Check Point Research
WEEKLY INTELLIGENCE REPORT
July 17 - 23, 2023

TOP ATTACKS AND BREACHES

- The Microsoft Exchange email account espionage campaign, which has been attributed to Chinese threat actor 'Storm-0558', has reportedly accessed the email account of United States ambassador to China and compromised hundreds of thousands of individual United States government emails. Researchers warn that the method used in the campaign could also have targeted user accounts other Microsoft services, such as OneDrive and Azure environments.

- Tampa General Hospital in Florida, United States, has announced that confidential information of 1.2 million patients of the hospital has been disclosed in a cyber-attack. The data includes identifying details such as names, addresses and Social Security numbers, as well as medical history and treatment information. Ransomware group Snatch has claimed responsibility for the attack and posted the data to its leak site.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Snatch)

- American cosmetics giant Estée Lauder has stated that its network had been accessed by a third party in a cybersecurity incident, and that data had been stolen by the attackers. Two separate ransomware groups, Black Cat (ALPHV) and Cl0p, have each claimed to have compromised the company and are threatening to disclose the exfiltrated data if not paid ransom.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats
  (Ransomware.Win.BlackCat, Ransomware.Win.Clop, Ransomware_Linux_Clop)

- Norwegian mining and recycling corporation TOMRA has been forced to shut down parts of its network and some of its offices after discovering that a threat actor had gained access to its systems. The company claims that it is unaware of any ransom demands or data encryption.

- Software development platform GitHub has found a social engineering campaign targeting technology firm employees on the platform. According to GitHub, North Korean APT group Lazarus aimed to gain users' trust to 'collaborate' on a shared repository, which would deliver malware once run.

- Malware sharing platform VirusTotal has posted a public apology after it has been revealed that a list containing information of more than 5,000 of the site's customers has been shared online. According to VirusTotal, the list was leaked as result of employee human error.

VULNERABILITIES AND PATCHES

- Citrix has published a security advisory addressing CVE-2023-3519, a critical unauthenticated remote code execution zero-day vulnerability affecting its ADC and gateway products. According to security researchers, the vulnerability has already been exploited in the wild by Chinese APT groups, while others say that the exploits have been available for purchase on the dark web.

  Check IPS blade provides protection against this threat *(Citrix NetScaler Remote Code Execution (CVE-2023-3519))*

- Adobe has released an out-of-band security update addressing 3 vulnerabilities in Adobe ColdFusion. Among the vulnerabilities are CVE-2023-38204, a critical remote code execution vulnerability, and CVE-2023-38205, a critical security bypass vulnerability which has been exploited in the wild.
- Oracle has published its July critical patch advisory. This month's patch includes fixes for more than 500 security vulnerabilities affecting a wide array of Oracle products.
- Atlassian has released a security advisory addressing 3 high severity remote code execution vulnerabilities. Two of the vulnerabilities affect Confluence DC&S, and the third affects Bamboo.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed BundleBot, a new infostealer which is being spread via malicious Facebook ads and compromised accounts. The malware abuses the dotnet bundle (single-file), self-contained format, which results in a single, large binary file that is difficult to detect by security tools.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(InfoStealer.Win.FakeGoogleAI, InfoStealer.Wins.BYOSDownloader)*

- Check Point Research has discovered multiple Facebook scam pages with hundreds of thousands of followers, impersonating popular generative AI services. After an infection chain of several steps, the victims are tricked to downloaded an info stealer that exfiltrates their online passwords, crypto wallets and any information saved in their browser
- Check Point researchers have identified a malicious Node Package Manager (NPM) package that is still being delivered to users even after being removed from the NPM registry. The package, which aimed to harvest victims' credentials, was still being delivered to users via the popular CDN 'jsdelivr'.
- The Ukrainian CERT has discovered an ongoing spyware campaign targeting the country's defense forces. The agency has attributed the campaign to Turla, a threat actor known to be affiliated with the Russian FSB. The initial infection vector used in the campaign was spear-phishing emails containing malicious attachments, which would eventually deliver backdoor payloads.