Revealed: How Governments Can Take Control of Smartphones

June 25, 2014

> ***Note from Pastor Kevin Lea**: I became aware of this technology a few years ago. Ever since then, I avoid talking about sensitive things when there is a smart phone (or even a desk phone – which can also be bugged) in the vicinity. We live at a time when I believe we should assume that everything we say is being recorded (by God **and** Big Brother, who is playing god). So sad that most are concerned only about what they say in front of others, rather than the One to Whom we will all answer.*
>
> "A good man out of the good treasure of his heart brings forth good things, and an evil man out of the evil treasure brings forth evil things. But I say to you that for every idle word men may speak, they will give account of it in the day of judgment. For by your words you will be justified, and by your words you will be condemned." *Matthew 12:35-37 NKJV*

Photo by Brian Klug / flickr.com

'Legal malware' produced by the Italian firm Hacking Team can take total control of your mobile phone. That's according to Russian security firm Kaspersky Lab and University of Toronto's Citizen Lab(which also obtained a user manual).

Operating since 2001, the Milan-based Hacking Team employs over 50 people and offers clients the ability to "take control of your targets and monitor them regardless of encryption and mobility," while "keeping an eye on all your targets and manage them remotely, all from a single screen."

It's the first time Remote Control Systems (RCS) malware has been positively linked with mobile phones and it opens up a new privacy threat potential to mobile phone users.

"Our latest research has identified mobile modules that work on all well-known mobile platforms, including as Android and iOS," wrote Kaspersky researcher Sergey Golovanov.

"These modules are installed using infectors – special executables for either Windows or Macs that run on already infected computers. They translate into complete control over the environment in and near a victim's computer. Secretly activating the microphone and taking regular camera shots provides constant surveillance of the target – which is much more powerful than traditional cloak and dagger operations."

Police can install the spy malware directly into the phone if there is direct access to the device, or if the owner of the phone connects to an already infected computer, according to Wired.

Various softwares can also lure users to download targeted fake apps.

Once inside an iPhone, for instance, it can access and activate all of the following: control of Wi-Fi, GPS, GPRS, recording voice, e-mail, SMS, MMS, listing files, cookies, visited URLs, cached web pages, address book, call history, notes, calendar, clipboard, list of apps, SIM change, live microphone, camera shots, support chats, WhatsApp, Skype, and Viber.

While the malware can be spotted by some of the more sophisticated anti-virus software, it takes special measures to avoid detection – such as *"scouting"* a victim before installation, *"obfuscating"* its presence, and removing traces of its activity.

Hacking Team has maintained that its products are used for lawful governmental interceptions, adding that it does not sell items to countries blacklisted by NATO or repressive regimes.

Wired reported that there have been cases where the spying apps were used…

To read this article in its entirety, go to:
http://rt.com/news/168228-hacking-team-smartphones-malware/