Public Transportation ISAC Daily Open-Source Cyber Report

By APTA • Jun 09, 2026

Smart Brevity® count: 5 mins...1329 words

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

CISA Adds Two Known Exploited Vulnerabilities to Catalog

Image credit: Cybercory

9 June 2026

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

- CVE-2026-42271 BerriAI LiteLLM Command Injection Vulnerability
- CVE-2026-50751 Check Point Security Gateway Improper Authentication Vulnerability

These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risks to the federal enterprise.

Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities established the KEV Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise. BOD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the BOD 22-01 Fact Sheet for more information.

Although BOD 22-01 only applies to FCEB agencies, CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of KEV Catalog vulnerabilities as part of their vulnerability management practice. CISA will continue to add vulnerabilities to the catalog that meet the specified criteria.

Read full article here

White House unveils AI security strategy

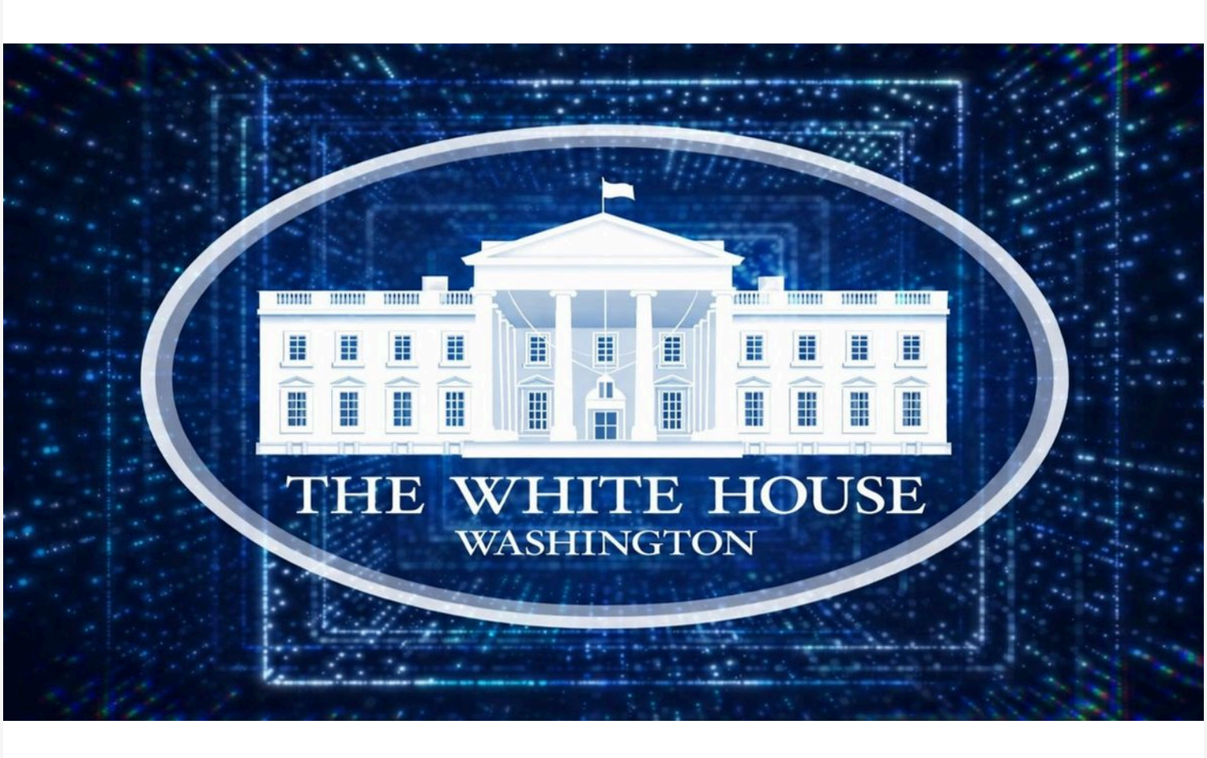

Image credit: Industrial Cyber

8 June 2026

The White House has rolled out an AI security strategy to bolster cybersecurity across both government and private sectors in response to the rise of advanced AI technologies.

