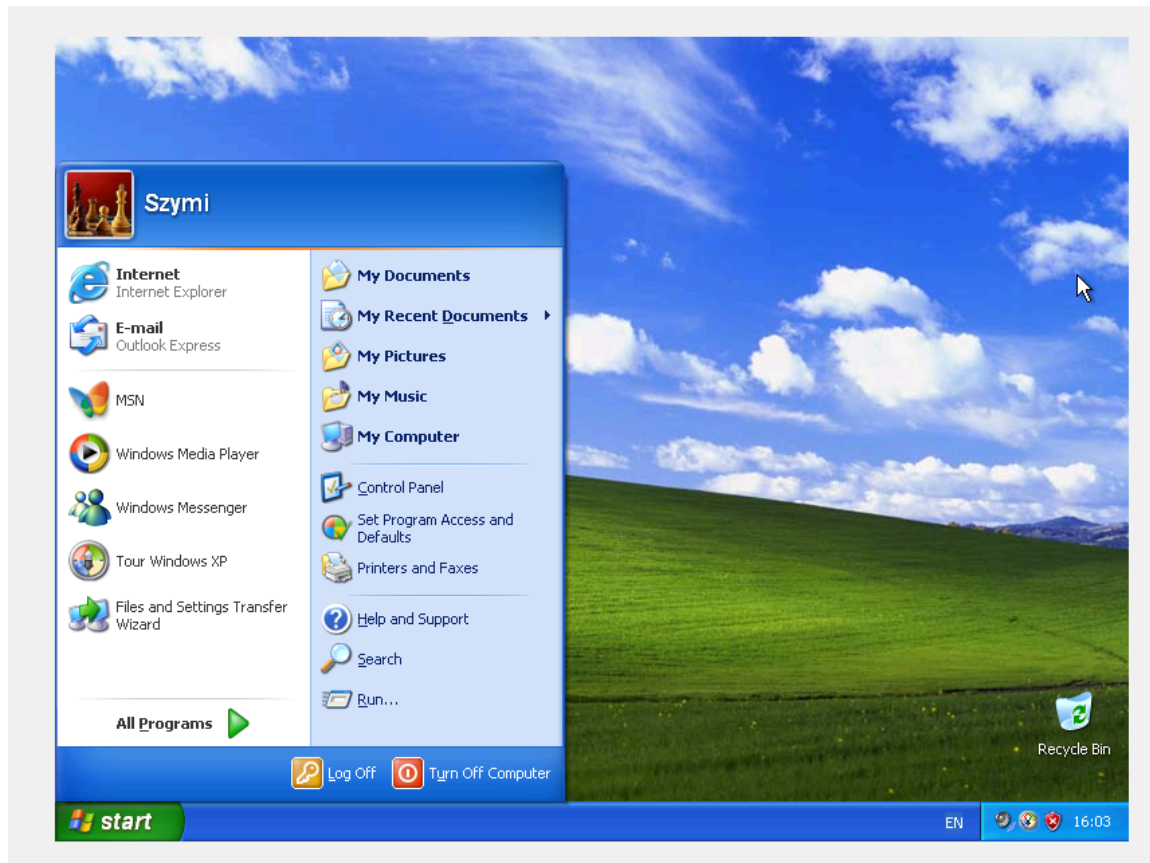
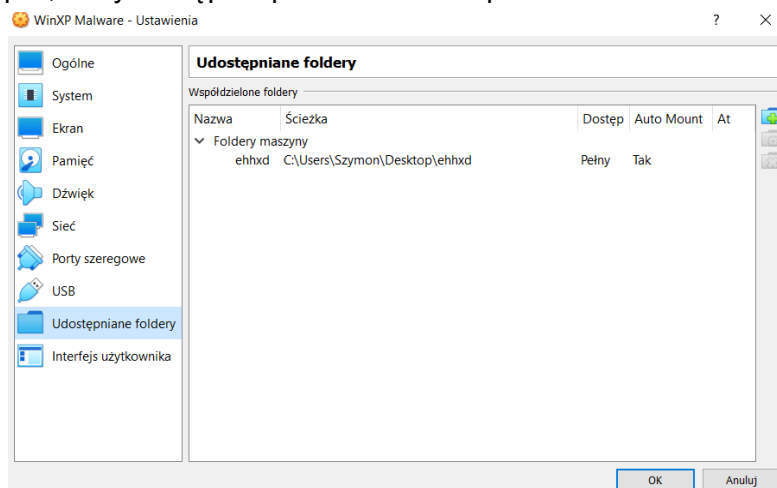


