

Incident Response & Forensics:

Anti-Forensics



Why investigations are becoming more difficult

GLOBAL CAPABILITY.
PERSONAL ACCOUNTABILITY.

Tom Van de Wiele – Senior Security Consultant



Contents

- Introduction
- The categories of anti-forensics:
 - Data Destruction
 - Data Hiding
 - Data Encryption
 - Data Contraception
 - Denial of Service
- Q&A

Introduction – Attacker Perspective

- Obstruct an investigation
- Buy time
- Investigations are limited in time
 - Example: in the UK 2 to 3 x 8h maximum - depends on the case
- If the recovery takes longer: attacker wins!
- Hide origin of crime or mischief
 - “If you can find it, you haven’t hidden it well enough”
- Corrupt work data of forensic analyst
- Directly attack the forensic analyst

Introduction – Investigator Perspective

- Test of performance & accuracy of forensic tools
- Are you going to comb through a 320GB hard drive manually?
 - Forensic tools are your eyes and ears!
- Exploitation of bad assumptions in forensic software
- Comparison on performance & accuracy of forensic tools performing the same operations
- Not enough research is being done

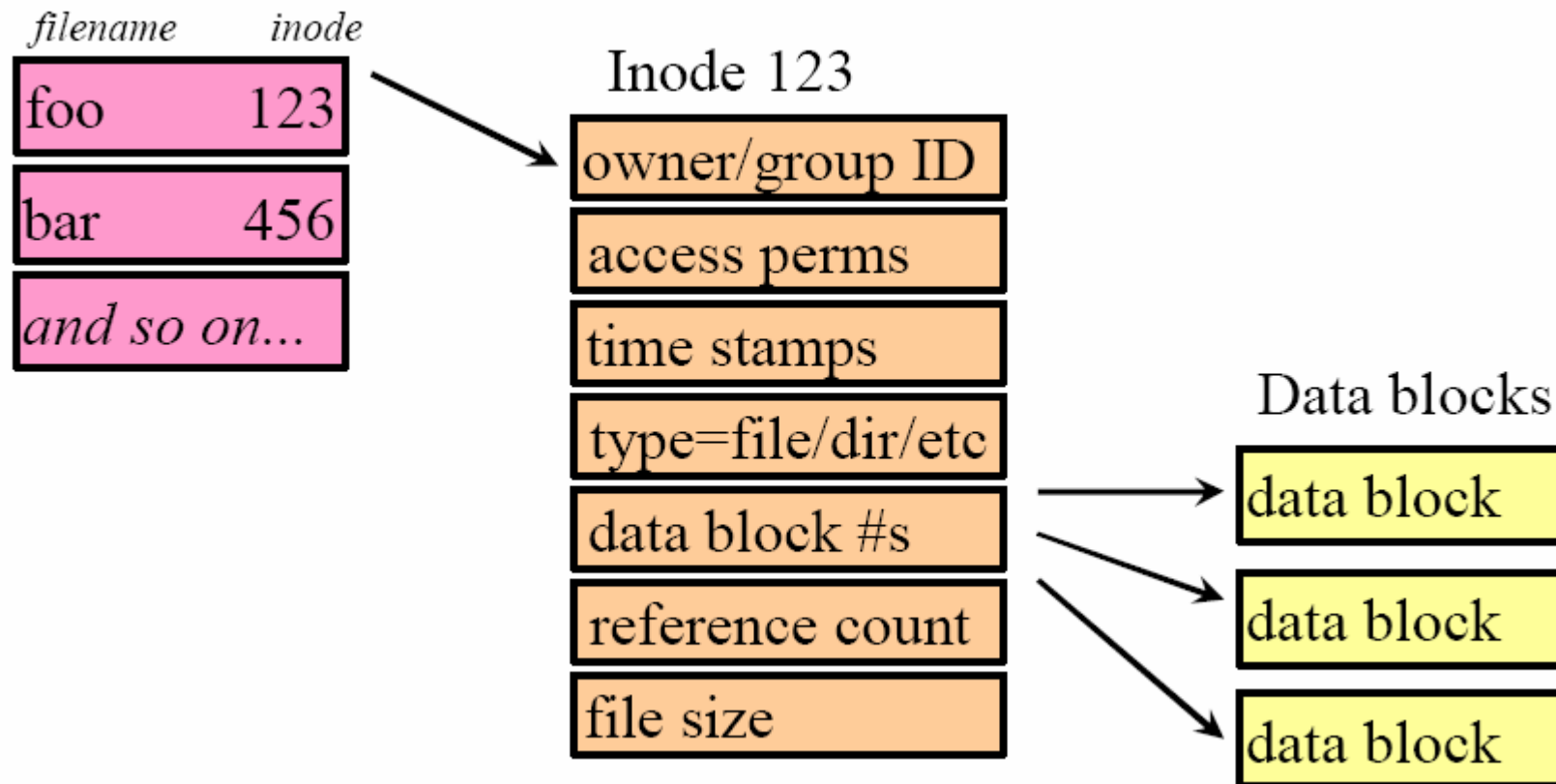
Data Destruction

- Easiest of the three categories
- Attackers want to hide their tracks
- Basically: overwriting data with x amount of data for y amount of time
- Several ways, standardized and others
- Want a real life forensic case? Buy a hard drive on eBay :)

Data Destruction

- Deleting
- Removal of reference to data
- Example:
 - UNIX file systems
 - Data is unlinked: unlink()
 - Inode is freed – set to “unallocated”
 - Data remains!
 - Similar system for NTFS and the Master File Table (MFT)

Data Destruction – Persistence of Data



