March 15-21, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Taiwanese electronics giant Acer has been hit by The REvil ransomware group, demanding a 50 million USD ransom in exchange for their file recovery and data privacy.

  Check Point SandBlast and SandBlast Agent provide protection against this threat (Ransomware.Win32.Revil)

- A fake version of Clubhouse, an audio-based social media app, has been distributed, delivering the BlackRock credentials-stealing malware. The app was distributed via phishing websites, falsely declaring the app will be downloaded from Google Play.

  Check Point Harmony Mobile provides protection against this threat

- CISA and FBI have issued a warning against an ongoing Trickbot spear-phishing campaign, despite the global takedown attempt that took place in October 2020. The campaign relies on a traffic infringement phishing scheme.

  Check Point SandBlast and Anti-Bot provide protection against this threat (Botnet.Win32.TrickBot)

- New malware has been targeting macOS applications developers. The malware, called 'XcodeSpy', disguises itself as a legitimate Xcode open source project that provides Apple developers a code used to animate the iOS Tab Bar based on user interaction.

- New espionage campaign dubbed 'Operation Diànxùn' has been targeting telecommunications companies in the US and India. The campaign is most likely run by the Chinese APT group 'Mustang Panda', and the primary attack vector may have been a phishing website disguised as a Huawei company career page.

- Eastern Health, one of Melbourne's largest metropolitan public health services, has fallen victim to a cyber attack, leaving many of its systems offline and forcing the facilities to postpone less urgent medical procedures.

VULNERABILITIES AND PATCHES

- Researchers have discovered vulnerabilities in two WordPress plugins, Elementor and WP Super Cache. The flaws might allow an attacker to execute arbitrary code and gain control over a vulnerable website.
- Critical vulnerabilities have been found in the popular bulletin board software MyBB. The flaws could be chained together to achieve remote code execution and do not require a privileged account.
- New bug in the popular video conferencing software Zoom could lead to accidental sensitive data leakage while using the screen sharing feature. The flaw, assigned CVE-2021-28133, enables the exposure of contents of applications that are not shared to other call attendees for a brief time period.
- Attackers have recently begun exploiting the flaw assigned CVE-2021-22986 in F5 BIG-IP and BIG-IQ networking devices. The bug, a critical unauthenticated remote command execution vulnerability, has only recently been patched, and a variety of proof-of-concept exploit codes has been published by researchers.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released an update to its Evasions Encyclopedia, a collection of techniques used by malware to detect and evade virtualized environment, often used for automated analysis. The update covers the topics of timing and human-like behavior.
- Check Point Research has revealed that the increasing unemployment rates, caused mainly by the Covid-19 pandemic's influence on global economy, have led job seekers to turn to the Darknet and hacking forums in search of positions or quick income from cybercrime activities.
- Internet scams in the US have peaked in 2020, as according to the FBI, there has been a 69% increase compared to 2019 and the largest number in the past two decades. Internet scams resulted in 4.2 billion USD in losses within the US, and the Covid-19 related scams played a key role.
- CopperStealer, a previously unknown malware, has been collecting account information, such as passwords and cookies, with versions tailored to Facebook, Google, PayPal etc. Distributed via fake software cracks and malvertising campaigns, the malware also features downloader capabilities.
- The US Government Accountability Office (GAO) has concluded that the distribution system of the national electrical grid, which delivers electricity to customer homes, is highly vulnerable to cyber threats and currently does not have a security strategy.
- Researchers have disclosed a technique used to hide up to 3MB of data, including MP3 audio files and ZIP archives, within a PNG image posted on Twitter. This could allow threat actors to embed malicious content within uploaded images. Downloading the image and changing its extension could lead to infection.