Sandbox detection: leak, abuse, test

Zoltan Balazs, MRG-Effitas
In cooperation with CrySyS lab, Budapest

We need to go faster than hyper speed. Jump straight to ludicris speed

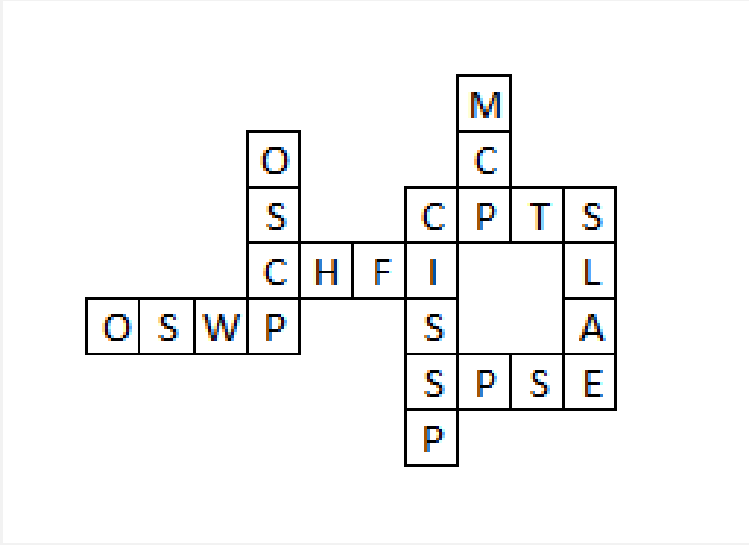
2015

Peter Kleissner
@Kleissner

Following

I heard there is a new rule at #botconf, everytime someome says "cyber" you have to drink a shot!

root@kali:~# whoami



Zoltan Balazs

I'm NOT a CEH

Creator of the Zombie Browser Toolkit

https://github.com/Z6543/ZombieBrowserPack

Creator of the HWFW Bypass tool

- Idea later(?) implemented by nation state attackers in Duqu 2.0

https://github.com/MRGEffitas/hwfwbypass

Invented the idea of encrypted exploit delivery via Diffie-Hellman key exchange, to bypass exploit detection appliances

- Recently implemented by Angler and Nuclear exploit kit developers

root@kali:~# whoami

How may I help you?

Are you analyzing malware and don't know why it is not running on your sandbox?

Are you writing a malware during pentest?

Are you developing a new malware analysis sandbox?

Are you testing malware analysis sandboxes, because you want to buy one?

Are you bored and just want to watch a fun presentation?

Current malware analysis

Static automated – malware is not started

- Easy to bypass

Dynamic automated – malware is started

- This presentation is about this type of analysis

Manual

- Hard to keep up with daily 400 000 new samples
- Analysis can take days, even weeks

Malware analysis sandbox – past and present

Malware analysis sandboxes were used by malware analysts in the past

These sandboxes are sold to companies, who lack

- Resources
- Skills
- People

Sold as magic boxes to detect APT malware on the network

What's wrong with the current sandbox detection techniques?

Too much focus on virtualization

- but handy in targeted attacks!

