Global Information Assurance Certification Paper

Netspionage

By

John F. Kiesler

Version 1.4b

GSEC Practical Assignment

Abstract

Over the past several years, theft of proprietary or classified data via the Internet by either domestic or foreign entities (*netspionage [17])* has become ever more prevalent, sweeping the information landscape. The tools and techniques being employed are maturing and have become widespread. The perpetrators carry out their nefarious deeds for a wide range of reasons, mostly to support financial and/or intelligence rewards.

Over the course of the past several years, the Internet has provided the ideal environment for nefarious entities to exploit the information infrastructure for *netspionage*. The Internet provides the criminal, cyber terrorist and nation state with plausible deniability, anonymity, and a tremendous volume of target and information-rich opportunities.

Without an effective strategy to mitigate these threats, the corporation, federal environment or private users leave themselves and their information vulnerable. Although there are a number of tools and techniques available, this paper addresses four, and provides considerations to help mitigate against these potential vulnerabilities.

Background

Over the course of the past several years, statistics have been compiled to help industry become familiar with trends associated with the threat. The statistics that have been gathered are not too surprising as vulnerabilities and exploitations continue to surface. According to a 1997 American Society for Industrial Security (ASIS) survey of Fortune 1000 firms, companies in the U.S. are believed to have lost roughly $250 billion annually to information thieves. More than half (56 percent) of the 172 companies responding to the survey reported at least one attempted or suspected information misappropriation. Over a 17-month period, some 1,100 documented incidents of intellectual property theft were identified, worth an estimated $44 billion. Although it is very difficult to assign numbers to potential loss due to information theft, it is unquestionably a serious and alarming trend. Further, implications to national security are a key element to these findings as well.

This alarming trend is confirmed. Five years later, a 2002 Computer Crime and Security Survey report revealed 90% of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months and 80% acknowledged financial losses due to computer breaches [13]. As anticipated, the most serious financial losses occurred through theft of proprietary information. Interestingly, 74% cited their Internet connection as a frequent point of attack. [1]

There are many web sites that exist to provide tremendous resources for tools, information and training on potential exploits and vulnerabilities both for the security expert and those with malicious intent.

An annual conference occurs called DEF CON - a computer underground hackers convention, for those who conduct netspionage to meet to discuss the latest.

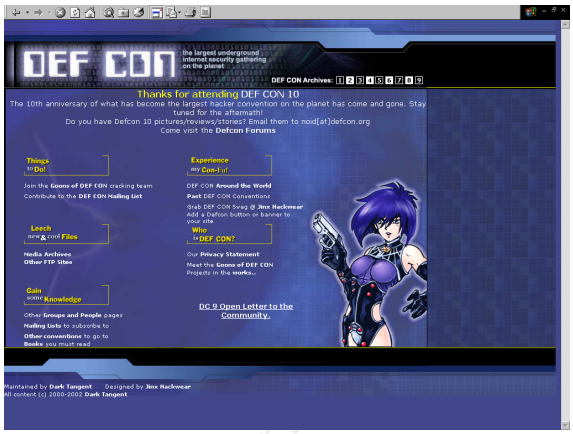

Figure 1 - DEF CON

Certainly the information is available to carry out theft of information. The dilemma for the security professional, though, is assigning attribution to those who commit these crimes. There have been several studies that attempt to determine the level of foreign exploitation. In a recent Federal Bureau of Investigations (FBI) report, it was revealed by U.S. companies that although domestic competitors are engaged in competitive intelligence exploiting the information domain, there is increased *netspionage* by companies and governments from China, Japan, France and others.

"We're seeing more and more cases," said William Perez, acting chief of the FBI's financial crimes unit. "A country like the U.S. is a very juicy target" because of the prominence of its high-technology companies, he said. The Internet arouses the greatest fear because it gives skilled hackers the possibility of entering untold databases with anonymity, often from far-off locations where there are no statutes against computer crime. Laws concerning computer crime are slowly maturing and becoming more robust. However, the criminal element recognizes that international law lags significantly. It is common to weave attacks through foreign sites in advance to reaching the “crown jewels.” As law enforcement attempts to resolve the source, frequently the investigation stalls once a foreign ISP is reached – particularly one where no computer crime laws exist.

