Building Your Own Automated Malware Analysis Lab for Insights on Active Threats

Kurtis Armour

November 15, 2017
New talk - Who dis?

- whoami
  - Kurtis Armour
  - @S3Ns3

- I do security stuff
  - 6 years in the security space
  - Penetration Testing, Endpoint Security, Vulnerability Management

- Interested in security research around attacking and defending environments
Introduction

- The goal of this talk
- Education about the threat landscape
- Malware analysis environments
- Making use of in-house labs
Threat Landscape
Threat Landscape

▪ What type of cyber attacks are targeting the users in your organization?
  ▪ Malware – delivered via:
    ▪ Exploitation – Malvertising, Exploit Kits, Drive-by Downloads
    ▪ Social Engineering – Phishing Emails

▪ What can be learned from these attacks?
  ▪ Skillset of adversary
  ▪ Targeted or random
  ▪ Tools at their disposal
  ▪ Components of their attack infrastructure
Threat Landscape

- What type of systems can be used to harvest data?
  - Honeypots
  - Sandboxes
  - Physical machines for analysis

- What type of defenses can be used to stop these attacks?
  - Layers of technology
Malware Analysis
Malware Analysis

- Malware analysis is used to understand the functionality, potential impact and inner workings of malicious code.

- Two types of analysis
  - Static (Code Analysis)
  - Dynamic (Behavioral Analysis)

- Static Analysis Toolsets
  - PE Tools, Strings Extraction, etc

- Dynamic Analysis Toolsets
  - Process/File/Network monitoring tools, etc
Malware Analysis

- Environment Types:
  - Virtual
  - Physical

- Connectivity Types:
  - Internet enabled
  - Air-gapped

- Operating System Types:
  - Windows, Linux, OSX, Android, iOS
Malware Analysis

- What type of functionality do you want from a malware analysis lab?
  - Repeatability
  - Scalability
  - Isolation
  - Accuracy
  - Time Efficient
  - Actionable Data
Malware Analysis

- What does a typical setup look like for a malware analysis environment?
Automating Malware Analysis
Automating Malware Analysis

- Why should malware analysis be automated?
- What makes sense for a small organization with a small security team?
- Do cloud based malware analysis systems make sense?
- What are some negatives about automating malware analysis?
Automating Malware Analysis

- Examples of cloud based malware analysis systems
  - Comodo Automated Analysis System and Valkyrie
  - Joe Sandbox Cloud (Community Edition)
  - Malwr (also see MalwareViz)
  - sandbox.pikker.ee
  - SecondWrite (free version)
  - VxStream Sandbox (Hybrid Analysis)
  - ThreatExpert
  - ThreatTrack
  - ViCheck
### Automating Malware Analysis

![Screenshot of a web interface for analyzing malware]

**Analysis**

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>STARTED</th>
<th>COMPLETED</th>
<th>DURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILE</td>
<td>2017-11-08 10:36:45</td>
<td>2017-11-08 10:39:02</td>
<td>157 seconds</td>
</tr>
</tbody>
</table>

**File Details**

- **FILE NAME**: Scanned 0931658.pdf.htm
- **FILE SIZE**: 64 bytes
- **FILE TYPE**: ASCII text, with no line terminators
- **MD5**: 6216f3a7cd2f7967e85f95f3f5e31601
- **SHA1**: 0931658f22a232f7de016f5615f3f5e31601
- **SHA256**: 35b5390a19e6690a48127a14354d90d7325225c5f6c7f468cc7a39287c8ebe410
- **SHA256**: 746f6e5a03bad2b52c7fca5a444aa1f707e67b65f716d3d297bed1c727bfe5684e0b4aacc0363624e22cf37770e5d2eb6eb5847ae7a712f2121549b6b44e6c5e4
- **CRC32**: 3502475E
- **F3DDEEP**: None matched
- **YARA**: None matched
Making Use Of In-House Labs
Making Use Of In-House Labs

- Why would you want an in-house malware analysis lab?
  - Control the test environment
  - Ability to change testing platform adhoc depending on sample
  - Keep potential metadata leakage from reaching public systems
  - Ability to test your own security stack against malware samples
Making Use Of In-House Labs

John Lambert
@JohnLaTwC

Another LuckyStrike macro doc--this time from Poland. It only decrypts properly if run in the right victim domain.

shellint.com/blog/2016/9/13 ...
Making Use Of In-House Labs

- Examples of free Malware Analysis Toolkits (for in-house lab environments)
  - Zero Wine
  - Buster Sandbox Analyzer
  - Malheur
  - REMnux
  - Cuckoo Sandbox
What is Cuckoo?

Cuckoo Sandbox is the leading open source automated malware analysis system.

You can throw any suspicious file at it and in a matter of minutes Cuckoo will provide a detailed report outlining the behavior of the file when executed inside a realistic but isolated environment.

Malware is the swiss-army knife of cybercriminals and any other adversary to your corporation or organization.

In these evolving times, detecting and removing malware artifacts is not enough: it’s vitally important to understand how they operate in order to understand the context, the motivations, and the goals of a breach.

Cuckoo Sandbox is free software that automated the task of analyzing any malicious file under Windows, OS X, Linux, and Android.
Making Use Of In-House Labs – Cuckoo Sandbox

- Cuckoo can provide data on the following components:
  - Traces of calls performed by all processes spawned by the malware.
  - Files being created, deleted and downloaded by the malware during its execution.
  - Memory dumps of the malware processes.
  - Network traffic trace in PCAP format.
  - Screenshots taken during the execution of the malware.
  - Full memory dumps of the machines.
Making Use Of In-House Labs – Cuckoo Sandbox

**Cuckoo host**
Responsible for guest and analysis management.
Start analysis, dumps traffic and generates reports.

**Analysis Guests**
A clean environment when run a sample.
The sample behavior is reported back to the Cuckoo host.

**Virtual network**
An isolated network where run analysis virtual machines.
Making Use Of In-House Labs – Cuckoo Sandbox

- Cuckoo sandbox can be setup within a few hours in a non complex deployment
- https://cuckoo.sh/docs/installation/index.html - it is documented in detail

- There are two main components to getting the system up and running:
  1. Preparing the Cuckoo Host (management server):
     - Installation of a Linux OS
     - Installation of Python Libraries
     - Installation of Virtualization Software
     - Installation of Module Dependencies
     - Installation of Database
     - Configuration changes specific to your install
2. Preparing the Cuckoo Guest (malware testing OS):
   - Creation of Virtual Machine (controlled by management server)
   - Installation of a Testing OS (Win XP or Win 7)
   - Installation of Python Libraries
   - Configuration of Virtual Networking
   - Installation of the Agent (communicates with the management server)
   - Complete Snapshot of Final VM image (used as clean workstation)
Submitting a sample can be done via the WebUI or the command line.
Making Use Of In-House Labs – Cuckoo Sandbox

Configure your Analysis

Global Advanced Options
Options you change here are globally persisted to all files in your selection.

Network Routing

| NONE | DROP | INTERNET | INETSIM | TOR |

VPN via
Select

Package

| exe | LOW | MEDIUM | HIGH |

Priority

Timeout

| SHORT 60 | MEDIUM 120 | LONG 300 | ... | SECONDS |

© 2017 Scalar Decisions Inc. Not for distribution outside of intended audience.
Making Use Of In-House Labs – Cuckoo Sandbox
Making Use Of In-House Labs – Cuckoo Sandbox

- Results are populated in the backend database and presented via the WebUI.
- Information collected includes:
  - Static Analysis
  - Harvested Artifacts
  - Behavioral Analysis
  - Network Analysis
  - Dropped Files
  - Dropped Buffers
  - Process Memory
Making Use Of In-House Labs – Takeaways

- Utilizing the data harvested from malware analysis
- Testing your own security stack
- Custom hardening is always an option for VM detection
- Replicate a similar environment to production
Malware Analysis Best Practices
Best Practices

- Don’t run malware samples connected to the internet if you are unsure of the potential action of the malicious code.
- Any data on a machine that has had malware on it should be considered compromised and/or could be stolen.
- Utilize snapshot technology to save a clean state of a virtual machine.
- If you are tunneling through a VPN it should be outside of the infected VM (malware can be endpoint aware)
- If you are sharing a malicious sample with a vendor be sure to encrypt the file (shared password)
References

- https://www.slideshare.net/chrissanders88/cissa-lightning-talk-building-a-malware-analysis-lab-on-a-budget
- http://executemalware.com/?p=175
- http://techgenix.com/building-malware-analysis-lab/
- https://rastamouse.me/2017/05/playing-with-cuckoo/
References

- https://remnux.org/
- https://zeltser.com/malware-analysis-tool-frameworks/
- https://zeltser.com/automated-malware-analysis/
- Malware Analyst’s Cookbook
- Practical Malware Analysis