

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The University of Pennsylvania and the University of Phoenix were [hit](#) by data breaches after attackers exploited zero-day vulnerabilities in Oracle E-Business Suite servers. At least 1,488 people at UPenn and numerous students, alumni, donors, staff, faculty, employees, and suppliers at Phoenix were impacted. The ClOp ransomware gang is likely responsible, as part of a broader campaign.

*Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat (Oracle Multiple Products Remote Code Execution; Ransomware.Win.Clop; Ransomware.Wins.Clop; Ransomware.Wins.Clop.ta. *)*

- Financial software provider Marquis Software Solutions has [disclosed](#) a data breach that impacted over 74 banks and credit unions across the US and exposed sensitive data of more than 400,000 customers. The Akira ransomware gang is possibly responsible for the attack, which exploited vulnerabilities in SonicWall firewalls to gain network access.

*Check Point Threat Emulation provides protection against this threat (Ransomware.Wins.Akira.ta. *; Ransomware.Wins.Akira)*

- American pharmaceutical firm Inotiv has [reported on](#) a ransomware attack that occurred in August 2025. The Qilin ransomware group claimed responsibility, leaking personal information from over 9,500 individuals, including current and former employees and their family members.

Check Point Threat Emulation and Harmony Endpoint provide protection against this threat

- South Korean retail giant Coupang has [confirmed](#) a data breach that resulted in the exposure of personal information belonging to nearly 34 million clients, including full names, phone numbers, email addresses, and more. No payment details or account passwords were leaked in the incident.
- YouTube app for Android TV, SmartTube, has [been](#) targeted in an attack that resulted in the compromise of its developer signing keys and the distribution of a malicious update containing hidden malware. The incident impacted Android TV, Fire TV Stick, and similar device users.
- Belgian postal and package delivery service, Bpost, has [suffered](#) a data breach that resulted in the exfiltration of 5,140 files totaling about 30.46GB from a third-party exchange platform. The stolen data reportedly includes personal and business information of some customers of the affected department. The ransomware group TridentLocker has claimed responsibility for the attack.
- Canadian wireless telecommunications provider, Freedom Mobile, has [experienced](#) a data breach that resulted in attackers gaining unauthorized access to its customer account management platform and stealing personal information, including names, addresses, dates of birth, phone numbers, and account numbers. The company has not disclosed the exact number of affected customers.

VULNERABILITIES AND PATCHES

- Check Point has [elaborated](#) on the critical React2Shell vulnerability, CVE-2025-55182, that affects React 19.x and related server-side frameworks such as Next.js 15.x/16.x. The vulnerability enables unauthenticated remote code execution via malicious HTTP requests targeting the server's decoding process. Exploitation allows attackers to gain full control over application servers, intercept sensitive data, inject false transactions, and potentially pivot deeper into enterprise environments.

Check Point IPS provides protection against this threat (React Server Components Remote Code Execution (CVE-2025-55182))

- Check Point Research [revealed](#) a vulnerability in OpenAI Codex CLI that allowed attackers to achieve remote code execution via malicious project-local configuration files (MCP entries) executed without user prompts. OpenAI released a patch in version 0.23.0 to address the automatic execution risk.
- Check Point Research [shared](#) details of a critical exploit in Yearn Finance's yETH pool, where an attacker abused a smart contract flaw to mint trillions of tokens with a minuscule deposit, resulting in the theft of approximately \$9 million in assets from the Ethereum-based DeFi protocol.

THREAT INTELLIGENCE REPORTS

- Check Point [summarizes](#) a multiyear Salt Typhoon cyber-espionage campaign that compromised 80 telecom providers worldwide and a US state Army National Guard network, chaining SIM-based credential theft, network scans, Ivanti/PAN-OS/Cisco CVEs and GTP/GTPDOOR abuses to exfiltrate sensitive communications and configuration data.
- US and Canadian cybersecurity agencies [outlined](#) BRICKSTORM, a stealthy backdoor used by Chinese affiliated hackers to infiltrate VMware vSphere environments and maintain long-term access. The campaign targeted government services and IT, stealing credentials via VM snapshots and creating hidden machines.
- The ShadyPanda threat actor [ran](#) a seven-year campaign weaponizing verified Chrome and Edge extensions to infect over 4.3 million devices with spyware for remote code execution, payload delivery, traffic redirection, credential and cookie theft, browser fingerprinting, HTTPS credential interception, and behavioral biometrics exfiltration.
- Researchers [identified](#) a campaign weaponizing Velociraptor, a digital forensics tool, to establish stealthy command channels and maintain persistence in enterprise environments. Attackers exploited SharePoint's "ToolShell" chain using CVE-2025-49706 and CVE-2025-49704, linked to Storm-2603, and in confirmed cases delivered Warlock ransomware.
- Albiroix, a new Android banking trojan sold as Malware-as-a-Service (MaaS), [targets](#) over 400 financial and crypto apps using VNC-style remote control, accessibility abuse, overlays, and black-screen masking for on-device fraud. The malware is spread via smishing, WhatsApp lures, and fake apps with droppers over unencrypted TCP C2 channels using structured JSON messages.