Check Point
SOFTWARE TECHNOLOGIES LTD.

Aug 24 - 30, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The New Zealand stock exchange (NZX) has suffered four consecutive days of DDoS attacks, causing severe disruptions, eventually halting trade. Few details have been released regarding the attack. In November 2019 New Zealand's CERT warned financial companies of DDoS attacks with extortion purposes, mentioning Russian-linked APT group Fancy Bear.

- Researchers have found a data leak disclosure post published by the REvil ransomware operators claiming to have stolen sensitive data from US-based Valley Health Systems, including information related to clients, employees, and patients.

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

- The operators of the Latin American banking Trojan Grandoreiro have launched a new campaign targeting Spanish users with emails posing as Spain's tax agency to lure victims to install its payload.

- In an attempt to deploy ransomware in Tesla's Gigafactory in Nevada, a Russian citizen has offered a Tesla employee $1 million for access to company's network. The plan was to distract attention with a DDoS attack while exfiltrating corporate data to be used for extortion. Tesla's employee reported the proposition, resulting in the arrest of the alleged hacker, possibly also behind the attack on travel giant CWT

- Iranian APT group Charming Kitten has been targeting journalists and academics using fake LinkedIn accounts and WhatsApp. Attackers impersonated journalists from DeutscheWelle and Jewish Journal, approached targets over the phone and used compromised news groups' websites to deliver malware.

  Check Point SandBlast and Anti-Phishing provide protection against this threat

- A new Info-stealing malware called Anubis is currently spreading in the wild, targeting Windows systems. The malware is designed to steal system information, credentials, credit card details, and cryptocurrency wallets from infected systems.

  Check Point SandBlast Agent and Anti-Virus provide protection against this threat *(Infostealer.Win32.Anubis).*

VULNERABILITIES AND PATCHES

- Cisco has released updates to fix nine bugs, eight of which were rated high severity, impacting a range of its products. Six of the vulnerabilities reside in Cisco's NX-OS for its Nexus-series Ethernet switches and MDS-series Fibre Channel storage area network switches.
- Microsoft has fixed vulnerabilities in Microsoft Azure Sphere that could be exploited to execute arbitrary code and elevate privileges.
- A new flaw has been found in DVB-T2 set-top boxes THOMSON THT741FTA and Philips DTR3502BFTA. Both devices do not encrypt traffic to and from their servers or connected devices, which can expose the devices to ransomware and botnet attacks.
- Vulnerabilities reported in Slack messaging tool could allow attackers achieve HTML injection, arbitrary code execution, and Cross-Site Scripting (XSS) on latest Slack desktop versions for Mac, Windows and Linux.
- Researchers have reported vulnerabilities in the EMV (integrated chip) credit card standard, allowing actors to perform payment without the use of a PIN code and to postpone notification of declined transactions.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published a thorough review of Gozi, a banker that evolved into a malicious content delivery platform. The publication reviews Gozi's genealogy, from its observation in 2006, through the source code leak in 2010 and to its various branches, common features and prominent strains.

  Check Point SandBlast and Anti-Bot provide protection against this threat *(Trojan.Win32.Gozi)*

- Check Point researchers have exposed a new campaign of the notorious banking Trojan Qbot, involving a new attack method. The malware has been delivered by Emotet in its latest campaign, mostly targeting US and European organizations.

  Check Point SandBlast Agent provides protection against this threat

- Malicious behavior has been reported in an advertising SDK, used by 1,200 apps in the Apple App Store. The SDK, developed by Chinese Mintegral, is said to include modules designed to spy on user activity and log PIIs and URL requests on external servers, steal revenue from other ad networks, and modules to hide this activity and bypass Apple's review process. Mintegral denied the allegations

- The Lemon_Duck cryptominer, reported in February to target IoT devices, is now seeking large enterprise Linux systems. Researchers report a current campaign using XMRig to mine Monero, attempting to infiltrate enterprise networks by brute forcing SSH connections on port 22/tcp.

  Check Point SandBlast provides protection against this threat