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:

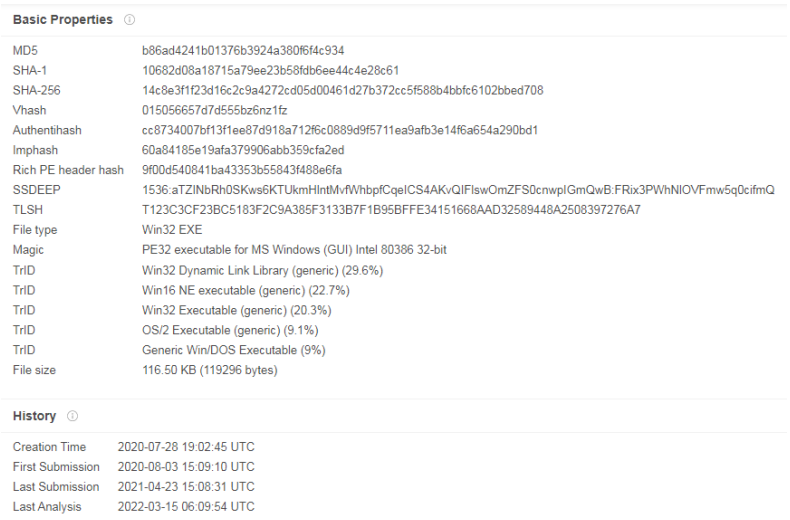
Nombre de la muestra	MD5	Primera vez subido a Virus Total	Nombre
REvil1	b86ad4241b01376b3924a380f6f4c934	03/08/2020	“Ransom:Win32/Revil.A”
REvil2	f0c97dcb65a030a214f6dd33cf4a8566	06/08/2019	“Ransom:Win32/Revil.B”
REvil3	21d01fa87dfcaf971ff7b63a1a6fda94	09/09/2021	“Ransom:Win32/Revil.A”
REvil4	ff0e2ce0af118bae62969a5e897b59b2	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.

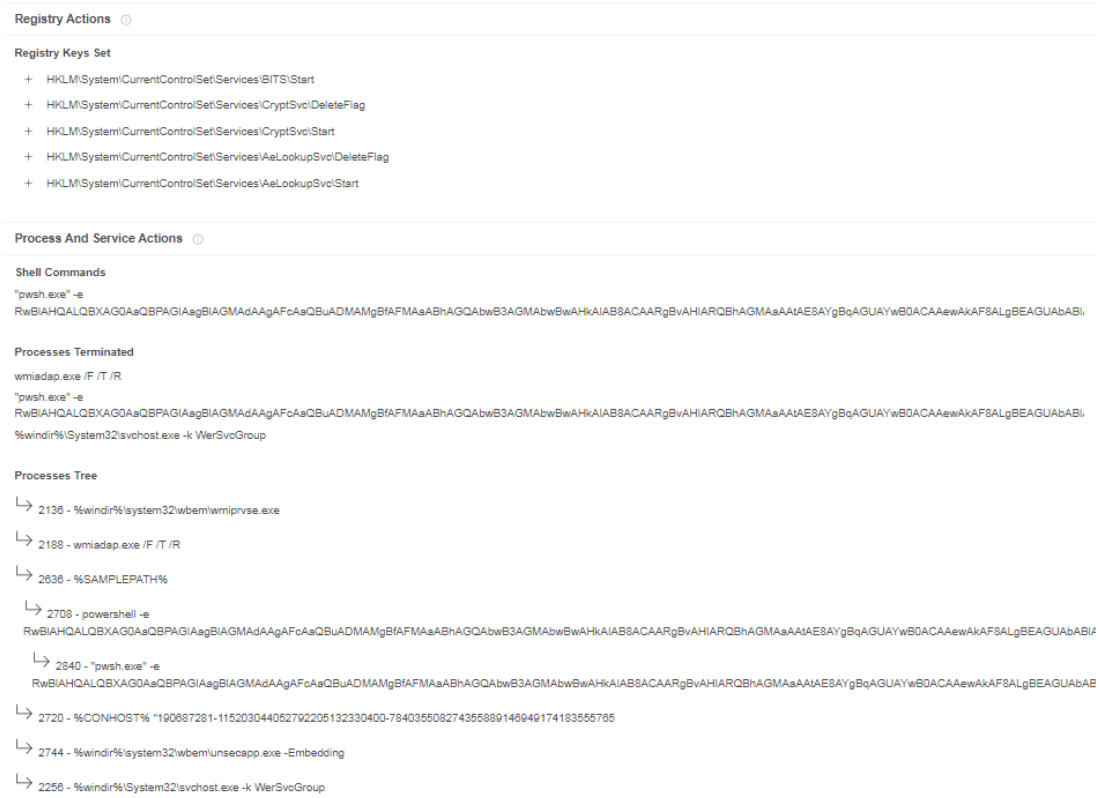


Basic Properties

MD5	b86ad4241b01376b3924a380f6f4c934
SHA-1	10682d08a18715a79ee23b58fdb6ee44c4e28c61
SHA-256	14c8e3f1f23d16c2c9a4272cd05d00461d27b372cc5f588b4bbfc6102bbed708
Vhash	015056657d7d555bz6nz1fz
Authentihash	cc8734007bf13f1ee87d918a712f6c0889d9f5711ea9afb3e14f6a654a290bd1
Imphash	60a84185e19afa379906abb359cfa2ed
Rich PE header hash	9f00d540841ba43353b55843f488e6fa
SSDEEP	1536:aTZINbRh0SKws6KTUkmHIntMvfWhbpfCqeICS4AKvQIFIswOmZFS0cnwpIGmQwB:FRix3PWhNlOVFmw5q0cifmQ
TLSH	T123C3CF23BC5183F2C9A385F3133B7F1B95BFFE34151668AAD32589448A2508397276A7
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



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.

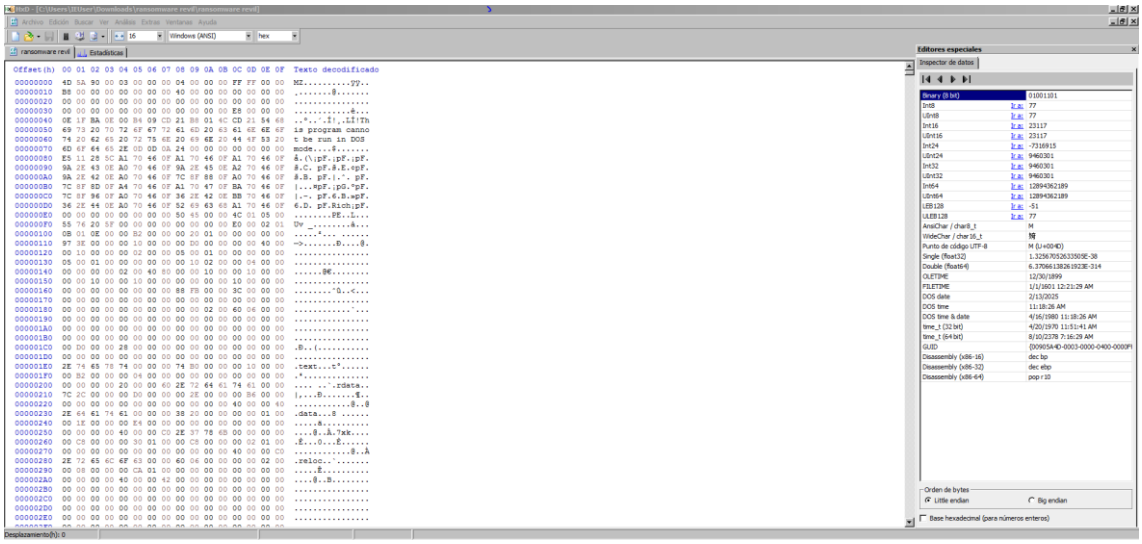
Utilizaremos la herramienta HxD, que permite abrir e identificar elementos de archivos en binario. Los elementos mas importantes de este proceso son:

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.

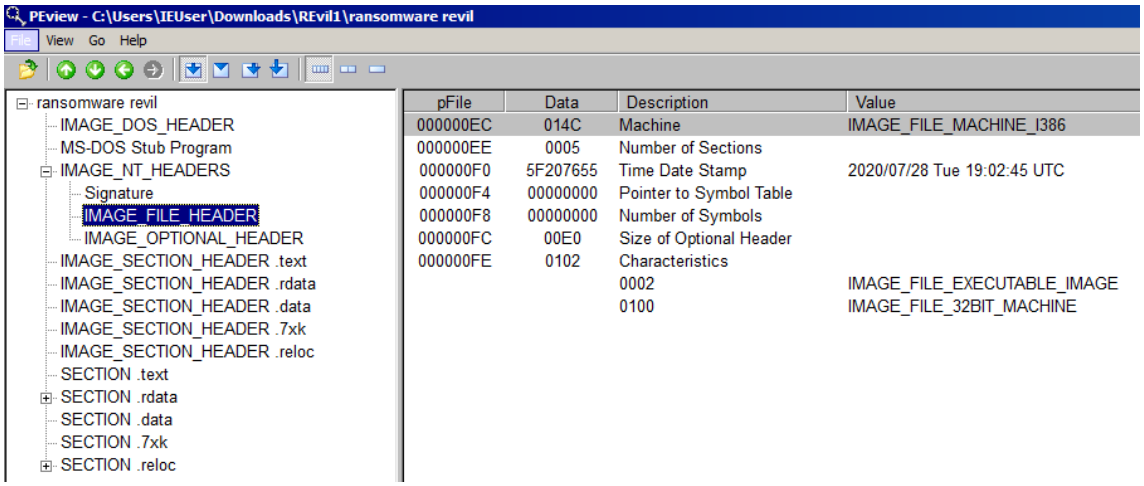


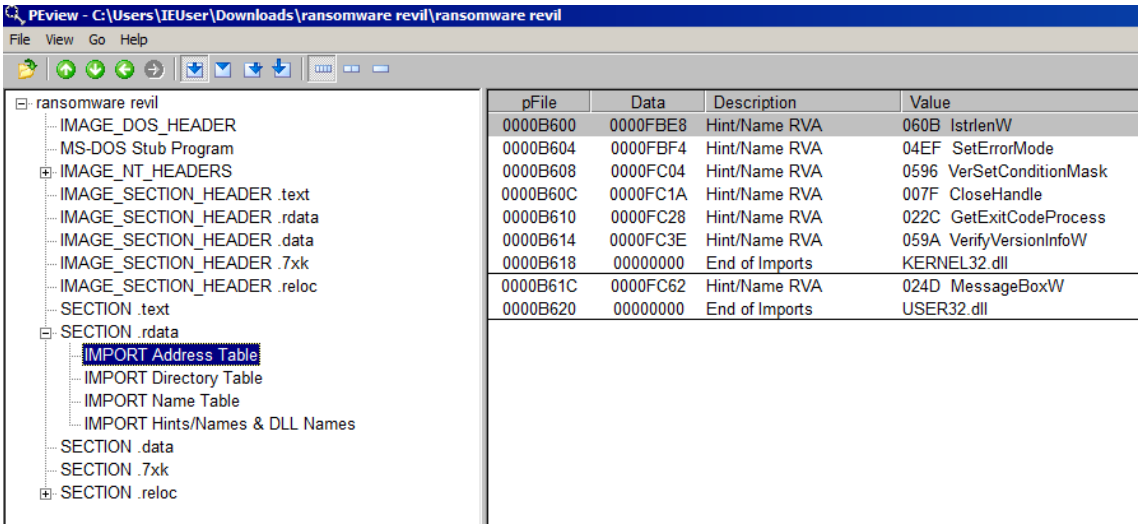
Para obtener los algoritmos de codificación utilizados para encapsular el archivo, es decir, las funciones o técnicas utilizadas para obtener el contenido de un fichero con únicamente una secuencia de caracteres, utilizaremos la herramienta “HashMyFiles”

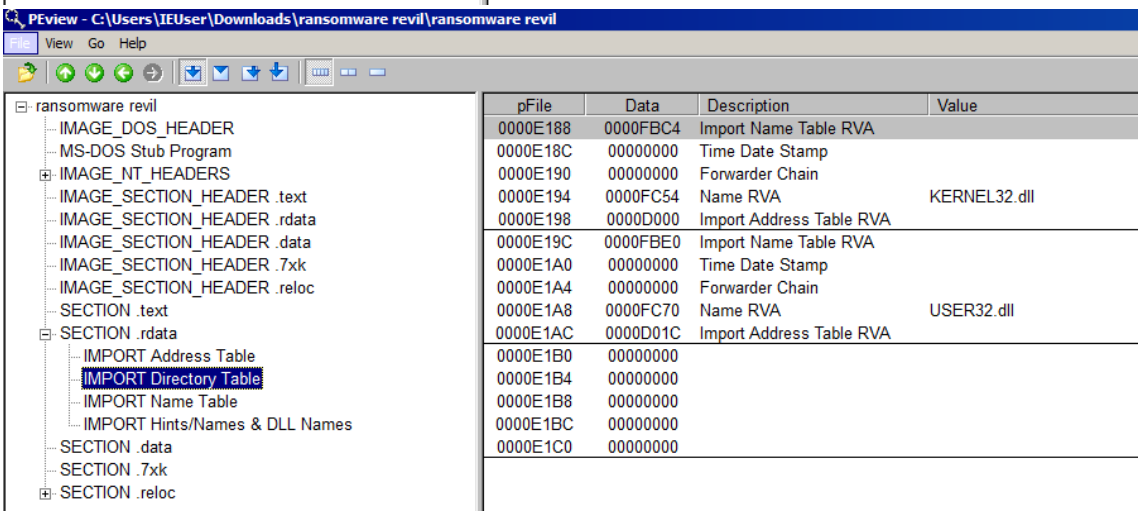
Además de facilitarnos la información anteriormente citada, nos ofrece datos como cuando se creó el malware, ruta en la que se encuentra, tamaño del archivo…

```
==================================================
Filename            : ransomware revil
MD5                 : b86ad4241b01376b3924a380f6f4c934
SHA1                : 10682d08a18715a79ee23b58fdb6ee44c4e28c61
CRC32               : 44767a73
SHA-256             : 14c8e3f1f23d16c2c9a4272cd05d00461d27b372cc5f588b4bbfc6102bbed708
SHA-512             : 54fd19cfc37255e7ddf3456d1a2989558522cf58e5eee6ca916c19542921fe3ba4e7a431a35e0e1edbfc37c5651d392e7c3c54eb408754c0488021b16fdf92c9
SHA-384             : 21c5851803d26c4946f7dae1e5c35991b103d7d97ea7a19d48b753b67ce0100e1c48971657f42453c9bd4b67ee0f6958
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
==================================================
```

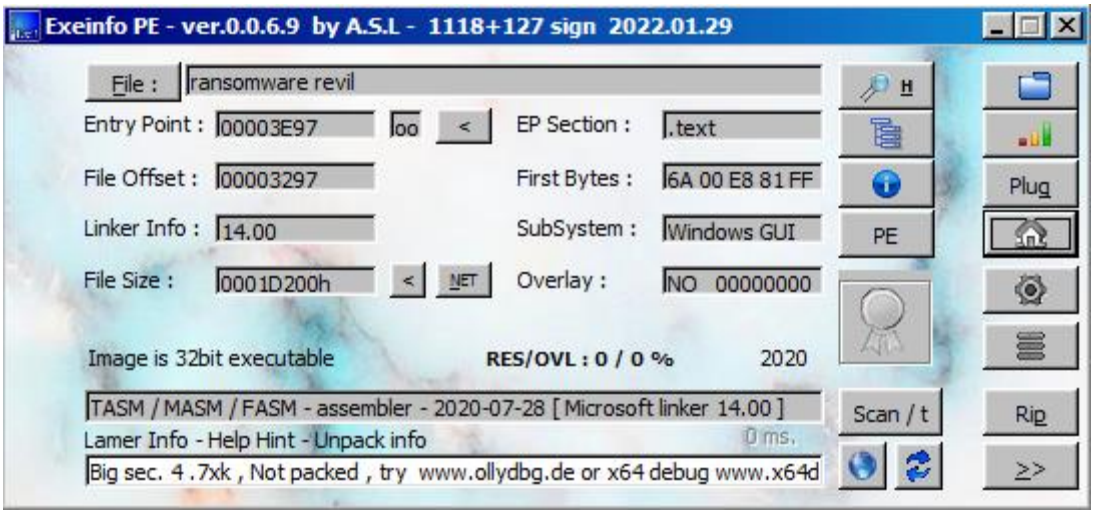
El análisis de cabeceras resulta ser un proceso útil y de gran importancia en el análisis estático de malware, ya que por un lado proporciona información general y por otra informa sobre las DLLs y funciones utilizadas.







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 para 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	ed49b23df7defab3df933c778183b12c019ab253330090f214f4bb5c2f89bcbc
Vhash	115056657d7d556bz3!z
Authentihash	a727ff1be32a59255cffea21dcbb3da972451403aa427e79a5d9cae996ed6a52
Imphash	c4c29c7e6a6897be412c7fedfcca8fe4
Rich PE header hash	b25cffe5d8f5190aa58ab8fad74e8066
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

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

Shell Commands

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

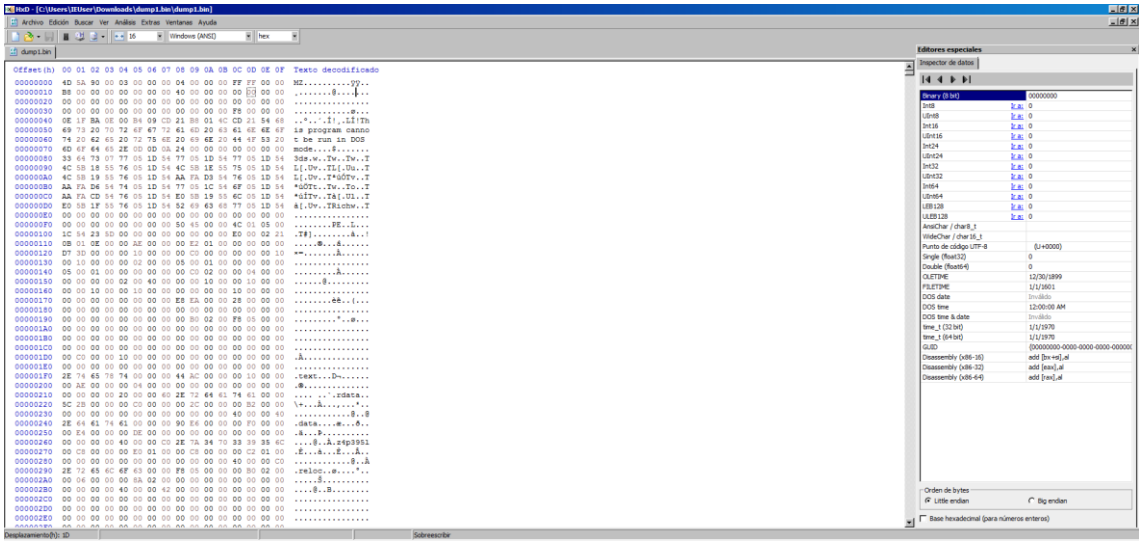
Processes Terminated

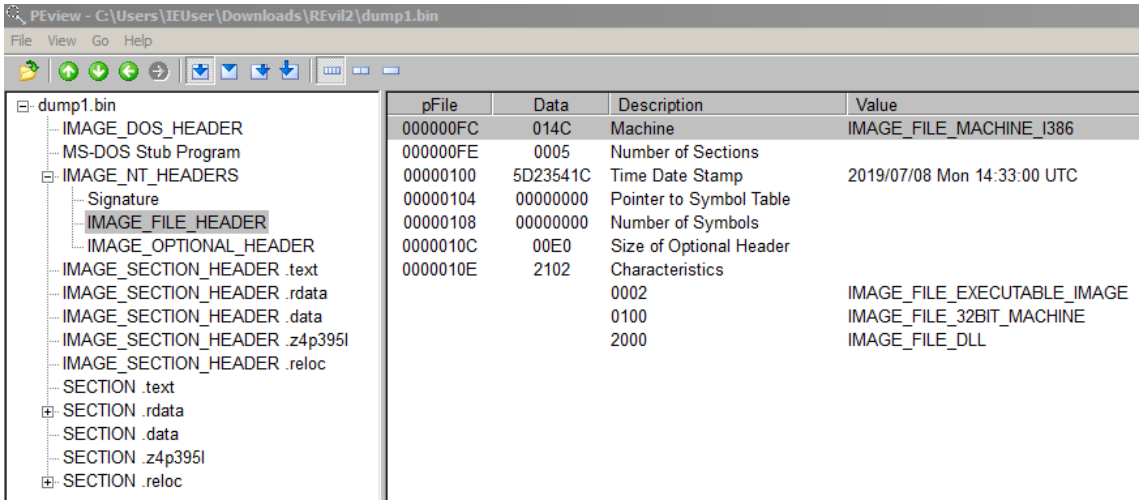
%CONHOST% "2018137818-1354459855142465142191087655 6-336004356-661671151-1041938976-1116811662
%windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
wmiadap.exe /F /T /R
%windir%\system32\vssvc.exe
"%ComSpec%" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures
vssadmin.exe Delete Shadows /All /Quiet

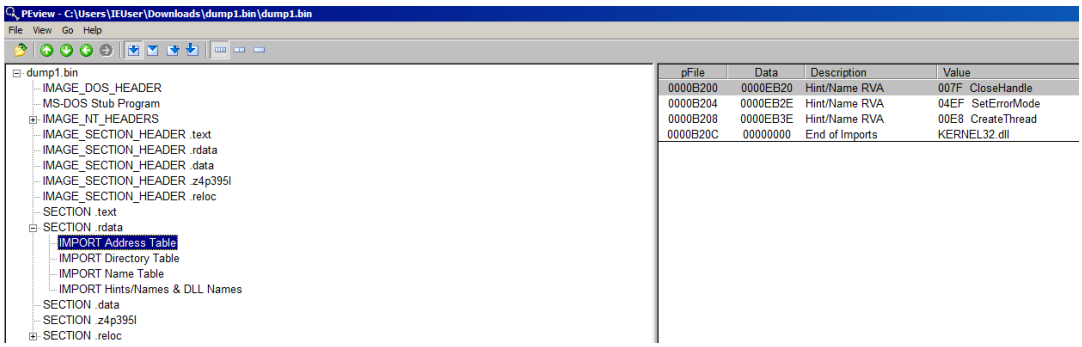
Processes Tree

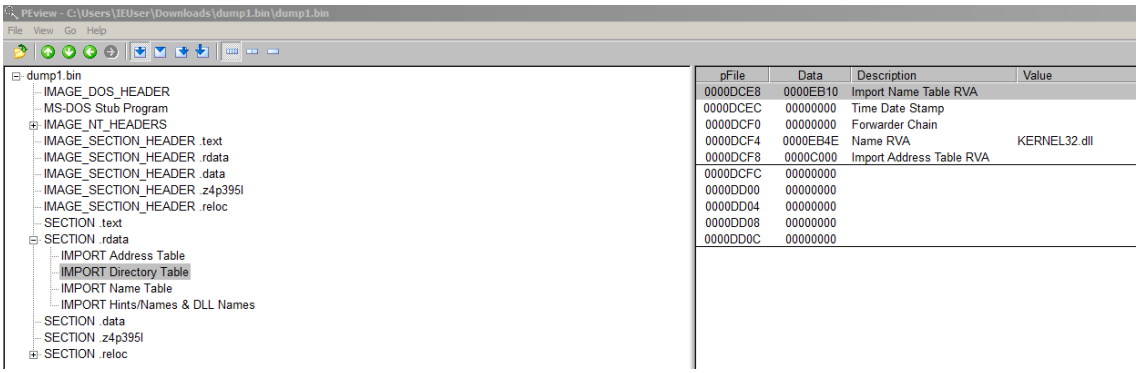
↳ 2828 - %CONHOST% "2018137818-1354459855142465142191087655 6-336004356-661671151-1041938976-1116811662
↳ 2956 - %windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
↳ 2088 - %windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}
↳ 1420 - wmiadap.exe /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\vssvc.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 ignoreallfailures
↳ 2844 - vssadmin.exe Delete Shadows /All /Quiet

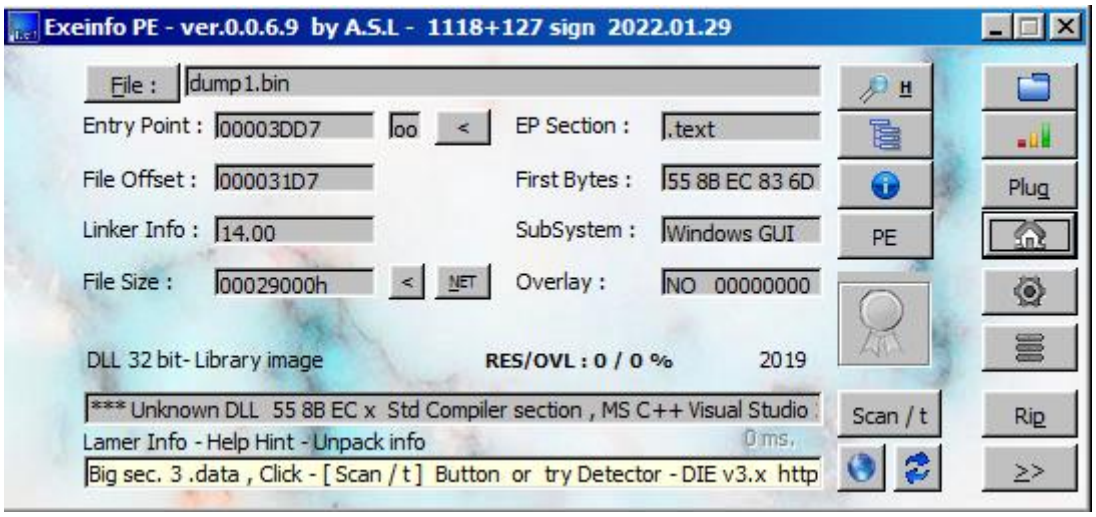
```
================================================
Filename            : dump1.bin
MD5                 : f0c97dcb65a030a214f6dd33cf4a8566
SHA1                : b23175fa1d3989baa2e3d8b5c7192554c24abf18
CRC32               : 01ebb94c
SHA-256             : ed49b23df7defab3df933c778183b12c019ab253330090f214f4bb5c2f89bcbc
SHA-512             : 24d7963631784357c4615ef94cecda9caaf47bc33896d6c897da324d55bda70713da4957f82ead8764f82cf6af1b5d9c8d3ad015fe3354694e9c331abbb67485
SHA-384             : fb81c6bc5b73f39c12b8b71f4b4bd7826d4a9c3b9f3a331b4910a6fb2cfea9022f658f01110ac48473bbe8f01a8c02ea
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
================================================
```











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	f3caa9831fc715af4f47cd98803549902dffe30a
SHA-256	ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83
Vhash	015046657d156019zc9z4tz
Authentihash	98aba482d8013656c1d60ff7d90326e69b1d64814834bcdd756625a92958f160
Imphash	eb68d746c420bd3a83ab3b0473d926ae
Rich PE header hash	d9e1b5346af5c0187ed8782fd7f10bdc
SSDEEP	1536:ASOoRSNl/XT9yYSvVKJJgpBy7bICS4AUsiz8djOK: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\DREDGE\%windir%\system32\DRIVERS\en-US\intelppm.sys.mui[PROCESSORWMI]
+ HKLM\Software\Microsoft\WBEM\WDM\DREDGE\%windir%\system32\DRIVERS\HDAudBus.sys[HDAudioMofName]
+ HKLM\Software\Microsoft\WBEM\WDM\DREDGE\%windir%\System32\Drivers\en-US\portcls.SYS.mui[PortclsMof]
+ HKLM\Software\Microsoft\WBEM\WDM\DREDGE\%windir%\system32\advapi32.dll[MofResourceName]
+ HKLM\Software\Microsoft\WBEM\WDM\DREDGE\%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

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

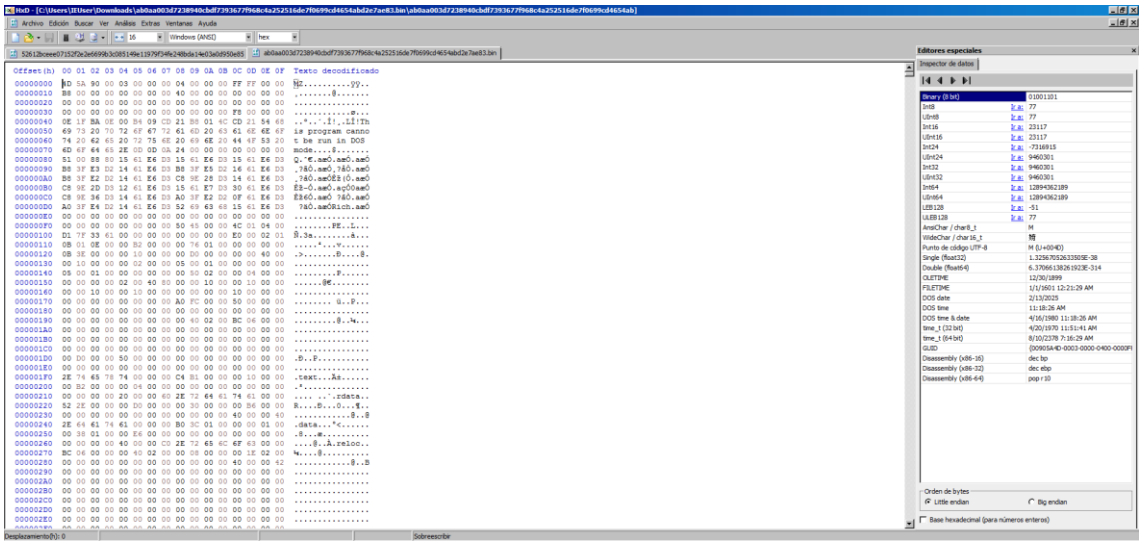
↳ 2764 - %windir%\system32\wbem\unsecapp.exe -Embedding

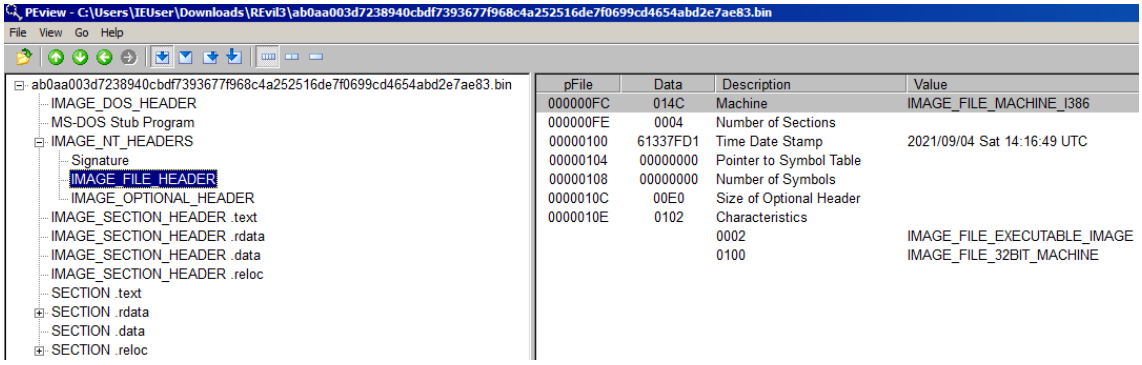
↳ 1712 - %windir%\system32\wbem\wmiprvse.exe

