CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** June 27th - July 10th
Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 13

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Discord Falsely Bans Accounts for False Flagging from Auto Bans	Technology, Gaming, Social Media	An automatic image checking tool falsely flags images for suspected CSAM. These false flags come from the images containing grids within them, which was also used as an overlay in child exploitation content. These false bans come after other false bans found on Meta social media as well as Tumblr.	If using an automated tool to scan images for child exploitation content, have an employee personally check the images before enforcing any sort of ban or otherwise.
Opera GX Auto Add-On Installation	Technology, Gaming	A vulnerability within Opera GX, the gaming version of the Opera browser, allows websites to install malicious browser add-ons that can extract info from visited sites in secret. This is possible because of Opera's 0 prompt install process for customization mods, which allows a web page to install a malicious payload in total silence.	Install the latest version of Opera GX browser, at least version 130.0.5847.89, to avoid this vulnerability.
AI Hallucinations lead to Phantom Typo-Squatted Websites	Infrastructure, Technology, Education, Manufacturing	When prompted, AI can generate website URL's that do not exist, and attackers are beginning to use these hallucinations in their favor to squat on these domains with malicious intent. These new domains have no backing overall, and thus are not noted for being unsafe, so users can blindly stumble into scams by clicking on links from a platform that they believe they can trust.	Confirm link legitimacy before entering any email of password, or before entering into the site.

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
North Korean Hackers Publish Malicious Packages	Technology	North Korean threat actors linked to the Contagious Interview campaign have been noted for publishing 108 unique malicious packages spanning npm, Go, Packagist, and Google Chrome. This ongoing activity is noted as PolinRider. The attackers take over maintainer accounts to send malicious npm packages or malicious VS code extensions. Once in, they push malicious code secretly on GitHub to be pulled and spread infection.	If you've installed a compromised file, consider the environment compromised and rotate all secrets from a clean machine.
Iranian-Linked Hackers use new C2 framework to target Israeli Organizations	IT-providers, Government Sector	Hackers linked to Iran's Ministry of Intelligence and Security are using a previously undocumented modular command-and-control framework dubbed Cavern. After initial access into an IT organization, the attackers moves laterally through strong connections to a true target. The modular formation of Cavern allows for tailoring towards a specific profile of attack, as well as enhanced hiding from forensics.	Update any known vulnerabilities in your system and scrutinize IT-provider relationships.

CERIAC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** CISA ICS Advisory: Gardyn IoT Hub (ICSA-26-183-03)- CVE-2026-13768 exposes a privileged IoT Hub key that could allow an attacker to access the IoT Hub Registry Manager, obtain connection information for managed devices, or control connected systems
- **CISA ICS Medical Advisory:** CISA Medical Advisory: OFFIS DCMTK Toolkit- A critical path traversal flaw could allow an attacker to write files outside intended directories, expose sensitive medical information, cause memory exhaustion, or crash imaging services.

Security Awareness Theme

July Focus: Spear Phishing Attacks

Like a standard phishing attack, a spear phishing attack is a social engineering tactic that attempts to get you to click on a link, enter credentials, or install a file that you would not otherwise interact with. Unlike a standard phishing attack, a spear phishing attack is directly targeted at you or a small group of people and typically has a much higher success rate due to its targeted nature. Bad actors may use OSINT techniques to gather information on your work, organizations, or hobbies to create a convincing message or offer exclusive opportunities, or they may gain access to a trusted account, such as a friend or coworker's, and use that account to perform a spear phishing attack. Spear phishing attacks are now being automated using AI techniques, allowing threat actors to more easily create incredibly convincing messages, or even generate deepfake video or voice messages.

