Public Transportation ISAC Daily Open-Source Cyber Report

By APTA • Jun 15, 2026

Smart Brevity® count: 5.5 mins...1463 words

This issue brings you the latest developments in cybersecurity threats, underscoring the ongoing need for vigilance.

CISA Adds One Known Exploited Vulnerability to Catalog

Image credit: Cybercory

15 June 2026

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

- CVE-2026-35273 Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability

This type of vulnerability is a frequent attack vector for malicious cyber actors and poses significant risks to the federal enterprise.

Binding Operational Directive (BOD) 26-04: Prioritizing Security Updates Based on Risk establishes vulnerability management requirements for Federal Civilian Executive Branch (FCEB) agencies, updating BOD 22-01. BOD 26-04 reinforces the importance of the KEV catalog and requires federal agencies to prioritize rapid remediation of high-risk vulnerabilities, specifically those identified by Common Vulnerabilities and Exposures (CVEs) listed in CISA's Known Exploited Vulnerabilities (KEV) catalog on publicly exposed assets that grant total control of the asset post-exploitation, while deferring action for lower-risk vulnerabilities. BOD 26-04 further establishes basic expectations for when agencies must check whether threat actors compromised the system before the patch was applied.

While BOD 26-04 applies only to FCEB agencies, CISA encourages all organizations to adopt risk-based vulnerability management and prioritize remediation of KEV catalog vulnerabilities. CISA will continue to add vulnerabilities to the catalog that meet the specified criteria.

Read full article here

FBI disrupts massive AI-powered phishing service using a million URLs

Image credit: Bleeping Computer

14 June 2026

In a major cybercrime bust, the FBI, along with Google and Black Lotus Labs, dismantled the Outsider Enterprise, a Chinese phishing-as-a-service operation using thousands of websites to steal sensitive data.

Why it matters: The operation led to over $1.9 billion in losses, affecting millions of users globally.

- The FBI's action is part of Operation Riptide, targeting cybercrime infrastructure.
- Thousands of phishing domains now redirect to an FBI page, disrupting criminal activities.

The big picture: Outsider Enterprise employed AI and phishing kits to impersonate trusted brands, impacting users worldwide.

- Google linked 9,000 fake websites and over a million URLs to this operation.
- A civil lawsuit and collaboration with telecom providers aim to block fraudulent messages.

Details: The FBI seized servers, payment wallets, and a Telegram bot used by the network.

- Google is pushing for anti-scam legislation, including the Stop SCAMS Act, to enhance legal protections against AI-enabled fraud.
- Android's AI defenses continue to warn users and block malicious messages.

Read full article here

GAO: DHS cyber modernization efforts bolster resilience

Image credit: GAO

12 June 2026

DHS cyber modernization bolsters resilience: The U.S. Government Accountability Office (GAO) highlights how DHS's cybersecurity programs, like CISA's CDM and CyberSentry, enhance federal network defenses amidst evolving threats.

- **Challenges:** Programs face cost increases and schedule changes, with staffing declines impacting oversight and operations.

GAO findings on DHS programs: The GAO report reveals that DHS cybersecurity programs have adjusted baselines and increased costs by $11.4 billion, primarily due to added capabilities and unforeseen expenses.

- **Program progress:** Despite challenges, most programs are meeting revised goals, with key performance milestones achieved.

Program hurdles amidst dynamic environment: DHS programs navigate a rapidly changing landscape, balancing modernization with risk management and mission delivery.

- **Oversight changes:** Reorganization within DHS affects program oversight, while funding levels shape execution.

Future outlook: Continued investment in cybersecurity is crucial as government networks face sophisticated threats.

- **Budget impact:** Funding constraints and workforce reductions could hinder program advancements.
- **Ongoing monitoring:** GAO will continue to track DHS's acquisition efforts and program performance.

