Check Point SOFTWARE TECHNOLOGIES LTD.

Dec 07 - 13, 2020

YOUR CHECK POINT THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The US Treasury Department and US Department of Commerce were victims of a cyberattack compromising their internal email traffic. Perhaps related, SolarWinds IT management software has been exploited in a supply chain attack, adding malicious code to its software updates released between March and June 2020.
- Habana Labs, Israeli AI processor developer owned by Intel, suffers an attack by Pay2Key, a ransomware developed by Iranian hackers and first reported by Check Point Research. Hackers have stolen Habana Labs data including source-code and business documents, and are threatening to expose it if ransom is not paid.

  Check Point SandBlast Agent provides protection against this threat
- Researchers have revealed a phishing campaign executed by the Russian APT28 hacking group, delivering the Zebrocy malware, mainly used against governments and commercial organizations engaged in foreign affairs. The campaign uses lure documents related to Sinopharm International Corporation, a pharmaceutical company going through COVID-19 vaccine clinical tests.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Trojan-Downloader.Win32.Zebrocy)
- Foxconn, the electronics contract manufacturer in Mexico, has been hit by "DoppelPaymer" ransomware. The hacking group claims to have stolen unencrypted files before encrypting the facility system.

  Check Point SandBlast Agent provides protection against this threat (Ransomware.Win32.DoppelPaymer)
- Music streaming giant Spotify has suffered a data breach caused by a security vulnerability exposing users' private account information including email address, user name and password, date of birth, and gender.
- Trickbot malware is spreading in a massive phishing campaign targeting the UK, pretending to be a Subway order confirmation including the user's first name, implying that the attack might follow a data breach.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Trojan-Banker.Win32.TrickBot)
- FireEye has reported a breach and data exfiltration, as hackers stole FireEye's "red team" hacking tools.

  Check Point Anti-Bot provides protection against these tools (Backdoor.Win32.Beacon; Trojan.Win32.Rubeus)

VULNERABILITIES AND PATCHES

- Check Point researchers have found vulnerabilities in Valve's Game Networking Sockets, also known as "Steam Sockets", the core networking library used in a wide variety of games including Valve's own titles and several third-party titles. If exploited, an attacker could take over hundreds of thousands of computers without needing gamers to click on a malicious email or link.
- OpenSSL has released a security advisory regarding the EDIPartyName NULL vulnerability that can allow attackers to cause a denial-of-service condition (CVE-2020-1971).
- Microsoft December 2020 patch Tuesday fixes 58 vulnerabilities, nine of them are rated as critical, including remote code execution (RCE) bugs in SharePoint, Exchange Server, Edge and more.

  Check Point IPS provides protection against these threats (CVE-2020-17096; CVE-2020-17152; CVE-2020-17144; CVE-2020-17121; CVE-2020-17140; CVE-2020-17158)
- Cisco has addressed a new critical RCE vulnerability that affects several versions of Cisco Jabber for Windows, MacOS and mobile.
- Critical site-wide cross-site request forgery (CSRF) vulnerability has been found on Glassdoor, a website for job hunting and posting anonymous company reviews. The vulnerability impacted both job seekers and employer accounts on the web domain.
- Adobe Flash Player has received its final updates, ahead of a complete shutdown at the end of the year.

THREAT INTELLIGENCE REPORTS

- "OceanLotus", or APT32 hacking group, has allegedly been traced to an IT firm in Vietnam. The group is accused of spying on political dissidents and businesses, as well as trying to break into China's Ministry of Emergency Management and Wuhan government following the COVID-19 outbreak. It has long been suspected of spying on behalf of the Vietnamese government.
- CISA and FBI warn of a rise in phishing, ransomware, DDoS and Zoom-bombing attacks, targeting students and faculty in K-12 educational sectors.
- Researchers have discovered a botnet called PGMiner targeting PostgreSQL, an open-source relational database management system. The botnet exploits a disputed RCE flaw to compromise database servers, and installs a cryptocurrency miner.

  Check Point IPS provides protection against this threat (PostgreSQL Remote Code Execution (CVE-2019-9193))
- MountLocker ransomware as-a-service, operating since July 2020, is now offering double extortion capabilities to its affiliates.

  Check Point SandBlast Agent provides protection against this threat