CEROC
Cybersecurity Education, Research and Outreach Center

Bi-Weekly Cybersecurity Threats Update

Prepared by: CEROC Student SOC **Date Range:** April 13th, 2026 - April 24th, 2026
Distribution: Public Sector Partners, Local Governments, IT Department *Volume 2 Issue 8*

Top 5 Cybersecurity Threats

Threat	Sector	Summary	Recommended Action
RedSun Microsoft Windows Defender Zero-Day	General	RedSun is a proof-of-concept attack for an unpatched Elevation of Privilege (EoP) vulnerability targeting Windows Defender. It was publicly disclosed April 16th, 2026 by the security researcher who operates on GitHub under the alias "Nightmare-Eclipse." RedSun abuses a flaw in Windows Defender to achieve SYSTEM privileges to unprivileged Windows users.	Monitor network traffic and endpoint detection systems for signatures associated with RedSun and BlueHammer GitHub repositories. A patch is not available from Microsoft yet.
Vercel Data Breach	Web-App Infrastructure	Vercel, a major cloud platform powering Next.js hosting and serverless deployment, confirmed a security breach on April 19th. The root cause was a Lumma Stealer infection at Context.ai – a third-party AI tooling vendor – in February 2026.	Configure authenticator app and passkey as specified in Vercel's security advisory. Deleting your Vercel account is NOT sufficient to eliminate risk.
Invanti EPMM RCE	Government, Enterprise Infrastructure	A critical vulnerability in Invanti Endpoint Manager Mobile (EPMM), an on-premises mobile device platform. Attacker can send specially crafted HTTP requests to the map-aft-store-url endpoint (without authentication) to inject and execute arbitrary code on the EPMM appliance.	Immediately apply Invanti's RPM 12.x.0.x or 12.x.1.x security update. Federal agencies were required to act by April 11th, all other organizations should treat this as overdue.
Handala Hack Team	Energy, Government Infrastructure, National Defense	Handala is an Iran-affiliated hacktivist group with a large spike in activity as of April 2026 due to U.S.-Iran tensions. Their threat has caused an increase in cyber risk.	Maintain backup copies of critical data, and deploy advanced email filtering with attachment sandboxing.
Qilin RaaS Group	Healthcare, Manufacturing, Government	Qiling is a prolific Ransomware as a Service (RaaS) group that has claimed over 1,000 victims. Primary targets have included North American manufacturing, healthcare, professional services, and government entities.	Qilin specifcally attempts to compromise backup infrastructure, so all backup access should be audited and heavily restricted. Enforce MFA to avoid stolen accounts being sold.

CERIAC
Cybersecurity Education, Research and Outreach Center

Important Government and ISAC Alerts

- **CISA ICS Advisories:** Delta Electronics ASDA-Soft - CISA released an ICS advisory identifying a stack-based buffer overflow vulnerability in Delta Electronics ASDA-Soft that could allow attackers to execute arbitrary code if exploited.
- **CISA ICS Medical Advisory:** ZOLL ePCR IOS Mobilr Application - CISA issued an ICS Medical Advisory back in February of this year identifying a vulnerability in the ZOLL ePCR mobile application that could expose sensitive healthcare data or allow unauthorized access if exploited.

Security Awareness Theme

April Focus: Social Engineering Tactics

Social Engineering is the art of manipulating people into divulging confidential information or performing actions that compromise security. Unlike traditional technical hacks that target software or networks, social engineers target human psychology by exploiting their trust through fear, urgency, or even the feeling of being left out. In the modern era of AI, obvious spelling errors and language barriers are largely a thing of the past. That's why it is important to know the signs, so you can keep yourself safe!

Phishing, and it's many cousins.

- Phishing is the art of sending a malicious email with the goal of getting the recipient to click a link, or share important information.
- Phishing is not the only method. Attackers can engage in Vishing (voice call), Smishing (SMS texts), and even Quishing (QR codes).

Always verify contact information!

- True to the old saying, if it's important, it's worth a face-to-face conversation. If there is a true sense of urgency, they can speak with you in-person.
- Be sure to check where the message is coming from. Is the domain in the email correct? Is the phone number area and country code correct? Does the link provided lead to a trustworthy domain?

Sector-Specific Highlights

- **Healthcare:** [Brockton Hospital Ransomware Attack](#) - Brockton Hospital (MA) suffered a ransomware attack on April 6th by the Anubis group. ER and chemotherapy services were disrupted with a 2+ week downtime. According to SuspectFile, which was contacted by the attackers, only non-critical systems were encrypted, and 2TB of data (including patient PII) was stolen. ***Prevention Tips:*** *Maintain offline backups and rehearse downtime procedures so clinical staff can resume their work.*

- **Utilities/Industrial:** [Iranian-Affliated Cyber Actors Exploit PLCs](#) - The CISA has issued a warning that Iranian APTs are actively exploiting internet-facing Rockwell Automation PLCs across U.S. water, energy, and government OT networks. ***Prevention Tips:*** *Apply Rockwell Automation patches, and all Studio 5000 Logix Designer updates immediately.*

- **Education:** [McGraw Hill Data Breach](#) – McGraw Hill confirmed a data breach in April 2026 after attackers exploited a Salesforce misconfiguration, exposing data tied to millions of users. The incident, linked to the Shiny Hunters extortion group, highlights risk from third-party cloud environments and misconfigured services. ***Prevention Tips:*** *Regularly audit cloud configurations, restrict third-party access, and implement strong monitoring to detect unauthorized data access and misconfigurations early.*

- **Public Safety/Financial:** [AI-Driven Cyber Attacks](#) - The financial and business sector has been facing with an increase in AI-driven cyber-attacks, such as deepfake voice fraud targeting wire transfers, and synthetic identity fraud bypassing KYC controls. ***Prevention Tips:*** *Implement Know Your Customer (KYC) fraud detection upgrades to identify synthetic identities and AI-generated fake applicants.*

Recommended Tools and Federal Resources

- CISA Protective DNS Resolver– Blocks access to known malicious domains by filtering DNS traffic, helping organizations prevent phishing, malware, and command-and-control communications before a connection is established.
- NIST Risk Management Framework (RMF) – A structured process that helps organizations identify, assess, and manage cybersecurity risk across systems.
- CIS Critical Security Controls (CIS Controls) - A prioritized set of best practices designed to help organizations defend against the most common cyber threats and improve overall security posture.

Emerging Trends to Watch

- *Credential Abuse & Management Plane Attacks* – Attackers avoid attacking a system and instead use valid credentials fetched from breach dumps, phishing, or password spraying. This gives attackers an easy way in with access to these exposed accounts permission levels so they can target systems without setting off any flags. ***Prevention Tips:*** *Enforce phishing-resistant MFA across all privileged accounts with consistent auditing and rotation.*
- *Expansion of AI Attack Surface (Agent & Tool Abuse)*– Attackers are beginning to target software and integrations widely dependent on by companies and developers. Rather than targeting peripheral devices, attackers have shown patience in poisoning widely depended upon packages to gain access. ***Prevention Tips:*** *Mark dependency version with lockfiles, stop auto-installing latest version and use a package scanner such as Socket or Snyk for suspicious package behavior. Isolate third-party integrations with least permissions required.*
- *Insider Ransomware Negotiators* - Hacker groups have begun employing ransomware negotiators to provide sensitive information to the group in order to further increase the profit that the hacker group could gain from the ransomware, all without the victims knowledge. ***Prevention Tips:*** *Vet ransomware negotiation firms thoroughly, log and review all communication the negotiator has with the attackers, split your communication across different channels so no party has full picture of the attack.*