

Electronic Counter Intelligence

(What is, How can & Protection from)

Insight into Information Age In-Security

Licensed Release : 2nd May 2003

© 2003 All Rights Reserved
Nagendra Technology Consulting

www.nagendra.com

About Author

Nagendra Technology Consulting is comprised of intelligent, experienced, forward-thinking technology consultant who possess the expertise to provide straight answers & insights into technological problems, and resources necessary to find innovative solutions for the most challenging problems from end to end.

Agreement/Legal Disclaimer

LEGAL DISCLAIMERS/NO-LIABILITIES

The information contained in this report is for general guidance on matters of interest only. The application and impact of laws can vary widely based on the specific facts involved. Given the changing nature of laws, rules and regulations, and the inherent hazards of electronic communication, there may be delays, omissions or inaccuracies in information contained in this report. Accordingly, The information on this report is provided with the understanding that the authors and publishers are not herein engaged in rendering technical, legal, accounting, tax, or other professional advice and services. As such, it should not be used as a substitute for consultation with professional consultant, accounting, tax, legal or other competent advisers. Before making any decision or taking any action, you should consult a professional

Copyright

© 2003 Nagendra. All rights reserved. Neither this publication nor any part of it may be reproduced, stored in a retrieval system, or transmitted any form or by any means, electronic, mechanical, photocopying, recording or otherwise, permission must be obtained from Author.

Document Author :

Nagendra <root@nagendra.com>

Table of Content

Introduction.....	4
What's at risk.....	5
Types of Intelligence Compromises.....	6
Signs of Bugging/Leaks	7
How To Interact in Compromised Communications.....	8
Compromises - Targets.....	9
Damage Control.....	11
Professional Debugging and Security Sweeps	12
Conclusion.....	13
References/Links.....	14

Introduction

Never have businesses been as worried about compromised networks, tapped phones, bugged rooms or insecure computer systems as they are today, and with good reason.

It's not been business as usual in this information age. It's cold out there in the corporate world, and a lot of competitors would like to come in, through various means of eavesdropping, to your cozy office.

Can this be countered ?

Yes; (the world of Electronics Counter Intelligence comes to rescue)

It's the art of reconnaissance to collect information on the informant itself, during these scenarios.

Electronics Counter Intelligence Defined :

ECI :

“Control Processes to block sources of Information Leaks, to Disable the source, to prevent sabotage, and to gather Information on Intelligence Source & Destination.”

Business espionage in recent years has become more sophisticated - and often frighteningly ordinary. Out of 10 security sweeps at least two positive match could be obtained.

This whitepaper explores the world of Electronic Espionage in this information age & Counter Intelligence to avoid, detect & recovery from it.

What's at risk

Electronics Business Espionage can affect every day business and life.

Consider the following:

- Your company has been recently marginally underbid on a tender that should have been won.
- Your Product & its USP just appeared on your closest competitors product line which is strikingly similar looking to yours
- A competitor will steal your new patent & designs because it is cheaper and quicker than doing their own research.
- Sensitive or very private information has become public for no reason.
- You are rapidly losing your most experiences personal/behind the scene employees along with their entire teams to other competitors.

Many businesses/corporates greatly under value their proprietary information.

Who's at Risk :

Companies :

- IT Services Companies
- Software Product/Solution Providers
- Head-hunters
- Research & Biotech Companies
- Media/Creative Agencies

Individuals :

- CEO's/CFO's/CTO's
- Stock Analysts
- HR Managers
- High Profile Lawyers
- Research Scientists
- Architects

Types of Intelligence Compromises

Internal :

Typically, internal threats include, employees from all levels of the target organization, including management personnel, disgruntled personnel (known or unknown) and all other persons that work directly for, or have regular unescorted access to the target facility. Internal threats can be electronic or non-electronic in nature.

