Cyber Steganography

Cyber "Insecurity" That's Not Publicized Much

© 2014 W.P.Lidinsky

Introduction

Although little publicized, cyber steganography is a growing threat

It is being used by terrorist organizations, spies, drug cartels and others

Some known uses include

- *Communication in order to organize attacks or schedule drug deliveries*
- *Stealing of proprietary intellectual property*
- *Provide manuals on making and delivering bombs*
- *Keep parts of an organization separate*

© 2014 W.P.Lidinsky

Introduction

The detection of cyber steganography is difficult and sometimes not possible in a timely way

Detection is called ***steganalysis*** or more precisely cyber steganalysis

© 2014 W.P.Lidinsky

Al-Qaeda & Porn

Berlin, May 2011

Suspected al-Qaeda member arrested

Had in his possession a flash memory with a password-protected folder

Password was cracked by authorities

Within the folder was a porn video that could be viewed without difficulty

OK. So the guy liked to watch porn.

But why was it password-protected?

And wasn't watching porn strictly against his religion?

© 2014 W.P.Lidinsky

Al-Qaeda & Porn

So the authorities investigated further

Applying steganalysis to the video they found, hidden within the video, 141 text files

These text files included

A list of al-Qaeda's current operations

Reports on the status of these operations

Plans for future operations

Mistakes made in past operations

So how did a terrorist hide all this in a seemingly "innocent" video file?

And how did the authorities detect and extract the hidden info?

© 2014 W.P.Lidinsky

Operation Shady RAT

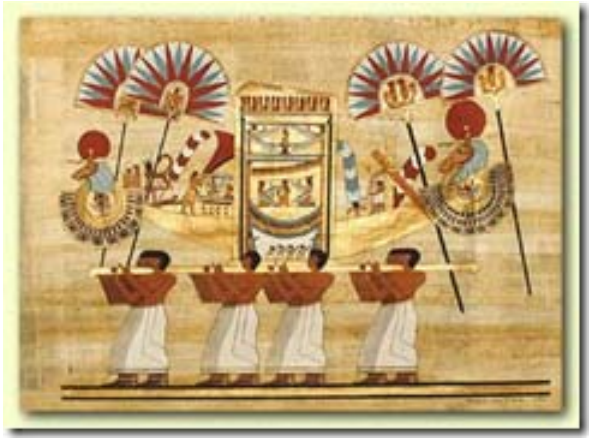
This attack had been going on unnoticed for 5 years

McAfee finally discovered it in mid 2011

Stole intellectual property from over 70 corporations, government agencies and NGOs in 14 countries

Seemingly innocuous-looking image files were used to carry commands to previously infected computers

Examples of some of the image files that were used:



© 2014 W.P.Lidinsky

Russian Moles

June 2010

FBI arrested 11 Russian “moles” who had been living in the U.S. for years as U.S. citizens

These moles used a Russian-devised stego tool to conceal their electronic communication with the Russian SVR (Russian foreign intelligence agency)

Communication was done using image files

Covert information was hidden in carrier image file by sender

Carrier image file was posted to public web sites by sender

Later the carrier image file was copied by the receiver

Covert information was then extracted by the receiver

Classical spyware “drop box” scheme adapted to the cyber world

© 2014 W.P.Lidinsky

How?

How can one hide potentially harmful information in a seemingly innocent carrier file so that the carrier file can be rendered (e.g., viewed, played) as though it carried nothing.

Even more, how can one

Examine a file to determine if it carries hidden information

Extract and understand the hidden information

Or at least remove it

The Steganography course in Spring 2015 will focus on these issues

© 2014 W.P.Lidinsky

Modern Cyber Steganography

Modern Cyber Steganography

Today digital information can be hidden many different ways

Two factors common to many modern cyber-stego schemes

*A **carrier** or **overt** file*

Seemingly “clean”. Innocent.

*A **covert** file to be **hidden***

Plans to destroy a building

Information about a new stealth aircraft

The name and picture of a CIA undercover agent

Anything!

© 2014 W.P.Lidinsky

Overt or Carrier Files

Carrier files can be of many different types

- *Document files (e.g., text, spreadsheet, word processor)*
- *Image files (e.g., jpeg, bmp, gif, tiff)*
- *Video files (e.g., avi, flv, H120, H261 through H265, mpeg1, mpeg4)*
- *Audio files (e.g., mp3, wav, G711, G729)*
- *Web page files*

Most of the above are in the public domain

There are many more that are proprietary

- *e.g., realAudio, realVideo…*

© 2014 W.P.Lidinsky

Hidden or Covert Files

The file(s) to be hidden can usually be anything

So the nature of the file actually is irrelevant

- *Don't care if the file is text, doc, xls, bmp, avi, mp3…*
- *Don't care if the file is compressed, encrypted or both*
- *Don't care what encryption or compression algorithm is used*
- *Almost any covert file can be hidden in another overt or innocent file, which becomes the carrier*

© 2014 W.P.Lidinsky

Stego Result

Using normal means the viewer or listener cannot detect whether the file is or is not carrying hidden information.