A well-publicized example of foreign exploitation of U.S. business information occurred in Russia almost ten years ago. In 1994, a group of Russian hackers stole codes and passwords from corporate customers of Citibank and transferred $10 million to overseas accounts. Six Russians were extradited and pleaded guilty to computer fraud in federal court in New York. Citibank said it recovered all but $400,000 of the money. [5] The ability to transfer money from a large banking institution like Citibank certainly serves as a grim reminder of the increasing number of incidents and potential vulnerabilities to even our most secure institutions.

Computer Emergency Response Center (CERT) located at Carnegie Mellon University corroborates the above. The number of vulnerabilities and incidents continue to increase exponentially. [1]

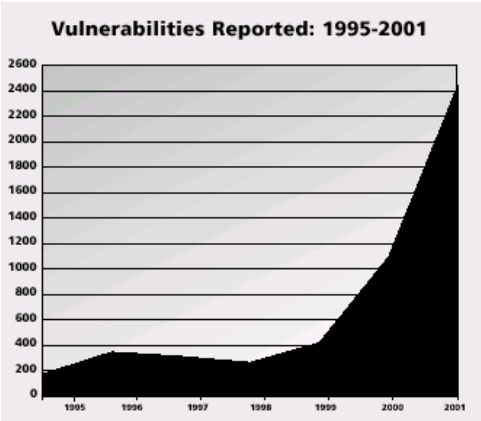

Figure 2 - Vulnerabilities

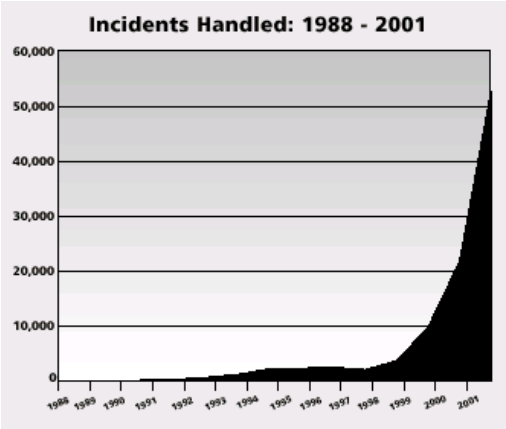

Figure 3 - Incidents

Complicating efforts further to track the nefarious is when foreign entities employ *"go betweens or hackers for hire"*. Hackers for hire working for foreign nationals are not merely the stuff of James Bond films, Exodus Communication security chief Bill Hancock said. He's been chasing a Chinese national for six to seven years who regularly hires U.S. teen-agers to hunt down documents. In one case, Hancock said a 17-year-old U.S. hacker was paid $1,000 -- and promised $10,000 more -- for stealing design documents for kitchen appliances from U.S. firms. [17] Hiring hackers for hire not only provides foreigners a degree of plausible deniability, but also helps stall prosecution, as the *go between* is frequently a minor, thus provided a degree of protection from criminal prosecution.

In addition to the vulnerabilities that exist, there are other variables that exist to support the attractiveness of *netspionage*. Corporations today are migrating from an information-saturated environment to one that takes information to the next level - "decision-quality information." The information itself becomes more lucrative and valuable for an adversary to take the necessary risks. This "enriched" information is also becoming more available to a wider audience, both employees and customers alike, sometimes through emerging technologies like portals. Corporations are web-enabling their applications and databases to provide these business-leveraging opportunities like portals. Vulnerabilities, by placing key corporate assets on the web, become obvious.

Through corporations' business transformation efforts, a number of elements emerge facilitating exploitable opportunities for an adversary. Four of these that will be addressed within this paper include:

- Increased theft and exploitation of laptops;
- Increased exploitation of wireless technologies;

- Increased employment of spyware; and
- Increased employment of steganography tools.

1. Increased theft of laptops and other mobile tools

Figure 4 - Laptop

As laptops increase in functionality, industry continues to integrate use of laptops into traditional business practices. Frequently, executives, scientists, marketers, and the corporate financial team travel with laptops to maximize efficiencies. In addition to increased productivity and efficiencies these mobile devices create additional threats.

The threats most commonly associated to the laptop are both theft and gaining physical access to clone information resident on the laptop. The Computer Security Institute reported that approximately 57% of corporations experienced a loss related to laptop theft and an insurance industry estimate states that over 319,000 laptop were stolen in 1999. [2] This is of particular concern to organizations were the workforce is very mobile and maintains very sensitive information, such as military, law enforcement and executives.

