Check Point
SOFTWARE TECHNOLOGIES LTD.

April 20-26, 2020

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point has investigated a Business Email Compromise attack targeting a financial organization and their business partner. The attacking group, the Florentine Banker, manipulated four transactions of over 1 million GBP into their own bank accounts using advanced phishing tactics to target the mail accounts of key individuals inside the victim companies and manipulating email correspondences.

  Check Point CloudGuard SaaS provides protection against this threat

- Hackers have abused the login system of Nintendo, resulting in the leakage of 160,000 user accounts. The breach was discovered after a number of users complained of their accounts being accessed; many of the hacked accounts were abused to purchase features and virtual coins.

- A database containing 400,000 payment card records belonging to South Korean and US banks and financial companies has been uploaded to a hacking forum. The source of the data remains unknown.

- SeaChange, an international supplier of video delivery software solutions, has been hit by the Sodinokibi ransomware. The attackers apparently exploited an unpatched Pulse Secure VPN server using CVE-2019-11510 and stole documents from the company prior to deploying the ransomware.

  Check Point Anti-Bot and IPS blades provide protection against these threats (Ransomware.Win32.Sodinokibi, Pulse Connect Secure File Disclosure (CVE-2019-11510))

- A data dump containing 25,000 email credentials allegedly belonging to National Institutes of Health, World Health Organization, Gates Foundation and other organizations has been discovered. The leaked credentials appear to be an aggregation of previously-breached usernames and passwords.

- The city of Torrance, California, has suffered a DoppelPaymer ransomware attack. The attackers stole 200GB of data prior to deploying the ransomware, and demanded $689,000 in ransom.

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

- Over 309 million Facebook profiles are being offered for sale on the dark web. The data, which did not include passwords, was collected by illegal scraping activity abusing Facebook's API.

VULNERABILITIES AND PATCHES

- Two critical vulnerabilities have been discovered in the default mailing app installed on iPhones and iPads, and might have been exploited for two years by attackers targeting high-profile victims. The flaws can be exploited by sending a crafted email message, which may allow the attacker to take control over the device.

  Check Point CloudGuard SaaS provides protection against this threat

- IBM Data Risk Manager has been found vulnerable to four Zero-Day exploits which, when chained together, may allow an unauthenticated attacker to execute code as root. A Proof-of-Concept exploit was published.

  Check Point IPS blade provides protection against this threat *(IBM Data Risk Manager Command Injection)*

- Unpatchable hardware vulnerability in FPGA chips may allow an attacker to break bitstream encryption, modify functionality and even implant hardware Trojans.

- Researchers have discovered a method to abuse anti-virus software to execute a malicious file with high-level permissions. The flaw resides in the small timeframe between the anti-virus's initial file scan and the cleanup operation. An attacker can initiate a race condition to disable the anti-virus software during this timeframe.

THREAT INTELLIGENCE REPORTS

- The FBI has issued a warning for US health organizations against Covid-19-related phishing attempts. According to the FBI and other official agencies, threat actors are actively attempting to send phishing attempts over email, containing malicious Microsoft Word Documents, 7-Zip compressed files, Microsoft VBS files, Java and Executables.

- A malware botnet comprising over 35,000 compromised Windows machines has been taken down after being active since May 2019. The botnet, which was named "Victory Gate", was mainly operated for the purpose of mining Monero cryptocurrency, with victims in public and private organizations, mostly from Latin America. Victory Gate propagates via removable devices such as USB drives, which install a malicious payload into the system.

  Check Point Anti-Bot blade provides protection against this threat *(Botnet.Win32.VictoryGate)*

- China-linked APT Winnti has targeted a South Korean video gaming company called Gravity as well as a German chemical company in recent campaigns. The group, typically motivated by espionage and financial gain, has deployed a malware containing a unique C2 communication method that abuses the iodine source code, an open-source software used for tunneling IPv4 data through a DNS server.

  Check Point Anti-Bot blade provides protection against this threat *(Backdoor.Win32.Winnti)*