CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** March 16th, 2025 - March 27th, 2026
Distribution: Public Sector Partners, Local Governments, IT Department *Volume 2 Issue 6*

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Cisco Secure Firewall RCE	Government, Finance, Healthcare	Insecure deserialization in the web interface of Cisco Secure Firewall Management Center allows unauthenticated root access.	Apply Cisco's March 11th patch, restrict management interface access to internal networks only.
ConnectWise ScreenConnect Privilege Escalation	IT-Managed Services, Education	An authentication bypass vulnerability was discovered in ConnectWise ScreenConnect where a threat actor server-level cryptographic material can obtain unauthorized access, including privilege escalation.	Update ScreenConnect instances to the latest security release and rotate all cryptographic keys and credentials.
Microsoft SharePoint Vulnerability	Government, Education, Healthcare, Enterprise Collaboration Services	A vulnerability in Microsoft SharePoint allows an attacker to execute code over the network by abusing unsafe data deserialization. During this reporting period, CISA added the flaw to its Known Exploited Vulnerabilities Catalog, indicating active exploitation.	Apply Microsoft's security updates for affected SharePoint versions as soon as possible, limit external exposure of on-premise SharePoint servers, and review logs for suspicious administrative or web requests.
Handala Threat Group	General	An Iranian-linked group focusing on psychological operations and hack-and-leak campaigns, with their most recent attack being on the Stryker Corporation. Handala primarily gains entry via compromised credentials. Once they have access, they issue remote-wipe commands through Microsoft Intune.	Configure Intune/UEM to require Multi-Admin Approval for bulk actions.
Medusa RaaS Group	General	Medusa is a Russia-based Ransomware-as-a-Service (RaaS) group known for its "double extortion" model and aggressive targeting of public safety and healthcare. They frequently use Initial Access Brokers to buy valid RDP credentials or exploit unpatched vulnerabilities in Remote Monitoring Management tools.	Implement strict offline backups and utilize Endpoint Detection and Response.

CERC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** Schneider Electric Plant iT/Brewmaxx - *CISA released an ICS advisory for Schneider Electric Plant iT/Brewmaxx identifying multiple vulnerabilities that could allow privilege escalation and potentially lead to remote code execution if exploited. These issues affect industrial control systems used in manufacturing and energy sectors, posing risks to operational environments.*
- **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.*

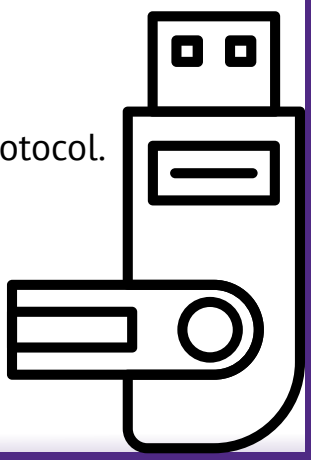
Security Awareness Theme

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:** [CISA Ugers Organizations to Harden Endpoint Management Systems] - Following the cyber-attack on the Stryker Corporation on March 11th, CISA has highlighted a critical vulnerability in healthcare supply chain. Concurrently, industry reports indicate that 50% of providers still lack adequate network segmentation for their Operational Technology. ***Prevention Tips:*** *Implement multi-admin approval for bulk actions in management consoles like Microsoft Intune.*

- **Utilities/Industrial:** [Targeting of OT Remote Management] - Water and wastewater utilities are seeing a surge in targeting of Cisco Secure Firewall Management Center (FMC) and ScreenConnect instances. NIST has officially initiated an overhaul of SP 800-82. ***Prevention Tips:*** *Utilities should immediately audit all internet-facing remote access tools.*

- **Education:** [K-12 Identity Gaps] – A recent report found that while 97% of school IT staff use MFA, only 13% of students are protected by it. This "Identity Gap" makes students the primary vector for credential-harvesting campaigns. ***Prevention Tips:*** *School systems should move toward a Zero-Trust model for student identity, prioritizing phishing-resistant MFA for older students and staff.*

- **Public Safety/Financial:** [Heightened Cyber Threats in Financial Services] - The New York State Department of Financial Services issued an alert to remind individuals and entities of the increased risk of cyber-attacks arising from ongoing global conflicts. ***Prevention Tips:*** *Financial institutions should enable number matching or challenge-responsive verification for MFA.*

Recommended Tools and Federal Resources

- CISA Logging Made Easy (LME) Guidance– Helps organizations improve logging practices to better detect, investigate, and respond to cybersecurity incidents.
- NIST Privacy Framework – Helps organizations identify and manage privacy risks while protecting sensitive data and supporting compliance efforts.
- CISA Secure by Design Initiative - Provides guidance to help organizations and software vendors build security into systems from the start rather than adding it later.

Emerging Trends to Watch

- Exploitation of Third-Party Plugins and Add-ons – Attackers are increasingly exploiting vulnerabilities in third-party plugins and add-ons to gain initial access or execute malicious code, often targeting components that are not regularly patched or monitored. . ***Prevention Tips:*** *Regularly update plugins, remove unused components, and monitor systems for unusual behavior tied to third-party integrations.*
- *Abuse of Remote Management Tools for Persistence*– Threat actors are using legitimate remote access and management tools to maintain persistence and control over compromised systems while blending in with normal administrative activity. ***Prevention Tips:*** *Restrict remote access tools, monitor for unusual remote sessions, and enforce least-privilege access controls.*
- *Exploitation of Backup Systems and Recovery Infrastructure* - Attackers are increasingly targeting backup systems to delete or disable recovery data before launching ransomware, preventing organizations from restoring systems without paying. ***Prevention Tips:*** *Secure backups with separate credentials, maintain offline or immutable backups, and regularly test recovery procedures.*