



## Mobile Devices – The Spy Within

In an era, where globalization through technology, has brought the significance of the protection of your virtual knowledge to the forefront, you are mandated to combat pro-actively towards the safe retention of your trade secrets. However, the specialization with which this technical field has progressed from plug-and-play bugging devices, to advance covertly listening devices including the eavesdropping of your communication devices, requires the services of innovative, up to date experts. It is the mission and overall objective of Advanced Corporate Solutions, to provide you with the necessary pro-active aids and means to protect your Company I.P through Electronic Counter-Measures Investigations “Debugging” and the implementation and management of Counter Espionage and Counter Crime Measures.

### The security risk associated with Mobile devices

Mobile devices, which include smart phones and tablet computers, provide increased functionality and ease of use to people, anywhere and anytime.

Smart phones are the new computers. These devices contain a tremendous amount of personal and even business related information. With the rapidly increasing advances in technology, everyday life is starting to depend on these wireless technologies, but it brings greater risk and some unique security threats.



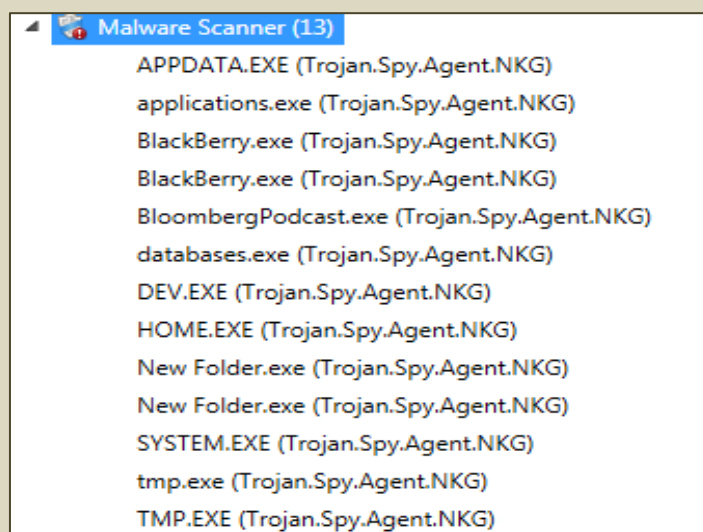
**Mobile device malware (malicious code) has increased exponentially over the past few years. The sophistication of these exploits has also increased exponentially, making detection and eradication very difficult.**

Anyone can install eavesdropping software on your smart phone, as long as they have access to your phone even for a few minutes. This can result in them gaining access to all your private data such as SMS's, emails, pictures, location information, call logs and even listen in on actual calls.

Cellebrite is a world leader in the development of advance mobile forensic hardware and software products. The Universal Forensic Extraction Device (UFED) Touch Ultimate from Cellebrite is an example of hardware used by mobile device investigators to gather information from mobile devices that may contain infected and malicious data.



**Some malicious code will even allow the attacker to switch on the microphone of the device unnoticed and listen in on Conversations or use the camera to secretly take pictures.**



**An example of a mobile device result after being scanned for malware**

It is clearly visible that a myriad of software spyware is installed on this device rendering the user's phone vulnerable leaving all their valuable information at risk.

**For further information,  
please contact Riaan Bellingan (Snr) on +27 (0) 82 491 5086,  
André Oosthuizen on +27 (0) 83 260 6125,  
Riaan Bellingan (Jnr) on +27 (0) 72 671 5764  
and visit [www.acsolutions.co.za](http://www.acsolutions.co.za).**

**[CLICK HERE FOR REAL-LIFE EVENTS!!!](#)**