July 16 – July 22, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Singapore's largest healthcare group, 'SingHealth' has suffered a major data breach affecting 1.5 million patients, including the country's prime minister. The stolen data includes patient's name, address, National Registration Identity Card numbers, and for several victims also details on dispensed medicines.
- Sensitive documents of over 100 manufacturing companies including Fiat, Toyota, Tesla and ThyssenKrupp were left exposed on an unsecured server owned by Level One Robotics, an industrial automation service provider. Over 150 gigabytes of data were made public by the breach, including factory floor plans and robotic configurations.
- 'MoneyTaker' hacking group has stolen about $1 million from the Russian PIR bank. The group has gained access to the bank by compromising outdated router, and then used the Bank's Automated Work Station Client to generate payment orders and transfer the money to 17 accounts created in advance.
- 'RoboCent', a political robocalling company, has exposed personal details and political affiliation of hundreds of thousands of US voters, leaving an AWS bucket online without authentication.
- 18,000 Huawei routers have been compromised in one day by a single botnet operator dubbed 'Anarchy', who is believed to be the threat actor behind several Mirai variants. Later on this week, also Dasan and D-Link routers running GPON firmware were targeted in an attempt to create a botnet.

  Check point IPS and Anti-Bot blades provide protection against this threat *(Huawei HG532 Router Remote Code Execution (CVE-2017-17215); Trojan-Backdoor.Linux.Mirai; Dasan GPON Router Remote Command Injection (CVE-2018-10562); Dasan GPON Router Authentication Bypass (CVE-2018-10561))*

- Security researches have uncovered an ongoing cyber espionage campaign targeting Ukrainian government institutions via spear phishing. The campaign involved three different remote access Trojans (RATs) that share infrastructure and connect to the same C&C servers.

  Check point IPS, Anti-Virus and Anti-Bot blades provide protection against this threat *(Microsoft Outlook Remote Code Execution (CVE-2017-0199); Trojan.Win32.Vermin; Trojan.Win32.sobaken; Trojan.Win32.Quasar)*

VULNERABILITIES AND PATCHES

- Security researchers have discovered two vulnerabilities affecting Dongguan Diqee 360 smart vacuum cleaners as well as other Dongguan devices, including DVRs, surveillance cameras, and smart doorbells. The vulnerabilities may allow attackers to run malicious code on a device with admin privileges, perform video surveillance and steal private data from infected machines.
- Cisco has patched four critical security authentication vulnerabilities in its Policy Suite for mobile carriers. The vulnerabilities may allow remote attackers to exfiltrate information, compromise wireless subscriber account information, modify any data contained in the Policy Builder database and more.
- About 500 million Internet-of-Things (IoT) devices have been found vulnerable to an old-time attack called DNS Rebinding. As part of this attack, the victim's browser or device is tricked into binding to a compromised DNS server and is then redirected to a malicious resource. Flaws which may allow similar attacks have also been observed in Google Home devices, Roku TV and more.

THREAT INTELLIGENCE REPORTS

- Researches have released a proof-of-concept for a new GPS spoofing attack, manipulating road navigation systems. The new technique, dubbed 'GangWang', allows attackers to lure victims into driving to incorrect locations, by crafting the GPS inputs to the target device in a way that navigation instruction and displayed routes on the map remain consistent with the physical road network.
- Security researchers have discovered a precursor of the infamous Proton macOS RAT dubbed "Calisto" still under development. Calisto allows remote attackers to gain full control over an infected machine, enables remote login and screen sharing, gains persistence, and adds a secret root account to a victim's workstation.

  Check point Anti-Virus blade provides protection against this threat *(Trojan-Backdoor.OSX.Calisto)*
- A malware that uses Exchangeable Image File Format (EXIF) data to hide its code has migrated to a new platform: GoogleUserContent sites. In this technique, threat actors embed malicious code within uploaded images, capable of uploading a predefined web shell or arbitrary files, placing defacement pages, establishing backdoors and more.

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