Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Reversing the Steganography Myth in Terrorist Operations: The Asymmetrical Threat of Simple Intellig

Commonly available IT software and equipment such as 802.11b wireless networks, laptop and desktop computers, high-capacity media devices, and a little creative thinking, make it possible, indeed simple, to facilitate efficient, short-duration, and completely anonymous communications between even casual hosts. This paper discusses various ways and methods for simple, clandestine communications that are virtually undetectable and untraceable using common technology.

Copyright SANS Institute

Author Retains Full Rights

AD

Reversing the Steganography Myth in Terrorist Operations: The Asymmetrical Threat of Simple Intelligence Dissemination Techniques Using Common Tools

by
Robert J. Bagnall
Senior SOC Security Engineer
Counterpane Internet Security

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Robert J. Bagnall GSEC v1.4

Reversing the Steganography Myth in Terrorist Operations: The Asymmetrical Threat of Simple Intelligence Dissemination Techniques Using Common Tools

Abstract

The events of September 11th prompted significant discussion and speculation as to the use of Steganography by terrorists for clandestine and secured communications. Numerous prominent figures in the industry have written articles and given interviews debating whether or not terrorists are using Stego to disseminate information to sleeper cells both in America and abroad. USA Today, for example, quoted "US Officials" this way: "U.S. officials and experts say it's the latest method of communication being used by Osama bin Laden and his associates to outfox law enforcement. Bin Laden and others are hiding maps and photographs of terrorist targets and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites, U.S. and foreign officials say." (http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm) Mostly, the commentary was not a question of if but rather how long.

I contend, however, that Steganography is not required, nor significantly used, by terrorist organizations for a number of reasons. Commonly available IT software and equipment such as 802.11b wireless networks, laptop and desktop computers, high-capacity media devices, and a little creative thinking, make it possible, indeed simple, to facilitate efficient, short-duration, and completely anonymous communications between even casual hosts. In this paper, using common technology, I will demonstrate various ways and methods for simple, clandestine communications that are virtually undetectable and untraceable.

In order to be most effective, clandestine data transmission between parties must be simple, stealthy, and efficient. Many would say security of the data is important, but data security in this case can also be viewed as a vector of the exposure time of the data in question to outside parties. Additionally, focus will be given to both short and long range data transmission, including transmission through methods as simple as a physical hand-off of data between parties to more complicated means across larger distances between parties which do not have physical contact, such as wireless and Internet transmissions.

First we will examine three high-capacity data storage devices, their immunity to detection, and the ease with which they can be transferred between parties. Next, we will examine short burst dissemination through the use of wireless transmissions in high-density populations, such as Washington, DC or San Francisco. Lastly, we will examine the use of the web in simple, effective, and virtually undetectable intelligence dissemination.

Steganography and the Case Against It

Steganography is defined by SANS (in GSEC Online Training, Section 10.4.4 http://giactc.giac.org/cgi-bin/momaudio/s=10.4.4/a=yBTFYFYKCO9/SE_44) as literally

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

meaning “covered writing”, or using images to hide data. Since the time of the Ancient Greece, man has sought to use hidden words and masking techniques in order to convey intelligence information without compromise. Today, Steganography is used in computers to hide information within graphics, such as .jpeg, .gif, and .bmp files, the most common image types. Numerous websites cover the topic, such as StegoArchive.com (http://members.tripod.com/steganography/stego.html). This site also offers links to Steganography software like Steganos Security Suite 4® (http://www.steganos.com/./es/), or even Stego freeware tool sets like The Third Eye® or ImageHide®. There are pages for Windows, MAC, BSD, and Linux Stego tools, advice, and information.

In order to work effectively, Stego requires the use of software, the ability to transmit the masked intelligence once complied by the software, and the ability to unmask the message from the software on the other end. Stego requires specific software, the presence of which on a suspect’s computer only serves to increase the light of suspicion upon them. On pages 245 and 246 of his book *Secrets and Lies*, Bruce Schneier, CTO of Counterpane Internet Security® (a Managed Security Service (MSS) company), describes the process of Steganography this way:

“Steganography offers a measure of privacy beyond that provided by encryption. If Alice wants to send Bob an email message securely, she can use any of several popular email encryption programs. However, an eavesdropper can intercept the message and, while she might not be able to read it, she will know that Alice is sending Bob a secret message. Steganography allows Alice to communicate with Bob secretly; she can take her message and hit it in a GIF file of a pair of Giraffes.”

After the terrorist attacks of September 11th, many prominent industry pundits speculated on the use of Steganography by terrorist organizations such as Al-Qaeda. Most agreed that the use of Stego by terrorists was not a question of “if” but rather “for how long”. In an article discussing the subject, Bruce Schneier stated “It doesn't surprise me that terrorists are using this trick.“ (www.counterpane.com/crypto-gram-0109a.html#6). Former National Security Agency instructor and experimental nuclear physicist", Dr Robert Koontz, further claimed that “coded images show plans for massive germ attack on US killing millions “. Speculation ran amok as to the types of information that would pass best through the use of Stego. There were even online reports of a Stego research effort published on the subject in the months before the attack by a PhD candidate at the University of Michigan named Niels Provos (http://www.citi.umich.edu/u/provos/stego/). It was dedicated to uncovering the extent to which terrorists and other international miscreants were already utilizing Stego for intelligence dissemination. The dissertation’s resurfacing immediately caused a stir because it could find little proof that Stego was in use by anyone based upon a cross-section of thousands of common online images. Observers debunked the report as not using good scientific methods or enough empirical data to paint an accurate picture. But Schneier’s book puts the Stego discussion in its proper perspective as he further explains:

“So far so good. But that’s not how the system really works. The eavesdropper isn’t stupid; as soon as she sees the giraffe picture she’s going to get suspicious. Why would Alice send Bob a picture of two giraffes?”

Also, what Schneier doesn’t mention is the alternative method of posting

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

images files with embedded data to web sites. This is even more obvious as these images can be downloaded by anyone with access to the site. Once downloaded, they can then be examined and dissected at the investigator's leisure. This makes posting Stego-embedded image files to publicly accessible web sites a foolhardy endeavor for even the most novice of terrorists. Schneier continues:

"The point here is that Steganography isn't enough. Alice and Bob must hide the fact that they are communicating anything other than innocuous photographs. This only works when Steganography can be used within existing communications patterns…If Alice and Bob change their communications patterns to hide the messages, it won't work. An eavesdropper will figure it out.