Read full article here

Ransomware attacks jump 48%, overall cyberattack activity declines

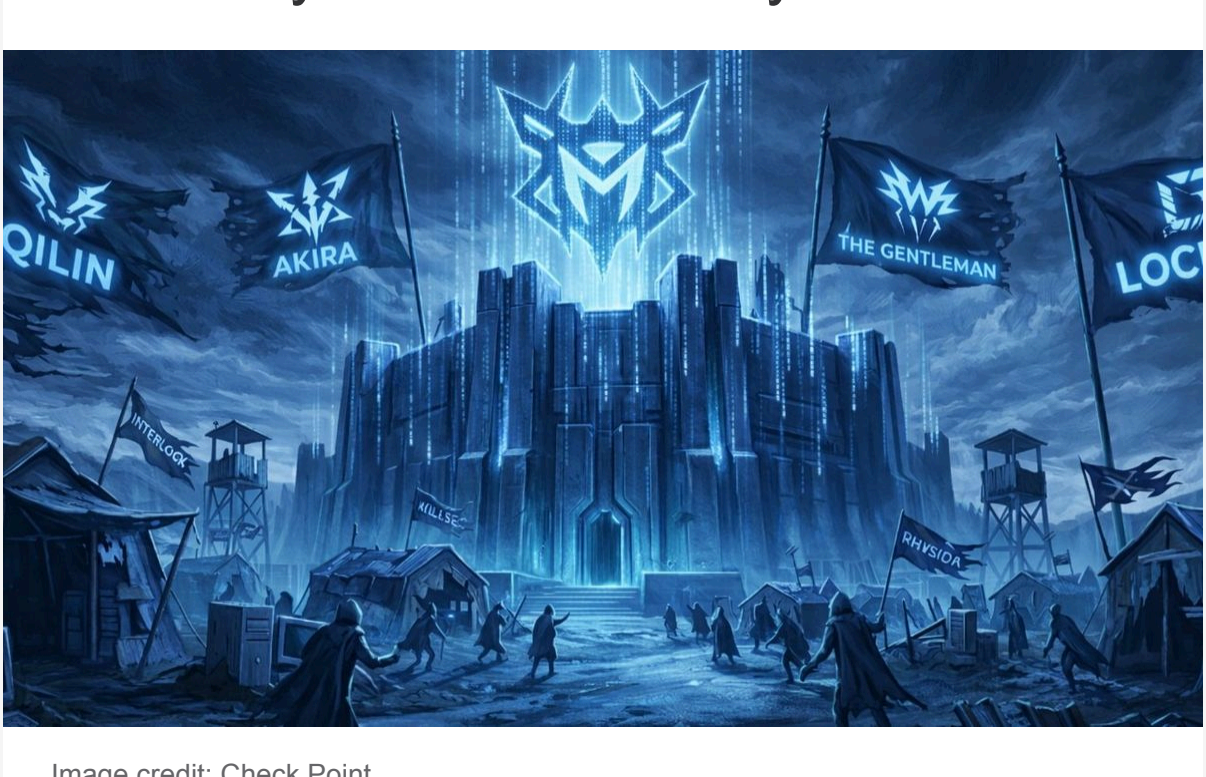

Image credit: Check Point

12 June 2026

Global cyberattack activity eased in May 2026 after a sharp rebound in April, according to Check Point Research.

Why it matters: The ransomware landscape is fragmenting, with 61 active groups in May alone, presenting a volatile threat to organizations worldwide.

- Ransomware attacks jumped 48% from the previous year, the highest year-over-year growth rate in 2026.
- Business services were hit hardest, accounting for 35% of victims.

By the numbers: The top three ransomware groups, Qilin, The Gentlemen, and DragonForce, accounted for 39% of attacks.

- Qilin led with 14% of attacks and The Gentlemen rose to second followed by DragonForce.
- The other 61% of ransomware attacks were distributed across 58 additional active groups, a level of fragmentation that reflects just how industrialized and competitive the ransomware market has become.

The big picture: As sectors like agriculture and hospitality digitize, they are becoming prime targets, with agriculture seeing a 51% surge in attacks.

- Latin America tops attack rates with 3,149 weekly attacks, a 13% increase from the previous year.
- Rapid digitalization continues to outpace security maturity, emphasizing the need for a prevention-first, AI-powered security strategy.

Read full article here

Chinese hackers hijack auth flow, spy on isolated network for a decade

Image credit: Bleeping Computer

13 June 2026

Chinese hackers, part of the Velvet Ant group, infiltrated an isolated critical infrastructure network, maintaining access for a decade.

Why it matters: This breach demonstrates the vulnerabilities in authentication systems, even those without direct internet access.

- Velvet Ant executed a sophisticated attack by backdooring Linux PAM and OpenSSH components, ensuring persistent access.
- Their operations highlight the importance of securing login systems as critical security assets.

