March 8-14, 2021

Check Point SOFTWARE TECHNOLOGIES LTD.

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Security footage and live feed data of some 150,000 surveillance cameras has been accessed by a hacker collective. The data was managed by Verkada, a Silicon Valley startup. Breached cameras were located in hospitals, schools, state departments and companies including Tesla and Cloudflare.

- New spam campaign that delivers the NanoCore RAT has been distributing a malicious Adobe icon file to lure the victim into downloading a malicious RAR file, which downloads the RAT when it is unzipped.

  Check Point IPS and Anti-Bot provide protection against this threat (RAT.Win32.NanoCore)

- Ransomware groups are exploiting the recently revealed Microsoft Exchange server vulnerabilities to compromise Exchange servers and download a new ransomware called 'DearCry'. The Norway parliament has suffered a data breach leveraging those flaws leading to data theft. Check Point Research has published statistics of the current exploit attempts on organizations by country and vertical.

  Check Point IPS and SandBlast Agent provide protection against these threats (relevant protections)

- Molson Coors, a multinational brewing company based in Milwaukee, has admitted it has undergone a cyber attack, most likely ransomware, which has crippled the company's beer production and delayed shipments.

- New DDoS Botnet dubbed 'ZHtrap' has been collecting devices such as routers, DVRs and UPnP network devices and transforming them into honeypots in order to track new potential bots for infection.

- New variant of the XCSSET malware for Mac machines has been observed, compiled for the new Apple Silicone chips. The malware allows data theft from popular applications such as Telegram, Skype and Notes, and features ransomware encryption capabilities.

VULNERABILITIES AND PATCHES

- Adobe has patched vulnerabilities in its FrameMaker, Animate, Photoshop, Creative Cloud Desktop and Connect products. Some 9 vulnerabilities are rated critical, among them an arbitrary code execution flaw in FrameMaker assigned CVE-2021-21056.
- Microsoft has issued a security update to address 89 flaws, among them 14 critical vulnerabilities. Among those is an Internet Explorer vulnerability assigned CVE-2021-26411, which has been actively exploited by attackers and enables an actor to run a chosen file by causing the victim to view a compromised webpage.

  Check Point IPS provides protection against these threats (e.g., Microsoft Internet Explorer Memory Corruption (CVE-2021-26411))
- Researchers have discovered three 15-year-old vulnerabilities in the Linux kernel component SCSI – Small Computer System Interface. The flaws, found in the component since its development, might allow an attacker with basic privileges to gain root privileges.

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a new dropper dubbed 'Clast82', designed to avoid Google Play Store Protect detection. The malware is spread via the 9 applications found on Google Play, and delivers AlienBot, a mobile banker and remote access Trojan distributed in a malware-as-a-service model.

  Check Point Harmony Mobile provides protection against this threat
- Check Point Research has reviewed in-depth the Dynamically Generated Image feature of the Windows Sandbox, including components and execution flow.
- Check Point Research has released its monthly global review of the prominent malware for February. The Trickbot malware, a Banker and Infostealer, has integrated new techniques into its arsenal and is currently at the top of the rank.
- The FBI has issued a warning stating that threat actors are likely to integrate synthetic content, relying on image, audio and video deepfake technologies, into campaigns aimed at influencing public and leadership opinions.
- Researchers have concluded that the Chinese threat group 'SPIRAL' is responsible for the distribution of the SUPERNOVA web shell, a backdoor found on public-facing SolarWinds server on two incident, exploiting a flaw in SolarWinds Orion.

  Check Point IPS provides protection against this threat (SolarWinds SUPERNOVA .NET Webshell Traffic)