Check Point
SOFTWARE TECHNOLOGIES LTD.

May 13 - 19, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The web skimming script "MageCart" has been found injected to the subscription website of the Forbes magazine as well as of seven others, stealing payment data of subscribers. Forbes was probably a victim of the supply chain attack conducted by MageCart group last weekend in which it compromised "Picreel", a web marketing software supplier whose code is integrated inside Forbes's.

  Check Point Anti-Bot blade provides protection against this threat (Trojan.Win32.Magecart)

- BlackTech cyber group has been exploiting an ASUS update process for the windows cloud storage service "WebStorage", to deliver the Plead backdoor. According to researches the group targeted the update process in a man-in-the-middle attack (MitM), thus were able to push a malicious update.

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

- The popular Q&A platform for programmers "Stack Overflow" has suffered a major data breach exposing users' name, email and IP addresses. Threat actors have managed to exploit a flaw in the company's development tier and to gain unauthorized access to its production version.

- The organized cybercrime network behind "GozNym" banking malware, which is responsible for stealing nearly $100 million from over 41,000 victims across the globe, has been indicted by law enforcements.

- The infamous hacking forum "0Gusers" has been hacked, and its database was published in another hacking forum. The breach exposed sensitive information of 113,000 users/hackers including email addresses, passwords, IP addresses, and private messages.

- Personally-identifiable information belonging to nearly 90% of Panama's citizens has been exposed due to an online unprotected Elasticsearch server. The exposed information includes full names, birth dates, national ID numbers, medical insurance numbers, and other personal data.

- Over 12,000 unsecured MongoDB databases have been deleted over the past three weeks by attackers dubbed "Unistellar", demanding ransom in exchange to the restoration of the data.

©2019 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content

VULNERABILITIES AND PATCHES

- Facebook has patched a critical zero-day vulnerability in WhatsApp, which was exploited in the wild to remotely install the Pegasus advanced mobile spyware. The vulnerability is a buffer overflow in WhatsApp VOIP stack, and allows attackers to run arbitrary code by calling the targeted device over WhatsApp audio call.
- Microsoft has released its patch Tuesday for May, addressing 79 vulnerabilities, including a critical "wormable" RDP flaw that resides in the Remote Desktop Services, and a Windows privilege escalation flaw related to the way the Windows Error Reporting (WER) system handles files.
- A critical vulnerability dubbed "Thrangrycat" has been found affecting millions of Cisco products supporting Trust Anchor module (TAm), and may allow attackers to implant a persistent backdoor.
- A Misconfiguration flaw has been found in the Bluetooth-supported version of Google's Titan Security Keys, which provide an additional layer of security against Phishing attacks. The flaw may allow an attacker who is physically close to the Security Key to communicate with it or with the device the key is paired to.
- A security bug in Twitter's iOS app has led to a collection and leak of users' location data with a third-party advertising company.
- Intel CPUs are vulnerable to a new class of vulnerabilities dubbed "Microarchitectural Data Sampling" (MDS), which can utilize speculative execution to potentially leak sensitive data from a system's CPU.

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

THREAT INTELLIGENCE REPORTS

- An analysis reviewing the North Korean APT group "ScarCruft" activity has revealed that the group has expanded its espionage arsenal and added malware capable of harvesting Bluetooth information. The analysis also discovered some overlaps with the DarkHotel APT.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat *(Trojan.Win32.Karkoff)*
- New sophisticated technique named "Cipher Stunting" is being used by threat actors to evade detection and run their malicious campaigns undisturbed. The technique involves tampering with TLS signatures at large scale, thus helping malicious activity to masquerade as live human traffic.