cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Panama's Ministry of Economy and Finance (MEF) was hit by a ransomware attack that resulted in the theft of more than 1.5TB of data, including emails, financial documents, and budgeting details. The compromised information exposes sensitive institutional records tied to the country's fiscal operations and management. The attack was claimed by the INC Ransom group.

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

- Vietnam's National Credit Information Center (CIC) has experienced a data breach that resulted in the theft and leak of sensitive personal information tied to major Vietnamese financial institutions. The exposed records include personally identifiable information such as contact details and payment identifiers. The attack was claimed by ShinyHunters threat actor.

- American furniture company Lovesac has suffered a data breach that resulted in unauthorized access to its internal systems, exposing full names and other undisclosed personal information of an unconfirmed number of individuals. The attack occurred between February 12, 2025, and March 3, 2025, with the RansomHub ransomware gang later claiming responsibility and threatening to leak the stolen data if a ransom was not paid.

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

- New York Blood Center, a leading independent blood center serving upwards of 75M people in the US, has confirmed a ransomware attack that resulted in the theft of patient and employee data, including names, health information, Social Security numbers, government IDs, and financial account details. The incident impacted thousands, with more than 10K people in Texas affected.

- Streaming platform Plex has been a victim of a data breach that resulted in the theft of customer authentication data from one of its databases, including email addresses, usernames, and securely hashed passwords. The breach exposed a limited subset of customer data, but no payment card information was involved, and no exact volume of affected users or records was disclosed.

- British train operator London North Eastern Railway (LNER) has disclosed a data breach that resulted in unauthorized access to customer contact details and information on previous journeys through a compromised third-party supplier. Banking, payment card, and password data were not affected, and ticket sales and train operations remained unaffected.

- Brazilian dating app Sapphos has suffered a data breach that resulted in unauthorized access to sensitive user data via an insecure direct object reference (IDOR) vulnerability in its API. Approximately 17K users were affected, exposing personal information.

VULNERABILITIES AND PATCHES

- Microsoft's September 2025 Patch Tuesday report addresses 81 vulnerabilities, including two publicly disclosed zero-days. CVE-2025-55234, an elevation of privilege flaw in Windows SMB Server exploitable via relay attacks, and CVE-2024-21907, a denial of service risk in Newtonsoft.Json impacting SQL Server through improper handling of exceptional conditions.

- CVE-2024-40766, a critical improper access control flaw (CVSS 9.3) in SonicWall SSL VPN appliances (Gen 5–7, SonicOS 7.0.1-5035 and earlier), allows attackers to bypass access controls and in some cases crash firewalls. The vulnerability is actively exploited in the wild, including by Akira ransomware operators, with incidents tied to migrated configurations lacking credential resets.

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

- A vulnerability in Cursor AI editor allows arbitrary code execution via .vscode/tasks.json when opening a repository with Workspace Trust disabled. Exploitation can compromise developer environments, exfiltrate credentials or API keys, and enable supply-chain attacks.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed the global cyber threats in August 2025, revealing a 101% YoY surge in cyber attacks against agriculture sector, with increase in attacks on education, telecom, and government sectors. The US saw a 20% YoY increase in attacks, Africa the highest weekly attack rates, and ransomware rose 14% YoY, led by Qilin and Akira targeting manufacturing and business services.

- Check Point Research identified a new extortion group Yurei, that uses a Go based, open-source ransomware, for double extortion via files encryption and data theft. The malware retains flaws like failing to completely delete Windows Shadow Copies and reuses PowerShell wallpaper commands. Evidence links Yurei's activity to Morocco, with code artifacts connecting it to earlier families like SatanLockv2.

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

- Researchers uncovered an ongoing campaign by WhiteCobra group, flooding VS Code, Cursor, and Windsurf marketplaces with 24 malicious VSIX extensions to steal cryptocurrency. The extensions use fake branding and manipulate downloads to deliver LummaStealer on Windows and unknown macOS malware.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (InfoStealer.Win.Lumma; InfoStealer.Wins.Lumma; InfoStealer.Wins.Lumma.ta.; Trojan.Wins.Lumma.ta.*)*

- Researchers found a new malware strain targeting exposed Docker APIs with expanded infection capabilities, observed in August 2025 through honeypots. This version blocks external API access and deploys a binary containing previously used tools with broader functionality.