

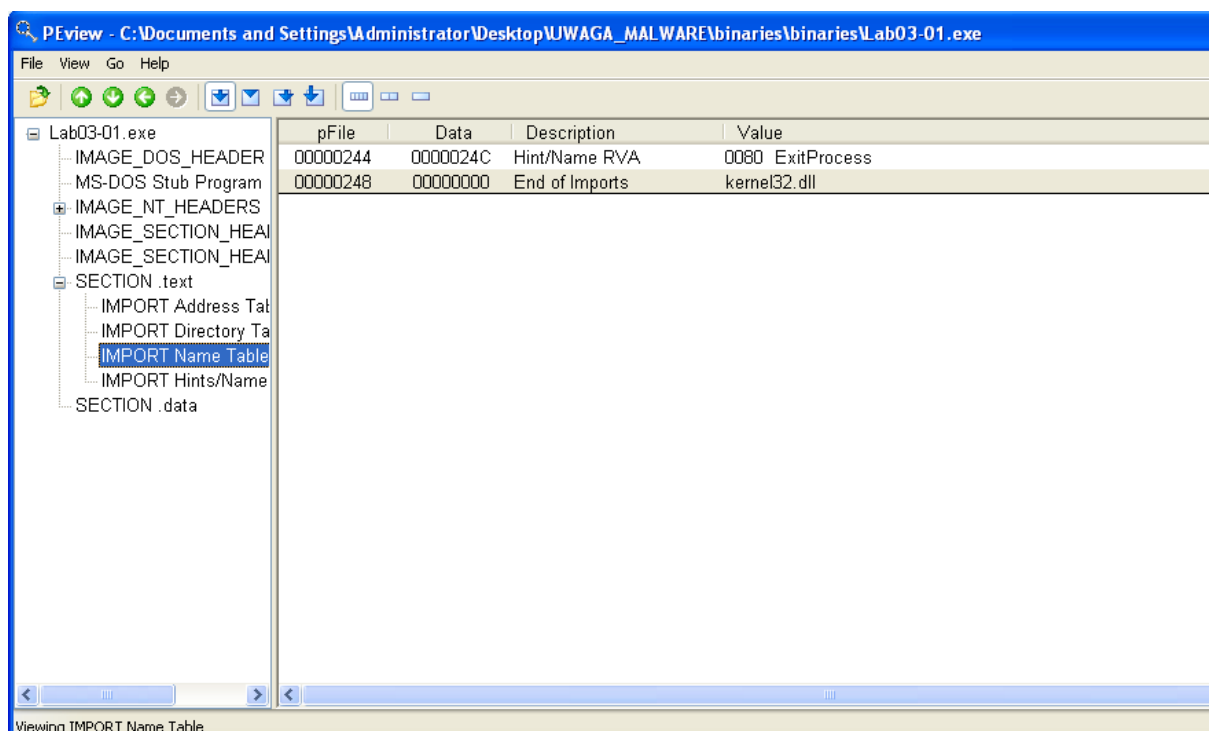
# Laboratorium 3 - Analiza Dynamiczna

Julia Sadecka, Cyberbezpieczeństwo

## Laboratorium 3.1

### 1. Importy i Łącuchy

W PView możemy zobaczyć, że oprócz importu do biblioteki kernel23.dll znajduje się import do 0080 ExitProcess. Jeżeli chodzi o stringi to możemy znaleźć w nich np. adres URL “malwareanalysis.com”, a także lokalizacje plików.



Screenshot01 - PView, importy plików

Offset	Type	Strings recognized as registry key
0000162F	ASCII	SOFTWARE\Classes\http\shell\open\commandV
000018E5	ASCII	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
00001735	ASCII	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
0000165B	ASCII	Software\Microsoft\Active Setup\Installed Components\

Offset	Type	Strings recognized URL
0000169D	ASCII	www.practicalmalwareanalysis.com

Offset	Type	Strings found
0000190F	ASCII	Explorer\Shell Folders
000016D4	ASCII	admin
000016AA	ASCII	malwareanalysis.com
00001694	ASCII	test

Screenshot02 - PPEE, stringi pliku 3.1

## 2. Indykatory hostowe

C:\WINDOWS\system32\vmx32to64.exe - który ma taką samą wielkość jak plik Lab03-01.exe. Jest więc jego kopią tylko zapisaną w innym miejscu.

