

4th Lab

Juan Esteban Murcia y Rodrigo Castillo

September 3, 2020

1 Static Analysis

1.1 Get the hash of the malware and search for it in Virus Total. Is it recognized as a malware for some antivirus?

The library outlook.dll is recognized by virustotal as a malware by 59/70 antiviruses.



Figure 1: Hash

1.2 Analyze the strings using the command line tool "Strings". Which are the strings more suspicious and why?

inside the list we can find the library *kernel32.dll* which is really powerful, also, we can see that it is importing *sleep* library, that means that the malware probably is not going to execute immediately, sometimes, malwares are programmed with delay with the purpose of being sneaky. Also, it seems to be exporting functions for installing purposes like *installA* , *install* ...

```

GetModuleFileNameA
Sleep
TerminateThread
WaitForSingleObject
GetSystemTime
CreateThread
GetProcAddress
LoadLibraryA
GetLongPathNameA
GetTempPathA
ReadFile
CloseHandle
CreateProcessA
GetStartupInfoA
CreatePipe
GetCurrentDirectoryA
GetLastError
lstrlenA
SetLastError
OutputDebugStringA
KERNEL32.dll
RegisterServiceCtrlHandlerA
RegSetValueExA
RegCreateKeyA
CloseServiceHandle
CreateServiceA
OpenSCManagerA
RegCloseKey
RegQueryValueExA
RegOpenKeyExA
DeleteService
OpenServiceA
SetServiceStatus
ADVAPI32.dll
WSASocketA
WS2_32.dll
InternetReadFile
HttpQueryInfoA
HttpSendRequestA

```

Figure 2: Strings

etc, It's also importing libraries for networking , this can be used by the malware for remotely installing processes later. There is a library that is interesting not because of its potential but it talks about the way that the program was made, the library *malloc* its a *C* library, that means that the pogram was made in C or C++.

The malware is also connecting to an attacker's localhost in *practicalmalwareanalysis.com*

1.3 Is the malware packed? Analyze it with PEiD. Unpack if possible.

The malware is not packed but its a c++ program .

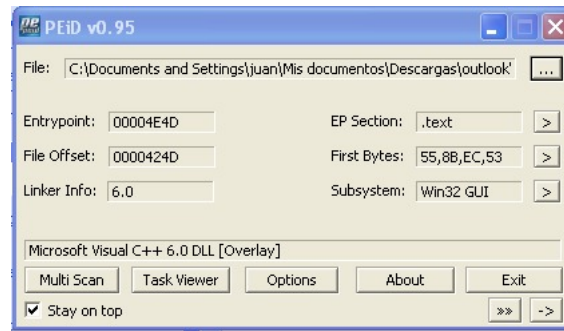


Figure 3: PEid

1.4 Analyze the PE with PEView and review detailed the "text", "data", "rdata" and "resource" sections (Use "Resource Hacker" to access to the resource section). What information is useful from theses sections?

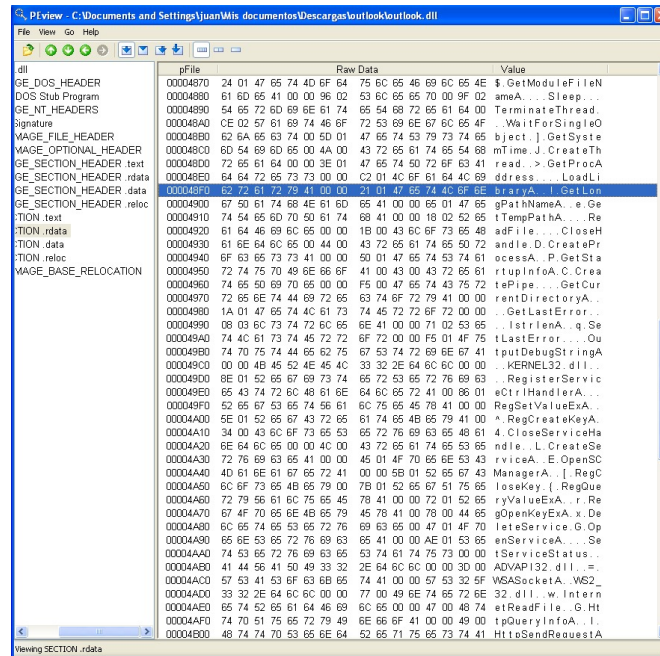


Figure 4: Rdata

PEview - C:\Documents and Settings\Juan\My documents\Descargas\outlook\outlook.dll