"This is important. I've seen Steganography recommended for secret communications in oppressive regimes, where the simple act of sending an encrypted email could be considered subversive. This is bad advice…Steganography programs exist to hide files on your hard drive. This can work, but you still need a good cover story."

Schneier's point is significant because it clearly debunks the most popular justification for Terror, Inc.'s use of Stego: because they can. Sure Steganography tools and techniques are readily available, but does it make any sense to use it? In light of other easier, more commonly available, less conspicuous means of disseminating intelligence, I ask why bother? Why take such an obvious and consuming step, one which requires training, specific software, and techniques, when mission objectives are more easily and efficiently accomplished in any number of ways?

Schneier's final point is also important: "One issue with Steganography is bandwidth. It's easy to hide a few bits of information; hiding an entire email message is a lot harder." Basically, it's easy to place small amounts of information into an image without significant degradation or risk issues, but not more detailed or larger chunks of information.

While I believe that Steganography is in fact in use by major terrorist organizations and organized crime alike, I dispute the fact that Stego is either wide spread or the most common or efficient method for intelligence distribution by such groups. There are several reasons why Stego is a second choice, at best, some of which we have just discussed. But there are more.

First, Stego is limited in scope. It requires specific tools and the knowledge to use those tools. While both can be readily attained, they require some level of effort. In the case of terrorist cells, this knowledge must also be disseminated across a wide geographic area and between numerous groups who many not (or should not) know that the other groups exist. Terrorist sleeper cells are often deliberately unaware of the others within the same terror organization so as to limit the ability of law enforcement or Intel groups to trace and connect them. Using Stego tools across these groups would therefore provide an established link that could be traced. This could then, in turn, provide plausible deniability if the perpetrator were to be apprehended.

Second, Stego is easily traceable since it requires specific tools to function properly. Thus, the presence of such tools to mask and then unmask data within images on a computer system would normally signify a user with advanced knowledge and perhaps a more sinister goal than typical end users. One may imply that this could be achieved by transmitting Stego data through images on a compromised victim host,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

rather than the terrorist's own machine, but this requires still more additional training to achieve such ends.

Third, Stego can be undone by others with similar tool sets or other forensic capabilities. Thus, the mere presence of data hidden within images on a system allows law enforcement authorities to make certain assumptions and take their investigation to the next level. Random examination of images posted online is how Provos' research project on the extent of Stego use was even possible.

I contend therefore that Steganography is not a significant player within terrorist operations online simply due to the fact that it's more effort than they have to expend in order to successfully pass intelligence information. Today, common tools and equipment make it possible for end user terrorists with virtually no knowledge to transmit and receive information with ease. Intelligence transmission and reception points, for example, can be set up and dismantled without the need for uncommon or hard-to-use tools or equipment, by personnel with minimal knowledge or technical understanding.

Understanding the limits of Stego, combined with a strong knowledge of our opponents' operations, tactics, and beliefs, allows us to understand why groups like al-Qaeda would prefer other methods. In his book, *Holy War, Inc*., Peter L. Bergen outlines the way Osama bin Laden built the world's most notorious terrorist organization as "a veritable corporation that has exploited twenty-first-century communications and weapons technologies in the service of a medieval reading of the Koran and holy war". This is a group with brutal designs and cut-throat efficiency, which provides further evidence that Stego is, at best, a minor player in terror operations. There are many more efficient ways to pass intelligence data, and complicated encryption or security masking measures are not required. Readily available mass storage devices, for example, can pass through detection systems, wireless LANs can be brought up or down in a matter of seconds, and provide the means to be a virtually untraceable center point for intelligence distribution. The three test cases contained in this paper demonstrate alternatives to the risks and pains of Steganography. They examine how to carry out clandestine intelligence trafficking without detection, with minimal investment, knowledge, effort, or money.

Test Case 1:
Intelligence Handling Via Micro Storage Devices

Data storage methods have improved dramatically in the past 5 years. As the capacities for data storage increase, the size and mobility of the devices themselves diminishes. This, in turn, reduces the possibility of detection of such devices in restricted environments, making it easy to transport, pass off, or even steal sensitive data without being caught. Moreover, the Plug-n-Play (PnP) capability of today's Operating Systems (OSes), applications, and media devices, offer the ability to cross platforms without regard for compatibility issues.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Figure 1

One such device is the Sony Memory Stick®. Figure 1 shows that the Memory Stick is no bigger than a stick of Wrigley's® gum, and is smaller than a human thumb. Memory Sticks come in various sizes from 4 Megabytes (MB) up to 256MB. These sizes enable the Memory Stick to be used for anything from simple document theft or malware injection into a target network to more complicated and involved efforts such as passing information from handlers to agents. In fact, Laptop magazine recently commented that Sony is "planning on rolling out Memory Stick peripherals that are more than just flash memory—they extend the functionality of connected devices" (Laptop Magazine, Sept 01, pp62-71). Options include using the Memory Stick as a bootable device or security token to protect system access security and provide authentication. Figures 2-5 demonstrate how a Memory Stick may be concealed in a pack of gum with ease.

Figures 2, 3

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Figures 4, 5

Once concealed, the Memory Stick is capable of being transferred between persons effortlessly, and without fear of discovery. Built of plastic, it is undetectable to airport screening equipment and can be passed through metal detectors without triggering alarms. In this example, a handler travels through an American airport security checkpoint with the Memory Stick concealed in the manner described above. With no visual clues as to the presence of the media device and no alert warnings from airport metal detectors, the handler passes easily through security and on to his destination. If for any reason something else in his possession triggers an alert or concern from security, a basic search of his belongings will not reveal the media device.

Another example could demonstrate how to pass a Memory Stick between parties without detection. A public information transfer could easily happen between a handler (the data giver) and client (the data receiver), and does not require that they know one another or have prior knowledge of each other. The client arrives at a news stand and asks the handler (working the stand) for “a pack of gum, the paper, and a diet Jolt Cola”. The handler, knowing by prearrangement that this is the signal for the hand-off (yet not knowing the client by face or name prior to the hand-off), offers the gum pack containing the Memory Stick but lets the client know that there is no such thing as diet Jolt Cola. The client pays for the gum and paper and departs, taking the new intelligence with him. The entire transaction takes seconds and draws no undue attention from other patrons.

