



Hidden Messages in Spam

> 2005 John Retterer

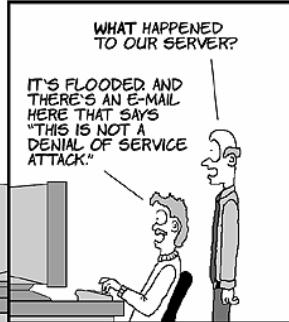
User Friendly on spam

USER FRIENDLY by Illiad



<http://www.userfriendly.org>
Copyright (c) 1999 Illiad

ZLOTNIKS!
SENDINK ME
SPAM...WILL
FIXINK THEIR
LEETLE RED
WAGON...



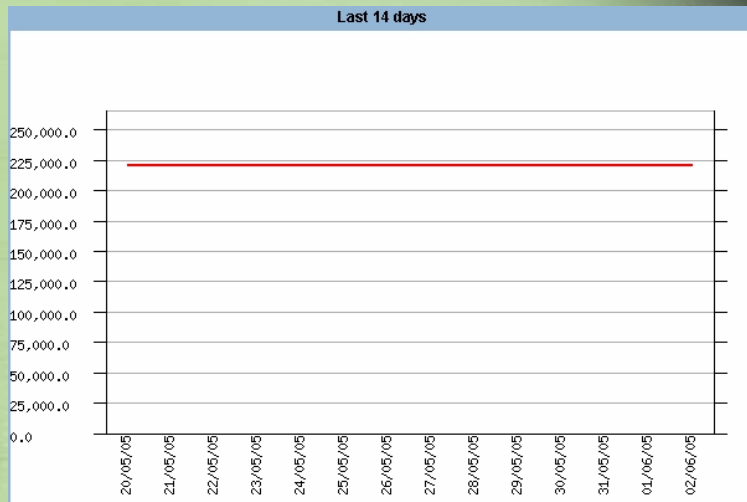


A spam by any other name...

Email commonly referred to as “spam”, (which by the way is a hormel foods registered trademark... they must be proud huh?)

Spam email Is also known as UCE – UBE. Most spam is sent to end users via open mail relays, or anonymous re mailers. Lets take a minute to check out some statistics to get a feel for how bad this problem really is. Most industry professionals believe that if we can control the open mail relays, we will be able to exert some control over the spammers.

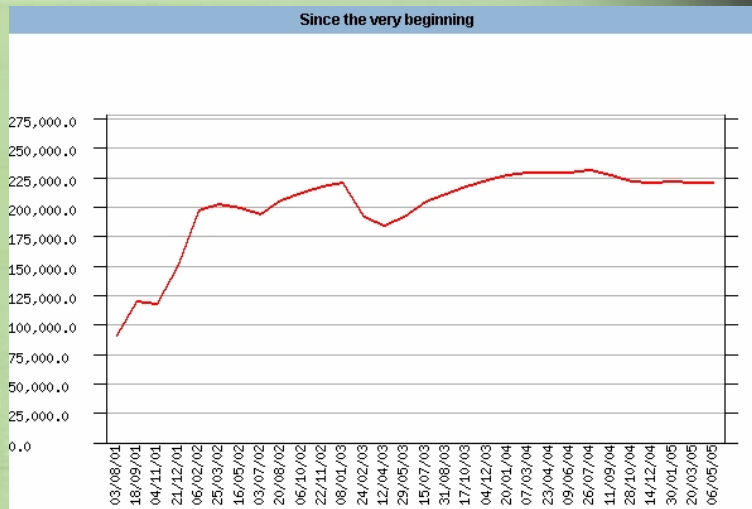
Open Mail Relays - ORDB



4

This statistic was taken from ORDB.ORG – the open relay database. This shows that a quarter of a million open mail relays are being tracked in the database at this time.

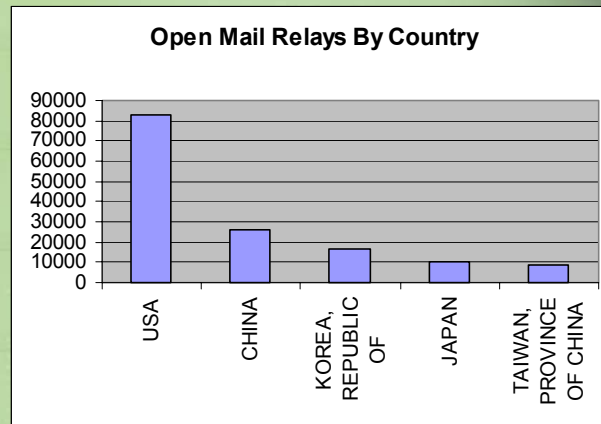
Open Mail Relays - ORDB



5

This statistic was also taken from ORDB.ORG showing the amount of open relays over time from March 2001 to the present. Although this problem has been identified for quite some time it doesn't appear to have had much success at controlling them yet. I was not able to find statistics on how many total mail servers existed in this period for comparisons sake.

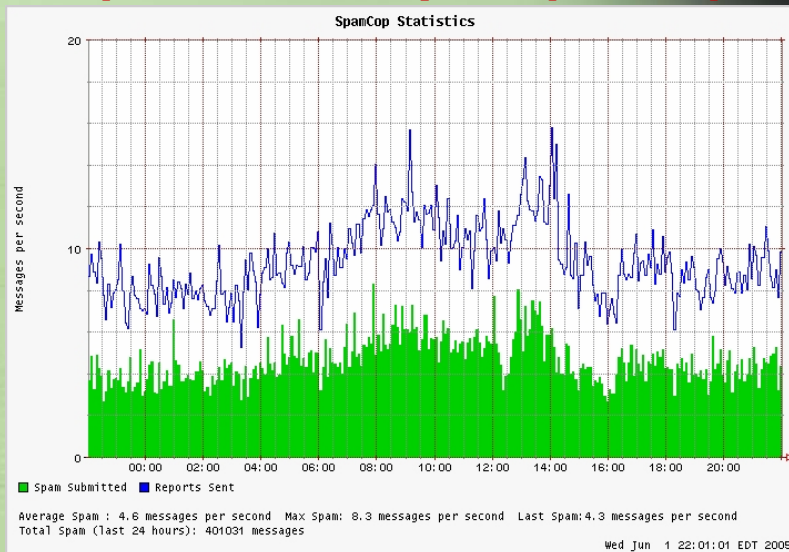
Open Mail Relays



6

So where are all of these open mail relays? Right here at home. The dangers of having an open mail relay somewhere on your network are real. Legitimate users of other mail servers in the same DNS domain might be blacklisted by other service providers. Any of you that have tried to get unblacklisted know that this can take some time and is best if avoided if possible.

Open Mail Relays - SpamCop



Here are the SPAMCOP stats for the last 24 hours as of last night. As you can see there is an average of 4.6 with a max of 8.3 messages per second.

Spam as a Covert Channel

> Purpose

Secret Communication

> What is the advantage?

Hiding in plain sight

Forged email sources

Re-Mailers and proxies can hide origin - sender is anonymous

Spam is broadcast - recipient remains anonymous

Plausible deniability

> What is the level of difficulty?

Common applications

Examples

Tools for further research

Some of the points I would like to discuss today will hopefully invoke some thought, and maybe even enlighten you a little to the potential of this subject. We will take a look at some disturbing ways that these seemingly harmless messages can be used. What I would like to talk a little bit about today is the potential effectiveness of this type of communication and it's ability to be used as a covert channel.

More than meets the eye?

- Email designed to be caught by spam filters
- Not Random text in headers, contents or signatures
- Reused from multiple sources (not one specific spammer)
- Usually not porn or scams (Do not want casual recipients looking too closely)
- HTML frequently contains invalid / broken links

Dr. Curtis Kret (Pseudonym)

Secure Science Corporation

9

In the course of my research I learned that Dr. Curtis Kret from Secure Science Corporation spoke at the black hat briefings on a similar subject last year. Worthy of mention is the fact that Curtis Kret is a pseudonym – now why would a guy in a room full of hackers use a pseudonym?? Dr. Krets briefing paper focused mainly on tracking spammers, although he did touch on the point of how effective it would be if used as a covert channel. His presentation is titled “Nobody's anonymous” and can be found at [www.blackhat.com / breifings section / 2004 briefings](http://www.blackhat.com/briefings/2004/briefings), if you are interested in examining headers to track and identify spammers this is a very informative paper and I recommend taking a look at it.

Spam makes an effective covert channel

- Two way blind conversation
- Closely resembles a Chain "Cut-Out"

A Cut-Out is a courier or mechanism used to pass information and devices from one party to another while operating in a "denied area" or a hostile environment.

There are two forms of cut-outs: block and chain.

- A block cut-out is an agent familiar with the entire network or cell and those who are in it.
- A chain cut-out is simply an agent who is aware of only the person providing the information and the party who is receiving the information.
- The chain cut-out helps to maintain the compartmentalization of the network, which increases security by maintaining everyone's anonymity.