The attack chain: Initial compromise occurred via internet-facing servers, with Velvet Ant deploying a modified GS-Netcat reverse shell for encrypted access.

- The group used a SOCKS5 proxy for network traffic tunneling, allowing reach to internal systems.
- A unique aspect was modifying Nginx configurations to establish a remote execution path into the isolated network.

Complex cleanup: The extensive replacement of critical components made remediation challenging, risking operational outages.

- Organizations are advised to protect authentication components with EDR, file integrity monitoring, and multi-factor authentication.
- Sygnia recommends planning for offline recovery with strict backup protocols.

Bottom line: This incident underscores the need for continuous monitoring and stringent security measures to prevent long-term breaches.

Read full article here

Ukrainian pleads guilty in Conti ransomware case

Image credit: Bleeping Computer

12 June 2026

A Ukrainian national, extradited from Ireland, has admitted to conspiracy charges in the U.S. over his role in the Conti ransomware operation.

Why it matters: The Conti group was among the most prolific cybercrime gangs, affecting over 1,000 victims and gathering $150 million in ransoms.

- Lytvynenko's plea highlights the persistent international efforts to combat cybercrime, notably impacting healthcare, government, and business sectors.

Driving the news: Oleksii Lytvynenko, 44, pleaded guilty to wire fraud conspiracy, admitting to deploying ransomware and possessing stolen data from U.S. and international victims.

- He was involved in coding malware for the group's attacks, underscoring the technical sophistication of these operations.

Zoom out: The Conti gang emerged from the Ryuk group and was linked to the TrickBot syndicate, notorious for large-scale attacks.

- After shutting down due to leaks and law enforcement pressure, its members splintered into other ransomware groups.

What's next: Lytvynenko's extradition and plea may lead to a maximum 20-year imprisonment, further deterring cybercrime activity and signaling continued global legal actions against such threats.

Read full article here

Other Cyber News of Interest

Image credit: Adobe Stock

Emerging Threats

What The FIFA World Cup 2026 Means for Fraud

Over 80% of Sports Organizations Targeted by Hackers in the Last Year

Fancy Bear Hackers Abuse EdgeRouters and Cloud Services to Launch Stealthy Cyberattacks

ShinyHunters Uses Oracle Zero-Day to Rampage Universities

Pharma giant Novo Nordisk discloses breach of clinical trials data

Critical Vulnerabilities

Over 400 Arch Linux packages compromised to push rootkit, infostealer

Palo Alto PAN-OS Vulnerability Allows Attackers to Execute Arbitrary Commands as Root User

Microsoft Outlook and Word Vulnerabilities Allow Attackers to Execute Malicious Code

phpBB forum fixes auth bypass bug lurking for a decade

Microsoft fixes Windows update failures linked to WUSA installer

Agentjacking Attack Tricks AI Coding Agents into Running Malicious Code

Mitigation

US Gov asks Anthropic to ban foreign national access to Fable, Mythos

Senate proposes bill to require CISA updates to critical infrastructure cybersecurity plans amid AI-driven threats

Maine disables data breach notification portal after fake disclosures

Cyber Studies

Claroty finds authentication bypass, RCE flaws in Vertiv UPS management cards that could disrupt data center operations

Cyberattack disrupts Mackay Sugar operations, exposing growing agri-industrial cyber risks

Latest cybersecurity advisories and notices

Image credit: IoT World Today

Latest CISA cybersecurity and advisories here.

Latest Microsoft security updates here.

Latest Drupal security advisories here.

Latest CISCO security advisories here.

Latest SUSE security advisories here.

Latest UBUNTU security notices here.

Latest Checkpoint advisories here.

Latest Red Hat product Errata notices here.

Latest zero-day initiative advisories here.

.

NOT FOR PUBLIC DISSEMINATION

TSA Transportation Security Operations Center 866- 615- 5150 and TSOC.ST@tsa.dhs.gov

For questions regarding this product and/or if you know someone interested in joining and receiving this product contact the PT-ISAC at PT-ISAC@APTA.com.

Disclaimer: This product contains news articles compiled from open-source and commercially available information. Information contained is for situational awareness only and does not represent the views of the PT ISAC. Only the analyst comments represent the views of the PT-ISAC.