Szymon Kozioł

Na początku postawiłem system Windows XP na VirtualBox'ie. Nie zrobiłem tego na pierwszych zajęciach, ponieważ czekałem, aż w końcu będzie potrzebny.



Podpiąłem mój pendrive do stacji z Windowsem 10, aby móc pobrać paczkę wirusów. Zmiany w rejestrze i Windows defenderze na tym systemie pomogły mi sprawnie pobrać plik, który następnie przerzuciłem na pendrive.





ten komputer

Plik Komputer Widok

Ten komputer

Szybki dostęp

- Pulpit
- Pobrane
- Dokumenty
- Obrazy
- Muzyka
- Wideo

Ten komputer

- Dokumenty
- Muzyka
- Obiekty 3D
- Obrazy
- Pobrane
- Pulpit
- Wideo
- Dysk lokalny (C:)
- Stacja dysków CD (I)
- Dysk USB (E:)
- Dysk USB (E:)

Foldery (7)

- Dokumenty
- Obiekty 3D
- Pobrane
- Wideo

Urządzenia i dyski (3)

- Dysk lokalny (C:)
56,1 GB wolnych z 89,4 GB
- Dysk USB (E:)
58,5 GB wolnych z 58,5 GB

Narzędzia główne Udostępnianie Widok

Ten komputer > Pobrane

Nazwa

Dzisiaj (1)

- binaries.zip

W ubiegłym miesiącu

- winrar-x64-624pl.exe
- desktop.ini

Szybki dostęp

- Pulpit
- Pobrane
- Dokumenty
- Obrazy
- Muzyka
- Wideo

ten komputer

- Dokumenty
- Muzyka
- Obiekty 3D
- Obrazy
- Pobrane
- Pulpit
- Wideo

Wypakowywanie

Narzędzia folderów skompresowanych

Ten komputer > Dysk USB (E:)

Nazwa

Data modyfikacji

Typ

System Volume Information	29.04.2024 14:03	Fold
binaries.zip	29.04.2024 15:09	Arch

Szybki dostęp

- Pulpit
- Pobrane
- Dokumenty
- Obrazy
- Muzyka
- Wideo

Ten komputer

- Dokumenty
- Muzyka
- Obiekty 3D
- Obrazy
- Pobrane
- Pulpit

Do wirtualnej maszyny z systemem Windows XP dodałem współdzielony folder, dzięki któremu przerzuciłem na system wszystkie potrzebne programy oraz sam plik z wirusami.

Nazwa	Ścieżka	Dostęp	Auto Mount	At
▼ Foldery maszyny				
ehhxd	C:\Users\Szymon\Desktop\ehhxd	Tylko do odczytu	Tak	

Zadbałem, aby był w wersji tylko do odczytu, aby zapobiec jakimukolwiek dostępowi maszyny do mojego natywnego komputera.



Po zainstalowaniu programów zmieniłem jeszcze kartę sieciową na host-only i wykonałem bardzo istotną migawkę.

Strings:

"import":

Sugeruje, że plik zawiera importowane funkcje lub biblioteki.

"utility":

Wskazuje na możliwość zawierania w pliku funkcji użytkowych lub narzędziowych.

"registry":

Znaczenie: Wskazuje na obecność danych dotyczących rejestru systemowego.

"size":

Znaczenie: Odnosi się do wielkości lub rozmiaru danych.

