CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A supply chain breach involving Salesloft's Drift integration to Salesforce exposed sensitive customer data from multiple organizations, including Cloudflare, Zscaler, Palo Alto Networks, and Workiva. The attackers accessed Salesforce CRM systems via compromised OAuth tokens, stealing contact details, account records, support case data, and even authentication tokens and cloud secrets, potentially affecting over 700 organizations. The campaign has been attributed to the threat actor UNC6395.
- Jaguar Land Rover has confirmed a cyber attack that resulted in severe disruption to its global IT systems. The attack forced production and retail operations to halt and factory staff to stay at home. The incident involved a data breach, the extent of which has not yet been disclosed. A group of English-speaking cybercriminals have claimed responsibility for the attack via Telegram.
- Manufacturer Bridgestone Americas has suffered a cyber attack that resulted in operational disruptions. The disruption impacted several of its North American facilities, with production facilities in South Carolina and Quebec. While no evidence of customer data theft or interfaces compromise were reported, the incident could lead to supply shortages.
- Fintech platform Wealthsimple has disclosed a data breach that resulted in unauthorized access to personal information belonging to less than 1% of its clients. Personal data includes contact details, government IDs, account numbers, IP addresses, Social Insurance Numbers, and dates of birth. No customer funds were stolen, and account passwords were not compromised in the incident.
- The Pennsylvania Attorney General's Office confirmed that a ransomware attack caused its ongoing two-week service outage, which disrupted its website, email, and phone systems. Officials refused to pay the ransom and are working through alternative channels.
- The City of Baltimore was scammed out of more than $1.5 million. The threat actor spoofed a city vendor, gained access to its Workday account, and tricked Accounts Payable employees into approving fraudulent bank changes. A lack of proper verification procedures allowed two large payments to be sent, of which only the smaller was recovered.
- Brazilian fintech giant Sinqia S.A. has experienced a cyber attack that resulted in hackers breaching its systems and attempting to steal $130 million. The actors tried to make unauthorized transactions on Brazil's Pix real-time payment system. The incident led to Sinqia's access to Pix being revoked.
- Gaming website Chess.com has suffered a data breach that resulted in the exposure of personal information for 4,541 users through a compromised third-party file transfer tool. The breach occurred between June 5 and June 18, and reportedly no banking information or member account credentials, including usernames and passwords, were leaked.

VULNERABILITIES AND PATCHES

- A patch has been released for zero-day vulnerabilities CVE-2025-55177 in WhatsApp and CVE-2025-43300 in Apple's iOS, iPadOS, and macOS. These vulnerabilities were actively exploited in targeted attacks against specific individuals. CVE-2025-55177 involved incomplete authorization in device synchronization, allowing processing of arbitrary URLs. It could be chained with CVE-2025-43300, an out-of-bounds write flaw, for sophisticated exploitation. No technical details or proof-of-concept have been published, but exploitation was observed in the wild.

- Details on a critical ViewState deserialization vulnerability (CVE-2025-53690) in Sitecore were disclosed. The vulnerability enabled remote code execution on affected internet-facing instances and observed actively exploited in the wild. Attackers leveraged the flaw for initial compromise, privilege escalation, credential dumping, Active Directory reconnaissance, and lateral movement using open-source tools and malware. Exploitation led to the creation of local administrator accounts, deployment of persistence mechanisms, and exfiltration of sensitive configuration files.

  Check point IPS blade provides protection against this threat *(Sitecore Multiple Products Insecure Deserialization (CVE-2025-53690)*

- NVIDIA released September 2025 security updates addressing multiple high and medium severity vulnerabilities across BlueField, ConnectX, DOCA, Mellanox DPDK, Cumulus Linux, and NVOS. Exploits could allow attackers to escalate privileges, tamper with configurations, cause denial of service, or expose sensitive information.

THREAT INTELLIGENCE REPORTS

- Check Point reports on Hexstrike-AI, a newly released AI-powered framework that orchestrates more than 150 specialized agents to scan, exploit, and persist inside targets, reducing exploitation time from days to minutes. Though designed for red-team testing, threat actors quickly tried to repurpose it to weaponize different vulnerabilities. The tool shows how AI orchestration can rapidly accelerate large-scale, real-world exploitation.

- Amazon disrupted a watering hole campaign by Russia-linked APT29 (Midnight Blizzard), which used compromised websites to redirect victims into attacker-controlled Microsoft device code authentication flows. The campaign demonstrated APT29's evolving tactics, including obfuscated JavaScript injections, server-side redirects, and rapid infrastructure adaptation.

- Researchers identified a novel China-aligned threat actor, GhostRedirector, leveraging a C++ backdoor - "Rungan", and an IIS module -"Gamshen", to compromise at least 65 Windows servers, primarily in Brazil, Thailand, and Vietnam. Gamshen manipulates IIS responses to Googlebot for SEO fraud, while Rungan provides remote command execution and persistence. The attackers gain initial access via likely SQL Injection and create rogue admin users to ensure long-term access across different sectors including healthcare, retail, transportation, and education.