Oggi andremo ad effettuare un'analisi dinamica basica su un malware presente sulla nostra macchina virtuale.

Come prima cosa, facciamo un analisi basica per inquadrare il malware e capire di cosa stiamo parlando:

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	54	0000446C	00000000	00000000	000046B8	00004000

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00002E96	00001000	00003000	00001000	00000000	00000000	0000	0000	60000020
.rdata	000008F2	00004000	00001000	00004000	00000000	00000000	0000	0000	40000040
.data	000007DC	00005000	00001000	00005000	00000000	00000000	0000	0000	C0000040
.rsrc	00006084	00006000	00007000	00006000	00000000	00000000	0000	0000	40000040

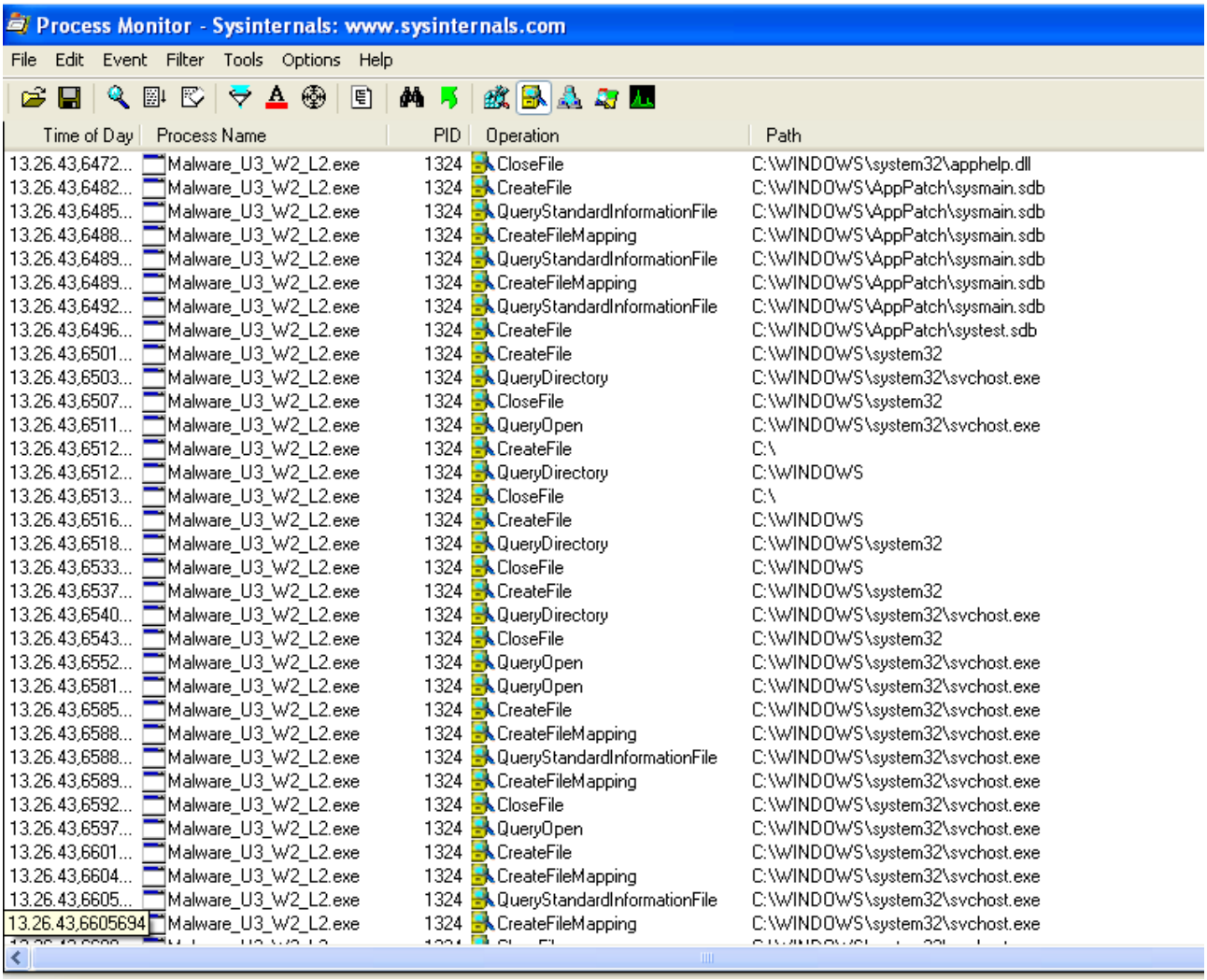
Property	Value
File Name	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W...
File Type	Portable Executable 32
File Info	No match found.
File Size	52.00 KB (53248 bytes)
PE Size	52.00 KB (53248 bytes)
Created	Saturday 20 August 2022, 12.05.40
Modified	Friday 08 April 2011, 12.54.59
Accessed	Tuesday 28 March 2023, 10.27.11
MD5	E2BF42217A67E46433DA8B6F4507219E
SHA-1	DAF263702F11DC0430D30F9BF443E7885CF91FCB