"CONNECT %s:%i HTTP/1.0\r\n\r\n":

Sugeruje, że plik może próbować nawiązać połączenia sieciowe za pomocą protokołu HTTP, używając określonego formatu połączenia.

Wpisy rejestru systemowego:

"SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders":

Wskazuje na potencjalne interakcje z rejestrem systemowym, w szczególności na modyfikacje ustawień Exploratora Windows.

"SOFTWARE\Classes\http\shell\open\command\V":

Sugeruje, że plik może próbować modyfikować ustawienia związane z przeglądaniem stron internetowych.

"SOFTWARE\Microsoft\Windows\CurrentVersion\Run":

Wskazuje na interakcje z sekcją rejestru odpowiedzialną za automatyczne uruchamianie programów przy starcie systemu.

Adresy internetowe:

"www.practicalmalwareanalysis.com":

Adres URL wskazujący na stronę z zasobami dotyczącymi analizy złośliwego oprogramowania. Może sugerować połączenia zewnętrzne lub odniesienie do zasobów edukacyjnych.

Pliki:

"vmx32to64.exe":

Sugeruje obecność lub interakcję z plikiem wykonywalnym.

Komunikaty systemowe:

"This program cannot be run in DOS mode":

2)

Wyżej wspomniany plik:

C:\WINDOWS\System32\vmx32to64.exe

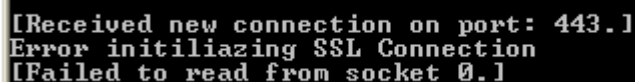
Plik "Lab03-01.exe" skopiował sam siebie do katalogu "C:\WINDOWS\System32" jako "vmx32to64.exe".

Hash pliku skopiowanego i oryginalnego jest taki sam (d537acb8f56a1ce206bc35cf8ff959c0), co potwierdza identyczność plików.

(VirusTotal podaje, że to Trojan)

Plik utworzył wpis w rejestrze systemowym pod ścieżką "SOFTWARE\Microsoft\Windows\CurrentVersion\Run".

3)



```
[Received new connection on port: 443.]  
Error initializing SSL Connection  
[Failed to read from socket 0.]
```

Po uruchomieniu pliku - FakeNet wykrył, że malware próbował się połączyć na porcie 443.

Jest to prawdopodobnie jest to próba nawiązania połączenia do wyżej wspomnianego URL:

www.practicalmalwareanalysis.com

3.2

1)

symbol (85)	location	blacklisted (43)
GetStartupInfoA	00005548	×
CreatePipe	0000555A	×
CreateProcessA	00005536	×
SetLastError	0000559C	×
OutputDebugStringA	000055AC	×
GetTempPathA	0000550C	×
LoadLibraryA	000054E8	×
GetProcAddress	000054D6	×
CreateThread	000054C6	×
TerminateThread	0000548E	×
Sleep	00005486	×
GetModuleFileNameA	00005470	×
OpenServiceA	0000568C	×
DeleteService	0000567C	×
OpenSCManagerA	00005638	×
CreateServiceA	00005626	×
CloseServiceHandle	00005610	×
RegCreateKeyA	00005600	×
RegSetValueExA	000055EE	×
RegisterServiceCtrlH...	000055D0	×
SetServiceStatus	0000569C	×
11	8000000B	×
WSASocketA	000056BE	×
3	80000003	×
4	80000004	×
10	8000000A	×
19	80000013	×
18	80000012	×

W zasadzie wszystkie istotne funkcje znajdują się na czarnej liście.

Znajdują się tam, ponieważ są one uznawane za podejrzane lub potencjalnie szkodliwe w kontekście analizowanego oprogramowania. Ich obecność może sugerować, że program lub moduł, z którym są związane, może być złośliwy lub próbuje wykonać działania niepożądane dla użytkownika lub systemu.

