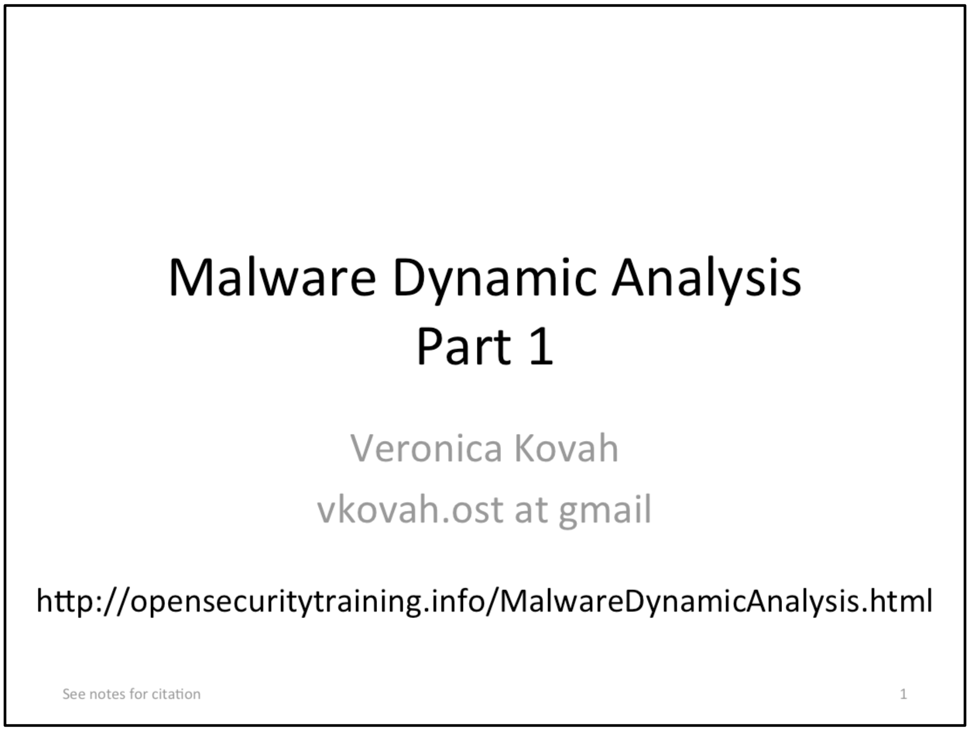


Malware Dynamic Analysis Part 1

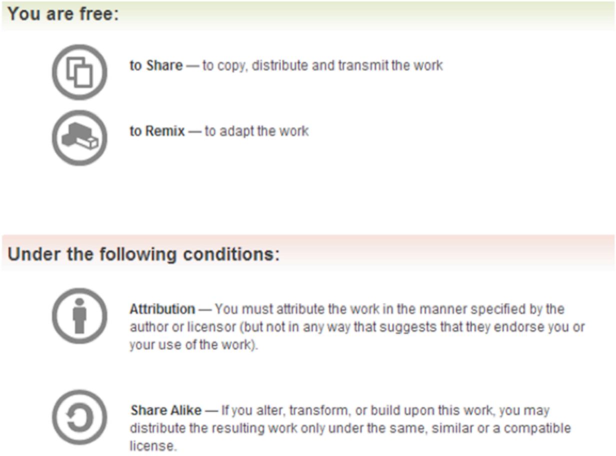
Veronica Kovah
vkovah.ost at gmail

http://opensecuritytraining.info/MalwareDynamicAnalysis.html

See notes for citation

All materials is licensed under a Creative Commons “Share Alike” license

http://creativecommons.org/licenses/by-sa/3.0/



You are free:

to Share — to copy, distribute and transmit the work

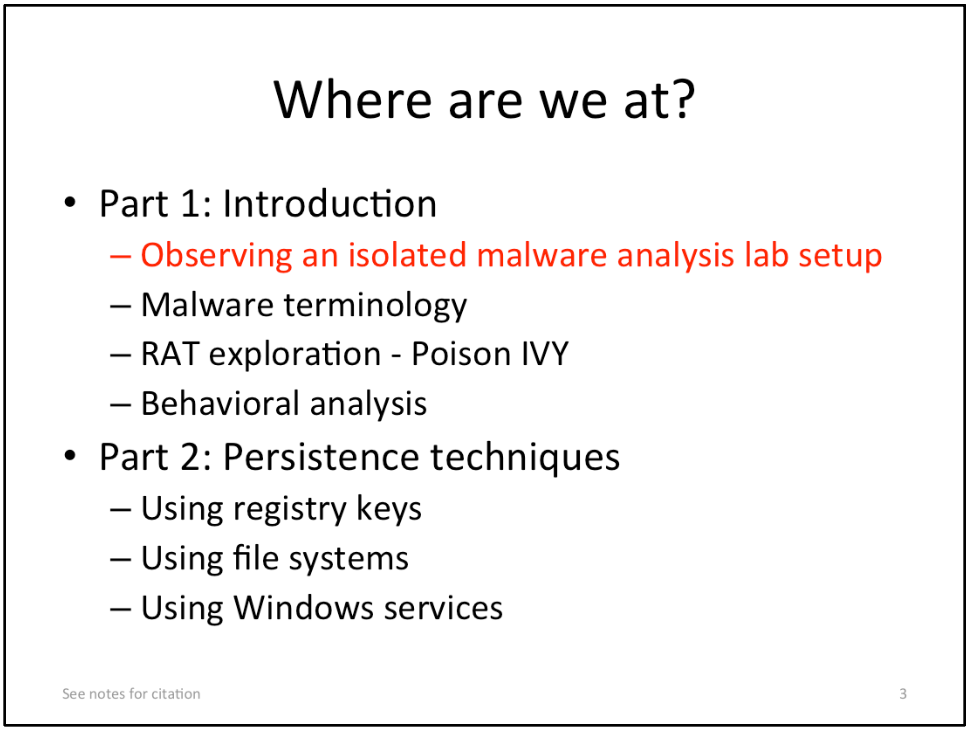
to Remix — to adapt the work

Under the following conditions:

Attribution — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

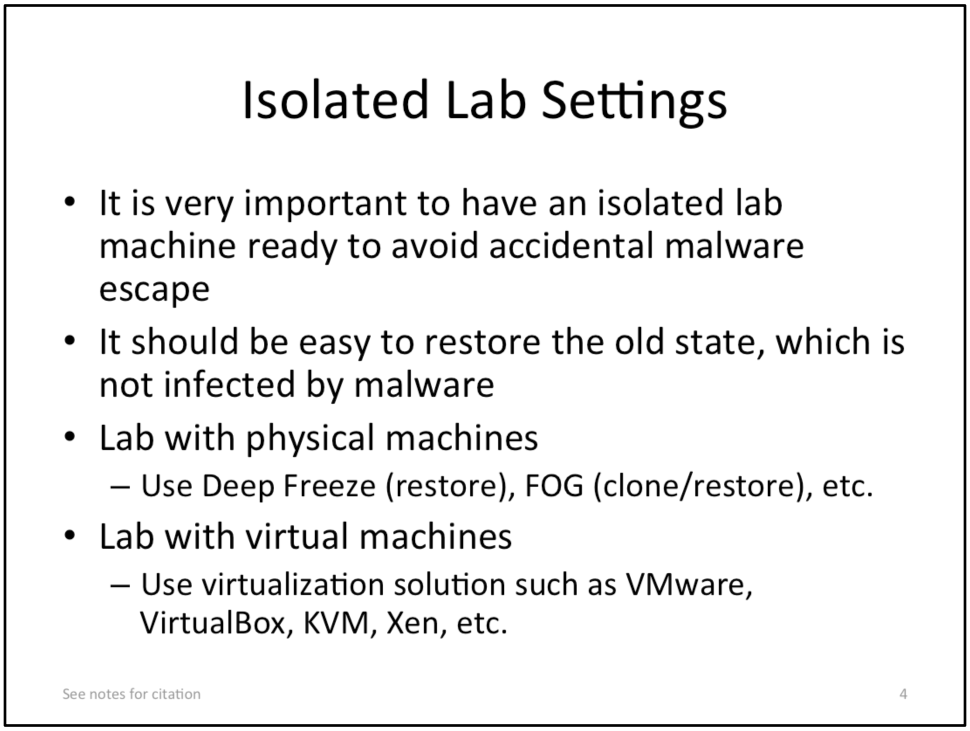
See notes for citation



Where are we at?

- Part 1: Introduction
  - Observing an isolated malware analysis lab setup
  - Malware terminology
  - RAT exploration - Poison IVY
  - Behavioral analysis
- Part 2: Persistence techniques
  - Using registry keys
  - Using file systems
  - Using Windows services

See notes for citation



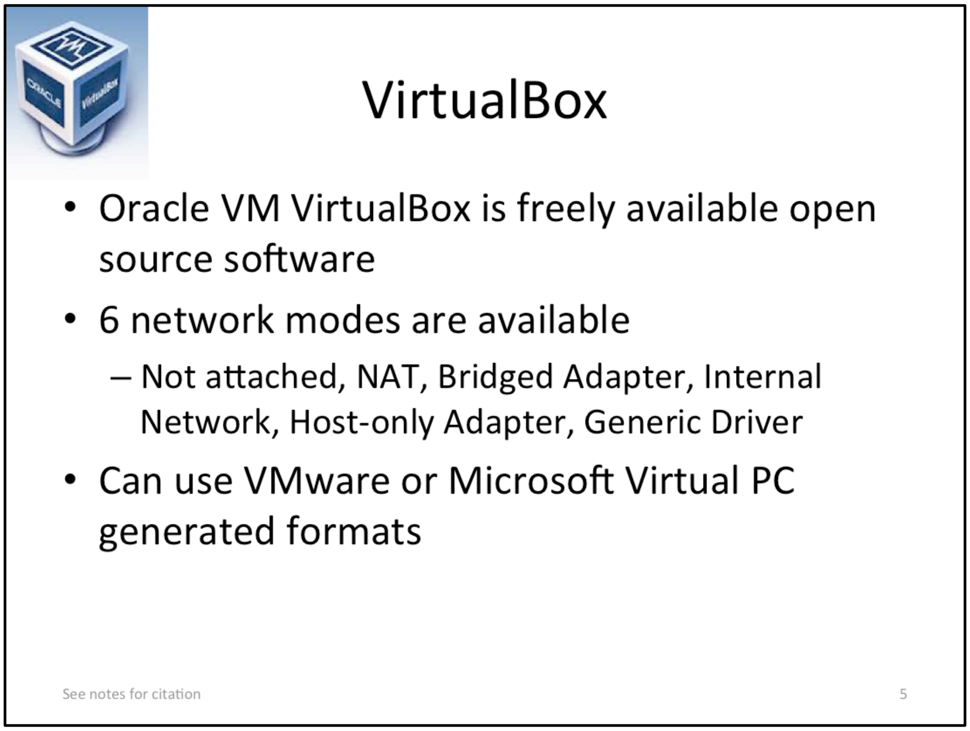
Isolated Lab Settings

- It is very important to have an isolated lab machine ready to avoid accidental malware escape
- It should be easy to restore the old state, which is not infected by malware
- Lab with physical machines
  - Use Deep Freeze (restore), FOG (clone/restore), etc.
- Lab with virtual machines
  - Use virtualization solution such as VMware, VirtualBox, KVM, Xen, etc.

See notes for citation

[References]

- Deep Freeze, http://www.faronics.com/products/deep-freeze/standard/
- FOG, http://sourceforge.net/projects/freeghost/
- Vmware, http://www.vmware.com/
- VirtualBox, https://www.virtualbox.org/
- KVM, http://www.linux-kvm.org/page/Main_Page
- Xen, http://www.xen.org/



VirtualBox

- Oracle VM VirtualBox is freely available open source software
- 6 network modes are available
  - Not attached, NAT, Bridged Adapter, Internal Network, Host-only Adapter, Generic Driver
- Can use VMware or Microsoft Virtual PC generated formats

See notes for citation

5

[References]

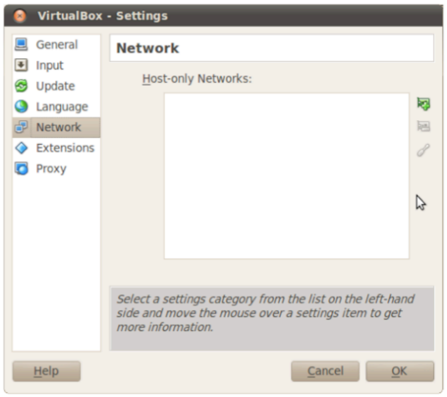
- VirtualBox, https://www.virtualbox.org/
- Chapter 6. Virtual networking, Oracle VM VirtualBox User Manual, http://www.virtualbox.org/manual/ch06.html

[Image Sources]

- https://www.virtualbox.org/graphics/vbox_logo2_gradient.png

2 Host-only Networks

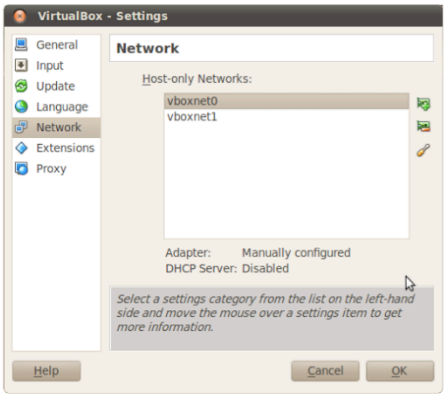
- File->Preferences…->Network



Network

Host-only Networks:

Select a settings category from the list on the left-hand side and move the mouse over a settings item to get more information.



