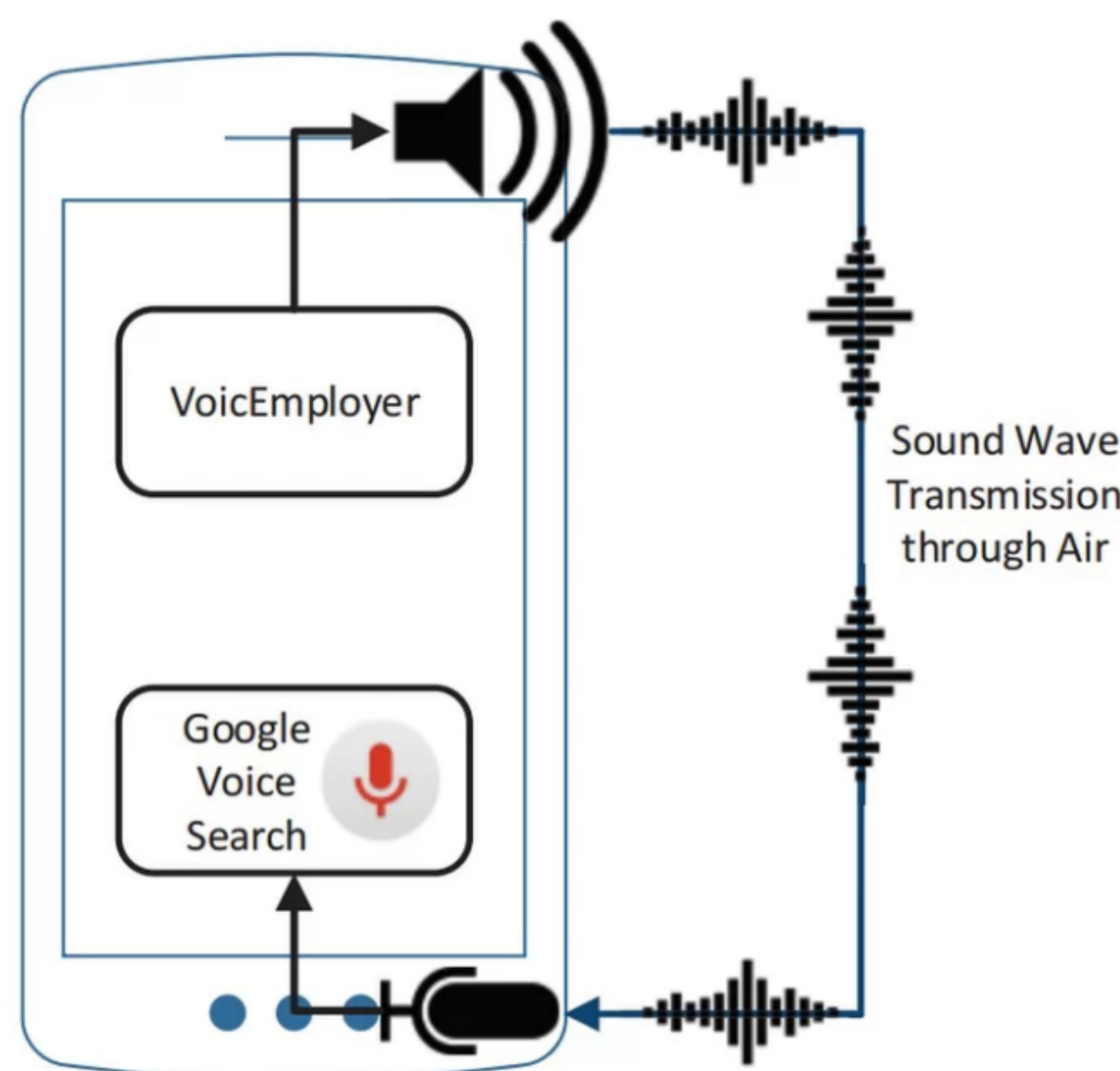


SECURITY &gt; NEWS

## Loudmouth Android Malware Speaks Your Secrets

by MARSHALL HONOROF &amp; JILL SCHARR Jul 29, 2014, 10:16 AM



A new type of Android malware talks about you behind your back — and like a rebellious teenager, it doesn't need your permission to blab your secrets late into the night.

