Check Point
SOFTWARE TECHNOLOGIES LTD.

April 30 - March 5, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- A new campaign of the Zeus Sphinx banker is targeting clients of US, Canadian and Australian banks using COVID-19 themed emails. Emails titled "COVID 19 relief" contain password-protected Word documents with malicious macros.

  Check Point SandBlast, Anti-Bot and Anti-virus provide protection against this threat (Trojan-Banker.Win32.Zeus)

- Personal details of more than 4.9 million Georgians have been published on a hacking forum. The source of the information, which includes names, addresses, DOB, ID and mobile numbers, is still unclear.

- Japan's CERT has found an APT campaign exploiting patched Firefox and Internet Explorer vulnerabilities (CVE-2019-17026 and CVE-2020-0674) and targeting Japanese entities. The same vulnerabilities were previously used by the Peninsula APT, active for more than 10 years, focusing on Chinese targets.

  Check Point IPS blade provides protection against this threat (Microsoft Internet Explorer Use After Free (CVE-2020-0674))

- Marriott hotels have disclosed a security breach affecting 5.2 million guests. The company informed guests via email and provides personal-information-monitoring services to those impacted. Marriott was fined $123 million last year for a 2018 breach of 327 million records.

- Recently detected Magecart campaign has claimed 17 e-commerce sites using a new credit card skimmer, dubbed MakeFrame. The activity is attributed to Magecart group 7. Researchers report of a 20% increase in Magecart attacks since the beginning of the Corona pandemic.

- Mandrake, a newly revealed spyware / banker, is targeting Australian Android users. This financially motivated malware has been active since 2016, customizing attacks to each individual victim.

- Sonatrach, Algeria's national oil company, is the latest victim of the Maze ransomware group. As part of its double-extortion strategy, the attackers posted Sonatrach's investment plans, financials and other details on a dedicated site, threatening to publish additional information unless ransom is paid.

  Check Point SandBlast provides protection against this threat

VULNERABILITIES AND PATCHES

- A critical vulnerability in the WordPress SEO plugin, Rank Math, could allow attackers to give administrator privileges to any registered user. The plugin is currently installed on more than 200,000 sites. Patched version of the plugin has been released.
- Mozilla has released a new Firefox version to address two actively exploited vulnerabilities (CVE-2020-6819 and CVE-2020-6820). Both vulnerabilities are use-after-free issues and can lead to RCE attacks.
- Experts have published POC exploits for a Windows vulnerability (CVE-2020-0796) to demonstrate its exploitation for local privilege escalation. Researchers discovered 48,000 vulnerable servers exposed online.

  Check Point IPS blade provides protection against this threat (Microsoft Windows SMBv3 Remote Code Execution (CVE-2020-0796))
- Google has published Chrome version 80.0.3987.162 that include fixes to eight security issues, three of which are high severity vulnerabilities.

THREAT INTELLIGENCE REPORTS

- Check Point Research have shown that since the beginning of the coronavirus outbreak there is a drop of 17% monthly in the overall number of cyberattacks globally, while the number of coronavirus-related cyberattacks keeps increasing.
- The FBI has issued a warning regarding a new wave of attacks by FIN7 APT group. Attackers target businesses by sending USB devices through the US Postal Service, offering gift cards. The USB emulates keyboard strokes to initiate its infection-chain through PowerShell.
- The recent surge in Zoom conference application usage is followed by increased scrutiny to its privacy policy and vulnerabilities. Critics complain of unsolicited data sharing with Facebook, unmet promises of end-to-end encryption, exposure to UNC path injection that exposes users to credential stealing and threat of uninvited participant and more.
- Researchers have examined 150,000 Android applications and discovered that 8.5% contained backdoors allowing access to admin-only functions, master passwords and more. Sixteen percent of the examined preinstalled apps extracted from Samsung smartphones included hidden backdoors.
- Forty-two million records of Iranian Telegram users have been exposed online on an unprotected Elasticsearch cluster, revealing user IDs and phone numbers. Telegram is prohibited in Iran and the data originated from an unofficial fork version of the open source application. The leaked data exposes users to risk both from Iranian authorities and by additional attackers.