Public Transportation ISAC Daily Open-Source Cyber Report

By APTA • Jun 02, 2026

Smart Brevity® count: 5 mins...1369 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

2 June 2026

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

- CVE-2024-21182 Oracle WebLogic Server Unspecified Vulnerability

This type of vulnerability is a frequent attack vectors 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

ENISA report finds cybersecurity maturity rising across critical sectors

Image credit: ENISA

1 June 2026

The EU Agency for Cybersecurity (ENISA) released its latest report, showing steady improvements in cybersecurity maturity across critical sectors.

Why it matters: As organizations adapt to evolving policy requirements and cyber threats, sectors like banking, electricity, and telecommunications lead in maturity.

- Trust services, aviation, and financial market infrastructures have recently moved into the high maturity band.
- Significant improvements in maturity were recorded across several sectors including rail, road transport, aviation, and maritime.

Driving the news: The report identifies key factors advancing cybersecurity, such as legislative developments and increased political focus.

- Despite progress, maturity varies significantly across sectors due to skill shortages and sector-specific challenges.
- The maritime and rail sectors remain exposed due to the complexity of their operating environments, which involve close coordination among infrastructure operators, transport providers, and technology suppliers.
- Dependence on long-lived operational technology and information technology systems, together with extensive supply chain relationships, increases vulnerability to cyber threats.

What's next: ENISA expects continued enhancements as cybersecurity legislation and organizational efforts drive investment and preparedness.

- More sectors are anticipated to emerge from the risk zone, improving overall cyber resilience.

Read full article here

Anthropic to Open Mythos AI to ENISA

Image credit: LinkedIn

1 June 2026

The European Union is on the brink of accessing Anthropic's cutting-edge AI model, Mythos, through the Project Glasswing initiative for cybersecurity advancements.

Why it matters: Mythos has the potential to revolutionize cybersecurity by autonomously detecting and exploiting vulnerabilities at unmatched speed.

- This access allows the EU to gain critical insights into AI-assisted vulnerability research, essential for bolstering defenses against sophisticated cyberattacks.

The big picture: With access to Mythos, ENISA becomes the first EU entity integrated into Project Glasswing, highlighting the importance of international cooperation in cybersecurity.

- Anthropic's decision aligns with broader efforts to prepare for the influx of AI models capable of significant impact on global security.

What's next: Ongoing negotiations between Anthropic and the European Commission aim to finalize safe access terms for ENISA.

- These discussions are key to ensuring Mythos is utilized effectively and responsibly within the EU's cybersecurity framework.