	pFile	Raw Data	Value
GE_DOS_HEADER	00004E00	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
DOS_Stub_Program	00004E10	59 32 39 75 62 60 56 6A	64 41 30 30 00 00 00 00 Y29ubmVjdA==...
GE_NT_HEADERS	00004E20	E8 60 00 10 00 00 00 00	70 72 61 63 74 69 63 61practica
Signature	00004E30	6C 60 61 6C 77 61 72 65	61 6E 61 6C 79 73 69 73malwareanalysis
WAVE_FILE_HEADER	00004E40	2E 63 6F 60 00 00 00 00	00 00 00 00 00 00 00 00com.....
WAVE_OPTIONAL_HEADER	00004E50	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00serve.ht
GE_SECTION_HEADER_text	00004E60	00 00 00 00 00 00 00 00	73 65 72 76 65 2E 68 74ml.....
GE_SECTION_HEADER_data	00004E70	60 6C 00 00 00 00 00 00	00 00 00 00 00 00 00 00m.....
GE_SECTION_HEADER_reloc	00004E80	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00m.....
ITION_text	00004E90	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00m.....
ITION_data	00004EA0	00 00 00 00 00 00 00 00	0C 69 00 10 04 60 00 10m.....
ITION_reloc	00004EB0	C8 60 00 10 88 60 00 10	64 57 35 7A 64 58 42 77m6zdxBw
WAVE_BASE_RELOCATION	00004EC0	62 33 4A 30 00 00 00 00	63 32 78 6C 5A 58 41 3D b3J0.....c2xIZXA=
	00004ED0	00 00 00 00 59 32 31 68	00 00 00 00 63 58 56 70Y2lk.....cXVp
	00004EE0	64 41 30 30 00 00 00 00	2A 2F 2A 00 20 57 69 6E dA==.....Win
	00004EF0	64 6F 77 73 20 59 59 20	36 2E 31 31 00 00 00 00 dows XP 6.1.....
	00004F00	74 74 00 00 43 72 65 61	74 65 50 72 6F 63 65 73 t1..CreateProce
	00004F10	73 41 00 00 68 65 72 6E	65 6C 33 32 2E 64 6C 6C sA...kerne132.dll
	00004F20	00 00 00 00 77 62 00 00	2E 65 78 65 00 00 00 00wb.....exe...
	00004F30	5C 00 00 00 47 45 54 00	48 54 54 50 2F 31 2E 31 \\.GET.HTTP/1.1
	00004F40	00 00 00 00 25 73 20 25	73 00 00 00 31 32 33 34%s%...1234
	00004F50	35 36 37 38 39 30 31 32	33 34 35 36 00 00 00 00 567890123456...
	00004F60	63 64 00 00 71 75 69 74	00 00 00 00 65 78 69 74 cd...quit...exit
	00004F70	00 00 00 00 67 65 74 66	69 6C 65 00 63 60 64 2Egetfile.cmd
	00004F80	65 78 65 20 2F 63 20 00	3E 00 00 00 41 42 43 44 exe /c>...ABCD
	00004F90	45 46 47 48 49 4A 4B 4C	4D 4E 4F 50 51 52 53 54 EFGHIJKLMNOPRST
	00004FA0	55 56 57 58 59 5A 61 62	63 64 65 66 67 68 69 6A UWXYZabdefghij
	00004FB0	68 6C 6D 6E 6F 70 71 72	73 74 75 76 77 78 79 7A klmnopqrstuvwxy
	00004FC0	30 31 32 33 34 35 36 37	38 39 3A 2F 00 00 00 00 0123456789-/+...
	00004FD0	20 20 21 3E 00 00 00 00	3C 21 20 20 00 00 00 00 ->...c1...
	00004FE0	88 51 00 10 00 00 00 00	2E 50 41 58 00 00 00 00 0.....PAX...
	00004FF0	88 51 00 10 00 00 00 00	2E 50 41 44 00 00 00 00 0.....PAD...
	00005000	44 65 70 65 6E 64 4F 6E	53 65 72 76 69 63 65 00 DependOnService
	00005010	52 70 63 63 73 00 00 00	53 65 72 76 69 63 65 44 RpcSs...ServiceD
	00005020	6C 6C 00 00 47 65 74 4D	6F 64 75 6C 65 46 69 6C l1.GetModuleFil
	00005030	65 4E 61 6D 65 25 25 2D	67 65 74 20 64 6C 6D 20 eName() get dll
	00005040	70 61 74 68 00 00 00 00	50 61 72 61 6D 65 74 65 path...Paramete
	00005050	72 73 00 00 54 79 70 65	00 00 00 00 53 74 61 72 rs...Type...Star
	00005060	74 00 00 00 4F 62 6A 65	63 74 4E 61 6D 65 00 00 t...ObjectName...
	00005070	4C 6F 63 61 6C 53 79 73	74 65 6D 00 45 72 72 6F LocalSystem.Erro
	00005080	72 43 6F 6E 74 72 6F 6C	00 00 00 00 44 69 73 70 rControl...Disp
	00005090	6C 61 79 4E 61 6D 65 00	44 65 73 63 72 69 70 74 lavName.Descript

Viewing SECTION_data

PEview - C:\Documents and Settings\Juan\My documents\Descargas\outlook\outlook.dll

	pFile	Raw Data	Value
GE_DOS_HEADER	00004E00	6E 68 69 67 76 72 61 7A	63 6F 6E 20 61 6E 64 20location and
DOS_Stub_Program	00004E10	6C 6F 63 61 74 69 6F 6E	20 69 6E 66 6F 72 6D 61 location informa
GE_NT_HEADERS	00004E20	74 69 6F 6E 2C 20 61 6E	64 20 6E 6F 74 69 66 69 tion, and notifi
Signature	00005100	65 73 20 61 70 70 6C 69	63 61 74 69 6F 6E 73 20 es applications
WAVE_FILE_HEADER	00005110	77 68 65 6E 20 74 68 69	73 20 69 6E 66 6F 72 6D when this inform
WAVE_OPTIONAL_HEADER	00005120	61 74 69 6F 6E 20 63 68	61 6E 67 65 73 2E 00 00 ation changes...
GE_SECTION_HEADER_text	00005130	49 6D 61 67 65 50 61 74	68 00 00 00 25 53 79 73 ImagePath...%Sys
GE_SECTION_HEADER_data	00005140	74 65 6D 52 6F 6F 74 25	5C 53 79 73 74 65 6D 33 tnmRoot%\System3
GE_SECTION_HEADER_reloc	00005150	32 5C 73 76 63 68 6F 73	74 2E 65 78 65 20 2D 68 2\svchost.exe -k
ITION_text	00005160	20 00 00 00 53 59 53 54	45 4D 5C 43 75 72 72 65 ...SYSTEMCurre
ITION_data	00005170	6E 74 43 6F 6E 74 72 6F	6C 53 65 74 5C 53 65 72 ntControlSet\Ser
ITION_reloc	00005180	76 69 63 65 73 5C 00 00	43 72 65 61 74 65 53 65 vices\...CreateSe
WAVE_BASE_RELOCATION	00005190	72 76 69 63 65 28 25 73	29 2D 65 72 72 6F 72 20 rvice(%s) error
	000051A0	25 64 00 00 49 6E 74 72	61 6E 65 74 2D 4E 65 74 %d..Intranet Net
	000051B0	77 6F 72 68 2D 41 77 61	72 65 6E 65 73 73 2D 28 work Awareness (
	000051C0	49 4E 41 2B 29 00 00 00	25 53 79 73 74 65 6D 52 INA)...SystemR
	000051D0	6F 6F 74 25 5C 53 79 73	74 65 6D 33 32 5C 73 76 oot%\System32\sv
	000051E0	63 68 6F 73 74 2E 65 78	65 2D 2D 68 2D 6E 65 74 chost.exe -k net
	000051F0	73 76 63 73 00 00 00 00	4F 70 65 6E 53 43 4D 61 svcs...OpenSCMa
	00005200	6E 61 67 65 72 28 29 00	59 6F 75 20 73 70 65 63 nager() You spec
	00005210	69 66 79 2D 73 65 72 76	69 63 65 2D 6E 61 6D 65 ify service name
	00005220	20 6E 6F 74 2D 69 6E 20	53 76 63 68 6F 73 74 2F not in Svchost/
	00005230	2F 6E 65 74 73 76 63 73	2C 2D 6D 75 73 74 2D 62 /netsvcs, must b
	00005240	65 2D 6F 6E 65 2D 6F 66	2D 66 6F 6C 6C 6F 77 69 e one of followi
	00005250	6E 67 3A 00 52 65 67 51	75 65 72 79 56 61 6C 75 ng...RegQueryValu
	00005260	65 45 78 28 53 76 63 68	6F 73 74 5C 6E 65 74 73 eEx(Svchost\nets
	00005270	76 63 73 2D 00 00 00 00	6E 64 74 73 76 63 73 00 vcs)...netsvc
	00005280	52 65 67 4F 70 66 6E 4B	65 79 45 78 28 25 73 29 RegOpenKeyEx(%s)
	00005290	20 4B 45 59 5F 51 55 45	52 59 5F 56 41 4C 55 45 KEY_QUERY_VALUE
	000052A0	20 73 75 63 63 65 73 73	2E 00 00 00 52 65 67 4F success...RegO
	000052B0	70 65 6E 4B 65 79 45 78	28 25 73 29 2D 4B 45 59 penKeyEx(%s) KEY
	000052C0	6F 51 55 45 52 59 5F 56	41 4C 55 45 2D 06 72 72 _QUERY_VALUE err
	000052D0	6F 72 2D 2E 00 00 00 00	53 4F 46 54 57 41 52 45 or...SOFTWARE
	000052E0	50 4D 69 63 72 6F 73 6F	66 74 5C 57 69 6E 64 6F \Microsoft\Windo
	000052F0	77 73 2D 4E 54 5C 43 75	72 72 65 6E 74 56 65 72 ws NT\CurrentVer
	00005300	73 69 6F 6E 5C 53 76 63	88 6F 73 74 00 00 00 00 sion\Svchost....
	00005310	49 50 52 49 50 00 00 00	75 6E 69 6E 73 74 61 6C IPRIP...uninstal
	00005320	6C 2D 73 75 63 63 65 73	73 00 00 00 4F 70 65 6E l success...Open
	00005330	53 65 72 76 69 63 65 28	25 73 29 2D 65 72 72 6F Service(%s) erro
	00005340	72 2D 32 00 4F 70 65 6E	53 65 72 76 69 63 65 28 r 2.OpenService(
	00005350	25 73 29 2D 65 72 72 6F	72 2D 31 00 75 6E 69 6E %s) error 1.unin
	00005360	73 74 61 6C 6C 2D 69 73	2D 73 74 61 72 74 69 6E stall is startin

Viewing SECTION_data

Figure 5: data and text sections

Clearly in this images we can find really important information, like how the malware is opening and using registry keys, create a host service with the name of IPRIP, adding all the dynamic libraries and functions the malware seems to be using.

