Check Point
SOFTWARE TECHNOLOGIES LTD.

May 28 – June 3, 2018

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Two of Canada's largest banks, the Bank of Montreal (BMO) and Simplii Financial, have suffered major data breaches, affecting about 90,000 Canadian bank customers. In both cases, the attackers have contacted the bank to blackmail it, requesting a $1 million ransom from each bank to avoid data disclosure.

- Honda Car India has left personal data of over 50,000 users exposed on two public unsecured Amazon S3 buckets. The exposed data belongs to the users of the remote car management app 'Honda Connect App', and includes names, phone numbers, emails, passwords, Car VIN, Car Connect IDs, and more.

- The cryptocurrency trading startup "Taylor" has been hacked and $1.35 million worth of Ether were stolen from the company's wallets. The threat actor behind the attack is suspected to be the same one involved in the CypheriumChain hack in March, due to the use of similar wallet address.

- The website of the event ticketing company "Ticketfly" has been compromised and defaced. The attacker has also gained access to the website's database containing customer information, including names, physical addresses, phone numbers and email addresses.

- Security researches have revealed that the infamous 'Cobalt group' is still active despite their leader's arrest. The recent campaign includes phishing emails disguised as Kaspersky threat alert that lead to the infection with the 'CobInt Trojan'. The campaign targets banks in Russia and other former Soviet states.

  Check point IPS blade provides protection against this threat *(Cobalt Strike Payload Remote Code Execution; Cobalt Strike Beacon Suspicious Communication; Cobalt Strike Scripted Web Delivery Remote Code Execution; Cobalt Strike Stager Remote Code Execution)*

- An anonymous group of hackers have defaced the screens at the Mashhad airport in Iran to protest against the government and military's activity in the Middle East. The attackers have also compromised the email account of the head of Mashad airport civil aviation to spread their achievements.

VULNERABILITIES AND PATCHES

- Several vulnerabilities have been discovered in EOS blockchain platform which allows developers to build applications over the blockchain infrastructure. One of the vulnerabilities may allow a remote attacker to control over the virtual currency transactions and to access financial and private data, including the user's key stored in the wallet, key user profiles, and more.
- GitHub, GitLab and Microsoft VSTS have issued security updates to address a critical vulnerability in Git repository hosting services. The vulnerability may allow attackers to create a malformed Git repository containing a specially-built Git submodule, and execute arbitrary code on victims' systems.
- A security flaw has been discovered in the JScript component of the Windows operating system. The flaw may allow an attacker to execute malicious code within a sandboxed environment on a target computer, and requires user's interaction such as downloading a JS file.

THREAT INTELLIGENCE REPORTS

- The RIG Exploit Kit has added the Internet Explorer zero-day vulnerability tracked as CVE-2018-8174 to its attacks.

  Check point IPS blade provides protection against this threat *(Microsoft Windows VBScript Engine Remote Code Execution (CVE-2018-8174); RIG Exploit Kit URL; RIG Exploit Kit Landing Page; RIG Exploit Kit Website Redirection)*

- Security researches have revealed a new technique that causes physical damage to hard drives by leveraging sonic and ultrasonic signals. An attacker can use this technique to compromise victim's machine by playing malicious sounds attached to an email or a web page, using a nearby external speaker or a target system's own built-in speakers.
- Two new strains of malwares have been discovered being used by the North Korean APT group known as 'Hidden Cobra'. The malwares dubbed 'Joanap' and 'Brambul' are Remote Access Trojan (RAT), and Server Message Block (SMB) worm respectively, and have been used by the group since 2009 to target companies in the media, aerospace, financial, and critical infrastructure sectors across the world.

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

- Security researches have uncovered two infamous banking Trojans, IcedID and TrickBot, are collaborating and sharing their profits.

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