The Memory Stick is also compatible with numerous devices for file recognition and transfer. Current versions of Windows and MAC OS X auto-read Memory Sticks in a PnP format. Figures 7-9 show three reader devices and ways in which Memory Sticks can be accessed from various PC and MAC desktop and portable machines.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Figures 7-9

Other devices which behave and operate similarly to the Memory Stick include USB disk drive media devices, such as the Disk-on-Key® device by M-Systems®, and portable MP3 music players like the Apple iPod® (see Figures 10-11). These devices, while more physically conspicuous than the Memory Stick, offer greater storage capacities, equally simple PnP compatibility, and (in the case of the music players) raise even fewer concerns at most security checkpoints. This is due to a general lack of understanding of the technology by physical security personnel.

The Disk-on-Key media device (Figure 10 below), can gather from 4 to 512MB of data from a machine in seconds because, like the other devices, modern OSes read it as a hard disk device. This gives it drag-n-drop capability and does not require special software in most cases to operate. In fact, M-Systems own website (www.diskonkey.com) sites the advantages of the product as "No driver installation required. Crosses the boundaries between Macintosh and PC. Personal, reliable, pocketable". Although only touting Mac and PC compatibility, Disk-on-Key is Linux kernel 2.4.0 compatible as well, providing a formidable, not easily traceable data leak or attack vector within your organization.

Figures 10, 11

The Apple iPod (Figure 11 above, www.apple.com/ipod) is even more stealthy in its operation. Capable of storing up to 20GB of music or data, the iPod software already comes with the ability to store and retrieve contact information. Moreover, data not recognized as a music file or contact by the iPod's internal OS can still be placed into the iPod folder yet will not show up in a visual inspection of the device by security personnel without a prior knowledge of various asymmetric ways to use the iPod for data storage. Storing intelligence on the iPod without detection, therefore, becomes as

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

easy as dragging data files into the iPod folder and then designating them as “hidden files”. Without a good bit of work by a diligent investigator, the data will go unnoticed, preventing law enforcement from the ability to stop the data flow or prosecute the handler. Figure 12 is a screen shot demonstrating a test file dragged onto the iPod.

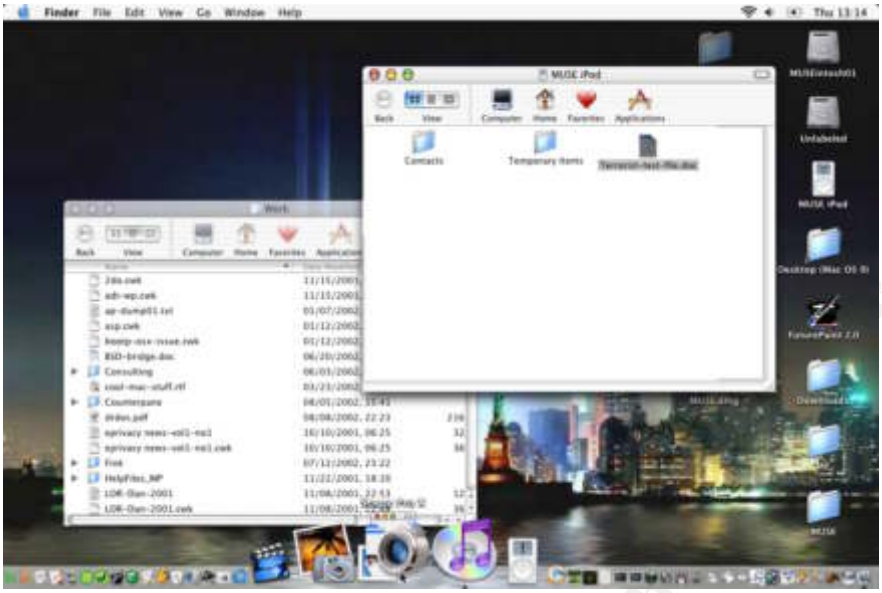


Figure 12

Perhaps the most powerful feature of the iPod is the fact that it is a bootable device. This makes it possible to potentially bypass security measures put in place at government facilities by booting directly into an installed OS on the iPod and then reading the machine drive and transferring data from it to the iPod. Since everything occurs on the victim machine, it is virtually untraceable even with extensive logging by today’s more popular logging applications.

Table 1 below outlines the best usage scenarios and advantages and disadvantages for various media devices. Specific scenarios require specific applications of specific hardware.

Media Type	Advantages	Disadvantages	Best Use Scenario
Sony Memory Stick	Size, material construction, storage capacity, compatibility.	Memory Stick readers not as common on many systems	Airport or other metal detectors, person-to-person exchanges, or where a micro-compact device size is critical
M-Systems USB “Disk-on-Key”	Size, storage capacity, compatibility, common connector (USB)	Material construction, certain OS driver requirements	Quick, slip-n-go data theft and transfer.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Apple iPod MP3 Player	Lg storage capacity, compatibility, masked function	Largest storage device, material construction, some secure areas do not allow media devices through.	Airports, person-to-person exchanges, where large storage capacities are required, or where data theft requires bypassing installed OSes (MAC only).

Data disposal for the Memory Stick or other media devices described here can be performed in any number of ways. Since these devices are most often read by modern OSes the same as an additional hard drive, common free and fee data scrubbing utilities such as SafeShred v1.0 for the MAC by Code Tek (www.codetek.com) or CyberScrub for the PC (www.cyberscrub.com), by the company of the same name, can be used to safely and securely delete any data that may cause prosecutory or litigious concerns or that may thwart plans for some act of terrorism. CyberScrub even claims to have "military grade" scrubbing capability, overwriting data numerous times. This is a key point to true data security as simply deleting the files will not be enough to safely avoid detection and recovery by competent computer forensics specialists. The data must be overwritten multiple times, particularly in the case of terrorists whose actions and media devices will be investigated by such groups as the DoD, FBI, NSA, and CIA. These groups possess the most sophisticated computer forensics prowess in the world today.

Test Case 2:
Intelligence Handling Via Wireless Devices

Another efficient and virtually untraceable alternative to Stego is intelligence handling via wireless devices. While wireless connectivity protocols such as 802.11 are known to be susceptible to attack and penetration, it really doesn't matter if they are used by terror organizations is specific ways. It takes mere minutes to set up a wireless Access Point (AP), and only seconds to bring it down. Once established, an AP can become a temporary hub for intelligence dissemination to terrorist cells who do not require any knowledge of one another in order to effectively transfer information.