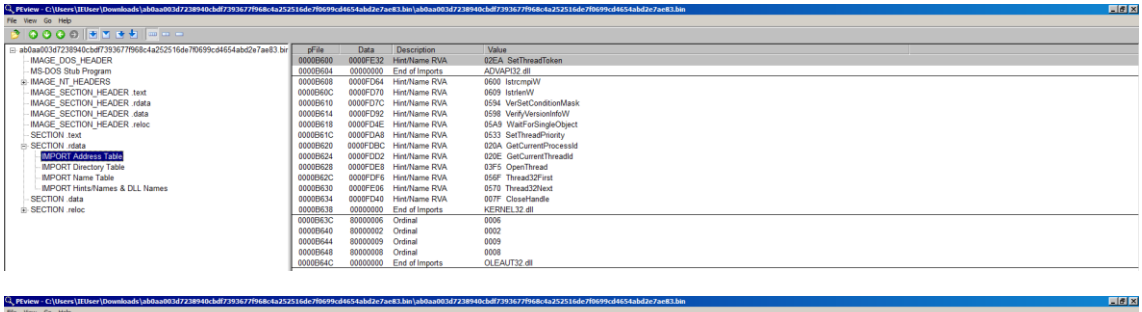
↳ 2792 - %windir%\system32\vssvc.exe

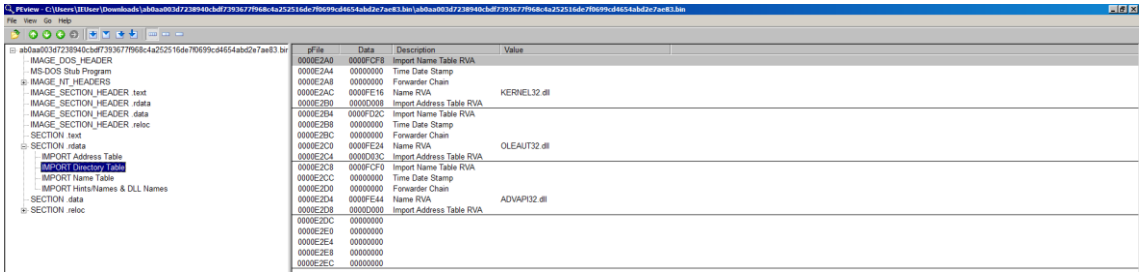
↳ 2624 - %SAMPLEPATH%

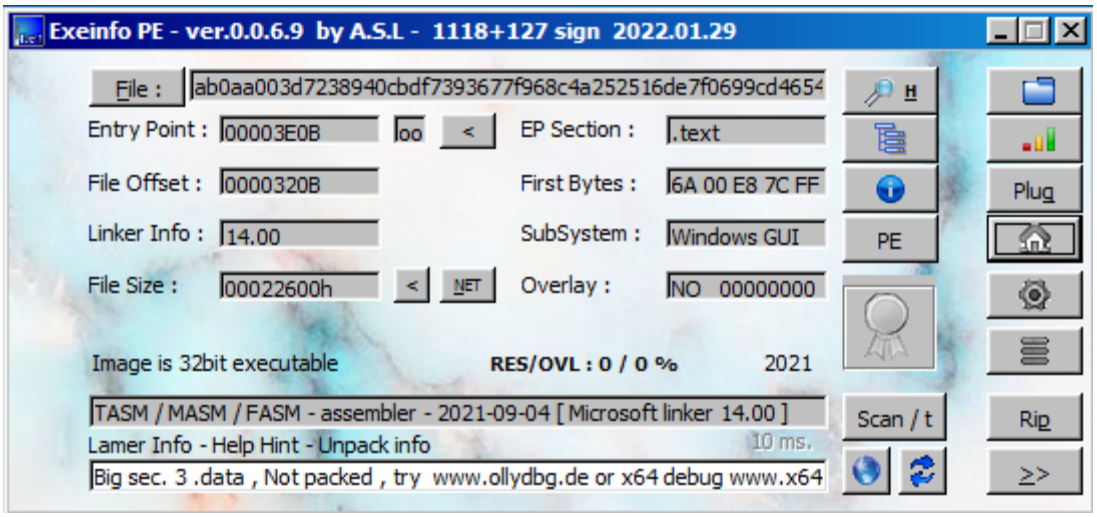
```
===============================================
Filename          : ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83.bin
MD5               : 21d01fa87dfcaf971ff7b63a1a6fda94
SHA1              : f3caa9831fc715af4f47cd98803549902dffe30a
CRC32             : 8b26aae3
SHA-256           : ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83
SHA-512           : f89997f8c31d77029f1087257a5b24337f9989bebfbe4169067acae72a5dd50ce118d273fae00690ef2e2bf345901d723034992f53dd3e5b9df5cbe9be2e67fa
SHA-384           : 3b3deee222c3154ad7653693695 0f0f739e2803a253a2e570b8a2b743f3e4039e61f7ccabd6d8bf4eabdd65b713f34ae
Full Path         : C:\Users\IEUser\Downloads\ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83.bin\ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83.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
File Size         : 140,800
File Version      :
Product Version   :
Identical         :
Extension         : bin
File Attributes   : A
===============================================
```




PEview - C:\Users\IEUser\Downloads\REvil3\ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83.bin
File View Go Help
ab0aa003d7238940cbdf7393677f968c4a252516de7f0699cd4654abd2e7ae83.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 .reloc
SECTION .text
SECTION .rdata
SECTION .data
SECTION .reloc
pFile Data Description Value
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







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/M4PI8iwpIAXpzK88ICS4Aer9Ds5kYk/gm729Tq2Kke:+/LPrIAZZEqIgQ29Tq2Kke
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\vssvc.exe

Processes Tree

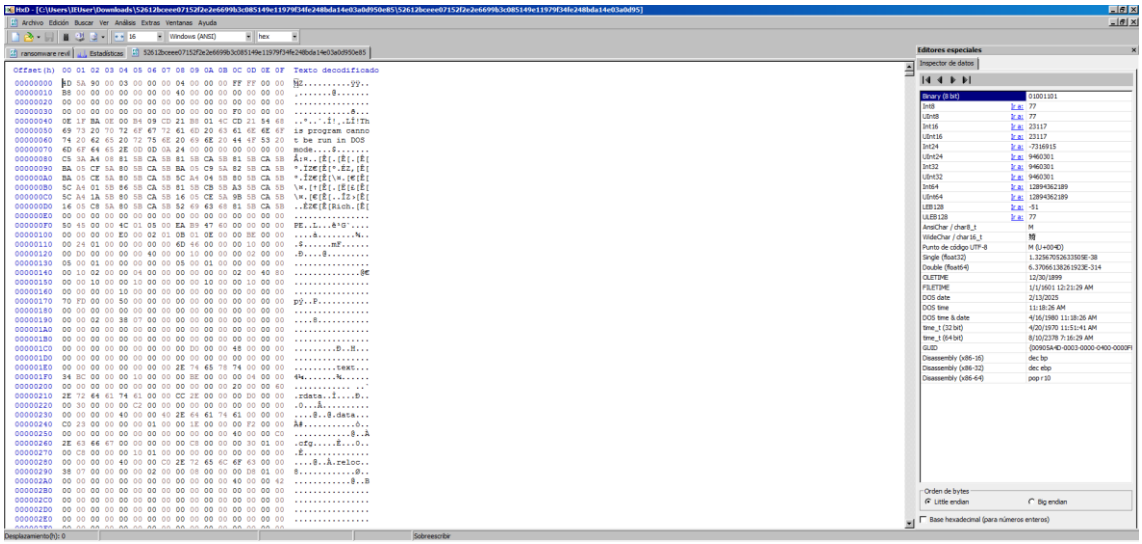
↳ 2320 - %windir%\System32\svchost.exe -k WerSvcGroup

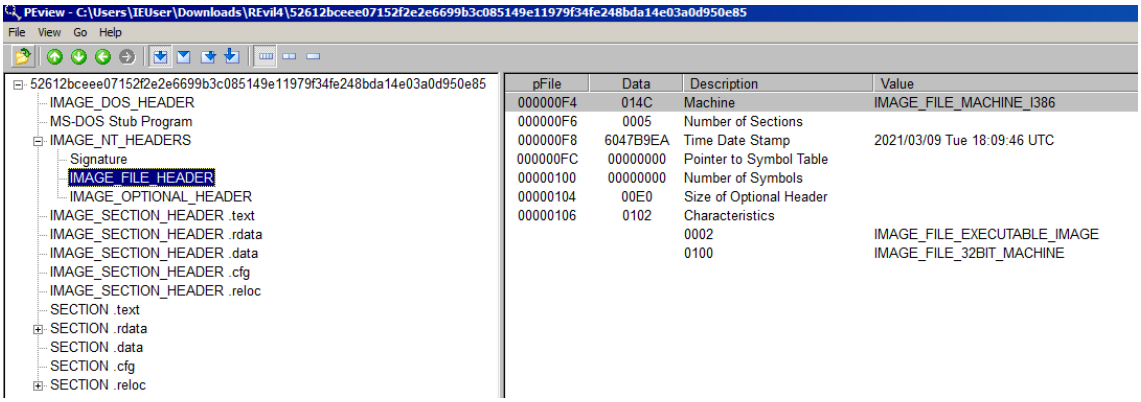
↳ 1840 - %windir%\system32\DllHost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5}

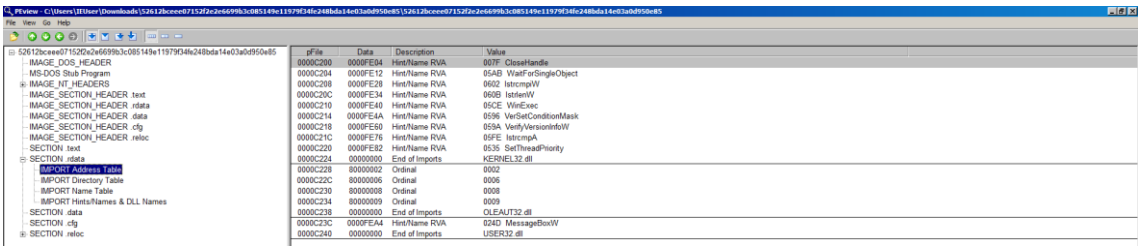
↳ 2868 - %windir%\system32\vssvc.exe

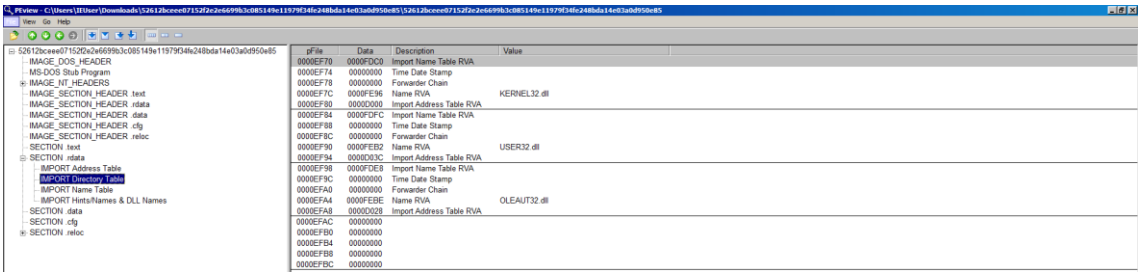
↳ 2692 - %SAMPLEPATH%

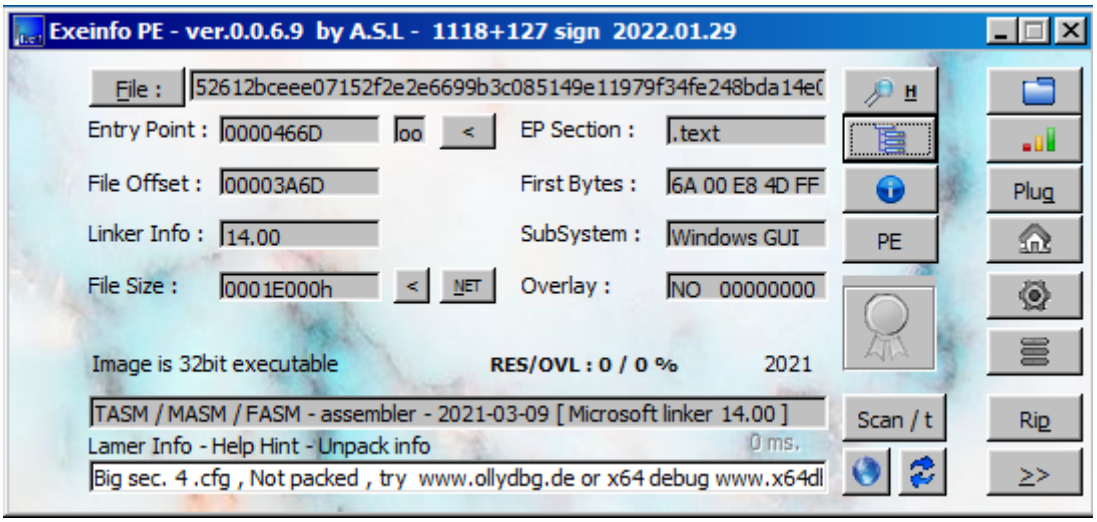
```
================================================
Filename          : 52612bceee07152f2e2e6699b3c085149e11979f34fe248bda14e03a0d950e85
MD5               : ff0e2ce0af118bae62969a5e897b59b2
SHA1              : 5bc65c73cae94509905c6a4ba657a61360bb96f2
CRC32             : 351197a9
SHA-256           : 52612bceee07152f2e2e6699b3c085149e11979f34fe248bda14e03a0d950e85
SHA-512           : 7f205bc47555b356b7f9901a43d8b1a597128041a0b3c12109f3396bce095d2e96b4b9bede21d319ac27ff0b924c0e13cf3b19076bc31406b8278d39a7a2c8e9
SHA-384           : a04788d34f8a9f36f758bdf4d5cdff9097eda81b6ddf6e45402973f124bece1332e3344b198a3757b1443d92c1cc6d2d
Full Path         : C:\Users\IEUser\Downloads\52612bceee07152f2e2e6699b3c085149e11979f34fe248bda14e03a0d950e85\52612bceee07152f2e2e6699b3c085149e11979f34fe248bda14e03a0d950e85
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
================================================
```











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	3c5d7a41dc538494d7f2d958ab9db819c46868ac5b1bbfbd547cbae48192ac1e
Imphash	a71572da77751977cfaaa54c9d130359
SSDEEP	6144:viYY7HL6OXYevtqsuJ40gxBekUNYkdOGINJcHC7KAU93Jobv:vdYjeOXX1lFTve53v
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\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5
+ HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\07E032E020B72C3F192F0628A2593A19A70F069E
+ HKU\S-1-5-21-1143565567-962705147-4090495373-1003\SOFTWARE\CLASSES\LOCAL SETTINGS\MUICACHE\8\52C64B7E
+ HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\47BEABC922EAE80E78783462A79F45C254FDE68B
+ HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436
+ HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43
+ HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\3679CA35668772304D30A5FB873B0FA77BB70D54
+ HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEMCERTIFICATES\ROOT\CERTIFICATES\CDD4EEAE6000AC7F40C3802C171E30148030C072
+ HKU\S-1-5-21-1143565567-962705147-4090495373-1003\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\EXPLORER
+ HKU\S-1-5-21-1143565567-962705147-4090495373-1003\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\CA\CERTIFICATES\A9CE8E8879AB0CCB17A1FEEED83E720F3D925DF8

Registry Keys Deleted

HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEMCERTIFICATES\ROOT\CERTIFICATES
HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES
HKU\S-1-5-21-1143565567-962705147-4090495373-1003\SOFTWARE\MICROSOFT\SYSTEMCERTIFICATES\CA\CERTIFICATES

Process And Service Actions

Processes Created

C:\Users\Olivia\AppData\Local\Temp\OHQZtl7mTtgqf6.exe

C:\WINDOWS\SysWOW64\cmd.exe

C:\WINDOWS\SysWOW64\vssadmin.exe

C:\Users\Olivia\AppData\Local\Temp\u51dsD72XvKONa3NIwSMm.exe

C:\Users\Lucas\AppData\Local\Temp\ment.exe

Shell Commands

C:\Users\Olivia\AppData\Local\Temp\OHQZtl7mTtgqf6.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\u51dsD72XvKONa3NIwSMm.exe

C:\Users\Lucas\AppData\Local\Temp\ment.exe

Processes Tree

↳ 3080 - C:\Users\Olivia\AppData\Local\Temp\OHQZtl7mTtgqf6.exe

↳ 3912 - C:\WINDOWS\SysWOW64\cmd.exe

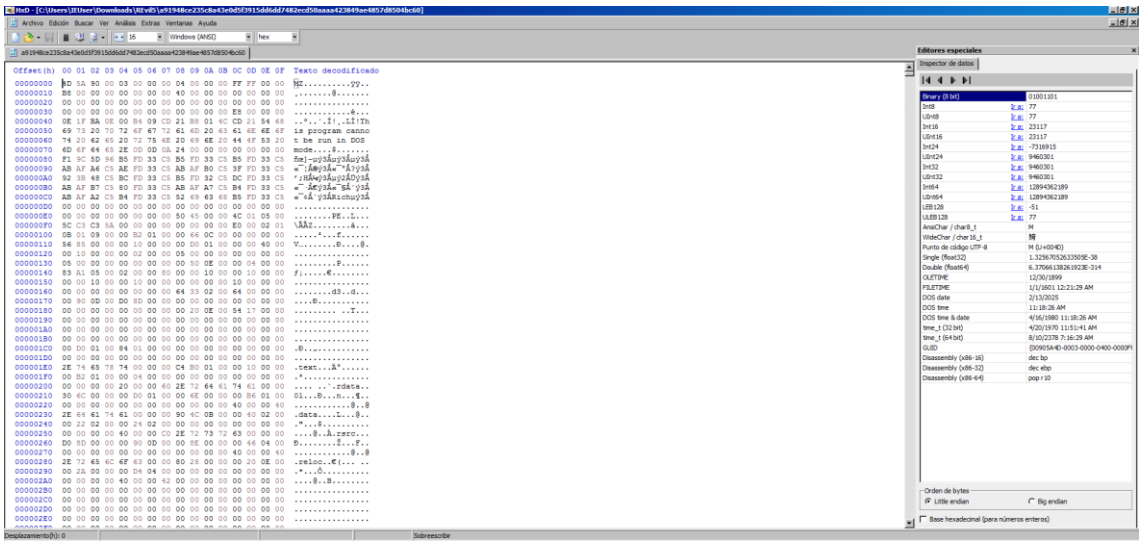
↳ 796 - C:\WINDOWS\SysWOW64\vssadmin.exe

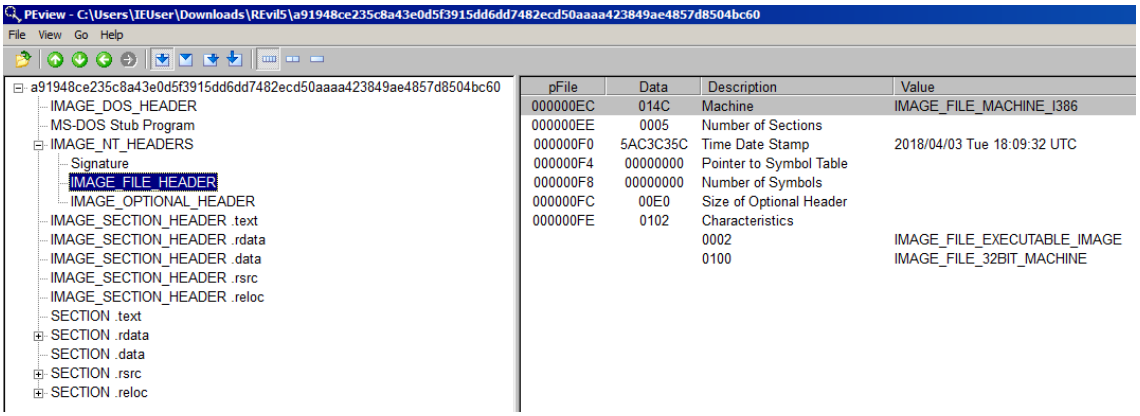
↳ 3904 - C:\Users\Olivia\AppData\Local\Temp\u51dsD72XvKONa3NIwSMm.exe

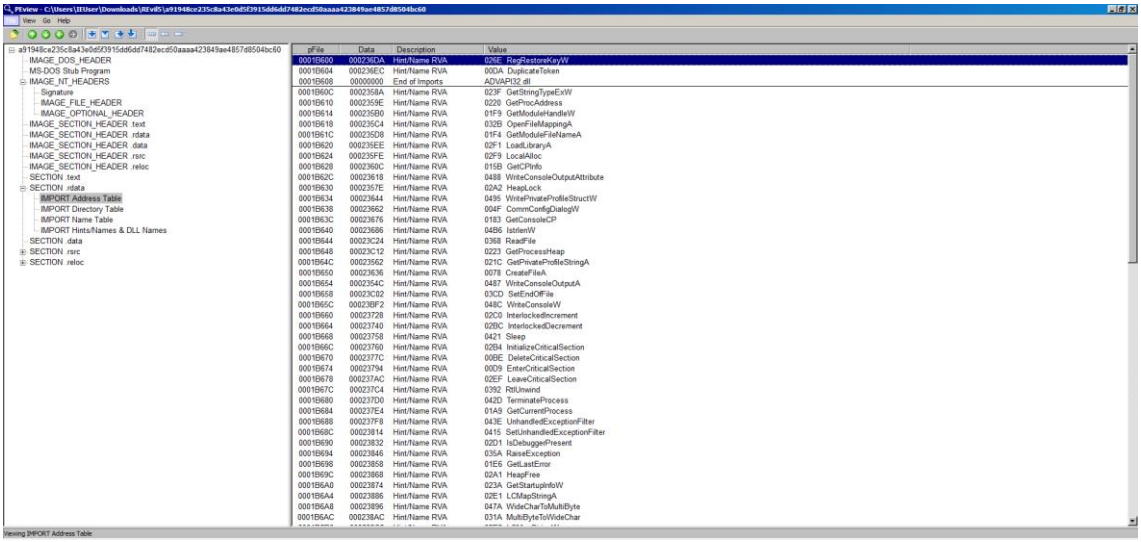
↳ 4788 - C:\WINDOWS\SysWOW64\cmd.exe

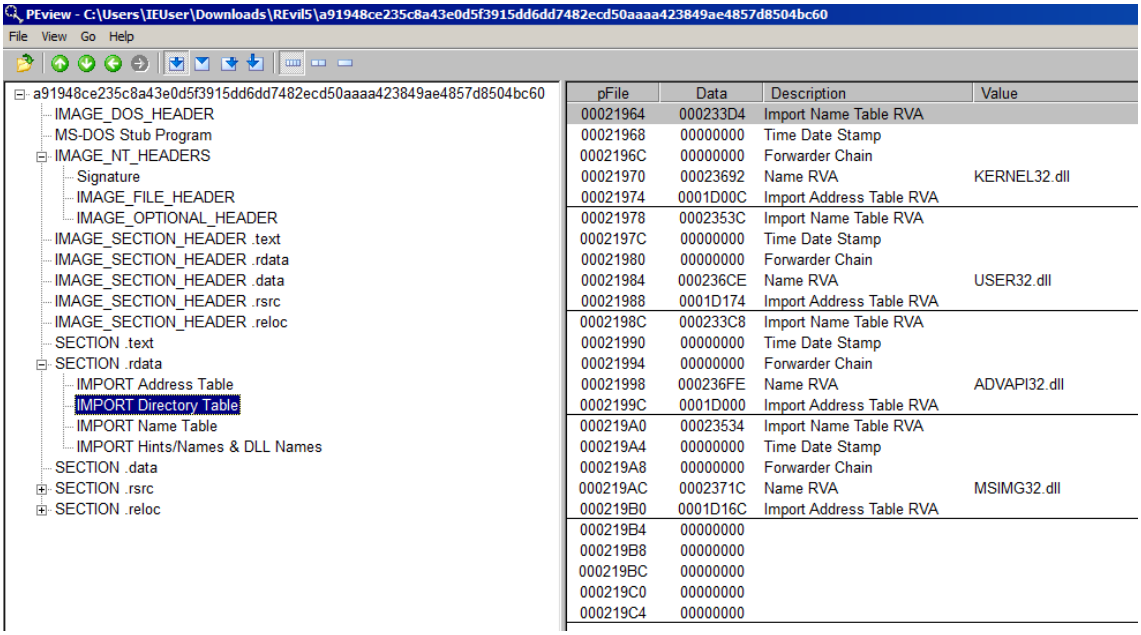
↳ 6868 - C:\WINDOWS\SysWOW64\vssadmin.exe

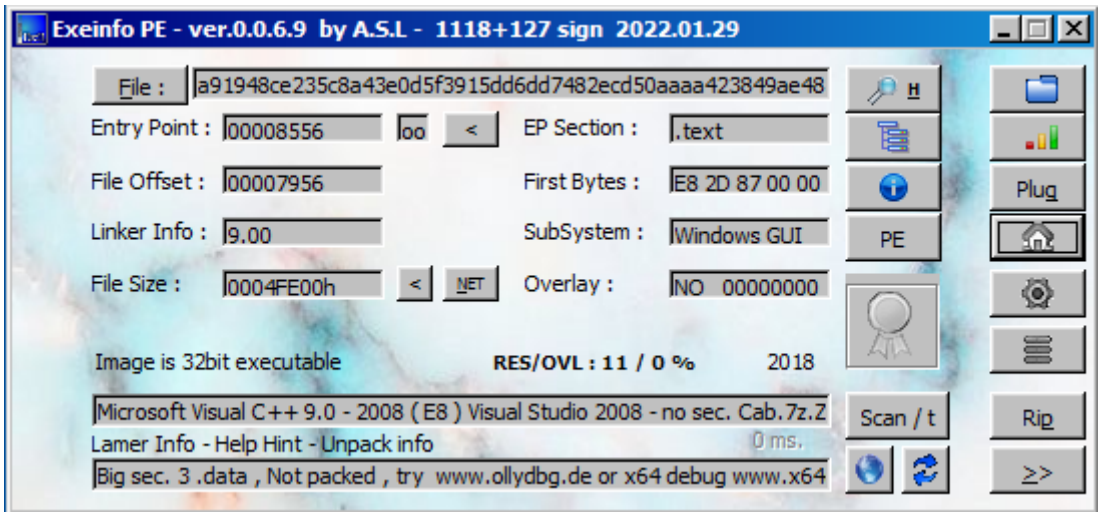
```
=====================================================
Filename          : a91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60
MD5               : 0bb803ea960f1f2c88f4e0cd808c196e
SHA1              : 590053863146f758fcb7a876c02f5d4459aa6a43
CRC32             : e9e5590a
SHA-256           : a91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60
SHA-512           : 460f68c551136dc519c3ffaadf18d8536c2914c2bfafa0e2d06926664f4b3e493e5e1c2dcd6d826d7637200289ff36b70330bbc0c91187ba8dffc7569d9c9718
SHA-384           : 03d7e5de87157a4e37fea8e27afa473e43e250270ca65912db672f2e959e848cc9db860966e9555b880206cc5018aeec
Full Path         : C:\Users\IEUser\Downloads\REvil5\a91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60
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\a91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60
File View Go Help
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
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



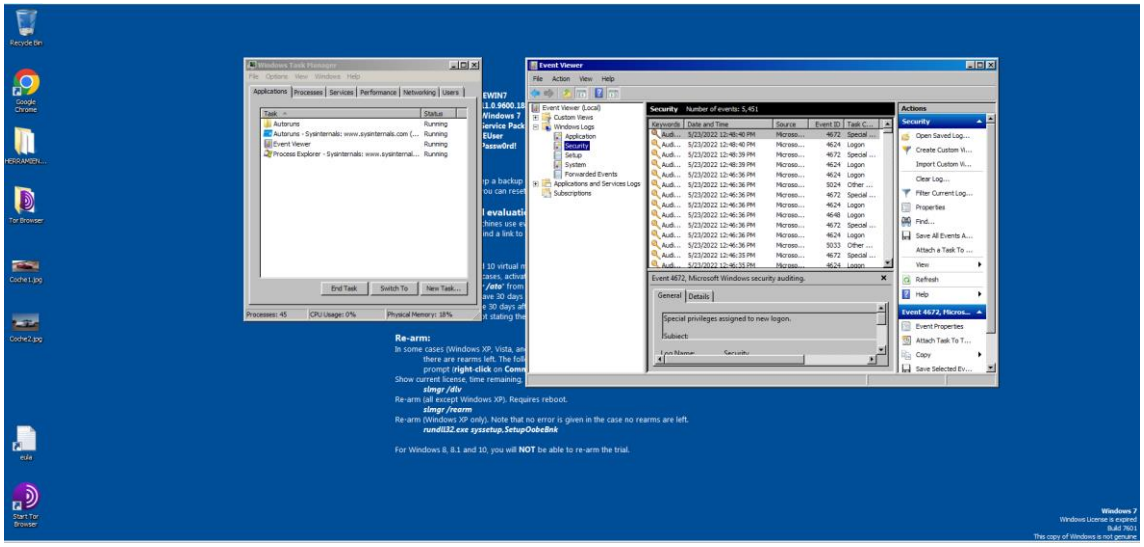

PEview - C:\Users\IEUser\Downloads\REvil5\a91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60
File View Go Help
a91948ce235c8a43e0d5f3915dd6dd7482ecd50aaaa423849ae4857d8504bc60
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_SECTION_HEADER .text
IMAGE_SECTION_HEADER .rdata
IMAGE_SECTION_HEADER .data
IMAGE_SECTION_HEADER .rsrc
IMAGE_SECTION_HEADER .reloc
SECTION .text
SECTION .rdata
IMPORT Address Table
IMPORT Directory Table
IMPORT Name Table
IMPORT Hints/Names & DLL Names
SECTION .data
SECTION .rsrc
SECTION .reloc
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 0001D00C 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

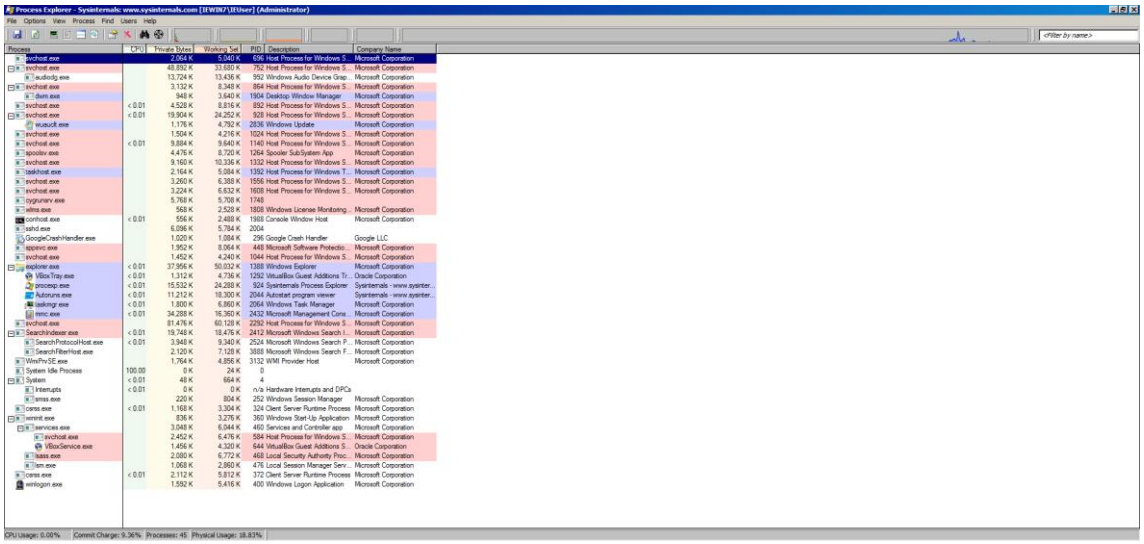


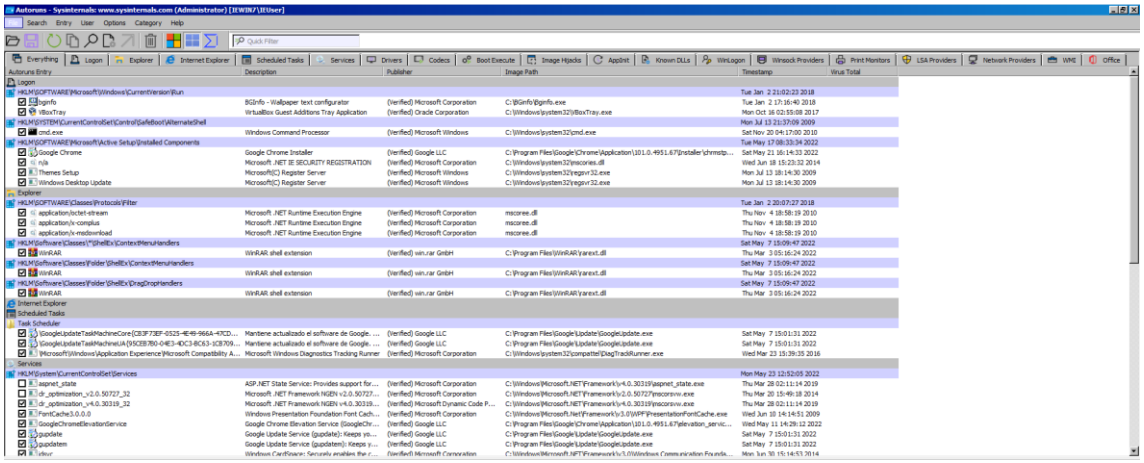
ANALISIS DINAMICO:

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.

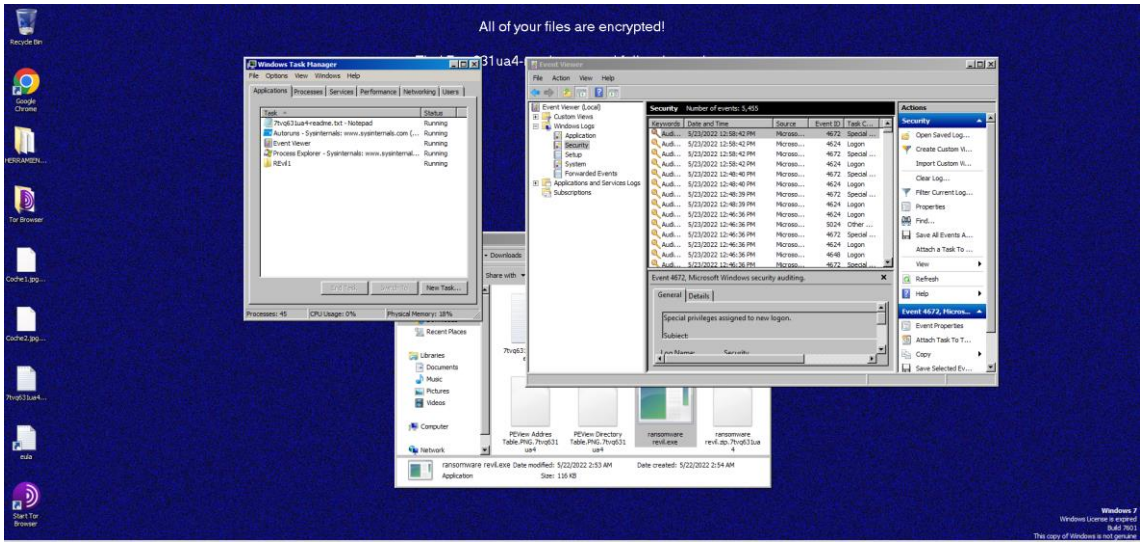
Al iniciar una “snapshot” de la máquina virtual, siempre serán los mismos procesos y servicios los que se iniciaran, por lo que solamente lo comprobaremos una vez.

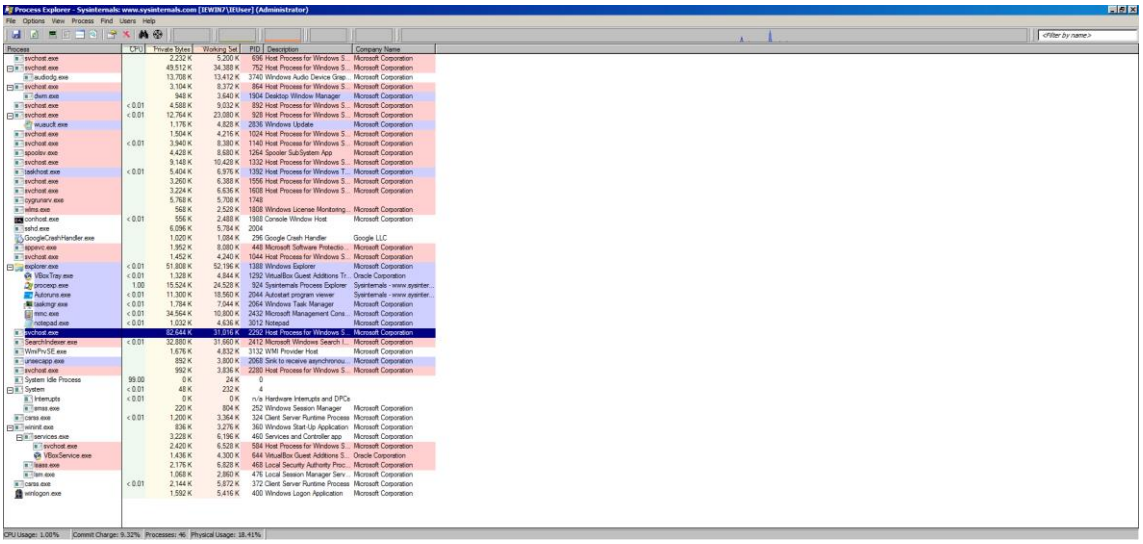


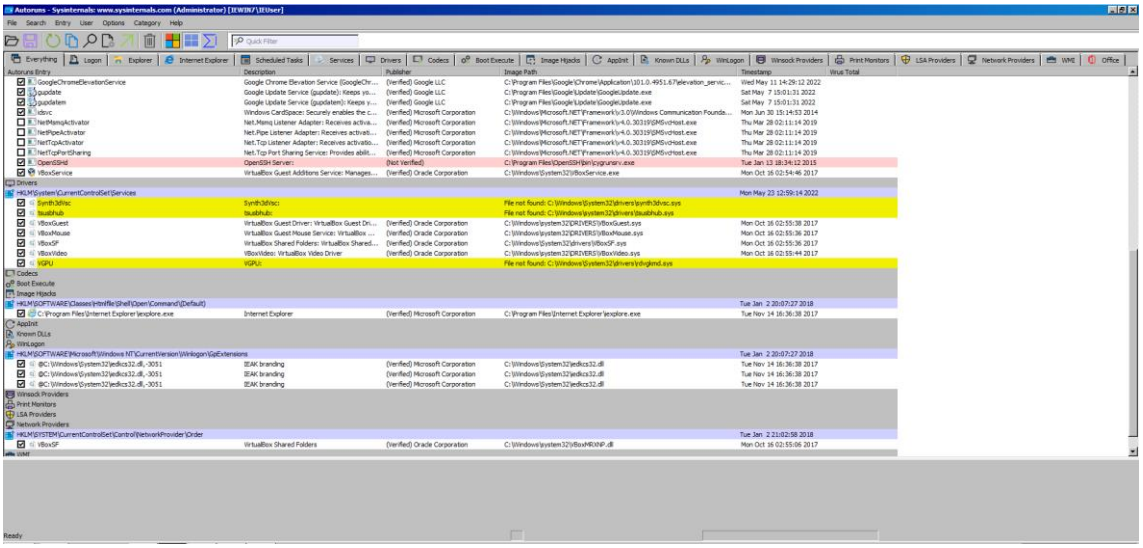


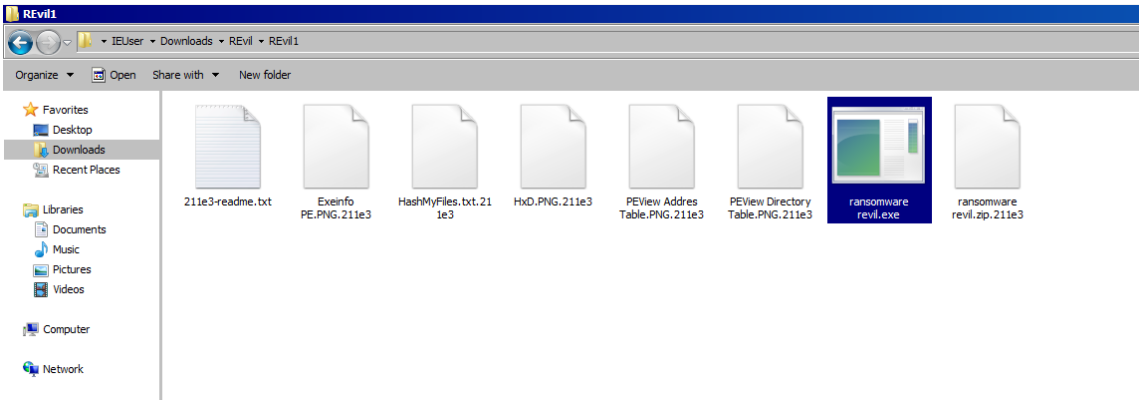


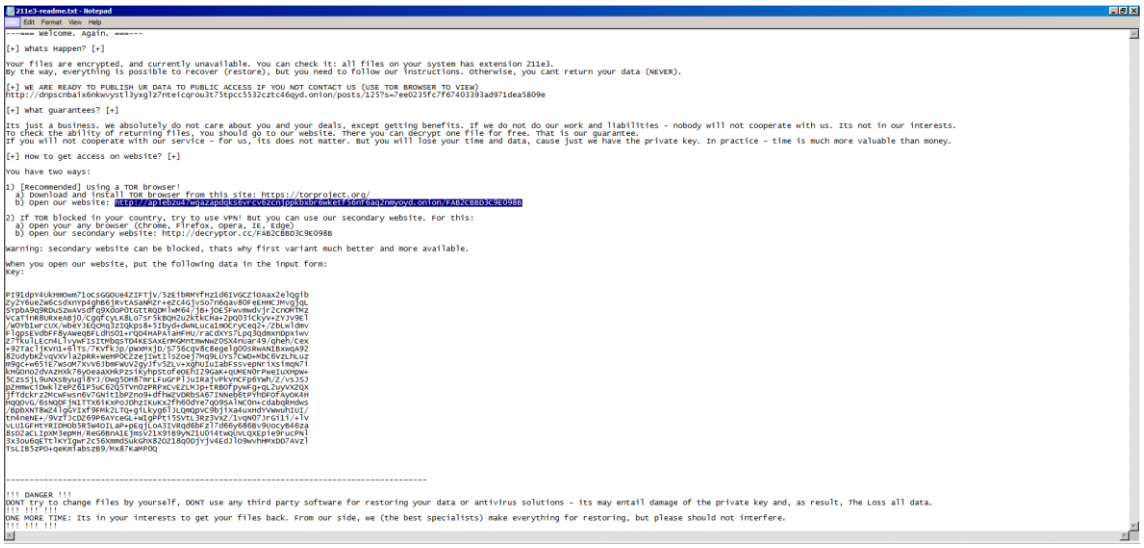
MUESTRA 1:







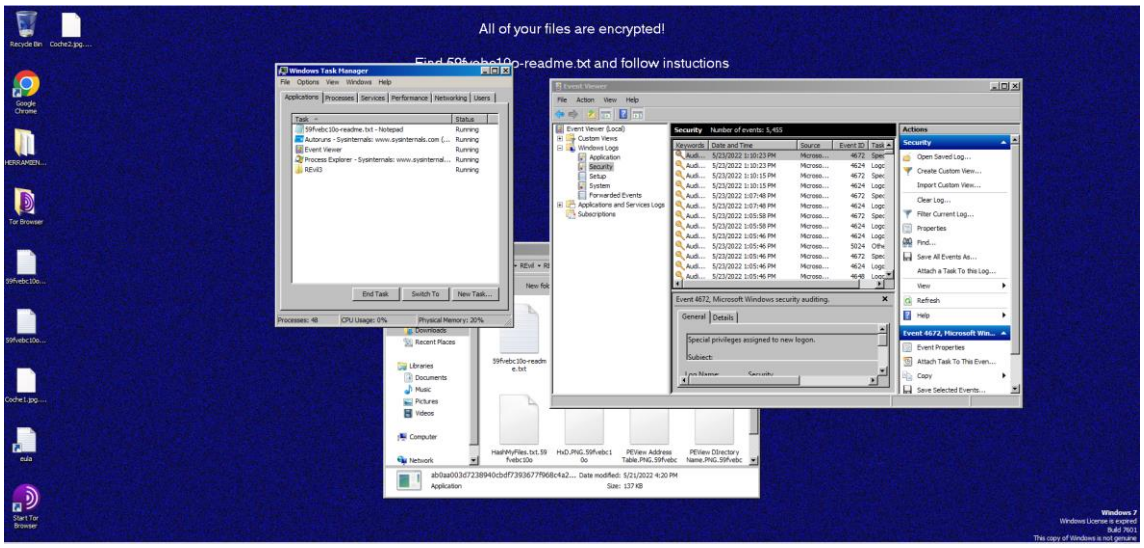

REvil1
IEUser ▸ Downloads ▸ REvil ▸ REvil1
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
211e3-readme.txt
Exeinfo PE.PNG.211e3
HashMyFiles.txt.211e3
HxD.PNG.211e3
PEView Addres Table.PNG.211e3
PEView Directory Table.PNG.211e3
ransomware revil.exe
ransomware revil.zip.211e3

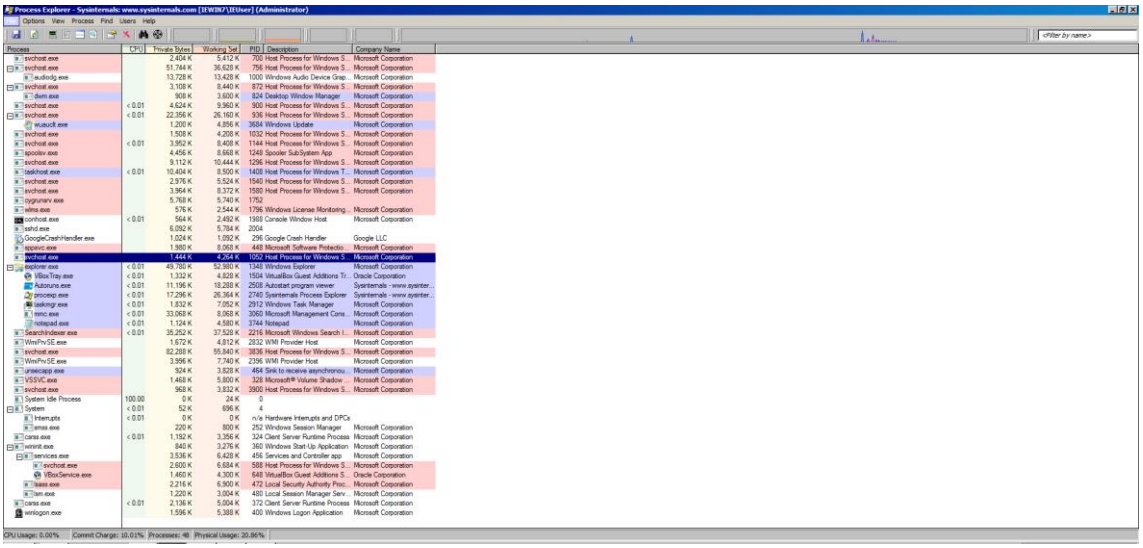


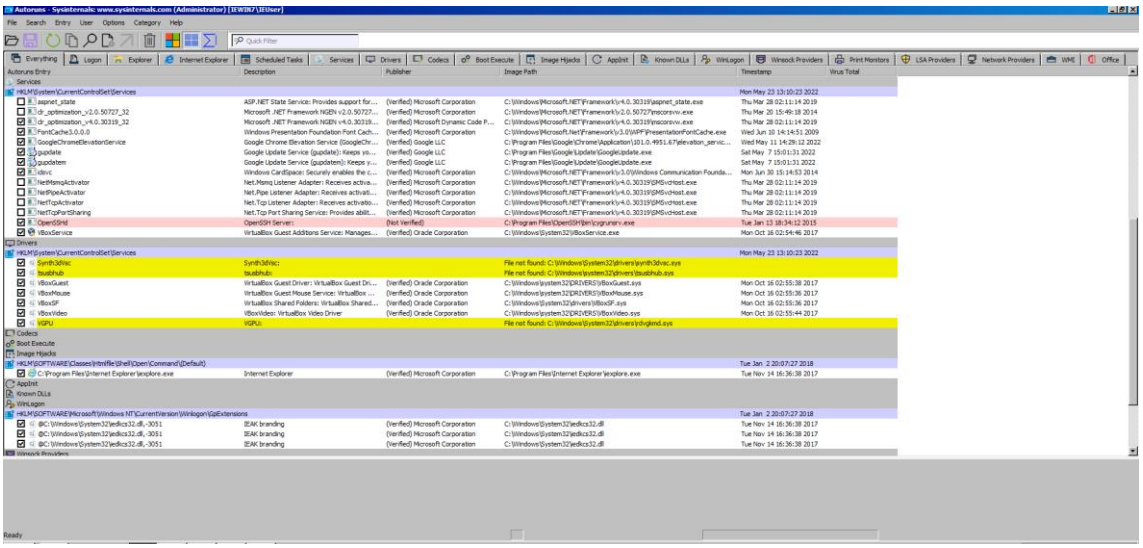
MUESTRA 2:

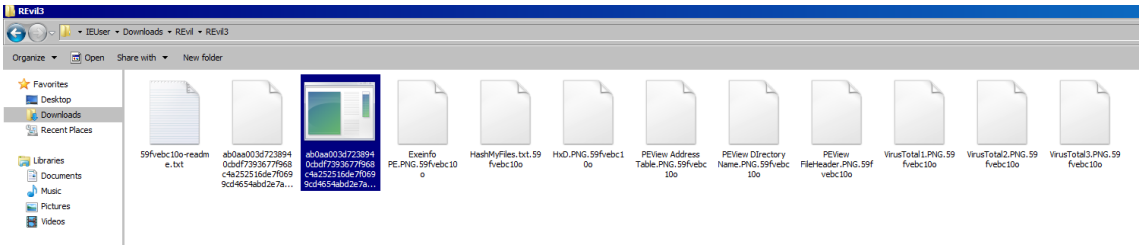
Esta muestra no he conseguido ejecutarla en modo dinámico.

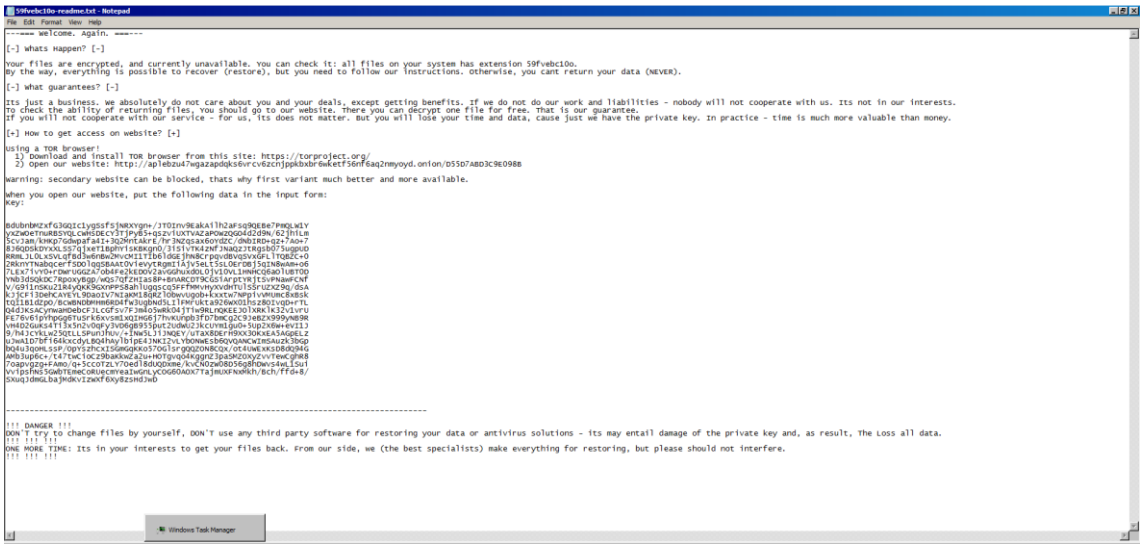
MUESTRA 3:



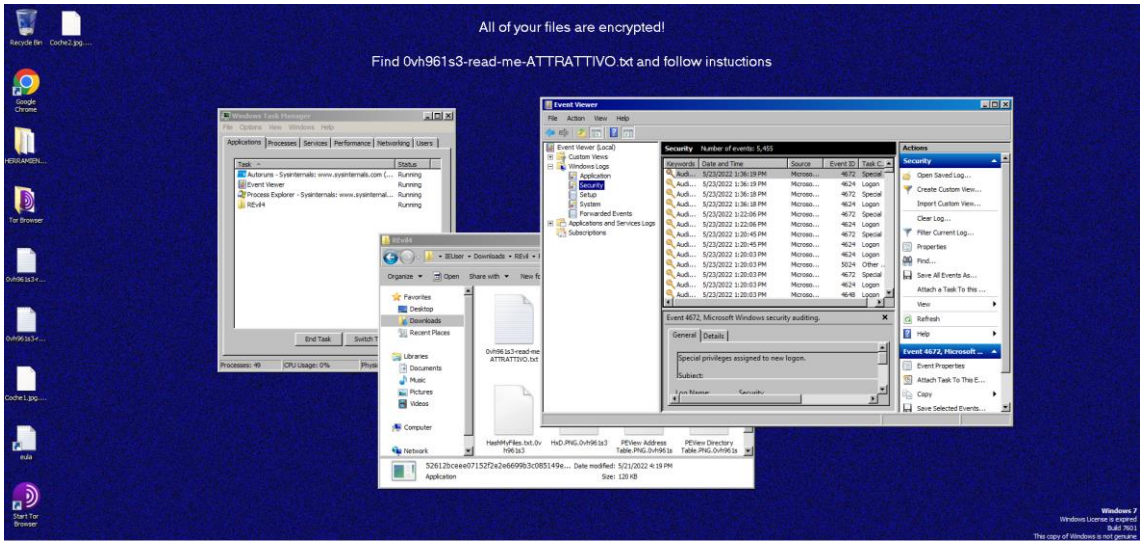

Process Explorer - Sysinternals: www.sysinternals.com [IEWIN7\IEUser] (Administrator)

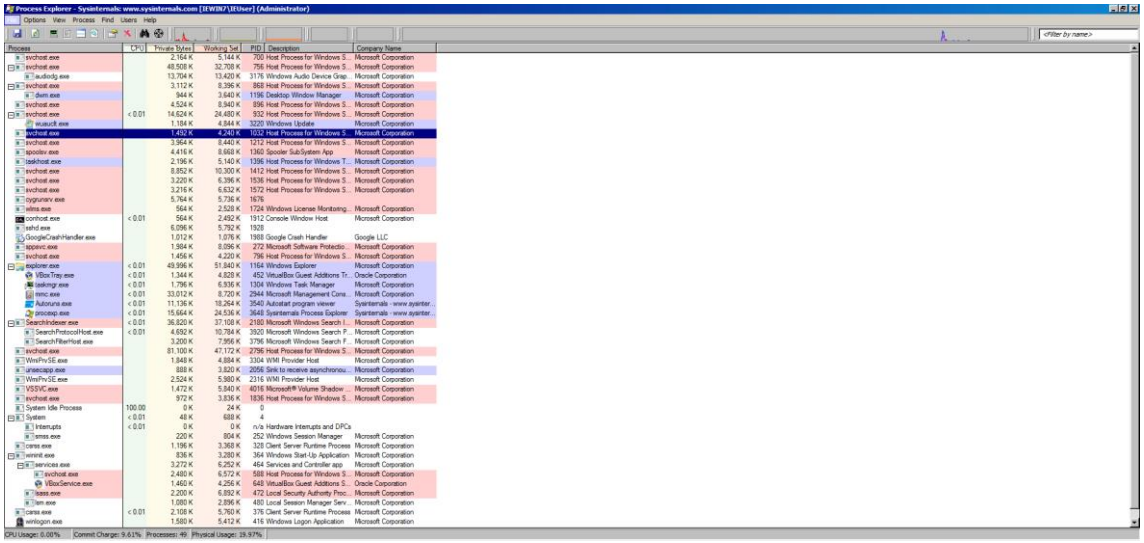

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [IEWIN7\IEUser]

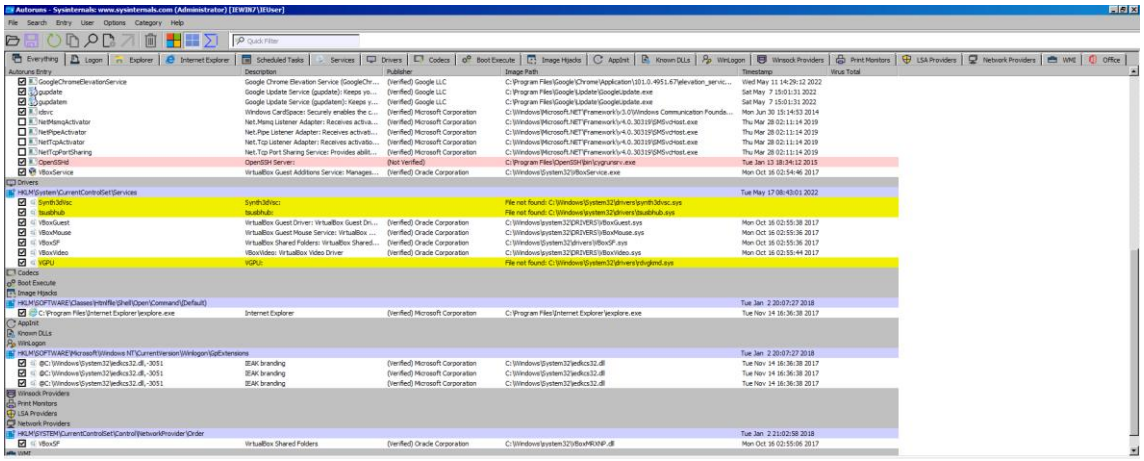

REvil3
IEUser ▸ Downloads ▸ REvil ▸ REvil3
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
59fvebc10o-readme.txt
ab0aa003d723894 0cbdf7393677f968 c4a252516de7f069 9cd4654abd2e7a...
ab0aa003d723894 0cbdf7393677f968 c4a252516de7f069 9cd4654abd2e7a...
Exeinfo PE.PNG.59fvebc10o
HashMyFiles.txt.59fvebc10o
HxD.PNG.59fvebc10o
PEView Address Table.PNG.59fvebc10o
PEView DIrectory Name.PNG.59fvebc10o
PEView FileHeader.PNG.59fvebc10o
VirusTotal1.PNG.59fvebc10o
VirusTotal2.PNG.59fvebc10o
VirusTotal3.PNG.59fvebc10o

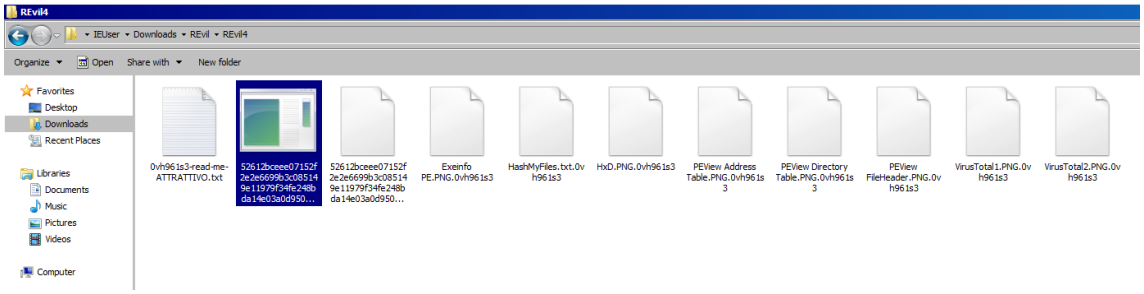

59fvebc10o-readme.txt - Notepad
File Edit Format View Help
---=== Welcome. Again. ===---
[-] Whats Happen? [-]
Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension 59fvebc10o.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).
[-] What guarantees? [-]
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.
To check the ability of returning files, you should go to our website. There you can decrypt one file for free. That is our guarantee.
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 on website? [+]
Using a TOR browser!
1) Download and install TOR browser from this site: https://torproject.org/
2) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/D55D7ABD3C9E098B
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 form:
Key:
!!! DANGER !!!
DON'T 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.
!!! !!! !!!
ONE MORE 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.
!!! !!! !!!
Windows Task Manager

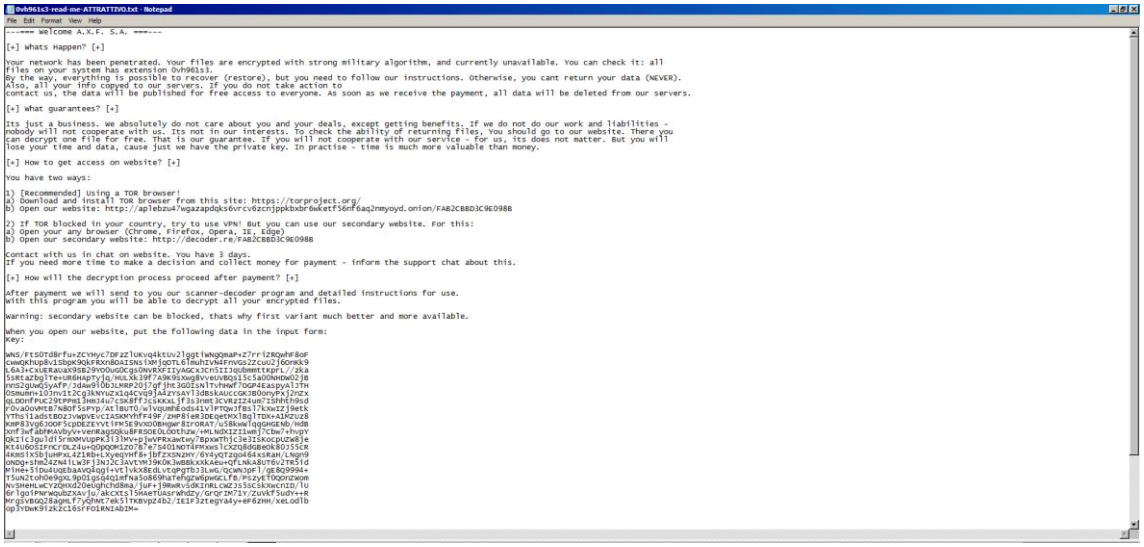
MUESTRA 4:


All of your files are encrypted!
Find 0vh961s3-read-me-ATTRATTIVO.txt and follow instuctions
Windows Task Manager
Event Viewer
Windows 7
Windows License is expired
Build 7601
This copy of Windows is not genuine


Process Explorer - Sysinternals: www.sysinternals.com [IEWIN7\IEUser] (Administrator)

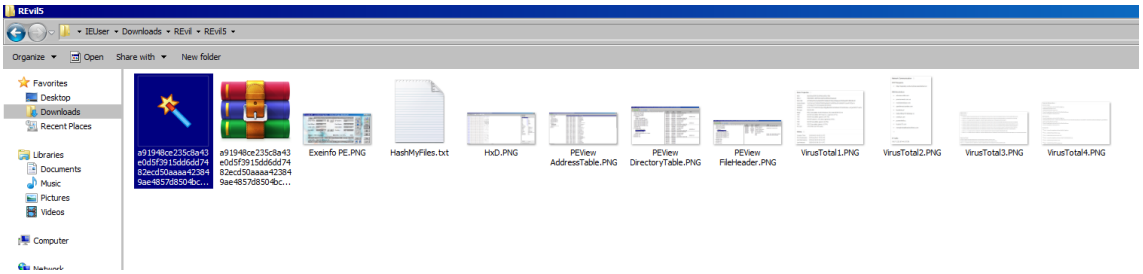






MUESTRA 5:

A la hora de modifica 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 ningún tipo de consecuencia de tipo malware.



CONCLUSION

Aunque se traten de diferentes muestras, los resultados obtenidos en los análisis son casi idénticos. Para empezar, lo 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	66c04002fbda157960a612491acc2839	20/10/2020	Gen:Heur.Ransom.REntS.Gen1 (B)”
Avaddon4	64497a0fa912f0e190359684de92be2d	06/06/2020	Gen:Heur.Mint.Titirez.VuW@IWozZSmG
Avaddon5	7f02bf886c4b01b21217126cb9fec95c	23/06/2020	Gen:Heur.Mint.Titirez.1.23
Avaddon6	c83f30c065f7f61428eac2370ddb4f53	24/06/2020	Gen:Heur.Variadic.A.23.4
Avaddon7	1d71701e9824c730dffbcaef428a2f64	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:Cs6JmdFn5KLOCgHWcAvcrOcEsKfR9uA7rmFbbbbpccf: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
<HKLM>\Software\Wow6432Node\Microsoft\Tracing\ulcgjhm_RASAPI32
<HKLM>\Software\Wow6432Node\Microsoft\Tracing\ulcgjhm_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\{c84d25co-f368-11e4-889d-806e6f6e6963}\MaxCapacity
+ <HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{c84d25co-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

Processes Terminated

<SYSTEM32>\wbem\wmiprvse.exe

%WINDIR%\syswow64\wbem\wmic.exe

%WINDIR%\syswow64\vssadmin.exe

%WINDIR%\servicing\trustedinstaller.exe

Processes Tree

↳ 2844 - <PATH_SAMPLE.EXE>

↳ 992 - %WINDIR%\syswow64\wbem\wmic.exe

↳ 2044 - %WINDIR%\syswow64\vssadmin.exe

↳ 2064 - %WINDIR%\syswow64\wbem\wmic.exe

↳ 1816 - %WINDIR%\syswow64\vssadmin.exe

↳ 2092 - %WINDIR%\syswow64\wbem\wmic.exe

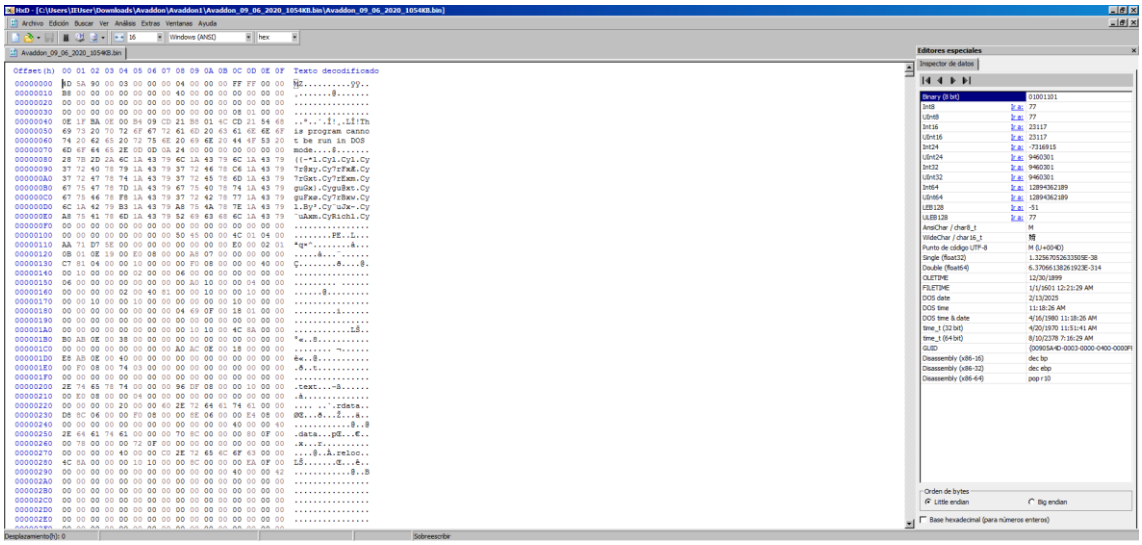
↳ 2984 - %WINDIR%\syswow64\vssadmin.exe

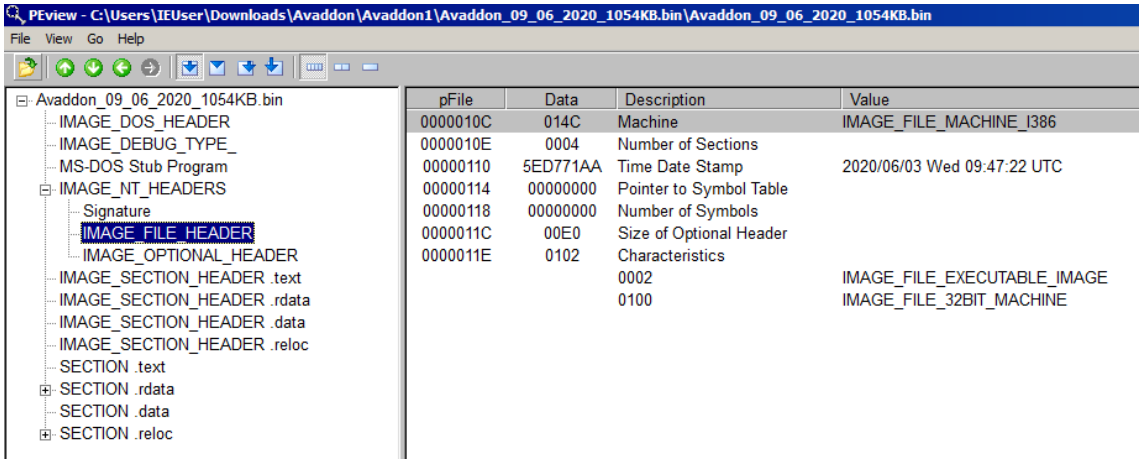
↳ 1020 - <SYSTEM32>\svchost.exe

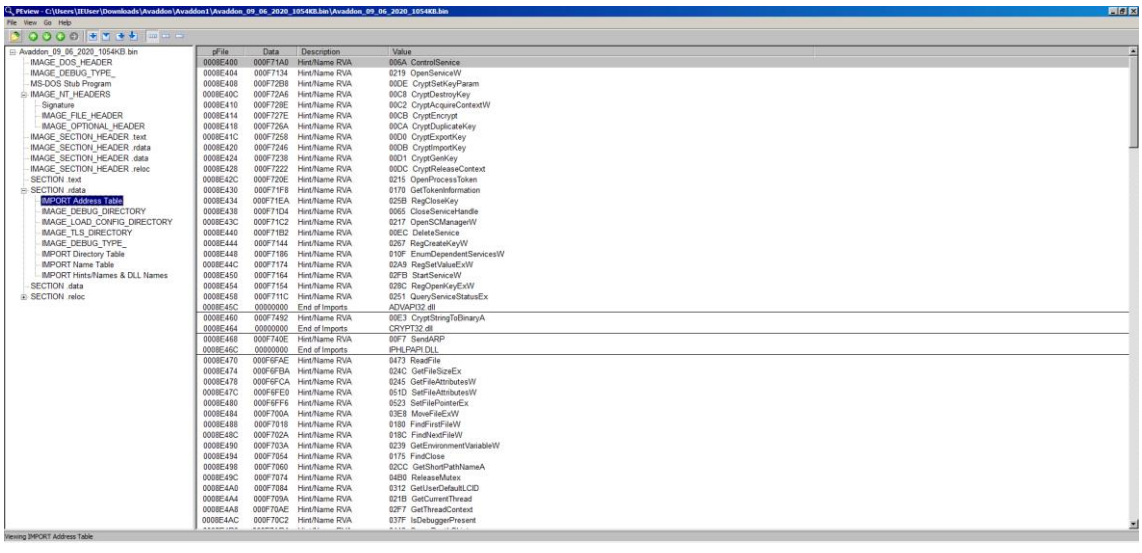
↳ 860 - <SYSTEM32>\svchost.exe

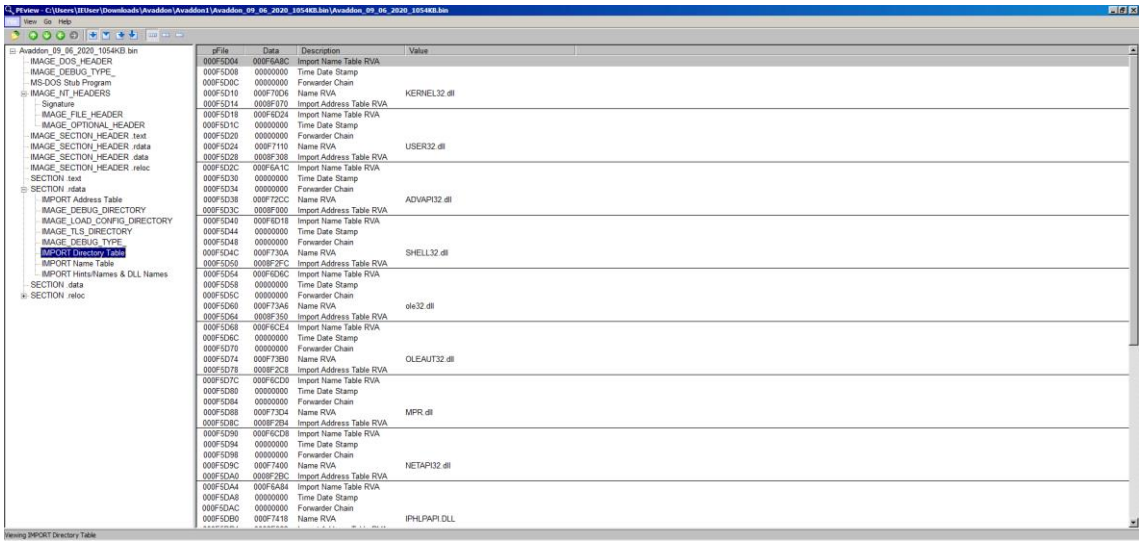
↳ 2396 - <SYSTEM32>\taskeng.exe

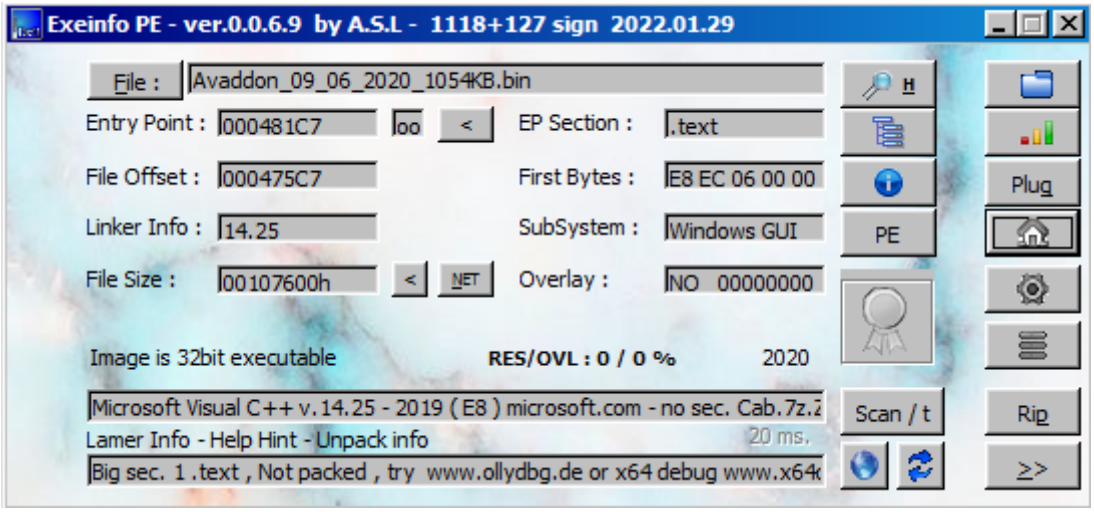
```
================================================
Filename          : Avaddon_09_06_2020_1054KB.bin
MD5               : c9ec0d9ff44f445ce5614cc87398b38d
SHA1              : 591ffe54bac2c50af61737a28749ff8435168182
CRC32             : 5c77ad84
SHA-256           : 05af0cf40590aef24b28fa04c6b4998b7ab3b7f26e60c507adb84f3d837778f2
SHA-512           : c340baeb66fc46830b6b77b2583033ade6e10b3de04d82ece7e241107afe741442585bf2ea9d6496af93143c37e9676d4f1e1d301d55632b88b12daadadd43f0
SHA-384           : ac6c07905c0e58a343fa1bc0b6037c91916771ead6f9ec32e2f5c303c5cbca8a622a3e8bfbf8bbdbe7d9f117ad79754c
Full Path         : C:\Users\IEUser\Downloads\Avaddon\Avaddon1\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
================================================
```




PEview - C:\Users\IEUser\Downloads\Avaddon\Avaddon1\Avaddon_09_06_2020_1054KB.bin\Avaddon_09_06_2020_1054KB.bin
File View Go Help
Avaddon_09_06_2020_1054KB.bin
IMAGE_DOS_HEADER
IMAGE_DEBUG_TYPE_
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 .reloc
SECTION .text
SECTION .rdata
SECTION .data
SECTION .reloc
pFile Data Description Value
0000010C 014C Machine IMAGE_FILE_MACHINE_I386
0000010E 0004 Number of Sections
00000110 5ED771AA Time Date Stamp 2020/06/03 Wed 09:47:22 UTC
00000114 00000000 Pointer to Symbol Table
00000118 00000000 Number of Symbols
0000011C 00E0 Size of Optional Header
0000011E 0102 Characteristics
0002 IMAGE_FILE_EXECUTABLE_IMAGE
0100 IMAGE_FILE_32BIT_MACHINE







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	fc42cbd5939fcb8b6851021497041c80acd81ce7a43b952ab7807d5a05d2ed97
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% "965650925-1742588889-815005604297997287392118414309347 94-186087007-239538697

%CONHOST% "1690847865-1646689566-198359547476315672363841732203596247574013865-1159207040

%CONHOST% "157875538984634274 9-996002207-336189444-981002267-1622663493626387941-1651395670

%CONHOST% "901094332-133340804820130327188890017511181227893706538 9-18634858902719184

%CONHOST% "-100895108519430569 59-111397224650297213715662880 84-979532928-16353184241947206807

wmic SHADOWCOPY DELETE /nointeractive

vssadmin Delete Shadows /All /Quiet

Processes Tree

↳ 1140 - %CONHOST% "965650925-1742588889-815005604297997287392118414309347 94-186087007-239538697

↳ 2848 - %CONHOST% "1690847865-1646689566-198359547476315672363841732203596247574013865-1159207040

↳ 1988 - %CONHOST% "157875538984634274 9-996002207-336189444-981002267-1622663493626387941-1651395670

↳ 2772 - %CONHOST% "901094332-133340804820130327188890017511181227893706538 9-18634858902719184

↳ 2792 - %CONHOST% "-100895108519430569 59-111397224650297213715662880 84-979532928-16353184241947206807

↳ 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%

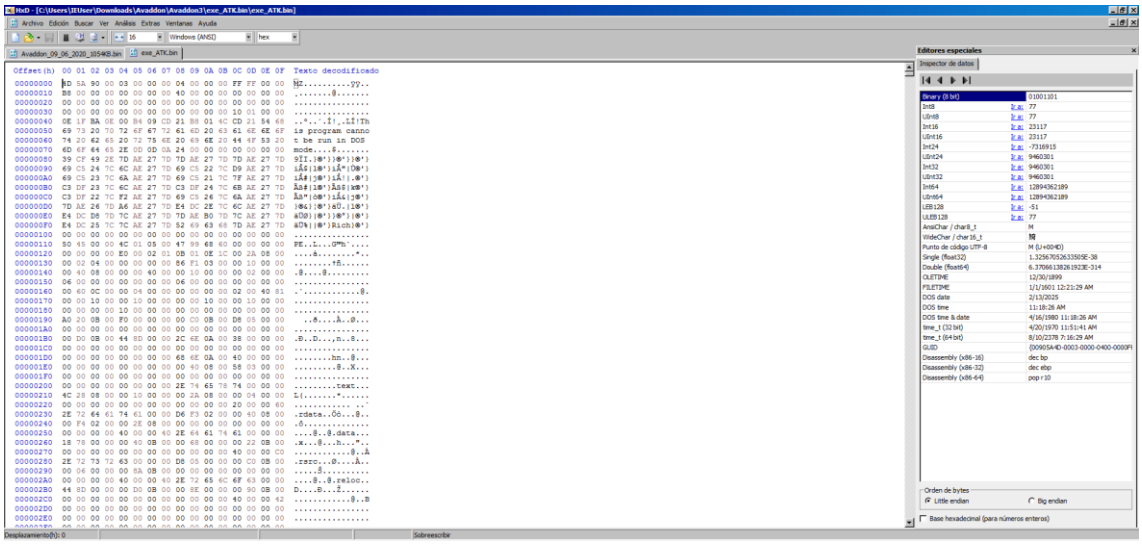
↳ 1252 - vssadmin Delete Shadows /All /Quiet

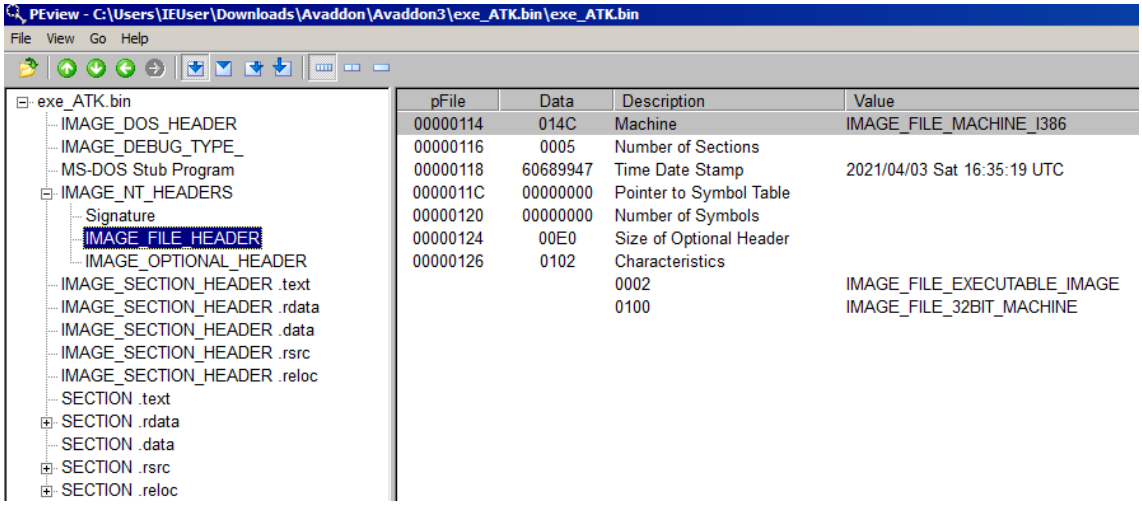
↳ 2836 - wmic SHADOWCOPY DELETE /nointeractive

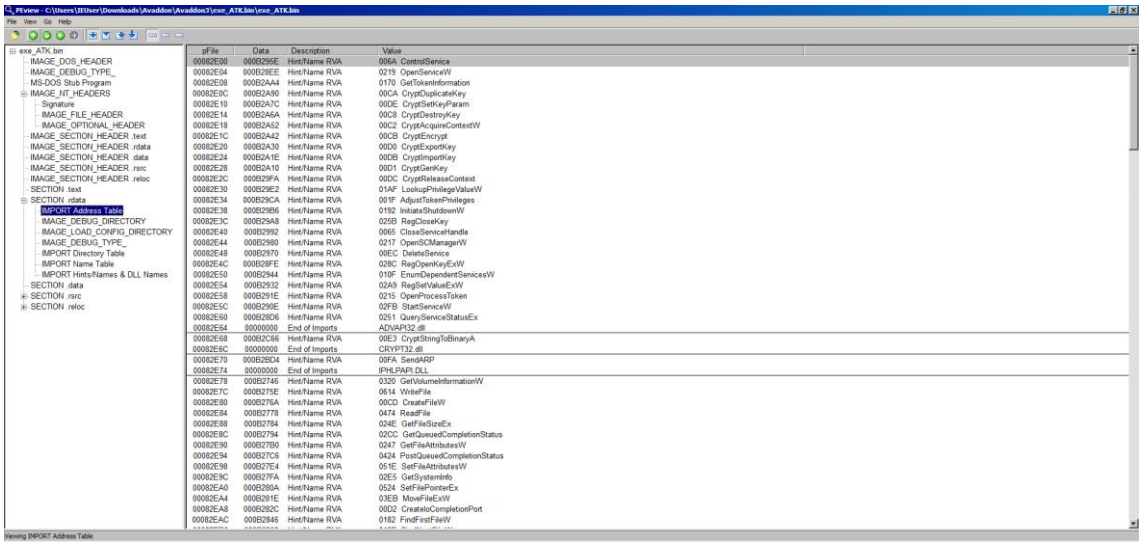
↳ 2172 - vssadmin Delete Shadows /All /Quiet

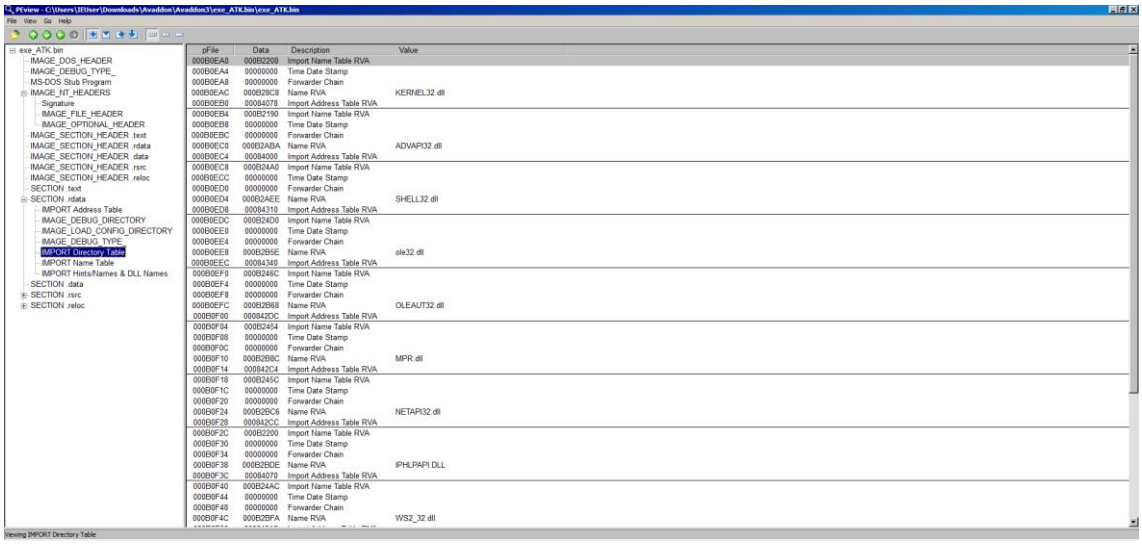
↳ 1156 - wmic SHADOWCOPY DELETE /nointeractive

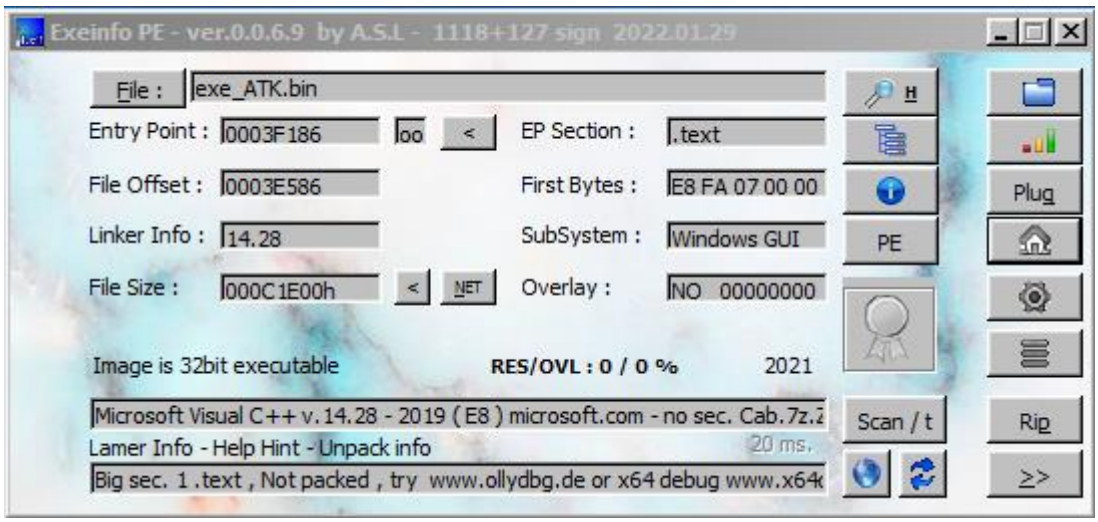
```
================================================
Filename          : exe_ATK.bin
MD5               : 4c08871e90158382f7df438bb3df373c
SHA1              : 600fec77e276a5a9c9477c6c327958e5048eb67c
CRC32             : 5ac63a38
SHA-256           : fc42cbd5939fcb8b6851021497041c80acd81ce7a43b952ab7807d5a05d2ed97
SHA-512           : c716c15d322afca842487972c1b2f4d0f5dc2caf0a16b6ba3e560467120d1110df6594a5e0924af17b9e0956eecf63b97b11482798c4255a6673f6751fdbeaa8
SHA-384           : 365e3fa204bc6fc02e5276a011c91b3e668368b7be8b35baa4ffd52d8e1eecd01b98e974b61e4df71c6b4b07971c0a1b
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
================================================
```




PEview - C:\Users\IEUser\Downloads\Avaddon\Avaddon3\exe_ATK.bin\exe_ATK.bin
File View Go Help
exe_ATK.bin
IMAGE_DOS_HEADER
IMAGE_DEBUG_TYPE_
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
pFile Data Description Value
00000114 014C Machine IMAGE_FILE_MACHINE_I386
00000116 0005 Number of Sections
00000118 60689947 Time Date Stamp 2021/04/03 Sat 16:35:19 UTC
0000011C 00000000 Pointer to Symbol Table
00000120 00000000 Number of Symbols
00000124 00E0 Size of Optional Header
00000126 0102 Characteristics
0002 IMAGE_FILE_EXECUTABLE_IMAGE
0100 IMAGE_FILE_32BIT_MACHINE







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	6baf357b0cd827321a087fdf06e1179a
Rich PE header hash	eeb3a440d3c8d698b4fe961a97fb024f
SSDEEP	12288:d1820d0A4YBAdovipWC+TEd+fmOwAjWyUeStuuMUu3Qri6ZNBARyhz:dN0dT4YBAdovipWC+TEd+OvPyUeKwkih
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\A\{f496b51a-9ea4-11ea-8c2a-167c9a143b03}\DefaultObjectStore\LruList\0000000000002B99\ObjectLru
+ \\REGISTRY\A\{f496b51a-9ea4-11ea-8c2a-167c9a143b03}\DefaultObjectStore\LruList\0000000000002B99\ObjectId
+ \\REGISTRY\A\{f496b51a-9ea4-11ea-8c2a-167c9a143b03}\DefaultObjectStore\LruList\CurrentLru
+ \\REGISTRY\A\{f496b51a-9ea4-11ea-8c2a-167c9a143b03}\DefaultObjectStore\LruList\0000000000002B91\ObjectLru
+ \\REGISTRY\A\{f496b51a-9ea4-11ea-8c2a-167c9a143b03}\DefaultObjectStore\LruList\0000000000002B91\ObjectId
+ \\REGISTRY\A\{f496b51a-9ea4-11ea-8c2a-167c9a143b03}\DefaultObjectStore\LruList\0000000000002B97\ObjectLru
+ \\REGISTRY\A\{f496b51a-9ea4-11ea-8c2a-167c9a143b03}\DefaultObjectStore\LruList\0000000000002B97\ObjectId
+ \\REGISTRY\A\{f496b51a-9ea4-11ea-8c2a-167c9a143b03}\DefaultObjectStore\ObjectTable\663\Indexes\FileIdIndex-{853201e6-2d75-11ea-a138-806e6f6e6963}\10000000097C6
+ HKLM\SYSTEM\ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\{B5DA8633-954C-4495-AE46-0BB5B5FB1CDC}\Connection\PnpInstanceID
+ HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\RestartManager\Session0007\Owner

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

Processes Tree

↳ 2956 - %CONHOST% "-260849738941439525-1029886583-1420825593447920167860034218860575686-1389866313

↳ 2144 - %CONHOST% "2089844091877143898710516516-1131488703-4108436301001671822159476648 7-1327803531

↳ 2140 - %CONHOST% "1919300169-5865450192098464028416873827-1872497341139922601668516928074 5736633

↳ 2364 - %CONHOST% "-1534163988-1364208163-2122299713385083271430945848136393803 7-9920482021916321092

↳ 2096 - %windir%\System32\svchost.exe -k WerSvcGroup

↳ 1460 - %windir%\system32\vssvc.exe

↳ 2832 - %CONHOST% "-754413395-738616361-9715274061810577020178150296 6-1410551156-5992777771843068637

↳ 648 - %CONHOST% "2026979306191083045221057908185313888057724196915345250 75-243517029-1992540871

↳ 2228 - %CONHOST% "1016212533-1514765871125295892118518281661215953832-729584820606131 16-292718238

↳ 2896 - %windir%\system32\wbem\wmiprvse.exe

Process And Service Actions

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% "2089844091877143898710516516-1131488703-4108436301001671822159476648 7-1327803531

%CONHOST% "1919300169-5865450192098464028416873827-1872497341139922601668516928074 5736633

%CONHOST% "-1534163988-1364208163-2122299713385083271430945848136393803 7-9920482021916321092

%windir%\system32\vssvc.exe

%CONHOST% "-754413395-738616361-9715274061810577020178150296 6-1410551156-5992777771843068637

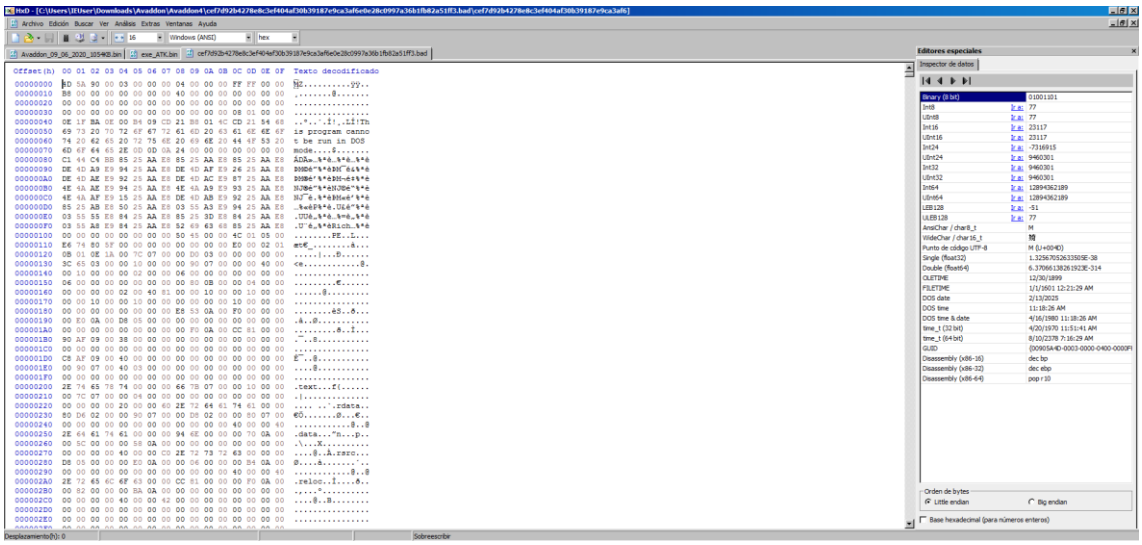
%CONHOST% "2026979306191083045221057908185313888057724196915345250 75-243517029-1992540871

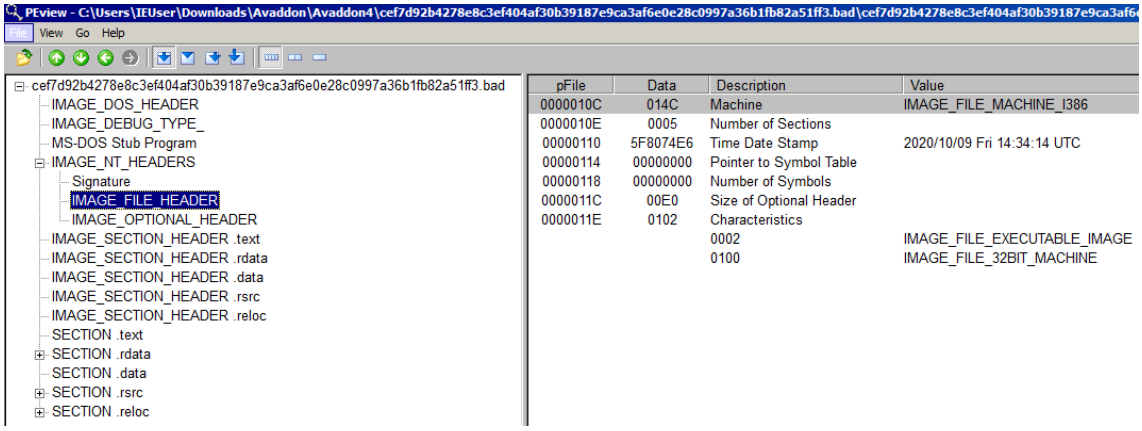
%CONHOST% "1016212533-1514765871125295892118518281661215953832-729584820606131 16-292718238

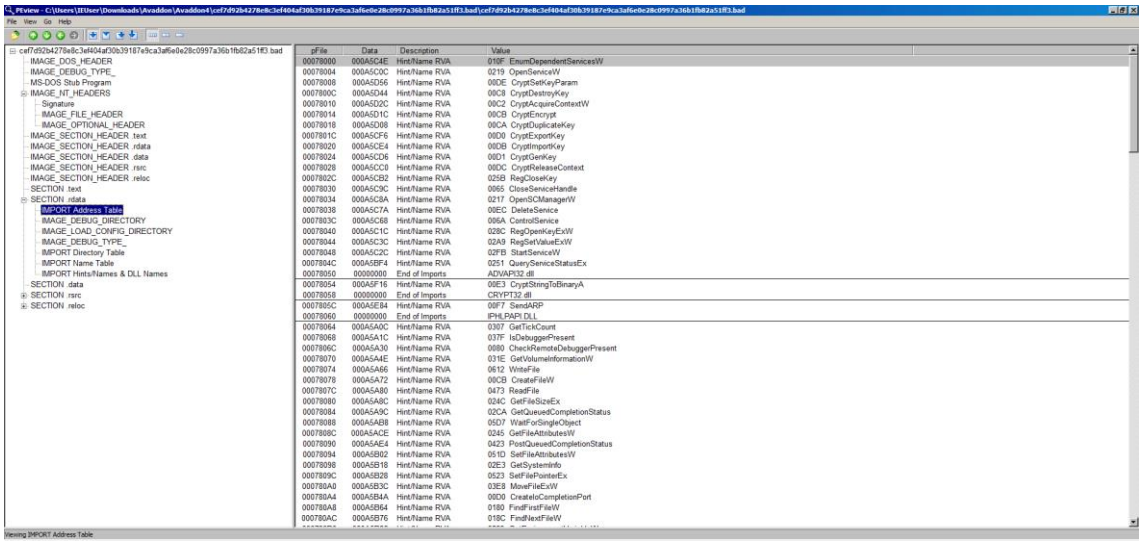
%CONHOST% "216982706-63329709-785246364-1887251676-1861466497842605838-1365409149-1072901913

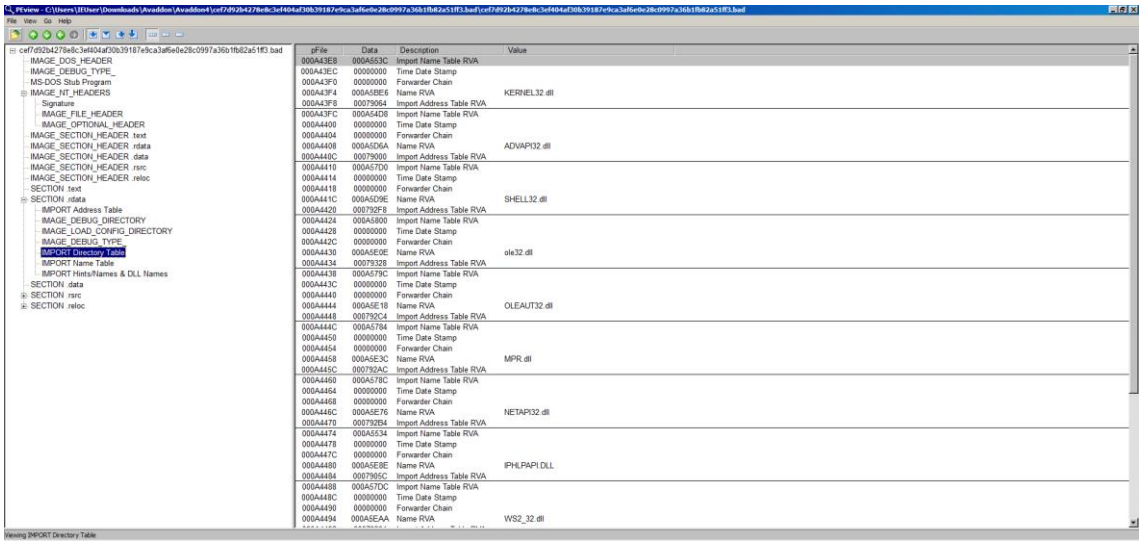
"%ComSpec%" /c vssadmin.exe Delete Shadows /All /Quiet

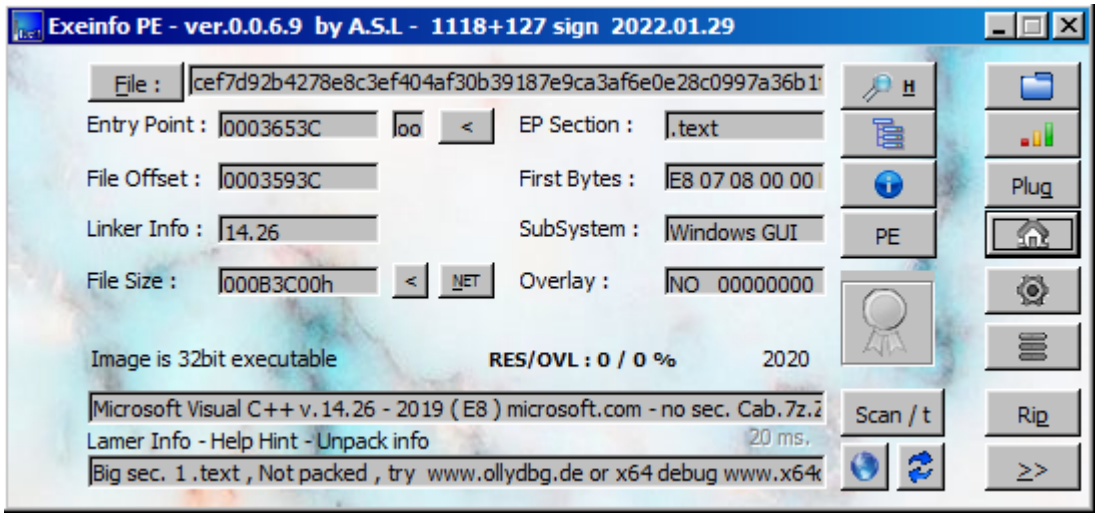
```
====================================================
Filename            : cef7d92b4278e8c3ef404af30b39187e9ca3af6e0e28c0997a36b1fb82a51ff3.bad
MD5                 : 66c04002fbda157960a612491acc2839
SHA1                : 27e1265900f37a7e8f7a8741d9f484ebaccf8176
CRC32               : b16c8036
SHA-256             : cef7d92b4278e8c3ef404af30b39187e9ca3af6e0e28c0997a36b1fb82a51ff3
SHA-512             : a9b3c475fc6e4c915a173286e12df8d9a140d390a4409156098a3f9c73ea9d6314ee89aa4cb81d5b6f46db4a014f1fd0b0762d6789c9a8c8344e9687b8e059ce
SHA-384             : 76b99d251b19a4939cf8f519e6fcab2c7e02b7878f53fb35d98611e8565e9545413f9363aef969e4fdc090ffe04ae7d3
Full Path           : C:\Users\IEUser\Downloads\Avaddon\Avaddon4\cef7d92b4278e8c3ef404af30b39187e9ca3af6e0e28c0997a36b1fb82a51ff3.bad\cef7d92b4278e8c3ef404af30b39187e9ca3af6e0e28c0997a36b1fb8
Modified Time       : 5/23/2022 9:42:07 AM
Created Time        : 5/23/2022 10:10:44 AM
Entry Modified Time: 5/23/2022 10:10:44 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
====================================================
```











MUESTRA 4:

53 de 70

Microsoft: Undetected

G

Data: “Gen:Heur.Mint.Titirez.VuW@IWozZSmG”

Basic Properties

MD5	64497a0fa912f0e190359684de92be2d
SHA-1	2fb1c523b8fc9bb082ef5b66c5a5537b3f6026c3
SHA-256	9c9c4f20e4be9403e80e4f4bc09dcdcabdfcfd061950d7a226fa19b220e6d3bd
Vhash	075056657d1d155az57nz2ez3
Authentihash	29d7ebc009856c731a9f7804bd216c48ac43f69e84e0703aa5b0b50794a90623
Imphash	9943a4c29092af4ae3928f37f95eddad
Rich PE header hash	f7f6f19554250bf39b1b01b1b7865271
SSDEEP	12288:vBiWJbNtHpOIqPw9aKojrO3LcHvC/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\rsa\s-1-5-21-1960123792-2022915161-3775307078-1001\f58155b4b1d5a524ca0261c3ee99fb50_36d1130a-ac2e-44f7-9dc1-e424fbcbe0ee

%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

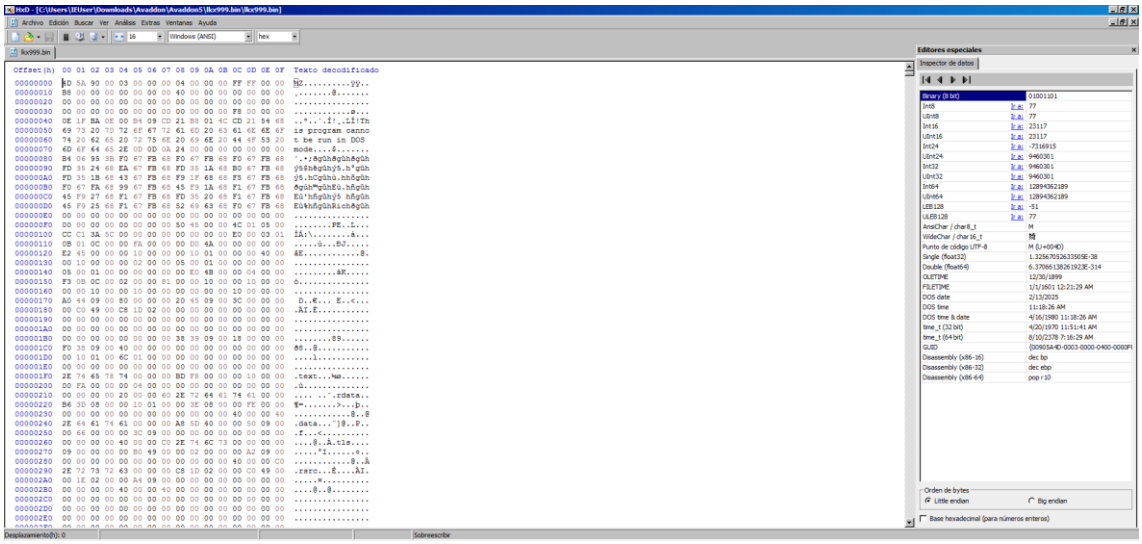
%WINDIR%\syswow64\wbem\wmic.exe

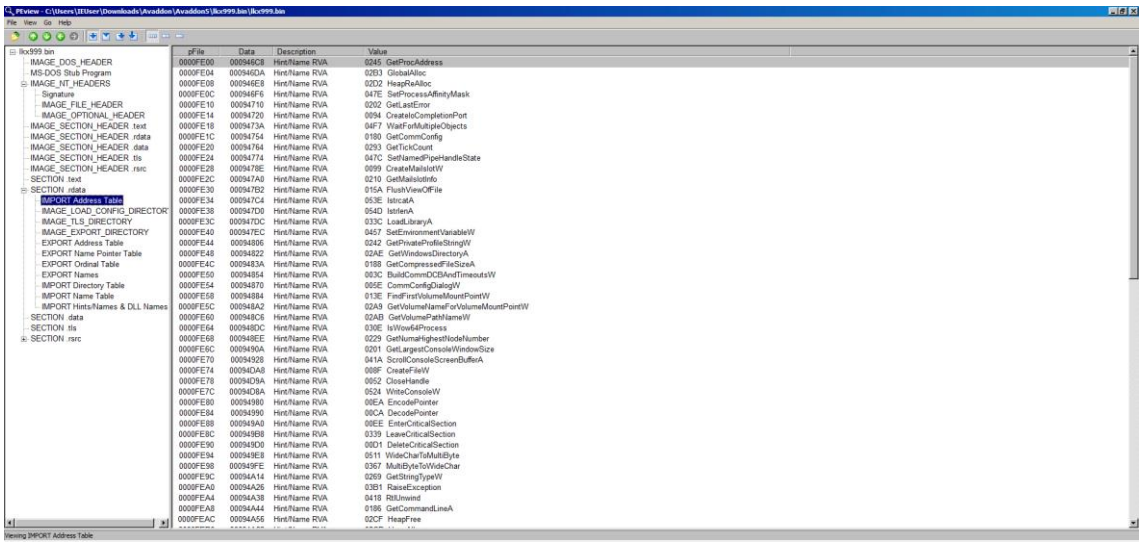
%WINDIR%\syswow64\vssadmin.exe

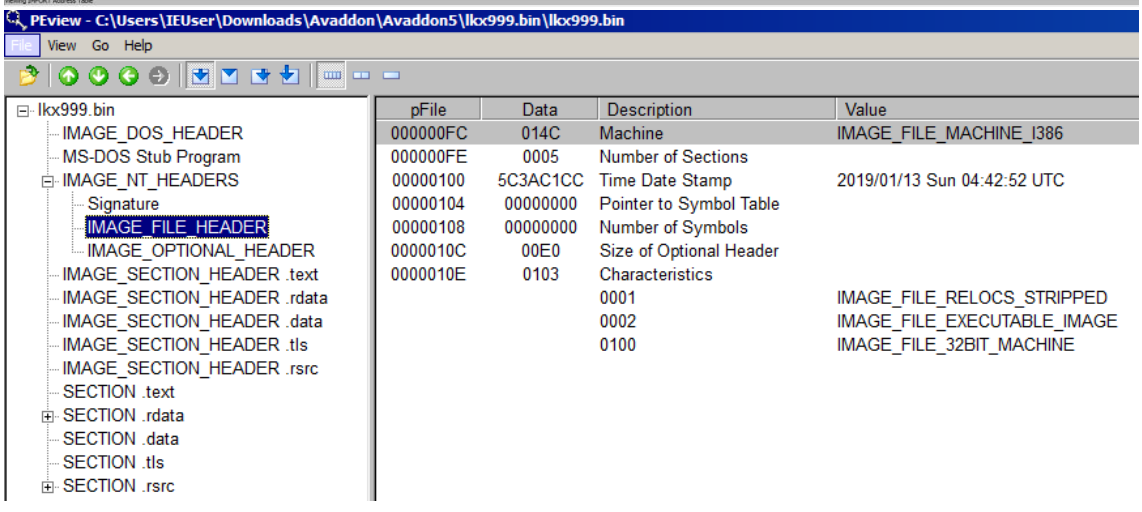
Processes Tree

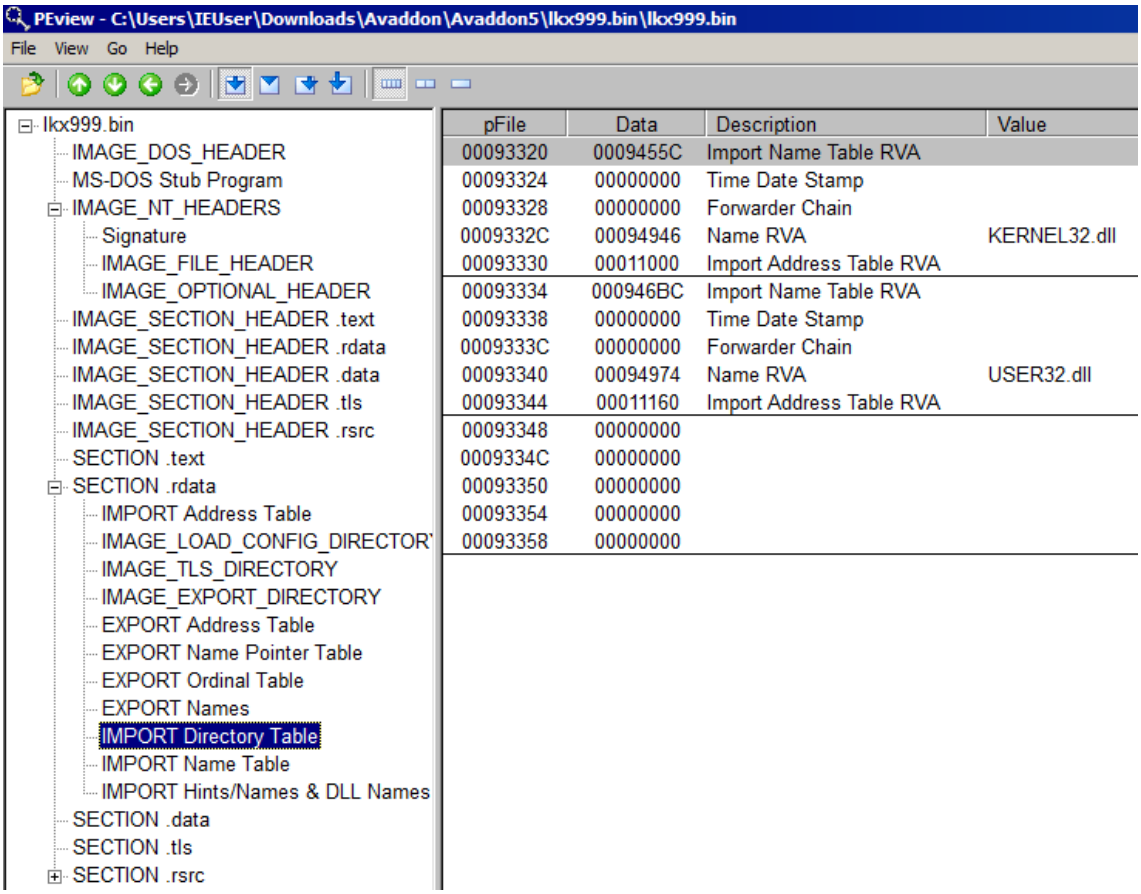
- 1684 - <PATH_SAMPLE.EXE>
  - 3016 - %WINDIR%\syswow64\wbem\wmic.exe
  - 2264 - %WINDIR%\syswow64\vssadmin.exe
  - 2916 - %WINDIR%\syswow64\wbem\wmic.exe
  - 2772 - %WINDIR%\syswow64\vssadmin.exe
  - 2276 - %WINDIR%\syswow64\wbem\wmic.exe
  - 3060 - %WINDIR%\syswow64\vssadmin.exe
- 508 - <SYSTEM32>\svchost.exe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

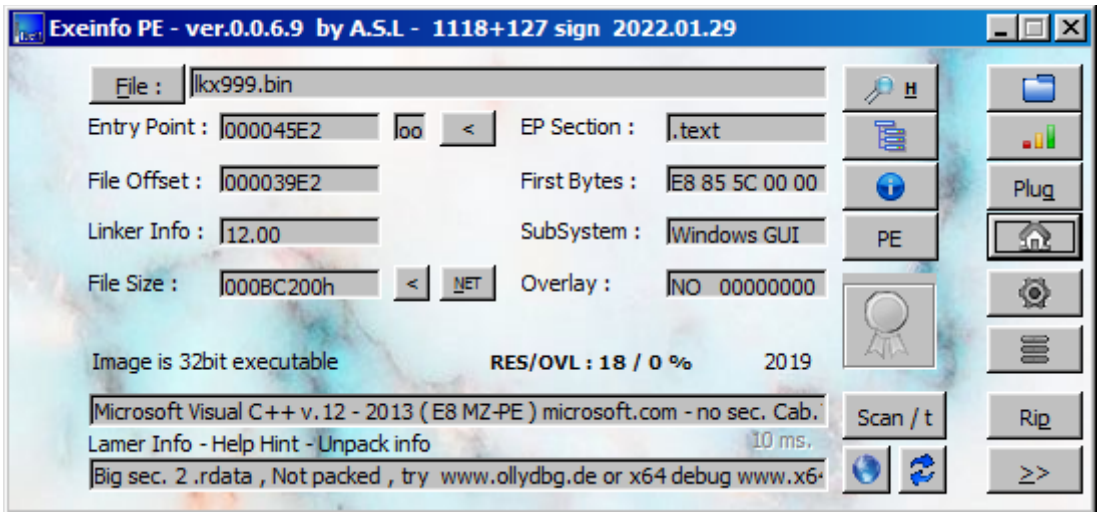
```
================================================
Filename          : lkx999.bin
MD5               : 64497a0fa912f0e190359684de92be2d
SHA1              : 2fb1c523b8fc9bb082ef5b66c5a5537b3f6026c3
CRC32             : 74441f2c
SHA-256           : 9c9c4f20e4be9403e80e4f4bc09dcdcabdfcfd061950d7a226fa19b220e6d3bd
SHA-512           : 96a17a8d601e11b005badb47ac3a3522da697f62707beb05f2dc5169e0d8cc343a4c7cf41fbbde09b2d10abf4c4cf3ab293cccaf40a0b65787130c7484690f30
SHA-384           : 53a6d61e67816e7d9ae7d963415e6676b4c22671dedf62bd1e902790bd92f9e6c46e12ffa069e9150ad26e8111035c2c
Full Path         : C:\Users\IEUser\Downloads\Avaddon\Avaddon5\lkx999.bin\lkx999.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\llkx999.bin\llkx999.bin
File View Go Help
llkx999.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 .rsrc
SECTION .text
SECTION .rdata
SECTION .data
SECTION .tls
SECTION .rsrc
pFile Data Description Value
000000FC 014C Machine IMAGE_FILE_MACHINE_I386
000000FE 0005 Number of Sections
00000100 5C3AC1CC Time Date Stamp 2019/01/13 Sun 04:42:52 UTC
00000104 00000000 Pointer to Symbol Table
00000108 00000000 Number of Symbols
0000010C 00E0 Size of Optional Header
0000010E 0103 Characteristics
0001 IMAGE_FILE_RELOCS_STRIPPED
0002 IMAGE_FILE_EXECUTABLE_IMAGE
0100 IMAGE_FILE_32BIT_MACHINE





