International Investigators, Inc
3216 N. Pennsylvania Street
Indianapolis, Indiana 46205

(800) 403-8111
Fax: (317) 926-1177
timwilcox@iiiweb.net

www.iiiweb.net

CELL PHONE SPYWARE FACTS

- The manner in which spyware is installed on the phone is dependent upon the capabilities of the phone itself
    - Smart phones can have spyware downloaded from websites, Bluetooth connection, mms messages, and pc connection.
- There is no single spyware program that can be installed on all phones since there are many different OS's and each one must have code written for the specific OS.
- Symbian OS is the most common OS but has hundreds if not thousands of different versions depending on the software development intended on the device. Many spyware programs cannot work for more than a few versions, if even more than one version.
- Spyware programs that can be installed via Bluetooth connection claim to be able to install software remotely but as with all Bluetooth devices it must have been paired with the target phone first.
- It is possible for the remote installation of spyware onto a target phone, but this involves "tricking" the user into downloading and installing the malware.
    - Sending bogus mms messages with the intent to install malware is the easiest way to trick a target user. By sending messages with fake links could get the user to unknowingly download spyware programs. Most of these attacks involve making the user think the messages came from the carrier and posing as upgrades to the firmware on the phone especially through email. Some techniques use photos embedded with third party stegnography hiding the spyware.
- Some spyware claims that it can extract data and voice from a target phone without installing any spyware on the target phone. We are still researching a specific software with this claim but at this time we can neither confirm nor deny this possibility.
- Spyware programs can collect the following information and possibly more: contact data, mms, sms, phone call history, email history, webpage history, pictures, video, GPS location, cell tower triangulation history (less accurate), file system information.
- Spyware programs can remotely become a covert third party to conversations as well as use the phone as a bug so that room audio is available whenever the bad guy chooses. The spyware can alert the bad guy when a call is made as well as texts and emails so they can call the phone and listen in. No call history for the bad guys phone is saved on the phone although it will show up in the service providers records.
- As far as prevention of spyware installation is concerned, blackberry's have the best protection by far. The security code can only be guessed a certain number of times before it completely erases all information from the phone and has no obvious "backdoor" to circumvent this issue. Other phones can be protected more or less by passwords but the password must not be too easy to guess and some phones can allow a reset of the password, which is not that hard to accomplish in the wrong hands.
- There is no known blanket spyware protections that will protect all cell phones

UNCONVENTIONAL COVERT ESPIONAGE TECHNIQUES

The following techniques can be found and ordered (purchased) over the internet from foreign spy device suppliers, shipped to the US and rarely intercepted by US Customs.

A device that can be cleverly concealed in a FAX machine, which will copy all faxed documents along with the phone numbers and at a later time, upon a command from the bad guy, download all of the copies. This device can also be commanded, by the bad guy, to turn on an amplified microphone to monitor the conversations around the fax machine. There are many configurations that are available.

A similar device to the FAX bug can be installed in a printer or copy machine. Most of the newer copy machines utilize a hard drive that maintains a copy of every document copied (scanned). These are easily accessed by service techs or "others" that have physical access to the office area.

Most offices utilize shredders; some have a large collection box which is periodically picked up by a trusted shredding company. Others utilize the small standalone units. There is an overseas company that provides a bugged shredder that has a hidden digital scanner built into the injected molded plastic document insertion top.

There are 3 models:

- One has a hidden micro SD card that will hold 30k to 40k of documents.
- One has an electrical "digital carrier current" transmitter that transmits the documents over the electrical power lines to a matched receiver somewhere else in the building. That receiver has a printer connected so that while the document is being shredded in one office, it is being printed out in another office.
- The third model incorporates a RF transmitter/receiver which is connected to a document storage device. This allows the bad guy to pull his vehicle into the office parking lot and transmit a RF signal to the shredder (similar to a garage door opener) which causes the unit to "burst transmit" all of the stored documents to the bad guy's receiver.

Several overseas companies offer Cellular bugs, which are an entire cell phone packaged in a tiny circuit, cleverly hidden in innocent appearing appliances, i.e.: Computer Mouse, Computer Keyboard, Power Strip Surge Suppressor, Table Clock, Wall Clock, Wall Thermostat, Clock Radio, Electric Pencil Sharpener, and many more devices that have an ongoing electrical power source. They even have them designed for monitoring you in your car with a bugged Radar Detector and Car DC to AC Power Inverter.

For those offices or homes that utilize Comcast, Bright house, AT&T U-verse, etc. BEWARE... If they provide broadband for your computers and VoIP for your phone service, you can be monitored by the bad guys. All cable subscribers have an IP address. This is so that the cable company can perform remote diagnostics, firmware and software modifications and upgrades. There are a number of software programs available, i.e. (Wireshark), that will allow the bad guys to invade your IP address (by "spoofing" the carrier for the address) and monitor your VoIP phone calls, turn on the microphones in your computers and listen to the conversations around your computers. They can also view everything on your computer hard drive. Your most secure source for TV is through the Satellite or Dish networks. VoIP is inherently vulnerable regardless of the provider. Skype is also vulnerable.