Data Destruction

Deleting

- Deleted file attributes and content persist in unallocated disk blocks
- Overwritten data persists as tiny modulations on newer data
- Information is digital, but storage is analog!

Data Destruction

Wiping

- Overwriting data using certain algorithms
- Some operating systems already have tools (MacOSX, Linux, Solaris)
- Popular tools: wipe, shred, PGP secure delete
- “DBAN”: Linux distribution for wiping
- Impossible to get data back through software
- Magnetic analysis still possible

Data Destruction – Wiping Standards

Method	Security Level	Phases	Details
Quick Erase	Low	1	Zeros
RCMP TSSIT OPS-II	Medium	8	Alternating byte write
DoD short	Medium	3	3 phases of DoD 5220
DoD 5220-22.M	Medium	7	Random chars + streams
Gutmann Wipe	High	35	Static data + random datastream
PRNG Stream	Medium-High	8	Use of Pseudo Random Number Generator (PRNG)

Data Destruction

Wiping Standards

- Did 5220.22-M
- NAVSO P5239-26
- AFSSI-5020
- AR380-19

<http://www.usaid.gov/policy/ads/500/d522022m.pdf>

Data Destruction

Using the “shred” tool

```
[root@teletran-1 root]# shred -v /tmp/foo
shred: /tmp/foo: pass 1/25 (random)...
shred: /tmp/foo: pass 2/25 (444444)...
shred: /tmp/foo: pass 3/25 (999999)...
shred: /tmp/foo: pass 4/25 (222222)...
shred: /tmp/foo: pass 5/25 (249249)...
shred: /tmp/foo: pass 6/25 (6db6db)...
...
shred: /tmp/foo: pass 19/25 (333333)...
shred: /tmp/foo: pass 20/25 (555555)...
shred: /tmp/foo: pass 21/25 (666666)...
shred: /tmp/foo: pass 22/25 (db6db6)...
shred: /tmp/foo: pass 23/25 (777777)...
shred: /tmp/foo: pass 24/25 (492492)...
shred: /tmp/foo: pass 25/25 (random)...
[root@teletran-1 root]#
```

Data Destruction

What are we looking for as an investigator?

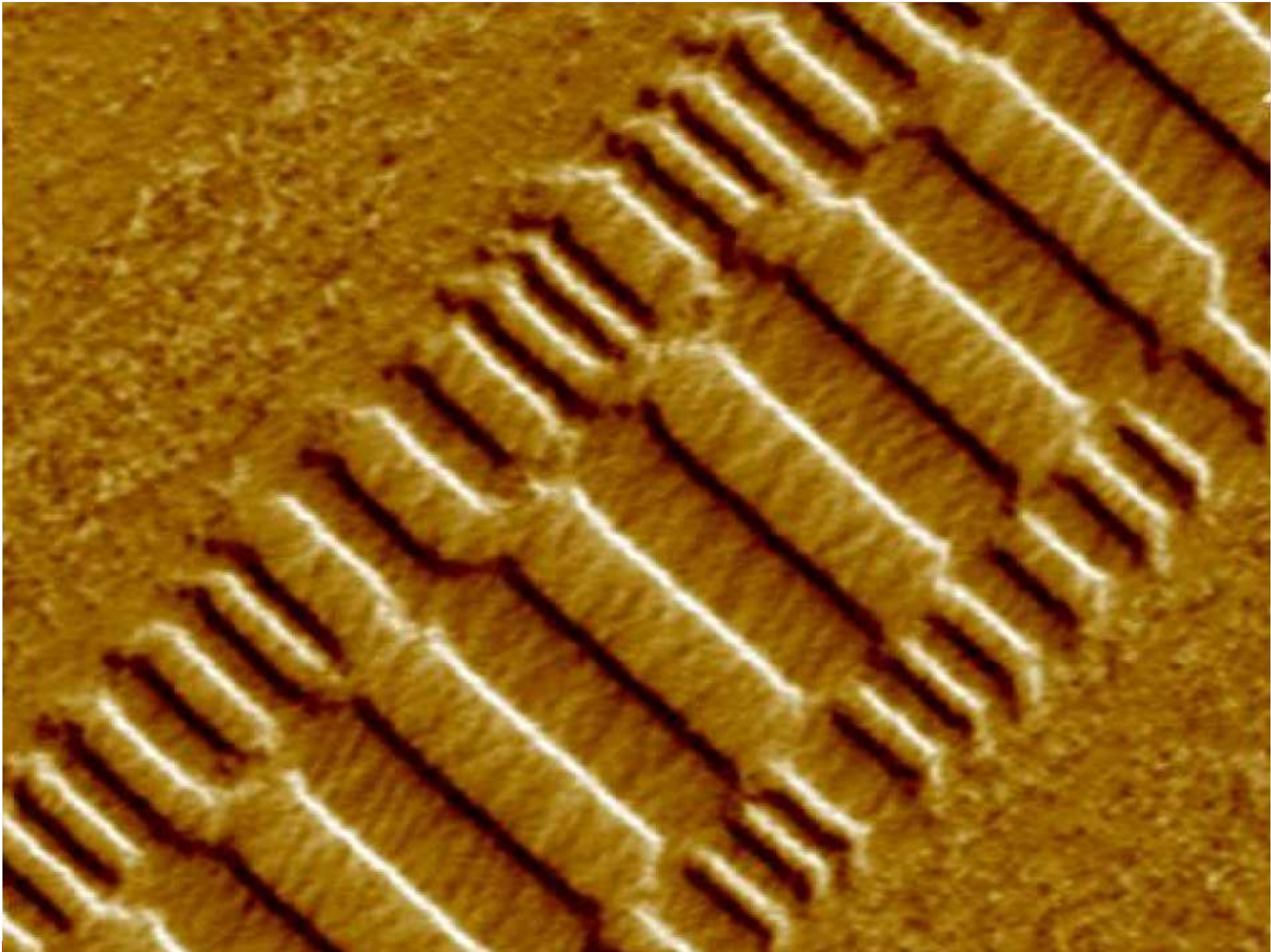
- Deleted File Residue
- “Dirty” inodes and directory entries
- “Dirty” data blocks
- File System Activity
- Inode time stamps
- Known anti-forensic tools
- Strings

Data Destruction

Software versus Hardware

- Media analysis is still possible
- Expensive, depending on size of disk
- Magnetic analysis
- Overhead analysis

