

Las muestras de software ransomware as a service de la variante REvil que se van a estudiar han sido obtenidas de la fuente publica Any Run y son:

Nombre de la muestra	MD5	Primera vez subido a Virus Total	Nombre
REvil1	b86ad4241b01376b3924a380f6f4c934	03/08/2020	“Ransom:Win32/Revil.A”
REvil2	f0c97dc65a030a214f6dd33cf4a8566	06/08/2019	“Ransom:Win32/Revil.B”
REvil3	21d01fa87dfcaf971ff7b63a1a6fd94	09/09/2021	“Ransom:Win32/Revil.A”
REvil4	ff0e2ce0af118bae62969a5e897b59b2	17/03/2021	“Ransom:Win32/Revil.A”
REvil5	0bb803ea960f1f2c88f4e0cd808c196e	28/04/2019	“Trojan:Win32/Malgent.B”

ANALISIS ESTATICO:

MUESTRA 1:

Para tener una referencia sobre el malware a analizar, se utilizará la ayuda de Virus Total, el cual nos informa que 57 de los 67 motores de búsqueda de antivirus lo reconocen como malicioso. Profundizándonos un poco más, podemos obtener que Microsoft reconoce este malware como “Ransom:Win32/Revil.A” y GData como “Gen:Variant.Razy.525651”, lo que este último no nos proporciona ningún tipo de información relevante.

En las propiedades básicas se puede observar datos con gran valor, como los algoritmos MD5, SHA-1 y SHA-256. También se puede ver la fecha de creación, siendo el 28 de julio de 2020 y la primera vez que se observó el 3 de agosto de 2020.

Basic Properties ⓘ	
MD5	b86ad4241b01376b3924a380f6f4c934
SHA-1	10682d08a18715a79ee23b58fdb6ee44c4e28c61
SHA-256	14c8e3ff23d16c2c9a4272cd05d00461d27b372cc5f588b4bbfc6102bbcd708
Vhash	015056657d7d555bz6nz1fz
Authentihash	cc8734007b1f11fe87d918a712fc0889d9f5711ea9afb3e14f6a654a290bd1
Imphash	60a64185e19afa379906abb359cf2ed
Rich PE header hash	9f00d540841ba43353b55843f488e6fa
SSDEEP	1536:atZINbRi05Kw6KTUkmHlnMvWWhbpfCqeICs4AKvQlFlswOmZFS0cnwp/GmQwB:FRix3PWhNIOVfmw5q0cfmQ
TLSH	T123C3CF23BC5183F2C9A385F313B7F1B95BFFE34151668AAD32589448A2508397276A7
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Dynamic Link Library (generic) (29.6%)
TrID	Win16 NE executable (generic) (22.7%)
TrID	Win32 Executable (generic) (20.3%)
TrID	OS/2 Executable (generic) (9.1%)
TrID	Generic Win/DOS Executable (9%)
File size	116.50 KB (119296 bytes)

History ⓘ	
Creation Time	2020-07-28 19:02:45 UTC
First Submission	2020-08-03 15:09:10 UTC
Last Submission	2021-04-23 15:08:31 UTC
Last Analysis	2022-03-15 06:09:54 UTC

```

Registry Actions ⓘ
Registry Keys Set
+ HKLM\System\CurrentControlSet\Services\BITS\Start
+ HKLM\System\CurrentControlSet\Services\CryptSvc\DeleteFlag
+ HKLM\System\CurrentControlSet\Services\CryptSvc\Start
+ HKLM\System\CurrentControlSet\Services\AeLookupSvc\DeleteFlag
+ HKLM\System\CurrentControlSet\Services\AeLookupSvc\Start

Process And Service Actions ⓘ
Shell Commands
"pwsh.exe" -e
RwBIAHQALQBXAG0AaQBPAG!AagBiAGMAdAAgAfCaaQBuADMAMgBfAFMAaAbhAGQAbwB3AGMAbwBwAHkA|AB8ACAARgBvAH|ARQBhAGMAaAA|AE8AYgBqAGUAYwB0ACAAewAkAF8ALgBEAGUAbAB|

Processes Terminated
wmiadap.exe /F /T /R
"pwsh.exe" -e
RwBIAHQALQBXAG0AaQBPAG!AagBiAGMAdAAgAfCaaQBuADMAMgBfAFMAaAbhAGQAbwB3AGMAbwBwAHkA|AB8ACAARgBvAH|ARQBhAGMAaAA|AE8AYgBqAGUAYwB0ACAAewAkAF8ALgBEAGUAbAB|
%windir%\System32\svchost.exe -k WerSvcGroup

Processes Tree
↳ 2136 - %windir%\system32\wbem\wmprvse.exe
↳ 2188 - wmiadap.exe /F /T /R
↳ 2636 - %SAMPLEPATH%
↳ 2708 - powershell -e
RwBIAHQALQBXAG0AaQBPAG!AagBiAGMAdAAgAfCaaQBuADMAMgBfAFMAaAbhAGQAbwB3AGMAbwBwAHkA|AB8ACAARgBvAH|ARQBhAGMAaAA|AE8AYgBqAGUAYwB0ACAAewAkAF8ALgBEAGUAbAB|
↳ 2840 - "pwsh.exe" -e
RwBIAHQALQBXAG0AaQBPAG!AagBiAGMAdAAgAfCaaQBuADMAMgBfAFMAaAbhAGQAbwB3AGMAbwBwAHkA|AB8ACAARgBvAH|ARQBhAGMAaAA|AE8AYgBqAGUAYwB0ACAAewAkAF8ALgBEAGUAbAB|
↳ 2720 - %CONHOST% "190687281-11520344052792205132330400-78403550827435588914694917418355785
↳ 2744 - %windir%\system32\wbem\unsecapp.exe -Embedding
↳ 2256 - %windir%\System32\svchost.exe -k WerSvcGroup

```

Posteriormente, insertaremos la muestra en la plataforma Any Run y observaremos la ejecución que se produce en el sandbox de 60 segundos que nos proporciona el registro estándar en la página.

Una vez obtenida una ligera idea de la forma en la que actual el malware, podemos empezar con el análisis estático de la muestra.

Utilizaremos la herramienta HxD, que permite abrir e identificar elementos de archivos en binario. Los elementos mas importantes de este proceso son:

Magic Number: (4D 5A) MZ

Texto: "This program cannot be run in DOS mode"

PE Header: PE

Los datos que proporcionan estos tres elementos, nos permiten decir que se trata de un archivo ejecutable.

Para obtener los algoritmos de codificación utilizados para encapsular el archivo, es decir, las funciones o técnicas utilizadas para obtener el contenido de un fichero con únicamente una secuencia de caracteres, utilizaremos la herramienta “HashMyFiles”

Además de facilitarnos la información anteriormente citada, nos ofrece datos como cuando se creó el malware, ruta en la que se encuentra, tamaño del archivo...

```
=====
Filename      : ransomware_revil
MD5          : b86ad4241b01376b3924a380f6f4c934
SHA1         : 10682d08a18715a79ee23b58fdb6e6a44c4e28c61
CRC32        : 44767a73
SHA-256       : 14c8e3f1f23d16c2c9a4272cd05d00461d27b372cc5f588b4bbfc6102bbbed708
SHA-512       : 54fd19cfc37255e7df3456d1a298958522f58e5eee6ca916c19542921fe3ba4e7a431a35e0e1edbfc37c5651d392e7c3c54eb408754c0488021b16fdf92c9
SHA-384       : 21c58518093d26c4946f7daee15c35991b103d7d97ea7a19d48b753b67ce0100e1c48971657f42453c9bd4b67ee0f6958
Full Path    : C:\Users\IEUser\Downloads\ransomware_revil\ransomware_revil
Modified Time : 5/22/2022 2:53:40 AM
Created Time  : 5/22/2022 2:54:01 AM
Entry Modified Time: 5/22/2022 2:54:01 AM
File Size     : 119,296
File Version  :
Product Version:
Identical     :
Extension     :
File Attributes: A
=====
```

El análisis de cabeceras resulta ser un proceso útil y de gran importancia en el análisis estático de malware, ya que por un lado proporciona información general y por otra informa sobre las DLLs y funciones utilizadas.

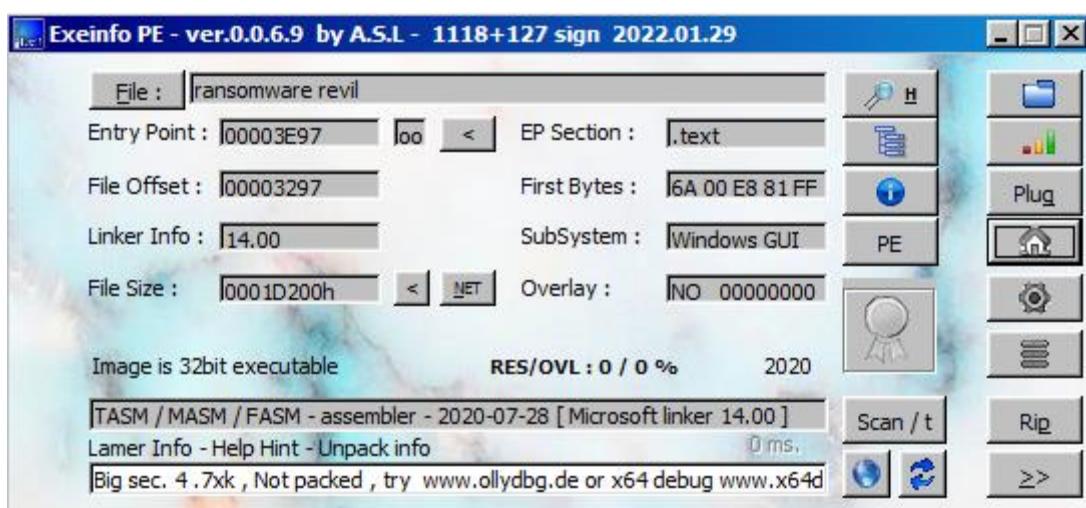
pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0005	Number of Sections	
000000F0	5F207655	Time Date Stamp	2020/07/28 Tue 19:02:45 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	0102	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE

The screenshot shows two instances of the PEView application. The left pane displays the file structure of 'ransomware revil' with various sections like IMAGE_DOS_HEADER, IMAGE_NT_HEADERS, and sections for text, data, and imports. The right pane shows tables of imported functions from DLLs like KERNEL32.dll and USER32.dll.

pFile	Data	Description	Value
0000B600	0000FBE8	Hint/Name RVA	060B IstrlenW
0000B604	0000FBF4	Hint/Name RVA	04EF SetErrorMode
0000B608	0000FC04	Hint/Name RVA	0596 VerSetConditionMask
0000B60C	0000FC1A	Hint/Name RVA	007F CloseHandle
0000B610	0000FC28	Hint/Name RVA	022C GetExitCodeProcess
0000B614	0000FC3E	Hint/Name RVA	059A VerifyVersionInfoW
0000B618	00000000	End of Imports	KERNEL32.dll
0000B61C	0000FC62	Hint/Name RVA	024D MessageBoxW
0000B620	00000000	End of Imports	USER32.dll

pFile	Data	Description	Value
0000E188	0000FBC4	Import Name Table RVA	
0000E18C	00000000	Time Date Stamp	
0000E190	00000000	Forwarder Chain	
0000E194	0000FC54	Name RVA	KERNEL32.dll
0000E198	0000D000	Import Address Table RVA	
0000E19C	0000FBE0	Import Name Table RVA	
0000E1A0	00000000	Time Date Stamp	
0000E1A4	00000000	Forwarder Chain	
0000E1A8	0000FC70	Name RVA	USER32.dll
0000E1AC	0000D01C	Import Address Table RVA	
0000E1B0	00000000		
0000E1B4	00000000		
0000E1B8	00000000		
0000E1BC	00000000		
0000E1C0	00000000		

La herramienta Exeinfo PE nos proporciona información del PE Header. Se trata de un encapsulador de información que administra el código del archivo que le envuelve, nos proporciona elementos de gran utilidad como puede ser el tipo de fichero, en el entorno que está desarrollado y “Lamer Info”, que nos indica si se encuentra empaquetado.



La identificación de strings nos permite distinguir elementos como puede ser calcular hash, detectar direcciones IP o URLs, recopilar metadatos, strings...

Para completar el análisis estático del malware, utilizaremos una herramienta anti-ransomware, la cual nos permite saber si existe algún método para recuperar los archivos que se encuentran encriptados y eliminar el software malicioso del sistema.

MUESTRA 2:

58 de 69 motores de búsqueda antivirus

Microsoft: "Ransom:Win32/Revil.B"

GData: "DeepScan:Generic.Ransom.AmnesiaE.04123F8A"

Basic Properties ⓘ

MD5	f0c97dcb65a030a214f6dd33cf4a8566
SHA-1	b23175fa1d3989baa2e3d8b5c7192554c24abf18
SHA-256	ed49b23df7defab3df933c778183b12c019ab253330090f214f4bb5c2f89bcfc
Vhash	115056657d7d556bz3!z
Authentihash	a727ff1be32a59255cffea21dcbb3da972451403aa427e79a5d9cae996ed6a52
Imphash	c4c29c7e6a6897be412c7fedfcc8fe4
Rich PE header hash	b25cffef5d8f5190aa58ab8fad74e8066
SSDEEP	3072:AZPM0OGdUKV10OTed7/kBazzFbULOHoiPyH53ZV6:AZPMnGZVyO6F/M4qyPU53Z
TLSH	T142F3E16FAE52C1F1E4C342F2132F2F275E7FBD30445228AAD3224D8D6B16455A22A75B
File type	Win32 DLL
Magic	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
TrID	Win32 Dynamic Link Library (generic) (29.6%)
TrID	Win16 NE executable (generic) (22.7%)
TrID	Win32 Executable (generic) (20.3%)
TrID	OS/2 Executable (generic) (9.1%)
TrID	Generic Win/DOS Executable (9%)
File size	164.00 KB (167936 bytes)

History ⓘ

Creation Time	2019-07-08 14:33:00 UTC
First Submission	2019-08-06 23:15:37 UTC
Last Submission	2019-08-06 23:15:37 UTC
Last Analysis	2021-05-26 15:20:29 UTC

Registry Actions ①

Registry Keys Set

- + HKLM\SOFTWARE\Wow6432Node\QtProject\OrganizationDefaults\sxsP
 - + HKLM\SOFTWARE\Wow6432Node\QtProject\OrganizationDefaults\Xu7Nnkd
 - + HKLM\SOFTWARE\Wow6432Node\QtProject\OrganizationDefaults\BDDC8
 - + HKLM\SOFTWARE\Wow6432Node\QtProject\OrganizationDefaults\sMMnxpgk
 - + HKLM\SOFTWARE\Wow6432Node\QtProject\OrganizationDefaults\pvg
 - + HKLM\SOFTWARE\Wow6432Node\QtProject\OrganizationDefaults\f7gVD7
 - + HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{853201e6-2d75-11ea-a138-806e6f6e6963}DeleteProcess (Leave)
 - + HKLM\SYSTEM\ControlSet001\Services\VSS\Diag\VolSnap\Volume{853201e6-2d75-11ea-a138-806e6f6e6963}DeleteProcess (Enter)
 - + HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
 - + HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
- ▼

Registry Keys Deleted

HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\First Counter
HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Last Counter
HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\First Help
HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Last Help
HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Object List

Process And Service Actions ①

Shell Commands

"%ComSpec%" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignorefailures
vssadmin.exe Delete Shadows /All /Quiet

Processes Terminated

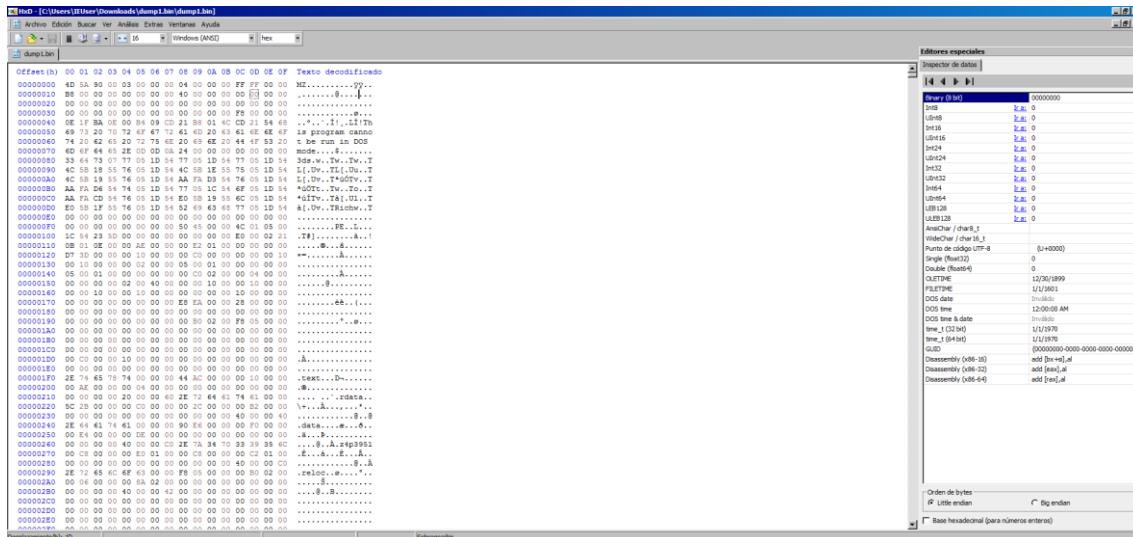
%CONHOST% "2018137818-13544598551424651421910876556-336004356-661671151-1041938976-1116811662
%windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
wmiadap.exe /F /T /R
%windir%\system32\vsrssvc.exe
"%ComSpec%" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignorefailures
vssadmin.exe Delete Shadows /All /Quiet

Processes Tree

↳ 2828 - %CONHOST% "2018137818-13544598551424651421910876556-336004356-661671151-1041938976-1116811662
↳ 2956 - %windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
↳ 2088 - %windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
↳ 1420 - wmiadap.exe /F /T /R
↳ 3036 - %windir%\system32\NOTEPAD.EXE C:\tmp\p6tb0-readme.txt
↳ 2760 - %windir%\system32\wbem\unsecapp.exe -Embedding
↳ 1052 - %windir%\system32\wbem\wmiprvse.exe
↳ 2884 - %windir%\system32\vsrssvc.exe
↳ 2628 - %Sandbox_DLL_LOADER_X86% %SAMPLEPATH% %WORKDIR% 483
↳ 2780 - "%ComSpec%" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignorefailures
↳ 2844 - vssadmin.exe Delete Shadows /All /Quiet

^

```
=====
Filename : dump1.bin
MD5 : f0c97dcbe65a030a214f6dd33cf4a8566
SHA1 : b23175fa1d3989baa2e3dbb5c7192554c24abf18
CRC32 : 01eb94c
SHA-256 : ed49b23df7defab3df933c778183b12c019ab253330090f214f4bb5c2f89bc
SHA-512 : 24d7963631784357c4615ef94cecd9aaaf47bc3896d6c897da24d55bda0713da4957f82ead8764f82cf6af1b5d9c8d3ad015fe3354694e9c331abbb67485
SHA-384 : fb81c6bc5b73f9c12bab71f4b4bd7826d4a9c3b9f3a331b4910a6fb2cfea9022f658f01110ac48473bbe8f01a8c02ea
Full Path : C:\Users\IEUser\Downloads\dump1.bin\dump1.bin
Modified Time : 5/21/2022 4:17:02 PM
Created Time : 5/21/2022 4:21:24 PM
Entry Modified Time: 5/21/2022 4:21:24 PM
File Size : 167,936
File Version :
Product Version :
Identical :
Extension : bin
File Attributes : A
=====
```



PView - C:\Users\IEUser\Downloads\REvil2\dump1.bin

pFile	Data	Description	Value
000000FC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000FE	0005	Number of Sections	
00000100	5D23541C	Time Date Stamp	2019/07/08 Mon 14:33:00 UTC
00000104	00000000	Pointer to Symbol Table	
00000108	00000000	Number of Symbols	
0000010C	00E0	Size of Optional Header	
0000010E	2102	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE
	2000		IMAGE_FILE_DLL

PView - C:\Users\IEUser\Downloads\dump1.bin\dump1.bin

pFile	Data	Description	Value
0000B200	0000EB20	Hint/Name RVA	007F CloseHandle
0000B204	0000EB2E	Hint/Name RVA	04EF SetErrorMode
0000B208	0000EB3E	Hint/Name RVA	00E8 CreateThread
0000B20C	00000000	End of Imports	KERNEL32.dll

PEView - C:\Users\IEUser\Downloads\dump1.bin\dump1.bin

pFile	Data	Description	Value
0000DCE8	0000EB10	Import Name Table RVA	
0000DCEC	00000000	Time Date Stamp	
0000DCF0	00000000	Forwarder Chain	
0000DCF4	0000EB4E	Name RVA	KERNEL32.dll
0000DCF8	0000C000	Import Address Table RVA	
0000DCF0	00000000		
0000DD00	00000000		
0000DD04	00000000		
0000DD08	00000000		
0000DD0C	00000000		

Exeinfo PE - ver.0.0.6.9 by A.S.L - 1118+127 sign 2022.01.29

File : dump1.bin

Entry Point : 00003DD7 EP Section : .text

File Offset : 000031D7 First Bytes : 55 8B EC 83 6D

Linker Info : 14.00 SubSystem : Windows GUI

File Size : 00029000h Overlay : NO 00000000

DLL 32 bit- Library image RES/OVL : 0 / 0 % 2019

*** Unknown DLL 55 8B EC x Std Compiler section , MS C++ Visual Studio

Lamer Info - Help Hint - Unpack info 0ms,

Big sec. 3.data , Click - [Scan / t] Button or try Detector - DIE v3.x http://

Scan / t Rip >>

MUESTRA 3:

53 de 69 motores de búsqueda antivirus

Microsoft: "Ransom:Win32/Revil.A"

GData: "Gen:Variant.Ransom.Sodinokibi.B"

Basic Properties ⓘ

MD5	21d01fa87dfcaf971ff7b63a1a6fda94
SHA-1	f3caa9831fc715af4f47cd98803549902dff30a
SHA-256	ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83
Vhash	015046657d156019zc9z4tz
Authentihash	98aba482d8013656c1d60ff7d90326e69b1d64814834bcdd756625a92958f160
Imphash	eb68d746c420bd3a83ab3b0473d926ae
Rich PE header hash	d9e1b5346af5c0187ed8782fd7f10bdc
SSDEEP	1536:ASOOoRSNI/XT9yYSvVKJJgpBy7bICs4AUisz8djOK:WPaKJJctOqjOK
TLSH	T1A7D3AF77B96142B3CA8781F2237B3F1B9AFEBE300021A5B7C36185841D655D5A72B227
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Dynamic Link Library (generic) (29.6%)
TrID	Win16 NE executable (generic) (22.7%)
TrID	Win32 Executable (generic) (20.3%)
TrID	OS/2 Executable (generic) (9.1%)
TrID	Generic Win/DOS Executable (9%)
File size	137.50 KB (140800 bytes)

History ⓘ

Creation Time	2021-09-04 14:16:49 UTC
First Submission	2021-09-09 08:18:10 UTC
Last Submission	2022-03-22 10:19:20 UTC
Last Analysis	2022-03-23 10:35:41 UTC

Registry Actions ⓘ

Registry Keys Set

- + HKLM\SOFTWARE\Wow6432Node\XMT0qpW\5XB29
 - + HKLM\SOFTWARE\Wow6432Node\XMT0qpW\JgC
 - + HKLM\SOFTWARE\Wow6432Node\XMT0qpW\CsUQ
 - + HKLM\SOFTWARE\Wow6432Node\XMT0qpW\6mna6tT
 - + HKLM\SOFTWARE\Wow6432Node\XMT0qpW\OKDigiPr
 - + HKLM\Software\Microsoft\WBEM\WDM\DRIDGE%\windir%\system32\DRIVERS\en-US\intelppm.sys.mui[PROCESSORWMI]
 - + HKLM\Software\Microsoft\WBEM\WDM\DRIDGE%\windir%\system32\DRIVERS\HDAudBus.sys[HDAudioMofName]
 - + HKLM\Software\Microsoft\WBEM\WDM\DRIDGE%\windir%\System32\Drivers\en-US\portcls.SYS.mui[PortclsMof]
 - + HKLM\Software\Microsoft\WBEM\WDM\DRIDGE%\windir%\system32\advapi32.dll[MofResourceName]
 - + HKLM\Software\Microsoft\WBEM\WDM\DRIDGE%\windir%\system32\en-US\advapi32.dll.mui[MofResourceName]
- ▼

Registry Keys Deleted

HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\First Counter
HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Last Counter
HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\First Help
HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Last Help
HKLM\SYSTEM\ControlSet001\Services\WmiApRpl\Performance\Object List

Process And Service Actions ①

Processes Terminated

```
%windir%\System32\svchost.exe -k WerSvcGroup  
wmiadap.exe /F /T /R  
%windir%\System32\svchost.exe -k swprv  
%windir%\system32\vssvc.exe
```

Processes Tree

```
└─ 2252 - %windir%\System32\svchost.exe -k WerSvcGroup  
└─ 1160 - wmiadap.exe /F /T /R  
└─ 2368 - %windir%\system32\NOTEPAD.EXE C:\tmp\alkx6-readme.txt  
└─ 2864 - %windir%\System32\svchost.exe -k swprv  
└─ 2764 - %windir%\system32\wbem\unsecapp.exe -Embedding  
└─ 1712 - %windir%\system32\wbem\wmiprvse.exe  
└─ 2792 - %windir%\system32\vssvc.exe  
└─ 2624 - %SAMPLEPATH%
```

```
=====  
Filename : ab0aa003d7238940cbf7393677f968c4a252516de7f0699cd4654abd2e7ae83.bin  
File Size : 140,800  
File Version :  
Product Version :  
Identical :  
Extension : bin  
File Attributes : A  
=====
```

SHA1 : f4c01b0831fc715afaf47cd98803549902dfffe30a
CRC32 : 0b26aae3
SHA-256 : ab0aa003d7238940cbf7393677f968c4a252516de7f0699cd4654abd2e7ae83
SHA-512 : f89997f8c31d77029f10872575h24337f9980bebfbe169967cae72a5d50ce119d273fae00690ef2e2bf345901d723034992f53dd3e5b9df5cbe9be2e67fa
SHA-384 : 3b3dee222c3154ad765369369508f0f739e2803a253a2e570bb82b743f3e4039e61f7calbded8bf4abfd65b713f34ae
Full Path : C:\Users\IEUser\Downloads\ab0aa003d7238940cbf7393677f968c4a252516de7f0699cd4654abd2e7ae83.bin
Modified Time : 5/21/2022 4:20:41 PM
Created Time : 5/22/2022 2:35:53 AM
Entry Modified Time: 5/22/2022 2:35:53 AM
=====

Hex - [C:\Users\IEUser\Downloads\ab0aa003d7238940cbf7393677f968c4a252516de7f0699cd4654abd2e7ae83.bin]

Archivo Edición Buscar Ver Análisis Extras Ayuda

Windows hex

Detalles(b) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Texto descodificado

00000000 F0 CA 90 00 00 00 00 00 04 00 00 FF FF 00 009.....
 00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
 00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000040 0E 1F 3A 08 00 00 04 00 C3 21 80 01 4C CD 21 54 48 L...L1Th
 00000050 69 73 20 70 72 67 72 61 60 20 61 64 4F 4F is program canno
 00000060 69 73 20 70 72 67 72 61 60 20 61 64 4F 4F is program canno
 00000070 4D 4F 64 45 2F 00 00 00 24 00 00 00 00 00 00 00 mode...
 00000080 51 00 88 00 15 61 E6 20 15 61 E6 D1 15 61 E6 03 Q_`E,aed,aed,aed
 00000090 61 64 45 2F 00 00 00 00 00 00 00 00 00 00 00 00
 000000A0 B6 3F E2 02 14 61 E6 C0 20 14 61 E6 03 740,aed(2) aed
 000000B0 C8 9E 2D 03 12 61 E6 20 15 61 E7 03 30 61 E6 03 E8_0,aed,aed0,aed
 000000C0 A0 3F E4 04 14 61 E6 20 52 60 63 61 E6 03 740,aed,aed
 000000D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00PE_L...
 00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000110 0B 01 0E 00 00 00 00 00 00 00 00 00 00 00 00 00v.....
 00000120 0B 1F 0E 00 00 00 00 00 00 00 00 00 00 00 00 00B...
 00000130 00 00 00 00 00 02 40 00 00 10 00 00 00 00 00 00P.....
 00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000001B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000001C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00B_P.....
 000001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00A.....
 00000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 009_8.....
 00000240 ZE 44 41 74 61 00 00 B0 01 00 00 01 00 00 00 00data...<.....
 00000250 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00000260 00 00 00 00 00 00 C3 2E 72 65 67 63 00 008_A,zeloo..
 00000270 BC 04 00 00 00 00 00 02 00 00 00 00 00 00 12 52 00
 00000280 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00B.....
 00000290 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000002A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000002B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000002C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 000002D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Descomprimir: 0 Subscribirse

C:\PView - C:\Users\IEUser\Downloads\REvil3\ab0aa003d7238940cbf7393677f968c4a252516de7f0699cd4654abd2e7ae83.bin

File View Go Help

	pFile	Data	Description	Value
ab0aa003d7238940cbf7393677f968c4a252516de7f0699cd4654abd2e7ae83.bin	000000FC	014C	Machine	IMAGE_FILE_MACHINE_I386
	000000FE	0004	Number of Sections	
	00000100	61337FD1	Time Date Stamp	2021/09/04 Sat 14:16:49 UTC
	00000104	00000000	Pointer to Symbol Table	
	00000108	00000000	Number of Symbols	
	0000010C	00E0	Size of Optional Header	
	0000010E	0102	Characteristics	
		0002		IMAGE_FILE_EXECUTABLE_IMAGE
		0100		IMAGE_FILE_32BIT_MACHINE

C:\PView - C:\Users\IEUser\Downloads\ab0aa003d7238940cbf7393677f968c4a252516de7f0699cd4654abd2e7ae83.br

