CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** March 3rd, 2025 - March 13th, 2026
Distribution: Public Sector Partners, Local Governments, IT Departments *Volume 2 Issue 5*

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
The Gentlemen Ransomware Group	General	A newer Ransomware group that has been targeting medium to large companies in the Healthcare, Manufacturing, Construction, and Insurance sectors with attacks concentrated in the Asia-Pacific region, and the United States. Attacks have spanned at least 17 countries.	Enforce driver allowlisting and restrict administrative tool usage. Monitor for unauthorized AnyDesk sessions.
Android Zero Day	General	An integer overflow in the graphics subcomponent allows an attacker to cause severe memory corruption which would bypass security controls and gain unauthorized control over the system.	Update your Android OS on your smartphone or tablet to the latest version.
Akira RaaS Group	General	A ransomware group active since March 2023, operating as a Ransomware-as-a-Service (RaaS) platform targeting organization globally across critical industries including healthcare, manufacturing, finance.	Enforce phishing-resistant MFA on all external-facing services, patch VPN and hypervisor vulnerabilities promptly.
Java Security Engine Authentication Bypass	Enterprise Software	A logic error was discovered in *pac4j-jwt*, a popular Java-based security engine for web applications. The flaw is in the *JwtAuthenticator* component when processing encrypted JSON Web Tokens (JWE).	Upgrade the *org.pac4j:pac4j-jwt* dependency to the latest fixed versions (4.5.9+, 5.7.9+, or 6.3.3+)
Nginx UI Unauthenticated Backup	Technology Infrastructure	The Backup API endpoints for the Nginx UI lack authentication checks, and the system inadvertently sends the AES-256 encryption keys and Initialization Vectors in plain text within the HTTP response headers. Attackers can remotely download the entire system backup and decrypt it using the provided keys.	Upgrade Nginx UI to version 2.3.3 or newer immediately. If an update is not immediately possible, restrict access to the Nginx UI port (usually 9000) using firewall rules or a VPN, and disable the backup API endpoint.

CERC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** Delta Electronics CNCSoft-G2 *CISA released an ICS advisory describing vulnerabilities in Delta Electronics CNCSoft-G2 software that could allow attackers to execute arbitrary code or disrupt system operations if exploited. Organizations using affected products should review vendor guidance and apply recommended security updates or mitigations.*
- **CISA ICS Medical Advisory:** Grassroots DICOM (GDCM) *CISA issued an ICS Medical Advisory describing vulnerabilities in the Grassroots DICOM (GDCM) library that could allow attackers to exploit improper handling of DICOM medical imaging files.*

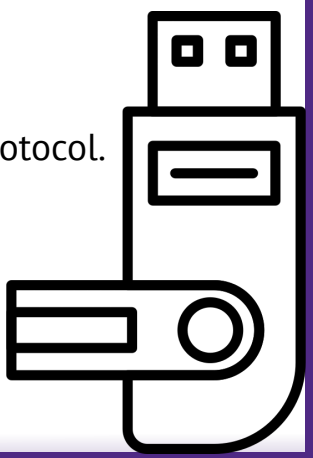
Security Awareness Theme

March Focus: Untrusted USB Drives

Untrusted USB Drives are not just storage tools; they can be programmed to act as Human Interface Devices (HID). When plugged in, the computer identifies the USB as a keyboard instead of a storage drive. This allows the drive to then input malicious commands at inhuman speeds to give threat actors access to your system or network. Beyond software-level attacks, "USB Killers" can also be used to permanently destroy hardware by delivering a high-voltage electrical surge through the data lines, physically frying the motherboard and rendering the entire computer unusable.

Practice Physical Discipline

- Never plug in a USB device found in a public place!
- If you find a lost device, turn it over to IT or Security personnel immediately without testing it.
- Conduct "USB Drop" simulations to test employee awareness and reinforce the policy that curiosity should never override security protocol.



Endpoint Detection and Response

- Utilize Endpoint Detection and Response tools to disable USB ports by default or restrict them to "Read-Only" mode for authorized, encrypted, company drives.

Sector-Specific Highlights

- **Healthcare:** Stryker Ransomware Attack - Stryker, a global medical technology giant was recently hit with a "wiper" ransomware attack, where instead of encrypting and leaking the data that was being held for ransom, the malware deleted it permanently. ***Prevention Tips:*** *Ensure you have up-to-date backups of important information segmented from production on your enterprise's network.*

- **Utilities/Industrial:** Dragos OT Cybersecurity Report - Dragos reports that threat groups are increasingly targeting industrial systems, moving beyond basic reconnaissance to attempts at real-world operational disruption. ***Prevention Tips:*** *Organizations should improve visibility into OT networks, limit remote access pathways, and monitor unusual activity that could indicate attackers moving from IT into operational systems.*

- **Education:** Wagon Mound Public Schools Data Leak – A new attack by the Interlock ransomware group hit the Wagon Mount Public Schools in New Mexico. Rather than just locking files, the group exfiltrated 80 GB of sensitive data, including staff/student passport numbers, residence addresses, and school architectural blueprints. ***Prevention Tips:*** *Implement checks for government-issued IDs for student enrollment to counter AI-synthetic identities.*

- **Public Safety/Financial:** US Executive Order 14390 - The White House issued a new order directing federal agencies to crack down on cybercrime networks responsible for financial fraud, ransomware, and impersonation scams. The initiative focuses on protecting vulnerable communities and improving coordination across law-enforcement and financial regulators. ***Prevention Tips:*** *Public safety and financial organizations should strengthen fraud-detection tools, verify user identities more rigorously, and share threat information with federal partners.*

Recommended Tools and Federal Resources

- NIST Vulnerability Metrics Calculator (CVSS Calculator)– Helps organizations evaluate the severity of software vulnerabilities using the Common Vulnerability Scoring System to better prioritize remediation efforts.
- NIST Computer Security Resource Center (CSRC) – Provides cybersecurity standards, guidelines, and best practices to help organizations improve security and manage cyber risk.
- NIST National Vulnerability Database (NVD) - Provides detailed information on publicly disclosed cybersecurity vulnerabilities to help organizations prioritize patching and risk mitigation.

Emerging Trends to Watch

- Token Theft and Session Hijacking in Cloud Services – Attackers are targeting authentication tokens to maintain access without repeated logins, bypassing traditional security controls. ***Prevention Tips:*** *Implement strong identity monitoring, shorten session lifetimes where possible, and monitor authentication logs for abnormal token use or unusual login patterns.*
- *Unauthorized Use of third-Party AI Tools (Shadow AI)* – Organizations face increased risk from employees using unapproved AI tools that may expose sensitive data. ***Prevention Tips:*** *Establish clear policies for approved AI tools, monitor data access and sharing, and provide training to employees on safe use of generative AI technologies.*
- *Malicious Browser Extensions* - Threat actors are distributing malicious browser extensions that can steal credentials, capture browsing activity, or inject malicious scripts into web sessions. These extensions often appear legitimate and are installed through official extension marketplaces. ***Prevention Tips:*** *Restrict installation of browser extensions through enterprise policies, review installed extensions regularly, and monitor for unusual browser-based authentication activity.*