Powered by AXIOS HQ

Public Transportation ISAC Daily Open-Source Cyber Report

By APTA • Jun 01, 2026

Smart Brevity® count: 5 mins...1292 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

1 June 2026

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

- CVE-2026-0257 Palo Alto Networks PAN-OS Authentication Bypass 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

Funding and staffing shortages slow public sector cybersecurity initiatives

Image credit: Linkedin

29 May 2026

A SANS Institute survey reveals that only one in three public sector cybersecurity initiatives is fully funded, despite increasing cyber threats and operational demands.

Why it matters: Funding and staffing shortfalls hinder the ability of government cybersecurity programs to effectively respond to threats.

- Limited budgets force security leaders to prioritize risks, often leaving critical areas underprotected.

By the numbers:

- 63% of respondents cite budget limitations as a primary obstacle.
- More than half report difficulty recruiting and retaining qualified professionals.
- 27% of organizations report breaches directly linked to these capability gaps.
- Only 22% of organizations rate themselves as capable of executing their cybersecurity strategies at scale.

What's next: Addressing these gaps requires prioritizing workforce development, automation, and technology integration to transform strategic frameworks into operational capabilities.

- Organizations must secure resources to advance from mid-level maturity to optimized cybersecurity operations.

Read full article here

Chinese hackers exploit Iran conflict to target maritime and energy sectors

Image credit: SecurityWeek

29 May 2026

Cybersecurity firm ESET reports that Chinese-backed hacking groups are exploiting the Middle East conflict to target maritime and energy sectors.

- China-aligned groups were being used to improve Beijing's visibility into maritime, energy and political developments in the region.

Why it matters: These cyber incursions are part of China's broader strategy to enhance its influence and gather intelligence in key global industries.

- The Gulf region's geopolitical landscape makes it a critical area for state-backed cyber activities.

Broader scope: Beyond the Middle East, Chinese espionage is targeting Central American governments and South Korean tech firms, aligning with Beijing's strategic goals.

Regional focus: Cyber operations in Syria and Latin America underscore China's interest in regional stability and commercial opportunities.

Global repercussions: These continuous cyber efforts reflect China's ambition to monitor and control pivotal sectors worldwide.

