CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** May 15th - June 10th
Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 11

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
CVE-2026-27771	Devops, Enterprise IT, Education, Software Development	CVE-2026-27771 is a critical authorization vulnerability in Gitea's container registry that allowed unauthenticated access to private repository images due to missing access controls in the registry API. This could lead to the exposure of sensitive container images, application builds and embedded secrets.	Administrators should upgrade to Gitea v1.26.2 or later, monitor registry access logs for unauthorized activity, and rotate any secrets stored in affected container images.
CVE-2026-33244	E-commerce, Education Technology. Software Developemnt	This React Router Framework Mode vulnerability allows Cross-Site Scripting (XSS) when untrusted Location header values are improperly handled in pre-rendered redirection pages. Successful exploitation could enable session hijacking or malicious client side code execution.	Organization should upgrade React Router to v7.13.2 or later, avoid using untrusted redirect inputs and implement validation for redirect URLs.
TA4922	Financial, Information Technology, Human Resources,	TA4922 is a financially motivated threat actor, that primarily targets financial and tax related functions. Tactics and Techniques include the use of social engineering to gain initial access, often via malicious links, which leads to the delivery of remote access trojans for persistence and exploitation	Block or restrict execution of files from email and web downloads where possible, enforce MFA on all financial/admin account and monitor for suspiciouos outbound connections.
VariantBamBoo	Software Development, Financial, Cloud, Telecommunications	VerdantBamboo is a likely Chinese state linked threat actor that targets edge network appliances for initial access. It uses living of the land techniques to maintain persistence and facilitate data exfiltration. The group has been recently associate with deployment of the BRICKSTORM backdoor to sustain long term access to compromised systems.	Harden perimeter devices by disabling unnecessaray services and enforcing strict access control to mitigate and prevent unauthorized system access.

CERIAC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** Hitachi Energy - A vulnerability affecting Hitachi Energy RTU500 devices may impact system availability and could also compromise confidentiality and integrity. Successful exploitation could disrupt operations in important infrastructure sections including, dams, energy, water, and wastewater systems.
- **CISA ICS Medical Advisory:** Fourth Frontier Frontier x Mobile Application - A vulnerability in the Fourth Frontier Frontier X and Frontier X2 mobile applications could allow an attacker to read and modify arbitrary handle values, potentially allowing for clinical readings to be altered. The issue affects multiple versions of the mobile application and may impact patient data integrity.

Security Awareness Theme

June Focus: Secure Supply Chains

Supply chain security foces on protecting the products, software, services, and third -party vendors that organization rely on to operate. Modern organization depend on a complex network of suppliers, contractors, cloud providers, all of which can become entry points for cyberattacks if their systems are compromised. Many major breaches do not begin with a direct attack against the the target organiation; instead, attackers exploit weaknesses in a supplier, software update or third party service to gain access. These risks arise from using unvetted vendors failing to monitor third party access, deploying software from untrusted sources or overlooking vulnerabilities in open source components. Maintaining a secure supply chain requires careful vendor management, continuous monitoring, and verification of the products and services used throughout the organization.

Warning signs

- Vendors requesting excessive system access
- Software updates from unexpected or unverified sources
- Missing security documentation
- Third party tools with known vulnerabilities

Protect your supply chain

- Limit third party access to only what is required
- Verify software updates and downloads before installing
- Keep software dependencies updated with security patches
- Report suspicious vendor communications or unexpected software changes

Sector-Specific Highlights

- **Healthcare:** Denta Quest data breach - Exposure of approximately 2.6 million account records following an extortion attempt involving ~234 GB of stolen data. DentaQuest confirmed the incident on June 2, after unauthorized network access attributed to the threat group ShinyHunters. Exposed data reportedly included names, email addresses, phone numbers, gender, date of birth, government-issued IDs, and health insurance information (as reported via HIBP).
- **Prevention Tips:** Do not share personal information via email or informal channels. Enforce MFA, least privilege access, and network segmentation.

- **Utilities/Industrial:** Eversource – In mid-May, Eversource Energy detected unauthorized activity involving employee credentials, likely obtained through phishing. Two employee accounts were confirmed impacted, and approximately 3,000 current or former individuals' records were accessed. No operational disruption to utility systems or critical infrastructure was reported.
- **Prevention Tips:** Verify links and requests before interacting, enforce MFA, apply least privilege access, and reset credentials if compromise is suspected or linked to breach exposure.

- **Education:** Typosquatted npm packages– Malicious or typosquatted NPM packages have been identified executing install-time scripts (preinstall/postinstall) that silently harvest credentials and CI/CD tokens. These packages often impersonate trusted namespaces or organizations and are executed automatically during installation.
- **Prevention Tips:** Enforce dependency verification and integrity checks, restrict or monitor install scripts, and rotate credentials when exposure is suspected.

- **Public Safety/Financial:** Malicious Minecraft mods target yound adults – Malicious Minecraft .jar mods distributed via platforms such as YouTube have been used to infect user systems with malware known as WeedHack. After installation, the mod communicates with a command-and-control (C2) server to download additional payloads, enabling full system compromise. The free variant enables credential and crypto wallet theft, while paid premium variants reportedly include webcam access and keylogging.
- **Prevention Tips:** Verify the safety and source of all downloadable mods, avoid untrusted YouTube-linked downloads, and scan .jar files before execution.

Recommended Tools and Federal Resources

- **Resources | CISA** – CISA provides operational cybersecurity guidance, including vulnerability advisories, industry sector alerts, and near daily updates that include press releases and blog posts. Its publications often include mitigation recommendations and are developed in coordination with agencies such as the FBI and NSA, making them extremely valuable with respects to improving organizational security posture.
- **Claude Fable / Mythos**– Anthropics Claude model family includes advanced LLMS systems such as Claude Fable 5 (previously publicly available with no estimate as to when it will be rereleased). Reports describe experimental or research oriented variants such as Mythos 5 as having enhanced reasoning with the potential of aiding discovery and security research. Claimed capabilities such as zero day discovery, however, remain unverified and should be treated as speculative despite the tools promising capabilities.
- **Have I Been Pwned:** A public breach notification service that allows users to check whether email addresses or phone numbers have appeared in known data breaches. It aggregates publicly disclosed breach datasets to help individuals and organizations assess exposure from credential leaks and compromised accounts, and to determine when password resets or account remediation may be necessary.

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 email, and attack workflows. Agentic systems with their enhanced autonomy are able to plan, use tools, and execute multi-step executions. The autonomous nature increases the risk for tool abuse, data exfiltration, and prompt injection attacks that manipulate model inputs to produce unintended or harmful outputs.
- **AI Driven Penetration Tools**: AI-assisted offensive security tools combine LLMs with cybersecurity toolchains to automate tasks typically performed by security analysts, including reconnaissance, vulnerability scanning, and exploitation assembly. While these systems can reduce manual effort, they require more computational resources through high API usage when using enterprise models such as OpenAI or Anthropic. Open-source implementations, however, are becoming increasingly accessible, lowering the barrier for not only experimentation but potential misuse.
- **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) now are being faced with larger volumes of higher quality social engineering attempts that make detection and response more challenging while also increasing the likelihood of a successful phishing attempt.