

Laboratorium 3 Analiza Dynamiczna

Wstęp

Laboratorium 3 pokazuje w jaki sposób można wykorzystać **Analizę Dynamiczną** do identyfikacji i opisu działania malware'u

Zostają użyte narzędzia do analizy zmian rejestrów, powstawania procesów oraz zapisu zdarzeń.

Spis treści

- [Laboratorium 3 Analiza Dynamiczna](#)
 - [Wstęp](#)
 - [Spis treści](#)
 - [Sumy Kontrolne](#)
 - [Laboratorium 3.1](#)
 - [Importy](#)
 - [Indykatory Hostowe](#)
 - [Indykatory sieciowe](#)
 - [Laboratorium 3.2](#)
 - [Importy](#)
 - [Instalacja](#)
 - [Uruchomienie](#)
 - [Jak odnaleźć](#)
 - [Filtr procmon](#)
 - [Indykatory sieciowe](#)
 - [Laboratorium 3.3](#)
 - [Informacje ogólne](#)
 - [Modyfikacje Pamięci](#)
 - [Indykatory Hostowe](#)
 - [Działanie programu](#)
 - [Laboratorium 3.4](#)
 - [Ciekawe Informacje](#)
 - [Działanie Programu](#)
 - [Blokada Analizy Dynamicznej](#)
 - [Dalsza Analiza](#)

Sumy Kontrolne

File	Checksum SHA-256	Virustotal score
Lab03-01.exe	EB84360CA4E33B8BB60DF47AB5CE962501EF3420BC7AAB90655FD507D2FFCEDD	64/70
Lab03-02.dll	5ECED7367ED63354B4ED5C556E2363514293F614C2C2EB187273381B2EF5F0F9	57/69

File	Checksum SHA-256	Virustotal score
Lab03-03.exe	AE8A1C7EB64C42EA2A04F97523EBF0844C27029EB040D910048B680F884B9DCE	61/70
Lab03-04.exe	6AC06DFA543DCA43327D55A61D0AAED25F3C90CCE791E0555E3E306D47107859	49/68

