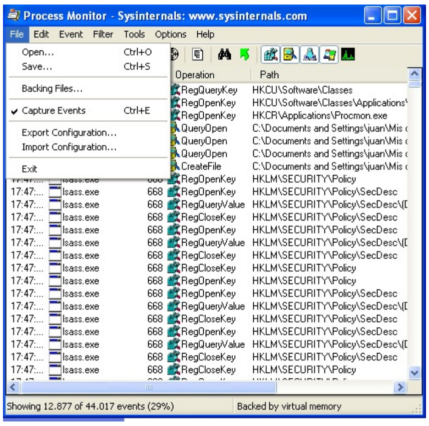
4th Lab: Disassembly And IDAPro

Rodrigo Castillo featuring Juen Esteban Murcia

29 de agosto de 2020

1. Process monitor:

Here, my team started to capture events :

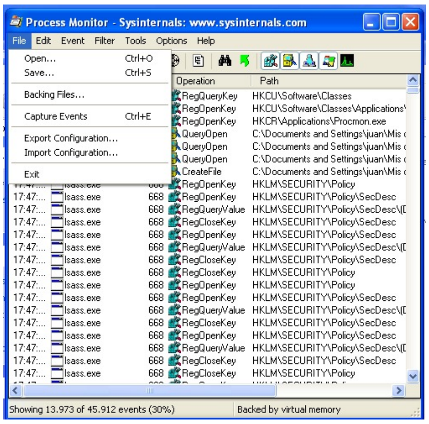


```
                              Operation      Path
                              RegQueryKey    HKCU\Software\Classes
                              RegOpenKey     HKCU\Software\Classes\Applications\
                              RegOpenKey     HKCR\Applications\Procmon.exe
                              QueryOpen      C:\Documents and Settings\juan\Mis
                              QueryOpen      C:\Documents and Settings\juan\Mis
                              QueryOpen      C:\Documents and Settings\juan\Mis
                              CreateFile     C:\Documents and Settings\juan\Mis
                              RegOpenKey     HKLM\SECURITY\Policy
17:47:...   lsass.exe   668   RegOpenKey     HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegOpenKey     HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy
17:47:...   lsass.exe   668   RegOpenKey     HKLM\SECURITY\Policy
17:47:...   lsass.exe   668   RegOpenKey     HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegOpenKey     HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy

Showing 12.877 of 44.017 events (29%)      Backed by virtual memory
```

Figura 1: Event Capture

then, we stop capturing events. :

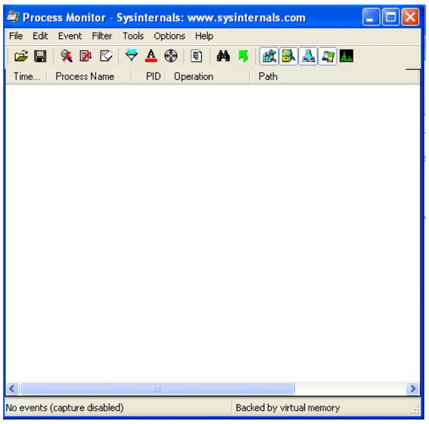


```
                              Operation      Path
                              RegQueryKey    HKCU\Software\Classes
                              RegOpenKey     HKCU\Software\Classes\Applications\
                              RegOpenKey     HKCR\Applications\Procmon.exe
                              QueryOpen      C:\Documents and Settings\juan\Mis
                              QueryOpen      C:\Documents and Settings\juan\Mis
                              QueryOpen      C:\Documents and Settings\juan\Mis
                              CreateFile     C:\Documents and Settings\juan\Mis
                              RegOpenKey     HKLM\SECURITY\Policy
17:47:...   lsass.exe   668   RegOpenKey     HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegOpenKey     HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy
17:47:...   lsass.exe   668   RegOpenKey     HKLM\SECURITY\Policy
17:47:...   lsass.exe   668   RegOpenKey     HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegOpenKey     HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy\SecDesc
17:47:...   lsass.exe   668   RegCloseKey    HKLM\SECURITY\Policy

Showing 13.973 of 45.912 events (30%)      Backed by virtual memory
```