Dead Drop Spike

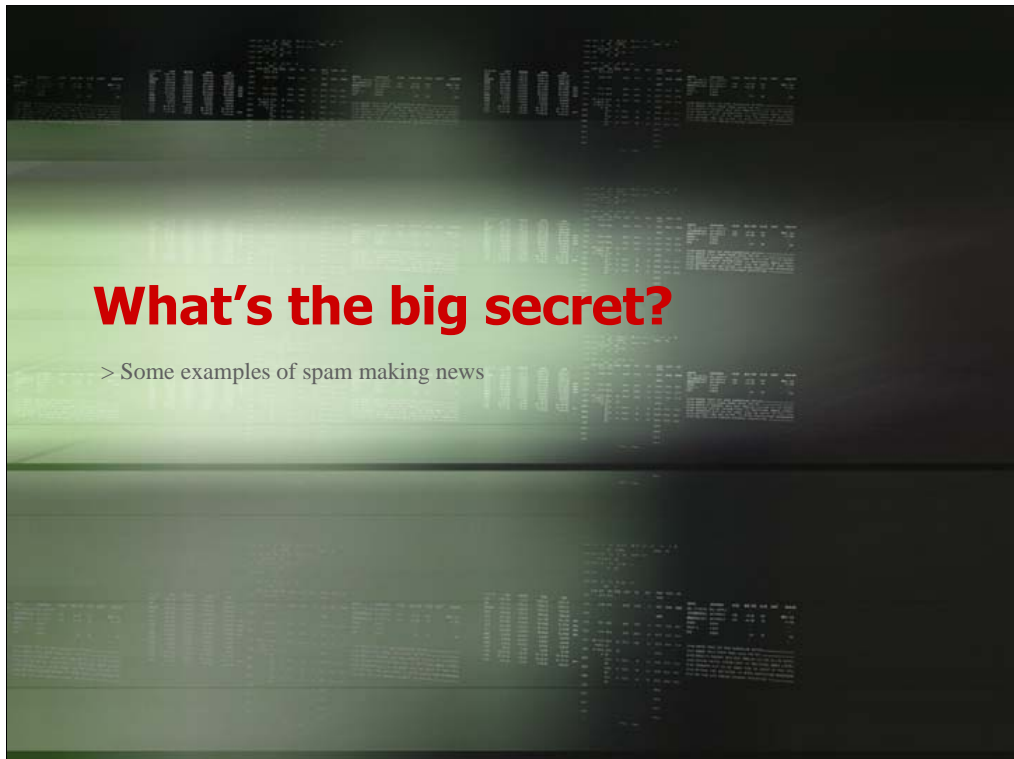
10

Spam can be two way blind.

All the recipient needs to know is some signal, address, name or key phrase that tips it off as an encoded message.

The sender only needs to know the address of the recipient.. Even if he doesn't know which recipient in a list is the intended party.

Much like the dead drop spike in the picture above All I have to know is where to put it... and all you have to know is where to find it.



So what's the big secret? Let's take a look at how spam is making news, and being used in a covert way.

AFF 419s and spam

News Analysis
21 January, 2004

US intelligence links 419s to terrorist attacks
Wayne Madsen

US intelligence sources have linked the ubiquitous Internet financial fraud spam emails, known as Advance Fee Fraud 419 (AFF 419) messages, to coded communications by terrorist groups and international organized crime syndicates.

According to the sources, who spoke on the condition of anonymity, the 419s have been used to clandestinely plan a number of terrorist actions, especially in Africa.

419 is the number of the section in the Nigerian penal code outlawing financial fraud. The coded transmissions are often found in sentences dealing with the assassinations of or coups d'état against former African heads of state.

According to US intelligence, such messages have contained actual planning information for three actual events in West Africa: the March 2003 assassination in Abidjan of the Saudi ambassador to the Ivory Coast, the killing of former Ivory Coast leader Robert Guei in September 2002, and an attempted Ivory Coast coup in January 2001 that resulted in a number of deaths.

With millions of 419s being sent on the Web, it was easy to hide coded communications within a few selected emails.

Terrorists and criminals choose Nigeria, the Ivory Coast, Ghana, Sierra Leone, Benin, Zimbabwe, Liberia, and other African nations as bases for their activities because of lax financial supervision and law enforcement by local authorities.

The fraudsters in these countries are aided and abetted by associates who have obtained employment in banks, post offices, and passport and taxation agencies in Western countries. Recently, 419s have started emanating from non-African locations such as Eastern Europe and Asia.

