October 3 – 9, 2022

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- CommonSpirit Health, the second-largest nonprofit hospital chain in the U.S with 140 hospitals and over 1,000 facilities in 21 states, suffered a cybersecurity incident that disrupted medical services across the country. Facilities in Iowa, Nebraska, Tennessee and Washington were among those affected. The nature of the attack is still unclear, yet a ransomware attack is a possibility.
- Russian-speaking threat group Killnet claims responsibility for attacks taking down different US state government websites, including those of Colorado, Kentucky, Mississippi and others.
- Binance, the world's largest cryptocurrency exchange, announced that Binance Smart Chain has been hacked, and crypto coins worth almost $570 million were stolen.
- RansomEXX Ransomware group claims to have stolen over 7GB of data belonging to the Italian luxury sports car manufacturer Ferrari. The stolen data allegedly include contracts, invoices, internal company information, repair manuals and more. A Ferrari spokesperson confirms the data leak, but denies being a victim of a ransomware attack.

  Check Point Threat Emulation provide protection against this threat (Ransomware.Wins.Ransomexx)
- Colombia's National Food and Drug Surveillance Institute (INVIMA) has been a victim of a cyber attack that disrupted the systems used to manage the import authorization of vital medicines, as well as the access to its website.
- The City of Tucson, Arizona, has disclosed a data breach that occurred during May, which caused the leak of personal information of more than 123,500 individuals. The leaked data includes names, Social Security numbers, drivers' licenses, state identification numbers, and passport numbers.
- Taiwanese chip maker ADATA has allegedly been a victim of a ransomware attack launched by RansomHouse gang. While the threat actors claim to obtain 1TB of data, the company denies the current breach, saying the leaked files are from a ransomware attack that occurred on May 2021.
- 'DNS' (Digital Network System), a Russian retail chain, disclosed they were affected by a data breach just hours after alleged data belonging to the company was leaked on a popular hacking forum by a group called 'NLB Team'. The leaked data has not yet been verified, but contains information of presumed millions of DNS customers and employees.

VULNERABILITIES AND PATCHES

- NSA, CISA, and the FBI have released a joint advisory including the top CVEs used since 2020 by People's Republic of China (PRC) state-sponsored threat actors to target the US government and critical infrastructure networks.

  Check Point IPS provides protection to all vulnerabilities mentioned in the report

- A critical zero-day RCE vulnerability in Zimbra Collaboration Suite (ZCS) is currently being exploited. Tracked CVE-2022-41352, the flaw will let threat actors overwrite the Zimbra webroot, implant shellcode in the web root to gain remote code execution, and access users' personal accounts.

- Fortinet has disclosed a critical security flaw, tracked CVE-2022-40684, in FortiOS and FortiProxy. The flaw is an authentication bypass vulnerability on the administrative interface, which could allow remote threat actors to log into unpatched devices. Fortinet advised to update vulnerable products.

THREAT INTELLIGENCE REPORTS

- Check Point Research shares findings on activity of Bumblebee loader, a recent threat that has gained a lot of attention due to its many links to several well-known malware families. Infected standalone computers will likely be hit with banking Trojans or infostealers, whereas organizational networks can expect to be hit with more advanced post-exploitation tools such as CobaltStrike.

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

- Researchers have revealed an Iranian hacking group dubbed "AppMilad" uses a new RatMilad Android Spyware disguised as VPN app, in an extensive campaign primarily targeting Middle Eastern enterprises. The malware can perform a wide range of malicious actions after it is installed on a victim's device including file manipulation, audio recording, and application permission modification.

- Researchers have discovered a malware called LilithBot, associated with threat group dubbed Eternity (aka EternityTeam; Eternity Project) who sells LilithBot as Malware-as-a-Service (MaaS) in the dark web. LilithBot has advanced capabilities allowing it to steal information and upload it as a zip file to its Command and Control.

- Researchers have observed a new technique dubbed "Bring Your Own Driver", used by The BlackByte ransomware gang, exploiting a targeted system by abusing a legitimate signed driver with an exploitable vulnerability.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Win.BlackByte)*