CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- American consumer credit reporting agency TransUnion has suffered a data breach that resulted in the exposure of sensitive personal information for over 4.4 million individuals in the United States. The leaked data includes names, billing addresses, phone numbers, email addresses, dates of birth, unredacted Social Security Numbers, transaction reasons, and customer support messages.
- Miljödata, a major Swedish IT provider, has disclosed a cyber attack that resulted in service disruptions to over 200 Swedish municipalities. The attack raised concerns over the theft of sensitive personal data, including medical certificates, rehabilitation cases, and occupational injury reports.
- Healthcare Services Group has suffered a data breach that resulted in the unauthorized access and exfiltration of sensitive personal information from its network. The incident impacted approximately 624,000 individuals, exposing data that may include full names, Social Security numbers, driver's license and state identification numbers, financial account details, and account credentials.
- The Maryland Transit Administration (MTA) has experienced a cyber attack that resulted in disruption of Mobility paratransit service. The attack affected scheduling systems and related real-time information and call-center systems, preventing users from booking trips.
- The State of Nevada has confirmed a cyber attack that resulted in widespread disruption of services. The attack affected governmental websites, phone systems, and online platforms, forcing the closure of all state offices and impacting the availability of various state technology systems.
- Nissan has suffered a data breach that resulted in four terabytes of sensitive design studio data being stolen from its subsidiary Creative Box Inc. These include 3D vehicle models, financial documents, VR workflows, and photos. The breach impacts Nissan only, exposing proprietary experimental and concept vehicle designs but no external clients or contractors. Qilin ransomware group claimed responsibility for the attack and published samples of the stolen information.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (Ransomware.Wins.Qilin.)*
- Farmers Insurance has disclosed a data breach that resulted in the theft of sensitive customer information, including names, addresses, dates of birth, driver's license numbers, and/or the last four digits of Social Security numbers. The breach impacted 1,111,386 customers.
- Auchan has suffered a data breach that resulted in unauthorized access to sensitive data from several hundred thousand customer loyalty accounts. The personal information exposed includes full names, titles, client status, postal addresses, email addresses, phone numbers, and loyalty card numbers. No banking data, passwords, or PINs were compromised in the incident.

VULNERABILITIES AND PATCHES

- WhatsApp has released a patch for a zero-click authorization vulnerability (CVE-2025-55177) affecting iOS and Mac versions of the app, which allowed attackers to process content from arbitrary URLs via abused linked device synchronization messages. This vulnerability, exploited in targeted zero-day attacks, was used alongside an Apple OS-level flaw (CVE-2025-43300) in sophisticated spyware campaigns against select users. Successful exploitation enabled remote code execution.
- Citrix has fixed a critical remote code execution vulnerability (CVE-2025-7775) in NetScaler ADC and NetScaler Gateway, which was exploited as a zero-day via a memory overflow bug allowing unauthenticated RCE on unpatched systems. Additional patched vulnerabilities include CVE-2025-7776 (memory overflow, DoS) and CVE-2025-8424 (improper access control).
- Passwordstate, a password manager used by over 29,000 organizations, has released a patched version, addressing a high-severity authentication bypass vulnerability. The flaw allows threat actors to craft a malicious URL targeting the Emergency Access page, granting unauthorized access to the administration section, and does not yet have a CVE ID.
- Google has released a security update for Google Chrome, addressing CVE-2025-9478, a critical use after free vulnerability in ANGLE. Malicious attackers could craft websites to trigger memory corruption and achieve remote code execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research revealed the ZipLine campaign, a sophisticated phishing operation targeting US supply chain-critical manufacturing companies by leveraging legitimate-appearing business interactions initiated through corporate “Contact Us” forms. The attack involves multi-week email exchanges, followed by the delivery of the custom MixShell implant. Technical analysis reveals advanced persistence mechanisms, dynamic payload customization, and infrastructure spoofing.
- Check Point Research have uncovered an active campaign attributed to the Silver Fox APT group that abuses newly discovered and previously known vulnerable, Microsoft-signed kernel drivers. This in order to terminate protected security processes and evade EDR/AV detection on fully updated Windows 10/11 systems. The attackers employ a dual-driver strategy for cross-version compatibility, embedding both drivers in a single loader, which incorporates anti-analysis measures and ultimately delivers the ValleyRAT remote access trojan.
- Check Point researchers uncovered an active phishing campaign in which threat actors abused Google Classroom’s invitation system to send over 115,000 phishing emails targeting 13,500 organizations across the globe within a single week. The attackers distributed fake Google Classroom invitations containing commercial offers, directing recipients to communicate via WhatsApp. This allowed them to bypass enterprise monitoring and leverage Google’s legitimate infrastructure to evade security measures.