However, the use of 419s to pass terrorist planning information is waning because the number of spam emails being transmitted across the Web has dramatically decreased in recent months

News brought to you from [Computer Fraud & Security](#)

12

Anyone remember the Advance Fee Fraud scams that made the news a while back? In this article from 2004, it mentions that spam email was used to encode logistics information for distribution among the attackers.

Techno Robbers

Out of office' emails used to tip off burglars

Tif draws up guidelines to protect workers

Andy McCue, [Computing](#) 04 Dec 2002

Burglars are using information contained in 'out of office' auto-reply emails to target the homes of workers on holiday.

Criminals are buying lists of email addresses over the internet and sending mass-mailings in the hope of receiving automatic 'out of office' emails identifying employees away on holiday, according to blue chip user group The Corporate IT Forum (Tif).

Thieves cross-reference information in the email reply with publicly available data from online directories such as 192.com or bt.com. The burglars can often discover the name, address and telephone number of the person.

'You wouldn't go on holiday with a note pinned to your door saying who you were, how long you were away for and when you were coming back so why would you put this in an email?' said Tif chief executive David Roberts.

Tif has drawn up guidelines for workers to avoid falling victim, including keeping messages bland; redirecting enquiries to another colleague; not giving out your job title, not saying you are away on holiday; and not including personal contact details.

If that's not bad enough ... techno robbers? This news story talks about robbers buying mailing lists and sending out spam emails to phish for auto responders from people out on vacation. They used a web directory like yahoo people search and got their home addresses, and well you probably can figure out the rest.

Tactical spam

Spam is Winning the War on Terrorism

Sep 20 2003 by Jim Bauman

SPAM, "What is it good for? ...Absolutely nothin'" Hey, now hold on a minute! The Pentagon has found a use for it. Its covert operation has recently been made public.

For years, federal IT specialists and their highly paid consultants had consistently failed to track down and monitor laptops used by al-Qaeda operatives. To help in the search, the Pentagon enlisted the top twelve SPAMMERS in the world. They became "The Dirtiest Dozen," a reference to the Hollywood movie about twelve convicts who storm a Nazi stronghold and kill the top brass and their wives. Within hours, the Dirtiest Dozen had located the e-mail addresses of all al-Qaeda operatives and had overstuffed their mail databases with messages about Viagra, male and female appendage enhancement, a Ginsu knives blowout sale (ouch!), and various other tedium.

Success came in many ways. American and British Army units in Iraq and Afghanistan were able to capture scores of al-Qaeda members by following the trails of inoperative and abandoned al-Qaeda laptops. **In one case, Mr. El-Ziad, who was heavily bandaged, spoke from his jail cell at Guantanamo. He said that a week ago in a cave near the Pakistan border, "I was waiting for a communication from the most revered one when the computer began to smoke, pop, and make fizzing noises. I grabbed it and ran with it out of the cave, and all the time it was getting hotter and hotter to the touch. I screamed in pain as it burned my hands. I threw it into the poopy pit." The subsequent methane explosion killed nine of his comrades.**

Where the computers weren't fried, the bank accounts of some al-Qaeda cells were drained when they responded to the Nigerian e-mail scam. Some operatives were apprehended at their apartments in America and Britain when their discount pharmaceuticals from Canada were delivered.

This has to be the most entertaining of the three stories. I can't speak to the authenticity or accuracy of this story as it seems a little far fetched, but it was so funny I couldn't help but include it.



Lets talk about some simple techniques that could be used to hide data in a message.

Spam Mimic explanation

Explanation

There are terrific tools (like PGP and GPG) for encrypting your mail. If somebody along the way looks at the mail they can't understand it. But they do know you are sending encrypted mail to your pal.

The answer: encode your message into something innocent looking.

Your messages will be safe and nobody will know they're encrypted!

There is tons of spam flying around the Internet. Most people can't delete it fast enough. It's virtually invisible. This site gives you access to a program that will encrypt a short message into spam. Basically, the sentences it outputs vary depending on the message you are encoding. Real spam is so stupidly written it's sometimes hard to tell the machine written spam from the genuine article.

16

Spam Mimic is the most logical place to start. You can find it on the web at www.spammimic.com. It is a very simple web interface to encode a short message into what appears to be your everyday spam email.

spam
mimic

who's watching you surf?

