August 11 – 17, 2025

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Canadian House of Commons has suffered a data breach. The incident resulted in unauthorized access to a database containing employees' names, office locations, email addresses, and information on House-managed computers and mobile devices, reportedly due to vulnerability in Microsoft software.

- The Office of the Pennsylvania Attorney General, US has experienced a cyber attack that resulted in the disruption of its phone, email, and website systems. The outage has impacted the communication systems and some public services, with no information released regarding any data leakage or specific data compromised.

- U.K. Telecom provider, Colt Technology Services, has confirmed a cyber attack, causing multi-day outages of hosting and porting services, Colt Online, and Voice API platforms, with support systems severely disrupted. The WarLock ransomware gang has claimed responsibility, offering to sell for $200,000 a batch of one million documents allegedly stolen from Colt, including financial, employee, customer and executive data, as well as internal emails, and software development information.

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

- Connecticut's Connex Credit Union has suffered a data breach that resulted in the theft of personal and financial information after unauthorized access to its systems in early June 2025. The breach impacted approximately 172,000 members, exposing names, account numbers, debit card information, Social Security numbers, and government IDs.

- Global staffing company Manpower has suffered a data breach that resulted in the theft of personal information of nearly 145,000 individuals. The RansomHub ransomware gang has claimed responsibility for this attack, which was limited to the Lansing, Michigan franchise and did not impact ManpowerGroup's corporate network. The breach allegedly exposed 500GB of sensitive client and corporate data, including passport scans, IDs, and Social Security numbers.

- Yes24, South Korea's largest ticketing and online book retailer, was hit by a ransomware attack that took its website and mobile app offline for several hours, disrupting concert ticket sales, e-book access, and community forums for thousands of users. This marks the company's second ransomware-related service outage in less than two months, following a previous incident in June.

- WestJet Airlines confirmed a cyber attack, which exposed sensitive passenger data, including names, birth dates, contact details, travel document information, and booking records. The breach's origin remains unknown, and no threat actor has claimed responsibility.

VULNERABILITIES AND PATCHES

- Microsoft's August 2025 Patch Tuesday fixed 107 vulnerabilities, including one publicly disclosed zero-day in Windows Kerberos and 13 Critical flaws across Windows, Office, NTLM, GDI+, MSMQ, Azure, DirectX, and Hyper-V. The most common risks were elevation of privilege and remote code execution. While no active exploitation has been confirmed, several vulnerabilities present significant risks for full system compromise, making prompt patching essential.

- Check Point Research has uncovered six vulnerabilities—including the first publicly disclosed bug in a Rust-based Windows kernel component—ranging from critical to moderate severity and impacting Microsoft Windows systems. Notable CVEs include CVE-2025-30388 and CVE-2025-53766, both enabling arbitrary code execution via crafted files, as well as CVE-2025-47984, which allows remote memory leakage over the network. Successful exploitation could trigger system-wide crashes, execute malicious code, or expose sensitive memory contents to remote attackers.

- A critical remote code execution vulnerability, CVE-2025-20265, has been identified in the RADIUS subsystem of Cisco Secure Firewall Management Center (FMC). It affects versions 7.0.7 and 7.7.0 where RADIUS authentication is enabled, allowing unauthenticated remote attackers to execute arbitrary shell commands with elevated privileges via crafted user input. Successful exploitation impacts web and SSH management interfaces, though the issue has not been observed exploited in the wild.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports on a global rise in cyber and ransomware attacks in July 2025, driven by sophisticated threat actor escalations across all sectors. The average number of cyber attacks per organization per week reached 2,011, with the education sector at 4,248 and telecommunications at 2,769, while the agriculture sector recorded an 81% annual increase. Ransomware attacks surged by 28% year over year, with North America experiencing 52% of incidents, and three ransomware groups—Qilin (12% of attacks), Inc. Ransom (9%), and Akira (8%)—dominating publicly disclosed victim data.

- Check Point warns against Instagram's new "Friend Map" feature, which poses major privacy and safety risks. The feature logs users' movements and stores data unencrypted on Meta's servers, where it can fuel stalking, burglary, scams —and attract cybercriminals. Unlike Apple's secure Find My, the Friend Map is tied to Meta's ad ecosystem, increasing exploitation risks.

- Researchers have analyzed the Crypto24 ransomware group, which executes multi-stage attacks by blending legitimate administrative tools like AnyDesk with custom malware for stealthy lateral movement and persistence. The group targets high-profile organizations across Asia, Europe, and the USA, focusing on financial services, manufacturing, and technology sectors, employing methods such as privileged account creation, Google Drive-based data exfiltration, and remote desktop exploitation to maintain ongoing surveillance and maximize operational impact.