Can a Cell Phone Be Bugged?

By

Thomas J. Slovenski
Certified Mobile Forensics Examiner
and Instructor
Cellular Forensics, LLC
South Carolina
SLED PDC 2073

Introduction:

Practically every day, we hear a report about someone’s cell phone being “bugged”. From famous stars to politicians to everyday housewives, the same phrase is lamented:
“I think my cell phone is bugged!”

The compromise of a cell phone’s security can be very dangerous. No one will doubt that a Fortune 500 company could lose years of R&D results, new products and company secrets if a key employee’s cell phone was “bugged”. Terrorists could infiltrate our military strategies and place soldiers in harm's way. Police Officers security could be compromised on a high end narcotics raid and even a bank account could be cleaned out due to inept security of one’s cell phone. Lastly, a doctor or attorney could be in a world of hurt if their clients records, and emails were compromised. The dangers and aftermath of a compromised cell phone are quite evident as well as devastating.

But, is this threat called “Mobile Spyware” all “hype” or dangerously real?
In 2008, after being asked this question by numerous law enforcement officers and civilians, this Mobile Forensics Examiner attempted to find someone with the answers. My search took me to well known computer virus software companies and experts who would not give me an answer or did not know of one. The answers were not to be found.

Finally I found someone in a foreign country who knew what I was talking about and who was able to start to answer the questions I had. From this platform I then found further answers on my own through many hours of testing and evaluating mobile spyware products and countless cell phones of different brands and operating systems. From all this investment of time, money and energy, I developed my own series of tests, examinations and procedures in mobile forensic spyware discovery and eradication. I finally had the answers I was looking for about these mobile “Bugs”.

Consequently, I became the first Mobile Examiner in the USA to offer a bona-fide forensic service strictly for the discovery of Mobile Spyware on a victim’s cell phone. From there I went on to teach numerous international military, law enforcement and civilian investigators the answers I found and the procedures needed for a proper mobile forensic spyware examination.

**Mobile Phone Spyware Q & A**

I will attempt to answer the most commonly asked questions with answers based on my many years of mobile spyware examinations:

1. *Is there really such a thing as "Mobile Phone Spyware."* The answer is YES. Google mobile phone spyware and see for yourself.

2. *Do they all work as described?* No, they don't. I have tested a plethora of them and found those that were mere marketing hype and a money stealing ploy than the real thing. But, I also found those that actually did work and worked quite well.
3. Does the Bad Guy have to have the phone in hand to put the spyware on the phone? In most cases, yes. However, I have seen at least one program that will work without the phone manually injected. Technology is ever evolving and the spyware market is a huge money maker for hackers.

4. What Spy Programs work? Sorry, due to liability reasons, I am not at liberty to tell you which ones do work.

5. Is Mobile Spyware Illegal? If you've looked at many of the popular spyware programs on the web, you will no doubt see where they market them as "family safety" type programs. However, nefariously using these programs to spy on a spouse, lover, colleague or partner is illegal and is classified as "Wiretapping."

6. What are some of the signs that my phone may be bugged? Common indicators are:
   - battery life greatly depleting
   - background noise that you can't identify
   - others knowing your plans

7. Can the Spyware be seen with the naked eye? If an average examiner can get deep enough in to a phone, he may be able to see it. BUT, seeing it and identifying what it is are two different stories. The really effective spyware programs are made to hide in plain sight. One would need to know what to look for since the programs change with each new update and operating system they infect. What was identified last year could be a whole different animal come this year. Think of spyware like any bug, it changes for its environment.

8. Can the average phone examiner find the spyware? Not really. Unless they have been trained on what to look for, where it hides and how to find it, the average examiner is lost.
9. *Can Mobile Spyware be installed in any phone?* Generally, any Smart Phone, Android or iPhone, is in danger of infection. Feature Phones such as a cheap flip phone or a feature only phone does not have the operating system to handle a big complicated spyware program.

10. *Does an Android Phone have to be "rooted" to become infected?* No.

11. *Does an iPhone have to be "jailbroken" to be infected?* Usually, yes. But again, I have seen a new culprit that bypasses the phone altogether and gets right into the iPhones backup system and pulls the data. So no longer is the iPhone sacred ground. It's data can be hacked as well.

12. *When the infected phone’s data is captured, where does it go?* It depends on the spyware program being used. Some spyware programs will send the stolen data and phone calls directly to the suspect's phone, while others will load them into a cloud account for the suspect to view at their pleasure.

13. *Is there a program on the market that I can install on my Smart Phone that will catch spyware?* Everyone likes the warm fuzzy feeling they get from watching a program scan their phone. But looks aren't everything. Since all virus/spyware programs are reactive, that means they are only as good as the programmers behind them. No program is as current as the market. They are always playing catch-up. The only way to really know if you have spyware on your phone is to have it examined by a knowledgeable examiner specializing in mobile spyware discovery.

14. *If spyware is found on my phone, is there a way to find out who put it on there?* Yes, there are ways.
Conclusion

With the ever increasing availability of Smart Phones, there will always be the danger of infection through spyware. Knowing of it's existence is half the battle. Combating it is like fighting any other virus, whether it be a cold or a digital virus: constant vigilance and precautions need to be taken to avoid infection. However, if infected, there are ways to find the "bug" and defeat it.

About the Author: Tom Slovenski is a licensed and certified Cellular Forensic Examiner. As a former police veteran and digital forensics examiner, Tom has over 25 years of experience in law enforcement and digital investigations. Tom specializes in mobile forensic examinations and data recovery, as well as spyware discovery and tower analysis. Tom is also a vetted instructor for the US Department of States Anti Terrorism Assistance Program and is the published author of "Cellular Forensics for First Responders" available on Amazon.com. He can be reached at 864-962-7307 or at tom@cellularforensics.com. Visit his website: http://cellularforensics.com for more information.