First time here? ... Read the [explanation](#).
Hope you're using the [secure connection](#)

Encode○○○ - Turn a short message into spam
○○○**Decode** - Turn spam back into the original message

[home](#) | [encode](#) | [decode](#) | [explanation](#) | [credits](#) | [faq & feedback](#) | [terms](#) | [Français](#)
Copyright © 2000-2005 spammimic.com, All rights reserved

17

It's really simple to use. This is the entry page. To encode a test message click encode.

spam mimic

Anonymizer.com totally private web surfing, searching and downloads. [click here](#)

Encode

Enter your short secret message:

- ◆ Encode with as password
- ◆ **NEW** Encode as fake PGP

[home](#) | [encode](#) | [decode](#) | [explanation](#) | [credits](#) | [faq & feedback](#) | [terms](#) | [Français](#)

Copyright © 2000-2005 spamimic.com, All rights reserved

18

Add your text message and click the encode button. Also note the option to encode with a password.



This is what the output looks like ... A way of using text itself is to use random words or phrases as a means of encoding the information. Different words can be given different values.

Spam Mimic Faking PGP



The image shows a web browser window displaying the 'Spam Mimic Faking PGP' interface. The page has a blue header with the 'mimic' logo on the left and 'Anonymizer.com' with the tagline 'protection for your online privacy' on the right. Below the header, the main content area is blue and contains the following text: 'Encode', 'What better place to hide an encoded message but... inside an encoded message! This page will encode your message so it looks like its PGP-encrypted but its really just base64-encoded. Yes, its crazy and dangerous -- we know. Use at your own risk.' Below this text is a text input field with the placeholder 'Enter your secret message:' and the text 'Welcome NOITR 2005!'. A button labeled 'Encode' is positioned below the input field. Underneath the button are two radio button options: 'Encode as spam' and 'Encode as spam with a password'. At the bottom of the page, there is a navigation menu with links for 'home', 'encode', 'decode', 'explanation', 'credits', 'faq & feedback', 'terms', and 'Français'. A copyright notice 'Copyright © 2000-2005 spammimic.com, All rights reserved.' is visible at the very bottom. The page number '20' is displayed in the bottom right corner of the browser window.

Encode

What better place to hide an encoded message but... inside an encoded message!
This page will encode your message so it looks like its PGP-encrypted but its really just base64-encoded.
Yes, its crazy and dangerous -- we know. Use at your own risk.

Enter your secret message:

Welcome NOITR 2005!

Encode

- Encode as spam
- Encode as spam *with* a password

[home](#) | [encode](#) | [decode](#) | [explanation](#) | [credits](#) | [faq & feedback](#) | [terms](#) | [Français](#)

Copyright © 2000-2005 spammimic.com, All rights reserved.

20

If you selected the encode as fake PGP option – this is the encode interface. Same operation here- type a message and click encode.

Spam Mimic Fake PGP Output

-----BEGIN PGP MESSAGE-----

Charset: ISO-8859-1

Version: GnuPG v1.2.5 (MingW32)

Comment: Using GnuPG with Thunderbird -

<http://enigmail.mozdev.org>

V2VsY29tZSBOT0lUUiAyMDA1IQ==

-----END PGP MESSAGE-----

Remember what the fake pgp encode page said – base64 encoding. Use this at your own risk.

Steganography

- > Steganography - derived from the Greek words meaning "covered writing" - essentially involves hiding information or communications inside something so unremarkable that no one would suspect it's there. It's the cyber-equivalent of invisible ink or the "dead drops" that spies use to pass secrets.

Lets take a few moments to discuss steganography. Nothing fancy here either, we will stick to the widely available internet tools.

Hiding Information in the order of letters

- > Can the letters be scrambled without affecting readability?
- > One blog writes, "Aoccdrnig to a rscheearch at an Elingsh uinervtisy, it deosn't mtttaer in waht oredr the ltteers in a wrod are, the only iprmoetnt tihng is taht frist and lsat ltteer is at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae we do not raed ervey lteter by it slef but the wrod as a wlohe. "
- > "Can the order of these letters carry a message? Sure. In order to experiment with using this for steganography, I took the source code from my disco lists project and adapted it to handle words. The webpage explains how the order of items in any set can carry a message. Some have used it to order the colors in a palette of a picture, I used it to scramble a list of songs, but it can also work with the letters. All you have to do is set aside the first and last letters as well as any duplicates."
- > <http://www.wayner.org/texts/mimic/>

23

This is a bit that I am sure most of you have seen before. Those of you that haven't - try reading the second paragraph above and see how easy it really is to read.

Spam authors often use a similar text jumbling technique to defeat spam filters. The interesting part is that the middle letters can be arranged in such a way to encode a message. Remember – the authors intent where his intentions are covert is most likely to not draw attention from casual observers. The encoded portion may be only a small section of the email body, or subject.