Warning signs

- Requests to move platforms
- Asking for login credentials
- Sending files
- Person acting differently than they normally would

Protect yourself against spear phishing attacks

- Scrutinize all messages received, even from trusted sources
- Report any suspected breached accounts to your IT department
- Notify others who may be hit by a similar spear phishing attack

Sector-Specific Highlights

- **Healthcare:** AdaptHealth Reports Material Cybersecurity Incident and Theft of Patient Data - AdaptHealth disclosed on July 3, 2026 that a threat actor obtained files containing patient protected health information through a social engineering attack on a third-party contractor. The attacker used stolen contractor credentials to access cloud-based patient management systems and document storage platforms. ShinyHunters threat group listed AdaptHealth on its data leak site and threatened to publish the data if a ransom was not paid.
- **Prevention Tips:** Conduct immediate security awareness training for all staff on social engineering and credential phishing tactics. Implement strict access controls limiting contractor and third-party access to only systems required for their role.

- **Utilities/Industrial: Google, FBI Disrupt NetNut Residential Proxy Network Powered by Millions of Devices-** Google and the FBI coordinated to disrupt NetNut, a residential proxy network that powered millions of compromised devices, allowing cybercriminals and nation-state actors to mask their identities during attacks
- **Prevention Tips:** Audit network traffic for suspicious proxy connections and unusual outbound traffic patterns to residential IP addresses. Implement egress filtering to block unauthorized proxy traffic.

- **Education: Conversation on Cyber**– Cyber security has seen a raise of appearance in school board meetings by 8.2%, showing a clear increase in the attention being paid to the cyber security of students and teachers over time. This briefing also shows an increase in talks of AI of 10.8%; due to the prevalence of AI usage with cyber security, these two are most likely related.
- **Prevention Tips:** School systems should invest in in-house cyber security teams as well as informing students on the new age of cyber related dangers presented by AI automation.

- **Public Safety/Financial:** EU Unveils AI Cybersecurity Action Plan - To combat the increasing weaponization of AI in attacks, the European Commission is utilizing the same technology in its new Action Plan. To safely manage these risks, the EU is establishing a secure testing platform alongside standardized blueprints, so critical sectors can evaluate advanced AI tools and deploy them defensively before widespread adoption.
- **Prevention Tips:** Public safety and critical infrastructure organizations should leverage this new EU testing platform and secure blueprints to safely stress test AI tools before full deployment.

Recommended Tools and Federal Resources

- **Picus Autonomous Exposure Validation Platform** – The Picus Autonomous Exposure Validation Platform continuously simulates real-world attack chains to prove which vulnerabilities can actually bypass your defenses, helping security teams focus on fixing validated risks instead of chasing theoretical threats.

- **FBI Cyber Alerts** - The platform provides regularly updated FBI cybersecurity advisories that contain threat actor information and indicators of compromise (IOCs), including IP addresses, domains, and file hashes. It also includes mitigation guidance and reporting instructions for cyber incidents.

- **Hunchly** - Screen captures any research you do, highlighting specific words, and recording instances of specific url's along with timestamps. This tool can greatly help OSINT investigations by making the recording process automatic.

Emerging Trends to Watch

- **Agentic AI Powered Cyber Attacks:** The emergence of advanced LLMs has enabled attackers to leverage agentic capabilities for malicious purposes, including the automation of malware generation, phishing emails, and attack workflows. Agentic systems with their enhanced autonomy can plan, use tools, and execute multi-step attacks. This autonomous nature increases the risk of tool abuse, data exfiltration, and prompt injection attacks that manipulate model inputs to produce unintended or harmful outputs.

- **Targeting Secure Messaging Systems:** State-sponsored threat actors are increasingly targeting secure messaging platforms such as Signal, WhatsApp, and Telegram in addition to traditional email. Recent campaigns have focused on stealing backup recovery keys, authentication tokens, and user credentials to gain persistent access to encrypted conversations and messages.

- **AI Phishing Campaigns:** AI systems can rapidly generate convincing phishing emails, fake login pages, and tailored social engineering lures in minutes. This significantly reduces the time and skill required to launch a phishing campaign. As a result, security operation centers (SOCs) are now facing larger volumes of higher-quality social engineering attempts that make detection and response more challenging while also increasing the likelihood of successful phishing attacks.