Network

Host-only Networks:

vboxnet0
vboxnet1

Adapter: Manually configured
DHCP Server: Disabled

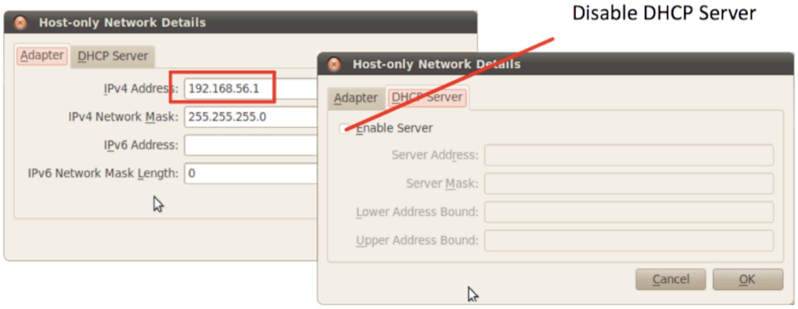
Select a settings category from the list on the left-hand side and move the mouse over a settings item to get more information.

See notes for citation

[References]

- Oracle VM VirtualBox User Manual, http://www.virtualbox.org/manual/UserManual.html

Network Details



Host-only Network Details

IPv4 Address: 192.168.56.1

IPv4 Network Mask: 255.255.255.0

IPv6 Address:

IPv6 Network Mask Length: 0

Host-only Network Details

☐ Enable Server

Server Address:

Server Mask:

Lower Address Bound:

Upper Address Bound:

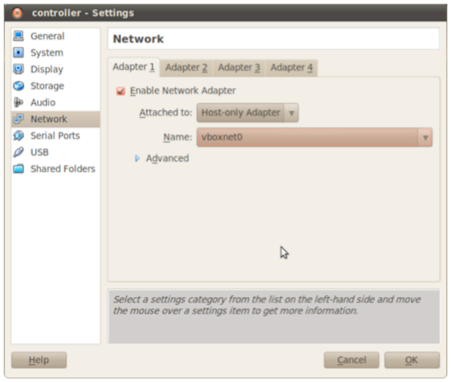
Disable DHCP Server

- Same for vboxnet1 except IPv4 address, 192.168.57.1
- On host machine, check if you see new network interfaces
  - $ ifconfig

See notes for citation

VM’s network setting (1)

- Start *controller* VM first
  - C:\> ipconfig
- Open *controller* VM’s Settings, change Network->Adapter 1



☑ Enable Network Adapter

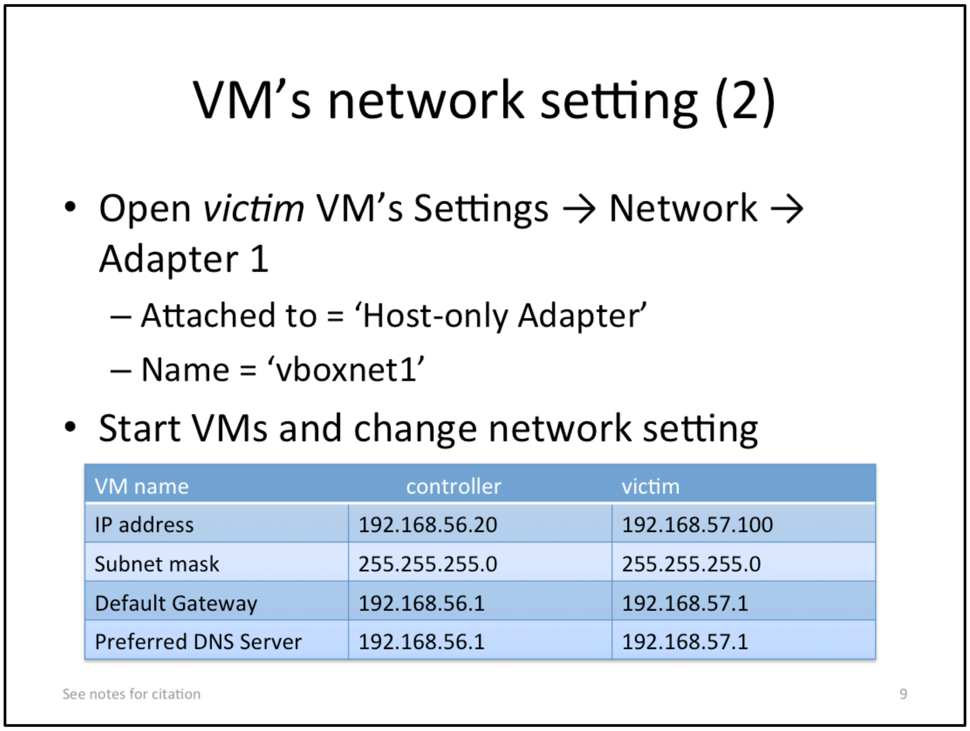
Attached to: Host-only Adapter

Name: vboxnet0

Advanced

Select a settings category from the list on the left-hand side and move the mouse over a settings item to get more information.

See notes for citation



VM’s network setting (2)

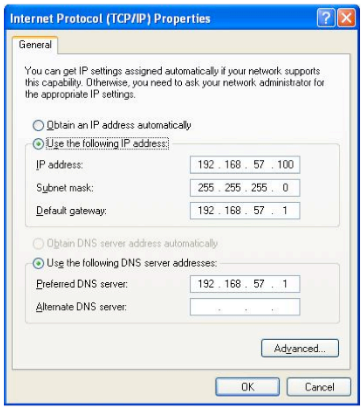
- Open *victim* VM’s Settings → Network → Adapter 1
  - Attached to = ‘Host-only Adapter’
  - Name = ‘vboxnet1’
- Start VMs and change network setting

VM name	controller	victim
IP address	192.168.56.20	192.168.57.100
Subnet mask	255.255.255.0	255.255.255.0
Default Gateway	192.168.56.1	192.168.57.1
Preferred DNS Server	192.168.56.1	192.168.57.1

See notes for citation

Change IP on Windows

- Start → Control Panel → Network Connections → Local Area Connection → Properties → Internet Protocols (TCP/IP) → Properties



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 57 . 100

Subnet mask: 255 . 255 . 255 . 0

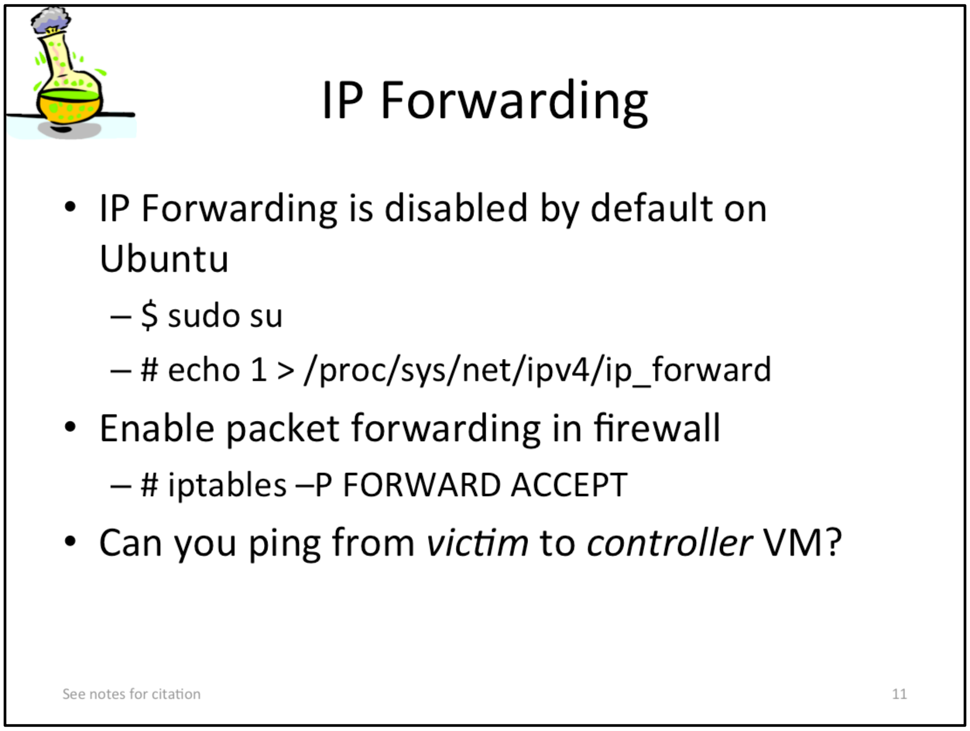
Default gateway: 192 . 168 . 57 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 57 . 1

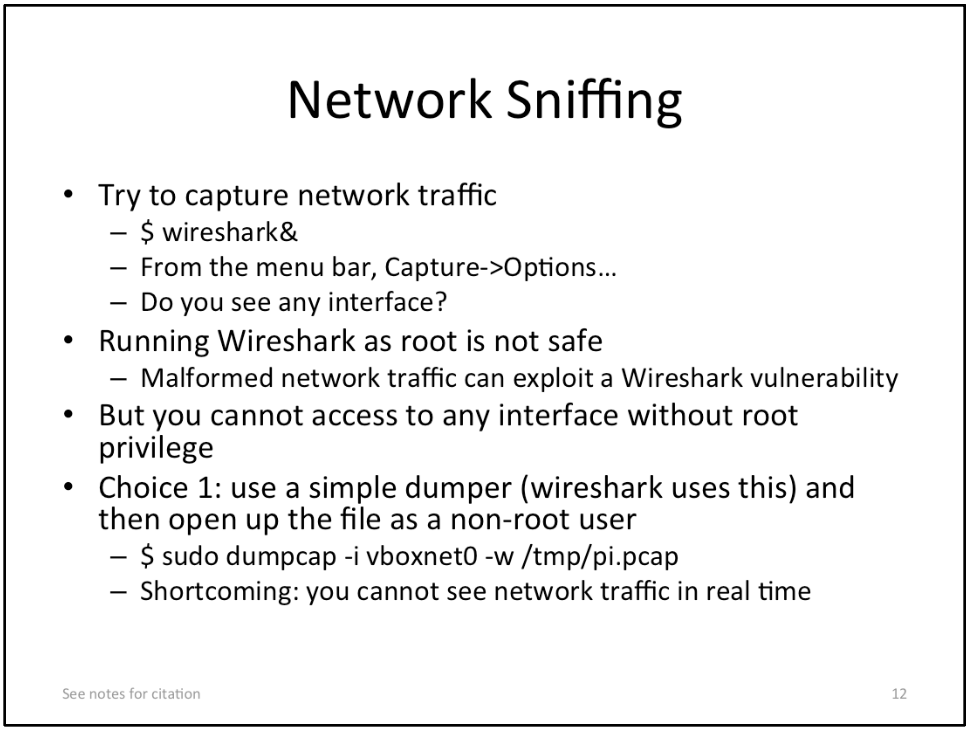
Alternate DNS server: . . .



IP Forwarding

- IP Forwarding is disabled by default on Ubuntu
  - $ sudo su
  - # echo 1 > /proc/sys/net/ipv4/ip_forward
- Enable packet forwarding in firewall
  - # iptables –P FORWARD ACCEPT
- Can you ping from *victim* to *controller* VM?