Hiding Information using line shifting

- > Line Shift Coding Protocol
- > In line shift coding, we simply shift various lines inside the document up or down by a small fraction (such as $1/300$ th of an inch) according to the codebook. The shifted lines are undetectable by humans because it is only a small fraction but is detectable when the computer measures the distances between each of the lines.

24

Line shifting is fairly simple and self explanatory. The lines of a text message are shifted ever so slightly and by finding out whether a line has been shifted up or down we can represent a single bit, 0 or 1. If we put the whole document together, we can embed a number of bits and therefore have the ability to hide a large amount of information.

Hiding Information using word shifting

- > Word Shift Coding Protocol
- > The word shift coding protocol is based on the same principle as the line shift coding protocol. The main difference is instead of shifting lines up or down, we shift words left or right. This is also known as the justification of the document. The codebook will simply tell the encoder which of the words is to be shifted and whether it is a left or a right shift. Again, the decoding technique is measuring the spaces between each word and a left shift could represent a 0 bit and a right shift representing a 1 bit.
- > The quick brown fox jumps over the lazy dog.
- > The quick brown fox jumps over the lazy dog.

25

In this example the first line uses normal spacing while the second has had each word shifted left or right by 0.5 points in order to encode the sequence 01000001, that is 65, the ASCII character code for A. Without having the original for comparison it is likely that this may not be noticed and the shifting could be even smaller to make it less noticeable.

Hiding Information using white space

- > White Space Manipulation
- > One way of hiding data in text is to use white space. If done correctly, white space can be manipulated so that bits can be stored. This is done by adding a certain amount of white space to the end of lines. The amount of white space corresponds to a certain bit value.

26

Due to the fact that in practically all text editors, extra white space at the end of lines is skipped over, white space manipulation won't be noticed by the casual viewer. In a large piece of text, this can result in enough room to hide a few lines of text or some secret codes. A program which uses this technique is SNOW, which is freely available. I'll recommend some other freely available software for your experimentation at the end of this presentation.

Hiding Information in MP3s

- > MP3Stego
- > The MP3 format is probably the most widespread compression format currently used for music files. Due to this, it also happens to be very good for hiding information in. The more inconspicuous the format, the more easily the hidden data may be overlooked.

27

Another example of hiding information in files is MP3stego . The technique used here is similar to minute frequency transformations. Basically the data to be hidden is stored as the MP3 file is created, during the compression stage. To retrieve the data all you need to do is uncompress the MP3 file and read the parity bits. An interesting note is the presence of extremely large MP3s of odd choices of speeches and plays that you can find in alt.anonymous.messages .

Hiding Information in pictures

- > Every picture is made up of pixels and every pixel is represented with a number. In many cases, the number is really made up of 3 numbers representing the amount of red, green and blue in the pixel. These are usually 8 bit values between 0 and 255. A red pixel might have the value (255,0,0), a blue one might be (0,0,180), a purple one might be (240,0,250) and so on.

Another way to think of these values is as bits. Each pixel is represented with 24 bits with 8 bits allocated to the three colors. A red pixel may be (11111111,00000000,00000000), a blue one may be (00000000,00000000,10110100) and so on.

The least significant bit is the right most one in this binary notation. So $255 = 11111111$ and the least significant bit is a 1. If you change this bit, the value becomes $254 = 11111110$.

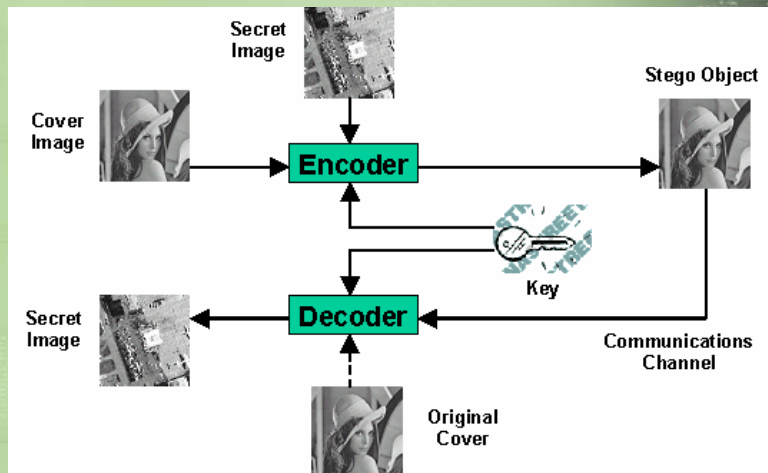
The least significant bits for all of the red, green and blue values in all of the pixels is the least significant bit plane. In most cases, replacing the least significant bit will change nothing. The difference between 254 and 255 or 140 and 141 is so small that your eyes won't even pick it up. In many cases, replacing two or three planes won't make a difference. The best place to see changes quickly is to look at the sky or similar smooth part of the image.