More and more legitimate targets in virtualized environments

- but not the CEO on the road

Methods already known and flagged as malicious

- VmWare IO ports

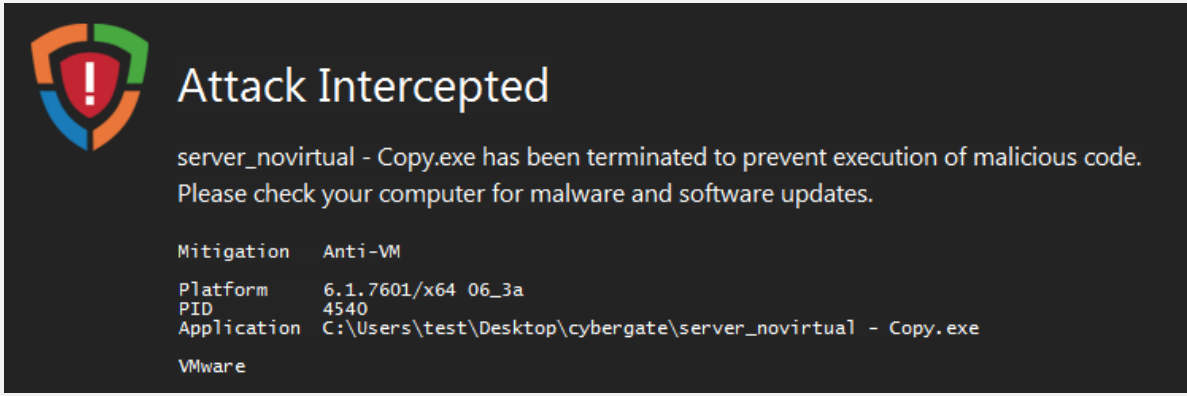
Methods already known, defeated and flagged