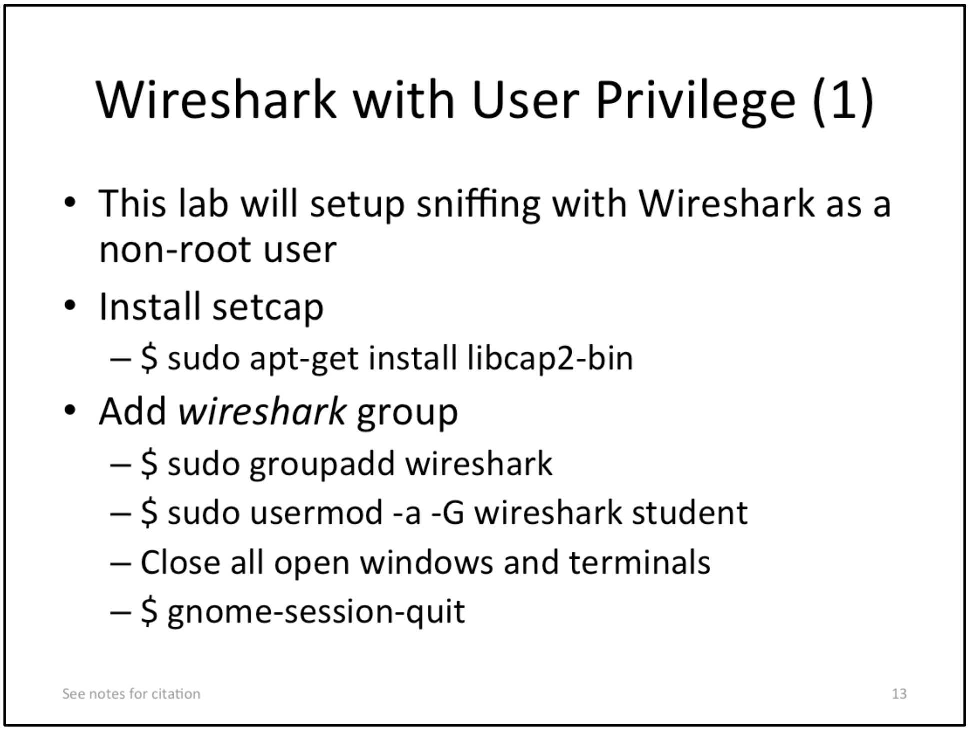
See notes for citation



Network Sniffing

- Try to capture network traffic
  - $ wireshark&
  - From the menu bar, Capture->Options…
  - Do you see any interface?
- Running Wireshark as root is not safe
  - Malformed network traffic can exploit a Wireshark vulnerability
- But you cannot access to any interface without root privilege
- Choice 1: use a simple dumper (wireshark uses this) and then open up the file as a non-root user
  - `$ sudo dumpcap -i vboxnet0 -w /tmp/pi.pcap`
  - Shortcoming: you cannot see network traffic in real time

See notes for citation



Wireshark with User Privilege (1)

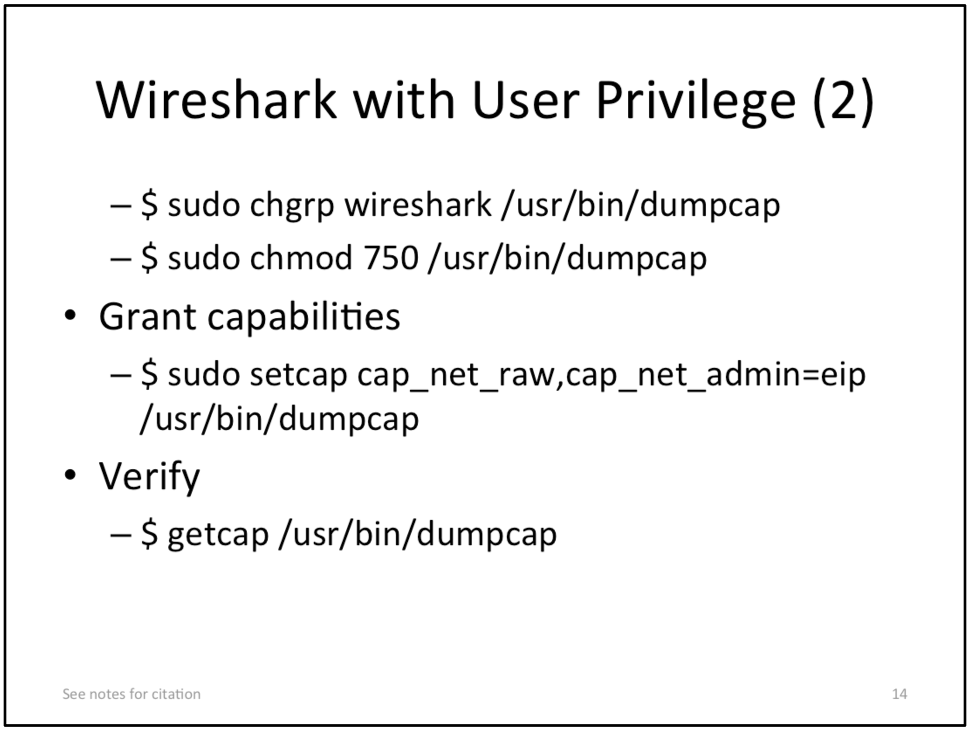
- This lab will setup sniffing with Wireshark as a non-root user
- Install setcap
  - $ sudo apt-get install libcap2-bin
- Add *wireshark* group
  - $ sudo groupadd wireshark
  - $ sudo usermod -a -G wireshark student
  - Close all open windows and terminals
  - $ gnome-session-quit

See notes for citation

13

[References]

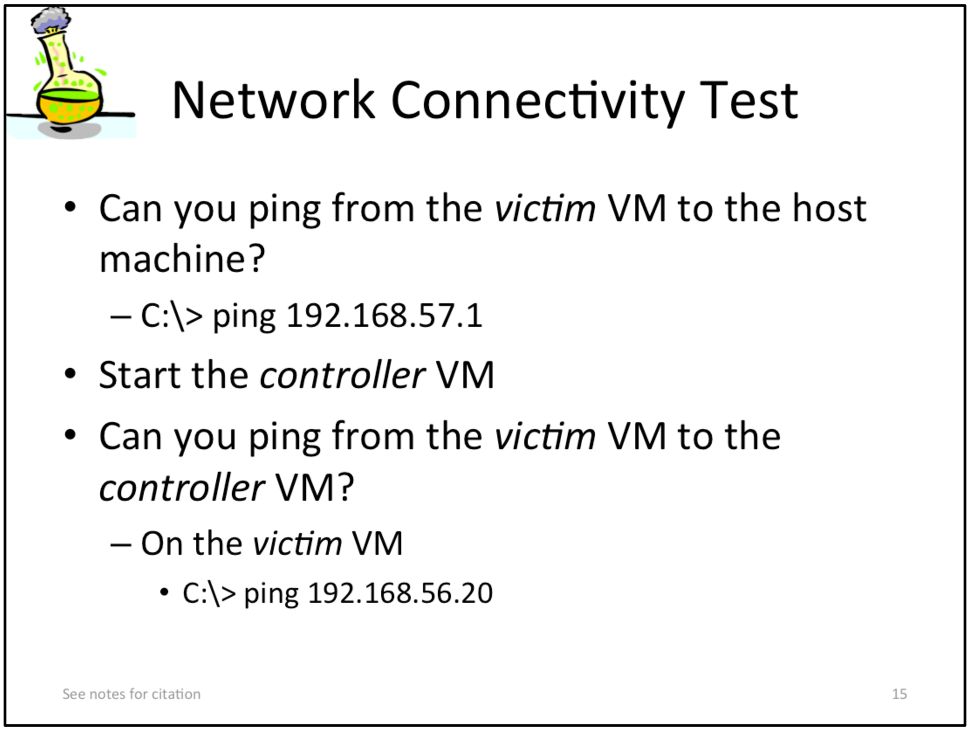
- Jeremy Stretch, Sniffing with Wireshark as a Non-Root User, http://packetlife.net/blog/2010/mar/19/sniffing-wireshark-non-root-user/



Wireshark with User Privilege (2)

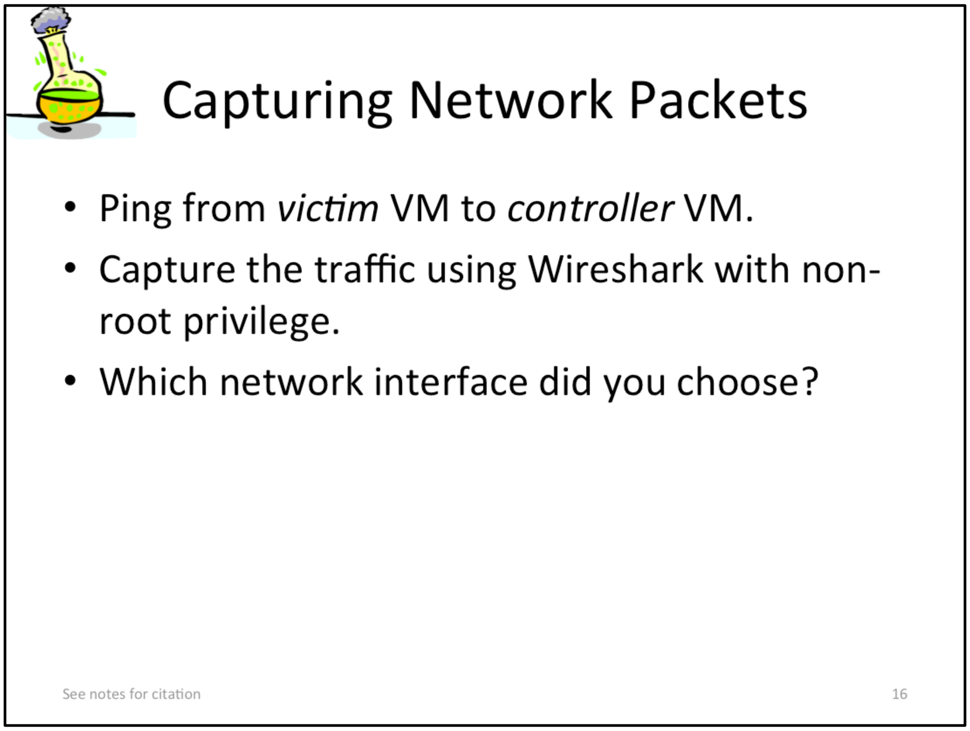
  - $ sudo chgrp wireshark /usr/bin/dumpcap
  - $ sudo chmod 750 /usr/bin/dumpcap
- Grant capabilities
  - $ sudo setcap cap_net_raw,cap_net_admin=eip /usr/bin/dumpcap
- Verify
  - $ getcap /usr/bin/dumpcap

See notes for citation



Network Connectivity Test

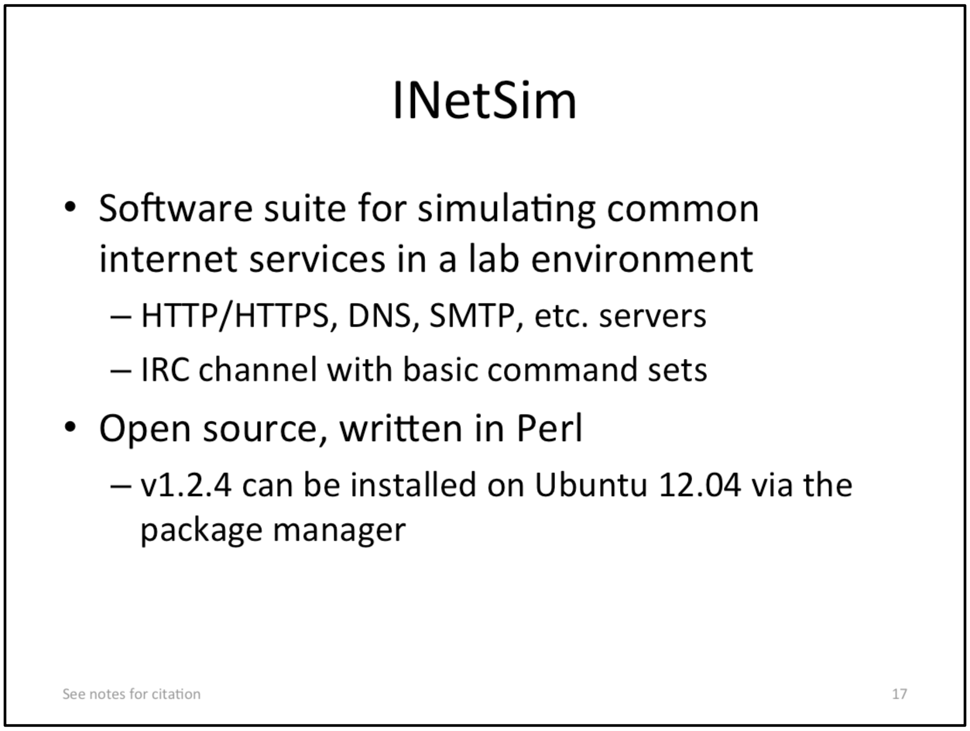
- Can you ping from the *victim* VM to the host machine?
  - C:\> ping 192.168.57.1
- Start the *controller* VM
- Can you ping from the *victim* VM to the *controller* VM?
  - On the *victim* VM
    - C:\> ping 192.168.56.20



Capturing Network Packets

- Ping from *victim* VM to *controller* VM.
- Capture the traffic using Wireshark with non-root privilege.
- Which network interface did you choose?

