Check Point
SOFTWARE TECHNOLOGIES LTD.

Apr 19 - 25, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The notorious ransomware gang REvil is claiming to have stolen data and schematics from Apple supplier Quanta Computer, and are demanding $50 million to not release the data online. As proof, the hackers have already released data about unreleased MacBook Pros and iMac.

  Check Point Harmony Endpoint provides protection against this threat

- Click Studio, Australian software company developing the Passwordstate password manager, has suffered a data breach potentially exposing their 29,000 enterprise customers. Any customer who did In-Place Upgrades within the 26-hour attack timeframe would have had their credentials compromised and needs to replace them.
- Radixx, a subsidiary of Sabre Corporation that serves the low-cost airline carrier segment, has suffered from an outage impacting its reservation system, affecting customers of approximately 20 airlines. According to the company, the outage was cause by a malware infection in their systems.
- The 93rd Academy Awards were being abused by threat actors in a phishing campaign luring people into giving up credentials to stream the Oscar-nominated films.
- Threat actors are actively using a fake Microsoft DirectX 12 download site with to distribute malware that steals cryptocurrency files, passwords, and cryptocurrency wallets.
- QNAP NAS storage devices are being hit by a new strain of ransomware named “Qlocker”. The malware moves all files stored on the device to password-protected 7zip archives and demands a $550 ransom.
- HashiCorp, open-source software tools and Vault maker, has disclosed a security incident that occurred due to the recent Codecov supply chain attack. HashiCorp’s private key used for signing software releases was exposed, which might have led to malicious software versions allegedly signed by the vendor.

VULNERABILITIES AND PATCHES

- Security vendor SonicWall has addressed three zero-day vulnerabilities already exploited in the wild, affecting both its on-premises and hosted email security products (CVE-2021-20021, CVE-2021-20022, CVE-2021-20023).
- A critical security vulnerability has been found in the Homebrew Cask package manager for MacOS and Linux that could exploited to perform remote code executing (RCE) on user machines.
- Google has released Chrome 90 for Windows, Mac, and Linux containing 7 security fixes.
- Drupal has released a security update to address a critical cross-site scripting vulnerability.

THREAT INTELLIGENCE REPORTS

- Check Point Research have demonstrated how the ToxicEye Remote access Trojan exploits Telegram to steal data from victims, using it for command and control.

  Check Point SandBlast and Anti-Bot provide protection against this threat (RAT.Win.TelegramRat; RAT.Win.ToxicEye)

- New cryptomining botnet is actively scanning for vulnerable Windows and Linux enterprise servers to infect them with the XMRig Monero miner and self-spreader malware payloads.
- The Mount Locker ransomware, rebranded "Astrolocker", has added new features in its recent campaign.

  Check Point Harmony Endpoint provides protection against this threat

- CISA, the US Cybersecurity and Infrastructure Security Agency, has reported finding the SUPERNOVA web shell collecting credentials on a SolarWinds Orion server, as an unrelated part of the SolarWinds supply chain attack, probably conducted by different threat actors.
- Researchers have identified additional technical data about the SolarWinds supply chain attack, especially around the attackers' infrastructure and patterns used by the threat actors.
- Apple's AirDrop, a feature that allows Mac and iPhone users to wirelessly transfer files between devices, has been leaking users' hashed emails and phone numbers. The flaw is known since 2019 and Apple has yet to find a fix.
- Researchers have found a new Linux Botnet abusing infrastructure-as-code (IaC) tools, using a network of proxies to get to the TOR network. The malware is currently running the Monero cryptominer – XMRig.

For comments, please contact: TI-bulletin@checkpoint.com