Laboratorium 3.1

Importy

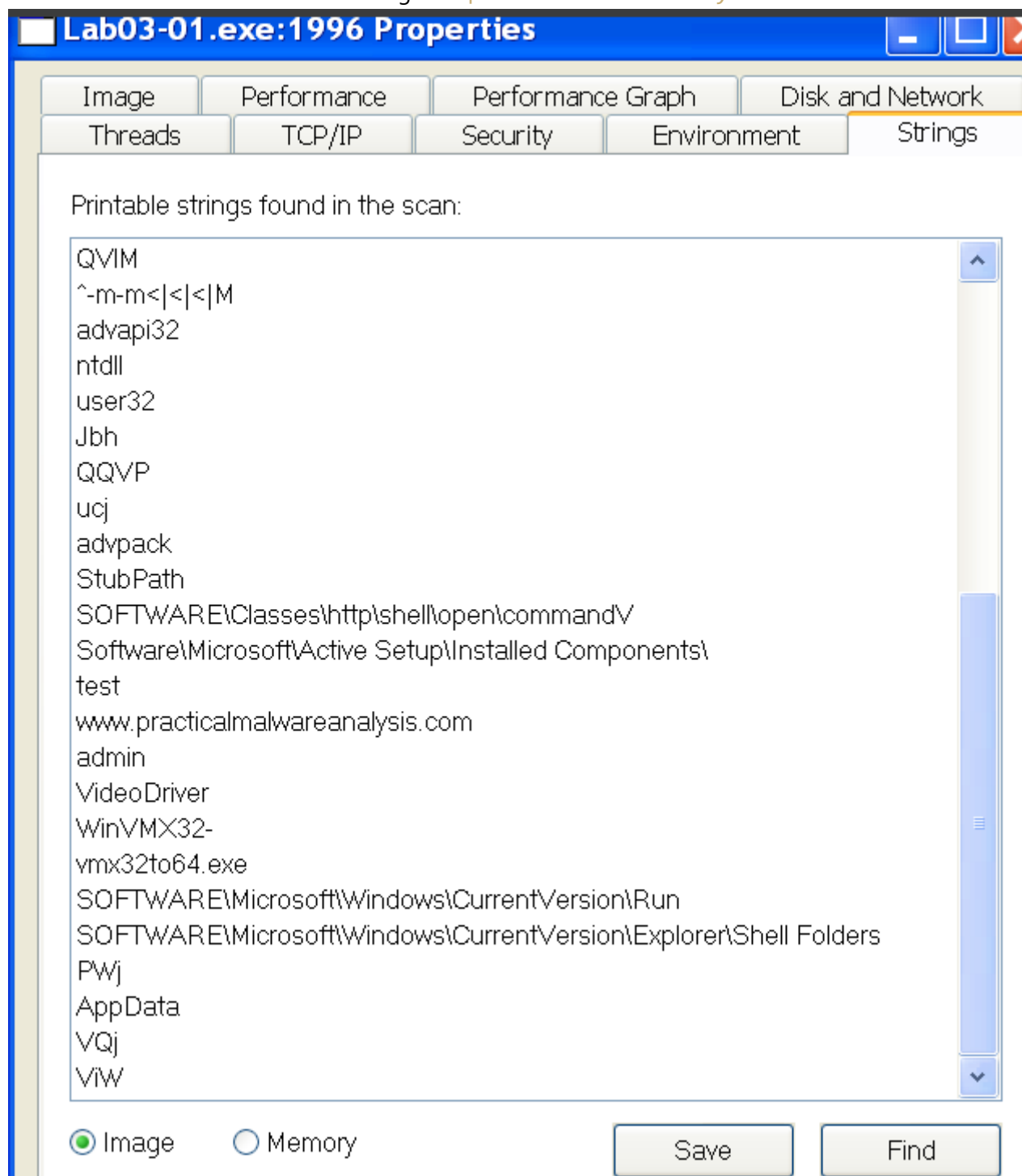
Program nie importuje **żadnych funkcji** (poza *ExitProcess*).

Indykatory Hostowe

Używając procmon, nie znalazłem **żadnej próby** połączenia z internetem.

Natomiast w aplikacji *procexp* zauważyłem **nowy proces Lab03-01.exe**,

Gdzie w właściwościach znalazłem string www.practicalmalwareanalysis.com.



Indykatory sieciowe

Po analizie programem *regshot* zauważyłem, że uruchomienie pliku spowodowało **powstanie zmian w procesie IPRIP**.

Aby uruchomić ten proces należy użyć komendy `net start IPRIP`.

Jak odnaleźć

Aby odnaleźć uruchomiony malware **zrobiłem shot** rejestru, a po uruchomieniu procesu **zrobiłem drugiego shot**.

Po porównaniu zauważyłem, że dużo kluczy zostało **dodanych i zmodyfikowanych**.

```
-----
Keys added: 6
-----
HKLM\SYSTEM\ControlSet001\Services\IPRIP
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security
-----
Values added: 22
-----
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Wow64: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\IPRIP>Description: "Depends INA+, Collects and s
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService: 52 00 70 00 63 00 53 00
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and s
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security\Security: 01 00 14 80 B8 00 00 (
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Type: 0x00000020
```

Jednocześnie miałem włączone **przechwytywanie zdarzeń w procmon**.

Zauważyłem, że tych zmian dokonał proces **net1.exe**.

Filtr procmon

Aby wyświetlić najwięcej istotnych informacji należy dodać filtr, który zawiera wszystkie zdarzenia *net1.exe*.

Indykatory sieciowe

Używając *fakenet* przechwyciłem ruch, który próbuje wykonać proces.

Pojawiły się 2 strony, z którymi próbował się połączyć:

- practicalmalwareanalysisi.com
 Queries
 practicalmalwareanalysis.com: type A, class IN
- download.windowsupdate.com
 Queries
 www.download.windowsupdate.com: type A, class IN

Druga strona nie należy do Microsoftu i jest oznaczana przez przeglądarkę za **potencjalnie niebezpieczną**.

