



Informacji jest nadal bardzo dużo

Natomiast znalezienie pliku jpg było łatwiejsze:

```
(kali㉿kali)-[~/sledcza]
$ strings kali.dmp | grep "Image Viewer"
Ristretto Image Viewer
Image Viewer
00051808.jpg - Image Viewer [1/6]
00051808.jpg - Image Viewer [1/6]
00051808.jpg - Image Viewer [1/6]
00051808.jpg - Image Viewer [1/6]
00051808.jpg - Image Viewer [1/6]
```

## VOLATILITY

Program nie potrzebuje, żadnych bibliotek ponieważ pobrałem wersję standalone

```
(kali㉿kali)-[~/sledcza/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ../memory3.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO      : volatility.debug      : Determining profile based on KDBG search...
           Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
           AS Layer1            : IA32PagedMemoryPae (Kernel AS)
           AS Layer2            : FileAddressSpace (/home/kali/sledcza/memory3.vmem)
           PAE type             : PAE
           DTB                  : 0x319000L
           KDBG                 : 0x80544ce0L
           Number of Processors : 1
           Image Type (Service Pack) : 2
           KPCR for CPU 0       : 0xffdff000L
           KUSER_SHARED_DATA    : 0xffdf0000L
           Image date and time  : 2010-08-15 18:24:00 UTC+0000
           Image local date and time : 2010-08-15 14:24:00 -0400
```

KDBG jest to debugger dla kernela linuxa. Jeżeli jego adres zostanie osiągnięty, Kernel przestaje być wykonywany i można go wtedy debugować.

Z kolei DTB wskazuje na Directory Table Base address. Pozwala on procesorowi zmapować virtualne adresy do adresów fizycznych, kiedy program jest uruchamiany

Adres KPCR wskazuje na adres w którym się on znajduje. Możemy stwierdzić, że zrzut został wykonany na maszynie z systemem windows ponieważ ten adres jest ustalony w Windowsie

```
(kali@kali)-[~/sledcza/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ../memory3.vmem --profile=WinXPSP3x86 pslist
```

Volatility Foundation Volatility Framework 2.6

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0x810b1660	System	4	0	58	183		0		
0xff2ab020	smss.exe	544	4	3	21		0	2010-08-11 06:06:21 UTC+0000	
0xff1ecda0	csrss.exe	608	544	10	369	0	0	2010-08-11 06:06:23 UTC+0000	
0xff1ec978	winlogon.exe	632	544	20	518	0	0	2010-08-11 06:06:23 UTC+0000	
0xff247020	services.exe	676	632	16	269	0	0	2010-08-11 06:06:24 UTC+0000	
0xff255020	lsass.exe	688	632	19	344	0	0	2010-08-11 06:06:24 UTC+0000	
0xff218230	vmacthlp.exe	844	676	1	24	0	0	2010-08-11 06:06:24 UTC+0000	
0x80ff88d8	svchost.exe	856	676	17	199	0	0	2010-08-11 06:06:24 UTC+0000	
0xff217560	svchost.exe	936	676	10	272	0	0	2010-08-11 06:06:24 UTC+0000	
0x80fbf910	svchost.exe	1028	676	71	1341	0	0	2010-08-11 06:06:24 UTC+0000	
0xff22d558	svchost.exe	1088	676	5	80	0	0	2010-08-11 06:06:25 UTC+0000	
0xff203b80	svchost.exe	1148	676	14	208	0	0	2010-08-11 06:06:26 UTC+0000	
0xff1d7da0	spoolsv.exe	1432	676	13	135	0	0	2010-08-11 06:06:26 UTC+0000	
0xff1b8b28	vmtoolsd.exe	1668	676	5	221	0	0	2010-08-11 06:06:35 UTC+0000	
0xff1fdc88	VMUpgradeHelper	1788	676	4	100	0	0	2010-08-11 06:06:38 UTC+0000	
0xff143b28	TPAutoConnSvc.e	1968	676	5	100	0	0	2010-08-11 06:06:39 UTC+0000	
0xff25a7e0	alg.exe	216	676	6	105	0	0	2010-08-11 06:06:39 UTC+0000	
0xff364310	wscntfy.exe	888	1028	1	27	0	0	2010-08-11 06:06:49 UTC+0000	
0xff38b5f8	TPAutoConnect.e	1084	1968	1	61	0	0	2010-08-11 06:06:52 UTC+0000	
0xff3865d0	explorer.exe	1724	1708	12	341	0	0	2010-08-11 06:09:29 UTC+0000	
0xff3667e8	VMwareTray.exe	432	1724	1	49	0	0	2010-08-11 06:09:31 UTC+0000	
0xff374980	VMwareUser.exe	452	1724	6	189	0	0	2010-08-11 06:09:32 UTC+0000	
0x80f94588	wuaucflt.exe	468	1028	4	134	0	0	2010-08-11 06:09:37 UTC+0000	
0xff3ad1a8	IEXPLORE.EXE	2044	1724	10	366	0	0	2010-08-15 18:11:17 UTC+0000	
0x80fdc368	logon.scr	124	632	1	15	0	0	2010-08-15 18:21:28 UTC+0000	
0xff125020	cmd.exe	1136	1668	0		0	0	2010-08-15 18:24:00 UTC+0000	2010-08-15 18:24:00 UTC+0000

