CEROC SENTINEL
CYBERSECURITY EDUCATION, RESEARCH AND OUTREACH CENTER

The Official Cyber Threat Newsletter from the CEROC Student-led Security Operations Center

Prepared by: CEROC Student SOC **Date Range:** July 1st - July 18th, 2025 **Distribution:** Public Sector Partners, Regional EMA's, IT Departments

Volume 1 Issue 3

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Wave of ICS Vulnerabilities Identified by CISA (7/10, 7/15)	All Sectors	CISA issued 19 new advisories covering ICS systems from vendors such as Siemens, Hitachi, LITEON, and more. Flaws range from weak authentication to code execution risks in energy, manufacturing, and automation environments.	Review the July 10th and July 15th advisories. Patch affected devices, restrict access, and monitor industrial networks for unusual activity.
FBI Alert: Scammers Impersonating Health Fraud Investigators	Healthcare, Public Safety	Cyber criminals are posing as health insurance agents via fake emails and texts, tricking users into revealing sensitive medical and financial information. These scams are targeting both patients and providers.	Be cautious with unexpected messages. Don't share personal info without verification. Enable MFA and report suspicious communications to your provider.
Facebook Malware Campaign Targets Cryptocurrency Users	All Sectors	Attackers launched a global scam using fake Pi Network ads on Facebook, stealing wallet recovery phrases and installing malware disguised as crypto apps. Over 140 fake ads detected so far.	Don't click on crypto ads or enter wallet phrases online. Only download apps from official stores. Use antivirus software and hardware wallets when possible.
FortiWeb SQL Injection Vulnerability Identified	All Sectors	A severe SQL injection flaw was discovered in Fortinet's FortiWeb firewall, potentially allowing attackers to take control of protected web servers. No active exploitation has been confirmed.	If using FortiWeb versions 7.0-7.6, apply the latest updates immediately. Audit web access logs and restrict admin access.
CISA issues advisory for flaw in train remote brake systems	Transportation, Industrial	CISA has identified a flaw affecting End-of-Train and Head-of-Train devices in remote brake control systems. Attackers could potentially send fake brake commands to a train, causing disruptions to the braking systems and operations.	Isolate critical train systems from internet and business networks and use firewalls to block unauthorized access. Reach out to device manufacturers for updates and support. Only allow remote access through secure methods.

CERIAC
Cybersecurity Education, Research and Outreach Center
SENTINEL

Important Government and ISAC Alerts

- **CISA ICS Advisory:** High-Severity Vulnerabilities in Hitachi Energy Asset Suite – *CISA has issued a warning about multiple serious flaws in Hitachi Energy's Asset Suite products. These vulnerabilities could let attackers gain unauthorized access, escalate privileges, or run remote code on critical systems.*
- **CISA ISC Advisory:** High-Severity Vulnerability in LITEON EV Chargers – *CISA has issued an advisory regarding LITEON IC48A and IC80A EV Chargers where FTP server access credentials are stored in plaintext. Exploitation could allow attackers access to sensitive information when accessing the chargers.*

Security Awareness Theme

July Focus: Strong Passwords and MFA

Weak or reused passwords are still one of the easiest ways hackers gain access to your personal and professional accounts. Strong password habits paired with multi-factor authentication (MFA) are critical to keeping your data safe.

Password tips:

- Use strong, unique passwords for every account
- A strong password is at least 12+ characters and uses a mix of letters, symbols, and numbers.
- Use a password manager to store and generate secure passwords
- Regularly check for compromised credentials (Google Password Checkup, Firefox Monitor)

What is MFA?

Multi-factor authentication, also called two-factor authentication (2FA), helps keep accounts and data secure by adding a **second layer of protection**. Alongside the password, you are also required to authenticate using a second method such as a **one-time code** sent to your phone or email, **a bio-metric key** such as fingerprint or face ID, or **a physical device** such as a security key. Most major apps and websites now have MFA integrated and have made it easy to activate through settings.

Sector-Specific Highlights

- **Healthcare:** Episource Ransomware Attack Affects 5.4+ Million - Episource LLC suffered a major ransomware breach compromising personal and medical data of over 5.4 million individuals. Affected data includes diagnoses, prescriptions, insurance info, and Medicare/Medicaid IDs.
- **Utilities:** EPA issues Cyber Alert for Water Facilities – The EPA and DHS are warning utility operators of likely cyberattacks by pro-Iranian hacktivists targeting U.S. water infrastructure. Past incidents show attackers exploiting OT systems to force manual operation. ***Prevention Tips:*** *Disconnect OT devices from public-facing internet, replace default passwords, and enable MFA for remote access.*
- **Education:** Weak Passwords Plague Education Sector – A new report highlights widespread use of weak credentials in school and universities, and has experts warning that weak passwords leave millions of student and staff records vulnerable. ***Prevention Tips:*** *Require 12+ character passwords, deploy password managers for faculty and staff, audit login practices, and use MFA.*
- **Public Safety:** Cyberattacks on Emergency Services Spike – The PSTA and MS-ISAC report a 60% rise in cyberattacks on systems like 911 centers, CAD systems, and public safety radios. Ransomware has quadrupled, with average downtime reaching 15 days per incident. ***Prevention Tips:*** *Segment internal systems to contain threats, modernize outdated tech, tighten access controls, and join threat-sharing networks to stay up-to-date on attacks.*

Recommended Tools and Federal Resources

- CISA Shields Up – Up-to-date guidance on active threats and protection strategies for all organizations.
- CIS Benchmarks – Free, expert-developed security configuration guidelines for operating systems and apps.
- HC3 Healthcare Cybersecurity Resources – Security info tailored to healthcare providers, including threat briefings and alerts.

Emerging Trends to Watch

- 35% Surge in Infostealer Malware Attacks – Infostealer malware (malware that steals passwords, browser data, and sensitive information) is on the rise and has increased by 35% globally. These attacks often enter systems through phishing emails, malicious websites, outdated software, or pirated apps. ***Prevention Tips:*** *Watch for unusual login activity or sudden password resets. Enforce MFA, deploy strong antivirus tools, and conduct anti-phishing campaigns.*

- Linux Servers Face 56% Increase in Cyberattacks - Cyber threats targeting Linux servers, which power much of the cloud and web infrastructure, have jumped by 56% in 2025. Attackers exploit unpatched vulnerabilities to deploy malware, launch DDoS attacks, or steal data. ***Prevention Tips:*** *Regularly update Linux systems/software and implement firewalls to monitor for unusual traffic.*

- Deepfakes Drive Sophisticated Social Engineering– Scammers are now using AI-powered deepfake audio and video to impersonate executives and public figures in real time, especially during video calls or phone-based phishing. These fake interactions can fool staff into wiring funds or revealing credentials. ***Prevention Tips:*** *Require multi-channel verification for any fund transfers or account changes. Monitor for anomalous behavior during meetings or calls.*

CEROC SENTINEL

Contact cerocssoc@tntech.edu for questions or concerns regarding cyber news.