But, by effective analysis, can an apparently “clean” file be shown to be a carrier?

© 2014 W.P.Lidinsky

An Interesting “Rumor”

eBay contains many images on its web pages

You can post an image of something that you want to sell

There was a study of whether eBay images were carriers

Claimed that over 30% of the downloaded images were carriers containing hidden information

Some stego experts re-evaluated eBay images and found nothing

But others were able to show that there was hidden information but were not able to extract it.

So if the hiding is really good, it's hard (maybe impossible) to tell

© 2014 W.P.Lidinsky

Legitimate Uses of Stego

Hiding trademarks and copyrights in image files

Hiding copyrights in digital music files

Called ***digital watermarking***

© 2014 W.P.Lidinsky

Some Stego Examples

A Very Simple Text Example

Send the binary number 57 hidden in a carrier text file.

The carrier with 57 hidden in it is:

Hi Yalinne. I saw the your project proposal. It was great. But I suggest, because your proposal was short, that you provide some more detail.

Steganalysis of this example is easy

© 2014 W.P.Lidinsky

Picture Hidden in a Picture

File showing a Galapagos tortoise

Pinta island subspecies

"Lonesome George"

There is a picture of a naturalist named Patricia in this image

© 2014 W.P.Lidinsky

PowerPoint Hidden in Audio Carrier File

A wav sound file is the carrier (overt file)

