Malware Dynamic Analysis
Part 5

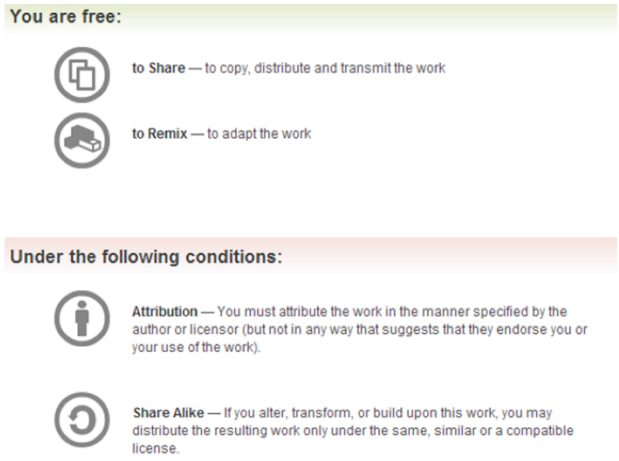
Veronica Kovah
vkovah.ost at gmail

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/



See notes for citation

2

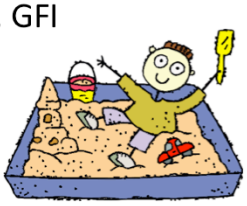
Where are we at?

- 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

See notes for citation

Malware Analysis Sandbox

- Provides file system, registry keys, and network traffic monitoring in controlled environment and produces a well formed report
- Using a sandbox is more efficient and sometimes more effective
- Configure your own sandbox such as Joebox, GFI Sandbox, and Cuckoo Sandbox.
- Use public sandbox such as ThreatExpert, GFI ThreatTrack, and Anubis
  - Do not submit malware to a public sandbox if it reveals sensitive information about your organization and/or customer.



See notes for citation

4

[References]

- Joe Sandbox, http://www.joesecurity.org/index.php/joe-sandbox-standalone
- GFI Sandbox, http://www.gfi.com/malware-analysis-tool
- Cuckoo Sandbox, http://www.cuckoosandbox.org
- ThreatExpert, http://www.threatexpert.com/submit.aspx
- GFI ThreaetTrack, http://www.threattrack.com/
- Anubis, http://anubis.iseclab.org/

[Image Sources]

- http://plannerwire.net/wp-content/uploads/2011/02/Playing-Sandbox_meeting_planners.gif

Cuckoo Sandbox

- Open source automated malware analysis system
- Analyzes PE, PDF, MS Office, PHP scripts, etc.
- Outputs JSON/HTML/MAEC reports
- Customization
  - Machinery Modules: virtualization software
  - Analysis Package: how to conduct the analysis procedure
  - Processing Modules: how to analyze raw results
  - Signatures
  - Reporting Modules
  - Auxiliary Modules: to be executed in parallel to every analysis

See notes for citation 5

[References]

- Cuckoo Sandbox Book, http://docs.cuckoosandbox.org/en/latest

[Image Sources]

- http://www.cuckoosandbox.org/graphic/cuckoo.png

Poison Ivy

- Revert the *victim* VM to "cuckoo" snapshot
- Open three terminals
- Terminal #1, run inetsim
  - $ sudo inetsim
- Terminal #2, run Cuckoo Sandbox v1.0
  1) $ cd ~/MalwareClass/tools/cuckoo
  2) Edit conf/auxiliary.conf (to sniff on vboxnet1)
  3) $ python ./cuckoo.py
- Terminal #3, submit piagent.exe to Cuckoo
  1) $ cd ~/MalwareClass/tools/cuckoo/utils
  2) $ python ./submit.py~/MalwareClass/samples/PoisonIvy/piagent.exe

See notes for citation

Cuckoo Sandbox Results

- Task results are generated under {Cuckoo Root}/storage/analysis/[task number]/
  - {Cuckoo Root} = ~/MalwareClass/tools/cuckoo
  - *reports* directory includes reports in different formats
  - *logs* directory includes raw data named <process id>.bson
  - *shots* directory includes screen shots
  - *files* directory includes dropped files. You can then run dropped executables through on their own
- Submitted sample will be copied to {Cuckoo Root}/storage/binaries/MD5NAME, where MD5NAME is the md5 of the submitted sample
  - A symbolic link (named *binary*) exists under the task result directory

See notes for citation

Poison Ivy Results

- $ cd ~/MalwareClass/tools/cuckoo/storage/analysis/1/reports
- $ firefox report.html &
- $ gedit report.json &
- $ firefox report.maec-4.0.1.xml &

See notes for citation

Malware Attribute Enumeration and Characterization (MAEC)

- "a standardized language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns"

https://maec.mitre.org/about/index.html

- A standard is necessary to provide a common way to share malware analysis results among organizations to avoid duplicate, inaccurate work

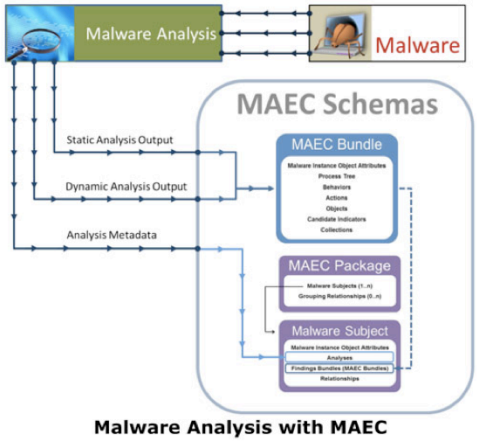
See notes for citation 9

[References]

- MAEC, https://maec.mitre.org

MAEC (2)

- Supported tools
  - Native: Cuckoo Sandbox
  - Via a translator: Anubis, ThreatTrack, ThreatExpert
- Would be very useful to search openmalware.org samples based on attributes, could make a new search engine: "Ask MAEC!"



Malware Analysis with MAEC

See notes for citation

10

[References]

- MAEC Use Cases, http://maec.mitre.org/language/usecases.html
- MAEC in Use, http://maec.mitre.org/about/inuse.html

[Image Sources]

- http://maec.mitre.org/language/images/usecases-1.jpg

Parite (1) – Cuckoo v1.0

- We will learn how to interpret a sandbox's results based on what we have learned so far
- Submit parite sample to Cuckoo Sandbox v1.0
  1) $ cd ~/MalwareClass/tools/cuckoo/utils
  2) $ python submit.py ~/MalwareClass/samples/parite/malware.exe
- Kill the cuckoo.py process with ctrl-c once the analysis is done

Parite (2) - Cuckoo v0.5

- Install Cuckoo Sandbox v0.5's agent on the *victim* VM
  - Copy agent.py from the host machine to the *victim* VM
    - Use WinSCP on the *victim* VM
    - It's located at ~/Updates/cuckoo/agent/agent.py in the host machine
    - Open a DOS terminal and start the agent C:\python27\python.exe c:\agent.py
  - Make a snapshot with the name "cuckoo05"

See notes for citation

Parite (3) - Cuckoo v0.5

- Terminal #2, run Cuckoo Sandbox v0.5
  1) $ cd ~/Updates/cuckoo
  2) $ python ./cuckoo.py
- Terminal #3, submit parite sample to Cuckoo
  1) $ cd ~/Updates/cuckoo/utils
  2) $ python submit.py ~/MalwareClass/samples/parite/malware.exe

See notes for citation

Parite (4)

- Consult public sandbox results as well under ~/Updates/public_sandbox_results/parite/
  - anubis: $ evince ./anubis/report.pdf
  - threatexpert: $ firefox ./threatexpert/report.html
  - threattrack: $ evince ./threattrack/analysis.pdf

Q1. ~~(SKIP) Does this drop files with randomized names?~~

Q2. How does it persist?

Q3. How does it maneuver?

Q4. Does it have self-avoidance?

Q5. Does it self-destruct?

Q6. Where does it try to connect to?

Answers for Parite Lab (1)

A2.

- Created “Run” registry value HKLM\Software\Microsoft\Windows \CurrentVersion\RUN\fmsiocps to “C:\Windows\fmsiocps.exe”
- Modified “AppInit_Dlls” registry value HKLM\Software\Microsoft\Windows NT \CurrentVesion\Windows\AppInit_Dlls to “fmsiocps.dll”

See notes for citation

Answers for Parite Lab (2)

A3.

- Dll injection via AppInit_Dlls
- Dll injection using CreateRemoteThread() API
  - OpenProcess (PID=1760)→VirtualAllocEx → NtWriteVirtualMemory →CreateRemoteThread
  - Now you are interested in the process name of PID 1760 :D

A4. Yes, mutex “Residented” is created

A5. Yes, the submitted sample file was deleted

A6. 192.5.5.241 (per ThreatExpert result)

See notes for citation

16

Nitol

- Consult “Parite” lab slides for how to submit the sample to both versions of Cuckoo Sandbox and answer the following questions about Nitol:

Q1. ~~(SKIP) Does this drop files with randomized names?~~

Q2. How does it persist?

Q3. How does it maneuver?

Q4. Does it have self-avoidance?

Q5. Does it do self-destruction?

Q6. Where does it try to connect to?

See notes for citation

Answers for Nitol (1)

A2.

1) Registered an auto-start service
   – HKLM\System\CurrentControlSet\Services \Distribuijq
2) Created lpk.dll under multiple directories for DLL search order hijacking; this technique also makes the malware persistent

A3. DLL search order hijacking (lpk.dll)

See notes for citation

Answers for Nitol (2)

A4. Yes, Distribuijq (per ThreatExpert result)

- ShimCacheMutex is opened by side effect

A5. Yes, it moves itself to
C:\DOCUME~1\student\LOCALS~1\Temp\SOFTWARE.LOG

A6. tutwl.3322.org

- Microsoft took down the entire 3322.org (google "Operation b70") but they came back online after agreeing to clean out malware users

See notes for citation

19

[References]

- Andrew Davis, Leveraging the Application Compatibility Cache in Forensic Investigations, https://dl.mandiant.com/EE/library/Whitepaper_ShimCacheParser.pdf

IMworm

- Consult “Parite” lab slides for how to submit the sample to both versions of Cuckoo Sandbox and answer the following questions about IMworm:

Q1. ~~(SKIP) Does this drop files with randomized names?~~

Q2. What's the file's original name?

Q3. How does it persist?

Q4. Does it have self-avoidance?

Q5. Does it do self-destruction?

Q6. Where does it try to connect to?

See notes for citation

20

Answers for IMworm (1)

A2. worm2007.exe

A3. Using file system and registry key

- Created C: \Document and Settings\All Users\Start Menu\Programs\Startup\MSconfig.exe, which is a copy of the malware itself
- Set registry values HKLM\SOFTWARE\Microsoft\Windows NT \CurrentVersion\Winlogon\Userinit & Shell to C:\Windows\system\lsass.exe, which is a copy of the malware itself

Answers for IMworm (2)

A4. No apparent mutex

– ShimCacheMutex is opened by side effect

A5. No apparent self-destruction

A6. Tried to get http://quicknews.info/YMWorm.exe

See notes for citation