CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Air France has experienced a data breach that resulted in unauthorized access to customer data through a compromised external customer service platform. The attack exposed personal information, including names, email addresses, phone numbers, frequent flyer program details, and recent transactions, but did not affect customer financial or sensitive personal data.
- Google has suffered a data breach that resulted in the exposure of approximately 2.55 million business contact records from its Salesforce CRM, including business names, phone numbers, and sales notes of potential Google Ads customers. The attack is linked to ShinyHunters and possibly to Scattered Spider, who extorted Google and threatened to leak the stolen data.
- Bouygues Telecom, a French internet service provider, has confirmed a cyberattack that resulted in unauthorized access to personal data from 6.4 million customer accounts. The data breach affected a segment of its mobile and fiber-to-the-home customers, exposing limited personal data.
- Pandora, a Danish jewelry manufacturer and retailer, has suffered a data breach that resulted in the theft of customer names, birthdates, and email addresses from its Salesforce database. The breach impacted the personal information of customers, but no passwords, IDs, or financial data were exposed.
- The US Federal Judiciary has confirmed a cyber attack that resulted in unauthorized access to its electronic case management systems, exposing confidential court documents including sensitive sealed filings and potentially the identities of confidential informants.
- American Public Broadcasting Service (PBS) has suffered a data breach that resulted in the exposure of corporate contact information for 3,997 employees and affiliates, including names, corporate emails, job titles, departments, locations, hobbies, and supervisor names.
- Pakistan Petroleum Limited (PPL) has experienced a cyber-attack that resulted in its IT systems being crippled, with servers encrypted, backups blocked, and financial operations suspended for two days. Vital data—encompassing operational records, contracts, and employee information—was exfiltrated and is now being held hostage. Blue Locker claimed responsibility for the attack.
- The University of Western Australia has suffered a data breach that resulted in unauthorized access to password information of thousands of staff members and students. The incident forced a lockout of all users and mandatory password resets, with no evidence that any other data or systems were compromised.

VULNERABILITIES AND PATCHES

- Check Point Research has identified a persistent remote code execution vulnerability in the Cursor IDE, tracked as CVE-2025-54136. The vulnerability is caused by insufficient validation of Model Context Protocol (MCP) configuration changes. After a user's initial approval of a benign MCP plugin, attackers with write access can modify MCP commands to execute arbitrary or malicious code on victims' machines each time the project is opened, without any further prompts or interaction.

- Cisco has disclosed five critical vulnerabilities in Dell ControlVault3 firmware and its associated Windows APIs, collectively named "ReVault." These flaws (CVE-2025-24311, CVE-2025-25050, CVE-2025-25215, CVE-2025-24922, CVE-2025-24919) enable attackers to achieve arbitrary code execution, persistent firmware implants, and privilege escalation, potentially bypassing Windows authentication and persisting across OS reinstalls.

- Trend Micro has released an advisory addressing vulnerabilities CVE-2025-54987 and CVE-2025-54948, two critical severity Remote Code Execution vulnerabilities (9.4 CVSS) in Trend Micro Apex One management console. The vulnerabilities have been actively exploited in the wild.

THREAT INTELLIGENCE REPORTS

- Researchers have analyzed recent updates to Raspberry Robin, a sophisticated malware downloader active since 2021, revealing advanced obfuscation techniques and improvements in network encryption, such as a transition from AES-CTR to ChaCha-20 and the introduction of per-request randomized counters and nonces. The malware now utilizes obfuscated stack pointers, complex initialization loops to hinder brute-force decryption, modified RC4 key structures, and employs a new local privilege escalation exploit (CVE-2024-38196).

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (Trojan.Wins.RaspberryRobin.ta., Trojan.Wins.RaspberryRobin.*)*

- Researchers have uncovered a novel AV-killer malware abusing the legitimate ThrottleStop.sys driver (CVE-2025-7771), used in the wild since at least October 2024. This malware, delivered alongside the vulnerable driver, leverages two exposed IOCTL interfaces to perform arbitrary physical memory reads and writes via MmMapIoSpace, enabling privileged kernel-level calls to locate and terminate a wide range of antivirus and EDR processes.

- Ukrainian Computer Emergency Response Team (CERT-UA) has analyzed a wave of cyber-espionage attacks by UAC-0099, leveraging a court-summons phishing lure. These attacks begin with phishing emails sent via UKR.NET that deliver HTA files containing obfuscated VBScript, which drop files, create scheduled tasks, and deploy the MATCHBOIL C# loader—followed by the MATCHWOK backdoor and DRAGSTARE stealer.