November 4 – November 10, 2019

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- At least two Spanish companies have been hit with ransomware. Everis, a major IT services and consulting company has been infected by the BitPaymer ransomware, while Spain's largest radio station Cadena SER suffered from a ransomware of an unknown family.

  Check Point SandBlast Anti-Ransomware provides protection against this threat *(Ransomware.Wins.BitPayme)*

- The Japanese cybersecurity company TrendMicro has fallen victim to an internal data breach carried out by one of its employees. The employee sold data of 68,000 customers to phone scammers, who used it to carry out tech support scams, calling customers impersonating TrendMicro support employees.

- A Brooklyn hospital has suffered an attack by an undisclosed ransomware family that led the hospital to lose patient data such as names and cardiac and dental images.

- Facebook has suffered a data leak incident that affected users in Facebook groups, giving over 100 3rd party apps access to the members' private information such as their names, pictures and group activities. This breach follows Facebook's change to its Group API access parameters back in April 2018.

- It is now being disclosed that two former Twitter employees had accessed sensitive and non-public information of Twitter accounts associated with known Saudi critics. Highly personal information was accessed including email addresses, devices used, browser information, birthdates, full activity logs, IP addresses associated with the accounts and phone numbers.

- Predator the Thief, an infostealer allegedly developed by Russian speaking hackers, has recently been spotted as the payload in a new phishing campaign threatening its victims with fake subpoenas from the UK Ministry of Justice, urging them to click on the malicious link within 14 days. The malware looks for cryptocurrency wallets, network configurations, browser information, VPN and FTP credentials, email data and gaming logins.

  Check Point Anti-Virus blade provides protection against this threat *(Trojan-PSW.Win32.Predator.TC)*

VULNERABILITIES AND PATCHES

- Light Commands is a newly discovered attack vector for smart home devices that manipulates them to execute inaudible and invisible commands by shining a laser at them. The attack exploits a vulnerability in the embedded microphones and all major devices are vulnerable including Google Home, Alexa and Siri.
- Researchers have discovered multiple vulnerabilities (CVE-2019-13103, CVE-2019-13104, CVE-2019-13105, CVE-2019-13106) in the universal bootloader Das U-Boot that is used in embedded devices such as Amazon Kindles and ARM Chromebooks. Once exploited, they allow the attackers to gain full control of the device.
- Nvidia has released patches for 12 vulnerabilities in its products, four of them categorized with high severity. All of the vulnerabilities require physical access and might be exploited for privilege escalation and denial of service.
- A vulnerability in Amazon's smart video doorbell "Ring" that allowed an attacker with physical proximity to the device to gain access to the credentials of the owner's network has been reported.

THREAT INTELLIGENCE REPORTS

- Researchers have analyzed the activity of the DarkUniverse APT group that was secretly active between the years 2009 and 2017. According to their research, the group has targeted both civilian and military organizations from Asia, Europe and Africa and used highly targeted phishing documents to deliver the malware payload.
- Ryuk ransomware has been upgraded with the ability to wake computers in "sleeping" mode in order to encrypt them, as well as the option to send ARP requests across the infected network to discover new machines to encrypt.

  Check Point SandBlast Anti-Ransomware provides protection against this threat *(Ransomware.Win.Ryuk)*
- ZIP files with two "ZIP structures" have been spotted by researchers delivering Nanocore RAT via malicious emails. The threat actor is hiding the malicious payload in the second "ZIP structure", thus hiding it from Anti-Virus products that will only check the first one.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(RAT.Win32.Nanocore)*

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