January 13 - 19, 2019

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Hackers have stolen personal information in an attack on the Australian P&N bank. The attack focused on the bank's CRM system that stored a great deal of sensitive personal and financial information.
- Australia has experienced a data breach of a bushfire donation site - hackers abused the outdated Magneto CMS using a Magecart script named "ATMZOW", stealing donors' information.
- After more than a week of shutting down operations and working using pen and paper, money transfer agency Travelex is partially restoring operations; Har Shalom Temple in New Jersey is another victim of a Sodinokibi ransomware attack this week, having the entire Temple's network shuttered.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat (Ransomware.Win32.Sodinokibi.TC)
- New Mexico's Public Regulation Commission (PRC) has been hit by ransomware, forcing new requests to be submitted on paper and sent by postal mail.
- Maze ransomware is actively copying victims' data before encrypting their files, using the encrypted data to extort the victims. Maze has released 14GB of data they claim were stolen from the cable manufacturer SouthWire. This publication is part of an alarming trend of new "extortion blogs" where ransomware groups publish the data of victims who would not pay. A similar site has been announced by the Nemty ransomware group.

  Check Point SandBlast Agent and Anti-Bot blade provide protection against these threats (Ransomware.Win.Maze.A; Ransomware.Win32.Nemty.TC)
- The FBI has seized WeLeakInfo, a website that sold access to breached data. The site offered hackers a convenient search option for a name, email or username of a potential target, offering passwords.
- A Hacker has leaked passwords for over half a million servers, routers and IoT devices, allowing remote access to these devices. The hacker used a mass-scanning method, using a DDos booter to scan and find the information.

VULNERABILITIES AND PATCHES

- Microsoft has announced a fix to a major vulnerability in Windows 10's cryptographic engine. The vulnerability (CVE-2020-0601) was exposed by the NSA and is considered critical. Proof of concept exploits have already been published for this vulnerability.

  Check Point IPS and Threat-Emulation blades provide protection against this threat (Microsoft Windows CryptoAPI Spoofing (CVE-2020-0601); Trojan.Wins.CVE-2020-0601)

- A ciritical zero-day vulnerability in Internet Explorer (CVE-2020-0674) allowing remote code execution has been revealed, and had already been exploited in the wild in limited attacks, according to Microsoft.

  Check Point IPS blade provides protection against this threat (Microsoft Internet Explorer Use After Free (CVE-2020-0674))

- A Proof of Concept has been published regarding critical Cisco DCNM flaws (CVE-2019-15975, 15976, 15977).

- Two WordPress plugins have been reported to contain critical bugs, exposing 320,000 websites to potential attacks. Threat actors might use these vulnerabilities to gain administrator control over a website.

- Adobe has released its first security patch of 2020, mostly dealing with Illustrator's arbitrary code execution issue, as well as several other issues.

THREAT INTELLIGENCE REPORTS

- Check Point's 2020 Cyber Security report has been published, surveying the current cyber-attack threats that enterprises face, as well as global and regional attack statistics.

- Threat actors are attacking Citrix servers, exploiting the CVE-2019-19781 vulnerability, then patching infected servers after installing their own backdoor, blocking out competing malicious actors from abusing the bug. Researchers have dubbed the attack NOTROBIN, and noted that the hackers retained access using a secret passphrase.

  Check Point IPS blade provides protection against this threat (Citrix Multiple Products Directory Traversal (CVE-2019-19781))

- Ryuk Ransomware has been shown to use the "Wake-on-Lan" (WoL) feature to turn on powered off devices, then attempt to encrypt them. The Ransomware will use an infected computer to send a WoL packet based on the device's ARP table, looking for home addresses, and waking potential victim computers, extending its spread throughout the network.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat