CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- American telecom giant AT&T has disclosed a massive data breach that exposed personal information of 110M of its customers. The data was stolen from the company's workspace on a third-party cloud platform, referring to Snowflake. The leaked data allegedly includes the full metadata of all of AT&T mobile customers, which can be used to find people's close contacts.

- Pharmacy giant Rite Aid has been a victim of a ransomware attack that resulted in the theft of 45M records of clients' personal information. The data allegedly includes names, addresses, driver's license ID numbers, dates of birth, and Rite Aid rewards numbers. RansomHub ransomware group has claimed responsibility, threatening to leak the stolen data by July 22.

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

- Dallas County has been a victim of a ransomware attack that resulted in the exposure of personal data for over 200K individuals. The exposed data includes names, Social Security numbers, medical information and more. Play ransomware gang has claimed responsibility.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (Ransomware.Win.Play; Ransomware.Wins.PLAY)

- Japanese technology giant Fujitsu has experienced a cyber-attack that resulted in the potential theft of personal and customer information due to malware discovered on multiple work computers. The company has not specified the type of malware used or the exact nature of the stolen data. No threat actor has claimed responsibility yet.

- The American Radio Relay League (ARRL) has disclosed a ransomware attack that resulted in the theft of personal information, including names, addresses, and Social Security numbers of 150 employees. Although ARRL has not attributed the attack to a specific ransomware gang, sources indicate that the Embargo ransomware might be responsible.

- Advance Auto Parts has suffered a data breach that impacting nearly 2.3M job applicants and current and former employees, with the stolen data being sold on an underground forum by a hacker known as 'Sp1d3r'. The breach, part of a larger campaign targeting Snowflake accounts, exposed sensitive information such as full names, Social Security numbers, driver's licenses, and government ID numbers.

- The City of Philadelphia has confirmed a data breach that affected more than 35K individuals' personal information. The exposed data includes names, addresses, Social Security numbers, medical information, and limited financial information.

VULNERABILITIES AND PATCHES

- Check Point Research has identified a new zero-day vulnerability, CVE-2024-38112, that is being exploited in the wild, potentially impacting millions of users. The flaw is leveraging Internet Explorer shortcut files to lure Windows 10/11 users for remote code execution.
  Check Point provides protection against this threat *(Internet Shortcut File Remote Code Execution)*

- Microsoft's July 2024 Patch Tuesday addresses 139 vulnerabilities including 5 critical remote code execution flaws, among which is CVE-2024-38060, a flaw in the Windows Imaging Component related to TIFF (Tagged Image File Format) image processing. The updates cover various Microsoft products, with significant patches for privilege elevation in Windows Hyper-V and spoofing in the MSHTML platform.

- GitLab has released several patches, among which is a critical severity issue, CVE-2024-6385, in GitLab Community and Enterprise editions versions from 15.8 to 16.11.6, 17.0 to 17.0.4, and 17.1 to 17.1.2. This flaw allows attackers to trigger a pipeline as another user under certain circumstances.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released June 2024's Most Wanted Malware that highlights a shift in the Ransomware-as-a-Service (RaaS) landscape, with RansomHub surpassing LockBit3 to take top position as the most prevalent group. Additionally, a Windows backdoor dubbed BadSpace was identified, spreading via fake browser updates

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

- Check Point Research has delved into the usage of compiled V8 JavaScript by malware authors, highlighting its role in evading static detections and obscuring source code. Compiled V8 JavaScript, a feature of Google's V8 engine, allows attackers to compile JavaScript into low-level bytecode, making it difficult to analyze statically. This technique has been employed across various malware types such as RATs, infostealers, miners, and ransomware.

- Researchers share detailed technical analysis of APT41's new tooling, focusing on their use of DodgeBox loader which loads the MoonWalk backdoor. DodgeBox is new variant of StealthVector used by the China affiliated threat actor. This loader incorporates various evasive techniques such as call stack spoofing, DLL sideloading, DLL hollowing and environmental guardrails.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Trojan.Win.APT41; APT.Win.APT41; Trojan.Wins.APT41; APT.Wins.APT41.ta.*)*

- Researchers have discovered a new ransomware strain named "Estate", leveraging CVE-2023-27532 to exploit dormant accounts on FortiGate Firewall SSL VPNs for initial network access. The Estate Ransomware deploys a persistent backdoor on the failover server and conducts lateral movement via RDP. It utilizes tools such as NetScan, AdFind, and various NirSoft utilities.