CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Scania, a Swedish manufacturer of heavy trucks and engines, has suffered a data breach that resulted in the theft of insurance claim documents from its Financial Services systems via compromised credentials of an external IT partner. The stolen data is likely to contain personal, financial, or medical information. The attack has been linked to a threat actor named 'Hensi,' who posted samples of the stolen data on hacking forums after an extortion attempt.
- American insurance giant Aflac has suffered a data breach, carried out by attackers who may have stolen sensitive information, including customers' personal and health data, Social Security numbers, claims details, and other personal information. Millions of users across the US and Japan may be impacted by this breach involving a wide range of sensitive documents.
- Satellite communications company Viasat has experienced a cyberattack that resulted in unauthorized access through a compromised device. While the company states there is no evidence of customer impact, the breach aligns with the actions of China-aligned Salt Typhoon APT group, which has previously infiltrated telecom networks globally and accessed sensitive data.
- The Washington Post confirmed it is investigating a cyberattack that targeted Microsoft email accounts belonging to several of its journalists—particularly those on national security and economic policy teams who cover China. The intrusions, suspected to be the work of a foreign government, prompted a company-wide password reset.
- The Federal State Information System for Veterinary Surveillance (VetIS) in Russia has experienced a cyberattack that resulted in the Mercury platform, used for certifying animal-based products, being taken offline. This disruption forced businesses to revert to paper-based veterinary certification, causing supply chain chaos and halting the delivery of goods to major retailers like Lenta and Yandex Lavka.
- Iranian Bank Sepah has experienced a cyberattack, resulting in disruptions to customer services, including account access, withdrawals, and card payments, and may have also impacted gas station transactions reliant on the bank’s systems. The anti-Iranian hacking group Predatory Sparrow has claimed responsibility for the attack, citing retaliation for the bank’s alleged role in supporting Iran’s military and nuclear programs.
- Indian car share company Zoomcar has suffered a data breach that resulted in the theft of the personal information of approximately 8.4 million users. The compromised dataset includes names, phone numbers, car registration details, addresses, and email addresses, though financial information and passwords appear unaffected. No threat actor has claimed responsibility yet.

© 2025 Check Point Software Technologies Ltd. All Rights Reserved

VULNERABILITIES AND PATCHES

- A critical remote code execution (RCE) vulnerability (CVE-2025-23121), was addressed in Veeam Backup & Replication (VBR) software. Exploitable by authenticated domain users, this flaw allows attackers to execute code remotely on the Backup Server, with successful exploitation potentially leading to unauthorized access and manipulation of backup environments. The vulnerability has not been explicitly noted as exploited in the wild.

- Details on multiple vulnerabilities in Sitecore Experience Platform have been disclosed, including a pre-auth remote code execution (RCE) chain leveraging CVE-2025-34509 for hardcoded credentials, and post-auth RCE exploits CVE-2025-34510 via path traversal and CVE-2025-34511 through unrestricted file uploads. The vulnerabilities allow unauthorized attackers to gain valid session cookies, bypass permissions, and execute arbitrary code. Successful exploitation could result in full administrative control of affected instances.

- Citrix has published an advisory addressing two vulnerabilities in NetScaler ADC and NetScaler Gateway. CVE-2025-5349 is an Improper access control in the management interface, while CVE-2025-5777 is a memory over-read flaw due to insufficient input validation when configured as a Gateway. While no active exploitation has been confirmed, the severity and public exposure warrant urgent patching, as both flaws are considered critical and allow access to sensitive data.

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a multi-stage malware campaign targeting Minecraft users through malicious repositories on GitHub under the Stargazers Ghost Network, posing as legitimate mods. The malware chain, developed by a Russian-speaking threat actor, begins with a Java-based downloader disguised as a Minecraft mod, initiating a chain of malicious activity, downloading infostealer components, and exfiltrating sensitive data such as Minecraft account tokens, Discord and Telegram credentials, browser information, cryptocurrency wallet data, and VPN service details.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat

- Check Point researchers have uncovered a sophisticated phishing campaign targeting US citizens by impersonating state Departments of Motor Vehicles (DMVs). The campaign utilized SMS phishing to distribute fake toll violation alerts, directing victims to cloned DMV websites that harvested personal and financial data. Technical analysis revealed shared infrastructure, phishing kits with reused front-end assets, and Chinese-language code comments, attributing the operation to a likely China-based threat actor.

- Researchers have identified a new Python-based version of the GolangGhost RAT, dubbed PylangGhost, deployed by the North Korean-linked group Famous Chollima. Active since May 2025, the Windows-focused malware mirrors its Golang predecessor in capabilities, targeting crypto and blockchain professionals in India via fake job-interview or skill-testing sites that trick victims into executing malicious commands.

© 2025 Check Point Software Technologies Ltd. All Rights Reserved