Property	Value
Empty	No additional info available

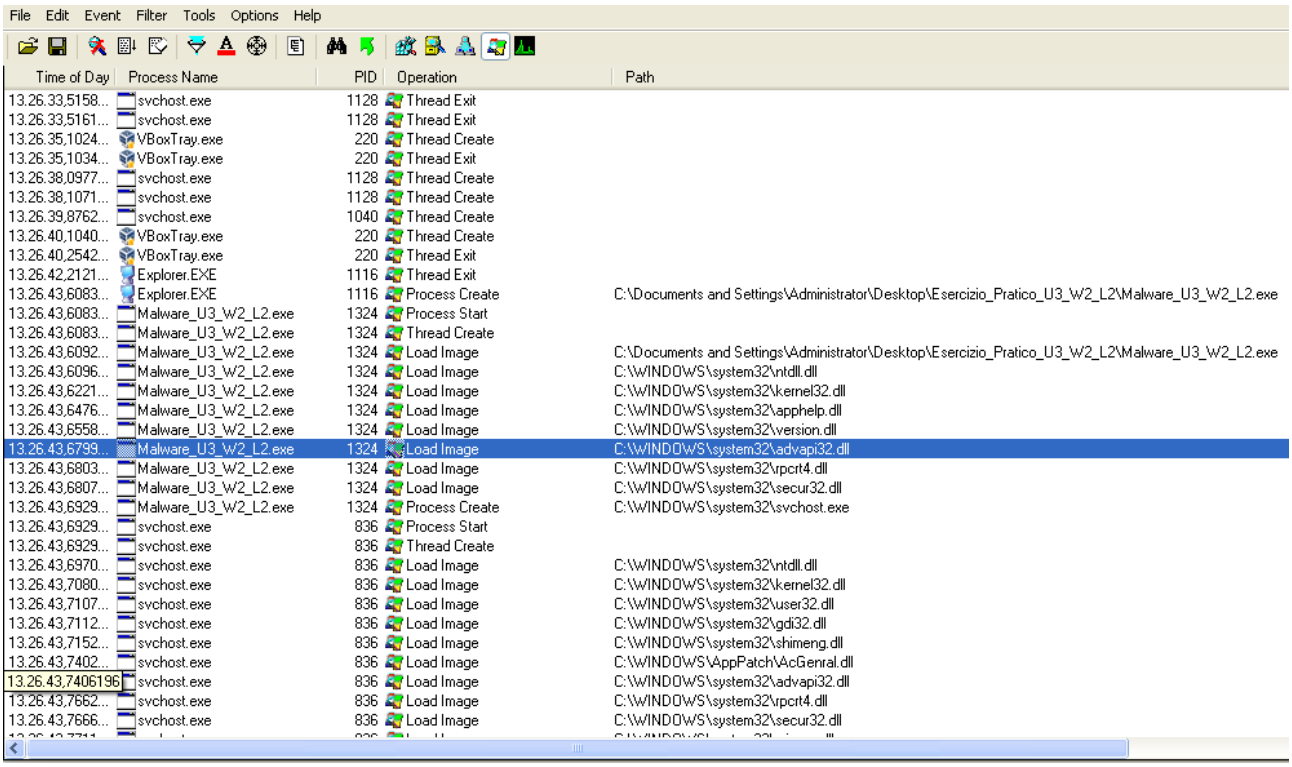
Cyren	W32/Dropper.gen8!Maximus	DrWeb	Trojan.Inject.64211
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Trojan.ExplorerHijack.dqW@aO9ui...
eScan	Gen:Trojan.ExplorerHijack.dqW@aO9ui3p	ESET-NOD32	Win32/Spy.KeyLogger.QRM
Fortinet	W32/Generic.AP.419160	GData	Gen:Trojan.ExplorerHijack.dqW@aO9ui3p
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.oa!s1
Ikarus	Trojan.Injector	Jiangmin	Trojan/Generic.xbgc