Wykonanie powyższego polecenia daje nam taki wynik. Są to aktywne procesy

Wyświetla się kilka kolumn.

Offset(V) informuje nas o wirtualnym adresie w pamięci RAM.

PID to numer procesu.

PPID to numer procesu któremu podlega dany proces (Parent)

Thds oznacza numer wątku na którym operuje dany proces

Hnds Reprezentuje „Handles”. Jest to struktura danych zawierająca pliki, potoki, regiony pamięci itp. Na których operuje dany proces.

Wow64 to technologia pozwalająca działać aplikacjom 32-bitowym na architekturze 64-bitowej. Znajduje się na każdym Windowsie 64-bitowym i w powyższym przypadku nie jest używana przez żaden proces

Start i Exit informują o czasie kiedy proces został uruchomiony i zamknięty

V w rubryce offset mówi, że jest to adres wirtualny, a nie fizyczny

Proces cmd został rozpoczęty 15.08.2010 o godzinie 10:24:00 i zaraz potem został od razu zamknięty

System i smss.exe nie mają pola w rubryce Sess, ponieważ Sess informuje do jakiej sesji czy też użytkownika jest przypisany proces. System i smss.exe należą do systemu, dlatego nie ma w nich informacji o sesji

Do VMwareUser.exe należy PID 452

```
(kali@kali)~/sledcza/volatility_2.6_lin64_standalone
$ ./volatility_2.6_lin64_standalone -f ../memory3.vmem --profile=WinXPSP3x86 pslist -P
Volatility Foundation Volatility Framework 2.6
Offset(P) Name PID PPID Thds Hnds Sess Wow64 Start Exit
0x01214660 System 4 0 58 183 0 0 2010-08-11 06:06:21 UTC+0000
0x05471020 smss.exe 544 4 3 21 0 0 2010-08-11 06:06:23 UTC+0000
0x066f0da0 csrss.exe 608 544 10 369 0 0 2010-08-11 06:06:23 UTC+0000
0x066f0978 winlogon.exe 632 544 20 518 0 0 2010-08-11 06:06:23 UTC+0000
0x06015020 services.exe 676 632 16 269 0 0 2010-08-11 06:06:24 UTC+0000
0x05f47020 lsass.exe 688 632 19 344 0 0 2010-08-11 06:06:24 UTC+0000
0x06384230 vmacthlp.exe 844 676 1 24 0 0 2010-08-11 06:06:24 UTC+0000
0x0115b8d8 svchost.exe 856 676 17 199 0 0 2010-08-11 06:06:24 UTC+0000
0x063c5560 svchost.exe 936 676 10 272 0 0 2010-08-11 06:06:24 UTC+0000
0x01122910 svchost.exe 1028 676 71 1341 0 0 2010-08-11 06:06:24 UTC+0000
0x061ef558 svchost.exe 1088 676 5 80 0 0 2010-08-11 06:06:25 UTC+0000
0x06499b80 svchost.exe 1148 676 14 208 0 0 2010-08-11 06:06:26 UTC+0000
0x06945da0 spoolsv.exe 1432 676 13 135 0 0 2010-08-11 06:06:26 UTC+0000
0x069d5b28 vmtoolsd.exe 1668 676 5 221 0 0 2010-08-11 06:06:35 UTC+0000
0x0655fc88 VMUpgradeHelper 1788 676 4 100 0 0 2010-08-11 06:06:38 UTC+0000
0x0211ab28 TPAutoConnSvc.e 1968 676 5 100 0 0 2010-08-11 06:06:39 UTC+0000
0x05f027e0 alg.exe 216 676 6 105 0 0 2010-08-11 06:06:39 UTC+0000
0x04c2b310 wscntfy.exe 888 1028 1 27 0 0 2010-08-11 06:06:49 UTC+0000
0x049c15f8 TPAutoConnect.e 1084 1968 1 61 0 0 2010-08-11 06:06:52 UTC+0000
0x04a065d0 explorer.exe 1724 1708 12 341 0 0 2010-08-11 06:09:29 UTC+0000
0x04be97e8 VMwareTray.exe 432 1724 1 49 0 0 2010-08-11 06:09:31 UTC+0000
0x04b5a980 VMwareUser.exe 452 1724 6 189 0 0 2010-08-11 06:09:32 UTC+0000
0x010f7588 wuauclt.exe 468 1028 4 134 0 0 2010-08-11 06:09:37 UTC+0000
0x0485d1a8 IEXPLORE.EXE 2044 1724 10 366 0 0 2010-08-15 18:11:17 UTC+0000
0x0113f368 logon.scr 124 632 1 15 0 0 2010-08-15 18:21:28 UTC+0000
0x02e47020 cmd.exe 1136 1668 0 0 0 0 2010-08-15 18:24:00 UTC+0000 2010-08-15 18:24:00 UTC+0000
```

Przy użyciu -P zamiast adresów wirtualnych wyświetlane są adresy fizyczne.

```
(kali@kali)~/sledcza/volatility_2.6_lin64_standalone
$ ./volatility_2.6_lin64_standalone -f ../memory3.vmem --profile=WinXPSP3x86 pstree
Volatility Foundation Volatility Framework 2.6
Name Pid PPID Thds Hnds Time
0x810b1660:System 4 0 58 183 1970-01-01 00:00:00 UTC+0000
. 0xff2ab020:smss.exe 544 4 3 21 2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe 632 544 20 518 2010-08-11 06:06:23 UTC+0000
... 0xff255020:lsass.exe 688 632 19 344 2010-08-11 06:06:24 UTC+0000
... 0xff247020:services.exe 676 632 16 269 2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe 1668 676 5 221 2010-08-11 06:06:35 UTC+0000
..... 0xff125020:cmd.exe 1136 1668 0 0 2010-08-15 18:24:00 UTC+0000
.... 0x80ff88d8:svchost.exe 856 676 17 199 2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe 1432 676 13 135 2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe 1028 676 71 1341 2010-08-11 06:06:24 UTC+0000
..... 0x80f94588:wuauclt.exe 468 1028 4 134 2010-08-11 06:09:37 UTC+0000
..... 0xff364310:wscntfy.exe 888 1028 1 27 2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe 936 676 10 272 2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e 1968 676 5 100 2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e 1084 1968 1 61 2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe 1088 676 5 80 2010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe 844 676 1 24 2010-08-11 06:06:24 UTC+0000
..... 0xff25a7e0:alg.exe 216 676 6 105 2010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe 1148 676 14 208 2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper 1788 676 4 100 2010-08-11 06:06:38 UTC+0000
... 0x80fdc368:logon.scr 124 632 1 15 2010-08-15 18:21:28 UTC+0000
.. 0xff1ecda0:csrss.exe 608 544 10 369 2010-08-11 06:06:23 UTC+0000
. 0xff3865d0:explorer.exe 1724 1708 12 341 2010-08-11 06:09:29 UTC+0000
. 0xff3667e8:VMwareTray.exe 432 1724 1 49 2010-08-11 06:09:31 UTC+0000
. 0xff374980:VMwareUser.exe 452 1724 6 189 2010-08-11 06:09:32 UTC+0000
. 0xff3ad1a8:IEXPLORE.EXE 2044 1724 10 366 2010-08-15 18:11:17 UTC+0000
```

