Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The American Greater Richmond Transit Company (GRTC), which provides services for millions of people, has been a victim of cyber-attack that impacted certain applications and parts of the GRTC network. The Play ransomware gang claimed responsibility for the attack.

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

- Multinational retailer Aldo has acknowledged a ransomware attack that impacted the systems of an unspecified franchise partner. The LockBit ransomware gang has claimed responsibility for the attack.

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

- AlphV (aka BlackCat) ransomware gang claimed responsibility for cyber-attacks on three victims: American medical provider Norton Healthcare; IT services and business consulting company HTC Global Services; and Tipalti, an Israeli fintech software provider startup with headquarters in Canada. The attack on Tipalti has allegedly resulted in the compromise of over 265GB of confidential information belonging to the company and its customers, including the video game Roblox and streaming platform Twitch. According to AlphV, an insider from Tipalti was and is still actively involved in the attack.

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

- American multinational confectionery company Hershey has disclosed a data breach that affected more than 2,200 people as the result of a successful email phishing attack against the company. The stolen data potentially includes full names, health and medical details, debit and credit card data, financial account information and more.

- Japanese car manufacturer Nissan has confirmed a cyber-attack that affected Nissan Oceania, its Australian and New Zealand regional division, and took systems offline as a precaution. The company did not share specific information on the type or extent of the breach.

- The Hunters International ransomware group claimed responsibility for cyber-attacks on the Australian shipbuilder Austal USA and Florida water agency, St. Johns River Water Management District. The attacks affected Florida water agency's information technology environment and potentially impacted Austal's USA documents, recruiting information, finance details, certifications, and engineering data.

VULNERABILITIES AND PATCHES

- Google's December 2023 Android security update addresses 85 vulnerabilities, notably including a critical zero-click remote code execution flaw (CVE-2023-40088) in the Android System component. The update addresses 84 other security vulnerabilities, with three critical ones related to privilege escalation and information disclosure in Android Framework and System components (CVE-2023-40077, CVE-2023-40076, and CVE-2023-45866), and another critical flaw in Qualcomm's closed-source components (CVE-2022-40507).

- Atlassian has released software fixes to address four critical vulnerabilities that could lead to remote code execution (RCE). These flaws include a deserialization vulnerability in the SnakeYAML library (CVE-2022-1471), and RCE vulnerabilities in Confluence Data Center and Confluence Server, Assets Discovery for Jira Service Management and in Atlassian Companion app for macOS (CVE-2023-22522, CVE-2023-22524, CVE-2023-22523).

THREAT INTELLIGENCE REPORTS

- Check Point Research has examined various attack vectors in modern Outlook and compared the user interoperability required for each scenario when attackers use Outlook to deliver their exploits. The attack vectors have been observed in three categories: the “obvious” Hyperlink attack vector, the “normal” attachment attack vector, and the “advanced” attack vector.

  Check Point Threat Emulation and IPS provide protection against this threat.

- Check Point Research has identified a shift in the targeting of the Iranian hacktivist proxies which are now extending their cyber operations to include targets in other countries besides Israel, with a particular emphasis on the United States. Moreover, groups such as CyberAv3ngers and Cyber Toufan appear to be adopting a narrative of retaliation in their cyberattacks. They claim to target US entities using Israeli technology, suggesting a strategy of simultaneously targeting both Israeli and US interests.

- Check Point Research exposes a troubling trend in the cryptocurrency landscape. Deceptive actors are manipulating pool liquidity, sending token prices soaring by 22,000%. The manipulation of pool liquidity resulted in a swift and calculated theft of $80,000 from unsuspecting token holders. This incident sheds light on the evolving strategies scammers employ to exploit decentralized finance platforms.

- The Russia-based actor Star Blizzard (aka COLDRIVER/Callisto Group) persistently employs spear-phishing attack techniques for information-gathering purposes. The threat actor has been observed targeting individuals and organizations in the UK and US that involved in international affairs, defense, and logistics support to Ukraine.