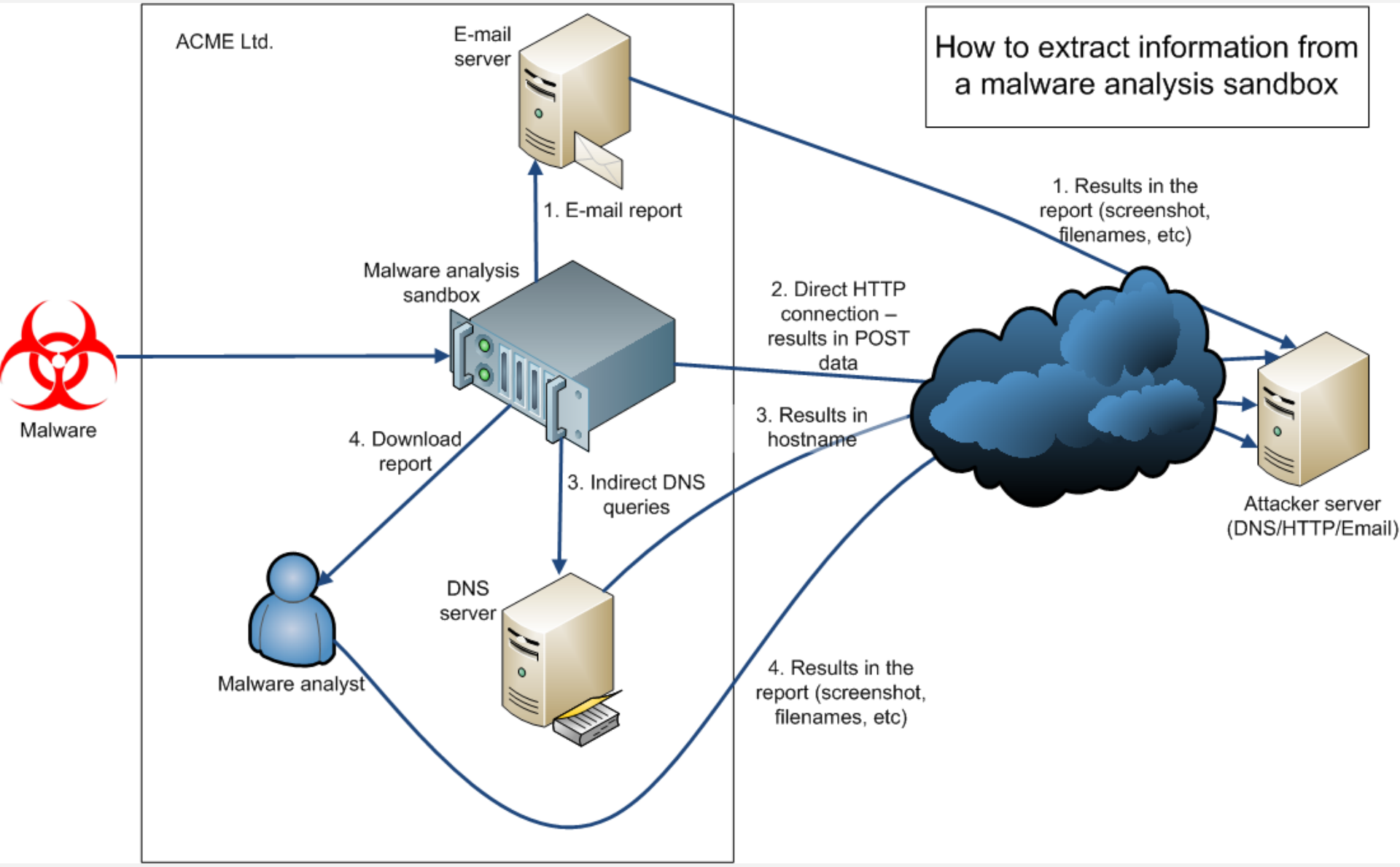
- ProductID

Workstation disguised as a VM

VACCINATION

Disguises the computer as that of a virus researcher, making sandbox-aware malware self-terminate.




How to extract information from a malware analysis sandbox
ACME Ltd.
E-mail server
1. E-mail report
Malware analysis sandbox
Malware
4. Download report
3. Indirect DNS queries
DNS server
Malware analyst
1. Results in the report (screenshot, filenames, etc)
2. Direct HTTP connection – results in POST data
3. Results in hostname
4. Results in the report (screenshot, filenames, etc)
Attacker server (DNS/HTTP/Email)

Demo

How to interpret results

Both “sandbox detection effectiveness” and “probability of busted” is measured

Good sandbox detection effectiveness, easily flagged as malicious


Normal effectiveness, possible flagged


Hard to get flagged as malicious

not effective


Screen resolution

Screen Resolution Statistics

As of today, 99% of our visitors have a screen resolution of 1024x768 pixels or higher:

Date	Other high	1920x1080	1366x768	1280x1024	1280x800	1024x768	800x600	Lower
January 2014	34%	13%	31%	8%	7%	6%	0.5%	0.5%

Pro tip

- Can be used in exploit kits, before exploit
- How many people browse the web with 800*600, or even 1024*768?
- Are these people your target?

