

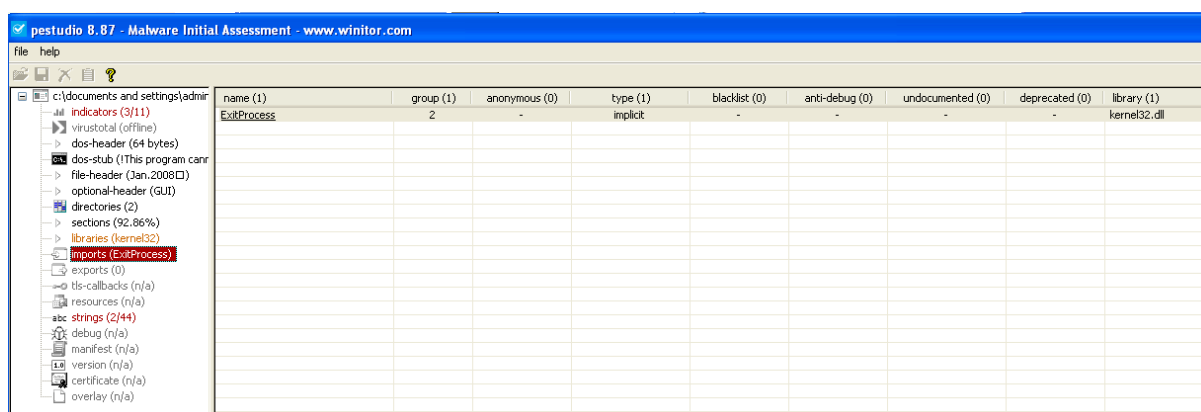
Analiza dynamiczna

Arkadiusz Ryba

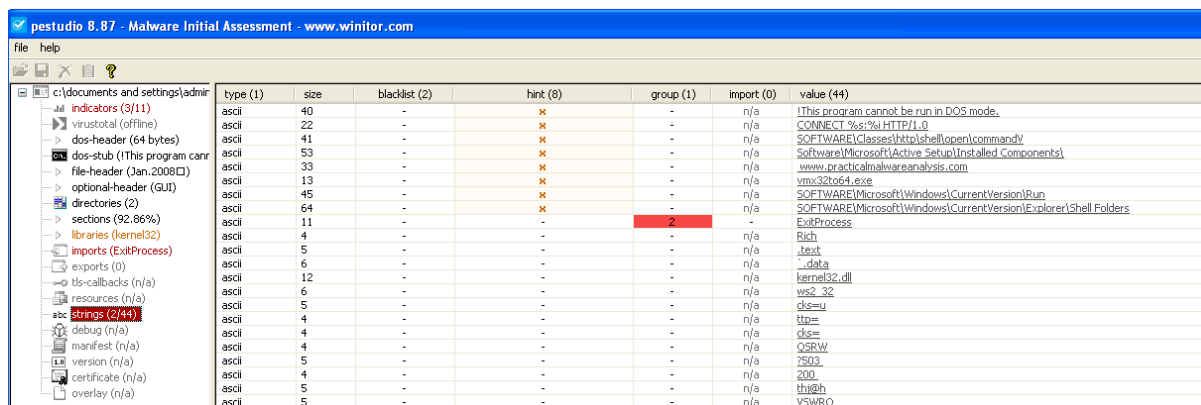
Laboratorium 3.1

Przeprowadź analizę złośliwego oprogramowania znajdującego się w pliku Lab03-01.exe. Wykorzystaj do tego celu podstawowe narzędzia do analizy dynamicznej. Odpowiedz na poniższe pytania:

1. Jakie importy i łańcuchy jesteśmy w stanie odszukać w tym pliku?



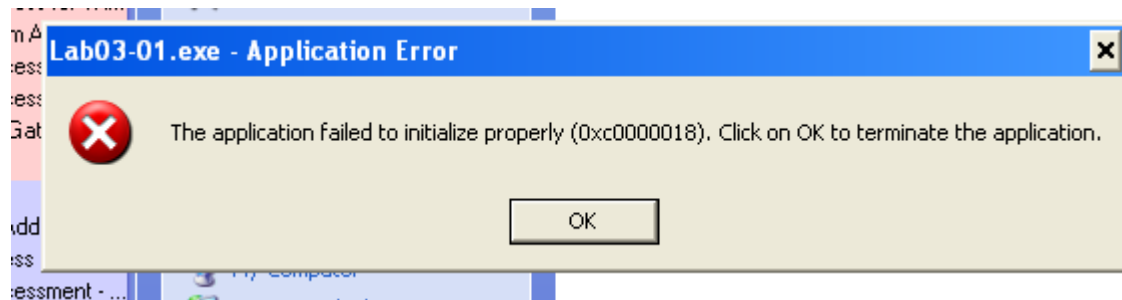
Program **pestudio** wskazał odniesienie jedynie do jednego importu - **ExitProcess** i biblioteki **kernel32.dll**. Jest to naprawdę mała liczba a tym samym podejrzane - najprawdopodobniej plik jest jakoś spakowany.



