November 30 - December 6, 2020

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point has published a warning against cyber attackers leveraging the online shopping spree around Thanksgiving to distribute shipping and package tracking-related phishing email campaigns. Some 440% increase in campaigns impersonating online shopping services was observed throughout November.
- Cyber Attackers have been searching for ways to monetize the production and purchase of COVID-19 vaccines. A widespread phishing campaign targets organizations associated with The Vaccine Alliance's Cold Chain Program; Pfizer vaccine doses have been offered for sale on the dark web; Interpol warns against criminals attempting to steal and falsify vaccines.
- A government database belonging to the Brazilian Ministry of Health has been exposed to the public, due to a misconfiguration. The private information of over 243 million Brazilians, including full name, home address and medical information, has been leaked as a result.
- US retail giant Kmart has suffered an attack by the Egregor ransomware, influencing back-end services but leaving its online stores unaffected. The ransomware gang has also hit TransLink, the manager of Metro Vancouver's transportation network. Phone lines, online services and payment systems were disrupted.

  Check Point SandBlast Agent provides protection against this threat *(Ransomware.Win32.Egregor)*
- AstraZeneca, a British-Swedish multinational pharmaceutical company and one of the most prominent COVID-19 vaccine developers, may have been breached by North Korean actors. The hackers impersonated recruiters, sending malicious files disguised as lucrative job offers. Among the victims are COVID-19 researchers.
- Israeli insurance company Shirbit has been breached and hackers are threatening to leak customer insurance and private information unless their demands for over 1 million USD are met.

VULNERABILITIES AND PATCHES

- Check Point Research has analyzed the impact of a recently exposed vulnerability in Google Play Core Library, an app's runtime management interface, used to manage language resources, feature modules and more. Assigned CVE-2020-8913, the flaw allows Local-Code-Execution within applications that have the vulnerable version of Play Core. Although Google has patched the library and a new version is available, several popular applications are still using the old and vulnerable one.

  Check Point SandBlast Mobile provides protection against this threat

- VMWare has released a fix addressing a zero-day vulnerability in VMware Workspace One Access, Access Connector and more. The bug, assigned CVE-2020-4006, was originally reported to the company by the NSA.
- Researchers have reviewed severe memory corruption vulnerabilities in Apple's AWDL protocol that could allow an attacker to gain control over a remote device without interaction, and spread between iPhone devices.

THREAT INTELLIGENCE REPORTS

- Researchers have released a review of the threat landscape of the education sector, which has been rapidly changing due to digitalization trends and the massive shift to remote studies. Student privacy is the biggest concern nowadays, as well as compromised learning and videoconferencing systems.
- The Trickbot botnet has recently integrated a module focusing on Unified Extensible Firmware Interface (UEFI) vulnerabilities into its toolset. UEFI-level bootkit could enhance the malware's persistency capabilities, most notably during recovery attempts from ransomware attacks.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Botnet.Win32.Trickbot; Trojan-Banker.Win32.TrickBot)

- Researchers have discovered a new backdoor and document stealer used by the Russia-affiliated Turla APT. The backdoor leverages legitimate services such as Dropbox to exfiltrate files and receive commands.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Trojan.Win32.Turla; Turla)

- BISMUTH, a nation-state espionage group linked to Vietnam, has been distributing crypto mining malware to distract their targets from their data exfiltration operations and create an additional monetization channel.

For comments, please contact: TI-bulletin@checkpoint.com