First, let's discuss the tools required for the job. In order to be effective for clandestine intelligence dissemination, the 802.11 AP and network must be swift in setup, easy-to-operate, and allow multiple system types and OSes to utilize it without difficult steps. For this example, we will use the Apple Airport® 802.11b wireless base station.

The Apple Airport is a $299 wireless AP available online (www.apple.com/airport/) that allows both PCs and MACs to connect to it with relative ease. It allows up to 50 simultaneous users access and 128-bit encryption. Security can be further enhanced by requiring a password to access the network or a single-click configuration which allows the network not to appear at all unless requested by the user through a specific series of steps (see below). It even comes with built-in Firewall (FW)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

software. For the purposes of this example, however, the airport AP could be used without any form of encryption or security enhancement. Figure 13 shows the Apple Airport.

Figure 13

Next, terrorist cells must have a way of accessing the airport once configured. Since the airport allows both PCs and MACs to access it, this example will use both an Apple Titanium Powerbook® (Figure 14) and a Sony C1-VP Picturebook® (Figure 15). For the easiest setup via PC, the MAC compatible Proxim® 802.11 PCMCIA card (formerly the Farallon card) will be used (Figure 16). This is because the Proxim card allows basically PnP setup and access to the airport, where some other cards require a more complex configuration.

Figures 14-16

Lastly, since the example demonstrates communications between terrorist cells, which do not have prior knowledge of one another, the site must be in a preset location or area, and must broadcast for a specific length of time to properly disseminate information. In this example, we will utilize a clock face location plan for the AP's location in the city, and the weather report for the time and duration that the AP remains active and available.

The clock face plan for location is simple enough: using an overhead map of the city of Washington, DC (our example city), each month the AP name (FREEnet in this case) will appear in a different quarter of the city for the given duration. In the map in Figure 17, the non-shaded portion of the map indicates the area of the city where APs will be active during the month of August. Starting at the top with the city divided in quarters, the month of January of a given year occupies the first quarter. Then, in c a clockwise manner, February the next quarter to the right, March the next quarter, and so on. This simple instruction makes it possible for a terrorist to keep the fact in memory without a difficult learning curve and thus be in the right quarter during the right month to receive vital intelligence necessary for carrying out attacks. Because if its simplicity, the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

terrorist also does not need to creates or possess physical evidence (i.e.: instructions on paper or in email), making prosecution more difficult.

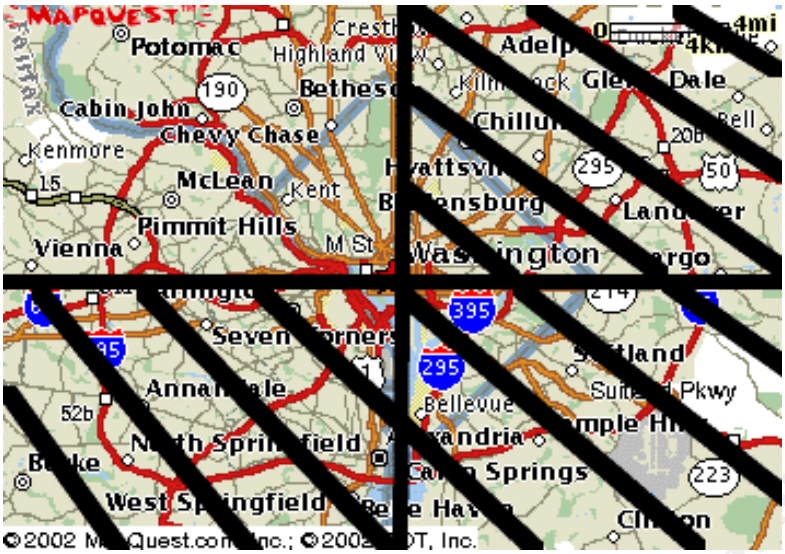


Figure 17

Using the local DC weather report for AP uptime and duration is even simpler. In this example, my Verizon® cellular phone is set to receive text alerts with local DC weather reports daily at 0600 hours. To set this up I accessed daily information deliveries at the Verizon phone support site for text messaging (www.vtext.com) and chose to have weather alerts sent at 0600 daily (Figure 18). The weather information arrives on my cell phone at 0600 each morning, which clues me into what time the FREEnet AP will come up and how long it will remain up.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Figure 18

To achieve this, I simply take the day's low and high temperatures and split them up in the following manner:

Day's Low Temp	Day's High Temp	First time FREEnet AP comes up	How long it stays up	Second time FREEnet AP comes up	How long it stays up
79 degrees	91 degrees	0700 hours	90 minutes	2100 hours	10 minutes
		based upon the 7 digit in the low temp applied to the local times that fall between midnight and noon.	based upon the 9 digit in the low temp multiplied by 10.	based upon the 9 digit in the high temp applied to the local times that fall between noon and midnight.	based upon the 1 digit in the high temp multiplied by 10.

***NOTE: for temps that are triple digits (i.e.: 105 degrees or 115 degrees for a high temp) the duration of how long the AP will stay up is still multiplied by 10. Thus, 105 = 50 minutes and 115 = 150 minutes respectively. For a zero reading (i.e.: 90 degrees), the default duration time is 10 minutes.**

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Here's how it all works: Using the month of August and the weather report to my cell phone in Figure 19a-c below, I know that the FREEnet wireless AP will be up on Friday at 0700 hours for 40 minutes and again at 2100 hours for 20 minutes. On Saturday, the AP will come up at 0700 and stay up for 30 minutes and then come up again at 2100 and remain up for 10 minutes. Finally on Sunday, the AP comes up at 0700 and stays up for 10 minutes and then again at 2000 and stays up for 80 minutes.

Using this simple, repeatable pattern, a terrorist cell could receive directions, instructions, or other intelligence from a higher cell or single operative, yet would never have to meet them in person or have knowledge of them if arrested. Also, if arrested, the terrorist's actions and the information they carried would not draw undue attention unless they were arrested at the moment they downloaded the information. If you remember Figures 7-9 above, a terrorist could use a Sony Memory Stick to capture the downloads from the FREEnet AP, then remove the Memory Stick from the system in question and disseminate it in a person-to-person hand off, or simply upload it to their web-based email account to be stored relatively anonymously online and out of the sight of prying law enforcement eyes.

