Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Iranian Hacktivist group 'Black Reward' claim to have breached Iran's government and exfiltrated data related to the country's nuclear program. After the group's demands to release political prisoners were not met, the group eventually released 50GB of allegedly sensitive data. Iran's nuclear agency confirmed the breach, but claim the perpetrator was a foreign country.

- Over 2 TB of information related to more than 65,000 of Microsoft's customers have been exposed by security researchers in an event dubbed 'BlueBleed'. The leak was caused by a misconfigured Azure Blob Storage which allowed remote unauthorized access for a long period of time.

- Canadian members of parliament have been urged to change their email passwords, after a cyber attack affected the servers of the Canadian parliament. Though the nature of the attack has not been disclosed, it is believed to likely be a ransomware incident.

- Several Australian companies have been breached - The country's largest health insurance firm, Medibank, froze trading on the Australian stock exchange after confirming a 200GB data breach; In a breach of wine retailer Vinomofo's network data of over 500,000 customers was leaked; an attack on energy company EnergyAustralia exposed payment data of hundreds of the company's customers.

- Global retail corporation METRO has faced IT infrastructure outage following a ransomware attack, causing disruptions and delays to both physical and online sales.

- Researchers have observed various threat groups attempting to exploit a recently disclosed remote code execution vulnerability in VMware - CVE-2022-22954.

  Check Point IPS provides protection against this threat *(VMware Workspace Remote Code Execution (CVE-2022-22954))*

- Russian-affiliated hacktivist group 'Killnet' has launched a DDoS attack against government websites in Bulgaria, causing them to become inaccessible. Killnet said that Bulgaria was targeted due to its "betrayal to Russia" and the supply of weapons to Ukraine.

- Researchers have identified a sophisticated spyware campaign targeting government organizations in Hong Kong, attributed to China. The spyware, dubbed 'Spyder Loader', has been successfully active in some of the organizations' networks for over a year.

VULNERABILITIES AND PATCHES

- A critical remote code execution vulnerability has been discovered in Apache Commons, and dubbed 'Text4Shell' (CVE-2022-42889). The vulnerability is considered less easily exploitable than its namesake from last year, 'Log4Shell' (CVE-2021-44228), and less organizations are exposed.

  Check Point CloudGuard AppSec and IPS provide protection against this threat (Apache Commons Text Remote Code Execution (CVE-2022-42889))

- Oracle has published its Critical Patch for the month of October. The patch includes fixes to 370 security vulnerabilities in many of the company's products.

- Cisco has released a security patch for Cisco Identity Services Engine. The update addresses vulnerabilities that could potentially allow an attacker to gain control of targeted systems.

- Mozilla has released version 106 of Firefox. The new version includes security fixes for 6 vulnerabilities which could lead to information disclosure, denial of service or memory corruption.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published an analysis of the Black Basta ransomware, which extorted more than 89 high-profile organization since May 2022. Black Basta employs multiple tools to verify that is not being debugged or run on a sandbox before activating in order to avoid detection, and uses multi-threading and partial file encryption to minimize the length of the encryption process.

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

- The US CISA warns against the threat of ransomware group Team Daixin. The group has lately been targeting American companies in the healthcare sector.

  Check Point Threat Emulation provides protection against this threat

- Iran's 'Domestic Kitten' APT group has been utilizing Android malware in their surveillance operation against Iranian citizens, according to researchers. The malware masquerades as a legitimate translation app, and contains a wide variety of spying tools.

  Check Point Harmony Mobile provides protection against this threat