Windows XP Shutdown.wav

An entire PowerPoint lecture is hidden in it

The entire introduction lecture from ITMS-538 a year ago

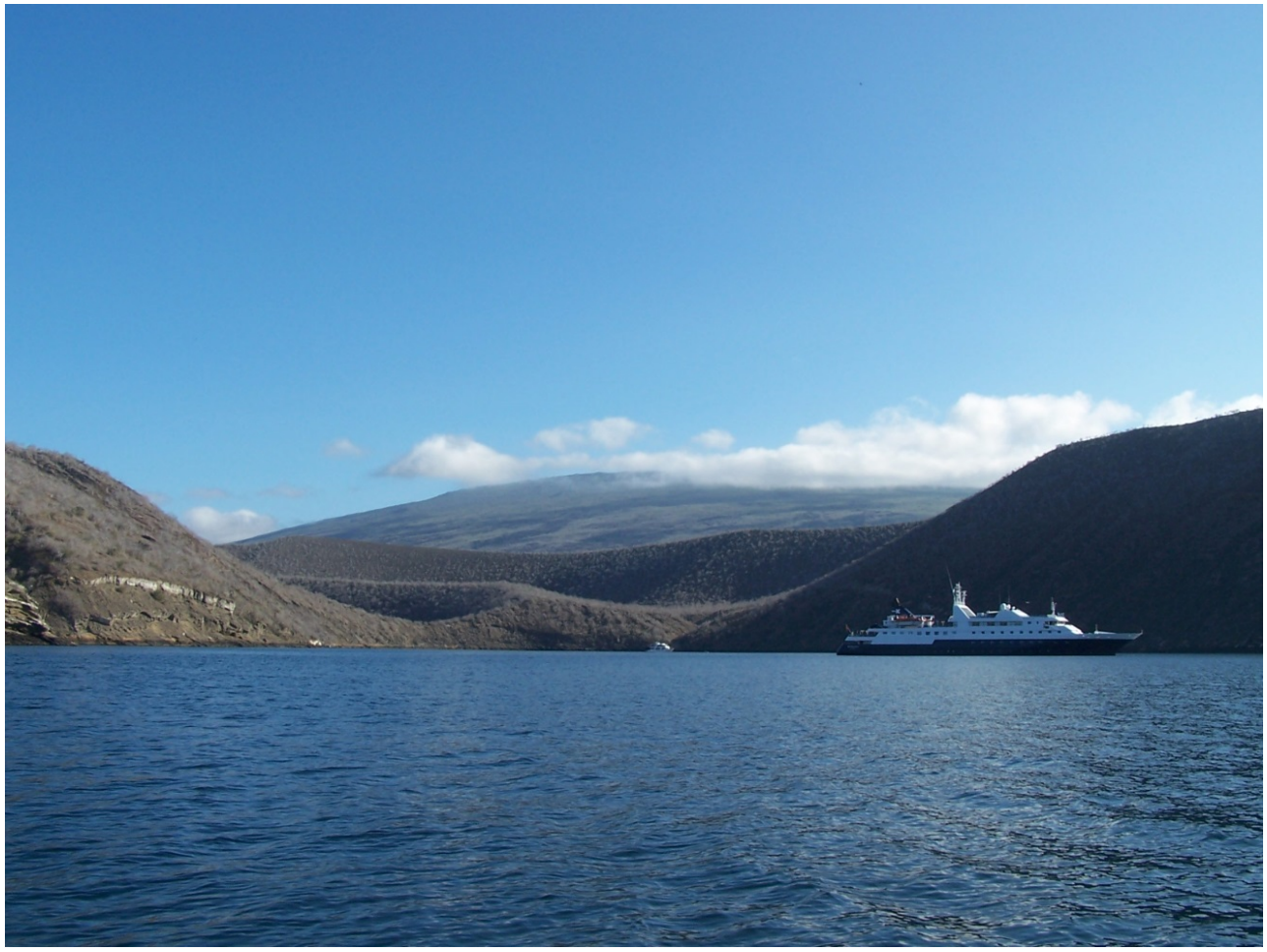
Now a demonstration

1st: Windows XP Shutdown-clean.wav

2nd: Windows XP Shutdown-compPPThidden.wav

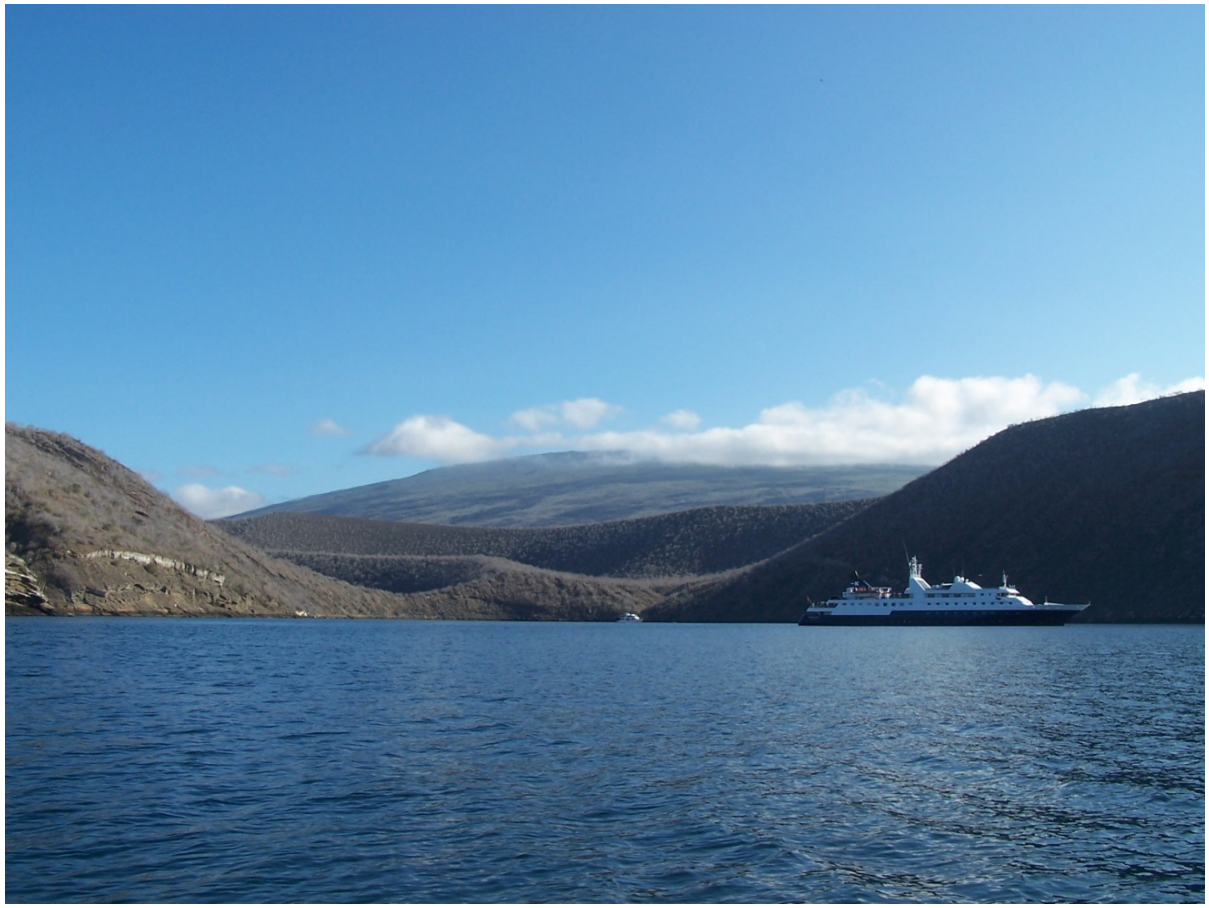
© 2014 W.P.Lidinsky

"Clean" JPG File
Tagus Cove in Galapagos Islands



© 2014 W.P.Lidinsky

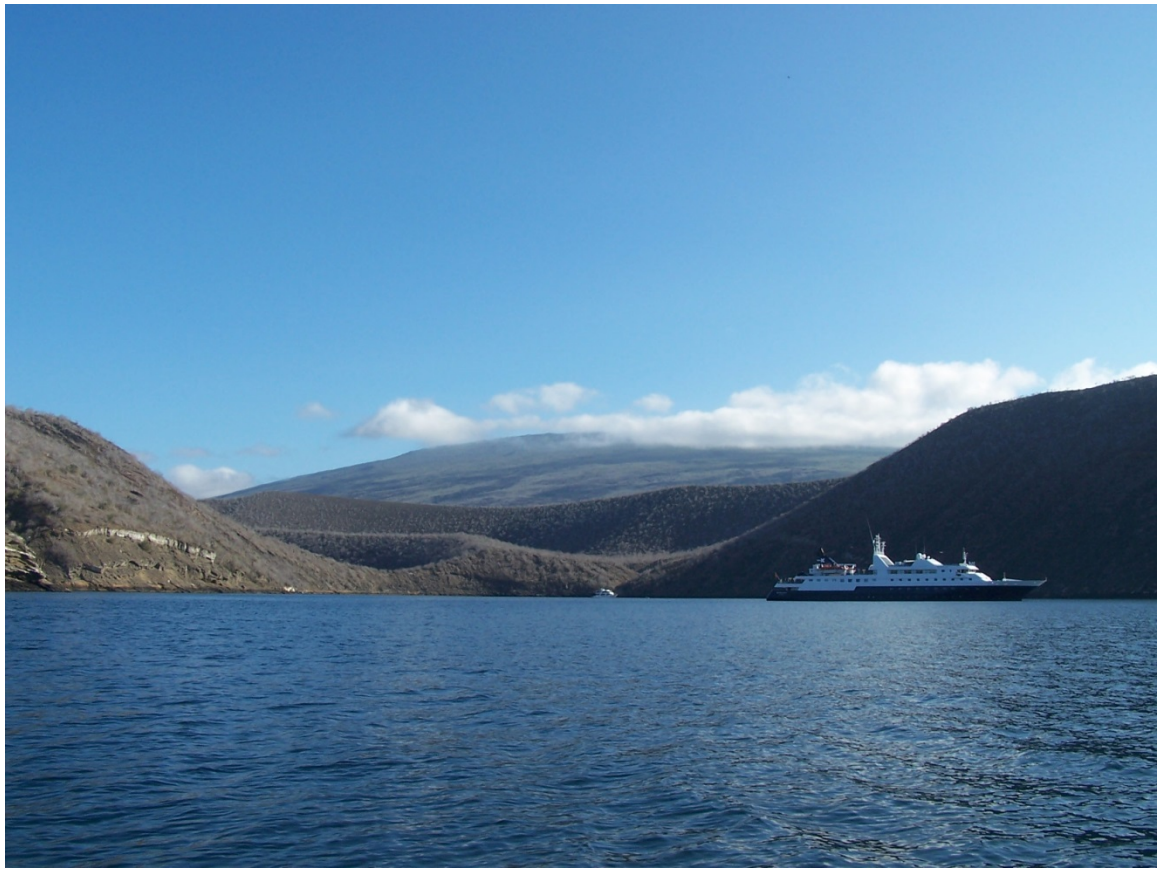
A JPG File with .doc Hidden Info



Tagus Cove JPG Carrier With a MSWord doc Hidden

© 2014 W.P.Lidinsky

A JPG File with .bmp Hidden Info

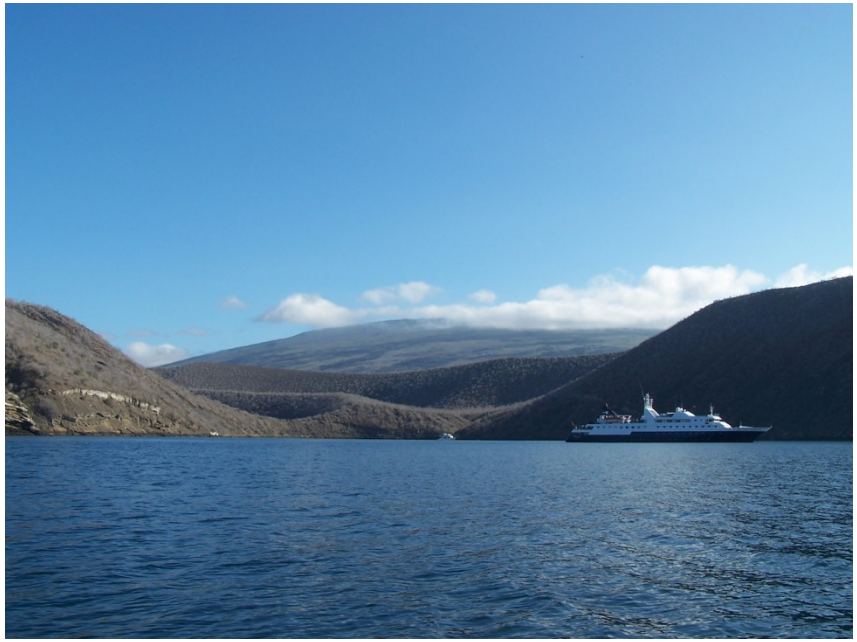


Tagus Cove JPG (608KB) Carrier With bmp Image (11.7MB) Hidden: 12.3MB

© 2014 W.P.Lidinsky

Comparison of “Clean” Carrier and Carrier with Hidden .doc File

Tagus Cove JPG
With Nothing Hidden



Tagus Cove JPG Carrier
With MSWord Hidden

© 2014 W.P.Lidinsky

Stego Demo: Stegazaurus

© 2014 W.P.Lidinsky

Stegazaurus History

Several years ago when I was lecturing at the FBI's Regional Crime Forensic Lab (RCFL) in Chicago

Some members from FBI in Milwaukee mentioned that there was a concern regarding covert info being hidden in mp3 files

One of the saving issues that made it less of a concern is that there were very few mp3 stego tools available