Figura 2: Stop Capturing events

then, my team proceed to clean the dispay :



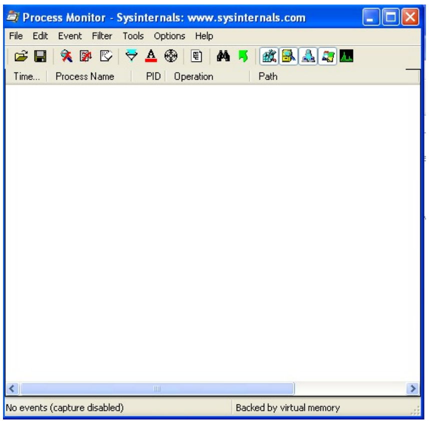
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time... Process Name PID Operation Path

No events (capture disabled)

Backed by virtual memory

Figura 3: Cleaning Display

after this, my teem proceed to take the snapchot of the machine before infecting it :



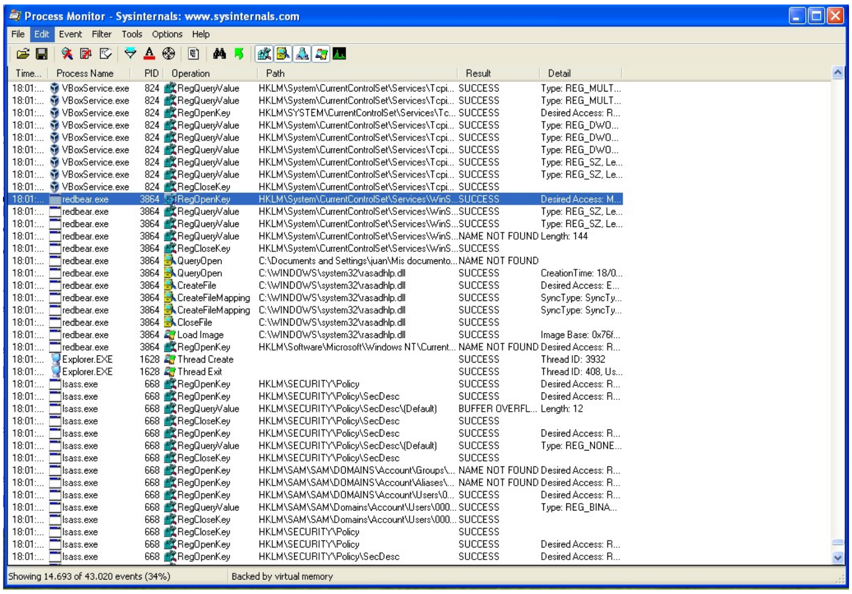
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time... Process Name PID Operation Path

No events (capture disabled)

Backed by virtual memory

Figura 4: Snapchot of the machine before running the malware

At this point, we are able to review the events that redbear is running :