NOTE: All of the above eavesdropping and data interception techniques are criminal offenses covered under Public Law 90-351, Title III, Chapter 18, USC2510-2520 and most state laws

RECOMMENDATIONS

- Be cognizant of all of the above malevolent technologies.

- Employ as many countermeasures as possible.
- During sensitive meetings remove all cell phones or purchase cell signal detectors and jammers.
- Purchase and install acoustic noise generators (white/pink noise transducers) in offices/conference rooms where sensitive meetings take place, and hidden motion activated video cameras which will record and document unauthorized intruders.
- Periodically employ a high level technical surveillance countermeasures (TSCM) team to conduct "sweeps" in the sensitive areas. Some larger firms utilize "Safe rooms" that provide a high level of voice privacy.

WHAT ARE SOME INDICATORS THAT MY CELL PHONE MIGHT HAVE MALWARE/SPYWARE?

Top 10 suspicious indicators that your cell phone might have illegally installed spyware:

1. Battery is warm when not in use
2. Battery life is noticeably diminished each day.
3. Some Blackberry's; communication icon on right screen flashing
4. Small pauses of audible communication while talking
5. Light audible tones, beeps or clicks throughout conversation
6. Flashing or flickering on display or change of brightness
7. Some spyware programs require the spy to manually mute their phone, therefore you might hear them in the background at the beginning of conversation or when they tap in.
8. Slower internet access.
9. Suspicious 3rd parties have detailed knowledge of your private conversations and locations (GPS)
10. You have opened a suspicious email or one from a potential spy. (allowing Trojan horse to install spyware remotely)

The smarter the cell phones the easier it is to hide spyware.

If the eavesdropping perpetrator has effectively installed spyware on your phone, then that perpetrator has total control, i.e. obtain all text messages, emails, internet sites visited GPS location, photos and videos obtained, etc.

ABOUT US

In 2004, International Investigators, Inc., our parent company, was involved in a Technical Surveillance Countermeasures sweep of a Client's home and office in Orange County, California. When no bugs, eavesdropping devices or wire taps were found in either location, one of our team members began further questioning of our Client in an attempt to determine what could possibly have been used to conduct an effective eavesdropping operation on her private conversations with her attorney and others. It was learned that the only common denominator was her cell phone which her estranged husband had physical access to during their cohabitation. Her husband was an IT expert with a large company and had access to this spyware technology. At that point we had no experience with cell phone bugs or how to handle them, but knew the

protocol when examining computers for Trojan horses or spyware. Since a cell phone was just a less complicated computer at that time, we treated it as such. Upon further investigation a malware (usually referred to as spyware or Trojan horse), program was found in the phone that enabled her husband to monitor her cell phone conversations and more specifically to remotely turn on her cell phone while it was in the standby mode, either in her purse or on a table and obtaining clear audio of conversations surrounding the phone. This was the beginning of our mobile forensics lab.

Today our mobile forensics lab division utilizes state of the art software and hardware platforms to search for even the most covert malware programs that can be installed in today's high-tech phones. We are part of a mobile forensics collaboration with the leading examiners in the United States that exchange information so that we are always aware of new malware programs that are literally "born" each day. Mobile forensics examiners in the collaboration find nearly 10 to 15 new malware programs per day with well over 4,000 completely different types or variations known to be in existence presently.

OUR PROCEDURE

The first step involves always keeping powered phones in a Faraday case to prevent signals from leaving and entering the phone. One problem that is becoming more prevalent is that more malware/spyware programs are being found with remote software removal functions that allow the perpetrator to remove the malware from the phone remotely. Although it can sometimes leave traces of its prior existence, more information could have been detected and obtained had the phone been protected from these removal functions, therefore by keeping the phones in Faraday cases we remove this problem completely.

Examiner then physically examines the phone while in a Faraday case to determine if there are any signs of malware while testing the functionality of the phone. This can provide valuable first clues as to the type of malware that has already been installed into the device.

In order to obtain any information from the phone we must first connect to the phone's operating system SIM card if applicable. The two main methods of connecting the phone itself involve either a USB connection and/or a Blue Tooth connection. We always use USB connections since it is the most secure connection and easiest to work with when the phone is in the Faraday case. Once the phone is connected to our software, we then perform a memory dump. This basically extracts all possible data from the phone onto our computer for isolated examination. We then search through the data for any signs of malware and attempt to locate its origin, although locating its origin is not likely, it is however possible. We then run the data through a 2nd software package that attempts to locate any malware that might have been missed on the 1st run. This process is extensive and can take many hours on some phones. **WE WILL NOT DELETE ANYTHING FROM THE PHONE UNLESS YOU REQUEST THAT WE DO SO.**

Once the examination is complete, we then generate a detailed report of our exact findings. Some reports are more extensive than others depending upon the model examined and how robust its operating system is.

CAN I EXAMINE MY OWN PHONE?