1.5 When the file was compiled?

The file was created on 2010 : 09 : 27 20 : 00 : 25 – 05 : 00

```
ExifTool Version Number : 10.80
File Name                : outlook.dll
Directory                :
File Size                 : 24 KB
File Modification Date/Time : 2011:04:26 14:52:40-05:00
File Access Date/Time     : 2020:08:31 18:23:52-05:00
File Inode Change Date/Time : 2020:08:31 18:23:34-05:00
File Permissions          : rw-rw-r--
File Type                 : Win32 DLL
File Type Extension       : dll
MIME Type                 : application/octet-stream
Machine Type              : Intel 386 or later, and compatibles
Time Stamp                : 2010:09:27 20:00:25-05:00
PE Type                   : PE32
Linker Version             : 6.0
Code Size                 : 16384
Initialized Data Size      : 51712
Uninitialized Data Size    : 0
Entry Point                : 0x4e4d
OS Version                 : 4.0
Image Version              : 0.0
Subsystem Version          : 4.0
Subsystem                  : Windows GUI
```

1.6 Which imported libraries and functions can be seen from the static analysis?

Those are the libraries and functions that the program is importing. From here, we can see very important information such as the keys that the malware is creating, here there are the imported libraries:

	pFile	Data	Description	Value
outlook.dll				
IMAGE_DOS_HEADER	00004000	0000568C	HintName RVA	0147 OpenServiceA
MS-DOS Stub Program	00004004	0000567C	HintName RVA	0170 DeleteService
IMAGE_NT_HEADERS	00004008	0000566C	HintName RVA	0172 RegOpenKeyExA
Signature	0000400C	00005658	HintName RVA	017B RegQueryValueExA
IMAGE_FILE_HEADER	00004010	0000564A	HintName RVA	0169 RegCloseKey
IMAGE_OPTIONAL_HEADER	00004014	00005638	HintName RVA	0145 OpenSCManagerA
IMAGE_SECTION_HEADER	00004018	00005626	HintName RVA	004C CreateServiceA
IMAGE_SECTION_HEADER	0000401C	00005610	HintName RVA	0034 CloseServiceHandle
IMAGE_SECTION_HEADER	00004020	00005600	HintName RVA	0156 RegCreateKeyA
IMAGE_SECTION_HEADER	00004024	000055EE	HintName RVA	0166 RegSetValueExA
SECTION .text	00004028	000055D0	HintName RVA	018E RegisterServiceCtrlHandlerA
SECTION .data	0000402C	0000559C	HintName RVA	01AE SetServiceStatus
IMPORT Address Table	00004030	00000000	End of imports	ADVAPI32.dll
IMPORT Directory Table	00004034	00005548	HintName RVA	0150 GetStartupInfoA
IMPORT Name Table	00004038	0000555A	HintName RVA	0043 CreatePipe
IMPORT Hints/Names	0000403C	0000556B	HintName RVA	00F5 GetCurrentDirectoryA
IMAGE_EXPORT_DIRECTORY	00004040	00005536	HintName RVA	0044 CreateProcessA
EXPORT Address Table	00004044	00005590	HintName RVA	0388 InitiateA
EXPORT Name Points	00004048	0000559C	HintName RVA	0271 SetLastError
EXPORT Ordinal Table	0000404C	000055AC	HintName RVA	01F5 OutputDebugStringA
EXPORT Names	00004050	00005520	HintName RVA	001B CloseHandle
SECTION .data	00004054	0000551C	HintName RVA	0219 ReadFile
SECTION .reloc	00004058	0000550C	HintName RVA	0165 GetTempPathA
IMAGE_BASE_RELOC	0000405C	000054F0	HintName RVA	0121 GetLongPathNameA
	00004060	000054E8	HintName RVA	012C LoadLibraryA
	00004064	000054D6	HintName RVA	013E GetProcAddress
	00004068	000054C6	HintName RVA	004A CreateThread
	0000406C	000054B6	HintName RVA	0150 GetSystemTime
	00004070	000054A0	HintName RVA	02CE WaitForSingleObject
	00004074	0000548E	HintName RVA	028F TerminateThread
	00004078	00005466	HintName RVA	0296 Sleep
	0000407C	00005520	HintName RVA	011A GetLastError
	00004080	00005470	HintName RVA	0124 GetModuleFileNameA
	00004084	00000000	End of imports	kernel32.dll
	00004088	000055E4	HintName RVA	004C _chdir
	0000408C	000055D8	HintName RVA	01C5 _stricmp
	00004090	000055C8	HintName RVA	00D0 _adjust_lbr
	00004094	000055B8	HintName RVA	0291 malloc
	00004098	000055B2	HintName RVA	010F _system
	0000409C	000055AA	HintName RVA	025E free
	000040A0	00005592	HintName RVA	003E _rtime_initialize@UAC@UAC
	000040A4	00005572	HintName RVA	00CA _except_handler3
	000040A8	0000556C	HintName RVA	0041 _CxxThrowException
	000040AC	0000556E	HintName RVA	01C1 _stricmp

1.7 There is some exports?

Yes, there are exports, it exports several functions that seems to have installing and uninstalling purposes.