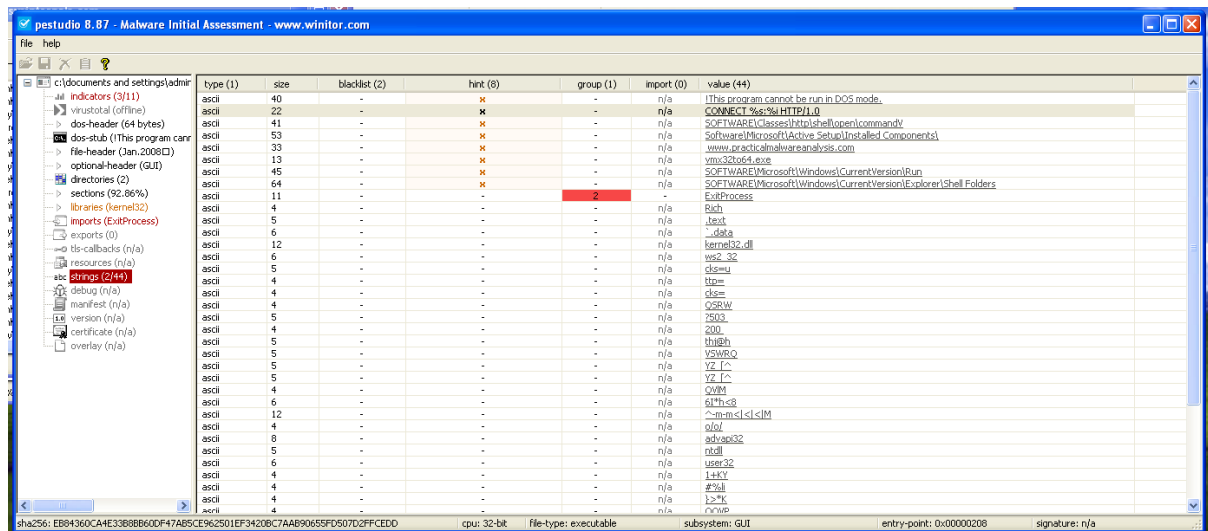
Również brak importów w stringsach

2. Podaj wszystkie indykatory hostowe związane z tym programem.

Niestety nie byłem w stanie uruchomić programu



Aczkolwiek udało mi się znaleźć coś podejrzanego



Program próbuje się z czymś połączyć po protokole **HTTP** w wersji 1

3. Czy wśród zebranych informacji znajdują się jakieś pomocne indykatory sieciowe mogące opisać analizowane złośliwe oprogramowanie?

Jedynie domena znaleziona w poprzednim podpunkcie

Laboratorium 3.2

Przeprowadź analizę złośliwego oprogramowania znajdującego się w pliku Lab03-02.dll. Wykorzystaj w tym celu podstawowe narzędzia do analizy dynamicznej. Odpowiedz na poniższe pytania:

1. Wypisz najistotniejsze funkcje analizowanego pliku. Które z nich znajdują się na czarnej liście i dlaczego?

Funkcji jest naprawdę sporo - aż 85

Na czarnej liście znalazło się 31 funkcji m.in. funkcje odpowiedzialne za odczytywanie rejestru, obsługę systemu plików, połączenia (sockety), zamykanie systemu

2. W jaki sposób można zmusić program malware do instalacji?

e help
🔍 📁 🗑️ 📄

c:\documents and settings\admin\

- all indicators (318)
- virustotal (offline)
- > dos-header (64 bytes)
- dos-stub (This program can't be started)
- > file-header (Sep.2010)
- > optional-header (GUI)
- directories (4)
- > sections (95.74%)
- > libraries (2/5)
- imports (31/85)
- exports (5)
- tls-callbacks (n/a)
- resources (n/a)
- strings (27259)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (unknown)

ordinal (5)	name (5)	location	duplicated (0)	anonymous (0)	gap (0)	forwarded (0)
1	!rpc!	.text:10004706	-	-	-	-
2	ServiceMain	.text:10003196	-	-	-	-
3	UninstallService	.text:10004B18	-	-	-	-
4	installA	.text:10004B0B	-	-	-	-
5	uninstallA	.text:10004C2B	-	-	-	-

6256: SECCD367ED63564B4ED5C556E2363514293F614C2C2EB187273381B2EFSOF9
cpu: 32-bit
file-type: dynamic-link-library
subsystem: GUI
entry-point: 0x00004E4D
signature: Microsoft Visual C++ 6.0

Program posiada funkcje eksportujące **Install**

Można wymusić ją za pomocą narzędzia typu `rundll32`

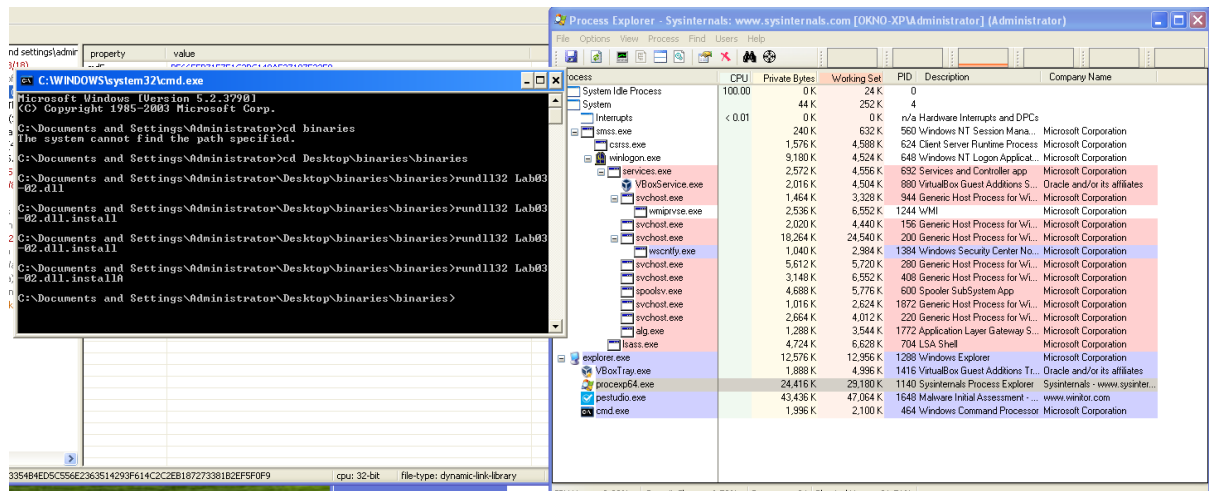
3. W jaki sposób po zainstalowaniu złośliwego oprogramowania można go uruchomić?

```
C:\Documents and Settings\Administrator>cd Desktop\binaries\binaries
C:\Documents and Settings\Administrator\Desktop\binaries\binaries>rundll32 Lab03-02.dll
```

