Check Point
SOFTWARE TECHNOLOGIES LTD.

September 21-27, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Following last week's emergency directive issued by CISA, Microsoft has warned that attackers are actively exploiting the critical Zerologon vulnerability (CVE-2020-1472) to attack Microsoft Windows servers using publicly available PoC exploits.

  Check Point IPS blade provides protection against this threat *(Microsoft Netlogon Elevation of Privilege (CVE-2020-1472))*

- Tyler Technologies, the largest provider of software and technology services to the United States public sector, has suffered a cyberattack most likely involving the RansomExx ransomware. Tyler has warned that its credentials were used for remote access to several of its clients and advised for password reset.

- $150 million have been stolen from several hot wallets of the Singapore-based cryptocurrency exchange KuCoin. KuCoin stated that hackers obtained private keys to its wallets, and promised to reimburse affected users and publish the wallet address of the hacker and the list of stolen funds.

- Another DDoS attack hits financial institutions; several Hungarian banks and telecommunication services were disrupted by a distributed attack originating from servers in Russia, China and Vietnam.

- The network of an unspecified US federal agency has been recently compromised, according to a CISA report. The threat actor behind the attack used compromised O365 credentials to implant malware, evaded the agency's anti-malware protection and gained persistent access to the network.

- A major data breach in an Indian government COVID-19 tracking app has exposed personal data of more than 8 million citizens. The exposed data included full names, gender, age, residential address, and contact numbers of everyone who had tested COVID-19 positive in the Indian state of Uttar Pradesh.

- Luxottica, the world's largest eyewear company, has been hit by a ransomware attack, leading to the shutdown of its operations in Italy and China. Experts suspect the source of the breach was a Citrix ADX controller device, vulnerable to the critical (CVE-2019-19781) flaw.

VULNERABILITIES AND PATCHES

- Check Point Research has exposed a vulnerability (CVE-2020-1895) in the iOS and Android versions of Instagram. The high severity vulnerability resides in the open source JPEG format decoder, Mozjpeg, and could have enabled attackers to access victim's camera, microphone and other components.

  Check Point SandBlast Mobile provides protection against this threat

- Cisco Systems has released a series of fixes in a wide range of products. Twenty nine of the patched vulnerabilities are rated high severity.

- Google has released a new version of Chrome, fixing ten security flaws. The successful exploitation of the most severe of these could allow an attacker to execute arbitrary code by getting the victim to visit a specially crafted webpage.

- Apple has patched four vulnerabilities affecting macOS Catalina, High Sierra and Mojave.

THREAT INTELLIGENCE REPORTS

- Facebook has removed accounts and pages of several Russian, Chinese and Philippine disinformation networks conducting coordinated inauthentic behavior (CIB). The Chinese operations were engaged in US elections and China's interests in the Philippines and Southeast Asia. The Russian networks were involved in creating factious media entities and amplify their content.

- Microsoft has published that earlier this year it removed 18 Azure Active Directory applications that were used by the Chinese APT-40 threat actor group as part of their multistage infection chain.

- Researchers report a Russian speaking threat-actor, OldGremlin, has been linked to at least nine ransomware attacks this year on medical labs, banks, manufacturers, and software developers in Russia. A large Russian medical company hit by the actor received ransom demands of $50K in cryptocurrency.

- Researchers have exposed an ongoing cyber espionage operation against Indian defense units. The operation, active for more than a year, has been attributed to the Pakistani Transparent Tribe APT group.

- CISA and the FBI have issued a joint statement warning of threat actors actively spreading false information about compromised voting systems and voter registration databases in order to discredit the electoral process. According to CISA, attempts to compromise election infrastructure could only slow down but not prevent voting efforts.

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