CEROC
Cybersecurity Education, Research and Outreach Center
SENTINEL

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

Prepared by: CEROC Student SOC **Date Range:** June 7th – June 30th, 2025 **Distribution:** Public Sector Partners, Local EMA's, IT Departments

Volume 1 Issue 2

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Zero-Day Vulnerability in Google Chrome (CVE-2025-5419)	All Sectors	A serious flaw in Chrome's V8 engine is being actively exploited. Hackers can trick users into visiting a malicious webpage, giving them control of the browser. Chromium-based browsers like Edge and Brave may also be affected.	Update Chrome to version 137.0.7151.68 or newer immediately. Check your current version by going to *chrome://settings/help* in the browser. Enable auto-updates for any Chromium-based browsers.
Roundcube Webmail Remote Code Execution (CVE-2025-49113)	Government, Education, Public Sector	A 10-year-old flaw found in Roundcube email software lets attackers take over servers if they gain access. Exploits are already available online.	Upgrade Roundcube to 1.6.11. Restrict admin/webmail interfaces to trusted IPs. Use strong passwords and enable MFA. Monitor for strange session behavior.
Ransomware Exploiting SimpleHelp RMM (CVE-2024-57727)	Utilities, IT, Critical Infrastructure	Hackers are using unpatched SimpleHelp software to install ransomware targeting IT and billing systems. The flaw allows unauthorized server file access and affects versions 5.5.7 and earlier.	Upgrade to the latest SimpleHelp version. Remove outdated installs, monitor systems for intrusion signs, and secure network configurations.
FBI Alert: BADBOX 2.0 Targeting Smart Devices	All Sectors	Cybercriminals are pre-installing malware in smart home and car devices that creates secret backdoors into home networks. Some devices may already be infected before purchase.	Avoid unknown or unofficial device brands. Do not disable security features like Google Play Protect. Monitor your network for strange traffic. Only buy from trusted vendors.
CISA ICS Advisories – Siemens and AVEVA Flaws	Industrial, Energy, Manufacturing	Multiple critical bugs in ICS software from Siemens and AVEVA allow attackers to take control of devices or crash them. Some use default passwords or give guest users too much access.	Patch affected Siemens and AVEVA devices immediately. Remove guest access, keep ICS systems isolated from other networks, and change default credentials. Review CISA alert for full details.

CERIAC
Cybersecurity Education, Research and Outreach Center
SENTINEL

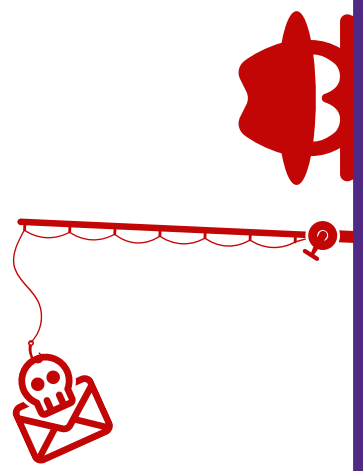
Important Government and ISAC Alerts

- **CISA ICS Advisory:** Siemens Energy Services – *CISA has issued a high-severity advisory about a flaw in Siemens Energy Services equipment that could allow attackers to remotely control energy output systems. The vulnerability exists in the G5DFR component, which uses default credentials that are rarely changed.*
- **CISA Alert:** SinoTrack GPS Devices – *CISA warns that SinoTrack GPS devices used in vehicles are highly vulnerable to attacks due to weak and well known login credentials. Some models allow remote disabling of fuel systems. Organizations with fleet vehicles could have their movements tracked or operations disrupted remotely.*

Security Awareness Theme

June Focus: Phishing Emails

Phishing emails can often appear to come from trusted companies like banks, utility providers, or government agencies. They may try to trick you into clicking malicious links or sharing personal information.
Train employees to **pause and inspect** before clicking.



Common Red Flags:

- Generic greetings (“Dear user”)
- Claims of an urgent or time-sensitive issue
- Encourages you to click a link or open an attachment
- Offers monetary rewards or prizes
- Claims of account or billing issues

Action tips:

- Hover over links to preview the real URL
- Keep security software up-to-date
- Report or delete suspicious emails

Current Threat:

- A phishing kit called EvilProxy has resurfaced
- Sends fake Microsoft 365 and Upwork emails
- Tricks users into visiting fake login pages

Sector-Specific Highlights

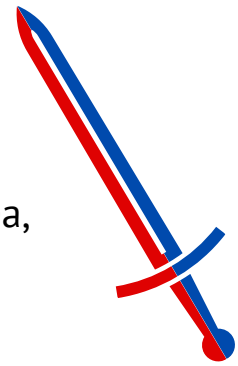
- **Healthcare:** Federal Cyber Cuts Raise Concerns – Recent proposals under the Trump Administration include $500 million in cuts to CISA and reductions across key agencies like HHS and NSC. Various cyber advisory board and committees have also been eliminated or downsized.
- **Utilities/Industrial:** Chinese "Kill Switches" found in Solar Equipment – Hidden cellular radios and components were found in Chinese-made solar inverters and batteries. These devices weren't disclosed in documentation and may allow remote system shutdowns. ***Prevention Tips:*** *Work with energy vendors to validate hardware security and disable undocumented radios or communication ports.*
- **Education:** Cyberattack at Columbia University – A cyberattack at Columbia University caused an outage of all systems requiring a university ID and resulted in over 400 GB of stolen data. Higher education institutes have become a more common target of cyberattacks due in part to the wealth of personal info and research data in their systems.
- **Public Safety/Financial:** FBI & CISA: Surge in Play Ransomware Attacks – Over 900 organizations have been recently hit by Play Ransomware. Victims often receive follow-up phone threats, and payment instructions are given via direct contact, bypassing traditional ransom notes. ***Prevention Tips:*** *Enforce strong passwords and MFA, keep software and devices updated, segment networks and block unused ports.*

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

Artificial Intelligence: A double-edged sword



- AI Platforms Actively Disrupting Threat Actor Activity – OpenAI has shared details of how threat actors tried to misuse AI tools for fraud, malware, and misinformation – highlighting activity from North Korea, China, and Russia.

- AI-Powered Hacking Tools on the Rise –Hackers are using bots to scan for weak spots such as outdated software or reused passwords. Automated scanning has increased with 36,000 scans per second recorded globally. ***Prevention Tips:*** *Enforce multi-factor authentication, set account lockouts after too many failed logins, and keep systems fully updated.*

Zero Trust Moves from Concept to Action

- Zero Trust is a network model that helps stop insider threats and unauthorized access. NIST has released SP 1800-35, a hands-on guide to implementing Zero Trust Architecture with 19 real-world examples. It emphasizes inventorying assets, enforcing access policies, and continuous monitoring.

CEROC SENTINEL

Next month's Security Awareness Theme: Strong passwords and Multi-Factor Authentication (MFA)