Basic Computer Forensic Concept

Sang YOUNG CISSP CISA CHFI CEH CFSA

PISA

Disclaimer

- This material is NOT intended to be adopted in the course of attacking any computing system, nor does it encourage such act.
- PISA takes no liability to any act of the user or damage caused in making use of this report.
- The points made here are deliberately kept concise for the purpose of presentation. If you require technical details plea se refer to other technical references.

Basic Procedures

- Obtains the evidences
  - Storage Media
    - Make a forensic copy
  - Computer
- Prepare Computer Forensics Tools
  - Workstation
- Data Extraction
- Data Analysis

PROFESSIONAL INFORMATION SECURITY ASSOCIATION

Making Forensic Copy

- Using White Blocker
  - Software : Only work with DOS
  - Hardware : Work with all operating system
- Example: Using Ghost

ghost -afile=a:\err.log ***-fro -id*** *-z9 -ws- -autoname split=600*

An Organization for Local Information Security

Authenticating the Forensic Copy

- Using Cryptographic Checksum
  - SHA-1
  - MD5
- CRC32 is used in some tool

Notes:
NIST is sponsoring a project call Computer Forensics Tool Test (CFTT) to evaluate disk drive imaging tools.
http://www.cftt.nist.gov

PROFESSIONAL INFORMATION SECURITY ASSOCIATION

Looking for Potential Evidences

- Getting all files
- Eliminate well-known files
  - Operating System Files
  - Files from software package
    - RDS from NSRL (http://www.nsrl.nist.gov)
    - HashKeeper from National Drug Intelligence Center
    - Open Source (http://ftimes.sourceforge.net/FTimes/HashDig.shtml)
    - Hash Set from EnCase
    - KFF from FTK
- Examining the content of rest file
  - Keyword search

An Organization for Local Information Security

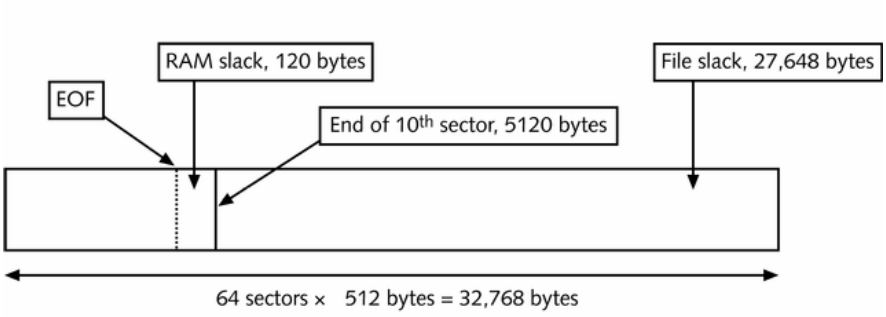
Data Hiding Method

- Hide it using operating system function
  - File system that support hiding file
  - ADS
- Rename the file extension
- Stored in Slack Area
- Deleted file
- Unallocated sector
- Deleted Partition
- Partition Gap
- Marked as bad sector/bad block
- Bit-Shifting
- Steganography

PROFESSIONAL INFORMATION SECURITY ASSOCIATION

Disk Slack Area

Drive size	Number of sectors	FAT16	FAT32
256-511 MB	16	8 KB	4 KB
512 MB-1 GB	32	16 KB	4 KB
1-2 GB	64	32 KB	4 KB
2-8 GB	8	N/A	4 KB
8-16 GB	16	N/A	8 KB
16-32 GB	32	N/A	16 KB
More than 32 GB	64	N/A	32 KB