## 3. Indykatory sieciowe

Kierują nas na stronę: [practicalmalware.com](http://practicalmalware.com)

# Laboratorium 3.2

## 1. Funkcje pliku

CreateServiceA	x	implicit	-	advapi32.dll
CloseServiceHandle	-	implicit	-	advapi32.dll
RegCreateKeyA	x	implicit	-	advapi32.dll
RegSetValueExA	x	implicit	-	advapi32.dll
RegisterServiceCtrlHandlerA	-	implicit	-	advapi32.dll
SetServiceStatus	-	implicit	-	advapi32.dll
11 (inet_addr)	x	implicit	x	ws2_32.dll
WSASocketA	x	implicit	-	ws2_32.dll
3 (closesocket)	x	implicit	x	ws2_32.dll
4 (connect)	x	implicit	x	ws2_32.dll
10 (ioctlsocket)	x	implicit	x	ws2_32.dll
19 (send)	x	implicit	x	ws2_32.dll
18 (select)	x	implicit	x	ws2_32.dll
151 (WSAFDIsSet)	x	implicit	x	ws2_32.dll
16 (recv)	x	implicit	x	ws2_32.dll
22 (shutdown)	x	implicit	x	ws2_32.dll
115 (WSAStartup)	x	implicit	x	ws2_32.dll
57 (gethostvalue)	x	implicit	x	ws2_32.dll
116 (WSACleanup)	x	implicit	x	ws2_32.dll

Screenshot03 - pestudio, functions

Czerwony 'x' oznacza, że importy są z czarnej listy. Jest ich sporo. Większość pochodzi z biblioteki ws2\_32.dll i wininet.dll. Znajdują się na czarnej liście ponieważ zostały zidentyfikowane jako szkodliwe lub niebezpieczne.

Niektóre z zaznaczonych funkcji:

- CreateService  
Tworzy usługę, którą można uruchomić w czasie rozruchu. Złośliwe oprogramowanie wykorzystuje usługę CreateService do utrzymywania trwałości, ukrywania się lub ładowania sterowników jądra.
- connect  
Służy do łączenia ze zdalnym gniazdem.
- recv  
Odbiera dane ze zdalnej maszyny. Złośliwe oprogramowanie często wykorzystuje tę funkcję do odbierania danych ze zdalnego serwera dowodzenia i kontroli.
- InternetOpen  
Inicjuje funkcje dostępu do Internetu wysokiego poziomu z WinINet, takie jak InternetOpenUrl i InternetReadFile. Z tej i innych funkcji możemy wnioskować, że malware próbuje się połączyć do Internetu.
- InternetReadFile  
Odczytuje dane z otwartego URLa.

## 2. Instalacja

pFile	Data	Description	Value
00004D28	00004706	Function RVA	0001 Install
00004D2C	00003196	Function RVA	0002 ServiceMain
00004D30	00004B18	Function RVA	0003 UninstallService
00004D34	00004B0B	Function RVA	0004 installA
00004D38	00004C2B	Function RVA	0005 uninstallA

Screenshot04 - PEview, exports

W importach i exportach możemy zobaczyć, że sporo ich jest związanych z Service, więc można się domyślać, że trzeba go zainstalować jako service.