See notes for citation



INetSim

- Software suite for simulating common internet services in a lab environment
  - HTTP/HTTPS, DNS, SMTP, etc. servers
  - IRC channel with basic command sets
- Open source, written in Perl
  - v1.2.4 can be installed on Ubuntu 12.04 via the package manager

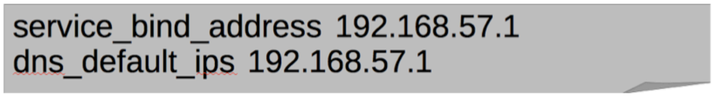
See notes for citation

[References]

- Thomas Hungenberg and Matthias Eckert, INetSim, http://www.inetsim.org/

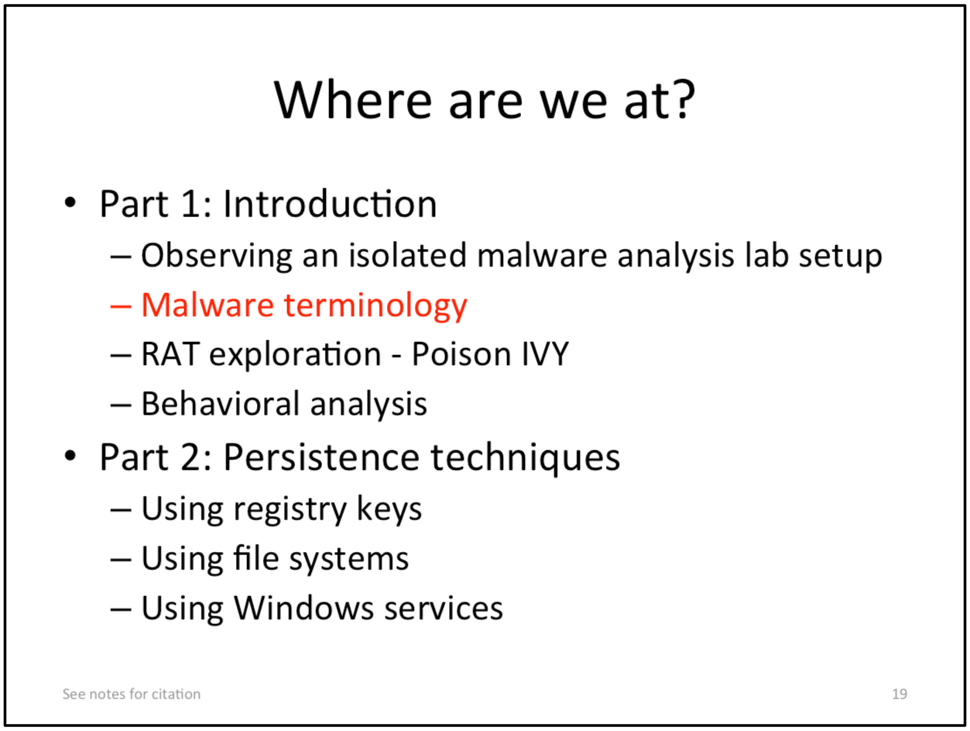
inetsim setup

- On the host machine
  - $ gedit /etc/inetsim/inetsim.conf



```
service_bind_address 192.168.57.1
dns_default_ips 192.168.57.1
```

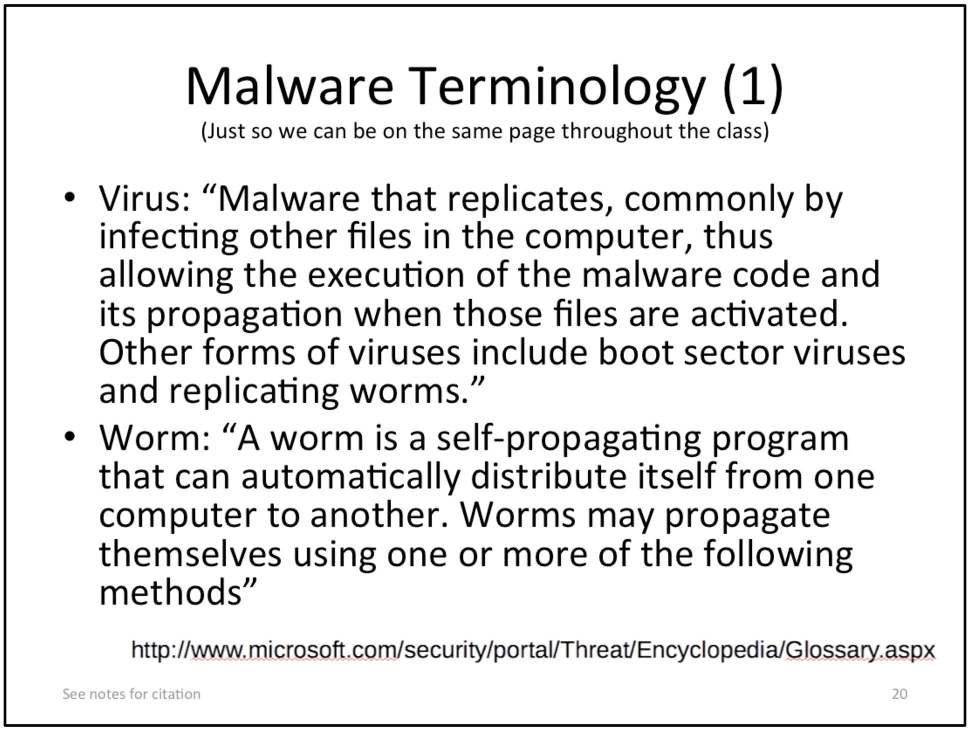
  - $ sudo inetsim
  - $ wireshark &
    - listen on vboxnet1
- On the *victim* VM
  - c:> ping www.google.com



Where are we at?

- Part 1: Introduction
  - Observing an isolated malware analysis lab setup
  - Malware terminology
  - RAT exploration - Poison IVY
  - Behavioral analysis
- Part 2: Persistence techniques
  - Using registry keys
  - Using file systems
  - Using Windows services

See notes for citation



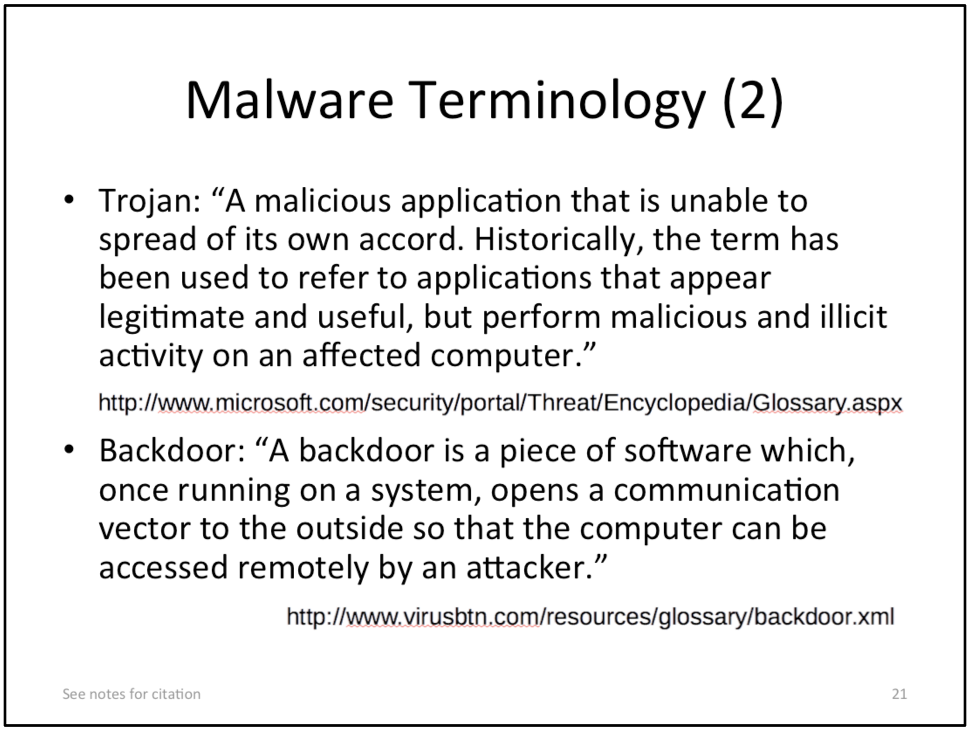
Malware Terminology (1)

(Just so we can be on the same page throughout the class)

- Virus: “Malware that replicates, commonly by infecting other files in the computer, thus allowing the execution of the malware code and its propagation when those files are activated. Other forms of viruses include boot sector viruses and replicating worms.”
- Worm: “A worm is a self-propagating program that can automatically distribute itself from one computer to another. Worms may propagate themselves using one or more of the following methods”

http://www.microsoft.com/security/portal/Threat/Encyclopedia/Glossary.aspx

See notes for citation



Malware Terminology (2)

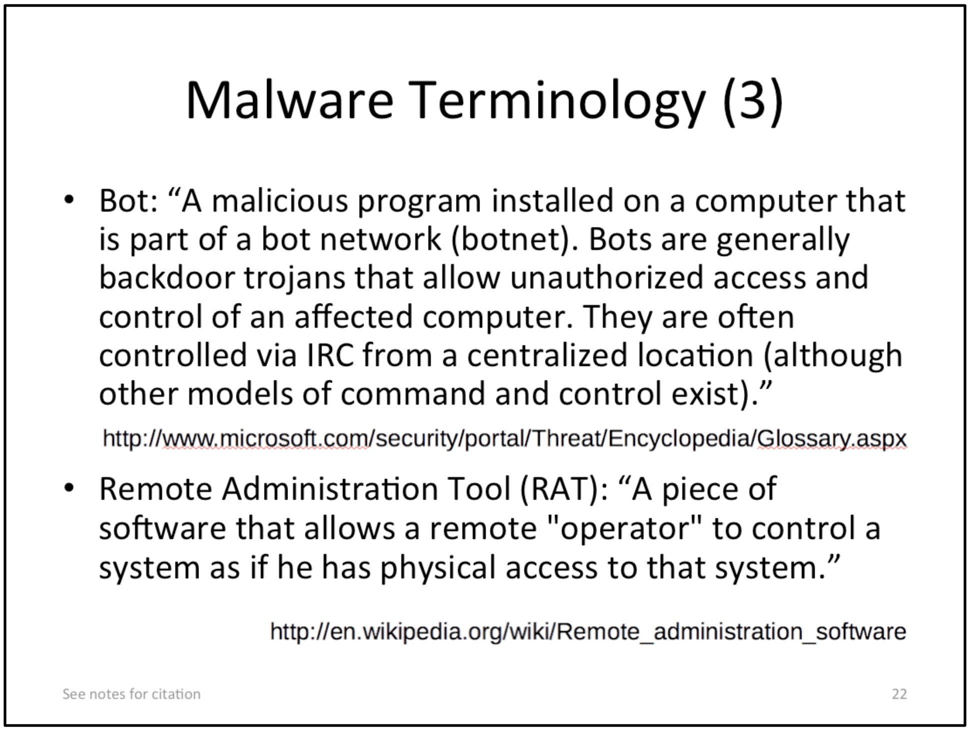
- Trojan: “A malicious application that is unable to spread of its own accord. Historically, the term has been used to refer to applications that appear legitimate and useful, but perform malicious and illicit activity on an affected computer.”

  http://www.microsoft.com/security/portal/Threat/Encyclopedia/Glossary.aspx

- Backdoor: “A backdoor is a piece of software which, once running on a system, opens a communication vector to the outside so that the computer can be accessed remotely by an attacker.”

  http://www.virusbtn.com/resources/glossary/backdoor.xml

See notes for citation



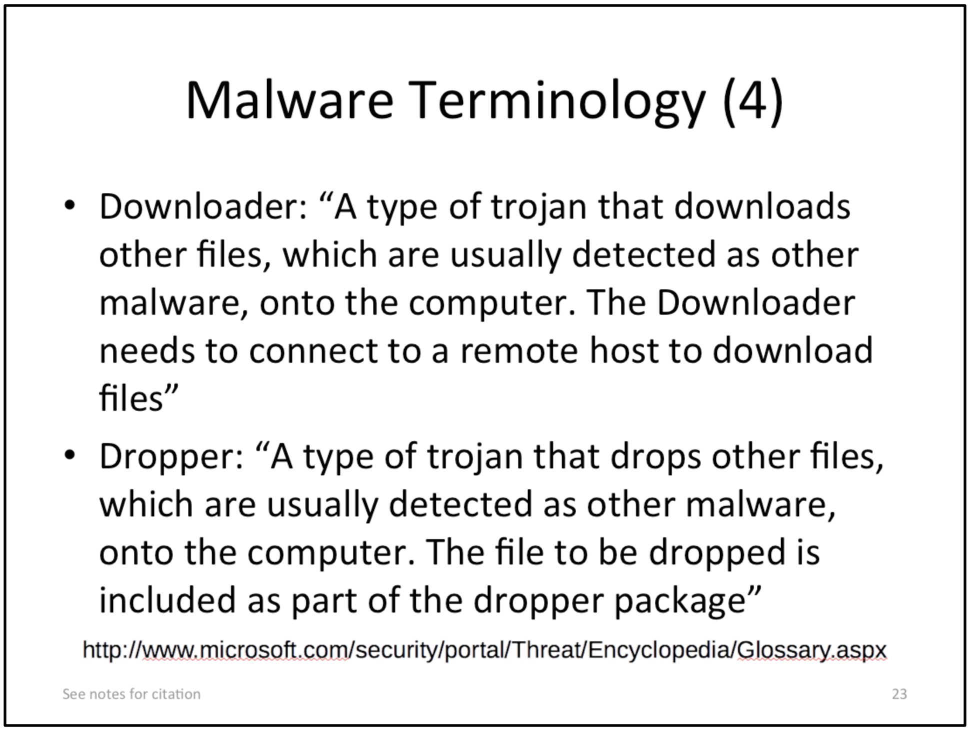
Malware Terminology (3)

- Bot: “A malicious program installed on a computer that is part of a bot network (botnet). Bots are generally backdoor trojans that allow unauthorized access and control of an affected computer. They are often controlled via IRC from a centralized location (although other models of command and control exist).”

  http://www.microsoft.com/security/portal/Threat/Encyclopedia/Glossary.aspx

- Remote Administration Tool (RAT): “A piece of software that allows a remote "operator" to control a system as if he has physical access to that system.”

