CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** May 9th - May 21st
Distribution: Public Sector Partners, Local Governments, IT Departments

Volume 2 Issue 10

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
Cisco Catalyst Authentication Bypass	Telle-communications	A vulnerability within the Cisco Catalyst SD-WAN controller enables an attacker to remotely bypass authentication requirements and obtain administrative privileges through crafted requests. Successful exploitation could allow a threat actor to gain high-privilege access, enabling the manipulation of network configurations.	There are no reported work around or mitigation strategies aside from migrating to a fixed released
Hugging Face Typo Squat	AI & ML, DevOps, Acadamia, Healthcare, Government	A registered user cloned the new OpenAI privacy filter tool repository and embedded malicious code. The popularity of the cloned repository led to approximately 244,000 downloads, enabling the malware to steal users' personal data.	Always verify the legitimacy of repositories claiming to be from trusted vendors before pulling from them.
Ollama CVE-2026-7482	Research & Academia, Public, Software development	An out-of-bounds read vulnerability was discovered in Ollama that allows remote process memory to be leaked. The vulnerability impacts more than 300,000 servers globally. CVSS score of 9.1.	Migrate to a fixed or current release, restrict network access, and deploy authentication proxies in front of all Ollama instances.
Shiny Hunters	Education, Education Tech,	A ransomware attack against Instructure, the parent company of Canvas, allegedly involved 275 million student records and 3.65 TB of data. Reports indicate that SH agreed to remove themselves and delete the stolen data in exchange for an undisclosed payment. SH is known to infiltrate systems using social engineering techniques, primarily voice phishing (vishing).	Advise employees through continuous awareness training on appropriate channels for sharing login information. Login credentials should never be shared outside of secure, verified interactions, preferably in person.
TeamPCP Shai-Hulud Worm	Sectors that heavily utilize open-source software or third-party packages	TeamPCP is distributing the Shai-Hulud worm through compromised npm and PyPI packages as part of a supply chain campaign. Once installed, the malware executes within developer environments, self propagates throughout the system and exfiltrates sensitive data such as API keys, SSH keys, and password manager tokens.	Closely monitor and verify all third-party dependencies before integrateing services. Enforce least privilege access for developer credeentials and regularly rotate secret keys.

CERIAC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** ZKTeco CCTV Cameras – ZKTeco CCTV Cameras contain a vulnerability that, if exploited, could allow an attacker to bypass authentication mechanisms and gain unauthorized access to sensitive information. This could lead to exposure of surveillance data and compromise the confidentiality and integrity of monitored environments.
- **CISA ICS Medical Advisory:** Grassroot DICOM (GDCM) Library – A vulnerability exists in the Grassroots DICOM (GDCM) library that can be exploited when a specially crafted file is processed. An unauthenticated attacker could trigger a denial-of-service condition during file parsing, potentially disrupting medical imaging workflows and impacting the availability of healthcare services.

Security Awareness Theme

May Focus: Safe Data Handling & Transport

Safe data handling and transport refers to how sensitive data is stored, accessed, shared, and moved both inside and outside of an organization. This includes everything from emails and company documents on the cloud, to transferring files via USB drives or 3 party services. Even simple routine actions like sending an attachment or copying data to a personal device can introduce risk if not done securely. Breaches often don't come from sophisticated hacks, they come from simple mistakes like sending sensitive information to the wrong recipient, using unsecured file-sharing tools, or storing data in unapproved locations.

Limit Access

- Networks with **no password** required or **vague names ("Free_ Wifi")**
- Duplicate Wi-Fi names with slight spelling differences
- Unexpected login pop-ups or security warnings
- HTTPS missing from websites
- Requests to install certificates or software

Know your data!