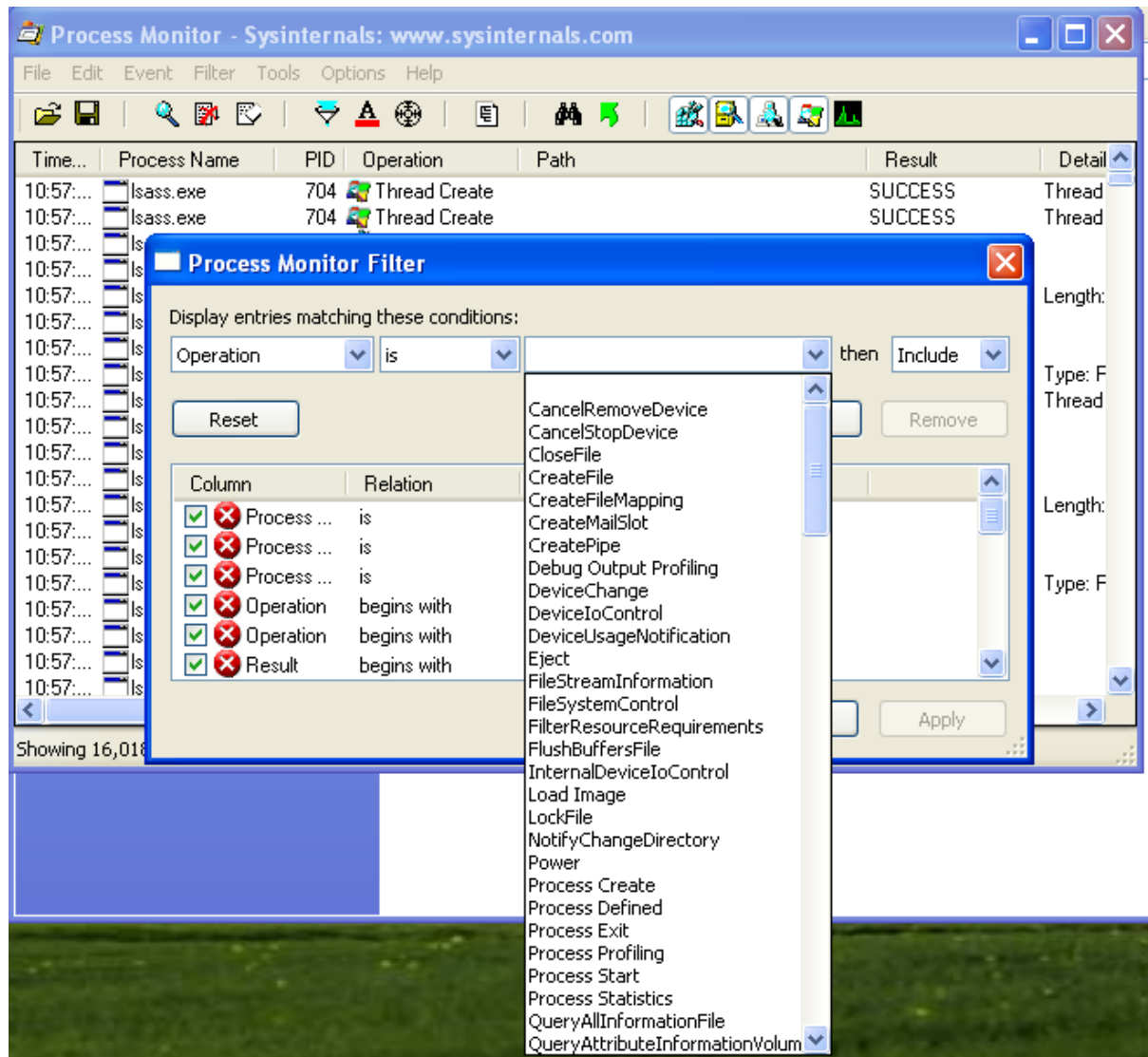
za pomocą narzędzia `rundll32`

4. Jak można odszukać proces działający jako złośliwe oprogramowanie?

W programie **Process Explorer** brak śladów działania programu, mimo wielokrotnej próby jego uruchomienia

