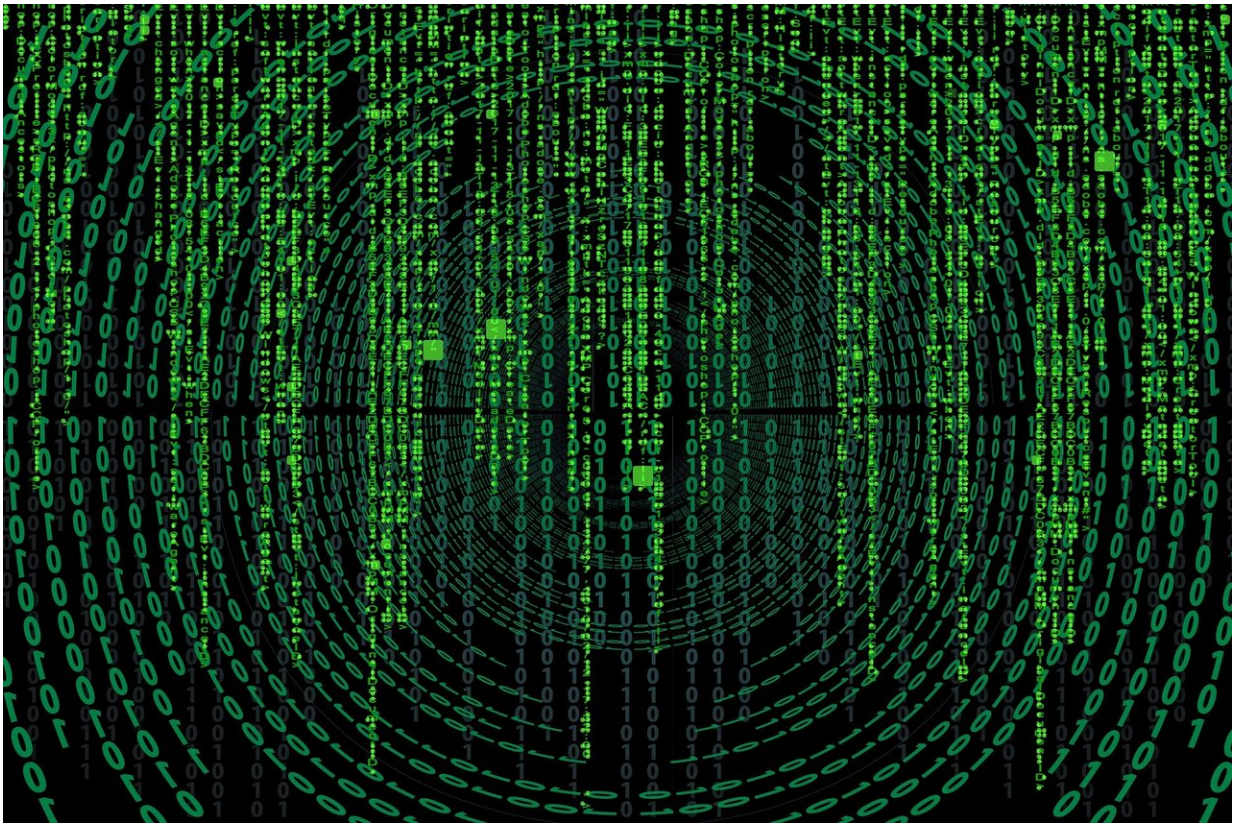
Powerful snooping Android malware spotted by Kaspersky Lab

January 18 2018, by Nancy Owano



Credit: CC0 Public Domain

Kaspersky Lab malware researchers have found spying capabilities in Android malware. The malware is dubbed Skygofree. How ambitious is it? *Kaspersky Lab Daily* commented that Skygofree was "overflowing"

with functions.

Nikita Buchka and Alexey Firsh wrote about it at length. Once the device is infected, the attackers get full remote control.

The two pointed out that "Skygofree has no connection to Sky, Sky Go or any other subsidiary of Sky, and does not affect the Sky Go service or app."

Then why pick that name? The name was chosen "because we found the word in one of the domains."

Several sites like *Android Police* pointed out this was no run of the mill malware. "Security firms spot new malware variations all the time, but most of them aren't very sophisticated," wrote Ryan Whitwam. Meanwhile, Skygofree was in a completely different league, he said.

Skygofree, from back in 2014, went through some additions in the form of new features. It now has spying capabilities that plain and simple were not seen before.

"Over the past three years, it has grown from a rather simple piece of malware into full-fledged, multifunctional spyware," said *Kaspersky Lab Daily*.

"With 48 different commands in its latest version, the malware has undergone continuous development," wrote Dan Goodin in *Ars Technica*. "It relies on five separate exploits to gain privileged root access that allows it to bypass key Android security measures."

One of the never-before-seen features was in recording surrounding audio in specified locations.

What can it do? Rather, what can't it do? Buchka and Firsh on January 16 walked readers through the capabilities. (1) can record audio surroundings by way of the microphone when an infected device is in a specified location; (2) can get at WhatsApp messages via Accessibility Services; (3) can connect the affected device to Wi-Fi networks controlled by cybercriminals; (4) Skygofree can secretly turn on the front-facing camera and take a shot when the user unlocks the device.

"The malware is distributed through fake mobile operator websites, where Skygofree is disguised as an update to improve mobile Internet speed. If a user swallows the bait and downloads the Trojan, it displays a notification that setup is supposedly in progress, conceals itself from the user, and requests further instructions from the command server, " said *Kaspersky Lab Daily*.

Who may be behind the spyware? Any clues found? *Ars Technica*'s Dan Goodin said traces included a domain name registered by an Italian IT firm.

The researchers said they were pretty confident that the developer of the Skygofree implants was an Italian IT company. Cory Doctorow in *Boing Boing*: "The researchers hypothesize that Skygofree is a product of an unnamed Italian firm that sells it to governments, corporations or criminals."

Kaspersky Labs said that data found indicated several people in Italy were infected, said Goodin.

But, why Italy? "The researchers trace the malware to Italy based on subtle and inconclusive clues," said Doctorow, "such as a domain referenced in the code that is registered to an Italian company." (Doctorow also remarked, "It is common for malware writers to obfuscate or misdirect researchers about the origins of their products.")

Meanwhile, the campaign remains ongoing, said Goodin.

As for Windows, they also discovered spyware tools for Windows "that form an implant for exfiltrating sensitive data on a targeted machine." They found a version at the beginning of last year, but said they were unsure if this implant has been used in the wild.

Whitwam said the good news was "you probably don't have to fret about Skygofree. As long as you don't install sketchy APKs, it's impossible to become infected with Skygofree."

More information: securelist.com/skygofree-follo … f-hackingteam/83603/