Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research (CPR) revealed a large spike in attacks committed by advanced persistent threat groups (APTs) around the world, using lures utilizing the war between Russia and Ukraine. Most of the attacks started with spear-phishing emails that contained documents with malicious macros dropping malware such as Loki.Rat backdoor.

  Check Point Threat Emulation provides protection against this threat (InfoStealer.Wins.Machete)

- The Russian threat group COLDRIVER targeted one of NATO's Centres of Excellence military training organizations, as well as multiple Eastern European countries, using phishing attacks to steal data.

- Security researchers discovered a new spear-phishing campaign that took place in Russia and targeted dissenters with opposing views to those promoted by the government. Victims were lured to open a malicious attachment or link that infected them with Cobalt Strike.

  Check Point Threat Emulation and Anti-Bot provide protection against this threat (Trojan.Win32.CobaltStrike)

- The Pakistan-based threat group APT36 conducted a new campaign against the Indian government. The group used the laced Kavach authentication apps, which are used by the Indian military and other government agencies to access critical IT systems.

- Cybercriminals are compromising WordPress sites to insert a malicious script that uses visitors' browsers to perform distributed denial-of-service (DDoS) attacks on Ukrainian targets.

- US photography company Shutterfly disclosed a data breach after suffering from a Conti ransomware attack that occurred on December 2021.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Win32.Conti)

- A bug in Palo Alto Networks customer support tickets exposed information belonging to thousands of customers.

- CISA and the US Department of Energy released a joint warning of attacks against internet-connected uninterruptible power supply (UPS) devices utilizing default usernames and passwords. Organizations can mitigate such attacks by removing management interfaces from the internet.

VULNERABILITIES AND PATCHES

- Security researchers discovered a zero-day vulnerability in the Spring framework. The flaw, dubbed Spring4Shell, could allow an unauthenticated attacker to take control of a targeted system remotely. Users are recommended to upgrade to versions 5.3.18 or later and 5.2.20 or later.

  Check Point IPS, Harmony Endpoint for Linux and CloudGuard Containers Security provide protection against this threat *(Spring Core Remote Code Execution (CVE-2022-22965); Exploit_Linux_Spring4Shell_B; Exploit_Linux_Spring4Shell_A)*

- Apple provided urgent fixes for two zero-day vulnerabilities that were exploited in the wild and affect its mobile and desktop operating systems. The flaw tracked as CVE-2022-22675 could allow an application to execute arbitrary code with kernel privileges.

- Trend Micro fixed CVE-2022-26871, a vulnerability in its Apex Central product management console, which could allow a remote attacker to execute arbitrary code on the compromised system. Trend Micro observed active attempts of exploitation of this flaw in the wild.

- The DevOps platform GitLab has released an update addressing CVE-2022-1162, which could allow an adversary to seize control of accounts.

- Zyxel has pushed security updates for a critical vulnerability tracked as CVE-2022-0342. The flaw could allow an attacker to bypass the authentication and obtain administrative access to the device.

THREAT INTELLIGENCE REPORTS

- Check Point Research (CPR) observed an increase in global cyberattacks globally in the past month. Additionally, in the past week, CPR observed a 39% rise in cyberattacks against Ukraine and a 17% rise in cyberattacks against Russia.

- The Hive ransomware group was observed using a new obfuscation technique involving IPv4 addresses and a series of conversions that execute shellcode which leads to downloading Cobalt Strike beacons.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Ransomware.Win32.Hive; Trojan.Win32.CobaltStrike)*

- Researchers uncovered a new Russia-linked Android malware that might be related to the Russia-based threat group Turla. The app is able to access the device's location and spy on it, while it is concealed from unaware users.

- A new malware dubbed BlackGuard is being sold on Russian-speaking hacking forums. The malware works as a malware-as-a-service and is capable to steal information and evade detection.