CHECK POINT RESEARCH

June 2 – 8, 2025

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- American tax company, Optima Tax Relief, has disclosed a ransomware attack that resulted in the theft of 69GB of sensitive data, including corporate records and customer case files containing personal information such as Social Security numbers, phone numbers, and home addresses. The attack impacted the company's servers in a double-extortion scheme, where data was both stolen and encrypted. The Chaos ransomware gang has claimed responsibility for the attack.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.Chaos.ta.; Botnet.Win.Chaos; Trojan.Win.Chaos)*

- Luxury jewelry brand, Cartier, has suffered a data breach that included an unauthorized access to its systems and the theft of limited customer information, including names, email addresses, and countries of residence. The attack did not compromise sensitive data such as passwords, credit card numbers, or banking details but poses a heightened risk of targeted phishing or malicious communications directed at impacted customers. No threat actor has claimed responsibility yet.

- Government systems in Ohio, Oklahoma, and Puerto Rico were targeted by cyberattacks, disrupting services for thousands of residents. The City of Durant, Oklahoma and Lorain County, Ohio experienced ransomware attacks that caused outages in payment systems, court operations, and emergency communications. Puerto Rico's Department of Justice also confirmed a cyberattack affecting its Criminal Justice Information Office, prompting service suspensions

- Outdoor clothing brand, The North Face, has experienced a data breach that resulted in the exposure of customers' personal information during a credential stuffing attack on April 23, 2025. The compromised data includes full names, purchase history, shipping addresses, email addresses, dates of birth, and telephone numbers, though payment information was not impacted.

- Tupolev, Russia's strategic warplane maker, was hacked in a cyberattack that resulted in the exfiltration of over 4.4GB of sensitive data. The stolen files included internal communications, personal details of employees, engineer resumes, procurement records, and confidential meeting minutes. The attack was reportedly carried out by Ukraine's Defense Intelligence agency.

- Lee Enterprises, a major US newspaper group, was hit by a ransomware attack in February 2025 that exposed personal data of around 40K individuals, including SSNs, driver's licenses, financial and medical details. The attack disrupted printing, delivery, and internal systems. The Qilin ransomware gang claimed responsibility, alleging the theft of 350GB of data across 120K sensitive documents.

  Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.Qilin)

VULNERABILITIES AND PATCHES

- A critical vulnerability (CVE-2025-49113) in Roundcube webmail was disclosed and patched, enabling post-authentication remote code execution (RCE). The flaw caused by unsanitized $_GET['_from'] input leading to PHP object injection. Exploitation has been observed in the wild using brute-forced or stolen credentials via CSRF. A working exploit is reportedly being sold on underground forums.

  Check Point IPS provides protection against this threat (Roundcube Webmail Remote Code Execution (CVE-2025-49113))

- A critical static credential vulnerability (CVE-2025-20286, CVSS 9.9) was fixed in Cisco ISE cloud deployments on AWS, Azure, and OCI. The flaw allows unauthenticated attackers to reuse shared credentials across identical deployments, enabling access to sensitive data, limited admin actions, and service disruption. A proof-of-concept exploit exists, but no active exploitation was observed.

- A patch has been released to address CVE-2025-5419, a high-severity out-of-bounds read and write vulnerability in Chrome's V8 JavaScript engine. This zero-day, observed being actively exploited in the wild, could potentially lead to arbitrary code execution or data corruption. Affected versions include Chrome across Windows, macOS, and Linux.

- Qualcomm patched three zero-day vulnerabilities (CVE-2025-21479, CVE-2025-21480, and CVE-2025-27038) in its Adreno GPU driver. The flaws involve improper authorization and a use-after-free bug, causing memory corruption and unauthorized command execution during Chrome rendering. Exploits have been observed in the wild, enabling attackers to bypass Android kernel protections.

THREAT INTELLIGENCE REPORTS

- The FBI warns that the BADBOX 2.0 malware campaign has infected over 1 million Android-based IoT devices, including smart TVs, streaming boxes, projectors, and tablets, mostly made in China. The botnet routes cybercriminal activity through residential proxies, enabling ad fraud and credential stuffing via command-and-control servers. Most affected countries are Brazil (37.6%), the US (18.2%), Mexico (6.3%), and Argentina (5.3%).

- Google uncovered a financially motivated campaign by UNC6040 targeting Salesforce via voice phishing, tricking employees into approving fake apps like altered Data Loaders to steal data. The group also uses stolen credentials to access cloud tools like Okta and Microsoft 365, relying on phishing panels and Mullvad VPN.

- Researchers discovered "PathWiper", a new wiper malware used in an attack on Ukrainian critical infrastructure. Deployed via a legitimate admin framework, it used VBScript to run an executable that overwrites MBR and NTFS data on connected drives. PathWiper resembles HermeticWiper but uses more advanced methods to target storage volumes.