TOP ATTACKS AND BREACHES

- Check Point Research has found sensitive data of a number of mobile applications exposed and available to anyone. By searching VirusTotal, CPR found 2113 mobile applications whose databases were unprotected and exposed throughout the course of a three month research study.

  Check Point CloudGuard for Application Security provides protection against this threat

- Check Point Research reveals how hackers performed flash loan attacks to claim free tokens on ApeCoin Cryptocurrency, fraudulently earning millions of dollars.

- Check Point Research has spotted several ads and sites on the Darknet which aim at raising money for the Ukrainian people on a cryptocurrency basis and appear to be fraudulent.

- TransUnion South Africa has been victim of a breach in which the hacker group named N4aughtysecTU stole 4TB of data. Attackers who claim to be based in Brazil are demanding a $15 million ransom over the sensitive data which includes credit score, banking details and ID numbers.

- A DDoS attack has targeted several Israeli Government websites, rendering portals inaccessible for a short time. The attack was not yet officially attributed.

- A new wiper malware has been discovered to be used in attacks targeting Ukrainian organizations. Dubbed “CaddyWiper”, it is designed to damage the targeted system and delete data, programs, hard drives and more.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Win.TouchTrapFiles.A)*

- Chinese state-sponsored APT actors are conducting cyber-attack against Ukrainian governmental targets in an attempt to collect information on the ongoing war with Russia.

- Threat actors are spreading fake Antivirus and “critical security updates” for Windows through an email phishing campaign that imitates Ukrainian government organizations, to lure Ukrainian victims into downloading the attachment. Once downloaded, the file named “BitdefenderWindowsUpdatePackage.exe.” drops Cobalt Strike beacons and other malware.

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

VULNERABILITIES AND PATCHES

- Seven remote code execution and DoS vulnerabilities have been found in ClickHouse DBMS. By triggering the flaws, a threat actor could crash the ClickHouse server, leak memory content or trigger remote code execution.
- A vulnerability tracked CVE-2022-0811, "cr8escape", has been discovered in the Kubernetes container engine CRI-O, and could be exploited to execute malware, exfiltrate data and perform lateral movement.
- An unpatched zero-day flaw in PHP-based HTML to PDF converter dompdf has been unveiled. If exploited it could lead to remote code execution in certain configurations.

THREAT INTELLIGENCE REPORTS

- Check Point Research has updated statistics on cyber attacks observed around the Ukraine-Russian conflict. The last 7 days showed the highest number of overall cyber attacks, not only since the advent of the conflict, but also the beginning of the year. In Ukraine, the average weekly attacks per organization last week were 20% higher than before the beginning of the conflict.
- Researchers have revealed details of the initial-access broker group working with Conti and Diavol ransomware gangs. The group called "Exotic Lily" breaches into the victim's system by exploiting CVE-2021-40444, a flaw in Microsoft MSHTML.

  Check Point Harmony Endpoint, IPS and Threat Emulation provide protection against these threats *(Microsoft Internet Explorer MSHTML Remote Code Execution (CVE-2021-40444); Trojan.Win32.Diavol; Ransomware.Win32.Conti)*
- The FBI warns of US critical infrastructure sectors, including financial services, critical manufacturing, government facilities and more, being targeted with the AvosLocker ransomware.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win.TouchTrapFiles.A)*
- CISA and the FBI warn that Russian state-sponsored threat actors have successfully attacked the network of an NGO by exploiting Windows PrintNightmare (CVE-2021-34527) and Default Multifactor Authentication Protocols.

  Check Point IPS provides protection against this threat *(VERS_Microsoft Windows Print Spooler Service Code Execution (CVE-2021-34527))*
- Researchers have found a connection between BlackCat and BlackMatter ransomware TTPs, suggesting that some affiliates of BlackMatter are now deploying BlackCat Ransomware.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats *(Ransomware.Win.BlackCat.E; HEUR:Trojan-Ransom.Win32.BlackCat; Trojan-Ransom.Win32.BlackMatter)*