November 9-15, 2020

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has further investigated the newly revealed 'Pay2Key' ransomware, tracing several ransom payments to an Iranian cryptocurrency exchange, and concluded that the malware, which focuses on Israeli organizations, is most likely of Iranian origin.

  Check Point SandBlast Agent provides protection against this threat (Ransomware.Win32.Pay2Key)

- BigBasket, India's largest online food and grocery store, has suffered a data breach, leading to the exposure of the personal credentials of over 20 million customers. The records, that include email and home addresses, hashed passwords and dates of birth, are offered for sale on the dark web for over 40,000 USD.

- The North Face, an American outdoor recreation product company, has detected a credential-stuffing attack targeting its official website. The company has reset an undisclosed number of customer accounts.

- Nation-sponsored APT groups, including the infamous North Korean Lazarus Group and Russian FancyBear, have been targeting institutions involved with COVID-19 vaccine and treatment development. The most common tactic observed in this attack wave is spear-phishing using pandemic-related themes.

- New espionage operation has been leveraging a custom-made malware toolset in a campaign targeting financial institutions in South Asia and global entertainment companies. The campaign is carried out by a 'Hackers-for-Hire' group and was most likely commissioned by a well-funded organization.

- The FBI has published a previously classified alert warning against the leakage of proprietary source code from US government agencies as well as companies in the technology, finance, manufacturing sectors, as a result of a misconfiguration of instances of the SonarQube code review tool.

- A new modular backdoor has been discovered by researchers, designed to collect payment information from Oracle Restaurant Enterprise Series Point-of-Sale software. Its targets include bars, restaurants and hotels worldwide.

VULNERABILITIES AND PATCHES

- Google has patched two high severity zero-day vulnerabilities in the Chrome web browser for Linux, Windows and Mac. Exploits to both flaws, that were disclosed to Google by anonymous sources, exist in the wild. CVE-2020-16013 is an inappropriate implementation flaw leading to remote code execution.
- Intel has published 40 security advisories addressing flaws in a variety of products, including its Processor, Active Management Technology, Data Center Manager Console and NUC firmware. Among them is a critical flaw in Intel Wireless Bluetooth (CVE-2020-12321), allowing privilege escalation and Denial of Service.
- Adobe has released updates for Adobe Connect and Adobe Reader Mobile (ARM), patching 3 new vulnerabilities, including CVE-2020-24441, a flaw in ARM that could lead to sensitive information disclosure.
- Some 112 vulnerabilities have been addressed in Microsoft's latest security update, for products including Microsoft Office, Exchange Server, Azure Sphere, Teams and more. Among these is a zero-day flaw in Windows Kernel assigned CVE-2020-17087, which might lead to local privilege escalation.

  Check Point IPS provides protection against this threat *(Microsoft Windows Kernel Local Elevation of Privilege (CVE-2020-17087))*

THREAT INTELLIGENCE REPORTS

- Check Point has released its predictions towards the 2021 threat landscape, revolving around the influences of the COVID-19 pandemic, attackers' revolution and future platforms. Researchers predict that attackers will utilize deepfake techniques to create targeted content integrated into cyber-attacks.
- Researchers reveal that the Ragnar Locker ransomware group has recently integrated Facebook into its payment extortion process, using hacked account to distribute advertisement meant to publicly pressure the victims into paying the ransom.

  Check Point SandBlast Agent provides protection against this threat *(Ransomware.Win32.Ragnar)*
- Series of critical security flaws has been revealed by researchers, following an investigation of up-to-date implementations of DNS Cache Poisoning Attacks. These flaws leverage network side channels that exist in all operating systems, enabling an attacker to inject a malicious DNS record into a DNS cache.
- An article reviews the disruption efforts taken by government agencies as well as private security corporations against the Trickbot botnet between September-November 2020, and its current activity rate.

  Check Point SandBlast Agent and Anti-Bot provide protection against this threat *(Trojan-Banker.Win32.TrickBot)*
- Researchers have observed an increase in the rate of attacks targeting the manufacturing sector. Common attack methods include ransomware capable of disrupting industrial processes, confidential manufacturing information theft and vulnerabilities that could lead to loss of control over manufacturing environments.