Why it matters: AI advancements introduce new national security challenges that necessitate coordinated efforts between federal agencies and the private sector.

- The focus is on safeguarding American intellectual property and upgrading digital infrastructures to counter external threats.

What's new: The strategy includes developing voluntary partnerships with AI developers and increasing the use of AI-enabled defenses.

- This approach aims to maintain U.S. leadership in AI while minimizing regulatory burdens.

Driving the news: Executive Order 14409 directs federal agencies to work collaboratively with the private sector, emphasizing the protection of national security systems and critical infrastructure.

- It also establishes a framework for the secure deployment of frontier AI models and calls for AI cybersecurity enhancements.

Go deeper: The administration plans to create an AI cybersecurity clearinghouse and prioritize enforcement of cybercrime laws against AI misuse.

- Developers are encouraged to voluntarily engage with the government to assess AI models' security implications before public release.

Read full article here

Qilin claims hack of the Shipping Association of New York & New Jersey

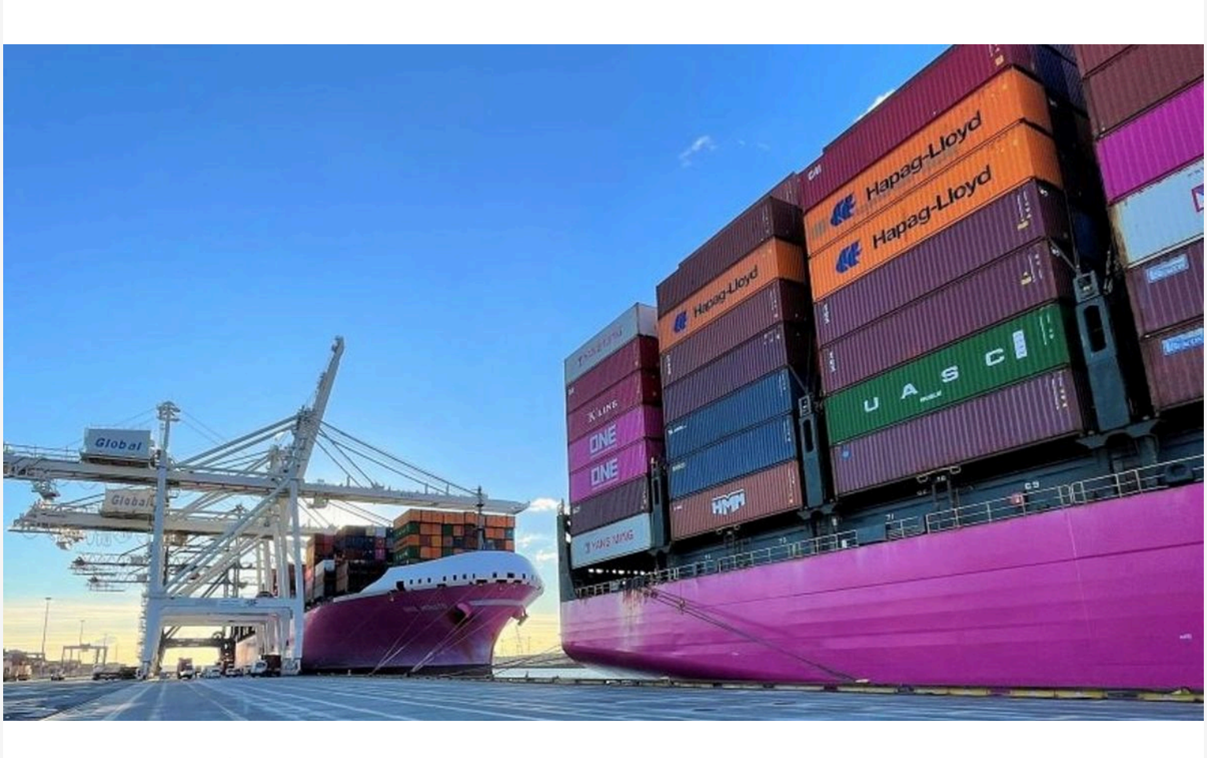

Image credit: SANYNJ

8 June 2026

The Qilin ransomware gang claims to have hacked the Shipping Association of New York & New Jersey (SANYNJ), a key player in North America's maritime industry.

