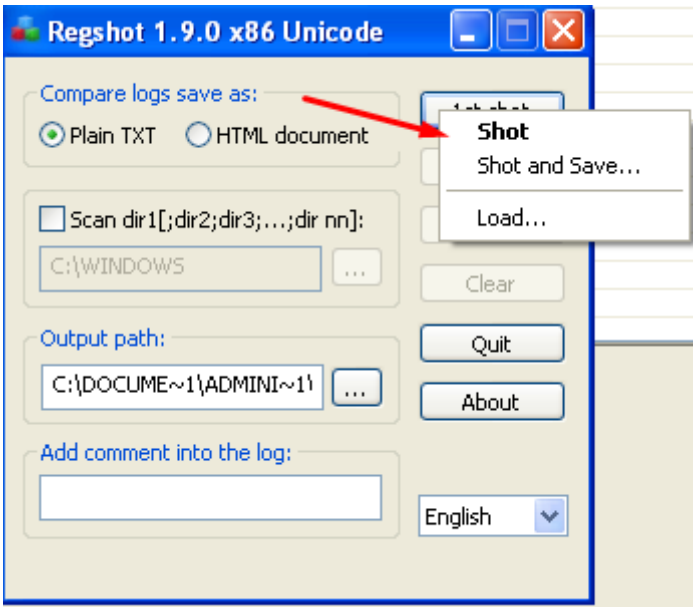
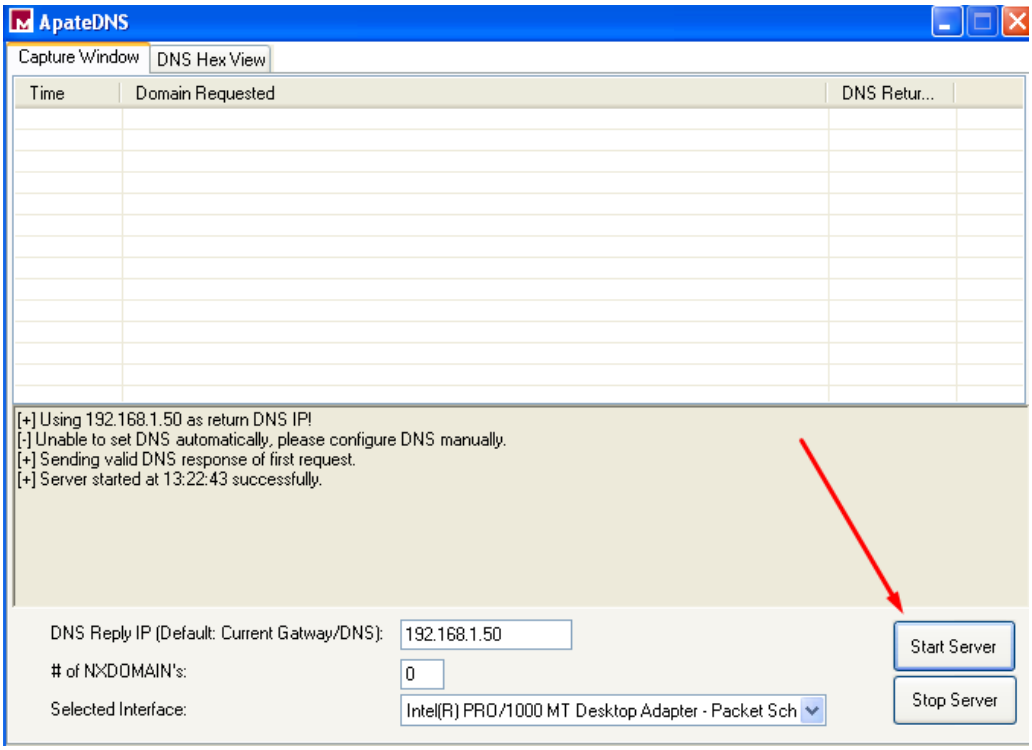
Alaimo Alessandro
10/01/2023