JavaScript

- screen.width, screen.height
- works in almost all browser, except Tor browser

Screen resolution

43%: 1024x768 – this is a problem

36%: 800x600 – this is an even bigger problem

640x480 – this is just LOL

1024x697

1280x800

1280x960

1680x1050

1916x1066

Installed software

Python 2.5.1

Tracer

PHP 5.3.8

Python winappdbg 1 4

Debugging Tools for Windows x86

Python winappdbg 1 4

Strawberry Perl

VMware Tools

VEware Tools

Running processes on sandboxes

C:\SandCastle\tools\

- FakeServer.exe
- FakeHTTPServer\FakeHTTPServer.exe
- BehaviorDumper.exe

C:\Python27\python.exe

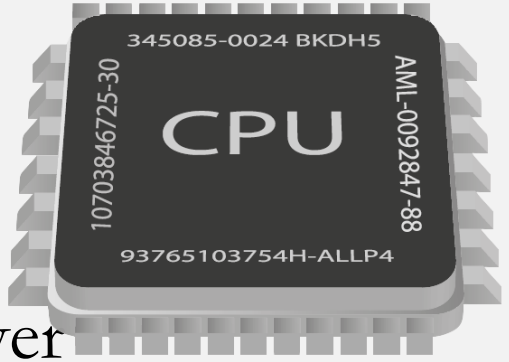
C:\tsl\RaptorClient.exe

C:\mapp_start_folder\snowball.exe > the sample renamed

C:\tools\dumper.exe

C:\VxStream\StaticStreamMgr.exe

CPU type



AMD Opteron tm Processor 3365 – server

AMD Phenom tm 9550 Quad Core Processor – server

Intel Pentium III Xeon processor – server

Intel R Xeon R CPU E5 2620 0 2 00GHz - server

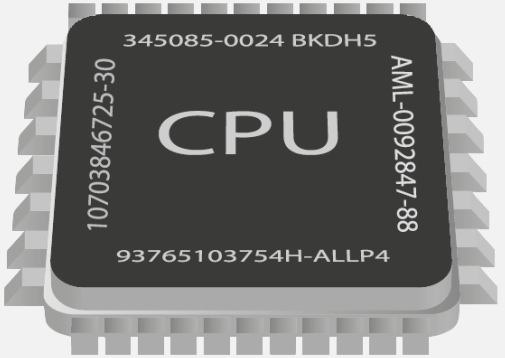
Intel Pentium Pro processor - ???

Intel Pentium II processor - ???

Intel R Atom TM CPU D525 1 80GHz – desktop

Intel R Core TM 2 Duo CPU T7700 2 40GHz – desktop

CPU 2



Most of the time:

- Number of Cores 1

Rarely seen in sandboxes:

- Number of Cores 2
- Number of Cores 4 (Sandbox in Ukraine)

Computer system – which one can be your real target (e.g. CEO)

Bochs
VirtualBox
VMware Virtual Platform
KVM
X7SPT DF – Supermicro Server Platform
MYTUAL MYVTUAL Platform
OptiPlex 990 – Dell desktop
4287A72 – Thinkpad
P5Q SE – Asus desktop
68% Virtualized, 18% desktop, 14% server


Mouse

80% no mouse movement

20% mouse moved

X:0 Y:0

X:400 Y:300

X:600 Y:600

Memory size

133 730 304	804 818 944
133 734 400	1 073 201 152
267 894 784	1 073 274 880
267 952 128	1 073 328 128
536 330 240	3 219 877 888
536 403 968	4 293 337 088
804 765 696	4 294 500 352

