June 13 – 19, 2022

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has exposed an Iranian spear-phishing operation targeting high profile Israeli and US executives. As part of their operations, the attackers take over existing accounts of the executives and create impersonating accounts to lure their targets into long email conversations. The operation aims at stealing personal information, passport scans, and access to email accounts.

- CERT Ukraine has issued a warning concerning Russian hackers, possibly the state-sponsored APT group Sandworm, launching attacks exploiting the Follina critical vulnerability (CVE-2022-30190) in Microsoft Windows Support Diagnostic Tool. The campaign leverages malicious emails with DOCX attachments targeting media and news outlets in Ukraine.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat (Microsoft Support Diagnostic Tool Remote Code Execution (CVE-2022-30190); Exploit.Win.Follina*; Dropper.Win32.Sandworm)

- The China-linked Gallium APT group (aka Softcell) has been targeting financial organizations and government entities over the past year, specifically in a number of Southeast Asian countries in addition to Russia, Belgium and Australia. The group has been leveraging a new remote access Trojan called "PingPull" to perform espionage activities.

- The RansomHouse extortion group has claimed responsibility on an attack against Shoprite Holdings, Africa's largest supermarket chain. The company disclosed that customers' personal information might have been compromised. RansomHouse posted on their extortion site samples of what they claim to be 600GB worth of stolen data from the retailer.

- Kaiser Permanente, a US based healthcare provider, has revealed that a data breach through an employee's email account recently exposed sensitive data of over 69,000 of their members.

- The largest ever-recorded HTTPS DDoS attack has recently been mitigated, with 26 million request per second. The attack targeted a Cloudflare customer and originated from cloud service providers rather than residential internet service providers, indicating the use of hacked virtual machines.

- Taiwanese Network Attached Storage (NAS) Company QNAP has revealed it has been investigating a Deadbolt ransomware attack on its users. In addition, a new wave of eCh0raix ransomware (aka QNAPCrypt) attacks has been increasingly targeting QNAP devices.

  Check Point Threat Emulation provides protection against these threats (Ransomware.Wins.deadbolt; Ransomware.Win32.Ech0raix)

VULNERABILITIES AND PATCHES

- Microsoft has issued a fix to address the critical Follina vulnerability (tracked CVE-2022-30190) that is currently being exploited, recommending users to urgently update and patch.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat *(Microsoft Support Diagnostic Tool Remote Code Execution (CVE-2022-30190); Exploit.Win.Follina*)*

- Citrix is urging users to update to protect against a critical Application Delivery Management (ADM) flaw tracked CVE-2022-27511, which could let remote unauthenticated hackers reset admin passwords on unpatched systems.

- A new high-severity vulnerability tracked CVE-2022-27924, affecting Zimbra email solution, has been disclosed. The flaw could be leveraged by unauthenticated attackers to steal login credentials without user interaction.

THREAT INTELLIGENCE REPORTS

- The US Department of Justice announced it has disrupted the Russian RSocks malware botnet's infrastructure used to hack millions of machines, mobile and IoT devices worldwide for use as proxy servers.

- The BlackCat ransomware gang now has a website available to let their victims' customers and employees verify if their data was stolen in a ransomware attack, as part of double extortion schemes. Threat actors aim for the employees to apply further pressure on the initial victim to pay the ransom and have their personal data removed from the web. BlackCat is currently targeting Microsoft Exchange servers with exploits leveraging unpatched vulnerabilities.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win.BlackCat)*

- A global Interpol operation codenamed "First Light 2022" was conducted against crime groups behind telecommunications and social engineering frauds. Law enforcement seized 50 million dollars of illicit funds and arrested thousands of operators, fraudsters and money launderers.

- A new Android malware named MaliBot has been spotted targeting users in Spain and Italy. The infostealer disguises itself as crypto mining applications under different names and focuses on stealing financial information, crypto wallets and more personal data.

  Check Point Harmony Mobile provides protection against this threat