July 9 – July 15, 2018

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Security researchers have revealed the Chinese APT "TEMP.Periscope" is involved in a vast espionage operation targeting Cambodia's electoral system, in light of the forthcoming elections due July 2018. This includes compromises of Cambodian government entities charged with overseeing the elections, including the National Election Commission, Ministry of the Interior, Ministry of Foreign Affairs and International Cooperation, Cambodian Senate and the Ministry of Economics and Finance, as well as the targeting of opposition figures.

- Security researchers have exposed a highly-targeted mobile malware campaign that has been operating since August 2015 and found spying on 13 selected iPhones in India. For the attack, the attackers abused mobile device management (MDM) protocol - a type of security software used by large enterprises to control and enforce policies on devices used by their employees - to deploy and control malicious applications remotely.

- Security researchers claim the attack that hit Ticketmaster several weeks ago has been only one part of a massive credit card hacking campaign, conducted by the hacking group Magecart and affecting more than 800 e-commerce sites. The campaign comprised of the injection of malicious card-swiping code into third-party components of websites, including PushAssist, CMS Clarity Connect and Annex Cloud.

- The Security Service of Ukraine (SBU) has revealed that the VPNFilter malware was detected on the systems of the Aulska chlorine station in Ukraine, considered part of the country's critical infrastructure as it supplies chlorine to water treatment and sewage plants. The announcement attributed the attack to the Russian Intelligence, and claimed it has been blocked.

  Check point IPS and Anti-Bot blades provide protection against this threat (ASUSWRT AC53 Session Stealing Remote Command Execution (CVE-2017-6549); ASUSWRT LAN Backdoor Remote Command Execution; MiniUPnP MiniUPnPd ProcessSSDPRequest Denial of Service; MiniUPnPd 1.0 Stack Buffer Overflow Remote Code Execution; NETGEAR Routers Authentication Bypass; Portable SDK for UPnP Devices libupnp Device Service Name Stack Buffer Overflow; Portable SDK for UPnP Devices libupnp UUID Service Name Stack Buffer Overflow; Netgear WNR1000 Router Authentication Bypass; Trojan.Linux.VPNFilter)

- Israeli cryptocurrency company Bancor has announced it suffered a security breach, in which an unknown hacker had stolen roughly $13.5 million worth of cryptocurrency from two company wallets, and attempted to withdraw $10 Million more from another one, but a security feature embedded in the specific tokens had made it impossible for the hackers to move the funds to other wallets.

VULNERABILITIES AND PATCHES

- Cisco has patched a critical bug in their VoIp phones, allowing a potential command-injection and remote code execution on IP phones, as well as three other medium-severity vulnerabilities.
- Adobe has released security updates for Adobe Flash Player, addressing critical vulnerabilities in versions 30.0.0.113 and earlier. Successful exploitation could lead to arbitrary code execution. Over a Hundred flaws in other products were also patched in the recent update.
- Microsoft has released patches for 53 bugs, most of them in Internet Explorer.
- Researchers have discovered two new sub-variants of the Spectre processor vulnerability, dubbed Spectre 1.1 and 1.2. The first could allow an attacker to write and execute malicious code that may potentially be exploited to extract data from previously-secured CPU memory, including passwords and cryptographic keys. Variant 1.2 could allow to bypass the Read/Write PTE flags, enabling hackers to overwrite read-only data memory, code metadata, and code pointers to avoid sandboxes.

  Check point IPS blade provides protection against this threat (Meltdown/Spectre Multiple Browsers Speculative Execution (CVE-2017-5715; CVE-2017-5753; CVE-2017-5754; CVE-2018-3639))

THREAT INTELLIGENCE REPORTS

- Check Point has released its mid-year “Cyber Attack Trends” report. Ransomware no longer takes center-stage in the malware arena, overtaken by cryptomining malware across multiple platforms. Further, Cloud infrastructure has become one of the most attractive targets for threat actors. The analysis also reflects a return in the use of the rather old DrokBot Torjan, now in an attempt to steal a user’s credentials using web-injects that are activated as a user tries to login to their banking website.
- Security researchers have warned that the APT group dubbed “BlackTech” is using code-signing certificates stolen from Taiwanese-based tech firm D-Link and the security company “Changing Information Technology Inc.” to sign the code of the “Plead” malware. The new campaign, like other campaigns involving this malware, has been targeting victims in East Asia region, particularly Taiwan.
- A new version of the GrandCrab ransomware, numbered 4.1, has been spotted in the wild, mere days after the discovery of version 4, reflecting the fast evolution of the malware.

  Check point SandBlast provides protection against this threat