January 04-10, 2021

YOUR CHECK POINT

THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research has observed a 45% increase in attacks targeting healthcare organizations globally since the beginning of November. Main ransomware families used in these attacks are Ryuk and Sodinokibi.

  Check Point SandBlast and SandBlast Agent provide protection against these threats (Ransomware.Win32.Ryuk; Ransomware.Win32.Sodinokibi)

- The US Department of Justice has confirmed that it has been affected by the Solarwinds supply-chain attack, and that 3% of its employee email boxes were accessed in order to steal sensitive data.

  Check Point Anti-Bot and Anti-Virus provide protection against this threat (Backdoor.Win32.SUNBURST; Trojan.Win32.TearDrop)

- Official computers in the US congress may have been accessed and compromised by individuals as part of the mob that has raided Capitol Hill. One tweet that was deleted shortly after its posting implies that Speaker of the House Nancy Pelosi's inbox and additional resources may have been left accessible.

- The Reserve Bank of New Zealand has announced it has suffered a breach via a third-party file sharing service used to store sensitive data. The scope of the information accessed is still being evaluated.

- The FBI has issued an alert warning against a worldwide campaign targeting private sector companies and deploying the Egregor ransomware. The actor behind Egregor claims that 150 companies have been compromised since the beginning of the current campaign, in September 2020.

  Check Point SandBlast Agent provides protection against this threat (Ransomware.Win32.Egregor)

- Dassault Falcon Jet, a sales subsidiary of the French aircraft manufacturer Dassault Aviation, has fallen victim to a data breach that may have led to the exposure of personal information of employees and their families. The breached records include financial account, driver's license and social security number.

- Multiple source code repositories belonging to Nissan North America, comprising 20 gigabytes of data, have been exposed due to a misconfigured Git server in which default credentials were not replaced. Mobile applications, internal analysis tools and NissanConnect services were among the exposed tools.

VULNERABILITIES AND PATCHES

- 16 vulnerabilities have been discovered in the Nvidia GPU Display Driver, which supports graphics processing units, and vGPU, a software for virtual workstations, servers, apps and PCs. The most severe flaw exposed is CVE-2021-1051 that could lead to denial of service or escalation of privileges.
- Researcher has exposed multiple vulnerabilities in Fortinet's FortiWeb Web Application Firewall (WAF). The flaws reside in the FortiWeb admin interface and feature a blind SQL injection and a stack-based buffer overflow. They could be exploited by attackers to gain access into corporate networks
- Google has fixed some 43 vulnerabilities in Android, including a critical remote code execution flaw assigned CVE-2021-0316 in the System component that could allow a remote attacker to execute arbitrary code.

THREAT INTELLIGENCE REPORTS

- Check Point Research have released a monthly review of the top most distributed malware for December 2020. Emotet leads the rank after a month break in November, followed by the Trickbot Banker. The most exploited vulnerability is 'MVPower DVR Remote Code Execution', with 42% of the organizations impacted.

  Check Point IPS, SandBlast and Anti-Bot provide protection against this threat (MVPower DVR Remote Code Execution; Trojan.Win32.Emotet)

- Government agencies have stated that a widely-used project management software, JetBrains, may have been involved in the Solarwinds supply-chain attack. It is suspected that the company, with locations is the Czech Republic and Russia, has also been breached in order to distribute a backdoor to its customers.
- Researchers who have investigated over 60 cryptocurrency wallets used by the Ryuk ransomware operators to collect payments detected cryptocurrency exchange portals commonly used by the group and concluded that the hackers behind the operation currently hold over 150 million USD worth of bitcoin.

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

- APT27, a state-sponsored Chinese threat group, has been launching a ransomware campaign alongside its common espionage operations since early 2020. Five gaming companies have been hit by the campaign, which uniquely used BitLocker, a local drive encryption tool, for encryption instead of ransomware.
- A new attack vector demonstrates how hardware security keys used for 2FA, such as from Google and Yubico, can be cloned by threat actors via an electromagnetic side-channel flaw in the chip embedded in it.

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