Read full article here

Kimsuky deploys new malware in latest campaigns

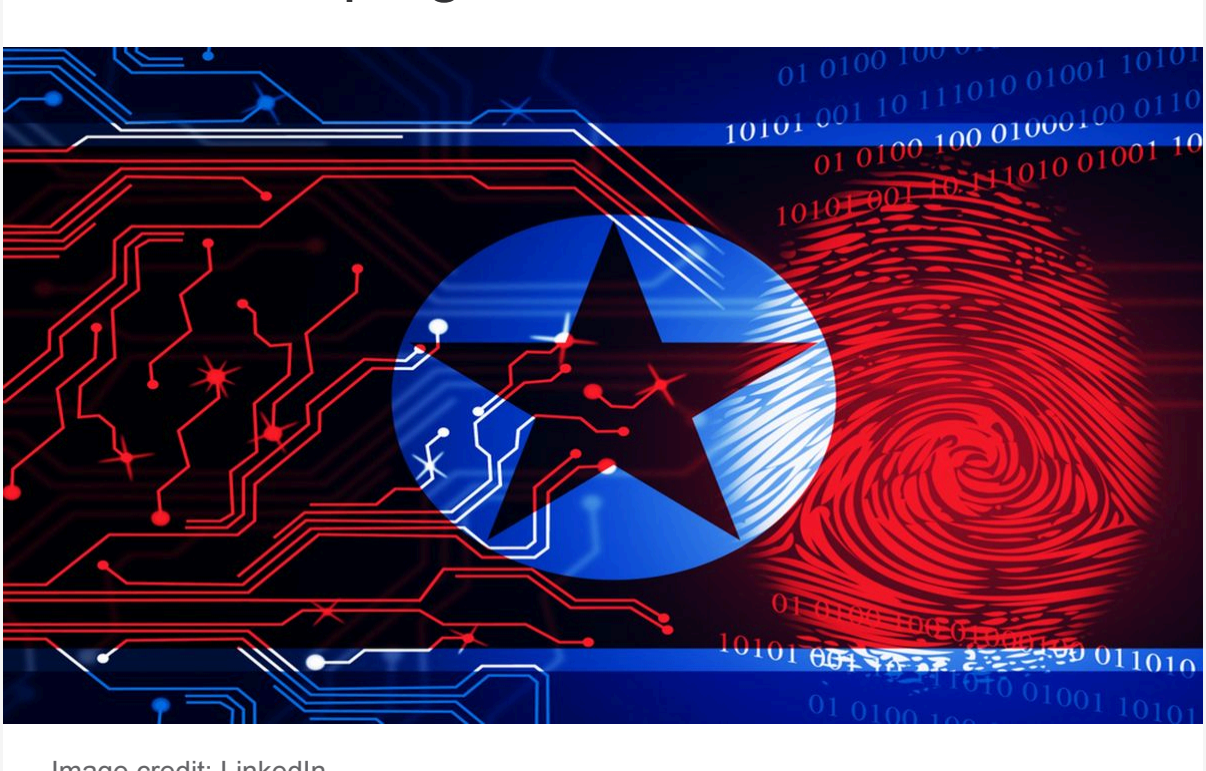

Image credit: LinkedIn

29 May 2026

North Korea's Kimsuky group has unleashed a series of sophisticated cyber attacks on South Korean military and corporate entities through March and April 2026.

Why it matters: These attacks showcase Kimsuky's ability to evolve and adapt, posing a significant threat to national security and corporate stability.

- The group employs advanced social engineering tactics, including spoofing security software and creating fake Webex meeting pages.

Driving the news: Kimsuky has been using a known malware family, HTTPSpy, disguised as South Korean security software installers.

- This tactic has been a consistent strategy since 2023, targeting messaging administrators with fake security tools.

What's new: In March, the group mimicked a South Korean B2B messaging service, while in April, they impersonated Cisco Webex, urging users to download malicious scripts.

- Both campaigns aimed to deliver HTTPSpy, a remote access trojan with extensive capabilities.

The bottom line: Kimsuky's adaptive strategies and use of advanced tools like JSONPing and HelloDoor indicate a persistent and evolving threat landscape, requiring vigilant cybersecurity measures.