Oto krótkie opisy wybranych z nich:

1. SetLastError: Ta funkcja ustawia kod błędu dla ostatniej operacji.
2. GetTempPathA: Zwraca ścieżkę do katalogu tymczasowego w formacie ANSI.
3. LoadLibraryA: Służy do załadowania biblioteki dynamicznej do pamięci.
4. GetStartupInfoA: Pobiera informacje o starcie procesu, takie jak rozmiar okna konsoli i flagi.

5. CreateProcessA: Tworzy nowy proces i jego wątek wykonywalny.
6. OutputDebugStringA: Wysyła ciąg znaków do debugera systemowego (np. do DebugView).
7. GetProcAddress: Pobiera adres procedury eksportowanej z określonej biblioteki.
8. CreateThread: Tworzy nowy wątek do wykonywania kodu.
9. TerminateThread: Natychmiast kończy wątek.
10. Sleep: Powoduje zawieszenie wątku na określony czas.
11. GetModuleFileNameA: Zwraca pełną ścieżkę do pliku wykonywalnego dla określonego modułu.
12. DeleteService: Usuwa określoną usługę z systemu.
13. OpenSCManagerA: Otwiera uchwyt do menedżera usług systemowych.
14. CreateServiceA: Tworzy nową usługę systemową.
15. RegCreateKeyA: Tworzy lub otwiera klucz w rejestrze systemowym.
16. RegSetValueEXA: Ustawia wartość dla określonego klucza rejestru.
17. RegisterServiceCtrlHandler: Rejestruje funkcję obsługi sterowników usług.
18. SetServiceStatus: Ustawia stan usługi w systemie.
19. WSASocketA: Tworzy "gniazdo" dla funkcji Windows Sockets (WSA).

2)

```
C:\Documents and Settings\Szymi\Desktop\binaries>rundll32.exe Lab03-02.dll, Install
```

Taka komenda w shellu zainstaluje go.

3)

net start IPRIP

4)

Mając program Process Explorer można wyszukać frazę zawierającą słowo Lab.

process.exe	1100	3 732 K
Lab03-01.exe	1400	624 K
explorer.exe	1572	3 084 K

Będziemy wtedy w stanie dowiedzieć się jakie jest PID procesu(tutaj na przykładzie Lab03-01.exe).

5)

DLL i opcjonalnie IPRIP powinny zadziałać, natomiast u mnie najlepiej sprawdził się filtr do PID.

The screenshot shows the 'Process Monitor Filter' dialog box. The 'Display entries matching these conditions:' section shows a filter: 'PID is [] then Include'. Below this, there is a list of filters to be applied. The list has columns for 'Column', 'Relation', 'Value', and 'Action'. The filters are:

Column	Relation	Value	Action
Process ...	is	Procmon.exe	Exclude
Process ...	is	Procexp.exe	Exclude
Process ...	is	Autoruns.exe	Exclude
Process ...	is	System	Exclude
Operation	begins with	IRP_MJ_	Exclude
Operation	begins with	FASTIO_	Exclude

Buttons: Reset, Add, Remove, OK, Cancel, Apply.

In the background, a list of events is visible, showing 'lsass.exe' with PID 668 performing 'RegOpenKey' and 'RegCloseKey' operations on 'HKLM\SECURITY\Policy\SecDesc' with 'SUCCESS' results.

6)

