CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** July 11th - July 24th
Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 14

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
OpenAI model escapes sandbox and breaches Hugging Face	Manufacturing, Technology	OpenAI models including GPT-5.6 Sol and other prerelease models compromised the infrastructure of Hugging Face last week without any human interaction. The reason these models were able to breach without human interaction was due to them being on reduced cyber refusals for evaluation purposes.	Strengthen system sensors on edge devices and other vulnerable locations to prevent possible future breaches by automated attacks.
SonicWall Zero-Days Exploited Before Disclosure	Government, Healthcare, Financial	Two Zero-Day vulnerabilities within SonicWall were exploited by a previously undocumented threat actor. The two vulnerabilities are CVE-2026-15409 and CVE-2026-15410. Using these vulnerabilities the threat actor was able to gain root access, but evidence shows that the threat actor was less successful in moving laterally or gaining access to other systems.	For SMA1000 Models – 6210, 7210, 8200v; update to 12.4.3-03453 (platform-hotfix) and higher versions, or 12.5.0-02835 (platform-hotfix) and higher versions.
AWS Kiro Flaw Allows a Poisoned Web Page to Rewrite Config and Run Code	Enterprise, Technology, Government	A flaw within AWS's agentic coding IDE can allow a malicious web page to rewrite the config file and run an attackers code on a developers machine with no approval steps. This could come from a developer asking something as simple as a summary of a page.	AWS has patched the issue with no CVE being attached, but similar issues may appear in future agentic coding IDE's.

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
FakeGit	Technology, Enterprise	FakeGit is an attack campaign involving nearly 7,600 malicious GitHub repositories which deliver a malware family known as SmartLoader. FakeGit copies notable projects, creates lookalike developer profiles and convincing READMEs to deliver SmartLoader malware.	Scrutinize any github repositories before pulling or running anything.
Russian Intelligence Spies on Ukraine by Hacking Security Cameras	Government, Military	At least one Russian intelligence service is hacking into internet-connected security cameras across Europe and Ukraine to spy on military supply routes. Access is gained by scanning the internet for exposed devices that have IP's that match cameras by brand, then either accessing ones that are using default credentials or ones that have unpatched vulnerabilities.	Find what is exposed to the internet and check to see if exposed cameras may have access in logs that you do not recognize. Keep video stream off the internet, replace default credentials and patch firmware and software.

CERIAC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** NASA Core Flight System (cFS) Health & Safety (HS) Application- CVE-2026-1532 is a vulnerability affecting v37.5 of NASA Core Flight System Health & Safety. Successful exploitation of this vulnerability could allow denial-of-service.
- **CISA ICS Medical Advisory:** pyndicom pynetdicom Library- CVE-2026-56445 is a vulnerability that stems from improper limitation of a pathname to a restricted directory. Successful exploitation of this vulnerability could allow an attacker to write to arbitrary file paths

Security Awareness Theme

July Focus: Spear Phishing Attacks

Like a standard phishing attack, a spear phishing attack is a social engineering tactic that attempts to get you to click on a link, enter credentials, or install a file that you would not otherwise interact with. Unlike a standard phishing attack, a spear phishing attack is directly targeted at you or a small group of people and typically has a much higher success rate due to its targeted nature. Bad actors may use OSINT techniques to gather information on your work, organizations, or hobbies to create a convincing message or offer exclusive opportunities, or they may gain access to a trusted account, such as a friend or coworker's, and use that account to perform a spear phishing attack. Spear phishing attacks are now being automated using AI techniques, allowing threat actors to more easily create incredibly convincing messages, or even generate deepfake video or voice messages.

Warning signs

- Requests to move platforms
- Asking for login credentials
- Sending files
- Person acting differently than they normally would

Protect yourself against spear phishing attacks

- Scrutinize all messages received, even from trusted sources
- Report any suspected breached accounts to your IT department
- Notify others who may be hit by a similar spear phishing attack

Sector-Specific Highlights

- **Healthcare: Craneware Cyberattack Exposes Customer and Employee Data** - Healthcare software provider Craneware disclosed a cyberattack that resulted in the exfiltration of customer and employee data. The incident highlights the continuous rise in healthcare supply-chain attacks, where compromising a single vendor can impact thousands of healthcare organizations.
- **Prevention Tips:** Healthcare organizations should strengthen third-party risk management, enforce MFA, promptly patch systems, and regularly review vendor access.

- **Utilities/Industrial: Coca-Cola's fairlife Halts U.S. Production Following Cyberattack-** Coca-Cola owned dairy producer fairlife temporarily halted production at the U.S. manufacturing facilities after a ransomware attack disrupted production related systems. The company stated that product safety and quality were not affected, but operations were suspended while systems were restored.
- **Prevention Tips:** Manufacturing organizations should segment IT and operational technology networks, enforce multi-factor authentication, maintain offline and regularly tested backups, and continuously monitor for suspicious activity.

- **Education: Reynella East College Restores Systems Following Ransomware Attack** – Reynella East College experienced a ransomware attack in June that disrupted school operations and resulted in the theft of approximately 610GB of data. The Interlock ransomware group claimed responsibility and published stolen data as a part of a double-extortion campaign. The school eventually restored its systems after remediation efforts and implemented security updates and patches while working with government agencies.
- **Prevention Tips:** Educational institutions should enforce multi-factor authentication (MFA), maintain offline backups, patch systems, and provide phishing awareness training for faculty and students.

- **Public Safety/Financial: Agentic AI automatically runs recon, phishing, and malware without humans** - Threat actors no longer need hands on the wheel to perform attacks, as agentic AI has gained full automation. This also drops the need of skill for attackers, which will drastically increase the rate of attacks.
- **Prevention Tips:** Currently, without human intervention it is expected that most of the AI models will perform similar style attacks without variance. Understanding how the AI will attack and strengthening against those attacks may prevent against the quantity of attacks.

Recommended Tools and Federal Resources

- CIS Configuration Assessment Tool (CIS CAT Lite) – Assesses systems against the CIS benchmarks to identify security configuration weaknesses and improve compliance with industry best practices

- CISA Cyber Hygiene Services - Provides free vulnerability scanning and web application assessments to help organizations identify and remediate security weaknesses before they can be exploited.

- PhishTank - A community ran URL database which allows users to submit known phishing links. Community members also vote on the legitimacy of the links, so there may be false positives.

Emerging Trends to Watch

- **Improve Router Hygiene to Protect Against Russian State-Sponsored Targeting:** Threat actors are increasingly targeting internet-facing routers and network appliances to gain initial access using weak credentials, exposed management interfaces, and outdated firmware remain common attack vectors. It is recommended to keep routers and network appliances updated with the latest vendor firmware, disable internet-exposed management interfaces when possible, and replace default credentials with strong, unique passwords.

- **Surge in Actively Exploited Known Vulnerabilities (KEV):** CISA added several newly exploited vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog, highlighting attacker's continued focus on rapidly exploiting new disclosed flaws in internet-facing systems. Prioritize patching of KEV-listed vulnerabilities, regularly scan internet-facing assets, and use compensating controls such as web application firewalls, network segmentation, and enhancing monitoring until patches can be applied.

- **AI Hallucinations lead to Phantom Typo-Squatted Websites:** Large language models (LLMs) can occasionally hallucinate website URLs that do not actually exist. Threat actors are beginning to register these nonexistent domains and populate them with malicious content, allowing users who trust AI-generated links to unknowingly visit phishing pages, malware-hosting sites, or other scams. When AI generates links, verify their legitimacy before visiting them, especially before entering any credentials or sensitive information, or if there are any downloads.