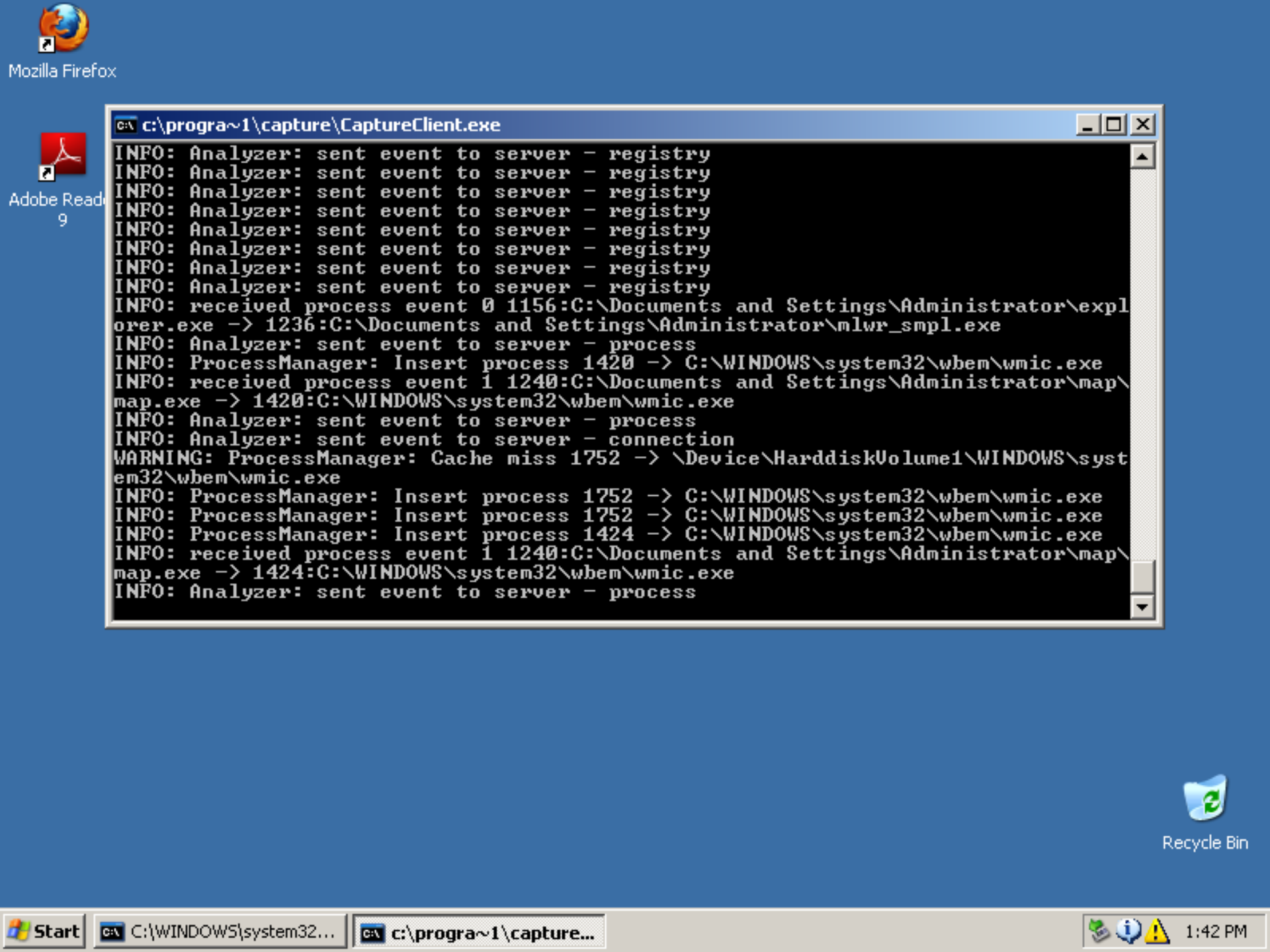
Machine name

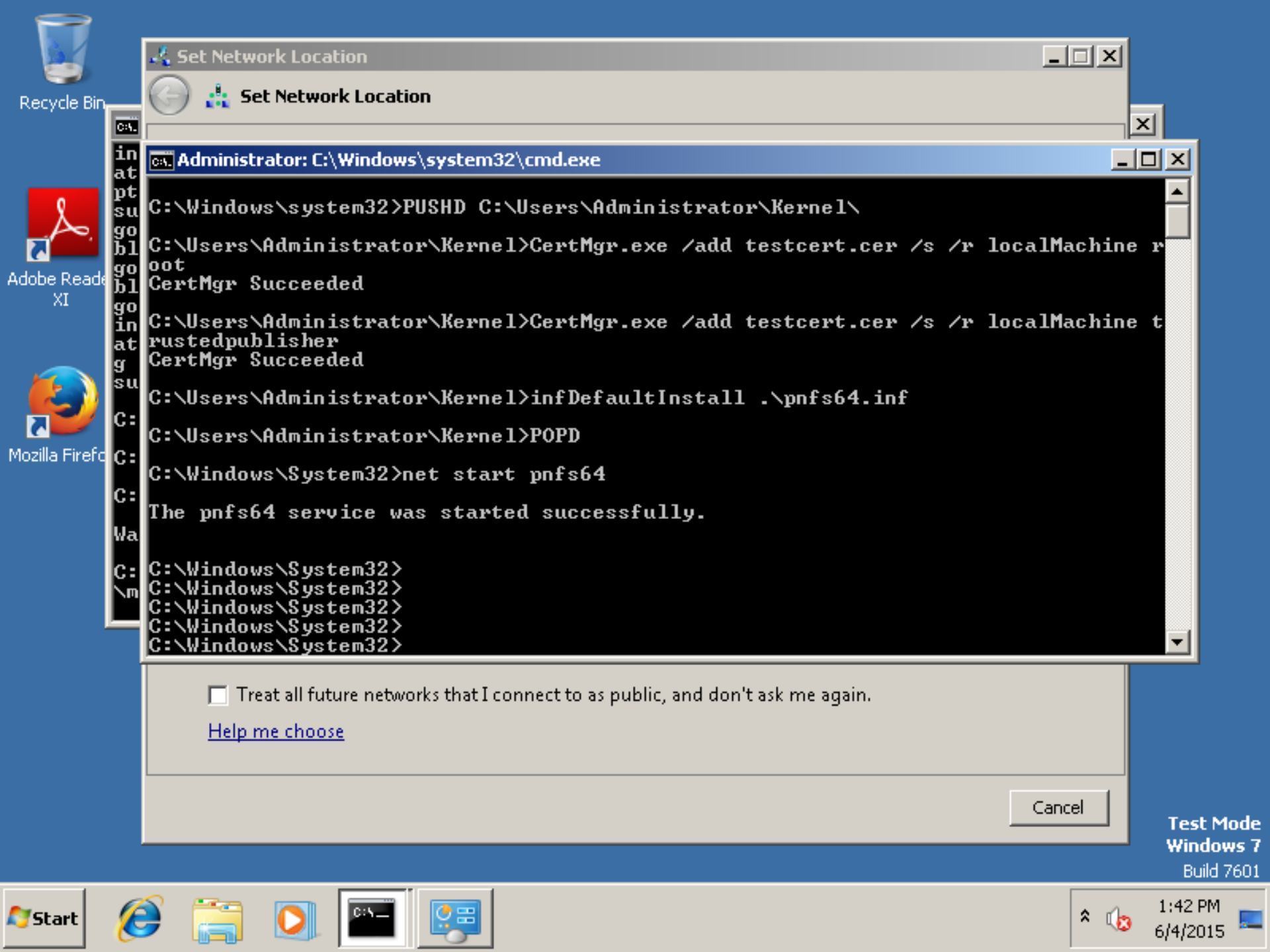
Antony PC
C2F3F0B206C14E9
CWS01_23
David PC
GOAT WXPSP2B
GT FDCCD9A7405D
HOME
HOME OFF D5F0AC
Klone PC