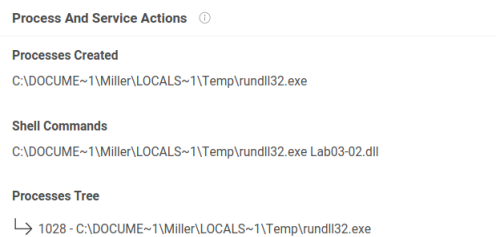
	pFile	Data	Description	Value
outlook.dll				
IMAGE_DOS_HEADER	00004028	00004706	Function RVA	0001 Install
MS-DOS Stub Program	0000402C	00003196	Function RVA	0002 ServiceMain
IMAGE_NT_HEADERS	00004030	00004B18	Function RVA	0003 UninstallService
Signature	00004034	00004B0B	Function RVA	0004 installA
IMAGE_FILE_HEADER	00004038	00004C2B	Function RVA	0005 uninstallA
IMAGE_OPTIONAL_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
SECTION .text				
SECTION .data				
IMPORT Address Table				
IMPORT Directory Table				
IMPORT Name Table				
IMPORT Hints/Names				
IMAGE_EXPORT_DIRECTORY				
EXPORT Address Table				
EXPORT Name Points				
EXPORT Ordinal Table				

1.8 What may be the functionalities of the malware?

My partner and I think that the malware is a dropper, because it has the capability of installing processes that it's going to use later. It also has the capability of creating network services using the *svrhost* process. This can mean that an attacker (*practicalmalwareanalysis*) can install other programs in the victim's machine.

1.9 From all previous answers, identify all host-based signatures for this malware.

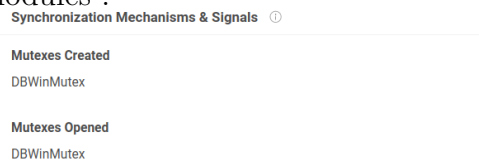
The next information is all the host-based signatures virustotal.com identified, but that we also identified with the static analysis, all these signatures are based on how the malware behaves inside an infected machine, which libraries it imports, which functions it exports, among other characteristics. processes:



The screenshot shows the 'Process And Service Actions' section of a VirusTotal report. It includes three sub-sections: 'Processes Created' with one entry, 'Shell Commands' with one entry, and 'Processes Tree' with one entry.

Process And Service Actions ⓘ
Processes Created C:\DOCUME~1\Miller\LOCALS~1\Temp\rundll32.exe
Shell Commands C:\DOCUME~1\Miller\LOCALS~1\Temp\rundll32.exe Lab03-02.dll
Processes Tree ↳ 1028 - C:\DOCUME~1\Miller\LOCALS~1\Temp\rundll32.exe

modules :



The screenshot shows the 'Synchronization Mechanisms & Signals' section of a VirusTotal report. It includes two sub-sections: 'Mutexes Created' and 'Mutexes Opened', both with one entry.

Synchronization Mechanisms & Signals ⓘ
Mutexes Created DBWinMutex
Mutexes Opened DBWinMutex

runtime modules :

Modules Loaded ⓘ

Runtime Modules

```
c:\windows\system32\wininet.dll
c:\windows\system32\imm32.dll
c:\documents and settings\miller\local settings\temp\lab03-02.dll
c:\windows\system32\mpr.dll
c:\windows\system32\comctl32.dll
c:\windows\system32\ws2help.dll
c:\windows\system32\rsaenh.dll
c:\windows\system32\ole32.dll
c:\windows\system32\secur32.dll
c:\windows\system32\msvcrt.dll
```

1.10 From all previous answers, identify all antivirus signatures for this malware.

As virustotal.com and we identified, the following information related to the presentation of the malware, however these characteristics can be easily modified by an attacker. Information like its hash values, its size, the names it might have, etc. hashes :

MD5	84882c9d43e23d63b82004fae74ebb61
SHA-1	c6fb3b50d946bec6f391aefa4e54478cf8607211
SHA-256	5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9
Vhash	124046655d5550c8z142qz71ze6z5
Authentihash	b76700f50d6f09408958f9e40f562908cd4050e0f992efaec0ca63e0fc9638e0
Imphash	3167552ee0bbbd4f5f440adf5f65bab8
SSDEEP	384:NcTA0TAKHWYvVvUYGXFgeJGjHwTACLPkIdSgbl/xAlrWdhoQsxRiAHZ:NcTA0TAK2y2oBCbH4gtxrWd5sxRL
File type	Win32 DLL
Magic	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
File size	23.50 KB (24065 bytes)
PEID packer	Microsoft Visual C++ v6.0 DLL

names

Names ⓘ

Lab03-02.dll
muestra2.dll
malsample.dll
malware4.dll
localfile~
malware.dll
hamit.dll
Mal02-02.dll
84882c9d43e23d63b82004fae74ebb61
smona_5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9.bin

history

History ⓘ

Creation Time	2010-09-28 01:00:25
First Submission	2012-03-16 12:46:35
Last Submission	2020-07-29 04:26:42
Last Analysis	2020-07-29 04:26:42

1.11 From all previous answers, identify all network-based signatures for this malware.

Finally, as we can check in the first image if the figure ??, the malware has a domain within its data setion, `practicalmalwareanalysis.com`, meaning that the malware is probably going to connect to that url, perform a DNS resolution and communicate with a command&control server.

