CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** August 8th - August 21st
Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 16

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Dropcatch domains receive influx	Technology, Infrastructure	2026 has seen an increase in hackers reacquiring expired domains in the hope of redirecting traffic to malware and scams. Just one of these threat actors, known as Sable Squirrel, has spent nearly $7 million dollars on these expired domains.	Do not trust newly registered websites, even if they claim to be long standing brands or well known names. If you are a company, set up autorenew on your domains so that your company website does not get dropcatched.
Previously Patched Microsoft Vulnerability Returns	Technology	CVE-2026-50656, also known as RoguePlanet, was discovered in June 2026 and patched a month later by Microsoft, but a security researcher going by Chaotic Eclipse has found a patch bypass and is using RoguePlanet in a new zero day going by ShieldBreak.	Microsoft is aware of the flaw and is working on a security update to address it.
CVE-2026-62878	Technology, Infrastructure	Given a 9.8 CVSS score, this vulnerability exists on Microsoft DNS servers and allows a stack-based overflow that lets a remote, unauthenticated user execute code with zero user interaction. Researchers have noted that it is “wormable” meaning that it could self-propagate across networks.	The vulnerability was completely patched August 11th by Microsoft, update any servers if they have not been updated since that date.

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
The City Forum Campaign	Industry, Sales	A single server has been pulling records from Salesforce and ServiceNow Service Portals. While many previous attacks on Salesforce abuse the older Aura architecture and overload with guest requests, this new attack also focuses on Salesforce Lightning Web Runtime websites, which has no public tools or writeups on known penetrations.	If on Salesforce, review logs and search for the IP 158.220.87.79, then strip the guest user of object and field level permissions. Also disable self-registration unless the site requires it.
North Korean Operatives Sneak into Employment	Cryptocurrency, Finance, Healthcare	The FBI is investigating North Korean IT workers, who infiltrate businesses by simply applying, passing interviews, and handing legitimate credentials. Once in the business, the North Korean operatives have the goal of exfiltrating information and money from the companies.	Often the documents will not completely match with the person hired, recruiters for remote positions should scrutinize all hired employees, and make an effort to fully check legitimacy.

CERIAC
Cybersecurity Education, Research and Outreach Center

Tennessee Tech College of Engineering

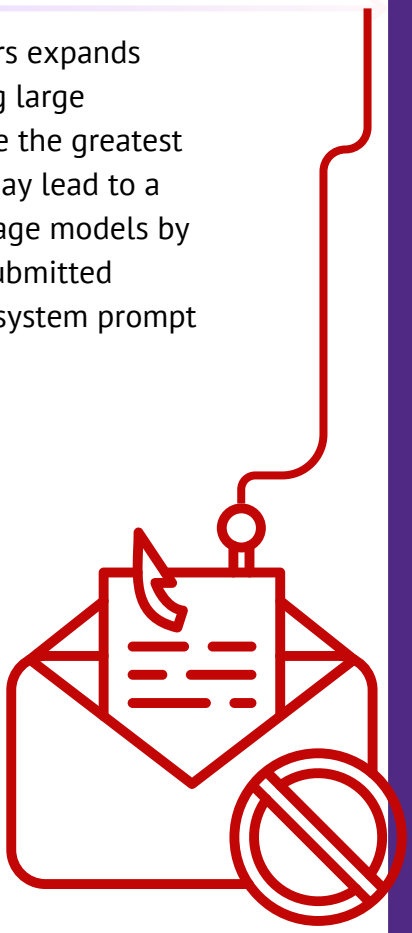
Important Government and ISAC Alerts

- **CISA ICS Advisories:** CISA Malcom- By exploiting this vulnerability, an attacker could cause a denial-of-service condition or execute arbitrary code.
- **CISA ICS Medical Advisory:** Flow Neuroscience FL-100- An attacker could exploit this vulnerability within Bluetooth range to manipulate brain stimulation parameters and override safety limits.

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: Major Genetic Data Firm Hacked**- Major genetic-testing firm Baylor Genetics says hack compromises sensitive patient data. This data include birthdates, lab test results, health insurance information, and a limited case of social security numbers. This intrusion occurred sometime in mid-June.
- **Prevention Tips:** This hack is a showing of the continued supply chain risks that the medical sectors face and should be properly noted and protected against.

- **Utilities/Industrial: Hacking Group Claims Mass Data Theft-** A Russian linked hacking group known as CL0P has claimed massive data theft from Shell, Phillips, GE, and dozens of others. The group is known for finding unexploited zero days and mass applying this knowledge for infiltration.
- **Prevention Tips:** Set up strong internal security using 2fa and network sensors to attempt to avoid infiltration by outside sources.

- **Education: Zoom Screen Sharing Bug Let Anyone Take Over Other Devices**- A vulnerability within the live annotation on Zoom during screen sharing could allow a user to completely take over the device of anyone present within the call. This vulnerability was found using AI pen testing tools and took less than 20 prompts total to find.
- **Prevention Tips:** This Zoom vulnerability was already patched, but AI being able to find vulnerabilities this dangerous so easily shows a movement in how cyber security operates.

- **Public Safety/Financial: Flock Gathering More Data Than Publicly Announced-** Flock's new AI agent can allow police officers to identify people's addresses, names, and relatives based on nothing but the cameras they drive by, and their general movements. These capabilities go much further than flock previously proclaimed their surveillance went.
- **Prevention Tips:** Check if Flock cameras are currently positioned within your communities and where they may be angled towards.

Recommended Tools and Federal Resources

- O.MG Cable – A USB cable with a hidden implant which allows a red team to emulate attack scenarios of advanced adversaries.
- Microsoft Sentinel SIEM - SIEM built into Microsoft Defender with capabilities to use Microsoft Copilot AI tooling to improve SOC response time
- Palo Alto Networks - Unit 42 offers a wide variety of training courses, cyber security products, and solutions to existing cyber problems that can improve the capabilities of cyber security personnel.

Emerging Trends to Watch

- **Government Begins Pressing Charges Against Rogue AI Agents:** House democrats have began pressing charges against two AI giants after rogue AI agents hack into companies in cyber security incidents. This shows a rise in fear of AI agents not given enough security boundaries and operating on unprecedented terms. As rogue AI becomes more commonplace, using AI pen testing tools on your own internal software may be a good way to get ahead of 0 day exploits that these rogue AI may perform.
- AI "mind viruses" may spread between agents: An injection performed on the system prompt of an AI agent may allow a persistence of malicious payloads within AI agents. A test done by Anthropic shows that when a file is injected into the system prompt at the start of each AI agent, simply adding malicious code creates a consistent virus within an AI agent group. Check any files injected into the system prompt of AI agents, and only allow persistence when absolutely necessary.
- 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.