Check Point
SOFTWARE TECHNOLOGIES LTD.

July 15 - 21, 2019

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Bulgarian government has suffered a major data breach exposing personal and financial information of 5 million citizens after threat actors managed to hack the country's tax reporting service. The threat actors, who claim to be Russians, sent some of the 21 GB of stolen information to the Bulgarian media.

- SyTech, a contractor for the Federal Security Service of the Russian Federation (FSB), has been hacked. The attackers have exfiltrated 7.5 Tera Bytes of data including projects and researches for an FSB unit engaging in electronic intelligence, and have also defaced the company's website.

- Security researches have revealed several scams leveraging the popularity of the face-modifying app "FaceApp". The scammers use fake websites offering fake "Pro" version of the application as a lure, and trick victims into clicking countless offers for installing other paid apps, ads, surveys, and more.

  Check Point SandBlast Mobile customers are protected from this threat

- Security researchers have discovered a sophisticated Hong Kong malvertising attacker who partnered with legitimate ad tech platforms and spread over 100 Million ads to date. This allowed him to gain access to premium audiences and redirect them to landing pages, which will infect them with malware.

  Check Point Anti-Virus blade provides protection against this threat (FiberAds)

- A new ongoing cyberespionage campaign has been discovered, conducted by StrongPity APT group. The campaign uses a new spyware designed to locate sensitive documents on the infected machines, and is dropped by malicious installers for legitimate software including WinBox for MikroTik's RouterOS.

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

- A new strain of Ransomware has been spotted in the wild named "DoppelPaymer" sharing most of its code with the infamous BitPaymer. DoppelPaymer is believed to be created by members of the TA505 group, and is capable of terminating processes that may interfere with file encryption.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Ransomware.Win32.Doppelpaymer)

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

VULNERABILITIES AND PATCHES

- Instagram has released a security patch to a critical vulnerability in its mobile version, which could allow an attacker to take over Instagram accounts without any user interaction. The vulnerability resides in the password recovery mechanism, which allows users to regain access after they forgot their password.
- Security researchers have revealed a serious flaw that exposed millions of sensitive private files stored on thousands of discontinued Lenovo NAS devices. The flaw may allow a remote unauthenticated attacker to access exposed devices by sending a specially crafted request via an unprotected API.
- A new vulnerability in the Bluetooth communication protocol has been spotted, and could potentially expose Windows 10, iOS and macOS devices to permanent global tracking and identifying.
- Remote code execution vulnerabilities have been found and patched in Atlassian Crowd and Atlassian Jira Server, exposing tens of thousands of servers to a potential risk.

  Check Point IPS Blade provides protection against these threats *(Atlassian Crowd Remote Code Execution (CVE-2019-11580), Atlassian Jira Server Remote Code Execution (CVE-2019-11581))*

THREAT INTELLIGENCE REPORTS

- A new attack method named "Media File Jacking" has been discovered, allowing attackers to manipulate media files received via WhatsApp and Telegram apps on Android without users' knowledge and in real-time. The attack can lead to payment manipulation scams, fake news distribution, and more.
- Security researchers have discovered that 'iOS URL Scheme' feature in Apple mobile devices can be abused to steal users' sensitive data via App-in-the-Middle attack. In this attack malicious apps can hijack sensitive data of certain apps, mainly in cases when the login process of the apps is related.
- Security researches have spotted a new Linux spyware named EvilGnome. EvilGnome is attributed to the Russia-linked 'Gamaredon' Group and is capable of taking screenshots, stealing files, capturing audio recording, and downloading and executing further malicious modules.

  Check Point Anti-Virus and Anti-Bot blades provide protection against this threat *(Spyware.Win32.EvilGnome)*
- A side-channel attack dubbed "Spearphone" has been discovered, allowing attackers to capture voice from Android smartphones' loudspeakers without requiring any permissions. The attack can be triggered when victims place phone or video calls on speaker, listen to a media file, or interact with the smartphone assistant.
- A report reviewing the activity of Mirai IoT botnet activity and abilities stresses that it has doubled its activity and introduced new and improved techniques to target enterprise-level hardware.

  Check Point IPS, Anti-Bot and Anti-Virus blades provide protection against this threat *(Weak Password Login Attempt Over Telnet; Backdoor.Linux.Mirai; Botnet.Win32.Mirai)*