Public Transportation ISAC Daily Open-Source Cyber Report

By APTA • Jun 11, 2026

Smart Brevity® count: 5 mins...1305 words

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

CISA: Patch smarter, not harder

Image credit: Industrial Cyber

11 June 2026

Artificial intelligence is accelerating the discovery of software vulnerabilities, challenging defenders to keep up. According to Verizon's 2026 Data Breach Investigations Report, only 26% of vulnerabilities in CISA's Known Exploited Vulnerabilities (KEV) Catalog were fully remediated in 2025, a decrease from the previous year's 38%.

Why it matters: Security teams need to adapt quickly to manage risks in the evolving threat landscape.

- The median resolution time for vulnerabilities has increased to 43 days.

CISA's directive: CISA's Binding Operational Directive 26-04 introduces a new framework prioritizing security updates based on risk, allowing agencies to defer lower-priority vulnerabilities.

- Agencies focus on vulnerabilities with public exposure, full automation potential, system control risks, and real-world exploitation evidence.

The approach: This framework emphasizes vulnerabilities at the network's edge, addressing threats effectively without compromising core networks.

- Threat actors often exploit configurations and credentials rather than product vulnerabilities.

Outcome: The directive represents a significant advancement in federal vulnerability management, enabling automation and scaling of security practices to counter AI-driven threats.

Read full article here

CISA issues new directive prioritizing security updates based on risk

Image credit: CISA

10 June 2026

The Cybersecurity and Infrastructure Security Agency (CISA) has released Binding Operational Directive 26-04, urging federal civilian agencies to enhance their vulnerability management policies.

Why it matters: Cyber threat actors exploit unpatched vulnerabilities, and AI's role in narrowing response times makes proactive measures crucial.

- This directive aligns vulnerability management with risk reduction strategies to maintain cybersecurity integrity.

The directive's focus: The new directive consolidates previous guidelines to prioritize high-risk vulnerabilities, ensuring efficient patching efforts.

- Incorporates factors like threat actor capabilities and asset deployment in network.

What's next: CISA will monitor compliance and support federal agencies in implementing the directive.

- Emphasizing the need to check for compromises before applying patches.

Driving the news: As part of CISA's response to the evolving threat landscape, the directive aims to expedite cybersecurity defenses of federal information systems in line with the Executive Order on AI Innovation and Security.

Read full article here

FBI seizes China-linked consulting sites targeting US clearance holders

Image credit: FBI

10 June 2026

The Justice Department and FBI have seized 13 fake consulting websites allegedly targeting US clearance holders to extract sensitive information.

Why it matters: The operation, linked to Chinese intelligence, posed a significant threat to national security by attempting to recruit Americans with access to classified data.

- These sites masqueraded as consulting firms offering vague consultancy roles to lure in current and former US government personnel.
- After the shutdown, visitors to these domains are now met with an FBI notice.

The big picture: The scheme began in November 2023, using fake company websites and social media to recruit individuals who might divulge information beneficial to the People's Republic of China.

- Job titles such as "Senior Analyst" and "International Affairs Consultant" were used to make the roles appear legitimate.
- The Justice Department's press release details the use of false personas, stolen identities, and AI-generated profiles to mask the operation.

What's next: Federal authorities are investigating the involvement of overseas accounts and the alleged bribery, identity theft, and money laundering linked to this scheme.

- The operators of these sites deny any foreign government ties, but scrutiny continues.

Read full article here

Microsoft Defender RoguePlanet zero-day grants SYSTEM privileges

Image credit: LinkedIn

10 June 2026

A new zero-day exploit, RoguePlanet, has emerged just after Microsoft's June 2026 Patch Tuesday, threatening Windows 10 and 11 systems.

Why it matters: This vulnerability, discovered by researcher Nightmare Eclipse, allows attackers to gain SYSTEM privileges through Microsoft's Defender, posing a significant security risk.

- The exploit works via a race condition, with a proven success rate on some devices.

The backdrop: Cybersecurity firm ThreatLocker confirmed the exploit's effectiveness on fully patched Windows 11 systems, showcasing its potential impact.

- RoguePlanet was initially a remote code execution vulnerability, targeting Defender's handling of remote SMB shares.

What's next: Microsoft is investigating and committed to protecting customers by addressing these security issues promptly.

- Organizations are advised to use application allowlisting as a preventative measure.
- The ongoing dispute between the researcher and Microsoft highlights the challenges in vulnerability disclosure practices.