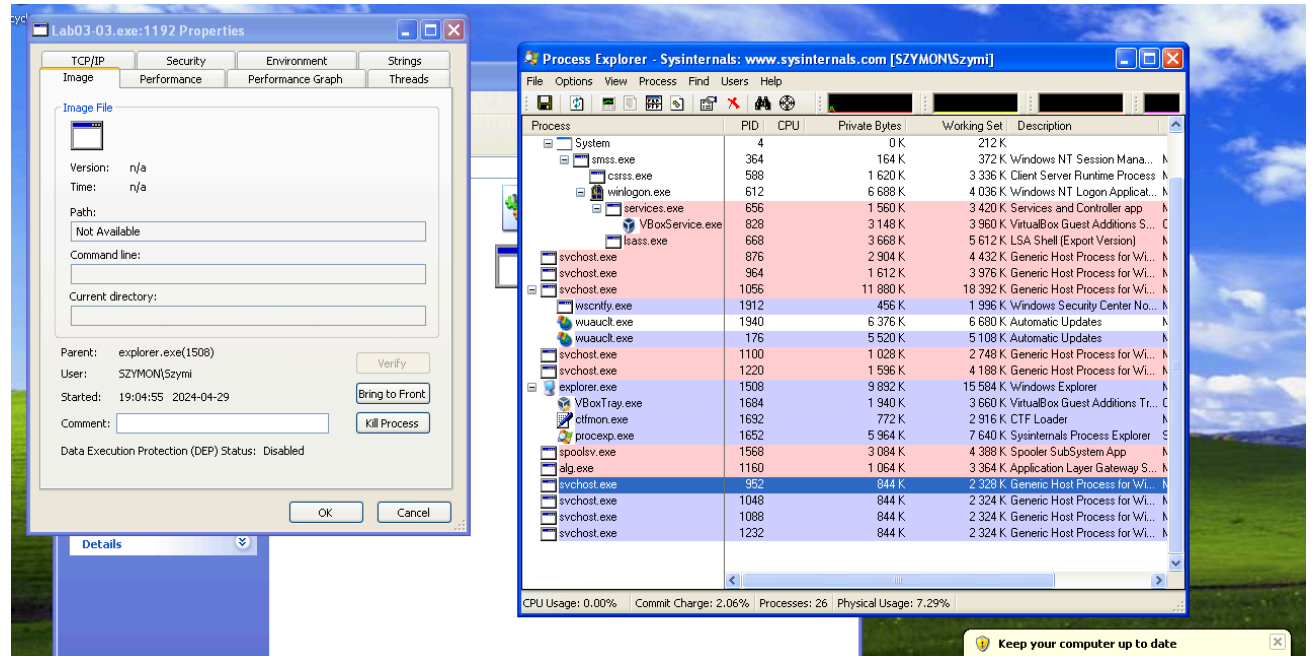
Usługa wysyła żądania DNS do practicalmalwareanalysis.com.

Usługa wysyła pojedyncze żądanie HTTP GET dla pliku /serve.html.

Usługa wysyła kilka pakietów do 80/tcp.

3.3

1)