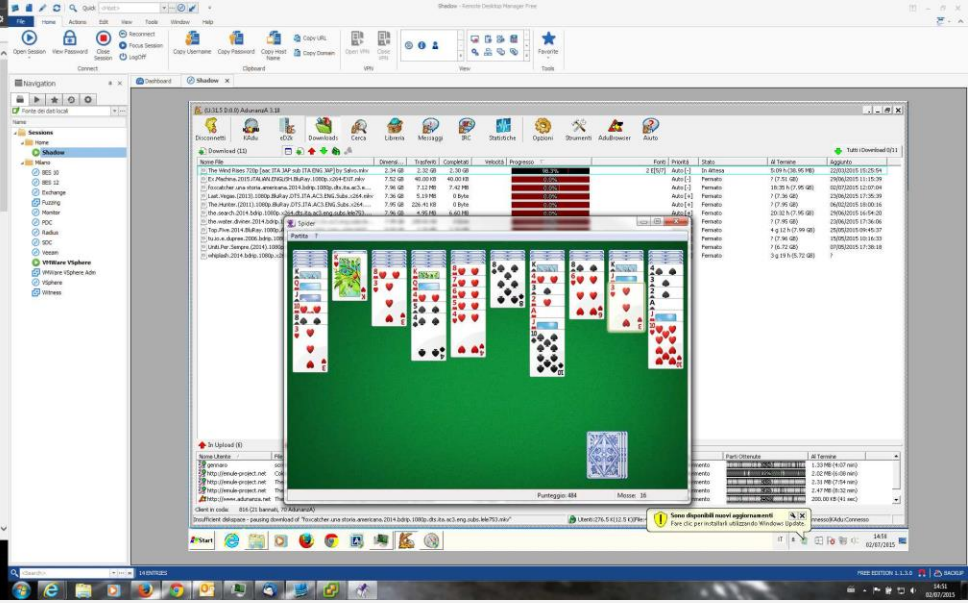
Machine name as a white-list can be powerful