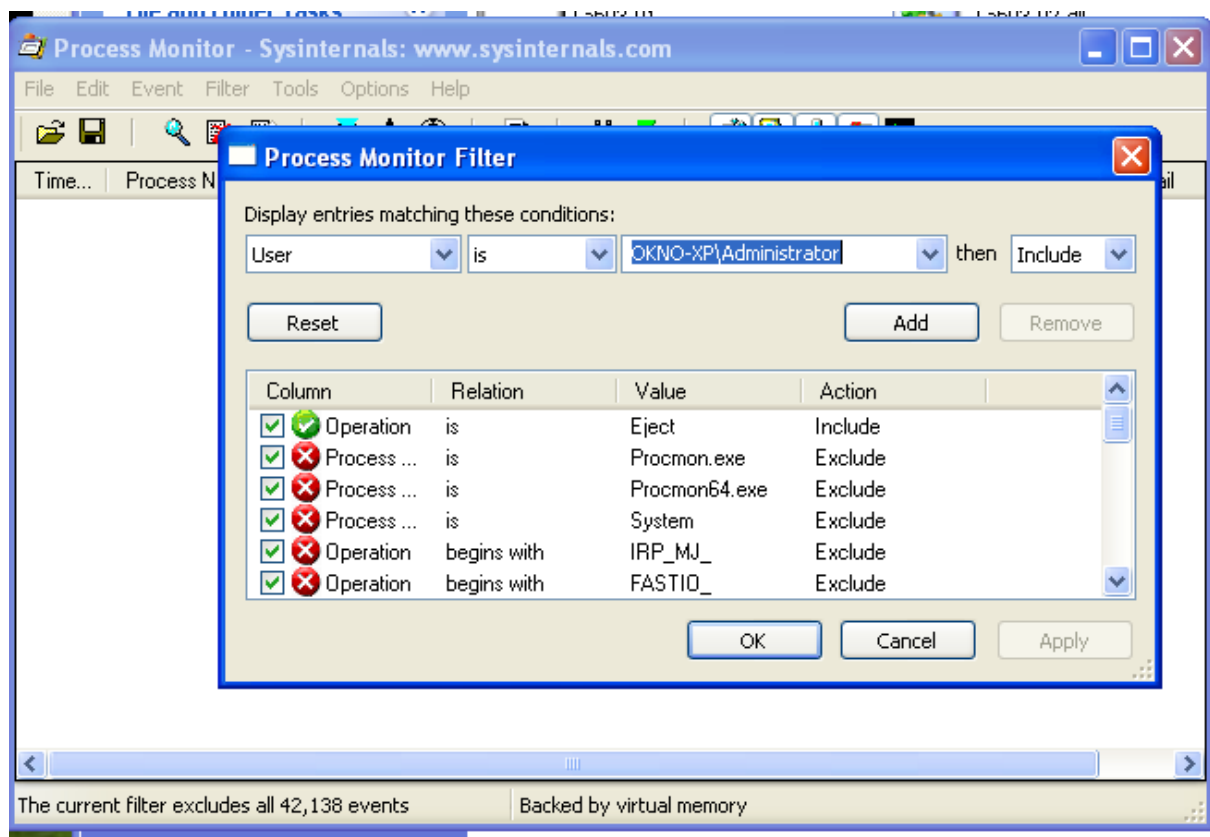


5. W celu zbierania informacji dotyczących złośliwego oprogramowania możemy wykorzystać program procmon. Jakich filtrów należy użyć, aby zebrać jak najwięcej istotnych informacji?

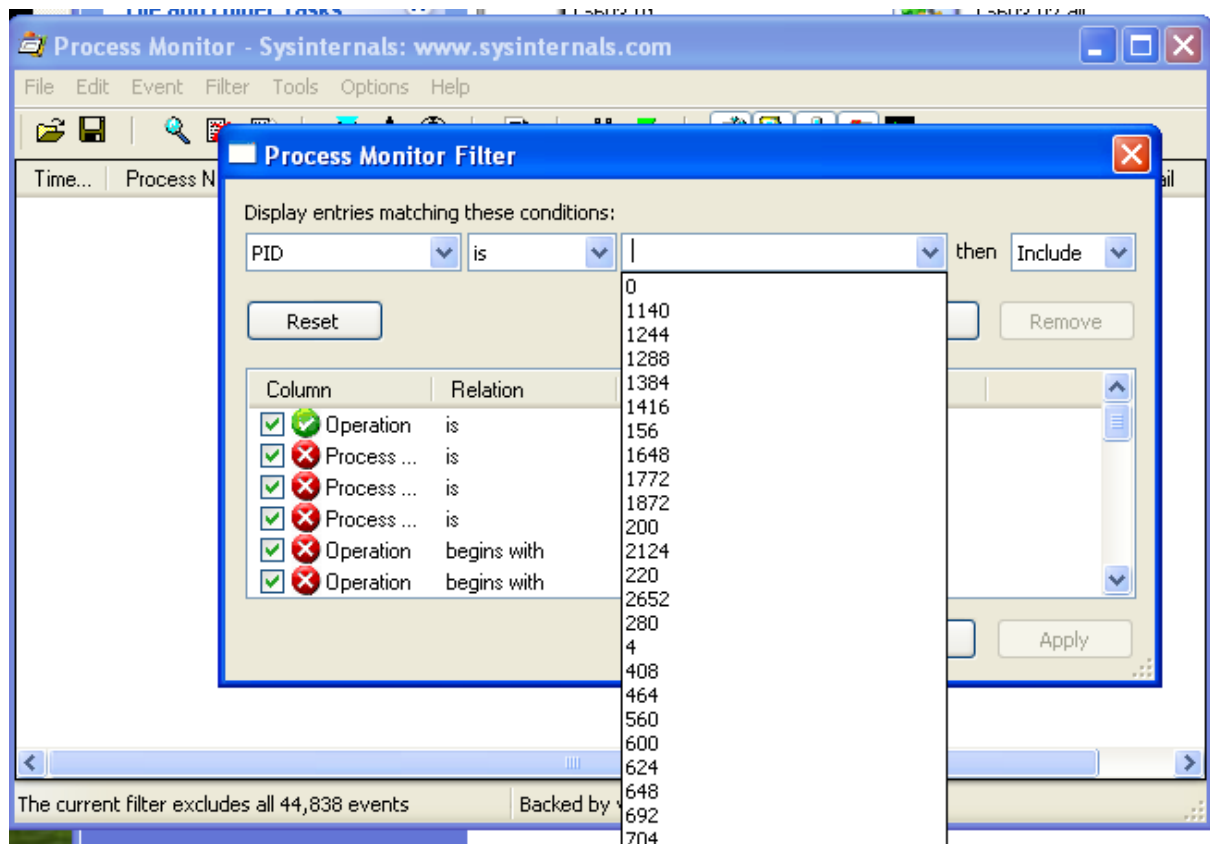


Prawdopodobniej najwięcej można odczytać filtrując po **Operation** z uwagi na możliwość wybrania danej funkcji