An Organization for Local Information Security

Steganographic Components

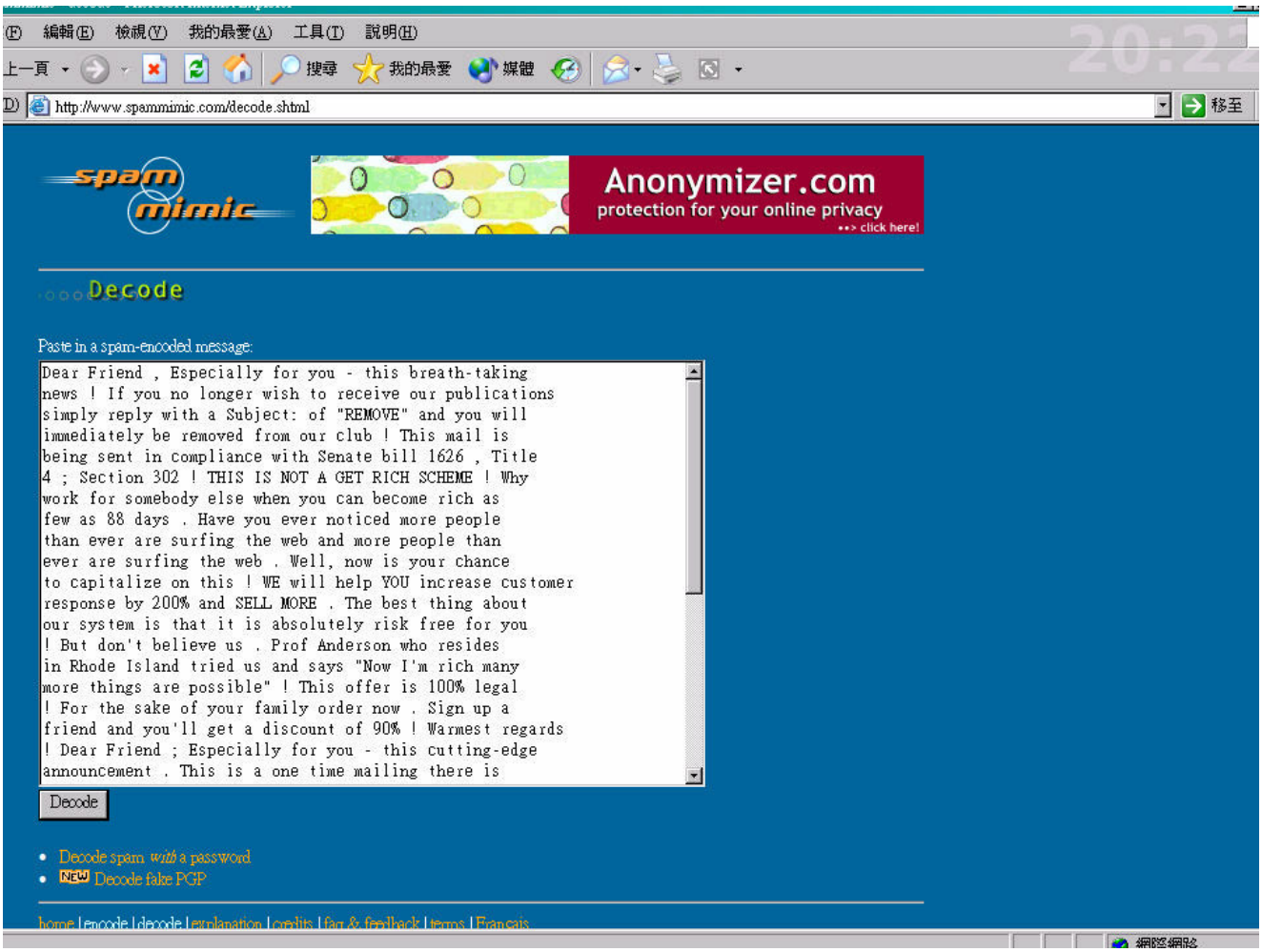
- Cover Objects
- Message
- Key
- Stego Tool

