March 11 – 17, 2019

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point researchers have discovered a new mobile adware campaign dubbed "SimBad" on Google Play Store. SimBad is capable of showing ads, generating phishing attacks and even installing remote applications. It has been found embedded in 206 applications with a combined download count of almost 150 million.
- Check Point researchers have exposed a massive campaign stealing data from more than 111 million users of 12 different Android mobile applications, using them to upload contact lists to Hangzhou Shun Wang Technologies controlled servers. The data stealing logic of the campaign, dubbed "Operation Sheep", hides inside the Software Development Kit (SDK) used by app developers, apparently unaware of its malicious nature.
- 39 percent of all Counter-Strike 1.6 servers, a popular multiplayer war game, have been found infected with the Belonard Trojan and used to compromise gamers' computers using various unpatched Remote Code Execution (RCE) vulnerabilities.
- The mobile phone of former Israeli military chief and leading candidate in the forthcoming elections, Benny Gantz, has been hacked by Iranian intelligence. Israeli officials had warned of foreign power interference and that cyber-attacks could influence the outcome of the upcoming election.
- "GMO", a Java Script Sniffer (JS Sniffer) code had been injected to seven online stores in the UK and US and used to steal payment information since May 2018. This card-skimming campaign has been exposing more than 500,000 exclusive users per month.
- Following a month long DDoS attack on the Philippine AlterMidya news website and other online media agencies, protesters have demonstrated in front of the Philippines National CERT, claiming the government is related to the cyber-attacks on local independent media organizations.

VULNERABILITIES AND PATCHES

- A new WordPress vulnerability allows unauthenticated remote attackers to perform remote code execution on WordPress websites.
- Adobe has released its monthly security update addressing two critical arbitrary code execution vulnerabilities—one in Adobe Photoshop CC and another in Adobe Digital Editions. Both critical vulnerabilities could allow an attacker to take control of an affected system.
- Microsoft has released its March 2019 software update addressing a total of 64 CVE-listed security vulnerabilities in its Windows operating systems and other products, 17 of which are rated critical, and two zero-day vulnerabilities which are actively being exploited in the wild.
- Security experts have discovered multiple vulnerabilities in the Moxa EDS and IKS industrial switches that could result in remote code execution, DoS and more. The vendor addressed some of the flaws in a security release.

THREAT INTELLIGENCE REPORTS

- DMSniff, a Point-of-Sale (POS) malware which uses a domain generation algorithm to create C&C domains on the fly to steal credit card data, has been deployed in attacks against small and medium-sized businesses during the past four years.

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

- A report to the United Nations (UN) Security Council states that North Korean backed hacking groups were behind multiple cyberattacks impacting financial institutions and cryptocurrency exchanges in Asia between January 2017 and September 2018, resulting in a total loss of $571 million.
- Powload info-stealer has been using steganography in PNG files to avoid detection. The infection chain consists of malicious emails with attached documents, which include a macro that runs a PowerShell script that downloads the PNG files and extracts their malicious content, which finally drops and executes the malware. The current campaign is targeting victims in Japan and Korea.

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