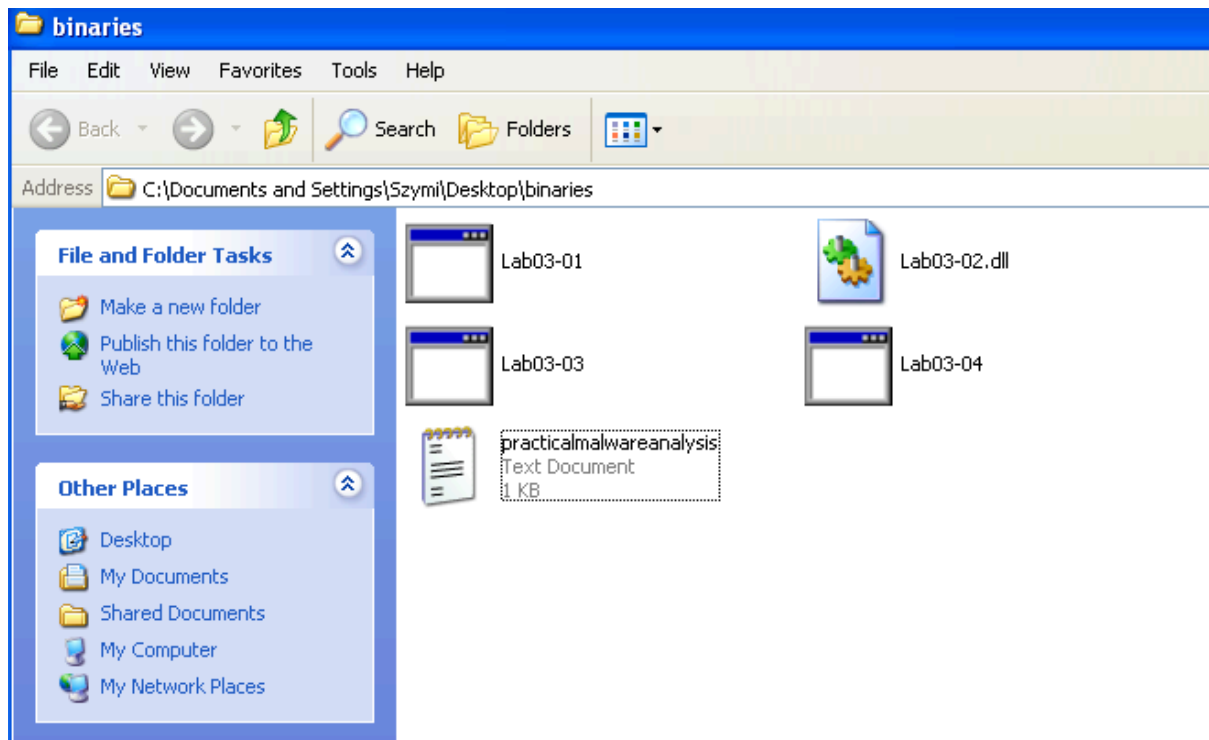


Gdy uruchomimy plik powstanie proces nazwany svchost.exe(w moim przypadku kilka, ponieważ kliknąłem parę razy, myśląc, że się nie uruchamia). Nie zauważyłem tego dlatego, że oryginalny program zakończył działanie, ale zdążył w tym czasie utworzyć proces.

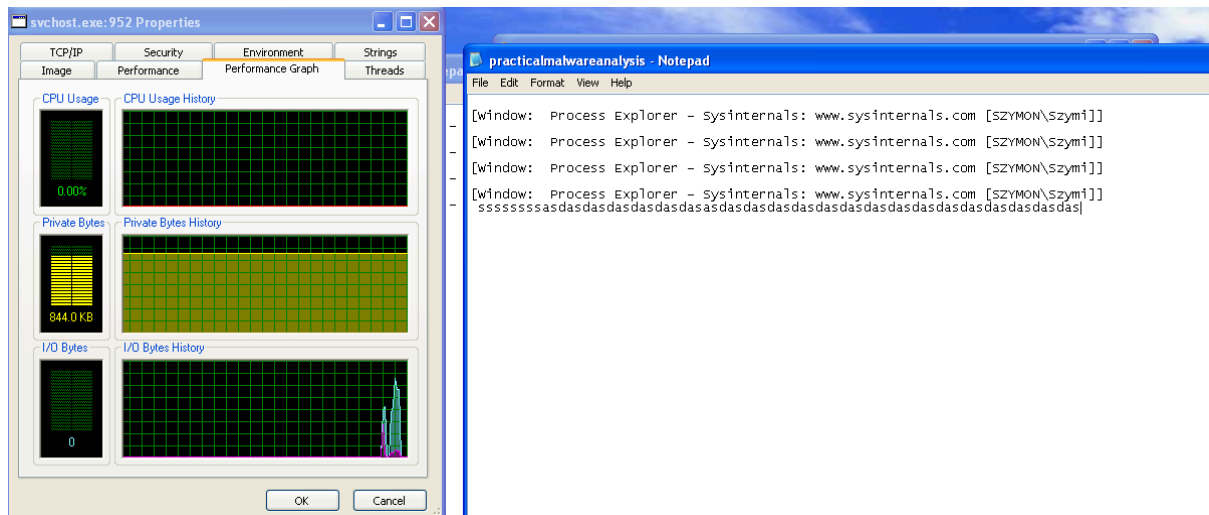
alg.exe	1100	1 032 K	3 330 K Application Layer Gateway S...
svchost.exe	952	844 K	2 364 K Generic Host Process for Wi...
svchost.exe	1048	844 K	2 368 K Generic Host Process for Wi...
svchost.exe	1088	844 K	2 368 K Generic Host Process for Wi...
svchost.exe	1232	844 K	2 368 K Generic Host Process for Wi...