Security experts at the Chinese University of Hong Kong detailed the malicious app, which they created and called VoicEmployer, in a paper titled "[Your Voice Assistant Is Mine](#)." It leverages Android's Google Voice Search, and since users generally need to be present for voice commands to work, no permissions are necessary for the app.

Once VoicEmployer is installed on a phone, it plays a low-volume audio file that says "Call number," then recites a phone number belonging to the malware's controllers. Google Voice Search hears the command and dials the number. Before you know it, your phone is whispering your sensitive data into the microphone.

**MORE:** [Best Android Antivirus Software 2014](#)

VoicEmployer asked Google Voice Search questions that warranted verbal responses: "What is my IP address?" "Where is my location?" "What is my next meeting?" A malefactor could even extract personal data by asking Google Voice Search to send an email, access a photo or listen to voicemail.

VoicEmployer might not be a particularly efficient method of data exfiltration, since calling victims at inopportune times and listening to data being recited takes some doing. But it could be an ideal way to target individuals, either to steal information from them or to wage psychological warfare through alarms in the middle of the night, whispered threats and the like.

Testing VoicEmployer on a Samsung Galaxy S3, a Meizu MX2 and a Motorola A953 (renamed Droid 2 in the United States), the researchers also found a vulnerability that lets VoicEmployer activate features even when the phone is locked. The malware tricks the phone into thinking a Bluetooth device — which, by default, can make hands-free voice commands to a phone — is connected.

"In theory, nearly all Android devices equipped with Google Services Framework [Google's built-in Android apps such as Voice Search] can be affected," the researchers wrote in their paper.

It was previously thought that apps with zero permissions couldn't do much damage, because they shouldn't be able to access a phone's most sensitive features. Yet if security experts could come up with such a program, so could enterprising cybercriminals. An app that required no permission could easily hide in any other app, including social media, streaming video or games.

There isn't much users can do to prevent this from happening; the fix to Google Voice Search will have to come from Google's end. Until then, avoid apps from questionable developers, keep your phone close at hand and consider turning it off at night — or checking the call record in the morning.

- [10 Things You Didn't Know Could Be Hacked](#)
- [How Your Next Hotel Room Could Be Hacked](#)
- [13 Security and Privacy Tips for the Truly Paranoid](#)

Jill Scharr and Marshall Honorof are staff writers for Tom's Guide. You can follow Jill on Twitter [@jillscharr](#) and on Google+ [Follow Jill Scharr](#). Follow Marshall [@marshallhonorof](#) and on Google+ [Follow Marshall Honorof](#).

2 COMMENTS

SECURITY &gt; NEWS

## Facebook Fighting FBI Over Encrypted Messages: Report

by PAUL WAGENSEIL Aug 17, 2018, 3:54 PM



Facebook is fighting the U.S. Justice Department over a demand that the social-networking service decrypt Messenger voice conversations in a California case related to the MS-13 gang, [Reuters reported](#) earlier today (Aug. 17).

Credit: Jaktraphong Photography/Shutterstock

The case is being kept under seal, but Reuters said three separate individuals who were not named had told the news agency that a judge heard arguments Tuesday (Aug. 14) about whether Facebook should be held in contempt of court for refusing the government's demands.

The government wants to listen to voice conversations involving a single individual in Fresno as they happen over Messenger, which lets users make encrypted voice calls.

2 COMMENTS

SECURITY &gt; NEWS

## Facebook Fighting FBI Over Encrypted Messages: Report

by PAUL WAGENSEIL Aug 17, 2018, 3:54 PM



Facebook is fighting the U.S. Justice Department over a demand that the social-networking service decrypt Messenger voice conversations in a California case related to the MS-13 gang, [Reuters reported](#) earlier today (Aug. 17).

MOST POPULAR

- 1 [Antivirus Software Isn't Very Secure, Researchers Find](#)
- 2 [Facebook Scam Tricks Users Into Hacking Themselves](#)
- 3 [Your iPhone May Spy on You \(Update: Apple Responds\)](#)

MOST POPULAR

- 1 [Best Wireless Home Security Cameras 2018](#)
- 2 [Best Antivirus Software and Apps 2018](#)
- 3 [Best Identity-Theft Protection 2018](#)

MOST POPULAR

- 1 [Best Wireless Home Security Cameras 2018](#)
- 2 [Best Antivirus Software and Apps 2018](#)
- 3 [Best Identity-Theft Protection 2018](#)

