

Malware Dynamic Analysis

Veronica Kovah
vkovah.ost at gmail

<http://opensecuritytraining.info/MalwareDynamicAnalysis.html>

See notes for citation

1

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 licens or (but not in any way that suggests that they endorse you or your use of the work).



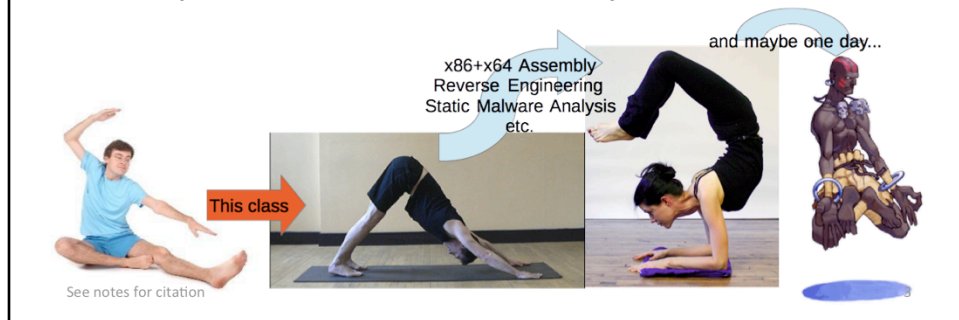
Share Alike — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same, similar or a compatible license.

See notes for citation

2

This class is for people

- Who are interested in computer security
- Who want to understand how malware works
- Who want to start working on malware analysis, or who have recently started



[Image Sources]

- Left, <http://test3-img.ehowcdn.com/article-new/ehow/images/a01/vv/m9/start-yoga-as-male-beginner-800x800.jpg>
- Middle-left, http://www.bbc.co.uk/northyorkshire/content/images/2006/04/05/downward_dog_400x300.jpg
- Middle-right, <http://www.spiritualhealingportal.com/images/photo/yoga9.jpg>
- Right, http://media.giantbomb.com/uploads/0/3/665089-a2dhalsim_thumb.png

 Thanks to 



- Xeno Kovah, Ben Schmoker and Frank Poz for reviewing class materials
- Ezra Moses, MITRE Institute tech support for setting up Ubuntu on the lab machines
- Openmalware.org (offensivecomputing.net) for sharing samples, very good resource

See notes for citation

4

[Image Sources]

- Top, <http://www.thirdcoastrs.com/AP-353%20ASIAN%20GNOME%20-%20BOWING%204web.jpg>
- Middle, http://thumbs.dreamstime.com/thumblarge_510/127589357290776N.jpg

About me and you

- BE in CS and MS in CE (but mostly CS background)
- Security related work experience:
 - Malware analysis and analysis tool development
 - Security product reverse engineering
 - Windows memory integrity measurement/verification
 - Vulnerability research
 - Network IDS/IPS signature development
- Like hands-on work (coding, debugging, and reversing)
- How about you? Any particular topic that you want to learn from this class?

Outline (1)



- 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

6

[Image Sources]

- <http://domaingang.com/wp-content/uploads/2012/10/domain-list.jpg>

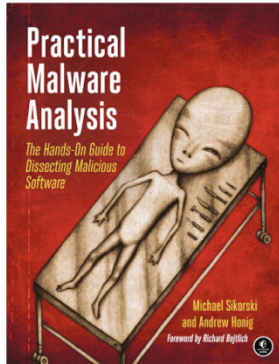
Outline (2)

- Part 3: Maneuvering techniques
 - (How malware strategically positions itself to access critical resources)
 - DLL/code injection
 - DLL search order hijacking...
- Part 4: Malware functionality
 - Keylogging, Phone home, Security degrading, Self-destruction, etc.

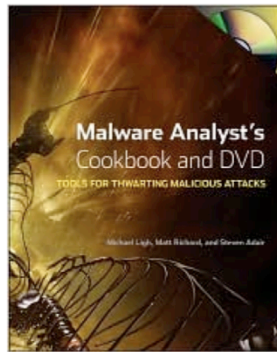
Outline (3)

- Part 5: Using an all-in-one sandbox
 - Cuckoo Sandbox
 - Malware Attribute Enumeration and Characterization (MAEC)
 - Different sandbox results comparison
- Part 6: Actionable output
 - Yara
 - Snort

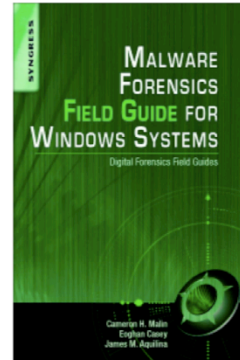
Books



Michael Sikorski
Andrew Honig



Michael Ligh
Steven Adair
Blake Hartstein
Matthew Richard



Cameron H. Malin
Eoghan Casey
James M. Aquilina



See notes for citation

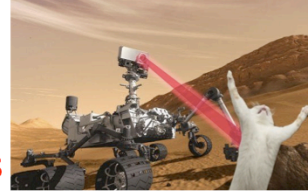
9

[Image Sources]

- Left, http://nostarch.com/sites/default/files/imagecache/product_main_page/practical_malware_analysis.png
- Middle, <http://img2.imagesbn.com/images/77180000/77183529.JPG>
- Right, <http://secure-ecsd.elsevier.com/covers/80/Tango2/large/9781597494724.jpg>

Class Conventions (1)

- Slides with  on the left corner means we will perform hands-on lab activities
- Slides with  include answers to lab questions, which often follows lab slides.
Please do not read the answers before you finish a lab ;)
- Slides with a green bar on top means it's background context



See notes for citation

10

[Image Sources]

- Top, http://thetalentcode.com/wp-content/uploads/119498535838791757esperimento_chimico_arch_01.svg_med.png
- Middle, Microsoft clip art
- Right, http://static.fjcdn.com/pictures/Curiosity+killed+the+cat.+source+smosh+facebook+page_06d5f5_3980829.jpg

Class Conventions (2)

- Lines starting with
 - `C:\>` means, you are asked to type in a DOS window on the Windows XP VM but it does not mean the command needs to be executed at the top level
 - `$` means, you are asked to type in a Linux terminal on the Ubuntu host machine

Class Materials

- On the Ubuntu host machine
 - \$ cd ~/MalwareClass && ls
 - \$ cd ~/Updates && ls
 - \$ virtualbox &
- On the *victim* VM
 - On Desktop, open MalwareClass directory
- Please see Notes for citation and check out the original works