Advanced Corporate Solutions

"Debugging" Specialists | 20 Years of Service Excellence (1995 - 2015)

dynamdre INNOVATIVE SOLUTIONS

THE REALITY OF

CYBER ESPIONAGE IN SOUTH AFRICA

A Case Study of cyber infiltration in the Bugging/Listening devices environment

September 2015

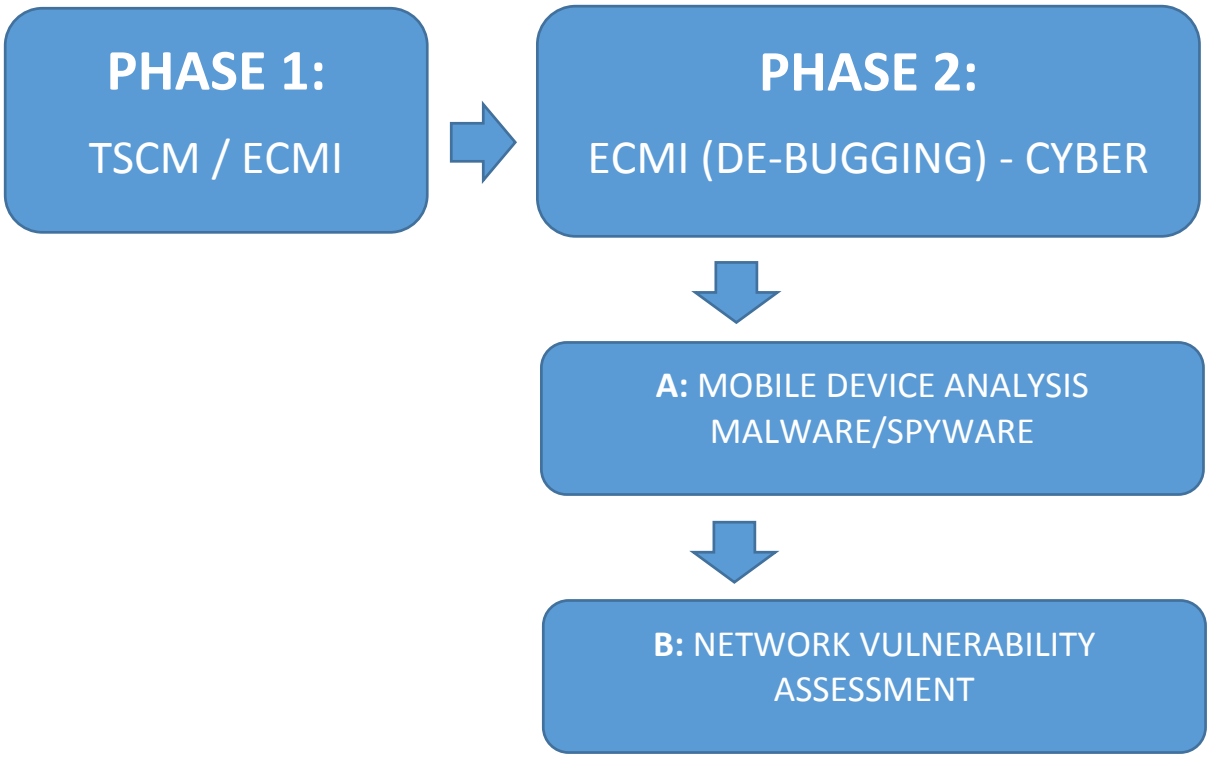
1. INTRODUCTION

Advanced Corporate Solutions in association with Dynamdre, a leading debugging cyber specialist company in SA, were tasked to assist in determining whether Technical Surveillance or Eavesdropping methods were being used to gain access to sensitive and confidential information pertaining to a certain Company. The scope of the task entailed:

- Physical Technical Surveillance Counter-Measures (TSCM) Investigations / Electronic Counter-Measures Investigations (ECMI), also known as "**de-bugging**" or "**sweeping**" operations.
- ECMI (De-bugging) – Cyber Investigations, consisting of Mobile Device Malware/Spyware Analysis and Network Vulnerability Assessments

2. METHOD

Investigations were conducted at the Company's Offices, in accordance with accepted best practices and procedures to ascertain and determine any method of leakage of sensitive information (Corporate Espionage). The phases entailed:



PHASE 1:

PHYSICAL TSCM / ECMI

("DE-BUGGING"/"SWEEPING")

The first stage covered Corporate TSCM/ECM Investigations using proprietary instrumentation and protocols.
ACS/Dynamdre executed a thorough electronic and physical examination to detect unauthorised audio or optical devices. The purpose was to identify GSM, 3g & 4g cellular eavesdropping devices, wireless transmitters (bugs), wire & mic tap, telephone compromise tap, carrier current bugs, micro wireless video devices, laser or infrared eavesdropping devices, etc.

