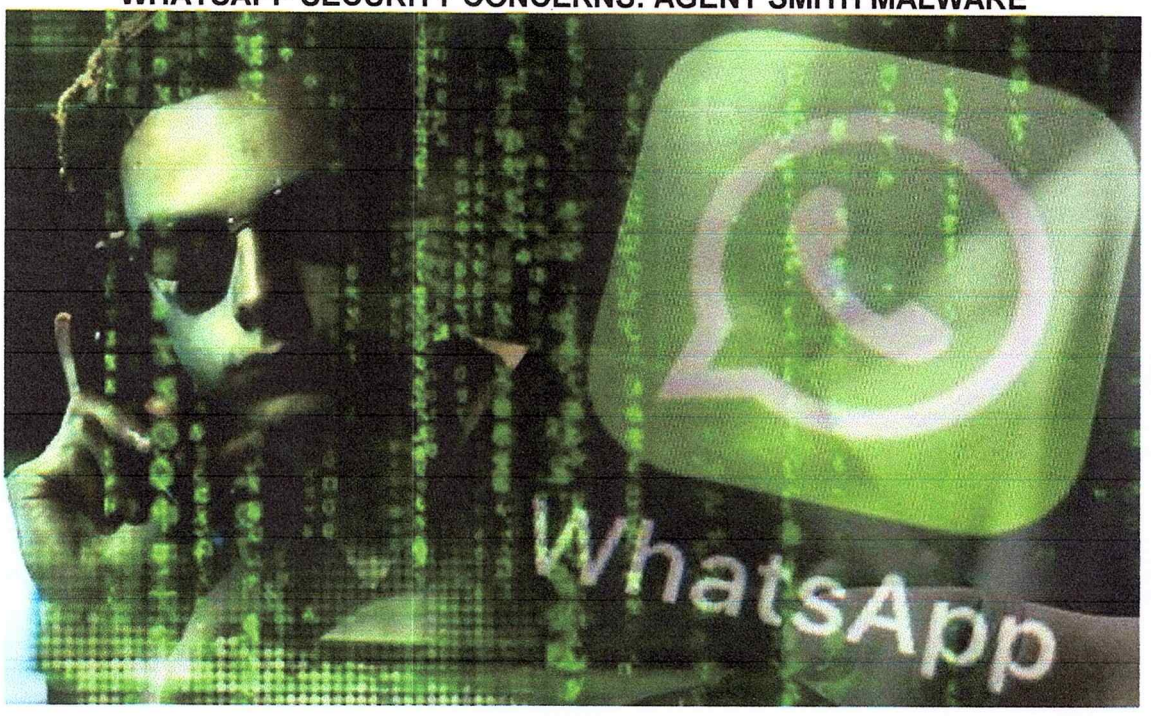
HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-13

WHATSAPP SECURITY CONCERNS: AGENT SMITH MALWARE



1. Background

A new type of malware known by the dubious pseudonym of "Agent Smith" had quietly spread to over 25 million mobile phones across the globe, creating WhatsApp security concerns. The said malware was secretly downloaded onto Android devices when users attempted to download certain apps such as WhatsApp. Instead of downloading the app, the user was actually downloading dangerous malware, leaving their mobile device completely exposed.

2. What is Agent Smith Malware?

Agent Smith is a type of particularly toxic malware that secretly replaces popular apps like WhatsApp on people's phones without their knowledge. The new version of the fake apps then displays a slew of ads right there on a user's phone. The malware works by exploiting existing weaknesses in Android operating systems. Recently, India was hit hardest by these Agent Smith attacks, though there were also a considerable number of victims throughout Australia, the UK, and the US.

The researchers found an increase in the abuse of the Janus vulnerability (designated as CVE-2017-13156) and observed popular tools, gaming, beauty filters, and adult content apps on the Play Store dropping the Agent Smith malware, which executes subsequent malicious app updates disguised as official Google patches. The malicious Android Package (APK) version extracts the installed app list, references it to its prey list sent from the command and control server (C&C), and extracts the base

APK to replace it with the malicious advertisement modules and APK, which it installs as fake updates.

Further, the goal of the attack appears to have been centered around serving up ads on Android users' mobile devices, although some security experts have warned that this malware could easily be used for more malicious intent like stealing someone's banking information or even spying on unsuspecting users through their camera or microphones.

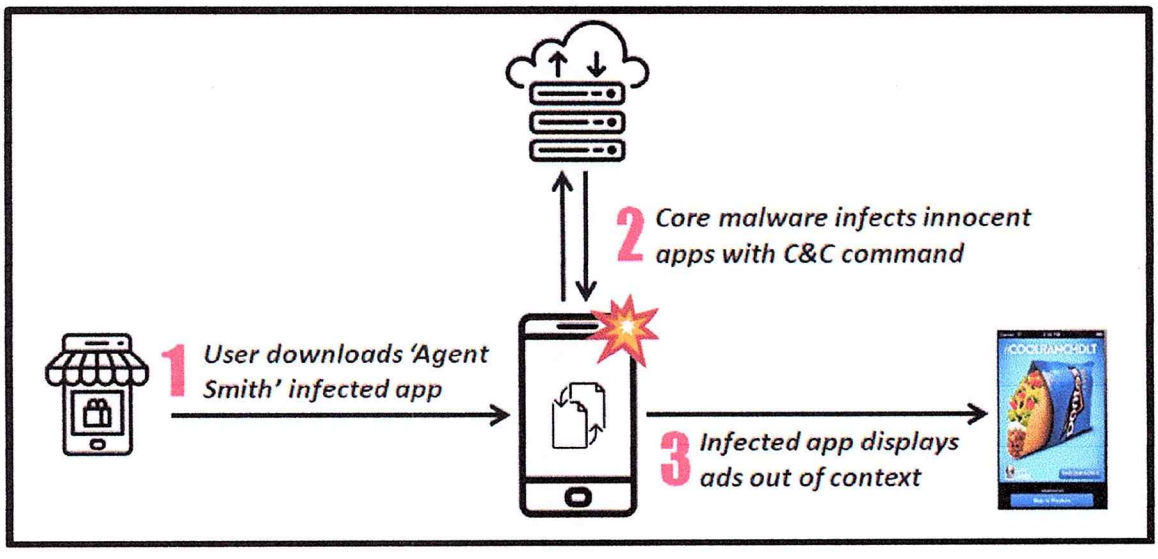
3. How the Agent Smith Malware Works.

Agent Smith malware works in three phases.

a. A dropper app lures the victim to installing the malware voluntarily. The initial dropper contains encrypted malicious files and usually takes the form of "barely functioning photo utilities, games, or other entertainment apps."

b. The dropper decrypts and installs the malicious files. The malware uses Google Updater, Google Update for U, or "com.google.vending" to disguise its activity.

c. The core malware creates a list of installed apps. If an app matches its "prey list," it patches the target app with a malicious advertising module, replacing the original as if it were a simple app update.



Interestingly, Agent Smith bundles together several Android vulnerabilities, including Janus, Bundle, and Man-in-the-Disk. The combination creates a 3-stage infection process, allowing the malware distributor to build a monetized (via adverts) botnet. The Check Point research team believes that Agent Smith is possibly the first campaign seen that integrates and weaponized all the vulnerabilities together, making the malware "as malicious as they come."

4. WhatsApp - A Breeding Ground for Scammers

The ubiquity of WhatsApp has also made it the ideal place for scammers to locate potential victims. The Singapore Police Force (SPF) released a crime advisory about a scam involving the hacking of WhatsApp accounts.

According to the SPF, the scam would begin with a target receiving a WhatsApp message (from a registered number on the victim's contact list, whose account has already been hacked) asking for a six-digit verification code to be sent to the victim's phone.

Once someone falls for the trap and sends the verification code, the victim completely loses control of their WhatsApp account.

5. How to Spot and Remove Agent Smith from Android

You can spot Agent Smith fairly easily. If your regularly used apps suddenly start producing an overwhelming number of adverts, it is a sure sign something is wrong. The ads the malware serves are difficult or impossible to exit, which is another indicator. But as Agent Smith acts almost silently between the adverts, picking up on subtle changes to your apps is incredibly difficult.

If you suspect something is wrong, you should complete an antimalware or antivirus scan on your device. Further, utilization of endpoint security applications on your mobile devices will catch and remove any malicious applications.

6. Recommendations

Protect yourself from Agent Smith Malware and other similar threats by following these tips:

a. Use a secure internal communication solution. Consumer chat apps like WhatsApp are practically crawling with spammers, scammers, and hackers. Yet organizations still use these platforms to share sensitive data every single day. It is absolutely essential to ensure that every member of the organization is using a compliant, secure messaging platform.

b. Users are advised to check their devices and uninstall suspected apps or newly installed apps if they suspect infection.

c. Regularly install patches and updates to the devices in time to make sure vulnerabilities are fixed accordingly.

d. Users and enterprises can consider using a multilayered mobile security solution to prevent adware and other potentially unwanted applications (PUAs) installation attempts on their devices.

e. Make sure everyone in the organization knows how to avoid cybersecurity threats and risks. Organizations should invest in educating their employees about basic security practices, such as secure password tips and how to identify phishing emails. This type of education should be conducted frequently because of the ever-evolving threats.

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization's overall cybersecurity posture. All units and offices are given permission and are encouraged

to redistribute this bulletin that will benefit the AFP organization as a whole for educational, and non-commercial purposes.

References:

- *https://www.beekeeper.io/blog/whatsapp-is-now-riskier-than-ever-as-security-concerns-reach-new-heights/*
- *https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/agent-smith-malware-infecting-android-apps-devices-for-adware*
- *https://www.makeuseof.com/tag/agent-smith-malware/*