Read/Write heads aren't 100% aligned with the drive

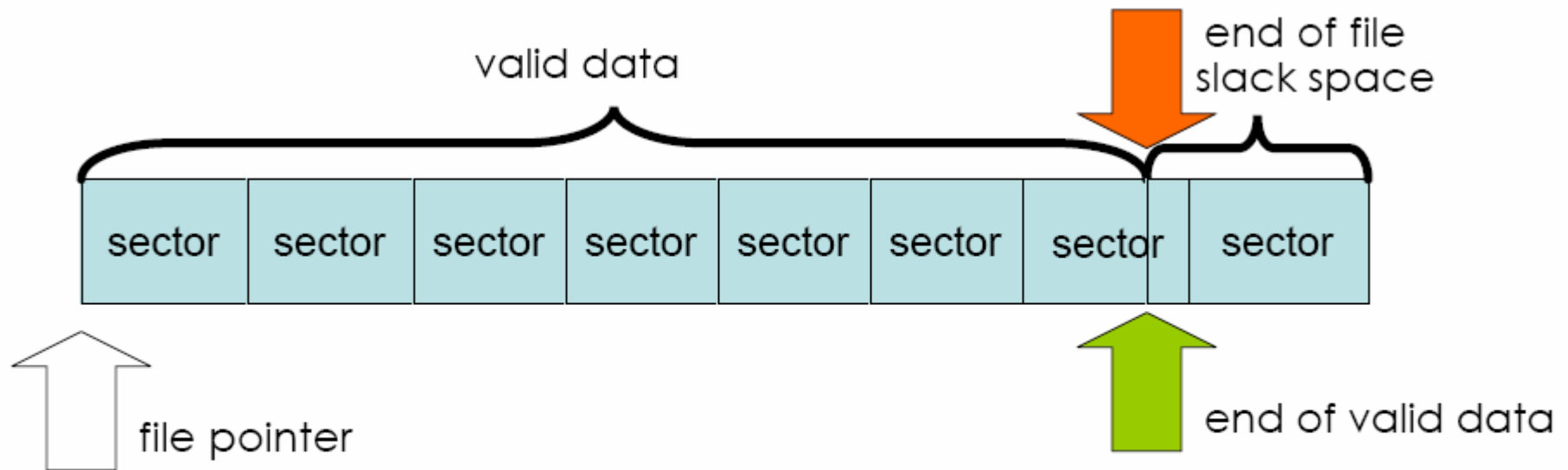


Data Hiding

- Covert
- Outside the scope of forensic tools
 - Temporarily
- Reliable
 - Data must not disappear
- Secure
 - Can't be accessed without correct tools
 - Encryption!

Data Hiding

Slackspace: Classic Example



1 cluster (4096 bytes) = 8 sectors (512 bytes)

Data Hiding

File System Insertion & Subversion Technique (FIST)

- Term coined by The Grugg
- FIST'ing is inserting data into places it doesn't belong
- Almost steganography
- Data storage in meta-data files
- Example: journals, directory files, OLE files, ...
- Modifying meta-data is dangerous
- Can be destroyed by maintenance tools (fsck, scandisk, etc)

Data Hiding

File System Insertion implementations

- RuneFS
 - Stores data in “bad blocks” file
- Wafften FS
 - Stores data in the ext3 journal file
- KY FS
 - Stores data in directory files
- Data Mule FS
 - Stores data in inode reserved space

Data Hiding

Alternative Data Streams: Classic Example

- Part of NTFS
- Not seen by virus scanners and anti-trojan programs
- Great for hiding logfiles, keyloggers or denial of service on the system (no more disk space)
- Can be viewed by forensic software (Encase)

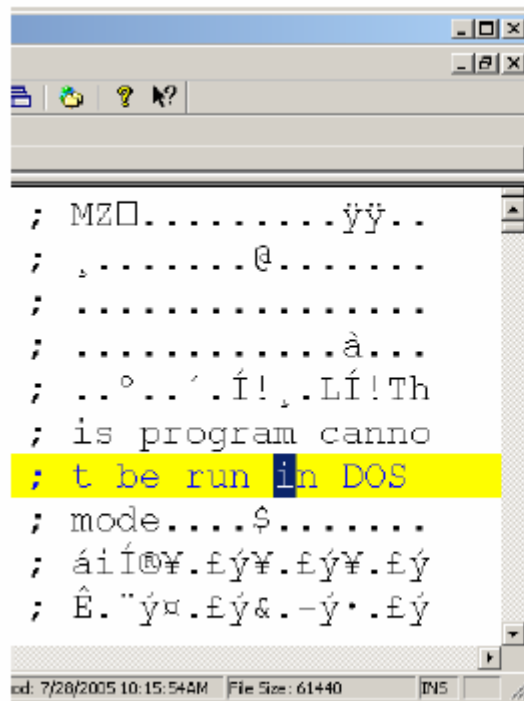
Data Hiding

Checksums

- Forensic investigator will compare md5sum of binaries to “known goods” and known attacks
- Attacker will:
 - Modify and recompile tools used
 - Make binary changes to stay under the radar
 - Use steganography and/or encryption

