Check Point
SOFTWARE TECHNOLOGIES LTD.

July 13 – 19, 2020

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- 130 Twitter accounts have been compromised of which 45 high profile accounts were used to promote a cryptocurrency fraud that yielded more than $120K. An ad that appeared before the attack on a gray-market site offered to sell control of Twitter accounts. Investigators believe attackers used credentials for a Twitter backend tool, found in an employee's Slack channel.
- Advisories from the UK, US, Canada and Australia warn that Russia's Foreign Intelligence Service (SVR) has been conducting espionage operations to target COVID-19 research organizations. APT29 (aka Cozy Bear) is believed to be behind the operation, using the WellMess malware.

  Check Point SandBlast provides protection against this threat (Trojan.Win32.WellMess)
- Ending a five months break that started in February, Emotet has returned to activity with a spam campaign targeting mostly US and UK victims. The current campaign aims to infect new end-users using attached word documents in English with malicious macros or URLs linking to the download of such documents.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Trojan.Win32.Emotet)
- French telecommunication company Orange confirmed it has suffered a ransomware attack on its business services division. Nefilim ransomware group assumed responsibility for the attack and added Orange to their data leak site, publishing an archive file containing stolen client data.
- Blackbaud, a cloud provider for non-profit, educational and healthcare organizations has detected and stopped a ransomware attack but was forced to pay ransom demands after attackers threatened to publish client information stolen in the attack.
- BlackRock, a new Android malware designed to steal passwords and card data, has reportedly been distributed as a fake Google update package on third-party sites. The malware uses Accessibility permissions to steal information from more than 330 applications including TikTok, Tinder, Instagram and more.

  Check Point SandBlast Mobile protect against this threat

VULNERABILITIES AND PATCHES

- Check Point Research has disclosed a 17-year-old wormable RCE vulnerability in Microsoft Windows DNS Servers, tracked as CVE-2020-1350, with CVSS 10.0. The bug, dubbed "SIGRed", is a wormable vulnerability allowing infection of other connected platforms without user interaction. Microsoft has issued a patch and CISA published an emergency directive to all agencies to patch systems within 24 hours.

  Check Point SandBlast Agent and IPS blades provide protection against this threat (Microsoft Windows DNS Server Remote Code Execution (CVE-2020-1350))

- Check Point Research has reported a flaw in Zoom conferencing app which could be used to impersonate corporate personnel and lure victims into fake Zoom meetings. An improper account validation allowed any meeting ID to be launched using any organization's Vanity URL, facilitating social engineering attacks.

- SAP has patched RECON, a critical vulnerability tracked as CVE-2020-6287 with a CVSS score of 10.0 affecting several SAP business solutions through the NetWeaver Application Server (AS) Java platform. POC publication was soon followed by mass scanning activity in search of vulnerable platforms.

  Check Point IPS blade provides protection against this threat (SAP NetWeaver Directory Traversal (CVE-2020-6286))

- Cisco has released a fix to 33 flaws in a variety of its devices, the most severe of which can be exploited to conduct RCE and privilege escalation attacks on Cisco's Small Buisness Wireless VPN Firewall routers.

- Adobe has released updates to patch 13 vulnerabilities affecting five of its applications including four critical issues. None of the vulnerabilities has been seen exploited in the wild.

THREAT INTELLIGENCE REPORTS

- A 2018 directive from president Trump, authorizing the CIA to conduct offensive cyber operations against foreign targets, specifically Russia, China, Iran and North Korea, has led to a series of covert operations, claims a recent report. The report attributes the leak of Iranian APT34 hacking tools, the breach of a subcontractor of the Russian FSB, and other operations, to the CIA's new modus operandi.

- An OPSEC error by the Charming Kitten Iranian APT, associated with the recent attacks on pharma company Gilead and US 2020 elections' candidates, provided researchers with access to 40 gigabytes of data including hours of training videos. The data, left on a misconfigured cloud server, records attacks on US and Greek Navy personnel and other TTPs.

- For the second time this year, malware has been found delivered through a tax software required by Chinese government for companies operating in the country. The malware, dubbed GoldenHelper, is bundled in the Golden Tax Invoicing Software.

  Check Point Anti-Virus blade provides protection against this threat (Trojan.Win32.GoldenHelper)