Report Analisi Dinamica Basica

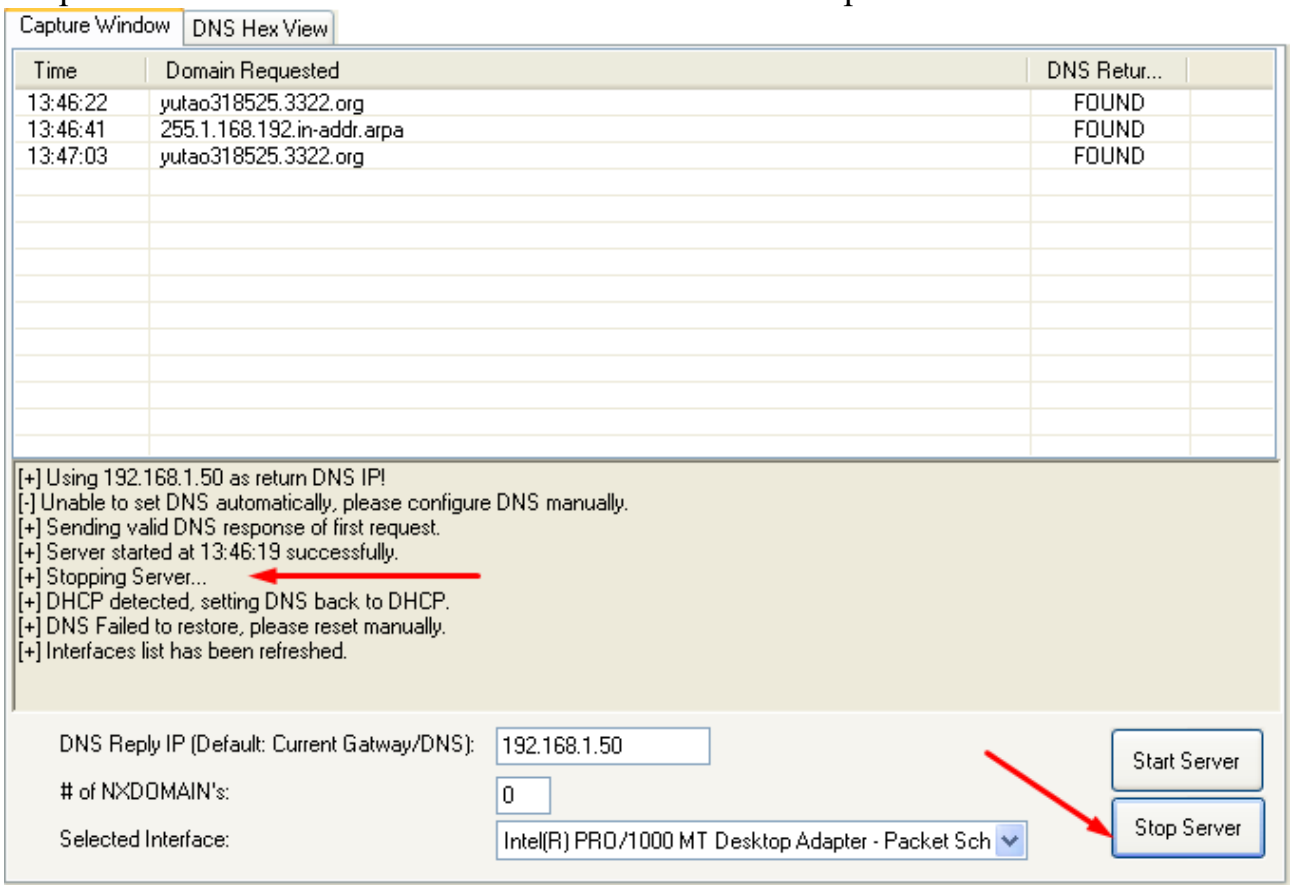
Per la risoluzione dell'esercizio, andiamo ad attivare la scheda di rete impostandola ad interna per poter utilizzare ApateDNS, in modo tale da controllare se il Malware cercherà di collegarsi ad internet. Fatto ciò, avviamo il computer e prima di ogni altra cosa, andiamo ad aprire Procmon, RegShot e ApateDNS. Prima dell'avvio di ApateDNS, andiamo a fare un primo shot sui registri di sistema con RegShot, come di seguito:



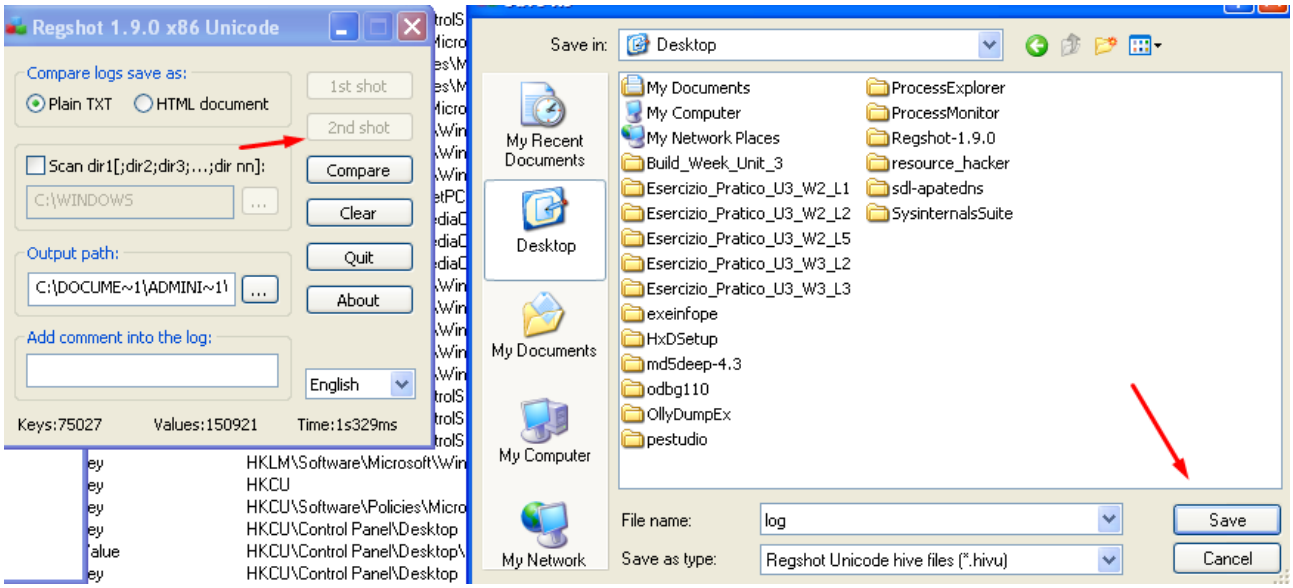
Ora andiamo ad impostare l'IP su ApateDNS ed avviamo il server:

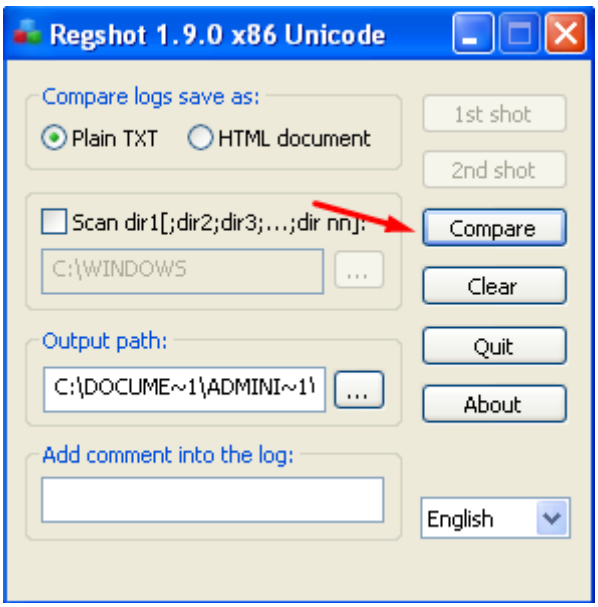


Fatto ciò, andiamo ad avviare il Malware ed andiamo ad aggiungere ai filtri il Process Name del Malware stesso. Aspettiamo qualche secondo ed interrompiamo la cattura dei processi ed andiamo a fermare il server creato con ApateDNS:



Fatto ciò, andiamo a fare il secondo shot con RegShot per poi andare a fare una comparazione:





Compare logs save as: ● Plain TXT ○ HTML document

Output path: C:\DOCUME~1\ADMINI~1\

English

```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2023/1/10 13:45:59  ,  2023/1/10 13:48:25
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

----------------------------------
Keys added: 10
----------------------------------
HKLM\SYSTEM\ControlSet001\Control\Print\Printers
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\DsDriver
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\DsSpooler
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\PrinterDriverData
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer\DsDriver
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer\DsSpooler
HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Microsoft XPS Document Writer\PrinterDriverData

----------------------------------
Values deleted: 2
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"

----------------------------------
Values added: 136
----------------------------------
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\DefaultSpoolDirectory: "C:\WINDOWS\System32\spool\PRINTERS"
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\ChangeID: 0x000E8C3E
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\Status: 0x00000080
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\Name: "Microsoft XPS Document Writer"
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\Share Name: ""
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\Print Processor: "WinPrint"
HKLM\SYSTEM\ControlSet001\Control\Print\Printers\Microsoft XPS Document Writer\Datatype: "RAW"
```

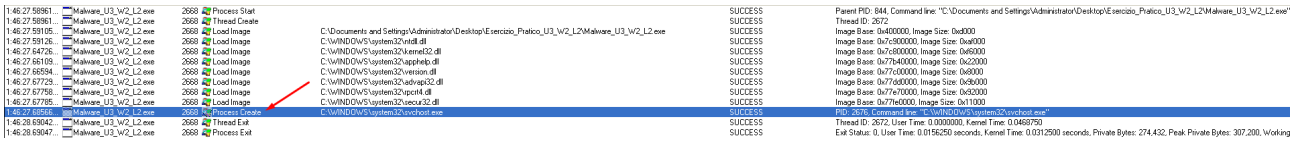
```
----------------------------------
Values modified: 15
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  DE C8 CC 48 F9 B4 87 A8 0E 15 83 8A 10 C3 C1 22 38 07 E5 79 E7 6B 44 07 21 A9 1B 51 43 B6 FE 7F 16
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  E4 C1 18 77 4E E2 4B 22 8C 85 C2 54 88 EA A4 0F F4 AE 63 32 BB 87 60 77 E1 16 3D 95 91 D7 4D 15 9C
HKLM\SYSTEM\ControlSet001\Control\Print\Providers\LogonTime:  70 B0 8B 9C F8 24 D9 01
HKLM\SYSTEM\ControlSet001\Control\Print\Providers\LogonTime:  DA 0A A1 E4 F9 24 D9 01
HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\EventMessageFile: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\EventMessageFile: "C:\WINDOWS\system32\ESENT.dll"
HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\CategoryMessageFile: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\ControlSet001\Services\Eventlog\Application\ESENT\CategoryMessageFile: "C:\WINDOWS\system32\ESENT.dll"
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\Count: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\Count: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInstance: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\Print\Providers\LogonTime:  70 B0 8B 9C F8 24 D9 01
HKLM\SYSTEM\CurrentControlSet\Control\Print\Providers\LogonTime:  DA 0A A1 E4 F9 24 D9 01
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ESENT\EventMessageFile: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ESENT\EventMessageFile: "C:\WINDOWS\system32\ESENT.dll"
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryMessageFile: "c:\windows\system32\ESENT.dll"
HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\ESENT\CategoryMessageFile: "C:\WINDOWS\system32\ESENT.dll"
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Count: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Count: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\NextInstance: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx:  07 00 00 00 06 00 00 00 02 00 00 00 1C
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx:  17 00 00 00 07 00 00 00 06 00 00 00 02

----------------------------------
Total changes: 163
----------------------------------
```