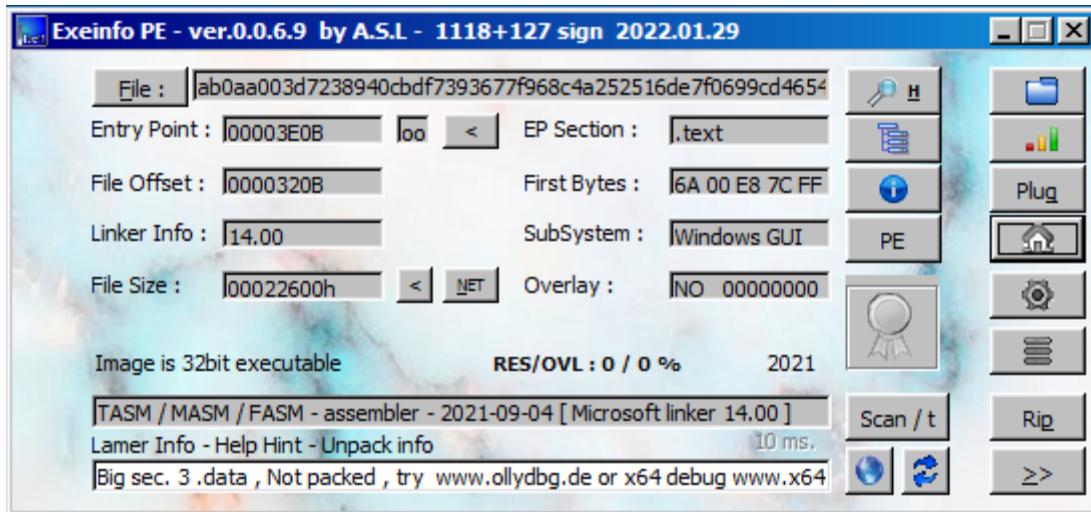
File View Go Help

	pFile	Data	Description	Value
ab0aa003d7238940cbf7393677f968c4a252516de7f0699cd4654abd2e7ae83.br	00000000	000000F2	HimName RVA	02EA_SetThreadToken
	00000004	00000000	End of Imports	ADVAPI32.dll
IMAGE_DOS_HEADER	00000000	00000000	Time Date Stamp	
MS-DOS Program Headers	00000000	00000000	Forwarder Chain	
IMAGE_NT_HEADERS	00000000	00000000	Verifier Chain	
Signature	00000000	00000000	Import Address Table RVA	KERNEL32.dll
IMAGE_FILE_HEADER	00000000	00000000	Import Address Table RVA	
IMAGE_OPTIONAL_HEADER	00000000	00000000	Time Date Stamp	
IMAGE_SECTION_HEADER.text	00000000	00000000	Forwarder Chain	
IMAGE_SECTION_HEADER.rdata	00000000	00000000	Verifier Chain	
IMAGE_SECTION_HEADER.data	00000000	00000000	Import Address Table RVA	ADVAPI32.dll
IMAGE_SECTION_HEADER.reloc	00000000	00000000	Forwarder Chain	
SECTION .text	00000000	00000000	Verifier Chain	
SECTION .rdata	00000000	00000000	Import Address Table RVA	OLEAUT32.dll
SECTION .data	00000000	00000000	Verifier Chain	
SECTION .reloc	00000000	00000000	Verifier Chain	

C:\PView - C:\Users\IEUser\Downloads\ab0aa003d7238940cbf7393677f968c4a252516de7f0699cd4654abd2e7ae83.br

File View Go Help

	pFile	Data	Description	Value
ab0aa003d7238940cbf7393677f968c4a252516de7f0699cd4654abd2e7ae83.br	00000000	000000F2	HimName RVA	02EA_SetThreadToken
	00000004	00000000	End of Imports	ADVAPI32.dll
IMAGE_DOS_HEADER	00000000	00000000	Time Date Stamp	
MS-DOS Program Headers	00000000	00000000	Forwarder Chain	
IMAGE_NT_HEADERS	00000000	00000000	Verifier Chain	
Signature	00000000	00000000	Import Address Table RVA	KERNEL32.dll
IMAGE_FILE_HEADER	00000000	00000000	Import Address Table RVA	
IMAGE_OPTIONAL_HEADER	00000000	00000000	Time Date Stamp	
IMAGE_SECTION_HEADER.text	00000000	00000000	Forwarder Chain	
IMAGE_SECTION_HEADER.rdata	00000000	00000000	Verifier Chain	
IMAGE_SECTION_HEADER.data	00000000	00000000	Import Address Table RVA	ADVAPI32.dll
IMAGE_SECTION_HEADER.reloc	00000000	00000000	Forwarder Chain	
SECTION .text	00000000	00000000	Verifier Chain	
SECTION .rdata	00000000	00000000	Import Address Table RVA	OLEAUT32.dll
SECTION .data	00000000	00000000	Verifier Chain	
SECTION .reloc	00000000	00000000	Verifier Chain	



MUESTRA 4:

62 de 70 motores de búsqueda antivirus

Microsoft: "Ransom:Win32/Revil.A"

GData: "Win32.Trojan-Ransom.Revil.A"

Basic Properties ⓘ

MD5	ff0e2ce0af118bae62969a5e897b59b2
SHA-1	5bc65c73cae94509905c6a4ba657a61360bb96f2
SHA-256	52612bceee07152f2e2e6699b3c085149e11979f34fe248bda14e03a0d950e85
Vhash	015056657d7d556bz99z4bz1fz
Authentihash	11702d0d2a96073bef35b1af75c42c00e9f779bd12b2f504be8c9a35981a3243
Imphash	031931d2f2d921a9d906454d42f21be0
Rich PE header hash	f5ce87f5b427852598305c9155ba3de2
SSDEEP	1536:J8A4krBJLarHZZd/M4Pl8iwplAXpzK88ICS4Aer9Ds5kYk/gm729Tq2Kke:+/LPrIAZZEqlgQ29Tq2Kke
TLSH	T197C3D023EDA242F2D94381F7033F2F17D6BEFD721D10586AD76049489A65182EA2B763
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Dynamic Link Library (generic) (29.6%)
TrID	Win16 NE executable (generic) (22.7%)
TrID	Win32 Executable (generic) (20.3%)
TrID	OS/2 Executable (generic) (9.1%)
TrID	Generic Win/DOS Executable (9%)
File size	120.00 KB (122880 bytes)

History ⓘ

Creation Time	2021-03-09 18:09:46 UTC
First Submission	2021-03-17 14:55:14 UTC
Last Submission	2021-03-17 14:55:14 UTC
Last Analysis	2022-02-15 15:15:44 UTC

Process And Service Actions

Shell Commands

```
%SAMPLEPATH%
```

Processes Terminated

```
%windir%\System32\svchost.exe -k WerSvcGroup
%windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
%windir%\system32\svssvc.exe
```

Processes Tree

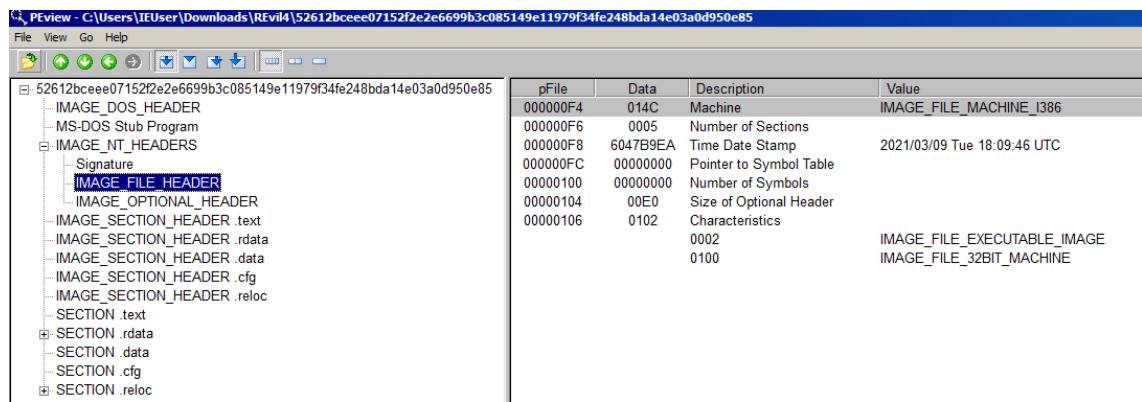
- ↳ 2320 - %windir%\System32\svchost.exe -k WerSvcGroup
- ↳ 1840 - %windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
- ↳ 2868 - %windir%\system32\svssvc.exe
- ↳ 2692 - %SAMPLEPATH%

```
=====
Filename : 52612bcc0ee07152fe2e6699b3c085149e11979f34fe248bda14e03a0d950e85
MD5 : ff0e2ce0af118aae2969a5e897595b2
SHA1 : 5bc65c73cae94599905c6aa4ba657ae1360bb96f2
CRC32 : 35119793
SHA-256 : 52612bcc0ee07152fe2e6699b3c085149e11979f34fe248bda14e03a0d950e85
SHA-512 : f7f205bc47555b3567ff9901a43db1a597128041a0b3c1210ff3396bce0995d2e96b4b9bede21d319ac27ff0b924c0e13cf3b198076bc31406b8278d39a7a2c8e9
SHA-384 : a04788d34f8a9f36f758bfdf4d5cdff9097eda81b6ddfe454d2973f124bec1332e334ab198a3757b1443d92c1c6d2d
Full Path : C:\Users\IEUser\Downloads\52612bcc0ee07152fe2e6699b3c085149e11979f34fe248bda14e03a0d950e85
Modified Time : 5/21/2022 4:19:33 PM
Created Time : 5/22/2022 2:27:12 AM
Entry Modified Time: 5/22/2022 2:27:12 AM
File Size : 122,880
File Version :
Product Version :
Identical :
Extension : 
File Attributes : A
```

====

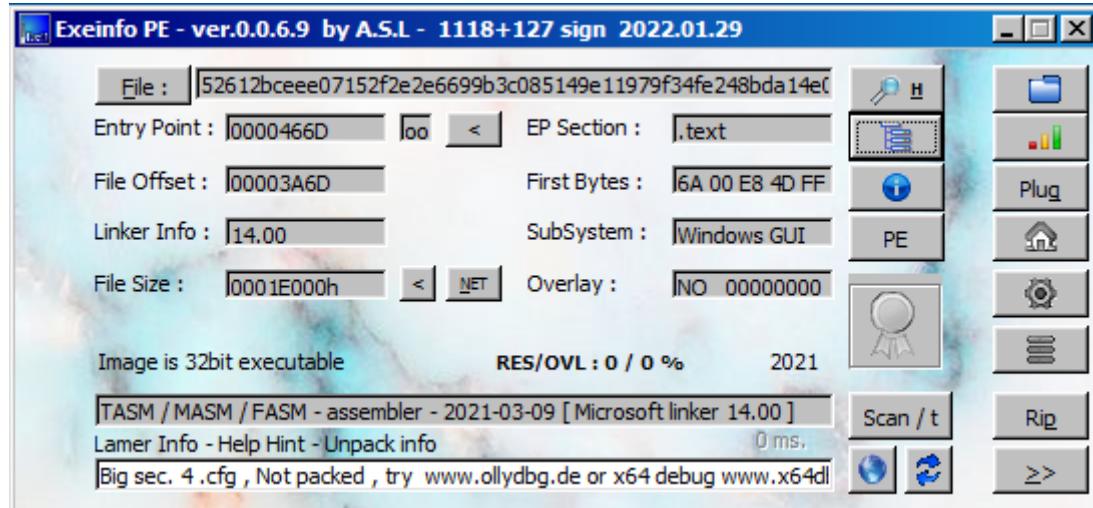
Editor especial	Inspector de datos
Hex	01001101
UInt8	77
UInt16	77
UInt16	23117
Int24	-7316915
UInt24	9400201
Int32	-2320292
UInt32	9400301
Int64	1289482189
Double (Float4)	1289482199
UInt128	77
ULInt128	77
AnsChar / Char 8,1	M
IndirectChar / char 8,1	
Punto de código UTF-8	M (1+00-E)
Singe (Float4)	1.328470263350E-38
Double (Float8)	0.000000000000000E+000
DWORD	12701399
FILETIME	1/1/0001 12:21:29 AM
DOS date	2/13/2022
DOS time	11:51:29 AM
DOS time & date	4/16/1980 11:38:26 AM
time, 1 (DWord)	4/20/1970 11:51:41 AM
time, 1 (Float4)	0.00002787718629 AM
GUID	{00000440-0003-0000-0000-000000000000}
Disassembly (x86-32)	dec hex
Disassembly (x86-32)	dec dec
Disassembly (x86-64)	rop r32

Opción de bytes: Little endian Big endian
Base hexadecimal (para números enteros)



PEView - C:\Users\IEUser\Downloads\52612bceee07152f2e2e6699b3c085149e11979f34fe248bda14e03a0d950e85			
File	View	Go	Help
File	Import Address Table	Import Name Table	Imports
Import Address Table			KERNEL32.dll
Import Name Table			OLEAUT32.dll
Imports			USER32.dll
Section .text			
Section .data			
Section .cfg			
Section .reloc			

PEView - C:\Users\IEUser\Downloads\52612bceee07152f2e2e6699b3c085149e11979f34fe248bda14e03a0d950e85			
File	View	Go	Help
File	Import Address Table	Import Name Table	Imports
Import Address Table			KERNEL32.dll
Import Name Table			OLEAUT32.dll
Imports			USER32.dll
Section .text			
Section .data			
Section .cfg			
Section .reloc			



MUESTRA 5:

58 de 71

Microsoft: "Trojan:Win32/Malgent.B"

GData: "Trojan.Brsecmon.1"

Basic Properties ⓘ

MD5	0bb803ea960f1f2c88f4e0cd808c196e
SHA-1	590053863146f758fcb7a876c02f5d4459aa6a43
SHA-256	a91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60
Authentihash	3c5d7a41dc538494d7f2d958ab9db819c46868ac5b1bbfb547cbae48192ac1e
Imphash	a71572da77751977cfaaa54c9d130359
SSDEEP	6144:viYY7HL6OXYYevtqsuJ40gxBekUNYkdOGINJcHC7KAU93Jobv:vdYjeOXX1IFTve53v
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (41%)
TrID	Win64 Executable (generic) (36.3%)
TrID	Win32 Dynamic Link Library (generic) (8.6%)
TrID	Win32 Executable (generic) (5.9%)
TrID	OS/2 Executable (generic) (2.6%)
File size	319.50 KB (327168 bytes)

History ⓘ

Creation Time	2018-04-03 18:09:32 UTC
First Submission	2019-04-28 21:57:35 UTC
Last Submission	2019-04-30 23:05:16 UTC
Last Analysis	2020-02-02 06:25:11 UTC

Network Communication ⓘ

HTTP Requests

- + <http://repository.certum.pl/nazwassl2sha2.cer>

DNS Resolutions

- + advance-refle.com
- + premiumweb.com.ua
- + neolaiamedispa.com
- + qandmmusiccenter.com
- + bychowo.pl
- + babysitting-hk.helpergo.co
- + ronielyn.com
- + powershell.su
- + kryptos72.com
- + memphishealthandwellness.com

▼

IP Traffic

198.71.233.87:443 (TCP)

Registry Actions ⓘ

Registry Keys Set

- + HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEM\CERTIFICATES\AUTHROOT\CERTIFICATES\4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5
- + HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEM\CERTIFICATES\AUTHROOT\CERTIFICATES\07E032E02B72C3F192F0628A2593A19A70F069E
- + HKUIS-1-5-21-1143565567-962705147-4090495373-1003\SOFTWARE\CLASSES\LOCAL SETTINGS\IMUICACHE\052C64B7E
- + HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEM\CERTIFICATES\AUTHROOT\CERTIFICATES\47BEABC922EA80E78783462A79F45C254FDE68B
- + HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEM\CERTIFICATES\AUTHROOT\CERTIFICATES\8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436
- + HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEM\CERTIFICATES\AUTHROOT\CERTIFICATES\0563B8630D62D75ABC8AB1E4BDFB5A899B24D43
- + HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEM\CERTIFICATES\AUTHROOT\CERTIFICATES\3679CA35668772304D30A5FB873B0FA77BB70D54
- + HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEM\CERTIFICATES\ROOT\CERTIFICATES\CD4EEAE6000AC7F40C3802C171E30148030C072
- + HKUIS-1-5-21-1143565567-962705147-4090495373-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER
- + HKUIS-1-5-21-1143565567-962705147-4090495373-1003\SOFTWARE\MICROSOFT\SYSTEM\CERTIFICATES\CA\CERTIFICATES\9CE8E8879AB0CCB17A1FEEED83E720F3D925DF8

▼

Registry Keys Deleted

HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEM\CERTIFICATES\ROOT\CERTIFICATES
HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEM\CERTIFICATES\AUTHROOT\CERTIFICATES
HKUIS-1-5-21-1143565567-962705147-4090495373-1003\SOFTWARE\MICROSOFT\SYSTEM\CERTIFICATES\CA\CERTIFICATES

Process And Service Actions

Processes Created

```
C:\Users\Olivia\AppData\Local\Temp\OHQZtl7mTlgqf6.exe
C:\WINDOWS\SysWOW64\cmd.exe
C:\WINDOWS\SysWOW64\vssadmin.exe
C:\Users\Olivia\AppData\Local\Temp\lu51dsD72XvKONa3NlwSMm.exe
C:\Users\Lucas\AppData\Local\Temp\lment.exe
```

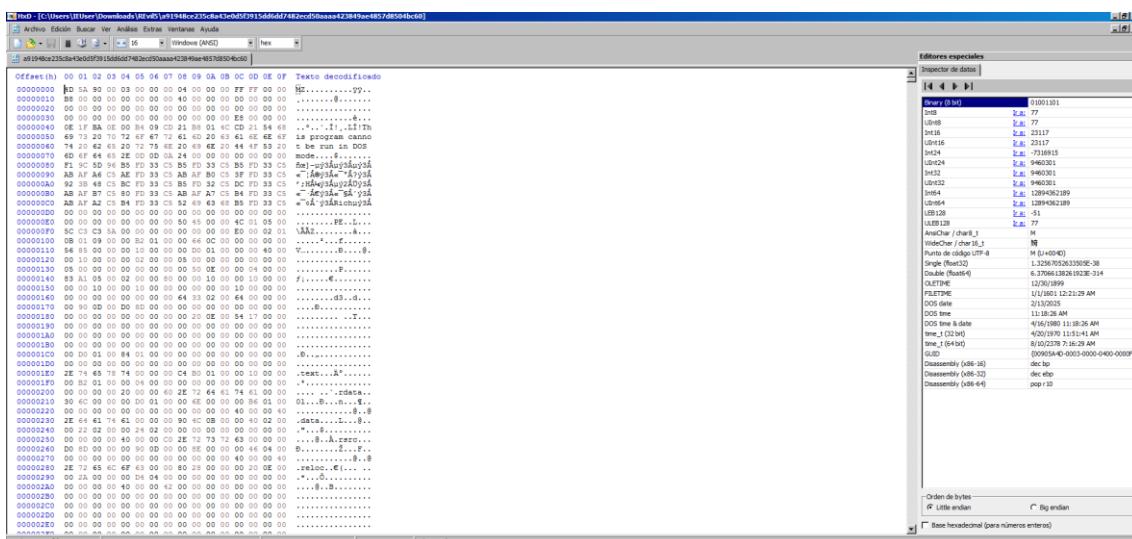
Shell Commands

```
C:\Users\Olivia\AppData\Local\Temp\OHQZtl7mTlgqf6.exe
C:\Windows\System32\cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures
vssadmin.exe Delete Shadows /All /Quiet
C:\Users\Olivia\AppData\Local\Temp\lu51dsD72XvKONa3NlwSMm.exe
C:\Users\Lucas\AppData\Local\Temp\lment.exe
```

Processes Tree

```
↳ 3080 - C:\Users\Olivia\AppData\Local\Temp\OHQZtl7mTlgqf6.exe
↳ 3912 - C:\WINDOWS\SysWOW64\cmd.exe
↳ 796 - C:\WINDOWS\SysWOW64\vssadmin.exe
↳ 3904 - C:\Users\Olivia\AppData\Local\Temp\lu51dsD72XvKONa3NlwSMm.exe
↳ 4788 - C:\WINDOWS\SysWOW64\cmd.exe
↳ 6868 - C:\WINDOWS\SysWOW64\vssadmin.exe
```

```
=====
Filename : a91948ce235c8a43e0d5f3915dd6d7482ecd50aaaa423849ae4857d8504bc60
MD5 : 0bb803ea960f1f2c88f4e0cd808c196e
SHA1 : 590053863146f758fc7ba876c02f5d4459aa6a43
CRC32 : e9e5590a
SHA-256 : a91948ce235c8a43e0d5f3915dd6d7482ecd50aaaa423849ae4857d8504bc60
SHA-512 : 460f68c551136dc519c3ffaaf18d8536c2914c2bfafa0e2d06926664fb3e493e5e1c2cd6d826d7637200289ff36b70330bbc0c91187ba8dffcc7569d9c9718
SHA-384 : 03d75de87157a4e37fea8e27afaa473e43e25b270ca65912db672f2e959e848c9db860966e9555b880206cc5018aeecc
Full Path : C:\Users\IEUser\Downloads\REvil5\91948ce235c8a43e0d5f3915dd6d7482ecd50aaaa423849ae4857d8504bc60
Modified Time : 5/23/2022 8:26:25 AM
Created Time : 5/23/2022 8:26:51 AM
Entry Modified Time: 5/23/2022 8:26:51 AM
File Size : 327,168
File Version :
Product Version :
Identical :
Extension :
File Attributes : A
=====
```



PEView - C:\Users\IEUser\Downloads\REvil5\91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60

File View Go Help

Tree View

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0005	Number of Sections	
000000F0	5AC3C35C	Time Date Stamp	2018/04/03 Tue 18:09:32 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	0102	Characteristics	
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE

Section Tree

- a91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60
 - IMAGE_DOS_HEADER
 - MS-DOS Stub Program
 - IMAGE_NT_HEADERS
 - Signature
 - IMAGE_FILE_HEADER**
 - IMAGE_OPTIONAL_HEADER
 - IMAGE_SECTION_HEADER.text
 - IMAGE_SECTION_HEADER.rdata
 - IMAGE_SECTION_HEADER.data
 - IMAGE_SECTION_HEADER.rsrc
 - IMAGE_SECTION_HEADER.reloc
 - SECTION.text
 - SECTION.rdata
 - SECTION.data
 - SECTION.rsrc
 - SECTION.reloc

PEView - C:\Users\IEUser\Downloads\REvil5\91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60

File View Go Help

Tree View

pFile	Data	Description	Value
00019500	000236DA	Hint/Name RVA	0CFE RegRestoreKeyW
00019501	00000000	Hint/Name RVA	0000000000000000
00019508	00000000	End of Imports	ADVAPI32.dll
0001950C	0002358A	Hint/Name RVA	023F GetStringTypeExW
00019510	0002359E	Hint/Name RVA	0220 GetProcAddress
00019511	000235A4	Hint/Name RVA	0200 GetProcAddressByNameW
00019519	000235C4	Hint/Name RVA	0325 OpenFileMappingW
0001951C	000235D0	Hint/Name RVA	01F4 GetModuleFileNameA
00019520	000235EE	Hint/Name RVA	02F1 LoadLibraryA
00019521	000235F0	Hint/Name RVA	02F5 LocalAlloc
00019523	0002360C	Hint/Name RVA	0100 LocalFree
0001952C	00023618	Hint/Name RVA	0488 WriteConsoleOutputAttribute
00019530	0002367E	Hint/Name RVA	02A2 HeapLock
00019531	000236A4	Hint/Name RVA	0495 WaitForSingleObjectExW
00019532	000236B0	Hint/Name RVA	0494 CreateConfigDialogW
0001953C	00023676	Hint/Name RVA	0183 GetConsoleCP
00019540	00023636	Hint/Name RVA	04B6 IsInfinite
00019544	00023234	Hint/Name RVA	0368 ReadFile
00019545	00023638	Hint/Name RVA	0200 SetProcessHeap
0001954C	00023562	Hint/Name RVA	021C GetPivotProfileStringA
00019550	00023636	Hint/Name RVA	0078 CreateFileW
00019554	0002354C	Hint/Name RVA	0487 GetProcAddressOutputA
00019555	00023548	Hint/Name RVA	0488 GetProcAddressOutputW
0001955C	000235F2	Hint/Name RVA	048C WriteConsoleW
00019560	00023728	Hint/Name RVA	02C0 InterlockedIncrement
00019564	00023740	Hint/Name RVA	02B0 InterlockedDecrement
00019565	00023744	Hint/Name RVA	0421 RtlEnterCriticalSection
00019566	00023747	Hint/Name RVA	0294 InitializeCriticalSection
00019570	0002377C	Hint/Name RVA	00B6 DeleteCriticalSection
00019574	00023770	Hint/Name RVA	0005 EnterCriticalSection
00019575	00023774	Hint/Name RVA	02B7 LeaveCriticalSection
0001957C	000237C4	Hint/Name RVA	0392 RtlLeave
00019580	000237E0	Hint/Name RVA	0420 TerminateProcess
00019584	000237E4	Hint/Name RVA	01A9 GetCurrentProcess
00019585	000237E8	Hint/Name RVA	0001 CreateThreadExW
0001958C	00023814	Hint/Name RVA	0415 SetUnhandledExceptionFilter
00019590	00023832	Hint/Name RVA	02D1 IsDebuggerPresent
00019594	00023846	Hint/Name RVA	0354 RaiseException
00019595	00023848	Hint/Name RVA	0355 RtlRaiseError
0001959C	00023868	Hint/Name RVA	02A1 HeadFile
000195A0	00023874	Hint/Name RVA	023A GetStartupInfoW
000195A4	00023895	Hint/Name RVA	02E1 LCMMapStringA
000195AB	00023896	Hint/Name RVA	0474 WideCharToMultiByte
000195AC	000238AC	Hint/Name RVA	031A MultiByteToWideChar

View IMPORT Address Table

PEView - C:\Users\IEUser\Downloads\REvil5\91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60

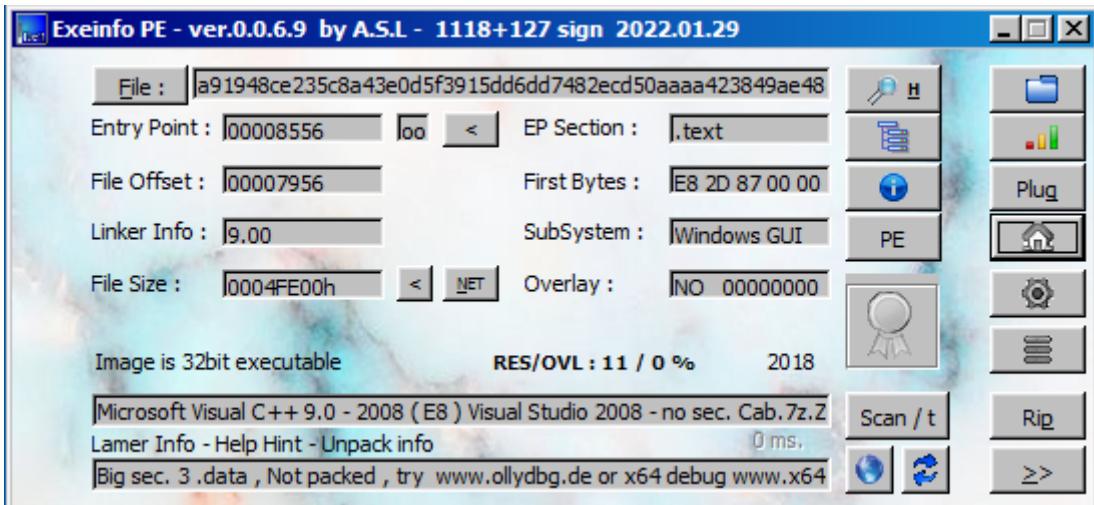
File View Go Help

Tree View

pFile	Data	Description	Value
00021964	000233D4	Import Name Table RVA	
00021968	00000000	Time Date Stamp	
0002196C	00000000	Forwarder Chain	
00021970	00023692	Name RVA	KERNEL32.dll
00021974	0001D000	Import Address Table RVA	
00021978	0002353C	Import Name Table RVA	
0002197C	00000000	Time Date Stamp	
00021980	00000000	Forwarder Chain	
00021984	000236CE	Name RVA	USER32.dll
00021988	0001D174	Import Address Table RVA	
0002198C	000233C8	Import Name Table RVA	
00021990	00000000	Time Date Stamp	
00021994	00000000	Forwarder Chain	
00021998	000236FE	Name RVA	ADVAPI32.dll
0002199C	0001D000	Import Address Table RVA	
000219A0	00023534	Import Name Table RVA	
000219A4	00000000	Time Date Stamp	
000219A8	00000000	Forwarder Chain	
000219AC	0002371C	Name RVA	MSIMG32.dll
000219B0	0001D16C	Import Address Table RVA	
000219B4	00000000		
000219B8	00000000		
000219BC	00000000		
000219C0	00000000		
000219C4	00000000		

Section Tree

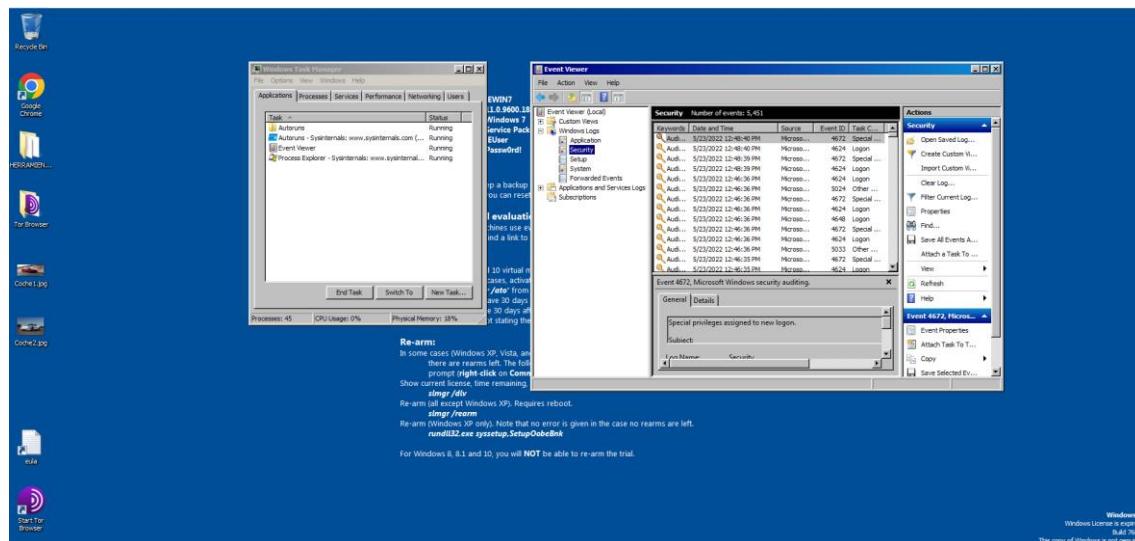
- a91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60
 - IMAGE_DOS_HEADER
 - MS-DOS Stub Program
 - IMAGE_NT_HEADERS
 - Signature
 - IMAGE_FILE_HEADER**
 - IMAGE_OPTIONAL_HEADER
 - IMAGE_SECTION_HEADER.text
 - IMAGE_SECTION_HEADER.rdata
 - IMAGE_SECTION_HEADER.data
 - IMAGE_SECTION_HEADER.rsrc
 - IMAGE_SECTION_HEADER.reloc
 - SECTION.text
 - SECTION.rdata
 - SECTION.data
 - SECTION.rsrc
 - SECTION.reloc

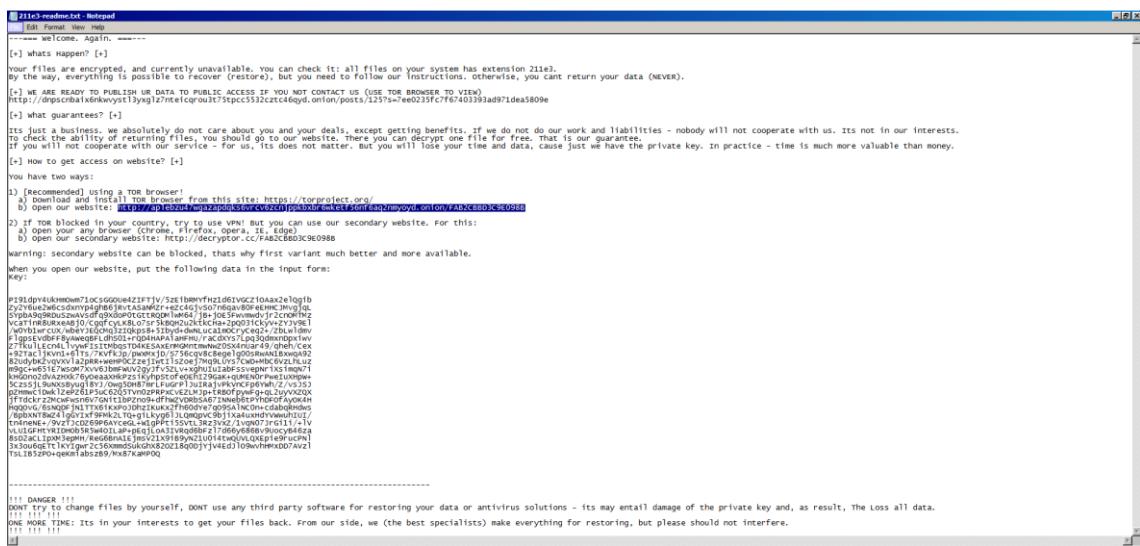


ANALISIS DINAMICO:

Iniciamos los programas “Process Explorer” y “Autoruns”, y los servicios “Visor de eventos” y el “Administrador de Tareas”, ya que nos permitirán observar los procesos y servicios que se están ejecutando antes de realizar un análisis.