It is nearly impossible on most phones to detect malware without the use of sophisticated software. Not only is forensic spyware detection software expensive, it is also highly complex and difficult to master. Furthermore, the software is only as good as the examiner who utilizes it. The examiner must not only know how to operate the software to its full potential but also be able to manually search through the data (lines of code) to find the spyware. An examiner must have completed multiple certification courses prior to becoming an expert examiner. This is particularly useful if any evidence obtained is to be introduced into a court of law. Credibility is very important in technical evidence.

HOW DO I GET MY PHONE TO YOU?

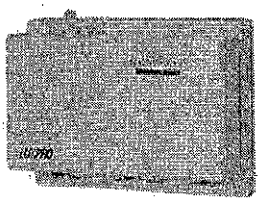
We recommend placing the phone in a well protected container with the battery separated from the phone and supplied along with the charger. If you are unable to remove the battery from the phone then we highly recommend that you turn it off and wrap the phone 8 or 10 times with metal foil which will essentially become a Faraday cage. This will prevent any signals from leaving or entering the phone prior to our examination. Once we receive your phone an examination begins within one business day and usually takes approximately seven days to complete prior to sending the phone back to you. Sometimes we are able to accomplish the examination in less time.

Rental:
$175.00/wk

COMPUTER KEYBOARD HIDDEN AUDIO MONITORING DEVICE
This revolutionary surveillance product has a wireless (GSM-based) audio monitoring device hidden inside a partially-functional computer keyboard.

New Feature: Voice Activation! The unit will call YOU when it detects sounds.

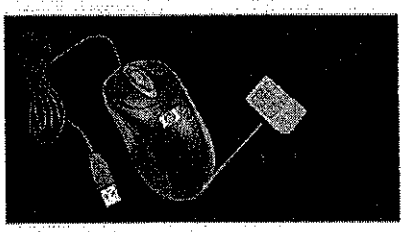
Price:
$1,209.00



Rental:
$175.00/wk

THERMOSTAT HIDDEN AUDIO MONITORING DEVICE
This revolutionary surveillance product has a wireless (GSM-based) audio monitoring device hidden inside a non-functional Thermostat.

New Feature: Voice Activation! The unit will call YOU when it detects sounds.

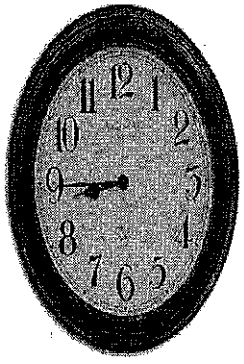


Price:
$1209.00

Rental:
$175.00/wk

COMPUTER MOUSE HIDDEN AUDIO MONITORING DEVICE
This revolutionary surveillance product has a wireless (GSM-based) audio monitoring device hidden inside a fully-functional Computer Mouse.

Now Includes Sound or Voice-Activation!

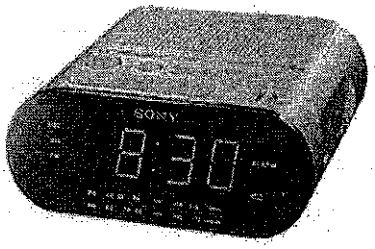


Price:
$1209.00

Rental:
$175.00/wk

WALL CLOCK HIDDEN AUDIO MONITORING DEVICE
This revolutionary surveillance product has a wireless (GSM-based) audio monitoring device hidden inside a fully-functional Wall Clock.

Now Includes Sound or Voice-Activation!



Rental:
$175.00/wk

ALARM CLOCK RADIO HIDDEN AUDIO MONITORING DEVICE
This revolutionary surveillance product has a wireless (GSM-based) audio monitoring device hidden inside a fully-functional Alarm Clock Radio.

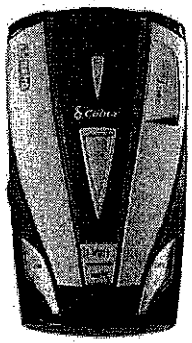
Now Includes Sound or Voice-Activation!

Price:
$1,209.00

Rental:
$175.00/wk

POWER STRIP HIDDEN AUDIO (GSM-BASED) MONITORING DEVICE
This revolutionary wireless (GSM-based) audio monitoring device is a fully-functional Power Strip.

Now Includes Sound or Voice-Activation!

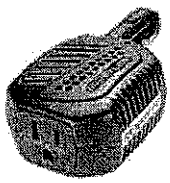


Price:
$1,209.00

Rental:
$175.00/wk

RADAR DETECTOR HIDDEN AUDIO MONITORING DEVICE
This revolutionary wireless (GSM-based) audio monitoring device is a non-functional Radar Detector.

Now Includes Sound or Voice-Activation!



Price:
$1,209.00

Rental:
$175.00/wk

CAR (DC TO AC) POWER INVERTER HIDDEN AUDIO MONITORING DEVICE
This revolutionary wireless (GSM-based) audio monitoring device is a non-functional **Car (DC to AC) Power Inverter**. Call in and monitor discreetly!

Now Includes Sound or Voice-Activation!