Time...	Process Name	PID	Operation	Path	Result	Detail
18:01:...	VBoxService.exe	824	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpi...	SUCCESS	Type: REG_MULT...
18:01:...	VBoxService.exe	824	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpi...	SUCCESS	Type: REG_MULT...
18:01:...	VBoxService.exe	824	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Tc...	SUCCESS	Desired Access: R...
18:01:...	VBoxService.exe	824	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpi...	SUCCESS	Type: REG_DWO...
18:01:...	VBoxService.exe	824	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpi...	SUCCESS	Type: REG_DWO...
18:01:...	VBoxService.exe	824	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpi...	SUCCESS	Type: REG_DWO...
18:01:...	VBoxService.exe	824	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpi...	SUCCESS	Type: REG_SZ, Le...
18:01:...	VBoxService.exe	824	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpi...	SUCCESS	Type: REG_SZ, Le...
18:01:...	VBoxService.exe	824	RegCloseKey	HKLM\System\CurrentControlSet\Services\Tcpi...	SUCCESS	
18:01:...	redbear.exe	3864	RegOpenKey	HKLM\System\CurrentControlSet\Services\WinS...	SUCCESS	Desired Access: M...
18:01:...	redbear.exe	3864	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinS...	SUCCESS	Type: REG_SZ, Le...
18:01:...	redbear.exe	3864	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinS...	SUCCESS	Type: REG_SZ, Le...
18:01:...	redbear.exe	3864	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinS...	NAME NOT FOUND	Length: 144
18:01:...	redbear.exe	3864	RegCloseKey	HKLM\System\CurrentControlSet\Services\WinS...	SUCCESS	
18:01:...	redbear.exe	3864	QueryOpen	C:\Documents and Settings\juan\Mis documento...	NAME NOT FOUND	
18:01:...	redbear.exe	3864	QueryOpen	C:\WINDOWS\system32\rasadhlp.dll	SUCCESS	CreationTime: 18/0...
18:01:...	redbear.exe	3864	CreateFile	C:\WINDOWS\system32\rasadhlp.dll	SUCCESS	Desired Access: E...
18:01:...	redbear.exe	3864	CreateFileMapping	C:\WINDOWS\system32\rasadhlp.dll	SUCCESS	SyncType: SyncTy...
18:01:...	redbear.exe	3864	CreateFileMapping	C:\WINDOWS\system32\rasadhlp.dll	SUCCESS	SyncType: SyncTy...
18:01:...	redbear.exe	3864	CloseFile	C:\WINDOWS\system32\rasadhlp.dll	SUCCESS	
18:01:...	redbear.exe	3864	Load Image	C:\WINDOWS\system32\rasadhlp.dll	SUCCESS	Image Base: 0x76f...
18:01:...	redbear.exe	3864	RegOpenKey	HKLM\Software\Microsoft\Windows NT\Current...	NAME NOT FOUND	Desired Access: R...
18:01:...	Explorer.EXE	1628	Thread Create		SUCCESS	Thread ID: 3932
18:01:...	Explorer.EXE	1628	Thread Exit		SUCCESS	Thread ID: 408, Us...
18:01:...	lsass.exe	668	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: R...
18:01:...	lsass.exe	668	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...
18:01:...	lsass.exe	668	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(Default)	BUFFER OVERFL...	Length: 12
18:01:...	lsass.exe	668	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
18:01:...	lsass.exe	668	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...
18:01:...	lsass.exe	668	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\(Default)	SUCCESS	Type: REG_NONE...
18:01:...	lsass.exe	668	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
18:01:...	lsass.exe	668	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\Groups\...	NAME NOT FOUND	Desired Access: R...
18:01:...	lsass.exe	668	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\Aliases\...	NAME NOT FOUND	Desired Access: R...
18:01:...	lsass.exe	668	RegOpenKey	HKLM\SAM\SAM\DOMAINS\Account\Users\0...	SUCCESS	Desired Access: R...
18:01:...	lsass.exe	668	RegQueryValue	HKLM\SAM\SAM\Domains\Account\Users\000...	SUCCESS	Type: REG_BINA...
18:01:...	lsass.exe	668	RegCloseKey	HKLM\SAM\SAM\Domains\Account\Users\000...	SUCCESS	
18:01:...	lsass.exe	668	RegCloseKey	HKLM\SECURITY\Policy	SUCCESS	
18:01:...	lsass.exe	668	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: R...
18:01:...	lsass.exe	668	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: R...

Showing 14.693 of 43.020 events (34%)   Backed by virtual memory

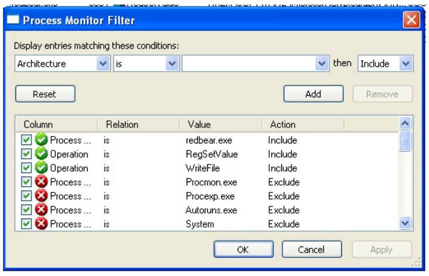
Figura 5: Events that Redbear is running

We can apreciete the keys and memory spaces where redbear is taking access , also, the .dll files he's calling and the files he is creating. we can check which of those process where correctly runned by the malware and which of those failed in the execution. also , we can see information about the keys that the malware is changing, this can be usefull because then we will use this for go deeper in te behavior of the malware.

