even the feeling of being left out. In the modern era of AI, obvious spelling errors and language barriers are largely a thing of the past. That's why it is important to know the signs, so you can keep yourself safe!

Phishing, and it's many cousins.

- Phishing is the art of sending a malicious email with the goal of getting the recipient to click a link, or share important information.
- Phishing is not the only method. Attackers can engage in Vishing (voice call), Smishing (SMS texts), and even Quishing (QR codes).

Always verify contact information!

- True to the old saying, if it's important, it's worth a face-to-face conversation. If there is a true sense of urgency, they can speak with you in-person.
- Be sure to check where the message is coming from. Is the domain in the email correct? Is the phone number area and country code correct? Does the link provided lead to a trustworthy domain?

Sector-Specific Highlights

- **Healthcare:** Stryker Cyber Incident - A March 2026 cyberattack caused a global network disruption at Stryker, impacting internal systems and highlighting how attacks on healthcare suppliers can disrupt operations across the medical ecosystem. ***Prevention Tips:*** *Strengthen vendor risk management, segment critical systems, and ensure contingency plans are in place to maintain operations during IT disruptions.*

- **Utilities/Industrial:** CISA ICS Security Risks - Industrial control systems continue to face increasing threats from exposed SCADA systems, weak credentials, and unpatched vulnerabilities, making critical infrastructure a frequent target. ***Prevention Tips:*** *Remove OT systems from public internet access, enforce strong authentication, and implement strict network segmentation between IT and OT environments.*

- **Education:** Harvard IT Cybersecurity Alert – Harvard issued a cybersecurity alert about a phishing campaign where attackers impersonate IT staff and use fake login pages and social engineering to steal user credentials. ***Prevention Tips:*** *Do not respond to unsolicited IT requests, verify all login pages before entering credentials, and enable multi-factor authentication to protect accounts from unauthorized access.*

- **Public Safety/Financial:** FINRA Cyber Fraud Warning - FINRA highlighted ongoing risks of account takeovers and cyber fraud, where attackers use stolen credentials and social engineering to access accounts and make unauthorized transactions, impacting firms and customers across the financial sector. ***Prevention Tips:*** *Implement strong authentication controls, monitor account activity for unusual behavior, and educate users on recognizing phishing and social engineering attempts.*

Recommended Tools and Federal Resources

- CISA Ransomware Readiness Assessment (RRA) – A no-cost self-assessment tool that helps organizations evaluate their preparedness against ransomware attacks and identify gaps in their defenses.
- NIST Cybersecurity Framework (CSF) 2.0 – Provides a structured set of guidelines and best practices to help organizations manage and reduce cybersecurity risk across their operations.
- CISA Decider Tool - Maps adversary behaviors to MITRE ATT&CK techniques, helping security teams analyze threats and improve defensive strategies.

Emerging Trends to Watch

- *AI - Driven Phishing & Social Engineering* – Attackers are leveraging generative AI to create highly convincing phishing emails, messages, and impersonations at scale, making attacks harder to detect. These campaigns often use automation and personalization to increase success rates. ***Prevention Tips:*** *Enforce phishing-resistant MFA, train users to recognize suspicious messages, and monitor unusual login or email activity across systems.*
- *Expansion of AI Attack Surface (Agent & Tool Abuse)* – AI systems and agents are introducing new attack surfaces, where attackers exploit misconfigurations, prompt injections, or excessive permissions to access data or execute actions. These risks increase as organizations integrate AI into core systems. ***Prevention Tips:*** *Limit AI system permissions, validate inputs, and monitor AI-related activity to detect misuse or abnormal behavior.*
- *AI - Accelerated Vulnerability Exploitation* - Threat actors are using AI to rapidly scan for and exploit vulnerabilities, significantly reducing the time between disclosure and active attacks. This allows attackers to target systems much faster than traditional patching cycles can keep up. ***Prevention Tips:*** *Prioritize rapid patching of critical systems, continuously scan for vulnerabilities, and monitor internet-facing assets for suspicious activity.*