Week of May 19, 2025

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources

CISA Welcomes Madhu Gottumukkala as the New Deputy Director

www.cisa.gov

The Cybersecurity and Infrastructure Security Agency (CISA) is proud to announce the appointment of Madhu Gottumukkala as its new Deputy Director. In this role, he will help lead CISA's mission to understand, manage, and reduce risk to the cyber and physical infrastructure that the American people rely on every day.

NSA and others are releasing:
RUSSIAN GRU TARGETING WESTERN LOGISTICS ENTITIES AND TECHNOLOGY COMPANIES
CYBERSECURITY ADVISORY

NSA and Others Publish Advisory Warning of Russian State-sponsored Cyber Campaign Targeting Western Logistics

www.nsa.gov

FORT MEADE, Md. - The National Security Agency (NSA) is joining several United States and foreign entities to release the Cybersecurity Advisory (CSA), "Russian GRU Targeting Western Logistics Entities and Technology Companies," to call attention to ...

NSA and others are releasing:
AI DATA SECURITY: BEST PRACTICES FOR SECURING DATA USED TO TRAIN & OPERATE AI SYSTEMS
CYBERSECURITY INFORMATION SHEET

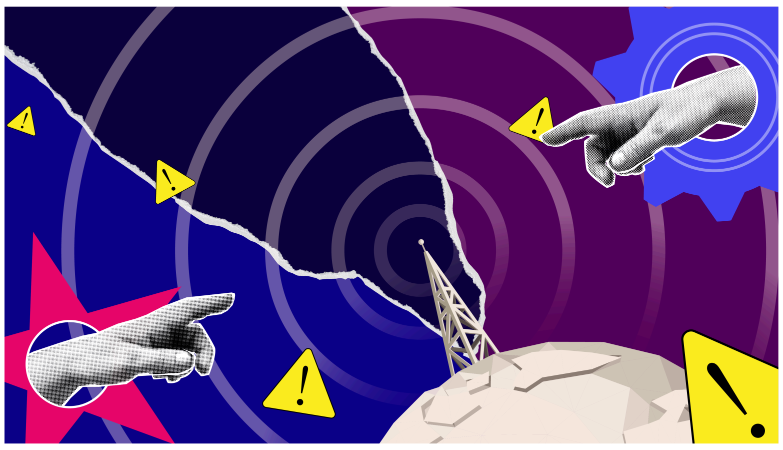
NSA's AISC Releases Joint Guidance on the Risks and Best Practices in AI Data Security

www.nsa.gov

FORT MEADE, Md. – The National Security Agency's Artificial Intelligence Security Center (AISC) is releasing the joint Cybersecurity Information Sheet (CSI), "AI Data Security: Best Practices for Securing Data Used to Train & Operate AI Systems," to ...

Cybercrimes, Scams & Incidents

Headlines related to cybercrimes and scams including international cybersecurity news and high-profile incidents like ransomware and malware attacks



'Whatever we did was not enough': How Salt Typhoon slipped through the government's blind spots

cyberscoop.com

Yet multiple sources told CyberScoop that there were failings that helped Salt Typhoon ultimately carry out their plan. "Arguably, clearly, whatever we did was not enough," said a former senior U.S. cybersecurity official, who nonetheless pointed to ...

KrebsOnSecurity Hit With Near-Record 6.3 Tbps DDoS

krebsonsecurity.com

KrebsOnSecurity last week was hit by a near record distributed denial-of-service (DDoS) attack that clocked in at more than 6.3 terabits of data per second (a terabit is one trillion bits of data).