Al iniciar una “snapshot” de la máquina virtual, siempre serán los mismos procesos y servicios los que se iniciaran, por lo que solamente lo comprobaremos una vez.

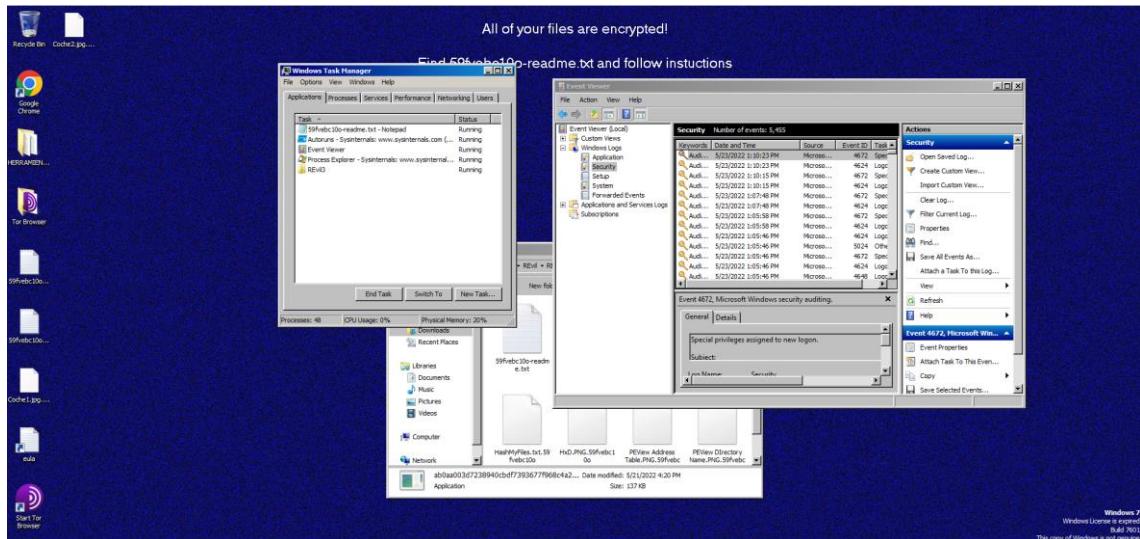




MUESTRA 2:

Esta muestra no he conseguido ejecutarla en modo dinámico.

MUESTRA 3:




```

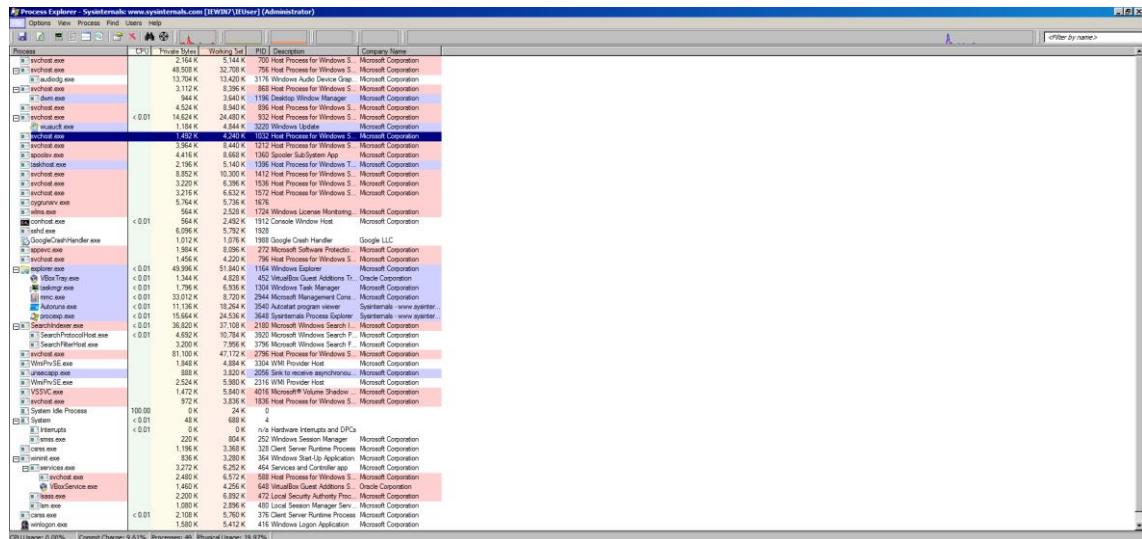
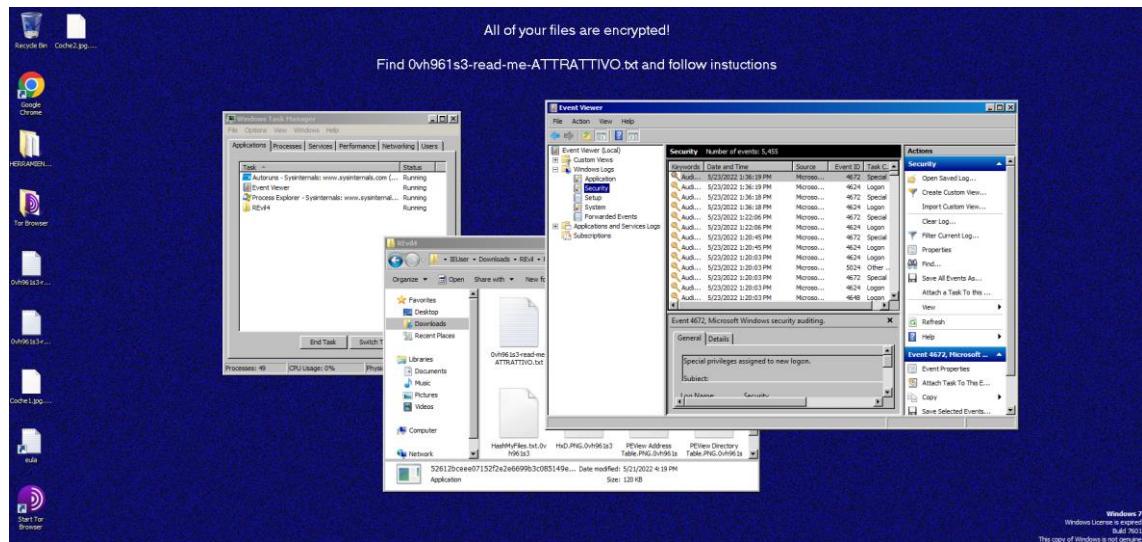
SVWebc100 reader.txt - Notepad
File Edit Format View Help
----- welcome. Again. -----
[-] what happen? [-]
Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension .59fvebc100.
By the way, everything is possible to recover (restore), but you need to follow our instructions. otherwise, you cant return your data (NEVER).
[-] what guarantee? [-]
Its just a business - we absolutely do not care about you and your deals, except getting benefits. If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practice - time is much more valuable than money.
[-] How to get access to website? [-]
using a TOR browser!
[2] Download and Install! TOR browser from this site: http://torproject.org
[2] Visit website: https://www.systinternals.com/whitepapers/59fvebc100.html
warning: secondary website can be blocked, thats why first variant much better and more available.
when you open our website, put the following data in the input field:
Key:
d0ubl3denc3f0rgt3c3y5f3f3NAXYh+J7D3mRgak1112ar3qB0867pq9w.W4Y
Y3Z20detrueSYLcWMS3cEcf3T3Pjy53+G2zTUXTAZ4POm2064d29m/62jH1w
S3vian_kmpk_captainfa1+30m3p5+7r3N2Q3axoyZC2c1Rm9g27>Ano7
RmmlL0LkxvLefBd3wrdwchmCH11fb616eJfmcRcpvbyqvxyL17q6C
RmmlL0LkxvLefBd3wrdwchmCH11fb616eJfmcRcpvbyqvxyL17q6C
TLE7L1v1yOr+derUGG2z/08f4e3k3D9vTa5ghdu50L1v12VL1HHFC6801ub10D
V_693110xu21840XK9xXwpS8ahIugcs3fFhemvxydh1515rU2X9g9c6SA
V_693110xu21840XK9xXwpS8ahIugcs3fFhemvxydh1515rU2X9g9c6SA
TQ1161d2px_ec6nlnhnnm004t7F34605h60L11Pw_Uktc92w0011s2B01vg+rl
Qd2j3Acymh00Dc73Lcd0s/F34605h60L11Pw_Uktc92w0011s2B01vg+rl
Qd2j3Acymh00Dc73Lcd0s/F34605h60L11Pw_Uktc92w0011s2B01vg+rl
VMD2GuGe41133n2d0vpy/V0Dq9p4nput7u002f3kcrnqfpu+3ip2Xew+ev113
VMD2GuGe41133n2d0vpy/V0Dq9p4nput7u002f3kcrnqfpu+3ip2Xew+ev113
UWA1D7pcc/64k6cd0t8q4nput7u002f3kcrnqfpu+3ip2Xew+ev113
AM3jupdc/_4774c10c39aduas+u+070gv4kgnqfpu+3ip2Xew+ev113
AM3jupdc/_4774c10c39aduas+u+070gv4kgnqfpu+3ip2Xew+ev113
Vv1psfNs56dt1mc0c0ceca1grn_yc66040X7ajmxfXnkh/bch/f7d8/
Squid2m2d64)9Kv12xk76ly825h07w0

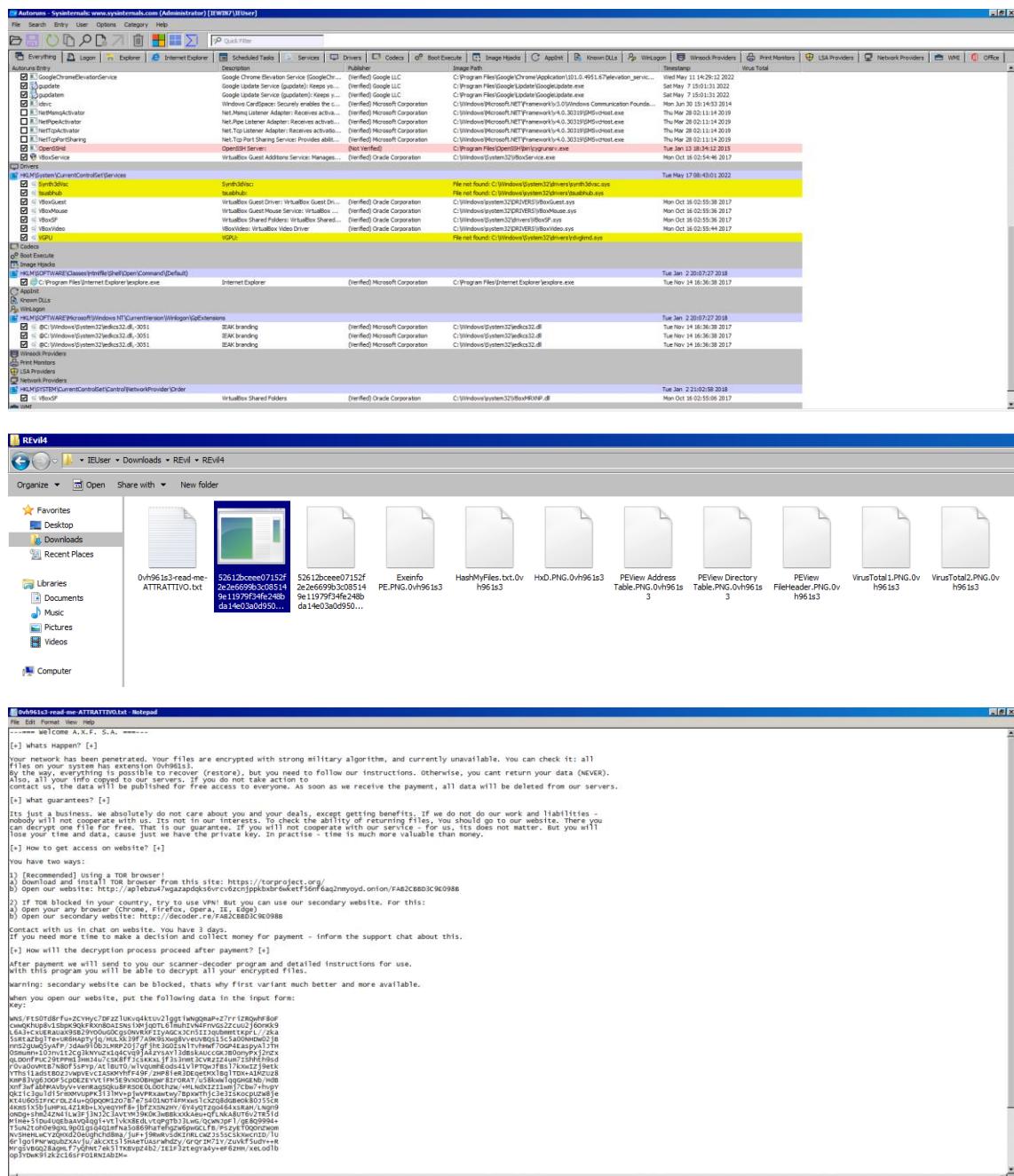
!!! DANGER !!!
!!! TRY TO CHANGE FILES BY YOURSELF, DON'T use any third party software for restoring your data or antivirus solutions - its may entail damage of the private key and, as result, The Loss all data.
!!! HOME TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere.
!!! DANGER !!

Windows Task Manager

```

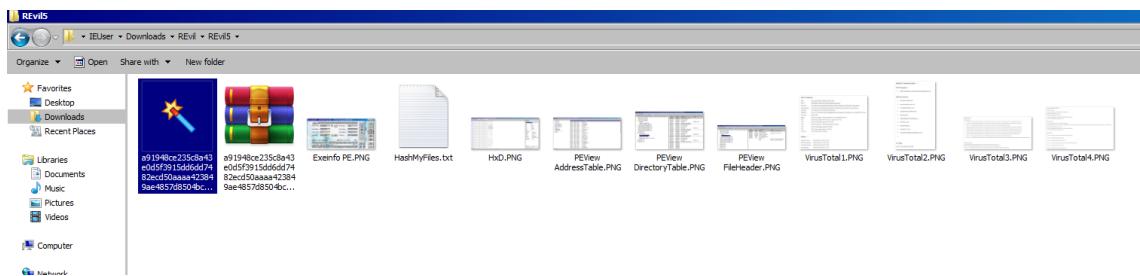
MUESTRA 4:





MUESTRA 5:

A la hora de modificar la extensión del archivo e incorporar “.exe” para convertirlo en un ejecutable, se transforma en una especie de aplicación que al ejecutarse produce un error en el maquina y produce un reinicio forzado sin ningn tipo de consecuencia de tipo malware.



CONCLUSION

Aunque se traten de diferentes muestras, los resultados obtenidos en los análisis son casi idénticos. Para empezar, la interfaz que se muestra una vez infectado el dispositivo no varía en el total de muestras analizadas, al igual que el proceso que sigue el malware para encriptar y obtener los ficheros del usuario al cual se le ha realizado el ataque.

Por otro lado, en el mensaje de rescate que envía el grupo ransomware se ven cambios mínimos, modificando principalmente la clave del usuario infectado, ya que cada uno debe tener una clave personal que será con la cual se realice el cifrado.

AVADDON

Las muestras de software ransomware as a service de la variante Avaddon que se van a estudiar han sido obtenidas de la fuente publica Any Run y son:

Nombre de la muestra	MD5	Primera vez subido a VirusTotal	Nombre
Avaddon1	c9ec0d9ff44f445ce5614cc87398b38d	03/06/2020	Trojan.GenericKD.46205682
Avaddon2	4c08871e90158382f7df438bb3df373c	21/05/2021	Gen:Variant.Ransom.Avaddon.3
Avaddon3	66c04002fbda157960a612491ac2839	20/10/2020	Gen:Heur.Ransom.REntS.Gen1(B)"
Avaddon4	64497a0fa912f0e190359684de92be2d	06/06/2020	Gen:Heur.Mint.Titirez.VuW@!Wo zZSmG
Avaddon5	7f02bf886c4b01b21217126cb9fec95c	23/06/2020	Gen:Heur.Mint.Titirez.1.23
Avaddon6	c83f30c065f7f61428eac2370ddb4f53	24/06/2020	Gen:Heur.Variadic.A.23.4
Avaddon7	1d71701e9824c730dffbcacf428a2f64	09/06/2020	Gen:Variant.Ransom.Avaddon.2

ANALISIS ESTATICO:

MUESTRA 1:

59 DE 69

Microsoft: "Trojan:Win32/Ulise!MSR"

GData: "Trojan.GenericKD.46205682"

Basic Properties ⓘ

MD5	c9ec0d9ff44f445ce5614cc87398b38d
SHA-1	591ffe54bac2c50af61737a28749ff8435168182
SHA-256	05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
Vhash	016046655d156173z12z92z23z8065z23z21z71z67z
Authentihash	18a501e209bca5ffd0c84763bb167b1524f3db86d5d6d2e926051b135a5fceed
Imphash	1156e59d43883136ef73eee451e94e3d
Rich PE header hash	1f751e2aac4a31991712f656456c5442
SSDEEP	24576:Cs6JmdFn5KLOCgHWcAvcrOcEsKfR9uA7rmFbbbbpcf:Cs6JY5KLOCyWcDUfRAA3mFbbbbpc4
TLSH	T152358D3DB4E1C071C73000F05998B7B2996EA9D2CB7204C77B8C9A9B1BB15D9A9375B3
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win64 Executable (generic) (32.2%)
TrID	Win32 Dynamic Link Library (generic) (20.1%)
TrID	Win16 NE executable (generic) (15.4%)
TrID	Win32 Executable (generic) (13.7%)
TrID	OS/2 Executable (generic) (6.2%)
File size	1.03 MB (1078784 bytes)

History ⓘ

Creation Time	2020-06-03 09:47:22 UTC
First Seen In The Wild	2020-06-03 18:47:22 UTC
First Submission	2020-06-04 14:30:39 UTC
Last Submission	2022-01-24 23:35:14 UTC
Last Analysis	2022-05-14 01:54:22 UTC

Network Communication ⓘ

HTTP Requests

- + http://www.microsoft.com/pki/certs/MicRooCerAut_2010-06-23.crt

DNS Resolutions

- + api.myip.com
- + api.myip.com
- + api.myip.com
- + microsoft.com
- + api.myip.com

IP Traffic

104.31.66.68:443 (TCP)

10.0.63.1:445

10.0.63.1:139

10.0.82.1:445

10.0.82.1:139

172.67.208.45:443 (TCP)

10.0.88.1:445

10.0.88.1:139

104.31.67.68:443 (TCP)

10.0.46.1:445

▼

Registry Actions ⓘ

Registry Keys Opened

<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings
<HKLM>\Software\Wow6432Node\Microsoft\Tracing
<HKL>\Software\Wow6432Node\Microsoft\Tracing\ulog\hm_RASAPI32
<HKL>\Software\Wow6432Node\Microsoft\Tracing\ulog\hm_RASMANCS
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
<HKCU>\Software\Microsoft\Windows NT\CurrentVersion\Network\Location Awareness
<HKLM>\System\CurrentControlSet\Services\Tcpip\Parameters
<HKLM>\System\CurrentControlSet\Control\SecurityProviders\Schannel
<HKCU>\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing
<HKCU>\Software\Microsoft\SystemCertificates\My

▼

Registry Keys Set

- + <HKL>\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
- + <HKL>\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin
- + <HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
- + <HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
- + <HKCU>\Software\Classes\Local Settings\MuiCache\12c\52C64B7E\LanguageList
- + <HKCU>\Software\Microsoft\Windows\CurrentVersion\Run\update
- + <HKLM>\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\update
- + <HKL>\System\MountedDevices\Z:
- + <HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{c84d25cc-f388-11e4-889d-806e6f6e8963}\MaxCapacity
- + <HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{c84d25cc-f388-11e4-889d-806e6f6e8963}\NukeonDelete

▼

Registry Keys Deleted

<HKCU>\Software\Microsoft\RestartManager\Session0001
<HKCU>\Software\Microsoft\RestartManager\Session0000
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
<HKL>\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
<HKL>\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
<HKCU>\Software\Microsoft\RestartManager\Session0001\RegFilesHash
<HKCU>\Software\Microsoft\RestartManager\Session0001\RegFiles0000
<HKCU>\Software\Microsoft\RestartManager\Session0001\Sequence
<HKCU>\Software\Microsoft\RestartManager\Session0001\SessionHash

Process And Service Actions

Processes Created

```
<PATH_SAMPLE.EXE>
%WINDIR%\syswow64\wbem\wmic.exe
<SYSTEM32>\iconhost.exe
%WINDIR%\syswow64\vsadmin.exe
<SYSTEM32>\vssvc.exe
<SYSTEM32>\taskeng.exe
```

Processes Terminated

```
<SYSTEM32>\wbem\wmpvse.exe
%WINDIR%\syswow64\wbem\wmic.exe
%WINDIR%\syswow64\vsadmin.exe
%WINDIR%\servicing\trustedinstaller.exe
```

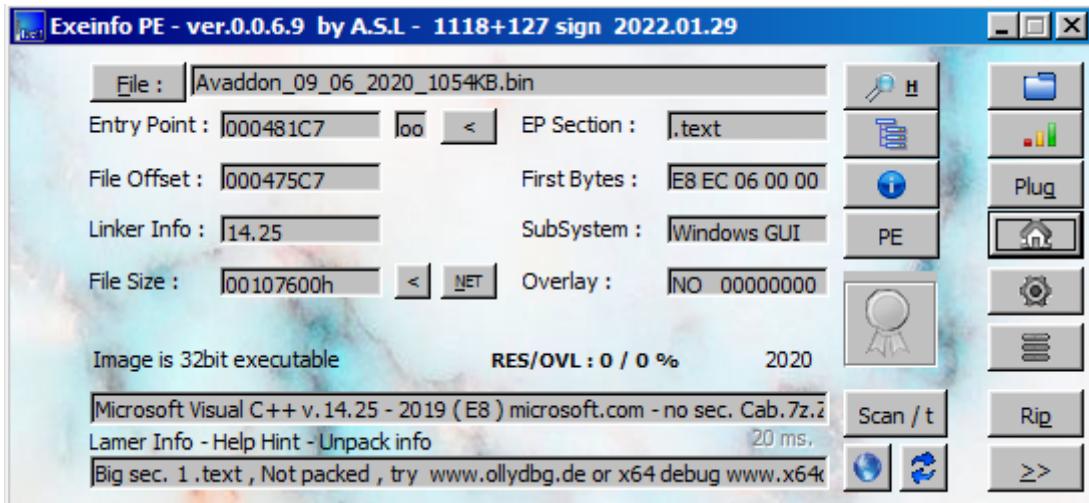
Processes Tree

```
└→ 2844 - <PATH_SAMPLE.EXE>
    └→ 992 - %WINDIR%\syswow64\wbem\wmic.exe
    └→ 2044 - %WINDIR%\syswow64\vsadmin.exe
    └→ 2084 - %WINDIR%\syswow64\wbem\wmic.exe
    └→ 1816 - %WINDIR%\syswow64\vsadmin.exe
    └→ 2092 - %WINDIR%\syswow64\wbem\wmic.exe
    └→ 2984 - %WINDIR%\syswow64\vsadmin.exe
    └→ 1020 - <SYSTEM32>\svchost.exe
    └→ 880 - <SYSTEM32>\svchost.exe
    └→ 2396 - <SYSTEM32>\taskeng.exe
```

▼

```
=====
Filename : Avaddon_09_06_2020_1054KB.bin
MD5      : c9ec0d9ff4f445ce5614cc87398b38d
SHA1     : 591ffe54bac2c50af61737a28749ff8435168182
CRC32    : 5c77ad84
SHA-256   : 05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
SHA-512   : c340baeb66fc46830b6b77b2583033ade6e10b3de04d82ece7e241107afe741442585bf2ea9d6496af93143c37e9676d4f1e1d301d55632b88b12daadadd43f0
SHA-384   : ac6c07905c0e58a343fa1bc0b6037c9191671ead6f9ec32e2f5c303c5cbc8a622a3e8bfb8bbdbe7d9f117ad79754c
Full Path : C:\Users\IEUser\Downloads\Avaddon\Avaddon_09_06_2020_1054KB.bin\Avaddon_09_06_2020_1054KB.bin
Modified Time : 5/23/2022 9:06:40 AM
Created Time  : 5/23/2022 9:49:08 AM
Entry Modified Time: 5/23/2022 9:49:08 AM
File Size    : 1,078,784
File Version :
Product Version :
Identical    :
Extension   : bin
File Attributes : A
=====
```


File	Data	Description	Value
Avaddon_09_06_2020_1054KB.bin			
IMAGE_DOS_HEADER	000F5D00	Import Name Table RVA	000F5D48C
IMAGE_DOS_HEADER_TYPE	000F5D00	Time Date Stamp	00000000
MS-DOS Sub Block	000F5D0C	Forwarder Chain	00000000
IMAGE_NT_HEADERS	000F5D10	Name RVA	0007F006
- Signature	000F5D14	Import Address Table RVA	0008F070
IMAGE_FILE_HEADER	000F5D18	Import Name Table RVA	0008F024
IMAGE_OPTIONAL_HEADER	000F5D1C	Time Date Stamp	00000000
IMAGE_SECTION_HEADER_tsr	000F5D20	Forwarder Chain	00000000
IMAGE_SECTION_HEADER_data	000F5D24	Name RVA	0007F110
IMAGE_SECTION_HEADER_data	000F5D28	Import Address Table RVA	0008F300
IMAGE_SECTION_HEADER_reloc	000F5D32	Import Name Table RVA	0008F010
SECTION_reloc	000F5D36	Time Date Stamp	00000000
SECTION_reloc	000F5D3A	Forwarder Chain	00000000
IMPORT Address Table	000F5D3E	Name RVA	0007F2CC
IMAGE_DEBUG_DIRECTORY	000F5D40	Import Address Table RVA	0008F018
IMAGE_LOAD_CONFIG_DIRECTORY	000F5D44	Time Date Stamp	00000000
IMAGE_TLS_DIRECTORY	000F5D48	Forwarder Chain	00000000
IMAGE_DEBUG_TYPE	000F5D52	Name RVA	0007F300
IMAGE_DEBUG_MISC	000F5D56	Import Address Table RVA	0008F2C0
IMPORT Name Table	000F5D5A	Import Name Table RVA	0008F06C
SECTION_data	000F5D5E	Time Date Stamp	00000000
SECTION_data	000F5D62	Forwarder Chain	00000000
SECTION_reloc	000F5D66	Name RVA	0007F345
SECTION_reloc	000F5D6A	Import Address Table RVA	0008F350
SECTION_reloc	000F5D6E	Import Name Table RVA	0008FCE4
SECTION_reloc	000F5D72	Time Date Stamp	00000000
SECTION_reloc	000F5D76	Forwarder Chain	00000000
SECTION_reloc	000F5D7A	Name RVA	0007F390
SECTION_reloc	000F5D7E	Import Address Table RVA	0008F2C8
SECTION_reloc	000F5D82	Import Name Table RVA	0008F0CD0
SECTION_reloc	000F5D86	Time Date Stamp	00000000
SECTION_reloc	000F5D8A	Forwarder Chain	00000000
SECTION_reloc	000F5D8E	Name RVA	0007F3D4
SECTION_reloc	000F5D92	Import Address Table RVA	0008F2D0
SECTION_reloc	000F5D96	Import Name Table RVA	0008F7400
SECTION_reloc	000F5D9A	Time Date Stamp	00000000
SECTION_reloc	000F5D9E	Forwarder Chain	00000000
SECTION_reloc	000F5DA2	Name RVA	0007F400
SECTION_reloc	000F5DA6	Import Address Table RVA	0008F484
SECTION_reloc	000F5DAE	Import Name Table RVA	0008F000
SECTION_reloc	000F5DB2	Time Date Stamp	00000000
SECTION_reloc	000F5DB6	Forwarder Chain	00000000
SECTION_reloc	000F5DBA	Name RVA	0007F418
Viewing IMPORT Directory Table			



MUESTRA 2:

57 de 69

Microsoft: "Ransom:Win32/Avaddon.MK!MTB"

GData: "Gen:Variant.Ransom.Avaddon.3"