Figures 19a-c

Test Case 3:
Intelligence Handling Via Free Portals and Services

The third example to discuss as an alternative to Steganography is the use of free portals and services, such as free email and web pages. Today, globally known companies such as Yahoo!®, Hotmail®, and others offer online email addresses completely free of charge. These addresses can be set up without using any of your actual real data. They are also called *covered accounts* in Intelligence circles, which

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

simply means an email account with bogus data. Figure 20 is a screenshot of a covered account I set up on Yahoo! for this paper. Some might argue that even this data can be traced back to the PC you posted it from based upon log data, which is true. But then again, you could set this up from a public library, a stolen PC, or even one of those roadside kiosk Internet connections available for free in many rest areas nationwide. This makes it possible to set up a completely anonymous and free intelligence communications conduit for short-term use in an untraceable manner.

Note that I checked the "List my new Yahoo! Mail address for free" option, so that others can find my address based upon preset directions from my terror cell leadership. Thus, other members of my cell or other cells going online could easily find cell members' addresses for information dissemination. Much in the same manner that we previously established a data dissemination process using the weather report, a simple process for establishing member email IDs and transmission times can be accomplished as well. Also note that I intentionally misspelled the word Taliban as "Taliman" in the username in case Yahoo! or some law enforcement entity is running scripts to data mine keywords and investigate owners.

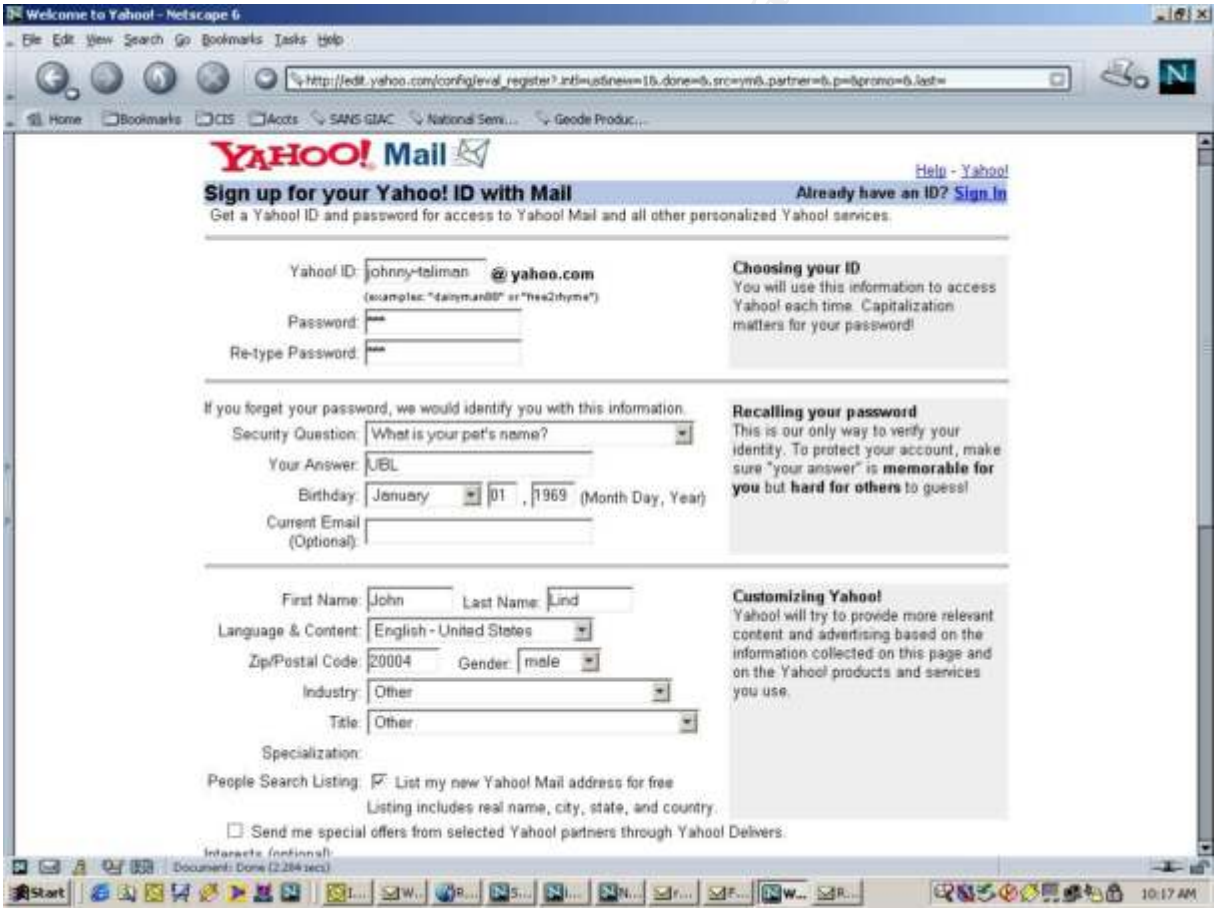


Figure 20

Once established, the cell could keep the addresses active for short periods, then rotate to a new set based upon previous instructions. After 90 days of inactivity, most free email providers like Yahoo! will automatically deactivate the accounts anyway

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

to conserve server space and reduce manageability overhead issues. The following simple chart outlines a potential process for a rotating schedule of cell member addressing to carry out clandestine operations:

Sample Process for Simple Email Rotation by Terror Cells	
Requirements	**Solution**
1. Unique yet simple user naming convention for each cell	Abbreviations based upon terror group, cell location (city), and cell order: "AQDC01" (al-Qaeda/Washington, DC/1st cell) "HSF01" (Hamas/San Francisco/1st cell)
2. Consecutive numbering based upon rank within the cell (unchanging)	001 = Cell Leader (CEO) 002 = Cell Operations Leader (COO) 099= Cell Operative (Employee)
3. Code for rotational period	Rotate between providers monthly.
4. Provider Rotation Schedule	Rotate on the following schedule: JAN: US-Yahoo! JUL: Israel FEB: US-Bigfoot AUG: India MAR: US-Hotmail SEP: Thailand APR: France OCT: Japan MAY: Russia NOV: Malaysia JUN: Philippines DEC: Turkey
Sample output: AQDC021@yahoo.com Good for the month of January for a generic operative of the first DC terror cell for al-Qaeda.	