Laboratorium 3.3

Informacje ogólne

Po włączeniu programu, *procep* wyświetlał proces tylko na chwilę, ponieważ program **bardzo szybko się wyłączał**.

Po naciśnięciu spacji można jednak **zatrzymać** odświeżanie i przyjrzeć się bliżej.

Po obejrzeniu stringów nie znalazłem nic ciekawego, dlatego użyłem *procmon*, aby zobaczyć co program wykonywał.

Zauważyłem, że tworzy on nowy plik **svchost.exe**,

16:28:2...	Lab03-03.exe	424	CreateFile	C:\WINDOWS\SysWOW64\svchost.exe	SUCCESS
------------	--------------	-----	------------	---------------------------------	---------

a następnie ten proces uruchamia.

16:28:2...	Lab03-03.exe	424	Process Create	C:\WINDOWS\system32\svchost.exe	
------------	--------------	-----	----------------	---------------------------------	--

W *procep* jest widoczny nie jako **usługa** (kolor czerwony), lecz jako **aplikacja** (kolor niebieski)


Oznaczony jest również jako proces należący do *Microsoftu*.

explorer.exe		9,668 K	2,568 K	1424 Windows Explorer	Microsoft Corporation
procep.exe	2.00	12,636 K	5,668 K	1308 Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon.exe		5,568 K	7,524 K	1596 Process Monitor	Sysinternals - www.sysinter...
svchost.exe		828 K	2,156 K	1268 Generic Host Process for Win...	Microsoft Corporation

Jako folder roboczy wskazany jest katalog z wirusami. Po kliknięciu jest on również zweryfikowany jako proces

Microsoftu, mimo że do niego nie należy.

Image File



Generic Host Process for Win32 Services
(Verified) Microsoft Windows Component Publisher

Version: 5.1.2600.5512

Build Time: Sun Apr 13 21:15:12 2008

Path:

Command line:

Current directory:

Autostart Location:

Parent: Lab03-03.exe(700)

User: WINXP\Administrator

Started: 10:00:54 PM 4/14/2023

Comment:

VirusTotal:

Data Execution Prevention (DEP) Status: Disabled

Modyfikacje Pamięci

Po sprawdzeniu stringów okazuje się, że znacznie się one od siebie różnią:

- **Image**

Printable strings found in the scan:

```
Parameters
System\CurrentControlSet\Services
nServiceMain
ServiceDll
ServiceDllUnloadOnStop
eventlog
ncach_np
\PIPE\
DefaultRpcStackSize
AuthenticationCapabilities
ImpersonationLevel
AuthenticationLevel
CoInitializeSecurityParam
Software\Microsoft\Windows NT\CurrentVersion\Svchost
\Registry\Machine\System\CurrentControlSet\Control\SecurePipeServers\
VS_VERSION_INFO
StringFileInfo
CompanyName
Microsoft Corporation
FileDescription
Generic Host Process for Win32 Services
FileVersion
5.1.2600.5512 (xpsp.080413-2111)
InternalName
svchost.exe
LegalCopyright
Microsoft Corporation. All rights reserved.
OriginalFilename
```


- **Memory**

Printable strings found in the scan:

```
!!!!  
!This program cannot be run in DOS mode.  
RichS  
.text  
.rdata  
@.data  
hPS@  
@hTP@  
hPW@  
hPW@  
hPS@  
toj  
PhPW@  
PhPW@  
hPW@  
hPS@  
htP@  
hxP@  
Glu  
GJu  
tzVS  
Glt%  
t/Ku  
GKu  
SVW  
YYh P@  
VWu  
t9UW
```

Oznacza to, że instrukcje które załadowane są do pamięci są **inne niż oryginalnego procesu** należącego do systemu. Jest to **wirus podszywający się pod ten proces**.

