December 31, 2018 – January 6, 2019

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Highly-sensitive personal data of more than 100 German politicians, including German Chancellor Angela Merkel, has been leaked in a recent attack. While the identity of the attackers and the method used are still unknown, the leaked data appears to have been collected from their personal smartphones.
- The popular browser-based game 'Town of Salem' has suffered a major data breach, exposing account data of more than 7.6 million players. The breached database contained players' email addresses, hashed passwords, IP addresses and some payment information.
- The Ryuk ransomware has hit the cloud hosting provider "Dataresolution.net", after the attackers used a hacked login account. The Ryuk campaign was studied last August by Check Point's research team, who associated it with the notorious North Korean APT Lazarus Group.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Trojan-Ransom.Win32.Ryuk)*
- A new campaign targeting Chromecast adapters has been launched in order to promote the popular YouTube channel "PewDiePie". The hackers utilized the Universal Plug and Play (UPnP) feature in Chromecasts that allows routers to forward public Internet ports to internal adapters and used it to connect to the device and display YouTube content.
- A data leak has affected over 2.4 million users of Blur, the password manager application. The leak potentially exposed users' email addresses, password hashes, IP addresses and, in some cases, full names and password hints.
- The official website of Dublin's tram system, the Luas, has been hacked and defaced. The hackers demanded ransom payment and threatened to otherwise publish the company's data.
- Marriott International has declared that the number of guests whose data was disclosed in the 2018 breach is 383 million, rather than the previously reported 500 million. They further declared that breached data also included non-encrypted passport numbers of these guests.

VULNERABILITIES AND PATCHES

- Security researchers have discovered a vulnerability in Guardzilla home video surveillance that allows all users to access each other`s saved home videos. The flaw is due to hard-coded credentials existing in all GZ501W camera models, common to all users, and used for storing saved video data.
- A security researcher has found a Zero-day vulnerability in Windows OS that enables overwriting a target file with arbitrary data. While the exploit's effects may vary, the researcher's Proof-of-Concept script was only able to produce a denial-of-service condition.
- A vulnerability has been found in Skype for Android that may allow an unauthenticated local user to bypass the lock screen and view photos and contacts or have browser access when answering an incoming Skype call on a locked device.
- The software company Yokogawa Electric has revealed a critical flaw in several of its automation products. The flaw, tracked as CVE-2018-16196, could be exploited by an attacker to stop the communication function of Vnet/IP Open Communication Driver, triggering a Denial-of-Service condition.

THREAT INTELLIGENCE REPORTS

- Facebook is accused of tracking non-users via Android apps, according to a new report. The analyzed Android apps, including Kayak, Yelp and Shazam, share their user data with Facebook through the Facebook Software Development Kit for app developers.
- The unCaptcha automated system has been modified and is able again to bypass Google reCAPTCHA by submitting the audio challenge to a Speech to Text software and typing in the output.
- Security researchers have analyzed the distribution technique used in the recent Emotet campaign, which targeted various countries in Latin America last November.

  Check Point Anti-Bot blade provides protection against this threat (Trojan.Win32.Emotet)

- A new variant of NRSMiner cryptocurrency mining malware was seen in the wild, infecting users in the southern region of Asia. The new variant leverages on NSA's leaked Eternal Blue exploit and has the ability to download new modules and remove files from older versions of the malware.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Trojan-Cryptominer.Win32.NRSMiner)