Dodatkowo w exportach znajduje się komenda installA. Używamy więc komendy:

```
rundll32.exe Lab03-02.dll, installA
```

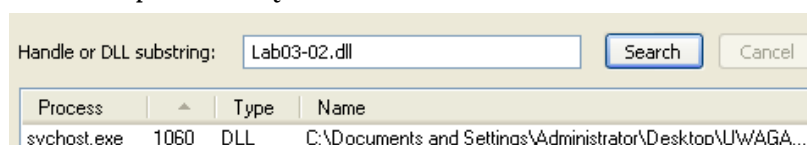
## 3. Uruchamianie

Uruchamiamy za pomocą komendy

```
net start IPRIP
```

## 4. Odszukanie złośliwego oprogramowania

W Process Explorer w zakładce Find wpisałam Lab03-02.dll i wyskoczyło, że działa on pod nazwą svchost.exe.



Screenshot05 - Process Explorer, Find

## 5. Filtry procmon

Najpierw należy w Process Name wpisać nazwę procesu, w naszym przypadku jest to svchost.exe. Możemy też dodać filtr po PID, które jest równe 1060.

Możemy dodać filtry typu operacji czy ścieżki plików.

<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Process Name	is	svchost.exe	Include
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	PID	is	1060	Include

Screenshot06 - Process Monitor, filtry

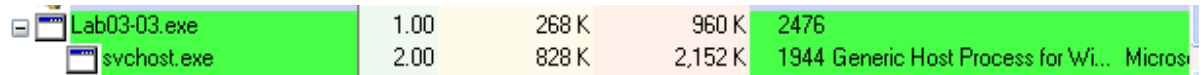
## 6. Indykatory sieciowe

Możemy znaleźć adres URL [practicalmalwareanalysis.com](http://practicalmalwareanalysis.com)

# Laboratorium 3.3

## 1. Analiza Process Explorer

Program przez krótki czas się pojawia w Process Explorer tworzy wtedy też nowy proces- svchost.exe, lecz szybko znika prawdopodobnie zamieniając się w svchost.exe. PID tego procesu to 1944.

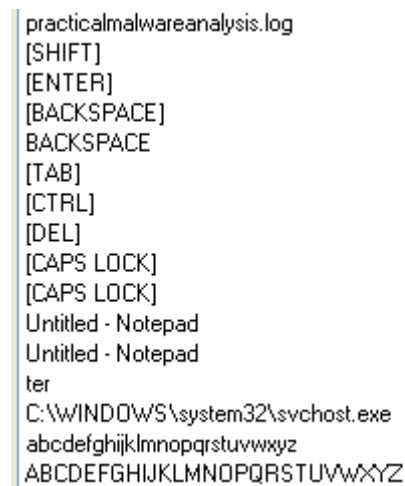


Lab03-03.exe	1.00	268 K	960 K	2476
svchost.exe	2.00	828 K	2,152 K	1944 Generic Host Process for Wi... Micros

Screenshot07 - Process Explorer, Process

## 2. Modyfikacje pamięci

Porównując obraz dysku z obrazem pamięci możemy zauważyć, że w obrazie pamięci znajdują się np. 'practicalmalwareanalysis.log', a także przyciski [SHIFT] [TAB] czy [CAPS LOCK], a także wszystkie litery klawiatury w postaci małej i dużej.



```
practicalmalwareanalysis.log
[SHIFT]
[ENTER]
[BACKSPACE]
BACKSPACE
[TAB]
[CTRL]
[DEL]
[CAPS LOCK]
[CAPS LOCK]
Untitled - Notepad
Untitled - Notepad
ter
C:\WINDOWS\system32\svchost.exe
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

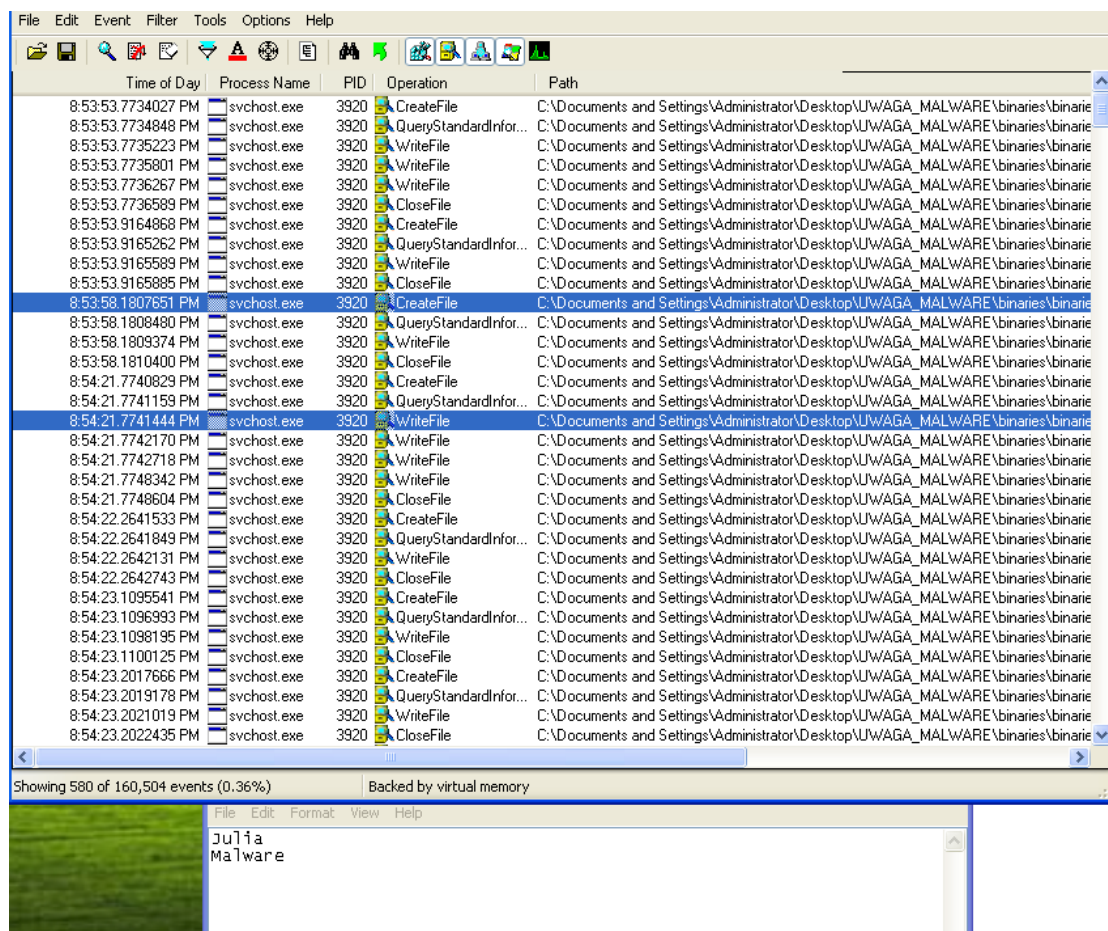
Screenshot08 - Process Explorer

## 3. Indykatory hostowe

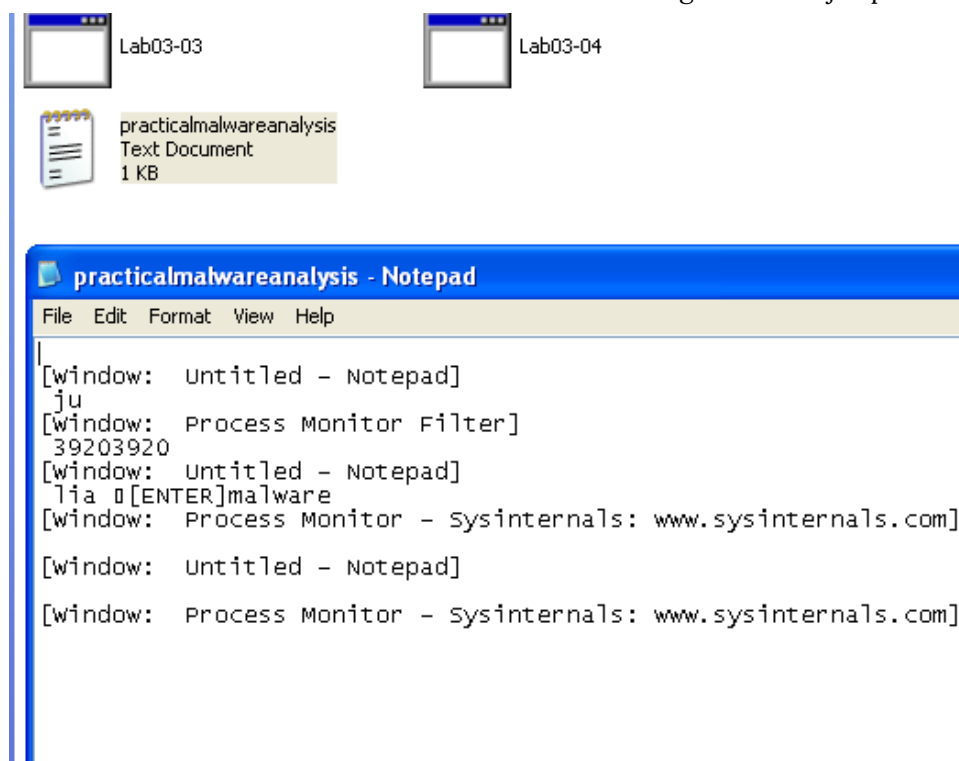
*practicalmalwareanalysis.log*

## 4. Działanie programu

Program odczytuje wszystkie znaki wprowadzone przez klawiaturę, także te napisane poza jakimkolwiek dokumentem czy cmd. Następnie zapisuje te znaki/whitespacy w pliku utworzonym w tym samym folderze w którym znajduje się program. Po każdym wprowadzeniu plik się modyfikuje. Jeżeli haker zdobyłby ten plik mógłby on dostać się do informacji m.in. o loginach i hasłach użytkownika.



Screenshot09 - Process Monitor, ukazanie stworzenia pliku tekstowego i zapisaniu do niego informacji wprowadzanych z klawiatury



Screenshot10 - Plik tekstowy wygenerowany przez malware z pliku Lab03-03.

# Laboratorium 3.4

## 1. Informacje o pliku

W PE możemy zauważyć sporo funkcji sieciowych (socket, send, connect).

Znajduje się także string z URL [practicalmalwareanalysis.com](http://www.practicalmalwareanalysis.com)

DeleteService	×	implicit	-	advapi32.dll
ShellExecuteA	×	implicit	-	shell32.dll
22 (shutdown)	×	implicit	×	ws2_32.dll
115 (WSAStartup)	×	implicit	×	ws2_32.dll
52 (gethostbyvalue)	×	implicit	×	ws2_32.dll
19 (send)	×	implicit	×	ws2_32.dll
23 (socket)	×	implicit	×	ws2_32.dll
9 (htons)	×	implicit	×	ws2_32.dll
4 (connect)	×	implicit	×	ws2_32.dll
3 (closesocket)	×	implicit	×	ws2_32.dll
16 (recv)	×	implicit	×	ws2_32.dll
116 (WSACleanup)	×	implicit	×	ws2_32.dll

Screenshot11 - pestudio, podejrzone funkcje pliku

-----
<a href="http://www.practicalmalwareanalysis.com">http://www.practicalmalwareanalysis.com</a>
SOFTWARE\Microsoft \XPS
NOTHING

Screenshot 12 - pestudio, podejrzaný string z URL

## 2. Zdarzenia towarzyszące uruchomieniu pliku

Plik z programem usunął się z danej lokalizacji. Poza tym nie znalazłam, żadnych informacji ani w PEview, ani w Wiresharku, ani w PEstudio

## 3. Blokada analizy dynamicznej

Program usuwa sam siebie z dysku przez co nie możemy go drugi raz otworzyć. Blokada ta może być spowodowana tym, że program wykrywa, że jest na maszynie wirtualnej.