CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** April 27th, 2026 - May 8th, 2026
Distribution: Public Sector Partners, Local Governments, IT Department *Volume 2 Issue 9*

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
WordPress Supply Chain Attack	Website Hosting Infrastructure	In 2025, a portfolio of 30+ WordPress plugins was sold. The buyer injected malicious code enabling a backdoor into every site with the plugin. The backdoor was activated in April of 2026, leading to a coordinated attack across world involving hundreds of thousands of sites. After header analysis on the initial email titled "Leak Test" the IP (45.130.41.9) of the domain host service traced back to St. Petersburg, Russia, suggesting this was an attack from a Russian cybercriminal group.	All of the plugins have been removed from the WordPress store, and an update disabling has been automatically pushed to all sites with the plugins.
Linux Kernel Zero-Day CopyFail	Technology Infrastructure	A proof-of-concept Zero-Day has been identified by Taeyang Lee. The logic bug in Linux kernel's authencesn cryptographic template allows an unprivileged local user to trigger a controller 4-byte write into the page cache of any readable file on the system.	Linus Torvald has released a patch for Linux kernels (a664bf3d603d).
cPanel & WHM Authentication Bypass	Web Hosting, Healthcare, Education	A proof-of-concept exploit has been published by security firm watchTowr. An attacker can manipulate the whostmgrsession cookie by omitting an expected segment of the value, avoiding the encryption process.	Restrict port exposure, especially on ports 2087 (WHM) and 2083 (cPanel). Immediately update cPanel and WHM to their most recent patches.
UAT-8302 APT	Energy, Government Infrastructure, National Defense	UAT-8302 is a China-linked advanced persistent threat group tracked by Cisco Talos, recently attributed to targeted attacks against government entities in South America and southeastern Europe.	Harden initial access points, audit PowerShell scripts and tasks, and protect Active Directory snapshots.
Tropic Trooper (APT23/Earth Centaur)	Healthcare, Manufacturing, Government	Tropic Trooper is a China-affiliated APT group that has recently pivoted to deploying a new attack chain using trojanized SumatraPDF documents and AdaptixC2 Beacon agents.	Block DLL sideloading, detect and disrupt persistent mechanisms, harden against the USBferry Air-Gap attack.

Important Government and ISAC Alerts

- **CISA ICS Advisories:** ABB Edgenius Management Portal - CISA issued this ICS Advisory on April 30, 2026, warning that the ABB Edgenius Management Portal versions 3.2.0.0 and 3.2.1.1 contain an authentication bypass vulnerability allowing for code execution, application uninstalling, and modification of configuration files.
- **CISA ICS Medical Advisory:** Grassroots DICOM (GDCM) Library - : CISA issued this ICS Medical Advisory warning that a memory leak vulnerability in the Grassroots DICOM (GDCM) library version 3.2.2, allows an unauthenticated remote attacker to send a specially crafted DICOM file that triggers massive memory allocations and resource depletion.

Security Awareness Theme

May Focus: Safe Data Handling & Transport

Safe data handling and transport focuses on how sensitive data is stored, accessed, shared, and moved both inside and outside of an organization. This includes everything from emails and company documents on the cloud, to transferring files via USB drives or 3rd party services. Even simple routine actions like sending an attachment or copying data to a personal device can introduce risk if not done securely. Breaches often don't come from sophisticated hacks, they come from simple mistakes like sending sensitive information to the wrong recipient, using unsecured file-sharing tools, or storing data in unapproved locations.

Limit Access

- Share and store data using company-approved platforms with built-in security controls.
- Only share data with individuals who genuinely need it for their task/job.
- Avoid broad or public sharing links.

Know your data!

- Understand what information is sensitive and treat it accordingly.
- Avoid personal devices and accounts. Do not transfer or store work data on personal USB drives, email accounts, or cloud services.
- Use encryption when transmitting or storing confidential information, especially outside the organization.

Sector-Specific Highlights

- **Healthcare: Medtronic Data Breach**- In April 2026, Medtronic confirmed a breach of corporate IT systems after the ShinyHunters group claimed to steal millions of records and internal data. ***Prevention Tips:*** *Healthcare tech organizations should separate corporate and operational networks to limit the impact of breaches and maintain strong incident response and disclosure plans.*

- **Utilities/Industrial:** Legacy ICS Systems Being Targeted - Legacy industrial control systems are increasingly vulnerable to modern cyberattacks, prompting CISA to urge organizations to prepare for cyber outages. ***Prevention Tips:*** *Enforce strict IT/OT network segmentation with monitored boundary points to detect and contain lateral movement before it reaches control systems.*

- **Education:** Confidence Drop in Education Sector Cyber Readiness – The 2026 NASCIO-Deloitte Cybersecurity Study found declining confidence in local government and public higher education cybersecurity as attackers increasingly target public sector systems for ransom and disruption. ***Prevention Tips:*** *State CISOs are centralizing cybersecurity support, and schools should work with them to share threat intelligence and incident response resources.*

- **Public Safety/Financial:** Frost & Citizens Bank Data Breach - In April 2026, the Everest ransomware group compromised a shared vendor, exposing millions of records from Frost Bank and Citizens Financial Group and triggering multiple lawsuits. ***Prevention Tips:*** *Financial institutions should strengthen third-party risk management and use phishing-resistant MFA to reduce vendor-related breaches.*

Recommended Tools and Federal Resources

- CISA Known Exploited Vulnerabilities – A catalog of vulnerabilities confirmed to have been exploited in the wild, intended to help organizations prioritize remediation within their vulnerability management programs.
- CISA No-Cost Cybersecurity Services – A database of free cybersecurity services and tools to help organizations reduce cybersecurity risk.
- NIST AI Risk Management Framework (AI RMF) - A concept note guiding critical infrastructure operators on managing risks in AI-enabled systems.

Emerging Trends to Watch

- *Agentic AI Hijacking* – Threat actors are now deploying adaptive autonomous agents capable of rewriting their own code in real time, targeting Model Context Protocol (MCP) servers, a key integration layer for enterprise AI, where a single misconfigured server can give an attacker control over every connected AI agent. ***Prevention Tips:*** *Strong identity controls, network segmentation, and behavior-based detection must be consistently applied, and incident response plans must account for autonomous retry and adaptation since agentic attackers do not stop after a failed attempt.*
- *AI-Powered Deepfake Social Engineering* – Deepfake scams surged in 2025, with AI voice cloning now enabling attackers to impersonate executives and officials to commit fraud and gain system access. ***Prevention Tips:*** *Organizations should use multi-channel verification and train employees to detect AI-generated deepfakes and impersonation attacks.*
- *Software Supply Chain Cascade Attacks* - Adversaries are increasingly targeting trusted integrations and interconnected systems, with supply chain attacks quadrupling over the past five years and taking an average of 267 days to detect and contain. ***Prevention Tips:*** *Organizations must strengthen identity protection, third-party monitoring, and vendor risk management since one compromised supplier can disrupt entire industries.*