Technology | CyberSecurity

Google Voice Search On Android Smartphones Could Be Exploited by Malware

By Ruan F
Updated August 20, 2014 06:32 IST

Researchers at the Chinese University of Hong Kong have developed a new malware application called VoiceImplyer to show how criminals could use Android’s voice search capability to steal important information without needing explicit permissions from users.

VoiceImplyer exploits Google Voice Search hooks built into the company’s Google Now personal digital assistant (PDA) and goes the PDA to call phone numbers of cyber-criminals, and makes the voice calls to deliver data over the phone.

Chinese researchers at the Hong Kong University have detailed VoiceImplyer’s attack in a research paper titled ‘Your Voice Assistant Is Fake’ to show how criminals could steal voice call records and personal data or even control the smartphone. They warn that all Android devices could be vulnerable to malware attacks.

VoiceImplyer is a Google Voice Search (GVS)-based attack.

“With imperceptible design, our GVS-attack can transform SMS, access private information, transmit sensitive data and achieve remote control without any permission,” the researchers say.

According to the VoiceImplyer developers, the malware app was designed to demonstrate that the so-called safe zone on voice calls could be gained access to sensitive user data, and is transmitted to cyber criminals.

VoiceImplyer attacks Androids by exploiting an already present vulnerability within the Google Search app aiming to steal phone numbers.

“This study may inspire application developers and researchers to rethink that voice permission doesn’t mean safety and the voice can be reused as a new attack surface,” the researchers say.

Real-world illustrations

To trigger voice Implyer malware works, researchers used a Samsung Galaxy S5 smartphone, and were reportedly successful in getting the malware to execute voice commands like “Ending call,” subject “message” to a malicious number. The malware successfully sent the call to the malicious number and transferred confidential user data by audio to the malicious number.

After the call to the malicious number is connected, VoiceImplyer exploits the Google Voice Search mechanism by posting the above user location-related queries, and takes the information to criminals.

“The voice channel is not just used for transmitting two information, actually any type of file can be translated to text format,” added the researchers.

Locked out

“When Google Search app receives an ACTION VOICE, COMMAND based intent, if the phone is securely locked, it must verify whether both microphone level is enabled and call before executing the intent. Voice Implyer can bypass this. Otherwise, a warning should be provided like ‘please unlock the device first!’ Therefore, in the situation of secure screen tools, the system cannot be launched and the phone is stuck,” the researchers explained.

Users are therefore strongly advised to secure their Android smartphones, especially those running Android 4.5 and above by locking them using a screen password, to combat GVS attacks.

Malware exploiting Android smartphones by breaching the phone’s security is nothing new.

There are daily reports of new malware being developed by cyber-criminals with the sole intention of tricking innocent smartphone users across the globe.

In late 2013, a recent study conducted by the Chinese-based Cheholis Mobile made public the fact that malware targeting the most popular smartphone operating system in the world, Android, has grown by 68.0% in the last 12 months.

However it should be noted that the vast majority of malware on the Android platform is found on unofficial third-party sources which are popular in countries like Russia and China, while the official Play Store is relatively safe.

YOU MIGHT LIKE THIS

Hardluck: Muda Meeting, Adda will change your life!

The Mindful Play of Order of 2015

See Why So Many People Are Upgrading To This Mattress

Opportunities Like This Are Making People Surprised...

Doctors Revive This Single Doctor By Using Electricity

Genius Around The World: Have You Been Waiting for This...?