Possiamo subito notare che la libreria esportata e la KERNEL32.DDL che, come sappiamo, e una libreria che permette l'interazione con il sistema operativo. Possiamo notare che informazioni importanti, quali .text, .rdata , .data e .rsc non sono compressi (come con UXP) e possiamo notare, tramite virus total, che si tratta di un trojan. Una volta che ci siamo accertati che in effetti è un malware, possiamo procedere con l'analisi dinamica:

una volta fatto partire process monitor, avvio il malware e ne studio i comportamenti. Nello specifico analizzo le azioni che effettua sul fyle system:

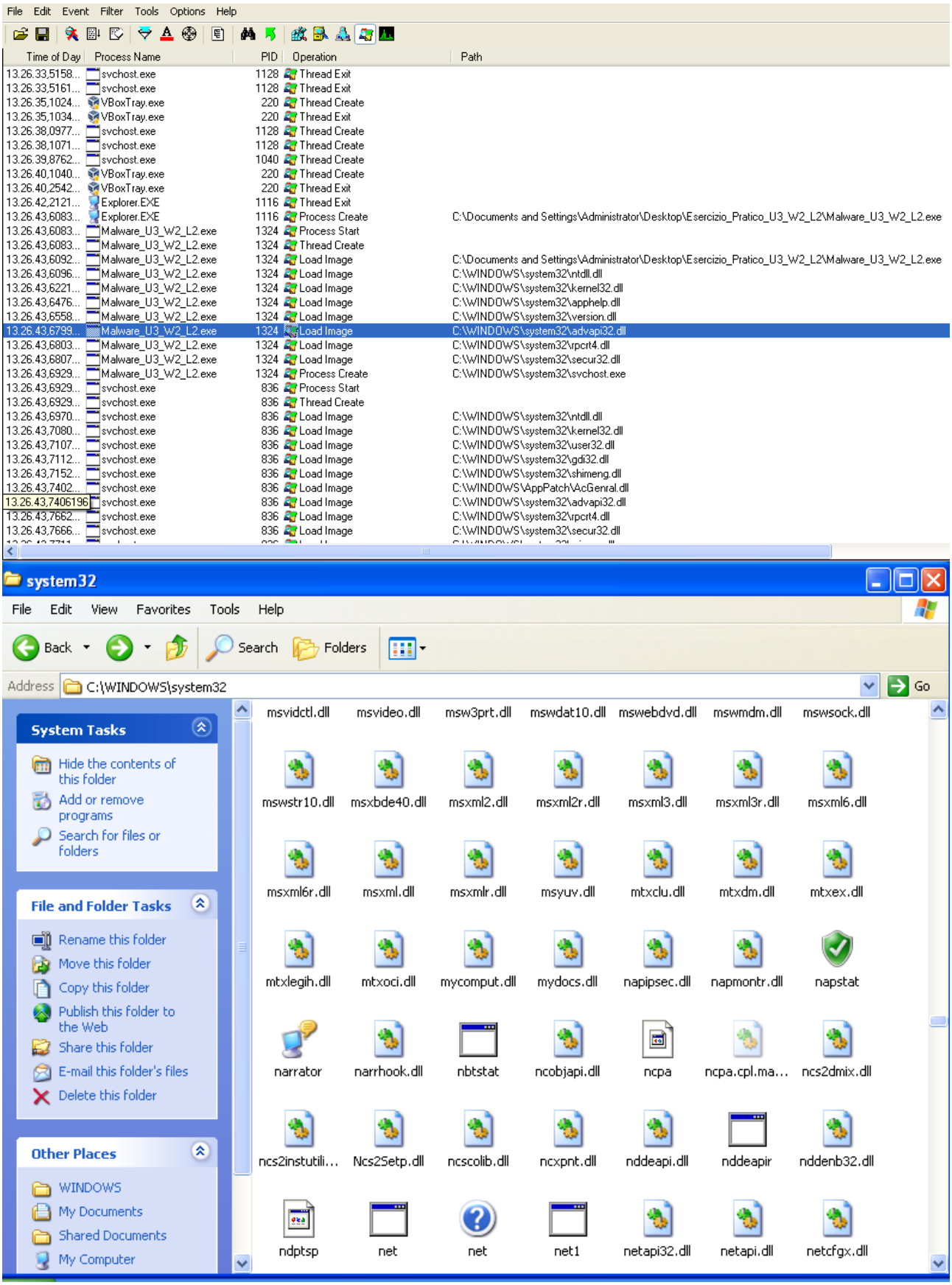


Possiamo subito notare che le azioni sono molte e dopo le analizzeremo nel dettaglio. Prima, analizzo le azioni che il malware fa sui processi ed i thread:



Time of Day	Process Name	PID	Operation	Path
13.26.33,5158...	svchost.exe	1128	Thread Exit	
13.26.33,5161...	svchost.exe	1128	Thread Exit	
13.26.35,1024...	VBoxTray.exe	220	Thread Create	
13.26.35,1034...	VBoxTray.exe	220	Thread Exit	
13.26.38,0977...	svchost.exe	1128	Thread Create	
13.26.38,1071...	svchost.exe	1128	Thread Create	
13.26.39,8762...	svchost.exe	1040	Thread Create	
13.26.40,1040...	VBoxTray.exe	220	Thread Create	
13.26.40,2542...	VBoxTray.exe	220	Thread Exit	
13.26.42,2121...	Explorer.EXE	1116	Thread Exit	
13.26.43,6083...	Explorer.EXE	1116	Process Create	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
13.26.43,6083...	Malware_U3_W2_L2.exe	1324	Process Start	
13.26.43,6083...	Malware_U3_W2_L2.exe	1324	Thread Create	