Read full article here

Oracle PeopleSoft servers hacked in ShinyHunters data theft attacks

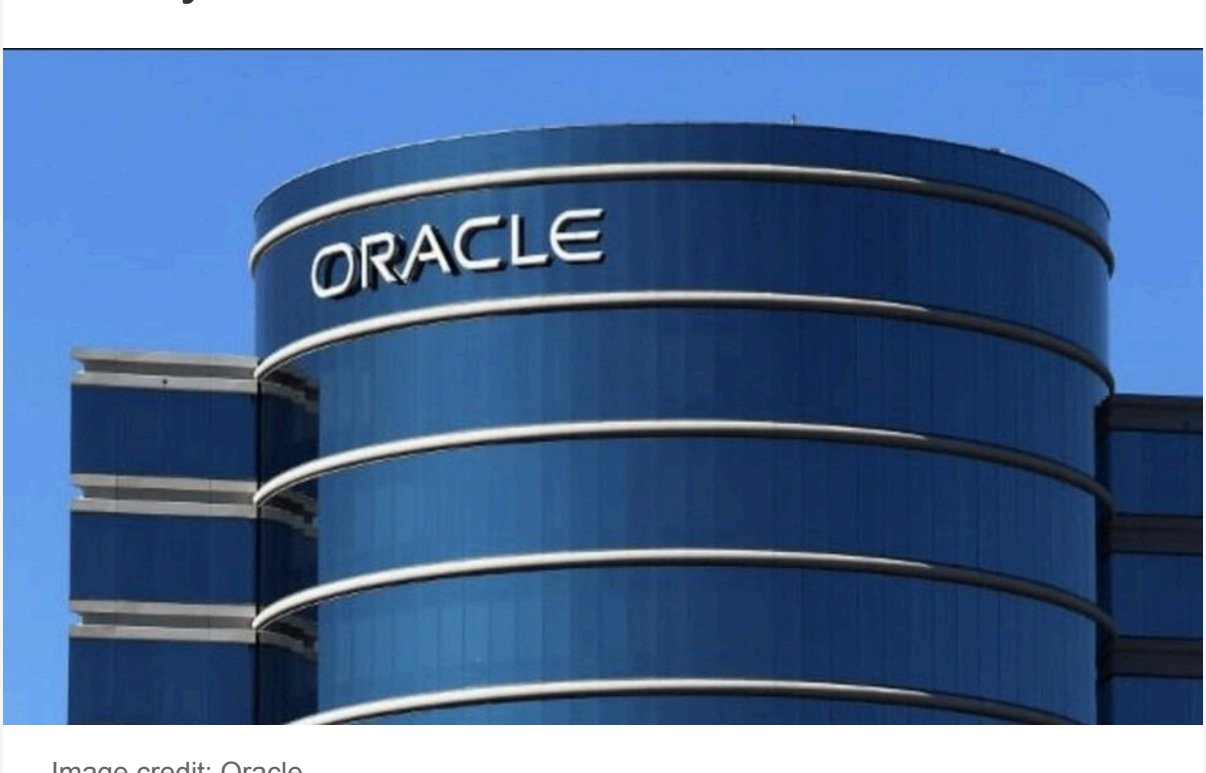

Image credit: Oracle

10 June 2026

Oracle PeopleSoft servers are being targeted by the ShinyHunters extortion gang, which claims to have stolen data from over 100 organizations.

Why it matters: These attacks pose significant cybersecurity risks to large organizations that rely on PeopleSoft for critical business operations.

- The education sector is notably impacted with several institutions already facing extortion demands.

Details: ShinyHunters uses a gadget chain of old and zero-day vulnerabilities for these attacks, claiming to have breached 300 instances.

- Nottingham University is among the victims with data already leaked publicly.

What's next: Organizations should urgently analyze logs for connections from the listed IP addresses to assess potential compromises.

- Immediate incident response is advised if indicators of compromise are discovered, including temporary removal of affected servers from internet access.