It is important to note that the use of non-US-based free email services, in countries such as Israel or Russia, would be preferable due to the complex nature of American law enforcement trying to get a foreign ISP to release information for investigation or prosecution. Moreover, any reasonably intelligent terror cell operatives would attempt to use (or establish themselves) free email services in developed nations with whom the United States lacks extradition agreements, reciprocal cyber law, and other law enforcement agreements, or at least whose cyber laws permit or only weakly punish offenders. Countries such as these could include India, the Philippines, Holland, and France.

With rotating contact data, terror cells can pass information and disseminate intelligence with impunity. Add to that the global nature of the Internet, and data can then be disseminated from the highest levels of a terror organization to its lowest operatives, in any country, at any time, and without suspicion. The very nature of the World Wide Web allows for anonymity, privacy, and stealth if even a few basic precautions are taken. How many times have we heard of stalking cases or hacking stories where one party had no idea what the other looked like, or how dangerous they really were, or how much personal data the attacker or stalker could gather about them

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

from the web. The loose structure of the Internet is ideal for terrorist groups, organized crime, or other dangerous individuals or entities who seek to exploit or harm others.

Along with free services, many web sites offer online storage and web page services either for free or at a low cost. Dial-up ISPs such as AT&T, Sprint, AOL, and MCI, offer megabytes of free storage and personal web space online with the purchase of a user account. In the case of AOL, this service doesn't even require a credit card as a user can pay by direct debit billing from a bank account. As was demonstrated during the investigations that followed 9-11, getting a bank account under a fake name and bogus Social Security Number (SSN) in the US is easy.

Once established under the fake ID and account, a terrorist intelligence collection or dissemination page is simple enough to post. It takes only a few steps and providers even offer templates and other quick start instructions designed to walk newbie web users through the basics of posting their pictures, links, and text to a personal web page. Figure 21 is a screenshot of a personal web page I set up through my AT&T account in a matter of minutes. Posting images or links or text takes only seconds more and is no more complicated than a drag-n-drop process.

Figure 21

To disseminate the latest intelligence a terrorist simply needs to pass the URL via email to the group. With 30 or more members in a cell, the page (and the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

intelligence contained within it) can be moved to a different cell user's personal page every month. Each time a team member has cycled through their turn to host the page, they simply close the account and open another with a different provider so that the next time they host they reside at an entirely different location. A process such as this, particularly when combined with the email rotation process above, would make it almost impossible for a law enforcement or intelligence agency to keep up an investigation with any regularity.

In order to further mask the presence of the page to outsiders, the host can choose to use no keywords or meta tags in their pages. Crawlers from major data mining search services such as Google® (www.google.com) or Altavista® (www.altavista.com) will eventually index the pages, but the cell member host can also change page content regularly to help thwart this. They can also change the main pages or place invisible link markers within the main page to allow connection to the real data while innocuous data (or no data at all) takes up the main page. Additionally, as they rotate monthly, the pages will need to be reindexed on a consistent basis. This further complicates the efforts of law enforcement.

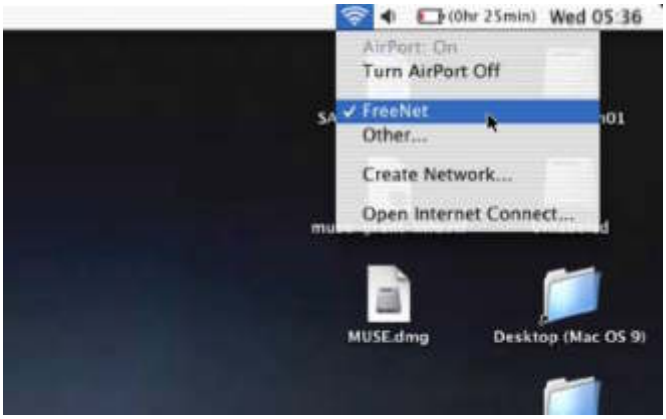
The Scenario In Action:

To carry the scenario to its full extent using the above examples, our intelligence collector client will be a DC taxi cab driver who is part of a terror cell. Being a cab driver gives him full access to the city and the terrorist APs that are replete within it. He drives the city on his normal routes (perhaps as a Dulles or Ronald Reagan airport taxi driver) ferrying passengers between destinations.

At the start of his day, he checks the "Eternal Hope" web site or his personal email on Yahoo! for messages. The "message of hope" for the day reads ***The Wind of Change is Coming***, which tells him that new intelligence for a terror attack is on its way to his city. His shift is 0600 to 1800, so he receives his weather report on his cell phone as he comes on shift. He picks up and drops off a couple passengers between 0600 and 0700, then turns his cab light to "off duty" (if necessary) so that he can patrol his area of interest uninterrupted yet inconspicuously.

At a stoplight in Georgetown, he finds the FREEnet AP with his Apple laptop (Figure 22) and logs in. Once in he connects to the Win98 box plugged into the network and draws three files off of the system and onto the Sony Memory Stick in his PCMCIA slot. By the time the light turns green he has downloaded an instruction file, a map image file, and an operations file. Perhaps the files are zipped and password protected, which he receives in his email later that day, or perhaps they are PGP encrypted (though using PGP or zip passwords means more overhead and more chance of linking otherwise unrelated terror persons and groups). He turns his off duty light back to "on duty" and continues his day. A week later, hundreds are killed by three homicide bombers on the Mall in Washington at the height of the tourist season.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.



The Future

The Future of Clandestine Intelligence Dissemination looks even more sinister. The introduction, success, and wide spread of Peer-to-Peer (P2P) applications such as Gnutella®, Kazaa®, and Morpheus®, make it possible to share files in short duration bursts without much fear of discovery. Here's how things work today and where they are headed:

Gnutella (www.gnutella.com/) burst on the scene just a couple years ago as a file sharing utility. It caused quite a stir in the law enforcement community (http://www.cyberlawenforcement.org/cleo_bio/kp.html) because it was Peer-to-Peer, meaning it did not require a central server to operate but could instead link two clients together directly online, and anywhere the Internet would carry them. This kind of decentralized global village concept was a bane to law enforcement, who cited its use to swap and disseminate child pornography (http://www.internetnews.com/bus-news/article.php/6_556161) very wide spread and virtually impossible to detect and trace.

