August 31 – September 06, 2020

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- More than a dozen European ISPs have reported DDoS attacks targeting their DNS infrastructure. The attacks reached 300Gbit/s in volume and were part of an extortion attempt, likely related to last week's attacks on the NZ stock exchange and other financial institutions across the world.
- Attackers have gained access to computer networks of the Norwegian parliament, compromising email account of lawmakers and employees. Officials report there is still no knowledge of who is behind the attack.
- The Warner Music Group has suffered a data breach lasting from April until August this year. In a Magecart type attack, several of Warner's US online stores have been compromised and installed with data skimmers, collecting customers' personal and financial information.

  Check Point Anti-Bot provides protection against this threat *(Trojan.Win32.Magecart)*
- A school district in North Carolina has suffered a data breach after having files stolen during an attack by the SunCrypt ransomware operators, causing the district to shut down its networks and halt remote learning.
- India's prime minister's Twitter account has been hacked and, and the hacker tweeted a request for COVID-19 donation along with a bitcoin wallet address. Twitter took action to secure the compromised account and determined the attack was not related to last month's Twitter accounts hack.
- ThiefBot, a new Banking Trojan for Android, has been used in a campaign targeting Turkish users.

  Check Point SandBlast Mobile provides protection against this threat
- Six apps with the Joker malware have been detected and removed from the Google Store, after they had been downloaded 200,000 times. Joker monetizes by sending premium rate SMS messages or conducting purchases through WAT billing. Joker avoided detection by initially submitting clean applications and adding malicious functionalities at later stages.

  Check Point SandBlast Mobile provides protection against this threat

VULNERABILITIES AND PATCHES

- Attackers are currently exploiting a vulnerability in QNAP network attached storage devices (NAS). Input sanitizing failure allows command injection, potentially leading to RCE. QNAP PSIRT addressed the issue in a 2017 update but many devices remain unpatched.

  Check Point IPS provides protection against this threat (QNAP NAS Remote Code Execution)

- More than half a million sites are exposed to an ongoing attack, aiming to exploit a vulnerability in File Manager, a WordPress plugin. The vulnerability allows unauthenticated attackers to upload and execute arbitrary code on WordPress sites. File Manager released version 6.9 with patches for the flaw.

- Cisco has issued a warning concerning a high severity zero-day vulnerability in its router software (CVE-2020-3566) that is actively exploited in the wild and could allow remote attackers to cause memory exhaustion resulting in process instability.

- Magento sites are vulnerable to RCE attacks, stemming from two vulnerabilities in a Magento plugin called Magmi (Magento Mass Import). A patch has only been published to one of the bugs.

- Microsoft has released a batch of Intel microcode-updates for Windows to fix hardware bugs in Intel's CPUs. The updates are not automatically installed through Windows Update and must be setup manually.

- WhatsApp has addressed six previously unpublished vulnerabilities in its iPhone and Android apps, some reported through a Facebook bug-bounty program.

THREAT INTELLIGENCE REPORTS

- Researchers report that the Chinese APT TA413 has deployed a new RAT and continues its campaigns targeting Tibetans. The new RAT, dubbed Sepulcher, has been deployed through spear phishing emails in two campaigns, the first one targeted European diplomatic and legislative bodies.

  Check Point SandBlast Agent and Anti-Virus provide protection against this threat (Trojan.Win32.Sepulcher)

- An Iranian APT, mostly associated with operations in North America and Israel, has been recorded in an attempt to sell access to networks it had previously hacked. The group, previously targeting governmental, business and research entities for espionage reasons, is monetizing by selling information with little intelligence value for the Iranian government.

- In response to a publication by the Russian news agency Kommersant claiming that Russian hackers had obtained voter records of more than 7.6 million American, CISA and the FBI stated they have not seen any cyber-attacks on voter registration databases or any system involving voting this year. Meanwhile, commander of the US Army Cyber Command stated it will increase its focus on offensive influence missions.