Fatto ciò andiamo a controllare da Procmon ciò che il Malware ha effettuato, iniziando a visualizzare le azione fatte su File System:

1:46:27.59153...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS
1:46:27.59529...	Malware_U3_W2_L2.exe	2668	CreateFile	C:	SUCCESS
1:46:27.59811...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\	SUCCESS
1:46:27.59936...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS
1:46:27.60191...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS
1:46:27.60334...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
1:46:27.60566...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	SUCCESS
1:46:27.60799...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS	SUCCESS
1:46:27.61007...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\AppPatch	SUCCESS
1:46:27.61135...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32	SUCCESS
1:46:27.61603...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS
1:46:27.61661...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS
1:46:27.61762...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\unicode.nls	SUCCESS
1:46:27.61820...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\locale.nls	SUCCESS
1:46:27.61913...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\sorttbls.nls	SUCCESS
1:46:27.61959...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\MALWARE_U3_W2_L2.EXE	SUCCESS
1:46:27.62051...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\ctype.nls	SUCCESS
1:46:27.62109...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS
1:46:27.62204...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS
1:46:27.62278...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS
1:46:27.62358...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS
1:46:27.62416...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS
1:46:27.62506...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS
1:46:27.62564...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS
1:46:27.62642...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS
1:46:27.63493...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS
1:46:27.63554...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS
1:46:27.63640...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\MALWARE_U3_W2_L2.EXE	SUCCESS
1:46:27.63686...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS
1:46:27.63790...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS
1:46:27.63850...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS
1:46:27.63948...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS
1:46:27.64007...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS
1:46:27.64636...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS
1:46:27.65726...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS
1:46:27.65833...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS
1:46:27.66018...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS
1:46:27.66150...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS
1:46:27.66253...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\AppPatch\systest.sdb	NAME NOT FOUND
1:46:27.66292...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32	SUCCESS
1:46:27.66362...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\	SUCCESS
1:46:27.66390...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS	SUCCESS
1:46:27.66475...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32	SUCCESS
1:46:27.66662...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS
1:46:27.66778...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS
1:46:27.66910...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS
1:46:27.67284...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS
1:46:27.67387...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\	SUCCESS
1:46:27.67414...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS	SUCCESS
1:46:27.67630...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32	SUCCESS
1:46:27.68034...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\	SUCCESS
1:46:27.68062...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS	SUCCESS
1:46:27.68108...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32	SUCCESS
1:46:27.68543...	Malware_U3_W2_L2.exe	2668	CreateFile	C:\WINDOWS\system32\svchost.exe.Manifest	NAME NOT FOUND

Ora controlliamo se ha creato un nuovo processo o thread, come di seguito:



Il processo creato ***svchost.exe,*** non è di per sé un virus poiché è un file usato da molte applicazioni Windows, anche se in passato hanno inserito file dannosi all'interno del servizio ***svchost.exe*** per impedirne il rilevamento.

Facendo un analisi un po' più approfondita, si riesce a trovare che il Malware usa la libreria rpcrt4.dll, la quale serve per effettuare connessioni UDP e TCP ad un IP non conosciuto, ma non avendo accesso ad internet ha fallito l'operazione. Possiamo categorizzare il Malware come un Trojan poiché non essendo di per sé malevolo, può ingannare le difese del PC e connettersi al server per scaricare materiale potenzialmente dannoso.