Google Voice Search On Android Smartphones Could be Exploited by Malware

By Rahul R

Updated August 20, 2014 08:32 BST

Researchers at Hong Kong University have developed a new malware to showcase that Google Voice Search service can be exploited by zero permission apps. (Reuters)

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

VoicEmployer exploits Google's Voice Search mechanism built into the company's Google Now personal digital assistant (PDA), and gets the PDA to call phone numbers of cyber-criminals, and recites (by voice) sensitive user data to criminals.

Chinese researchers at the Hong Kong University have detailed VoicEmployer GVS attack in a research paper titled *Your Voice Assistant is Mine: How to Abuse Speakers to steal Information and Control Your Phone*,' and warn that all Android devices could fall prey to attacks that are targeted to steal personal user data by exploiting Google Now (Voice-Search).

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

"With ingenious designs, our GVS-Attack can forge SMS/Email, access privacy information, transmit sensitive data and achieve remote control without any permission," the researchers say.

According to VoicEmployer's developers, the malware app was designed to demonstrate that the so-called safe zero permission Android apps could gain access to sensitive user data, and in turn transmit these to cyber criminals.

The researchers say VoicEmployer works by exploiting an already present vulnerability within the Google Search app allowing it to dial phone numbers.

"This study may inspire application developers and researchers rethink that zero permission doesn't mean safety and the speaker can be treated as a new attack surface."

Real-world illustrations

To illustrate how VoicEmployer malware works, researchers used a Samsung Galaxy S3 smartphone, and were reportedly successful in getting the malware to execute voice commands like "Email to [contacts], subject "meeting cancel", message "tomorrow's meeting has been cancelled," "What is my IP address?" and "Where is my location?"

The above voice commands were recognised by Google Now which provided feedback to these queries.

Also, the malware was successful in getting Google Now to execute the "call" voice command, to call a malicious number, and transfer confidential user data by audio input to the malicious number.

After the call to the malicious number is connected, VoicEmployer exploits the Google Voice Search mechanism by posing the above user location-related queries, and leaks this information to criminals.

"The voice channel is not just used for transferring text information. Actually any type of files can be translated to hex coding formats," added the researchers.

Locked out

"When Google Search app receives an ACTION_VOICE_COMMAND based Intent, if the phone is securely locked, it must strictly check whether a Bluetooth headset is connected with the phone. If the connect status is true, Voice Dialler can be started. Otherwise, a warning should be provided, like "please unlock the device first". Therefore, in the situation of secure screen lock, GVS-Attack cannot be launched and the phone is safe."

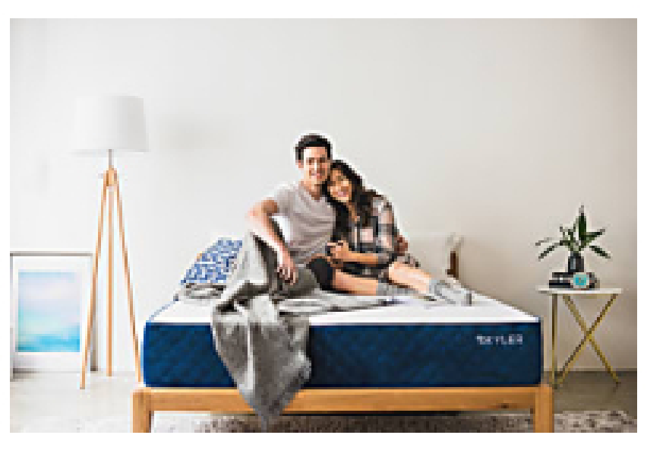
Users are therefore strongly advised to secure their Android smartphones (especially those running Android 4.1 and above) by locking them with a strong password, to combat GVS-attacks.

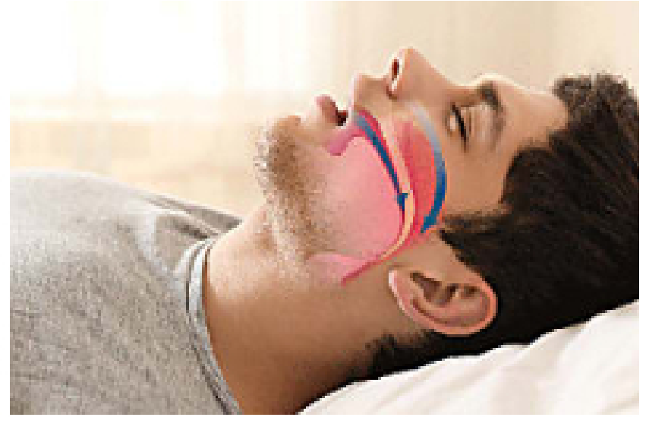
Malware attacking Android smartphones by breaching the device's security is nothing new.

