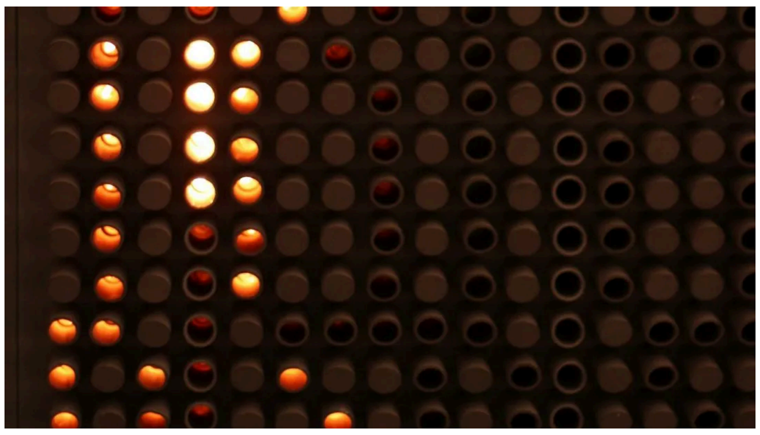
Week of January 12, 2026

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents



Western cyber agencies warn about threats to industrial operational technology

therecord.media

New guidance issued by Britain's National Cyber Secure Centre (NCSC), a part of signals and cyber intelligence agency GCHQ, sets out how organizations should securely connect equipment such as industrial control systems, sensors and other critical se...

Long-Running Web Skimming Campaign Steals Credit Cards From Online Checkout Pages - The Hacker News

thehackernews.com

Magecart web skimming campaign active since 2022 stealing credit card and personal data from compromised e-commerce checkout pages.

Malicious Chrome Extension Steals MEXC API Keys by Masquerading as Trading Tool - The Hacker News

thehackernews.com

A malicious Chrome extension posing as a trading tool steals MEXC API keys, enables withdrawals, and sends credentials to attackers via Telegram.

Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

Verizon outage: service is slowly returning for many — here's everything we know

www.techradar.com

The carrier says the outage is now resolved

California privacy agency appoints surveillance expert to board

therecord.media

The appointment of a strong proponent of civil liberties to the five-member board could have a significant impact on the agency's work.

Internet monitoring experts say Iran blackout likely to continue

therecord.media

Several internet access monitors tracking the situation said the government has continued the total internet shutdown and plans to implement a whitelist of limited, approved sites, indicating the internet blackout is likely to continue for several mo...

Palo Alto Fixes GlobalProtect DoS Flaw That Can Crash Firewalls Without Login - The Hacker News

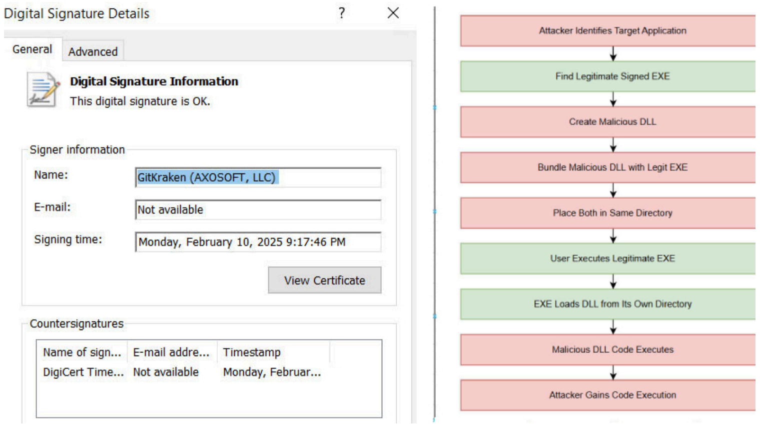
thehackernews.com

Palo Alto Networks fixed CVE-2026-0227, new GlobalProtect flaw that lets unauthenticated attackers trigger firewall DoS & maintenance mode.

Google to pay $8.25 million to settle lawsuit alleging children’s privacy violations

therecord.media

Google has agreed to pay $8.25 million to settle a class-action lawsuit centered on claims that it habitually and illegally collected data from devices belonging to children under age 13.


Digital Signature Details
?
General
Advanced
View Certificate
Attacker Identifies Target Application
Find Legitimate Signed EXE
Create Malicious DLL
Bundle Malicious DLL with Legit EXE
Place Both in Same Directory
User Executes Legitimate EXE
EXE Loads DLL from Its Own Directory
Malicious DLL Code Executes
Attacker Gains Code Execution

Digital Signature Information
This digital signature is OK.

Signer information

Name: GitKraken (AXOSOFT, LLC)

E-mail: Not available

Signing time: Monday, February 10, 2025 9:17:46 PM

Countersignatures

Name of sign...	E-mail addre...	Timestamp
DigiCert Time...	Not available	Monday, Februar...

Hackers Exploit c-ares DLL Side-Loading to Bypass Security and Deploy Malware - The Hacker News

thehackernews.com

Active malware exploits DLL side-loading in a signed GitKraken binary to deliver trojans, stealers, and remote access malware.

Oklahoma University Produces Its First Masters in Cybersecurity

www.govtech.com

Laci Henegar, Rogers State University's STEM coordinator, graduated in December with the university's first master's degree in cybersecurity policy, governance and training.

Data Breach May Have Hit 1M Charlotte, N.C., Telecom Users

www.govtech.com

The broadband and telecommunications company Brightspeed, which is based in the North Carolina city, is probing multiple reports its customers may have been victimized by a data breach.

California AG to probe Musk’s Grok for nonconsensual deepfakes

therecord.media

California’s attorney general said Wednesday that his office has opened a probe into the spread of nonconsensual sexually explicit material by the artificial intelligence tool Grok.

Hackers Use Fake PayPal Notices to Steal Credentials, Deploy RMMsHackers Use Fake PayPal Notices to Steal Credentials, Deploy RMMs - Infosecurity Magazine

www.infosecurity-magazine.com

A new wave of phishing-led intrusions abusing legitimate remote monitoring and management (RMM) tools has been documented, with attackers using fake PayPal alerts to gain both personal and corporate access. The activity, documented in an advisory pub...

Software Engineering Institute Researchers Rethink Cybersecurity for Modern Defense

www.cmu.edu

Government needs more agency buy-in to fight fraud with tech, officials say

fedscoop.com

Data experts with Treasury, the GAO and the Pandemic Response Accountability Committee say AI and data analytics can be used more effectively to detect fraud in federal programs.

__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.

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