Phase 1: Findings

No physical evidence was found of illicit eavesdropping devices and GSM bugs within offices, boardrooms, vehicles and telephone systems.

PHASE 2A:

ECMI (DE-BUGGING) – CYBER: MOBILE DEVICE MALWARE/SPYWARE ANALYSIS

The goal of the second stage was to conduct Vulnerability Assessments on various mobile devices using the CELLEBRITE UFED4PC[1] tool to examine the devices. Methods of extracting memory information:

1 Logical extraction (everything visual on the device)
2 File system extraction (user data and application data)
3 Physical extraction (all the data on the memory block, i.e. deleted files, application data and hidden code)

The Physical Analyser searches through every detail of the memory to acquire information.

All applications on mobile devices are accessible to review what permissions and values are assigned to them and the device is checked for any known trace of malicious code

Phase 2A: Findings

No evidence of any known malware threats were found on the mobile devices analysed. **However, evidence of communication from one IT Manager to another was found in the form of deleted WhatsApp and SMS text messages informing that the TSCM/ECMI Team was being monitored. They communicated that the physical TSCM/ECMI task was finalised and that they could resume eavesdropping by placing a Tablet computer under the Boardroom desk of the CEO to record discussions.**

[1] CELLEBRITE UFED4PC: has shown that it is the leader in analyzing mobile devices

PHASE 2B:

ECMI (DE-BUGGING) – CYBER: NETWORK VULNERABILITY ASSESSMENT

ACS/Dynamdre had authorisation to investigate specific staff members accused of information theft and supplying the information to the previous Managing Director of the Company. At this stage, Computer Forensics investigations were conducted with techniques aimed at gathering and preserving evidence from computing devices, for presentation in a Court of Law.

Structured investigations were performed, while a documented chain of evidence was compiled to establish what occurred on devices and who were responsible for it.

Cyber Forensic Investigators followed a standard set of operating procedures. After physically isolating devices to ensure that they cannot be contaminated, investigators made digital copies of the Storage Media and stored these in a secure facility.

A variety of techniques and proprietary forensic software applications were used to examine the copies, searching hidden folders and unallocated disk space for copies of deleted, encrypted, and/or damaged files. All evidence found was documented and verified in preparation for legal proceedings.

Phase 2B: Investigation and Findings

1. The task was to confirm if users of a computer had any access to confidential information that should not be in their possession.
2. An email address was provided, which seemed to have been used as a distribution channel for the information.
3. The possibility of communication between two suspects was investigated based on a list of keywords.
4. A specific laptop had three user accounts, one of which belonged to a senior employee, Mr. X. The findings and log information as follows:

    - A fair number of users accessed the machine.
    - All information about an important Audit was on the machine - User A.
    - The account activity of User A on the machine terminated on a certain date.
    - User accounts B and C were still active until the device was seized.
    - User A's password was changed and also logged on to the network by User B.
    - Mobile devices imaged previously contained conversations between User A and Mr X. These conversations contain numerous questions about classified documents.

The Tablet used by employees to eavesdrop by recording discussions and thereby gaining sensitive Company information, leading to a loss of R40,000,000 to the Corporate Client.

3. CONCLUSION

The value of employing ECMI (De-bugging) – Cyber Investigations in the Protection of Intellectual Property and investigation of crimes/legal actions is unquestionable. It allows for the gathering of information UNATTAINABLE through conventional methods.

These specific Investigations recently conducted for a Corporate Client, have enabled the Company to identify employees responsible for the theft of Intellectual Property to the value of some R 40,000,000 over a period of time. In this case study the Company's communication security was severely compromised, and this magnitude of loss could have been prevented by conducting regular TSCM/ECMI ("De-bugging") and Cyber Investigations.

Current technology is advancing at such a rapid pace that traditional TSCM/ECM investigation can no longer be seen as an individual discipline or practice, conducted on an ad-hoc basis. It has to be incorporated in all aspects of communication security to safeguard intellectual property and protect against future losses.

FOR MORE INFORMATION OR TO CONTACT US

Read more on our websites at:

www.acsolutions.co.za and www.dynamdre.co.za

For more information, please contact:

Riaan Bellingan (Senior) on +27 (0) 82 491 5086 or

email him at: riaan@acsolutions.co.za