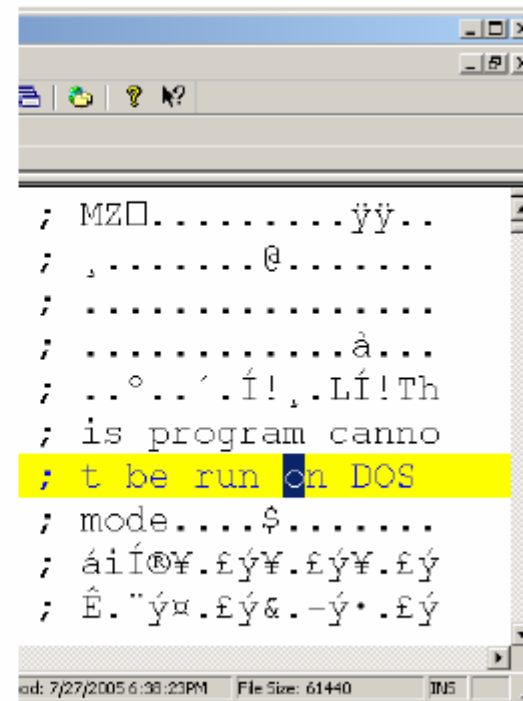
Data Hiding

One byte modification to a file...



```
; MZ.....ÿÿ..
; .....@.....
; .....
; .....à...
; ..°..'Í!..LÍ!Th
; is program canno
; t be run in DOS
; mode....$.
; áíí@¥.£ý¥.£ý¥.£ý
; Ê."ý¤.£ý&.-ý*.£ý
```

od: 7/26/2005 10:15:54AM File Size: 61440 IN5



```
; MZ.....ÿÿ..
; .....@.....
; .....
; .....à...
; ..°..'Í!..LÍ!Th
; is program canno
; t be run on DOS
; mode....$.
; áíí@¥.£ý¥.£ý¥.£ý
; Ê."ý¤.£ý&.-ý*.£ý
```

od: 7/27/2005 6:38:23PM File Size: 61440 IN5

Data Encryption

- Not popular on its own
- Steganography is better
- Encryption + Steganography = even better!
- Implies having a private secret key
- Examples: PGP disk, GPG, TrueCrypt, ...
- Not going to go into detail

Data Contraception

- Introduction
- Better not to create data than to have to destroy it afterwards
- Reduce quality of evidence
 - Prevent data from reaching the file system
 - Use memory!
 - Use standard tools, nothing exotic

Data Contraception

- Non-evident rootkits or trojans
- Run-time memory patching
 - > “Process Puppeteering”
- Utilize common, existing tools, not custom crafted ones that can be recovered by an investigator!
- Do not reinvent the wheel

Data Contraception

“Process Puppeteering”

- Uses memory manipulation
- Control a process and use it as proxy
- Syscall proxying
- Make an existing process perform the actions you want
- Steal / copy data
- Access system resources (filehandlers, sockets, etc)
- Used by Metasploit, Core Impact, others

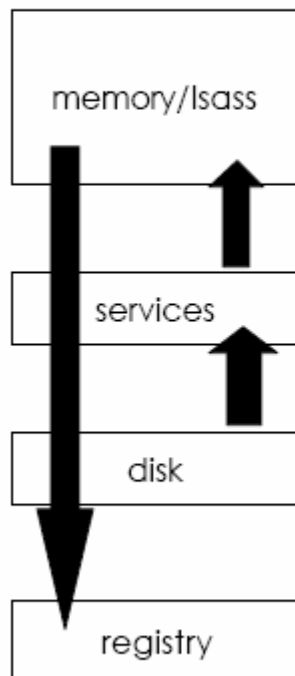
Data Contraception

Example: “SAM Juicer”

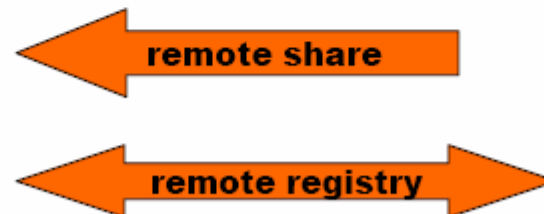
- SAM = Security Account Manager
- Holds hashed passwords for all users
- SAMjuicer is for NTFS
- Can dump the password hashes from the SAM table
- Does not access the disk!

