Sept 27 – Oct 3, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has discovered cyber attacks against the users of PIX, the instant payment solution created and managed by the Brazilian Central Bank. The attackers distributed two different variants of banking malware, named PixStealer and MalRhino, through two separate malicious applications on Google’s Play Store to carry out their attacks. Both malicious applications were designed to steal money of victims through user interaction and the original PIX application.

  Check Point Harmony Mobile provides protection against this threat

- Security researchers have uncovered the remote access malware Sarwent disguised into a fake Anti Pegasus Antivirus: Threat actors are targeting individuals fearing to become victim of the spyware and are using a fake Amnesty International website to lure them into downloading the malware.

  Check Point Anti-Virus provides protection against this threat (Backdoor.Win32.Sarwent)

- Hackers have stolen cryptocurrencies from 6,000 Coinbase customers after leveraging a vulnerability to bypass the company's SMS two-factor authentication security system.

- Japanese electronics supplier JVCKenwood has been victim of a Conti ransomware attack where 1.7 TB of data was allegedly stolen. Threat actors demanded a $7 million ransom.

  Check Point Harmony Endpoint provides protection against this threat (Ransomware.Win32.Conti)

- Tennessee-based shipping company Forward Air Corporation has disclosed a data theft after a ransomware attack that allowed threat actors to access current and former employees' sensitive information.

- Bandwidth.com has fell victim of a distributed-denial-of-service (DDoS) attack which follows a wave of campaigns targeting VoIP providers over the past weeks, leading to nationwide voice outages in the US.

- Texan luxury retailer Neiman Marcus has notified 4.6 million customers of a data breach resulting in contact details, payment & gift card numbers and credentials being stolen.

VULNERABILITIES AND PATCHES

- Google urges to upgrade to newly released Chrome 94.0.4606.71 for Windows, Mac, and Linux, patching two critical zero-day vulnerabilities tracked as CVE-2021-37975 and CVE-2021-37976.
- QNAP the Taiwanese network-attached storage (NAS) company has released patches for several vulnerabilities that could let threat actors inject and execute malicious code and commands remotely on vulnerable NAS devices.

THREAT INTELLIGENCE REPORTS

- Security experts alerted on a new malware "FoggyWeb" used by the Nobelium hacking group to deploy more payloads and steal sensitive info from Active Directory Federation Services (ADFS) servers.

  Check Point Anti-Virus provides protection against this threat (Backdoor.Win32.FoggyWeb)

- The Flubot banking Trojan is using a new technique to trick Android users and compromise their devices, trying to lure them into infecting themselves with a fake security update message, warning them of Flubot infection. However, the real infection is triggered once the victim clicks on the "install security update" button.

  Check Point Harmony Mobile provides protection against this threat

- Security researchers have found that the RansomExx gang corrupts Linux files during the encryption process, which may cause serious damages to the victims' files.

  Check Point Harmony Endpoint provides protection against this threat

- Developed by the Anglo-German spy firm Gamma International, the FinFisher malware can now infect Windows devices using a UEFI bootkit method that it injects in the Windows Boot Manager.

  Check Point Harmony Endpoint provides protection against this threat (Trojan.Win32.FinFisher)

- The Hydra banking Trojan has been targeting customers of Commerzbank, Germany's second-largest financial institution using a malicious APK called "Commerzbank Security" which can monitor and intercept all traffic from the victim's device.

  Check Point Harmony Mobile provides protection against this threat

- Threat actors are leveraging the new malware BloodyStealer sold on dark web forums to steal credentials for multiple gaming platforms accounts such as EA Origin, Steam or Epic Games Store.

  Check Point Anti-Virus provides protection against this threat

- US President Joe Biden announced he will bring together 30 countries to fast-track cooperation in fighting cybercrime, especially ransomware networks.