Read full article here

Russia FSB group Gamaredon hides worm in Windows data streams

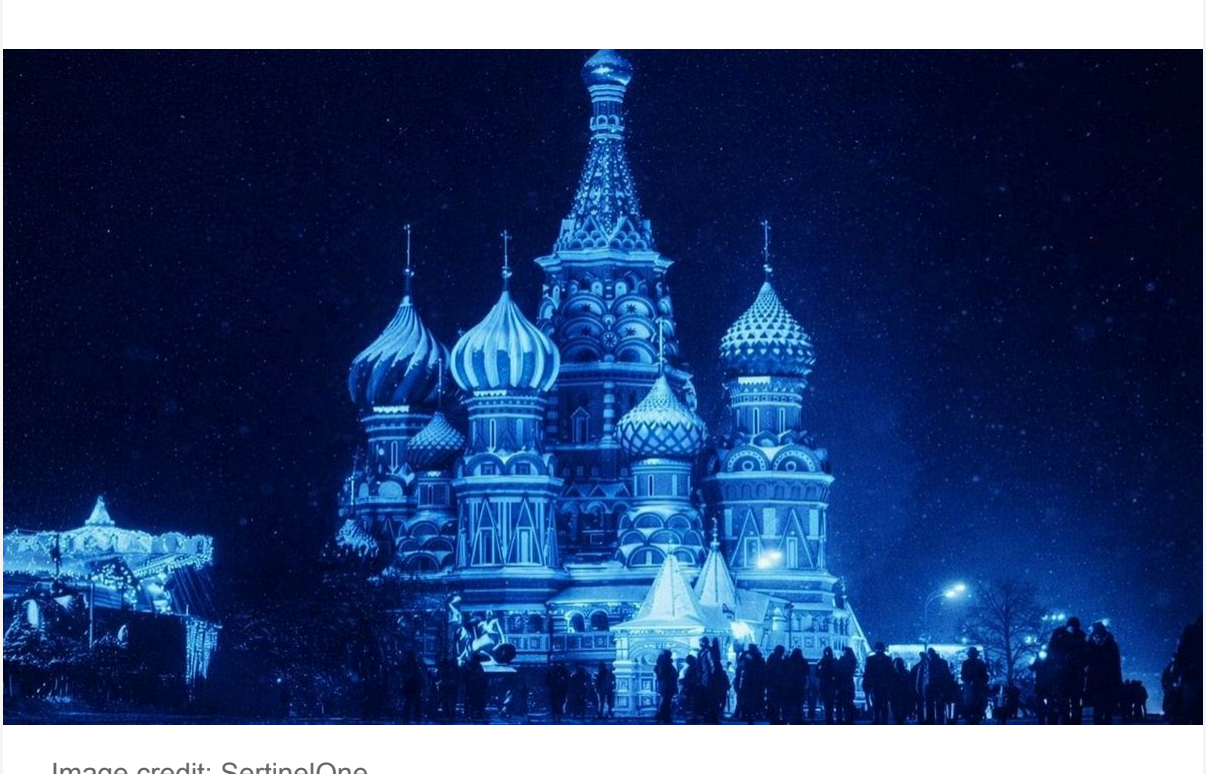

Image credit: SertinelOne

1 June 2026

A Russian state-linked worm is stealthily spreading across networks, using a Windows file feature to remain undetected.

Why it matters: This development poses a significant threat to governments and critical infrastructure, highlighting the ongoing tension and cybersecurity challenges.

- The worm, known as GammaWorm, is linked to Russia's Federal Security Service (FSB) through the espionage group Gamaredon.
- It utilizes fileless VBScript and NTFS Alternate Data Streams to conceal its presence.

Intrusion tactic: The attack begins with an xHTML file that deploys a malicious RAR archive exploiting a WinRAR flaw.

- This flaw, CVE-2025-8088, has been associated with other Russian cyber groups like Sandworm.
- The hidden HTA file in the Startup folder triggers the next phase, maintaining stealth.

Countermeasures: Sekoia recommends organizations to wipe infected systems completely and update WinRAR to version 7.13 or later.

- GammaWorm's use of Dead Drop Resolvers allows constant payload updates, complicating cleanup efforts.
- Proactive measures are crucial to prevent persistent threats.

Read full article here

DriveSurge uses ClickFix and fake updates to infect website visitors

Image credit: LinkedIn

1 June 2026

A newly identified threat actor, DriveSurge, is compromising thousands of legitimate websites, pushing malware onto unsuspecting visitors using fake browser updates and a social engineering trick known as ClickFix.

Why it matters: DriveSurge's sophistication and scale make it particularly dangerous.

- It silently injects malicious code into high-reputation websites, affecting browsers like Chrome, Firefox, and Safari.
- The operation uses a Traffic Distribution System to profile visitors and deliver targeted attacks.

The latest: Silent Push researchers report DriveSurge as the key driver of a surge in ClickFix and Fake Update campaigns.

- Operating as an Initial Access Broker, DriveSurge uses a Pay-Per-Install model to monetize infections.

Details: The campaign's infrastructure is built with obfuscation techniques and a failover system to ensure infection even if a delivery domain goes down.

- It targets both Windows and macOS, using multi-stage payloads to avoid detection.

What's next: Organizations should monitor for unusual JavaScript injections and audit third-party scripts to mitigate these threats.

