June 11 – 17, 2018

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Dixons Carphone, a UK-based electronics and telecom retailer has fallen victim to a major data breach. Threat actors gained access to 5.9 million payment cards details, and 1.2 million personal data records including names, addresses or email addresses.
- Threat actors have stolen about $40M worth of tokens stored in the servers of the South Korean cryptocurrency exchange Coinrail. The tokens were issued during to the initial coin offerings (ICOs) of Pundi X (NPXS), NPER (NPER), and Aston (ATX).
- Over 300,000 machines have been infected with a clipboard hijacker dubbed "ClipboardWalletHijacker". The malware hijacks Ethereum and Bitcoin transactions by replacing strings resembling wallet addresses with ones belonging to the malware's operator, thus modifying the destination of the transfer.
- An espionage campaign has targeted a national data center of an unnamed central Asian country, gaining access to a wide range of government resources in order to conduct watering hole attacks. The attack is attributed to the Chinese-speaking group dubbed "LuckyMouse", which used a Remote Access Trojan (RAT) called "HyperBro".

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

- The official Windows client used for mining Syscoin cryptocurrency and managing Syscoin funds has been compromised. An attacker gained access to its GitHub account and replaced the Windows client with a version containing the "Arkei Stealer" malware, which steals passwords and wallet private keys.
- Banco de Chile, Chile's largest financial institution, has been attacked with a wiper malware and $10M were stolen from it. The wiper, dubbed "MBR Killer", was used by the attackers to destroy over 9,000 computers and over 500 servers, as a distraction to the real target of the attack - the bank's SWIFT money transferring system.

  Check point Anti-Bot and Anti-Virus blades provide protection against this threat *(Trojan.Win32. Mbrkiller.TC.a)*

VULNERABILITIES AND PATCHES

- Microsoft has released its Patch Tuesday for June. The patch addresses 50 vulnerabilities, 11 of which are critical remote execution vulnerabilities. The patch addresses the following Microsoft products: Windows OS, Internet Explorer, Microsoft Edge, ChakraCore JavaScript engine, Microsoft Office and Microsoft Office Services and Web Apps.

  Check point IPS blade provides protection against this threat (Microsoft Internet Explorer Scripting Engine Memory Corruption (CVE-2018-8267); Microsoft Windows DNSAPI Remote Code Execution (CVE-2018-8225))

- A new security flaw dubbed "Lazy FP" has been discovered in Intel chips, affecting all devices running Intel Core-based microprocessors regardless of the installed operating systems. The flaw leverages a system performance optimization feature called "Lazy FP state restore", used for switching between processes, and could potentially be exploited to access sensitive information including encryption related data.

- VMware has addressed a critical vulnerability in AirWatch Agent, used for managing the AirWatch from mobile devices. The vulnerability affects the Android and Windows Mobile versions and may allow a remote attacker an unauthorized creation and execution of files from the infected machine.

- A critical flaw has been discovered in email encryption client which use OpenPGP standard, affecting GnuPG, Enigmail, GPGTools, and python-gnupg. The flaw, dubbed "SigSpoof", may allow remote attackers to create fake status messages or fake verification status of a signed email.

THREAT INTELLIGENCE REPORTS

- Security researchers have discovered a new Android banking Trojan under development dubbed "MysteryBot", which also contains features of keylogger and ransomware. MysteryBot appears to be related to the infamous LokiBot Android banking Trojan as it uses the same C&C server.

  Check point SandBlast Mobile customers are protected from this threat

- Security researches have revealed that thousands of Android devices are vulnerable to potential attacks, leaving insecure remote Android Debug Bridge (ADB) enabled. The research exposes that threat actors are using this misconfiguration to install a Monero crypto-miner on a wide selection of Android-based devices, including smartphones, DVRs, Android and smart TVs.

  Check point SandBlast Mobile customers are protected from this threat

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