Advanced Corporate Solutions

"Debugging" Specialists | www.acsolutions.co.za

CELEBRATING 20 YEARS

Technical Surveillance Counter-Measures (TSCM)

By Riaan Bellingan

International Companies doing business in Africa generally have their African offices situated in South Africa, not only due to the stability in the country, but also because it has the most advanced infrastructure on the African continent. Corporate and Industrial Espionage is however, a global threat which can't be ignored. In an era where globalization through technology has brought the significance of the protection of virtual knowledge to the forefront, Companies are mandated and morally obliged to take pro-active steps to ensure the safe retention of their **Company Trade Secrets and Intellectual Property (IP).** The specialization with which this technical field has progressed from plug-and-play bugging devices, to advanced covert listening devices, including the eavesdropping of communication devices, requires the services of innovative, up to date experts to counter this threat.

"De-Bugging" Partners for 20 years in Europe & Sub – Saharan Africa

Advanced Corporate Solutions (ACS), as a major role player and specialist in the TSCM industry in Sub-Saharan Africa over the past 20 years, has through continuous Research and Development, in co-operation with International experts in this field, managed to keep their clients informed of not only the current trends and research on eavesdropping and bugging devices, but also on Mobile Device analysis. **ACS** receives the most sophisticated equipment and training in the use thereof from firms such as Blake Technical SARL (Mr. Dean La-Vey), Shearwater TSCM (Mr. John Little and Dean La-Vey), Research Electronics International (REI) USA (Mr. Lee Jones) and Winkelmann UK (Mr. Stephen Read).

ACS electronic surveillance investigators have been trained by Mr. Dean La-Vey of Blake Technical and Shearwater, who also provides refresher training on a regular basis. ACS investigators met Mr. La-Vey for the first time in 1993 and together, over the past two decades have established a bond in the field of "de-bugging" services, working together in Research and Development, and also doing TSCM tasks on buildings, aircraft, boats and vehicles.

General awareness throughout their corporate client base regarding these risks is now more relevant than ever, and many companies, especially financial institutions, are allocating independent budgets specifically for this task. Recognizing the importance of the ***protection of Intellectual Property***, they encourage their clients to regularly assess their particular requirements regarding the security of their communication systems.

SHEARWATER Technical Surveillance Counter Measures

Shearwater TSCM

BLAKE TECHNICAL SARL

Raptor RXi
www.winkelmann.co.uk

ACS can provide assistance, advice and support to potential foreign investors in South Africa, with their proven track record and experience in Risk Analysis and Security Risk Management Services. It is the mission and overall objective of ACS, to provide their clients with the necessary pro-active aids and means to protect their IP through TSCM "Debugging" and the implementation and management of Counter Espionage and Counter Crime Measures.

Mobile Device Analysis

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.

Universal Forensic Extraction Device (UFED) Touch Ultimate www.cellebrite.com

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 a smart phone, as long as they have access to the phone even for a few minutes. This can result in them gaining access to all 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.

ACS has consistently invested both time and financial resources in developing a new generation of counter measure methods. In doing so, they are always ready and able to assist in the proactive combating of any and all forms of corporate espionage.

For further information, please visit www.acsolutions.co.za or contact: Riaan Bellingan on +27 (0) 82 491 5086