2 Dynamic Analysis

2.1 Take a snapshot of the register keys before the infection using the application Regshot.

eHre is the snapchot of the register keys

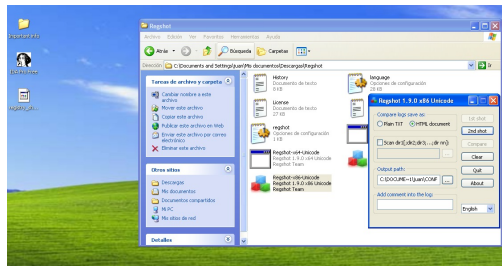


Figure 6: snapshot of the register keys

2.2 Take a snapshot of the virtual machine before the infection

here is the snapshot of the virtual machine before the infection :

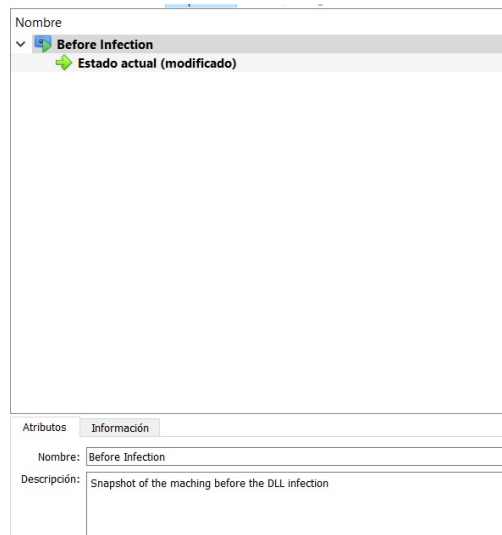


Figure 7: snapshot

2.3 Install the malware using the command: `C:\rundll32.exe outlook.dll, installA`

We proceed to install the malware using the command *C :> rundll32.exeoutlook.dll*

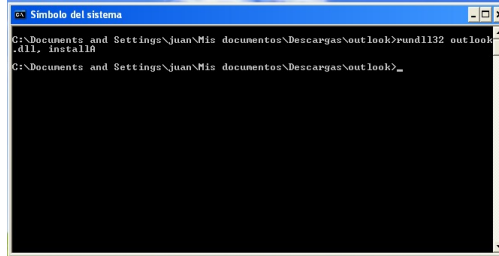


Figure 8: command

2.4 `installA` was a function identified previously in the static analysis?

Yes, `installA` was a function we identified with the static analysis inside the strings and in the exports.

2.5 Take a second snapshot of the register keys with Regshot. Identify the changes before and after the infection (keys created, modified, delete, etc)?

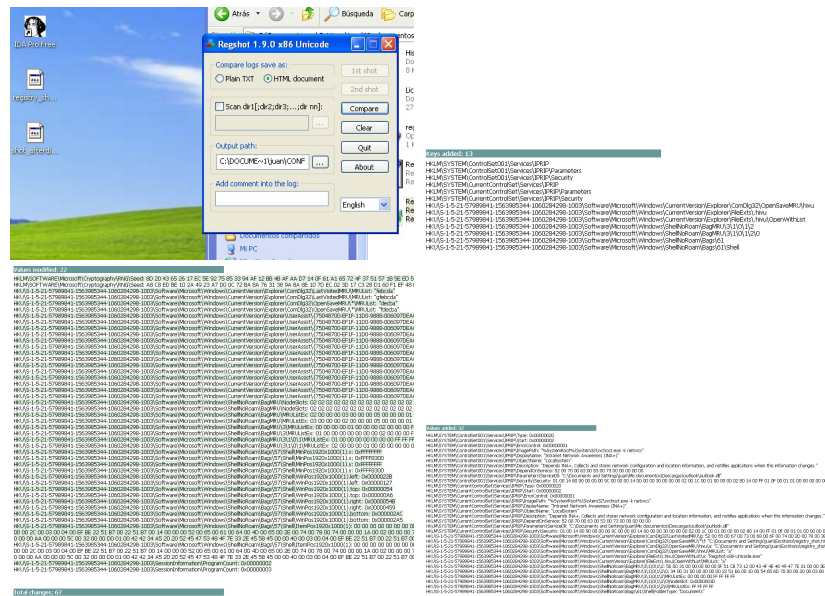


Figure 9: snapshots

- We can see that it included 13 new keys, and a good amount of them involve the new service IPRIP .
- A total of 22 keys values were modified, however the purpose of the modification can't be understood.
- And finally the infected dll added a total of 32 values to existing or new keys, most of these new values are for the IPRIP service.

2.6 Analyze in detail the register keys and identify the name of the service that was installed by the malware?

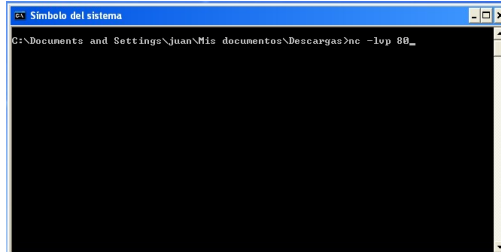
As we identified in the last point, the service the malware created is IPRIP, we know it is a service because it was located in the service path and it seems to use the svchost.exe executable, that hosts the services of the machine

2.7 Analyze the register keys and identify the name of the executable that apparently consumes (import) the DLL?

It is importing service host, It includes processes including Windows Auto Update and many required system services would be running in it. This can let the attacker control processes and windows versions in the victim's machine.