Procesy które są z wcięciem należą do procesu wyżej który ma mniej kropek. Widać w ten sposób które procesy podlegają któremu procesowi

Nie znajdziemy tu identyfikatora Sess

Procesem nadrzędnym procesu smss.exe jest System

smss.exe to program odpowiedzialny za zarządzanie sesjami (Windows Session manager subsystem

Aby odnaleźć wszystkie załadowane biblioteki dll przez proces wscntfy.exe należy najpierw poznać jego PID, a następnie wywołać polecenie:

```
(kali@kali)-[~/sledcza/volatility_2.6_lin64_standalone]
$ ./volatility_2.6_lin64_standalone -f ../memory3.vmem --profile=WinXPSP3x86 dlllist -p 888
Volatility Foundation Volatility Framework 2.6
*****
wscntfy.exe pid: 888
Command line : C:\WINDOWS\system32\wscntfy.exe
Service Pack 2

Base          Size      LoadCount Path
-----
0x01000000    0x6000      0xffff C:\WINDOWS\system32\wscntfy.exe
0x7c900000    0xb0000     0xffff C:\WINDOWS\system32\kernel32.dll
0x7c800000    0xf4000     0xffff C:\WINDOWS\system32\msvcrt.dll
0x77c10000    0x58000     0xffff C:\WINDOWS\system32\USER32.dll
0x77d40000    0x90000     0xffff C:\WINDOWS\system32\GDI32.dll
0x77f10000    0x46000     0xffff C:\WINDOWS\system32\SHELL32.dll
0x7c9c0000    0x814000    0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000    0x9b000     0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77f60000    0x76000     0xffff C:\WINDOWS\system32\SHLWAPI.dll
0x773d0000    0x102000    0x2 C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.2180_x-ww_a841ff9\comctl32.dll
0x20000000    0x2c5000    0x1 C:\WINDOWS\system32\xpsp2res.dll
0x5ad70000    0x38000     0x2 C:\WINDOWS\system32\uxtheme.dll
```

Wyciąganie wszystkich bibliotek dll:

```
(kali@kali)-[~/sledcza]
$ mkdir dll_dump

(kali@kali)-[~/sledcza]
$ ./volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone -f memory3.vmem --profile=WinXPSP3x86 dlldump -D dll_dump
Volatility Foundation Volatility Framework 2.6
Process(V) Name      Module Base      Module Name      Result
-----
0xff2ab020 smss.exe           0x048580000      smss.exe         Error: DllBase is paged
0xff2ab020 smss.exe           0x07c900000      Error: DllBase is paged
0xff1ecda0 csrss.exe          0x04a680000      csrss.exe        Error: e_magic 6268 is not a valid DOS signature.
0xff1ecda0 csrss.exe          0x07c900000      Error: DllBase is paged
0xff1ecda0 csrss.exe          0x075b40000      CSRSRV.dll       Error: DllBase is paged
0xff1ecda0 csrss.exe          0x077d40000      USER32.dll       OK: module.608.66f0da0.77d40000.dll
0xff1ecda0 csrss.exe          0x077e70000      RPCRT4.dll       Error: DllBase is paged
0xff1ecda0 csrss.exe          0x075e90000      sxs.dll          Error: DllBase is paged
0xff1ecda0 csrss.exe          0x077dd0000      ADVAPI32.dll     Error: DllBase is paged
0xff1ecda0 csrss.exe          0x075b50000      basesrv.dll      Error: DllBase is paged
0xff1ecda0 csrss.exe          0x07c800000      KERNEL32.dll     Error: DllBase is paged
0xff1ecda0 csrss.exe          0x077f10000      GDI32.dll        Error: DllBase is paged
0xff1ecda0 csrss.exe          0x075b60000      winsrv.dll       OK: module.608.66f0da0.75b60000.dll
0xff1ec978 winlogon.exe       0x001000000      winlogon.exe     OK: module.632.66f0978.1000000.dll
```