13.26.43,6092...	Malware_U3_W2_L2.exe	1324	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
13.26.43,6096...	Malware_U3_W2_L2.exe	1324	Load Image	C:\WINDOWS\system32\ntdll.dll
13.26.43,6221...	Malware_U3_W2_L2.exe	1324	Load Image	C:\WINDOWS\system32\kernel32.dll
13.26.43,6476...	Malware_U3_W2_L2.exe	1324	Load Image	C:\WINDOWS\system32\apphelp.dll
13.26.43,6558...	Malware_U3_W2_L2.exe	1324	Load Image	C:\WINDOWS\system32\version.dll
13.26.43,6799...	Malware_U3_W2_L2.exe	1324	Load Image	C:\WINDOWS\system32\advapi32.dll
13.26.43,6803...	Malware_U3_W2_L2.exe	1324	Load Image	C:\WINDOWS\system32\rpcrt4.dll
13.26.43,6807...	Malware_U3_W2_L2.exe	1324	Load Image	C:\WINDOWS\system32\secur32.dll
13.26.43,6929...	Malware_U3_W2_L2.exe	1324	Process Create	C:\WINDOWS\system32\svchost.exe
13.26.43,6929...	svchost.exe	836	Process Start	
13.26.43,6929...	svchost.exe	836	Thread Create	
13.26.43,6970...	svchost.exe	836	Load Image	C:\WINDOWS\system32\ntdll.dll
13.26.43,7080...	svchost.exe	836	Load Image	C:\WINDOWS\system32\kernel32.dll
13.26.43,7107...	svchost.exe	836	Load Image	C:\WINDOWS\system32\user32.dll
13.26.43,7112...	svchost.exe	836	Load Image	C:\WINDOWS\system32\gdi32.dll
13.26.43,7152...	svchost.exe	836	Load Image	C:\WINDOWS\system32\shimeng.dll
13.26.43,7402...	svchost.exe	836	Load Image	C:\WINDOWS\AppPatch\AcGenral.dll
13.26.43,7406196	svchost.exe	836	Load Image	C:\WINDOWS\system32\advapi32.dll
13.26.43,7662...	svchost.exe	836	Load Image	C:\WINDOWS\system32\rpcrt4.dll
13.26.43,7666...	svchost.exe	836	Load Image	C:\WINDOWS\system32\secur32.dll

