Veille Technologique – Réseau & Cybersécurité (18_11_2025 - 03_11_2025)

Sujet : SASE

Google on Monday released security updates for its Chrome browser to address two security flaws. The vulnerability in question is CVE-2025-13223 (CVSS score: 8.8) Microsoft this week pushed security updates to fix more than 60 vulnerabilities in its Windows operating systems and supported software.

Researchers have disclosed details of a new campaign that leverages a combination of social engineering and WhatsApp hijacking. The U.S. government is reportedly preparing to ban the sale of wireless routers and other networking gear from TP-Link Systems. A Ukrainian man indicted in 2012 for conspiring with a prolific hacking group was arrested in Italy and is now in custody in the United States.

A new campaign has leveraged Blender Foundation files to deliver an information stealer known as StealC V2. "This ongoing operation, active for at least six months, involves implanting malicious .blend files on platforms like CGTrader," Morphisec researcher Shmuel Uzan said.

- **Hackers Hijack Blender 3D Assets to Deploy StealC V2 Data-Stealing Malware** — The Hacker News (25/11/2025)
- https://thehackernews.com/2025/11/hackers-hijack-blender-3d-assets-to.html...
- **Why IT Admins Choose Samsung for Mobile Security** — The Hacker News (21/11/2025)
- https://thehackernews.com/2025/11/why-it-admins-choose-samsung-for-mobile.html...
- **Python-Based WhatsApp Worm Spreads Eternidade Stealer Across Brazilian Devices** — The Hacker News (19/11/2025)
- https://thehackernews.com/2025/11/python-based-whatsapp-worm-spreads.html...

Sujet : SD-WAN

Google is suing more than two dozen unnamed individuals allegedly involved in peddling a popular China-based mobile phishing service. The service helps scammers impersonate hundreds of trusted brands, blast out text message lures, and convert phished payment card data into mobile wallets from Apple and Google.

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. Hundreds of thousands of infected Internet of Things (IoT) devices are being rented to proxy services that help cybercriminals anonymize their traffic.

The U.S. government is reportedly preparing to ban the sale of wireless routers and other networking gear from TP-Link Systems. The tech company currently enjoys an estimated 50% market share among home users and small businesses. Experts say the proposed ban may have more to do with TP- Link's ties to China than any specific technical threats.

- **Drilling Down on Uncle Sam’s Proposed TP-Link Ban** — Krebs on Security (09/11/2025)
- https://krebsonsecurity.com/2025/11/drilling-down-on-uncle-sams-proposed-tp-link-ban/...
- **Google Sues to Disrupt Chinese SMS Phishing Triad** — Krebs on Security (13/11/2025)
- https://krebsonsecurity.com/2025/11/google-sues-to-disrupt-chinese-sms-phishing-triad/...
- **Aisuru Botnet Shifts from DDoS to Residential Proxies** — Krebs on Security (29/10/2025)
- https://krebsonsecurity.com/2025/10/aisuru-botnet-shifts-from-ddos-to-residential-proxies/...

Sujet : malware

A recently patched security flaw in Microsoft Windows Server Update Services (WSUS) has been exploited by threat actors to distribute malware known as ShadowPad. "The attacker targeted Windows Servers with WSUS enabled, exploiting CVE-2025-59287 for initial access," AhnLab Security Intelligence Center said.

The threat actor known as PlushDaemon has been observed using a previously undocumented Go-based network backdoor codenamed EdgeStepper to facilitate adversary-in-the-middle (AitM) attacks. The backdoor redirects DNS queries to an external, malicious hijacking node, effectively rerouting the traffic from legitimate infrastructure used for software updates to attacker-controlled infrastructure.

This week saw a lot of new cyber trouble. Hackers hit Fortinet and Chrome with new 0-day bugs. They also broke into supply chains and SaaS tools. Many hid inside trusted apps, browser alerts and software updates. Big firms like Microsoft, Salesforce, and Google had to react fast.

- ■ **Weekly Recap: Fortinet Exploit, Chrome 0-Day, BadIIS Malware, Record DDoS, SaaS Breach & More** — The Hacker News (24/11/2025)
- https://thehackernews.com/2025/11/weekly-recap-fortinet-exploit-chrome-0.html...
- **ShadowPad Malware Actively Exploits WSUS Vulnerability for Full System Access** — The Hacker News (24/11/2025)
- https://thehackernews.com/2025/11/shadowpad-malware-actively-exploits.html...
- **APT24 Deploys BADAUDIO in Years-Long Espionage Hitting Taiwan and 1,000+ Domains** — The Hacker News (21/11/2025)
- https://thehackernews.com/2025/11/apt24-deploys-badaudio-in-years-long.html...