Why it matters: The breach raises alarms over cybersecurity vulnerabilities in critical transportation infrastructure.

- SANYNJ, linked to one of North America's busiest ports, is now listed on Qilin's ransomware leak site.

Details: While Qilin shared limited information, they claim to have stolen data from the organization, though the link to the data was broken at the time of reporting.

- SANYNJ represents vital elements of maritime operations, including terminal operators and ocean carriers.

The backdrop: The Department of Homeland Security has warned of increased threats to the maritime sector and recent alerts from CISA highlight risks from Russian state-sponsored actors targeting Western logistics.

What's next: Monitoring and enhancing cybersecurity measures are crucial as threats to logistics and transportation continue to evolve. Organizations need to stay vigilant and prepared against potential cyberattacks.

Read full article here

ShinyHunters leak BCD Travel customers' data

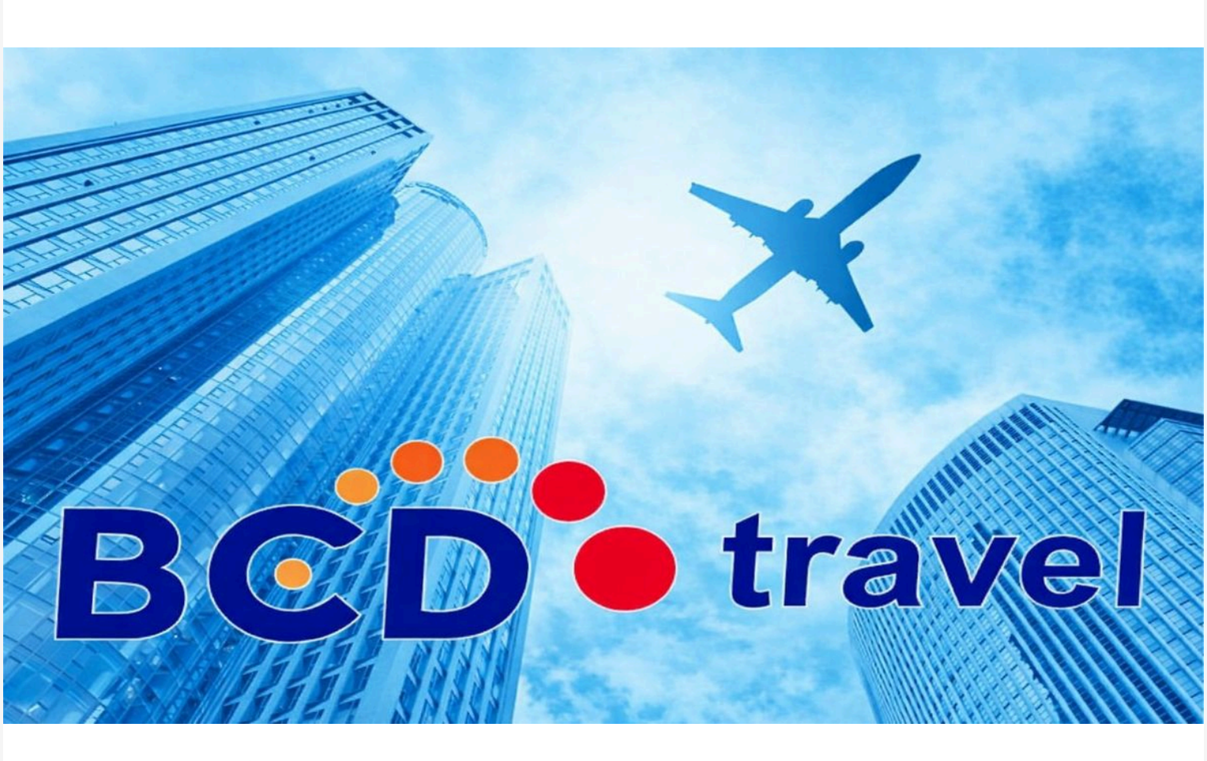

Image credit: BCD Travel

8 June 2026

Ransomware extortion group ShinyHunters published the personal information of approximately 396,000 customers of Dutch business travel agency BCD Travel on the dark web.

- BCD Travel is one of the largest business travel agencies in the world.
- At the end of May, ShinyHunters claimed to have exfiltrated over 30GB of compressed data.

Why it matters: This leak underscores the growing threat of ransomware attacks on global travel, exposing vulnerabilities in data protection.