Data Contraception – PWdump

Why an attacker will not use pwdump:



1. Opens a remote share
2. Hits disk
3. Starts a service to do dll injection
4. Hits registry
5. Creates remote registry conn
6. Often fails and doesn't clean up



Data Contraception – SAM Juicer

Example: “SAM Juicer”

memory/lsass

services

disk

registry

1. Slides over Meterpreter channel
2. Direct memory injection
3. Never hits disk & never hits the registry
4. Never starts a service
5. Data flows back over existing connection
6. Failure doesn't leave evidence



Data Contraception

Another example: HASH

- Developed by The Grugq
- Anti-Forensic shell
- Modular plugin framework
- Inline file transfer
- Command aliasing
- Plays nicely with metasploit / CANVAS

Downloadable at <http://www.tacticalvoip.com/tools.html>

Denial of Service

Introduction

- Forensic tools are standard (Encase, FTK, Sleuthkit, ... (?))
- Huge attack surface! Encase: 217 filetypes, 8 file systems
- 320GB of potential payload on your desk
- Forensic software not tested enough
- Defcon 15 presentation (iSec Partners)

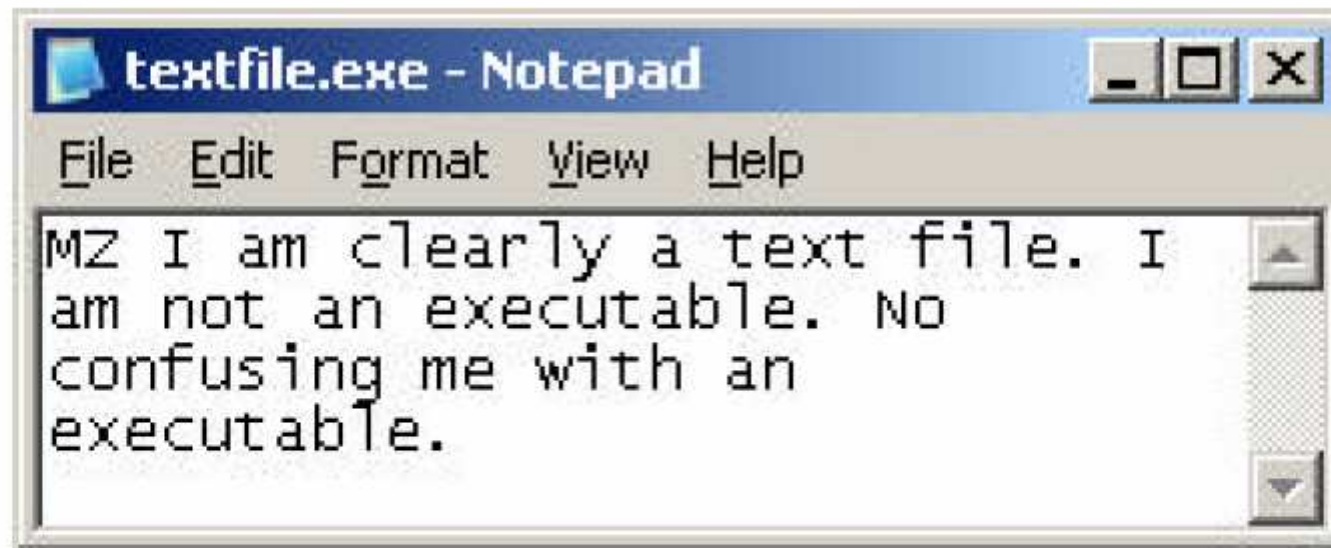
Denial of Service

Examples of the findings of iSec Partners:

- Mangle MBR => Encase can't acquire
- Corrupt NTFS partition table => Encase can't analyze
- File viewers (MS Office, Image/Video viewers) potential targets
- Bogus or null pointers in file system => makes Sleuthkit hang
- Long file names, directory loops, encrypted file loops
- Encase <6.7 cannot analyze beyond the 25th partition table

Encase...

Old Encase example of data manipulation



Encase
output

	Name	File Ext	File Type	Signature
<input checked="" type="checkbox"/> 21	textfile.exe	exe	Windows Executable	Match

Denial of Service

Why?

- Evidence hiding
- Code execution
- Evidence corruption
- Compromise of forensic workstation
- Denial of service – stall the investigation

http://www.isecpartners.com/files/iSEC-Breaking_Forensics_Software-Paper.v1_1.BH2007.pdf

Conclusion

- Keep your forensic software up to date!
- **NO INTERNET ACCESS ON FORENSIC WORKSTATION!**
- Trust your eyes & brain, then trust your tools
- Need for custom written tools, write your own! (and let me know)
- Try to fool a certain aspect of a forensic tool and write a countermeasure – be responsible in your disclosure!
- Need for more research

Thank You!