Indykatory Hostowe

Używając programu *Fakenet* zauważyłem, że proces nie produkuje żadnego ruchu sieciowego. Po upewnieniu się w *PEstudio*, nie znalazłem żadnej importowanej funkcji związanej z siecią.

<u>ExitProcess</u>	-	implicit	-	kernel32.dll
<u>TerminateProcess</u>	x	implicit	-	kernel32.dll
<u>GetCurrentProcess</u>	-	implicit	-	kernel32.dll
<u>UnhandledExceptio...</u>	-	implicit	-	kernel32.dll
<u>GetModuleFileNameA</u>	-	implicit	-	kernel32.dll
<u>FreeEnvironmentStr...</u>	-	implicit	-	kernel32.dll
<u>FreeEnvironmentStr...</u>	-	implicit	-	kernel32.dll
<u>WideCharToMultiByte</u>	-	implicit	-	kernel32.dll
<u>GetEnvironmentStri...</u>	x	implicit	-	kernel32.dll
<u>GetEnvironmentStri...</u>	x	implicit	-	kernel32.dll
<u>SetHandleCount</u>	-	implicit	-	kernel32.dll
<u>GetStdHandle</u>	-	implicit	-	kernel32.dll
<u>GetFileType</u>	-	implicit	-	kernel32.dll
<u>GetStartupInfoA</u>	-	implicit	-	kernel32.dll
<u>HeapDestroy</u>	-	implicit	-	kernel32.dll
<u>HeapCreate</u>	-	implicit	-	kernel32.dll
<u>HeapFree</u>	-	implicit	-	kernel32.dll
<u>RtlUnwind</u>	-	implicit	-	kernel32.dll
<u>WriteFile</u>	x	implicit	-	kernel32.dll
<u>HeapAlloc</u>	-	implicit	-	kernel32.dll
<u>GetCPInfo</u>	-	implicit	-	kernel32.dll
<u>GetACP</u>	-	implicit	-	kernel32.dll
<u>GetOEMCP</u>	-	implicit	-	kernel32.dll
<u>HeapReAlloc</u>	-	implicit	-	kernel32.dll
<u>LoadLibraryA</u>	-	implicit	-	kernel32.dll
<u>MultiByteToWideChar</u>	-	implicit	-	kernel32.dll
<u>LCMapStringA</u>	-	implicit	-	kernel32.dll
<u>LCMapStringW</u>	-	implicit	-	kernel32.dll
<u>GetStringTypeA</u>	-	implicit	-	kernel32.dll
<u>GetStringTypeW</u>	-	implicit	-	kernel32.dll

Działanie programu

Program przy włączeniu modyfikuje i tworzy kilka kluczy w rejestrach.

Następnie tworzy nowy proces o nazwie **svchost.exe** podszywając się pod usługę systemu windows utrudniając tym samym wykrycie.

Próba wykrycia ruchu sieciowego kończy się niepowodzeniem i patrząc na to, że program nie importuje funkcji sieciowych zakładam, że wirus nie łączy się z siecią.

Importuje on natomiast ponad 50 funkcji z biblioteki **KERNEL32.DLL** co świadczy o tym, że prawdopodobnie jego celem jest wyżądanie szkód w systemie.

Laboratorium 3.4

Ciekawe Informacje

Po analizie w *PEstudio* zauważyłem ciekawe importy.

Znajdują się tu funkcje do manipulowania rejestrami oraz funkcje sieciowe.

