Introduction to Malware Reversing

a brief introduction to reversing malware

- Brandon Lum -

Brandon Lum

Temasek Polytechnic

Cyber & Digital Security

↓

Carnegie Mellon University

Computer Science

Cryptography

@ University of Wollongong

IT Audit and Pentest

@ KPMG

Lumex Security

:::Innovative Security Insights:::

Contents

- About Reversing Malware
- Basic Static Analysis (& Anti-RE)
- Basic Dynamic Analysis

Why RE Malware?

- Prevention and Containment
- Research
- Fun

Reversing Malware

Reversing Malware

- Set up a Virtual Environment
- Get the necessary tools ready
- Snapshot is your best friend

Static Analysis

Basic Static Analysis

- Finding out information about the Malware by looking at the file itself (**without execution**).

Techniques

- File Signatures
- Strings within file
- Portable Executable (PE) Headers + Resources

File Signatures

File Signatures

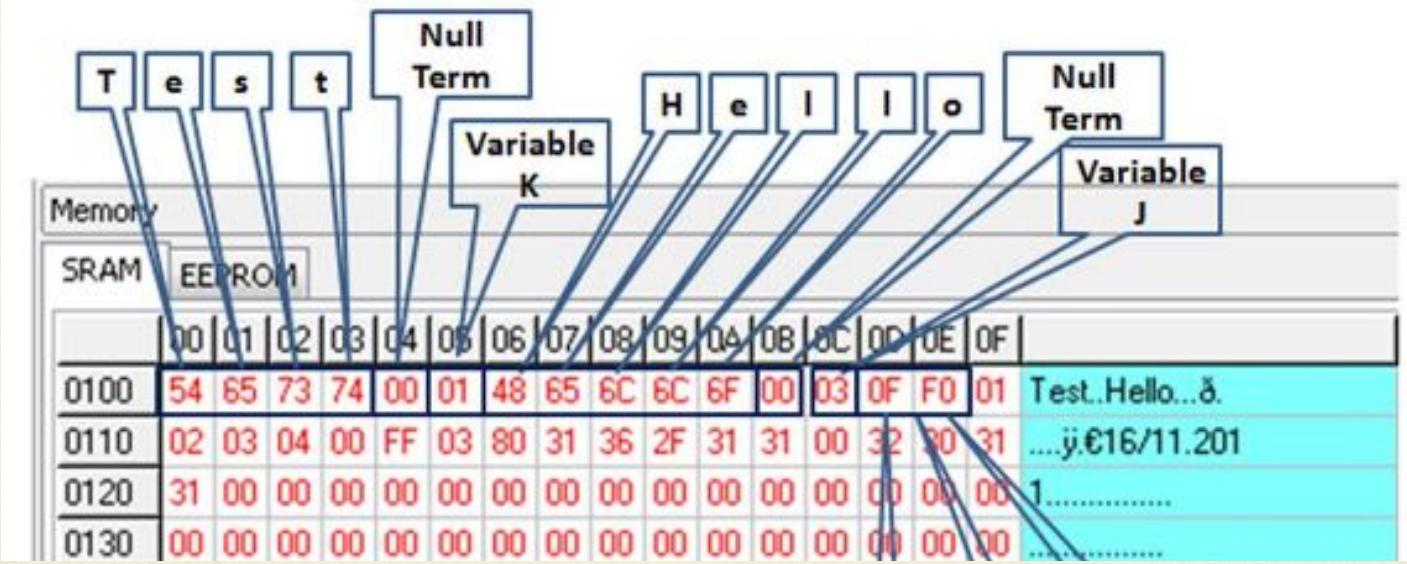
- Leveraging on the analysis of others'
  - Anti-Viruses have their own analysis of Malware, based on:
    - Signature
    - Heuristics