PSPUBWS PC
PUBLIC EA8367E7
RON AC13BF686B1
ROOT D
SANDBOXA
TESPC0
test PC
USER201
USERDOMAIN
vwinxp maltest
WILBERT SC1317


My Computer
Mozilla Firefox
Adobe Reader 9
Recycle Bin
start
11:29 AM


Mozilla Firefox
Adobe Read
9
c:\progra~1\capture\CaptureClient.exe
INFO: Analyzer: sent event to server - registry
INFO: Analyzer: sent event to server - registry
INFO: Analyzer: sent event to server - registry
INFO: Analyzer: sent event to server - registry
INFO: Analyzer: sent event to server - registry
INFO: Analyzer: sent event to server - registry
INFO: Analyzer: sent event to server - registry
INFO: Analyzer: sent event to server - registry
INFO: received process event 0 1156:C:\Documents and Settings\Administrator\explorer.exe -> 1236:C:\Documents and Settings\Administrator\mlwr_smpl.exe
INFO: Analyzer: sent event to server - process
INFO: ProcessManager: Insert process 1420 -> C:\WINDOWS\system32\wbem\wmic.exe
INFO: received process event 1 1240:C:\Documents and Settings\Administrator\map\map.exe -> 1420:C:\WINDOWS\system32\wbem\wmic.exe
INFO: Analyzer: sent event to server - process
INFO: Analyzer: sent event to server - connection
WARNING: ProcessManager: Cache miss 1752 -> \Device\HarddiskVolume1\WINDOWS\system32\wbem\wmic.exe
INFO: ProcessManager: Insert process 1752 -> C:\WINDOWS\system32\wbem\wmic.exe
INFO: ProcessManager: Insert process 1752 -> C:\WINDOWS\system32\wbem\wmic.exe
INFO: ProcessManager: Insert process 1424 -> C:\WINDOWS\system32\wbem\wmic.exe
INFO: received process event 1 1240:C:\Documents and Settings\Administrator\map\map.exe -> 1424:C:\WINDOWS\system32\wbem\wmic.exe
INFO: Analyzer: sent event to server - process
Recycle Bin
Start
C:\WINDOWS\system32...
c:\progra~1\capture...
1:42 PM

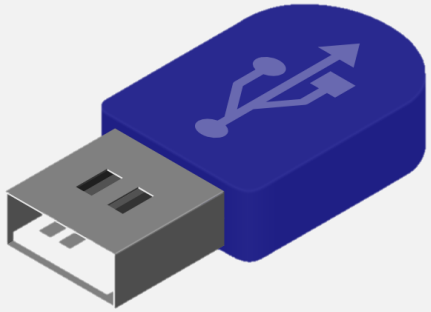

Recycle Bin
Adobe Reade XI
Mozilla Firefo
Set Network Location
Set Network Location
Administrator: C:\Windows\system32\cmd.exe
C:\Windows\system32>PUSHD C:\Users\Administrator\Kernel\
C:\Users\Administrator\Kernel>CertMgr.exe /add testcert.cer /s /r localMachine root
CertMgr Succeeded
C:\Users\Administrator\Kernel>CertMgr.exe /add testcert.cer /s /r localMachine trustedpublisher
CertMgr Succeeded
C:\Users\Administrator\Kernel>infDefaultInstall .\pnfs64.inf
C:\Users\Administrator\Kernel>POPD
C:\Windows\System32>net start pnfs64
The pnfs64 service was started successfully.
C:\Windows\System32>
C:\Windows\System32>
C:\Windows\System32>
C:\Windows\System32>
C:\Windows\System32>
Treat all future networks that I connect to as public, and don't ask me again.
Help me choose
Cancel
Test Mode
Windows 7
Build 7601
Start
1:42 PM
6/4/2015



