Week of October 27, 2025

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents

New ChatGPT Atlas Browser Exploit Lets Attackers Plant Persistent Hidden Commands

thehackernews.com

Cybersecurity researchers have discovered a new vulnerability in OpenAI's ChatGPT Atlas web browser that could allow malicious actors to inject nefarious instructions into the artificial intelligence (AI)-powered assistant's memory and run arbitrary code.

Aisuru Botnet Shifts from DDoS to Residential Proxies

krebsonsecurity.com

Aisuru, the botnet responsible for a series of record-smashing distributed denial-of-service (DDoS) attacks this year, recently was overhauled to support a more low-key, lucrative and sustainable business: Renting hundreds of thousands of infected Internet of Things (IoT) devices to proxy services that help cybercriminals anonymize their traffic.

Critical WordPress Plugin Bugs Exploited En Masse

www.infosecurity-magazine.com

Threat actors are attempting to exploit three critical CVEs from 2024 impacting two popular WordPress plugins, according to Wordfence. The security vendor claimed that the bugs affect the GutenKit and Hunk Companion plugins which have over 40,000 and…

Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

Defense Contractor Boss Pleads Guilty to Selling Zero-Day Exploits to Russia - Infosecurity Magazine

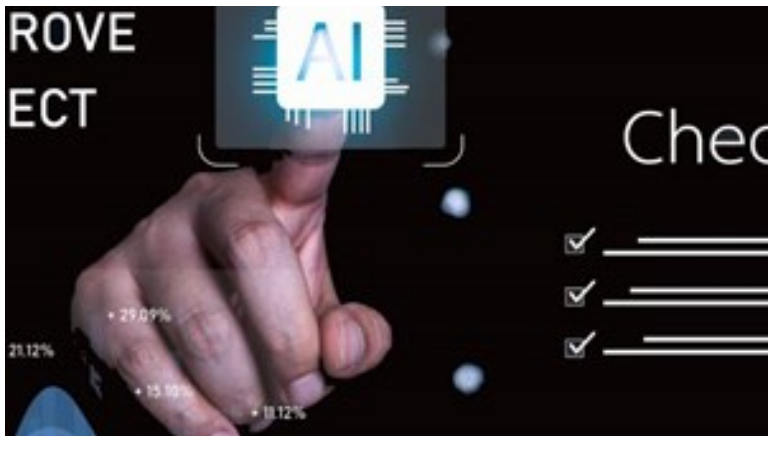
www.infosecurity-magazine.com

The former boss of a US defense contractor has pleaded guilty to selling zero-day exploits to a Russian cyber broker whose clients include the Kremlin. Australian national Peter Williams, 39, was general manager at L3Harris cyber-division Trenchant. …

Chrome to Make HTTPS Mandatory by Default in 2026

www.infosecurity-magazine.com

Google Chrome will enhance security with enforced HTTPS connections from version 154, set for release in October 2026



One In Four Employees Use Unapproved AI Tools, Research Finds

www.infosecurity-magazine.com

Shadow AI is emerging as one of the top forms of shadow IT, a new 1Password report has revealed. The unauthorized use of AI tools was found to be the second-most prevalent form of shadow IT, ranking only behind email, according to 1Password's 2025 An…

Chrome Zero-Day Exploited to Deliver Italian Memento Labs' LeetAgent Spyware - The Hacker News

thehackernews.com

The zero-day exploitation of a now-patched security flaw in Google Chrome led to the distribution of an espionage-related tool from Italian information technology and services provider Memento Labs, according to new findings from Kaspersky. The wave ...

Trump Administration Hiring Freeze Disrupts Cyber Workforce Program

www.govtech.com

Starting in February, CyberCorps program recruits received cancellation notices for work offers at agencies like NASA, the Department of Health and Human Services and the Defense Contract ...

Europol Warns of Rising Threat From Caller ID Spoofing Attacks

www.infosecurity-magazine.com

A growing wave of caller ID spoofing attacks, in which criminals falsify the number displayed on a phone to appear legitimate, has prompted Europol to call for urgent, coordinated action across Europe. The agency's new Position Paper on Caller ID Spo...

