Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- New victims of Clop ransomware gang that leveraged a zero-day security flaw (CVE-2023-0669) in the Fortra GoAnywhere Managed File Transfer system were disclosed. Among those are the American luxury brand retailer Saks Fifth Avenue, and City of Toronto.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat *(GoAnywhere MFT Insecure Deserialization (CVE-2023-0669); Ransomware.Win.Clop; Ransomware_Linux_Clop_A; Ransomware_Linux_Clop_B)*

- The City of Oak Ridge, Tennessee has experienced network issues that appeared to be a ransomware attack that affected its technology systems. No ransomware group claimed responsibility yet.

- The Italian luxury sports car maker Ferrari has announced a data breach following an extortion attack on the company's IT systems. The leaked data consists of the company's clients' personal information including full names, addresses, email addresses, and phone numbers.

- The Bitcoin ATM manufacturer General Bytes has confirmed a breach resulted in the theft of $1.6M cryptocurrency belongs to the company and its clients. The threat actors exploited a zero-day vulnerability (CVE-2023-28725) in its BATM management platform, the service interface that Bitcoin ATMs use to upload videos, which allowed them to upload a JavaScript script and run it with BATM user privileges.

- Latitude Financial Services, Australian consumer loans provider, confirmed a significant data breach. The leaked data consists of records of 14 million customers, including driver's license numbers, passport numbers and financial statement. Among the leaked data , driver's license numbers of 7.9 million Australian and New Zealand customers

- Initial access cyber-attacks that are affiliated to a Chinese state-sponsored cyberespionage group APT41, has been observed targeting the telecommunication sector in the Middle East. The threat actors infiltrate Internet-facing Microsoft Exchange servers to perform command execution, conduct reconnaissance, steal credentials, and perform lateral movement and data exfiltration activities.

  Check Point Threat Emulation provides protection against this threat *(APT.Wins.APT41)*

VULNERABILITIES AND PATCHES

- Researchers share findings on 55 zero-day vulnerabilities that were exploited in 2022. They indicated that Chinese state-sponsored cyber espionage groups exploited more zero-days than other cyber espionage actors. Four vulnerabilities were exploited by financially motivated threat actors, while 75% of them were linked to ransomware.

- Google has identified eighteen zero-day vulnerabilities in Exynos Modems. Four of them (CVE-2023-24033, CVE-2023-26496, CVE-2023-26497 and CVE-2023-26498) allow threat actors to remotely compromise smartphone devices using just the victim's phone number.

- Cisco has discovered two vulnerabilities in WellinTech's KingHistorian industrial control systems data manager. The first flaw, an information disclosure vulnerability (CVE-2022-45124) could allow an adversary to steal user's personal information such including names and passwords. The second flaw (CVE-2022-43663) could allow an adversary to perform a buffer overflow by sending a malicious packet to the targeted machine.

THREAT INTELLIGENCE REPORTS

- Check Point Research has detected malicious packages on PyPI, Python package index, that use phishing techniques to hide its malicious intent. The malicious packages stealthy downloading and executing obfuscated code as part of their installation process, leading to supply chain risks.

  Check Point CloudGuard Spectral provides protection against this threat.

- Researchers have uncovered a new variant of the FakeGPT Chrome extension, dubbed "ChatGPT-For-Google", based on an open-source project affecting thousands victims daily. The variant steals Facebook session cookies and compromises accounts under a cover of a ChatGPT integration for Browser, using malicious sponsored Google search results.

- Researchers share the tools, techniques and procedures (TTPs) of the North Korean state-sponsored cyberespionage group APT37 (aka ScarCruft). The threat actor primarily targets individuals in South Korean organizations through spear phishing emails. In addition, APT37 distributes the Chinotto PowerShell-based backdoor using various attack vectors.

  Check Point Harmony Endpoint provides protection against this threat (APT.Win.APT37)

- Nexus, a new Android botnet, has been observed in worldwide fraudulent campaigns. Nexus has similarities to SOVA Android banking Trojan, and mainly functions in Account Takeover against banking portals and cryptocurrency services. The malware is promoted on underground forums and Telegram as Malware-as-a-Service (MaaS).