Shortly thereafter, Napster® emerged (www.napster.com). Napster was a Gnutella spin off designed for global file sharing of MP3 and other music files. It operated slightly differently from Gnutella in that it required all users to traverse the Napster server in order to communicate P2P. This made it possible to gather data on file traders for prosecution and discouraged Napster's use by smart malcontents.

Competitors such as Kazaa and Morpheus sprung up riding the successful coattails of Napster. Kazaa and Morpheus, once a one-in-the-same product with Morpheus as the application and Kazaa as the biggest service utilizing it. The Morpheus app was designed for music file sharing but worked in a more P2P manner that closely resembled Gnutella. Later, a dispute between Kazaa and Morpheus (www.musiccity.com) split the two with Morpheus getting a GUI makeover and Kazaa creating its own app, complete with trace back and data mining capability for customer exploitation by advertisers.

In the face of the demise of Napster, Morpheus' popularity rose dramatically. As a true P2P app, file sharing went way beyond mere music. Images, video, or virtually any other data is now shared by users of the product worldwide. Because of its P2P nature, Morpheus and other Gnutella spin-offs make it extremely difficult for law enforcement or intelligence groups to catch purveyors of illegal wares, including terrorists.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Morpheus, shown here in Figures 23 thru 25, is the present and the future of intelligence dissemination for terror organizations. Using the second example above for wireless uptime, the same taxi-driving terrorist could use Morpheus to connect to the system on the other end of the wireless device (or anywhere else in the world for that matter) to share, upload, or receive intelligence in seconds. Although a new member of Morpheus must sign up, bogus user names can be created with ease. Figure 23 shows a sample user account on Morpheus.

Figure 24 shows an active connection setup using Morpheus. Note the "gnutellanet" name in the server URL. In Figure 25, a music file is being legitimately shared to my system from some user around the world. Based upon the information the user sees, there is no way to tell whom I am sharing with, where they live, or who they really are offline. I could just as easily have placed text or data or image files on my system to share, titled them with unique names that would not be found by typical music searches, and placed ".mp3" extensions on them to quell suspicion. Then, I could simply share them with a handler or other terror cell somewhere in the world. Morpheus lets you search for specific users as well as files to share, so keeping your cell close is simple.

