

Steganography Today's Risk to Your Organization

Steganography, which can be simply described as the hiding of data in plain site has been around since 400 years before the birth of Christ. With our ever increasing focus on security, data breaches and fraud very few companies have put a strategy in place to deal with this. We have firewalls, virus protection, spam filtering, we are moving towards the encryption of data on our laptops and desktops, we block through policy the writing of data to our USB thumb drives, yet as an industry we completely ignore the threats posed by steganography. As of Aug 15, 2007 there were 517 known Steganographic programs available. Many, like S-Tools are freely available on the internet and are easy to use. There are a few legitimate uses of steganography in the private and public sectors such as digital copywriting and the protection of intellectual property however, steganography is primarily used for illegal purposes by criminals.

Steganography can be traced back to 440 BC in ancient Greece. A message would be written on a wooden panel, then covered in wax and then a second message would be written on the wax. These tablets were commonly used for writing, so a message hidden in them would draw little suspicion. During times of armed conflict, runners would take these messages from the King or ruler of the day and communicate messages to the troops. The "false" message was the message on top, with the "real" message being hidden underneath the first layer of wax. During World War II it would be common to communicate secret messages using a newspaper publication. If one were to take the second letter of every word in every paragraph of an article, the letters would have meaning to the reader. To someone simply reading the article, they would be none the wiser that there was a hidden message contained in the article. Unfortunately these types of schemes are fairly easy to detect if one knows how to look for them.

These and other methods of hiding communications were still nothing compared to the types of applications developed with the invention of the Computer. Digital technology has made it all so much easier to hide messages and made it a lot harder to discover that message. For example we know that Steganography has been used for terrorist communication in today's times. Here is how it works. You want to communicate a message to a group of people. You communicate to them that on Saturday, between 12:00 and 12:30 they should download the picture of the bicycle that you will have posted on eBay. Inside that picture will be the hidden message that they will extract. Now, prior to 12:00 the picture will not contain any hidden messages. At exactly noon, the communicator will upload a "special" picture that looks absolutely identical to the previous one, yet has a hidden message inside. At 12:30 the "special" picture will be replaced with the original. In this scenario, there is very little risk of detection.

The key advantage of steganography over encryption schemes is that the messages do not attract attention to themselves. An encrypted message, no matter how secure, will arouse suspicion and may in and of itself be incriminating. Encryption is even illegal in some

countries. Steganography on the other hand is a technique that does not draw attention to itself and can easily stay under the radar.

Steganography can be used in a large amount of data formats in the digital world of today. The most popular data formats used are .bmp, .doc, .gif, .jpeg, .mp3, .txt and .wav. These formats are also popular because of the relative ease by data can be hidden inside of them. Let me explore the different types of techniques that are available. The first and least efficient is that of hiding a secret message inside of a text based message. One of the methods is called line shift encoding which involves shifting each line of text vertically up or down. Depending on the distance from the stationary line would depend on the value you would assign in your secret message. As you can see, this is not a very efficient system. A word shift system works the same way except horizontally by counting the spaces in between words to equate to values. This system is also not very effective. The last of the text based systems is to change certain text attributes of the letters, the size, font, style, etc in order to assign values and ultimately create a message. None of these systems is very effective.

The most popular and most effective method of coding secret messages is in digital images. Almost any type data, text or image can be hidden inside of digital images. There are images made up of 8 bit and 24 bit pixel image files. The advantage of the 8 bit system is that is it smaller (usually used in .GIF) files and 24 bit image files which are much larger and much better suited to steganography. The disadvantage of course is that they are larger and sometimes caught by email servers that either prevent or reject messages that are over a certain size. Least significant bit (LSB) encoding is by far the most popular of the coding techniques used for digital images. By using the LSB of each byte (8 bits) in an image for a secret message, you can store 3 bits of data in each pixel for 24-bit images and 1 bit in each pixel for 8-bit images. As you can see, much more information can be stored in a 24-bit image file.

But what does this all mean for the corporate security world today. We have been entirely focused on what causes us the most pain. We have been solely focused on the protection of our environment that we have up until now given little thought to information leaving our premises. Let me explain, starting at the firewall. A firewall protects us from intruders entering into our environment. It limits the type of traffic (inbound or outbound) and does content filtering. It can also be setup to block malicious file types from entering into our network, like .EXE, .BAT, .COM and so forth. Then we move on to our spam filter. Those annoying spam messages which now comprise 60-70 percent of all email coming into our organization. We make sure that we buy the best products to eliminate anywhere from 95-99 percent of all of that junk. Then we have virus protection on our servers and desktops making sure that no virus's or worms disturb or interfere with our normal operating environment. We don't want to have a repeat of SQL Slammer or Nachi. The next item on our list is to encrypt laptops so that in the event that one of them gets lost we don't risk sensitive data being exposed to the public.

But are we missing the point? Most fraud and crime today is committed by those inside the organization. We all send out documents as part of our normal day to day activities. Some organizations go as far as to say that you cannot send out a Word document, only a PDF so as to prevent any liability to the organization for any potential metadata hiding from normal sight in that document. It could be more than a little embarrassing to see all of the comments that were made to a document as it circulated around an office prior to giving it to the client, especially when those comments show inflated pricing or comments that we wish they never saw.

Think of the risks that steganography poses to your organization. I can easily take a document, hide it inside a picture using freely available steganographic tools and send out company confidential information to my competitors. I have worked on a lot of cases where an individual submits their resignation to Company "A" and the next week ends up working for Company "B" which is a direct competitor of their former company or starts up their own business in direct competition to their former employer. When I come in and analyze the computer activity of the now departed employee I will inevitably find all of the company's sensitive information such as price lists, customer lists, supplier lists, and all other forms of intellectual property in a deleted form on the computer. A further search will find that this information has either been copied to a CD a USB thumb drive or has been sent out via email. Imagine working covertly for the competition by being employed by your current employer and sending out the latest strategy documents, business plans or new product offerings.

Outside of the corporate environment steganography is also being used by the criminal element. Child pornography is now starting to be distributed inside of other pictures, contact lists for grow operations are being hidden and stored and covert communications between criminals are becoming more prevalent. A few of the more popular steganographic tools are

- a) S-Tools v4 - Hides secret files in .BMP, .GIF or .WAV files.
- b) MP3 Stego - Embeds hidden data into .MP3 audio files.
- c) Steganos 3 - Security Suite that uses strong encryption and stego techniques to hide data in audio and/or digital images

It is my belief and recommendation that organizations should institute a policy of scanning for steganography on both inbound and outbound traffic. There will be a price to pay in the time it takes to scan for hidden messages, but I believe the time has come for us a community to move this up on the priority list. The leader in Steganographic detection today is Wetstone Technologies (www.wetstonetech.com) who offer detection algorithms that can be integrated into Application Firewalls, Intrusion Detection solutions and content filtering products. The detection algorithms are provided as DLL's along with an API so as to integrate the solution with a customers existing infrastructure.

