CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- American money transfer service MoneyGram has experienced a cyber-attack which led to significant network outages that disrupted its services globally. The attack has affected money transactions, particularly in the Caribbean, Jamaica and Mexico. No threat actor has claimed responsibility yet.

- The Centers for Medicare & Medicaid Services (CMS) federal agency has disclosed being a victim of a data breach that resulted in the exposure of personal and health information for over 3.1M individuals. The breach, which stemmed from the 2023 MOVEit attack by the Cl0p ransomware group, compromised names, Social Security numbers, Medicare identifiers, and more.

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

- American automobile dealership group AutoCanada has been a victim of a ransomware attack that resulted in the exposure of employee data, including names, addresses, payroll information, and social insurance numbers. The Hunters International ransomware gang has claimed responsibility for the attack, leaking terabytes of sensitive data, such as HR records, financial documents, and personal employee information. There is no indication that customer data was exfiltrated in the breach.

- The Arkansas City water treatment facility has disclosed a cyberattack that impacted at least one of its computers. While there were no disruptions to the water supply or services, the facility had to switch to manual operations to contain the incident.

- Franklin County, located southeast of Kansas City, was hit by a ransomware attack that resulted in the exposure of sensitive personal information for nearly 30K residents. The breached data included names, Social Security numbers, driver's license numbers, financial account details, and medical information from county poll book records. No threat actor has claimed responsibility yet.

- The City of Richardson, Texas, has confirmed a cyber-attack involving an encryption attempt of files on its network. While a small number of files were encrypted, the city's security systems prevented further damage, and there is no early indication that sensitive data was accessed.

- Network Rail's public Wi-Fi services, operated by the British communications company Telent, were compromised at 20 UK train stations, displaying Islamophobic messages to users. The affected stations include key commuter hubs in London, Reading, Leeds, and Glasgow.

- UK Fylde Coast Academy Trust (FCAT) was hit by a ransomware attack that compromised its IT infrastructure, affecting 10 schools across Blackpool and Lancashire. The attack disrupted operations, forcing schools to revert to non-IT processes and limiting access to essential systems.

VULNERABILITIES AND PATCHES

- NVIDIA has disclosed a software update for a critical vulnerability (CVE-2024-0132) in the NVIDIA Container Toolkit. This Time-of-Check Time-of-Use (TOCTOU) flaw allows attackers to escape container confines and gain full access to the host system, potentially leading to code execution, privilege escalation, and data tampering. The vulnerability affects all versions up to v1.16.1 and has been addressed in version v1.16.2.

- Researchers discovered a vulnerability in Kia's web portal, allowing them to remotely control connected car features such as tracking locations, unlocking doors, and starting engines. By exploiting the portal's API, they gained unauthorized access using vehicle license plates and a tool that converts them into VINs. Although Kia has since patched the flaw, this is the second such vulnerability found in its systems, with similar issues also affecting other carmakers.

- A vulnerability in the ChatGPT macOS app allows attackers to implant persistent spyware, dubbed SpAIware, into the app's memory via indirect prompt injection, enabling continuous data exfiltration of user inputs and future chat sessions. OpenAI addressed the issue in version 1.2024.247 of the app.

THREAT INTELLIGENCE REPORTS

- Check Point Research uncovered a malicious app on Google Play designed to steal cryptocurrency, marking the first time a crypto drainer targeted mobile users exclusively. Disguised as a legitimate Web3 tool using the trusted WalletConnect protocol, the app evaded detection for five months and was downloaded over 10,000 times. By exploiting social engineering and advanced crypto-drainer tactics, the attackers stole around $70,000 from over 150 victims.

  Check Point Harmony Mobile provides protection against this threat

- Check Point Research analyzed DLL Hijacking techniques, focusing on how malicious actors exploit legitimate applications to run malicious code by abusing dynamic library dependencies. The study examined documented cases involving state-sponsored actors like Lazarus Group and Tropic Trooper, highlighting the use cases of evasion, persistence, and privilege escalation.

- Researchers identified two previously undocumented malware samples tied to the North Korean APT group Kimsuky, also known as Sparkling Pisces. The first, KLogEXE, is a keylogger that collects and exfiltrates user activity, while the second, FPSpy, is an advanced backdoor capable of data collection and command execution. Both samples share a codebase, suggesting a link between the two.

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

- Microsoft found that the Storm-0501 threat group is launching multi-staged ransomware attacks on hybrid cloud environments in the US. The group compromises on-premises systems, moves laterally to cloud environments, and causes data exfiltration, credential theft, backdoor access, and ransomware deployment across sectors like government, manufacturing, transportation, and legal.