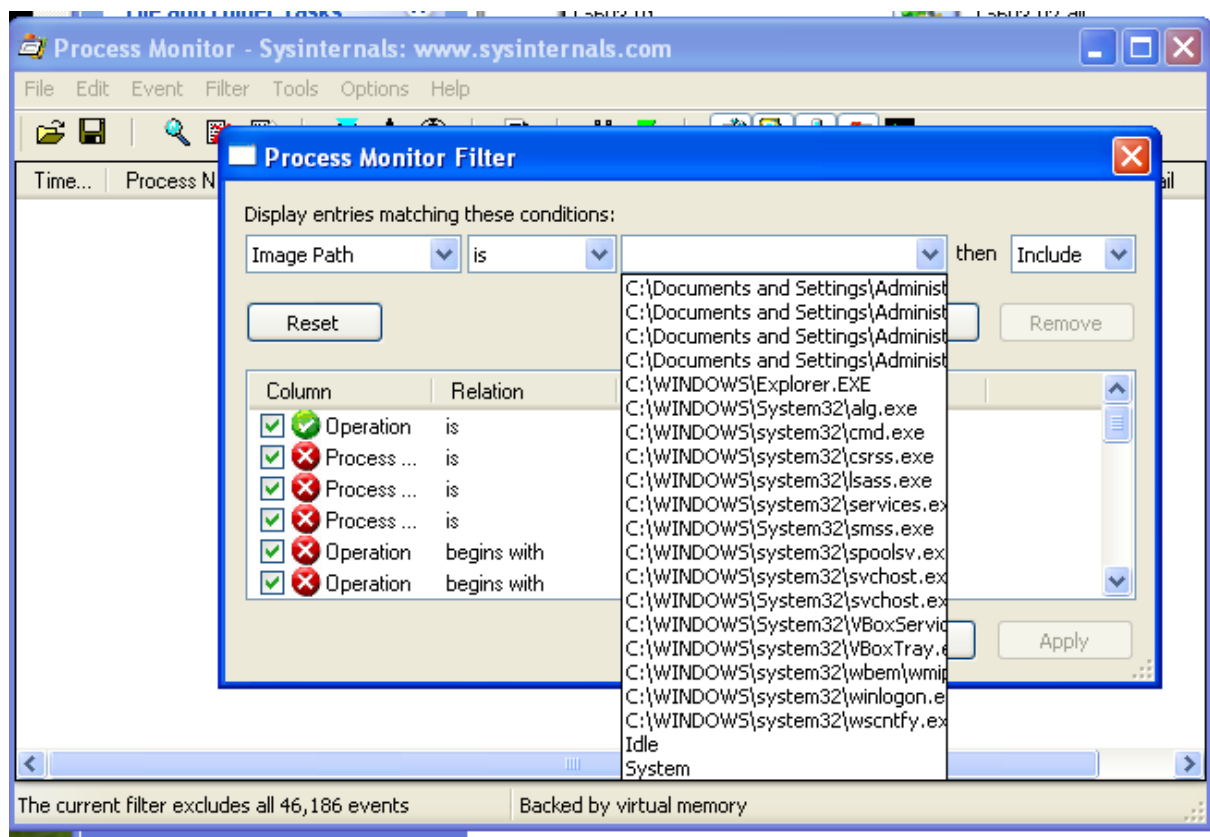
Przydatne również będzie wyświetlanie procesów tylko od jednego użytkownika



Oraz klasycznie po PID



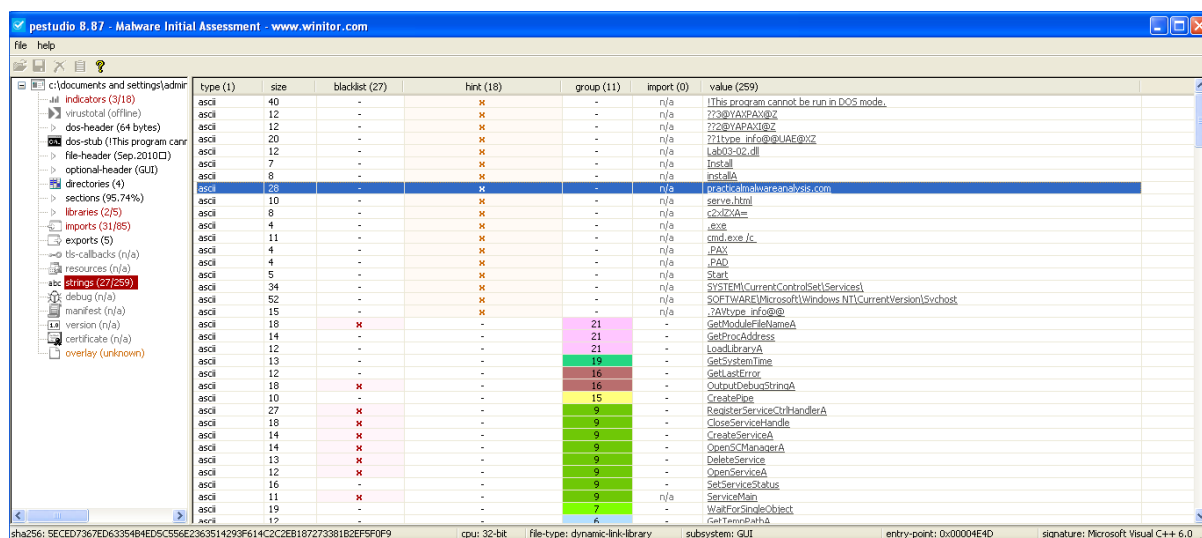
lub po ścieżce



6. Odszukaj przydatne indykatory sieciowe dla analizowanego pliku.

Z uwagi na obecne funkcje zarządzania połączeniem sieciowym program ewidentnie próbuje się z czymś połączyć

		FUNCTIONS
3	-	WSASocketA
3	-	WS2_32.dll
3	-	InternetReadFile
3	-	HttpQueryInfoA
3	-	HttpSendRequestA
3	-	HttpOpenRequestA
3	-	InternetConnectA
3	-	InternetOpenA
3	-	InternetCloseHandle
3	-	WININET.dll
2	-	Sleep
2	-	TerminateThread
2	-	CreateThread
2	-	CreateProcessA
2	-	GetStartupInfoA
2	-	GetCurrentDirectoryA
2	-	CreateProcessA
1	-	RegSetValueExA
1	-	RegCreateKeyA
1	-	RegCloseKey
1	-	RegQueryValueExA
1	-	RegOpenKeyExA



Udało się znaleźć domenę practicalmalwareanalysis.com oraz plik serve.html

Laboratorium 3.3

Przeprowadź analizę złośliwego oprogramowania znajdującego się w pliku Lab03-03.exe. Wykorzystaj do tego celu podstawowe narzędzia do analizy dynamicznej. Odpowiedz na poniższe pytania:

1. Jakie informacje jesteś w stanie odszukać w trakcie analizy pliku Lab03-03.exe przy pomocy programu Process Explorer?

Process Name	Private Bytes	Working Set	Process ID	Company Name
explorer.exe	12,112 K	20,948 K	1256	Windows Explorer
VBoxTray.exe	1,888 K	4,880 K	1384	VirtualBox Guest Additions Tr...
procexp64.exe	22,832 K	26,876 K	1480	Sysinternals Process Explorer
Lab03-03.exe	< 0.01	432 K	1,392 K	1676

Program uruchamia się po czym po bardzo krótkiej chwili się wyłącza - najprawdopodobniej żeby uniknąć odkrycia

Udało mu się jednak uruchomić inne procesy - svchost.exe

Process Name	Private Bytes	Working Set	Process ID	Company Name
winlogon.exe	9,832 K	4,348 K	628	Windows NT Logon Applicat...
services.exe	2,568 K	4,516 K	672	Services and Controller app
VBoxService.exe	1,780 K	4,004 K	892	VirtualBox Guest Additions S...
svchost.exe	1,528 K	3,356 K	940	Generic Host Process for Wi...
wmiprvse.exe	2,804 K	6,692 K	948	WMI
svchost.exe	1,908 K	4,192 K	128	Generic Host Process for Wi...
svchost.exe	20,132 K	25,140 K	184	Generic Host Process for Wi...
wscntfy.exe	1,040 K	2,924 K	960	Windows Security Center No...
svchost.exe	5,672 K	5,652 K	268	Generic Host Process for Wi...
svchost.exe	3,040 K	6,028 K	364	Generic Host Process for Wi...
spoolsv.exe	4,876 K	5,776 K	536	Spooler SubSystem App
svchost.exe	1,016 K	2,628 K	1820	Generic Host Process for Wi...
svchost.exe	2,752 K	3,996 K	1952	Generic Host Process for Wi...
alg.exe	1,292 K	3,492 K	1216	Application Layer Gateway S...
lsass.exe	5,048 K	6,672 K	700	LSA Shell

2. Odszukaj zachodzące modyfikacje pamięci.

Program pierwotnie próbował coś odczytać

Disk I/O	
Reads	1
Read Delta	0
Read Bytes	4.0 KB
Read Bytes Delta	0
<hr/>	
Writes	0
Write Delta	0
Write Bytes	0
Write Bytes Delta	0
<hr/>	
Other	0
Other Delta	0
Other Bytes	0
Other Bytes Delta	0

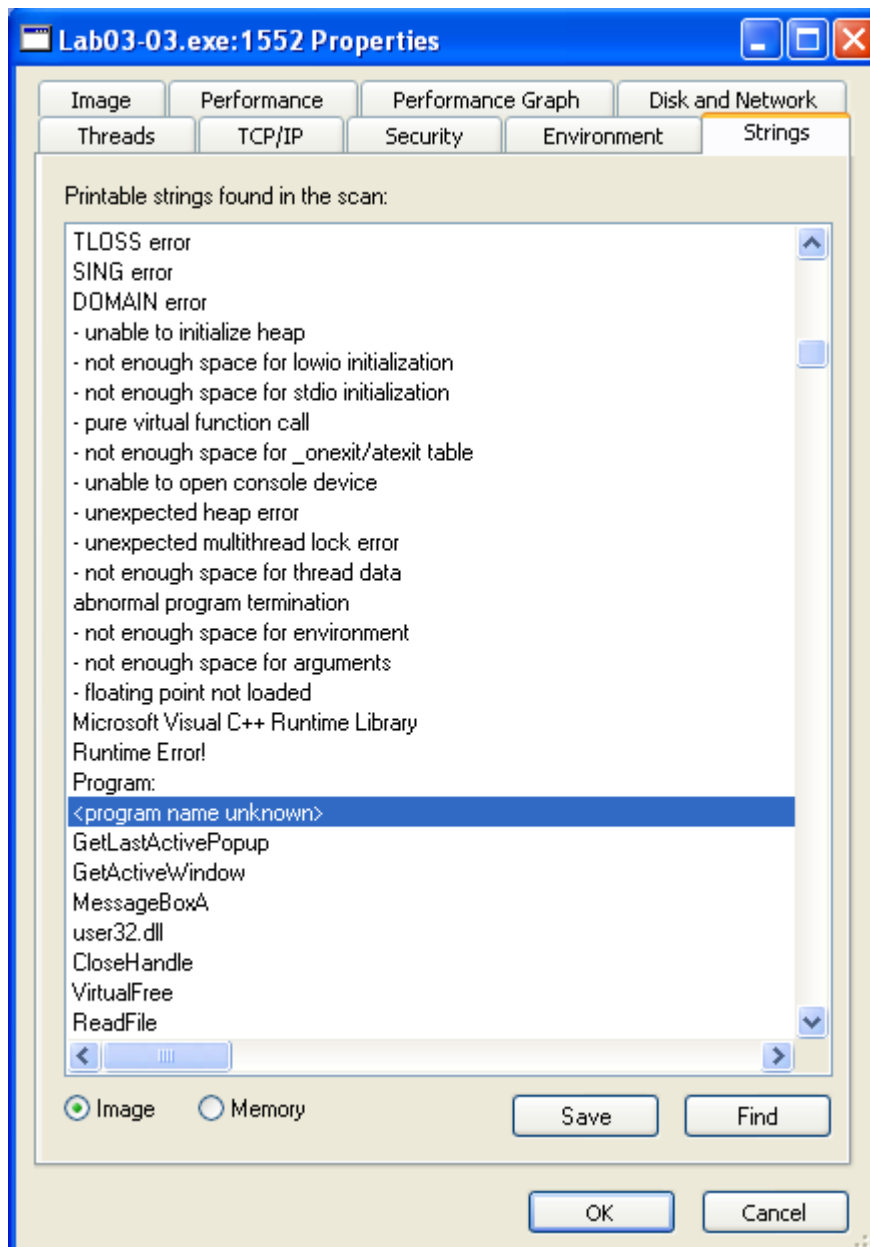


W procesie jego dziecka można zauważyć podejrzane napisy

```
[Window:
ConsoleWindowClass
practicalmalwareanalysis.log
[SHIFT]
[ENTER]
[BACKSPACE]
BACKSPACE
[TAB]
[CTRL]
[DEL]
[CAPS LOCK]
[CAPS LOCK]
```

Mogą one świadczyć o byciu **keyloggerem**

3. Wypisz indykatory hostowe należące do tego złośliwego programu.



Nie udało mi się znaleźć nic ciekawego

4. Opisz działanie tego programu.

Najpierw program uruchamia się po czym rozpoczyna kolejne procesy - po czym samoistnie się wyłącza - w celu ukrycia swojego działania. Następnie działa jak keylogger w trybie administratora, przechwytyje pewną grupę znaków.

