

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** August 22nd - September 4th

Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 17

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
CISA Adds Seven Exploited Flaws to Catalog	AI Infrastructure	CISA has added known exploited vulnerabilities to their catalog that have a range of CVSS 6.5 to CVSS 10.0. These exploits have been used to deploy a reverse shell and crypto miners on targeted systems. These attacks have been specifically aimed towards AI servers as API keys have become a lucrative target.	All of the exploits being used in these hacks have been patched. Check your systems to see if you are running anything with known vulnerabilities, then update systems as needed.
Exploited JFrog Flaw Allows Attackers to Mint Admin Tokens	Technology, Finances, Healthcare	A critical flaw in JFrog Artifactory allows a threat actor to bypass authentication and gain complete administrative access to the system. Due to the complete access this vulnerability gives to the threat actor, CVE-2026-82329 was given a CVSS score of 9.8.	This vulnerability was patched by JFrog with Artifactory version 7.161.20. If you are using JFrog Artifactory and have not updated since August 28 th , update your systems.
PaperCut flaws allow attackers to execute code without authentication	Education, Healthcare, Retail, IT services	Two vulnerabilities have been discovered in PaperCut NG and MF that allow attackers to bypass authentication and execute arbitrary java code inside the application's process. According to PaperCut, attackers are making use of CVE-2026-81578 to bypass authentication, allowing them to edit configuration files to exploit CVE-2026-82078 and gain Remote Code Execution.	PaperCut is currently investigating active exploitation of these vulnerabilities. For now, they recommend installing the most recent emergency patch and restricting web access to the application server to only trusted IP addresses

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Akira Ransomware Continues Threat on Industries	Manufacturing, Professional Services, Finance, and Technology	Akira Ransomware, who appeared in March of 2023, have continued applying their skills as a ransomware-as-a-service group. Their most recent attack was against CGP MEP, a London based building services consultancy, where they listed 260 GB of sensitive data on their leaks website. They are notable for exploiting edge vulnerabilities in systems, then after gaining access they can go from initial access to exfiltration with extreme speeds.	Patching edge devices that have known vulnerabilities greatly decreases the risk factor posed by Akira Ransomware. If MFA is compromised, reset any MFA credentials.
Qilin Performs Data Exfiltration on ATF	Manufacturing, Healthcare, Technology	Qilin is a Russia-linked ransomware-as-a-service group that has been active since mid-2022. Their most recent attack was against the Bureau of Alcohol Tobacco, Firearms and Explosives, where they claimed responsibility and posted approximately 6.3 gigabytes of highly sensitive data. Qilin mainly gains access through phishing techniques or exposing vulnerable edge devices. Once in, Qilin uses double extortion and advanced rust based payloads.	Train employees on avoiding phishing techniques. Perform timely patches and vulnerability mitigation, and deploy advanced endpoint detection and response solutions.



Important Government and ISAC Alerts

-  **CISA ICS Advisories: [All-Line Equipment Company Fuel-Boss](#)**- An attacker can exploit improper neutralization of argument delimiters in a command or buffer copy without checking size of input to execute arbitrary commands or code remotely on affected systems.
-  **CISA ICS Medical Advisory: [Pulsetto Vagus Nerve Stimulator](#)**- CVE-2026-18844 allows an adversary to use hidden commands to disable electrical safety mechanisms or modify other settings. These hidden commands are sent over bluetooth, and are sent without authentication or encryption, yet are fully processed when the device is powered on.



Security Awareness Theme

August Focus: Rogue AI Agents

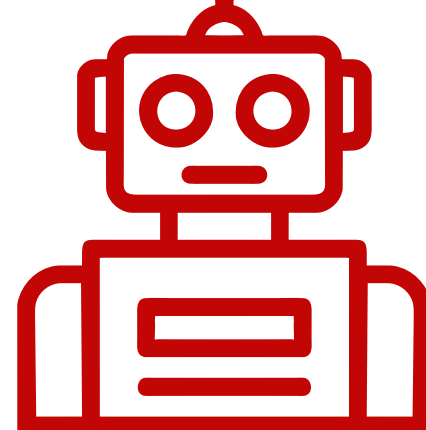
As AI models become more powerful, and research projects become more intense, the possibility of rogue AI agents becomes more of a reality. An AI agent is considered rogue when it judges that an action, even if it violates its original scope or rules, progresses it towards its goal and performs that action anyways; agents going rogue can possibly cause harm to the testing environment, or the agent may breach the testing environment entirely. A recent example is the breach of OpenAI agents and a subsequent intrusion into Hugging Face systems.

Now that rogue agents are not just a fear and have become a reality, large language model providers such as OpenAI and Anthropic face ridicule from multiple governments, claiming that the lack of control could provide a large danger to financial sectors and general business. AI providers must now implement kill switches and other more extreme security measures to regain the trust of the overall public.



