ISSUE 26

The Circuit

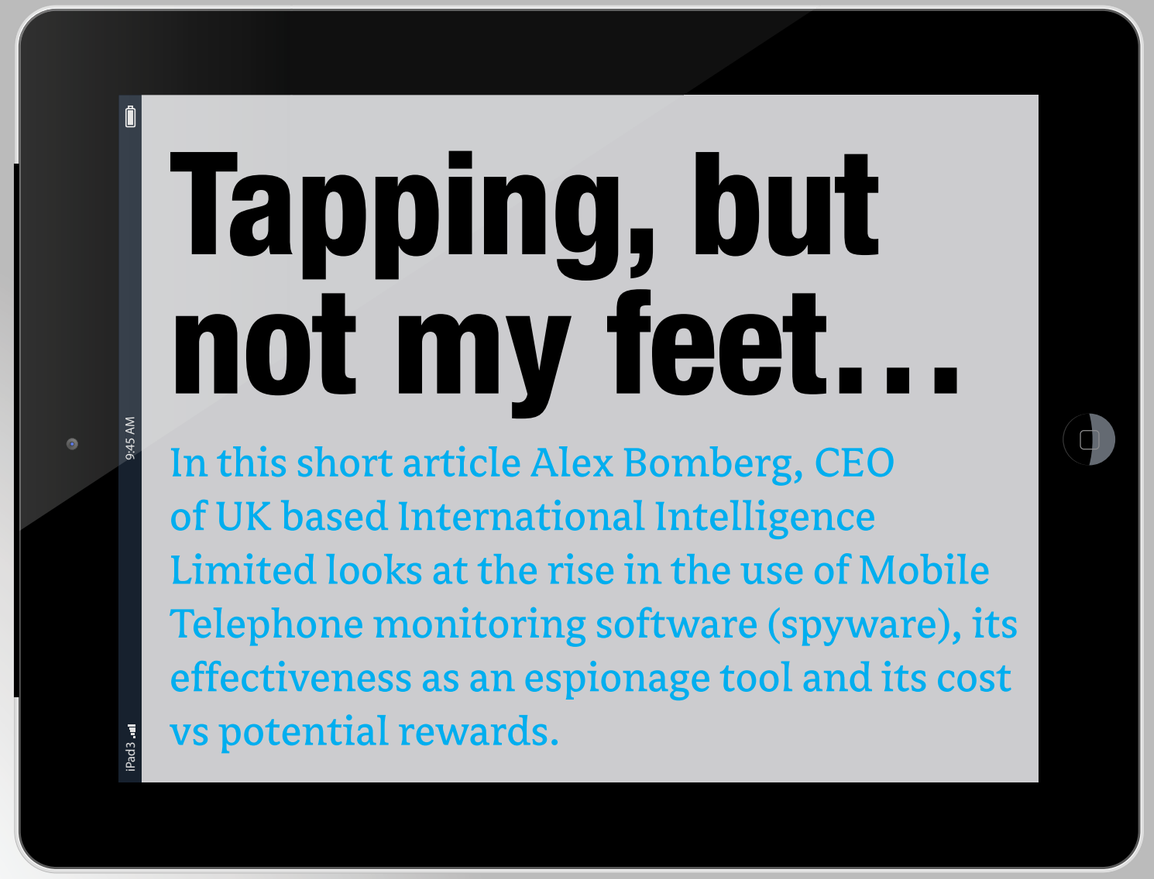
www.circuit-magazine.com

Tapping Impenetrable? Think Again!

Columbia
A Chance for Peace?

How disciplined is your mind? | Presentation skills | Patient Handover

By: Alex Bomberg



Tapping, but not my feet…

In this short article Alex Bomberg, CEO of UK based International Intelligence Limited looks at the rise in the use of Mobile Telephone monitoring software (spyware), its effectiveness as an espionage tool and its cost vs potential rewards.

"People are three times more likely to open a message attachment on a mobile device than they are on a desk top computer, because they think it's safe"

Part of our remit to all of our clients is to educate them and keep them abreast to any new trend or threat, from a rise in theft due to economic turndown to the more targeted corporate crimes such as acts of espionage. Many companies spend hundreds of thousands of pounds each year on security and IT security to ensure that secrets stay exactly that, secret. If you were to leak one average days' worth of emails or text messages to your largest competitor, just how much damage might that cause?

Intelligence at what cost?

The use of mobile/cell phone devices and their impact on our lives, communication habit and behaviour is exactly what will define this short period history. According to the Pew Research Internet Project, as of January 2014 90% of Americans (adults) have a cell phone and 58% own a smartphone (Pew Research, 2014) and this is exactly how the majority of people access business data, communications and emails. >

By: Alex Bomberg

It's not just a phone anymore, it's a computer, more powerful than the home computers of the late 1990's, the Samsung Galaxy S5 for example has 2GB of Ram and a 2.5GHz Quad-Core processor.

"Smart phones" have totally changed human behaviour. According to one 2012 academic paper by James Roberts, Ph.D., professor of Marketing at Baylor's Hankamer School of Business, people (on average) check there mobile/cell phone every six minutes during the working day.

This is not a new threat and is being more widely used as an espionage tool due to the huge amount of intelligence that can be gathered with just one well-placed phone. Mobile telephone or Cell phone monitoring software is now very, very widely available and has been a growth sector since the mid 2000's.