A 2000 Justice Department internal report revealed the FBI and four other federal law enforcement agencies during 1999 lost more than 400 of its own laptop computers. This finding reached public attention in mass, particularly as it was discovered that in some cases, the laptops might have contained classified national security information. [12] The FBI is not the only agency victim to high-profile laptop theft.

That same year (January 2000), the State Department disclosed that a classified laptop with information about arms control was missing from a conference room. You can imagine the implications should U.S. State Department strategies, adversary assessments, and technical concerns become known to an adversary. The ensuing furor resulted in an FBI investigation and the firing of two high-level diplomats. Four others received career-stalling reprimands. A subsequent audit of the department's laptops accounted for its remaining 60 classified laptops, but 15 of its 1,913 unclassified laptops were still missing. [9]

In spite of these concerns, according to NASA's Deputy Chief Information Officer, there certainly are solutions to mitigate the risks associated with laptops. NASA uses data-theft detection tools and full data encryption to foil would-be thieves and hackers. NASA also is using theft-deterrent tools, such as locks that secure

the laptop to a desk and secure briefcases. NASA also has limited access to agency-issued laptops to those who really need them, such as employees who travel frequently and those who need to work at home. [7]

All of these efforts are important and should become a key part of any agencies security plan to mitigate laptop theft. As most of us are all too aware, laptops frequently contain the similar content as a users' desktop, and thus include corporate strategies, financial data, proprietary information, etc.

Of parallel concern, laptops also provide an adversary with network topology, configuration management schema, and other vital information. This is easily accomplished by studying the configuration for remote network access.

A security strategy should at a minimum include the following elements:

- Data encryption policy and tools
- Conduct routine inventories
- Establish deadlines for employees to report the loss or theft
- Improve disciplinary measures
- Strengthen the policy for proper storage
- Ensure all property is accounted when employees leave
- Improve the documentation of the destruction of laptops and hard drives

2. Increased Use of Wireless Devices and Networks

Wireless LANs (WLANs) have become very appealing over the last few years for a number of reasons. With wireless, you no longer have to drop cable to every desktop and users can connect from just about anywhere within range. Wireless LAN's provide always-on network connectivity while allowing employees to roam throughout a building without being bound by wires. Further, WLAN's are emerging as low cost solutions and easily deployed. However, there is a cost associated with this capability - a lot of vulnerability.

With a WLAN, transmitted data is broadcast over the air using radio waves. This means that any WLAN client within an access point service area can receive data transmitted to or from the access point. Because radio waves travel through ceilings, floors, and walls, transmitted data may reach unintended recipients on different floors or even outside the building that houses the access point. With a WLAN, the boundary for the network has moved. Without stringent security measures in place, installing a WLAN can be the equivalent of putting Ethernet ports everywhere, including the parking lot.

Because of these security concerns, many network managers have been reluctant or unwilling to deploy WLANs, especially in light of the vulnerability of the Wired Equivalent Privacy (WEP) keys that are used to encrypt and decrypt transmitted data. The 802.11 standards define WEP as a simple mechanism to

protect the over-the-air transmission between WLAN access points and network interface cards (NICs). Working at the data link layer, WEP requires that all communicating parties share the same secret key. To avoid conflicting with U.S. export controls that were in effect at the time the standard was developed, 40-bit encryption keys were required by IEEE 802.11b, though many vendors now support the optional 128-bit standard. WEP can be easily cracked in both 40- and 128-bit variants by using off-the-shelf tools readily available on the Internet, such as AirSnort, which enables an attacker to passively monitor and analyze packets of data and then use this information to break the WEP key that encrypts the packets.

Figure 5 - Airsnort Availability Website

As with other networks, security for WLANs focuses on access control and privacy. Robust WLAN access control provides vital security controls and prevents unauthorized users from communicating through access points - the WLAN endpoints on the Ethernet network that link WLAN clients to the network. Strong WLAN access control ensures that legitimate clients associate with trusted, rather than "rogue" access points. It is these rogue access points, which serve as the launch pad for malicious activities. WLAN privacy ensures that only the intended audience understands the transmitted data. The privacy of transmitted WLAN data is protected only when that data is encrypted with a key that can be used only by the intended recipient of the data.

