TOP ATTACKS AND BREACHES

- Check Point Research has investigated the attack against Iranian broadcasting that occurred in late January. CPR was able to discover part of the tools that were utilized in this operation, including the evidence of the usage of a destructive wiper malware.

- Check Point Research has discovered a new implementation of the Trickbot banking Trojan. CPR counts over 140,000 machines infected by Trickbot since November 2020, as the threat actors try stealing credentials to financial and other services provided by 60 well-known corporations, including Amazon, Microsoft, Google and PayPal.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat

- Ukraine has been at the center of a series of targeted DDoS attacks on its armed forces, defense ministry, public radio and national banks websites. The US Government has officially attributed the attacks to Russia's Main Directorate of the General Staff of the Armed Forces.

- An Iran affiliated threat actor called "TunnelVision" has actively been exploiting VMware Horizon and deploying ransomware on US and Middle-East based targets. The group has been leveraging 1-day vulnerabilities including Fortinet FortiOS, ProxyShell and Log4Shell.

  Check Point IPS provides protection against these threats *(VERS_Fortinet FortiOS Directory Traversal (CVE-2018-13379); Microsoft Exchange Server Remote Code Execution (CVE-2021-34473); Apache Log4j Remote Code Execution (CVE-2021-44228))*

- The FBI has announced that the BlackByte ransomware gang successfully broke into US critical infrastructures networks from several organizations in the past three months.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Win32.BlackByte)*

- State sponsored threat actors affiliated with the Russian government have been targeting US cleared defense contractors in cyber-espionage campaigns for at least two years. Attackers extracted confidential data related to the state's defense and intelligence programs and capabilities, while leveraging known vulnerabilities including: CVE-2018-13379, CVE-2020-0688 & CVE-2020-17144.

  Check Point IPS provides protection against these threats *(VERS_Fortinet FortiOS Directory Traversal (CVE-2018-13379); VER1 Microsoft Exchange Server Remote Code Execution (CVE-2020-0688); Microsoft Exchange Memory Corruption (CVE-2020-17144))*

VULNERABILITIES AND PATCHES

- A new zero-day vulnerability has been discovered in Magento Open Source and Adobe Commerce platforms. The critical flaw tracked as CVE-2022-24087 could be exploited to achieve remote code execution (RCE) from an unauthenticated user.
- An arbitrary backup download vulnerability in the UpdraftPlus plugin has been discovered and patched, affecting over 3 million WordPress websites. If exploited, the flaw could allow low privileged users to download the site's latest available backups, including usernames and hashed passwords.
- Cisco has patched a high severity flaw tracked as CVE-2022-20653 that could allow a remote hacker to crash Cisco Secure Email appliances with weaponized emails.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have discovered that hackers are dropping malicious executable files in Microsoft Teams conversations. The file writes data to the Windows registry, installs DLL files and creates shortcut links that allow the program to self-administer.

  Check Point Harmony Email provides protection against this threat

- Researchers have revealed how a glitch in a Saudi activist's iPhone led them to evidence that the device was compromised with NSO's spyware Pegasus. This led to the discovery of TTPs used by Pegasus, namely sending malicious images over invisible text messages, and the exposure of thousands of iPhone users who were targeted.
- Top members of the Trickbot gang are now part of the Conti Ransomware operation. Conti has been working mostly with trusted/known affiliates in the past, which allowed them to better avoid law enforcement.

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

- CISA warns US leaders of critical infrastructures organizations to increase vigilance and resilience due to high risk of being targeted by foreign influence campaigns, with misinformation, disinformation and malformation (MDM) tactics.
- A new botnet written in Go language has emerged and has been targeting Windows machines. Named "Kraken", it can download and execute secondary payloads on the target and can extract data, execute shell command, steal cryptocurrencies, take screenshots while persevering in the systems.