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

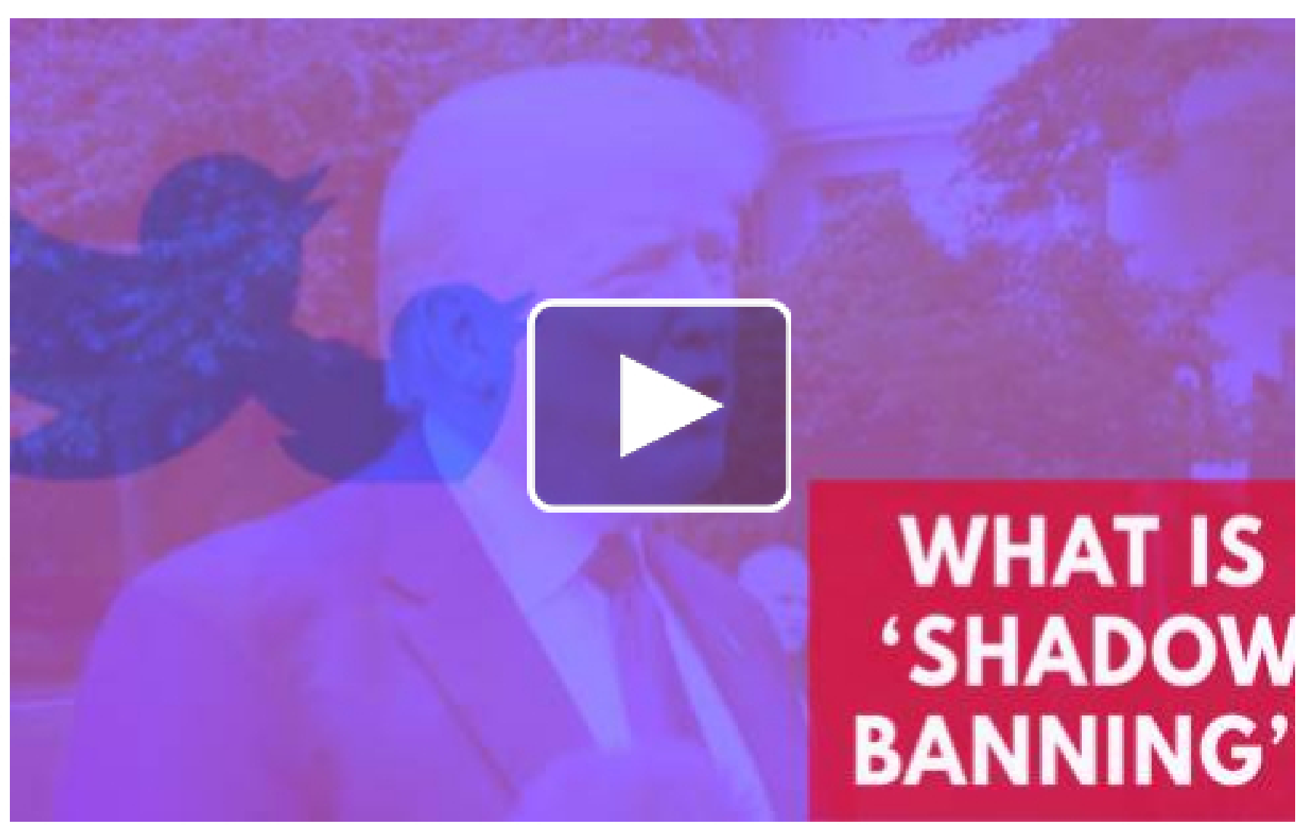
In fact, a recent study conducted by China-based Cheetah Mobile made public the fact that malware targeting the most popular smartphone operating system in the world, Android, has grown by 600% in the last 12 months.

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





IBT VIDEO



Is Twitter 'Shadow Banning' Conservatives?

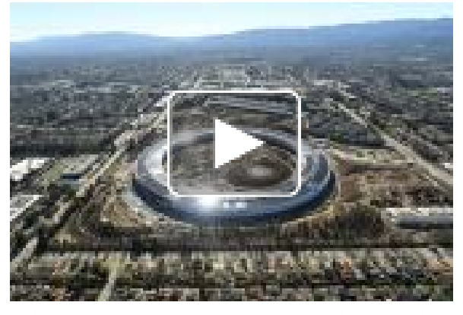
COLUMNISTS

Thomas Coughlin

A new gold standard in the age of blockchain

READ MORE

Can Twitter change its 'core' and remain Twitter?



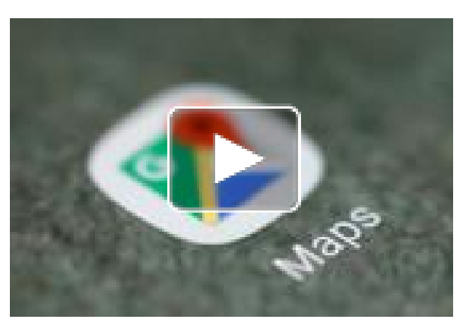
The Apple car? Analyst claims it could be on the road by 2025

Twitter muzzles alt-right conspiracy theorist Alex Jones for a week

Tesla stock price: Is Elon Musk's $420-a-share proposal fair?

There's a reason Siri, Alexa and AI are imagined as female – sexism

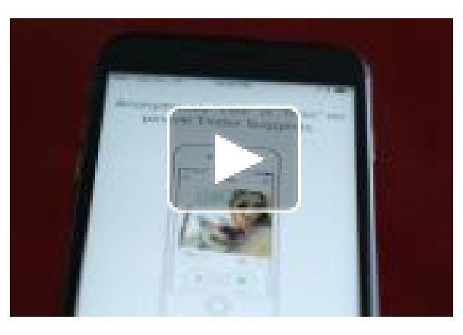
Why Amazon doesn't worry about its lack of Alexa shoppers



Google tracks your movements, like it or not

Why Elon Musk should take Tesla private

Questions and legal concerns mount over Elon Musk's bombshell Tesla buyout tweet



Tinder feeling the love as user growth beats expectation