CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** January 16th, 2026 - February 1st
Distribution: Public Sector Partners, Local Governments, IT Departments *Volume 2 Issue 2*

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Desktop Window Manager	Information Technology	The Desktop Window Manager (DWM) allows a locally authenticated threat actor to extract protected data by abusing the handling of memory in the DWM.	Apply the security updates patch released by Microsoft on January 13, 2026.
Palo Alto Networks	Technology Infrastructure	A vulnerability in Palo Alto Networks PAN-OS software enables an unauthenticated attacker to cause a denial of service to the firewall. Repeated attempts to trigger this issue results in the firewall entering into maintenance mode.	Palo Alto has released an emergency patch to all effected versions of PAN-OS. If you believe you have a compromised version, visit Palo Alto's website and acquire their latest security patch.
Cisco OS Command Injection	Network Infrastructure	A vulnerability in the improper validation of user-supplied input in HTTP requests could allow unauthenticated remote attackers to execute arbitrary commands on the underlying operating system of an affected device through Cisco software.	Cisco has released a temporary solution as of January 22nd, and "strongly recommends that customers upgrade to the fixed software."
Chainlit AI SSRF Vulnerability	Cloud Services, AI Platforms, SaaS Providers	A Server-Side Request Forgery (SSRF) vulnerability in the Chainlit AI framework allows authenticated users to force the server to make unauthorized requests to internal or cloud metadata services.	Upgrade Chainlit to version 2.9.4 or later to remediate the vulnerability. Organizations should also enforce strict URL validation and restrict outbound network access from application servers.
APT28 Threat Actors	General	APT28 is a Russia-linked, state-sponsored cyber-espionage threat actor associated with the GRU that frequently targets government, defense, and public sector organizations. APT28 relies on phishing and legitimate admin tools to move through networks while blending in with normal activity.	Make sure any internet-facing devices are fully patched and properly configured and keep an eye out for unusual login activity or device behavior. Use multi-factor authentication whenever possible.

CERIAC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** CISA Publishes Five New Known Exploited Vulnerabilities to Catalog *The CISA published five new vulnerabilities to their KEV based on evidence of active exploitation. These types of vulnerabilities are frequent to attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.*
- **CISA ICS Medical Advisory:** American Hospital Association - Authentication Bypass *A critical authentication bypass vulnerability that allows administrative login to FortiNet hosted services. Following authentication via SSO, it has been observed that the actor creates a local admin account and downloads customer config files.*

Security Awareness Theme

February Focus: **Public Wi-Fi Networks**

Public Wi-Fi Networks that are usually found in cafes, airports, hotels, and even malls are usually convenient but often unsecured. This is because they usually lack strong encryption, making available for attackers to intercept data or trick user into connecting to malicious network.

Train yourself to **pause and inspect** before joining an open network.

Common Red Flags:

- Networks with **no password** required or **vague names (“Free_ Wifi”)**
- Duplicate Wi-Fi names with slight spelling differences
- Unexpected login pop-ups or security warnings
- HTTPS missing from websites
- Requests to install certificates or software

Action Tips to Stay Safe:

- Avoid logging into sensitive accounts (Email, Bank, etc)
- Disable auto-connect to open Wi-Fi networks
- Only visit websites with HTTPS
- Keep devices updated with security patches

Sector-Specific Highlights

- **Healthcare:** ShinyHunters Phishing Campaign - Over the past month, the ShinyHunters group has targeted over 100 organizations across the healthcare sector, using phishing and related access campaigns that lay groundwork for ransomware/data theft. ***Prevention Tips:*** *Companies should move toward phishing-resistant MFA and implement security keys where possible.*

- **Utilities/Industrial:** Joint Cybersecurity Advisory for Ransomware - U.S. agencies have reported ransomware actors exploiting unpatched remote monitoring software to compromise utility billing and management platforms, demonstrating a current threat to water/electric infrastructure. ***Prevention Tips:*** *Verify all remote monitoring software is up to date and enforce least-privilege access.*

- **Education:** Microsoft Ordered to Stop Tracking Children – Microsoft has been ordered by the Austrian Data Protection Authority to cease the use of tracking cookies in Microsoft 365 Education after it was found that Microsoft illegally installed cookies on the devices of a minor without consent. ***Prevention Tips:*** *IT Administrators should check the cookies installed on Microsoft 365 to ensure compliance with privacy standards.*

- **Public Safety/Financial:** Infostealers & Credential Theft Campaigns in Finance - Threat actors have been leveraging cross-platform languages such as Python in order to abuse trusted platforms and utilities to silently deliver credential-stealing malware at scale. Attackers are reported to have been weaponizing WhatsApp and PDF tools, focusing on the MSI installer that ultimately delivers the information stealer. ***Prevention Tips:*** *Use email filtering and sandboxing to stop malware-laden attachments and links. Monitor for unusual login locations or behavior and automate account lockouts.*

Recommended Tools and Federal Resources

- MS-ISAC – A free resource suite to help state and local governments build cybersecurity awareness and education programs.
- CISA Cross-Sector Cybersecurity Performance Goals (CPGs) – Prioritized best practices to help organizations reduce cybersecurity risk.
- NIST Cybersecurity Framework (CSF) 2.0 – A voluntary framework to help organizations manage and reduce cybersecurity risk.

Emerging Trends to Watch

- SSRF Exploitation of Cloud Metadata Services– Attackers increasingly abuse server-side request forgery (SSRF) to access internal cloud metadata services and steal credentials or sensitive configuration data. These attacks are harder to detect because traffic originates from normally trusted systems. ***Prevention Tips:*** *Restrict outbound access from application servers, allow-list URLs, and block cloud metadata endpoints where not required.*

- Exploitation of Internet-Facing Network Devices – Threat actors continue to target unpatched or misconfigured firewalls, VPNs, and edge devices to gain initial access to networks, particularly in government and critical infrastructure environments. Successful exploitation often enables long-term access with limited visibility. ***Prevention Tips:*** *Patch promptly, disable unused services, change default credentials, and monitor authentication logs for suspicious activity.*

- Abuse of Legitimate Administrative Tools ("Living off the Land") - Attackers increasingly use built-in tools such as PowerShell and remote management utilities to evade detection by blending in with normal administrative activity. This makes malicious behavior harder to distinguish from legitimate use. ***Prevention Tips:*** *Monitor unusual administrative tool usage, restrict privileged access, and enforce least-privilege controls with robust logging.*