External :

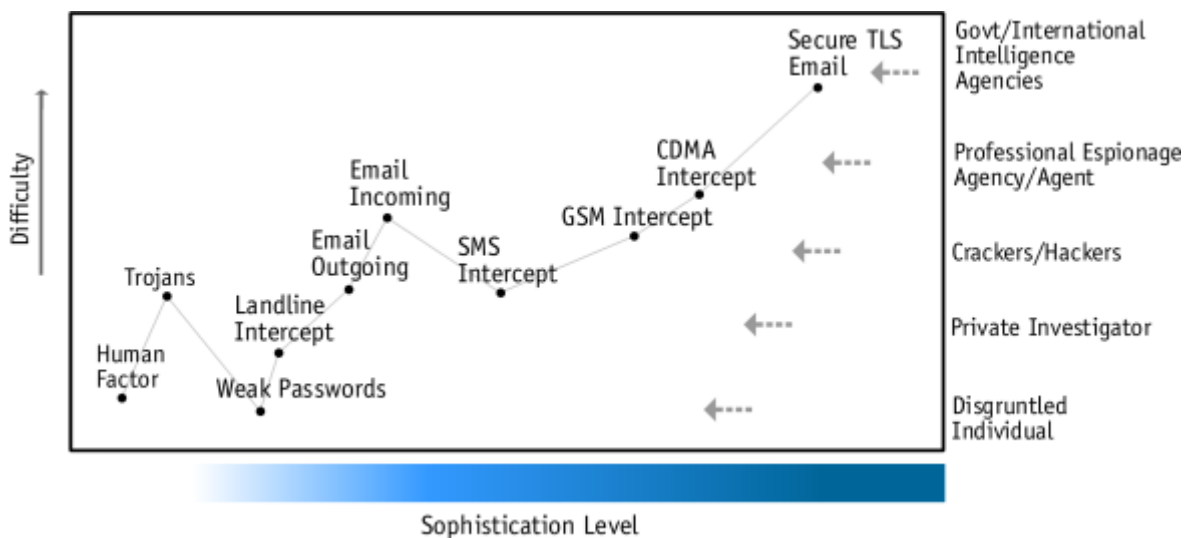
Typically, external threats include, outside contract personnel, including service and maintenance staff (computer/office equipment service personnel, internet service provider, etc.), business competitors, industrial spies. External threats can be electronic or non-electronic in nature.

Threat Sophistication Diagram :

The below diagram shows various Electronic/IT Communication threat to capability reference lookup

Threats include :

- **Human Factors** - Weak Passwords, Disgruntled Employees,
- **Voice Communication** - Wire Phones, Mobile Phones
- **Data/Network Services** - Email Incoming(POP3/IMAP),SMTP
- **Messaging** - SMS/IM
- **Secure Email** - TLS Email(SMTP), POP3SSL



Signs of Bugging/Leaks

(General - Non Technical)

If eavesdropping on anything you say, email, or do could increase someone else's wealth or influence, then you are a potential target.

Some top signs include :

- Desktop computer suddenly freezes doing non-tival tasks or unknown programs in task bar/process list

Has someone installed surveillance software on your computer without your knowledge or consent?

With hundreds of commercially available spy software in use worldwide, there's a good chance your computer may be bugged which can capture & record every web site you visit, email you read or write every chat room you enter, your banking information & record all your passwords.

- Others know your confidential business or professional trade secrets

This is the most obvious indicator of covert eavesdropping activities. Theft of confidential information is a multi-billion dollar underground industry. Often the loss of your secrets will show up in very subtle ways so you should always trust your instincts in this matter. When your competitors know things that are obviously private, or the media finds out about things they should not know, then it is reasonable to suspect technical eavesdropping or bugging.

- Secret meetings and bids seem to be less than secret

Confidential meetings and bids are very popular targets for corporate spies. How would you like the plans for the corporate takeovers you're planning to become public knowledge? Would copies of your product designs/code be of any use to your competitors? Would it be beneficial for your competitors to know how much you're quoting for the same project?

- People seem to know your activities when they shouldn't

They may accidentally revel something in a conversation which there are unable to explain credibly, you are surprised to find out somebody knew something they shouldn't have.

- Strange Behavior of your Email account

One day your unable to check you email accounts as it says "mailbox locked by another processes" or "multiple logins detected" or the password you got over email as result of some confirmations isn't working or has already been confirmed, or you get a email from a known contact but its's body is missing

- You have noticed strange sounds or volume changes or empty calls

Surveillance devices often cause slight anomalies on the telephone line such a volume shift or drop-out, GSM Mobile calls if they are from/to known numbers without voice suddenly which wasn't before.

