July 27 – August 02, 2020

Check Point
SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Travel management giant CWT has paid hackers $4.5M in bitcoin after it had been hit with the Ragnar Locker ransomware and attackers threatened to publish two terabytes of stolen data.

  Check Point SandBlast provides protection against this threat (Ransomware.Win32.Ragnarlocker)

- China linked hackers have compromised the Vatican computer networks and the Catholic diocese of Hong Kong. This attack occurred in May, ahead of expected discussions between the Vatican and China regarding the renewal of a 2018 agreement that established their relations.

- Docker servers hosted on cloud platforms such as AWS, Azure, Alibaba Cloud and more, with exposed APIs, have been targeted by attackers who use them to run malicious cryptomining containers.

- 386 million stolen records, including names, emails, home addresses, credit card numbers and more have been made available for free by a hacker known as ShinyHunters. The data is a result of 18 separate data breaches including nine that had not been previously disclosed.

- German Dussmann Group has suffered a ransomware attack by the Nefilim gang. The gang posted documents on its leak site claiming it had stolen 200GB of data in the attack.

  Check Point SandBlast provides protection against this threat (Ransomware.Win32.Nefilim)

- Two campaigns, which target network attached storage devices (NAT) of the Taiwanese QNAP, have infected over 62,000 devices worldwide. The QSnatch spyware used in the attack prevents firmware updates and requires full factory reset before firmware upgrade for its removal and patching.

- An anti-NATO disinformation campaign has been using compromised news websites in Poland and Lithuania to plant false stories aimed to discredit NATO.

VULNERABILITIES AND PATCHES

- Check Point Research has reported server-side vulnerabilities in the OkCupid dating app, which could allow threat actors to expose users' sensitive data, perform actions on behalf of users and more. As demonstrated in the Ashley Madison 2015 hack, dating apps hold intimate information that can be used for sextortion attacks.
- BootHole, a newly discovered vulnerability (CVE-2020-10713) in the GRUB2 bootloader, threatens billions of Linux and Windows devices. The vulnerability allows attackers to interfere with the boot process preceding the OS startup and potentially receive full control of victim systems.
- A vulnerability in Zoom conferencing platform, which stems from not limiting the number of password entry-attempts, could have allowed hackers to conduct brute-force attacks and enter any private zoom session. Zoom has issued a fix to the problem.
- A critical vulnerability in the WordPress plugin wpDiscuz could allow remote attackers to execute arbitrary code and take over accounts. The plugin, with more than 80K installations, released a fixed version.

  Check Point IPS blade provides protection against this threat (WordPress Suspicious File Upload)
- Cisco has issued a warning concerning a critical flaw in its data center network manager (DCNM) that could let remote attackers log in with admin privileges (CVE-2020-3382). The company issued fixes for this and several other critical flaws.

THREAT INTELLIGENCE REPORTS

- The North Korean APT group Lazarus has developed and used its own custom ransomware, dubbed VHD, indicating its intensions to join the profitable ransomware scene. Researchers attribute VHD to Lazarus since it was used together with the MATA backdoor, a signature tool of Lazarus.

  Check Point SandBlast provides protection against this threat (Ransomware.Win32.VHD)
- Researchers report of a North Korean cyberespionage campaign that targets employees in the US defense and aerospace sector through fake job offers on LinkedIn. The attack is attributed the Lazarus APT group.
- Twitter investigation has revealed that the multiple celebrity account take over attack, which yielded more than $100K, was achieved through phone voice spear phishing (vishing) of its employees. A 17 year-old from Florida has been arrested and identified as responsible for the attack.