Industry News

Headlines collected from across the cybersecurity industry related to legislation, business, and big tech

Mozilla fixes Firefox zero-days exploited at hacking contest - BleepingComputer

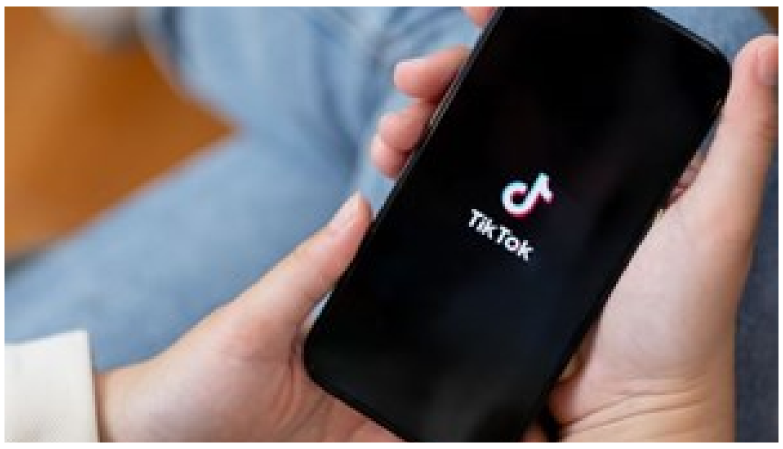
www.bleepingcomputer.com

Mozilla released emergency security updates to address two Firefox zero-day vulnerabilities demonstrated in the recent Pwn2Own Berlin 2025 hacking competition.

Oops: DanaBot Malware Devs Infected Their Own PCs

krebsonsecurity.com

Initially spotted in May 2018 by researchers at the email security firm Proofpoint, DanaBot is a malware-as-a-service platform that specializes in credential theft and banking fraud.. Today, the U ...



AI-Generated TikTok Videos Used to Distribute Infostealer Malware

www.infosecurity-magazine.com

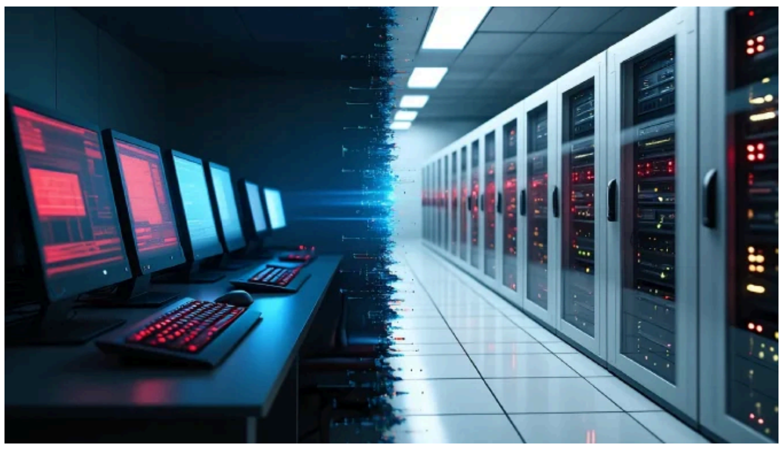
A new malware campaign has been observed using TikTok's viral nature and vast user base to spread information-stealing malware such as Vidar and StealC.. According to a new advisory by Trend Micro, this latest social engineering effort marks a shift ...

https://www.bleepingcomputer.com/news/security/us-indicts-leader-of-qakbot-botnet-linked-to-ransomware-attacks/

US indicts leader of Qakbot botnet linked to ransomware attacks - BleepingComputer

www.bleepingcomputer.com

The U.S. government has indicted Russian national Rustam Rafailevich Gallyamov, the leader of the Qakbot botnet malware operation that compromised over 700,000 computers and enabled ransomware ...