File Signatures

Strings

Strings

- Strings are identified by a NULL terminating character



- _^]3
- hp @
- SVW
- %8 @
- %D @
- %\ @
- %` @
- CloseHandle
- UnmapViewOfFile
- IsBadReadPtr
- MapViewOfFile
- CreateFileMappingA
- CreateFileA
- FindClose
- FindNextFileA
- FindFirstFileA
- CopyFileA
- KERNEL32.dll
- malloc
- exit
- MSVCRT.dll
- __p__fmode
- _stricmp
- kerne132.dll
- kernel32.dll
- .exe
- C:*
- C:\windows\system32\kerne132.dll
- Kernel32.
- Lab01-01.dll
- C:\Windows\System32\Kernel32.dll
- WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
- http://www.practicalmalwareanalysis.com/updater.exe

- _^]3
- hp @
- SVW
- %8 @
- %D @
- %\ @
- %` @
- CloseHandle
- UnmapViewOfFile
- IsBadReadPtr
- MapViewOfFile
- CreateFileMappingA
- CreateFileA
- FindClose
- FindNextFileA
- FindFirstFileA
- CopyFileA
- KERNEL32.dll
- malloc
- exit
- MSVCRT.dll
- __p__fmode
- _stricmp
- **kerne132.dll**
- kernel32.dll
- .exe
- C:*
- **C:\windows\system32\kerne132.dll**
- Kernel32.
- **Lab01-01.dll**
- C:\Windows\System32\Kernel32.dll
- WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
- **http://www.practicalmalwareanalysis.com/updater.exe**

Strings

- IP Addresses (N)
- URLs (N)
- File Paths (H)
- Registry Keys (H)
- Error Messages (which may hint functionality)
- APIs, Functions, etc.

Portable Executables (PEs)