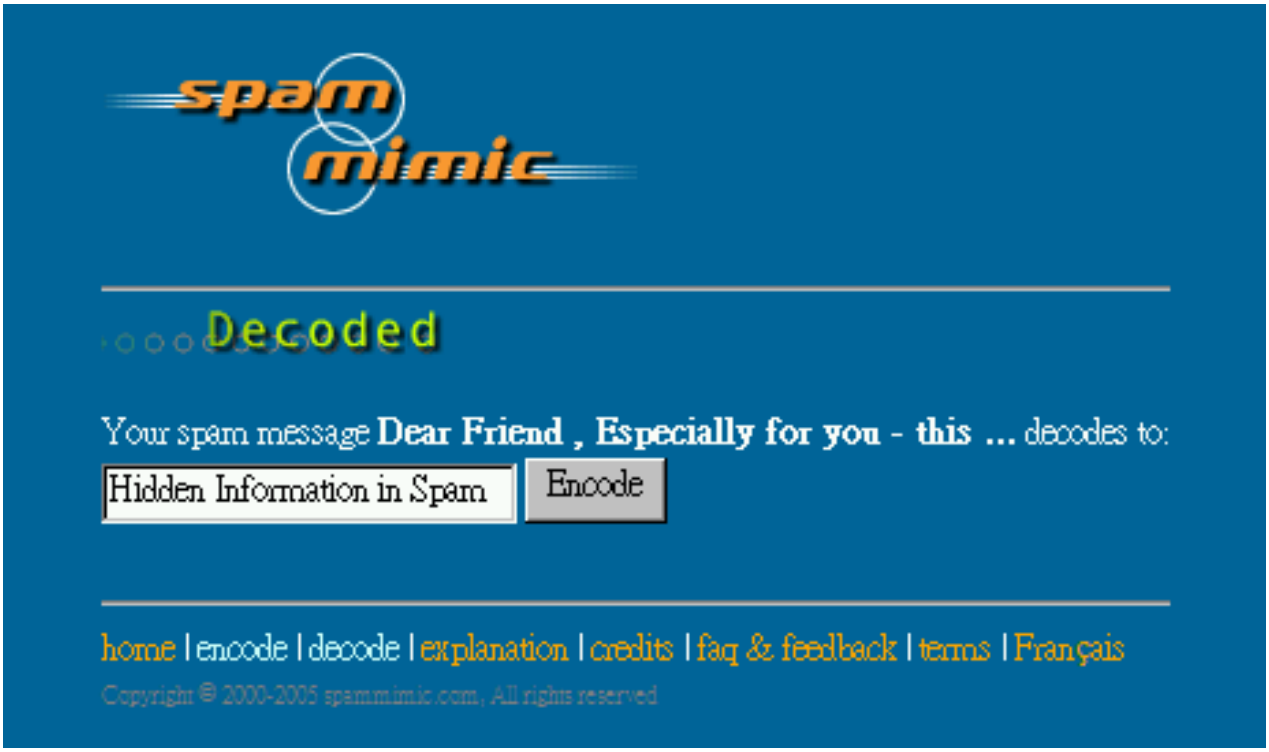
PROFESSIONAL INFORMATION SECURITY ASSOCIATION

Steganography

- Image
- MP3
- Movie
- Text File
- Excel ←→ Word
- Hidden in an email

An Organization for Local Information Security


(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛 媒體
http://www.spammimic.com/decode.shtml
移至
spam mimic
Anonymizer.com
protection for your online privacy
•••> click here!
Decode
Paste in a spam-encoded message:
Dear Friend , Especially for you - this breath-taking
news ! If you no longer wish to receive our publications
simply reply with a Subject: of "REMOVE" and you will
immediately be removed from our club ! This mail is
being sent in compliance with Senate bill 1626 , Title
4 ; Section 302 ! THIS IS NOT A GET RICH SCHEME ! Why
work for somebody else when you can become rich as
few as 88 days . Have you ever noticed more people
than ever are surfing the web and more people than
ever are surfing the web . Well, now is your chance
to capitalize on this ! WE will help YOU increase customer
response by 200% and SELL MORE . The best thing about
our system is that it is absolutely risk free for you
! But don't believe us . Prof Anderson who resides
in Rhode Island tried us and says "Now I'm rich many
more things are possible" ! This offer is 100% legal
! For the sake of your family order now . Sign up a
friend and you'll get a discount of 90% ! Warmest regards
! Dear Friend ; Especially for you - this cutting-edge
announcement . This is a one time mailing there is
Decode
Decode spam with a password
NEW Decode fake PGP
home | encode | decode | explanation | credits | faq & feedback | terms | Français


spam mimic
Decoded
Your spam message Dear Friend , Especially for you - this ... decodes to:
Hidden Information in Spam
Encode
home | encode | decode | explanation | credits | faq & feedback | terms | Français
Copyright © 2000-2005 spammimic.com, All rights reserved

