Check Point
SOFTWARE TECHNOLOGIES LTD.

April 5-11, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Iranian threat group APT34, also dubbed 'OilRig', has recently launched a new campaign according to Check Point Research. The campaign is focused on a Lebanese target and leverages an alleged job opportunity document and a new backdoor called 'SideTwist'.

  Check Point SandBlast provides protection against this threat

- Pierre Fabre, a prominent French pharmaceutical and cosmetics company, has suffered an attack by the REvil ransomware, leading to a temporary pause in all production processes. The gang has demanded a $25 million ransom.

- The user data of Swarmshop, a popular underground carding shop, has been leaked online. The breach has led to the exposure of some 12,300 records of the shop's admins, sellers, and buyers, that include their nicknames, hashed passwords, contact information and activity log.

- Some 500 million records belonging to LinkedIn users have been breached and are being offered for sale on a hacker forum. Leaked information includes members' full names, email addresses, phone numbers, gender and more. LinkedIn claims that entire data originates in public sources.

- More than 530,000 Huawei users have been infected with the Joker mobile malware, after downloading several malicious applications from the company's official Android store, AppGallery, disguised as a virtual keyboard, camera, sticker collection or game app. The malware features spyware capabilities such as SMS messages and contact list theft.

  Check Point Harmony Mobile provides protection against this threat

- SQL database containing some 1.3 million Clubhouse application users has been leaked online, and is now available for free on a popular hacking forum. Additionally, threat actors have been utilizing Facebook ads promoting Clubhouse in order to deliver the Ragnar Locker ransomware.

  Check Point SandBlast Agent provides protection against this threat *(Ransomware.Win32.Ragnar)*

VULNERABILITIES AND PATCHES

- New critical remote code execution vulnerability in several Cisco Small Business routers has been exposed. The flaw resides in the web-based Management Interface. The company has announced that due to the age of these routers, the flaw will not be patched.
- Researchers have discovered a vulnerability in the popular open-source learning platform Moodle. The flaw could enable any user with a Moodle account to take over accounts of students, professors or even admins from the same educational institution. The flaw relies on the private chat board feature of the platform.

THREAT INTELLIGENCE REPORTS

- Check Point Research has discovered a new Android malware capable of spreading itself and distributing further payloads via WhatsApp conversations. The malware disguises itself as a Netflix content enabler application called 'FlixOnline', that can be found on Google Play store.

  Check Point Harmony Mobile provides protection against this threat

- New backdoor distributed by the North Korean APT Lazarus has been found. Called 'Vyveva', the tool has been in use since 2018, and has recently been deployed in a targeted espionage attack against a South African freight logistics company.
- Facebook has published its monthly Coordinated Inauthentic Behavior Report, including a review of a long-term disinformation operation leveraging the social media platform, originating in a troll farm in Albania. The operation primarily targeted Iranian users and might be tied to an Iranian group opposing the regime.
- Threat actors have been leveraging legitimate corporate contact forms in order to deliver phishing emails carrying the IcedID info-stealing malware. The forms contain enterprise lawsuit threats, and the malware can be used to download additional payload onto the victim machine.

  Check Point Anti-Virus and Anti-Bot provide protection against this threat *(Trojan-Downloader.Win32.IcedID)*

- Visa, a global payments processor, has been warning against an increase in the deployment of web-shells on compromised servers as part of attacks aiming to exfiltrate credit card information collected from users of online shopping platforms.

  Check Point SandBlast and SandBlast Agent provide protection against this threat *(Ransomware.Win32.Revil)*

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