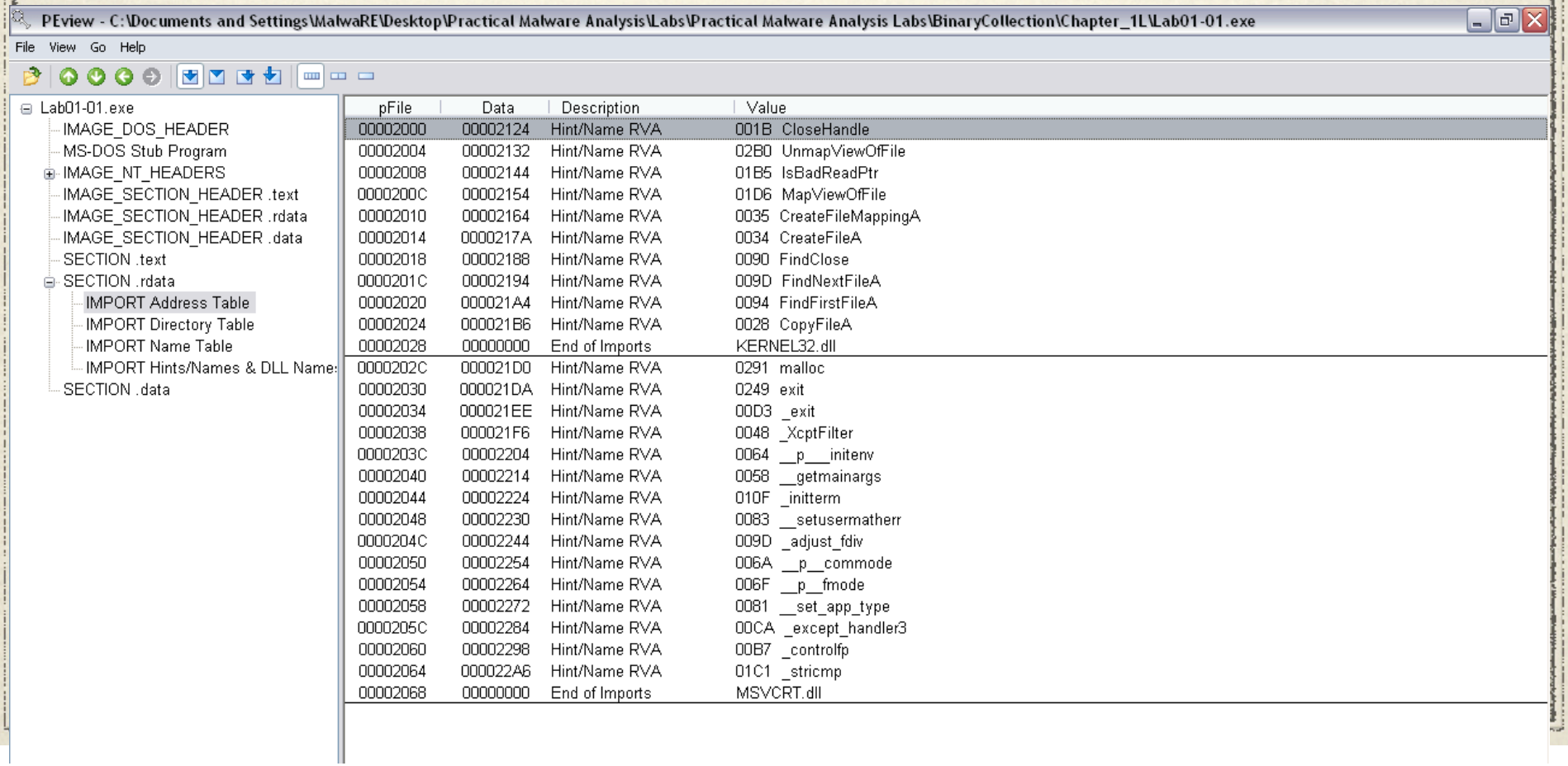
Portable Executables

- .text - Executable Code
- .data - Stores global data throughout program
- .rsrc - Stores resources needed by EXE

- Other sections:
  .rdata, .idata, .edata, .pdata, .reloc

Portable Executable (PE) Headers

- Information about APIs and DLLs used



Other information in PE headers

- Compile Time
- Information of code and data sections within the PE

Demo 1:

Static Analysis
Lab 01-01 (Static Analysis)
Lab 01-04 (Resources)
Lab 01-02 (Packing)

Functions to Note

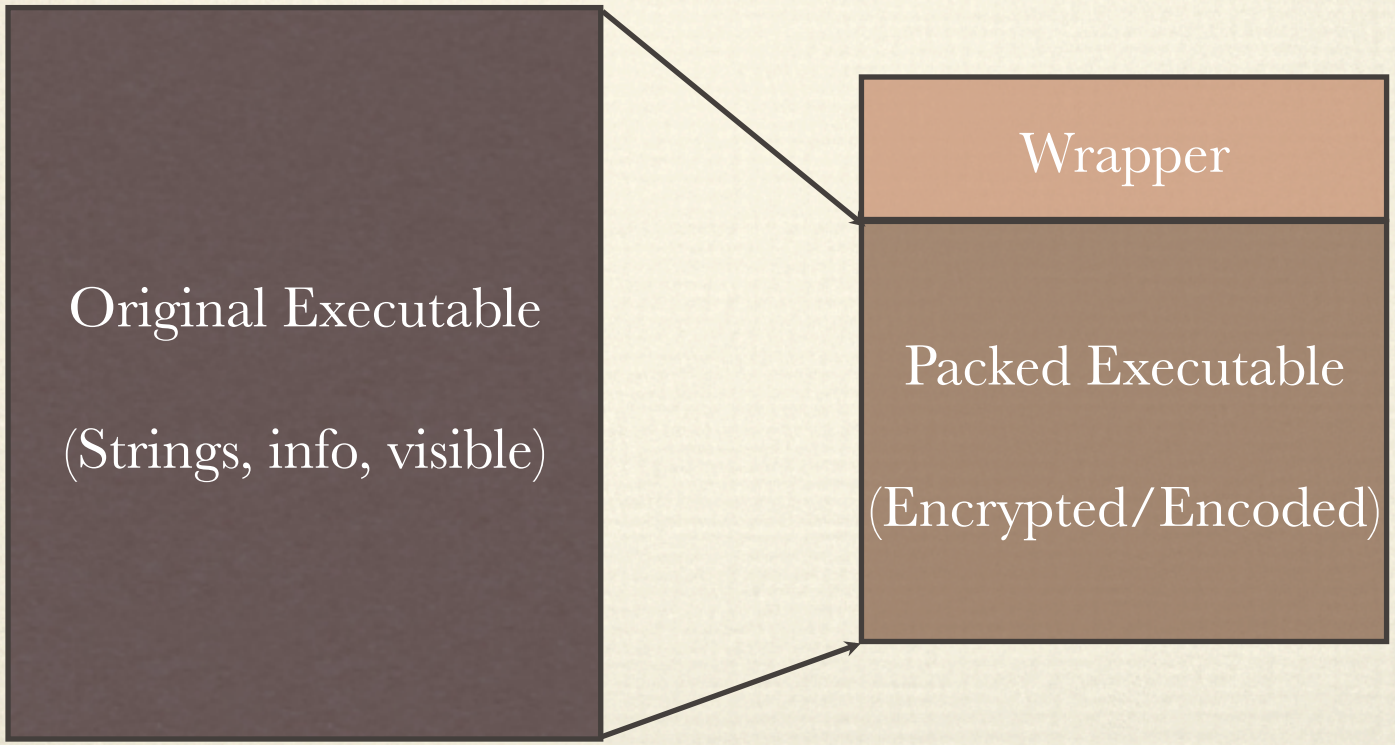
- Network Communications:
  - w32_32.dll: gethostbyaddr, connect, close socket, etc.
  - urlmon.dll: URLDownloadToFile
  - wininet.dll: InternetOpenURL, InternetConnect, etc.
- Process and Thread:
  - VirtualAllocEx, VirtualProtectEx, ReadProcessMemory, WriteProcessMemory