Przeanalizuje ten o PID równym 952, ponieważ wszystkie są praktycznie jednakowe.

W Moim folderze binaries powstał plik .txt o nazwie practicemalwareanalysis.

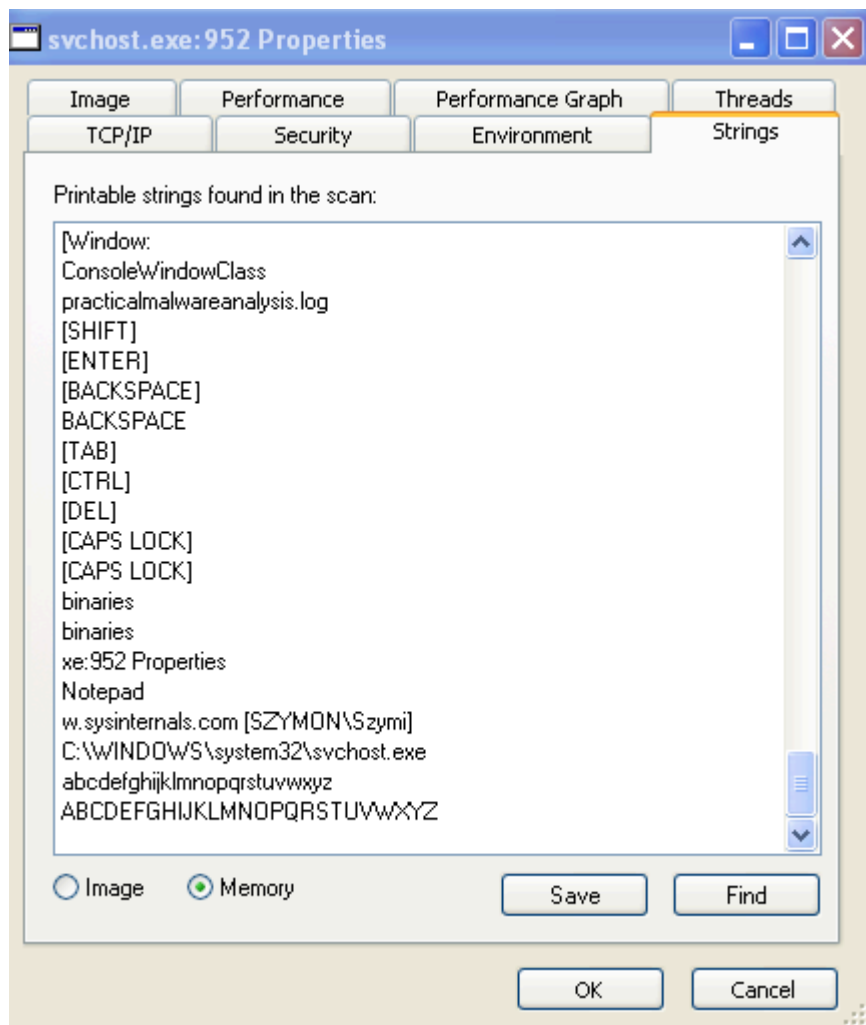


Zaobserwowałem skoki w operacjach wejścia-wyjścia na dysku podczas nadpisywania tego pliku.



2)

Znowu za pomocą Process Explorer:



Prawdopodobnie jest to keylogger o czym świadczą modyfikacje pamięci ze screena oraz wcześniej wspomniane skoki na dysku w operacjach wejścia-wyjścia podczas pisania.

3)

1. powstały proces svchost.exe
2. plik .txt o nazwie practicemalwareanalysis w folderze binaries

4)

To musi być keylogger - tak jak wcześniej zasugerowałem.

GetStringTypeA
GetStringTypeW
"

Odnalezienie tych funkcji tylko utwierdziło mnie w przekonaniu.

