Check Point
SOFTWARE TECHNOLOGIES LTD.

Dec 28, 2020 - Jan 03, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Microsoft internal investigation of the recent SolarWinds supply-chain attack has revealed that the threat actors managed to move laterally in their network and gain access to Microsoft source-code repositories.
- A new large-scale phishing campaign is abusing Facebook ads to redirect users to compromised GitHub pages asking for their Facebook credentials. The campaign targeted 615,000 users in multiple countries, mainly in Nepal, the Philippines and Egypt.

  Check Point Anti-Phishing provides protection against this threat
- A data breach broker is currently selling over 350 million stolen user records of 26 companies on a hacker forum. Some of the data breaches included in this offer had not been previously disclosed.
- Al-Qard Al-Hassan, a financial organization affiliated with Hezbollah in Lebanon, has been hit by a hacker group name Spiderz that leaked information including bank account numbers, government IDs and passports, as well as registration forms and account statements.
- An Emotet campaign has hit Lithuania's National Public Health Center (NVSC) and several municipalities. After successfully infecting several computers, the malware began sending fake emails in order to spread itself, forcing NVSC to temporarily shutdown its email systems.

  Check Point SandBlast and Anti-Bot provides protection against this threat (Trojan.Win32.Emotet)
- US telecom T-Mobile has suffered a second data-breach for 2020. The breach included costumers' proprietary network information (CPNI), including their phone numbers and call records, but not customer names or email addresses. The company's security team have found the breach through "a malicious, unauthorized access to the system".

VULNERABILITIES AND PATCHES

- Researchers have discovered a backdoor account in more than 100,000 Zyxel firewalls, VPN gateway, and access point controllers. The hardcoded admin-level backdoor account can grant attackers root access to devices via SSH or WEB administration panel.
- Google has patched a bug in its feedback tool incorporated across its services that could be exploited by an attacker to potentially steal screenshots of sensitive Google Doc documents by embedding them in a malicious website.

THREAT INTELLIGENCE REPORTS

- Check Point Research has done a thorough analysis of Dridex, one of the most prevalent banking Trojans active since 2014, including its background, targets and delivery methods. The report also explains the methodology behind tracking the malware's indicators.

  Check Point SandBlast and Anti-Bot provide protection against this threat *(Banking.Win32.Dridex; Trojan.Win32.Dridex)*

- The FBI is warning owners of smart home devices with voice and video capabilities of "swatting" attacks – offenders hack into a house's smart camera and speakers, and then call emergency services to report a crime at the victim's residence. As the SWAT team arrives, they watch them through the camera and communicate with them through the speakers, occasionally live-streaming the event.
- Researchers have spotted a new credential stealer malware written in AutoHotkey (AHK), an open source scripting language for Windows that provides easy keyboard shortcuts, fast micro-creation, and software automation. The malware is targeting customers of a bank in US and Canada in an ongoing campaign that started early in 2020.
- Security experts have found several documents relating to the coronavirus vaccine allegedly stolen from the European Medicines Agency leaked in the DarkWeb.
- A new self-spreading Golang-based malware has been targeting Windows and Linux servers since early December. The malware has been targeting services such as MySQL, Tomcat admin panel, and Jenkins that are protected with weak passwords.

  Check Point SandBlast provides protection against this threat *(Trojan.Win32.Golang)*

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