Check Point
SOFTWARE TECHNOLOGIES LTD.

April 15 - 21, 2019

# YOUR CHECK POINT
# THREAT INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- Check Point Research has uncovered several phishing scams related to the TV series Game of Thrones. The fraudulent sites acquire personal information or convince the user to install an unwanted program.

  *Check Point SandBlast Agent provides protection against this threat*

- 500 million iOS users have been exposed to a malvertising campaign conducted by the threat group eGobbler, exploiting a Chrome for iOS vulnerability to bypass the browser's built-in pop-up blocker.

- A Phishing scam in Instagram is luring users to enter compromised links using an Instagram profile called "@The_HotList_95". The users received personal messages prompting them to enter the profile, which contained a link to a fake Instagram login page.

- Eight unsecured databases containing scarped data and email addresses of nearly 60 million LinkedIn users have been found online. LinkedIn's investigation yielded that the exposed databases belong to a third-party company that aggregated data from multiple sources, including LinkedIn.

- Personal data of over 100 million users of the Indian search service JustDial has been exposed, after an unprotected database was found online. The leaked data contained usernames, email addresses, mobile numbers, addresses, occupation and even photos.

- Sensitive information of Iranian drivers has been left exposed online after a ride-hailing company in Iran left a database publicly available. The database contained over 6.7 million records including names, Iranian ID number and phone number.

- Security researchers have uncovered the Sea Turtle cyber espionage campaign, using DNS hijacking to compromise servers of ministries of foreign affairs, military organizations, intelligence agencies and energy companies in the Middle East and North Africa.

  *Check Point IPS blade provides protection against the exploited vulnerabilities (Cisco Adaptive Security Appliance Web Services Denial of Service (CVE-2018-0296); Apache Tomcat PUT Method Arbitrary File Upload Remote Code Execution (CVE-2017-12615; CVE-2017-12617) etc.)*

## VULNERABILITIES AND PATCHES

- Broadcom WiFi chipset drivers have been found vulnerable to potential remote code execution and denial-of-service attacks. The vulnerabilities discovered include heap buffer overflows and frame validation bypass which may allow a remote attacker to compromise the device in which the chip is installed.
- A security researcher has managed to take control over Windows Live Tiles after Microsoft failed to delete some of the entries for the disabled subdomain that still maintains the Live Tiles content for around 2,500 websites.
- A new filter feature in AdBlock browser extensions may allow attackers to remotely inject arbitrary code into web pages. The new filter introduces the option of re-writing web requests and may be leveraged to perform online credential theft or potentially malicious page redirection.

## THREAT INTELLIGENCE REPORTS

- White-hat hackers have managed to break into the French government's secure messaging application. While available on Google Play Store, the newly-launched, end-to-end encrypted application was supposed to be accessible only by officials and politicians with government-associated email accounts.
- Experts have discovered a large-scale DDoS attack abusing the ping-based hyperlink auditing feature in HTML5, which allowed the attackers to send requests to the target website from users of a popular chat application in China. The attack peaked at 7,500 requests per second from 4,000 user IP addresses.

  *Check Point IPS blade will provide protection against this vulnerability in the next releases*
- Source code of tools used by the Iran-linked group OilRig, also known as APT34, has been leaked on Telegram after another hacker group disclosed details about OilRig's hacking tools, members and operations.
- A new variant of HawkEye infostealer has been observed in the wild, spread through malicious email campaigns. The infection chain includes weaponized Excel spreadsheets and Word Documents, exploiting an old arbitrary code execution bug in Microsoft Office.

  *Check Point SandBlast and Anti-Bot blades provide protection against this threat (Infostealer.Win32.Hawkeye)*
- Scranos, a cross-platform, rootkit-enabled spyware, continues to release new variants to the wild as its operators are continuously testing new components on infected users. The main components include cookie extraction, credential theft, installation of additional programs and sending phishing messages to the victim's contact lists on social media platforms.

  *Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Spyware.Scranos)*