- Avoid logging into sensitive accounts (Email, Bank, etc)
- Disable auto-connect to open Wi-Fi networks
- Only visit websites with HTTPS
- Keep devices updated with security patches

Sector-Specific Highlights

- **Healthcare:** West Pharmaceutical Services ransomware attack – A large scale healthcare manufacturing organization that suffered a ransomware attack on May 4th. While the incident was reportedly contained, attackers were able to encrypt and potentially exfiltrate significant volumes of sensitive data with no amounts reported. **Prevention Tips:** Create, maintain, and continuously update business continuity and incident response plans to provide rapid recovery and minimize operational disruption. Ensure system backups are regularly performed to mitigate data loss in the event of security incidents.
- **Utilities/Industrial:** Siemens SIMATIC – Siemens SIMATIC systems, including SIMATIC 4100, contain multiple vulnerabilities that could impact the confidentiality, availability, and integrity of control operations. If exploited, these weaknesses may allow unauthorized access, disruption of automated processes, or manipulation of critical workflows. **Prevention Tips:** Siemens released a patched version of SIMATIC 4100 it is strongly recommended to migrate to the latest secure release. Organizations should also segment networks, enforce strict access controls, and continuously monitor systems.
- **Education:** Canvas Ransomware Attack – On April 25th, 2026, a cybercriminal group exfiltrated approximately 3.65 TB of data from a major learning management system operated by a leading education technology provider. After approximately two weeks of disruption, services were restored, and a financial settlement was reportedly made to prevent public release of the stolen data. **Prevention Tips:** Organizations should implement regular cybersecurity awareness training to help employees recognize and resist phishing attempts.
- **Public Safety/Financial:** B1ack's Stash credit card release – A major dark web carding marketplace released approximately 4.6 million stolen credit card records for free due to internal disputes within the market. The dataset reportedly includes full payment card details along with personally identifiable information such as names, addresses, phone numbers, and email addresses. Most of the compromised records are associated with U.S. victims. **Prevention Tips:** Enable transaction alerts, increase phishing awareness, and enforce MFA when completing transactions online.

Recommended Tools and Federal Resources

- **OpenAI Daybreak** – A tool developed by OpenAI designed to support threat detection, analysis, and defensive security. It is intended for integration into advanced GPT-5.5 Cyber environments for enhanced AI-assisted cybersecurity operations.
- **TryHackMe** – An online cybersecurity training platform that provides guided learning paths, interactive labs, and hands-on challenge environments. It is designed for beginners through advanced users to develop practical skills relating to all things cybersecurity.
- **AIRecon** – An autonomous AI-driven reconnaissance tool that automates security assessments, penetration testing, and bug bounty reconnaissance. It operates within a controlled Linux Docker environment and leverages local AI models to assist with target discovery and analysis.

Emerging Trends to Watch

- GitHub action malicious alterations – GitHub Actions used for automation workflows have been increasingly repurposed to execute malicious code within affected CI/CD pipelines. Once triggered, the malicious code can silently run during routine build or deployment processes, allowing attackers to harvest sensitive information such as secrets, API keys, and credentials. This data can then be exfiltrated to attacker controlled servers, potentially enabling further compromise of software repositories, development environments, and downstream production systems.

- iOS and Android linked encrypted communications – Upon installation of end-to-end encrypted (E2EE) RCS, both Apple iPhone and Android devices can securely communicate using encrypted messaging. This ensures that messages, images, videos, and other shared content are protected in transit and can only be decrypted by the intended recipients. Even when messages are exchanged between different platforms, the encryption prevents interception or tampering by third parties, improving cross-platform communication security and further reducing the risk exposing data while in transit.

- Bauman Moscow State Technical University Hacker Academy – Bauman Moscow State Technical University secretly creates fresh talent for Russian hacker groups Sandworm and Fancy Bear. The institution, known as Russia's equivalent to MIT, secretly offers students to enroll in an academy that focuses on information warfare, electronic reconnaissance and disinformation tactics. This reflects a broader trend of nation-states integrating cyber operations activities into formal technical education. This raises concerns about the development and scaling of state funded cyber campaigns that could be seen in the coming years.