cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- France's Ministry of Economy has disclosed a data breach resulted from an unauthorized access to the national bank account registry FICOBA, impacting information tied to 1.2 million accounts. Exposed data includes names, addresses, account identifiers and, in some cases, tax-related identifiers. Officials said the intrusion involved compromised government credentials.
- Japanese tech giant Advantest Corporation was hit by a ransomware attack that resulted in the deployment of ransomware within portions of its network following unauthorized access by a third party on February 15. The incident may have impacted certain internal systems, and the potential compromise of customer or employee data remains unclear.
- University of Mississippi Medical Center, an academic healthcare system in Mississippi, has suffered a ransomware attack that forced closures across its clinic network and disrupted access to electronic medical records. The organization canceled elective procedures and shifted to manual processes. Systems were taken offline and no ransomware group claimed responsibility.
- Ukraine's central bank, the National Bank of Ukraine (NBU), has faced a supply-chain incident affecting a contractor that runs its collectible coin online store. Exposed information includes customer registration data, such as names, emails, phone numbers, and delivery addresses. The bank indicated that payment information was not affected.

AI THREATS

- Check Point Research unveiled a technique that repurposes AI assistants like Grok and Microsoft Copilot as covert C2 proxies by abusing web-browsing URL fetch features without authentication. Malware exfiltrates host data via query parameters and retrieves commands from AI-generated summaries through hidden WebView2, bypassing inspection of AI traffic.
- A Russian-speaking financially motivated threat actor leveraged commercial generative AI tools to conduct mass credential abuse of 600 FortiGate devices in 55 countries from January 11 to February 18, 2026. The attackers targeted Veeam servers, exploiting CVE-2023-27532 and CVE-2024-40711.

  Check Point IPS provides protection against this threat *(Veeam Backup and Replication Insecure Deserialization (CVE-2024-40711))*
- Researchers uncovered a Shai-Hulud-like npm supply chain worm spreading via typosquatted packages, stealing developer and CI secrets, exfiltrating via GitHub API with DNS fallback, and propagating by poisoning workflows and git hooks, with MCP server injection targeting AI coding assistants and harvesting LLM API keys.

© 2026 Check Point Software Technologies Ltd. All Rights Reserved

VULNERABILITIES AND PATCHES

- Dell RecoverPoint for VMs, impacted by CVE-2026-22769 (CVSS 10.0) in versions before 6.0.3.1, has been exploited as a zero-day since mid-2024 by suspected Chinese group UNC6201. Attackers used hardcoded Tomcat credentials for unauthenticated root access, deploying SLAYSTYLE, BRICKSTORM, and the GRIMBOLT backdoor, and creating Ghost NICs to pivot and persist in VMware environments.

  Check Point IPS and Threat Emulation provide protection against this threat *(Dell RecoverPoint For Virtual Machines Arbitrary File Upload (CVE-2026-22769); Trojan.Wins.SLAYSTYLE; Trojan.Wins.BRICKSTORM.ta.*; Trojan.Wins.GRIMBOLT)*

- Grandstream GXP1600 series VoIP phones are affected by CVE-2026-2329, a critical unauthenticated stack-based buffer overflow in the web API allowing root RCE. Exploitation enables credential theft, SIP proxy reconfiguration, and covert call interception. Firmware version 1.0.7.81 fixes the issue.

  Check Point IPS provides protection against this threat *(Grandstream GXP1600 Stack Overflow (CVE-2026-2329))*

- A flaw in Microsoft 365 Copilot allows the “Work Tab” Chat feature to summarize emails protected by confidentiality sensitivity labels, bypassing configured Data Loss Prevention (DLP) policies. The code-level defect enables Copilot to access labeled content in Sent Items and Draft folders, exposing restricted data in AI-generated summaries.

- Google has patched CVE-2026-2441, a high-severity Chrome zero-day in the CSS component in Google Chrome prior to 145.0.7632.75, confirmed exploited in the wild. The use-after-free flaw can enable remote code execution within the browser sandbox via a crafted page.

  Check Point IPS provides protection against this threat *(Google Chrome Use After Free (CVE-2026-2441))*

THREAT INTELLIGENCE REPORTS

- Researchers have discovered Keenadu, an Android firmware backdoor delivered via supply chain compromise. It uses RC4-encrypted payloads, DexClassLoader, and permission bypass frameworks for ad fraud, search hijacking, and monetization, with links to Triada and BADBOX.

- Researchers analyzed Arkanix Stealer, a MaaS infostealer with Python and C++ implants, dynamic server side configuration, and modules including ChromElevator and HVNC. It uses phishing lures, steals from 22 browsers, Telegram and Discord and targets VPN, gaming and crypto wallets.

- Researchers have analyzed a spam campaign that abused Atlassian Jira Cloud notifications to bypass email filters by exploiting trusted atlassian.net sender domains with valid SPF and DKIM authentication. The attackers rapidly spun up trial instances and used Jira Automation alongside the Keitaro TDS to distribute localized lures targeting government and corporate sectors.

- Researchers identified a Booking.com-themed phishing campaign active since January 2026 that targets hotel partners and guests with a three-stage chain. It leveraged look-alike domains and IDN homographs, collected visitor fingerprinting with decoy pages, conducted partner account takeovers, and used WhatsApp lures to fake payment portals behind Cloudflare CAPTCHA.

© 2026 Check Point Software Technologies Ltd. All Rights Reserved