CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** February 16th, 2025 - February 27th, 2026
Distribution: Public Sector Partners, Local Governments, IT Departments *Volume 2 Issue 4*

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Google Chrome RCE Vulnerability	General	A vulnerability in Google Chrome's CSS engine allows for Remote Code Execution within the browser's sandbox. The issue stems from a memory corruption flaw in the Chromium rendering engine.	Update Google Chrome to version 145.0.7632.75 (Windows/Mac) or 144.0.7559.75 (Linux).
Windows Shell Zero-Day	Digital Infrastructure	Attackers can bypass Windows SmartScreen security prompts to trick a user into click a malicious link or shortcut file. This allows the attacker to execute content without the standard "Are you sure?" warnings.	Deploy the Microsoft February 2026 Cumulative Update immediately. Utilize Endpoint Detection and Response to monitor for unusual *shell32.dll* activity.
Azure SDK for Python RCE Vulnerability	Cloud Service Providers	A flaw in the Azure SDK for Python allows an unauthenticated attacker to spend specially crafted tokens to trigger code execution on any system utilizing the vulnerable library.	Update the *azure-core* and related Python packages to the latest version via pip. Audit all Python-based microservices interacting with Azure for outdated SDK dependencies.
GitHub Copilot Command Injection Flaw	Software Engineering, DevOps, R&D Departments	Improper neutralization of special elements used in a command in GitHub Copilot allows an unauthorized attacker to execute code over a network. Attackers can trick the AI assistant into executing malicious code or leaking sensitive variables (like API keys) during the development process.	Update Visual Studio, VS Code, and the GitHub Copilot extension to the latest February 2026 builds.
Lazarus (DPRK) Group	Cybersecurity, Mental Health Providers	North Korean state sponsored Lazarus Group has recently transitioned from pure espionage to using the Medusa Ransomware-as-a-Service (RaaS). Their newest targets have been in the mental health sector, totaling $260,000 in ransomed data.	Secure accounts by enforcing MFA for email and remote access, auditing permissions regularly, and monitoring for unusual activity.

CERC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** CISA Adds Two Known Exploited Vulnerabilities to Catalog
  CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.
- **CISA ICS Medical Advisory:** ZOLL ePCR iOS Mobile App *A vulnerability in the ZOLL ePCR iOS app could allow injected content to be interpreted when reports are rendered/ printed, which may expose local files containing sensitive data.*

Security Awareness Theme

February Focus: Password Security

Passwords are the backbone of our digital security; from the way we unlock our phones to the way we log in to all our online accounts. Over 68% of successful cyberattacks still originate from human error or credential misuse. Billions of stolen username-password pairs are traded on the dark web. If you reuse a password from a personal shopping site for your email, an attacker can automate attempts to log in to your professional accounts in seconds.

Prioritize Length over Complexity

- Short passwords can be cracked relatively fast, regardless of complexity.
- Instead, try implementing **Passphrases** for additional security.
- Example:
  - Old: P4ssw0rd67
  - New: iLoveMyD0gs4ever&theyLoveMe!

Make Multi-Factor Authentication Mandatory

- Create alternative ways to log in to your accounts.
- This way, attackers need more than just a password.
- If one factor is compromised, you can reset it.
  - Just use another form to verify your identity!
- Use MFA on all important online accounts.

Sector-Specific Highlights

- **Healthcare:** University of Mississippi Medical Center Ransomware Attack - The University of Mississippi Medical Center (UMMC) was hit by a ransomware attack that took its Epic electronic health record (HER) system offline, forcing seven hospitals to revert to "downtime procedures" (pen and paper). ***Prevention Tips:*** *Isolate legacy IoT and medical devices into separate VLANs to prevent lateral movement.*

- **Utilities/Industrial:** Compromised Operational Technology - A new sub-group, SYLVANITE, has been identified as the "breach time" that gains initial access before handing off control to more destructive actors. ***Prevention Tips:*** *Deploy passive monitoring tools to create a real-time inventory of every sensor and controller on the Operational Technology network.*

- **Education:** AI Student Federal Aid Theft – Lately higher education leaders have been warning of a surge in "Ghost Students" which are AI generated identities used to enroll in online courses to steal federal student aid. ***Prevention Tips:*** *Implement checks for government-issued IDs for student enrollment to counter AI-synthetic identities.*

- **Public Safety/Financial:** US Treasury AI Security Initiative - On February 18, 2026, the US Treasury launched a major public-private initiative to provide small and mid-sized banks with AI-driven cyber defense resources. The treasury is working to release deliverables for the Artificial Intelligence Executive Oversight Group (AIEOG) throughout the month of February. ***Prevention Tips:*** *Implement AI Security Posture Management (AI-SPM) to track data lineage and prevent sensitive financial models from being poisoned or manipulated.*

Recommended Tools and Federal Resources

- Joint Cyber Defense Collaborative (JCDC) Resources – The JCDC offers coordinated threat analysis and shared defensive guidance across federal, state, local, and private sector partners to strengthen cyber defense.
- CISA Ransomware Guidance & Resources – CISA's ransomware page provides best practices, playbooks, alerts, and mitigation guidance specifically focused on deterring, responding to, and recovering from ransomware attacks.
- NIST National Initiative for Cybersecurity Education Workforce Framework - Provides standardized cybersecurity workforce roles, knowledge, and skills to help organizations develop training programs.

Emerging Trends to Watch

- Exploitation of API Endpoints and Public-Facing Web Services– Threat actors are increasingly targeting exposed APIs and public-facing web services to extract data or gain unauthorized access through weak authentication or improper input validation. ***Prevention Tips:*** *Implement strong authentication for APIs, enforce input validation, apply rate limiting, and regularly review externally exposed services for unnecessary access.*
- Password Spray Attacks Against Cloud Services – Attackers continue conducting password spray campaigns against cloud email and identity platforms by attempting commonly used passwords across many accounts to avoid lockouts. ***Prevention Tips:*** *Require multi-factor authentication on all accounts, enforce strong password policies, and monitor repeated failed login attempts across multiple accounts.*
- *Data Exfiltration Through Misconfigured Cloud Storage* - Organizations continue to experience data exposure incidents due to misconfigured cloud storage services that allow public or unauthorized access. These issues often occur without malware and may go unnoticed for extended periods. ***Prevention Tips:*** *Regularly audit cloud storage permissions, disable public access by default, and implement automated monitoring to detect unintended exposure of sensitive data.*