Come possiamo vedere nelle azioni del malware sul fyle system, guardando le operazioni ed il path, si capisce che crea un file dentro la cartella SVChost.exe, che è un processo di sistema generico di windows che ospita diversi servizi del sistema operativo. Basta andare a vedere la cartella (che tra l'altro è nascosta per motivi di sicurezza) e si può notare quanti servizi ci sono all'interno (dai giochi alle varie funzionalità del sistema operativo) e si capisce che è un processo fondamentale per il corretto funzionamento del sistema operativo dalla grande varieta e quantita di azioni effettuate da quest'ultimo durante l'accensione e l'uso del computer:

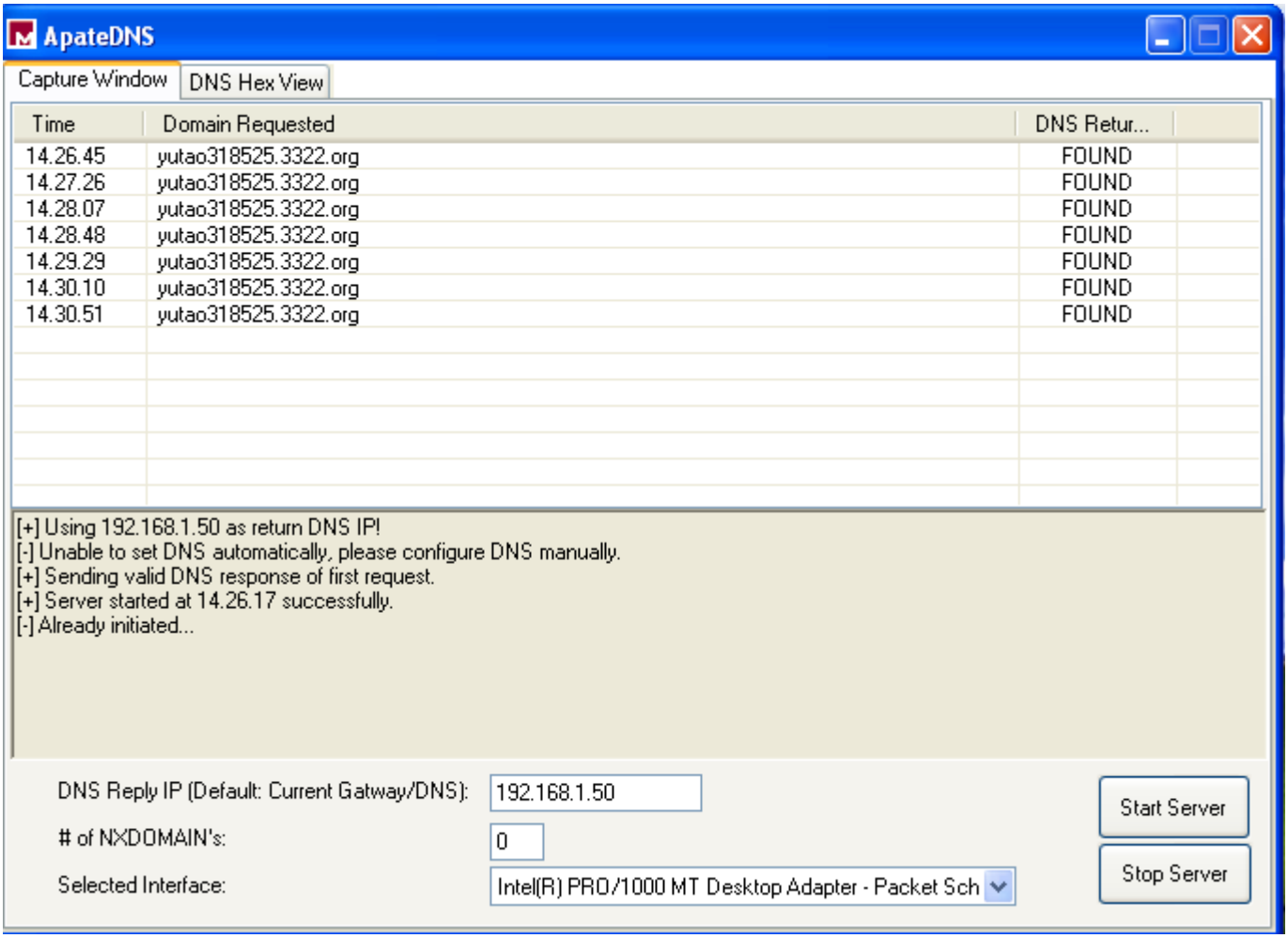


I malware generalmente creano file all'interno di questa cartella perche, essendo molto grande, si possono nascondere meglio ad un occhio disattento. Lo scopo del malware e la ragione per la quale si è

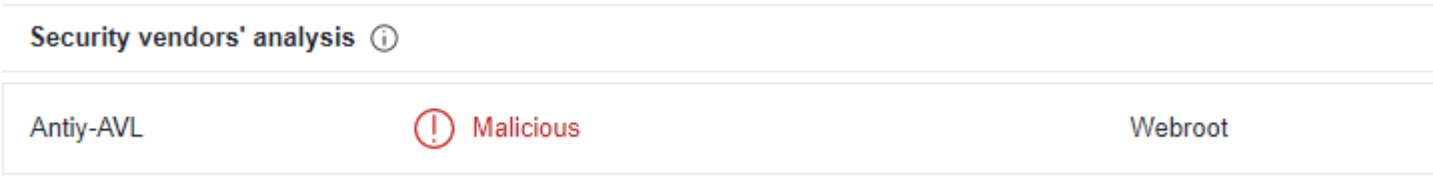
“intrufolato” in questo path è che se non preso in tempo ed individuato, si avvierà ogni volta ad avvio sistema operativo.

Come possiamo vedere infatti, una volta riavviato il computer, il malware non creerà più file all’interno del path, avendolo gia fatto, ma l’operation che farà sarà una query information file, quindi una richiesta di informazioni da rubare all’utente.