Basic Properties ⓘ

MD5	4c08871e90158382f7df438bb3df373c
SHA-1	600fec77e276a5a9c9477c6c327958e5048eb67c
SHA-256	fc42cbd5939fc8b6851021497041c80acd81ce7a43b952ab7807d5a05d2ed97
Vhash	075056651d15156193z12z921z33z5065z2bz87z
Authentihash	12ef2491c9c45304f7a6945a8094dd9a12cb54d75a1254e46f75b0399bdd44b2
Imphash	b56503b8c4f46a3a086734c09c6bd0f3
Rich PE header hash	d1bea2a661ac41ee1e80a607afed3f89
SSDEEP	24576:TCsK9+OXLpMePfl8TgmBTCDqEbOpPtpFh4xfq:5ROXLpMePfzVTCD7gPtLhofq
TLSH	T12FF48E223E82C43BD97601768E5CBBB544BFA83047261ECB67C87F5E4A205D25E31A77
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win64 Executable (generic) (32.2%)
TrID	Win32 Dynamic Link Library (generic) (20.1%)
TrID	Win16 NE executable (generic) (15.4%)
TrID	Win32 Executable (generic) (13.7%)
TrID	OS/2 Executable (generic) (6.2%)
File size	775.50 KB (794112 bytes)

History ⓘ

Creation Time	2021-04-03 16:35:19 UTC
First Submission	2021-05-21 13:10:07 UTC
Last Submission	2021-05-21 13:10:07 UTC
Last Analysis	2021-07-13 15:07:09 UTC

Registry Actions ⓘ

Registry Keys Set

- + \REGISTRY\A\{31187d3a-9eae-11ea-98e6-167c9a143b2d\}\DefaultObjectStore\ObjectTable\662\Indexes\FileIdIndex-\{853201e6-2d75-11ea-a138-806e6f6e6963\}\100000001F5DB
- + HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{37B08A27-AF67-4044-BC9A-D027A55EFB19\}\DynamicInfo
- + HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{37B08A27-AF67-4044-BC9A-D027A55EFB19\}\Path
- + HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{37B08A27-AF67-4044-BC9A-D027A55EFB19\}\Hash
- + HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{37B08A27-AF67-4044-BC9A-D027A55EFB19\}\Triggers
- + \REGISTRY\A\{31187d3a-9eae-11ea-98e6-167c9a143b2d\}\DefaultObjectStore\ObjectTable\663_FileId_
- + \REGISTRY\A\{31187d3a-9eae-11ea-98e6-167c9a143b2d\}\DefaultObjectStore\ObjectTable\663_ObjectLru_
- + \REGISTRY\A\{31187d3a-9eae-11ea-98e6-167c9a143b2d\}\DefaultObjectStore\ObjectTable\663_Usn_
- + \REGISTRY\A\{31187d3a-9eae-11ea-98e6-167c9a143b2d\}\DefaultObjectStore\ObjectTable\663_ObjectId_
- + \REGISTRY\A\{31187d3a-9eae-11ea-98e6-167c9a143b2d\}\DefaultObjectStore\ObjectTable\663\AeFileID

▼

Process And Service Actions

Shell Commands

```
vssadmin Delete Shadows /All /Quiet  
wmic SHADOWCOPY DELETE /nointeractive
```

Processes Terminated

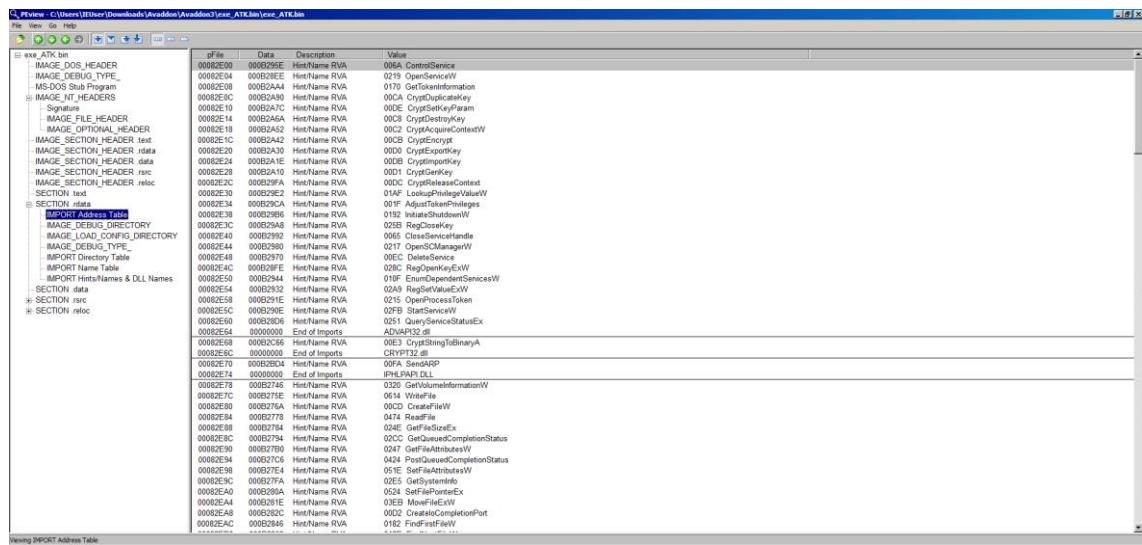
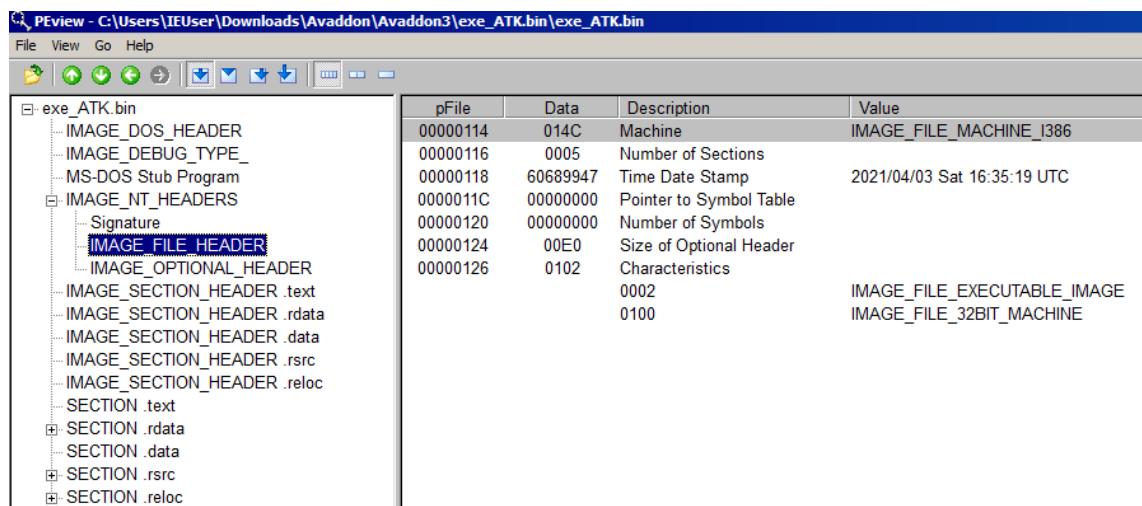
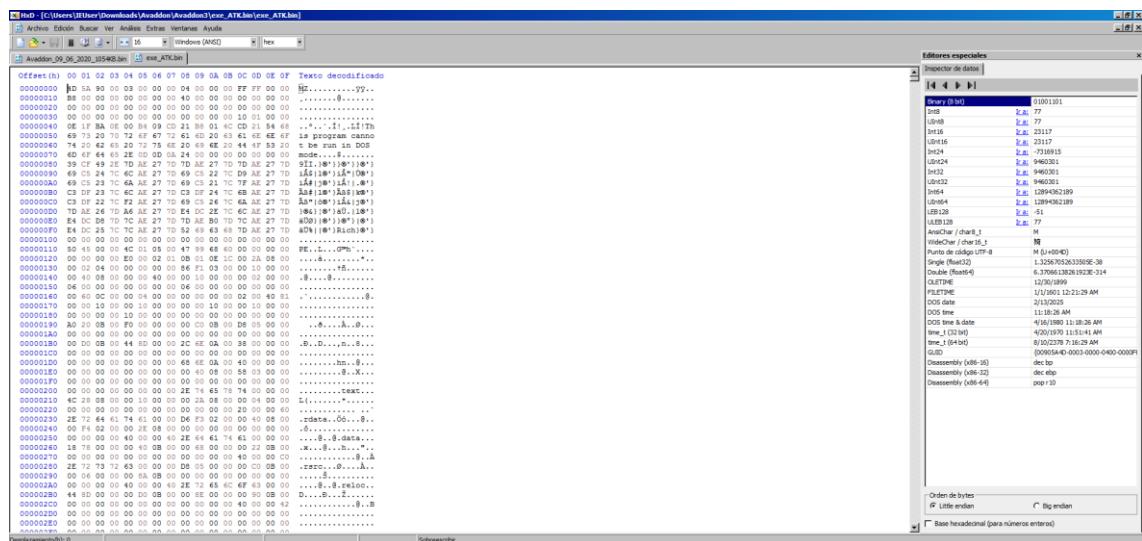
```
%CONHOST% '965650925-1742588889-81500560429799728739211841430934794-188087007-239538897  
%CONHOST% '1690847865-1646689566-198359547476315672363841732203596247574013885-1159207040  
%CONHOST% '1578755389848342749-998002207-336189444-981002267-1622663493626387941-1651395670  
%CONHOST% '901094332-1333408048201303271868900175111812278937065389-18634858902719184  
%CONHOST% '-10089510851943056959-11139722465029721371566288084-979532928-16353184241947206807  
wmic SHADOWCOPY DELETE /nointeractive  
vssadmin Delete Shadows /All /Quiet
```

Processes Tree

```
↳ 1140 - %CONHOST% '965650925-1742588889-81500560429799728739211841430934794-188087007-239538897  
↳ 2848 - %CONHOST% '1690847865-1646689566-198359547476315672363841732203596247574013885-1159207040  
↳ 1988 - %CONHOST% '1578755389848342749-998002207-336189444-981002267-1622663493626387941-1651395670  
↳ 2772 - %CONHOST% '901094332-1333408048201303271868900175111812278937065389-18634858902719184  
↳ 2782 - %CONHOST% '-10089510851943056959-11139722465029721371566288084-979532928-16353184241947206807  
↳ 3044 - %windir%\System32\svchost.exe -k swprv  
↳ 2976 - %windir%\sysWOW64\wbem\wmiprvse.exe -secured -Embedding  
↳ 2780 - wmic SHADOWCOPY DELETE /nointeractive  
↳ 2784 - wmic SHADOWCOPY DELETE /nointeractive  
↳ 2808 - wmic SHADOWCOPY DELETE /nointeractive  
↳ 2968 - %windir%\system32\vssvc.exe  
↳ 2648 - %SAMPLEPATH%  
↳ 1252 - vssadmin Delete Shadows /All /Quiet  
↳ 2836 - wmic SHADOWCOPY DELETE /nointeractive  
↳ 2172 - vssadmin Delete Shadows /All /Quiet  
↳ 1158 - wmic SHADOWCOPY DELETE /nointeractive
```

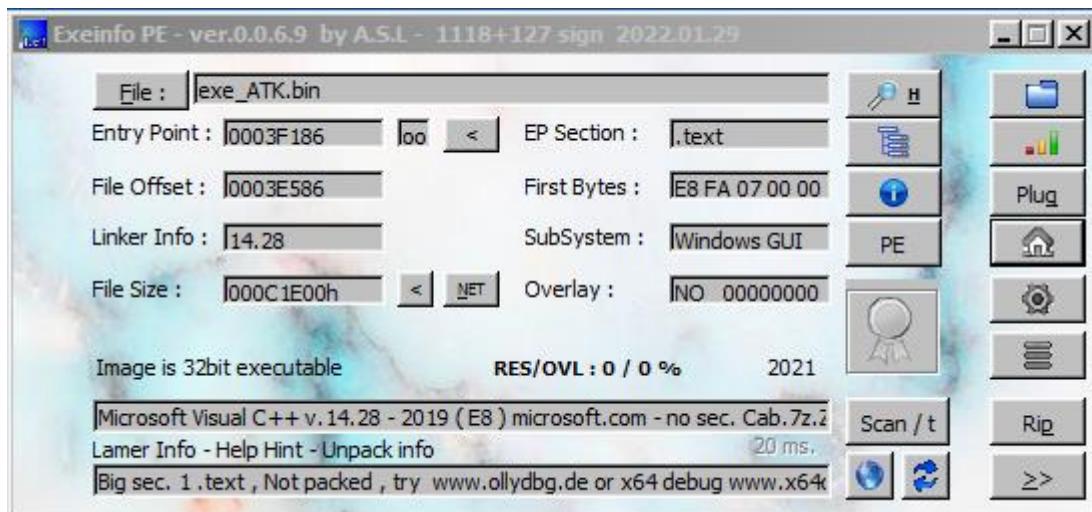
^

```
=====
Filename : exe_ATK.bin
MD5      : 4c08871e90158382f7df438bb3df373c
SHA1     : 600fec77e276a5a9c9477c6c327958e504eb67c
CRC32    : 5ac63a38
SHA-256   : fc42cbd5939fcbb8b6851021497041c80acd81ce7a43b952ab7807d5a05d2ed97
SHA-512   : c716c15d322afca842487972c1b2f4d0f5dc2caf0a16b6ba3e560467120d110df6594a5e0924af17b9e0956eecf63b97b11482798c4255a6673f6751fdbeaa8
SHA-384   : 365e3fa204bcfc02e5276a01c91b3e668368b7be8b35baaadff52d8e1eedcd01b98e974b61e4df71c6b4b07971c0a1b
Full Path : C:\Users\IEUser\Downloads\Avaddon\Avaddon3\exe_ATK.bin\exe_ATK.bin
Modified Time : 5/23/2022 9:40:22 AM
Created Time  : 5/23/2022 10:00:11 AM
Entry Modified Time: 5/23/2022 10:00:11 AM
File Size    : 794,112
File Version : 10.0.17763.831 (WinBuild.160101.0800)
Product Version : 10.0.17763.831
Identical    :
Extension   : bin
File Attributes : A
=====
```



S:\PView C:\Users\Uther\Downloads\Avaddon\Avaddon\Texec_ATK\bin\texec_ATK.exe

	Data	Description	Value
exe_ATK	00002208	Import Name Table RVA	
IMAGE_DOS_HEADER	0000E4A4	Time Date Stamp	
MS-DOS Sub Block	0000E4A8	Forwarder Chan	
Signature	0000E4AC	Name RVA	KERNEL32.dll
IMAGE_NT_HEADERS	0000E4B0	Import Address Table RVA	
IMAGE_FILE_HEADER	0000E4B4	Time Date Stamp	
IMAGE_OPTIONAL_HEADER	0000E4B8	Forwarder Chan	
IMAGE_SECTION_HEADER .text	0000E4C0	Name RVA	ADVAPI32.dll
IMAGE_SECTION_HEADER .idata	0000E4C4	Import Address Table RVA	
IMAGE_SECTION_HEADER .rdata	0000E4C8	Import Name Table RVA	
IMAGE_SECTION_HEADER .reloc	0000E4CC	Time Date Stamp	
SECTION .text	0000E4D0	Forwarder Chan	
SECTION .idata	0000E4D4	Name RVA	SHELL32.dll
IMPORT Address Table	0000E4D8	Import Address Table RVA	
IMAGE_DEBUG_DIRECTORY	0000E4DC	Import Name Table RVA	
IMAGE_LOAD_CONFIG_DIRECTORY	0000E4E0	Time Date Stamp	
IMAGE_DEBUG_TYPE	0000E4E4	Forwarder Chan	
IMAGE_NT_HEADERS	0000E4E8	Name RVA	ole32.dll
IMPORT Name Table	0000E4EC	Import Address Table RVA	
IMPORT HintNames & DLL Names	0000E4F0	Import Name Table RVA	
SECTION .data	0000E4F4	Time Date Stamp	
SECTION .rsrc	0000E4F8	Forwarder Chan	
SECTION .reloc	0000E4FC	Name RVA	OLEAUT32.dll
SECTION .idata	0000E4F0	Import Address Table RVA	
IMAGE_DEBUG_DIRECTORY	0000E4F4	Import Name Table RVA	
IMAGE_LOAD_CONFIG_DIRECTORY	0000E4F8	Time Date Stamp	
IMAGE_DEBUG_TYPE	0000E4FC	Forwarder Chan	
IMAGE_NT_HEADERS	0000E500	Name RVA	MPR.dll
IMPORT Address Table	0000E504	Import Address Table RVA	
IMAGE_DEBUG_DIRECTORY	0000E508	Import Name Table RVA	
IMAGE_LOAD_CONFIG_DIRECTORY	0000E50C	Time Date Stamp	
IMAGE_DEBUG_TYPE	0000E510	Forwarder Chan	
IMAGE_NT_HEADERS	0000E514	Name RVA	NETAPI32.dll
IMPORT Address Table	0000E518	Import Address Table RVA	
IMAGE_DEBUG_DIRECTORY	0000E51C	Import Name Table RVA	
IMAGE_LOAD_CONFIG_DIRECTORY	0000E520	Time Date Stamp	
IMAGE_DEBUG_TYPE	0000E524	Forwarder Chan	
IMAGE_NT_HEADERS	0000E528	Name RVA	IPHLPAPI.dll
IMPORT Address Table	0000E52C	Import Address Table RVA	
IMAGE_DEBUG_DIRECTORY	0000E530	Import Name Table RVA	
IMAGE_LOAD_CONFIG_DIRECTORY	0000E534	Time Date Stamp	
IMAGE_DEBUG_TYPE	0000E538	Forwarder Chan	
IMAGE_NT_HEADERS	0000E54C	Name RVA	WS2_32.dll
IMPORT Address Table	0000E540	Import Address Table RVA	
IMAGE_DEBUG_DIRECTORY	0000E544	Import Name Table RVA	
IMAGE_LOAD_CONFIG_DIRECTORY	0000E548	Time Date Stamp	
IMAGE_DEBUG_TYPE	0000E54C	Forwarder Chan	
IMAGE_NT_HEADERS	0000E550	Name RVA	



MUESTRA 3:

55 de 70

Microsoft: "Ransom:Win32/Avaddon.C!MTB"

GData: "Gen:Heur.Ransom.REntS.Gen1 (B)"

Basic Properties ⓘ

MD5	66c04002fbda157960a612491acc2839
SHA-1	27e1265900f37a7e8f7a8741d9f484ebaccf8176
SHA-256	cef7d92b4278e8c3ef404af30b39187e9ca3af6e0e28c0997a36b1fb82a51ff3
Vhash	075056651d15156143z12z911z33z5065z2bz87z
Authentihash	4bc758745103896400afa66174619b3776fca7ddeabb15d98f02c139e5cb9d79
Imphash	6baef357b0cd827321a087fdf06e1179a
Rich PE header hash	eeb3a440d3c8d698b4fe961a97fb024f
SSDeep	12288:d1820d0A4YBAdovipWC+TEd+fmOwAjWyUeStuuMJu3Qri6ZNBARyhz:dN0dT4YBAdovipWC+TEd+OvPyUeKwkh
TLSH	T19AF49E2179D2C077E16502748E48EBB584BEF8720B370DD7A3D46B0E5A60AE25F31A77
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win64 Executable (generic) (32.2%)
TrID	Win32 Dynamic Link Library (generic) (20.1%)
TrID	Win16 NE executable (generic) (15.4%)
TrID	Win32 Executable (generic) (13.7%)
TrID	OS/2 Executable (generic) (6.2%)
File size	719.00 KB (736256 bytes)

History ⓘ

Creation Time	2020-10-09 14:34:14 UTC
First Submission	2020-10-20 02:05:16 UTC
Last Submission	2020-10-20 02:05:16 UTC
Last Analysis	2021-06-09 11:23:48 UTC

Registry Keys Set

+ \REGISTRY\{f496b51a-9ea4-11ea-8c2a-167c9a143b03\}\DefaultObjectStore\lruList\0000000000002B99\ObjectLru
+ \REGISTRY\{f496b51a-9ea4-11ea-8c2a-167c9a143b03\}\DefaultObjectStore\lruList\0000000000002B99\ObjectId
+ \REGISTRY\{f496b51a-9ea4-11ea-8c2a-167c9a143b03\}\DefaultObjectStore\lruList\CurrentRru
+ \REGISTRY\{f496b51a-9ea4-11ea-8c2a-167c9a143b03\}\DefaultObjectStore\lruList\0000000000002B91\ObjectLru
+ \REGISTRY\{f496b51a-9ea4-11ea-8c2a-167c9a143b03\}\DefaultObjectStore\lruList\0000000000002B91\ObjectId
+ \REGISTRY\{f496b51a-9ea4-11ea-8c2a-167c9a143b03\}\DefaultObjectStore\lruList\0000000000002B97\ObjectLru
+ \REGISTRY\{f496b51a-9ea4-11ea-8c2a-167c9a143b03\}\DefaultObjectStore\lruList\0000000000002B97\ObjectId
+ \REGISTRY\{f496b51a-9ea4-11ea-8c2a-167c9a143b03\}\DefaultObjectStore\lruList\0000000000002B97\ObjectLru
+ \REGISTRY\{f496b51a-9ea4-11ea-8c2a-167c9a143b03\}\DefaultObjectStore\lruList\0000000000002B97\ObjectId
+ HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318\}\{B5DA8633-954C-4495-AE46-0BB5B5FB1CDC\}\Connection\PnpInstanceId
+ HKUIS-1-5-21-57582322-3065301323-1442773979-1000\Software\Microsoft\RestartManager\Session0007\Owner

▼

Registry Keys Deleted

HKLMSYSTEM\ControlSet001\Services\WmiApRp\Performance\First Counter
HKLMSYSTEM\ControlSet001\Services\WmiApRp\Performance\Last Counter
HKLMSYSTEM\ControlSet001\Services\WmiApRp\Performance\First Help
HKLMSYSTEM\ControlSet001\Services\WmiApRp\Performance\Last Help
HKLMSYSTEM\ControlSet001\Services\WmiApRp\Performance\Object List

Processes Tree

```
↳ 2956 - %CONHOST% "-260849738941439525-1029886583-1420825593447920167860034218860575686-1389866313
↳ 2144 - %CONHOST% "2089844091877143898710516516-1131488703-41084363010016718221594766487-1327803531
↳ 2140 - %CONHOST% "1919300169-5865450192098464028416873827-18724973411399226016685169280745736633
↳ 2364 - %CONHOST% "-1534163988-1364208163-21222997133850832714309458481363938037-9920482021916321092
↳ 2096 - %windir%\System32\svchost.exe -k WerSvcGroup
↳ 1460 - %windir%\system32\lssvc.exe
↳ 2832 - %CONHOST% "-754413395-738616361-97152740618105770201781502966-1410551156-5992777771843068637
↳ 648 - %CONHOST% "202697930619108304522105790818531388805772419691534525075-243517029-1992540871
↳ 2228 - %CONHOST% "1016212533-1514765871125295892118518281661215953832-72958482060613116-292718238
↳ 2896 - %windir%\system32\wbem\wmiprvse.exe
▼
```

Process And Service Actions ①

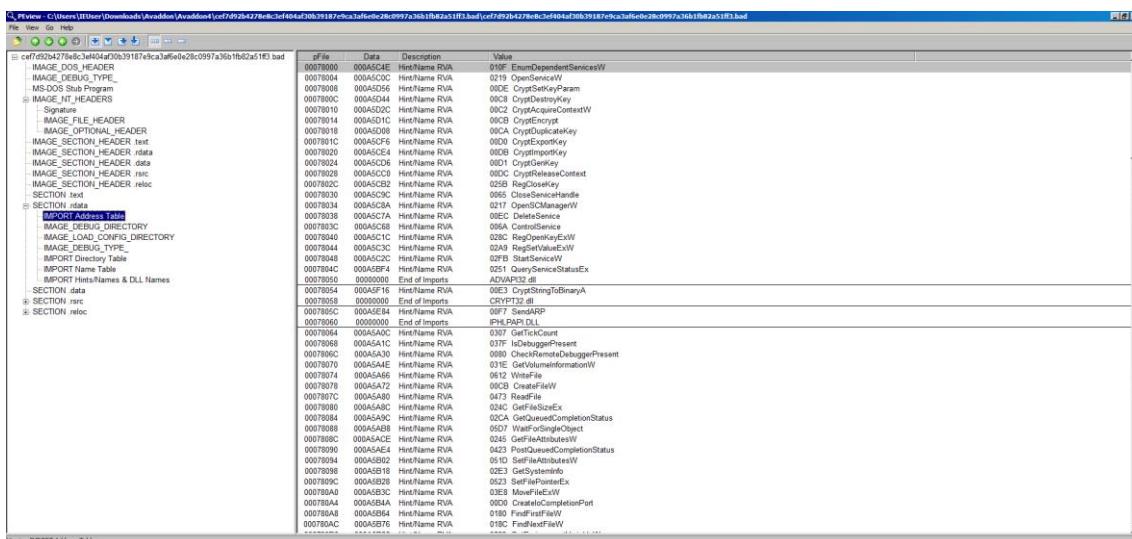
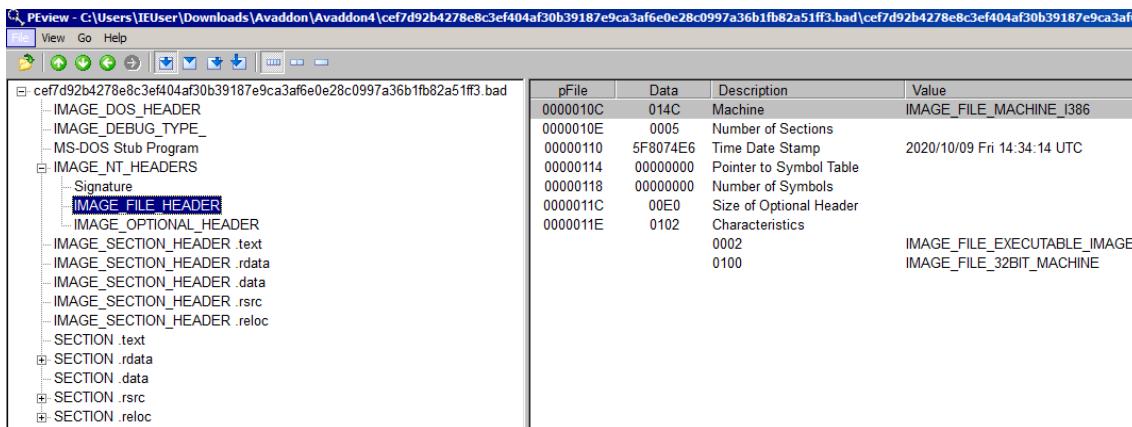
Shell Commands

```
"%ComSpec%" /c vssadmin.exe Delete Shadows /All /Quiet
vssadmin.exe Delete Shadows /All /Quiet
"%ComSpec%" /c wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
"%ComSpec%" /c bcdedit.exe /set {default} recoveryenabled No
"%ComSpec%" /c bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
"%ComSpec%" /c wbadmin DELETE SYSTEMSTATEBACKUP
"%ComSpec%" /c wmic.exe SHADOWCOPY /nointeractive
wmic.exe SHADOWCOPY /nointeractive
```

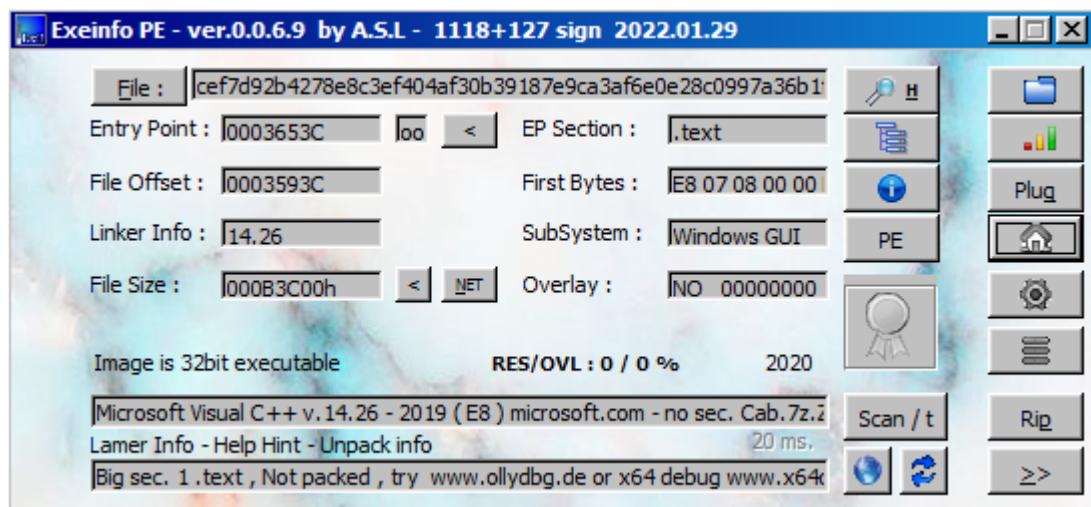
Processes Terminated

```
%CONHOST% "-260849738941439525-1029886583-1420825593447920167860034218860575686-1389866313
%CONHOST% "2089844091877143898710516516-1131488703-41084363010016718221594766487-1327803531
%CONHOST% "1919300169-5865450192098464028416873827-18724973411399226016685169280745736633
%CONHOST% "-1534163988-1364208163-21222997133850832714309458481363938037-9920482021916321092
%windir%\system32\lssvc.exe
%CONHOST% "-754413395-738616361-97152740618105770201781502966-1410551156-5992777771843068637
%CONHOST% "202697930619108304522105790818531388805772419691534525075-243517029-1992540871
%CONHOST% "1016212533-1514765871125295892118518281661215953832-72958482060613116-292718238
%CONHOST% "216982706-63329709-785246364-1887251676-1861466497842605838-1365409149-1072901913
"%ComSpec%" /c vssadmin.exe Delete Shadows /All /Quiet
▼
```

```
=====
Filename : cef7d92b4278e8c3ef404af30b39187e9ca3af6e0e28c0997a36b1fb82a51ff3.bad
MD5 : 66c04002fbda157960a612491acc2839
SHA1 : 27e126590bf37a7e8f7a8741d9f484bacccf8176
CRC32 : b16c8038
SHA-256 : ce7d92b4278e8c3ef404af30b39187e9ca3af6e0e28c0997a36b1fb82a51ff3
SHA-512 : a993c475f664c015a17328e12fd89a140d390440915698a3fc73eae99d614ee89aa4cb81d5b6f46db4a014f1fd0b0762d6789c9a8c8344e9687b8e059ce
SHA-384 : 76b999d251b19a493cf8f5196fcab27e02b787f3fb3d98611e8565e9545413f363aaef69e4fd090ffed4e7d3
Full Path : C:\Users\IEUser\Downloads\Avaddon\Avaddon4\cef7d92b4278e8c3ef404af30b39187e9ca3af6e0e28c0997a36b1fb82a51ff3.bad\cef7d92b4278e8c3ef404af30b39187e9ca3af6e0e28c0997a36b1fb82a51ff3.bad
Modified Time : 5/23/2022 9:42:07 AM
Created Time : 5/23/2022 10:18:44 AM
Last Modified Time : 5/23/2022 10:18:44 AM
File size : 736,256
File Version : 10.0.17763.831 (WinBuild.160101.0800)
Product Version : 10.0.17763.831
Identical :
Extension : bad
File Attributes : A
=====
```



File	Data	Description	Value
IMAGE_DOS_HEADER			
IMAGE_DOS_HEADER	000A43E8	Import Name Table RVA	
IMAGE_DOS_HEADER_Type_	00000000	Time Date Stamp	
MS-DOS Sub-Block	00000000	Forwarder Chain	
IMAGE_NT_HEADERS			
Signature	000A43F0	Name RVA	KERNEL32.dll
IMAGE_NT_HEADERS	000A43F0	Import Address Table RVA	
IMAGE_FILE_HEADER	000A43FC	Import Name Table RVA	
IMAGE_OPTIONAL_HEADER	000A4400	Time Date Stamp	
IMAGE_SECTION_HEADER_text	000A4400	Forwarder Chain	
IMAGE_SECTION_HEADER_rdata	000A4400	Name RVA	ADVAPI32.dll
IMAGE_SECTION_HEADER_data	000A4410	Time Date Stamp	
IMAGE_SECTION_HEADER_rsrc	000A4410	Forwarder Chain	
IMAGE_SECTION_HEADER_resc	000A4410	Name RVA	SHELL32.dll
SECTION_text	000A4414	Time Date Stamp	
SECTION_rdata	000A4418	Forwarder Chain	
SECTION_data	000A441C	Name RVA	OLEAUT32.dll
SECTION_rsrc	000A4420	Time Date Stamp	
SECTION_resc	000A4424	Forwarder Chain	
SECTION_netc	000A4428	Name RVA	MPR.dll
IMPORT Address Table			
IMAGE_DEBUG_DIRECTORY	000A442C	Import Name Table RVA	
IMAGE_LOAD_CONFIG_DIRECTORY	000A442E	Time Date Stamp	
IMAGE_DEBUG_TYPE	000A4430	Forwarder Chain	
IMAGE_DEBUG_MISC	000A4434	Name RVA	ole32.dll
IMAGE_DEBUG_MISC	000A4438	Import Address Table RVA	
IMAGE_DEBUG_MISC	000A443C	Import Name Table RVA	
IMAGE_DEBUG_MISC	000A4440	Time Date Stamp	
IMAGE_DEBUG_MISC	000A4444	Forwarder Chain	
IMAGE_DEBUG_MISC	000A4448	Name RVA	OLEAUT32.dll
IMAGE_DEBUG_MISC	000A444C	Import Address Table RVA	
IMAGE_DEBUG_MISC	000A4450	Import Name Table RVA	
IMAGE_DEBUG_MISC	000A4454	Time Date Stamp	
IMAGE_DEBUG_MISC	000A4458	Forwarder Chain	
IMAGE_DEBUG_MISC	000A445C	Name RVA	MPR.dll
IMAGE_DEBUG_MISC	000A4460	Import Address Table RVA	
IMAGE_DEBUG_MISC	000A4464	Import Name Table RVA	
IMAGE_DEBUG_MISC	000A4468	Time Date Stamp	
IMAGE_DEBUG_MISC	000A4472	Forwarder Chain	
IMAGE_DEBUG_MISC	000A4476	Name RVA	NETAPI32.dll
IMAGE_DEBUG_MISC	000A4480	Import Address Table RVA	
IMAGE_DEBUG_MISC	000A4484	Import Name Table RVA	
IMAGE_DEBUG_MISC	000A4488	Time Date Stamp	
IMAGE_DEBUG_MISC	000A4492	Forwarder Chain	
IMAGE_DEBUG_MISC	000A4496	Name RVA	IPHLPAPI.dll
IMAGE_DEBUG_MISC	000A449A	Import Address Table RVA	
IMAGE_DEBUG_MISC	000A449C	Import Name Table RVA	
IMAGE_DEBUG_MISC	000A44BC	Time Date Stamp	
IMAGE_DEBUG_MISC	000A4490	Forwarder Chain	
IMAGE_DEBUG_MISC	000A4494	Name RVA	WS2_32.dll



MUESTRA 4:

53 de 70

Microsoft: Undetected

G

Data: "Gen:Heur.Mint.Titirez.VuW@IWoZS SmG"

Basic Properties ⓘ

MD5	64497a0fa912f0e190359684de92be2d
SHA-1	2fb1c523b8fc9bb082ef5b66c5a5537b3f6026c3
SHA-256	9c9c4f20e4be9403e80e4f4bc09dcabdfcd061950d7a226fa19b220e6d3bd
Vhash	075056657d1d155az57nz2ez3
Authentihash	29d7ebc009856c731a9f7804bd216c48ac43f69e84e0703aa5b0b50794a90623
Imphash	9943a4c29092af4ae3928f37f95edad
Rich PE header hash	f7f6f19554250bf39b1b01b1b7865271
SSDEEP	12288:vBiWJbNtHpOlqPw9aKojrO3LcHvC/V07DhDPTVvExywMVG:JhVpFqPw9aKojrO3Lsv80PFxVG
TLSH	T17FF4F11276E0AC35EAB30B314D75FAF409EFB8729F71661A2688360F583D1F09962753
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (48.8%)
TrID	Win64 Executable (generic) (16.4%)
TrID	Win32 Dynamic Link Library (generic) (10.2%)
TrID	Win16 NE executable (generic) (7.8%)
TrID	Win32 Executable (generic) (7%)
File size	752.50 KB (770560 bytes)

History ⓘ

Creation Time	2019-01-13 04:42:52 UTC
First Submission	2020-06-06 14:53:35 UTC
Last Submission	2021-06-06 13:31:46 UTC
Last Analysis	2021-06-06 13:31:46 UTC

Network Communication ⓘ

DNS Resolutions

+ api.myip.com

IP Traffic

172.67.208.45:443 (TCP)
10.0.18.1:445
10.0.18.1:139
10.0.70.1:445
10.0.70.1:139

File System Actions ⓘ

Files Opened

%APPDATA%\microsoft\crypto\rsals-1-5-21-1960123792-2022915161-3775307078-1001\f58155b4b1d5a524ca0261c3ee99fb50_36d1130a-ac2e-44f7-9dc1-e424fbcbbe0ee
%WINDIR%\syswow64\wbem\wmic.exe
<SYSTEM32>\ntdll.dll
%WINDIR%\syswow64\ntdll.dll
%WINDIR%\syswow64\vssadmin.exe
C:\far2\addons\colors\custom_highlighting\black_from_fonarev.reg
C:\far2\addons\colors\custom_highlighting\black_from_july.reg
C:\far2\addons\colors\custom_highlighting\black_from_myodov.reg
C:\far2\addons\colors\custom_highlighting\colors_from_admin_essp_ru.reg
C:\far2\addons\colors\custom_highlighting\colors_from_gernichenko.reg

Files Written

```
%APPDATA%\<SAMPLE.EXE>  
z:\$recycle.bin\s-1-5-21-1960123792-2022915161-3775307078-1001\desktop.ini  
C:\Far2\Addons\Colors\Custom_Highlighting\black_from_Fonarev.reg  
C:\far2\addons\colors\custom_highlighting\262350-readme.html  
C:\Far2\Addons\Colors\Custom_Highlighting\black_from_july.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\black_from_Myodov.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_admin_essp_ru.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_Gernichenko.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_Sadovoj.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\Descript.ion
```

▼

Files Deleted

```
C:\Far2\Addons\Colors\Custom_Highlighting\black_from_Fonarev.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\black_from_july.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\black_from_Myodov.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_admin_essp_ru.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_Gernichenko.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_Sadovoj.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\Descript.ion  
C:\Far2\Addons\Colors\Custom_Highlighting\dn_like.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\FARColors242.reg  
C:\Far2\Addons\Colors\Custom_Highlighting\GreenMile.reg
```

▼

Files Copied

- + C:\Far2\Addons\Colors\Custom_Highlighting\black_from_Fonarev.reg
- + C:\Far2\Addons\Colors\Custom_Highlighting\black_from_july.reg
- + C:\Far2\Addons\Colors\Custom_Highlighting\black_from_Myodov.reg
- + C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_admin_essp_ru.reg
- + C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_Gernichenko.reg
- + C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_Sadovoj.reg
- + C:\Far2\Addons\Colors\Custom_Highlighting\Descript.ion
- + C:\Far2\Addons\Colors\Custom_Highlighting\dn_like.reg
- + C:\Far2\Addons\Colors\Custom_Highlighting\FARColors242.reg
- + C:\Far2\Addons\Colors\Custom_Highlighting\GreenMile.reg
- ▼

Files With Modified Attributes

%LOCALAPPDATA%\Microsoft\Windows\<INETFILES>\Content.IE5\index.dat
%APPDATA%\Microsoft\Windows\Cookies\index.dat
%LOCALAPPDATA%\Microsoft\Windows\History\History.IE5\index.dat
%APPDATA%\<SAMPLE.EXE>
z:\\$recycle.bin\s-1-5-21-1960123792-2022915161-3775307078-1001\desktop.ini
C:\Far2\Addons\Colors\Custom_Highlighting\black_from_Fonarev.reg
C:\Far2\Addons\Colors\Custom_Highlighting\black_from_july.reg
C:\Far2\Addons\Colors\Custom_Highlighting\black_from_Myodov.reg
C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_admin_essp_ru.reg
C:\Far2\Addons\Colors\Custom_Highlighting\Colors_from_Gernichenko.reg

▼

Files Dropped

- + C:\far2\262350-readme.html
- + C:\far2\addons\262350-readme.html
- + C:\far2\addons\colors\262350-readme.html
- + C:\far2\addons\colors\custom_highlighting\262350-readme.html
- + C:\Far2\Addons\Colors\Custom_Highlighting\black_from_Fonarev.reg
- + C:\far2\addons\colors\custom_highlighting\black_from_fonarev.reg.avdn
- + C:\Far2\Addons\Colors\Custom_Highlighting\black_from_july.reg
- + C:\far2\addons\colors\custom_highlighting\black_from_july.reg.avdn
- + C:\Far2\Addons\Colors\Custom_Highlighting\black_from_Myodov.reg
- + C:\far2\addons\colors\custom_highlighting\black_from_myodov.reg.avdn

▼

Registry Keys Opened

<HKCU>\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
<HKLM>\Software\Wow6432Node\Microsoft\Tracing
<HKLM>\Software\Wow6432Node\Microsoft\Tracing\qtwwwx_RASAPI32
<HKLM>\Software\Wow6432Node\Microsoft\Tracing\qtwwwx_RASMANCS
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
<HKCU>\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\Location Awareness
<HKLM>\System\CurrentControlSet\Services\Tcpip\Parameters
<HKLM>\System\CurrentControlSet\Control\SecurityProviders\Schannel
<HKCU>\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing
<HKCU>\Software\Microsoft\SystemCertificates\My

▼

Registry Keys Set

- + <HKLM>\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\System\EnableLUA
- + <HKLM>\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Policies\System\ConsentPromptBehaviorAdmin
- + <HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
- + <HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
- + <HKCU>\Software\Classes\Local Settings\MuiCache\12c\52C64B7E\LanguageList
- + <HKCU>\Software\Microsoft\Windows\CurrentVersion\Run\update
- + <HKLM>\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\update
- + <HKLM>\System\MountedDevices\Z:
- + <HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{c84d25cc-f368-11e4-889d-806e6f6e6963}\MaxCapacity
- + <HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{c84d25cc-f368-11e4-889d-806e6f6e6963}\NukeOnDelete

▼

Registry Keys Deleted

<HKCU>\Software\Microsoft\RestartManager\Session0001
<HKCU>\Software\Microsoft\RestartManager\Session0000
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\ProxyBypass
<HKLM>\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\ProxyBypass
<HKCU>\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\IntranetName
<HKLM>\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\IntranetName
<HKCU>\Software\Microsoft\RestartManager\Session0001\RegFilesHash
<HKCU>\Software\Microsoft\RestartManager\Session0001\RegFiles0000
<HKCU>\Software\Microsoft\RestartManager\Session0001\Sequence
<HKCU>\Software\Microsoft\RestartManager\Session0001\SessionHash

▼

Process And Service Actions ⓘ

Processes Created

```
<PATH_SAMPLE.EXE>
%WINDIR%\syswow64\wbem\wmic.exe
<SYSTEM32>\conhost.exe
%WINDIR%\syswow64\vssadmin.exe
<SYSTEM32>\vssvc.exe
<SYSTEM32>\taskeng.exe
%APPDATA%\<SAMPLE.EXE>
```

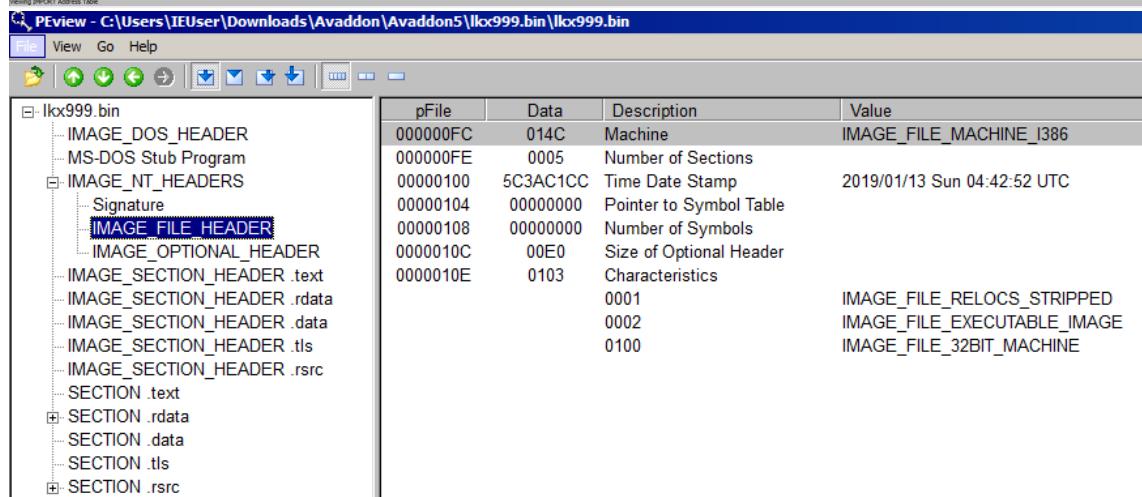
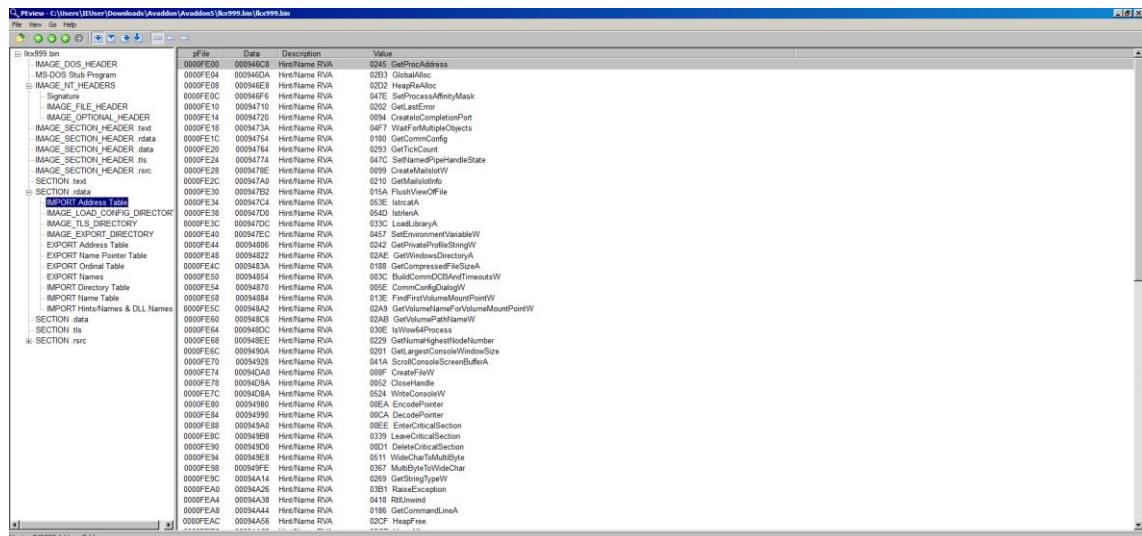
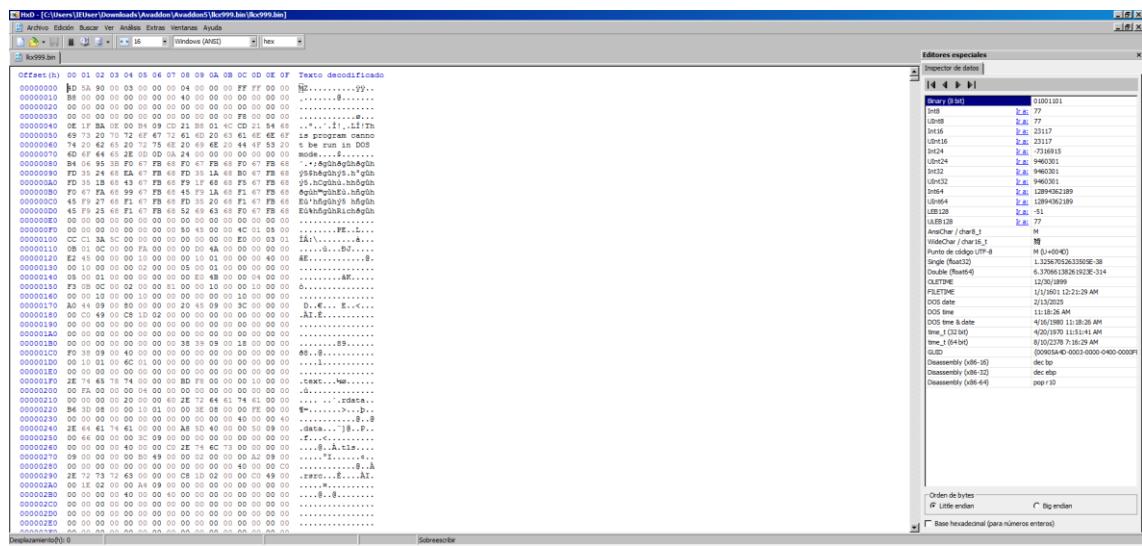
Processes Terminated

```
<SYSTEM32>\wbem\wmiprvse.exe
%WINDIR%\syswow64\wbem\wmic.exe
%WINDIR%\syswow64\vssadmin.exe
```

Processes Tree

```
↳ 1684 - <PATH_SAMPLE.EXE>
↳ 3016 - %WINDIR%\syswow64\wbem\wmic.exe
↳ 2264 - %WINDIR%\syswow64\vssadmin.exe
↳ 2916 - %WINDIR%\syswow64\wbem\wmic.exe
↳ 2772 - %WINDIR%\syswow64\vssadmin.exe
↳ 2276 - %WINDIR%\syswow64\wbem\wmic.exe
↳ 3060 - %WINDIR%\syswow64\vssadmin.exe
↳ 508 - <SYSTEM32>\svchost.exe
↳ 840 - <SYSTEM32>\svchost.exe
↳ 2140 - <SYSTEM32>\taskeng.exe
```

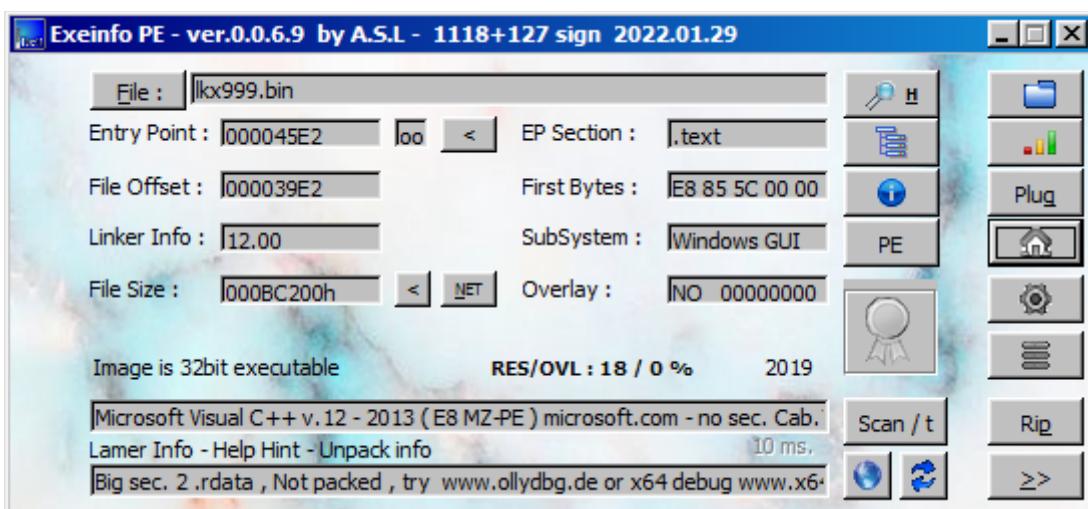
```
=====
Filename      : lqx999.bin
MD5          : 64497a0fa912f0e190359684de92be2d
SHA1         : 2fb1c523b8fc9bb82ef5b66c5a5537b3f6026c3
CRC32        : 74441f2c
SHA-256       : 9c94f20e4be9403e80e4f4bc09dcdcabdfcf061950d7a226fa19b220e6d3bd
SHA-512       : 96a17a8d601e11b005badbf47ac3a3522da697f62707beb05f2dc5169e0d8cc343a4c7cf41fbbde09b2d10abf4c4cf3ab293cccaf40a0b65787130c7484690f30
SHA-384       : 53a6d61e67816e7d9ae7d963415e6676b4c22671dedf62bd1e902790bd92f9e6c46e12ffa069e9150ad26e8111035c2c
Full Path     : C:\Users\IEUser\Downloads\Avaddon\Avaddon5\lqx999.bin\lqx999.bin
Modified Time : 5/23/2022 9:43:40 AM
Created Time  : 5/23/2022 10:21:55 AM
Entry Modified Time: 5/23/2022 10:21:55 AM
File Size     : 770,560
File Version  :
Product Version:
Identical    :
Extension    : bin
File Attributes: A
=====
```



PEview - C:\Users\IEUser\Downloads\Avaddon\Avaddon5\lhx999.bin\lhx999.bin

The left pane shows the file structure of lhx999.bin. The right pane displays a table of imports:

pFile	Data	Description	Value
00093320	0009455C	Import Name Table RVA	
00093324	00000000	Time Date Stamp	
00093328	00000000	Forwarder Chain	
0009332C	00094946	Name RVA	KERNEL32.dll
00093330	00011000	Import Address Table RVA	
00093334	000946BC	Import Name Table RVA	
00093338	00000000	Time Date Stamp	
0009333C	00000000	Forwarder Chain	
00093340	00094974	Name RVA	USER32.dll
00093344	00011160	Import Address Table RVA	
00093348	00000000		
0009334C	00000000		
00093350	00000000		
00093354	00000000		
00093358	00000000		



MUESTRA 5:

57 de 72

Microsoft: "Trojan:Win32/Obfuscator.SL!MTB"

GData: "Gen:Heur.Mint.Titirez.1.23"

Basic Properties ⓘ

MD5	7f02bf886c4b01b21217126cb9fec95c
SHA-1	7a060fac5d372811a8855d19bc8819204ac21416
SHA-256	4fd72c550987c7638e727c9d84b4940692bf94e101d3f5746bc4a8f377e49b37
Vhash	075056655d7d156018z59nz1fz
Authentihash	fe8a2a4dc07bb54f9610d98d30d8f2aa99eed7ecc229b8fe159005377bab95bb
ImpHash	86a8c98c8edbfb61c34b1f85a0a428b
SSDeep	12288:3m/rWGHAzP2oBMcjD6Bpd9dfyYajCa2FINQbrL51kEGp0nWF8zzumY12BSzSCQ:WFoP2o9DevfKDjCZNk51kZ0q8XsWSeD
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win64 Executable (generic) (52.9%)
TrID	Win16 NE executable (generic) (26.9%)
TrID	Win32 Executable (generic) (8.6%)
TrID	OS/2 Executable (generic) (3.8%)
TrID	Generic Win/DOS Executable (3.8%)
File size	712.50 KB (729600 bytes)

History ⓘ

Creation Time	2019-08-27 13:07:05 UTC
First Submission	2020-06-23 12:55:33 UTC
Last Submission	2020-06-24 08:26:37 UTC
Last Analysis	2020-07-17 04:41:27 UTC

Registry Actions ⓘ

Registry Keys Set

- + HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections
- + HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\{853201e4-2d75-11ea-a138-806e6f6e6963}\MaxCapacity
- + HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\{853201e4-2d75-11ea-a138-806e6f6e6963}\NukeOnDelete
- + HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
- + HKCU\Software\Microsoft\Windows\CurrentVersion\Run\update
- + HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections
- + HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\update
- + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\update\Index
- + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\update\ld
- + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\{402E94E6-42AE-493F-AD05-695AAD24BB29}\DynamicInfo
- + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\{402E94E6-42AE-493F-AD05-695AAD24BB29}\Path
- + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\{402E94E6-42AE-493F-AD05-695AAD24BB29}\Hash
- + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\{402E94E6-42AE-493F-AD05-695AAD24BB29}\Triggers

^

Process And Service Actions ⓘ

Shell Commands

```
wmic.exe SHADOWCOPY /nointeractive  
vssadmin.exe Delete Shadows /All /Quiet  
vssadmin.exe Delete Shadows /All /Quiet  
wmic.exe SHADOWCOPY /nointeractive  
vssadmin.exe Delete Shadows /All /Quiet  
wmic.exe SHADOWCOPY /nointeractive
```

Processes Terminated

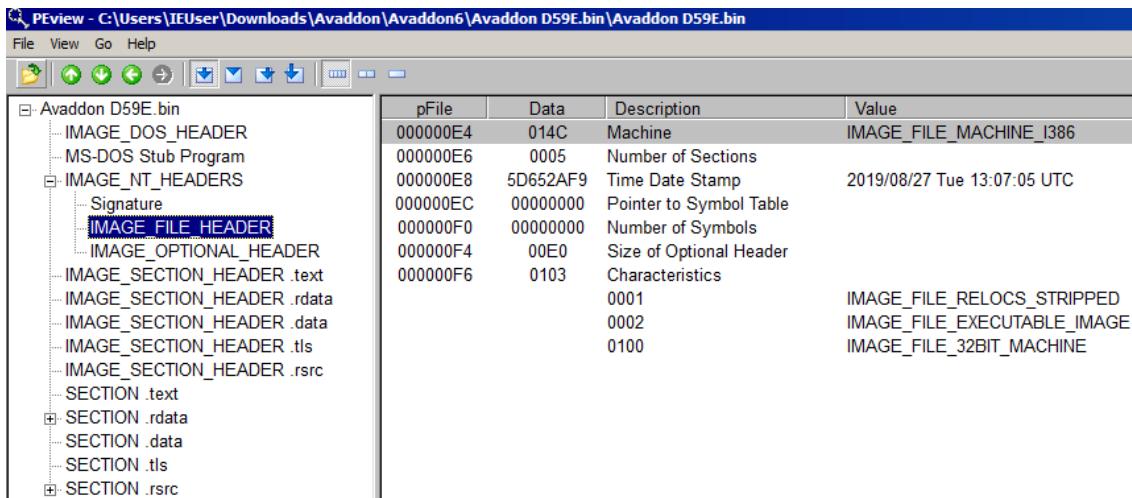
```
%CONHOST% "212576110631572305451135593037843077610453889521984895511-1297747946-1133383901  
%windir%\system32\svsvc.exe  
%APPDATA%\Microsoft%\SAMPLENAME%  
%CONHOST% "1443027416-1221665850-499906108920374635-120941158532863091594919369291652185  
%CONHOST% "2379956401666105652917512148-186124955-7830757797283409811660125127-1905251365  
%CONHOST% "1868586-1813920361524733721169034878712338856181027295067-19317147-552551622  
%CONHOST% "-1720500711-1495171606800849288-571409809-15241514181663693256857297584-58360345  
%windir%\System32\svchost.exe -k WerSvcGroup  
wmic.exe SHADOWCOPY /nointeractive  
vssadmin.exe Delete Shadows /All /Quiet  
vssadmin.exe Delete Shadows /All /Quiet  
wmic.exe SHADOWCOPY /nointeractive  
vssadmin.exe Delete Shadows /All /Quiet  
wmic.exe SHADOWCOPY /nointeractive  
taskeng.exe {F2A34D44-878A-4A94-AA79-7046024A9D6C}  
%APPDATA%\Microsoft%\SAMPLENAME%  
%CONHOST% "-412116424693365075519422071-1224374212144793552611196556544536931361705871864
```