- > <http://www.wayner.org/texts/mimic/>

28

This is a little in depth background on the theory of the steganalysis of images. What this really boils down to is some bit twiddling of the pixel data. The type of image that is used is of paramount importance in this case. High resolution photos with stego applied are easier to spot with the naked eye than lower quality images. This is mainly due to the image degradation caused by the manipulation of the pixel data. However, without the original to compare file sizes to, this would be hard or impossible to detect without a detection utility.

Hiding Information in pictures



29

This is a very generic flowchart of the process of image steganography. As you can see the secret image is encoded with the cover image into a stego object – transmitted across the communications channel and decoded.

StegHide & StegDetect



1 in 10 sampled images in select (interesting) newsgroups had embedded content.

30

Steghide and stegdetect are part of the same application package. A google search for steghide should help you find it pretty quickly. I found that by looking for images in certain “interesting” network newsgroups that roughly 1 in 10 images had weak steganography applied. This particular image had the FTP address as well as username and password to download a pirated copy of Corel 5 embedded.

Recognizing the interesting

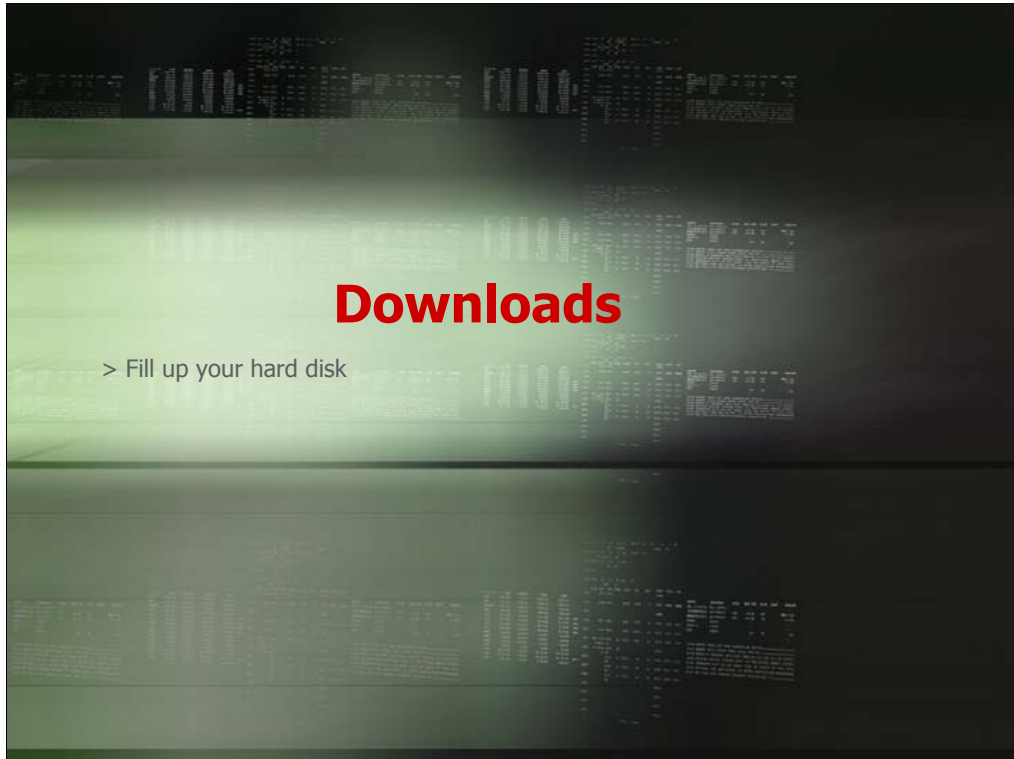
- > Research default spam filter rules
- > Remember that the author might want it to be filtered

What does all of this mean to me?

31

Spam filter rules could be a give away if the author intended to be filtered on purpose. Many websites for popular spam filter tools list the default filters on their sites.

Many times Enterprise organizations' security policies concentrate on inbound traffic only. The methods previously described present a unique risk of company secrets, intellectual property, or customer financial information to be encoded and sent out of the company network. Most IT professionals without specific knowledge in this area would be unable to recognize this as a threat. Some of the applications and techniques discussed should be considered for occasional audits of installed employee software to mitigate potential risk.