- DriveSurge: Indicators of Compromise

Read full article here

The Gentlemen RaaS features advanced encryption, self-propagation

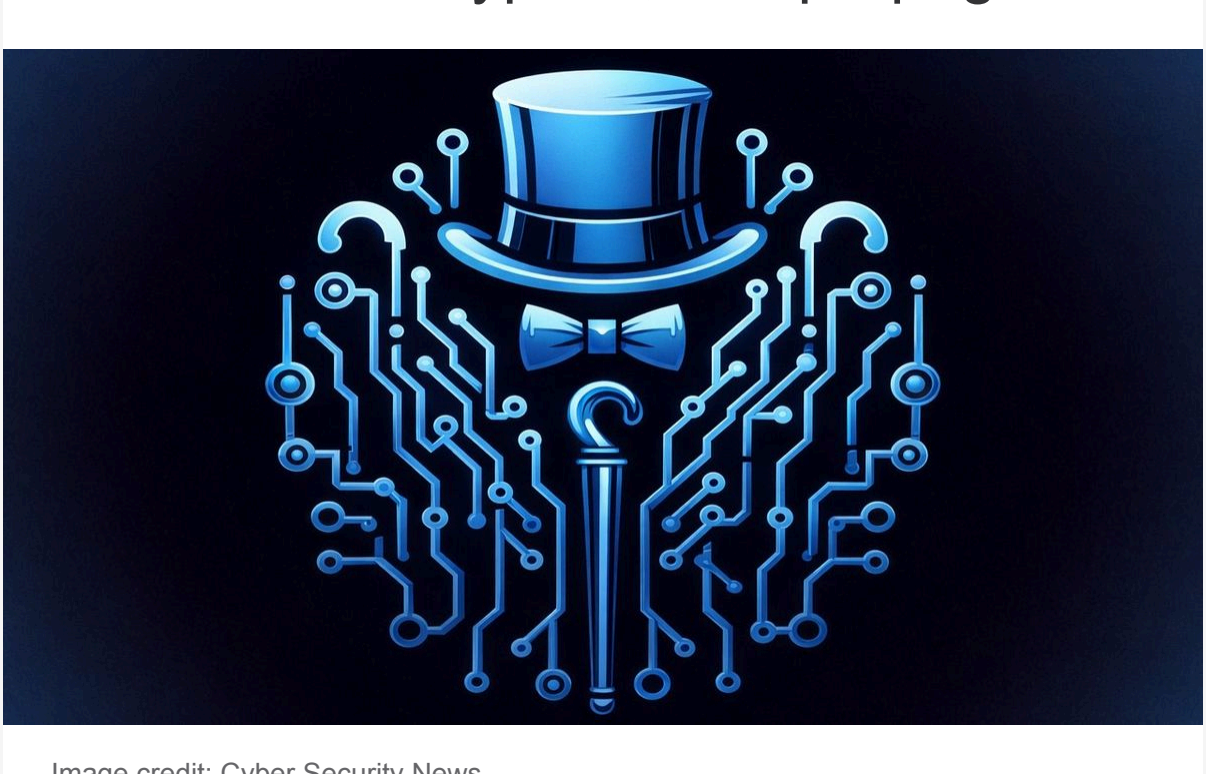

Image credit: Cyber Security News

1 June 2026

Microsoft Threat Intelligence warns of a growing ransomware-as-a-service (RaaS) operation, The Gentlemen, tracked as Storm-2697.

- The Gentlemen combine robust file encryption with aggressive self-propagation, jeopardizing entire enterprise networks.

Why it matters: The Gentlemen's advanced encryption and lateral movement techniques significantly heighten the threat level, spreading rapidly once initial access is gained.

- The Gentlemen use a hybrid cryptographic model that combines Curve25519 elliptic-curve cryptography with the XChaCha20 stream cipher.
- When the self-propagation feature is enabled, the ransomware transforms into a worm-like threat for lateral movement across reachable systems.

The big picture: Emerging in mid-2025, it evolved into a RaaS platform, recruiting affiliates to scale attacks.

- It targets sectors like transportation, education, healthcare, and finance globally, using data theft and double extortion techniques to increase victim pressure.
- Its partnership with BreachForums expands its reach, involving penetration testers and initial access brokers.

What's next: Organizations must adopt robust ransomware defense strategies.

- Implementing strong credential hygiene, system hardening, and layered security controls can mitigate the impact.
- Enabling cloud-based threat intelligence and machine learning protections enhances detection of new ransomware variants.

Read full article here

Other Cyber News of Interest

Image credit: Adobe Stock

Emerging Threats

China-Aligned Groups Ramp Up Attacks: Dragon Weave Hits Czech Republic and Taiwan

North Korean Famous Chollima Hackers Target PHP Developers Using Compromised Packagist Package

Critical Windows Netlogon RCE flaw now exploited in attacks

Unknown hacker group targeted Russian maritime universities, diplomats for nearly two years

Fake McAfee emails refuse to die as new round of phishing emails targets consumers

Critical Vulnerabilities

Microsoft investigates Office Apps, Teams file access issues

Critical Windows Netlogon Vulnerability in Attackers' Crosshairs

Miasma Supply Chain Attack Compromises Red Hat npm Packages with Credential-Stealing Worm

OpenAI Codex Authentication Tokens Stolen in codexui-android npm Supply Chain Attack

Dashlane password manager users locked out by brute force attacks

Mitigation

Microsoft fixes outage affecting MFA setup, MySignIn service

Spain arrests doxer leaking sensitive data of govt employees

Cyber Studies

Recent Palo Alto Networks Vulnerability Exploited for Weeks

Attackers Abuse Docker and Kubernetes Misconfigurations to Compromise Host Systems

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.