The 802.11 standard, a group of specifications for WLANs created by the Institute of Electrical and Electronics Engineers Inc. (IEEE), supports two means of client authentication: open and shared-key authentication. Open authentication involves little more than supplying the correct Service Set Identifiers (SSID). An SSID is a common network name for the devices in a WLAN subsystem. With shared-key authentication, the access point sends the client device a challenge text packet that the client must then encrypt with the correct WEP key and return to the access point. If the client has the wrong key or no key, authentication will fail and the client will not be allowed to associate with the access point. Shared-key authentication is not considered secure, because a hacker who detects both the clear-text challenge and the same challenge encrypted with a WEP key can decipher the WEP key.

Some WLAN vendors support authentication based on the physical address, or MAC address, of the client Network Interface Card (NIC). An access point will allow association by a client only if that client's MAC address matches an

address in an authentication table used by the access point. But MAC authentication is an inadequate security measure, because MAC addresses can be forged, or a NIC can be lost or stolen. [3] Again, not an effective solution for an enterprise that carries sensitive data over the WLAN. A combination of solutions must be employed to provide the necessary defense-in-depth layers. Without, exploitation is inevitable.

Recently, there was media attention of a Massachusetts-based business (based on securing e-business, RSA Security - http://www.rsasecurity.com/company/) that drove through the City of London armed with only a laptop, wireless network card and some free software downloaded from the Internet. They discovered they could pick up the traffic on dozens of corporate WLAN's, 'leaking' out of buildings, which could invariably allow them to grab companies' data without anyone in that company knowing. There have been a few substantiated reports that even an empty tin of Pringles will make a good wireless antenna/receiver. [10]

Figure 6 - Use of Pringles for Receiver

When attempting to mitigate wireless vulnerabilities, as referenced above, a layered approach is necessary. For example, consider implementation of 802.1x (standard referenced above for port-based access control) and VPN tunneling.

VPN Tunneling is commonly used to create a secure means of communication over an insecure link, such as remote access via the Internet to a company network for e-mail or other network access. It ensures security through both user authentication and encryption with user authentication in the system, where the user name and password are encrypted. Strong encryption methods such as RC5 and Triple-DES can be used with VPN Tunneling. [11]

3. Pervasive Use of Spyware

Spyware is any software that takes information from your system and employs an Internet connection to upload the information to a remote server without the users knowledge or consent. Spyware can be broken down into two different categories, surveillance software and adware. Surveillance software includes key loggers, screen capture devices, and trojans. Corporations, private

detectives, law enforcement, intelligence agencies, suspicious spouses, etc would use these, to include those engaged in *netspionage*.

The unknowingly installed spyware programs can [14]:

- Capture on-line activity and upload the information to a remote server maintained by a third-party.
- Cause Internet browser instability and slowness.
- Consume system resources and cause system errors. Spyware will consume bandwidth as it sends information to its remote server.
- Render systems vulnerable to attack or compromise. Spyware are executable programs that reside on systems and have the privileges of the user that installed it.

As an independent executable program, spyware has the capability to do anything a program can do, including capturing and forwarding of the following from your system:

- Every web site you visit
- Every email you read or write
- Every chat room you enter
- Banking information
- Passwords
- Keystroke monitoring

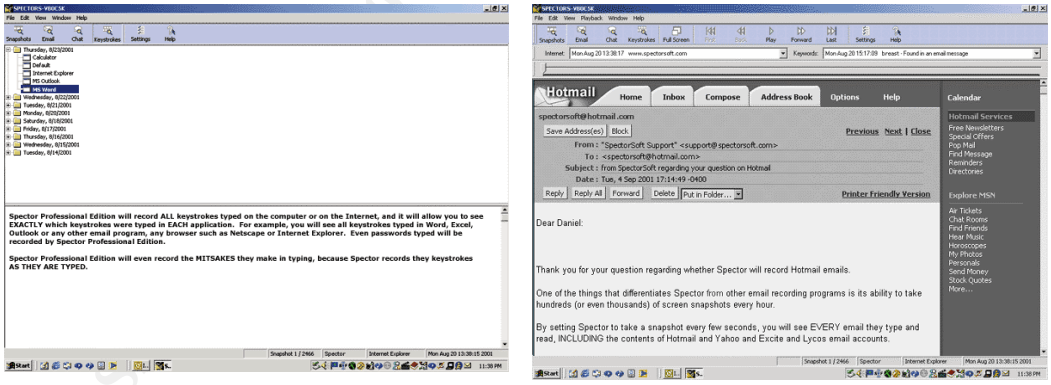

Figure 7 - Spyware Employed (Keystroke and Internet Recording) [15]

There are many methods to be employed to help mitigate the spyware threat. Much like above, a layered approach is best. Several of the techniques to be considered include:

- Use aggressive automated tools to detect spyware.

