Scottish Cyber Coordination Centre

Daily Threat Bulletin

02 September 2025

Vulnerabilities

Silver Fox Exploits Signed Drivers to Deploy ValleyRAT Backdoor

Infosecurity Magazine - 01 September 2025 16:45

Silver Fox APT abuses Microsoft-signed drivers to kill antivirus and deploy ValleyRAT remote-access backdoor.

High-Risk SQLi Flaw Exposes WordPress Memberships Plugin Users

Infosecurity Magazine - 01 September 2025 16:00

A vulnerability in the WordPress Paid Memberships Subscription plugin could lead to unauthenticated SQL injection on affected sites.

Amazon Stops Russian APT29 Watering Hole Attack Exploiting Microsoft Auth

Infosecurity Magazine - 01 September 2025 11:00

The campaign shows APT29's intentions to "cast a wider net in their intelligence collection efforts," said Amazon.

Threat actors and malware

Amazon disrupts Russian APT29 hackers targeting Microsoft 365

BleepingComputer - 01 September 2025 12:35

Researchers have disrupted an operation attributed to Russian state-sponsored threat group Midnight Blizzard, who sought access to Microsoft 365 accounts and data.

Supply-chain attack hits Zscaler via Salesloft Drift, leaking customer info

Security Affairs - 01 September 2025 18:37

Zscaler breach tied to Salesloft Drift attack exposed Salesforce data, leaking customer info and support case details in a supply-chain compromise. Zscaler discloses a data breach that is linked to the recent Salesloft Drift attack. The cybersecurity vendor confirmed it was affected by a campaign targeting Salesloft Drift, a marketing SaaS integrated with Salesforce.

When Browsers Become the Attack Surface: Rethinking Security for Scattered Spider

The Hacker News - 01 September 2025 18:25

As enterprises continue to shift their operations to the browser, security teams face a growing set of cyber challenges. In fact, over 80% of security incidents now originate from web applications accessed via Chrome, Edge, Firefox, and other browsers.

Scottish Cyber Coordination Centre

ScarCruft Uses RokRAT Malware in Operation HanKook Phantom Targeting South Korean Academics

The Hacker News - 01 September 2025 14:56

Cybersecurity researchers have discovered a new phishing campaign undertaken by the North Korea-linked hacking group called ScarCruft (aka APT37) to deliver a malware known as RokRAT.

Hackers Threaten Google Following Data Exposure

Security Boulevard - 01 September 2025 12:57

A recent breach involving a third-party Salesforce system used by Google has sparked an unusual escalation. Although no Gmail inboxes, passwords, or internal Google systems were accessed, attackers gained entry to a sales database that included names, phone numbers, email addresses, and internal notes related to small business clients.

Ransomware Attack on Pennsylvania's AG Office Disrupts Court Cases

Infosecurity Magazine - 01 September 2025 13:00

Pennsylvania's Attorney General confirmed the OAG had refused to pay a ransom demand to the attackers after files were encrypted

CISA and Partners Release Joint Advisory on Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage Systems

CISA Advisories -

CISA, along with the National Security Agency, Federal Bureau of Investigation, and international partners, released a joint Cybersecurity Advisory on People's Republic of China (PRC) state-sponsored Advanced Persistent Threat (APT) actors targeting critical infrastructure across sectors and continents to maintain persistent, long-term access to networks.This advisory builds on previous reporting and is based on real-world investigations conducted across multiple countries through July 2025.