When Clients Ask, "Is My Cell Phone Bugged?" Know What To Say

by Kevin D. Murray, CPP, CISM

It is a simple question, but most security professionals do not have a proper answer.

People come to you for help. You are expected to know. The worst thing you can do is turn them away. You can help. All it takes is a little easy-to-learn knowledge. Even if your technical abilities are nil, this article will get you started.

I have been asked, "Is my cell phone bugged?" often by long-term corporate clients to the average person who just calls in. Everyone has the same fear, and rightfully so. Infecting a smartphone with low-cost, highly-effective spyware is easy to do.

Visit some of the web sites selling these programs to see for yourself:

- Spyera
- Mobilespy
- Flexispy
- Mobistealth
- SpyBubble
- mSpy
- PhoneControl
- SPYPhoneTap
- Retina-X[1]

[1] According to The Wall Street Journal (Justin Scheck, "Stalkers Exploit Cellphone GPS," August 3, 2010), the company's operations director says Retina-X has sold 60,000 copies of its Mobile Spy software. At $99.97 for the annual subscription, this comes to $5,998,200 per year for simply licensing a piece of software—very profitable. With this enormous income, you can understand how spyware developers can hire some of the best software designers in the business—and they do.

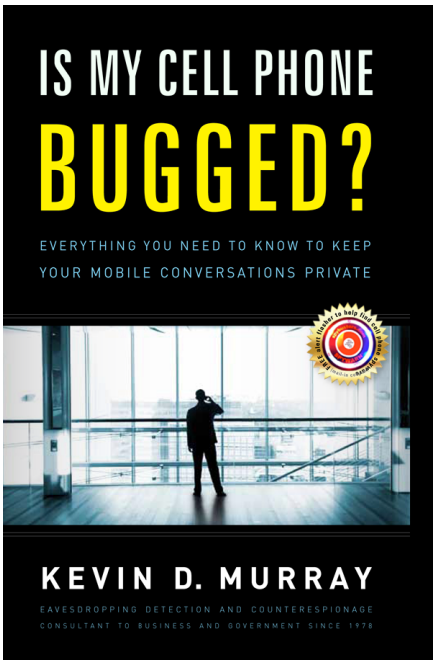
Myth
An expensive forensic exam of a smartphone is the best way to identify a spyware infection to solve the person's problem.

Reality
Their problem is not really the spyware, it's the spy. Tying the criminal to the crime will end the problem, not simply discovering spyware.

If you only find the spyware, the snoop remains free to spy again. Next time they may even resort to other surveillance methods, and certainly, they will be more covert about it.

The following advice is a light summary of detailed information contained in the book, "Is My Cell Phone Bugged?" Once you have read the book you will have a very important, new investigative skill.

Let's get started...



Step One
When asked, "Is my cell phone bugged?" don't turn them away.

Work with them to create a sting operation. Try to reveal circumstantial evidence which connects the snoop to the snooping.

Have them use their phone to spread information which will trigger a response from the snoop. Make sure the tidbit of information is used only once, and only with one form of communication: a phone call, text, email, adding a new a contact, and even going somewhere to generate interesting GPS information.

These bits of information should be something which will cause the snoop to react by saying something, or do something, based solely on that bit of information.

One positive result is not enough. You need to anticipate a coincidence defense. Generate three or more positive results. Keep a detailed log of all the actions (date, time, tidbit, reaction, etc.)

The end result: proof a problem exists, and that spyware was the method of interception. This ties the suspect to the crime. There is no other way they could have possibly known the information you planted has they not been using spyware.

Step Two

Conduct your own analysis of what the phone is doing. It's simple. An infected phone transmits more often than a phone without spyware. This is the common denominator of all spyware infections. The phone must work overtime to send the snoop duplicate texts, emails, contacts, phone logs, etc.

A. Begin the transmission test by first turning off all apps, Wi-Fi, 3G/4G. Those legitimate transmissions make spyware transmissions more difficult to spot. Be aware that all mobile phones regularly transmit information to the cell towers while in stand-by mode. It is this background activity you will be measuring, along with any spyware transmissions.

> Note: The book contains an electronic sensor which lights up when the phone transmits, but the test may also be accomplished by placing the phone near a radio or other piece of audio equipment and listening for the emissions. Cell phone transmissions often emit short raspy noises on nearby audio equipment when transmitting. Sound sample.[2]

B. Using a stopwatch – an on-line chess stopwatch works best[3] – time the moments when you hear the phone transmitting. An hour is usually long enough. The transmission rate for uninfected phones is about 4-5% or less. Conduct the test a few times, at different times of the day. This test is especially telling when conducted immediately after using the phone.

> Note: Think about where you will be conducting this test. An infected phone with GPS capability might reveal your location and cause the snoop to become suspicious.

The results you get from your sting and timing tests will lead you to a final conclusion.

Extra Credit: The book, "Is My Cell Phone Bugged?"[4] contains 18 observational questions about the phone in question. Ask the person you are assisting these questions, or send

---

[2] http://www.spybusters.com/mov/GSM Noise.mov

[3] http://www.online-stopwatch.com/full-screen-chess-timer/

[4] http://www.IsMyCellPhoneBugged.com

the questions as a survey to be filled out and returned. Their answers will provide additional supportive evidence about the likelihood of spyware having infected their phone.

Step Three
Now that you have collected the evidence, visit an attorney with the person you are helping. Explain the problem, share your collected evidence, and plan the best way to stop the snoop.

The solution may be an attorney's letter, a court order, or prosecution (criminal and/or civil). Both electronic surveillance and harassment laws may be used to stomp on the snoop's toes and stop the spying once and for all.

Don't be reluctant to learn this new investigative skill. It is effective and easy to learn. People look to you for protection. Don't let them down. You can help!

P.S. Consider including a copy of "Is My Cell Phone Bugged?" as part of your professional consultation with clients, or point them to IsMyCellPhoneBugged.com to purchase directly. It also makes a welcome business gift; low cost, high perceived value. Bulk pricing available.

About the Author

Kevin D. Murray, CPP, CISM is an independent, professional security consultant. He has been solving electronic eavesdropping, security, and counterespionage matters since 1973 while with Pinkerton's Inc., and from 1978 to present at his consulting firm, Murray Associates.

Murray Associates provides advanced eavesdropping detection (technical surveillance countermeasures, TSCM) and counterespionage consulting services to business, government, and at-risk individuals.

You can contact him at counterespionage.com and keep up with all the latest spy news and security tips at spybusters.blogspot.com

v.120915