© 2014 W.P.Lidinsky

Stegazaurus History

I tried to get students to look into this FBI concern as a forensic project

A few years ago I got a taker -- sort of

> *In my ITM 548 class, one of my students, Mike Zaturenskiy, decided to investigate the possibilities of inserting covert info into mp3 files*
>
> A good study of how and where to insert stuff
>
> The best tool yet

MP3 Stegazaurus

© 2014 W.P.Lidinsky

Stegazaurus Demo

I will now demonstrate the Stegazaurus tool

Play the clean file & view the image to be hidden

Insertion:

I will hide a covert image file

PeteSeeger&banjo-smallest.jpg

in the carrier file

BigRockCandyMountain-clean.mp3

Play the “dirty” file

Extraction:

I will then extract it

View the extracted file

© 2014 W.P.Lidinsky

But It's Not Steganalysis

Mike did really outstanding work

But it's not steganalysis

Two years ago I got a team to work on a steganalysis tool for Stegazaurus as their ITM448/449 project

Result: **MP3 Steg Detector**

© 2014 W.P.Lidinsky

MP3 Steg Detector

MP3 Steg Detector extends the MP3 Stegazaurus work

It detects and extracts covert material from MP3 files

From the ID tags, frame headers and side information

Team members

Ben Khodja, Erfan Setork, Kbrom Tewoldu, Zach Wagner

© 2014 W.P.Lidinsky

Detection

Called "***steganalysis***"

Detection of overt (carrier) files with hidden (covert) information is often very difficult

Extraction of the covert info can be even more difficult

Detection is much easier if you can compare the suspect overt file to the original overt file that is known not to be a carrier

But usually you don't have a "clean" overt file

Fortunately there are sometimes ways of getting a clean file

© 2014 W.P.Lidinsky

Terminology

Steganography

The science/art of hiding covert information

Steganalysis

The detection of the existence of covert information

The extraction of the covert information

But sometimes "*steganography*" is used to refer to both

In general, steganalysis is an unsolved research problem

Except for some forms of carriers where steganalysis is possible

© 2014 W.P.Lidinsky

Wrap-Up

In the past I've usually included a stego lecture near the end of this course because *ITMS539 Steganography* didn't exist

But now it does exist

So I'm not sure if I will or not

But since there are stego projects that some of you we hope that you will choose to do, I'm giving you at least a sense of what can be done with steganography

And more importantly, at least hints at ways in which you can do steganalysis

© 2014 W.P.Lidinsky