October 15 – 21, 2018

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- New APT group has been spotted dubbed “GreyEnergy” and considered a successor to the infamous BlackEnergy APT group. GreyEnergy uses its own malware framework to conduct cyber espionage operations in Ukraine and Poland, focusing mainly on critical infrastructures. Some of the malware’s modules are backdoor, file extraction, taking screenshots, keylogging, password and credential stealing.

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

- Above 35 million records of US voters have been found available for sale on the Dark Web. The seller provided records belonging to voters in 19 states, and claimed to have persistent access to voters’ records. The stolen records include personal, identifiable, information and voting history of US residents.

- The Onslow Water and Sewer Authority (ONWASA) has been targeted in a ransomware attack, significantly disrupting its ability to provide services in the week after a hurricane hit the east coast of the U.S. The unknown threat actors have used Emotet Trojan to launch the Ryuk ransomware.

  Check Point SandBlast, Anti-Bot and Anti-Virus blades provide protection against this threat (Trojan.Win32.Emotet; Trojan-Ransom.Win32.Ryuk)

- A threat actor has managed to hack to Argenta vending machines’ mobile application that allows user to connect to the machines and preform the payment. The threat actor has got access to the app’s DB containing the ‘UserWallets’ table and changed the values so his credit card will contain EUR 999.

- The authors of the infamous GandCrab Ransomware have released the decryption keys for all Syrian victims in an underground cybercrime forum. The release came as a response to a Tweet in which a Syrian victim asked for help after photos of his deceased children were encrypted.

  Check Point SandBlast, Anti-Bot and Anti-Virus blades provide protection against this threat (suspicious executable containing ransomware; Trojan-Ransom.Win32.GandCrab)

VULNERABILITIES AND PATCHES

- A security researcher has discovered a new passcode bypass that could be exploited on all current iPhone models, including the recently released iOS 12.0.1 version. The bypass may allow attackers with physical access to access photos and contacts on a locked iPhone.
- A critical code execution vulnerability has been discovered in the 'LIVE555' Streaming Media library used by popular media players including VLC and MPlayer, exposing millions of users to cyber-attacks.
- A zero-day vulnerability has been spotted, affecting thousands of applications which use older versions of the jQuery File Upload plugin. The vulnerability may allow attackers to upload arbitrary files on web servers, including command shells for sending out commands.
- A four-year-old severe vulnerability has been discovered in the Secure Shell (SSH) implementation library known as LibSSH. The vulnerability may allow anyone to bypass authentication and gain administrative control over a vulnerable server without requiring a password.
- Tumblr has released a security patch, addressing a flaw in its "Recommended Blogs" feature on the desktop version that could allow attackers to steal login credentials and sensitive user account information including email addresses, hashed passwords, IP addresses, and more.
- Three critical vulnerabilities have been discovered affecting 8 models of D-Link routers. Combining them together could allow attackers to get full control over the infected machines.

  Check Point IPS blade provides protection against this threat *(Linux System Files Information Disclosure)*

THREAT INTELLIGENCE REPORTS

- Check Point security researches have spotted a new version of Azorult Downloader and infostealer, distributed through the RIG exploit kit, among other methods. This version has renewed the encryption method of the embedded C&C domain string, and improved the cryptocurrency wallet stealer.

  Check Point Sandblast protects against this threat
- Between 2017 and 2018 Cryptocurrency exchanges have suffered a total loss of $882 million due to targeted attacks, five of which have been attributed to the North Korean Lazarus state-sponsored group.
- Security researches have published a deep analysis reviewing the tools and operations conducted by the Russia-linked cyberespionage group 'DustSquad', which focuses on Central Asian targets and diplomatic entities. The research has revealed a new sample of the malware targeting Windows systems, and disguised as a Russian version of Telegram.

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