Advanced Corporate Solutions
TSCM | "Debugging" Specialists | Service Excellence since 1995

dynamdre INNOVATIVE SOLUTIONS
Information Security I www.dynamdre.co.za

THE COAST IS CLEAR, PUT THE DEVICE BACK

"Mobile tablet used eavesdropping - Fact or Fiction"

How a Mobile Tablet was Maliciously Used to Spy

In this edition we look at how technology we take for granted, and used on a daily, was used for malicious eavesdropping.

Tablets let you do many of the same things as a traditional computer. Eavesdropping is a prevailing threat on tablet and mobile phones, with technology capable of tracking users, listening to their conversations and even logging their application usage becoming more pervasive and easier to come by.

Mobile devices contain access to all of our personal and corporate data. They are capable of tracking our location, listening to our conversations and seeing what we see, all in real time.

The TSCM / "Debugging" Investigation

The Managing Director (MD) of a leading South-African based company raised concerns that someone was gaining access to confidential information that, at the time, were only discussed within a restricted boardroom, accessed only by a closed group of confidants within the company.

The MD contacted Advanced Corporate Solutions (ACS), specialist in the field of Technical Surveillance Countermeasures (TSCM / "Debugging") to assist with a formal investigation into the matter. The team from ACS initiated a detailed sweep of the boardroom as well as adjacent offices.

Phase 1 of the investigation was conducted by making use of sophisticated, state of the art equipment, which unfortunately yielded no results and no malicious, eavesdropping devices were found within the target area. Being sure of his concerns, the MD requested that we propose any additional measures required to further the investigation and to try and uncover the source of information leakage.

Mobile devices were the only devices that were identified, as present during all the confidential meetings. We therefore suggested that a formal mobile forensic investigation and malware analysis be conducted on all the mobile devices present during the meetings.

The Digital Forensic Investigation

Phase 2 of our investigation focused on a formal digital forensic investigation and malware analysis, led by ACS and Dynamdre. The digital forensic investigation was conducted in accordance to industry best practices, which included the acquisition, imaging and forensic analysis of all devices that formed part of the scope of work.

Deleted messages were uncovered on the mobile devices and used as a source of information to the investigation. The content of some of the messages were quite alarming, as they implicated the IT manager and his involvement in the eavesdropping operation. The content of the messages detailed information relating to our TSCM / "Debugging" investigation phase to such extent that our team's arrival and progress made during the sweep, was discussed between the perpetrators. Not aware that phase 2 of our investigation would be initiated, the IT manager and perpetrators ended the communication with a message that read "It is safe now, you can put it back under the desk". Our team immediately went back to the restricted boardroom and found that a rogue tablet had been returned and neatly re-installed for eavesdropping purposes.

What can we learn from this?

Surveillance and eavesdropping have a wide variety of use cases, but they all essentially boil down to spying on a targeted user with an intended purpose.

These types of attacks are on the rise and growing in complexity - Mobile devices have rapidly become ground zero for a wide spectrum of risks that includes targeted surveillance, a range of malware families, non-compliant apps that leak data and vulnerabilities in device operating systems or apps. For some businesses and institutions, the ability to make secure calls and have secure conversations can make or break a company, safeguard the future of others and even save lives.

Whether you are a government, the military, a financial institution or simply a business where confidential information is discussed or shared, you need to be part of a proactive security culture.

TSCM / "Debugging" Sweeps / Assessments - Skilled TSCM / "Debugging" assessments needs to be conducted on a regular basis, at least once a month in high-profile areas of your organisation.

Advanced Corporate Solutions
TSCM | "Debugging" Specialists | Service Excellence since 1995

dynamdre INNOVATIVE SOLUTIONS
Information Security I www.dynamdre.co.za

Riaan Bellingan (Snr)
Office: +27 (0) 12 349 1779
Cell: +27 (0) 82 491 5086
Email: riaan@acsolutions.co.za
Website: www.acsolutions.co.za

Riaan Bellingan (Jnr)
Office: +27 (0)12 880 2238
Cell: +27 (0) 72 671 5764
Email: riaan@dynamdre.co.za
Website: www.dynamdre.co.za