Jacobs Journal Of Electronics and Communications

Short Commentary

Smart Phones And Surveillance Methods

Christos Beretas

Ethical Hacking (Red Team), City University of seattle, USA

*Corresponding author: Christos Beretas , Ethical Hacking (Red Team), city university of seattle, USA;

Email: c_beretas@yahoo.com

Received Date: 03-29-2019

Accepted Date: 04-08-2019

Published Date: 04-10-2019

Copyright: © 2019 Christos Beretas

Introduction

I decided to touch on a sensitive issue, so topical and important, which is about everyday life of all of us, I am talking about the smart phones, small smart phones, these small but powerful computers that everybody use them every day by doing more internet browsing rather than doing calls. The questions that arise about the security of smart phones are many, for example: may someone watch us? May the government hear what we saying and what messages we send? May they know our position? Let's analyze the issue below.

When referring to a smart phone surveillance, we refer to 3 spy methods, which are:

1. Signal interception over the air & man in the middle attack.
2. Hardware circuit.
3. Spy phone application.

The first case above to do requires expensive equipment that is not legally sold on the market to be purchased by an interested customers, there are various approaches to low-cost material, but these tapping systems are cumbersome and complex in their operation if we think the advent of 3G/4G networks that offer more security than the old 2G these cheap eavesdropper devices are partly useless and I say in partly because we should think that in smart phones devices in the choice of the network allows the following option 4G/3G/2G which means that where there is no 4G/3G network coverage the smart phone will operate on the 2G network and this is a security hole as the network is over vulnerable to cheap type of interceptor devices since the 2G network encryption algorithm provide low security. An expensive stolen state equipment would also be useless since its use keys that should be renewed regularly. Thus, state-owned services that have legal co-op equipment have the ability to make legitimate signal interception, here at this point, some one might think of this, an employee who has access to the system could be tapping someone else phone? the answer I believe is aware of it. Legally signal interception systemss are divided into 2 categories, those located in central buildings where sometimes require the assistance of the telecom provider and the base stations where, depending on the needs of the service, they move.

The second case above could be said to be based on the ignorance of the user, I say ignorance because in this case the smart phone has to be opened and a micro chip is placed inside, which will collect everything and send it back to the interested person device data usage either when the smart phone is in close proximity to a mobile transceiver, the connection is made and the data is transferred. Detecting such a micro chip is very difficult, and with the breakthrough of Internet of Things this technology is evolving. That's why we need to buy smart phones from trusted places, also a smart phone that is a gift from someone is an easy way to deceive, but not always.

The third case is the simplest and most widespread, based on the naive and ignorant of user about the security and use of smart phone and applications.

The rules are simple:

1. Do not leave the smart phone exposed to third parties.
2. Do not open messages that do not know.
3. Do not click hyperlinks that do not know.
4. Do not open files from strangers.
5. Your smart phone is not as safe as you may believe.

Generally, the signs that your smart phone is being taped are:

1. The battery ends quickly after data is being used continuously, so check the applications. It can also be a coincidence.
2. Interrupting calls while talking, also this could cause by interference in the connection, changing location and trying again may be interference only at that place.
3. Noise during speech, this is a sign of a conference, but keep in mind that with pprofessional signal interception devices there is no noise, also the noise someone may hear may be either a device damage or is from Interference.
4. The smart phone is warm; this meaning several processes is running, check the device.
5. The smart phone crashes and becomes slow, this is due also to other reasons, depending on the smart phone and depending on the monitoring software sometimes the monitoring software is "heavy" and the smart phone can not respond.
6. Text messages that are received by irrelevant numbers, messages you have sent, and the recipient has received a different message than you sent should be suspected of monitoring or network interference that may be due to other infections.
7. The smart phone works alone and does not turn off. Surveillance spy software do not allow the user to have full control over the device for the simple reason that they are trying to keep the spy software on the device.

The above are the basic rules that apply, continue reading:

1. Surveillance software does not appear in installed applications.
2. Resetting to factory settings may not permanently eliminate the surveillance software.
3. Scrambled applications are easily localized, while well-designed applications run on Stealth Mode and are extremely difficult to detect even with anti-malware control.
4. A smart phone surveillance software can be downloaded to the smart phone through another application.

Conclusion

Buying a smart phone from a trusted place we are protected from the second case above. A smart phone that could work exclusively on 4G/3G and not 2G networks would be the best. If we imagine a mobile phone, not a smart phone that could work exclusively on 4G/3G networks rather than 2G, the third case above will be eliminated. Communications security should in no way be taken safe.

Christos Beretas is an IT technologist and is involved in the security of networks and systems.Member of Alpha Beta Kappa Honor Society, Ohio, USA

References

1. Kevin D Murray. Is My Cell Phone Bugged? Everything You Need to Know to Keep Your Mobile Conversations Private. Emerald Book Company 2011.
2. John Martin. How To Hack A Cell Phone: Remotely Control Any Cell Phone Kindle Edition 2015.