Check Point
SOFTWARE TECHNOLOGIES LTD.

August 17 - 23, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The University of Utah has paid $457K to prevent attackers from publishing student and employee information stolen during a ransomware attack which ended on July 19th. The ransom has been paid by the university's cyber insurer.
- Taiwan has blamed four Chinese APT groups: Blacktech, Taidoor, MustangPanda and APT40 for conducting a long-term espionage operation. The operation targeted employees of companies that provide services to government entities.
- International IT giant Konica Minolta has been hit by RansomEXX ransomware, the same malware used in an attack on Texas department of transportation in June 2020, and its services were down for almost a week.
- South African credit reporting agency, Experian, has disclosed a data breach of personal information impacting 24 million customers. The attackers behind this operation were identified by local law enforcement, and a court order allowed to seize their equipment and wipe the stolen data.
- Voice phishing attacks are on the rise due to COVID-19 remote work policies and following the high-profile Twitter vishing scam. Researchers describe coordinated attacks, leasing of American voice actors, set-up of dedicated phishing pages to bypass MFA mechanism, in campaigns often focusing on corporate new hires.
- Thousands of Canadian government services accounts have been hacked in credentials stuffing attacks, some were later used to divert COVID-19 aid payments.
- A newly reported botnet dubbed FritzFrog, operating since early this year, has been targeting SSH servers. FritzFrog, written from scratch in GO, is a P2P botnet, does not have a centralized C2 and is fileless - operating completely from memory. It is currently used for Monero cryptomining but most likely intended for future infrastructure-as-a-service purposes.

Check Point Anti-Bot provides protection against this threat *(Botnet.Linux.FritzFrog)*

VULNERABILITIES AND PATCHES

- Microsoft has issued an out-of-band software update for Windows 8.1 and Windows Server 2012 R2 to patch two recently reported vulnerabilities CVE-2020-1530 and CVE-2020-1537.
- A vulnerability in Jenkins, an open source server software, tracked as CVE-2019-17638 with CVSS rating of 9.4, may allow unauthenticated attackers to receive sensitive data intended for other users.

  Check Point IPS provides protection against this threat (Jenkins Jetty Buffer Overflow (CVE-2019-17638))
- PoC exploits for two previously patched vulnerabilities in Apache Struts 2 have been published on GitHub. Successful exploitation of the bugs, tracked as CVE-2019-0230 and CVE-2019-0233, could allow RCE and DoS attacks.

  Check Point IPS provides protection against this threat (Apache Struts2 Content-Type Remote Code Execution)(Apache Tomcat CGI Servlet Remote Code Execution (CVE-2019-0232))
- A critical bug in Google's Gmail allowed attackers to send spoofed emails, bypassing both SPF and DMARC security protocols. The issue is caused due to missing verification when configuring mail routes.
- Cisco has released updates to multiple vulnerabilities on the Trek IP stack, known as Ripple20, exploitation of which could result in remote code execution or DoS. Update is required on multiple Cisco products.

THREAT INTELLIGENCE REPORTS

- The threat actor behind the GoldenSpy backdoor, delivered with compulsory tax-software for companies conducting business in China, is engaged in an effort to uninstall it, trying to cover their traces. Researchers report of several variants of the uninstaller, changing to avoid detection by published YARA rules.

  Check Point SandBlast and anti-Bot provide protection against this threat (Goldenspy)
- US CISA has published a malware analysis of a North Korean RAT, BLINDINGCAN, used by the Lazarus APT group in a campaign to recruit defense employees of American defense corporations through LinkedIn. This follows an extensive report by the US army describing North Korea's cyber arm 'Bureau 121' and its subdivisions, employing more than 6,000 hackers, many of which operate from abroad.

  Check Point Anti-Bot and Anti-Virus provide protection against this threat (RAT.Win32.BLINDINGCAN)
- Hidden Shadow, the threat actor behind the WannaRen ransomware, has submitted master decryption key to be used for a free decryption tool. WannaRen's integrated EternalBlue exploit mechanism made it spread rapidly in China, driving its developers to release keys, probably in fear of Chinese authorities' actions.

  Check Point SandBlast and Anti-Virus provide protection against this (Ransomware.Win32.wannaren)