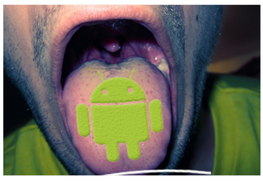
Security

Malware gets your Android blabbering to HACKERS

Boffins get your mobe to spill the beans using Google text-to-speech kit

By Darren Pauli 29 Jul 2014 at 06:33 13 SHARE



Researchers from the Chinese University of Hong Kong have developed bizarre malware that dictates contacts, emails and other sensitive text data in order to steal it.

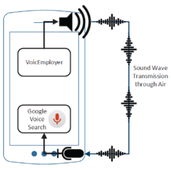
In the novel attack a seemingly innocuous app that required no permissions called a bad guy's phone number and blabbered the stolen data out of the speakers and down the microphone using Google Voice Services (GVS).

It affected 'nearly all' Android devices and could not be detected by VoicEmployer malware or victims, provided savvy hackers conducted the attack in the wee hours with the volume turned down.

The GVS-Attack was not nearly as powerful as malicious apps that required users to blindly grant permissions to enable widespread botting and bank account pilfering, but it did break new ground in the ability for malware to exploit the so called zero-permission state previously considered safe.

"Through invoking the speaker, this zero permission app can make phone calls, forge SMS/Email, steal personal schedules, get the user location, [and] transmit data remotely," Wenrui Diao, Xiangyu Liu, Zhe Zhou, and Kehuan Zhang wrote in a paper *Your Voice Assistant is Mine: How to Abuse Speakers to Steal Information and Control Your Phone*.

"Generally a mobile malware needs quite sensitive privileges (even root) to achieve remote control. However our attack doesn't need any permission.



"This inter-application communication channel and transmission media are beyond the control of Android OS."

User devices could be activated when the phones were securely locked due to a bug in which the Google Search app -- which granted more privileged access to bluetooth devices -- did not check if a device was actually attached.

Attackers could glean a users location, their IP address and possibly capture pictures by converting these to HEX before dictating it down the blower, researchers said.

Voice Command	Bypassed Permission(s)
Call ...	READ_CONTACTS, CALL_PHONE
Listen to voicemail	WRITE_SETTINGS, CALL_PHONE
Browse to Google dot com	INTERNET
Email to ...	READ_CONTACTS, GET_ACCOUNTS, INTERNET
Send SMS to ...	READ_CONTACTS, WRITE_SMS, SEND_SMS
Set alarm for ...	SET_ALARM
Note to myself ...	GET_ACCOUNTS, RECORD_AUDIO, INTERNET
What is my next meeting?	READ_CALENDAR
Show me pictures of ...	INTERNET
What is my IP address?	ACCESS_WIFI_STATE, INTERNET
Where is my location?	ACCESS_COARSE_LOCATION, INTERNET
How far from here to ...?	ACCESS_FINE_LOCATION, INTERNET

Bypassed permissions

The hack served more as a new avenue for targeted intelligence gathering operations rather than as a set and forget attack in which financial or login data would be pillaged en masse.

It could, *Vulture South* imagines, also serve as a means to terrify a population by whispering things as victims sleep, or ruin their mornings by setting alarms to blast at 3am across the world.

The researchers pulled off their attacks on a Samsung Galaxy S3, running both stock firmware and modded with CyanogenMod, a Meizu MX2 and a Motorola A953.

"This research 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." ®

Tips and corrections 13 Comments

MORE Malware Android Security

Most read


Google risks mega-fine in EU over location 'stalking'


Boss regrets pointing finger at chilled out techie who finished upgrade early


Google shaves half a gig off Android Poundland Edition


Home Office seeks Brexit tech boss – but doesn't splash the cash


Windows 10 Linux Distribution Overload? We have just the thing

You Might Also Like


Sysadmin sank IBM mainframe by going one VM too deep


Unbreakable smart lock devastated to discover screwdrivers exist


Australia on the cusp of showing the world how to break encryption

Recommended by outbrain

More from The Register


Sophos SafeGuard anything but – thanks to 7 serious security bugs
Your antimalware tools can get malware too, so get updating


Look, what's that over there? Sophos nips Windows DNS DLL false positive in the bud
Temporary file during update shuffled off to quarantine


Sophos to assimilate Invincea's intelligent machine tech to fight malware
Machine learning IP snapped up in $100m deal


Amazon, Google inject Bluetooth vuln vaccines into Echo, Home AI pals
UPDATED The BlueBorne ultimatum


Tech giants at war: Google pulls plug on YouTube in Amazon kit
You won't sell our stuff? We won't let you watch our vids


Europe plans special tax for Google, Apple, Facebook, Amazon
French minister says around two per cent of turnover sounds about right


Security FUD and malware outbreaks boost Sophos' coffers
Targeting the 'underserved mid-market' pays off nicely


Sophos buys Irish Barricade