If you are interested in trying this out for yourselves and don't know where to start, I will recommend a few free programs for you. The internet newsgroups are a great place to start that will have you producing results nearly immediately.

Stego Downloads

- > WINDOWS
- > Camera/Shy v0.2.23.1 (Freeware) - Scans for and delivers decrypted content from the Internet.
- > Camouflage (Freeware) - Can hide information in any digital file type by inserting it after the end of file marker. Information hidden this way will not affect how the carrier looks or behaves, although it will increase file size. Includes password protection.
- > CryptArkan (Shareware) - Uses WAV and BMP carrier files; hidden data can be directly read off an audio CD. Includes encryption.
- > ImageHide (Freeware) - Uses a variety of image carrier files.
- > JPegX (Freeware) - Uses JPEG carrier files and includes encryption and password protection.
- > JP Hide and Seek (Freeware) - Uses JPEG carrier files and includes encryption.

33

I suggest starting in alt.2600 with stegdetect and alt.anonymous messages with mp3stego for starters. I also highly recommend the use of anti-virus and a generous helping of common sense in these groups. Don't download anything that even looks like it might be a script, executable or a zip file.

Stego Downloads 2

- > **WINDOWS – Continued**
- > **JSteg Shell v2.0 (Freeware) - Uses JPEG carrier files; includes encryption.**
- > **MP3Stego (Freeware) - Uses MP3 carrier files.**
- > **Sam's Big Play Maker (Freeware) - A text generation tool that converts a message into an output that looks like a play.**
- > **Steghide 0.4.6b (Freeware) - Uses BMP, WAV and AU carrier files. Includes encryption.**
- > **S-Tools 4 - (Freeware) - Uses BMP, GIF, and WAV carrier files; includes password and encryption options.**
- > **wbStego4.3open (Freeware) - Uses BMP, TXT, HTML/XML, and PDF carrier files for both Windows and Unix. Includes a Wizard interface, encryption, and passphrase support.**

More Windows tools

Stego Downloads 3

- > **UNIX/LINUX**
- > **Covert TCP (Freeware)** - Uses TCP packets as carrier files.
- > **Hydan (Freeware)** - Uses executables as carrier files.
- > **JP Hide and Seek (Freeware)** - Uses JPEG carrier files and includes encryption.
- > **JSteg (Freeware)** - Uses JPEG carrier files.
- > **MP3Stego (Freeware)** - Output is an MP3 carrier file.
- > **Nicetext (Freeware)** - Text generation tool that converts a message into an innocuous message.
- > **Outguess v0.2 (Freeware)** - Uses JPEG carrier files.
- > **Snow (Freeware)** - Uses text files as carriers.
- > **Stealth (Freeware)** - A utility that removes the header information from PGP messages, leaving only the encrypted data which may then be hidden.

Some of the more impressive UNIX tools.

Stego Downloads 4

- > **UNIX/LINUX - Continued**
- > **Steganosaurus (Freeware) - A text-based steganography tool.**
- > **StegFS (Freeware) - Uses Linux file system for hiding information.**
- > **Steghide 0.3, Release 1 (Freeware) - Uses BMP, WAV and AU carrier files. Includes encryption.**
- > **StegParty (Freeware) - Hides information by making changes in text.**
- > **Stegtunnel (Freeware) - Uses TCP packets as carrier files.**
- > **Textto (Freeware) - Text generation tool that converts a message into an innocuous message.**
- > **Visual Cryptography (Freeware) - Hides information in two image files that must be layered to reveal.**
- > **wbStego4open (Freeware) - Uses BMP/TXT/HTML/PDF carrier files**

References

"**Nobody's Anonymous**" - Dr. Curtis Kret - Black Hat Briefings 2004 - <http://blackhat.com/presentation/bh-usa-04/bh-us-04-kret.pdf>

ORDB.ORG – the open mail relay database – <http://www.ordb.org>

Dictionary of Science and Culture - <http://www.explore-society.com/society/C/Cut-out.html>

"**US intelligence links 419s to terrorist attacks**" - Computer Security Online - <http://www.compseconline.com/> (login required)

"**Out of office' emails used to tip off burglars**" - Computer Active Magazine 2004 - <http://www.computeractive.co.uk/news/1137339>

"**Spam is Winning the War on Terrorism**" - Deadbrain - http://www.deadbrain.com/news/article_2003_09_20_4615.php

Steganography And Digital Watermarking - Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, School of Computer Science, The University of Birmingham. - <http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS5/Steganography.doc>

Spam Mimic - <http://www.spammimic.com>

Thank-You!

John Retterer – jretterer@icinetworks.net