

# Tracking Cyber Attackers II

Manu Malek

[mmalek@ieee.org](mailto:mmalek@ieee.org)

[www.cs.stevens.edu/~mmalek](http://www.cs.stevens.edu/~mmalek)

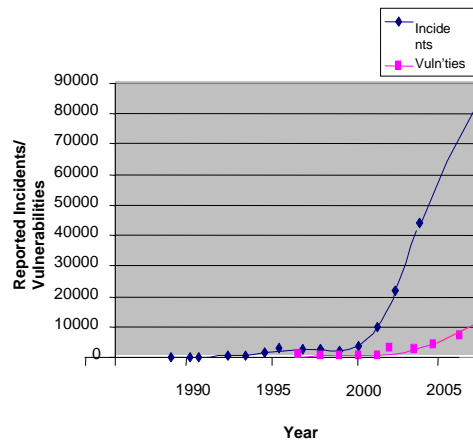
16 November 2009

## Outline

- ❖ Internet Security Trends
- ❖ Need to Track Cyber Attackers
- ❖ Methodology and Requirements
- ❖ Forensic Tools
- ❖ Hiding files
- ❖ Trojan Defense

## Internet Security Trends

- ❖ Rising rate of cyber attacks
- ❖ Increasing sophistication of attacks
- ❖ Increasing permeability of firewalls
- ❖ Increasing vulnerability of browsers



Adopted from [www.cert.org](http://www.cert.org)

## Need to Track Cyber Attackers

- ❖ National security
  - Potential for breaking into computer networks controlling sensitive processes
- ❖ Economic
  - Cyber attackers steal valuable information and intellectual property
- ❖ Legal
  - Corporations need to be prepared for possible litigation, e.g., for
    - Allegations of discrimination
    - Intellectual property claims
- ❖ Law enforcement
  - Agencies must be capable of tracking down law breakers

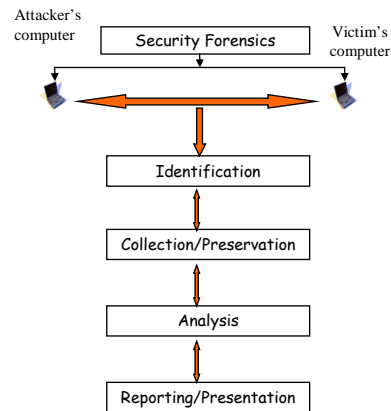
## Methodology for Tracking Cyber Attackers

❖ *Security (or IT) Forensic* techniques are used to track cyber attackers.

❖ *Security Forensics:*

The process of

- Identifying,
- Collecting and preserving,
- Analyzing, and
- Reporting and presenting digital evidence in a legally acceptable manner



## IT Requirements for Security Forensics

❖ The following capabilities are needed:

- Collecting relevant information from systems
- Being able to positively identify users who log on to systems
- Proving ownership and authenticity of evidence found on a system

## Forensic Data Collection in Client Computers

- ❖ Most operating systems provide significant logging capabilities.
  - Windows systems (2000/NT/XP) store log files in the directory `%systemroot%\system32\config\`
  - In UNIX, information about running processes is usually stored in `var/log/syslog`
  
- ❖ Protecting logs
  - Attackers could delete or modify logs
  - Logs should be protected

## Network-based Evidence

- ❖ Network monitoring can be performed to collect evidence:
  - **Event monitoring**: collecting network events, such as IDS alerts, network health monitoring alerts
  - **Trap-and-trace monitoring**: transaction data such as protocol flags
  - **Full-content monitoring**: collecting raw packets
  
- ❖ Network-based evidence can be found at endpoints and intermediate systems, such as
  - Authentication servers
  - Router logs
  - Firewall logs
  - Event logs from IDSs
  - Caller ID systems

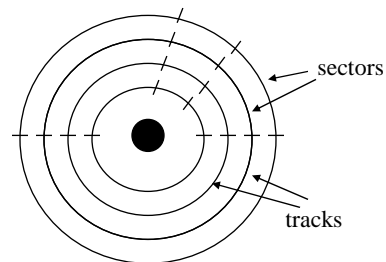
## Forensic Tools

- ❖ Many forensic tools and applications exist, e.g., for
  - Hard disk duplication
  - Text and file searching
  - Internet history analysis
  - Data hiding/revealing
  - Network forensics
  - Analysis of email files
- ❖ Some popular tools:
  - *EnCase* for drive forensics
  - *E-Trust* for industrial espionage cases
  - *Forensic Toolkit* (FTK)
  - *ProDiscover*
- ❖ Hardware and software-based key loggers can collect key strokes for specified periods of time.

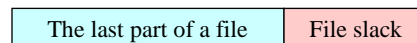
## Hidden Evidence

- ❖ Evidentiary data is not often readily observable.
- ❖ Evidence could be in
  - Deleted files
  - Encrypted files
  - Files in parts of the hard drive that are not readily exposed:
    - In System directory
    - ATA "Protected Area"
    - In file slacks
  - Files hidden in other files

A Disk Platter



Last sector of a cluster



## Hiding Files in other Files

- ❖ Files can be hidden in other files
- ❖ Steganography: storing hidden messages in such a way that no one other than the intended recipient knows of the existence of the message.