How To Interact in Compromised Communications Environment

You recognize signs of compromise and also your instincts back up the suspicion, now what to do

Here are few pointers :

- *Be Calm*

Don't do anything drastic (like formatting!) without knowing the extent or nature of compromise

- *Use E-Mail to contact but not on your normal desktop pc*

Be discreet & preferably create a new email account on a secure and unknown webmail service (a good one is www.myrealbox.com provides ssl webmail & tls smtp/pop)

- *Immediately contact a Electronic/IT Security specialist*

Use only secure communication method and contact a Electronic/IT Security Specialist (NTC : root@nagendra.com - Accepts TLS V3 Encrypted Mail)

- *Use the phone, but call from a phone away from your office or home*

- *Schedule a Vulnerability Analysis or Threat Assessment ASAP*

- *Consider having a Full Security Review & Sweep completed ASAP*

What NOT to do in your situation :

- *DO NOT Discuss this issue at the office, in your car, or at home*

- *DO NOT Try to find the bug or spyware yourself*

- *DO NOT Engage a private investigator to find it (they may be clueless on Electronic/IT Security)*

- *DO NOT Contact your hardware/software supplier to help (they may have planted it)*

- *DO NOT Contact the telephone company to help (they may laugh at you)*

- *DO NOT Contact the *BI/Intelligence Service for help (they may ignore you)*

- *DO NOT Try to get the local police to help (they may lack the ability)*

- *DO NOT Use your office telephone to initiate contact*

- *DO NOT Use your cellular or cordless phone to initiate contact*

Compromises - Targets

- Computers
- Phones
- Networks
- Human Factors
- Environment

Desktop Computers :

Someone can easily install surveillance software (called Keyloggers/recorders) on your computer without your knowledge or consent. With hundreds of commercially available spy software in use worldwide, there's a good chance your computer may be bugged which can capture & record every web site you visit, email you read or write every chat room you enter, your banking information & record all your passwords.

Computer Networks/ Non-Switched LAN's :

Wire-tap device that plugs into computer networks and eavesdrops on the network traffic. Like a telephone wiretap allows to listen in on other people's conversations, a "sniffing" program lets someone listen in on computer conversations. Many networks use "shared media", This means that there is no need to break into a wiring closet to install your wiretap, can be done from almost any network connection to eavesdrop on the entire office network.

Phone Bugging : Landline(Wire Phones) :

Telephone are excellent bugging device perfectly installed at every desk at office or in conference rooms. In most cases nothing has to be done to the telephone to turn it into an excellent room bug due to design flaws, but in most cases a simple capacitor can be installed and a wire snipped to turn your telephone into a very high quality eavesdropping device.

Phone Bugging : GSM Mobile :

The alleged security of GSM relies on the myth that encryption, mathematical scrambling of conversations which makes it impossible for anyone to intercept. And while this claim looks good on paper, it does not stand up to scrutiny. All the GSM voice privacy ciphers used worldwide can be broken by an attacker with just a single PC (running linux) and some radio hardware

...

Compromises - Targets..

Human Factor :

Weak Password(for desktop/network/email/intranet) :

Having no or very weak password to login to you desktop, network & email account can be a very easy target to gain entry into your communication for a external source.

What is a weak password? A password that is the same as the account name (e.g., account name: admin, password: admin) is the worst. Passwords that can be found in a dictionary of any language are also particularly vulnerable.

What is a strong password? A password with at least 8 characters, including a mix of upper-case letters, lower-case letters, numbers, and special characters (such as .,!#& etc) is a strong password. A great way to create a strong password is to think of an easy to remember phrase, like "I Want to get Bonus next year" and turn it into an acronym: IWtgB04y.

Social Engineering :

Social Engineering is hacker-speak for tricking a person into revealing their password.

A classic social engineering trick is for a hacker to send email claiming to be a system administrator. The hacker will claim to need your password for some important system administration work, and ask you to email it to him/her. It is possible for a hacker to forge email, making it look like it came from somebody you know to be a legitimate system administrator. Often the hacker will send this message to every user on a system, hoping that one or two users will fall for the trick.

Environment :

Conference Rooms :

Many larger companies have an executive conference room dedicated as a place to have confidential discussions, but the room as a convenience is filled with power points, un-firewalled multiple network access ports & more. Such a conference room normally has lots of glass, telephones which can be easily bugged, and audio visual/computing equipment that can be trojan'ed when not in use.

Damage Control

It is strongly recommend that a security expert be consultant for a complete infrastructure sweep security as soon as a compromise is suspected to properly determine the nature and extent of the compromise. See “Professional Debugging and Security Sweeps” for more information.