Reveal Password Protected Evidence

- Looking for backdoor
  - Quickens
    - Zero out offset 445-447
  - Microsoft Money:
    - Offset 444 = length of password
    - Offset 445+, the encrypted password
    - Encrypted password : XOR of strings “Microsoft Barney”
- Systematic Password Cracking
  - Dictionary Attack
  - Specialist Word-list Attack
  - Potential Word-list Attack
  - Brute force attack

PROFESSIONAL INFORMATION SECURITY ASSOCIATION

Brute Force Password Cracking

- Problem: Slow
  - Charset [a-z,0-9], Length=8 → 321 days
  - Based on Pentium 1.5 machine
- Solutions:
  - Increase the processing power
  - Increase number of machines : parallel cracking

An Organization for Local Information Security

Internet Related Evidences

- Email
- Visited URL

PROFESSIONAL INFORMATION SECURITY ASSOCIATION

Response Toolkit

- Collect all utilities
- Burn it to the CDROM or put it in the floppy disk
- Built-in tools
  - cmd.exe, netstat.exe, nbtstat, arp, ipconfig
- Resource Kit
  - rasusers.exe, kill, rmtshare, auditpol
- From 3rd parties
  - Foundstone :, fport
  - Sysinternals : psloggedon, PsList, ListDLLs
  - Others : netcat (nc.exe), md5sum
- Create a script (batch) file to run the above command

An Organization for Local Information Security

Sample Script (Batch) file

collect.bat

```
date /t
time /t
psloggedon
dir /ta /od /s /a c:\
dir /tw /od /s /a c:\
dir /tc /od /s /a c:\
netstat -an
fport
pslist
nbtstat -c
doskey / history
date /t
time /t
```

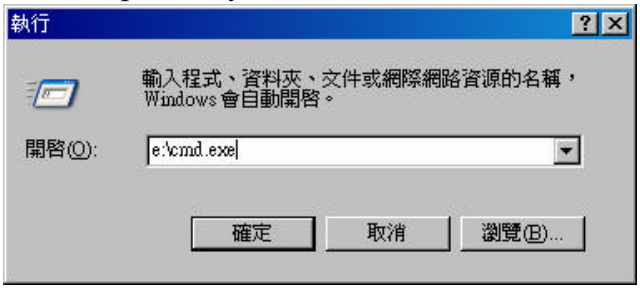

PROFESSIONAL INFORMATION SECURITY ASSOCIATION

Procedures to collect information

- Prepare your forensic workstation

  ```
  nc -l -p 10000 > result.txt
  ```

- Insert your toolkit into CDROM of the suspected system
- In the suspected system, start > run …



- Never run any command on the suspected system

An Organization for Local Information Security

Procedures to collect information

- In the Command Prompt enter the command:
  `collect | nc <your forensic workstation ip> 10000`
- Collect and analysis your information from your forensic workstation

PROFESSIONAL INFORMATION SECURITY ASSOCIATION

Linux Based Forensic Distribution

!!! Warning !!!
Don't mount EXT3 or reiserfs partitions. EVEN READ-ONLY.

- Penguin Sleuth Kit
  http://www.linux-forensics.com/
- F.I.R.E
  http://fire.dmzs.com/
- Helix
  http://www.e-fense.com/helix/
- INSERT
  http://www.inside-security.de/insert_en.html

An Organization for Local Information Security

Bootable Windows System CD

- Microsoft WinPE (Windows Preinstallation Environment)
  - Stripped down version of Windows XP
  - Can customize to add computer forensic tools
  - URL: http://www.microsoft.com/licensing/programs/sa/support/winpe.mspx
- BartPE
  - PE Builder : a utility to create bootable windows CD
  - Some forensic tool vendors create plug-in for it
  - URL: http://www.nu2.nu/pebuilder/

PROFESSIONAL INFORMATION SECURITY ASSOCIATION

The End

101 101101 1011 An Organization for Local Information Security