Read full article here

China-linked JDY botnet expands targeting of U.S. networks

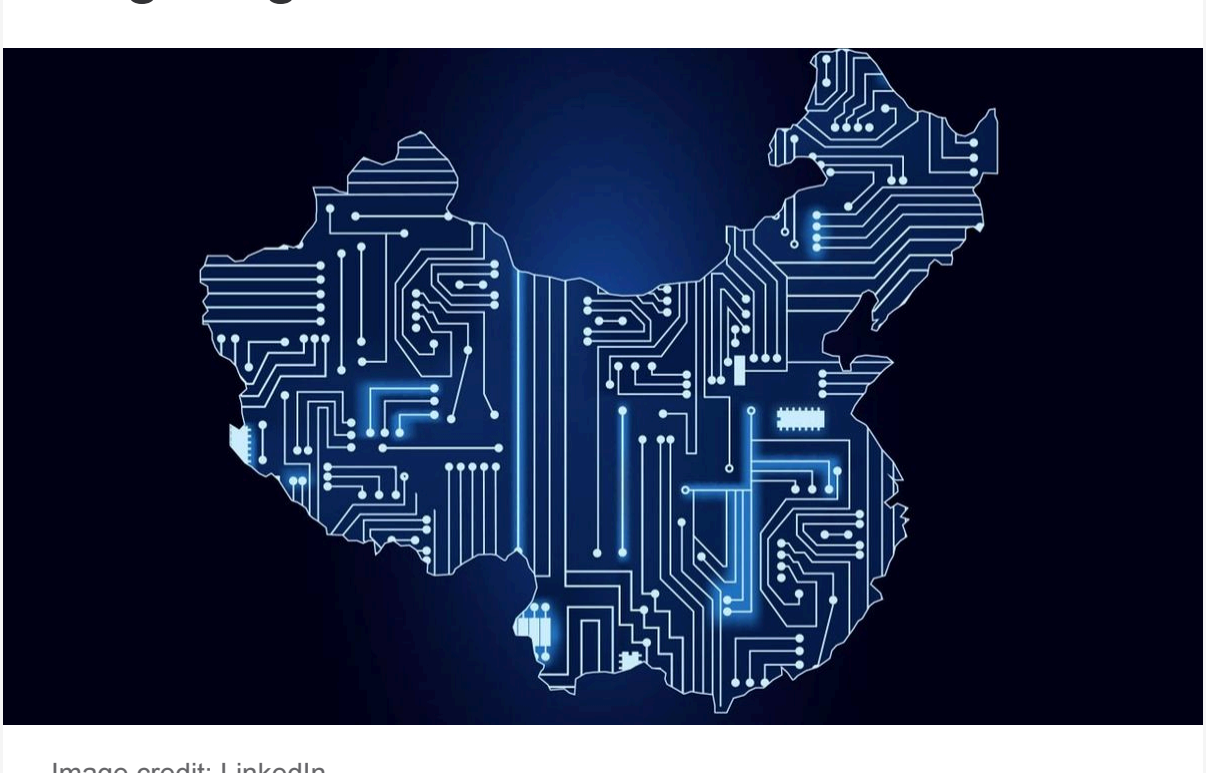

Image credit: LinkedIn

10 June 2026

The JDY botnet, linked to Chinese threat actors like Volt Typhoon, is broadening its reach in the U.S., focusing on military and associated networks.

Why it matters: The botnet has grown from 650 to over 1,500 compromised devices since January 2024, highlighting its rapid expansion and strategic targeting of vulnerable infrastructure.

- JDY is a distributed scanning network, not relying on sheer numbers but on identifying vulnerabilities post-public disclosures.
- U.S. military and associated networks are primary targets, raising national security concerns.

The big picture: CISA has warned about the risks posed by Volt Typhoon operatives to SOHO routers, underscoring the need for robust security measures.

By the numbers: Lumen researchers observed JDY scans rapidly targeting newly disclosed flaws, like CVE-2026-35616, shortly after Fortinet's disclosure.

- The botnet's control through hidden Tor services and use of tools like Platypus indicates sophisticated operations.

What's next: Organizations must update security patches and restrict unnecessary internet access to prevent recruitment into reconnaissance networks. Monitoring for unusual outbound scanning is crucial to defense.

Read full article here

Other Cyber News of Interest

Image credit: Adobe Stock

Emerging Threats

Chinese, North Korean Threat Groups Build on Asia-Pacific Success

Chinese influence operation used ChatGPT to stir debate on data centers

The Miasma worm source code briefly leaked on GitHub

ServiceNow Flaw Exploited to Gain Access to Customer Instances

Cyberattack shuts down major Australian sugar mills, disrupting harvest

Critical Vulnerabilities

Microsoft: Some Windows PCs fail to install latest monthly updates

Microsoft patches Exchange Server zero-day exploited in attacks

GitHub announces npm security changes to tackle supply-chain attacks

Ivanti: Max severity Sentry flaw allows code execution as root

Critical HVAC, UPS Vulnerabilities Could Let Hackers Disrupt Data Centers

Mitigation

Microsoft patches YellowKey, GreenPlasma, MiniPlasma zero-days

SSEN Transmission joins ENCS to strengthen cybersecurity collaboration across critical energy infrastructure

Cyber Studies

Energy and utilities sector targeted in 66% of observed APT campaigns, as Mustang Panda, Lazarus, Sandworm remain active

OT cybersecurity becomes a board-level priority as industrial security maturity rises

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.