A Google search for "monitoring software for mobile phones" gives hundreds and hundreds of results, it's only when you start to do some basic research into this software that it becomes very scary. Less than £100 is what you can pay for software to monitor a mobile/cell phone. And, this software can monitor ALL user activity on that device, covertly.

Worried yet? Well they cannot only see all of that information, they can activate the GPS and see your exact location, that plus see and have access to any files on your device this of course includes files in the form of email attachments.

There have also been cases of people stealing photographs off mobile devices for blackmail purposes (Sextortion) or for example the theft and release of photos of Scarlett Johansson.

"Some software can block actions such as calls to certain numbers or website access or even wipe the phone remotely. Most people would be totally buggered at this point!"

What is it possible to monitor?

Some phone monitoring software does allow users to record and monitor calls. Generally most software packages include the following as standard:

- SMS activity
- Ingoing-outgoing call log
- Location/GPS
- Internet browsing activity (URL's)
- Pictures & Videos
- Emails
- Sim-Card Changes

Some monitoring software offer the user (the person monitoring) the option to command the device to take photos, video, audio (background audio and calls), to view the target devices screen or as covered above, to wipe the device. So, this software that is available for under £100 can be used to turn your mobile/cell phone or device in to a GSM eavesdropping device, that you are carrying everywhere and regularly charging.

How?

Much of this software is marketed as "parental control software" or "cheating spouse" etc. and is legally sold and marketed as such.

Monitoring software is installed directly on to your telephone or device normally by having direct access to said phone or device. That said some companies make claims of offering "remote install" spy/monitoring software. At this present time I do not think that this is technically possible on some models of phone but it may well be on others.

Installation of software is very, very quick and can be done from start to finish within 5-15mins depending on the software and the device.

After signing up, purchasing the software and installing it, monitoring is normally done by logging on to a server. It really is that simple and is sold mainly as a subscription service.

Is this a viable espionage tool?

100% yes, absolutely mobile phone monitoring software if installed correctly is a great, cheap and easy tool for espionage. The most practical way of deployment would be gifting someone with a "new" phone. Installation and testing on a target phone might prove problematic if the phone could only be obtained for a short period, unless of course it went missing then was found an hour or day later – as often happens.

A £100 espionage tool that would enable monitoring or your email, telephone calls and texts, plus any mobile internet access; and people worry about Government monitoring! BYOD – Bring your own device

One very obvious threat to companies is individuals taking their own devices in to >

By: Alex Bomberg

Users are less likely to report a lost device to IT when it's their own for fear of losing their personal data.

the place of work; known as "Bring your own device" (BYOD). BYOD is a huge risk to companies, from employees brining in and using USB memory sticks to employee owned devices being used and sanctioned to receive work emails. When it comes to phones infected with monitoring software being introduced into this "controlled" environment, then risks increase especially when we consider file sharing.

"Users are less likely to report a lost device to IT when it's their own for fear of losing their personal data, along with any company information, when the device is wiped.*"
*(Deloitte CIO Journal, 2014).

Many businesses are well versed in Mobile Device Management (MDM) and there are many programmes and tools that aid in managing the use of BYOD's across corporate networks. But with many companies and organisations now moving more and more towards "Cloud computing" the mobile device remains a weak link.

It is imperative that IT Managers have an understanding of phone monitoring software and bear this in mind when it comes to managing a BYOD policy. The risks that monitored phones pose should not be underestimated, once they have access to corporate network or access corporate data.

Many savvy IT Managers in managing the BYOD issue are setting up "Shadow IT" systems, yet this is no defence to the damage caused by phone monitoring software, in that documents that are shared by the infected device or via sync'd email are going to be accessed and viewable by any "attacker", i.e. the person or persons that have infected said mobile phone.

Just the simple loss of a phone/device can be catastrophic. US technology giant Symantec Corporation in 2012 conducted a social experiment with 50 "lost" smartphones spread over five North American cities. Prior to the strategic placing of these 50 smartphones they were all loaded with what Symantec calls "a collection of simulated corporate and personal data". The smartphones were loaded with tracking and monitoring software to enable monitoring once the devices were found.

The findings were shocking:

- 83% had attempts to access business apps
- 89% had attempts to access personal apps
- 96% had attempts to access at least some type of data
- 50% of finders contacted the owner and offered to help return the phone

The most popular apps accessed were:

- Contacts
- Private Pictures
- Social Networking
- Webmail
- Passwords

The full report titled "The Symantec Smartphone Honey Stick Project" is available on-line.

Simple advice

1. Never accept a mobile telephone as a gift. Not ever.
2. Never leave your telephone unattended.
3. Never communicate ultra-sensitive information via unencrypted electronic means.
4. Ask your IT department what steps they are taking regarding this issue.
5. If you lose a phone/device that you use for work – report it to IT immediately.

Tell-tale signs of tampering

1. Drain in power. Does the device lose/use more power than normal?
2. Strange activity. Is the device functioning as is should?
3. Rebooting or powering down. Does your device reboot itself?
4. Odd text messages. Coded/scripted text messages?
5. Phone errors? Often spyware will cause errors to the phones operating system.

Is phone/device monitoring software invisible?

The simple answer to this is yes, most software it is hidden and invisible from "normal user" activity, in that a normal user would not even know where to start looking for software logs and programmes.

Want to know more'

If you would like to know more about this threat in more detail then please contact us via info@international-intelligence.co.uk or info@international-intelligence.fr