CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** October 3rd - October 14th
Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 20

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
LMCache is vulnerable to Remote Code Execution	IT and Technology	LMCache in multiprocess mode is vulnerable to RCE when --host is set to a routable address. The vulnerability allows an unauthenticated message to be read and executed as the user the service is running as, which is typically root.	Versions 0.3.9 to the latest version are affected, and no fix has been released yet. The best way to prevent this currently is to avoid setting --host to a routable address.
Max severity SonicWall SMA1000 flaw now exploited in attacks	IT, Network Security Infrastructure, Government	A recent exploit involving vulnerability CVE-2026-102255 allows remote attackers to perform unauthorized actions on SonicWall SMA1000 devices by targeting the WorkPlace Extraweb interface. Recent honeypot data indicates that attackers are actively exploiting the vulnerability to bypass authentication and deliver payloads.	A patch has been released for CVE-2026-102255 in firmware versions 12.4.3-03670, and 12.5.0-03082. It is advised that all SonicWall SMA1000 appliances are updated to these versions.
Breach in Discord security bot exposes 28 million users	Gaming, Software technology, Financial Services & Crypto	An attacker gained access to Double Counter, a Discord bot used in communities for verification and alt-account detection, and exfiltrated data belonging to over 28 million Discord users stored in its databaseDouble Counter says no passwords or stored card numbers were exposed, but a total of $7,316 was charged on one of the company's own cards.	Discord server administrators should delete any message sent by the Double Counter bot on October 4 between 12:00 and 16:30 UTC that invites users to another server.

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
ShinyHunters FBI Hacker Arrested	Government	Saif al-Din Khader, a ShinyHunters member linked to the recent FBI data breach, was detained October 3rd by Jordanian authorities. Khader is notably cooperating with the FBI, which may lead to more arrests of ShinyHunters personnel going forward.	ShinyHunters use a diverse list of tactics for gaining access to machines, so to avoid hackers with similar initial access tactics it is important to have phishing-resistant MFA, help desk verification procedures, and least-privilege access controls.
Chinese Government-linked Adversaries Steal Sensitive Data	Government, Manufacturing, Healthcare, Technology	Chinese government-linked actors are stealing sensitive data from companies worldwide, including United States critical infrastructure. The threat actors gain initial access using scanning tools, cross-site scripting attacks, and password spraying on Microsoft Exchange servers. They maintain persistence through VPN software. They exfiltrate emails and sensitive credentials using scripts.	The joint cybersecurity advisory recommends organizations prioritize disabling unused services and ports, sanitizing web applications against injection attacks, implementing MFA, and applying timely patches.

Important Government and ISAC Alerts

- **CISA ICS Advisories:** Swann Communications SWIFI-SE2KIC - A Missing Authentication for Critical Function vulnerability allows attackers to view video information without authentication. This vulnerability requires the attacker to be on the same network as the camera
- **CISA ICS Medical Advisory:** Pulsetto Vagus Nerve Stimulator (Update A) - Attackers can use undocumented commands to modify certain stimulation settings. Pulsetto has not responded to CISA requests to work on a mitigation, so not fix is available.

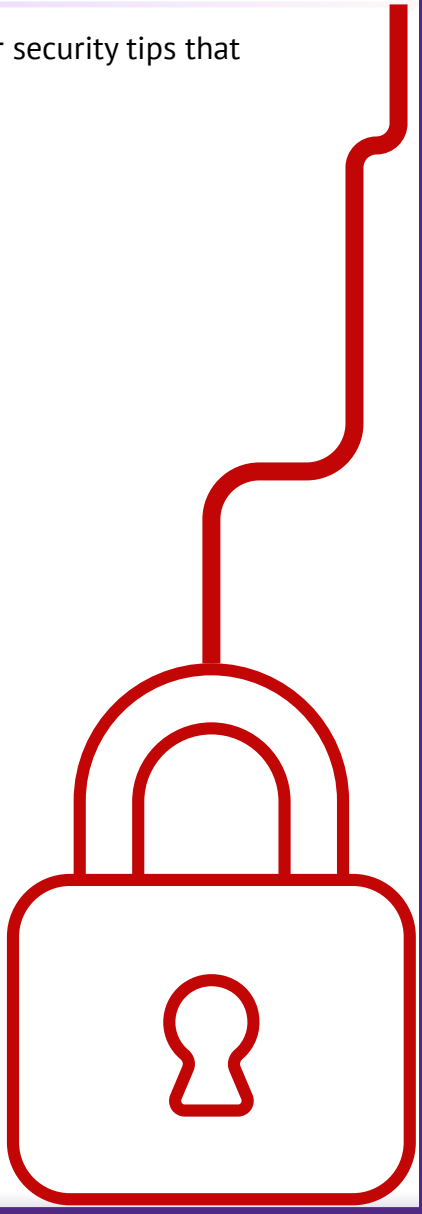
Security Awareness Theme

October Focus: Cybersecurity Awareness Month

For Cyber Security Month, the Sentinel will include a short list of general cyber security tips that can be applied to both industry and personal usage.

Cyber Security Month 5 Tips

- Passwords don't always need to be complicated strings of random characters. A long passphrase can be even stronger, and is much more memorable.
- Passwords aren't always enough to protect an account from attackers; enable multi-factor authentication on accounts, especially highly critical accounts such as banking and email.
- When receiving an email, text, or other form of communication that seems out of the normal, look for things such as calls to action, bad domains or unknown numbers, and broken grammar for possible indications of a phishing attack.
- When sharing information on social media, think of who all could see it. If your account is set to public, think if the information you're sharing could possibly be used against you.
- Public networks can have attackers who may intercept your connection and steal your information. Avoid accessing banking apps, or other applications with sensitive information, without using a VPN.



Sector-Specific Highlights

- **Healthcare: IQVIA fined $7.8 million for failing to properly anonymize health data**- IQVIA, a multinational medical data analysis and research company, was investigated by Italy's Data Protection Authority (GPDP) and found to be non-compliant with Italian standards for healthcare data anonymization, as was fined $7.8 million due to the severity of the infraction.
- **Prevention Tips:** When working with medical data be sure to anonymize information so that individuals cannot be reasonably identified and only process health data when there is a legal basis to do so.

- **Utilities/Industrial: Intermarché cyberattack exposes refrigeration security risks-** A cyberattack on multiple supermarket chains in France, including Intermarché, manipulated connected refrigeration systems, raising temperatures in refrigerators and freezers as high as 50 degrees Celsius (122 degrees Fahrenheit) and causing fires and food spoilage. Attackers exploited outdated firmware and direct internet exposure on the Danfoss AK-SM 800-A system used by these retailers to bypass authentication and remotely execute code.
- **Prevention Tips:** Danfoss urges customers to upgrade their AK-SM 800-A firmware to R4.3.1 and keep management interfaces off the internet.

- **Education: Osaka Metropolitan University has Data Leak**- Osaka Metropolitan University says a suspected ransomware attack on October 2nd, which took about 500 university related servers offline, may have exposed the data of at least 130,000 current and former students and teachers. The method of initial access, and if info was stolen, are currently not disclosed.
- **Prevention Tips:** To prevent breaches like this one, deploy phishing-resistant MFA for high-privilege accounts, apply quick patches to internet facing devices, and deprovision old accounts that no longer need access.

- **Public Safety/Financial: Unauthorized hardware implant found in crypto wallet from CryptoBilis-** Hardware implants have been found in Ledger crypto wallets sold by Southeast Asian reseller CryptoBilis. These implants allow recovery phrases to be transmitted through a cellular connection, which can allow an attacker to access the funds in the wallet without access to the original device.
- **Prevention Tips:** Ledger recommends not initializing any unused devices that may have been modified and move any assets to a new device purchased from Ledger if they are on a potentially modified device.

Recommended Tools and Federal Resources

- Nika – Nika is a code review and static analysis tool capable of cross-file taint analysis, AI exploitability analysis, and branch-aware scanning.
- Malwarebytes - Malwarebytes is a system monitoring tool that detects malware, viruses and scams by using advanced real time protection and is especially effective in conjunction with Windows Defender.
- BitLocker for Microsoft Windows - BitLocker encrypts drives to protect against unauthorized access or hardware changes, requiring a recovery key to decrypt the drive.

Emerging Trends to Watch

- Telegram bug allows hackers to hijack accounts with crafted links **:** Telegram Desktop fails to properly escape semicolons, which the app uses to separate instructions. A malicious user could craft a link that tricks the app into executing instructions that exfiltrate data and hijack accounts when the link is clicked. Ensure that Telegram Desktop is updated to the most recent version. This adds a confirmation window when clicking a link, which can warn a user if they are clicking a suspicious link.
- Claude Adception : A look-alike Claude download site exploited Bing paid promotion features to reach the top of search results and lead users to download malicious payloads. The download site was a Public Artifact which is a site that uses the claude.ai domain but is user generated. The domain combined with the paid promotion caused the site to appear legitimate with over 7,000 site visits before it was taken down. When installing software from an online source, avoid advertisements and paid promotions as they can redirect users to malicious sites.
- Small AI Models May Be Only Months Away from Self Replicating : Anthropic warns of the possibility of AI powered malware that can infiltrate a commercial internet-of-things network like TV's and even refrigerators. By self-replicating across the network, the AI can split the load of work to each major device, allowing stronger models to be run. This capability is unique to AI malware, as the malware can use the AI capabilities to break into various devices. One of the stronger capabilities of this form of malware is the lack of security for a majority of devices such as TVs. Install security on devices where downloads are more common and keep weaker devices from being internet-facing.