October 30 - November 5, 2017

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Information of over 45 million mobile phone accounts in Malaysia has been stolen and is being sold on the dark net. The accounts are from multiple companies, and it is unclear what the source of the breach was. As Malaysia has a population of 32 million, it is assumed that every mobile phone account in the country was affected by this breach.

- Researchers have published information about the recent activity of the threat group known as "Gaza Cybergang". The group specializes in social engineering by sending malicious messages and files with headlines that are related to current events in the Middle East. The group's targets are mostly located in the Middle East and North Africa.

  Check Point IPS blade provides protection against this threat (Microsoft Outlook Remote Code Execution (CVE-2017-0199))

- A fraudulent app that dubbed itself "Update WhatsApp Messenger" was downloaded over a million times from the Google Play Store. Fortunately, the app's impact was not severe, as it only sought to gain revenue by pushing advertisements. The app is still available on Google Play, but it has since changed its name and logo.

  Check Point Sandblast Mobile customers are protected from this threat

- Canadian company Verticalscope, which manages hundreds of forum sites totaling in over 40 million users, has been breached. Information of at least 2.7 million user accounts has been stolen and is being sold on the dark net. This is the second time in the last 2 years that the company is breached, following a 45-million user account theft on June 2016.

- A threat group has been discovered to be utilizing compromised web pages to manipulate Google's search results and push an infecting website to be the top result for certain queries. Entering the site would infect users with Panda, a variant of the Zeus banking Trojan.

  Check Point Anti-Bot blade provides protection against this threat (Trojan.Win32.Panda-banke; Operator.Panda)

VULNERABILITIES AND PATCHES

- A security researcher has discovered a bug in Google Issue Tracker, an internal tool Google uses to hold information about known bugs and security vulnerabilities in Google products. The researcher was able to gain information about any current security vulnerability in Google products. Google has since fixed this issue.

  Check Point IPS blade provides protection against this threat (Suspicious Site Containing Tech Scams; Microsoft Office Malicious Macros)

- TOR has released version 7.0.9, a security patch for the TOR browser. The patch was released after a vulnerability that could cause a specially-crafted webpage to bypass the browser and reveal the user's real IP address had been discovered.

- Wordpress has released version 4.8.3 in order to fix a severe SQL injection vulnerabilities.

  Check Point IPS blade provides protection against this threat (WordPress Core WPDB SQL Injection)

- Oracle has patched a default-account vulnerability in Oracle Identity Manager. The vulnerability is remotely-exploitable and was ranked 10/10 in the severity scale.

  Check Point IPS blade provides protection against this threat (Oracle Identity Manager Authentication Bypass (CVE-2017-10151))

- Apple has published security updates for multiple products. Some of the vulnerabilities addressed could result in remote code execution on affected products.

THREAT INTELLIGENCE REPORTS

- A technical analysis of the malicious spam email campaigns behind Locky and Trickbot has been published. A specially-designed botnet is used to spread the payload.

  Check Point IPS and Anti-Bot blades provide protection against this threat (Microsoft Office DDE Remote Code Execution; Operator.Locky; Trojan-Ransom.Win32.Locky; Operator.Trickbot; Trokan-Banker.win32.Trickbot)

- A new ransomware dubbed GIBON has been detected in the wild, as it is being spread by a malicious email spam campaign. Fortunately, a decryption tool for infected machines is available for download.

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