December 11 – 17, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Ukraine's largest mobile operator, Kyivstar, was hit by "largest cyber-attack on telecom infrastructure in the world", rendering millions without mobile and internet services for at least 48 hours. Reportedly, the attack also affected air raid sirens, ATMs, and point-of-sale terminals. Russia-affiliated group Solntsepek, who was previously linked to Russian military group Sandworm, claimed responsibility for the attack. Another Russia-aligned group, Killnet, claimed responsibility, however its involvement hasn't been proved. Kyivstar has 24.3 million mobile subscribers and over 1.1 million home internet subscribers.

- MongoDB disclosed a cybersecurity breach, revealing that their corporate systems were compromised resulting in the exposure of customer data. The threat actors are believed to have had persistent unauthorized access to the data for some time before the attack was detected on December 13th.

- Ontario Public Library revealed it fell victim to a ransomware attack, after it suffered a major systems outage caused by the cyber-attack. The library's digital services were disrupted, including WiFi, printers, the library website, and any other online products.

- A supposed ransomware attack caused a Swiss district court's IT system and telephone lines to be taken down. The attack represents a recent increase in ransomware attacks against Swiss organizations.

- The Central Bank of Lesotho is suffering outages due to a cyber-attack. The bank confirmed in a statement that the attack did not cause any financial losses, although it was forced to suspend some of its system to stop the infiltration. This made any inter-bank transfers in the country impossible, and could affect Lesotho's currency exchange rates with South Africa, its surrounding neighbor.

- The Hunters International ransomware gang attacked the Fred Hutchinson Cancer Center, claiming to have compromised 533GB of the organization's data. The group is also reportedly attempting to extort individual patients treated at the center, threatening to leak Social Security Numbers, lab results and medical history should the client not pay $50 to have their personal information removed.

- American radiology and oncology services provider Akumin was reportedly hit by two ransomware groups, BlackSuit and BianLian. According to the company's statement and information published by the groups, BlackSuit were able to exfiltrate and encrypt the data, whilst BianLian claimed to have 5 TB of highly sensitive data, including PHI (Personal Health Information).

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.BlackSuit, Ransomware_Linux_BlackSuit)

VULNERABILITIES AND PATCHES

- In December’s Patch Tuesday, Microsoft have issued security updates for 36 flaws and six non-Microsoft CVEs, one of which a zero-day vulnerability. Three critical flaws were fixed: Microsoft Power Platform Connector spoofing vulnerability (CVE-2023-36019), and two ICS Remote Code Execution vulnerability (CVE-2023-35630 ,CVE-2023-35641). The zero-day vulnerability (CVE-2023-20588) is a division-by-zero error on some AMD processors, and was classified as a medium severity vulnerability.

- Apple released security updates for multiple vulnerabilities in their products, including Safari, iOS and iPadOS, Sonoma, Ventura, and Monterey. Exploits can allow threat actors to take control of affected systems, and two of the vulnerabilities in iOS and iPasOS are reportedly being actively exploited.

- Adobe released nine patches to address 212 CVEs in their products. 186 of the vulnerabilities are cross-site scripting (XSS) bugs, while critical vulnerabilities in Adobe After Effects, Adobe Illustrator and Substance 3D Sampler were also addressed in this patch.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published a report highlighting the capabilities of the new Rhadamanthys stealer version 0.5.0. Rhadamanthys is an info stealer with a diverse set of modules that is being sold on the black market. In order to make it a coveted commodity in the malware market, the author of Rhadamanthys keeps updating it and adding new extensions, turning it into a multipurpose bot with a diverse set of features.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (InfoStealer.Wins.Rhadamanthys.E/F, InfoStealer.Wins.Rhadamathys.C/D/G)

- Check Point Research summarized November’s top cyber threats, including the new AsyncRAT campaign, where malicious HTML files were used to spread the malware; another observed top malware was the FakeUpdates downloader, which tricks users into running fake browser updates.

  Check Point Threat Emulation provide protection against this threat (RAT.Win32.AsyncRat, Downloader.WIN32.SocGholish, Dropper.Wins.SocGholish)

- Microsoft tackles Storm-1152, the primary group of sellers and creators of fraudulent Microsoft accounts that act as the gateway to various cybercrime activity: phishing, identity theft and fraud, and distributed denial of service (DDoS) attacks. The group runs a cybercrime-as-a-service ecosystem that includes websites and social media accounts, all used as distribution platforms for the group who has already sold over 750 million fraudulent accounts to other cyber criminals. Multiple groups engaged in ransomware and data theft were observed utilizing Storm-1152 accounts.