Public Transportation ISAC Daily Open-Source Cyber Report

By APTA • Jun 04, 2026

Smart Brevity® count: 5 mins...1390 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

4 June 2026

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

- CVE-2026-45247 Mirasvit Full Page Cache Warmer Deserialization of Untrusted Data 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) 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

U.S. sanctions crypto exchange used by IRGC ransomware groups

Image credit: Department of the Treasury

3 June 2026

The U.S. Treasury's Office of Foreign Assets Control (OFAC) has sanctioned Nobitex, Iran's largest cryptocurrency exchange, for facilitating payments tied to terrorist activities.

Why it matters: Nobitex played a key role in evading economic sanctions and was linked to the Islamic Revolutionary Guard Corps (IRGC) through ransomware transactions.

- It processed over 50% of Iranian digital asset inflows in 2025, aiding the regime's terrorist activities and sanctions evasion efforts.

Details: Nobitex also assisted Iran's central bank in accessing stablecoins, propping up the rial's value, and allowing regime insiders to evade international sanctions.

- The U.S. government's "Economic Fury" campaign also targets other Iranian exchanges: Wallex, Bitpin, and Ramzinex.

What's next: U.S. allies and foreign companies may face pressure to cease dealings with these entities as the sanctions take effect.

- The pro-Israel "Predatory Sparrow" group claimed to have hacked Nobitex, stealing $90 million in digital assets, highlighting the exchange's vulnerabilities.

Read full article here

China's intelligence uses online job platforms to lure Five Eyes nationals

Image credit: Bleeping Computer

3 June 2026

China targets Five Eyes personnel: Using online job platforms, China's military intelligence seeks to recruit individuals with access to classified or privileged information.

- **Five Eyes:** Individuals with access to sensitive information in the US, Canada, United Kingdom, Australia, and New Zealand.
- **Who is at risk:** Security clearance holders, military personnel, and those with indirect access to government information including academics, journalists, and people in the security and economic sectors.
- **Recruitment tactics:** Online ads lead to virtual interviews, probing for sensitive details, and requests for reports on strategic topics.

Why it matters: Even non-classified information can risk lives and national security, highlighting the threat to economic prosperity and democratic processes.

- **Consequences:** Individuals involved face legal actions, job losses, and clearance revocations if not reported.

Reporting incidents: Contact your corporate security office if targeted. National security agencies are coordinating with security offices to address this threat. In Canada, contact the RCMP National Security Information Network. In the US, contact the FBI or a local FBI office.

Read full article here

Chinese hackers use new Atlas RAT malware in cyberattacks

Image credit: LinkedIn

3 June 2026

A Chinese-speaking cybercrime group, TA4922, has broadened its attacks to Europe, introducing new malware and the Atlas backdoor.

Why it matters: TA4922's shift underscores a growing threat landscape, with financial motives driving diverse operations.

- The group targets networks for fraud, data theft, and selling access, now focusing on Germany, Italy, the UK, and South Africa.

The big picture: TA4922's activities have surged since March, with an unprecedented operational tempo.

- Proofpoint highlights overlaps with groups like Silver Fox, yet TA4922's distinct cybercrime focus sets it apart.

Atlas RAT and custom loaders: The malware arsenal includes Atlas RAT, offering capabilities like system reconnaissance and file theft.

- Techniques include anti-sandbox checks, keylogging, and webcam recording, with RomulusLoader deploying additional payloads.

What's next: TA4922's campaigns are poised to continue evolving, leveraging large language models for malware development.

- Indicators of compromise and C2 infrastructure details are included in Proofpoint's report.

Read full article here

FBI-flagged phishing kit Kali365 expands its reach

Image credit: Bleeping Computer

3 June 2026

The operators of Kali365, a phishing-as-a-service platform that drew recent FBI attention for helping attackers bypass multifactor authentication (MFA) on Microsoft 365 accounts, have significantly broadened both their capabilities and their target list.

- FBI PSA: Kali365 Phishing-as-a-Service Kit Hijacks Microsoft 365 Access Tokens

Why it matters: Kali365 now poses a broader threat, compromising accounts across AWS, Okta, Xerox, DocuShare, and Russian platforms like MAX Messenger.

- This expansion highlights an increased risk to both Western enterprises and Russian consumer platforms.

The big picture: Device code phishing, used by Kali365, exploits authentication workflows of devices without full browsers.

- Attackers trick victims into entering codes on legitimate sites, bypassing MFA safeguards.

What's next: Arctic Wolf advises comprehensive security training to combat these sophisticated phishing tactics.

- Organizations should be vigilant in spotting malicious activities related to Kali365.