Udało się wyciągnąć bibliotekę:

```
OK: module.124.113f368.77f60000.dll
```

PID 1668 należy do vmtoolsd.exe

```
(kali@kali)-[~/sledcza]
$ ./volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone -f memory3.vmem --profile=WinXPSP3x86 handles -p 1668 -t Process
Volatility Foundation Volatility Framework 2.6
Offset(V)  Pid      Handle      Access Type      Details
-----
0xff125020  1668     0x378       0x1f0fff Process          cmd.exe(1136)
```

Podany proces posiada aktywny uchwyt z procesem cmd.exe (1136)



```

(kali@kali)-[~/sledcza]
$ ./volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone -f memory3.vmem --profile=WinXPSP3x86 getsids | grep S-1-5-32-544
Volatility Foundation Volatility Framework 2.6
System (4): S-1-5-32-544 (Administrators)
smss.exe (544): S-1-5-32-544 (Administrators)
csrss.exe (608): S-1-5-32-544 (Administrators)
winlogon.exe (632): S-1-5-32-544 (Administrators)
services.exe (676): S-1-5-32-544 (Administrators)
lsass.exe (688): S-1-5-32-544 (Administrators)
vmacthlp.exe (844): S-1-5-32-544 (Administrators)
svchost.exe (856): S-1-5-32-544 (Administrators)
svchost.exe (1028): S-1-5-32-544 (Administrators)
spoolsv.exe (1432): S-1-5-32-544 (Administrators)
vmtoolsd.exe (1668): S-1-5-32-544 (Administrators)
VMUpgradeHelper (1788): S-1-5-32-544 (Administrators)
TPAutoConnSvc.e (1968): S-1-5-32-544 (Administrators)
wscntfy.exe (888): S-1-5-32-544 (Administrators)
TPAutoConnect.e (1084): S-1-5-32-544 (Administrators)
explorer.exe (1724): S-1-5-32-544 (Administrators)
VMwareTray.exe (432): S-1-5-32-544 (Administrators)
VMwareUser.exe (452): S-1-5-32-544 (Administrators)
wuauclt.exe (468): S-1-5-32-544 (Administrators)
IEXPLORE.EXE (2044): S-1-5-32-544 (Administrators)
logon.scr (124): S-1-5-32-544 (Administrators)
cmd.exe (1136): S-1-5-32-544 (Administrators)

```

SID S-1-5-32-544 Należy do Administratorów

```

C:\WINDOWS\system32\SAMLIB.dll
File version      : 5.1.2600.2180
Product version   : 5.1.2600.2180
Flags             :
OS                : Windows NT
File Type         : Dynamic Link Library
File Date         :
CompanyName       : Microsoft Corporation^
FileDescription   : SAM Library DLL^
FileVersion       : 5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)^
InternalName      : SAMLib.DLL^
LegalCopyright    : \xa9 Microsoft Corporation. All rights reserved.^
OriginalFilename  : SAMLib.DLL^
ProductName       : Microsoft\xae Windows\xae Operating System^
ProductVersion    : 5.1.2600.2180^

