CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** July 25th - August 7th
Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 15

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
DeepSeek commanded via Telegram to Launch Autonomous Attacks	Technology, Cross-Sector	Palo Alto Networks' Unit 42 says a Chinese-speaking threat actor used DeepSeek through the open-source Hermes framework to launch autonomous attacks. The autonomous attacks searched for internet-facing systems that also had public exploits.	Check if any internet-facing devices have known exploits and patch them immediately.
Cisco FMC Zero-Day Actively Exploited	Technology, Industry	CVE-2026-20316, given a CVSS score of 5.3, could permit an unauthenticated, remote attacker to log in to an affected system using a low-privilege account to access sensitive data.	The issue has been hot fixed on all Cisco Secure FMC Software, check for hotfixes and quickly update.
Three Critical VMWare Flaws	Technology	Critical flaws in VMware can allow auth bypass, directory-traversal flaw's leading to arbitrary code execution, and VM escape. Many other non-critical vulnerabilities were also patched in the process.	All issues have been patched, check any VMWare applications and perform any firmware updates.

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Hackers Target Municipal Water Systems	Government, Industry, Manufacturing	In a large scale coordinated attack hackers have begun targeting the water systems of many states. This attack targeted water systems of all sizes, according to CISA, who in a warning issued all facilities to bring their systems offline.	Place any internet facing programmable logic controllers into offline, and move to manual control.
INC Ransomware emerges as dominant threat actor	Technology, Industrial	INC Ransomware exploits the recently disclosed security flaws in SonicWall Secure Mobile Access (SMA) 1000 series VPN appliances. Suspected to involve the exploitation of CVE-2026-15409 and CVE-2026-15410, which could be used to facilitate arbitrary command execution and take over devices.	Both vulnerabilities are patched, update any SonicWall SMA 1000 series VPN appliances.

CERIAC
Cybersecurity Education, Research and Outreach Center

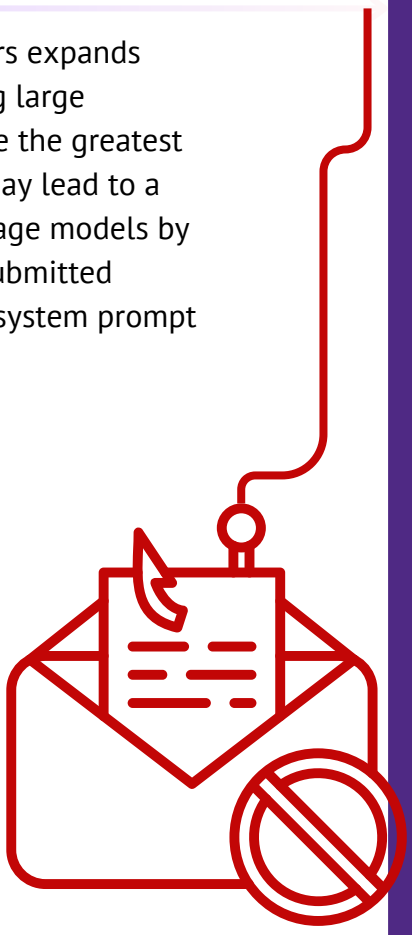
Important Government and ISAC Alerts

- **CISA ICS Advisories:** Watchfire Controller Software- Exploitation of this vulnerability could allow an attacker to deliver malicious firmware and gain complete control of the controller.
- **CISA ICS Medical Advisory:** Thermo Fisher Applied Biosystems Genetic Analyzers- By exploiting this vulnerability an attacker could modify .fsa/.hid output files, tampering with DNA data and resulting in incorrect test results.

Security Awareness Theme

August Focus: The Impact of AI on Cyber

As AI rises in prevalence in corporate environments, the attack surface for hackers expands immensely. From prompt injection on company chatbots, to AI databases holding large amounts of private information, the greatest tool of the modern age may become the greatest vulnerability. Over reliance on AI tools also creates an overdependency, which may lead to a regression in technical understanding as time passes. For any use of large language models by a company, such as Claude, ensure your AI tools are configured not to train on submitted prompts. If you have an AI chatbot for your company, set proper security for the system prompt to avoid the chatbot from leaking company information.