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	86a8c98c8edbfbc61c34b1f85a0a428b
SSDEEP	12288:3m/rWGhAzP2oBMcjD6Bpd9dfyYajCa2FlNQbrL51kEGp0nWF8zzumY12BSzSCQ: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\Id
+ 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\vssvc.exe

%APPDATA%\Microsoft\%SAMPLENAME%

%CONHOST% "1443027416-1221665850-499906108920374635-120941158532863091594919369291652185

%CONHOST% "237995640166610565291751214 8-186124955-783075779728340981166012 5127-1905251365

%CONHOST% "1868586-181392036152473372116903487871233885618102729 5067-19317147-552551622

%CONHOST% "-1720500711-1495171606800849288-571409809-1524151418166369325685729 7584-58360345

%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% "-412116424693365075519422071-122437421214479355261119655654453693136170587 1864

Processes Tree

↳ 2764 - %windir%\system32\DllHost.exe /Processid:{3EB3C877-1F16-487C-9050-104DBCD66683}

↳ 2824 - %CONHOST% "21257611063157230545113559303784307761045388952198489551 1-1297747946-1133383901

↳ 2896 - %windir%\system32\vssvc.exe

↳ 2220 - %APPDATA%\Microsoft\%SAMPLENAME%

↳ 2956 - %CONHOST% "1443027416-1221665850-499906108920374635-120941158532863091594919369291652185

↳ 2868 - %CONHOST% "23799564016661056529175121 48-186124955-783075779728340981166012 5127-1905251365

↳ 3000 - %CONHOST% "1868586-181392036152473372116903487871233885618102729506 7-19317147-552551622

↳ 2404 - wmiadap.exe /F /T /R

↳ 2084 - %CONHOST% "-1720500711-1495171606800849288-571409809-152415141816636932568572975 84-58360345

↳ 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}

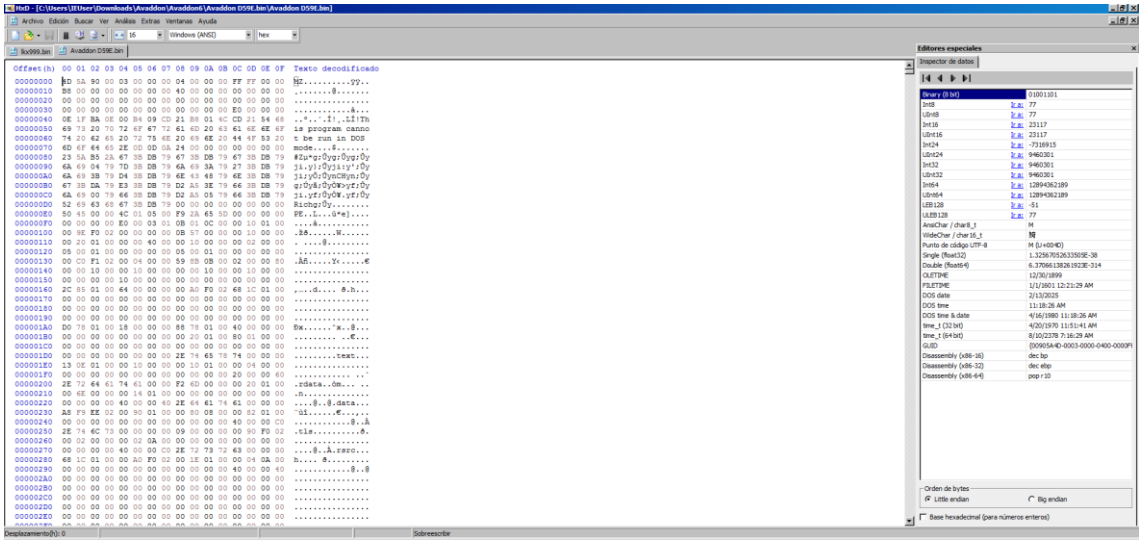
  ↳ 2228 - %APPDATA%\Microsoft\%SAMPLENAME%

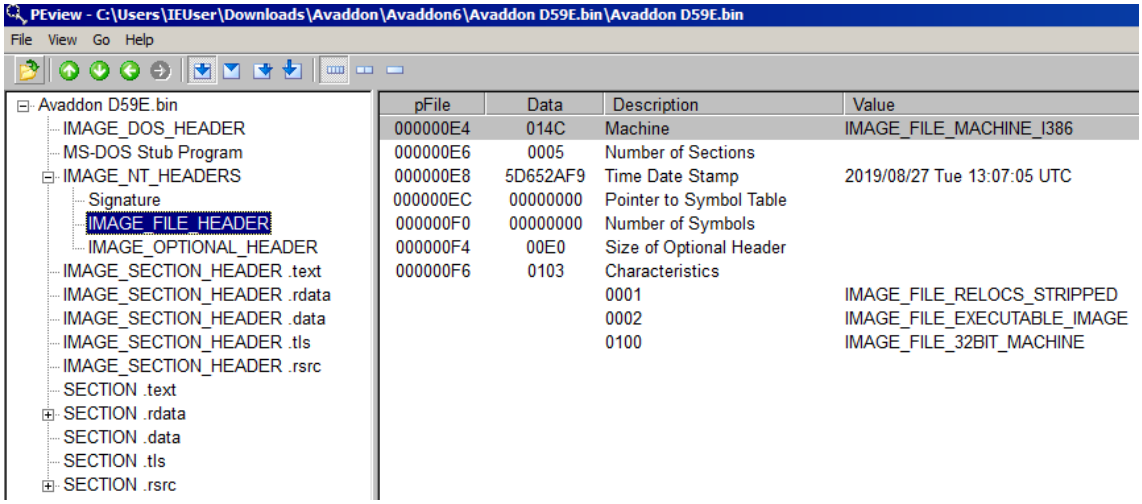
↳ 1824 - %windir%\System32\svchost.exe -k WerSvcGroup

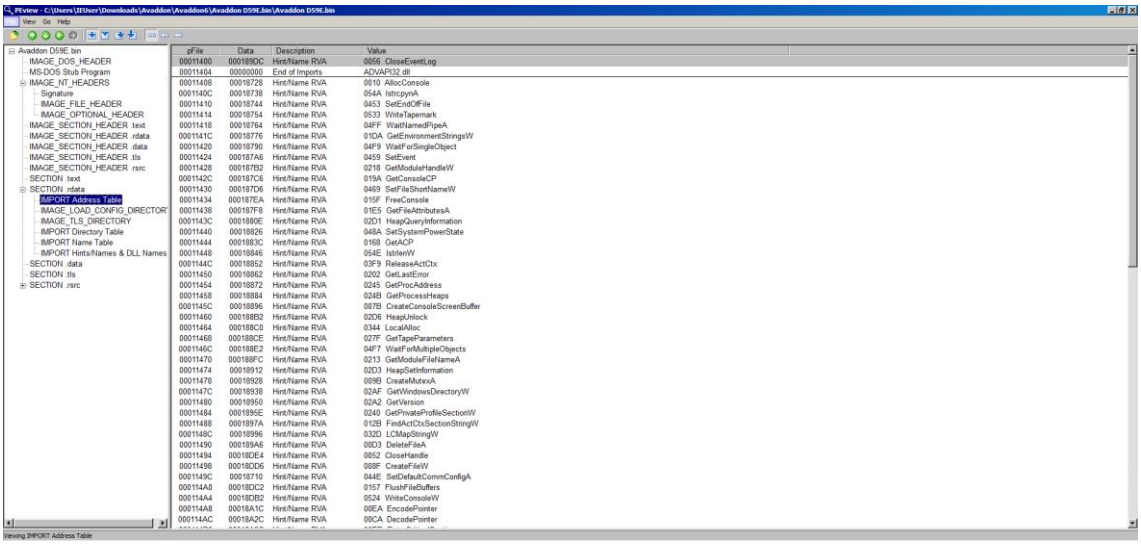
↳ 3040 - %CONHOST% "-41211642469336507551942207 1-122437421214479355261119655654453693136170587 1864

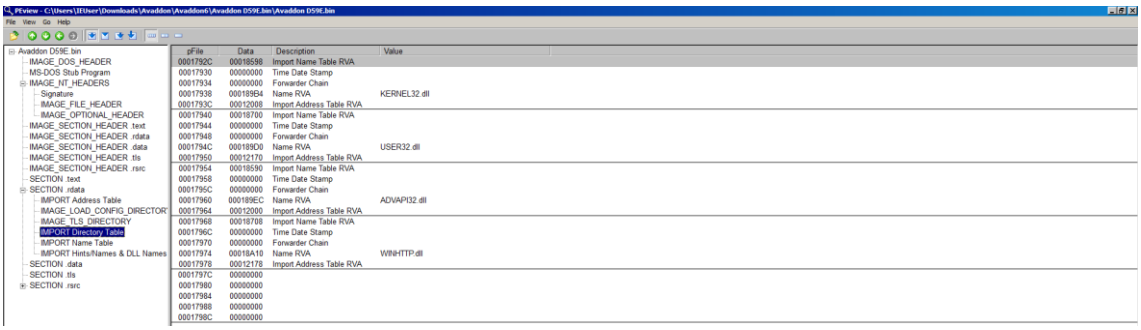
  ^

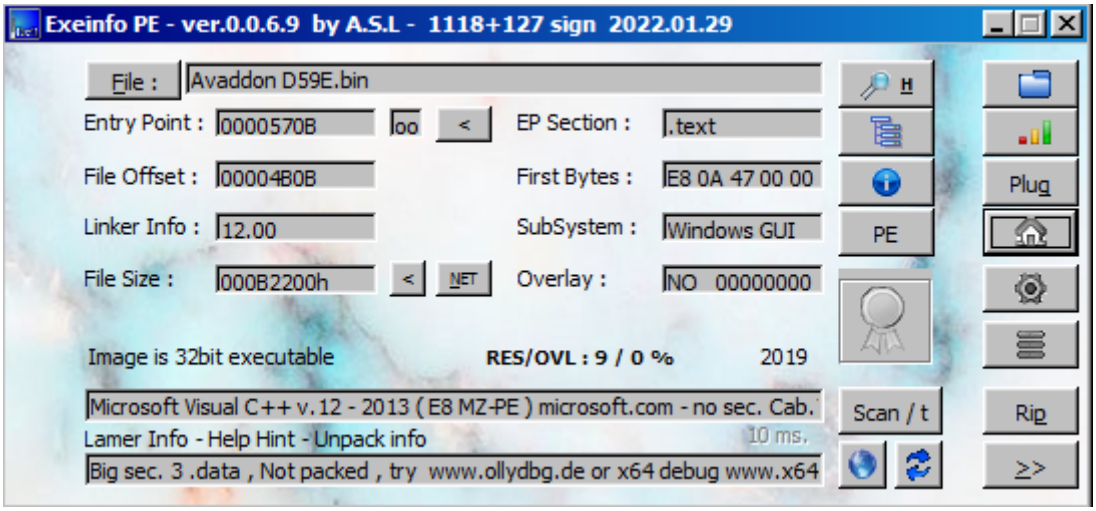
```
================================================
Filename            : Avaddon D59E.bin
MD5                 : 7f02bf886c4b01b21217126cb9fec95c
SHA1                : 7a060fac5d372811a8855d19bc8819204ac21416
CRC32               : fcb50910
SHA-256             : 4fd72c550987c7638e727c9d84b4940692bf94e101d3f5746bc4a8f377e49b37
SHA-512             : f10b6f5f5967912a79c43147d580de48861c5e2206a9558a03b3192618f293b0556747aa082948ff0108677834dbe4156264ae4f90b9e1816ab388a939c9ca9b
SHA-384             : 7b418bb6dab876d69f0bf1b75ce2ca86e5a4e6004114747a458f166583552c5bc9f8832141c54e1c4c7bcdbf17f92b0f
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
================================================
```











MUESTRA 6:

60 de 69

Microsoft: “Trojan:Win32/Vhapak.DEB!MTB”

GData: “Gen:Heur.Variadic.A.23.4”

Basic Properties

MD5	c83f30c065f7f61428eac2370ddb4f53
SHA-1	cfd70af0c89d7b00839c1d32852c53c603d35e32
SHA-256	bcb69244dc69a152af4dca3849bb4f3ca634ad785926304c672dbf8a3c38e7bc
Vhash	095066657d1d1d055az58lz
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% "1431808344167184924812789105301325436756-208102717136472687791535729O-765751054

↳ 2976 - %CONHOST% "-2060832753108186966220002391788541648051907011889754751563-1130245318888707380

↳ 2144 - %CONHOST% "-1625660353-368781985-5793939621507357770259291960-1070816484-703233938284088706

↳ 1044 - %CONHOST% "135016006-1826523016-365209721611325000-792108908-87420726-1981372252-1771182941

↳ 3020 - %CONHOST% "-1905368826194493783O-1948997755185695430l-2088921497176773124989552731284378432

↳ 1464 - %CONHOST% "-413275994-1168558164-2746645691918176499103006897 2-1053392575-1407275311-1099566014

↳ 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

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% "1431808344167184924812789105301325436756-208102717136472687791535729O-765751054