Laboratorium 3.4

Przeprowadź analizę złośliwego oprogramowania znajdującego się w pliku Lab03-04.exe. Wykorzystaj do tego celu podstawowe narzędzia do analizy dynamicznej. Odpowiedz na poniższe pytania:

1. Zbadaj strukturę PE oraz łańcuchy pliku Lab03-04.exe. Czy plik zawiera „ciekawe” informacje?

pestudio 8.87 - Malware Initial Assessment - www.winitior.com

	type (2)	size	blacklist (31)	hint (13)	group (14)	import (0)	value (300)
	ascii	40	-	x	-	n/a	This program cannot be run in DOS mode.
	ascii	11	-	x	-	n/a	command.com
	ascii	4	-	x	-	n/a	.com
	ascii	4	-	x	-	n/a	.bat
	ascii	4	-	x	-	n/a	.cmd
	ascii	23	-	x	-	n/a	SOFTWARE\Microsoft\XP
	ascii	13	-	x	-	n/a	kernel32.dll
	ascii	4	-	x	-	n/a	GET
	ascii	8	-	x	-	n/a	DOWNLOAD
	ascii	7	-	x	-	n/a	cmd.exe
	ascii	7	-	x	-	n/a	cmd
	ascii	39	x	x	-	n/a	http://www.practicalmalwareanalysis.com
	ascii	4	-	x	-	n/a	.exe
	ascii	15	-	-	22	-	GetActiveWindow
	ascii	18	x	-	21	-	GetModuleFileNameA
	ascii	16	-	-	21	-	GetModuleHandleA
	ascii	14	-	-	21	-	GetProcAddress
	ascii	12	-	-	21	-	LoadLibraryA
	ascii	12	-	-	20	-	SetStdHandle
	ascii	12	-	-	20	-	GetStdHandle
	ascii	19	-	-	19	-	GetSystemDirectoryA
	ascii	25	-	-	19	-	ExpandEnvironmentStringsA
	ascii	22	x	-	19	-	GetTimeZoneInformation
	ascii	13	-	-	19	-	GetSystemTime
	ascii	12	-	-	19	-	GetLocalTime
	ascii	13	-	-	19	-	GetVersionExA
	ascii	24	-	-	18	-	UnhandledExceptionFilter
	ascii	12	-	-	16	-	GetLastError
	ascii	10	-	-	15	-	CreatePipe
	ascii	14	x	-	9	-	CreateServiceA
	ascii	18	x	-	9	-	CloseServiceHandle
	ascii	20	x	-	9	-	CloseServiceHandle

Program zawiera nawiązania sieciowe - próbuje pobrać plik `cmd.exe` z jakiegoś serwera.

Są również zapytania HTTP

type (2)	size	blacklist (31)	hint (13)	group (14)	import (0)	value (300)
ascii	11	-	-	-	n/a	MessageBoxA
ascii	10	-	-	-	n/a	user32.dll
ascii	4	-	-	-	n/a	PATH
ascii	11	-	-	-	n/a	CloseHandle
ascii	12	-	-	-	n/a	KERNEL32.dll
ascii	12	-	-	-	n/a	ADVAPI32.dll
ascii	11	-	-	-	n/a	SHELL32.dll
ascii	15	x	-	-	n/a	DuplicateHandle
ascii	10	-	-	-	n/a	GetVersion
ascii	14	-	-	-	n/a	SetHandleCount
ascii	9	-	-	-	n/a	GetCPInfo
ascii	6	-	-	-	n/a	GetACP
ascii	8	-	-	-	n/a	GetOEMCP
ascii	19	-	-	-	n/a	WideCharToMultiByte
ascii	9	x	-	-	n/a	RtlUnwind
ascii	19	-	-	-	n/a	MultiByteToWideChar
ascii	12	-	-	-	n/a	LCMapStringA
ascii	12	-	-	-	n/a	LCMapStringW
ascii	14	-	-	-	n/a	CompareStringA
ascii	14	-	-	-	n/a	CompareStringW
ascii	13	-	-	-	n/a	Configuration
ascii	9	-	-	-	n/a	HTTP/1.0
ascii	5	-	-	-	n/a	HTTP/1.0

