November 27 – December 3, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research provides highlights about Cyber Av3ngers group activity, which has taken responsibility on defacing workstations at Pennsylvania's Aliquippa municipal water authority. Following the attack, CISA has published an advisory about this hacktivists group which is affiliated to Iranian Revolutionary Guard Corps (IRGC) and reportedly hit multiple water utility companies in the United States by targeting Unitronics' PLC devices.

- The service of 60 United States based credit unions has been disrupted, after Ongoing Operations, a cloud hosting provider firm, has been a victim of a ransomware attack. Security researchers believe that the threat actors had exploited the Citrix NetScaler 'Citrix Bleed' vulnerability (CVE-2023-4966) to gain access to the firm's network.

  Check Point IPS provides protection against this threat (Citrix NetScaler Information Disclosure (CVE-2023-4966))

- Japan's space agency, JAXA, has disclosed that it had been hit by a cyber-attack. JAXA claimed that important rocket or satellite related operations information had not been affected, but that the breach is still being investigate. According to Japanese media, the attack had occurred in the summer, and was discovered by Japan's police a few months later.

- Campaigns targeting customers of hospitality reservation service booking.com have recently ramped up. Threat actors target hotels to gain access to their booking.com administration portals. The attackers then contact the hotels' customers using the official app to redirect the payment to their own accounts.

- Official Israeli government agencies have announced that a cyber incident had affected the network of Ziv hospital in Safed. The newly founded hacktivist group Malek Team has taken responsibility for the attack and claims to have exfiltrated 500GB of patients' medical data from the hospital's servers.

- India's National Aerospace Laboratories, a government owned firm which develops civilian aircraft, has suffered a ransomware attack on its network. The LockBit ransomware group has claimed responsibility for the breach and has leaked several documents allegedly exfiltrated in the breach.

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

- More than $50m in customers' cryptocurrency has been stolen in a cyber-attack against blockchain platform KyberSwap. According to the company, the attackers used "a series of complex actions" to exploit a vulnerability and transfer funds from customers' wallets to their own.

VULNERABILITIES AND PATCHES

- Google has released an advisory for Google Chrome addressing seven security vulnerabilities. One of the vulnerabilities, CVE-2023-6345, is a critical integer overflow vulnerability in the Skia 2D graphics library, which could allow a remote attacker to perform sandbox escape. Google claims to be aware of an active exploit for this vulnerability existing in the wild.

- Apple has published security updates for its devices' operation systems to patch the information-disclosure vulnerability CVE-2023-42916. According to Apple, the company is aware of reports of the vulnerability being actively exploited in the wild against previous versions of iOS devices.

- Security researchers warn of active exploitation in large scale of OwnCloud vulnerability CVE-2023-49103, a critical information disclosure vulnerability in the graphapi OwnCloud from the last week.

- Zyxel has released an advisory addressing 6 security vulnerabilities affecting the company's NAS devices. Three of the vulnerabilities (CVE-2023-4473, CVE-2023-4474 and CVE-2023-35138) are considered critical and could allow an unauthenticated remote attacker to gain arbitrary code execution.

THREAT INTELLIGENCE REPORTS

- Researchers have uncovered a campaign targeting a United States company in the aviation sector. The threat actors used spear phishing emails to gain access to the victim firm's network, and installed a payload that collects information and creates a reverse shell. The researchers suspect the previously unfamiliar threat actor's motivation is commercial industrial espionage.

- The Ukrainian CERT has published an advisory warning of mass-targeting of Ukrainian citizens with emails leading to Remcos RAT infections. According to the report, the attackers sent malicious court summons to 15,000 Ukrainians using compromised email addresses of official judiciary authorities.

  Check Point Threat Emulation provides protection against this threat (RAT.Wins.Remcos.A, Injector.Win.RunPE.A)

- A campaign using a modified version of the notorious Gh0st Remote Access Trojan, dubbed SugarGh0st, has been discovered. The threat actors have targeted Uzbekistan's Ministry of Foreign Affairs, as well as users in South Korea. Security researchers assess that a Chinese nation-state group is behind the attacks.

  Check Point Threat Emulation provides protection against this threat (RAT.Win.Gh0stRAT, RAT.Wins.Gh0stRAT)

- Researchers warn of a new campaign distributing the Lumma information stealer malware. The attackers had first breached a legitimate website, then use phishing emails to direct victims to the compromised website, causing malicious content to be downloaded.

  Check Point Threat Emulation provides protection against this threat (InfoStealer.Win.LummaC2, InfoStealer.Wins.Lumma)