cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Several major European airports including Heathrow, Berlin, Brussels, Dublin, and Cork have experienced a cyber-attack, resulting in disruptions to electronic check-in and baggage drop systems using Collins Aerospace's MUSE software. The incident led to flights delays, cancellations, and diversions, with affected airports advising passengers to confirm travel plans.

- Luxury brands Gucci, Balenciaga, and Alexander McQueen were hit by a data breach that resulted in the theft of personal information of potentially millions of customers worldwide. The stolen data includes names, email addresses, phone numbers, physical addresses, and total amount spent by each customer, but not financial details such as credit card information. The cybercriminal group Scattered Lapsus$ Hunters claimed responsibility for the attack.

- Google has confirmed a cyber attack that resulted in hackers creating a fraudulent account within its Law Enforcement Request System platform, though no official data requests were made and no user data was accessed via the account. The incident raised concerns over potential unauthorized access and impersonation of law enforcement. The attack was claimed by Scattered Lapsus$ Hunters group.

- Hotels in Brazil and other countries have been victims of cyber-attacks that resulted in theft of guest payment card data from front-desk systems via phishing-delivered malware. The incidents involved VenomRAT enabling credential theft, remote access, and data exfiltration, impacting travelers' financial information across multiple regions. The campaign is attributed to the RevengeHotels group, which leveraged LLM-generated code.

  Check Point Harmony Endpoint provides protection against this threat *(RAT.Win.Venom; Loader.Win.Venom)*

- Venture capital firm, Insight Partners, has been a victim of a ransomware attack that resulted in data exfiltration and server encryption. The breach impacts 12,657 individuals and includes banking and tax data, personal information of current and former employees, limited partners' data, as well as fund, management and portfolio information.

- American jewelry company Tiffany's has suffered a data breach that resulted in the theft of customer personal data and gift card details. Attackers gained unauthorized access to company systems, compromising names, postal and email addresses, phone numbers, sales data, internal client reference numbers, as well as gift card numbers and associated PINs.

- SonicWall has disclosed a security incident involving unauthorized access to cloud-stored firewall backup preference files through brute-force attacks. According to the company, 5% of registered firewalls had their encrypted credential-containing backup files accessed, with information that could ease exploitation of affected devices.

VULNERABILITIES AND PATCHES

- Fortra has disclosed maximum severity vulnerability CVE-2025-10035 affecting the License Servlet of Fortra's GoAnywhere Managed File Transfer (MFT) software. The flaw results from deserialization of untrusted data, allowing remote, low-complexity command injection if the attacker can forge a valid license response signature. Successful exploitation targets externally exposed admin consoles and could enable unauthorized system access and command execution.
- A critical authentication bypass vulnerability in the Case Theme User WordPress plugin allowed unauthenticated attackers to gain access to arbitrary user accounts, including administrators, by exploiting flaws in the Facebook social login implementation when the target's email address is known. Mass exploitation has been observed in the wild with over 20,900 blocked attempts, as the flaw enables attackers to completely compromise vulnerable WordPress sites.
- Google has released a security patch addressing 4 vulnerabilities affecting Chrome. Among the vulnerabilities is CVE-2025-10585, a high severity type confusion vulnerability in V8. According to Google, an exploit for the vulnerability already exists in the wild, confirming that it could have potentially been exploited as a zero-day.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed a sophisticated ClickFix campaign leveraging fake job offers to deploy a Rust Loader, PureHVNC RAT, and the Sliver C2 framework across an eight-day intrusion. The investigation revealed multiple PureHVNC variants, features of PureRAT builder and PureCrypter, as well as details on PureCode, the developer of the malware.

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

- Researchers found that Russian threat actors Turla and Gamaredon collaborated in Ukraine, with Gamaredon's tools deploying and relaunching Turla's backdoor. On the shared machines, Gamaredon deployed a wide range of tools, while Turla only deployed Kazuar v3.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(APT.Win.Turla; APT.Wins.Turla.tays; APT.Wins.Turla.ta.*; InfoStealer.Wins.Gamaredon; InfoStealer.Win.Gamaredon; APT.Win.Gamaredon)*

- Researchers analyzed Iran's MuddyWater APT shifting from opportunistic to much more targeted spearphishing. It deploys custom malware (BugSleep, StealthCache, Phoenix), uses open-source tools, and operates across AWS, Cloudflare, DigitalOcean, OVH, M247, SEDO, and bulletproof hosts.

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

- Researchers detail a recent TA415 campaign against US government and academic targets tied to US–China economic issues. The group impersonated key orgs and figures, using obfuscated Python loaders to set up VS Code Remote Tunnels for remote access and data theft.