  http://en.wikipedia.org/wiki/Remote_administration_software

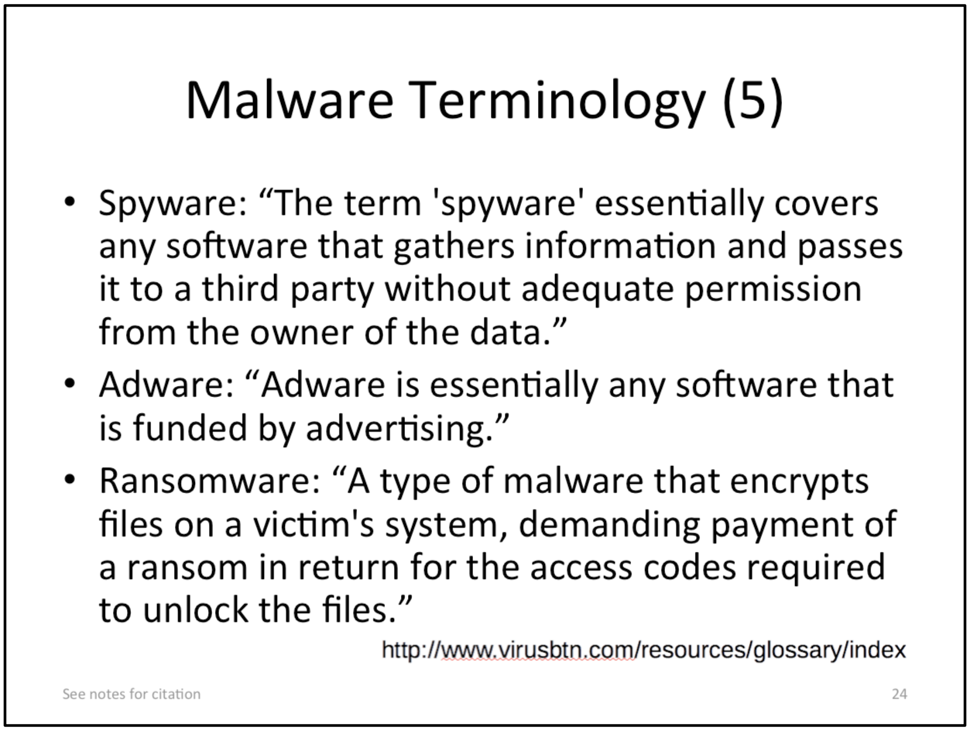


Malware Terminology (4)

- Downloader: “A type of trojan that downloads other files, which are usually detected as other malware, onto the computer. The Downloader needs to connect to a remote host to download files”
- Dropper: “A type of trojan that drops other files, which are usually detected as other malware, onto the computer. The file to be dropped is included as part of the dropper package”

http://www.microsoft.com/security/portal/Threat/Encyclopedia/Glossary.aspx

See notes for citation

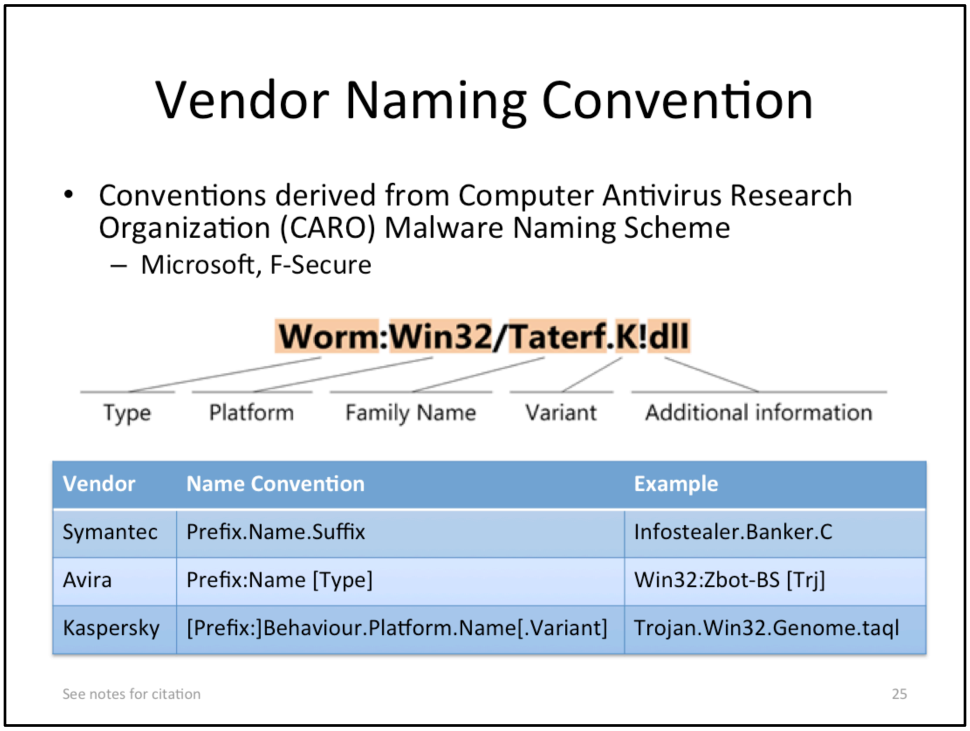


Malware Terminology (5)

- Spyware: “The term 'spyware' essentially covers any software that gathers information and passes it to a third party without adequate permission from the owner of the data.”
- Adware: “Adware is essentially any software that is funded by advertising.”
- Ransomware: “A type of malware that encrypts files on a victim's system, demanding payment of a ransom in return for the access codes required to unlock the files.”

http://www.virusbtn.com/resources/glossary/index

See notes for citation



Vendor Naming Convention

- Conventions derived from Computer Antivirus Research Organization (CARO) Malware Naming Scheme
  - Microsoft, F-Secure

Worm:Win32/Taterf.K!dll

Type Platform Family Name Variant Additional information

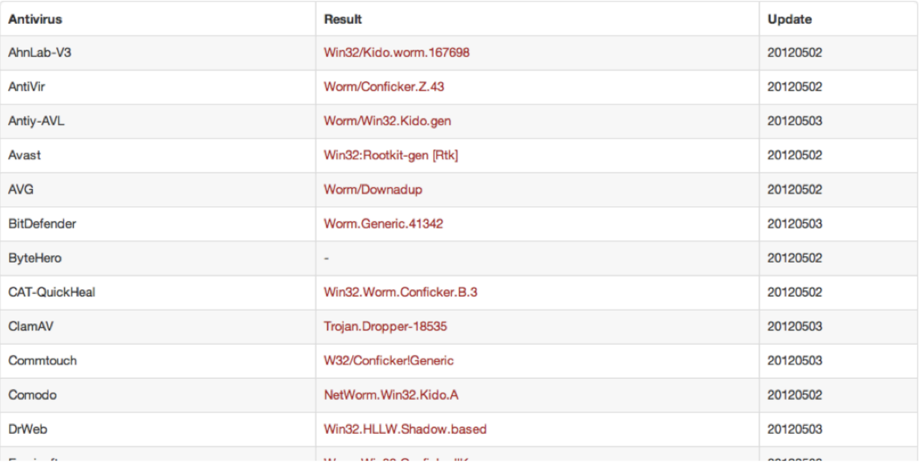
Vendor	Name Convention	Example
Symantec	Prefix.Name.Suffix	Infostealer.Banker.C
Avira	Prefix:Name [Type]	Win32:Zbot-BS [Trj]
Kaspersky	[Prefix:]Behaviour.Platform.Name[.Variant]	Trojan.Win32.Genome.taql

See notes for citation

[References]

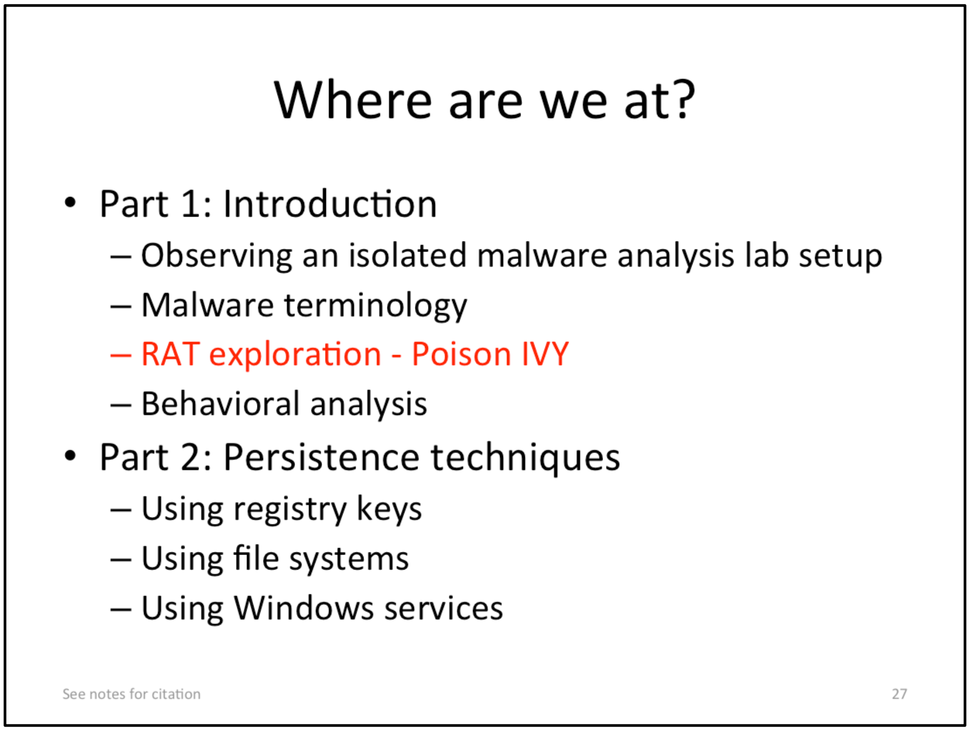
- Microsoft Malware Protection Center Naming Standards, http://www.microsoft.com/security/portal/Shared/MalwareNaming.aspx
- Virus Naming Conventions, http://www.symantec.com/security_response/virusnaming.jsp
- Michal Krejdl, What to imagine behind Win32:MalOb [Cryp], https://blog.avast.com/2009/07/29/what-to-imagine-behind-win32malob-cryp/
- Rules for naming detected objects, http://www.securelist.com/en/threats/detect?chapter=136

Non-standardized Naming Scheme



Antivirus	Result	Update
AhnLab-V3	Win32/Kido.worm.167698	20120502
AntiVir	Worm/Conficker.Z.43	20120502
Antiy-AVL	Worm/Win32.Kido.gen	20120503
Avast	Win32:Rootkit-gen [Rtk]	20120502
AVG	Worm/Downadup	20120502
BitDefender	Worm.Generic.41342	20120503
ByteHero	-	20120502
CAT-QuickHeal	Win32.Worm.Conficker.B.3	20120502
ClamAV	Trojan.Dropper-18535	20120503
Commtouch	W32/Conficker!Generic	20120503
Comodo	NetWorm.Win32.Kido.A	20120502
DrWeb	Win32.HLLW.Shadow.based	20120503

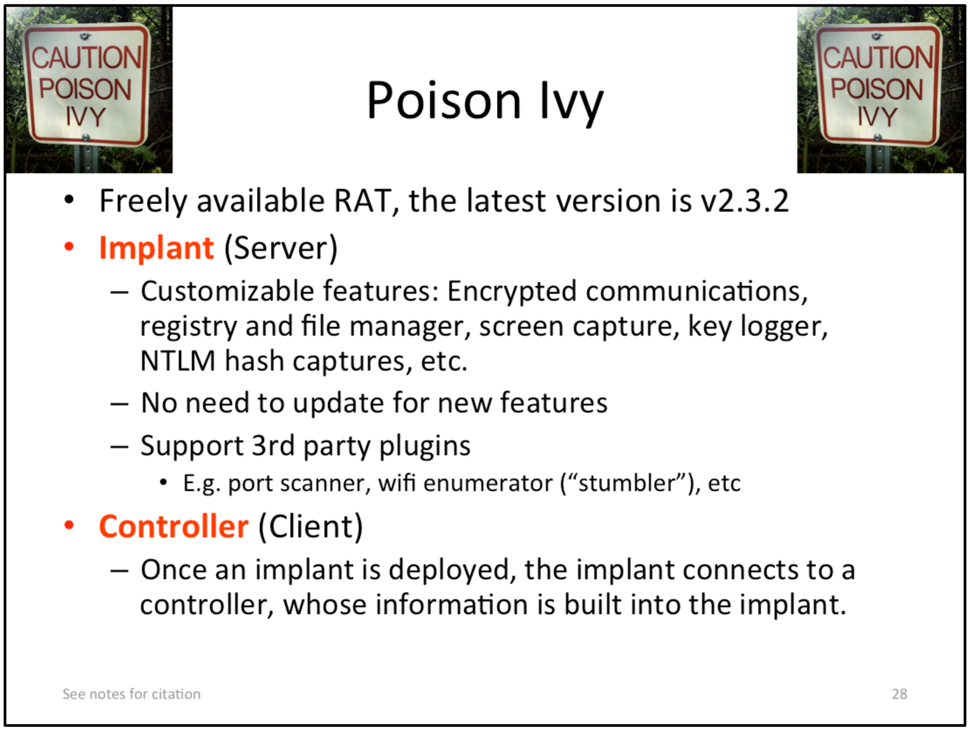
A result of a Conficker sample at https://www.virustotal.com



Where are we at?

- Part 1: Introduction
  - Observing an isolated malware analysis lab setup
  - Malware terminology
  - RAT exploration - Poison IVY
  - Behavioral analysis
- Part 2: Persistence techniques
  - Using registry keys
  - Using file systems
  - Using Windows services

See notes for citation



Poison Ivy

CAUTION
POISON
IVY

- Freely available RAT, the latest version is v2.3.2
- **Implant** (Server)
  - Customizable features: Encrypted communications, registry and file manager, screen capture, key logger, NTLM hash captures, etc.
  - No need to update for new features
  - Support 3rd party plugins
    - E.g. port scanner, wifi enumerator (“stumbler”), etc
- **Controller** (Client)
  - Once an implant is deployed, the implant connects to a controller, whose information is built into the implant.

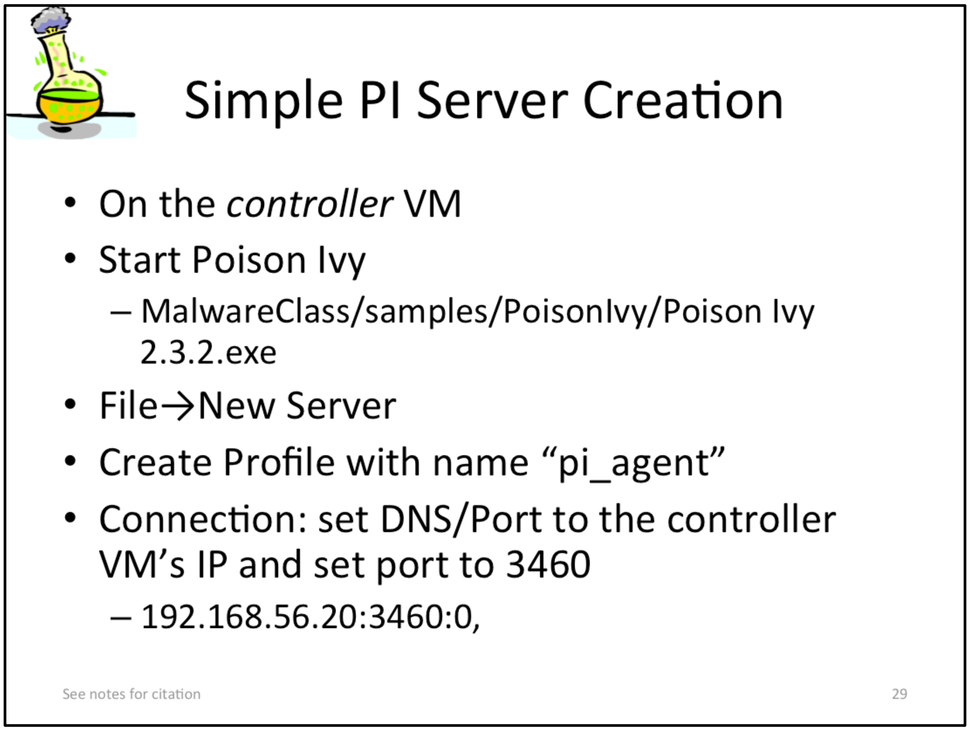
See notes for citation

[References]

- Poison Ivy – Remote Administration Tool, http://www.poisonivy-rat.com/

[Image Sources]

- http://25.media.tumblr.com/tumblr_m83rfveJWO1r6dcg4o1_500.jpg

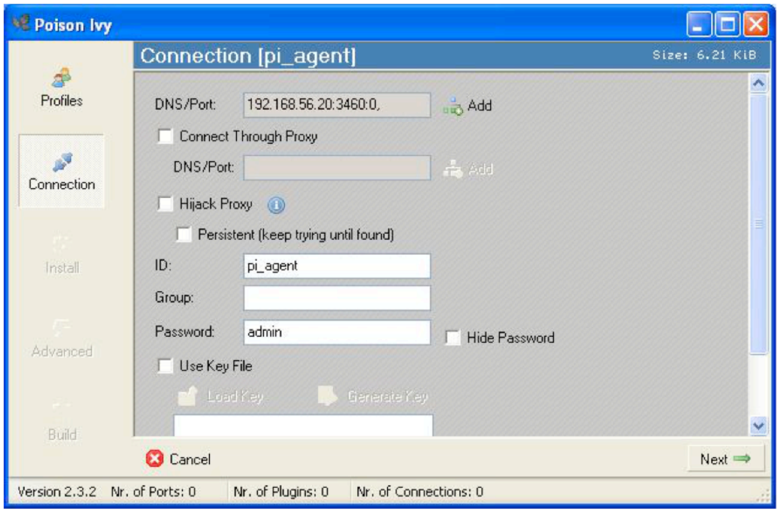


Simple PI Server Creation

- On the *controller* VM
- Start Poison Ivy
  - – MalwareClass/samples/PoisonIvy/Poison Ivy 2.3.2.exe
- File→New Server
- Create Profile with name “pi_agent”
- Connection: set DNS/Port to the controller VM’s IP and set port to 3460
  - – 192.168.56.20:3460:0,

See notes for citation

Connection



Poison Ivy

Connection [pi_agent]

Size: 6.21 KiB

DNS/Port: 192.168.56.20:3460:0,

□ Connect Through Proxy

DNS/Port:

□ Hijack Proxy

□ Persistent (keep trying until found)

ID: pi_agent

Group:

Password: admin

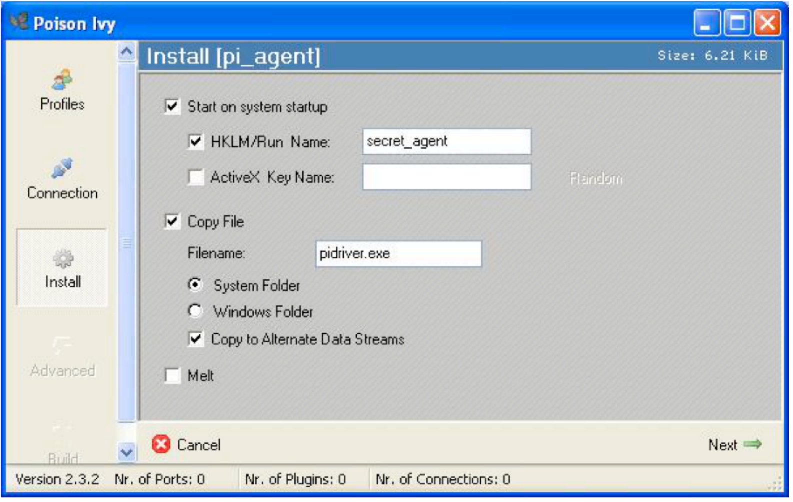
□ Hide Password

□ Use Key File

Version 2.3.2 Nr. of Ports: 0 Nr. of Plugins: 0 Nr. of Connections: 0

See notes for citation

Install



Poison Ivy

Install [pi_agent]

Size: 6.21 KiB

☑ Start on system startup

☑ HKLM/Run Name: secret_agent

□ ActiveX Key Name:

☑ Copy File

Filename: pidriver.exe

● System Folder

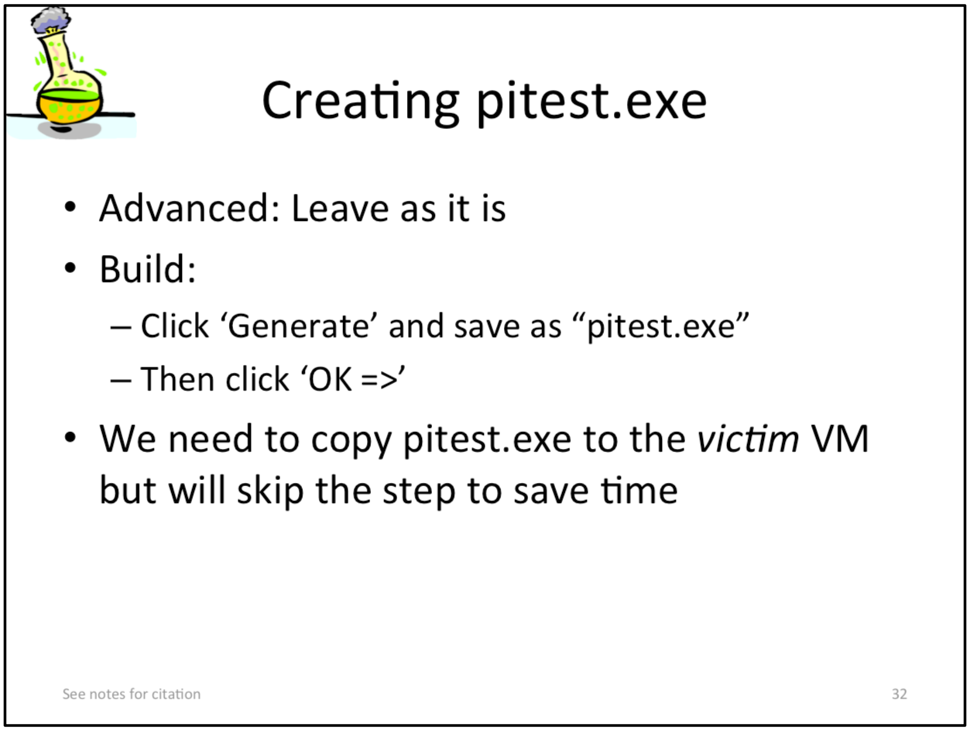
○ Windows Folder

☑ Copy to Alternate Data Streams

□ Melt

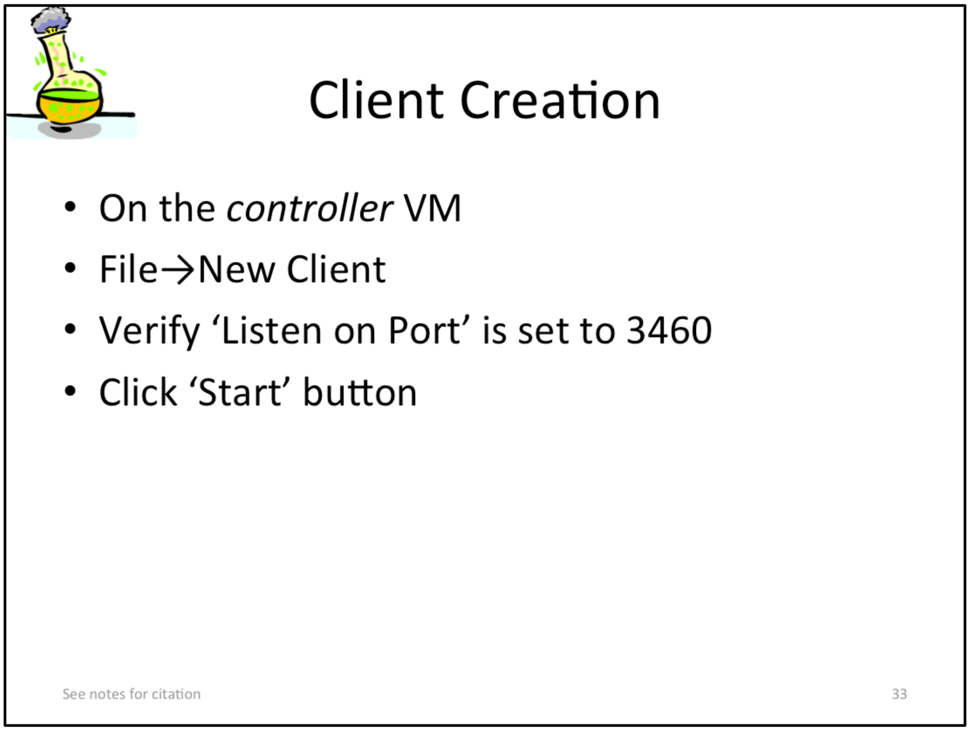
Version 2.3.2 | Nr. of Ports: 0 | Nr. of Plugins: 0 | Nr. of Connections: 0

See notes for citation



Creating pitest.exe

- Advanced: Leave as it is
- Build:
  - – Click ‘Generate’ and save as “pitest.exe”
  - – Then click ‘OK =>’
- We need to copy pitest.exe to the *victim* VM but will skip the step to save time



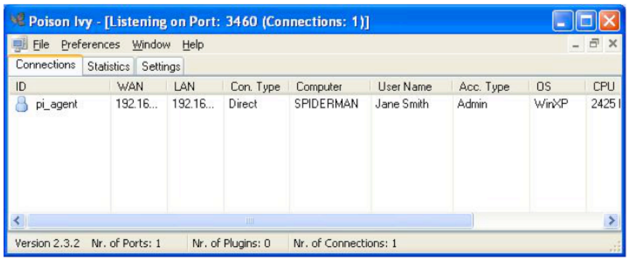
Client Creation

- On the *controller* VM
- File→New Client
- Verify ‘Listen on Port’ is set to 3460
- Click ‘Start’ button

See notes for citation

Executing Poison Ivy Implant

- On the *victim* VM
  - Execute the already prepared PI server (MalwareClass/samples/PoisonIvy/pi_agent.exe)
- Once a server connects to the client, you will see the following entry on the *controller* VM

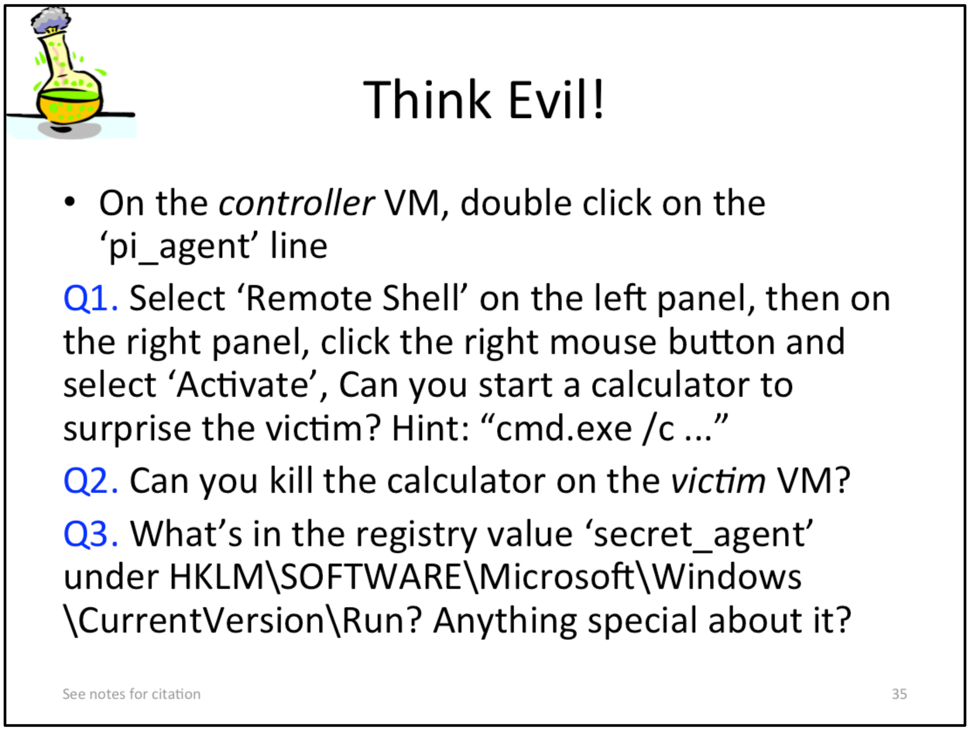


Poison Ivy - [Listening on Port: 3460 (Connections: 1)]

ID	WAN	LAN	Con. Type	Computer	User Name	Acc. Type	OS	CPU
pi_agent	192.16...	192.16...	Direct	SPIDERMAN	Jane Smith	Admin	WinXP	2425 I

Version 2.3.2 Nr. of Ports: 1 Nr. of Plugins: 0 Nr. of Connections: 1

See notes for citation



Think Evil!

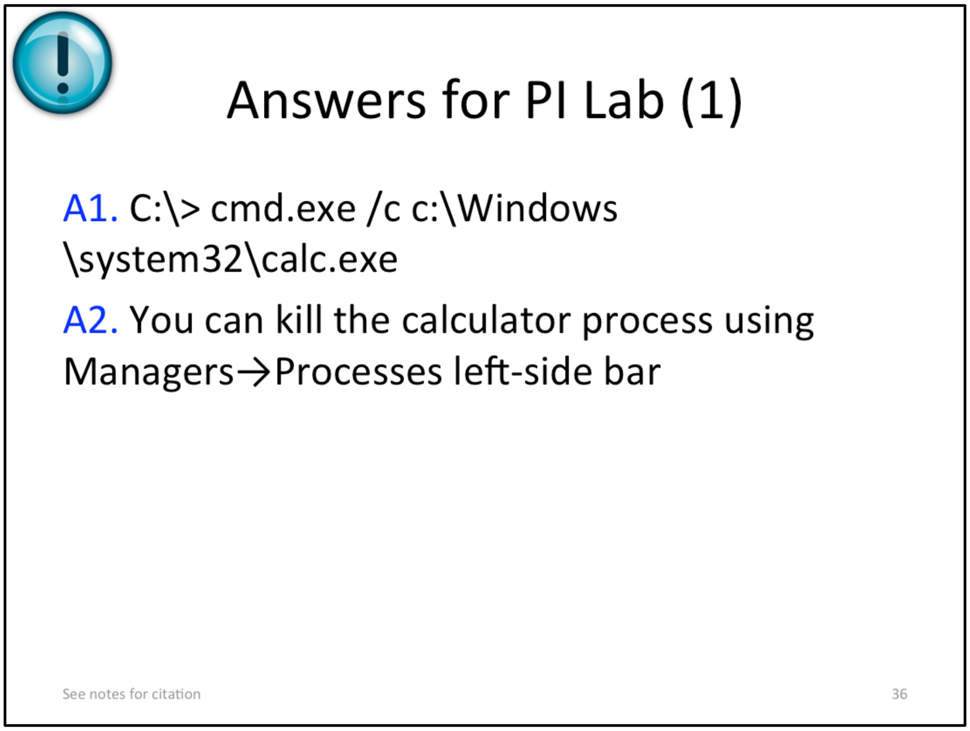
- On the *controller* VM, double click on the ‘pi_agent’ line

Q1. Select ‘Remote Shell’ on the left panel, then on the right panel, click the right mouse button and select ‘Activate’, Can you start a calculator to surprise the victim? Hint: “cmd.exe /c ...”

Q2. Can you kill the calculator on the *victim* VM?

Q3. What’s in the registry value ‘secret_agent’ under HKLM\SOFTWARE\Microsoft\Windows \CurrentVersion\Run? Anything special about it?

See notes for citation

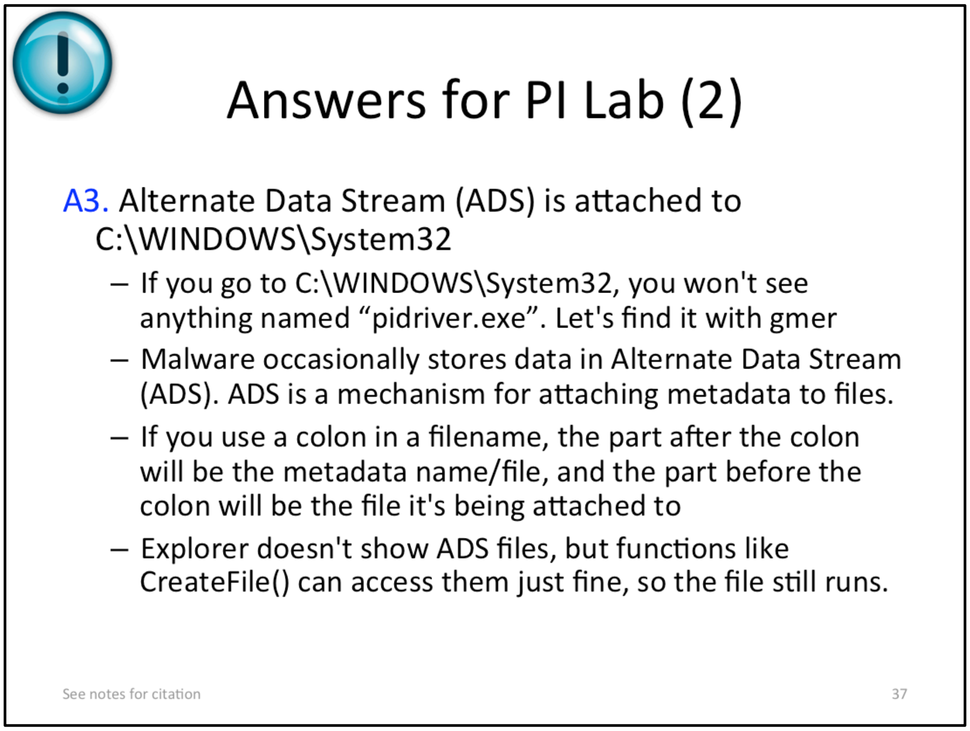


Answers for PI Lab (1)

A1. C:\> cmd.exe /c c:\Windows \system32\calc.exe

A2. You can kill the calculator process using Managers→Processes left-side bar

See notes for citation



Answers for PI Lab (2)

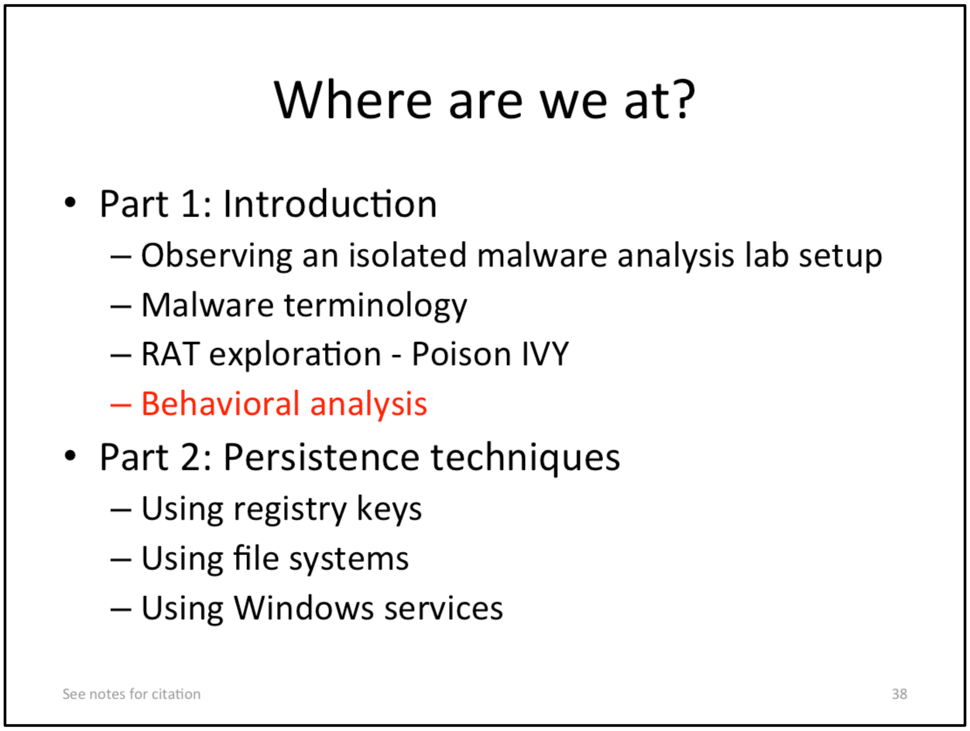
A3. Alternate Data Stream (ADS) is attached to C:\WINDOWS\System32

- If you go to C:\WINDOWS\System32, you won't see anything named “pidriver.exe”. Let's find it with gmer
- Malware occasionally stores data in Alternate Data Stream (ADS). ADS is a mechanism for attaching metadata to files.
- If you use a colon in a filename, the part after the colon will be the metadata name/file, and the part before the colon will be the file it's being attached to
- Explorer doesn't show ADS files, but functions like CreateFile() can access them just fine, so the file still runs.

See notes for citation

[References]

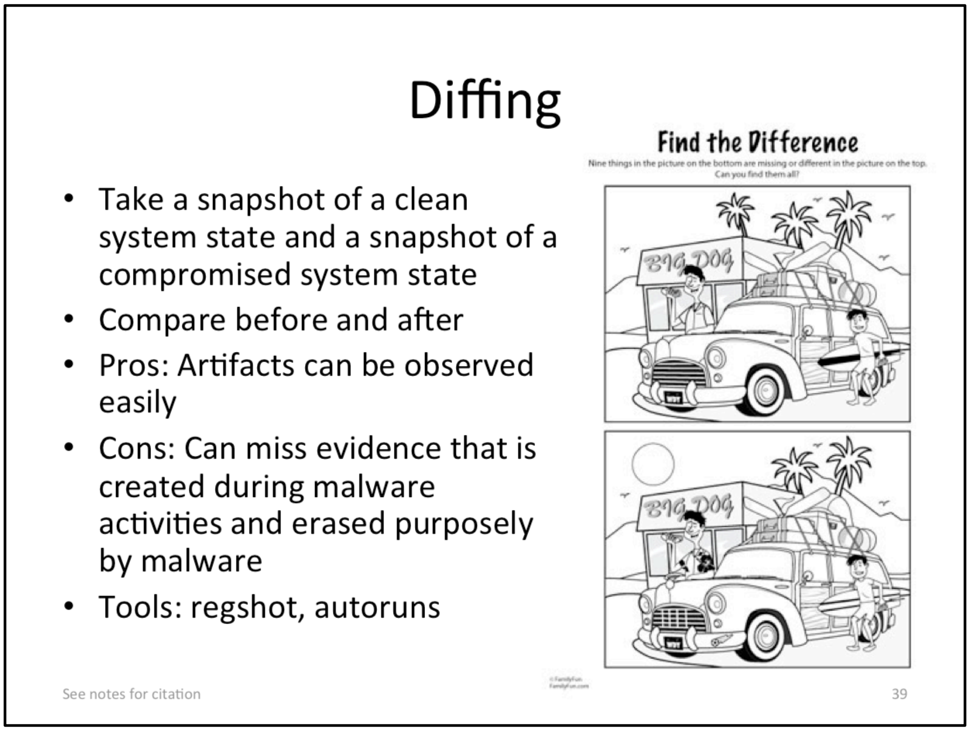
- GMER, http://www.gmer.net/
- AlternateStreamView, http://www.nirsoft.net/utils/alternate_data_streams.html



Where are we at?