Nation-State Cyber Ecosystems Weakened by Sanctions, Report Reveals - infosecurity-magazine.com

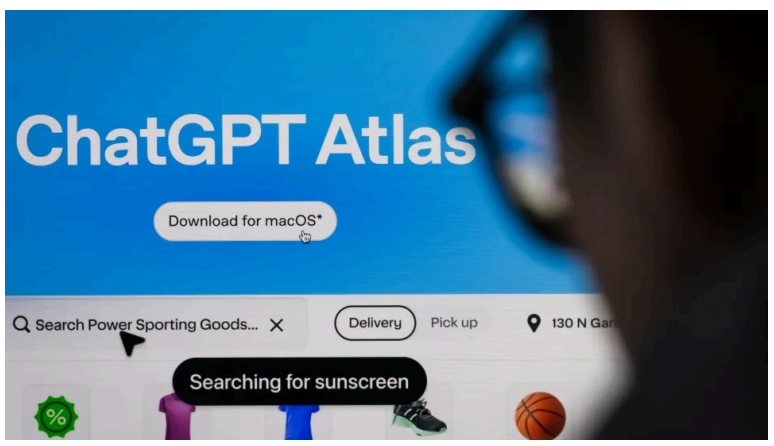
www.infosecurity-magazine.com

Cyber-related economic sanctions can alter adversary behavior, forcing underground networks to distance themselves from named actors

PHP Servers and IoT Devices Face Growing Cyber-Attack Risks

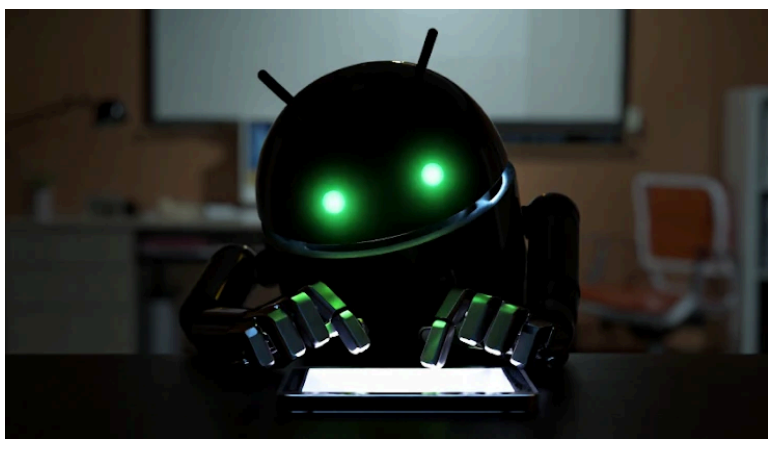
www.infosecurity-magazine.com

A rise in attacks on PHP servers, IoT devices and cloud gateways is linked to botnets exploiting flaws, according to new research published by Qualys



Exclusive: OpenAI's Atlas browser — and others — can be tricked by manipulated web content

cyberscoop.com



New Android Trojan 'Herodotus' Outsmarts Anti-Fraud Systems by Typing Like a Human - The Hacker News

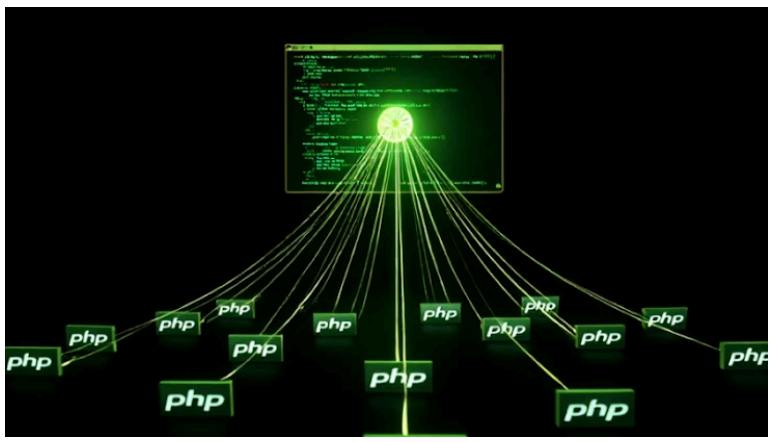
thehackernews.com

Herodotus, a new Android trojan, mimics human behavior to bypass biometrics and steal banking data.

Actively Exploited WSUS Bug Added to CISA KEV List

www.infosecurity-magazine.com

Network defenders have been encouraged to patch a new critical vulnerability in Windows Server Update Services (WSUS) which is being actively exploited. Microsoft issued an out-of-band update to fix the bug last Thursday, the same day that Huntress o...



Experts Reports Sharp Increase in Automated Botnet Attacks Targeting PHP Servers and IoT Devices - The Hacker News

thehackernews.com

Botnets exploit PHP flaws and cloud misconfigurations, launching 20 Tbps DDoS and large-scale credential attacks.

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