February 26 - March 4, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The German government has announced that it experienced a massive cyber-attack, where several of its networks, including an isolated one, were breached and infected with malware for about a year. The breach was only discovered in December, and included the servers of the Interior Ministry and other unspecified ones. German authorities suspect the Russian hacking group APT28 is behind the attack.

- Security researchers have revealed that the developer repository site GitHub was hit with a critical DDoS attack that took the site offline. It peaked at 1.35 Tera Bytes per second, making it the one of the world's largest DDoS attacks. Researchers suspect this attack exploited a recently discovered vulnerability in the Memcached protocol, usually used to speed up websites, to amplify the impact of DDoS attacks.

- Security researchers have identified a new campaign against humanitarian aid efforts to North Korea, targeting entities in South Korea, Vietnam, Singapore, Japan, Indonesia, Canada and Argentina. The campaign, spread by email, entices the user to download a malicious file which looks like a document but is in fact an executable file. Researchers suspect that in spite of the simplicity of the malware, the perpetrators are a nation-state level group.

  Check Point IPS blade provides protection against this threat *(Suspicious Executable Mail Attachment)*

- Security researchers have found that 42 models of low-cost smartphones are sold pre-infected with Triada banking Trojan. These models are popular in countries such as Russia, Poland, Indonesia, China, the Czech Republic, Mexico, Kazakhstan, and Serbia.

  Check Point Anti-Bot blade provides protection against this threat *(Trojan.AndroidOS.Triada.A)*

- Credit company Equifax has added 2.4 million Americans to the list of those who have had their personal data stolen as part of the company's massive 2017 data breach, bringing the total count of victims to around 148 million citizens. Social ID numbers weren't exposed for this newly found batch.

  Check Point IPS blade provides protection against this threat *(Apache Struts2 Content-Type Remote Code Execution (CVE-2017-5638))*

VULNERABILITIES AND PATCHES

- In addition to patching Windows systems against the Spectre and Meltdown exploits, Microsoft has also partnered with Intel to include firmware updates against such attacks in Windows Update, currently on a limited scale.

  Check Point SandBlast, IPS and Anti-Bot blades provide protection against this threat *(Meltdown/Spectre Multiple Browsers Speculative Execution (CVE-2017-5715; CVE-2017-5753; CVE-2017-5754; Trojan-Ransom.Win32.Spectre.A)*

- Further details were revealed on a recently patched Adobe vulnerability, which allows attackers to hide malicious JavaScript code in a PDF file. Adobe Acrobat Reader versions 2018.009.20050, 2017.011.30070 and earlier are affected.

  Check Point IPS blade provides protection against this threat *(Adobe Acrobat and Reader Out-of-bounds write (APSB18-02: CVE-2018-4901)*

THREAT INTELLIGENCE REPORTS

- A business clash between certificate issuing company DigiCert and its former UK-based reseller Trustico has led to the nullification of tens of thousands SSL certificates. In the process of terminating contractual obligations between the two companies, it came about that Trustico kept the details of at least 23,000 private SSL keys, in what is in fact a security breach as these keys should be known only to the site owners. Moreover, it emailed those keys to DigiCert, thus compromising their security and forcing DigiCert to revoke them on March 1st.

- Security researchers have identified a new large scale malspam campaign, targeting mostly the United States and Europe, leveraging a recently patched critical vulnerability in Adobe Flash Player, in an attempt to target yet unpatched systems. The email contains a link to a website, from which a Word document is downloaded. When the victim opens the document and enables macros, the vulnerability will be exploited, enabling the malware to run.

  Check Point IPS blade provides protection against this threat *(Adobe Flash Player Use After Free (APSB18-03: CVE-2018-4878)*

- Security researchers have concluded that the popular exploit kit “Rig”, customarily used to spread ransomware, had recently refocused, and is now mainly spreading cryptocurrency miners and information-stealing Trojans. This comes, as per the researchers, amidst a general drop in Exploit kits usage, with several major players gone, and Rig’s popularity fading.

  Check Point IPS blade provides protection against this threat *(RIG Exploit Kit Website Redirection; RIG Exploit Kit Rotator; RIG Exploit Kit Landing Page URL; Malicious Crypto Miner Downloader)*