Real “user” desktop, busy working

Screenshots from torrent Hacked Team c.pozzi\screenshots

USB Flash Drive



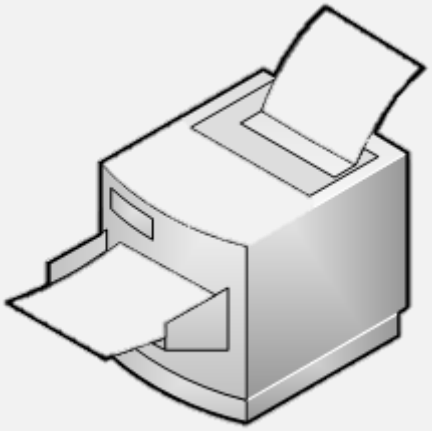
Usually:

- no flash drive

Rarely seen:

- 128MB USB2 0FlashDrive USB Device
- IPMI Virtual CDROM USB Device
- Kingston DataTraveler 2 0 USB Device

Printer



The only printers in sandboxes:

- Default Windows printers
- Adobe
- Office (Sendnote)

Recently modified/created files

Based on the folder you are looking at (Desktop, Documents, Appdata, Temp, …)

- it is usually less than 3 on sandboxes
- a lot more than 3 on desktops

Slow ☹

Where to implement these sandbox detection methods?

1. Before the malware is dropped, e.g. in Javascript or in shellcode
2. Automated decision, in the malware
    - Pro – no info leak about C&C
    - Con – not everything can be implemented here
3. Automated, on the C&C server
    - Pro – lot more possibilities
    - Con – C&C server info leaked
4. Manually, info from the C&C server
    - Pro – powerful e.g. analyze desktop screenshot
    - Con – expensive

Best approach

- Use all four layers, stop execution at first detection

The hard problems – Part 1

Is sleep function simulated?

- No (89%)
  - Sleep for a certain amount of time
  - Reach timeout limit (5 minutes)
  - PROFIT
- Yes (11%)
  - Easy to detect
  - Detect it and quit
  - PROFIT

Solution:

- Continuous sandboxing

The hard problems – Part 2

Network connection

Is there a HTTP connection to the Internet (directly or proxy)?

- Yes
  - Leak some data – e.g. multiple screenshots
  - Decide on server side
  - PROFIT
- No
  - If you don't target airgapped machines, it's safe to quit
  - PROFIT
- There is one, but it is emulated
  - Detect it by downloading a known object
  - Calculate hash
  - Compare
  - PROFIT

Lessons learned

Malware writers (penetration testers)

- It is incredibly easy to evade static and dynamic analysis
- Manual analysis is hard (or impossible) to defeat
  - But possible with lot of samples and new tricks on the long run!

Sandbox developers

- If you are selling your sandbox for $$$, try harder
- Dump a real user workstation and keep updated with user behavior
- It is hard to do it right, but easy to do it wrong

Blue team/defensive side

- Test your sandbox before buying
- Customize your sandbox to match your desktops
- Don't trust the marketing/sales department
- There are some good sandboxes out there!

The basics

https://github.com/hfiref0x/VMDE

https://github.com/hfiref0x/VBoxHardenedLoader

http://www.kernelmode.info/forum/viewtopic.php?f=11&t=1911

http://blog.michaelboman.org/2014/01/making virtualbox nearly undetectable.html

https://github.com/wmetcalf/buildcuckoo trusty

http://avtracker.info/

http://jbremer.org/vmcloak2/

https://www.youtube.com/watch?v=Ez_Gl5D_BV0

https://github.com/Yara-Rules/rules/blob/master/antidebug.yar

http://www.securitygalore.com/site3/vmd1-advisory

Hack the planet! One computer at a time …

https://github.com/MRGEffitas/Sandbox_tester

zoltan.balazs@mrg-effitas.com

https://hu.linkedin.com/in/zbalazs

Twitter – @zh4ck

www.slideshare.net/bz98

Greetz to @CrySySLab, @SpamAndHex

JumpESPJump.blogspot.com

Hack the planet!