2.8 Create a virtual network of 2 Virtual machines. One of them will be the infected machine, and the other will be the server of Command & Control. Install Netcat on the last one to emulate the behavior of a web server.

On the command and control machine ...



on the victim's machine we configured the DNS Spoof, so the malware is going to connect to our command and control server and not to the attacker server...

```
hosts - Bloc de notas
Archivo Edición Formato Ver Ayuda
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Este es un ejemplo de archivo HOSTS usado por Microsoft TCP/IP para Windows.
#
# Este archivo contiene las asignaciones de las direcciones IP a los nombres de
# host. Cada entrada debe permanecer en una línea individual. La dirección IP
# debe ponerse en la primera columna, seguida del nombre de host correspondiente.
# La dirección IP y el nombre de host deben separarse con al menos un espacio.
#
# También pueden insertarse comentarios (como éste) en líneas individuales
# o a continuación del nombre de equipo indicándolos con el símbolo #
#
# Por ejemplo:
# 102.54.94.97 rhino.acme.com      # servidor origen
# 38.25.63.10  x.acme.com         # host cliente x
127.0.0.1      localhost
169.254.125.41 practica1malwareanalysis.com
```

now, we are going to test the connection between the machines with the DNS spoofed...

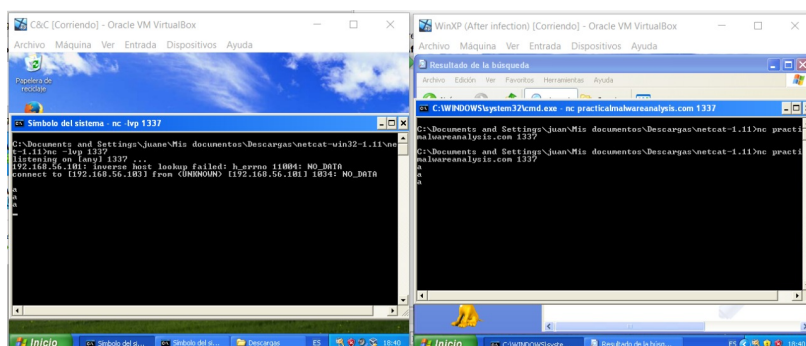


Figure 10: Connections

2.9 Start the malicious service in the infected machine using the command: net start IPRIP

now we initialized the service IPRIP. notice that the service was already initialized because we already found this service in previous section of this analysis.

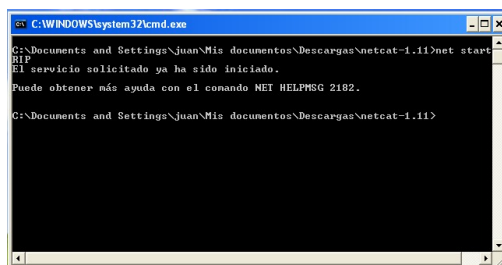


Figure 11: Service Initialized

2.10 Why IPRIP? Did you find the word (IPRIP) in some of the previous steps?

We found it interesting because it was consuming svchost.exe, this service allow the attacker to take control of the processes in the victim's machine.

2.11 Execute Process Explorer. Find the process that is running the malware using the "Find DLL" functionality of Process Explorer. Identify the Process Id (PID)

Using tool FindDll we identified the process that the library is running the process id is ...

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
smss.exe	168 K	1,768 K	32 K	364	Administrador de unidades de disco	Microsoft Corporation
svchost.exe	1,768 K	3,768 K	3,768 K	988	Host Process for Windows Services	Microsoft Corporation
netcat.exe	6,400 K	4,352 K	4,352 K	612	Aplicación de red de sockets	Microsoft Corporation
svchost.exe	1,504 K	1,504 K	1,504 K	1,504	Host Process for Windows Services	Microsoft Corporation
svchost.exe	2,136 K	3,440 K	3,440 K	624	Visualizador de eventos de Windows	Microsoft Corporation
svchost.exe	2,200 K	4,184 K	4,184 K	624	Visualizador de eventos de Windows	Microsoft Corporation
svchost.exe	1,916 K	4,032 K	4,032 K	1,916	Host Process for Windows Services	Microsoft Corporation
svchost.exe	1,612 K	3,560 K	3,560 K	1,612	Host Process for Windows Services	Microsoft Corporation
svchost.exe	12,160 K	21,168 K	21,168 K	1052	Host Process for Windows Services	Microsoft Corporation
svchost.exe	408 K	2,104 K	2,104 K	1,132	Host Process for Windows Services	Microsoft Corporation
svchost.exe	5,508 K	5,140 K	5,140 K	836	Activación automática	Microsoft Corporation
svchost.exe	1,068 K	2,088 K	2,088 K	1,068	Host Process for Windows Services	Microsoft Corporation
svchost.exe	1,600 K	4,188 K	4,188 K	1,600	Host Process for Windows Services	Microsoft Corporation
svchost.exe	2,268 K	4,388 K	4,388 K	1,612	Host Process for Windows Services	Microsoft Corporation
svchost.exe	1,056 K	3,300 K	3,300 K	1,056	Host Process for Windows Services	Microsoft Corporation

