Check Point Research

WEEKLY INTELLIGENCE REPORT

August 22 –28, 2022

TOP ATTACKS AND BREACHES

- Montenegro has suffered a large-scale cyber attack, affecting multiple government services. According to some sources, it potentially affected critical infrastructure, transportation and telecommunications. Montenegro's security agency has claimed that the attack was coordinated and persistent, and has concluded with certainty that it was conducted by Russia.

- Developers of libraries in the Python Package Index (PyPi) have been victims of a phishing campaign. The attackers sent emails designed to appear as official messages from PyPi, which supposedly required the developers' credentials to implement security safeguards. The affected libraries were injected with malicious code, in what PyPi claimed is the first phishing attack targeting its platform.

- A French hospital, CHSF, has been compromised by a ransomware attack, demanding $10M. The hospital has been forced to divert non-critical patients, and treat patients without the help of computer systems. According to French police, the Lockbit ransomware group is behind the attack.

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

- The Iran-affiliated threat group Mercury has targeted multiple Israeli organizations in the past few weeks. The group has exploited Log4j-2 vulnerabilities in the SysAid platform in order to gain initial access to the organizations, and deployed several tools to establish persistence and spread laterally in the infected environments.

  Check Point IPS provides protection against this threat (Apache Log4j Remote Code Execution (CVE-2021-44228); Apache Log4j Remote Code Execution (CVE-2021-44832); Apache Log4j Remote Code Execution (CVE-2021-45046))

- Popular password-management software developer LastPass has announced that its environment had been breached, resulting in portions of the source code being stolen. LastPass claims that users' master-passwords are not stored in the company's environment, and that therefore no user information was compromised.

- Plex streaming service has confirmed that its database had been breached, leaking usernames, email addresses and hashed passwords of over 15 million subscribers of the service. Plex has issued password resets for its customers following the leak.

- The Dominican Republic's Ministry of Agriculture has been affected by a Quantum ransomware attack.

VULNERABILITIES AND PATCHES

- Atlassian has patched a critical vulnerability in Bitbucket Server and Data Center. The vulnerability could allow attackers with access or read permissions to execute arbitrary code on Bitbucket repositories.
- GitLab has published new versions of GitLab CE and EE, which include security fixes to a critical vulnerability allowing remote code execution via the Import from GitHub API endpoint.
- Cisco has released security patches to software vulnerabilities affecting its products. Exploitation of some of the vulnerabilities could allow attackers to gain remote access to users' systems.
- Mozilla has released security updates addressing multiple vulnerabilities in Firefox and Thunderbird.

THREAT INTELLIGENCE REPORTS

- Check Point Research has discovered an active cryptocurrency mining campaign imitating "Google Translate Desktop" and other free software to infect PCs. Created by a Turkish speaking entity called Nitrokod, the campaign counts 111,000 downloads in 11 countries since 2019.

  Check Point Harmony Endpoint provides protection against this threat

- A study of the recent phishing campaign dubbed "0ktapus", targeting Cloudflare and Twilio employees, has revealed that over 9,000 accounts were affected in over 130 organizations. The threat actors exploited the stolen credentials in order to deliver supply chain attacks.
- Reports detailing the threat of emerging ransomware variants BlueSky and Black Basta have been published. Active since 2022, analysts estimate these threats to gain popularity in the upcoming months.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats

- 'MagicWeb', a post-compromise technique used by APT29 (Cozy Bear, Nobelium), modifies a legitimate DLL in affected environments to bypass AD FS and allow attackers to sign in as any user, with any claims.
- Analysis of Hyperscrape, a spyware tool used by Iranian group APT35 (Charming Kitten) has been published. After gaining access to the target's session or credentials, the tool allows automated scraping of the user's email accounts, specifically targeting Gmail, Yahoo Mail, and Outlook.

  Check Point Threat Emulation provide protection against this threat *(HackTool.Win32.HYPERSCRAPE.TC)*

- An analysis of GoldDragon malware, used by North-Korean APT group Kimsuky to target South-Korean diplomats, professors and researchers, has been published. Delivered via spear-phishing, the payload is highly targeted, and will be downloaded only when accessed by predetermined email addresses.

  Check Point Anti-Bot provides protection against this threat *(Trojan.Win32.Kimsuky)*