June 8 – 14, 2020

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Delhi-based hack-for-hire group BellTroX has allegedly targeted thousands of high-profile individuals and hundreds of organizations worldwide in a seven-year long campaign. The group used phishing kits to steal sensitive data from the victims and conduct commercial espionage on behalf of their clients.
- The Japanese gaming giant Nintendo reveals hackers have breached 300,000 accounts and may have gained access to personal information, including date of birth and email addresses. The accounts were abused to purchase features and virtual coins in popular games via the connected PayPal accounts.
- Hackers are targeting executives of a German task force supplying face masks and medical equipment against COVID-19. The hackers launched a spear-phishing campaign to steal Microsoft login credentials, targeting over 100 senior executives in 40 organizations.
- Threadstone Advisors, a US-based advisory firm, has been hit by the Maze ransomware. The attackers also stole data from the company's compromised servers, and threaten to publish it unless the ransom demands are met.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.Maze)*
- The City of Florence, Alabama has been hit by a ransomware attack, forcing them to pay $300,000 in ransom to get their data decrypted. The hackers have reportedly waited for over a month after breaching the city's system before deploying the DoppelPaymer ransomware.

  Check Point SandBlast and Anti-Bot blades provide protection against this threat *(Ransomware.Win32.DoppelPaymer)*
- The city of Knoxville, Tennessee, has been forced to shut down its computer network and some of its services after an undisclosed ransomware attacked their systems.
- A1 Telekom, the leading mobile network operator in Austria, has revealed that they had fought a network intrusion for six months, after hackers breached their systems and planted multiple backdoors in November 2019. It is suspected that the intruders were members of the China-linked APT Gallium.

VULNERABILITIES AND PATCHES

- SMBleed, a new vulnerability affecting the SMB protocol, may allow attackers to leak kernel memory remotely and execute arbitrary code. To exploit the flaw, an attacker can send a specially crafted packet to a targeted SMBv3 server. The latest Windows update provides a patch for this vulnerability.

  Check Point IPS blade provides protection against this threat (Microsoft Windows SMBv3 Client/Server Information Disclosure (CVE-2020-1206))

- SGAxe and CrossTalk, two new attacks against modern Intel processors, have been discovered. The SGAxe attack may allow attackers to extract sensitive data from SGX enclaves, and the CrossTalk attack may lead to leakage of information across CPU cores. Intel released a microcode update to the relevant software vendors.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have addressed the possible security and privacy risks users of the COVID-19 contact-tracing applications face, from GPS tracking and data collection to fake applications and unauthorized data theft.

  Check Point SandBlast Mobile provides protection against this threat

- Check Point Research team has found a commercial software tool called CloudEye offered by an Italian company, which serves as a malware dropper. While their operations is allegedly legitimate, the company seems to be making $500,000 a month from sales to cybercriminals.

  Check Point SandBlast provides protection against this threat (Dropper.Win.CloudEyE.)*

- Microsoft warns Kubernetes users of a hacking campaign that targets Kubeflow, a machine learning toolkit, aiming at delivering a cryptocurrency miner on internet-facing instances. Threat actors behind this campaign initially scan the Internet for exposed Kubeflow admin panels, and use them to move laterally and reach into the Kubernetes cluster to run an XMRig miner.

- Russia-linked Gamaredon APT is reportedly using a VBA macro tool targeting Microsoft Outlook that creates custom emails with malicious documents and uses the targets' email accounts to send spear-phishing emails to their contacts.

  Check Point Anti-Bot blade provides protection against this threat (Botnet.Win32.Gamaredon; Trojan.Win32.Gamaredon)

- Researchers have uncovered a malware, dubbed Stealthworker, targeting Windows and Linux servers running popular web services and platforms such as Magento, WordPress, Joomla and Drupal. The hackers use the infected hosts to launch brute force attacks against other systems.

  Check Point Anti-Bot blade provides protection against this threat (Trojan.Win32.Stealthworker)