June 1 – 7,2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Westech, a US military missile contractor, has been hit by the Maze ransomware after threat actors compromised its network and stole confidential documents from it. It is suspected that the hackers are of Russian origin, and that they may attempt to sell the stolen data to a foreign state.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Maze)*

- Maze ransomware operators have released data belonging to ST Engineering, a global engineering group specializing in aerospace, electronics and marine sectors. The ransomware operators claim to have stolen 1.5TB of data, including documents, contract information, NASA-related files and more.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Maze)*

- The business services giant Conduent has been hit by the Maze ransomware. It is suspected that a vulnerable Citrix server was used to compromise the company's network.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Maze, Citrix Multiple Products Directory Traversal (CVE-2019-19781))*

- The Sodinokibi ransomware operators have published data allegedly stolen from the UK power grid network middleman Elexon. The company managed to restore their data from backups. The attackers may have exploited Pulse Secure VPN to access Elexon's internal network.

  Check Point SandBlast, Anti-Bot and IPS blades provide protection against this threat *(Ransomware.Win32.Sodinokibi; Pulse Connect Secure Cross-Site Scripting (CVE-2019-11507))*

- An unsecured Amazon S3 bucket belonging to a student loan scheme company has exposed over 55,000 call recordings and 25,000 documents containing highly personal details of victims.

- Hackers have hijacked a domain belonging to a Japanese cryptocurrency exchange CoinCheck after managing to access their account at the Oname.com domain registrar. The hijacked domain was used to conduct spear-phishing attacks on customers and alter the main DNS entry of the company domain.

VULNERABILITIES AND PATCHES

- Two critical path traversal vulnerabilities affecting Zoom conferencing software may allow attackers to hack into participants' systems remotely. The vulnerabilities, patched in the latest update, could be exploited to write files to the system by sending specially crafted messages through the chat.
- SAP Sybase Adaptive Server Enterprise software has been found vulnerable to six flaws of different severity levels. The most severe vulnerability, tracked as CVE-2020-6248, allows arbitrary code execution when making database backups. All flaws were patched by the vendor.
- A vulnerability in VMWare Cloud Director has been discovered. The flaw, which may allow an attacker to gain access to sensitive information, is caused by improper handling of input to the Cloud Director.

  Check Point IPS blade provides protection against this threat *(VMware Cloud Director Remote Code Execution (CVE-2020-3956))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has spotted malicious files masquerading as Coronavirus-related medical leave forms to lure victims to open malicious mail attachments.
- Foreign hackers are targeting campaign staff members for US President Donald Trump and Democratic rival Joe Biden ahead of the November US election. Researchers revealed the involvement of two groups, China-linked APT 31 and Iran-linked APT35, in recent spear-phishing campaigns targeting personal Google accounts of individuals working in election campaigns.
- The China-related APT group Cycldek, also known as Goblin Panda, is targeting air-gapped networks to move laterally and exfiltrate sensitive data from protected networks. One of their new tools, USBCulprit, is capable of collecting documents and exporting them to a connected USB drive. The new ability, among others, was used in recent attacks the group conducted against governments in Southeast Asia.

  Check Point Anti-Bot and Anti-Virus blades provide protection against this threat *(Backdoor.Win32.USBCulprit.TC)*
- The eCh0raix ransomware is back after months of inactivity in a new campaign targeting QNAP storage devices. A surge in the number of victims reporting eCh0raix infections was detected.
- A multi-platform ransomware dubbed Tycoon has recently been discovered, after it was used in several highly targeted attacks against education and software companies. The ransomware, which was deployed through internet-exposed RDP servers, uses a Java Image File to evade detection.
- A fake ransomware decryptor for the STOP Djvu ransomware encrypts all of the victim's already encrypted data with another ransomware, called Zorab.

  Check Point Anti-Virus blade provides protection against this threat *(Ransomware.Win32.FakeDecryptor.TC)*