Filters are usefull because somethimes computers are running a lot of process that they need for mantain the computer working , as we can see in figure 5 , there are several processes that the machine is running , but there are many process that we dont want to see, such as Virtual Box processes. Filters allow to:

- focus in the process what we want to see
- search for processes that can be usefull to understand the malware
- search for specified actions

image of filters applied:



Display entries matching these conditions:

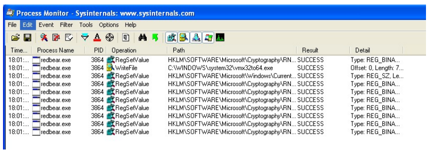
Architecture | is | | then Include

Column	Relation	Value	Action
☑ ✓ Process ...	is	redbear.exe	Include
☑ ✓ Operation	is	RegSetValue	Include
☑ ✓ Operation	is	WriteFile	Include
☑ ✗ Process ...	is	Procmon.exe	Exclude
☑ ✗ Process ...	is	Procexp.exe	Exclude
☑ ✗ Process ...	is	Autoruns.exe	Exclude
☑ ✗ Process ...	is	System	Exclude

Figura 6: Filters applied

now, with filters, processes window looks like this :

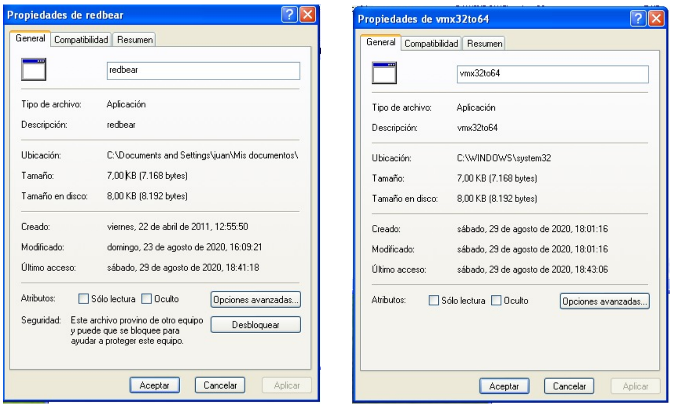
looking at the specific processes in process monitor, we can see that redbear created a key called videodriver . this key initialize the proccess of.



Time...	Process Name	PID	Operation	Path	Result	Detail
18:01:...	redbear.exe	3864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RN...	SUCCESS	Type: REG_BINA...
18:01:...	redbear.exe	3864	WriteFile	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS	Offset: 0, Length: 7...
18:01:...	redbear.exe	3864	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\Current...	SUCCESS	Type: REG_SZ, Le...
18:01:...	redbear.exe	3864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RN...	SUCCESS	Type: REG_BINA...
18:01:...	redbear.exe	3864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RN...	SUCCESS	Type: REG_BINA...
18:01:...	redbear.exe	3864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RN...	SUCCESS	Type: REG_BINA...
18:01:...	redbear.exe	3864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RN...	SUCCESS	Type: REG_BINA...
18:01:...	redbear.exe	3864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RN...	SUCCESS	Type: REG_BINA...
18:01:...	redbear.exe	3864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RN...	SUCCESS	Type: REG_BINA...
18:01:...	redbear.exe	3864	RegSetValue	HKLM\SOFTWARE\Microsoft\Cryptography\RN...	SUCCESS	Type: REG_BINA...

Figura 7: Processes filtered

Now, we can apreciate that the size of redbear is $7kB$, also, the space of the file that was created is also $7kB$, that is supicious because it can mean that the file is exactly the same:



redbear

Tipo de archivo: Aplicación

Descripción: redbear

Ubicación: C:\Documents and Settings\juan\Mis documentos\

Tamaño: 7,00 KB (7.168 bytes)

Tamaño en disco: 8,00 KB (8.192 bytes)

Creado: viernes, 22 de abril de 2011, 12:55:50

Modificado: domingo, 23 de agosto de 2020, 16:09:21

Último acceso: sábado, 29 de agosto de 2020, 18:41:18

Atributos: □ Sólo lectura □ Oculto

Seguridad: Este archivo provino de otro equipo y puede que se bloquee para ayudar a proteger este equipo.