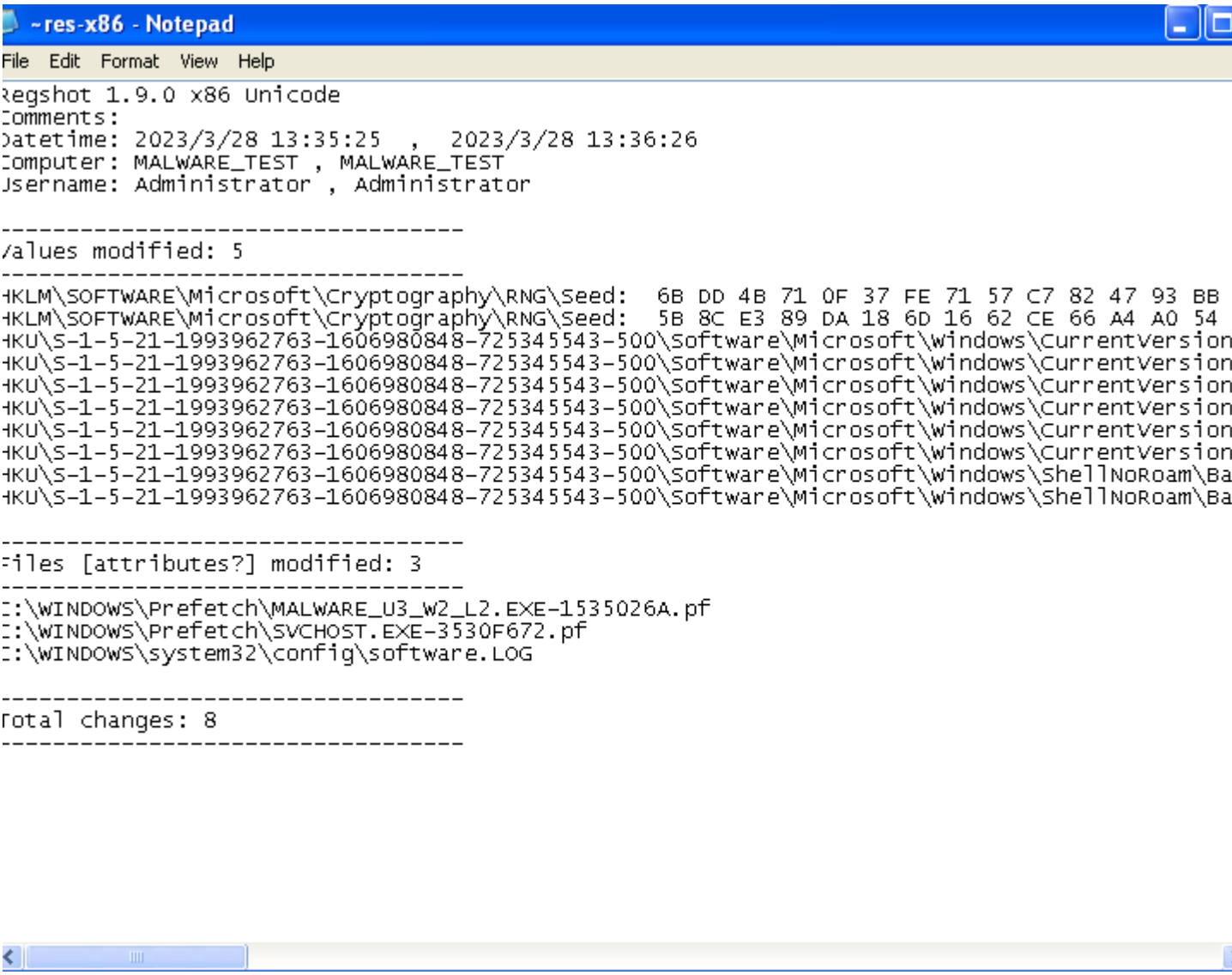
Ulteriori informazioni le possiamo estrapolare attivando ApateDNS, che simula un server DNS sullla porta 53 per intercettare tutti i collegamenti a domini o sottodomini che il malware vuole effettuare. Come possiamo notare dall’immagine, il malware cerca di connettersi a questo specifico dominio:



Come possiamo vedere, l’URL difatti è gia noto per essere un indirizzo malevolo:



Come possiamo vedere anche con REGSHOT, facendo partire il malware, esso effettua 3 operazioni:


~res-x86 - Notepad
File Edit Format View Help
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2023/3/28 13:35:25 , 2023/3/28 13:36:26
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator
Values modified: 5
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 6B DD 4B 71 0F 37 FE 71 57 C7 82 47 93 BB
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 5B 8C E3 89 DA 18 6D 16 62 CE 66 A4 A0 54
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Ba
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Ba
Files [attributes?] modified: 3
C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf
C:\WINDOWS\system32\config\software.LOG
Total changes: 8