January 25-31, 2021

YOUR CHECK POINT
THREAT INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The Europol and law enforcement agencies from eight countries have partnered in a joint operation in order to takedown the attack infrastructure of Emotet, the most prominent botnet distributed to-date. Authorities plan to uninstall the malware from victim machines on April 25, 2021.

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

- The US Department of Justice has announced it is launching a collaborative law enforcement operation to disrupt the attack activities of the Netwalker ransomware. Involved party has reported that the operation will include an attempt to recover ransom payments extorted from victims.

  Check Point SandBlast and Anti-Bot provide protection against this threat *(Ransomware.Win32.Netwalker)*

- 250 servers across the United States, United Kingdom, Lebanon, Israel and more have been breached by Volatile Cedar, an APT affiliated with Lebanon. The campaign focused on vulnerable Atlassian and Oracle 10g servers and exploited an Oracle vulnerability assigned CVE-2012-3152.

  Check Point Anti-Bot and Anti-Virus provide protection against this threat *(Trojan.Win32.Explosive)*

- Hacker has been offering for sale the phone numbers of over 500 million Facebook users, while allowing customers to look up a specific phone number of Facebook users for 20 USD per search via a Telegram bot. According to Facebook, the data relates to a vulnerability the company fixed in August 2019.

- Researchers suspect that North Korean APT Lazarus is behind a social engineering espionage campaign that has been targeting security researchers in the past few months. The group has established several Twitter accounts posting high quality security content in order to gain credibility.

- UScellular, the fourth-largest wireless carrier in the United States, has disclosed a data breach that led to the exposure of personal customer information. The attackers have managed to gain access to the provider's CRM via phishing scams targeting several employees who were logged-in to the database.

VULNERABILITIES AND PATCHES

- TikTok has released a fix for a vulnerability discovered by Check Point Research, within the video-sharing app's friend finder feature. The flaw allows an attacker to connect between profile details and phone numbers, while full exploitation can enable an attacker to construct a user-phone number database.
- Researchers warn against a recently exposed 10-year-old bug in Sudo, a common operating system utility that enables users to run programs with another user's privileges. The flaw, assigned CVE-2021-3156, could grant hackers root access to vulnerable Linux and Unix operating systems.
- Apple has patched three vulnerabilities that may have been exploited in the wild. Two of the flaws affect WebKit, Safari's browser engine, and could enable arbitrary code execution. Researchers estimate that all three flaws could be chained to allow an attacker to gain full control to a victim's device.
- New vulnerability in Microsoft Azure Functions has been disclosed. The flaw could be leveraged by an attacker to escalate privileges and escape the Azure Functions Docker container to the Docker host.

THREAT INTELLIGENCE REPORTS

- Check Point Research have analyzed the second phase of the SolarWinds supply-chain attack – access to victims' Azure cloud infrastructure - and present some of the key tactics and techniques used by the nation-state actors.
- Several months after a designated takedown operation, researchers have uncovered a new Trickbot campaign that has been targeting insurance companies and legal firms in North America since mid-January.

  Check Point SandBlast and Anti-Bot provide protection against this threat *(Trojan-Banker.Win32.TrickBot)*
- Researchers have discovered a new phishing kit capable of presenting a tailored phishing page to every victim based on their email domain. Dubbed 'LogoKit', the phishing infrastructure has been observed running on 700 domains over the last month.
- The Italian CERT has issued a warning against a new Android malware family dubbed 'Oscorp' that lures the user into installing an accessibility service and leverages it to collect user credentials and perform video and audio recordings.

  Check Point SandBlast Mobile provides protection against this threat

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