Figure 12: 1052

2.12 Execute Process Monitor and search the process using the PID

Having the process id, we found the process in the process monitor —

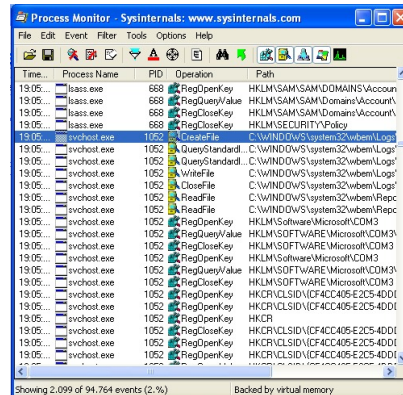


Figure 13: process of process id

2.13 Create filters to reduce the events to fewer than 10 events in the Process Monitor. Use filters that allow to identify keys and files modified or created.

We applied the following filters ...

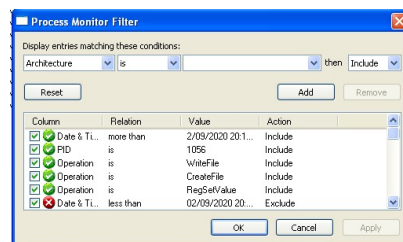


Figure 14: Filters

and we obtained these results ...

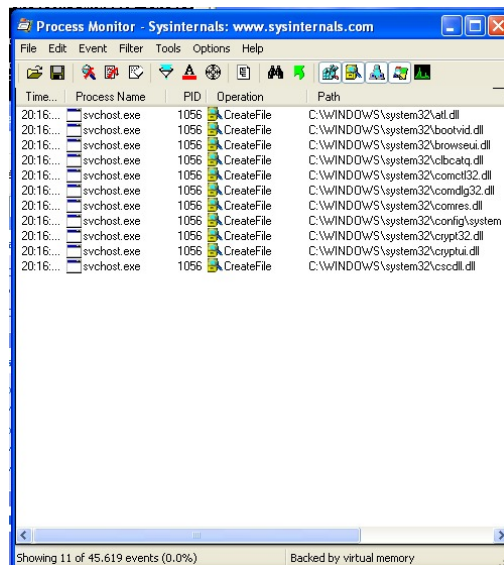


Figure 15: Filtered

2.14 Does the malware resolve some domain?

Yes, it resolving to www.practicalmalwareanalysis.com

2.15 Configure the nc tool with port 443, 8000 and 80. Which port is contacted on that domain? Capture the request done by the malware

configuration ...

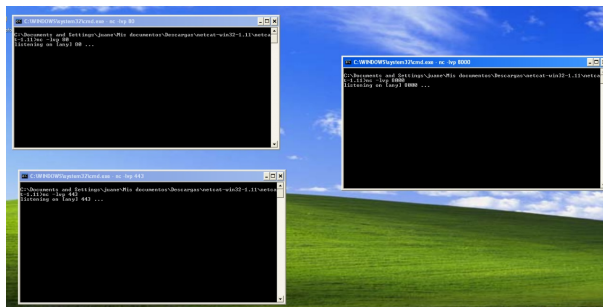
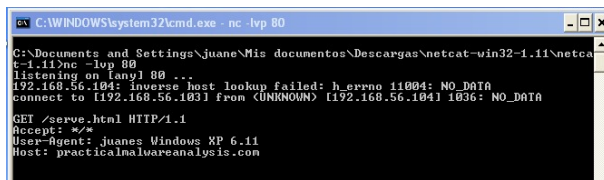


Figure 16: Configuration

we received communication at port 80 . and we get this



```
C:\WINDOWS\system32\cmd.exe - nc -lvp 80
C:\Documents and Settings\Juane\Mis documentos\Descargas\netcat-win32-1.11\netcat
t-1.11>nc -lvp 80
listening on [any] 80 ...
192.168.56.104: inverse host lookup failed: h_errno: NO_DATA
connect to [192.168.56.103] from <UNKNOWN> [192.168.56.104] 1836: NO_DATA
GET /serve.html HTTP/1.1
Accept: */*
User-Agent: juanes Windows XP 6.11
Host: practicalmalwareanalysis.com
```

Figure 17: Port80

2.16 From all previous answers, identify all host-based signatures for this malware.

Through all this work we found several host based signatures, the most noticeable are that it imports important dynamic libraries such as *kernel32.dll*, it exports functions such as *installA*, *install*, etc. It modifies and creates files and registry keys alike as seen in figure ??, and one of the most interesting ones is the creation of the service IPRIP that is hosted using the *svchost.exe* process of windows.

2.17 From all previous answers, identify all antivirus signatures for this malware.

This sections don't change much compared to the last status of the report, all due to that the dynamic analysis performed in this laboratory provide plenty of host-based signatures, that is the reason why we stick to our previous answers, the hash, creation time, the metadata, the size, etc.

2.18 From all previous answers, identify all network-based signatures for this malware.

We could confirm that the malware communicates with a command and control server using the *practicalmalwareanalysis.com* domain, we were able to verify that with the DNS spoof performed.