CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Library of Congress, part of the US Capitol complex and home to the world's largest media collection, was hacked by a foreign adversary, exposing email communications between Library staff and congressional offices from January to September 2024. The hack, described as sophisticated espionage, sought information on legislative inquiries but did not compromise House or Senate networks or the US Copyright Office.

- Giant American gambling and lottery company, International Game Technology (IGT), has confirmed a cyberattack that resulted in significant disruptions to portions of its internal IT systems and applications. The attack has impacted its operations, forcing some systems offline and affecting its ability to provide services to customers worldwide. No threat actor has claimed responsibility yet.

- The Mexican governmental platform Gob.mx has been hit by a ransomware attack by the group RansomHub, resulting in the theft of 313GB of data, including government contracts, insurance, and financial information. The attackers have threatened to release the stolen data to the dark web if an undisclosed ransom is not paid within 10 days.

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

- US space tech company Maxar Space Systems has been a victim of a data breach that resulted in unauthorized access to a system containing sensitive employee data, including home addresses, Social Security numbers, business contact details, employee numbers and more. The breach, originating from a Hong Kong-based IP address, lasted approximately one week before detection.

- London-based financial services company Finastra has suffered a cyberattack that resulted in the theft of 400GB of data from an internally hosted secure file transfer platform (SFTP) used to send files to customers. The stolen data was offered for sale on a criminal forum, allegedly containing sensitive information from the company's operations with its financial services clients.

- AI training software firm iLearningEngines has experienced a cyberattack that resulted in the theft of $250K through a misdirected wire payment and unauthorized access to its network. The attacker deleted email messages and accessed certain files, though the specific files remain unidentified.

- A threat actor identified as 'nears' (previously near2tlg) has claimed responsibility for a cyberattack on a French hospital that resulted in the exposure of sensitive health records for 750K patients. The attacker compromised a MediBoard account using stolen credentials. The leaked data includes full names, home addresses, phone numbers, health card histories, physician details, and prescriptions.

VULNERABILITIES AND PATCHES

- Over 2000 of Palo Alto Networks firewalls have been compromised in attacks exploiting two recently patched vulnerabilities: an authentication bypass (CVE-2024-0012) and a privilege escalation flaw (CVE-2024-9474) in the PAN-OS management web interface. These vulnerabilities enable attackers to gain administrator privileges and execute commands with root access, leading to malware deployment on affected devices.

  Check Point IPS provides protection against this threat *(Palo Alto Networks PAN-OS Authentication Bypass (CVE-2024-0012); Palo Alto Networks PAN-OS Command Injection (CVE-2024-9474))*

- Apple released patches for two zero-day vulnerabilities in macOS Sequoia JavaScriptCore (CVE-2024-44308) and WebKit (CVE-2024-44309) components. The first flaw allows arbitrary code execution via malicious webpages, while the second enables cross-site scripting attacks due to a cookie state management issue in WebKit. These vulnerabilities exploited in attacks on Intel-based Mac systems.

- Five critical local privilege escalation vulnerabilities have been discovered in the needrestart component, which is installed by default on Ubuntu Server. These vulnerabilities (CVE-2024-48990, CVE-2024-48991, CVE-2024-48992, CVE-2024-10224, and CVE-2024-11003) are actively being exploited and enable unprivileged users to gain root access without requiring user interaction.

THREAT INTELLIGENCE REPORTS

- Check Point Research has examined the activities of cyber criminals exploiting the Black Friday shopping season, identifying a significant increase in malicious websites and consistent phishing emails. The study revealed that approximately 3% of new Black Friday-related websites are malicious, with many impersonating well-known and boutique brands. These fraudulent sites often share similar design elements, indicating possible coordinated operations.

- Researchers have identified a new cash-out tactic, Ghost Tap, which exploits NFC relay techniques to steal funds from stolen credit cards linked to mobile payment systems like Google Pay and Apple Pay. Cybercriminals use publicly available tools such as NFCGate to relay NFC traffic, enabling them to conduct anonymous transactions at POS terminals in different locations, even across countries.

- Researchers have found multiple Linux backdoors, notably WolfsBane and FireWood, attributed to the China-aligned Gelsemium APT group. WolfsBane functions as the Linux counterpart to the Windows-based Gelsevirine backdoor. These malware variants are designed for cyberespionage, enabling the theft of sensitive data, maintaining persistent access, and evading detection.

- An ongoing supply chain attack, MUT-8694, targets npm and PyPI repositories using typosquatting. The campaign distributes infostealer malware, including Blank Grabber and Skuld Stealer, primarily affecting Windows users. These malicious packages impersonate legitimate libraries, referencing tools like MuMu Player, and leverage platforms like GitHub and repl.it to host payloads.