- Use an effective firewall that allows you to block spyware communication, such as Zone Alarm. With Stealth mode enabled, the firewall renders your computer invisible to the Internet and to potential intruders.
- Prevent regular tracking by cleaning up and deleting all temporary Internet files, cookies and the like often. This can be done through automated tools as well.
- Recognize the main spyware perpetrators (http://www.spywareinfo.com/)
- Realize, though, the true agent involved in *netspionage* will be employing new and/or difficult to detect tools.

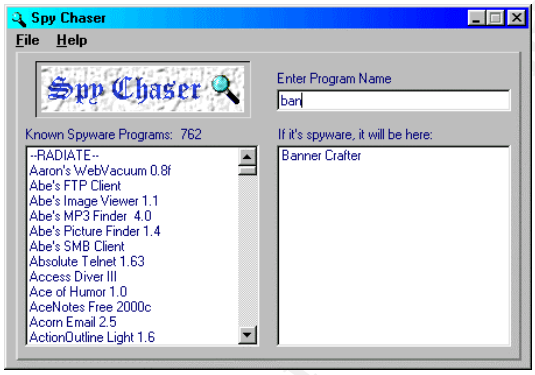

Figure 8 - Spyware Website

4. Sophistication of Steganography Tools

A final arrow in an adversaries quiver is the employment of steganography. Steganography provides an adversary an ability to communicate and disseminate sensitive or pilfered information with a minimal ability for security personnel detecting the event and supports plausible deniability.

Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Originating back to the ancient times, the term steganography is derived from the Greek word *steganos*, meaning covered or hidden, and *graphy,* meaning writing. In our computerized civilization, steganography has expanded to include covert inclusion of data in any other data source including text, audio, and video. [16]

We know that steganography is being used. There are several published examples of *agents* engaged in *netspionage*. The use of steganography has become a matured science over the past several years. There are many web sites and quite a few books now devoted to not only describing this tool, but also providing the steganography service at very low cost.

The appeal to an adversary is that information can be hidden in such a wide range of mediums. Within reason, any plain text, cipher text, other images, or anything that can be embedded in a bit stream can be hidden in an image. Although text and audio steganography can be employed quickly and successfully, it is image steganography that has matured most dramatically in

recent years with the development of fast, powerful graphical computers, and steganographic software readily available over the Internet for everyday users.

There are many ways to hide information in images. Straight message insertion can be done, which will simply encode every bit of information in the image. More complex encoding can be done to embed the message only in “noisy” areas of the image that will attract less attention. The message may also be scattered randomly throughout the cover image. The most common approaches to information hiding in images are:

- Least significant bit insertion
- Masking and filtering techniques
- Algorithms and transformations

Each of these can be applied to various images, with varying degrees of success. Each of them suffers to varying degrees from operations performed on images, such as cropping, or resolution decrementing, or decreases in the color depth.

Not surprisingly, steganography tools have become so pervasive that even the less technologically savvy thugs are using the capability. Although not to support netspionage, there are suspicions that steganography had been used by al Qaeda and Osama bin Laden to support their terrorist efforts. [6] Bin Laden had reportedly used (and still may be using) steganographic messages on the Internet to communicate to operatives its’ plans.

More direct to netspionage is a case whereby a French defense contractor had been duped. The contractor suspected its designs were somehow being leaked outside the company. The company had careful guards on how digital information could leave the premises, but later determined not careful enough. It was discovered a computer criminal, working as part of a team, had taken a job inside the French company. Then, he painstakingly embedded trade secrets inside Web site images, which he then posted on the company’s public Web site. An outside hacker then stole the secrets right from the company's home page. Investigators discovered the steganography by noticing slight variations in image file size. [17]

The ability to detect steganography is difficult though. Steganography detection is commonly referred to as “steganalysis” - the art of discovering and rendering useless such covert messages. There are few tools that help to predict the presence of hidden information through the use of known signatures. Steganalysis tools such as Stegdetect (freeware solution -

http://www.outguess.org/detection.php) and Steg Watch (commercial product) provide an ability to detect steganography content in text, audio and in images.