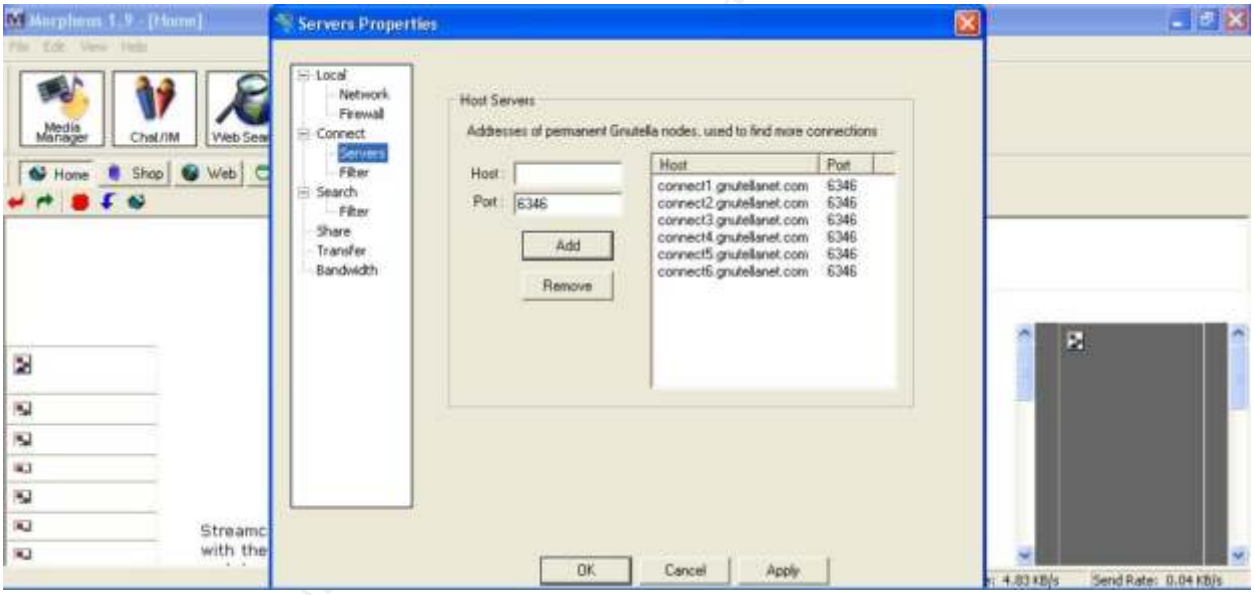


Figure 23

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

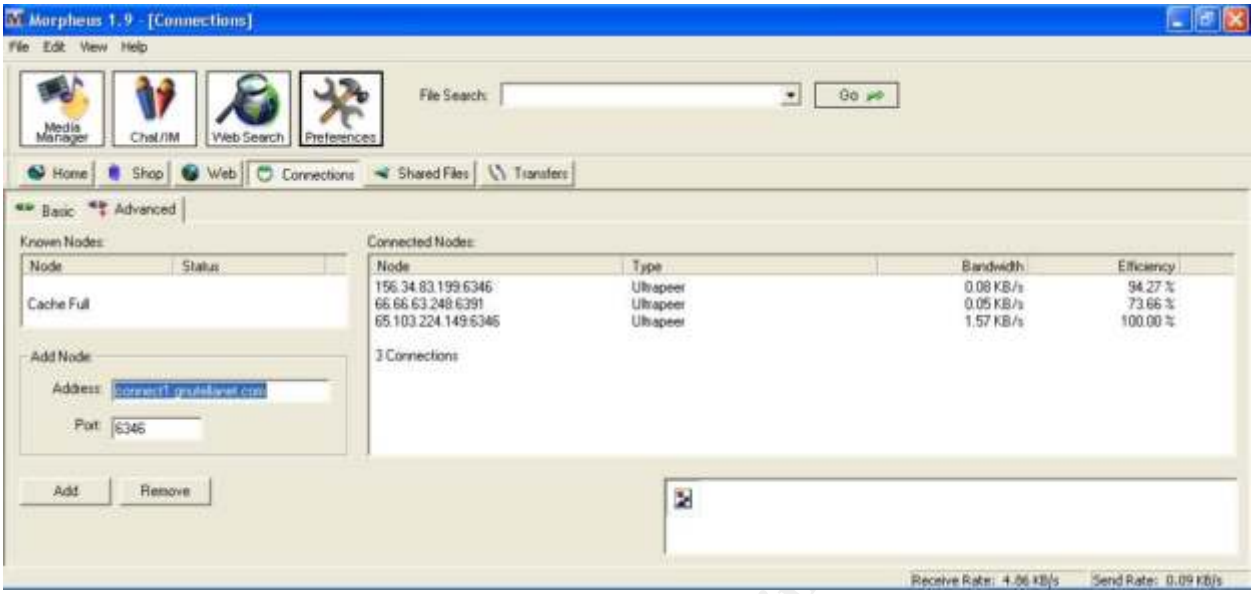


Figure 24

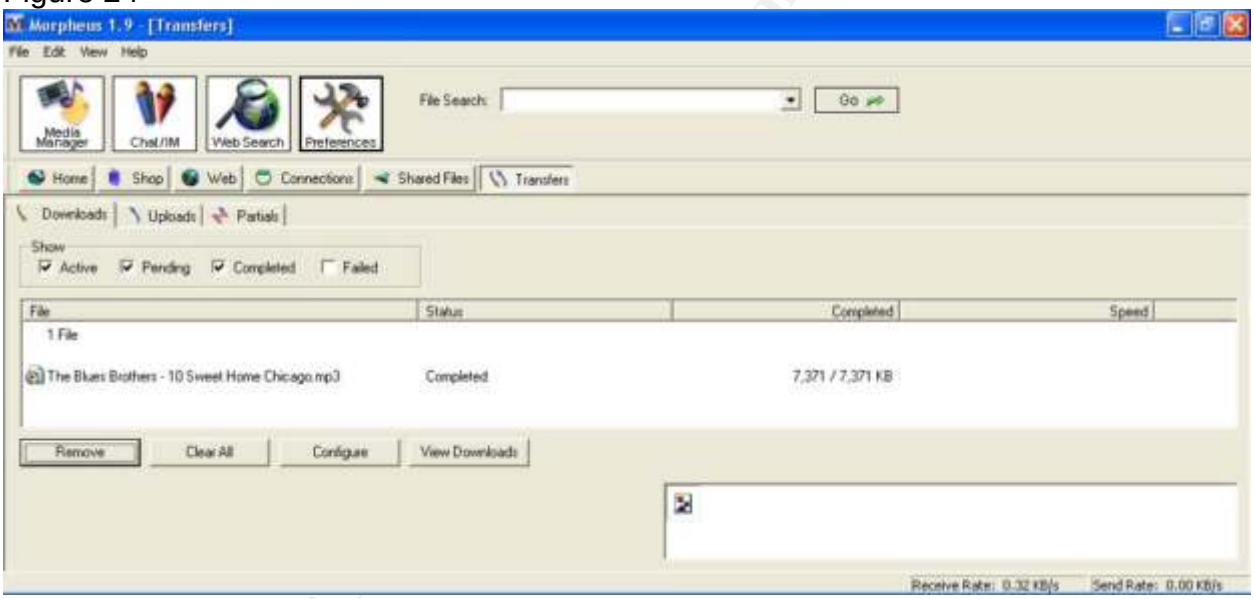


Figure 25

Perhaps the most disturbing thing about P2P apps like Gnutella is that Software Development Kits (SDKs) and special apps exist and are freely distributed. SDKs and other related software mean that savvy terror cells can create, distribute, and use their own specialized client apps to avoid detection and share or disseminate intelligence anonymously, and without detection. Figure 26 is a screenshot taken from the Gnutella web site listing just two development apps of those available. Note as well the presence of a development tab at the page masthead. Although under construction at the time this paper was written, it could soon be a breading ground for newer, more specialized and transparent Gnutella knock-offs. For the investment of time and effort involved, this capability would yield far more effective results for terror organizations than mere Steganography in images put up on some generic web site.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Figure 26

Conclusion

These chilling but completely plausible scenarios outline just how easy it is to disseminate timely intelligence in the Internet age. Steganography, while highly effective, doesn't even need to enter the equation in order for efficient and effective intelligence dissemination to take place. With a very limited budget and minimal technical expertise, terror cell members lying in wait within the U.S. can receive information and be activated to carry out their devastating work. It does not require specific training or complicated software that has traceable roots. It does not require secretive data hiding within the bits of an image file.

Today, moving intelligence in a virtually untraceable manner between parties who have no familiarity with one another can be easily accomplished without raising suspicions and without leaving potentially mission compromising information online buried in images that can be uncovered by law enforcement. In the Internet age, "cyber ghosts" pass unnoticed across networks with ease.

There is no point in working hard when one can work efficiently. Even terrorists will be lazy if given the chance. They will not be forced to engage in more difficult information operations pursuits, such as Steganography, until we as freedom loving people challenge and engage them more with stronger practices and policies, better enforcement, and greater vigilance.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Works Cited

[1] Laptop Magazine, September, 2001. "Mobile Storage Wars", pp 62-71.

[2] "SANS GIAC General Security Education Certification Online, Section 10.4.4" http://giactc.giac.org/cgi-bin/momaudio/s=10.4.4/a=yBTFYFYKCO9/SE_44).

[3] Breen, Christopher. Secrets of the iPod Berkeley: Peachpit Press. 2002. Ch3, pp 41-59.

[4] Counterpane Crypto-gram www.counterpane.com/crypto-gram-0109a.html#6

[5] "Detecting Steganographic Content on the Internet" http://www.citi.umich.edu/u/provos/stego/

[6] DeWitt, Michelle. Competitive Intelligence Competitive Advantage. Grand Rapids: Abacus. 1997. Ch 11-15. pp 165-195.

[7] Weisman, Carl J. The Essential Guide to RF & Wireless Upper Saddle River: Prentice Hall PTR. 2000. Ch 7, pp 165-193.

[8] Schneier, Bruce. Secrets & Lies: Digital Security in a Networked World New York: Wiley Computer Publishing. 2000. Ch 16, pp 245-246.

[9] Bergen, Peter L. Holy War, Inc. New York: The Free Press. 2001. Introduction.

[10] USA Today Online, Feb 05, 2001. http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm.

[11] The Stego Archive http://www.stegoarchive.com/

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 21st, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced