

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** September 19th - October 2nd

Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 19

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Mass exploitation of Magento critical flaw	E-Commerce	Attackers are targeting online storefronts using versions 2.4.2 to 2.4.9 of Magento by sending a POST request to unprotected upload endpoints to deploy a specially crafted file that bypasses validation and tricks the web server's file system into executing hidden code.	If the web server is running an affected version of Magento, download the most recent hotfix. After, check PaymentInformationManagement.php and GuestPaymentInformationManagement.php for malicious strings.
Over 500,000 secret keys exposed on GitHub	IT and software development	Researchers found 543,699 exposed credentials in public git repositories that are still active. These credentials can still be used to access the service they are linked to and billable if the service costs money to use, allowing potential malicious users to rack up massive charges for AI services.	Use environment variables to avoid hardcoded keys, as GitHub's push protection can miss hardcoded leaks
Apple Patches CoreGraphics Zero-Day Flaw Used in Targeted Attacks	IT, Computer Software, Government	Apple patched an out-of-bounds write vulnerability in its graphics rendering framework, CoreGraphics, that let attackers use maliciously crafted files to achieve arbitrary code execution when processed. Apple is aware of reports that this vulnerability may have been used in an "extremely sophisticated attack" against specific targeted individuals.	While the exploit might only be used in highly targeted attacks, it is still recommended to install iOS and iPadOS 26.7.1, macOS Sequoia 15.8.1, and macOS Tahoe 26.7.1 in which the flaw has been patched.

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
FBI Attacked by ShinyHunters	Government	Hacking group ShinyHunters claims they performed a breach and extraction on FBI employee information, including names, assignments, addresses, Social Security numbers, and in some cases family members. In this specific hack, ShinyHunters claim they used an Oracle PeopleSoft zero-day for entry, but this claim is unverified.	Heavily monitor third-party connected apps and track bulk downloads with an aggregated SIEM. ShinyHunters also use social engineering tactics, so transfer towards more secure MFA methods to avoid phishing attacks.
Storm-3069 Deploys Malware "NeedyMantis"	Telecommunications, Education, Healthcare, Government	On Monday, September 28 th Microsoft went into a deep dive on a recently discovered malware family known as NeedyMantis, linking it to China-based threat actor Storm-3069. NeedyMantis is a post-compromise malware, meaning that it provides the threat actors a backdoor into the system and provides stealth to actions.	This method of attack cleverly relies on an oversight in security in which a team may be too focused on protecting against initial intrusion and not focused at all on post-compromise security. To protect against this, have a rapid-response SOC team and a deployed SIEM.



Important Government and ISAC Alerts

-  **CISA ICS Advisories:** [MikroTik RouterOS](#) - An integer underflow vulnerability in the HTTP request body handling allows attackers to achieve remote code execution or cause a denial of service.
- **CISA ICS Medical Advisory:** [Orthanc DICOM Server](#) - An integer overflow exploit allows an attacker to write past the end of a heap allocation when Orthanc decodes the attacker's supplied PNG or JPEG image, resulting in the Orthanc process crashing and a denial-of-service condition. For this attack to work the adversary must be authenticated.



Security Awareness Theme

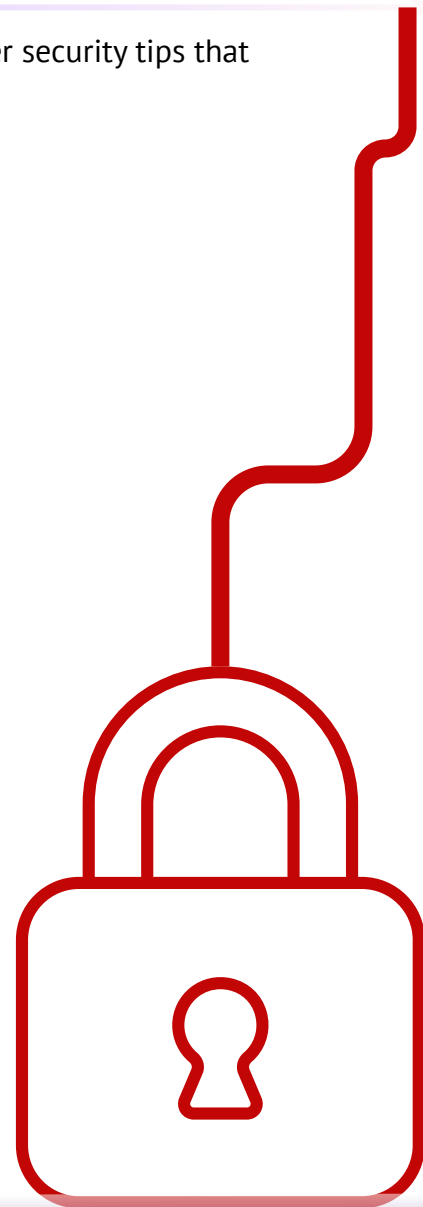
October Focus: Cybersecurity Awareness Month

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: Astrana Health Notifies SEC About Social Engineering Incident** - According to a forensic investigation, threat actors conducted a series of social engineering attempts against multiple employees. These social engineering attempts included impersonating company personnel and spoofing the company's main telephone number.
- Prevention Tips:** Teach employees about the many methods of phishing attacks that go beyond the more well-known standards of email and text, and how emails and cell phone numbers can be spoofed.
-  **Utilities/Industrial: CenterPoint Energy Confirms Network Compromise** - A hacker claimed on a cybercrime forum to have stolen 7.49 million customer files from CenterPoint Energy. CenterPoint has confirmed that an unauthorized third party had obtained personal information relating to a portion of the company's customer base through an "external-facing system", but never stated the exact number of affected customers, so the hacker's claimed figures remain unverified.
- Prevention Tips:** Customers should watch for follow-up disclosures from CenterPoint and assume possible driver's license and partial SSN exposure and act accordingly. CenterPoint security teams should audit the company's external-facing APIs for the controls the hacker claims were missing.
-  **Education: Mathspace Breach Exposes 1.08 Million Students and Staff** - An unpatched vulnerability allowed an attacker to gain access to an internal reporting system and download 1.08 million records of students, parents, school staff, and Mathspace staff. The specific flaw exploited was identified as CVE-2026-72898, a maximum-severity flaw that allowed injection of arbitrary SQL and privilege escalation.
- Prevention Tips:** Users of Mathspace should look out for phishing emails, avoid reusing their Mathspace passwords elsewhere, and check with their school's IT department for confirmation of whether their specific account was affected.
-  **Public Safety/Financial: \$387.5 million stolen in Bitget hack** - Bitget has reported \$387.5 million in cryptocurrency has been stolen after being hacked by North Korean threat actors. Bitget claims that threat actors gained access through a zero-day vulnerability.
- Prevention Tips:** There have not been enough details about the attack released to determine how to prevent it in the future, but Bitget has reported that the vulnerability has been fixed and that user funds have not been affected.



Recommended Tools and Federal Resources

- [**Domain Doppelgänger**](#) - Identifies potentially malicious websites with similar domain names to the given domain.
- [**VirusTotal**](#) - Inspects files, URLs, and search terms with over 70 antivirus scanners, URL/domain blocking services, and other tools to extract signals from the studied content.
- [**TruffleHog**](#) - Trufflehog checks a variety of sources for over 800 types of secrets, validates them to see if they are still live, and reports back which of the exposed secrets are.



Emerging Trends to Watch

- [**WordPress Core theme preview can lead to RCE chain**](#): Two vulnerabilities have been discovered in WordPress that allow an attacker to execute PHP code on a vulnerable server when used together. Attackers can use a specially crafted link to trick WordPress into installing a theme and loading a preview to trigger attacker-supplied PHP code without any visual changes to the website or administrator approval. WordPress released security fixes in version 7.1.1 that fixed these vulnerabilities. Administrators should update WordPress servers to the latest version to avoid these vulnerabilities.
- [**AWS AI agents can store and leak secrets**](#): When an AWS AI agent needs a credential, it stores it in memory as plain text. Because all the commands the agent runs are run as root, it can read the memory and get the plain text credential, which makes exfiltrating it very easy. The best way to mitigate this is to disable any tool that the AI agent doesn't need access to. It is also recommended to limit what each login key can do and to monitor outbound traffic to ensure that nothing is getting sent somewhere it shouldn't be.
- [**Bluetooth flaw allows DJI drones to be hijacked mid-air**](#): 16 top-selling DJI drones have a vulnerability in which all commands except for getting the WiFi network's name, password and MAC address lack any authorization checks before being executed. This can allow an attacker to connect to the drone's Bluetooth interface and change the WiFi password and SSID, alter wireless settings, disable or restart WiFi and Bluetooth, reboot or power off the aircraft, reset configurations, or possibly even hijack the drone itself. No exploitation of this vulnerability being used have been reported yet, and no prevention recommendations have been released. For now, the best way to prevent this is to keep the drones out of Bluetooth range of unauthorized individuals as much as possible until a fix is released.