May 7- 13, 2018

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Bycyklen, Copenhagen's city bikes network, has been breached and the organization's entire database was deleted, disabling the public's access to bicycles. The company announced that no user's data had been stolen, and had to manually reboot each bike in order to fix the issue.

- TreasureHunter Point-of-Sales malware source code has been leaked, together with its UI-builder and administrator panel. The leaked source code, spotted on top-tier Russian-speaking forum, may allow threat actors to create their own PoS malware, probably increasing the number of PoS threats and attacks.

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

- A new technique is being used by attackers to bypass the 'Safe Links' feature on Microsoft Office 365, designed to protect users from malware and phishing scams. The technique, dubbed "baseStriker attack", uses a <base> tag to split the malicious link in a way that 'Safe Links' fails to identify it.

- New Crypto-mining campaigns have targeted over 300 websites running on the Drupal content management system, leveraging the last critical remote-code execution vulnerabilities discovered on Drupal. Among the affected websites there are government and university portals, including a US federal agency, the Turkish Revenue Administration, and Chinese hardware maker 'Lenovo'.

  Check Point IPS blade provides protection against this threat *(Drupal Core Remote Code Execution (CVE-2018-7600, (CVE-2018-7602))*

- Panda Banking Trojan has been observed on 4 recent campaigns targeting online cryptocurrency exchanges, social media sites, and adult sites. The simultaneous campaigns target several regions and industries around the world, and part of its C&C is related to a known threat actor network in Russia.

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

VULNERABILITIES AND PATCHES

- Check Point researchers have discovered two severe vulnerabilities that reside in the default keyboard on all mainstream LG smartphone models. Both vulnerabilities could be used to remotely execute code with elevated privileges by manipulating the keyboard updating process.

  Check Point Sandblast Mobile customers are protected from this threat

- A severe flaw has been discovered in the end-to-end encrypted messaging app, Signal, for Windows and Linux Desktop version. The flaw may allow a remote attacker to execute malicious code on the victim's system, by sending a message over the app containing the JavaScript payload. Earlier in this week, security researchers have revealed that Signal's "self-destructing" messages can be recovered by the macOS client, potentially exposing sensitive messages.

- Microsoft has released its patch Tuesday for May, addressing 67 vulnerabilities, including an Internet Explorer zero-day flaw that can be exploited for remote code execution. The vulnerabilities affect Microsoft Windows, Explorer, Edge, Outlook, Office, .NET Framework, and others.

  Check Point IPS blade provides protection against this threat (Microsoft Windows VBScript Engine Remote Code Execution, Microsoft Win32k Elevation of Privilege, Microsoft Excel Remote Code Execution, Microsoft Edge Memory Corruption, Microsoft DirectX Graphics Kernel Elevation of Privilege)

THREAT INTELLIGENCE REPORTS

- Check Point Researchers have published an in-depth investigation into the dark side of the popular instant-messaging application, Telegram. The research revealed how telegram has become a comfortable environment for threat actors, who leverage the anonymity it provides to trade malware and hacking tools, to offer shady jobs, and a lot more.

- New variant of SynAck Ransomware has been spotted in the wild, employing the 'Process Doppelganging' technique to evade detection. Leveraging this technique allows SynAck Ransomware to run in memory disguised as a legitimate program, by using the Microsoft NTFS transactions.

  Check Point SandBlast Agent and Anti-Virus blades provide protection against this threat (Trojan.Win32.SynAck)

- Security researchers have uncovered a new strain of malware dubbed 'Vega Stealer', capable of stealing passwords and credit card data from Chrome and Firefox browsers. Vega stealer is a variant of 'August Stealer', and also has the ability to exfiltrate Word, Excel, PDF and text files from an infected machine.

- A new strain of the IoT botnet "Hide N' Seek" (HNS) has been discovered, and is persistent through device reboot. In order to achieve persistency, the malware uses Telnet to gain root privileges and copy itself to the /etc/init.d/ directory that allows it to start with the operating system after every reboot.