vmx32to64

Tipo de archivo: Aplicación

Descripción: vmx32to64

Ubicación: C:\WINDOWS\system32

Tamaño: 7,00 KB (7.168 bytes)

Tamaño en disco: 8,00 KB (8.192 bytes)

Creado: sábado, 29 de agosto de 2020, 18:01:16

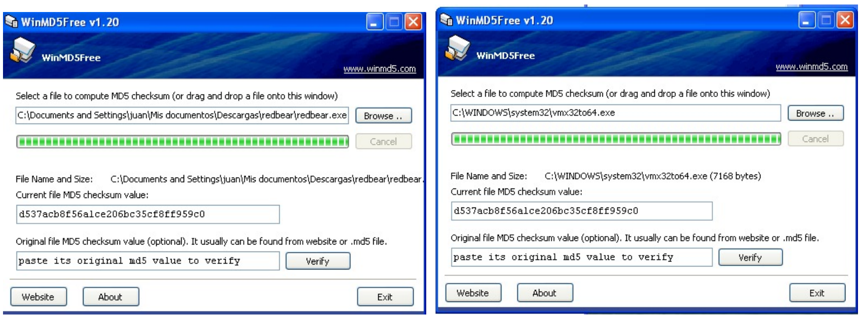
Modificado: sábado, 29 de agosto de 2020, 18:01:16

Último acceso: sábado, 29 de agosto de 2020, 18:43:06

Atributos: □ Sólo lectura □ Oculto

Figura 8: Sizes of both executables

for checking is the file is the same, we are going to check de hash,there are many hashing algorithm but we are going to use MD5.



Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\Documents and Settings\juan\Mis documentos\Descargas\redbear\redbear.exe

File Name and Size: C:\Documents and Settings\juan\Mis documentos\Descargas\redbear\redbear.

Current file MD5 checksum value:

d537acb8f56a1ce206bc35cf8ff959c0

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file.

paste its original md5 value to verify

Select a file to compute MD5 checksum (or drag and drop a file onto this window)

C:\WINDOWS\system32\vmx32to64.exe

File Name and Size: C:\WINDOWS\system32\vmx32to64.exe (7168 bytes)

Current file MD5 checksum value:

d537acb8f56a1ce206bc35cf8ff959c0

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file.

paste its original md5 value to verify

Figura 9: Hashes MD5 of both files

As we can see they are the same file ! :O , it means the program cloned itself to another path to hide from the owner of the machine.

this was our reaction when we saw that the hashes were the same : ¿Its a Colission?

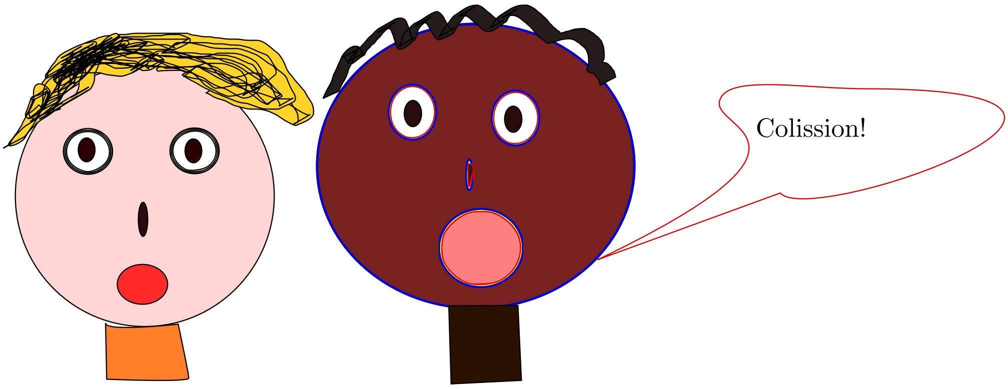
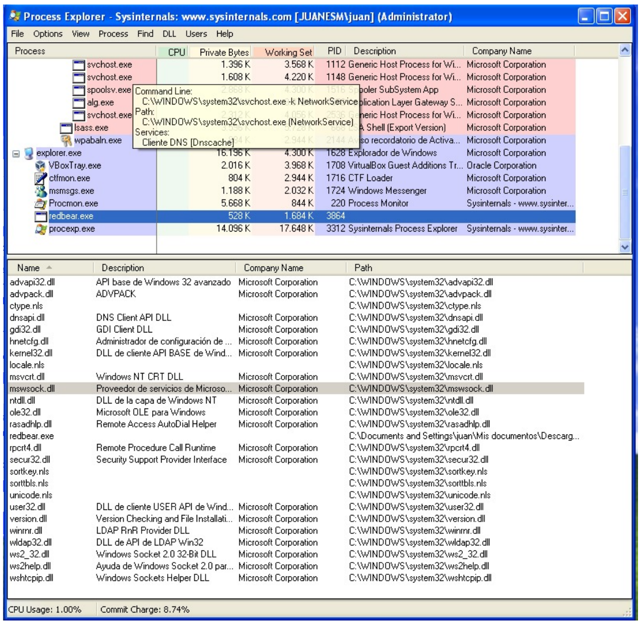