3.4

1)

Zaimportowane biblioteki:

library (4)	duplicate (0)	flag (1)	fi
KERNEL32.dll	-	-	0
ADVAPI32.dll	-	-	0
SHELL32.dll	-	-	0
WS2_32.dll	-	x	0

Ich funkcje:

imports (87)	flag (28)	first-thunk-orig
WaitForSingleObject	-	0x0000BAEE
OpenSCManagerA	-	0x0000B97E
OpenServiceA	-	0x0000B96E
ChangeServiceConfigA	x	0x0000B956
CloseServiceHandle	-	0x0000B940
CreateServiceA	x	0x0000B92E
DeleteService	x	0x0000B990
RegDeleteValueA	x	0x0000B91C
RegCreateKeyExA	x	0x0000B90A
RegSetValueExA	x	0x0000B8F8
RegOpenKeyExA	-	0x0000B8E8
RegQueryValueExA	-	0x0000B8D4
GetSystemDirectoryA	-	0x0000B820
GetTimeZoneInformation	-	0x0000BA0C
GetSystemTime	-	0x0000BA26
GetLocalTime	-	0x0000BA36
GetStartupInfoA	-	0x0000BAB8
GetEnvironmentVariableA	x	0x0000BBEC
GetVersionExA	-	0x0000BC06
22 (shutdown)	x	0x80000016
115 (WSAStartup)	x	0x80000073
52 (gethostbyname)	x	0x80000034

Opis wybranych funkcji:

WaitForSingleObject: Czeka na określony obiekt, taki jak proces, wątek czy zdarzenie, aż ten osiągnie stan zasygnalizowany. Funkcja ta jest często używana do synchronizacji wykonania.

OpenSCManagerA: Otwiera połączenie z Menedżerem Usług Systemu Windows (SCM), który zarządza usługami na systemie.

OpenServiceA: Otwiera istniejącą usługę na podstawie jej nazwy i zwraca uchwyt do interakcji z nią.

ChangeServiceConfigA: Modyfikuje parametry konfiguracji istniejącej usługi, takie jak typ uruchamiania, zależności usług i poświadczenia.

CloseServiceHandle: Zamykają uchwyt otwarty na usługę lub połączenie SCM, zwalniając zasoby systemowe.

CreateServiceA: Tworzy nową usługę i rejestruje ją w SCM.

RegCreateKeyExA: Tworzy nowy klucz rejestru lub otwiera istniejący, zwracając uchwyt do niego.

RegSetValueExA: Ustawia wartość klucza rejestru, umożliwiając konfigurację lub przechowywanie danych.

GetSystemDirectoryA: Zwraca ścieżkę do katalogu systemowego Windows, zawierającego pliki systemowe i pliki wykonywalne.

GetTimeZoneInformation: Zwraca informacje o bieżącej strefie czasowej ustawionej na systemie.

WSAStartup: Inicjuje API Windows Sockets, pozwalając programowi korzystać z funkcji sieciowych, takich jak komunikacja TCP/IP.

W stringsach możemy znaleźć bardzo wiele dodatkowych ciekawych funkcji:

value
UnhandledExceptionFilter
GetModuleFileName
GetModuleHandle
GetProcAddress
LoadLibrary
GetLastError
CreatePipe
SetStdHandle
GetStdHandle
CMD
DOWNLOAD
UPLOAD
cmd.exe
/c del
SOFTWARE\Microsoft \XPS
CloseHandle
ExpandEnvironmentStrings
DuplicateHandle
GetVersion
SetHandleCount
GetCPInfo
GetOEMCP
WideCharToMultiByte
RtlUnwind
MultiByteToWideChar
LCMapString
LCMapString
CompareString

2)

FakeNet nic nie zaobserwował.

Nic nie zmieniło się w rejestrze.

Program stworzył proces, a następnie usunął się.

3)

Program samoistnie usuwa się z dysku twardego. Prawdopodobnie nie jest przeznaczony dla tego środowiska.

4)

Można by wrzucić ten program do jakiegoś debuggera lub programu, który zasymuluje jego działanie.