So What’s Safe Meanwhile(Read Great Difficulty to Bug) :

- **Computer** : New Clean OS install (Linux) or distant Cyber Café
- **Network** : Use https sites , SSL webmail, TLS Email/SMTP/POP
- **Phone** : Pay Phone outside neighborhood area
- **Mobile** : Not Recommended; GSM Pre-Paid Card for 1800Mhz
- **Internet** : via GPRS Data Service or at distant Cyber Café

Professional Debugging and Security Sweeps

It is critical to get a Security Specialist out to the area to be inspected as quickly as possible (typically within 72 hours or less, the same day is ideal). It is important that you keep the area occupied & normal until the specialists arrive to prevent removal of any possible eavesdropping device.

If you are currently the target of compromised or eavesdropping, special steps must be taken to avoid alerting the eavesdroppers that you are seeking professional help to detect their activities. If such an eavesdropper learns that a team is about to perform a Security Sweep Service they will quickly remove (or turn off) their eavesdropping devices, and re-install them after the sweep has been completed (and no bugs will be found). Many Security sweeps can be compromised or ruined by clients who call the Security Specialist from the suspect facility.

All legitimate Security Specialists have extensive background in both electronics & Information Technology.

Private Investigators are rarely qualified to perform bug sweeps, their training, background, and equipment are for the INSTALLATION of bugging devices, NOT removal. An honest PI will usually bring in an outside Security Specialist as a consultant or on a referral basis.

Security Sweep/Recovery Service Provider :

Nagendra Technology Consulting provides complete security consulting services including design of secure communication system, traps to detect/track/lock a compromise, recovery of compromised data & communications & both electronic & IT Infrastructure sweeps for covert bugs/leaks & compromises.

Secure Email : root@nagendra.com

Web : <http://www.nagendra.com/>

NTC is comprised of a intelligent, experienced, forward-thinking technology consultant who possess the expertise to provide straight answers & insights into technological problems, and resources necessary to find innovative solutions for the most challenging problems from end to end.

Conclusion

This report provides another justification for 'defense-in-depth'. Communication Networks are an infrastructure enabler for us to perform our daily functions.

The general communication networks were never meant to be used as a security feature; although, they continue to be used in this manner. Providing a controlled communication infrastructure is a key component of any good defensive position.

While compromising a single person's computer or email or phone can gain the attacker access to lot of systems in the organization, the ability to collect/sniff userids and passwords for several others will effectively give away the keys to the kingdom over a period of time.

Managers must be aware that they have 2 realistic options. They can either manage the communication infrastructure appropriately and be part of the team trying to protect the environment, or they can configure the environment so that it is 'hands-off' or 'self-maintaining' which is *security-by-design*, that is desired if maximum security has to be achieved. Involving a Professional Electronics/IT Security specialist would be recommended while the infrastructure is still being designed and processes or policies are being created. This avoids lot of headache later & clean-up later once the damage has already been done.

Electronic/IT Infrastructure Security Services Provider :

Nagendra Technology Consulting provides complete secure hosting service including secure email & web hosting solution which provide Servers with 128Bit TLSv3 Encrypted Transport of email and access to webmail from point to point.

Secure Email : root@nagendra.com

Web : <http://www.nagendra.com/>

NTC is comprised of a intelligent, experienced, forward-thinking technology consultant who possess the expertise to provide straight answers & insights into technological problems, and resources necessary to find innovative solutions for the most challenging problems from end to end.

References / Links

IT Security :

<http://www.cert.org/>

The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

<http://www.sans.org/>

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. The SANS Institute enables more than 156,000 security professionals, auditors, system administrators, and network administrators to share the lessons they are learning and find solutions to the challenges they face.

Voice In-Security :

Commercial Intercepting Products :

(Examples found on a simple search on net)

http://www.endoacustica.com/gsm_interceptor007A.htm

Commercials GSM Interceptors(Disples Providers Claim of Security)

<Http://www.mobilephonebug.co.uk/erol.html>

Mobile Phone Bugs which can left in a conference room on later to dial and listen to what's happening even while switched off

Consulting Client Signup : It's really affordable to signup for a security technology consulting contract which not only cover the present report but also actual implementation & design of secure intelligent communication networks with indepth insights into custom technology solution & resources to be on the cutting edge.

Please contact root@nagendra.com to schedule a Meeting/Video-Conference to proceed futher