Figura 10: reaction

2. Process explorer

We proceed to exectute process explorer : in the lower part of the window we can apreciate



Process Explorer - Sysinternals: www.sysinternals.com [JUANESM\juan] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		1.396 K	3.568 K	1112	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1.608 K	4.220 K	1148	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		2.868 K	4.300 K	1516	Spooler SubSystem App	Microsoft Corporation
alg.exe					plication Layer Gateway S...	Microsoft Corporation
svchost.exe		2.312 K	4.056 K	2536	Generic Host Process for Wi...	Microsoft Corporation
lsass.exe				668	A Shell (Export Version)	Microsoft Corporation
wpabaln.exe			2.944 K	2144	so recordatorio de Activa...	Microsoft Corporation
explorer.exe		16.196 K	4.300 K	1628	Explorador de Windows	Microsoft Corporation
VBoxTray.exe		2.016 K	3.968 K	1708	VirtualBox Guest Additions Tr...	Oracle Corporation
ctfmon.exe		804 K	2.944 K	1716	CTF Loader	Microsoft Corporation
msmsgs.exe		1.188 K	2.032 K	1724	Windows Messenger	Microsoft Corporation
Procmon.exe		5.668 K	844 K	220	Process Monitor	Sysinternals - www.sysinter...
redbear.exe		528 K	1.684 K	3864		
procexp.exe		14.096 K	17.648 K	3312	Sysinternals Process Explorer	Sysinternals - www.sysinter...

Command Line:
C:\WINDOWS\system32\svchost.exe -k NetworkService
Path:
C:\WINDOWS\system32\svchost.exe (NetworkService)
Services:
Cliente DNS [Dnscache]

Name	Description	Company Name	Path
advapi32.dll	API base de Windows 32 avanzado	Microsoft Corporation	C:\WINDOWS\system32\advapi32.dll
advpack.dll	ADVPACK	Microsoft Corporation	C:\WINDOWS\system32\advpack.dll
ctype.nls			C:\WINDOWS\system32\ctype.nls
dnsapi.dll	DNS Client API DLL	Microsoft Corporation	C:\WINDOWS\system32\dnsapi.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\WINDOWS\system32\gdi32.dll
hnetcfg.dll	Administrador de configuración de ...	Microsoft Corporation	C:\WINDOWS\system32\hnetcfg.dll
kernel32.dll	DLL de cliente API BASE de Wind...	Microsoft Corporation	C:\WINDOWS\system32\kernel32.dll
locale.nls			C:\WINDOWS\system32\locale.nls
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	C:\WINDOWS\system32\msvcrt.dll
mswsock.dll	Proveedor de servicios de Microso...	Microsoft Corporation	C:\WINDOWS\system32\mswsock.dll
ntdll.dll	DLL de la capa de Windows NT	Microsoft Corporation	C:\WINDOWS\system32\ntdll.dll
ole32.dll	Microsoft OLE para Windows	Microsoft Corporation	C:\WINDOWS\system32\ole32.dll
rasadhlp.dll	Remote Access AutoDial Helper	Microsoft Corporation	C:\WINDOWS\system32\rasadhlp.dll
redbear.exe			C:\Documents and Settings\juan\Mis documentos\Descarg...
rpcrt4.dll	Remote Procedure Call Runtime	Microsoft Corporation	C:\WINDOWS\system32\rpcrt4.dll
secur32.dll	Security Support Provider Interface	Microsoft Corporation	C:\WINDOWS\system32\secur32.dll
sortkey.nls			C:\WINDOWS\system32\sortkey.nls
sorttbls.nls			C:\WINDOWS\system32\sorttbls.nls
unicode.nls			C:\WINDOWS\system32\unicode.nls
user32.dll	DLL de cliente USER API de Wind...	Microsoft Corporation	C:\WINDOWS\system32\user32.dll
version.dll	Version Checking and File Installati...	Microsoft Corporation	C:\WINDOWS\system32\version.dll
winrnr.dll	LDAP RnR Provider DLL	Microsoft Corporation	C:\WINDOWS\system32\winrnr.dll
wldap32.dll	DLL de API de LDAP Win32	Microsoft Corporation	C:\WINDOWS\system32\wldap32.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	C:\WINDOWS\system32\ws2_32.dll
ws2help.dll	Ayuda de Windows Socket 2.0 par...	Microsoft Corporation	C:\WINDOWS\system32\ws2help.dll
wshtcpip.dll	Windows Sockets Helper DLL	Microsoft Corporation	C:\WINDOWS\system32\wshtcpip.dll