Recognizing whether or not a file contains hidden embedded data requires evaluation of the compromised file to the real thing—this is daunting as the file could be an image, text, audio, etc. Further, when evaluating a suspect image, the eye cannot always categorize photographic loss because most steganography programs use slight algorithmic change of the color palette tables as referenced above. Compounding this, even if you did suspect that a secret message was possibly hidden inside one of your files, you need to know which software program was used, and then identify the password to open the file, should it be encrypted.

Of course the government is closely watching use of more sophisticated tools. The FBI and NSA are using all the tricks they have involving information capture and forensics, including the use of Carnivore, the FBI's packet sniffing system and Echelon, the theorized espionage network watching global communication.

Response to Netspionage

Through the use of an effective defense-in-depth strategy, a business or government entity can close in on neutralizing the *netspionage* threat. Defense-in-depth involves defensive layers of security at varying perimeters based on the enclave. The layers of security involve people, operations and technology at each layer. Examples of tools in a security manager's arsenal include:

- Awareness training
- Security education
- Building and implementing responsive security policies
- Knowing your employees [8]
- Effective background investigations
  - Analysts estimate 70% to 90% of all attacks on corporate networks occur internally - insider breaches are a hundred times more costly than attacks from outside the enterprise. [4]
- Identifying threats & vulnerabilities
- Security patches and fixes installed [8]
- Penetration Testing
- Contingency planning
- Internet and Intranet security
- Encryption solutions
- Portable computer theft protection
- Site security evaluation
- Internet security software solutions
- Network security auditing
- Security maintenance contracts

References

1. CERT CC Statistics. Carnegie Mellon Software Engineering Institute. URL: http://www.cert.org/stats/cert_stats.html

2. Christie Vincent and Jack Vaughan. “Security Experts Seek to Combat Laptop Theft” CNN. September 2000. URL: http://www.cnn.com/2000/TECH/computing/09/20/laptop.security.idg/

3. “Cisco Aironet Wireless LAN Security Overview” URL: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

4. CRYPTEK. “Network Security From the Inside Out”. May 2002. URL: http://www.cryptek.com/Company/presskit/corporate.pdf

5. “Cyberburglars Weave a Web Around Globe Computer Espionage Booms As Rivals and Governments Target Corporate Databases” International Herald Tribune. 19 February 1998. http://netsecurity.about.com/gi/dynamic/offsite.htm?site=http://www.reactnetwork.com/article3.html

6. Declan McCullagh. “Bin Laden: Steganography Master?” Wired News. 7 February 2001. URL: http://www.wired.com/news/politics/0,1283,41658,00.html

7. Diane Frank. “Laptops Present Major Security Concerns.” Federal Computer Week. 10 April 2000. URL: http://www.fcw.com/fcw/articles/2000/0410/cov-side2-04-10-00.asp

8. Dr. Robert Ing. "Improvised Technology In Counter-Intelligence Applications." 29 January 02. URL: http://www.pimall.com/nais/n.cntint.html

9. Joshua Dean. “Lost Laptops Compromise Secrets.” GovExec.com. 1 October 2001. URL: http://www.govexec.com/features/1001/1001managetech2.htm

10. Mark Ward. “Hacking with a Pringles Tube” BBC News. 8 March 2002. URL: http://news.bbc.co.uk/1/hi/sci/tech/1860241.stm

11. Max Schroeder. “Wireless Security.” Communications Convergence. 5 November 2002. URL: http://www.cconvergence.com/article/CTM20011031S0013

12. Philip Shenon. “FBI lose hundreds of guns, laptops.” The New York Times. 6 August 2002. URL: http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2002/08/06/MN226959.DTL

13. Rapalus, Patrice. "2001 Computer Crime and Security Survey". Computer Security Institute. 2001 http://www.gocsi.com/prelea/000321.html

14. Robert Vamosi. “What is Spyware?” ZDNet Reviews. 28 June 2001. URL: http://www.zdnet.com/products/stories/reviews/0,4161,2612053-1,00.html

15. SpectorSoft. PC Magazine’s Editor’s Choice. URL: http://www.spectorsoft.com/products/SpectorPro_Windows/index.html

16. Steganography- Webopedia URL: http://www.webopedia.com/TERM/s/steganography.html

17. “The Untold Tally of Netspionage.” MSNBC. 11 September 2000. URL: http://zdnet.com.com/2100-11-523788.html