TOP ATTACKS AND BREACHES

- North Korean government connected group initiated in March 2022 a spear-phishing campaign against journalists who specialize in the North Korea coverage. The group used Goldbackdoor malware that is linked to malware families that are attributed to APT37.
- Threat actor affiliated with a Chinese government targeted Russian officials during March 2022, with an updated version of PlugX RAT; a Windows backdoor that has been used by several Chinese state-sponsored actors over the years.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (RAT.Win.PlugX)
- A pro-Russian hacktivist group known as Killnet carried a series of DDoS attacks on public Romanian websites managed by the state entities.
- The Ukrainian CERT warns of an ongoing, yet unaffiliated, DDoS campaign targeting pro-Ukraine sites and the government web portals, by compromising WordPress sites.
- A 15.3 million request-per-second DDoS attack was recorded by the internet infrastructure company Cloudflare, marking it one of the largest HTTPS DDoS attacks ever.
- Rocket Kitten, Iranian state affiliated group, has been observed exploiting a recently patched VMware RCE vulnerability (CVE-2022-22954) to gain initial access and deploy a penetration testing tool on vulnerable systems.

  Check Point IPS provides protection against this threat (VMware Workspace Remote Code Execution (CVE-2022-22954))
- Threat analysts have revealed a recent campaign that uses the RIG Exploit Kit to deliver RedLine stealer malware – an info-stealing malware popular on the Russian Underground. The campaign relied on the Exploit Kit leveraging CVE-2021-26411 through compromised websites.

  Check Point IPS provides protection against this threat (Microsoft Internet Explorer Memory Corruption (CVE-2021-26411))
- FBI warns of BlackCat ransomware after that breached over 60 organizations worldwide.

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

VULNERABILITIES AND PATCHES

- Microsoft addressed a chain of critical vulnerabilities found in the Azure Database for PostgreSQL Flexible Server that could allow attackers to escalate privileges and gain access to other customers' databases after bypassing authentication.
- Microsoft disclosed a set of two privilege escalation vulnerabilities in the Linux operating system called "Nimbuspwn" (tracked as CVE-2022-29799 and CVE-2022-29800) which could allow threat actors to deploy payloads and perform other more sophisticated actions via arbitrary root code execution.
- QNAP is working on updating QTS and QuTS operating systems after major code execution related security issues were disclosed.
- A logical flaw that could allow threat actors to pass off suspicious malicious libraries as legitimate was disclosed in NPM, the default package manager for the Node.js JavaScript runtime environment.

THREAT INTELLIGENCE REPORTS

- Check Point Research published an overview of the ransomware economy to uncover the situation from the point of view of both the cybercriminal gangs and victim organizations. CPR reveals a 24% increase in ransomware attacks Year-over-Year, and the estimation that the collateral cost of a ransomware attack for victims is 7 times higher than the paid ransom.
- Microsoft published a report about Russian attacks against Ukraine since the war launch. The report mentions six separate Russian governmental groups that carried out 237 cyberattacks against Ukraine.

  Check Point Harmony Endpoint and Threat Emulation provide protection against those threats (Trojan.Wins.CaddyWiper, Trojan-Downloader.Win.Industroyer2, Trojan.Wins.IsaacWiper)
- Researchers state that a newly discovered malware loader called Bumblebee is likely the latest addition to the Conti gang, designed to replace the BazarLoader backdoor used to deliver ransomware payloads.
- The REvil operation returns to life, after the shut down in October 2021, this based on discovery of a REvil sample used by the new operation, and as their shame blog came back to life.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Win.Revil)
- Following Microsoft's decision to disable Visual Basic for Applications (VBA) macros by default, Emotet returns while attempting to develop new attack and methods for compromising Windows systems.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Trojan.Wins.Emotet)