Check Point
SOFTWARE TECHNOLOGIES LTD.

May 14 – May 20, 2018

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A campaign, possibly related to the Pakistani military, has been targeting high-ranking officials, mostly in Pakistan, Afghanistan, India, Iraq, and the United Arab Emirates. American, British, Australian, NATO and Iranian officials were impacted indirectly due to contact with targeted officials. The campaign, dubbed "Stealth Mango", spreads its malware using phishing links to a fake third-party Android app store, and possibly also by direct access to devices. Once installed, it gathers all data from the device.

  Check Point Sandblast Mobile customers are protected from this threat

- Security researchers have identified malware directed at the less-secured desktop version of the encrypted-messaging software Telegram. The malware, possibly created by a Russian speaker, could potentially give the attacker access to the victim's session, contacts, and previous chats.

- Rail Europe North America, a seller of European train tickets, has announced that its website had suffered a security breach, exposing clients' credit card data. The attack was exposed in February 2018, after having lasted 3 months. The attackers have injected the front-end of Rail Europe's website with a 'skimming' malware, meaning customers gave payment information directly to the hackers.

- DrayTek, a Taiwan-based manufacturer of broadband Customer Premises Equipment such as routers, switches, firewalls, and VPN devices, has announced that hackers are currently exploiting a zero-day vulnerability in some of their routers in order to change DNS settings, redirecting them to an unknown server located at 38.134.121.95. There are currently about 800,000 DrayTek routers connected to the internet, though the exploit may not be relevant to all of them.

- Security researchers have warned that the Satori botnet is being used for mass-scanning of the Internet for exposed Ethereum mining rigs. The scan attempts to locate devices with port 3333 exposed online, a port often used for remote management features by cryptocurrency-mining equipment.

  Check Point Anti-Bot blade provides protection against this threat *(Trojan.Linux.Satori.*)*

VULNERABILITIES AND PATCHES

- Security researchers had exposed a vulnerability, dubbed ZipperDown, impacting about 10% of all iOS apps, including Weibo, MOMO, NetEase Music, QQ Music, and Kwai. The vulnerability is based on a common programming error, which could possibly enable code execution in the affected apps.
- Security researchers have discovered zero day vulnerabilities in Adobe and Microsoft products, which they called "a masterpiece of offensive hacking", after the developing hackers uploaded a sample of the weaponized PDF file to a public malware scanning engine.

  Check Point IPS blade provides protection against this threat (Microsoft Win32k Elevation of Privilege (CVE-2018-8120); Adobe Acrobat and Reader Double Free (APSB18-09: CVE-2018-4990))
- Security researchers have discovered a critical remote command injection vulnerability in the DHCP client implementation of Red Hat Linux. The company has since released a relevant patch.

  Check Point IPS blade will provide protection against this threat in its next online package
- Cisco has released three critical patches to newly discovered vulnerabilities. The products patched include Digital Network Architecture Center, Enterprise NFV Infrastructure Software, IoT Field Network Director, and others.
- Samsung has released six patches to vulnerabilities found in its Qualcomm and Snapdragon processors used in Samsung handhelds, as well as in Snapdragon Wear and Automotive platforms.
- Microsoft has released three additional Windows update packages, one of which, KB4100347, contains additional CPU microcode updates for Intel processors, as part of the Spectre v2 mitigation effort.

  Check Point IPS blade provides protection against this threat (Meltdown/Spectre Multiple Browsers Speculative Execution)

THREAT INTELLIGENCE REPORTS

- Security researchers have revealed a proof-of-concept DDoS attack exploiting UPnP protocol to bypass mitigations and carry out DDoS amplification assaults. An attacker could theoretically locate open UPnP routers using Shodan scanner, access the device XML file and modify the port forwarding rules thus launching a port-obfuscated DNS amplification DDoS assault.
- Security researchers have reported on a new crypto-mining malware, dubbed WinstarNssmMiner, used in half a million attacks in 3 days. This malware is unique, as it crashes the host system upon detection by an anti-virus, presenting a new level of aggressiveness to crypto-mining malware.
- Security researchers have modified Spectre v1 to bypass a victim's SMRR protection mechanism and access data stored inside the System Management RAM (SMRAM), allowing an unprivileged attacker to read the contents of memory, including memory that should be protected by the range registers.