August 26 – September 1, 2024

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- California-based Patelco Credit Union has confirmed a data breach following a ransomware attack resulted in the exposure of sensitive personal information belongs to 726K clients and employees. The compromised data includes names, Social Security numbers, driver's license numbers, dates of birth, and email addresses. The RansomHub gang has claimed responsibility for the attack.

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

- Young Consulting (now Connexure) has suffered a data breach following a ransomware attack, resulting in the exposure of medical insurance information of over 950K individuals. BlackSuit ransomware group, a rebrand of the Royal gang, has claimed responsibility for the attack.

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

- The Toronto District School Board (TDSB) has been a victim of a ransomware attack that resulted in the exposure of personal information that belongs to an unspecified number of students from the 2023/2024 school year. The LockBit ransomware gang has claimed responsibility for the attack.

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

- The Seattle-Tacoma International Airport has experienced a cyberattack that resulted in ongoing IT system outages, disrupting reservation check-ins, and delaying flights. This disruption has severely impacted critical services, including baggage handling, flight information displays, and on-premise terminals, causing significant delays for thousands of travelers.

- Canadian airport parking service Park'N Fly has experienced a data breach that impacted approximately 1M clients following an unauthorized remote VPN access. The compromised data includes full names, email addresses, physical addresses, Aeroplan numbers, and CAA numbers, but does not involve financial information. No threat actor has claimed responsibility yet.

- US retailer Dick's Sporting Goods has been a victim of a cyberattack which involved unauthorized access to portions of its systems containing confidential information. The nature of the compromised data has not been disclosed, and no disruption to business operations has been reported.

- Irish Fota Wildlife Park has suffered a cyber-attack that resulted in the theft of payment card account numbers from customers who purchased tickets online between May 12 and August 27, 2024. User account information, including usernames, passwords, and email addresses, may have been accessed. Many individuals affected by the breach have reported receiving phishing attacks.

VULNERABILITIES AND PATCHES

- A critical vulnerability, CVE-2024-6386 (CVSS score: 9.9), in the WPML (WordPress Multilingual) plugin exposes over 1M WordPress sites to remote code execution attacks. The flaw allows authenticated users with contributor-level access or higher to inject and execute arbitrary PHP code via Twig templates. This vulnerability was patched in version 4.6.13.

  Check Point IPS provides protection against this threat (WordPress WPML Plugin Server-Side Template Injection (CVE-2024-6386))

- Google has acknowledged that CVE-2024-7965, a heap corruption vulnerability in Chrome, is being actively exploited in the wild. This vulnerability arises from an improper implementation in the V8 JavaScript and WebAssembly engine and has been addressed in Chrome's latest 128 release.

- Microsoft has fixed an ASCII smuggling vulnerability in Microsoft 365 Copilot. This issue involved using invisible Unicode characters to exfiltrate user’s sensitive data through clickable links, including multi-factor authentication (MFA) codes from emails.

- SonicWall has addressed a critical vulnerability, CVE-2024-40766 (CVSS score: 9.3), in its next-gen firewalls that could allow unauthorized access to the devices due to improper access control. This flaw affects SonicWall Firewall Gen 5, Gen 6, and Gen 7 devices running SonicOS 7.0.1-5035 and earlier versions and could potentially cause the firewall to crash under specific conditions.

THREAT INTELLIGENCE REPORTS

- Researchers have shared info on ManticoraLoader, a new Malware-as-a-Service (MaaS) from the AresLoader group. Compatible with Windows 7 and later, including Windows Server, ManticoraLoader features advanced obfuscation and information gathering, uses sophisticated evasion techniques, and persists on compromised systems.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Trojan-Downloader.Win.AresLoader; Trojan-Downloader.Wins.AresLoader)

- Microsoft has reported on a new malware, ‘Tickler,’ used by Iranian APT33 since at least July 2024. Tickler, a multi-stage C/C++ backdoor, delivers additional payloads and has targeted the aviation, oil and gas sectors, in addition to government entities in the USA and UAE.

- Researchers have uncovered an espionage campaign using a custom malware named ‘Voldemort’, aimed at intelligence gathering. The campaign used sophisticated impersonation of global tax authorities and targeted a range of industries worldwide with novel command and control tactics, including using Google Sheets and a saved search file for malicious operations.

- Researchers have identified a macOS variant of the HZ Rat backdoor, collecting sensitive data belongs to users of China’s DingTalk and WeChat. The malware replicates the functionality of its Windows version, utilizing shell scripts for payload delivery and supporting commands for executing shell commands, writing files, and more.