**Original Image**



+

**Hidden message**

```
101101011010101010  
100101000101101101  
101010100101011010  
101011110000101010  
100101110101101011  
010100101001000010  
011101010011110110  
111101110111010001
```

=

**Final image**



## Example: The LSB Algorithm

- ❖ In a digital black and white image, where each pixel is represented by 8 bits to represent its gray value, use the least significant bit (LSB) of each 8-bit word for the hidden message.
- ❖ The method can be extended to LSB plus additional bits.



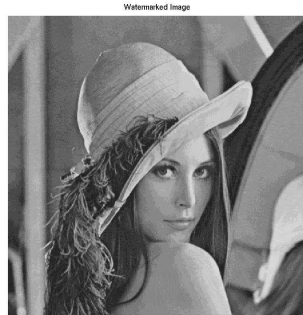
**Original**



**1 LSB**

## LSB Plus Additional Bits

4 LSBs



7 LSBs



## ***S-Tools***

- ❖ *S-Tools* is a freeware steganographic tool which can embed a message (audio file, image or text file) into an image of GIF or BMP format or audio in *wav* format.
- ❖ It is available from <http://www.spychecker.com>.

## What is Trojan Defense?

- ❖ The Trojan Defense:
  - The suspect claims "I didn't do it; someone else did."
  - The suspect claims that his/her computer was broken into and files (images, malware) planted in it; thus not responsible for what the computer did.
- ❖ The Trojan defense presents two problems:
  - The possibility of acquitting the guilty
  - The possibility of convicting the innocent.
- ❖ It presents the forensic investigators with a major challenge: to prove or disprove that the accused person is responsible for the evidence found on the computer.

## Trojans and Back-doors

- ❖ *Trojan* (or *Trojan horse*): a malicious program that is disguised as legitimate software
- ❖ The malicious program could, e.g.,
  - download tools that could be used for intrusion
  - upload sensitive data from the victim's computer
- ❖ Characteristics:
  - A Trojan can be attached to otherwise useful software, or it can be stand-alone.
  - The payload of a Trojan can be any type of malware, e.g., spyware, adware, back-door.
- ❖ *back-door*: a method of bypassing normal authentication which is hidden to casual inspection



## Trojan Making - Wrappers

- ❖ Many Trojans are created by Trojan-making kits, referred to as *wrappers*.
  - GUI-based or command-line driven *wrappers* are available, e.g., EliteWrap ([www.packetstormsecurity.org/trojans/](http://www.packetstormsecurity.org/trojans/))
- ❖ Trojan could be distributed to a mass audience, to targeted groups, or to individuals.
- ❖ Typical distribution mechanisms:
  - Attachment to e-mail
  - File sharing and removable media
  - Direct implant via hacking

## Trojan Making - Packers

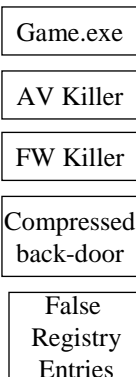
- ❖ The terms "packer" and "compressor" refer to utilities which compress a file, thus changing its binary structure.
  - Example: [www.programmerstools.org](http://www.programmerstools.org)
- ❖ Back-doors are usually detectable by Antivirus tools via their signatures.
- ❖ Even compressed back-doors would in most cases still be detectable.
- ❖ However, the attacker may use a compression algorithms not detectable by Antivirus tools.

## Antivirus and Personal Firewall Killers

- ❖ Malicious tools exist that shut down or disable the Antivirus (AV) application or the Personal Firewall (FW) software on the victim's computer.
  - Example: kiLLer ([www.illmob.org](http://www.illmob.org))
- ❖ A victim may inadvertently execute malware which deploys an AV/FW killer.
  - Then, forensic investigators often cannot see any events or logs alerting them to this incident.

## A Trojan Scenario

- ❖ The victim downloads a game from a P2P network.
- ❖ The game is a Trojan designed to deliver
  - An AV killer and a FW killer in the payload
  - A routine to implant false registry keys into the victim's system
  - A back-door to allow access to the victim's machine.
- ❖ The AV is first disabled so that when the back-door is decompressed, an AV response is not triggered.
- ❖ The FW Killer disables the personal FW software, allowing free traffic flow in and out of the victim's system.
- ❖ The back-door installs itself allowing the attacker remote access to the victim's machine.
- ❖ At the same time, the back-door notifies its "owner" of its presence via an outbound open port.
- ❖ The registry keys could
  - Ensure stealth start-up of rogue processes
  - Add falsified histories relating to Internet surfing activity



## Back-door/Trojans Forensics

- ❖ Back-door/Trojan kits have three components:
  - *Server*: the back-door itself, often wrapped up into the overall Trojan
  - *Client*: to control the back-door from a remote location
  - *Creator Tool*: to control the behavior of the back-door
- ❖ Existence of only the *server* part on a computer could be used as Trojan Defense.
- ❖ But the presence of *client* and/or *creator* should raise questions about the Trojan Defense.
- ❖ Corroborating evidence could be found in FW or proxy server logs.

## Conclusions

- ❖ Internet security attacks are on the rise
- ❖ Methods are needed to track cyber attackers
- ❖ Logs play an essential role in security forensics
- ❖ Effective tools are needed
- ❖ Experience counts!