Importuje on sporo bibliotek i funkcji, z których duża część jest na blackliście

pestudio 8.87 - Malware Initial Assessment - www.winitor.com							
file help							
c:\documents and settings\admin							
	type (2)	size	blacklist (31)	hint (13)	group (14)	import (0)	value (300)
indicators (2113)	ascii	5	-	-	-	n/a	R6000
virustotal (offline)	ascii	32	-	-	-	n/a	- not enough space for arguments
dos-header (64 bytes)	ascii	5	-	-	-	n/a	R6002
dos-stub (1This program canr	ascii	27	-	-	-	n/a	- floating point not loaded
file-header (Oct.2011D)	ascii	36	-	-	-	n/a	Microsoft Visual C++ Runtime Library
optional-header (Console)	ascii	14	-	-	-	n/a	Runtime Error!
directories (2)	ascii	9	-	-	-	n/a	Program...
sections (93.33%)	ascii	22	-	-	-	n/a	<program name unknown>
libraries (1/4)	ascii	21	-	-	-	n/a	SunMonTueWedThuFriSat
imports (32/87)	ascii	36	-	-	-	n/a	JanFebMarAprMayJunJulAugSepOctNovDec
exports (0)	ascii	18	-	-	-	n/a	GetLastError
tls-callbacks (n/a)	ascii	11	-	-	-	n/a	GetProcAddress
resources (n/a)	ascii	10	-	-	-	n/a	user32.dll
debug (n/a)	ascii	4	-	-	-	n/a	PATH
manifest (n/a)	ascii	11	-	-	-	n/a	CloseHandle
version (n/a)	ascii	12	-	-	-	n/a	kernel32.dll
certificate (n/a)	ascii	12	-	-	-	n/a	kernel32.dll
overlay (n/a)	ascii	11	-	-	-	n/a	ADVAPI32.dll
	ascii	15	-	-	-	n/a	SHELL32.dll
	ascii	10	-	-	-	n/a	DuplicateHandle
	ascii	14	-	-	-	n/a	GetVersion
	ascii	9	-	-	-	n/a	SetHandleCount
	ascii	6	-	-	-	n/a	GetCPInfo
	ascii	8	-	-	-	n/a	GetACP
	ascii	19	-	-	-	n/a	GetOEMCP
	ascii	9	-	-	-	n/a	WideCharToMultiByte
	ascii	19	-	-	-	n/a	RTUnwind
	ascii	12	-	-	-	n/a	MultiByteToWideChar
	ascii	12	-	-	-	n/a	LCMapStringA
	ascii	14	-	-	-	n/a	LCMapStringW
	ascii	14	-	-	-	n/a	CompareStringA
	ascii	14	-	-	-	n/a	CompareStringW

A część funkcji jest nawet nieznana lub zobsfukowana

name (87)	group (13)	anonymous (10)	type (1)	blacklist (32)	anti-debug (0)	undocumented (0)	deprecated (7)	library (4)
HeapAlloc	5	-	implicit	-	-	-	-	kernel32.dll
HeapDestroy	5	-	implicit	x	-	-	-	kernel32.dll
HeapCreate	5	-	implicit	-	-	-	-	kernel32.dll
VirtualFree	5	-	implicit	-	-	-	-	kernel32.dll
HeapFree	5	-	implicit	-	-	-	-	kernel32.dll
GetStringTypeA	5	-	implicit	-	-	-	x	kernel32.dll
22 (shutdown)	3	x	implicit	x	-	-	-	ws2_32.dll
115 (WSAStartup)	3	x	implicit	x	-	-	-	ws2_32.dll
52 (gethostbyname)	3	x	implicit	x	-	-	-	ws2_32.dll
19 (send)	3	x	implicit	x	-	-	-	ws2_32.dll
23 (socket)	3	x	implicit	x	-	-	-	ws2_32.dll
9 (htons)	3	x	implicit	x	-	-	-	ws2_32.dll
4 (connect)	3	x	implicit	x	-	-	-	ws2_32.dll
3 (closesocket)	3	x	implicit	x	-	-	-	ws2_32.dll
16 (recv)	3	x	implicit	x	-	-	-	ws2_32.dll
116 (WSACleanup)	3	x	implicit	x	-	-	-	ws2_32.dll
Sleep	2	-	implicit	-	-	-	-	kernel32.dll
CreateProcessA	2	-	implicit	x	-	-	-	kernel32.dll
ExitProcess	2	-	implicit	-	-	-	-	kernel32.dll
TerminateProcess	2	-	implicit	x	-	-	-	kernel32.dll
GetCurrentProcess	2	-	implicit	x	-	-	-	kernel32.dll
GetCommandLineA	2	-	implicit	-	-	-	-	kernel32.dll
GetStartupInfoA	2	-	implicit	-	-	-	-	kernel32.dll
GetExitCodeProcess	2	-	implicit	x	-	-	-	kernel32.dll
FreeEnvironmentStringsA	2	-	implicit	x	-	-	-	kernel32.dll
FreeEnvironmentStringsW	2	-	implicit	x	-	-	-	kernel32.dll
GetEnvironmentStrings	2	-	implicit	x	-	-	-	kernel32.dll
GetEnvironmentStringsW	2	-	implicit	x	-	-	-	kernel32.dll
GetEnvironmentVariableA	2	-	implicit	x	-	-	-	kernel32.dll
SetEnvironmentVariableA	2	-	implicit	x	-	-	-	kernel32.dll
ShellExecuteA	2	-	implicit	x	-	-	-	shell32.dll
RegDeleteValueA	1	-	implicit	x	-	-	-	advapi32.dll
RegCreateKeyExA	1	-	implicit	-	-	-	-	advapi32.dll
RegSetValueExA	1	-	implicit	x	-	-	-	advapi32.dll

2. Opisz zdarzenia towarzyszące uruchomieniu tego pliku.

Po uruchomieniu program usuwa się z folderu oraz procesów - w jego miejscu pojawia się konsola cmd. Poza tym nie zauważyłem żadnych podejrzanych zachowań

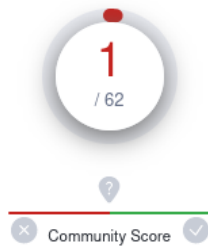
3. Co powoduje blokadę analizy dynamicznej?



Najprawdopodobniej program wykrywa obecność maszyny wirtualnej - a tym samym nie rozpoczyna swojego działania

4. W jaki sposób można uruchomić ten program




W debuggerze bądź za pomocą metod analizy statystycznej lub w sandboxie, który nie daje po sobie śladów

Również w serwisie [virustotal.com](https://www.virustotal.com)



 1 security vendor and no sandboxes flagged this file as malicious 

309d754e28b1b8d0e443ddb89aa6b0cd920a7d32c7f59e020f4866f89f111467	59.31 KB	2023-04-12 13:21:06 UTC
binaries.zip	Size	a moment ago
zip		

DETECTION		DETAILS	COMMUNITY
Security vendors' analysis 		Do you want to a	
NANO-Antivirus	 Trojan.Win32.MLW.dylhy	Acronis (Static ML)	 Undetected