- Part 1: Introduction
  - Observing an isolated malware analysis lab setup
  - Malware terminology
  - RAT exploration - Poison IVY
  - Behavioral analysis
- Part 2: Persistence techniques
  - Using registry keys
  - Using file systems
  - Using Windows services

See notes for citation



Diffing

- Take a snapshot of a clean system state and a snapshot of a compromised system state
- Compare before and after
- Pros: Artifacts can be observed easily
- Cons: Can miss evidence that is created during malware activities and erased purposely by malware
- Tools: regshot, autoruns

Find the Difference
Nine things in the picture on the bottom are missing or different in the picture on the top. Can you find them all?
BIG DOG
BIG DOG
© FamilyFun
FamilyFun.com

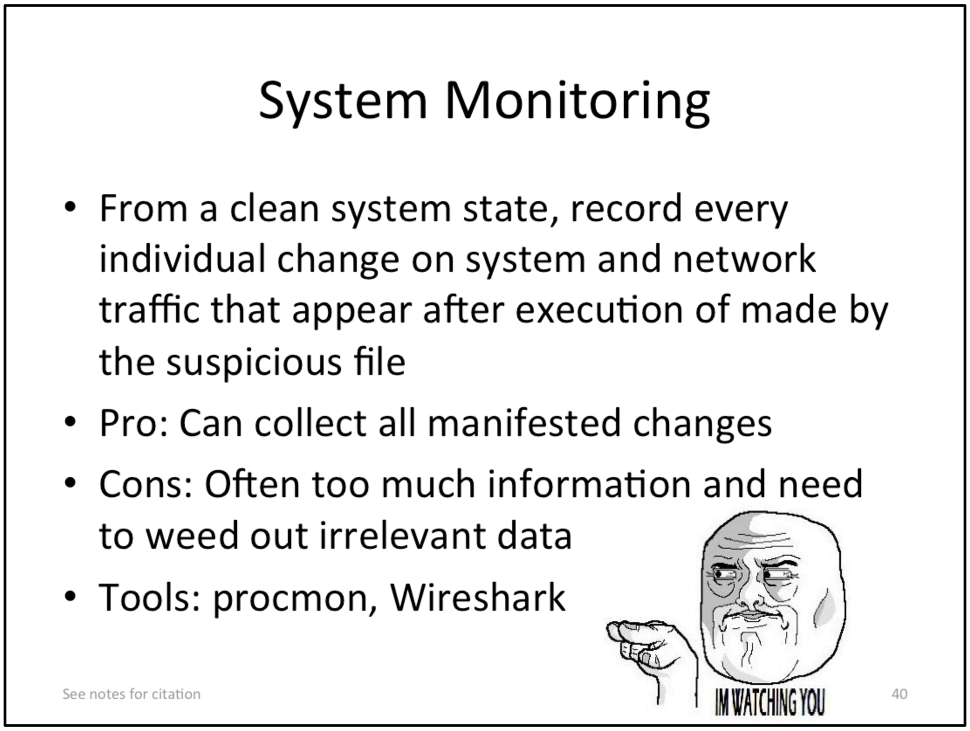
See notes for citation

[References]

- Regshot, http://code.google.com/p/regshot/
- Mark Russinovich et al., Autoruns, http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx

[Image Sources]

- http://familyfun.go.com/assets/cms/printables/0707c_findthedifference.jpg



System Monitoring

- From a clean system state, record every individual change on system and network traffic that appear after execution of made by the suspicious file
- Pro: Can collect all manifested changes
- Cons: Often too much information and need to weed out irrelevant data
- Tools: procmon, Wireshark

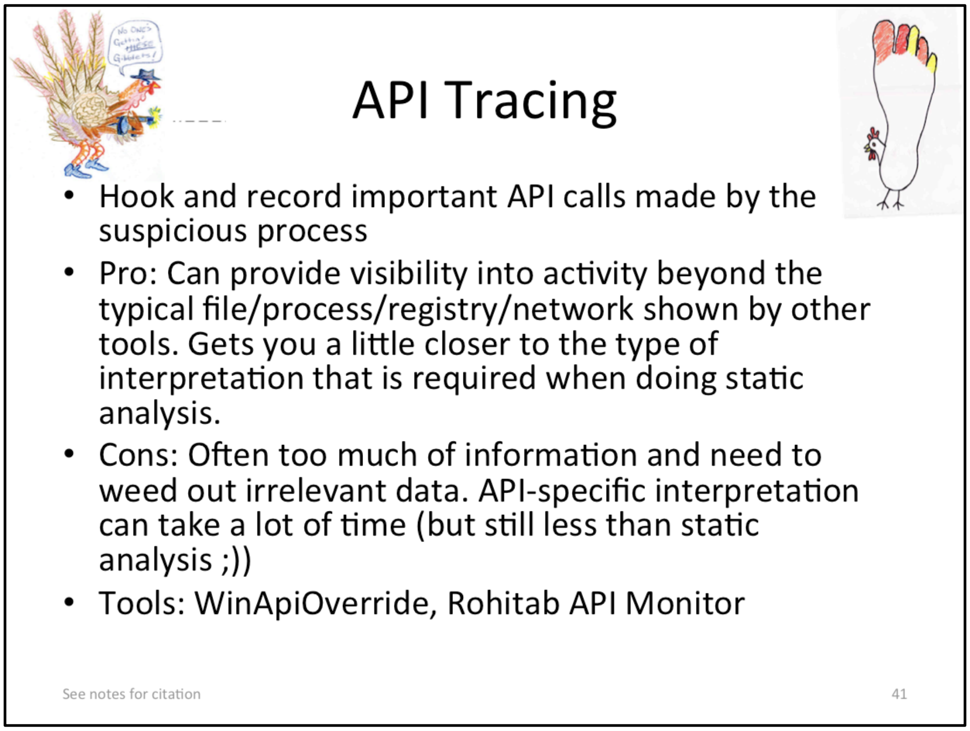
IM WATCHING YOU

See notes for citation

40

[Image Sources]

- http://i1.kym-cdn.com/entries/icons/original/000/007/195/im%20watching%20you%20-%20copia.jpg



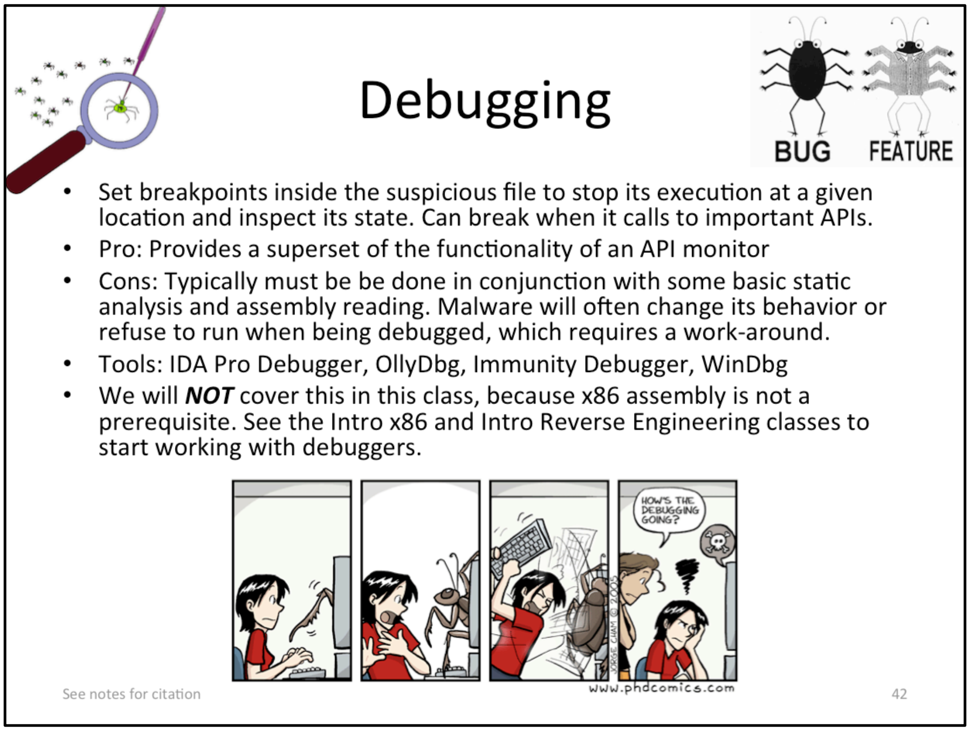
API Tracing

- Hook and record important API calls made by the suspicious process
- Pro: Can provide visibility into activity beyond the typical file/process/registry/network shown by other tools. Gets you a little closer to the type of interpretation that is required when doing static analysis.
- Cons: Often too much of information and need to weed out irrelevant data. API-specific interpretation can take a lot of time (but still less than static analysis ;))
- Tools: WinApiOverride, Rohitab API Monitor

See notes for citation

[References]
- WinAPIOverride, http://jacquelin.potier.free.fr/winapioverride32/
- API Monitor, http://www.rohitab.com/apimonitor

[Image Sources]
- Left, http://fc03.deviantart.net/fs39/f/2008/332/c/d/HAND_TURKEY_by_Bilious.jpg
- Right, http://dorpahdoo.files.wordpress.com/2010/11/foot-turkey.jpg



Debugging

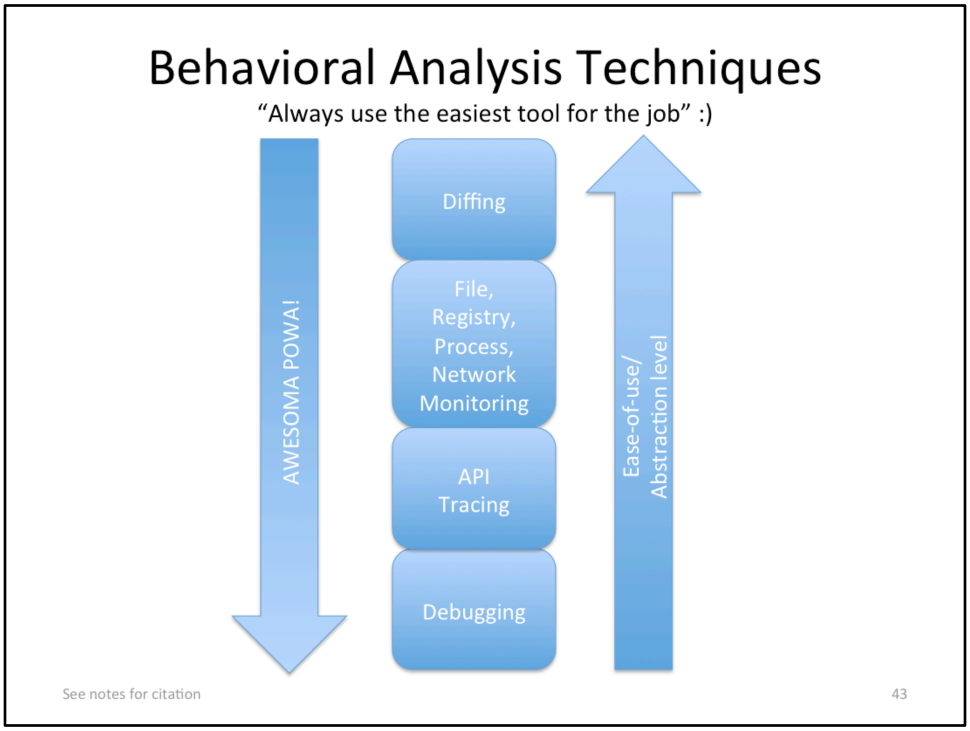
- Set breakpoints inside the suspicious file to stop its execution at a given location and inspect its state. Can break when it calls to important APIs.
- Pro: Provides a superset of the functionality of an API monitor
- Cons: Typically must be be done in conjunction with some basic static analysis and assembly reading. Malware will often change its behavior or refuse to run when being debugged, which requires a work-around.
- Tools: IDA Pro Debugger, OllyDbg, Immunity Debugger, WinDbg
- We will ***NOT*** cover this in this class, because x86 assembly is not a prerequisite. See the Intro x86 and Intro Reverse Engineering classes to start working with debuggers.

See notes for citation

42

[Image Sources]

- Top left, http://www.wpclipart.com/computer/humour/debugging.png
- Top right, http://www.phdcomics.com/comics/archive/phd011406s.gif
- Bottom, http://www.oraclealchemist.com/wp-content/uploads/2008/07/bug-feature.jpg



Behavioral Analysis Techniques

“Always use the easiest tool for the job” :)

AWESOMA POWA!

Diffing

File, Registry, Process, Network Monitoring

API Tracing

Debugging

Ease-of-use/ Abstraction level

See notes for citation

43