Chinese Hackers Exploit Trimble Cityworks Flaw to Infiltrate U.S. Government Networks

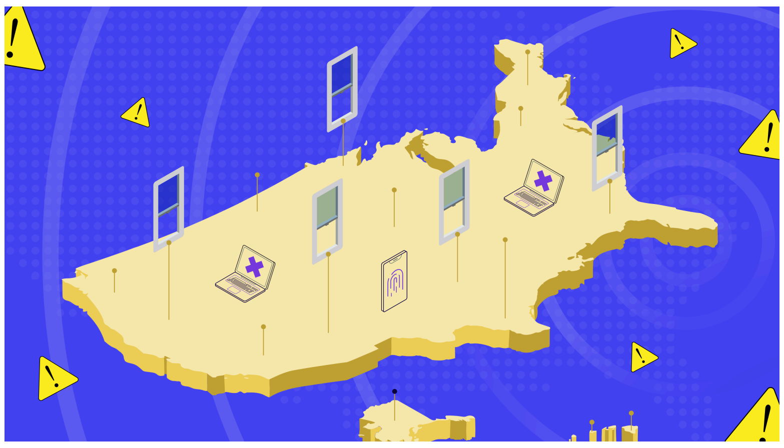
thehackernews.com

A Chinese-speaking threat actor tracked as UAT-6382 has been linked to the exploitation of a now-patched remote-code-execution vulnerability in Trimble Cityworks to deliver Cobalt Strike and VShell. "UAT-6382 successfully exploited CVE-2025-0944, con...

O2 UK patches bug leaking mobile user location from call metadata - BleepingComputer

www.bleepingcomputer.com

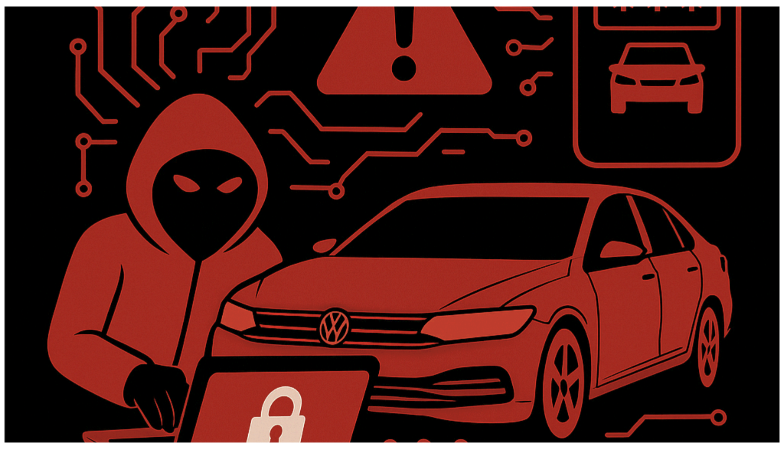
A flaw in O2 UK's implementation of VoLTE and WiFi Calling technologies could allow anyone to expose the general location of a person and other identifiers by calling the target.



A house full of open windows: Why telecoms may never purge their networks of Salt Typhoon | CyberScoop

cyberscoop.com

When the news broke that a Chinese hacking group known as Salt Typhoon had penetrated multiple U.S. telecommunications networks, gained access to the phones of a presidential campaign, and collected geolocation data on high-value targets around Washi...



Hacking My Car, and probably yours— Security Flaws in Volkswagen's App

loopsec.medium.com

Discovery Process (The fun technical part) It had been a while since I'd whipped out the trusty old Burp Suite.. After configuring my iPhone's Wi-Fi proxy and installing Burp's CA cert, I triggered a request with a random OTP to see what it looks lik...

AWS Default IAM Roles Found to Enable Lateral Movement and Cross-Service Exploitation - The Hacker News

thehackernews.com

Cybersecurity researchers have discovered risky default identity and access management (IAM) roles impacting Amazon Web Services that could open the door for attackers to escalate privileges, manipulate other AWS services, and, in some cases, even fu...

***Please be advised that** the following resources and materials are for informational purposes only. **The opinions and views expressed in these materials** are the opinions of the designated authors and do not reflect the opinions or views of **the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth).** The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.*

Official Quick Links

- CISA
- CIS/MS-ISAC
- CyberCom
- DHS
- DOJ
- FBI
- NIST
- NSA

External Quick links

- AIScoop
- BleepingComputer
- Cisco Talos Intelligence Group
- CSO Online
- CyberScoop
- Cybersecurity Dive
- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- ISSA International
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop
- The Hacker News
- The Record