<u>RegDeleteValueA</u>	x	implicit	-	advapi32.dll
<u>RegCreateKeyExA</u>	-	implicit	-	advapi32.dll
<u>RegSetValueExA</u>	x	implicit	-	advapi32.dll
<u>RegOpenKeyExA</u>	-	implicit	-	advapi32.dll
<u>RegQueryValueExA</u>	-	implicit	-	advapi32.dll
<u>DeleteService</u>	x	implicit	-	advapi32.dll
<u>ShellExecuteA</u>	x	implicit	-	shell32.dll
<u>22 (shutdown)</u>	x	implicit	x	ws2_32.dll
<u>115 (WSAStartup)</u>	x	implicit	x	ws2_32.dll
<u>52 (gethostbyvalue)</u>	x	implicit	x	ws2_32.dll
<u>19 (send)</u>	x	implicit	x	ws2_32.dll
<u>23 (socket)</u>	x	implicit	x	ws2_32.dll
<u>9 (htons)</u>	x	implicit	x	ws2_32.dll
<u>4 (connect)</u>	x	implicit	x	ws2_32.dll
<u>3 (closesocket)</u>	x	implicit	x	ws2_32.dll
<u>16 (recv)</u>	x	implicit	x	ws2_32.dll
<u>116 (WSACleanup)</u>	x	implicit	x	ws2_32.dll

W stringach znajduje się adres URL www.practicalmalwareanalysis.com.

Działanie Programu

Spośród zmian rejestrów, nie wykryłem nic podejrzanego.

```
-----
Values added:5
-----
HKLM\SYSTEM\ControlSet001\Services\knixer\Enum\0: "Sw\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\
HKLM\SYSTEM\CurrentControlSet\Services\knixer\Enum\0: "Sw\{b7eafdc0-a680-11d0-96d8-00aa0051e5
HKU\S-1-5-21-1606980848-507921405-1343024091-500\Software\Microsoft\Windows\CurrentVersion\Ex
HKU\S-1-5-21-1606980848-507921405-1343024091-500\Software\Microsoft\Windows\ShellNoRoam\MUICa
HKU\S-1-5-21-1606980848-507921405-1343024091-500\Software\Microsoft\Windows\ShellNoRoam\MUICa

-----
Values modified:9
-----
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: E6 B8 51 DF 4E B0 91 C5 40 60 7C 5A 5E C7 C7 D
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 85 13 27 85 05 51 B4 74 5C 7D CB AC 84 76 AB 4
HKLM\SYSTEM\ControlSet001\Services\knixer\Enum\Count: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\knixer\Enum\Count: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\knixer\Enum\NextInstance: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\knixer\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\knixer\Enum\Count: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\knixer\Enum\Count: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\knixer\Enum\NextInstance: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\knixer\Enum\NextInstance: 0x00000001
HKU\S-1-5-21-1606980848-507921405-1343024091-500\Software\Microsoft\Windows\CurrentVersion\Ex
HKU\S-1-5-21-1606980848-507921405-1343024091-500\Software\Microsoft\Windows\CurrentVersion\Ex
HKU\S-1-5-21-1606980848-507921405-1343024091-500\Software\Microsoft\Windows\CurrentVersion\Ex
HKU\S-1-5-21-1606980848-507921405-1343024091-500\Software\Microsoft\Windows\CurrentVersion\Ex
HKU\S-1-5-21-1606980848-507921405-1343024091-500\Software\Microsoft\Windows\ShellNoRoam\BagMR
HKU\S-1-5-21-1606980848-507921405-1343024091-500\Software\Microsoft\Windows\ShellNoRoam\BagMR
HKU\S-1-5-21-1606980848-507921405-1343024091-500\SessionInformation\ProgramCount: 0x00000004
HKU\S-1-5-21-1606980848-507921405-1343024091-500\SessionInformation\ProgramCount: 0x00000005
```

W *procexp* zauważyłem powstający proces, lecz szybko po tym został zabity. Sam program usuwa siebie samego z dysku.

Ruch sieciowy też nie jest produkowany.

Nie wykryłem w programie, żadnych podejrzanых aktywności poza krótkim czasem działania i usuwaniem siebie z dysku.

Blokada Analizy Dynamicznej

Program usuwa sam siebie z dysku, przez co nie możemy włączyć go drugi raz. Sam program działa też bardzo krótko co znacznie utrudnia analizę dynamiczną.

Możliwe, że malware wykrywa, że jest w maszynie wirtualnej.

Dalsza Analiza

Analiza dynamiczna na niewiele się tu zda.

Aby móc sprawdzić dokładne działanie programu potrzebna będzie zaawansowana analiza statyczna.