CPU Usage: 1.00% Commit Charge: 8.74%

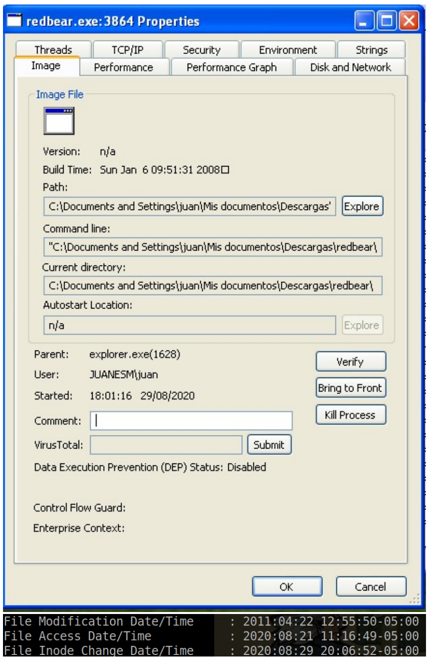
Figura 11: Process explorer execution

the .dlls that the process is using.
among them we can find libraries like :

- advapi32
- kernel32

- user32
- secure32

now proceed to check the metadata of the file : this can be interesting because we can see information about the file, such as the date when it was created and the type of binary it is.
 the ”verify”button works when you want to check that the signatures inside the file are valid.



redbear.exe:3864 Properties

Version: n/a
Build Time: Sun Jan 6 09:51:31 2008□
Path:
C:\Documents and Settings\juan\Mis documentos\Descargas'
Command line:
"C:\Documents and Settings\juan\Mis documentos\Descargas\redbear\
Current directory:
C:\Documents and Settings\juan\Mis documentos\Descargas\redbear\
Autostart Location:
n/a