Read full article here

AI-powered cybercrime tools surge on dark web

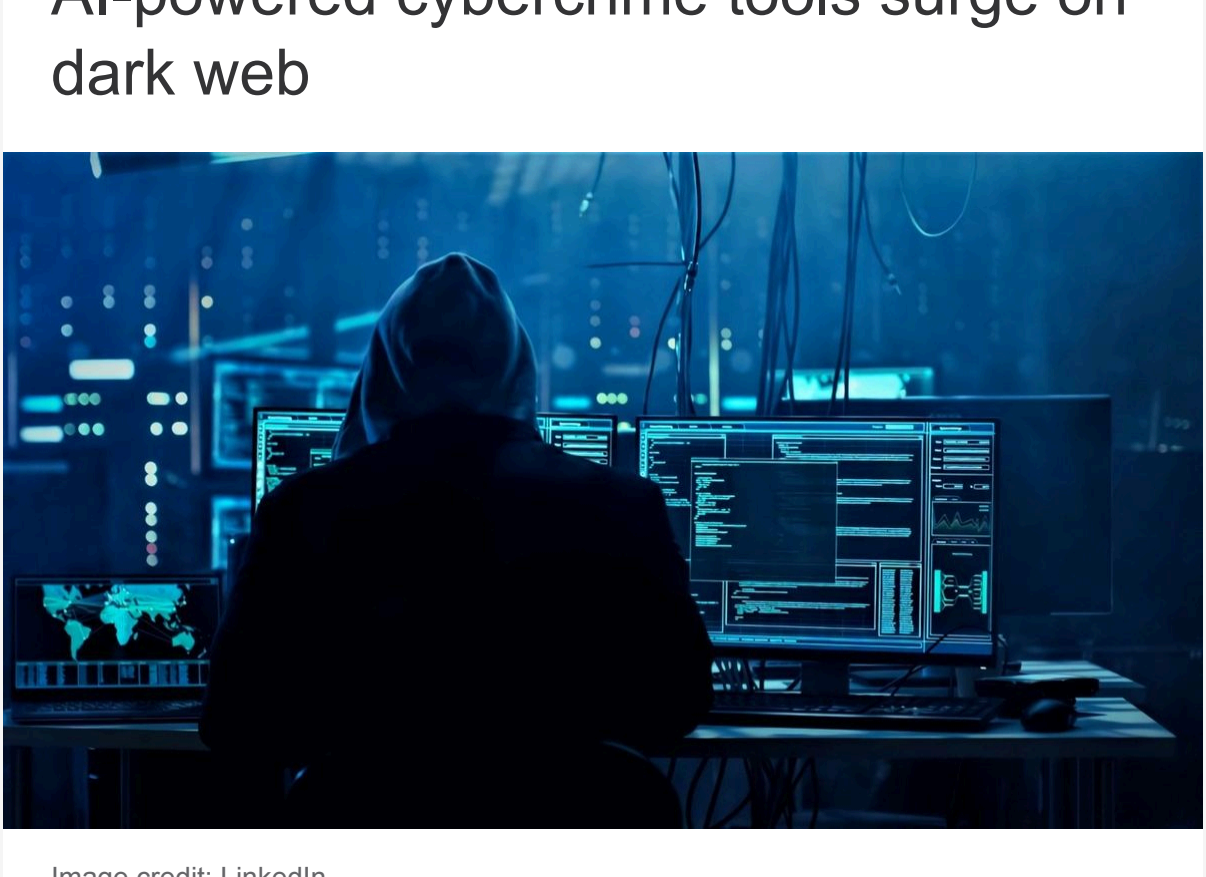

Image credit: LinkedIn

3 June 2026

The dark web is seeing a rise in AI-powered cybercrime tools bolstered by a robust price-tiered marketplace according to leading cybercrime experts and a recent Halcyon study.

Why it matters: The surge in AI-driven tools shows a sophisticated market, making cybercrime more accessible and harder to combat.

- **Explosive growth:** Posts mentioning AI tools jumped from 38 in December to 1486 in February, an increase of over 3810%.
- **Automated services:** These tools offer automated distribution, freemium options, and tiered pricing, lowering entry barriers for criminals.

What cybercriminals are selling:

- **Weaponized LLMs:** AI models hacked to perform malicious tasks, including new systems like WormGPT.
- **AI-enabled identity fraud:** Deepfakes for bypassing security measures, with some tools boasting a 92% success rate.
- **AI-augmented malware:** Live operational tools like AI-powered call centers capable of 25 languages.
- **Jailbroken AI services:** Cheap offerings on the dark web, with ChatGPT accounts starting at 10 cents.

Mitigation: Organizations must bolster defenses against low capability actors and sophisticated groups, focusing on:

- **AI-based protection:** Use AI to defend against accelerated attacks.
- **Verification protocols:** Reorient society around phone calls as primary attack vectors.
- **Policy and partnerships:** Coordination between public and private sectors is crucial for disruption.

Read full article here

Other Cyber News of Interest

Image credit: Adobe Stock

Emerging Threats

The Gentlemen Ransomware Group Uses Fortinet Exploits, AI, and Custom C2 Frameworks

Hackers Targeted Global Stock Exchange in Espionage Operation

New 'HTTP/2 Bomb' DoS attack crashes web servers in under a minute

Attackers Use AI to Automate EDR Evasion Testing

Google DoubleClick Abused in New Malspam Campaign to Deliver DesckVB RAT

Critical Vulnerabilities

Immediate Patching Urged as Microsoft 365 Android Apps Let Any App Steal Account Tokens via Leftover Debug Flag

VS Code zero-day lets hackers steal GitHub tokens in one click

Acer working to patch max severity zero-days in Wave 7 routers

Unpatched Windows Search URI Vulnerability Lets Attackers Steal NTLMv2 Hashes

WhatsApp, Slack Notifications Could Hijack Google Gemini on Android

Autonomous AI Tool Finds 2-Year-Old RCE Flaw in Redis (CVE-2026-23479)

Mitigation

Google adds Android protection against AI deepfake scam calls

Notorious Spanish Hacker Alcasec Jailed for 31 Months Over Data Theft

Police dismantle 9 crime groups in illegal streaming crackdown

Cyber Studies

Cyber Insurance Rates Are Dropping, but Exclusions Widen

Industrial cyber risk demands new governance approaches as operational environments become more interconnected

Cyber adversaries shift from data theft to operational disruption as industrial crown jewels come under siege

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.