When running strong AI models, make sure to

- Provide strong boundaries, even if the research is based on reduced safeguards in models
- Make sure that access to the wider internet is impossible for models, even if they were to breach the testing environment
- Properly keep track of agent goal alignments with alerts and surveillance
- Avoid giving tasks to AI agents where the likelihood of going rogue would be high
-





Sector-Specific Highlights

-  **Healthcare: Oncology Company Breach Adds to Growing Problem**- A cybersecurity incident at oncology company Novocure exposed records of more than 1,400 U.S. patients. This newest breach adds to the growing number of cyberattacks on the healthcare sector, as many cyber criminals seem to directly target this critical information.
- Prevention Tips:** Providers of healthcare and holders of patient information should require highly restrictive cyber security environments. To avoid data breaches, teach employees on the new AI driven phishing attacks, and have MFA enabled for all critical accounts.
-  **Utilities/Industrial: FBI Investigates Leak of 153 Million Licenses that Hit the Dark Web**- Database leak of idscans has lead 153 million methods of identification that would be used at Hertz counters, dispensary checkouts, and hotel counters across America. This data was publicly available on a web page on the dark web, where a user could search for a name, find an ID, and pay to unlock further information. The web page has since gone offline.
- Prevention Tips:** The server holding the ID's was breached and exfiltrated for over a year before security operators noticed and closed the access. When protecting sensitive information, quick intelligent response is the greatest factor in preventing greater damage.
-  **Education: SonicWall finds that education sector has the highest per device attack intensity of any sector**- SonicWall has released a study where they deployed an IPS onto education sector devices, finding very old vulnerable software and large amounts of malware. The largest threat for the education sector is their lack of updates for vulnerable systems, leaving easy access for knowledgeable adversaries.
- Prevention Tips:** As AI becomes more used in attacks, brute forcing vulnerable systems becomes easy for even inexperienced adversaries. Keeping track of your systems and performing software and hardware updates as necessary is a strong step to solidifying security.
-  **Public Safety/Financial: Bank of England warns of cyber threats to global financial system**- Bank of England Governor Andrew Bailey warns that the cyber risk posed by frontier AI models are the largest immediate concern for financial markets. His statement is that that these frontier models "may have the ability materially to alter the speed, scale and economics of cyber risk, which could undermine market confidence system-wide".
- Prevention Tips:** Recommendations are to improve vulnerability management, response, and recovery capabilities. The speed at which AI can exploit vulnerabilities in systems means that speed of response will be the most major factor in preventing larger damage to systems.



Recommended Tools and Federal Resources

- **[Spider-foot](#)** – An automated OSINT tool that maps out what is exposed about a given target on the internet. One of Spider-foot's greatest strengths is its ability to pivot from many different starting points across a vast module array.
- **[Prophet AI](#)** - An agentic AI SOC platform that automates alert triage, in-depth security investigations, threat hunting, and response actions.
- **[AdBlock](#)** - Blocks pop-up ads, videos and other unwanted content while browsing. As ad's can sometimes contain harmful material, having an adblock in corporate environments is important.



Emerging Trends to Watch

- **[TerminalFix uses fake CAPTCHAs to gain backdoor access](#)**: TerminalFix, a new variant of ClickFix, uses fake Cloudflare CAPTCHAs to trick site visitors into copying and executing malicious commands in their terminal. These commands allow the attacker to deploy a reverse-tunnel backdoor onto the system, granting the attacker remote access to the victim's internal network. The best way to mitigate this threat would be to restrict PowerShell and Run dialog execution where possible. Monitoring DLL sideloading indicators and enabling PowerShell script block logging can also help identify if your system is impacted.
- **[AI-accelerated impersonation attacks on the rise](#)**: Phishing emails and other business email compromise attempts are increasingly including AI-generated elements. AI can easily remove tells such as grammatical errors, generic greetings, and clumsy formatting to avoid spam filters, enable mass deployment of lookalike domains, and create deepfakes to allow attacks to advance past text-based communications. While this is a problem without one clean solution, it is recommended that you protect any domain you own, monitor for any lookalike domains, ensure any trusted third party you interact with is legitimate, and ensure anything you automate is secure.
- **[Hugging Face bug can download malicious scripts](#)**: A bug in Hugging Face versions 4.49.0 through 5.8.1 contains a vulnerability that can copy malicious scripts included with AI models without the consent of the user. While the scripts won't be run immediately without permission, they can still be inadvertently executed later when launching a trusted model. Currently there is no official fix, so it is recommended to be careful when loading untrusted models and to periodically clear the cache of Hugging Face to remove any unexpected content.