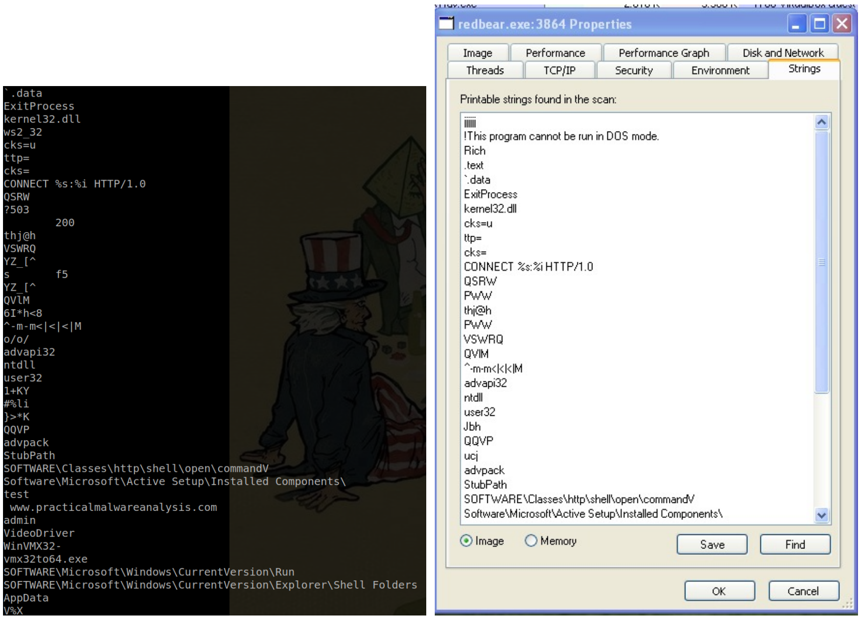
Parent: explorer.exe(1628)
User: JUANESM\juan
Started: 18:01:16 29/08/2020
Comment:
VirusTotal:
Data Execution Prevention (DEP) Status: Disabled

Control Flow Guard:
Enterprise Context:

```
File Modification Date/Time     : 2011:04:22 12:55:50-05:00
File Access Date/Time           : 2020:08:21 11:16:49-05:00
File Inode Change Date/Time     : 2020:08:29 20:06:52-05:00
```

Figura 12: Metadata

The strings in disk are the same that the strings in execution :



```
`.data
ExitProcess
kernel32.dll
ws2_32
cks=u
ttp=
cks=
CONNECT %s:%i HTTP/1.0
QSRW
?503
        200
thj@h
VSWRQ
YZ_[^
s       f5
YZ_[^
QVlM
6I*h<8
^-m-m<|<|<|M
o/o/
advapi32
ntdll
user32
1+KY
#%li
}>*K
QQVP
advpack
StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
test
 www.practicalmalwareanalysis.com
admin
VideoDriver
WinVMX32-
vmx32to64.exe
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
AppData
V%X
```

redbear.exe:3864 Properties

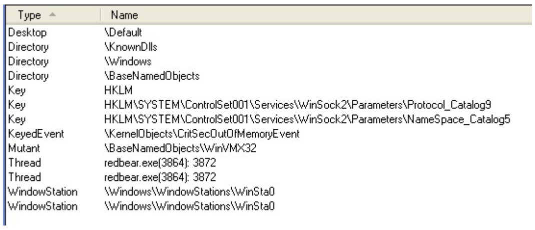
Printable strings found in the scan:

```
iiiiii
!This program cannot be run in DOS mode.
Rich
.text
`.data
ExitProcess
kernel32.dll
cks=u
ttp=
cks=
CONNECT %s:%i HTTP/1.0
QSRW
PWW
thj@h
PWW
VSWRQ
QVIM
^-m-m<|<|<|M
advapi32
ntdll
user32
Jbh
QQVP
ucj
advpack
StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
```

● Image ○ Memory

Figura 13: Strings

handles:



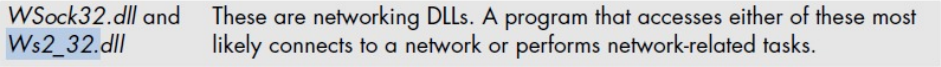
Type	Name
Desktop	\Default
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
Key	HKLM
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
Mutant	\BaseNamedObjects\WinVMX32
Thread	redbear.exe(3864): 3872
Thread	redbear.exe(3864): 3872
WindowStation	\Windows\WindowStations\WinSta0
WindowStation	\Windows\WindowStations\WinSta0

Figura 14: Handles

Mutant referst that is a modification of the original malware , with different hash.

2.1. ws2_32.dll and wshtcpip.dll libraries

library ws2_32.dll works for networking processes, but it also works for exhausting processes,processes that overcharge processors and make the machine slower.
wshtcpip library works for networking processes , is the library that handle tcp connections, as we know that redbear is a trojan, this library is the one that is going to send the conection to an attacker-host machine.



WSock32.dll and *Ws2_32.dll*	These are networking DLLs. A program that accesses either of these most likely connects to a network or performs network-related tasks.

Figura 15: Libs