Read full article here

JINX-0164 using LinkedIn social engineering to deploy macOS malware

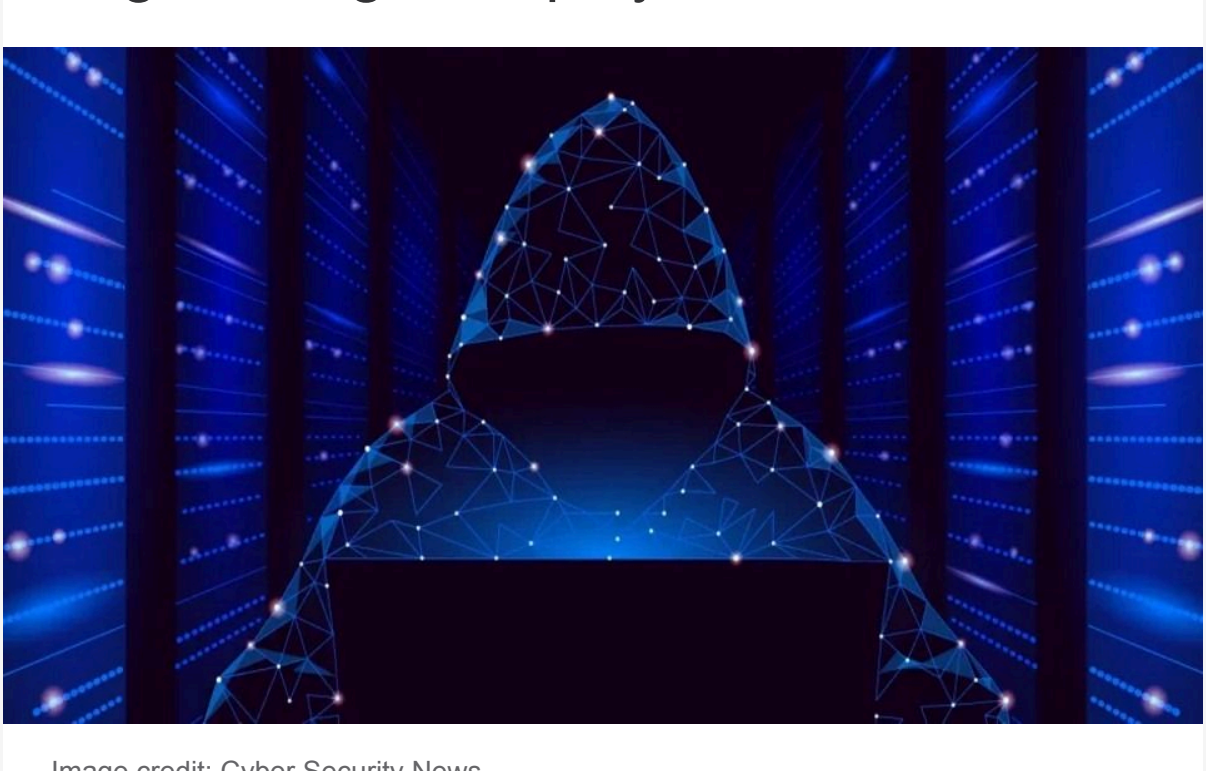

Image credit: Cyber Security News

29 May 2026

A new threat actor, JINX-0164, is targeting organizations using LinkedIn to deploy custom macOS malware.

Why it matters: This attack chain endangers the software development pipeline by combining social engineering with credential theft and supply chain sabotage.

- Developers are tricked via LinkedIn into downloading malware, compromising sensitive data.
- The operation further threatens organizations by integrating into their development infrastructure.

The big picture: The group's malware, AUDIOFIX, steals browser credentials and API tokens, while MINIRAT provides remote access. Both are specifically designed for macOS.

- These tools leverage encrypted communications and VPNs to avoid detection, making attribution difficult.

What's next: Organizations should deploy Endpoint Detection and Response solutions and enable audit logging.

- Security teams must monitor for suspicious VPN usage and unverified GitHub commits.
- Enabling GitHub Vigilant Mode can aid in detecting developer impersonation attempts.
- JINX-0164: Indicators of Compromise.

Read full article here

Dutch police dismantle massive botnet controlling 17 million devices

Image credit: Netherlands National Police

29 May 2026

A proxy botnet of 17 million devices has been taken offline following a successful operation by the Dutch National Police and the National Cyber Security Centre (NCSC).

The big picture: The botnet, controlling a vast network of infected routers, smartphones, and IoT devices, was operated through over 200 servers, masking cyberattacks as legitimate consumer traffic.

- Devices with trusted residential IPs were exploited to hide DDoS attacks, phishing, and malware distribution.

Why it matters: Cybercriminals' use of trusted consumer equipment, such as routers and smartphones, presents challenges for detection and prevention.

- The operation highlights the importance of robust security measures to prevent devices from becoming part of a botnet.

What's next: To protect your device, keep systems updated and use strong, unique passwords with two-factor authentication.

- Download software only from trusted sources and avoid suspicious links or attachments.
- Regularly check antivirus software to see which devices are connected to your network.

Read full article here

Other Cyber News of Interest

Image credit: Adobe Stock

Emerging Threats

Russian spies are aggressively seeking western technology as sanctions bite

ChatGPT share links abused to host fake outage pages to deliver malware

Fake Anthropic Sites Deliver Fileless Infostealer to Claude Code Users

The Com cyberattacks support violence and exploitation

Phishing email led to a breach of US food giant Rich Products

Critical Vulnerabilities

Notepad++ requires urgent update: hackers swapping configs to run malware

Exploit Code Published for Critical Flowise RCE Vulnerability

New CIFSwitch Linux flaw gives root on multiple distributions

WP Maps Pro bug exploited to create admin accounts on WordPress sites

Mitigation

Microsoft Releases KB5089573 for Windows 11 to Fix Patch Tuesday Install Issues

Google Chrome adds session cookie theft protection for all users

Scam broker sells data on 7M elderly Americans, gets 10 years in prison

Cyber Studies

With Complex Cloud Integrations, Small Errors Lead to Major Compromises

GitHub Service Abuse in Ongoing Vishing Campaigns

Darktrace identifies rising cyber exposure tied to AI-driven manufacturing operations

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.

Powered by AXIOS HQ