```

SAMLIB.exe posiada wersję 5.1.2600.2180

OS to Windows NT

```

C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
File version      : 7.17.512.1
Product version   : 7.17.512.1
Flags             :
OS                : Windows NT
File Type         : Application
File Date         :
CompanyName       : ThinPrint AG^
FileDescription   : TPAutoConnect User Agent^
FileVersion       : 7,17,512,1^
InternalName      : TPAutoConnect^
LegalCopyright    : Copyright (c) 1999-2009 ThinPrint AG^
OriginalFilename  : TPAutoConnect.exe^
ProductName       : TPAutoConnect^
ProductVersion    : 7,17,512,1^

```

Wersja pliku TPAutoConnect.exe to 7.17.512.1

LegalCopyright: Copyright © 1999-2009 ThinPrint AG

```
(kali㉿kali)-[~/sledcza]
$ ./volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone -f memory3.vmem --profile=WinXPSP3x86 iehistory
Volatility Foundation Volatility Framework 2.6
*****
Process: 1724 explorer.exe
Cache type "DEST" at 0x1387cd
Last modified: 2010-08-15 14:11:24 UTC+0000
Last accessed: 2010-08-15 18:11:26 UTC+0000
URL: Administrator@http://www.msn.com
Title: MSN.com
*****
Process: 2044 IEXPLORE.EXE
Cache type "DEST" at 0x24bdf45
Last modified: 2010-08-15 14:11:24 UTC+0000
Last accessed: 2010-08-15 18:11:26 UTC+0000
URL: Administrator@http://www.msn.com
Title: MSN.com
```

PID procesu IEXPLORE to 2044

Strona yahoo i bing nie zostały wyświetlone

Eksportowanie pliku

```
(kali㉿kali)-[~/sledcza]
$ ./volatility_2.6_lin64_standalone/volatility_2.6_lin64_standalone -f memory3.vmem --profile=WinXPSP3x86 procdump -p 468 -D Virus
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase Name Result
-----
0x80f94588 0x00400000 wuauclt.exe OK: executable.468.exe
```

```
(kali㉿kali)-[~/sledcza/Virus]
$ md5sum executable.468.exe
21c183cdabccc7675b50258313812bc7 executable.468.exe
```

33 / 70

Community Score

33 security vendors and no sandboxes flagged this file as malicious

88753ea526cdf8de9914cc40f46bd88e2f5e2c82530d55dc8cd0cc7b3c3ab73

wuauclt.exe

peexe

108.50 KB Size

2022-10-01 04:39:48 UTC 3 months ago

EXE

DETECTION

DETAILS

BEHAVIOR

COMMUNITY

Security vendors' analysis

Ad-Aware	Trojan.GenericKD.44099244	Alibaba	Backdoor.Win32/Swrort.91a8b81b
ALYac	Trojan.GenericKD.44099244	Arcabit	Trojan.Generic.D2A0E6AC
Avast	FileRepMalware [Trj]	AVG	FileRepMalware [Trj]
Avira (no cloud)	TR/Crypt.EPACK.Gen2	BitDefender	Trojan.GenericKD.44099244
Blkav Pro	W32.AIDetect.malware2	Comodo	Malware@#n8niyzyogj4v
Cybereason	Malicious.dabccc	Cylance	Unsafe
Cynet	Malicious (score: 99)	Emsisoft	Trojan.GenericKD.44099244 (B)
eScan	Trojan.GenericKD.44099244	GData	Trojan.GenericKD.44099244
Google	Detected	Ikarus	Trojan.Crypt
Kaspersky	Backdoor.Win32.Swrort.wvl	Kingsoft	Win32.Hack.Swrort.w (kcloud)
Lionic	Trojan.Win32.Swrort.4lc	MAX	Malware (ai Score=99)
MaxSecure	Trojan.Malware.74326942.susgen	McAfee	ArtemisI21C183CDABCC
Microsoft	Trojan.Win32/Ymacco.AA66	Rising	Trojan.Generic@AI.97 (RDML-owWZom3

Wyodrębniony plik jest wirusem