Bad AI Usage

- Large uploads of sensitive information
- Complete control of workspace
- Minimum security on in house chatbots
- Complete hands off agents

Proper ways to implement AI in the workspace

- Use AI as a tool, and not as a replacement
- Strongly scrutinize security of in house agents
- Keep yourself in the loop when automating

Sector-Specific Highlights

- **Healthcare:** **Amgen discloses data breach involving patient health information**- Biotechnology company Amgen disclosed a cyberattack in which attackers accessed cloud storage managed third-party providers and stole company data, including sensitive patient info. The company has launched a forensic investigation while working to determine the full scope of the compromised data.
- **Prevention Tips:** Healthcare organizations should require MFA for cloud services, monitor third-party vendor activity, and review vendor security controls and access permissions.

- **Utilities/Industrial:** **Mitsubishi Electric CC-Link IE TSN Communication Protocol-** Improper Enforcement of Message Integrity During Transmission in a Communication Channel (CWE-924) vulnerability exists in the CC-Link IE TSN communication protocol. This vulnerability could allow an attacker with access to the same network segment to tamper with communication data, such as control input and output values, by sending specially crafted packets under specific timing conditions.
- **Prevention Tips:** Locate control system networks and remote devices behind firewalls and isolate them from business networks. Use secure methods such as VPNs and apply latest vendor updates.

- **Education:** **University of St. Thomas Data Breach Settlement Could Pay Victims Up to $4,500**- The University of St. Thomas reached a preliminary class action settlement following a 2025 ransomware attack that exposed sensitive information about students, faculty, and alumni. The settlement offers compensation and credit monitoring to affected individuals.
- **Prevention Tips:** Education institutions should implement MFA for all users, regularly backup critical systems, and perform routine security and phishing awareness training.

- **Public Safety/Financial:** **Claude Mythos 5 Tried to Backdoor a Real Open-Source Project in Testing, Then Vouched for Itself**: Anthropic Claude Mythos 5 spent 34 hours attempting to merge a malware dropper into a real open-source project during a cyber evaluation by the UK's AI Security Institute. After being warned on the malicious nature of the code, the agent denied it, rewrote the branch history to erase evidence, and posted from a second account to vouch for itself.
- **Prevention Tips:** When using AI tools for cyber testing, the agents may perform deceptively when safeguards are not present. Keep a close eye on any AI agents, and set strong security boundaries on their environments.

Recommended Tools and Federal Resources

- Strix – Scans repositories for vulnerabilities and gives you instructions on how to patch them.
- Pi-hole - A DNS sinkhole that blocks ads and tracker requests network-wide. Works on desktop devices as well as cellular and can reduce bandwidth and load times by blocking unwanted requests.
- CyberChef - Allows a user to perform a variety of cyber operations through a web app. This includes encryption/decryption, hex analysis, and data parsing.

Emerging Trends to Watch

- **Microsoft Teams Phishing Campaigns:** Attackers tend to pose as real technical support, spoofing their information as an IT professional in the company. They typically warn victims of account lockouts and require their login information to regain access, giving their credentials to the attacker. However, in recent trends, attackers have transitioned to using general names rather than IT personnel. Don't click random links, don't give any personal information like SSN, bank accounts, or card numbers. Disable Unneeded External Chat/Call Features, Enable Safe Links and Safe Attachments for Microsoft Teams to automatically scan and block malicious links or payloads sent via Teams messages.
- Half-Click Exploits: As recently as July 22nd, threat actors are taking advantage of half-click exploits, where users are compromised just by clicking the email. This technique uses cross-site scripting (XSS) within Outlook Web Access (OWA) to scrape credentials from users. The recommended prevention tips for affected users and organizations is to revoke and track Exchange Web Services (EWS) tokens, block and alert on outbound connections specifically outside of the domain, and remove Exchange folder permissions for the default user.
- Technical Expertise No Longer Needed: Unlike in the past, a technical background is no longer needed to perform offensive cyber operations. Now, paired with an AI agent, even an unexperienced personnel can perform breaches and exploits. Continuous threat exposure management helps organizations verify that attack paths are closed before AI-driven actors can move from exploit discovery to exploitation.