CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- New York University (NYU) suffered a cyber-attack which resulted in the exposure of over 3 million applicants' data, including names, test scores, majors, and zip codes. The hacker redirected NYU's website to display this information, alleging the university's continued use of race-sensitive admissions policies despite the Supreme Court's 2023 ruling against affirmative action. The breach also included downloadable files containing admissions data dating back to 1989.

- Kuala Lumpur International Airport (KLIA) fell victim to a cyber-attack which resulted in the disruption of its immigration system, causing significant delays for both inbound and outbound travelers. The incident reportedly affected check-in counters and caused long queues across the airport. Authorities confirmed the hackers demanded a $10 million ransom payment.

- Ukrzaliznytsia, Ukraine's state-owned railway operator, has been the target of a major cyberattack, resulting in disruptions to its online services, including its mobile app used for ticket purchases. While the attack did not affect train schedules, it did cause significant inconvenience to passengers who had to purchase tickets physically at stations.

- Sam's Club, a U.S.-based warehouse supermarket chain owned by Walmart, is investigating claims of a potential cyber security incident. The Clop ransomware gang has listed Sam's Club on its dark web leak site, alleging that the company has ignored security concerns. The threat actors have not yet published any proof of the breach, and Sam's Club has not disclosed any specific details regarding the incident.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (Ransomware.Win.Clop; Ransomware.Wins.Clop; Ransomware.Wins.Clop.ta.)*

- Pennsylvania's Union County disclosed that it had suffered a ransomware attack. According to the county's statement, the information exfiltrated in the attack includes Social Security Numbers as well as driver's licenses. No ransomware group has taken responsibility for the attack yet.

- US mobility solutions firm Numotion had experienced a cyber-attack which resulted in a data breach impacting nearly 500,000 individuals. An unauthorized third party gained access to the email accounts of some of its employees between September 2, 2024, and November 18, 2024, following successful phishing emails.

- Abracadabra Finance had suffered a cyber-attack which resulted in the theft of approximately $13 million worth of digital currency. The breach was traced to vulnerabilities in their "cauldrons," isolated lending markets allowing users to borrow against various cryptocurrencies. The company is collaborating with security firms to investigate the incident and has offered a 20% bug bounty to the attacker for the return of the stolen funds.

VULNERABILITIES AND PATCHES

- Researchers have disclosed that Google Chrome zero-day exploit chain was used by APT group dubbed ForumTroll. The first vulnerability (CVE-2025-2783) allowed the attackers to bypass Google Chrome's sandbox protection, while it was design to run with additional exploit that enables remote code execution. Google released a fix to CVE-2025-2783.
- A critical vulnerability (CVE-2025-23120) in Veeam Backup & Replication software, that allows remote code execution by authenticated domain users, was recently patched. The flaw stems from inconsistent deserialization handling that permits exploitation via unblocked classes such as Veeam.Backup.EsxManager.xmlFrameworkDs and Veeam.Backup.Core.BackupSummary.
- Researchers have elaborated on a critical command injection vulnerability (CVE-2025-25364) in Speedify VPN on macOS. The lack of proper input validation of user-controlled fields (cmdPath and cmdBin) within XPC messages allows a local attacker to inject arbitrary commands. Successful exploitation could potentially lead to privilege escalation and full system compromise. The vulnerability has been patched in Speedify VPN version 15.4.1.

THREAT INTELLIGENCE REPORTS

- Researchers reported on a cyber espionage operation by Weaver Ant, a China-nexus threat actor targeting a major telecommunications provider in Asia. The group exploited home routers and deployed a novel web shell to infiltrate the network, aiming for continuous access and sensitive data collection. Weaver Ant's tactics include leveraging web shells and tunneling techniques to maintain persistence within the compromised environment.
- Researchers have uncovered a significant operational security failure within the BlackLock ransomware group by exploiting a misconfiguration in their data leak site (DLS). This flaw allowed access to internal commands, configuration files, and credentials, revealing that BlackLock, a rebranded version of the Eldorado ransomware group, has compromised 46 victims globally across various sectors, including technology, manufacturing, construction, finance, and retail.
- Researchers have detected a campaign by the Russia-linked threat actor Water Gamayun exploiting CVE-2025-26633, a zero-day vulnerability in the Microsoft Management Console (MMC). This flaw allows attackers to execute malicious code by manipulating .msc files and the Multilingual User Interface Path (MUIPath), enabling unauthorized code execution and data exfiltration. Microsoft has released a patch to address this vulnerability.
- CISA released a Malware Analysis Report on "Resurge", a backdoor malware targeting Ivanti Connect Secure appliances via CVE-2025-0282—a critical buffer overflow vulnerability disclosed in January. Resurge shares features with the SpawnChimera malware, including SSH tunneling, web shell deployment, and file manipulation to maintain persistence and evade detection. Threat actors can use it to escalate privileges, harvest credentials, and manipulate system integrity.