^

Processes Tree

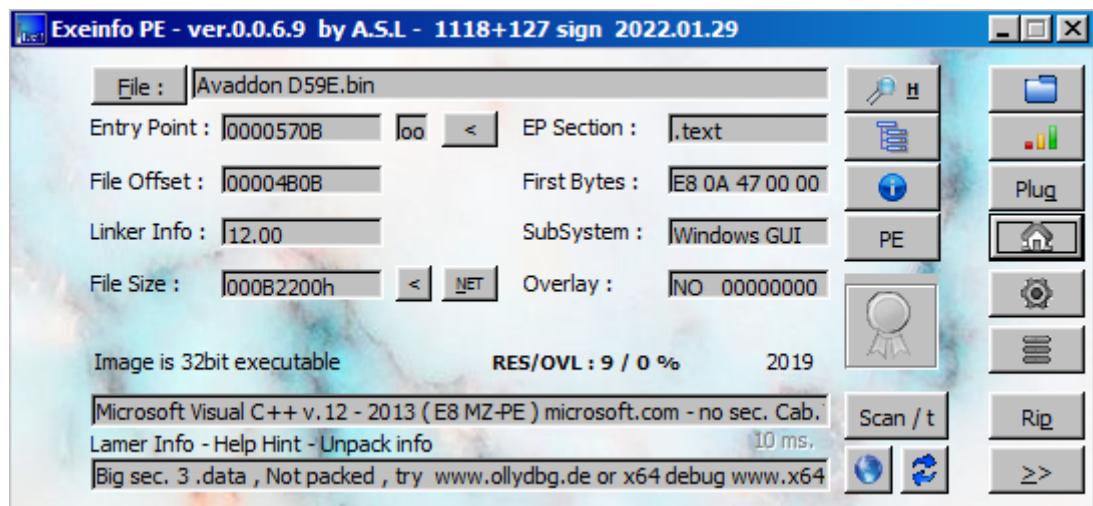
```
└→ 2764 - %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}
└→ 2824 - %CONHOST% "212576110631572305451135593037843077610453889521984895511-1297747946-1133383901
└→ 2896 - %windir%\system32\vssvc.exe
└→ 2220 - %APPDATA%\Microsoft\%SAMPLENAME%
└→ 2956 - %CONHOST% "1443027416-1221665850-499906108920374635-120941158532863091594919369291652185
└→ 2868 - %CONHOST% "2379956401666105652917512148-186124955-7830757797283409811660125127-1905251365
└→ 3000 - %CONHOST% "1868586-1813920361524733721169034878712338856181027295067-19317147-552551622
└→ 2404 - wmidap.exe /F /T /R
└→ 2084 - %CONHOST% "-1720500711-1495171606800849288-571409809-15241514181663693256857297584-58360345
└→ 260 - %windir%\system32\wbem\wmiprvse.exe
└→ 2280 - %windir%\System32\svchost.exe -k WerSvcGroup
└→ 2664 - %SAMPLEPATH%
└→ 2948 - wmic.exe SHADOWCOPY /nointeractive
└→ 2992 - vssadmin.exe Delete Shadows /All /Quiet
└→ 1968 - vssadmin.exe Delete Shadows /All /Quiet
└→ 3032 - wmic.exe SHADOWCOPY /nointeractive
└→ 2860 - vssadmin.exe Delete Shadows /All /Quiet
└→ 2816 - wmic.exe SHADOWCOPY /nointeractive
└→ 1788 - taskeng.exe {F2A34D44-878A-4A94-AA79-7046024A9D6C}
└→ 2228 - %APPDATA%\Microsoft\%SAMPLENAME%
└→ 1824 - %windir%\System32\svchost.exe -k WerSvcGroup
└→ 3040 - %CONHOST% "-412116424693365075519422071-1224374212144793552611196556544536931361705871864
^
```

```
=====
Filename : Avaddon D59E.bin
MD5 : f02bf886c4b01b21217126cb9fec95c
SHA1 : 7a060fac5d372811a8855d19bc8819204ac21416
CRC32 : fcba50910
SHA-256 : 4fd72c5509987c7638e727c9d84b49404692bf94e101d3f5746bc4a8f377e49b37
SHA-512 : f10b6ff5f5967912a79c43147d580de48861c5e2206a9558a03b3192618f293b0556747aa082948ff0108677834dbe4156264ae4f90b9e1816ab388a939c9ca9b
Full Path : C:\Users\IEUser\Downloads\Avaddon\Avaddon6\Avaddon D59E.bin\Avaddon D59E.bin
Modified Time : 5/23/2022 9:44:43 AM
Created Time : 5/23/2022 10:50:39 AM
Entry Modified Time: 5/23/2022 10:50:39 AM
File Size : 729,600
File Version :
Product Version :
Identical :
Extension : bin
File Attributes : A
=====
```



	pfile	Data	Description	Value
Avaddon D59E bin	0001980C	HdrName RVA	0058 CloseEventLog	
- IMAGE_DOS_HEADER	00019A01	00000000	End of Import	ADVAPI32.dll
- IMAGE_NT_HEADERS	00019A08	00000000	0010 CreateConsole	
- Signature	00019A0C	00000000	05AA IntCopyA	
- IMAGE_FILE_HEADER	00019A10	00000000	0451 SetEndOfFile	
- IMAGE_OPTIONAL_HEADER	00019A14	00000000	0533 WriteTapeDisk	
- IMAGE_SECTION_HEADER .text	00019A18	00000000	047F GetEnvironmentPck	
- IMAGE_SECTION_HEADER .rdata	00019A1C	00000000	01DA GetEnvironmentStringsW	
- IMAGE_SECTION_HEADER .data	00019A20	00000000	04F9 WafForSingleObject	
- IMAGE_SECTION_HEADER .rsrc	00019A24	00000000	0429 SetModuleHandleW	
SECTION .text	00019A2C	00000000	0216 SetThreadHandleW	
- IMAGE_SECTION_HEADER .rsrc	00019A30	00000000	015A GetConsoleCP	
SECTION .rdata	00019A34	00000000	0019 FreeConsole	
- IMPORT Address Table	00019A38	00000000	015F ReadProcessMemory	
- IMAGE_LOAD_CONFIG_DIRECTORY	00019A3C	00000000	005B WriteProcessMemory	
- IMAGE_TLS_DIRECTORY	00019A40	00000000	0201 HeapQueryInformation	
- IMPORT Directory Table	00019A44	00000000	048A SetSystemPowerState	
- IMPORT Name Table	00019A48	00000000	0169 GetACP	
- IMAGE_RESOURCE_TABLE	00019A4C	00000000	046E WriteFileW	
SECTION .data	00019A4E	00000000	03F9 ReleaseActCtx	
- SECTION .rsrc	00019A50	00000000	0202 GetLastError	
SECTION .rsrc	00019A54	00000000	0245 GetProcAddress	
- IMAGE_SECTION_HEADER .rsrc	00019A58	00000000	0203 ReadProcessMemory	
- IMAGE_SECTION_HEADER .rsrc	00019A5C	00000000	007B CreateSemaphoreExBuffer	
SECTION .rdata	00019A60	00000000	0202 HeapUnlock	
- IMAGE_SECTION_HEADER .rsrc	00019A64	00000000	0344 LocalAlloc	
- IMAGE_SECTION_HEADER .rsrc	00019A68	00000000	0275 ReadProcessParameters	
- IMAGE_SECTION_HEADER .rsrc	00019A6C	00000000	04F7 Win32nAllocateObjects	
SECTION .rdata	00019A70	00000000	0213 GetModuleFileNameA	
- SECTION .rsrc	00019A74	00000000	0203 HeapSetInformation	
SECTION .rdata	00019A78	00000000	0060 CreateMutexW	
- IMAGE_SECTION_HEADER .rsrc	00019A7C	00000000	024F OpenPrivateDirectoryW	
SECTION .rdata	00019A80	00000000	0242 GetVersion	
- IMAGE_SECTION_HEADER .rsrc	00019A84	00000000	0240 GetPrivateProfileSectionW	
SECTION .rdata	00019A88	00000000	0129 FindActxSectionStringW	
- IMAGE_SECTION_HEADER .rsrc	00019A8C	00000000	0322 DeleteActxW	
SECTION .rdata	00019A90	00000000	0023 DeleteFileA	
- IMAGE_SECTION_HEADER .rsrc	00019A94	00000000	0052 CloseHandle	
SECTION .rdata	00019A98	00000000	0087 CreateFileW	
- IMAGE_SECTION_HEADER .rsrc	00019A9C	00000000	044E SetFileConnConfigA	
SECTION .rdata	00019A9E	00000000	0157 FlushFileBuffers	
- SECTION .rsrc	00019A9F	00000000	0524 WriteConsoleW	
SECTION .rsrc	00019A9A	00000000	006A EncodePointer	
- SECTION .rsrc	00019A9C	00000000	00CA DecodePointer	

	pfile	Data	Description	Value
Avaddon D59E bin	0001979C	00000000	Import Name Table RVA	
- IMAGE_DOS_HEADER	0001979D	00000000	Time Date Stamp	
- IMAGE_NT_HEADERS	0001979E	00000000	Forwarder Chain	
- Signature	0001979F	00000000	KERNEL32.dll	
- IMAGE_FILE_HEADER	000197A0	00000000	Import Address Table RVA	
- IMAGE_OPTIONAL_HEADER	000197A4	00000000	0000000000000000	
- IMAGE_SECTION_HEADER .text	000197A8	00000000	Time Date Stamp	
- IMAGE_SECTION_HEADER .rdata	000197A9	00000000	Forwarder Chain	
- IMAGE_SECTION_HEADER .data	000197AC	00000000	USER32.dll	
- IMAGE_SECTION_HEADER .rsrc	000197AD	00000000	Import Address Table RVA	
SECTION .text	000197AE	00000000	Time Date Stamp	
- IMAGE_SECTION_HEADER .rsrc	000197B0	00000000	Forwarder Chain	
SECTION .rdata	000197B4	00000000	ADVAPI32.dll	
- IMPORT Address Table	000197B8	00000000	Import Address Table RVA	
- IMAGE_LOAD_CONFIG_DIRECTORY	000197B9	00000000	0000000000000000	
- IMAGE_TLS_DIRECTORY	000197BA	00000000	Time Date Stamp	
- IMPORT Directory Table	000197BC	00000000	Forwarder Chain	
- IMPORT Name Table	000197BD	00000000	Name Rva	
- IMAGE_RESOURCE_TABLE	000197BE	00000000	Forwarder Chain	
- IMAGE_SECTION_HEADER .rsrc	000197BF	00000000	0000000000000000	
SECTION .data	000197C0	00000000	2019	
- SECTION .rsrc	000197C4	00000000		
SECTION .rsrc	000197C8	00000000		
- IMAGE_SECTION_HEADER .rsrc	000197CC	00000000		
SECTION .rdata	000197D0	00000000		
- IMAGE_SECTION_HEADER .rsrc	000197D4	00000000		
SECTION .rdata	000197D8	00000000		
- IMAGE_SECTION_HEADER .rsrc	000197DC	00000000		
SECTION .rdata	000197E0	00000000		
- IMAGE_SECTION_HEADER .rsrc	000197E4	00000000		
SECTION .rdata	000197E8	00000000		
- IMAGE_SECTION_HEADER .rsrc	000197F2	00000000		
SECTION .rdata	000197F8	00000000		
- IMAGE_SECTION_HEADER .rsrc	000197FC	00000000		



MUESTRA 6:

60 de 69

Microsoft: "Trojan:Win32/Vhapak.DEB!MTB"

GData: "Gen:Heur.Variadic.A.23.4"

Basic Properties ⓘ

MD5	c83f30c065f7f61428eac2370ddb4f53
SHA-1	cf70af0c89d7b00839c1d32852c53c603d35e32
SHA-256	bcb69244dc69a152af4dca3849bb4f3ca634ad785926304c672dbf8a3c38e7bc
Vhash	095066657d1d1d055az58!z
Authentihash	6795911f3d70407b5851ac895d33a48252fab56e5c177d48d676666c67e15cc2
Imphash	e540445006624651055cf7eb5e9d1ea3
Rich PE header hash	846ca0e2fc712502429496055ff77f93
SSDEEP	24576:WvdmYEBLExewPcf5WHHs3Ggo6EoI+th0q:WhEBLug5WnsWn9KN
TLSH	T1F1151211FBD4D032F8664938D969C3B02F7BBCB36624509F67682B2F1E31AD096A4717
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win64 Executable (generic) (40.3%)
TrID	Win16 NE executable (generic) (19.3%)
TrID	Win32 Executable (generic) (17.2%)
TrID	OS/2 Executable (generic) (7.7%)
TrID	Generic Win/DOS Executable (7.6%)
File size	881.50 KB (902656 bytes)

History ⓘ

Creation Time	2019-01-31 21:39:33 UTC
First Submission	2020-06-24 23:28:08 UTC
Last Submission	2021-06-13 19:19:18 UTC
Last Analysis	2021-09-09 05:52:10 UTC

Registry Actions ⓘ

Registry Keys Set

- + HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections
 - + HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\{853201e4-2d75-11ea-a138-806e6f6e6963}\MaxCapacity
 - + HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\{853201e4-2d75-11ea-a138-806e6f6e6963}\NukeOnDelete
 - + HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings
 - + HKCU\Software\Microsoft\Windows\CurrentVersion\Run\update
 - + HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections
 - + HKLM\Software\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\update
 - + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\{FCB3887E-B9F5-45F8-87E4-0F57D11194A1}\DynamicInfo
 - + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\{FCB3887E-B9F5-45F8-87E4-0F57D11194A1}\Path
 - + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\{FCB3887E-B9F5-45F8-87E4-0F57D11194A1}\Hash
 - + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\{FCB3887E-B9F5-45F8-87E4-0F57D11194A1}\Triggers
 - + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\update\Index
 - + HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\update\Id
- ^

Processes Tree

```
↳ 2736 - %windir%\System32\svchost.exe -k WerSvcGroup
↳ 268 - %CONHOST% "1431808344167184924812789105301325436766-2081027171364726877915357290-765751054
↳ 2976 - %CONHOST% "-2060832753108186966220002391788541648051907011889754751563-1130245318888707380
↳ 2144 - %CONHOST% "-1625660353-368781985-5793939621507357770259291960-1070816484-703233938284088706
↳ 1044 - %CONHOST% "135016006-1826523016-365209721611325000-792108908-87420726-1981372252-1771182941
↳ 3020 - %CONHOST% "-19053688261944937830-19489977551866954301-208892149717677312498955273-1284378432
↳ 1464 - %CONHOST% "-413275994-1168558164-27466456919181764991030068972-1053382575-1407275311-1099566014
↳ 868 - %windir%\System32\svchost.exe -k WerSvcGroup
↳ 2140 - wmiadap.exe /F /T /R
↳ 2308 - taskeng.exe {46DF8262-1361-4C4C-AFEE-372D4FBFF177}
    ↳ 2332 - %APPDATA%\Microsoft\%SAMPLENAME%
↳ 2192 - %windir%\system32\wbem\wmiprvse.exe
↳ 2872 - %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}
↳ 3052 - %windir%\system32\vssvc.exe
↳ 2952 - %APPDATA%\Microsoft\%SAMPLENAME%
↳ 2612 - %SAMPLEPATH%
    ↳ 1292 - wmic.exe SHADOWCOPY /nointeractive
    ↳ 2160 - vssadmin.exe Delete Shadows /All /Quiet
    ↳ 3012 - vssadmin.exe Delete Shadows /All /Quiet
    ↳ 1140 - vssadmin.exe Delete Shadows /All /Quiet
    ↳ 2968 - wmic.exe SHADOWCOPY /nointeractive
    ↳ 1968 - wmic.exe SHADOWCOPY /nointeractive
^
```

Process And Service Actions (i)

Shell Commands

```
wmic.exe SHADOWCOPY /nointeractive  
vssadmin.exe Delete Shadows /All /Quiet  
vssadmin.exe Delete Shadows /All /Quiet  
vssadmin.exe Delete Shadows /All /Quiet  
wmic.exe SHADOWCOPY /nointeractive  
wmic.exe SHADOWCOPY /nointeractive
```

Processes Terminated

```
%windir%\System32\svchost.exe -k WerSvcGroup  
%CONHOST% "1431808344167184924812789105301325436756-2081027171364726877915357290-765751054  
%CONHOST% "-2060832753108186966220002391788541648051907011889754751563-1130245318888707380  
%CONHOST% "-1625660353-368781985-579393962150735770259291960-1070816484-703233938284088706  
%CONHOST% "135016006-1826523016-365209721611325000-792108908-87420726-1981372252-1771182941  
%CONHOST% "-19053688261944937830-19489977551856954301-208892149717677312498955273-1284378432  
%CONHOST% "-413275994-1168558164-27466456919181764991030068972-1053392575-1407275311-1099566014  
wmiadap.exe /F /T /R  
%APPDATA%\Microsoft\%SAMPLENAME%  
%windir%\system32\wssvc.exe  
%APPDATA%\Microsoft\%SAMPLENAME%  
wmic.exe SHADOWCOPY /nointeractive  
vssadmin.exe Delete Shadows /All /Quiet  
vssadmin.exe Delete Shadows /All /Quiet  
vssadmin.exe Delete Shadows /All /Quiet  
wmic.exe SHADOWCOPY /nointeractive  
wmic.exe SHADOWCOPY /nointeractive
```

^

```
=====
Filename      : Avaddon.bin
MD5          : c83f30c065f7f61428eac2370ddb4f53
SHA1         : cfd70af0c89d7b00839c1d32852c53c603d35e32
CRC32        : e63f795a
SHA-256       : bcb6924dc69a152af4dca3849b4f3c634ad785926304c672dbf8a3c38e7bc
SHA-512       : 26100fdf2ba32c0a2f5d27589e730e6af4a16b5cad16cb8ec6314e4291ca1858e35906645636617dacc7c72be6792b01f2bbc073c4468701326e8c889e1d51
SHA-384       : 192130017371271e29dc75d7a13469c5e842af2eac451157c30b9cd54e6f39454e749727f12db9e52eb4cfca1cf81cab
Full Path     : C:\Users\IEUser\Downloads\Avaddon\Avaddon\Avaddon.bin\Avaddon.bin
Modified Time : 5/23/2022 9:46:55 AM
Created Time   : 5/23/2022 10:56:43 AM
Entry Modified Time: 5/23/2022 10:56:43 AM
File Size      : 902,656
File Version   :
Product Version:
Identical      :
Extension      : bin
File Attributes: A
=====
```

Immunity Debugger - [C:\Users\IEUser\Downloads\Avaddon\Avaddon7\Avaddon.bin]

Editors especiales

Inspector de datos

Hex View (0x00000000 - 0x00000000)

Todos descodificados

00000000 CF 43 31 60 BB 22 5F 33 BB 22 SF 33 ICL <3>=3<3>_3
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 FF FF 00 00
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000A0 E4 54 F3 33 E1 22 5F 33 E4 54 F3 33 E4 54 F3 33 A7D3a=3,z152=3
000000B0 EB 22 SE 33 F7 22 5F 33 E4 54 F3 333=3....3=3
000000C0 8D 4D 43 60 BB 22 5F 33 E4 54 F3 333=3....3=3
000000D0 S2 49 C3 60 BB 22 5F 33 E4 54 F3 333=3....3=3
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000100 ED 13 00 00 00 10 00 00 00 01 00 00 00 00 00 00
00000110H.....B.....
00000120I.....
00000130L.....
00000140 F9 47 GE 00 02 00 00 F1 00 00 10 00 00 10 00 00
000001500.....
00000160P.....
00000170T.....
00000180U.....
00000190V.....
000001A0W.....
000001B0X.....
000001C0Y.....
000001D0Z.....
000001E0text.....
000001F0rsrc.....
00000200idata.....
00000210rdata.....
00000220data.....
00000230etc.....
00000240etc.....
00000250etc.....
00000260etc.....
00000270etc.....
00000280etc.....
00000290etc.....
000002A0etc.....
000002B0etc.....
000002C0etc.....
000002D0etc.....
000002E0etc.....

00000000 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Deshabilitar 0 Deshabilitar 1 Sobrescribir 2

PEView - C:\Users\IEUser\Downloads\Avaddon\Avaddon7\Avaddon.bin

File Structure

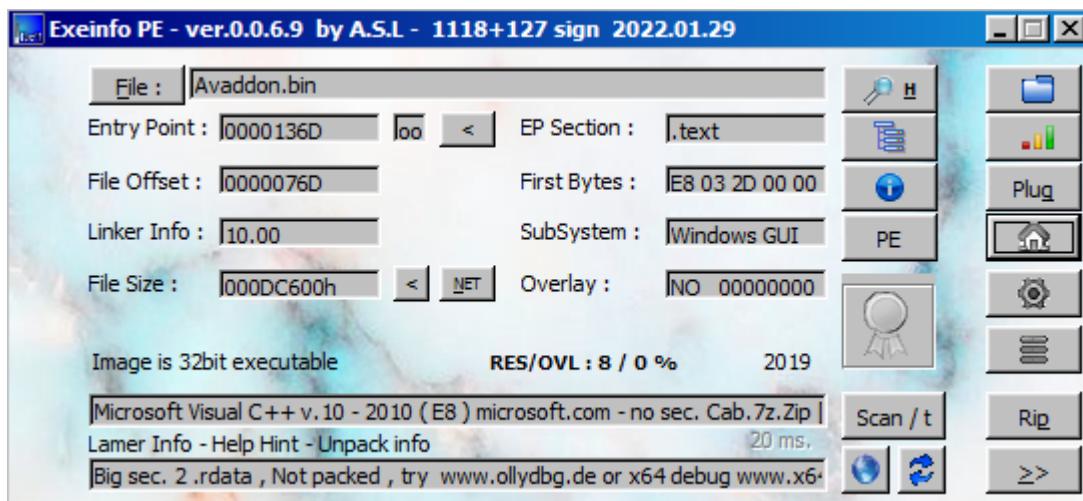
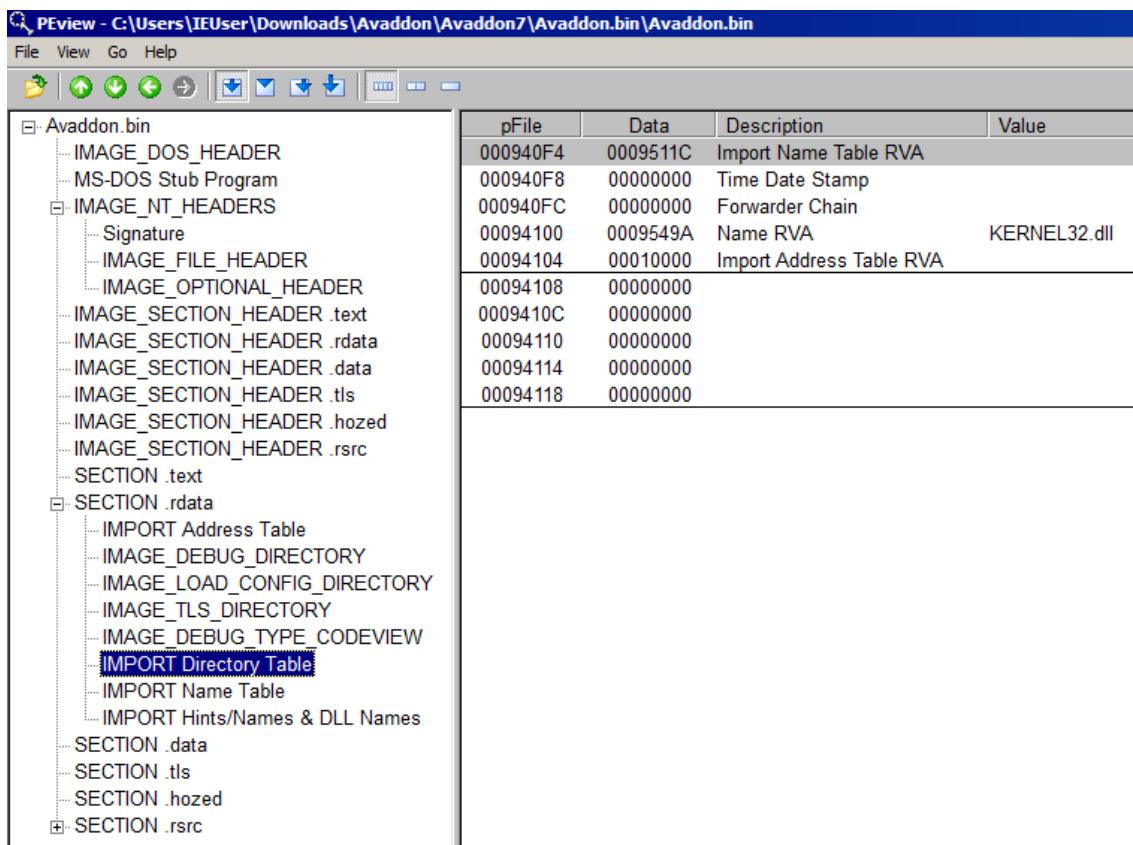
- Avaddon.bin
 - IMAGE_DOS_HEADER
 - MS-DOS Stub Program
 - IMAGE_NT_HEADERS
 - Signature
 - IMAGE_FILE_HEADER
 - IMAGE_OPTIONAL_HEADER
 - IMAGE_SECTION_HEADER .text
 - IMAGE_SECTION_HEADER .rdata
 - IMAGE_SECTION_HEADER .data
 - IMAGE_SECTION_HEADER .tls
 - IMAGE_SECTION_HEADER .hovedz
 - IMAGE_SECTION_HEADER .rsrc
 - SECTION .text
 - + SECTION .rdata
 - SECTION .data
 - SECTION .tls
 - SECTION .hovedz
 - + SECTION .rsrc
 - SECTION .text

pFile	Data	Description	Value
0000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
0000000EE	0006	Number of Sections	
0000000F0	5C536B15	Time Date Stamp	2019/01/31 Thu 21:39:33 UTC
0000000F4	00000000	Pointer to Symbol Table	
0000000F8	00000000	Number of Symbols	
0000000FC	00E0	Size of Optional Header	
0000000FE	0103	Characteristics	
	0001		IMAGE_FILE_RELOCS_STRIPPED
	0002		IMAGE_FILE_EXECUTABLE_IMAGE
	0100		IMAGE_FILE_32BIT_MACHINE

PEView - C:\Users\IEUser\Downloads\Avaddon\Avaddon7\Avaddon.bin

Import Address Table

pFile	Data	Description	Value
0000000F00	0000000F00	HintName RVA	0424 SetComputerNameW
0000000F04	0000000F04	HintName RVA	0090 CreateHardLinkA
0000000F08	0000000F08	HintName RVA	0400 SetComputerNameExA
0000000F0C	0000000F0C	HintName RVA	0094 GetTextCount
0000000F10	0000000F10	HintName RVA	0148 FindFirstVolumeMountPointA
0000000F14	0000000F14	HintName RVA	033F LoadLibraryW
0000000F18	0000000F18	HintName RVA	0054! InitLibrary
0000000F22	0000000F22	HintName RVA	0203 GetProcAddress
0000000F26	0000000F26	HintName RVA	0090 GlobalAlloc
0000000F30	0000000F30	HintName RVA	03C1 ReadFileW
0000000F34	0000000F34	HintName RVA	000D BuildCommDCBW
0000000F38	0000000F38	HintName RVA	028A GlobalFree
0000000F3C	0000000F3C	HintName RVA	0520! InterPrivateRwStringA
0000000F40	0000000F40	HintName RVA	01C1 GetProcAddress
0000000F44	0000000F44	HintName RVA	0181 GetMemoryMask
0000000F48	0000000F48	HintName RVA	0282 GlobalAddAtomW
0000000F4C	0000000F4C	HintName RVA	0246 GetProcAddressW
0000000F50	0000000F50	HintName RVA	007A OpenFileMappingA
0000000F54	0000000F54	HintName RVA	0233 GetProcAddress
0000000F58	0000000F58	HintName RVA	0247 GetProcessIdCounters
0000000F62	0000000F62	HintName RVA	0540! IstrmA
0000000F66	0000000F66	HintName RVA	0275 IsThreadStopPnW
0000000F70	0000000F70	HintName RVA	0209 IsTraceBuffer
0000000F74	0000000F74	HintName RVA	0187 GetCommandLineW
0000000F78	0000000F78	HintName RVA	0203 HeapGetInformation
0000000F7C	0000000F7C	HintName RVA	0265 GetSystemInfo
0000000F80	0000000F80	HintName RVA	0400 SetSystemInformation
0000000F84	0000000F84	HintName RVA	01C0 GetCurrentProcess
0000000F88	0000000F88	HintName RVA	04D1! UnhandledExceptionFilter
0000000F92	0000000F92	HintName RVA	0045! SetUnhandledExceptionFilter
0000000F96	0000000F96	HintName RVA	0200! GetProcAddress
0000000F9A	0000000F9A	HintName RVA	00EA! EncodePointer
0000000F9E	0000000F9E	HintName RVA	00CA! DecodePointer
0000000F9F	0000000F9F	HintName RVA	0304! IsProcessFeaturePresent
0000000FAC	0000000FAC	HintName RVA	0408! GetSystemPowerSetting
0000000FAD	0000000FAD	HintName RVA	0339! LeaveCriticalSection
0000000FAB	0000000FAB	HintName RVA	0219! GetModuleHandleW
0000000FAC	0000000FAC	HintName RVA	0119! ExitProcess



MUESTRA 7:

58 de 72

Microsoft: "Trojan:Win32/Ulise!MSR"

GData: "Gen:Variant.Ransom.Avaddon.2"

Basic Properties ⓘ

MD5	1d71701e9824c730dffbcacf428a2f64
SHA-1	cfae85cd6b410c2605fc5b0149ed1a07ff3dc9e3
SHA-256	4f198228806c897797647eecce0f92d4082476b82781183062a55c417c0bb197
Vhash	016046655d156173z12z92z23z8065z23z21z71z67z
Authentihash	15b9299faf9cd57c08fb1af12ac8e8592e299ffede32be6e4cba4c9761f1880d
Imphash	1156e59d43883136ef73eee451e94e3d
Rich PE header hash	1f751e2aac4a31991712f656456c5442
SSDEEP	24576:Cs6JmdFn5KLOCgHWcAvcrOcEsKfR9uA7rmFbbbbpcf:Cs6JY5KLOCyWcDUfRAA3mFbbbbpc4
TLSH	T1D7358D3DB4E1C071C73000F05998B7B2996EA9D2CB7204C77B8C9A9B1BB15D9A9375B3
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win16 NE executable (generic) (42.3%)
TrID	Win32 Dynamic Link Library (generic) (19.8%)
TrID	Win32 Executable (generic) (13.5%)
TrID	OS/2 Executable (generic) (6.1%)
TrID	Win64 Executable (generic) (6%)
File size	1.03 MB (1078784 bytes)

History ⓘ

Creation Time	2020-06-03 09:47:22 UTC
First Submission	2020-06-09 15:09:35 UTC
Last Submission	2020-06-09 15:09:35 UTC
Last Analysis	2020-10-31 22:07:46 UTC

Network Communication ⓘ

HTTP Requests

- + <http://ocsp.digicert.com/MFEwTzBNMEswSTAjBgUrDgMCGgUABBTBL0v27RVZ7Lbduom%2FrYB45SPUEwQU5Z1ZMIJHWMy%2BghUNoZ7OrUETfACEAo3h2ReX7SMIk79G%2B0UDDw%3D>
- + <http://ocsp.digicert.com/MFEwTzBNMEswSTAjBgUrDgMCGgUABBTBL0v27RVZ7Lbduom%2FrYB45SPUEwQU5Z1ZMIJHWMy%2BghUNoZ7OrUETfACEAo3h2ReX7SMIk79G%2B0UDDw%3D>

DNS Resolutions

- + [ocsp.digicert.com](#)
- + [MyPC](#)
- + [api.myip.com](#)
- + [wpad](#)

IP Traffic

172.67.208.45:443 (TCP)

File System Actions ⓘ

Files With Modified Attributes

C:\ed036e30937cf83f102d52b5e239\update\kb893803v2_wxp.cat
C:\MSOCache\All Users\{90140000-0115-0409-0000-0000000FF1CE}-C\OfficeLR.cab
C:\Users\Lucas\Desktop\SBS_consent_example_new.doc
C:\ae3344fb8ad85fd283a4b243471b71\update\update_wxp.inf
C:\Users\Lucas\Desktop\Unit 5 Practice Problems - Raphaels (key).docx
C:\ed036e30937cf83f102d52b5e239\update\kb893803v2_w2k.cat
C:\MSOCache\All Users\{90140000-00A1-0409-0000-0000000FF1CE}-C\OnoteLR.cab
C:\Users\Lucas\Desktop\WEF_Future_of_Jobs.pdf
C:\eula.1040.txt
C:\MSOCache\All Users\{90140000-0018-0409-0000-0000000FF1CE}-C\PowerPointMUI.msi

▼

Registry Actions ⓘ

Registry Keys Set

- + HKLM\SOFTWARE\WOW6432NODE\Microsoft\SystemCertificates\AuthRoot\Certificates\f5C27CF5FFF3029ACF1A1A4BEC7EE1964C77D784
- + HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\RestartManager\Session0001
- + HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\RestartManager\Session0001
- + HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\RestartManager\Session0000
- + HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\RestartManager\Session0001
- + HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\RestartManager\Session0000
- + HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\RestartManager\Session0000
- + HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\RestartManager\Session0000
- + HKLML\Software\WOW6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates\3913853E45C439A2DA718CDFB0F3E033E04FEE71
- + HKLML\Software\WOW6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates\5F3B8CF2F810B37D78B4CEEC1919C37334B9C774
- + HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Classes\Local Settings\muicache\{E6152C64B7E

▼

Registry Keys Deleted

- HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\Windows\CurrentVersion\Internet Settings\WPAD\{52-55-0A-00-02_52-56-00-00-02
- HKLM\Software\WOW6432Node\Microsoft\SystemCertificates\Root\Certificates
- HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\Windows\CurrentVersion\Internet Settings\WPAD\{3903E592-516A-4628-BD5F-B2BE4E7A24D
- HKLM\Software\WOW6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates
- HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\RestartManager\Session0000
- HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\RestartManager\Session0001
- HKU\S-1-5-21-3712457824-2419000099-45725732-1005\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- HKLM\Software\Microsoft\SystemCertificates\Root\Certificates
- HKLM\Software\Microsoft\SystemCertificates\AuthRoot\Certificates

Process And Service Actions ⓘ

Processes Created

```
C:\Users\Lucas\AppData\Local\Temp\EGtPWVqhtecTqHto94D.exe  
C:\Windows\SysWOW64\Wbem\wmic.exe  
C:\Windows\SysWOW64\vssadmin.exe  
C:\Users\Lucas\AppData\Roaming\EGtPWVqhtecTqHto94D.exe  
C:\Users\Lucas\AppData\Local\Temp\1d71701e9824c730dffbcacf428a2fnalysis_subject.exe  
C:\Users\Lucas\AppData\Roaming\1d71701e9824c730dffbcacf428a2fnalysis_subject.exe
```

Shell Commands

```
C:\Users\Lucas\AppData\Local\Temp\EGtPWVqhtecTqHto94D.exe  
wmic.exe SHADOWCOPY /nointeractive  
vssadmin.exe Delete Shadows /All /Quiet  
C:\Users\Lucas\AppData\Roaming\EGtPWVqhtecTqHto94D.exe  
C:\Users\Lucas\AppData\Local\Temp\1d71701e9824c730dffbcacf428a2fnalysis_subject.exe  
C:\Users\Lucas\AppData\Roaming\1d71701e9824c730dffbcacf428a2fnalysis_subject.exe
```

Processes Tree

```
↳ 2984 - C:\Users\Lucas\AppData\Local\Temp\EGtPWVqhtecTqHto94D.exe  
↳ 1808 - C:\Windows\SysWOW64\Wbem\wmic.exe  
↳ 2376 - C:\Windows\SysWOW64\vssadmin.exe  
↳ 2092 - C:\Windows\SysWOW64\Wbem\wmic.exe  
↳ 2908 - C:\Windows\SysWOW64\vssadmin.exe  
↳ 1168 - C:\Windows\SysWOW64\Wbem\wmic.exe  
↳ 2580 - C:\Windows\SysWOW64\vssadmin.exe  
↳ 2560 - C:\Users\Lucas\AppData\Roaming\EGtPWVqhtecTqHto94D.exe
```

Synchronization Mechanisms & Signals ⓘ

Mutexes Created

Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0000

Local\RstrMgr-3887CAB8-533F-4C85-B0DC-3E5639F8D511-Session0001

RasPbFile

LocalZonesLockedCacheCounterMutex

{2A0E9C7B-6BE8-4306-9F73-1057003F605B}

Local\RstrMgr3887CAB8-533F-4C85-B0DC-3E5639F8D511

LocalZonesCacheCounterMutex

Mutexes Opened

{2A0E9C7B-6BE8-4306-9F73-1057003F605B}

Modules Loaded ⓘ

Runtime Modules

c:\windows\system32\imm32.dll

c:\windows\system32\rutil.dll

c:\windows\syswow64\schannel.dll

c:\windows\syswow64\urlmon.dll

c:\windows\syswow64\usp10.dll

c:\windows\system32\rportremote.dll

c:\windows\system32\napinsp.dll

c:\windows\system32\apphelp.dll

c:\windows\syswow64\gdi32.dll

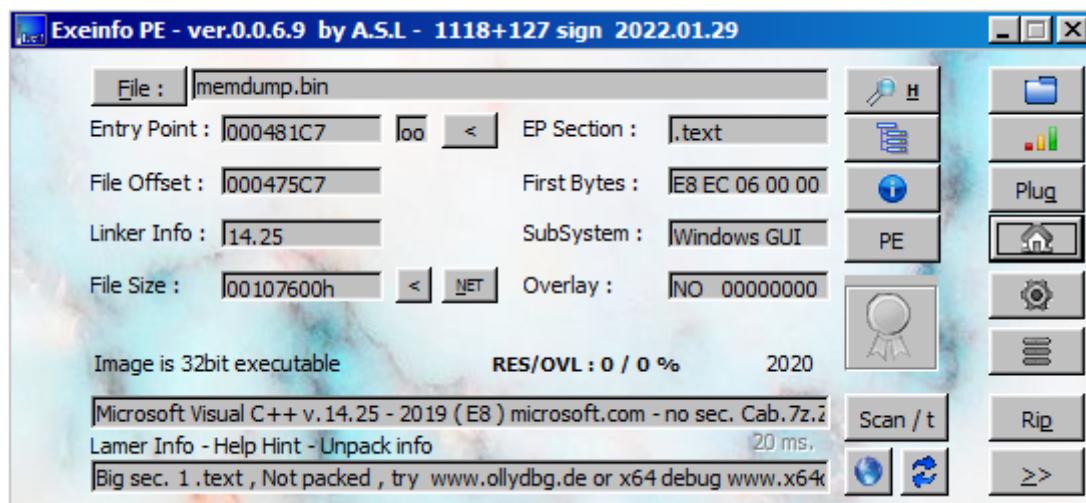
c:\windows\system32\dhcpsvc.dll

▼

```
=====
Filename      : memdump.bin
MD5          : 1d71701e9824c730dffbaef428a2f64
SHA1         : cfae85cd6b410c2605fc5b0149ed1a07ff3dc9e3
CRC32        : 9b47abde
SHA-256       : 4f198228806c897797647eecc0f92d4082476b82781183062a55c417c0bb197
SHA-512       : 511d4c8f44a9467f901cbd085bcc0bf9d96ed2a0ad7e924ab955b56b0d3c1df5fb5eb3341dbe8856c04cbcd99fa98c6bc32156765d922ef84e5215d8769d91
SHA-384       : 1ef2366edd23e07a6a2bc27004507df6ac59fd3ac0f49d00a00e0b91ce148e6fa029d12f9e9b5d1e5a24d11d61a1af
Full Path     : C:\Users\IEUser\Downloads\Avaddon\Avaddon7\memdump.bin\memdump.bin
Modified Time : 5/23/2022 11:10:34 AM
Created Time   : 5/23/2022 11:12:13 AM
Entry Modified Time: 5/23/2022 11:12:13 AM
File Size      : 1,078,784
File Version   :
Product Version:
Identical      :
Extension      : bin
File Attributes: A
=====
```


S:\PView C:\Users\Uther\Downloads\Avaddon\Avaddon7\memdump.bin\memdump.bin

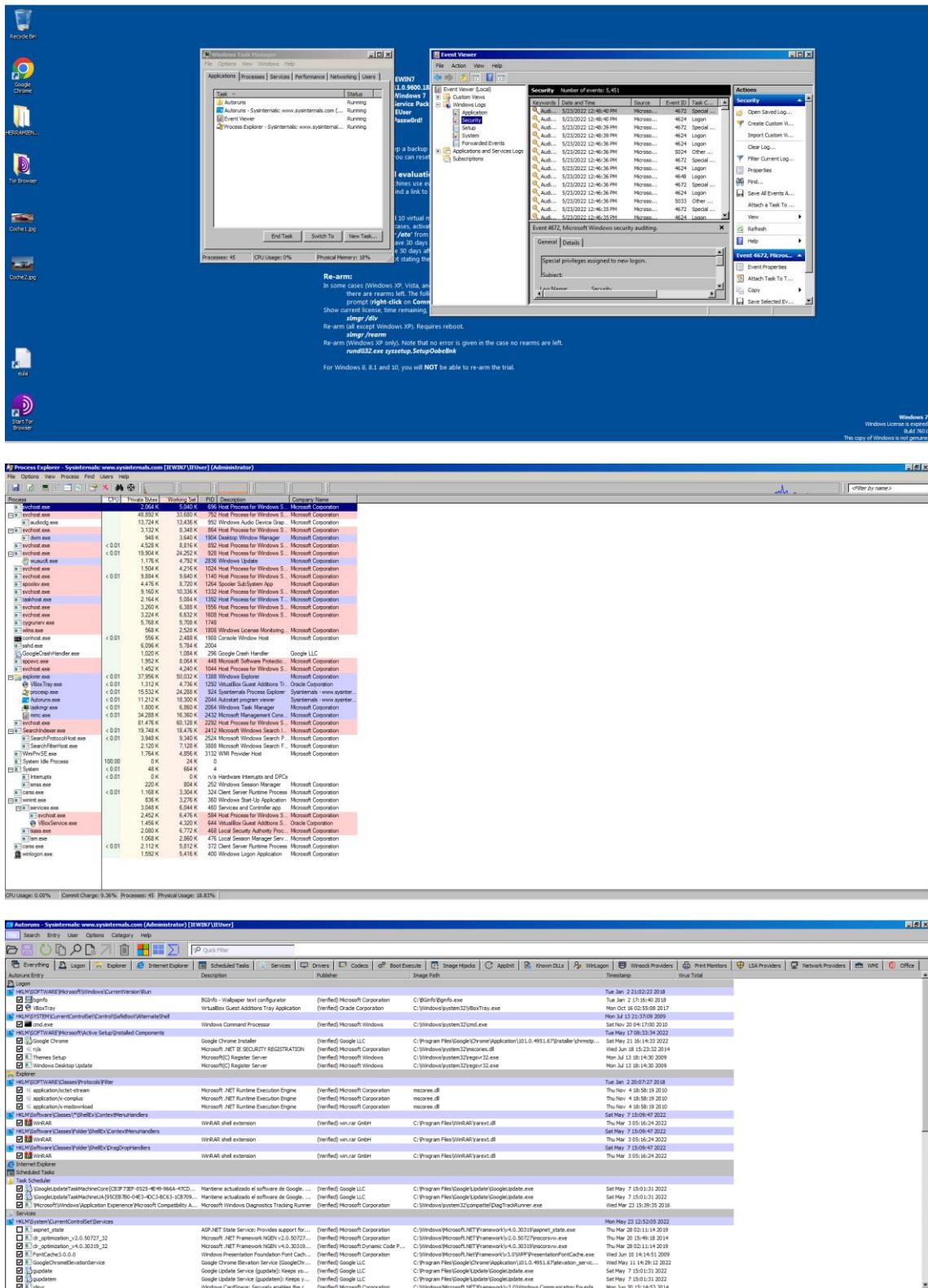
pFile	Data	Description	Value
IMAGE_DOS_HEADER	000F5000 00000000	Time Name Table RVA	
IMAGE_DOS_HEADER	000F5000 00000000	Time Date Stamp	
MS-DOS Sub Program	000F500C 00000000	Forwarder Chain	
IMAGE_NT_HEADERS	000F5010 000F7006	Name RVA	KERNEL32.dll
Signature	000F5014 00000000	Import Address Table RVA	
IMAGE_FILE_HEADER	000F5016 000F6024	Import Name Table RVA	
IMAGE_OPTIONAL_HEADER	000F501C 00000000	Time Date Stamp	
IMAGE_SECTION_HEADER .text	000F5020 00000000	Forwarder Chain	
IMAGE_SECTION_HEADER .rdata	000F5024 000F7100	Name RVA	USER32.dll
IMAGE_SECTION_HEADER .data	000F5028 00000000	Import Address Table RVA	
IMAGE_SECTION_HEADER .idata	000F502C 000F6A1C	Import Name Table RVA	
SECTION .text	000F5030 00000000	Time Date Stamp	
SECTION .idata	000F5034 00000000	Forwarder Chain	
IMAGE_DEBUG_DIRECTORY	000F5038 000F72CC	Name RVA	ADVAPI32.dll
IMAGE_LOAD_CONFIG_DIRECTORY	000F5040 00000000	Import Address Table RVA	
IMAGE_TLS_DIRECTORY	000F5044 00000000	Time Date Stamp	
IMAGE_DEBUG_TYPE	000F5048 00000000	Forwarder Chain	
IMAGE_RESOURCE自如	000F504C 00000000	Import Address Table RVA	
IMPORT Name Table	000F5050 00000000	Import Name Table RVA	
IMPORT Hint/Names & DLL Names	000F5054 00000000	Time Date Stamp	
SECTION .data	000F5058 00000000	Forwarder Chain	
SECTION .reloc	000F505C 00000000	Name RVA	OLEAUT32.dll
	000F5060 00000000	Import Address Table RVA	
	000F5064 00000000	Import Name Table RVA	
	000F5068 00000000	Time Date Stamp	
	000F5070 00000000	Forwarder Chain	
	000F5074 00000000	Name RVA	
	000F5078 00000000	Import Address Table RVA	
	000F507C 00000000	Import Name Table RVA	
	000F5080 00000000	Time Date Stamp	
	000F5084 00000000	Forwarder Chain	
	000F5088 00000000	Name RVA	MPR.dll
	000F5090 00000000	Import Address Table RVA	
	000F5094 00000000	Import Name Table RVA	
	000F5098 00000000	Time Date Stamp	
	000F509C 00000000	Forwarder Chain	
	000F50A0 00000000	Name RVA	NETAPI32.dll
	000F50B0 00000000	Import Address Table RVA	
	000F50A4 00000000	Import Name Table RVA	
	000F50A8 00000000	Time Date Stamp	
	000F50AC 00000000	Forwarder Chain	
	000F50B0 000F7418	Name RVA	IPHLPAPI.dll



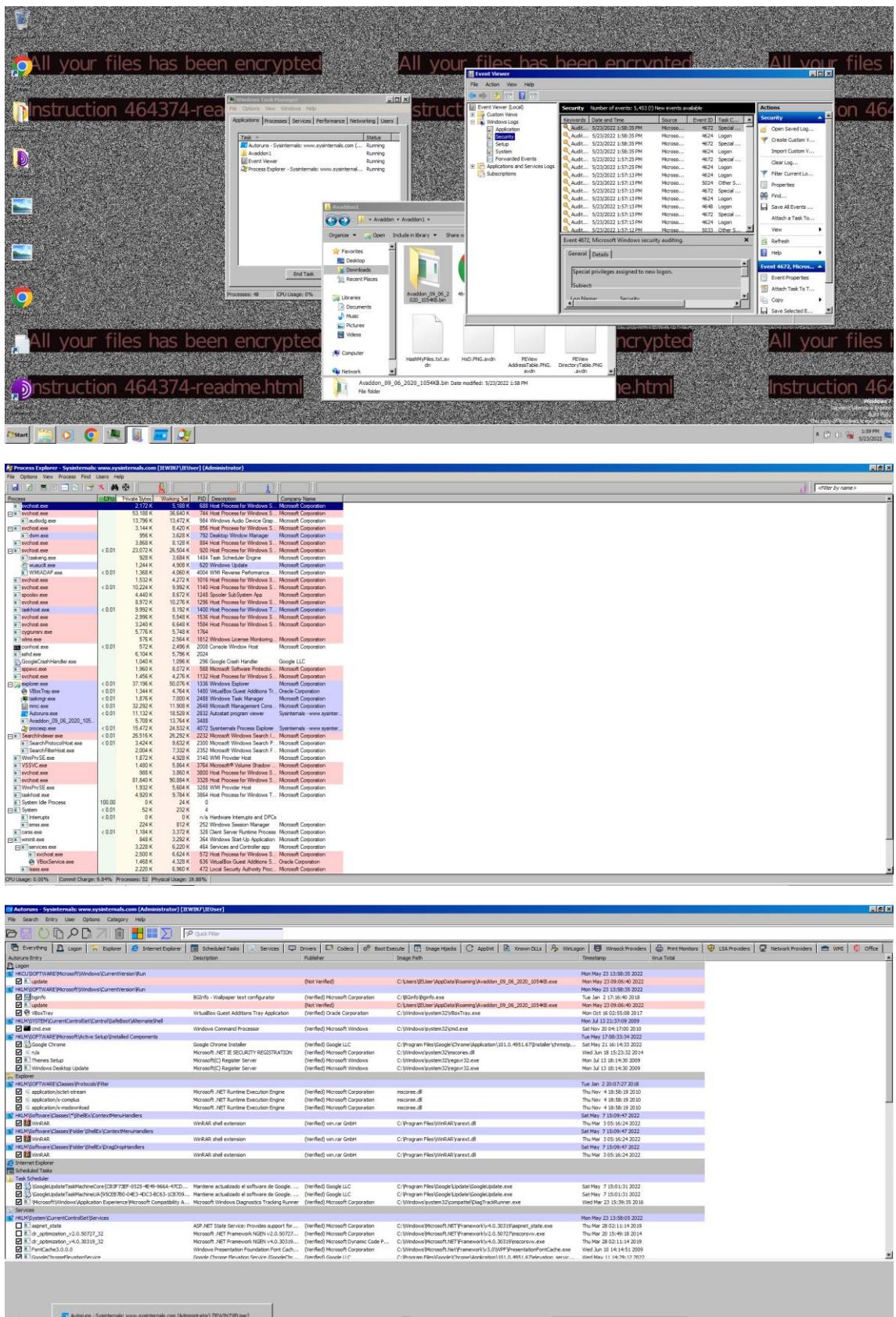
ANALISIS DINAMICO:

Iniciamos los programas “Process Explorer” y “Autoruns”, y los servicios “Visor de eventos” y el “Administrador de Tareas”, ya que nos permitirán observar los procesos y servicios que se están ejecutando antes de realizar un análisis.

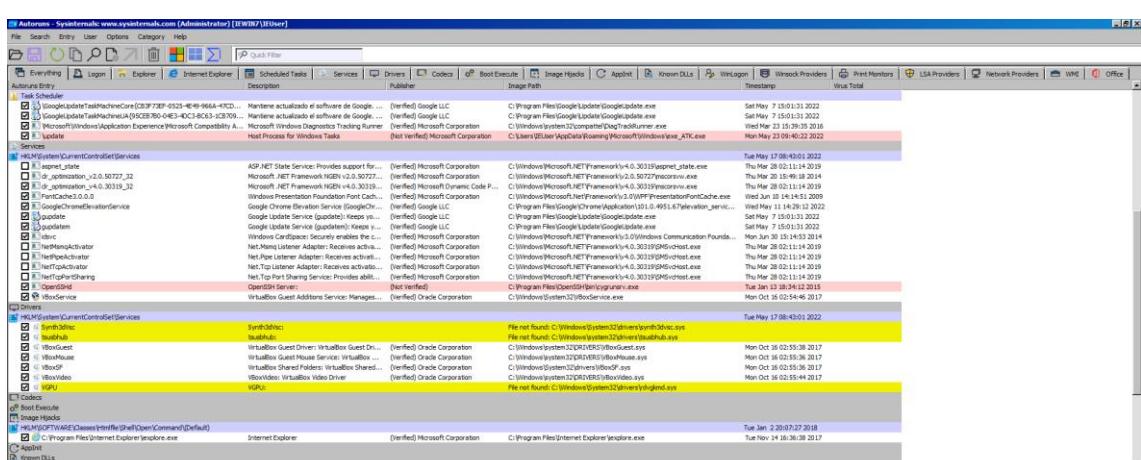
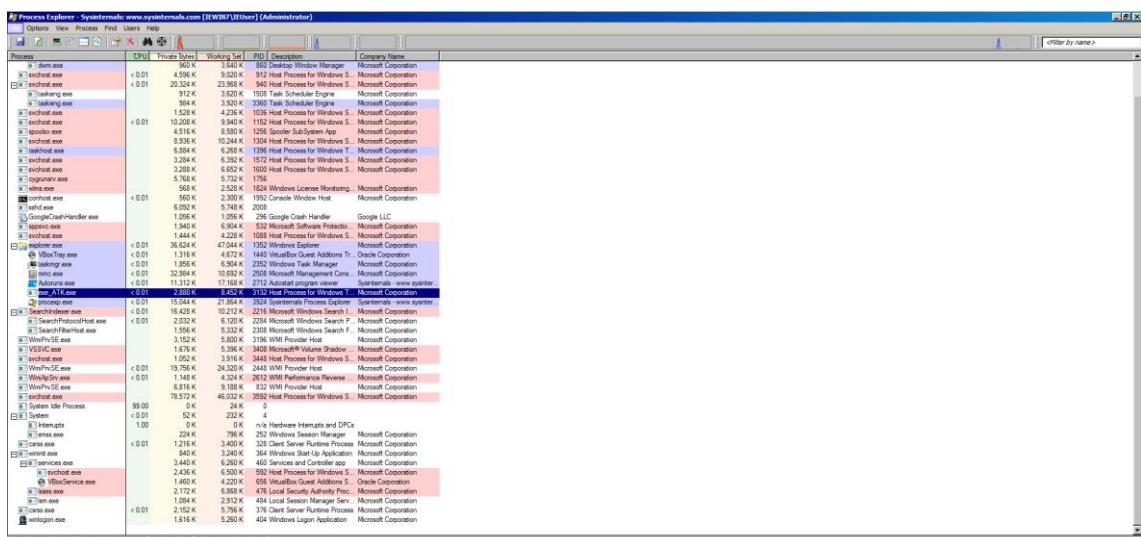
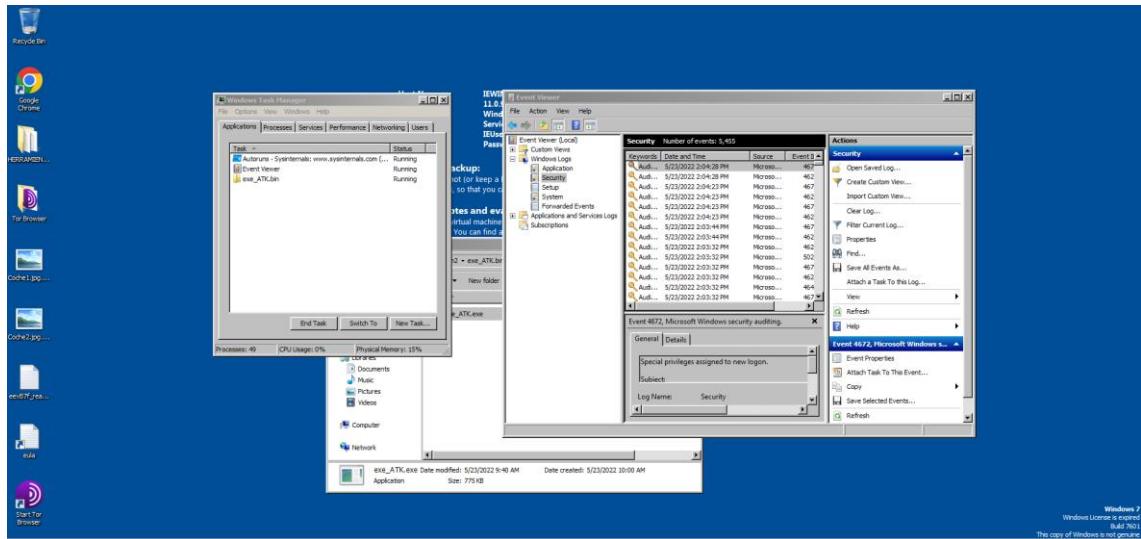
Al iniciar una “snapshot” de la máquina virtual, siempre serán los mismos procesos y servicios los que se iniciaran, por lo que solamente lo comprobaremos una vez.



MUESTRA 1:



MUESTRA 2:



The screenshot shows a Windows desktop with several icons on the desktop and two open windows. The top window is a ransomware message titled 'evnW7 ransom_1.txt - Notepad' containing a long string of encrypted file names and a warning message. The bottom window is the Windows Event Viewer titled 'Event Viewer (Local)' showing a list of security events from the 'Security' log.

```

----- YOUR network has been infected! -----
----- DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED -----  

All your documents, photos, databases and other important files have been encrypted and have the extension: .adCBaCCac  

You are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!  

The only way to restore your files is to buy our special software, only we can give you this software and only we can restore your files!  

We have also downloaded a lot of private data from your network.  

If you do not contact us in a 3 days we will post information about your breach on our public news website (avaddonung/rngel.onion) and after 7 days the whole downloaded info.  

You can get more information on our page, which is located in a Tor hidden network.  

How to get to our page  

1. Download Tor browser - https://www.torproject.org/  

2. Install Tor browser  

3. open file in Tor browser - avaddonung/rngel.onion  

4. Follow the instructions on this page  

Your ID:  

-----  

-----  

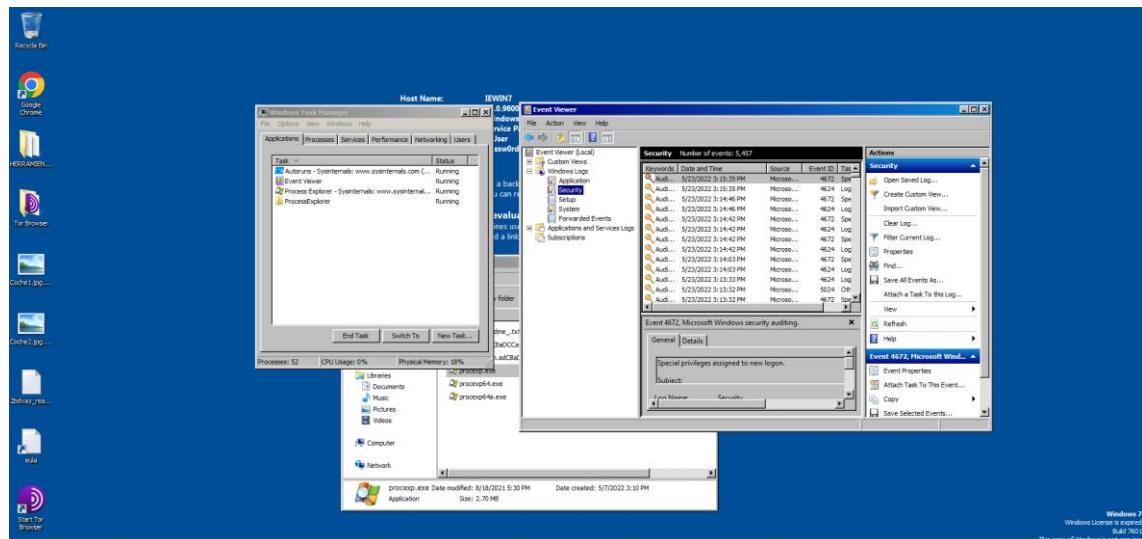
----- DO NOT TRY TO RECOVER FILES YOURSELF!  

----- DO NOT MODIFY ENCRYPTED FILES!  

----- OTHERWISE, YOU MAY LOSE ALL YOUR FILES FOREVER! * * *ZB

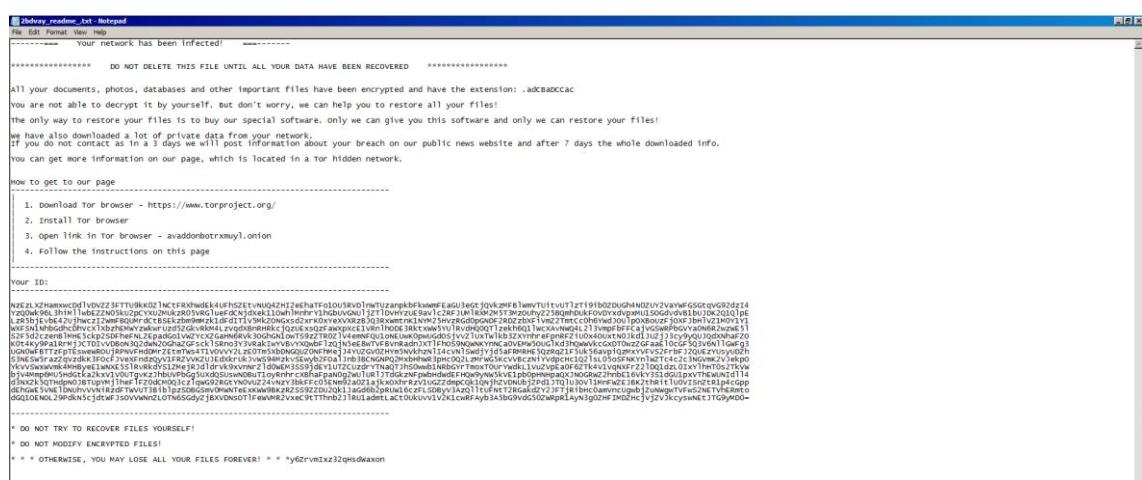
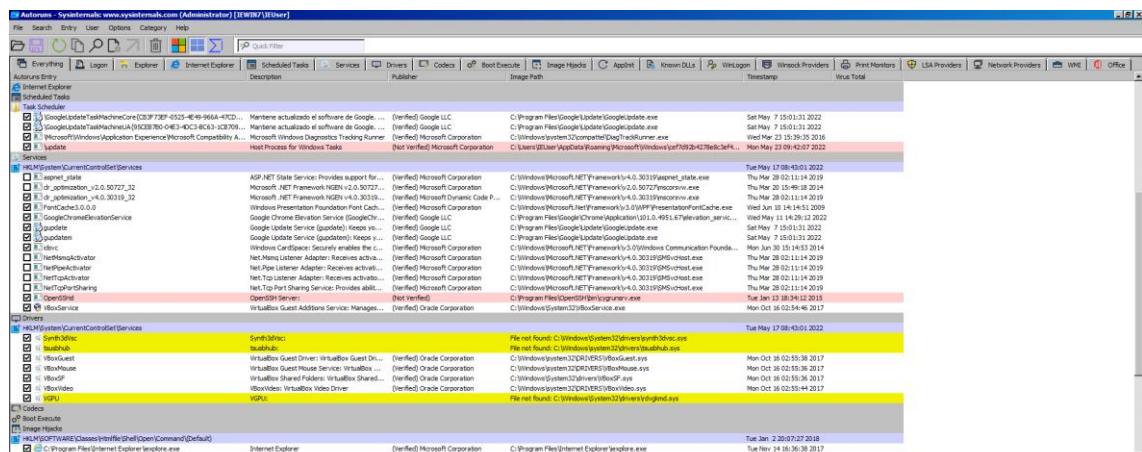
```

MUESTRA 3:

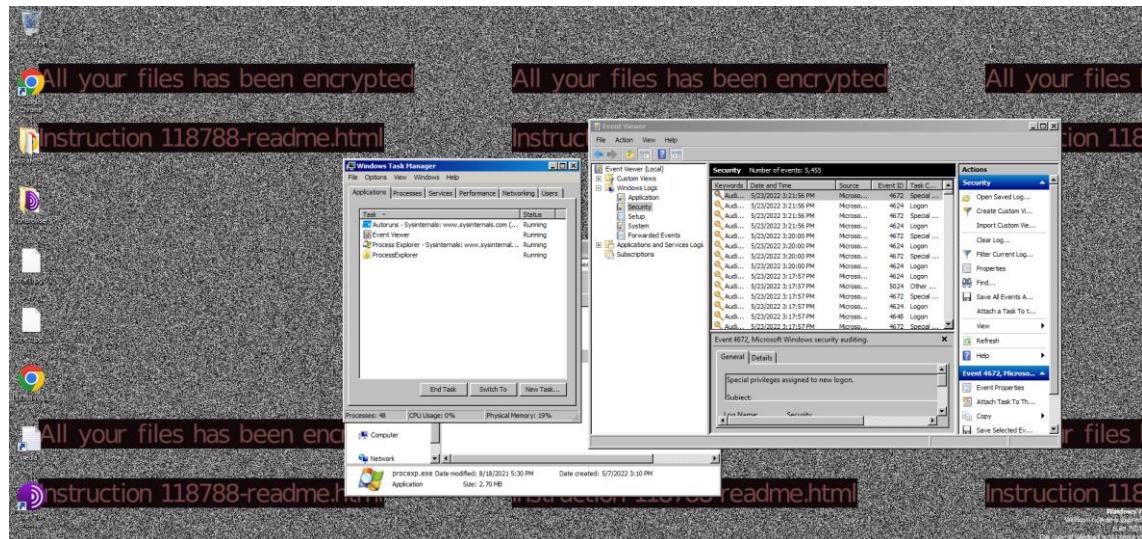


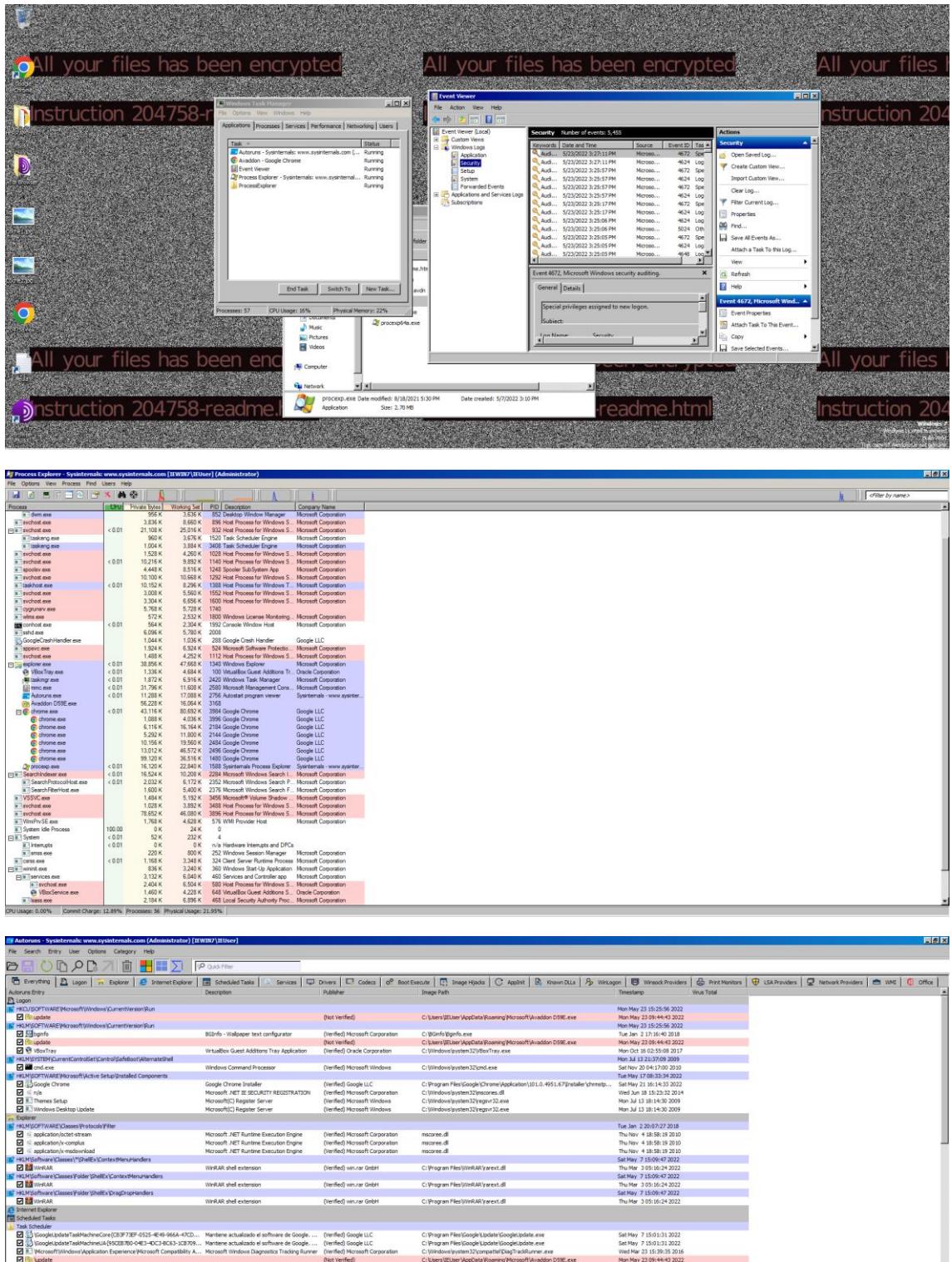
The screenshot shows a Windows desktop with several icons. Two windows are open: 'Process Explorer' (by Sysinternals) and 'Task Manager'. The Process Explorer window lists numerous processes, many of which are highlighted in red. The Task Manager window shows a list of running tasks.

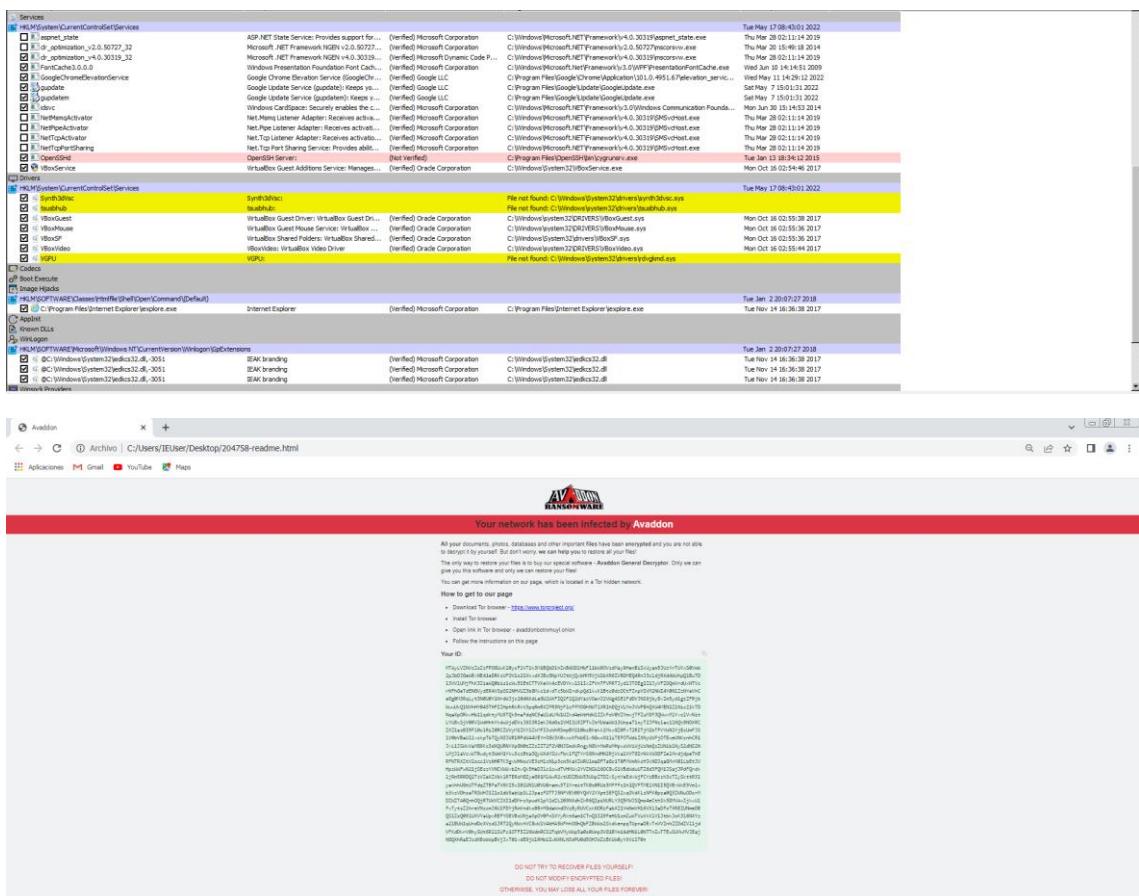
Process	CPU	Private Bytes	Working Set	RID	Description	Company Name
wchan.exe	< 0.01	2,344 K	5,300 K	704	Host Process for Windows S.	Microsoft Corporation
audiodg.exe	< 0.01	13,780 K	13,480 K	1,004	Windows Audio Device Obj.	Microsoft Corporation
evnW7.exe	< 0.01	3,244 K	8,576 K	876	Host Process for Windows S.	Microsoft Corporation
explorer.exe	< 0.01	9,708 K	9,696 K	904	Host Process for Windows S.	Microsoft Corporation
evnW7.exe	< 0.01	4,676 K	8,956 K	904	Host Process for Windows S.	Microsoft Corporation
taskhost.exe	< 0.01	19,016 K	21,448 K	940	Host Process for Windows S.	Microsoft Corporation
TaskSch.exe	< 0.01	304 K	304 K	948	Task Scheduler Engine	Microsoft Corporation
TaskHost.exe	< 0.01	1,396 K	4,125 K	1,058	Task Host	Microsoft Corporation
TaskHost.exe	< 0.01	1,096 K	4,008 K	1,058	Task Host	Microsoft Corporation
TaskHost.exe	< 0.01	10,196 K	10,192 K	1,152	Host Process for Windows S.	Microsoft Corporation
TaskHost.exe	< 0.01	4,404 K	8,804 K	1,354	SystemBackground App	Microsoft Corporation
TaskHost.exe	< 0.01	8,936 K	9,540 K	1,354	Processor Driver	Microsoft Corporation
taskhost.exe	< 0.01	3,944 K	6,296 K	1,396	Host Process for Windows T.	Microsoft Corporation
TaskHost.exe	< 0.01	3,776 K	6,112 K	1,396	Host Process for Windows S.	Microsoft Corporation
TaskHost.exe	< 0.01	3,002 K	6,116 K	1,416	Host Process for Windows S.	Microsoft Corporation
taskhost.exe	< 0.01	6,760 K	7,724 K	1,608	Windows Processes License Monitor	Microsoft Corporation
TaskHost.exe	< 0.01	564 K	2,724 K	1,608	Windows Processes License Monitor	Microsoft Corporation
TaskHost.exe	< 0.01	272 K	2,398 K	1,608	Windows Processes License Monitor	Microsoft Corporation
sndvol32.exe	< 0.01	6,120 K	5,780 K	1,252	Sound Class Handler	Google LLC
GoogleCrashHandler.exe	< 0.01	1,024 K	5,884 K	1,252	Google Crash Handler	Google LLC
SearchProtocolHost.exe	< 0.01	1,384 K	6,188 K	2,048	Search Protocol Host	Microsoft Corporation
TaskHost.exe	< 0.01	1,490 K	4,724 K	1,088	Host Process for Windows S.	Microsoft Corporation
regedit.exe	< 0.01	36,200 K	47,948 K	1,138	Windows Registry Editor Tr. & Services	Microsoft Corporation
TaskHost.exe	< 0.01	1,520 K	4,732 K	1,138	Windows Task Manager	Microsoft Corporation
taskhost.exe	< 0.01	1,840 K	6,808 K	2,192	Windows Task Manager	Microsoft Corporation
mmc.exe	< 0.01	2,156 K	10,988 K	10,988	Microsoft Management Cons.	Microsoft Corporation
offf93d427e8c3ef404af3.exe	< 0.01	1,157 K	3,900 K	10,440	3,180 Host Process for Windows T.	Microsoft Corporation
process.exe	74.00	15,020 K	21,688 K	3172	Systematic Process Explorer	Systecher - www.syster...
TaskHost.exe	< 0.01	5,024 K	17,520 K	17,520	Windows Task Host	Microsoft Corporation
SearchProtocolHost.exe	< 0.01	2,004 K	6,188 K	2,048	Search Protocol Host	Microsoft Corporation
SearchProtocolHost.exe	< 0.01	1,604 K	5,360 K	2,048	Windows Search F.	Microsoft Corporation
TaskHost.exe	< 0.01	1,704 K	6,296 K	2,048	Windows Task Host	Microsoft Corporation
evnW7.exe	< 0.01	1,108 K	3,936 K	2,128	Host Process for Windows S.	Microsoft Corporation
WinPvSE.exe	< 0.01	19,888 K	24,364 K	2,544	WMI Provider Host	Microsoft Corporation
TaskHost.exe	< 0.01	1,724 K	4,192 K	2,560	Windows Task Host	Microsoft Corporation
WinPvSE.exe	< 0.01	1,608 K	4,336 K	2,576	WMI Provider Host	Microsoft Corporation
WinPvSE.exe	< 0.01	6,820 K	9,208 K	2,576	WMI Provider Host	Microsoft Corporation
TaskHost.exe	< 0.01	4 K	0 K	0	n/a	
System	< 0.01	48 K	232 K	0	n/a	
vlan.exe	< 0.01	0 K	0 K	0	n/a	
TaskHost.exe	< 0.01	220 K	2,708 K	2,708	Windows Session Manager	Microsoft Corporation
CoreUI.exe	< 0.01	1,156 K	3,328 K	3,328	Client Server Process	Microsoft Corporation
wininit.exe	< 0.01	828 K	3,232 K	364	Windows Start-Up Application	Microsoft Corporation
TaskHost.exe	< 0.01	2,404 K	6,296 K	6,296	TaskHost	Microsoft Corporation
TaskHost.exe	< 0.01	2,592 K	6,652 K	6,592	Host Process for Windows S.	Microsoft Corporation
VBoxService.exe	< 0.01	1,468 K	4,228 K	6,592	VirtualBox Guest Additions S.	Oracle Corporation
TaskHost.exe	< 0.01	2,108 K	6,736 K	6,736	TaskHost	Microsoft Corporation
TaskHost.exe	< 0.01	1,078 K	2,332 K	494	Local Session Manager Serv.	Microsoft Corporation
TaskHost.exe	< 0.01	2,316 K	5,908 K	376	Client Server Runtime Process	Microsoft Corporation



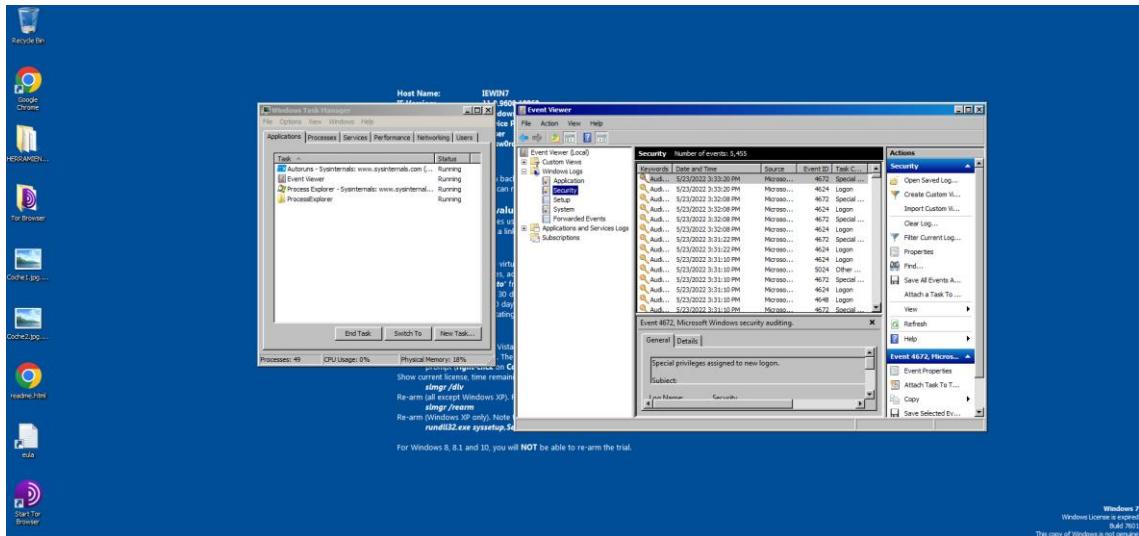
MUESTRA 4:

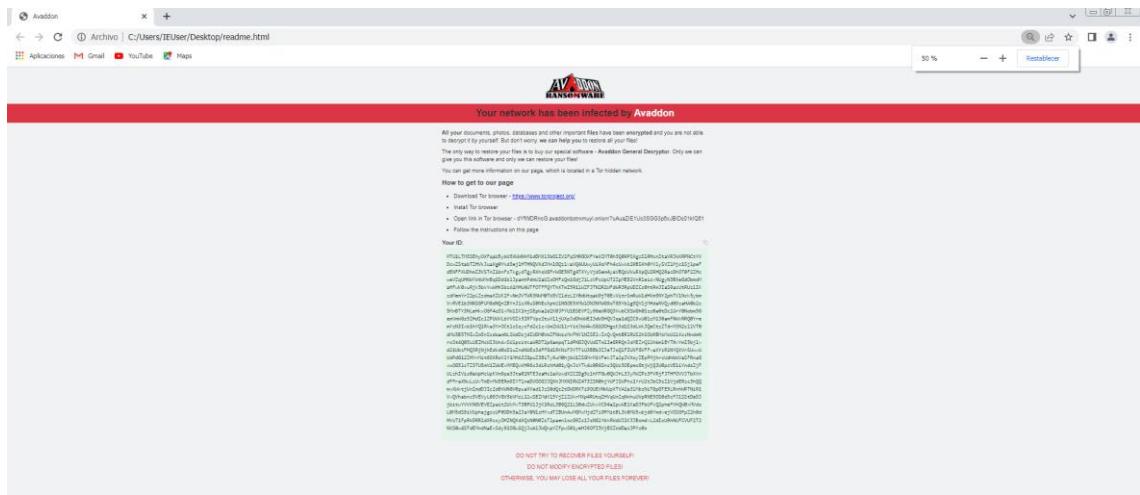




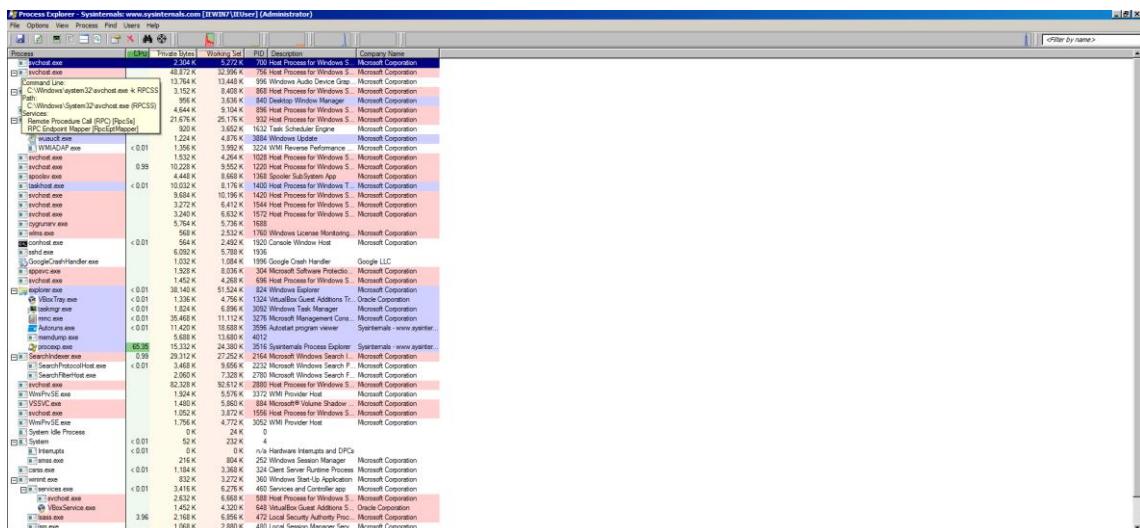
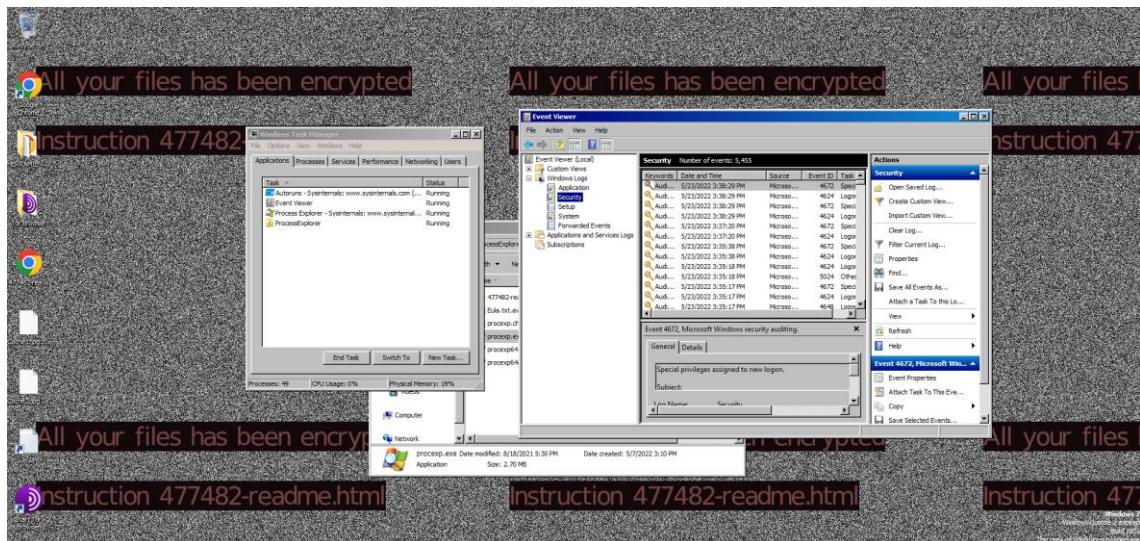


MUESTRA 6:





MUESTRA 7:



The screenshot shows the Autoruns interface under the Windows tab. It lists several running processes:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**:
 - update (Not Verified) - C:\Users\ElUser\AppData\Roaming\Imendump.exe
 - update (Not Verified) - C:\Windows\Win32\Imendump.exe
 - update (Not Verified) - C:\Windows\Win32\Imendump.exe
 - update (Not Verified) - C:\Windows\system32\BoxTray.exe
 - update (Not Verified) - C:\Windows\system32\BoxTray.exe
- HKEY_CURRENT_USER\Software\Microsoft\Active Setup\Installed Components**:
 - Google Chrome Installer (Verified) Microsoft LLC - C:\Program Files\Google\Chrome\Application\101.0.4951.67\Installer\chromep... Set Nov 20 17:00 2010
 - Microsoft .NET SECURITY REGISTRATION (Verified) Microsoft Corporation - C:\Windows\system32\resolv.dll Set Mar 20 16:19 2022
 - Micros(R) Register Service (Verified) Microsoft Corporation - C:\Windows\system32\regn32.exe Mon Jul 13 16:30 2009
 - Micros(R) Windows Desktop Update (Verified) Microsoft Corporation - C:\Windows\system32\regn32.exe Mon Jul 13 16:30 2009
- HKEY_CURRENT_USER\Software\Classes\ProtocolFilter**:
 - application/octet-stream (Verified) Microsoft Corporation - resolv.dll Tue Jan 2 20:07:27 2018
 - Microsoft .NET Runtime Executive Engine (Verified) Microsoft Corporation - resolv.dll Thu Nov 4 18:58:19 2010
 - application/x-pkcs12 (Verified) Microsoft Corporation - resolv.dll Thu Nov 4 18:58:19 2010
 - application/msword (Verified) Microsoft Corporation - resolv.dll Thu Nov 4 18:58:19 2010
- HKEY_CURRENT_USER\Software\Classes*\ShellEx\ContextMenuHandlers**:
 - winRAR (Verified) winrar GmbH - C:\Program Files\winRAR\yarext.dll Set Mar 18 15:32:32 2014
 - winRAR (Verifier) winrar GmbH - C:\Program Files\winRAR\yarext.dll Thu Mar 18 15:32:32 2014
 - winRAR (DragOrchestrator) (Verifier) winrar GmbH - C:\Program Files\winRAR\yarext.dll Set Mar 18 15:32:32 2014
 - winRAR (DragOrchestrator) (Verifier) winrar GmbH - C:\Program Files\winRAR\yarext.dll Thu Mar 18 15:32:32 2014
- Scheduled Tasks**:
 - Task Scheduler (Verified) Microsoft Corporation - C:\Windows\system32\TaskScheduler\runonce.exe Set Mar 23 15:39:35 2016
- Services**:
 - HKEY_LOCAL_MACHINE\CurrentControlSet\Services**:
 - APC.NET Data Service Provider (Verified) Microsoft Corporation - C:\Windows\Microsoft.NET\Framework\v4.0.30319\msasn1.dll Tue May 17 08:43:01 2022
 - Intershop .NET Framework Host v4.0.30319_32 (Verified) Microsoft Corporation - C:\Windows\Microsoft.NET\Framework\v4.0.30319\msasn1.dll Thu Mar 20 11:34 2019
 - NET_optimization_v4.0.30319_32 (Verified) Microsoft Corporation - C:\Windows\Microsoft.NET\Framework\v4.0.30319\msasn1.dll Thu Mar 20 11:34 2019
 - NET_optimized (Verified) Microsoft Corporation - C:\Windows\Microsoft.NET\Framework\v4.0.30319\msasn1.dll Wed Jun 10 14:51 2009
 - Google Chrome Browser Service (Verified) Google LLC - C:\Program Files\Google\Chrome\Application\101.0.4951.67\leveldown_service... Set May 11 14:42 2022
 - Google Chrome Browser Service (Verified) Google LLC - C:\Program Files\Google\Chrome\Application\101.0.4951.67\leveldown_service... Set May 11 14:42 2022
 - Google Update Service (Updated) (Verified) Google LLC - C:\Program Files\Google\Update\update.exe Set May 7 15:01:31 2022
 - Windows CardSpace: Securely enables the c... (Verified) Microsoft Corporation - C:\Windows\Microsoft.NET\Framework\v3.0\Windows CardSpace\Windows CardSpace Foundation Set May 30 14:53:20 2014
 - Net_Port_Adapter_Adapter (Verified) Microsoft Corporation - C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSDNSHost.exe Thu Mar 28 11:14 2019
 - Net_Port_Adapter_Adapter (Verified) Microsoft Corporation - C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSDNSHost.exe Thu Mar 28 11:14 2019
 - Net_Port_Sharing (Verified) Microsoft Corporation - C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSDNSHost.exe Thu Mar 28 11:14 2019
 - OpenSSH (Verifier) (Verified) Microsoft Corporation - C:\Program Files\OpenSSH\OpenSSH.exe Set Mar 23 15:39:35 2016
 - VirtualBox Guest Services: Manager... (Verified) Oracle Corporation - C:\Windows\system32\VirtualBoxGuestService.exe Mon Oct 16 05:54:46 2017
 - VirtualBox Guest Services: Manager... (Verifier) Oracle Corporation - C:\Windows\system32\VirtualBoxGuestService.exe Mon Oct 16 05:54:46 2017
 - HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Network\NlaService**:
 - File net (Verifier) C:\Windows\System32\drivers\nla.dll Set May 17 08:43:01 2022
 - Drivers**:
 - HKEY_LOCAL_MACHINE\CurrentControlSet\Control\DeviceClass\{4D3B85F5-0A41-4A14-BD43-C3DCC5E4CD7E}**:
 - Network Adapter (Verifier) Intel Corporation - C:\Windows\system32\driver\x64\iwlwifi.ko+x64 File net Bind C:\Windows\system32\driver\x64\iwlwifi.ko+x64 Mon Oct 30 05:16:38 2017
 - VirtualBox Guest Driver: VirtualBox Guest Dr... (Verified) Oracle Corporation - C:\Windows\system32\DRIVERS\VirtualBoxGuest.sys Mon Oct 30 05:16:38 2017
 - VirtualBox Shared Folders: VirtualBox Shared... (Verified) Oracle Corporation - C:\Windows\system32\DRIVERS\VirtualBoxSF.sys Mon Oct 30 05:16:38 2017
 - VirtualBox Video: VirtualBox Video Driver (Verified) Oracle Corporation - C:\Windows\system32\DRIVERS\VirtualBoxVideo.sys Mon Oct 30 05:16:44 2017
 - VGPU (Verifier)
 - Applets**:
 - C:\Program Files\Internet Explorer\ieToolbar.exe (Internet Explorer) (Verified) Microsoft Corporation - C:\Program Files\Internet Explorer\ieToolbar.exe Tue Jan 2 20:07:27 2018
 - Known Folders**:
 - C:\Windows\Temporary Internet Files\Low (Default) (Verified) Microsoft Corporation - C:\Windows\Temporary Internet Files\Low Set Nov 14 10:36:38 2017
 - HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GdiExtensions**:
 - IEC\Windows\system32\edicas32.dll_3051 (IEAK branding) (Verified) Microsoft Corporation - C:\Windows\system32\edicas32.dll Tue Jan 2 20:07:27 2018
 - IEC\Windows\system32\edicas32.dll_3051 (IEAK branding) (Verified) Microsoft Corporation - C:\Windows\system32\edicas32.dll Tue Nov 14 10:36:38 2017
 - IEC\Windows\system32\edicas32.dll_3051 (IEAK branding) (Verified) Microsoft Corporation - C:\Windows\system32\edicas32.dll Tue Nov 14 10:36:38 2017
 - Windows PowerShell**

Avaddon browser window showing a warning message:

YOUR NETWORK HAS BEEN INFECTED BY AVADDON

All your documents, photos, databases and other important files have been encrypted and you are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!

The only way to restore your files is to buy our special software - Avaddon General Decrypter. Only we can give you this software and only we can restore your files!

You can get more information on our page, which is located in a Tor hidden network.

How to get to our page

 - Download Tor browser - <http://www.torproject.org>
 - Install Tor browser
 - Open link in browser - avaddonbot@mxul.onion
 - Follow the instructions on this page

Your ID: [REDACTED]

DO NOT TRY TO RECOVER FILES YOURSELF!
DO NOT MODIFY ENCRYPTED FILES!

CONCLUSION

Una vez ejecutadas las 7 muestras de Avaddon observamos que los comportamientos de los malware son parecidos como en el caso anteriormente estudiado.