LAB 03 - BASIC ANALYSIS

MALWARE ANALYSIS AND INCIDENT FORENSICS

M.Sc. in Cyber Security

SYSTEMS AND ENTERPRISE SECURITY

M.Sc. in Engineering in Computer Science

A.Y. 2024/2025

SAPIENZA
UNIVERSITÀ DI ROMA

CIS SAPIENZA
CYBER INTELLIGENCE AND INFORMATION SECURITY

LAB_03-1.EXE

Answer the following questions:

1) When was this file compiled?
2) List a few imports or sets of imports and describe how the malware might use them.
3) What are a few strings that stick out to you and why?
4) What happens when you run this malware? Is it what you expected and why?
5) Name a procmon filter and why you used it.
6) Are there any host-based signatures? (Files, registry keys, processes or services, etc). If so, what are they?
7) Are there any network based signatures? (URLs, packet contents. etc) If so, what are they?
8) Is there anything that impeded your analysis? How so? How might you overcome this?
9) What do you think is the purpose of this malware?

LAB_03-1.EXE

Hints:

- Use a software that allows you to inspect the PE Header
  - Open the EXE in PeStudio
- Check the “compiler-stamp” value for the compilation date
- Look at the “Imports” tab
  - ShellExecuteExA - launches other processes via the shell
- Look at the “strings” tab
  - Notice “60.248.52.95:443” !!!

LAB_03-1.EXE

Hints:

- Use a software to monitor the malware execution
  - e.g. ProcMon
  - Analyze the trace looking for actions
- Filter out everything that is not directly or indirectly related to the EXE
- Look for network activities
- Look for file-level activities

LAB_03-2.EXE

Answer the following questions:

1) What is the md5sum? What of interest does VirusTotal Report?
2) List a few imports or sets of imports and describe how the malware might use them.
3) What are a few strings that stick out to you and why?
4) What happens when you run this malware? Is it what you expected and why?
5) Name a procmon filter and why you used it.
6) Are there any host-based signatures? (Files, registry keys, processes or services, etc). If so, what are they?
7) Are there any network based signatures? (URLs, packet contents. etc) If so, what are they?
8) Is there anything that impeded your analysis? How so? How might you overcome this?
9) What do you think is the purpose of this malware?

LAB_03-3.EXE

Answer the following questions:

1) Are there any indications that this malware is packed? What are they? What is it packed with?
2) Are you able to unpack it? Why or why not?
3) What are a few strings that stick out to you and why?
4) What happens when you run this malware? Is it what you expected and why?
5) Are there any host-based signatures? (Files, registry keys, processes or services, etc). If so, what are they?
6) Are there any network based signatures? (URLs, packet contents. etc) If so, what are they?
7) Is there anything that impeded your analysis? How so? How might you overcome this?
8) What do you think is the purpose of this malware?

LAB_03-4.EXE

Answer the following questions:

1) Are there any indications that this malware is packed? What are they? What is it packed with?
2) Are you able to unpack it? Why or why not?
3) What are a few strings that stick out to you and why?
4) What happens when you run this malware? Is it what you expected and why?
5) Are there any host-based signatures? (Files, registry keys, processes or services, etc). If so, what are they?
6) Are there any network based signatures? (URLs, packet contents. etc) If so, what are they?
7) Is the malware performing actions to persist in the target systems? Which strategy does it use?

PERSISTENCE IN WINDOWS

Techniques to survive after reboot of a Windows OS

- Registry Key
- File System
  - Startup locations
  - DLL search order hijacking
  - Trojanizing system files
- Windows Services
- Scheduled Tasks
- Browser extensions
- AppInit_DLLs

FREQUENTLY USED REGISTRY KEY

Administrator privilege is required to update HKLM (The list is not comprehensive nor more important than others, which are not listed here)
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\"Shell" and "UserInit"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\"Appinit_Dlls"
HKLM\System\CurrentControlSet\Control\Session Manager\KnownDlls
HKLM\System\CurrentControlSet\Services
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects

Without administrator privileges, malware can persist with the following registry keys (The list is not comprehensive nor more important than others, which are not listed here)
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Logon
HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

PERSISTENCE USING FILE SYSTEM

Startup locations

- For the logged-in user:
  %USERPROFILE%\Start Menu\Programs\Startup
- For all users:
  %ALLUSERSPROFILE%\Start Menu\Programs\Startup

MICROSOFT WINDOWS SERVICES

- Long-running executables without user interaction (like a *nix daemon)
- Can be automatically started when the computer boots
- CreateService() Windows API is called to register a service
- Registered services can be found under the registry key HKLM\System\CurrentControlSet\Services

SVCHOST

- C:\Windows\System32\svchost.exe is a generic host process for services that run from DLLs
- Multiple instances are often running
  - One instance contains a group of services
- Groups are listed in the registry key HKLM\Software\Microsoft\Windows NT\CurrentVersion\Svchost
- It is common to have malware name itself svchost.exe but run from somewhere other than C:\Windows\System32, e.g. C:\Windows
- Or alternatively they will just add a new DLL for the real svchost to run as a service

SCHEDULED TASKS

- Scheduled tasks are Window's alternative to cron jobs
- You can register tasks to be executed periodically
  - Widely used by legit software to schedule periodic update checks
- A malware may use the COM interface to register a new task
- It may also substitute an existing task with a different exe
- You may want to check the following directories:

  C:\Windows\System32\Tasks

  C:\Windows\SysWOW64\Tasks

  C:\Windows\Tasks

APPINIT DLLS

- DLLs that are specified in the AppInit_DLLs value in the Registry are loaded by user32.dll into every process that loads user32.dll
- These values can be abused to obtain elevated privileges by causing a malicious DLL to be loaded and run in the context of separate processes on the computer.
- The AppInit DLL functionality is disabled in Windows 8 and later versions when secure boot is enabled.