%CONHOST% "-2060832753108186966220002391788541648051907011889754751563-1130245318888707380

%CONHOST% "-1625660353-368781985-5793939621507357770259291960-1070816484-703233938284088706

%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\vssvc.exe

%APPDATA%\Microsoft\%SAMPLENAME%

wmic.exe SHADOWCOPY /nointeractive

vssadmin.exe Delete Shadows /All /Quiet

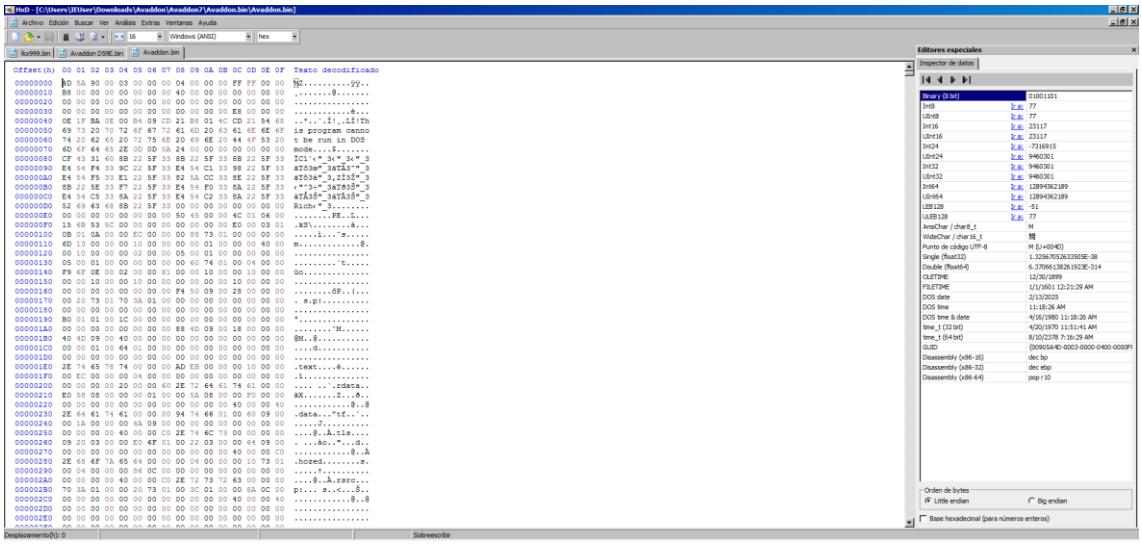
vssadmin.exe Delete Shadows /All /Quiet

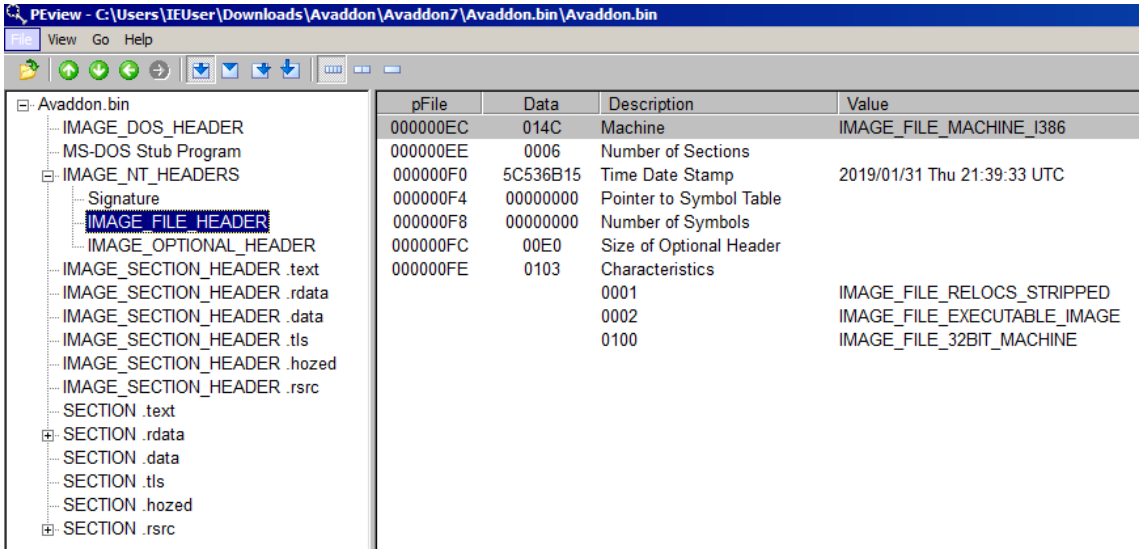
vssadmin.exe Delete Shadows /All /Quiet

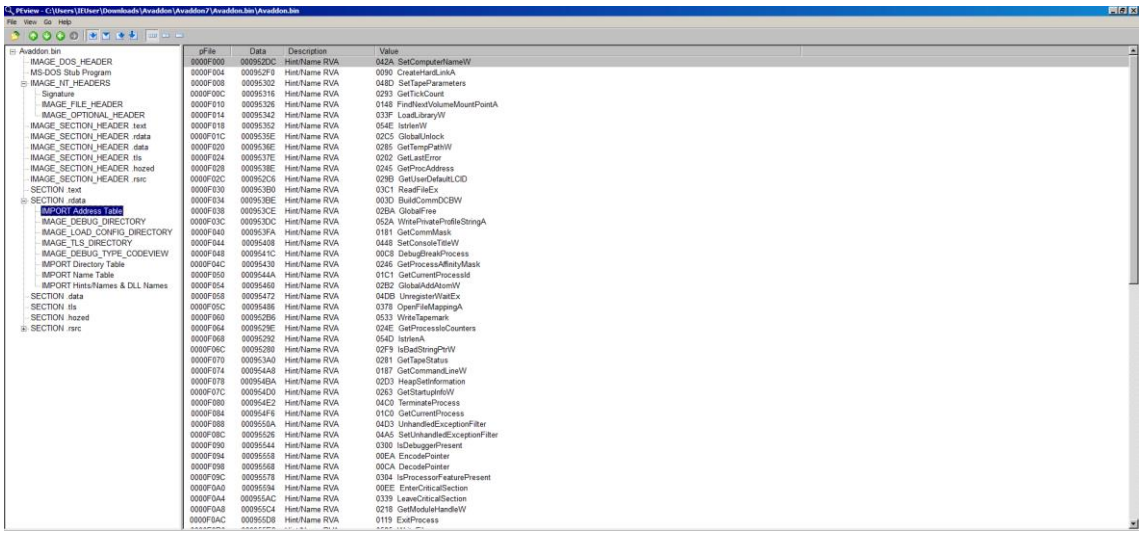
wmic.exe SHADOWCOPY /nointeractive

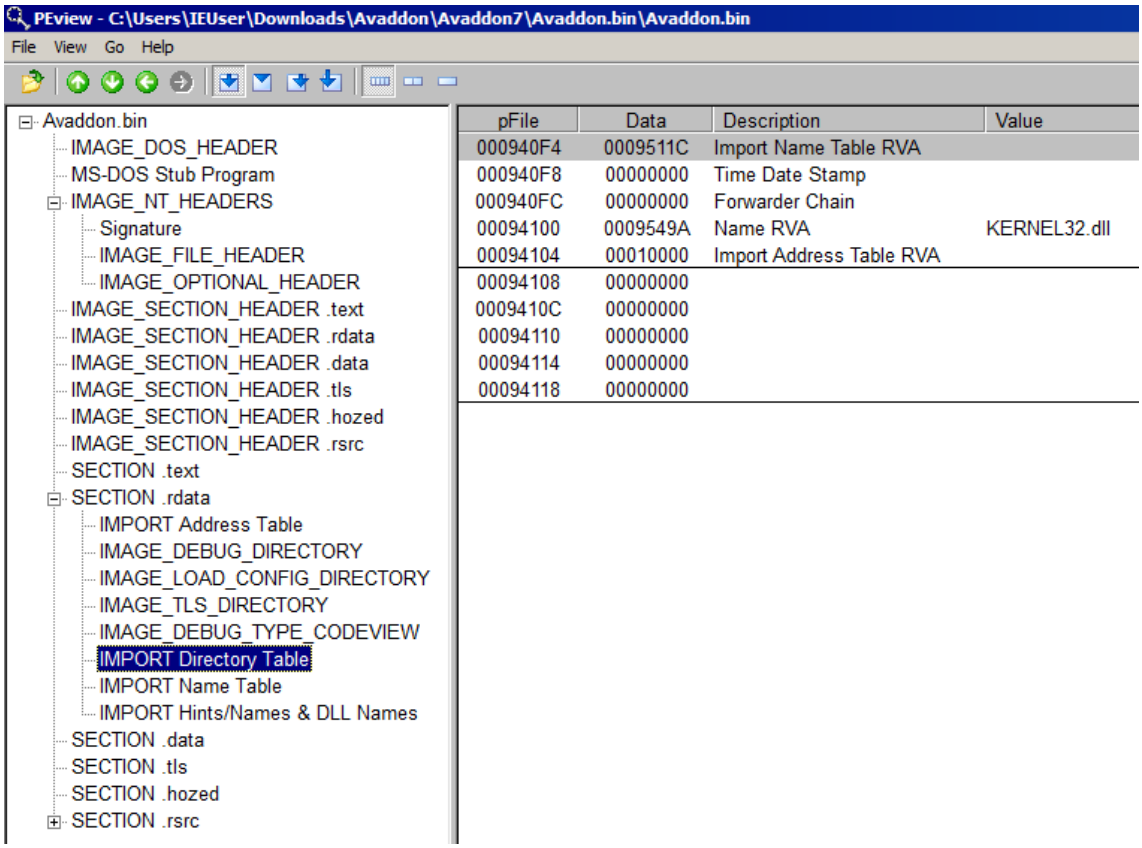
wmic.exe SHADOWCOPY /nointeractive

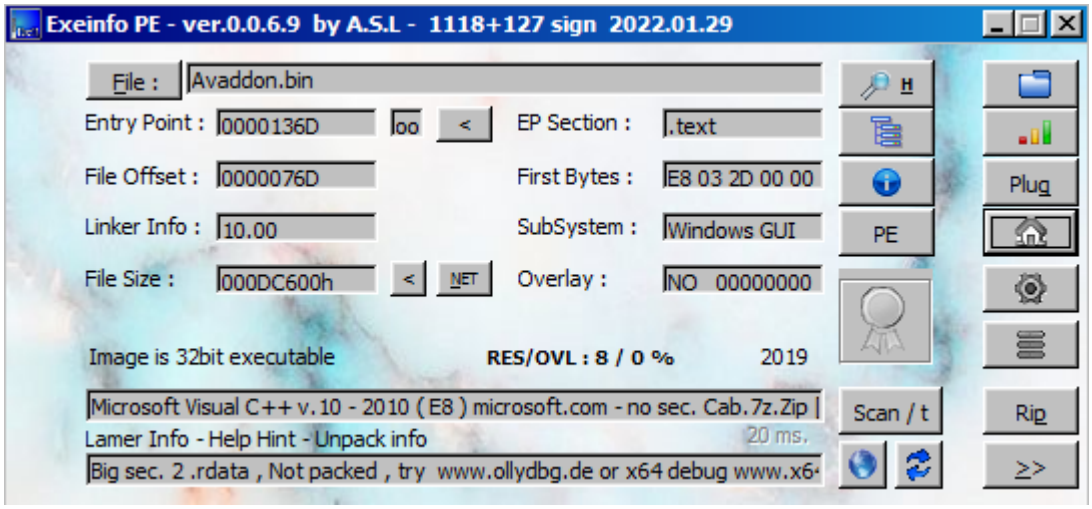
```
================================================
Filename          : Avaddon.bin
MD5               : c83f30c065f7f61428eac2370ddb4f53
SHA1              : cfd70af0c89d7b00839c1d32852c53c603d35e32
CRC32             : e63f795a
SHA-256           : bcb69244dc69a152af4dca3849bb4f3ca634ad785926304c672dbf8a3c38e7bc
SHA-512           : 26100fdf2bba32c0a2f5d27589e730e6af4a16b5cad16cb8ec6314e4291ca1858e35906645636617dacca7c72be6792b01f2bbc073c4468701326e8c889e1d51
SHA-384           : 192130017371271e29dc75d7a13469c5e842af2eac451157c30b9cd54e6f39454e749727f12db9e52eb4cfca1cf81cab
Full Path         : C:\Users\IEUser\Downloads\Avaddon\Avaddon7\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
================================================
```




PEview - C:\Users\IEUser\Downloads\Avaddon\Avaddon7\Avaddon.bin\Avaddon.bin
File View Go Help
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 .hozed
IMAGE_SECTION_HEADER .rsrc
SECTION .text
SECTION .rdata
SECTION .data
SECTION .tls
SECTION .hozed
SECTION .rsrc
pFile Data Description Value
000000EC 014C Machine IMAGE_FILE_MACHINE_I386
000000EE 0006 Number of Sections
000000F0 5C536B15 Time Date Stamp 2019/01/31 Thu 21:39:33 UTC
000000F4 00000000 Pointer to Symbol Table
000000F8 00000000 Number of Symbols
000000FC 00E0 Size of Optional Header
000000FE 0103 Characteristics
0001 IMAGE_FILE_RELOCS_STRIPPED
0002 IMAGE_FILE_EXECUTABLE_IMAGE
0100 IMAGE_FILE_32BIT_MACHINE







MUESTRA 7:

58 de 72

Microsoft: “Trojan:Win32/Ulise!MSR”

GData: “Gen:Variant.Ransom.Avaddon.2”

Basic Properties

MD5	1d71701e9824c730dffbcaef428a2f64
SHA-1	cfae85cd6b410c2605fc5b0149ed1a07ff3dc9e3
SHA-256	4f198228806c897797647eecce0f92d4082476b82781183062a55c417c0bb197
Vhash	016046655d156173z12z92z23z8065z23z21z71z67z
Authentihash	15b9299faf9cd57c08fb1af12ac8e8592e299ffede32be6e4cba4c9761f1880d
Imphash	1156e59d43883136ef73eee451e94e3d
Rich PE header hash	1f751e2aac4a31991712f656456c5442
SSDEEP	24576:Cs6JmdFn5KLOCgHWcAvcrOcEsKfR9uA7rmFbbbbpccf: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%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEAo3h2ReX7SMIk79G%2B0UDDw%3D
+ http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%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
+ HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\3913853E45C439A2DA718CDFB6F3E033E04FEE71
+ HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\SYSTEMCERTIFICATES\AUTHROOT\CERTIFICATES\5F3B8CF2F810B37D78B4CEEC1919C37334B9C774
+ HKU\S-1-5-21-3712457824-2419000099-45725732-1005\SOFTWARE\CLASSES\LOCAL SETTINGS\MUICACHE\E6\52C64B7E

Registry Keys Deleted

HKU\S-1-5-21-3712457824-2419000099-45725732-1005\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\INTERNET SETTINGS\WPAD\52-55-0A-00-02-02_52-56-00-00-00-02
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-B2BE4EC7A24D}
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\1d71701e9824c730dffbcaef428a2fnalysis_subject.exe

C:\Users\Lucas\AppData\Roaming\1d71701e9824c730dffbcaef428a2fnalysis_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\1d71701e9824c730dffbcaef428a2fnalysis_subject.exe

C:\Users\Lucas\AppData\Roaming\1d71701e9824c730dffbcaef428a2fnalysis_subject.exe

Processes Tree

↳ 2964 - 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

Local\ZonesLockedCacheCounterMutex

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

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

Local\ZonesCacheCounterMutex

Mutexes Opened

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

Modules Loaded

Runtime Modules

c:\windows\system32\imm32.dll

c:\windows\system32\rtutils.dll

c:\windows\syswow64\schannel.dll

c:\windows\syswow64\urlmon.dll

c:\windows\syswow64\usp10.dll

c:\windows\system32\rpcrtremote.dll

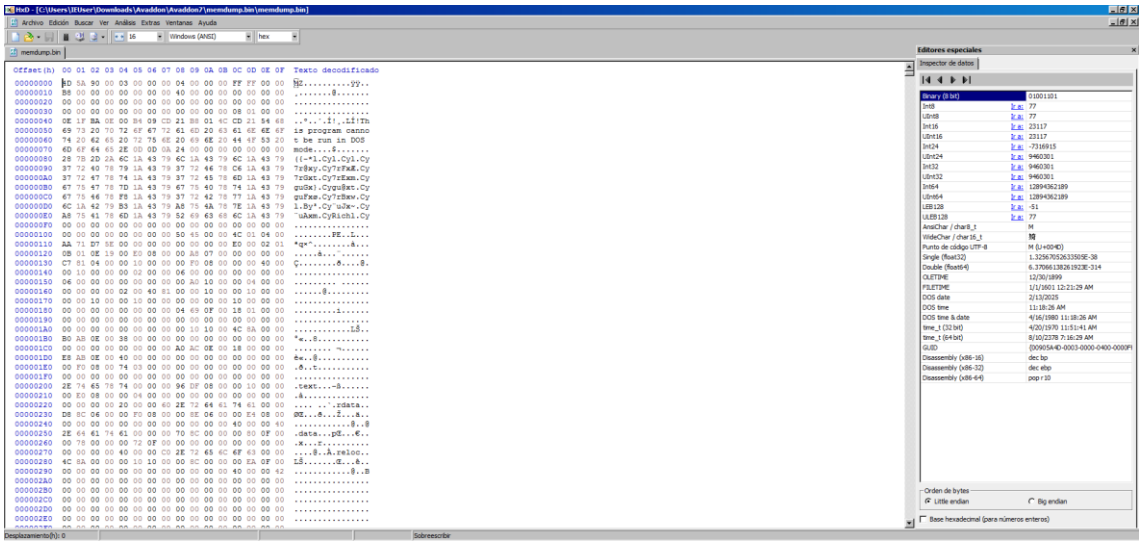
c:\windows\system32\napinsp.dll

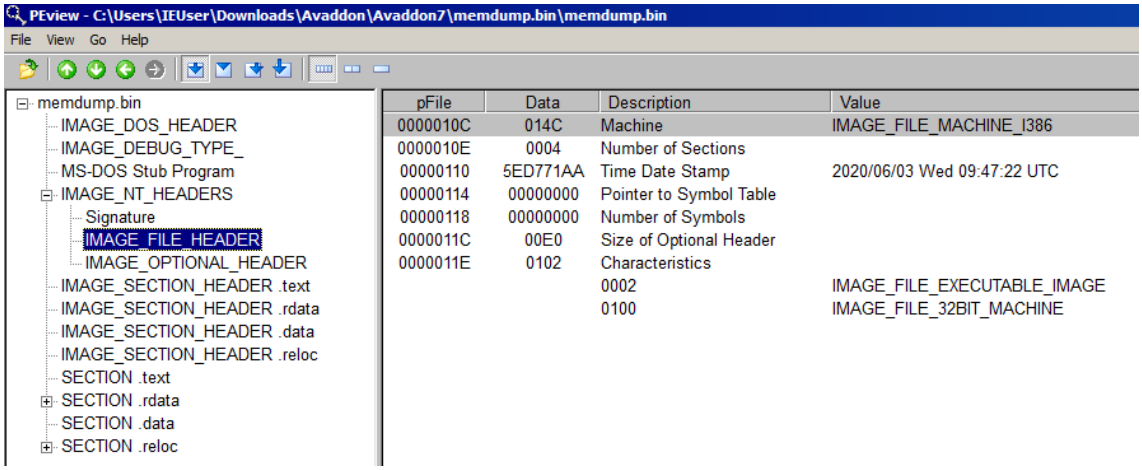
c:\windows\system32\apphelp.dll

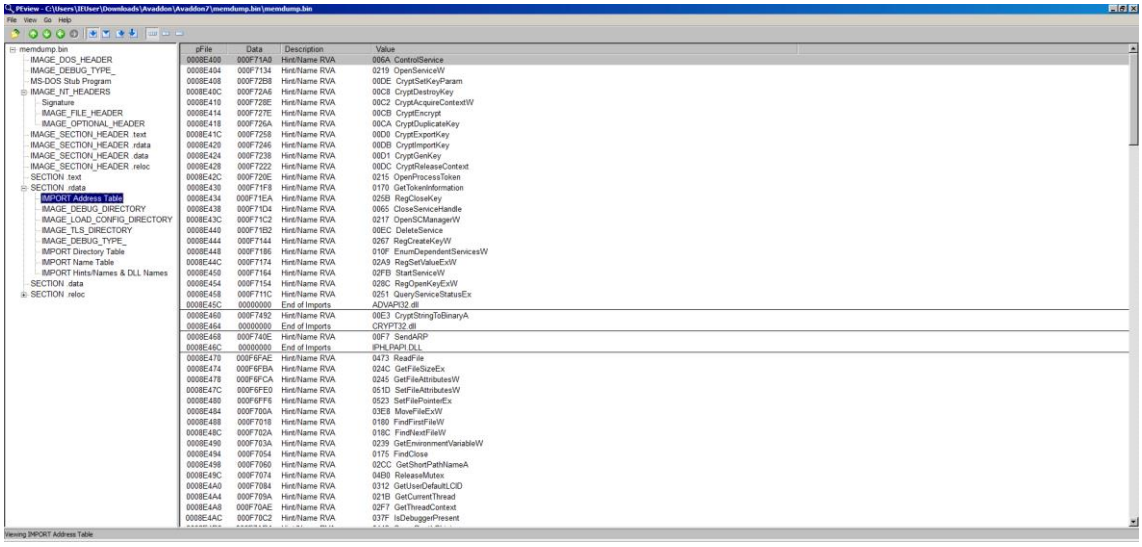
c:\windows\syswow64\gdi32.dll

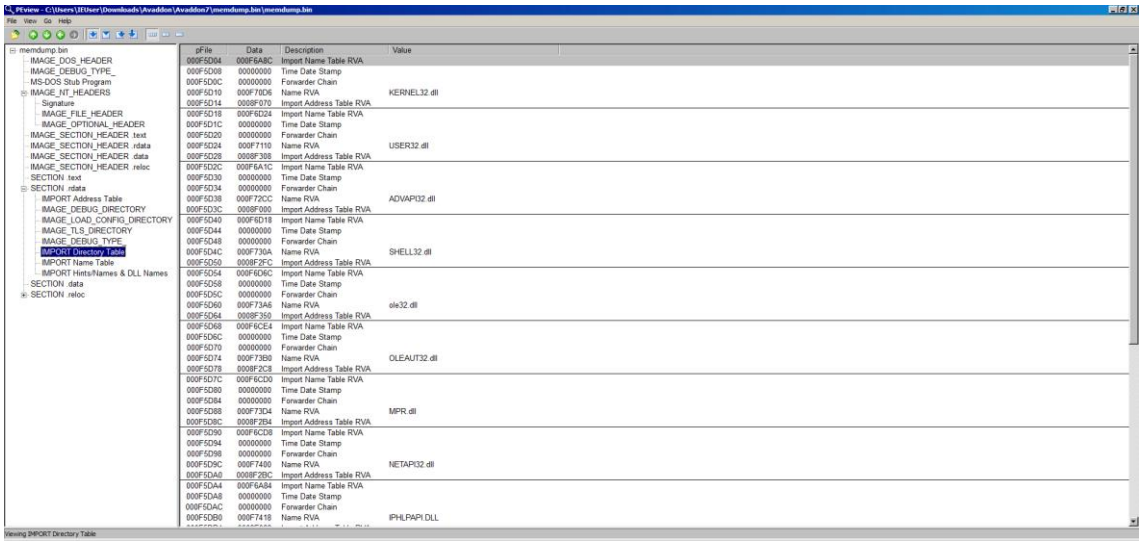
c:\windows\system32\dhcpcsvc6.dll

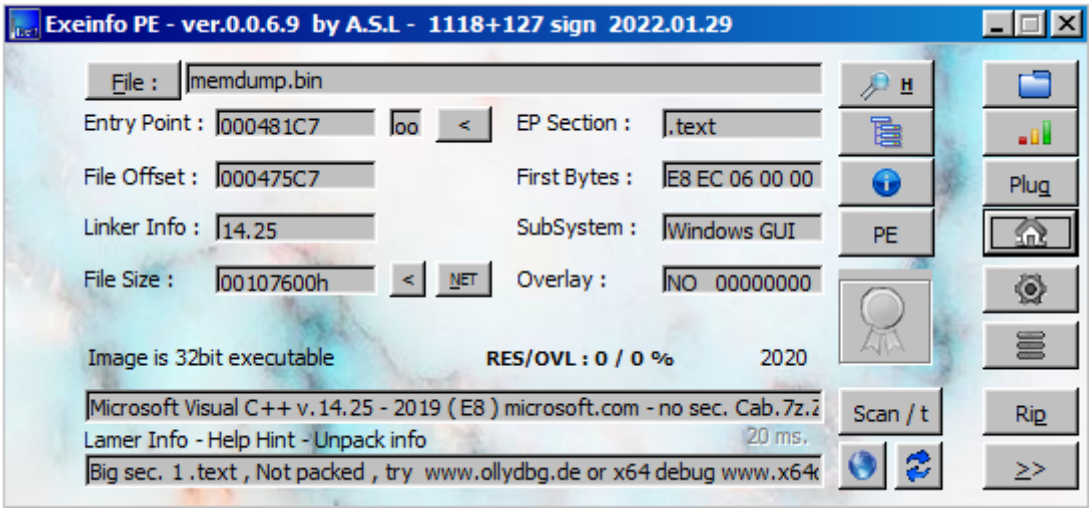
```
================================================
Filename           : memdump.bin
MD5                : 1d71701e9824c730dffbcaef428a2f64
SHA1               : cfae85cd6b410c2605fc5b0149ed1a07ff3dc9e3
CRC32              : 9b47abde
SHA-256            : 4f198228806c897797647eecce0f92d4082476b82781183062a55c417c0bb197
SHA-512            : 511d4c8f44a9467f901cbda085bcc0bfc9d96ed2a0ad7e924ab955b56b0d3c1df5fb5eb3341dbe8856c04cbcd99fa98c6bc32156765d922ef84e5215d8769d91
SHA-384            : 1ef2366edd23e07a6a2bcb27004507df6aac59fd3ac0f49d00a00eb91ce148eb6fa029d12f9e9b5d1e5a24d11d61a1af
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
================================================
```




PEview - C:\Users\IEUser\Downloads\Avaddon\Avaddon7\memdump.bin\memdump.bin
File View Go Help
memdump.bin
IMAGE_DOS_HEADER
IMAGE_DEBUG_TYPE_
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 .reloc
SECTION .text
SECTION .rdata
SECTION .data
SECTION .reloc
pFile Data Description Value
0000010C 014C Machine IMAGE_FILE_MACHINE_I386
0000010E 0004 Number of Sections
00000110 5ED771AA Time Date Stamp 2020/06/03 Wed 09:47:22 UTC
00000114 00000000 Pointer to Symbol Table
00000118 00000000 Number of Symbols
0000011C 00E0 Size of Optional Header
0000011E 0102 Characteristics
0002 IMAGE_FILE_EXECUTABLE_IMAGE
0100 IMAGE_FILE_32BIT_MACHINE



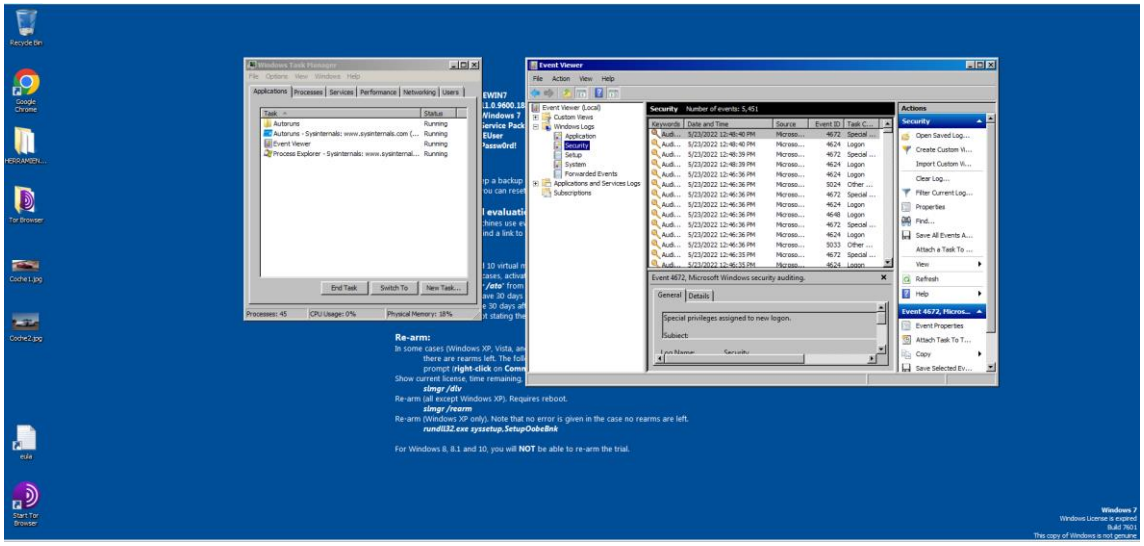


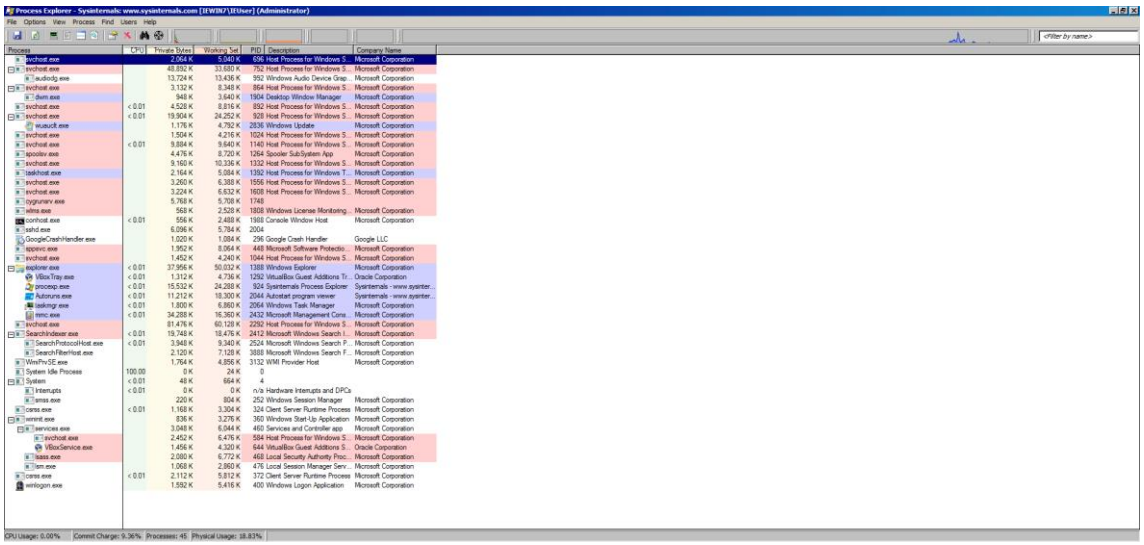


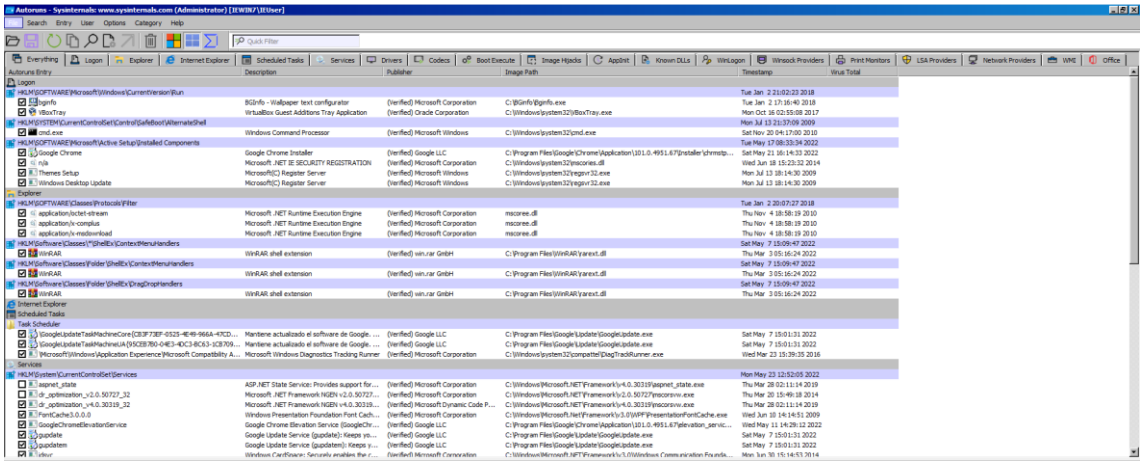
ANALISIS DINAMICO:

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.

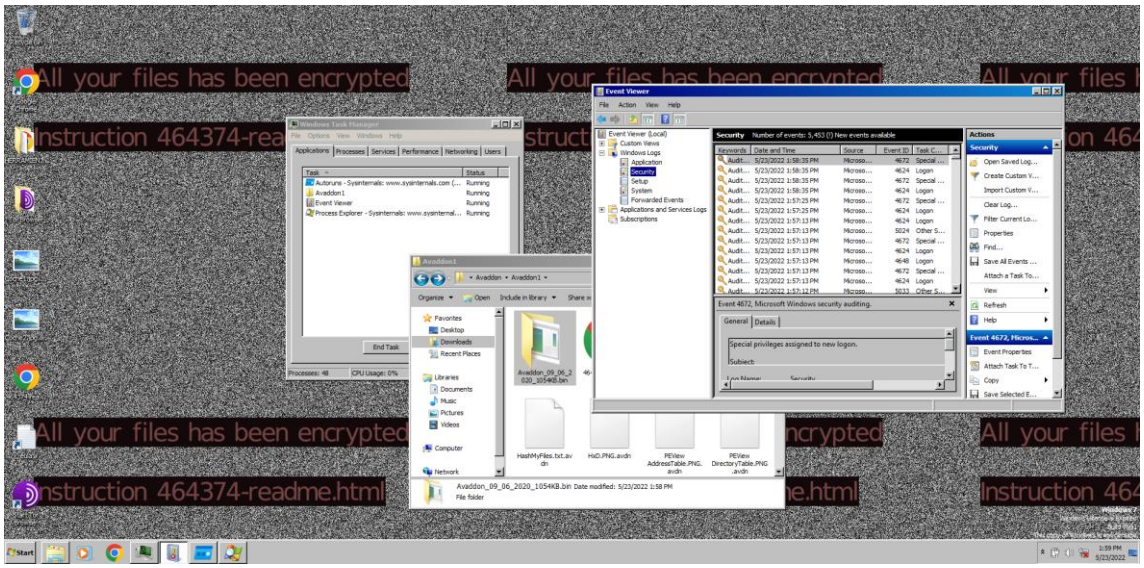
Al iniciar una “snapshot” de la máquina virtual, siempre serán los mismos procesos y servicios los que se iniciaran, por lo que solamente lo comprobaremos una vez.

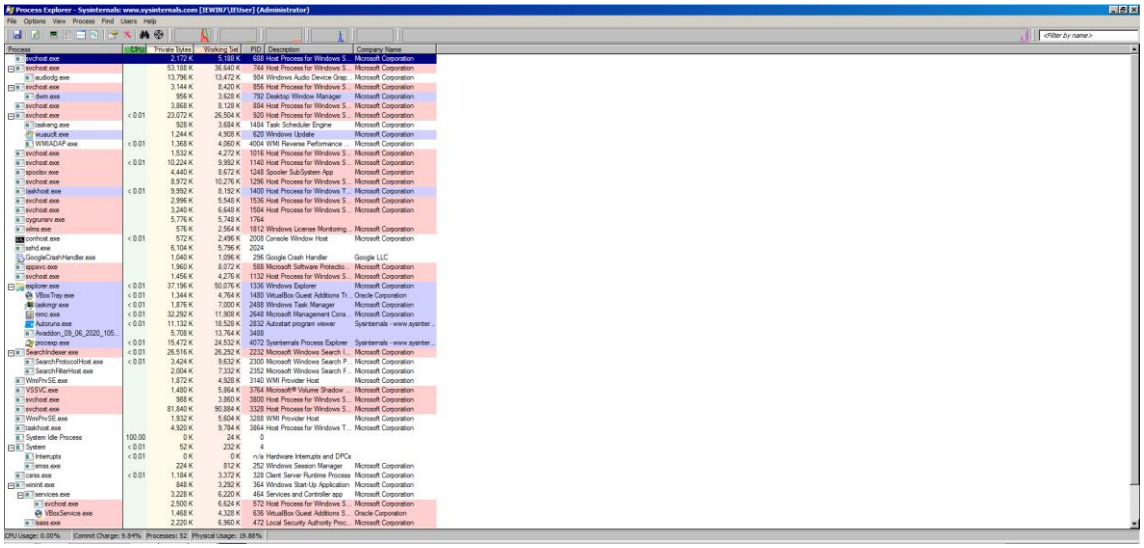


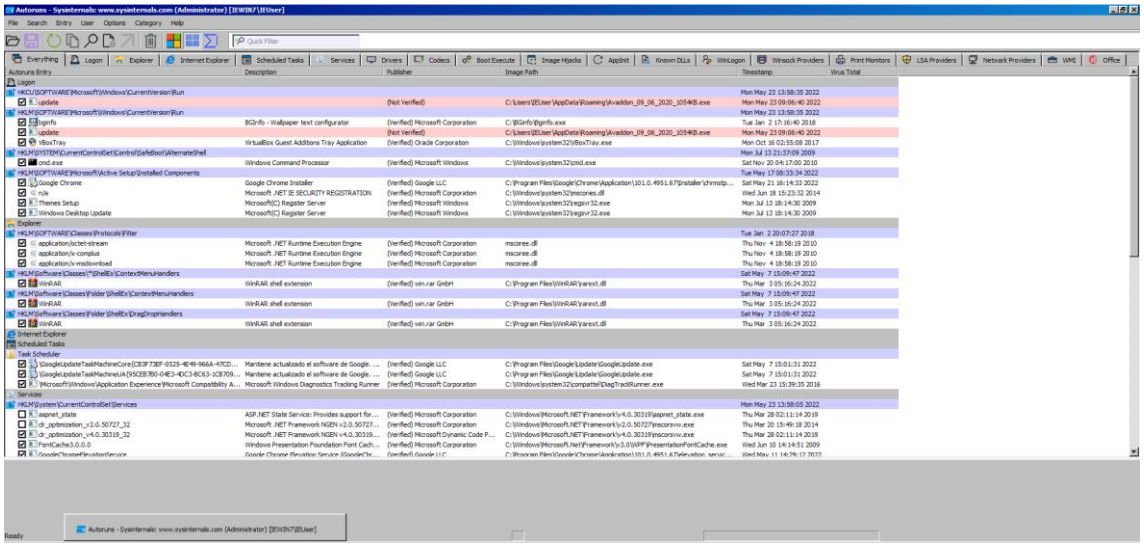




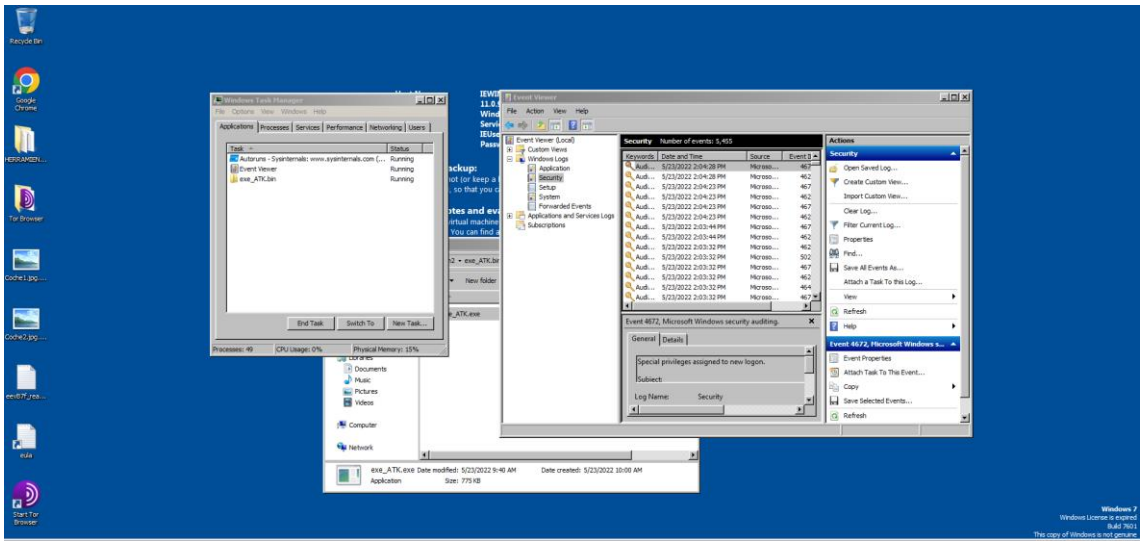
MUESTRA 1:

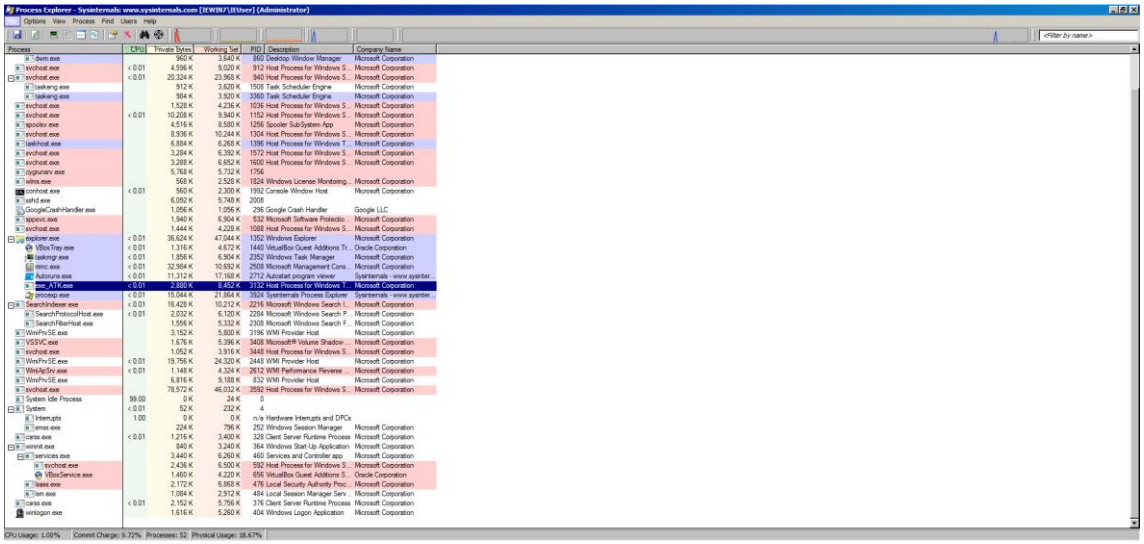

All your files has been encrypted
Instruction 464374-readme.html
Event Viewer
Windows Task Manager
Process Explorer - Sysinternals: www.sysinternals.com [IEWIN7\IEUser] (Administrator)

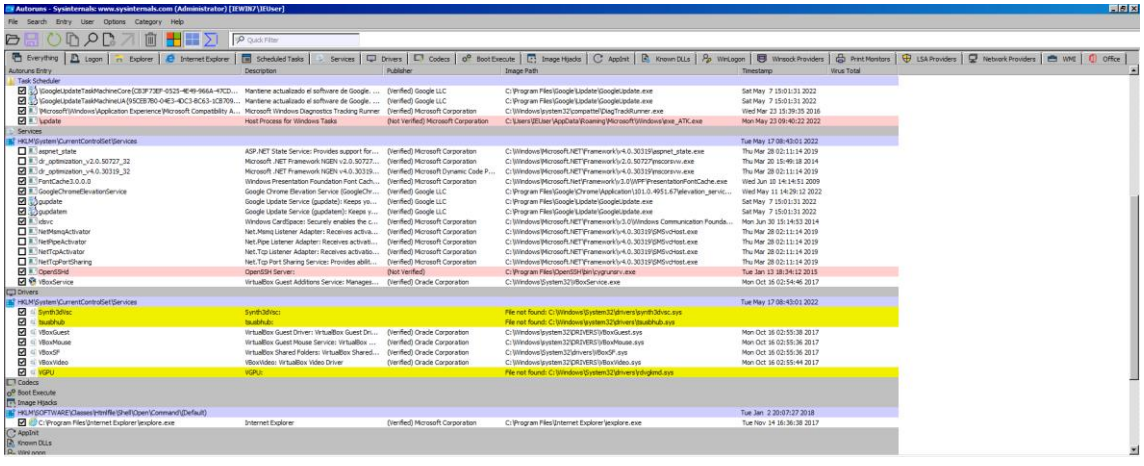


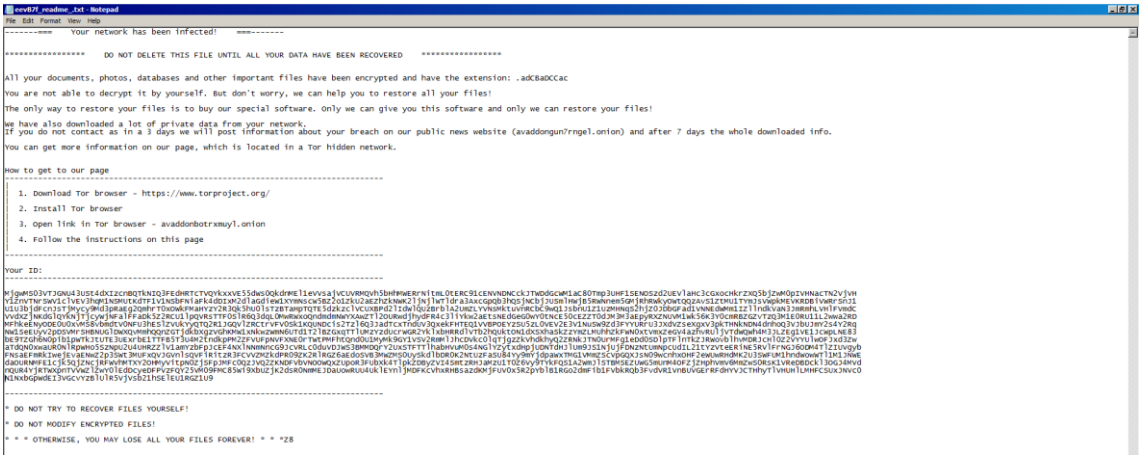

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [IEWIN7\IEUser]

MUESTRA 2:

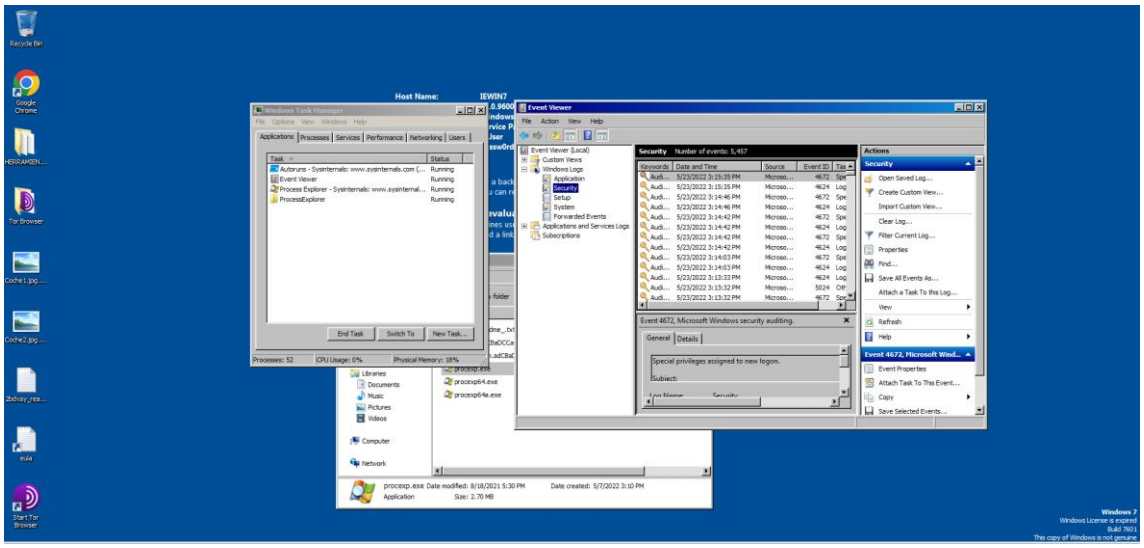

Windows Task Manager
Event Viewer
Windows 7
Windows License is expired
Build 7601
This copy of Windows is not genuine

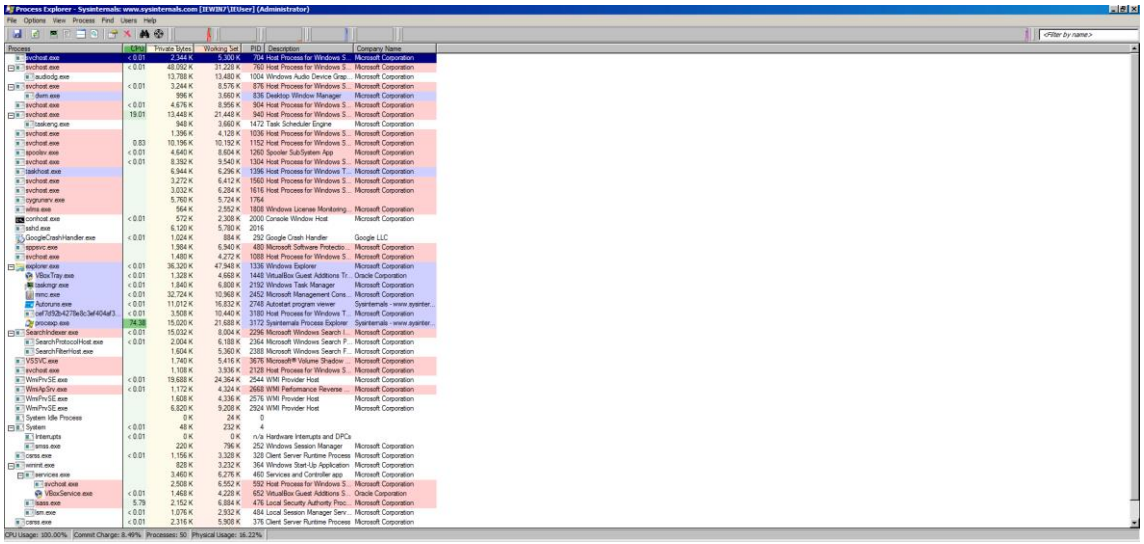

Process Explorer - Sysinternals: www.sysinternals.com [IEWIN7\IEUser] (Administrator)

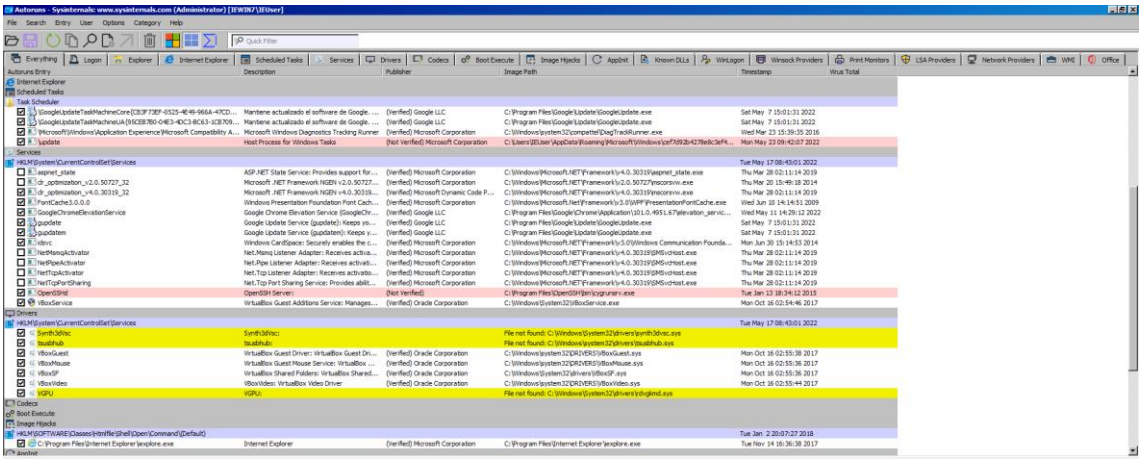

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [IEWIN7\IEUser]

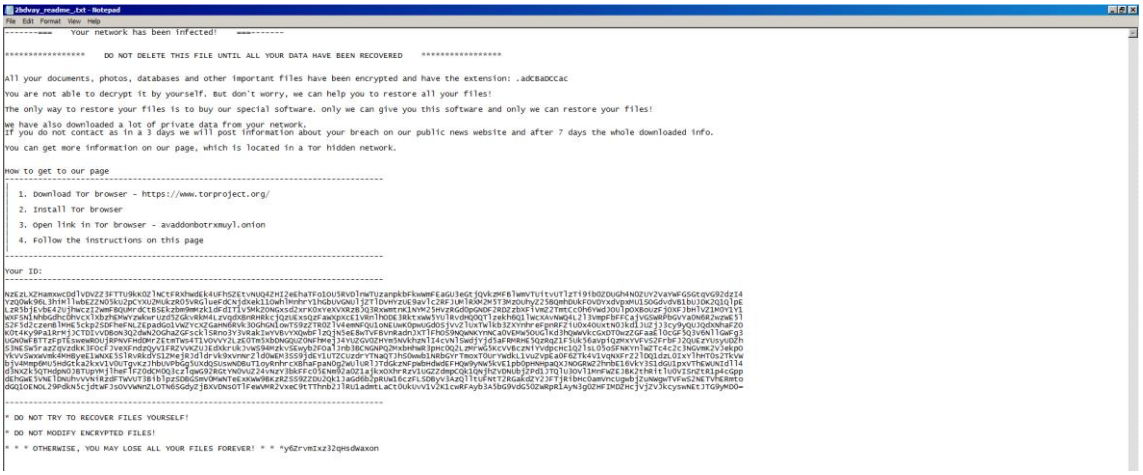

eevBJT_readme_.txt - Notepad
File Edit Format View Help
Your network has been infected!
DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED
All your documents, photos, databases and other important files have been encrypted and have the extension: .adCBaDCCac
You are not able to decrypt it 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 as in a 3 days we will post information about your breach on our public news website (avaddongun7rnge1.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 link in Tor browser - avaddonbotrxmuyl.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! * * *Z8

MUESTRA 3:

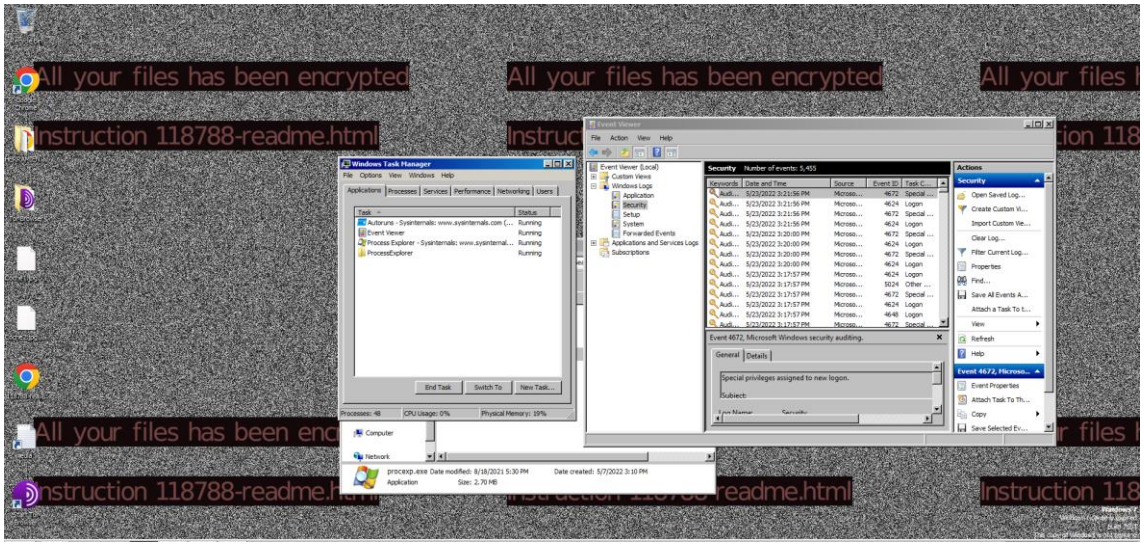

Host Name: IEWIN7
Windows Task Manager
Event Viewer
Process Explorer - Sysinternals: www.sysinternal...
ProcessExplorer
Security Number of events: 5,457
Event 4672, Microsoft Windows security auditing.
Special privileges assigned to new logon.
Windows 7

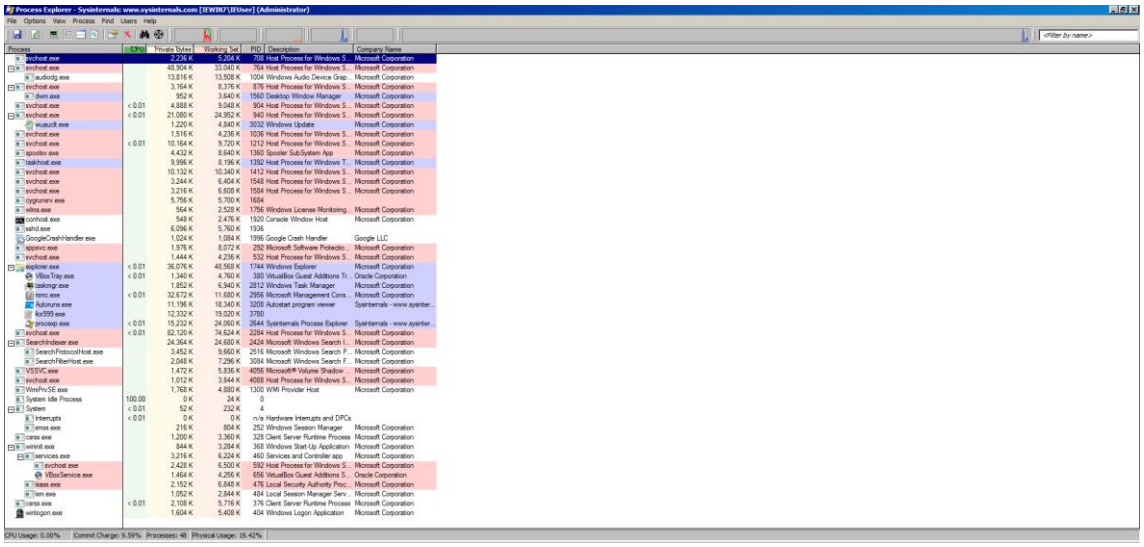

Process Explorer - Sysinternals: www.sysinternals.com [IEWIN7\IEUser] (Administrator)

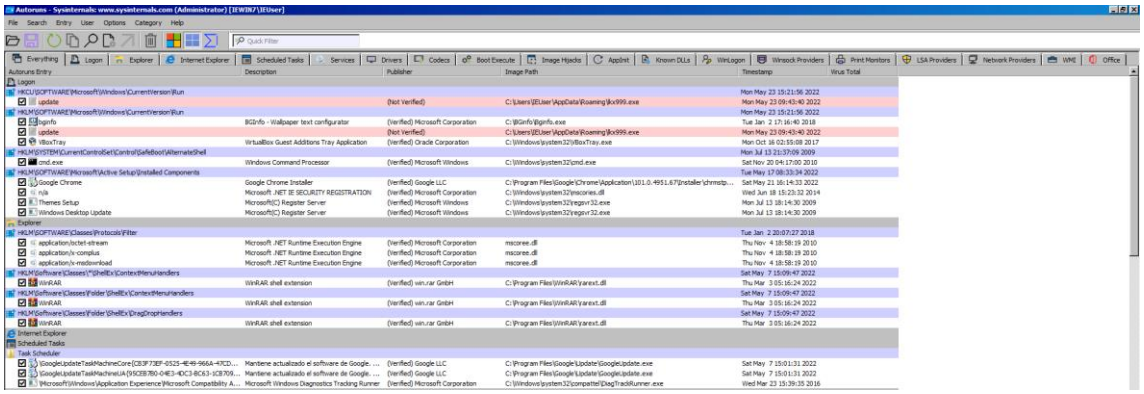



2bdvay_readme_.txt - Notepad
File Edit Format View Help
---------- Your network has been infected! ----------
********** DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED **********
All your documents, photos, databases and other important files have been encrypted and have the extension: .adCBaDCCac
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 as in a 3 days we will post information about your breach on our public news website 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 link in Tor browser - avaddonbotrxmuyl.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! * * *

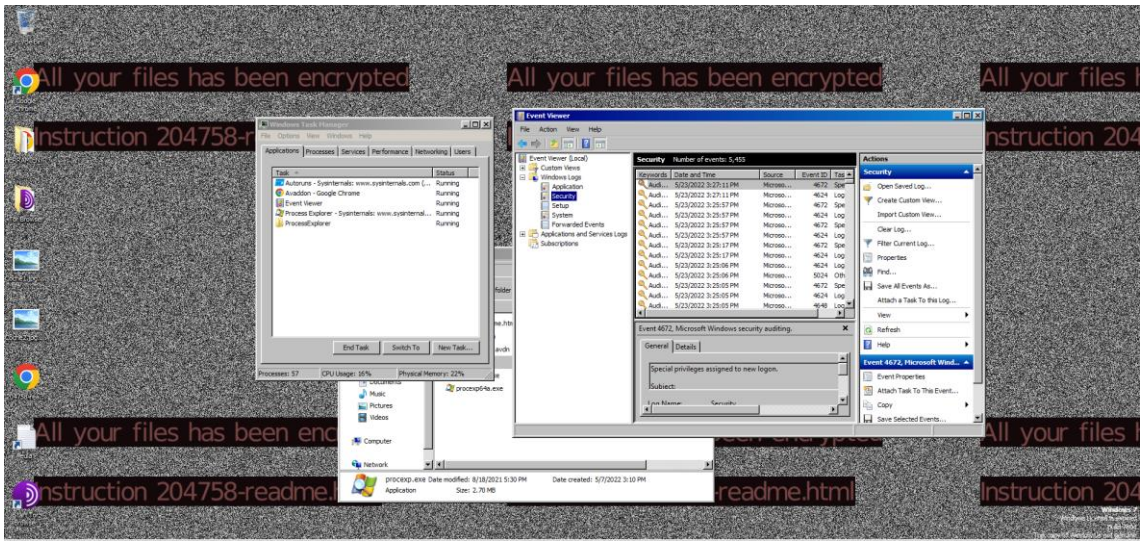
MUESTRA 4:

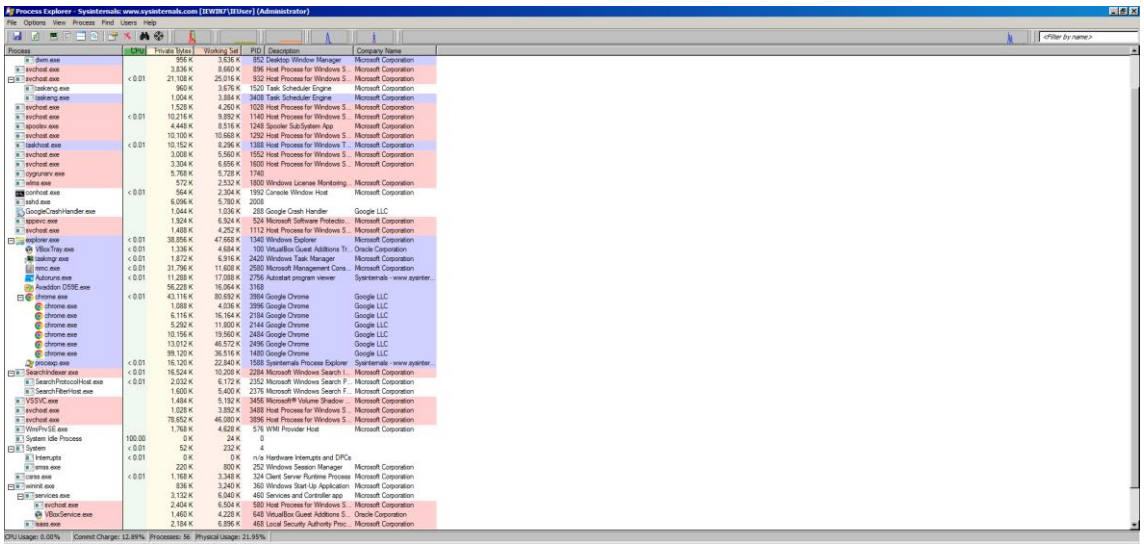

All your files has been encrypted
Instruction 118788-readme.html
Windows Task Manager
Event Viewer

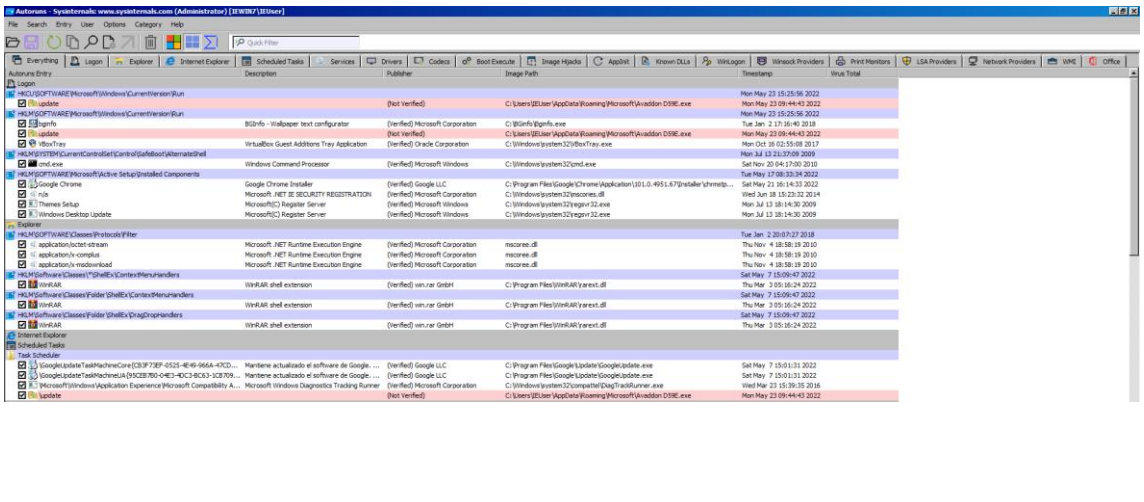


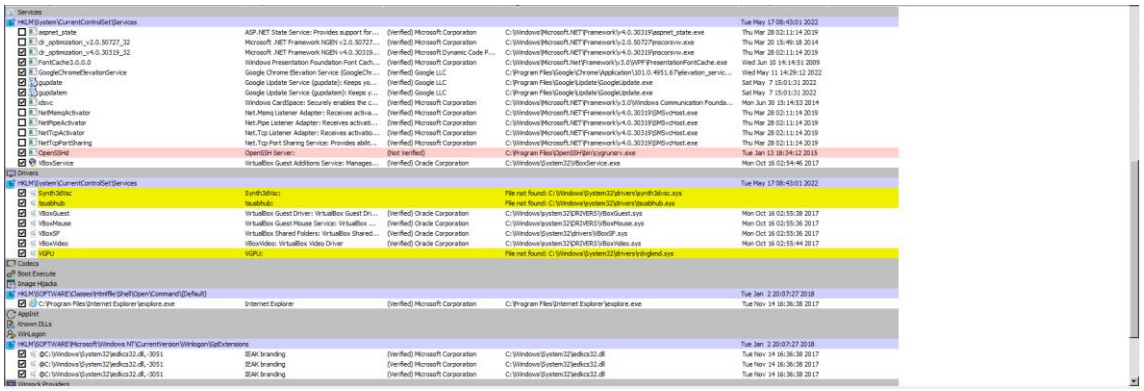


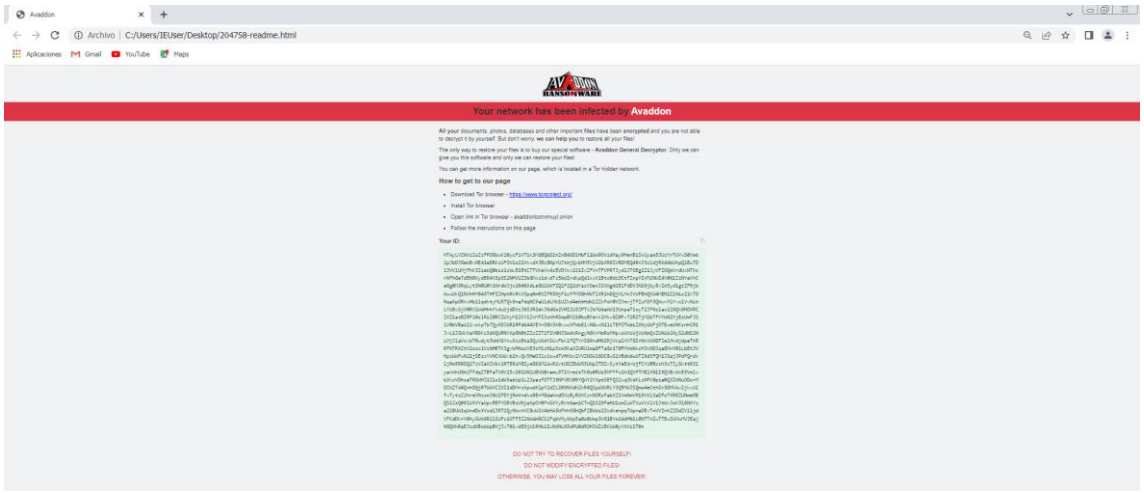
MUESTRA 5:


All your files has been encrypted
Instruction 204758-readme.html
Windows Task Manager
Event Viewer
Security
Actions

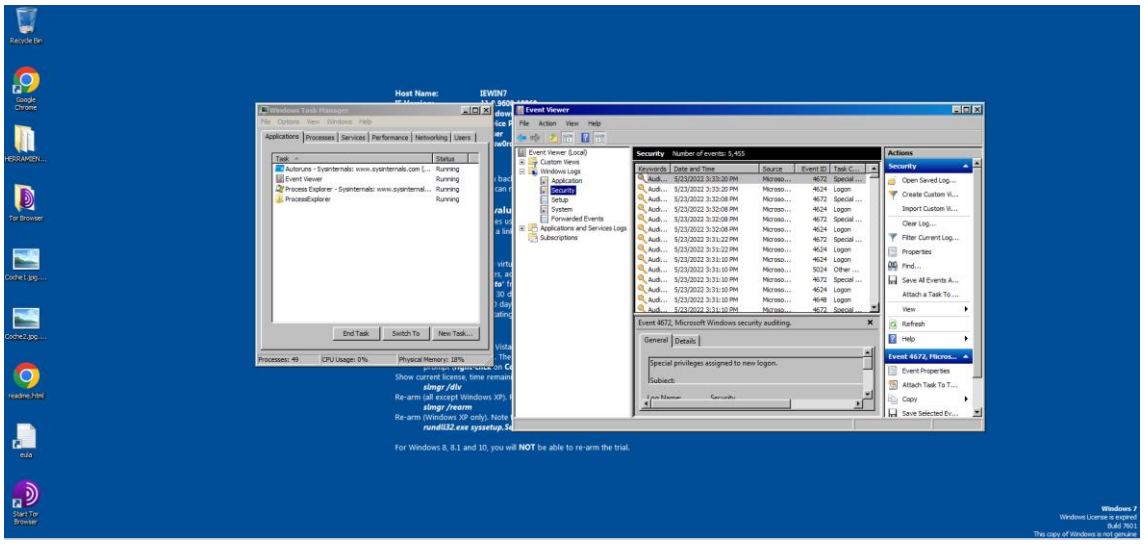

Process Explorer - Sysinternals: www.sysinternals.com [IEWIN7\IEUser] (Administrator)

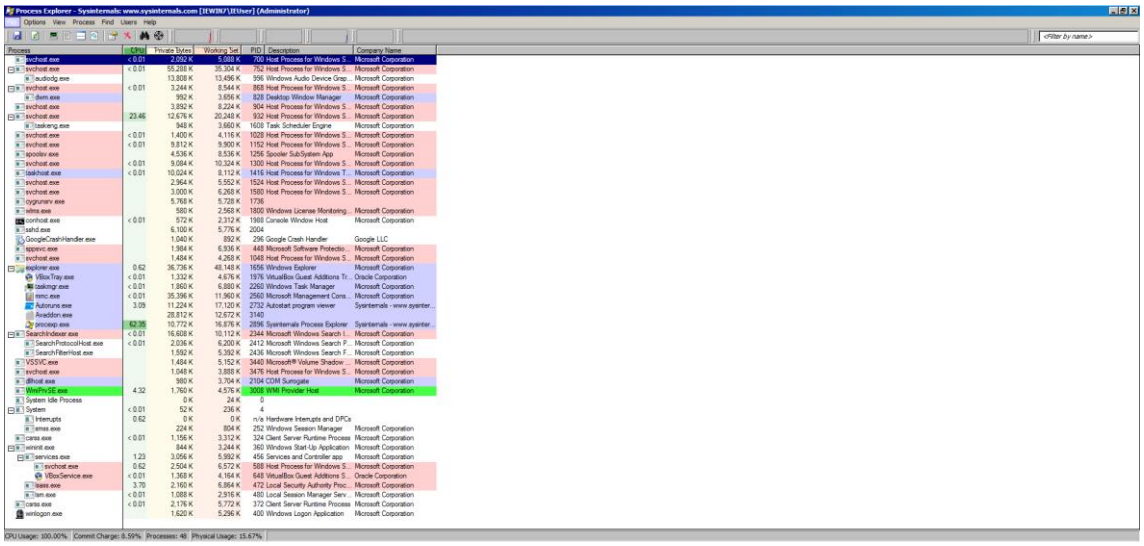

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [IEWIN7\IEUser]

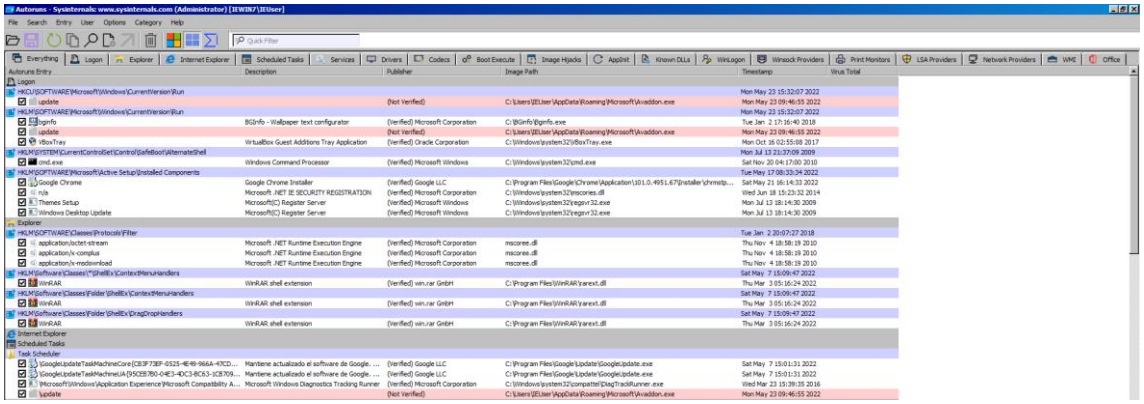


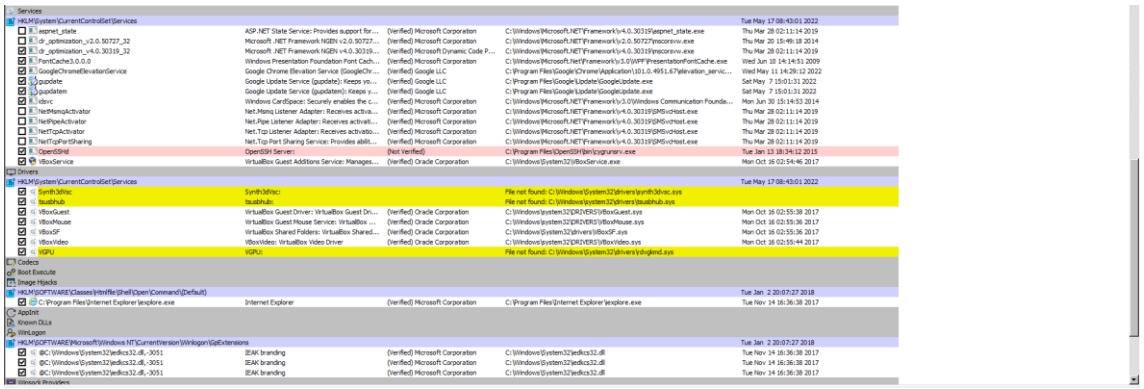

Avaddon
Archivo | C:/Users/IEUser/Desktop/204758-readme.html
Aplicaciones
Gmail
YouTube
Maps
Your network has been infected by Avaddon
How to get to our page
DO NOT TRY TO RECOVER FILES YOURSELF!
DO NOT MODIFY ENCRYPTED FILES!
OTHERWISE, YOU MAY LOSE ALL YOUR FILES FOREVER!

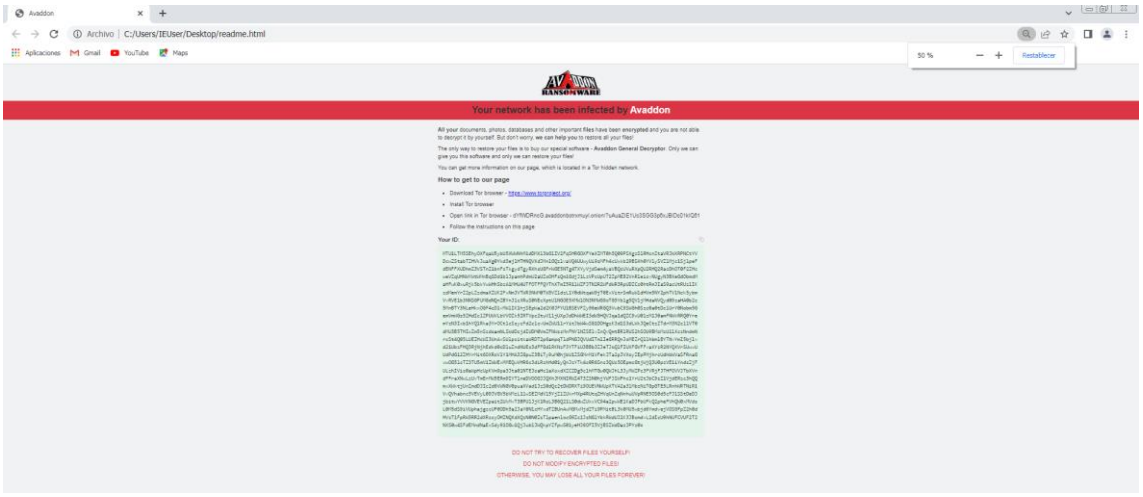
MUESTRA 6:


Host Name:
IEWIN7
Windows Task Manager
Event Viewer
Security
Number of events: 5,453
Event 4672, Microsoft Windows security auditing.
Special privileges assigned to new logon.
Subject:
Show current license, time remaining
slmgr /dlv
Re-arm (all except Windows XP).
slmgr /rearm
Re-arm (Windows XP only). Note
rundll32.exe syssetup.S
For Windows 8, 8.1 and 10, you will NOT be able to re-arm the trial.
Windows 7
Windows License is expired
Build 7601
This copy of Windows is not genuine

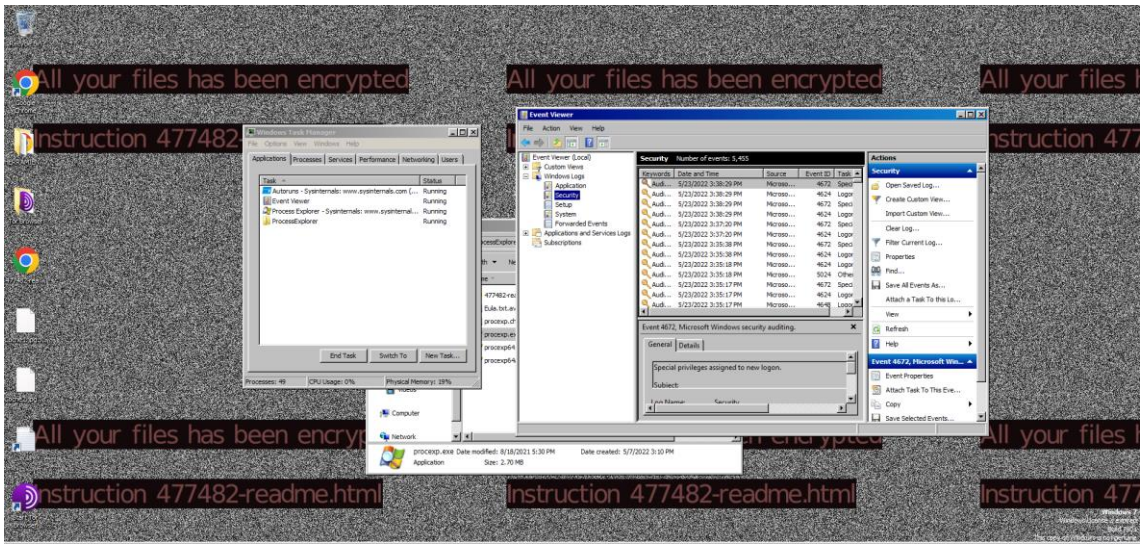

Process Explorer - Sysinternals: www.sysinternals.com [IEWIN7\IEUser] (Administrator)
Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name
svchost.exe < 0.01 2,092 K 5,088 K 700 Host Process for Windows S... Microsoft Corporation
svchost.exe < 0.01 55,208 K 35,304 K 752 Host Process for Windows S... Microsoft Corporation
audiodg.exe 13,808 K 13,496 K 996 Windows Audio Device Grap... Microsoft Corporation
svchost.exe < 0.01 3,244 K 8,544 K 868 Host Process for Windows S... Microsoft Corporation
dwm.exe 992 K 3,656 K 828 Desktop Window Manager Microsoft Corporation
svchost.exe 3,892 K 8,224 K 904 Host Process for Windows S... Microsoft Corporation
svchost.exe 23.46 12,676 K 20,248 K 932 Host Process for Windows S... Microsoft Corporation
taskeng.exe 948 K 3,660 K 1608 Task Scheduler Engine Microsoft Corporation
svchost.exe < 0.01 1,400 K 4,116 K 1028 Host Process for Windows S... Microsoft Corporation
svchost.exe < 0.01 9,812 K 9,900 K 1152 Host Process for Windows S... Microsoft Corporation
spoolsv.exe 4,536 K 8,536 K 1256 Spooler SubSystem App Microsoft Corporation
svchost.exe < 0.01 9,084 K 10,324 K 1300 Host Process for Windows S... Microsoft Corporation
taskhost.exe < 0.01 10,024 K 8,112 K 1416 Host Process for Windows T... Microsoft Corporation
svchost.exe 2,964 K 5,552 K 1524 Host Process for Windows S... Microsoft Corporation
svchost.exe 3,000 K 6,268 K 1580 Host Process for Windows S... Microsoft Corporation
cygrunsrv.exe 5,768 K 5,728 K 1736
wlms.exe 580 K 2,568 K 1800 Windows License Monitoring... Microsoft Corporation
conhost.exe < 0.01 572 K 2,312 K 1968 Console Window Host Microsoft Corporation
sshd.exe 6,100 K 5,776 K 2004
GoogleCrashHandler.exe 1,040 K 892 K 296 Google Crash Handler Google LLC
tpprovi.exe 1,964 K 6,936 K 448 Microsoft Software Protectio... Microsoft Corporation
svchost.exe 1,484 K 4,268 K 1048 Host Process for Windows S... Microsoft Corporation
explorer.exe 0.62 36,736 K 48,148 K 1656 Windows Explorer Microsoft Corporation
VBoxTray.exe < 0.01 1,332 K 4,676 K 1976 VirtualBox Guest Additions Tr... Oracle Corporation
taskmgr.exe < 0.01 1,860 K 6,880 K 2260 Windows Task Manager Microsoft Corporation
mmc.exe < 0.01 35,396 K 11,960 K 2560 Microsoft Management Cons... Microsoft Corporation
Autoruns.exe 3.09 11,224 K 17,120 K 2732 Autostart program viewer Sysinternals - www.sysinter...
Avaddon.exe 28,812 K 12,672 K 3140
procexp.exe 62.35 10,772 K 16,876 K 2896 Sysinternals Process Explorer Sysinternals - www.sysinter...
SearchIndexer.exe < 0.01 16,608 K 10,112 K 2344 Microsoft Windows Search I... Microsoft Corporation
SearchProtocolHost.exe < 0.01 2,036 K 6,200 K 2412 Microsoft Windows Search P... Microsoft Corporation
SearchFilterHost.exe 1,592 K 5,392 K 2436 Microsoft Windows Search F... Microsoft Corporation
VSSVC.exe 1,484 K 5,152 K 3440 Microsoft® Volume Shadow ... Microsoft Corporation
svchost.exe 1,048 K 3,888 K 3476 Host Process for Windows S... Microsoft Corporation
dllhost.exe 980 K 3,704 K 2104 COM Surrogate Microsoft Corporation
WmiPrvSE.exe 4.32 1,760 K 4,576 K 3008 WMI Provider Host Microsoft Corporation
System Idle Process 0 K 24 K 0
System < 0.01 52 K 236 K 4
Interrupts 0.62 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 224 K 804 K 252 Windows Session Manager Microsoft Corporation
csrss.exe < 0.01 1,156 K 3,312 K 324 Client Server Runtime Process Microsoft Corporation
wininit.exe 844 K 3,244 K 360 Windows Start-Up Application Microsoft Corporation
services.exe 1.23 3,056 K 5,992 K 456 Services and Controller app Microsoft Corporation
svchost.exe 0.62 2,504 K 6,572 K 588 Host Process for Windows S... Microsoft Corporation
VBoxService.exe < 0.01 1,368 K 4,164 K 648 VirtualBox Guest Additions S... Oracle Corporation
lsass.exe 3.70 2,160 K 6,864 K 472 Local Security Authority Proc... Microsoft Corporation
lsm.exe < 0.01 1,088 K 2,916 K 480 Local Session Manager Serv... Microsoft Corporation
csrss.exe < 0.01 2,176 K 5,772 K 372 Client Server Runtime Process Microsoft Corporation
winlogon.exe 1,620 K 5,296 K 400 Windows Logon Application Microsoft Corporation
CPU Usage: 100.00% Commit Charge: 8.59% Processes: 48 Physical Usage: 15.67%

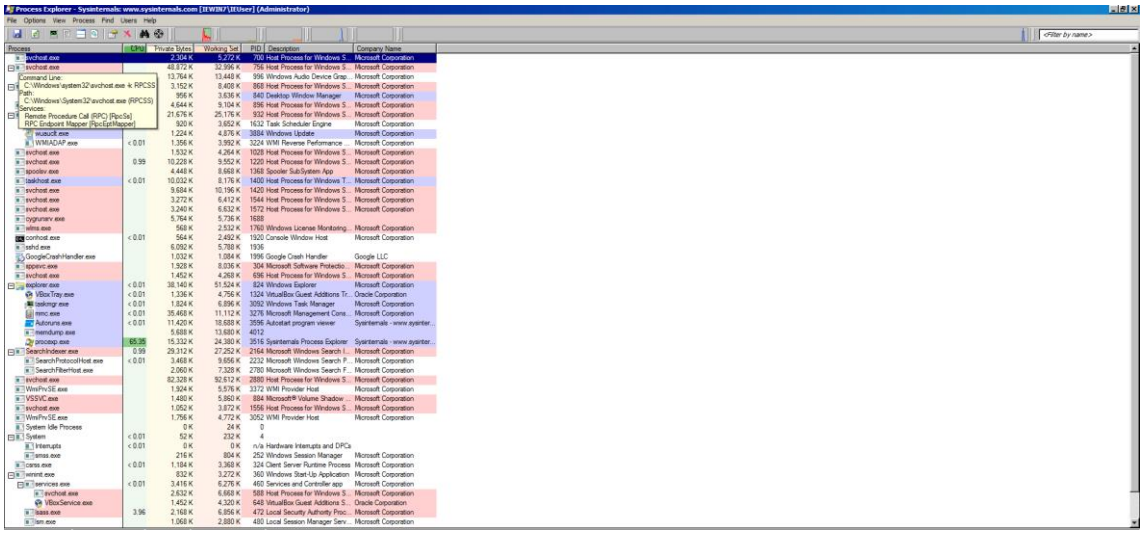

Autoruns - Sysinternals: www.sysinternals.com (Administrator) [IEWIN7\IEUser]
File Search Entry User Options Category Help
Quick Filter
Everything Logon Explorer Internet Explorer Scheduled Tasks Services Drivers Codecs Boot Execute Image Hijacks AppInit Known DLLs WinLogon Winsock Providers Print Monitors LSA Providers Network Providers WMI Office
Autoruns Entry Description Publisher Image Path Timestamp Virus Total
Logon
HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
update (Not Verified) C:\Users\IEUser\AppData\Roaming\Microsoft\Avaddon.exe Mon May 23 09:46:55 2022
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
bginfo BGInfo - Wallpaper text configurator (Verified) Microsoft Corporation C:\BGInfo\bginfo.exe Tue Jan 2 17:16:40 2018
update (Not Verified) C:\Users\IEUser\AppData\Roaming\Microsoft\Avaddon.exe Mon May 23 09:46:55 2022
VBoxTray VirtualBox Guest Additions Tray Application (Verified) Oracle Corporation C:\Windows\system32\VBoxTray.exe Mon Oct 16 02:55:08 2017
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
cmd.exe Windows Command Processor (Verified) Microsoft Windows C:\Windows\system32\cmd.exe Sat Nov 20 04:17:00 2010
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components
Google Chrome Google Chrome Installer (Verified) Google LLC C:\Program Files\Google\Chrome\Application\101.0.4951.67\Installer\chrmstp... Sat May 21 16:14:33 2022
n/a Microsoft .NET IE SECURITY REGISTRATION (Verified) Microsoft Corporation C:\Windows\system32\mscories.dll Wed Jun 18 15:23:32 2014
Themes Setup Microsoft(C) Register Server (Verified) Microsoft Windows C:\Windows\system32\regsvr32.exe Mon Jul 13 18:14:30 2009
Windows Desktop Update Microsoft(C) Register Server (Verified) Microsoft Windows C:\Windows\system32\regsvr32.exe Mon Jul 13 18:14:30 2009
Explorer
HKLM\SOFTWARE\Classes\Protocols\Filter
application/octet-stream Microsoft .NET Runtime Execution Engine (Verified) Microsoft Corporation mscoree.dll Thu Nov 4 18:58:19 2010
application/x-complus Microsoft .NET Runtime Execution Engine (Verified) Microsoft Corporation mscoree.dll Thu Nov 4 18:58:19 2010
application/x-msdownload Microsoft .NET Runtime Execution Engine (Verified) Microsoft Corporation mscoree.dll Thu Nov 4 18:58:19 2010
HKLM\Software\Classes*\shellex\ContextMenuHandlers
WinRAR WinRAR shell extension (Verified) win.rar GmbH C:\Program Files\WinRAR\rarext.dll Thu Mar 3 05:16:24 2022
HKLM\Software\Classes\Folder\shellex\ContextMenuHandlers
WinRAR WinRAR shell extension (Verified) win.rar GmbH C:\Program Files\WinRAR\rarext.dll Thu Mar 3 05:16:24 2022
HKLM\Software\Classes\Folder\shellex\DragDropHandlers
WinRAR WinRAR shell extension (Verified) win.rar GmbH C:\Program Files\WinRAR\rarext.dll Thu Mar 3 05:16:24 2022
Internet Explorer
Scheduled Tasks
Task Scheduler
\GoogleUpdateTaskMachineCore{C83F73EF-0525-4E49-966A-47CD... Mantiene actualizado el software de Google. ... (Verified) Google LLC C:\Program Files\Google\Update\GoogleUpdate.exe Sat May 7 15:01:31 2022
\GoogleUpdateTaskMachineUA{5ACEB780-04E3-4CC3-8C63-2CB709... Mantiene actualizado el software de Google. ... (Verified) Google LLC C:\Program Files\Google\Update\GoogleUpdate.exe Sat May 7 15:01:31 2022
\Microsoft\Windows\Application Experience\Microsoft Compatibility A... Microsoft® Windows Diagnostics Tracking Runner (Verified) Microsoft Corporation C:\Windows\system32\compattelrunner.exe Wed Mar 23 15:39:35 2016
update (Not Verified) C:\Users\IEUser\AppData\Roaming\Microsoft\Avaddon.exe Mon May 23 09:46:55 2022

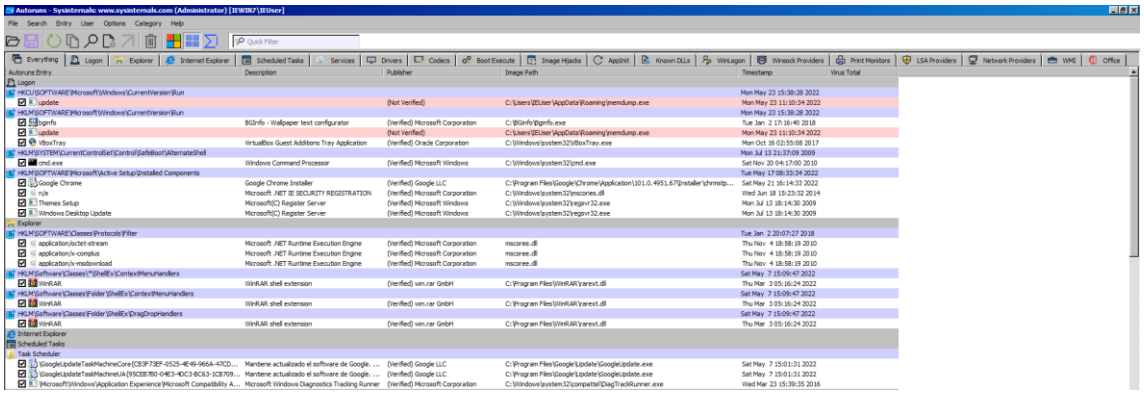

Services
HKLM\System\CurrentControlSet\Services
Tue May 17 08:43:01 2022
aspnet_state ASP.NET State Service: Provides support for... (Verified) Microsoft Corporation C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_state.exe Thu Mar 28 02:11:14 2019
clr_optimization_v2.0.50727_32 Microsoft .NET Framework NGEN v2.0.50727... (Verified) Microsoft Corporation C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe Thu Mar 20 15:49:18 2014
clr_optimization_v4.0.30319_32 Microsoft .NET Framework NGEN v4.0.3019... (Verified) Microsoft Corporation C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe Thu Mar 28 02:11:14 2019
FontCache3.0.0.0 Windows Presentation Foundation Font Cach... (Verified) Microsoft Corporation C:\Windows\Microsoft.Net\Framework\v3.0\WPF\PresentationFontCache.exe Wed Jun 10 14:14:51 2009
GoogleChromeElevationService Google Chrome Elevation Service (GoogleChr... (Verified) Google LLC C:\Program Files\Google\Chrome\Application\101.0.4951.67\elevation_servic... Wed May 11 14:29:12 2022
gupdate Google Update Service (gupdate): Keeps yo... (Verified) Google LLC C:\Program Files\Google\Update\GoogleUpdate.exe Sat May 7 15:01:31 2022
gupdatem Google Update Service (gupdatem): Keeps y... (Verified) Google LLC C:\Program Files\Google\Update\GoogleUpdate.exe Sat May 7 15:01:31 2022
idsvc Windows CardSpace: Securely enables the c... (Verified) Microsoft Corporation C:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication Founda... Mon Jun 30 15:14:53 2014
NetMsmqActivator Net.Msmq Listener Adapter: Receives activa... (Verified) Microsoft Corporation C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe Thu Mar 28 02:11:14 2019
NetPipeActivator Net.Pipe Listener Adapter: Receives activati... (Verified) Microsoft Corporation C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe Thu Mar 28 02:11:14 2019
NetTcpActivator Net.Tcp Listener Adapter: Receives activatio... (Verified) Microsoft Corporation C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe Thu Mar 28 02:11:14 2019
NetTcpPortSharing Net.Tcp Port Sharing Service: Provides abilit... (Verified) Microsoft Corporation C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe Thu Mar 28 02:11:14 2019
OpenSSHd OpenSSH Server: (Not Verified) C:\Program Files\OpenSSH\bin\cygrunsrv.exe Tue Jan 13 18:34:12 2015
VBoxService VirtualBox Guest Additions Service: Manages... (Verified) Oracle Corporation C:\Windows\System32\VBoxService.exe Mon Oct 16 02:54:46 2017
Drivers
HKLM\System\CurrentControlSet\Services
Tue May 17 08:43:01 2022
Synth3dVsc Synth3dVsc File not found: C:\Windows\System32\drivers\synth3dvsc.sys
tsusbhub tsusbhub File not found: C:\Windows\system32\drivers\tsusbhub.sys
VBoxGuest VirtualBox Guest Driver: VirtualBox Guest Dri... (Verified) Oracle Corporation C:\Windows\system32\DRIVERS\VBoxGuest.sys Mon Oct 16 02:55:38 2017
VBoxMouse VirtualBox Guest Mouse Service: VirtualBox ... (Verified) Oracle Corporation C:\Windows\system32\DRIVERS\VBoxMouse.sys Mon Oct 16 02:55:36 2017
VBoxSF VirtualBox Shared Folders: VirtualBox Shared... (Verified) Oracle Corporation C:\Windows\System32\drivers\VBoxSF.sys Mon Oct 16 02:55:36 2017
VBoxVideo VBoxVideo: VirtualBox Video Driver (Verified) Oracle Corporation C:\Windows\system32\DRIVERS\VBoxVideo.sys Mon Oct 16 02:55:44 2017
VGPU VGPU: File not found: C:\Windows\System32\drivers\vdvgkmd.sys
Codecs
Boot Execute
Image Hijacks
HKLM\SOFTWARE\Classes\InternetShortcut\Shell\Open\Command\(Default)
Tue Jan 2 20:07:27 2018
C:\Program Files\Internet Explorer\iexplore.exe Internet Explorer (Verified) Microsoft Corporation C:\Program Files\Internet Explorer\iexplore.exe Tue Nov 14 16:36:38 2017
AppInit
Known DLLs
WinLogon
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GpExtensions
Tue Jan 2 20:07:27 2018
@C:\Windows\System32\wdiscs32.dll,-3051 IEAK branding (Verified) Microsoft Corporation C:\Windows\System32\wdiscs32.dll Tue Nov 14 16:36:38 2017
@C:\Windows\System32\wdiscs32.dll,-3051 IEAK branding (Verified) Microsoft Corporation C:\Windows\System32\wdiscs32.dll Tue Nov 14 16:36:38 2017
@C:\Windows\System32\wdiscs32.dll,-3051 IEAK branding (Verified) Microsoft Corporation C:\Windows\System32\wdiscs32.dll Tue Nov 14 16:36:38 2017
Winsock Providers

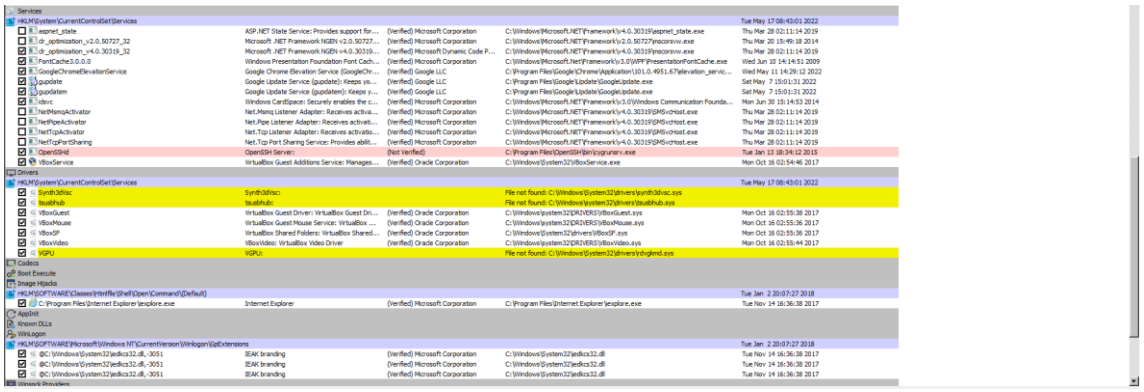

Avaddon
Archivo | C:/Users/IEUser/Desktop/readme.html
Aplicaciones
Gmail
YouTube
Maps
Restablecer
Your network has been infected by Avaddon
How to get to our page
DO NOT TRY TO RECOVER FILES YOURSELF!
DO NOT MODIFY ENCRYPTED FILES!
OTHERWISE, YOU MAY LOSE ALL YOUR FILES FOREVER!

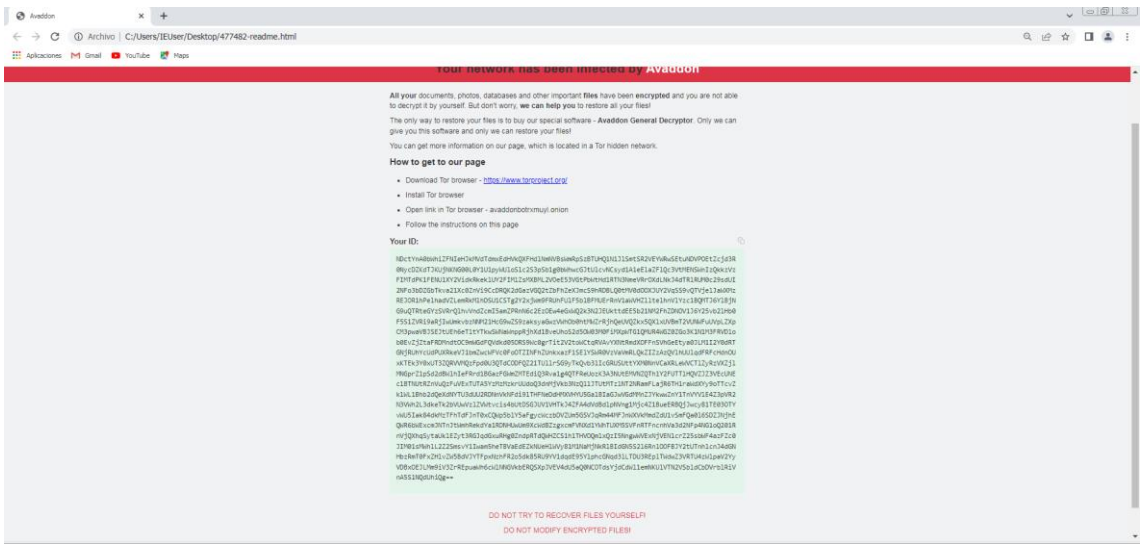
MUESTRA 7:


All your files has been encrypted
Instruction 477482-readme.html
Windows Task Manager
Event Viewer
procexp.exe


Process Explorer - Sysinternals: www.sysinternals.com [IEWIN7\IEUser] (Administrator)







CONCLUSION

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