October 2 -6, 2019

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has uncovered new information on an espionage campaign suspected to be conducted by the Egyptian government. The targets of the campaign are journalists, politicians, human rights activists and lawyers in Egypt. Most of the activity was conducted using malicious mobile apps, used to gather login credentials to email accounts, bypass privacy settings, and store call logs.

  Check Point Sand Blast Mobile provides protection against this threat

- The Iranian cyber espionage APT Phosphorus has reportedly attempted to retrieve Microsoft account information from accounts associated with US government officials, journalists and prominent Iranians living outside Iran. The group used fraudulent requests for account recovery via emails to gain access over the targeted accounts.
- A former Yahoo! software engineer has hacked into the Yahoo! accounts of nearly 6,000 users, mainly younger women, in search of private images and videos. He was also accused of using the information obtained from the hacked accounts to access their other online accounts, including iCloud, Gmail and Facebook.
- Ten hospitals and health service providers in the United States and Australia have been hit by ransomware attacks that resulted in a severe shutdown of parts in their IT infrastructure, impacting their ability to take in new patients.
- An unprotected ElasticSearch server has been discovered online, holding over 20 million tax records belonging to Russian citizens. The exposed data contained information from 2009 to 2016, and included tax information, ID numbers and other personal identifiable information.
- UAB Medical has fallen victim to a phishing attack, allowing the attackers to gain access to employee emails that contained health information for nearly 20,000 patients. The attackers also attempted to target the payroll system and redirect some of the employee payments.

- A database containing personal information of 92 million Brazilian citizens is being auctioned on underground markets. The records, 16GB in total, include names, date of birth and taxpayer ID. It is suspected that the origin of the data was a government organization.
- Four US food chains have disclosed that their Point-of-Sale (PoS) systems were infected with malware during the past year, scraping customer payment information at checkout. One of the food chains, who also owned PoS systems for fuel pumps, had the malware in their network since December 2018.
- A former American Express employee is suspected of abusing customer data for fraud by wrongfully gaining unauthorized access to cardholders' information. The accessed information includes names, addresses, Social Security numbers and credit card number.

VULNERABILITIES AND PATCHES

- A critical Zero-day vulnerability in Android mobile devices has been discovered and is being exploited in the wild. The Zero-day, tracked as CVE-2019-2215, is a use-after-free vulnerability in the kernel's binder driver that may allow escalation-of-privileges, resulting in potential full takeover of the device.

  Check Point Sand Blast Mobile provides protection against this threat

- A memory corruption bug has been revealed, which may allow remote code execution attacks on WhatsApp for Android devices. The bug resides in a GIF image parsing library used by the app, and may allow the attacker to run malicious code with the permissions WhatsApp has on the device.

  Check Point IPS will release protection against this threat in its next online package

- The Signal Private Messenger secure messaging app suffers from a logical vulnerability that could allow malicious user to force an incoming call to be answered, without the victim's interaction or approval. The design flaw is exploitable only on the Android versions of the messaging app.

THREAT INTELLIGENCE REPORTS

- Researchers have uncovered operations planned by SandCat, Uzbekistan's State Security Service. Severe OPSEC mistakes made by the group have led the researchers to discover four Zero-day exploits the group purchased and malware code in development.
- FTCode, an old PowerShell ransomware has resurfaced, and is being distributed in spam campaigns aimed at Italian recipients. The spam e-mails contain malicious Word documents in Italian, such as fake invoices or job applications, which contain embedded macros that execute PowerShell commands onto the target computer.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat (Trojan-Downloader.VBS.JasperLoader; Trojan-Downloader.JS.JasperLoader; Ransomware.Win32.FTCode)