Check Point
SOFTWARE TECHNOLOGIES LTD.

May 21- 27, 2018

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Coca-Cola has suffered a data breach, as a former employee was found in possession of an external hard-drive containing personal data of about 8,000 workers. The company was notified of the breach by law enforcement officials last September.
- Aultman Hospital in the US has been breached and private and medical data of over 40,000 patients was stolen. The attack was conducted by sending phishing emails to several of the hospital's employees.
- A campaign distributing the CryptON Ransomware has been leveraging computers with internet accessible Remote Desktop Services. Upon gaining remote access to the victim machine, the attackers execute the ransomware manually.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Trojan-Ransom.Win32.CryptON)*

- The "Roaming Mantis" Android Banking Trojan has been spotted in the wild with more sophisticated evasion techniques, and expanded capabilities and targets. It is now capable of web crypto-mining and phishing for iOS devices. The Trojan has also broadened its geographical distribution as its malicious APK now supports 27 languages rather than 4.

  Check Point Sandblast Mobile customers are protected from this threat

- More than 500,000 routers and storage devices across over 50 countries have been infected by VPNFilter, a highly sophisticated IoT botnet designed to gather intelligence, mass with internet communications and carry out destructive attack operations. Shortly after the exposure of the malware, the FBI has gained control over a key domain in the malware infrastructure.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Netgear DGN2200B Cross-Site Scripting; QNAP QTS Remote Command Injection(CVE 2013 0143); NETGEAR WNR2000 Authentication Bypass(CVE 2016 10176); Netgear WNDR4700 Router Authentication Bypass(CVE 2013 3071); VPNFilter Client Malicious Self-Signed Certificate; Netgear DGN Unauthenticated Command Execution); NETGEAR DGN2200 Remote Code Execution (CVE-2017-5521); Trojan.UNIX.VPNFilter.*)*

VULNERABILITIES AND PATCHES

- Four vulnerabilities in D-Link DIR-620 firmware, which runs on various D-Link routers, have been exposed. The firmware is highly popular in Russia, as one of Russia's most prominent Internet Service providers includes it in its standard package. The vulnerable version of the firmware has hardcoded default credentials, which can be exploited to gain access to the firmware and obtain personal data.

  Check Point IPS blade provides protection against this threat *(Web Servers Malicious URL Directory Traversal)*

- Researchers have found 14 vulnerabilities in the on-board computers of BMW cars, in a year-long security audit. The flaws affect high-profile BMW models such as BMW X and BMW series 7 since at least 2012, and some of the vulnerabilities can be leveraged to compromise a vehicle remotely.

- Both Microsoft and Google researchers have discovered a fourth variant of the Meltdown and Spectre security flaws, a set of hardware vulnerabilities found in modern processors and used to steal data currently processed on the machine. The flaw was assigned CVE 2018-3639.

  Check Point IPS and Anti-Bot blades provide protection against this threat *(Meltdown/Spectre Multiple Browsers Speculative Execution; Trojan-Ransom.Win32.Spectre.A)*

THREAT INTELLIGENCE REPORTS

- Security researches have published a report describing potential risks in smart devices for pet tracking. The research reveals several ways in which attackers could exfiltrate sensitive data from the trackers, including the pet's location and the owner's phone number, email address and home network details.

- BackSwap, a newly-revealed banking Trojan, uses new techniques to carry out its operation; to detect banking activity, the malware taps the 'message loop' Windows mechanism, a section of code found in all Windows GUI apps, and searches URL-like patterns related to the bank's name.

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

- Due to a flaw in the Z-Wave protocol, a wireless communication technology used mainly by home devices such as security systems and lighting controls, over 100,000 IoT devices from a variety of vendors are vulnerable to an attack that may allow unauthorized access to the devices.

- TheMoon botnet, which began its way in 2014 infecting Linux servers and in 2017 switched to IoT devices, has integrated a new zero-day exploit for the Dasan GPON router into its code.

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

- FontCode is a new technique of steganography that can be used to embed hidden content within individual font characters.