- Nearly 400,000 customer records, including names, emails, and phone numbers, were compromised.
- The attackers leaked the data after BCD Travel failed to meet a ransom deadline.

The big picture: ShinyHunters is notorious for targeting large organizations, adding new victims to its list regularly.

- Recent targets include telecom providers and international institutions, highlighting the group's broad reach.

What's next: Organizations must bolster cybersecurity measures to prevent data breaches and protect customer information from such threats.

Read full article here

Qilin linked to VPN flaw exploitation

Image credit: Bleeping Computer

8 June 2026

Israeli cybersecurity company Check Point has issued critical security updates to patch a flaw affecting Remote Access VPN and Mobile Access, exploited in zero-day attacks.

Why it matters: This vulnerability, tracked as CVE-2026-50751, allows unauthorized remote access by bypassing authentication on targeted VPNs and firewalls.

- Affects only deployments using the deprecated IKEv1 protocol without machine certificates.
- Attacks began May 7 and surged in June, impacting a few dozen organizations, with links to the Qilin ransomware.

Details: Check Point found another vulnerability, CVE-2026-50752, affecting certificate validation in IKEv1, potentially exploitable in man-in-the-middle attacks.

What's next: Customers are urged to apply updates immediately.

- Remove support for legacy clients and enforce IKEv2.
- Mandate Machine Certificate Authentication and enable IPS.
- Download the latest signatures to mitigate potential threats.

Read full article here

New Pink hacking group attacking enterprise users, impersonate IT staff

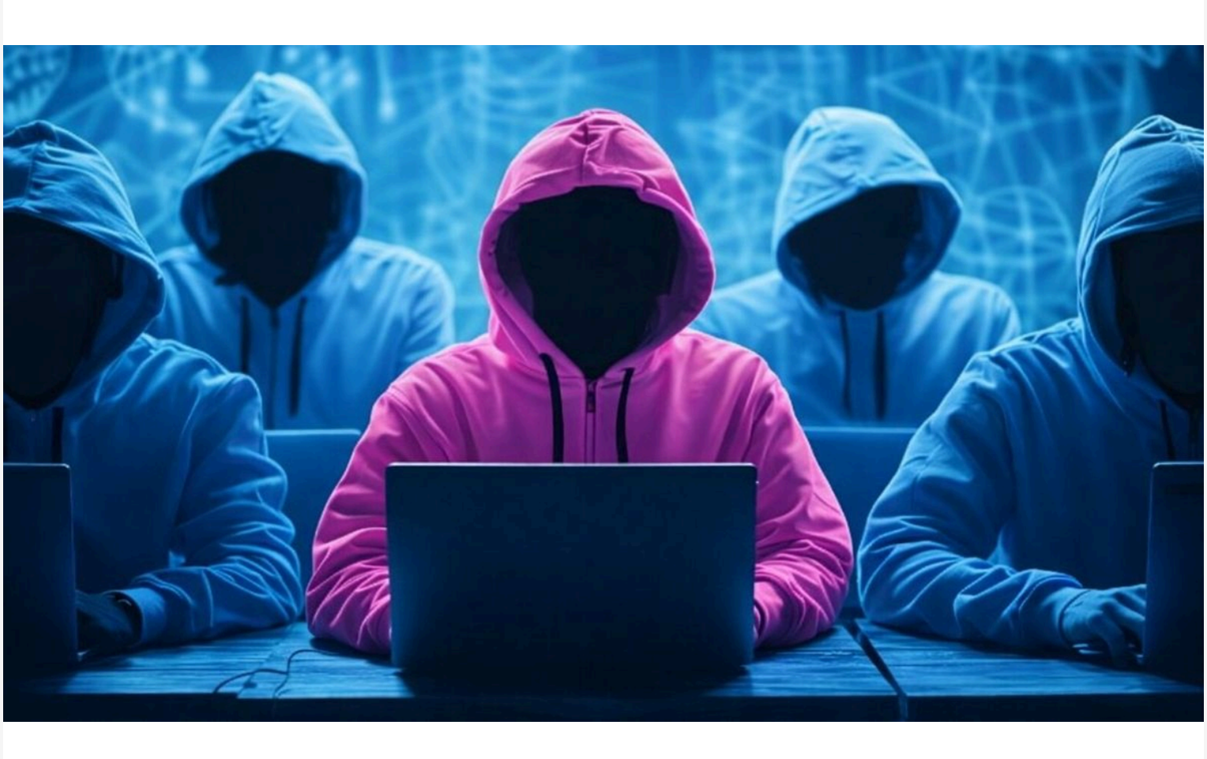

Image credit: LinkedIn

8 June 2026

A newly identified extortion group, Pink, has emerged as a serious threat to enterprise organizations, using social engineering tactics to steal cloud storage credentials and sensitive data.

Why it matters: Pink's tactics exploit human trust rather than technical vulnerabilities, making it particularly dangerous.

- The group impersonates internal IT staff over the phone, tricking employees into visiting attacker-controlled phishing pages.
- Once access is gained, Pink uses Microsoft's automation tools to sweep through cloud storage environments, quickly extracting data.

The big picture: Pink appears to be affiliated with the broader Com network, known for aggressive social engineering campaigns.

- The group also shares tactical similarities with other well-known threat actors such as Lapsus$, Scattered Spider, and ShinyHunters.

Protect your organization: Security experts recommend a people-first approach, including training employees to verify unexpected calls and using phishing-resistant authentication methods like FIDO2 keys.

Indicators of compromise: Pink's indicators of compromise.

Read full article here

Other Cyber News of Interest

Image credit: Adobe Stock

Emerging Threats

Hackers keep focus on 2026 FIFA World Cup and fans

WhatsApp says NSO targeted users with spearfishing attacks in violation of court order

'Hades' Campaign Against PyPI Puts New Spin on Shai-Hulud

North Korean Hackers Use Fake Coding Tasks to Steal Credentials

Over 20,000 Instagram accounts stolen in Meta AI support hack

Critical Vulnerabilities

One-Character Linux Kernel Flaw Enables Root Access, Exploits Now Public

Chrome Patches 429 Vulnerabilities Including 22 Critical Ones

Anthropic AI coding assistant could be tricked into revealing secrets, Microsoft warns

AI chatbot searches leading users to scam websites

Gogs patches critical zero-day enabling remote code execution

Critical UniFi OS bug lets hackers gain root without authentication

Mitigation

OpenAI Unveils ChatGPT Account Security Controls

New Apple feature automatically changes your compromised passwords

VS Code Adds 2-Hour Extension Auto-Update Delay to Limit Supply Chain Attacks

Cyber Studies

Scoping Water Sector Intrusions and the Need for Cyber-Physical Intelligence

Frontier AI, cyber defense, and critical infrastructure resilience take center stage in House hearing

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.