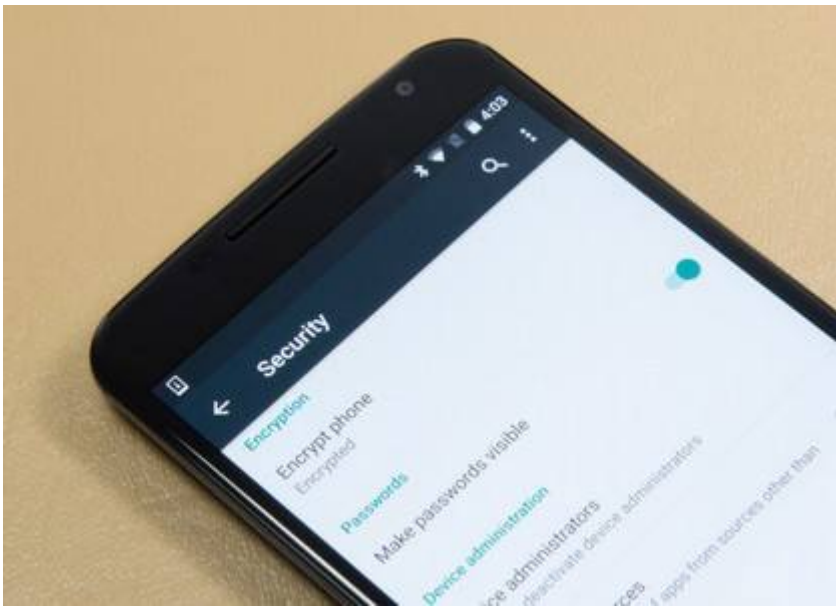
Researchers report >4,000 apps that secretly record audio and steal logs

SonicSpy family of apps pose as benign programs. Behind the scenes, they spy on users.

Dan Goodin -



Ron Amadeo
84

A single threat actor has aggressively bombarded Android users with more than 4,000 spyware apps since February, and in at least three cases the actor snuck the apps into Google's official Play Market, security researchers said Thursday.

Soniac was one of the three apps that made its way into Google Play, according to a blog post published Thursday by a researcher from mobile security firm Lookout. The app, which had from 1,000 to 5,000 downloads before Google removed it, provided messaging functions through a customized version of the Telegram communications program. Behind the scenes, Soniac had the ability to surreptitiously record audio, take phones, make calls, send text messages, and retrieve logs, contacts, and information about Wi-Fi access points. Google ejected the app after Lookout reported it as malicious.

Two other apps—one called Hulk Messenger and the other Troy Chat—were also available in Play but were later removed. It's not clear if the developer withdrew the apps or if Google expelled them after discovering their spying capabilities. The remaining apps—which since February number slightly more than 4,000—are being distributed through other channels that weren't immediately clear. Lookout

researcher Michael Flossman said those channels may include alternative markets or targeted text messages that include a download link. The apps are all part of a malware family Lookout calls SonicSpy.

"What's commonly seen in all SonicSpy samples is that once they compromise a device they beacon to command and control servers and await for instructions from the operator who can issue one of seventy three supported commands," Flossman wrote in the e-mail. "The way this has been implemented is distinct across the entire SonicSpy family."

Once installed, SonicSpy apps remove their launcher icon to hide their presence and then establish a connection to the control server located on port 2222 of arshad93.ddns[.]net.

The researcher said SonicSpy has similarities to another malicious app family called SpyNote, which security firm Palo Alto Networks reported last year. The name of the developer account—iraqwebservice—and several traits found in the apps' code suggest the developer is located in Iraq. Additionally, much of the domain infrastructure associated with SonicSpy has references to that country. The phrase "Iraqian Shield" appears constantly. Lookout is continuing to follow leads suggesting the developer is based in that part of the world.

The report from Lookout is the latest reminder about the risks of installing apps from third-party markets, but they also make clear that limiting sources to Google Play are no guarantee an app is safe. Android users should be wary of any non-Google app sources with the exception of Amazon's Android offerings. Users should also avoid installing Google Play apps of questionable value or utility, particularly when they have few downloads.

Dan Goodin Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications. **Email** dan.goodin@arstechnica.com // **Twitter** @dangoodin001