Resources

- PEs contain resources
  - Images
  - Scripts
  - Other PEs

Anti-Analysis Techniques

- Packing of Executables



Anti-Analysis Techniques

- Tell-tale signs of Packing
  - Packers Naming Conventions
  - Virtual Size Allocation VS Raw Data
  - Less than normal Imported Functions

Dynamic Analysis

Basic Dynamic Analysis

- Finding out information about the Malware by through executing the malware

Basic Dynamic Analysis

- Things to look out for
- Different ways to capture and view

Malware Behavior

- Host
  - Registry
  - Files
  - Processes
  - etc.

Malware Behavior

- Network
  - DNS Requests
  - HTTP/FTP/SSH Requests
  - etc.

Capture and View

- Snapshots - Compare Before/After
- Capturing all events
- Watch real-time
- Set up Infrastructure

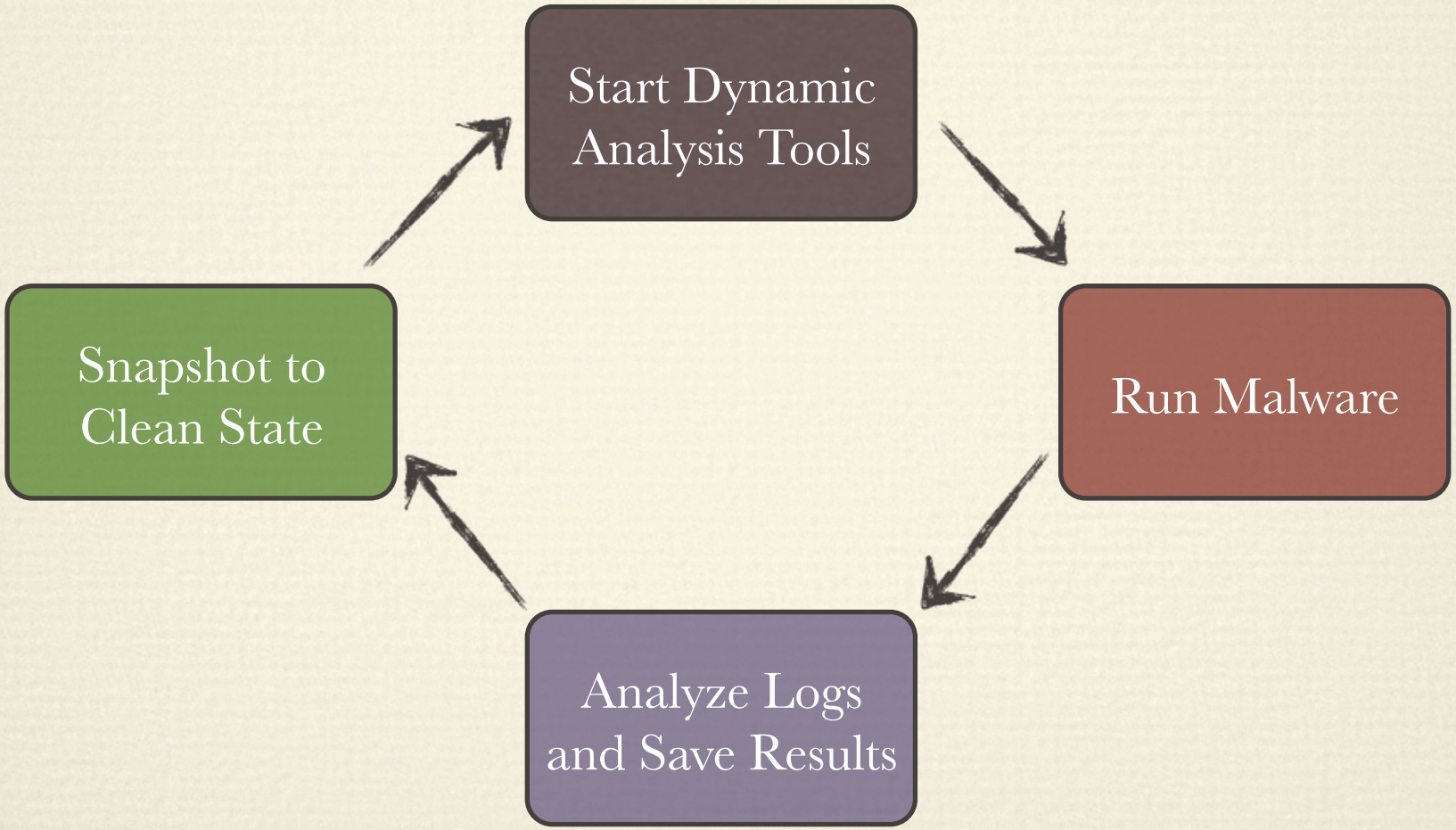
Demo 2:

Snapshot & Capture

Demo 3:

Capture & Network
Lab 03-01

Methodology for Dynamic Analysis



Conclusion

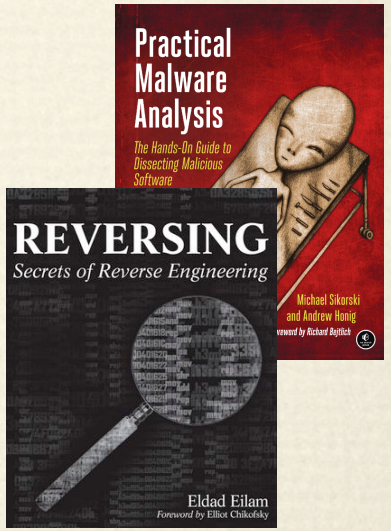
- Basic Static & Dynamic Analysis
  - Overview Malware Functionality
  - Clues to create signatures
- Next Step: Debug the code!

List of Tools

- Strings
- PEView
- Dependency Walker
- Resource Hacker
- Procmon
- Procexp
- Regshot
- Capture
- Wireshark
- Netcat/Fakenet
- FakeDNS/ApateDNS
- PEID
- UPX

References

- Malware RE Workshop by Chong Rong Hwa
- Practical Malware Analysis
- Reversing



Thank You

Brandon Lum

LUMJJB_AT_GMAIL_DOT_COM

http://lumexsec.wordpress.com