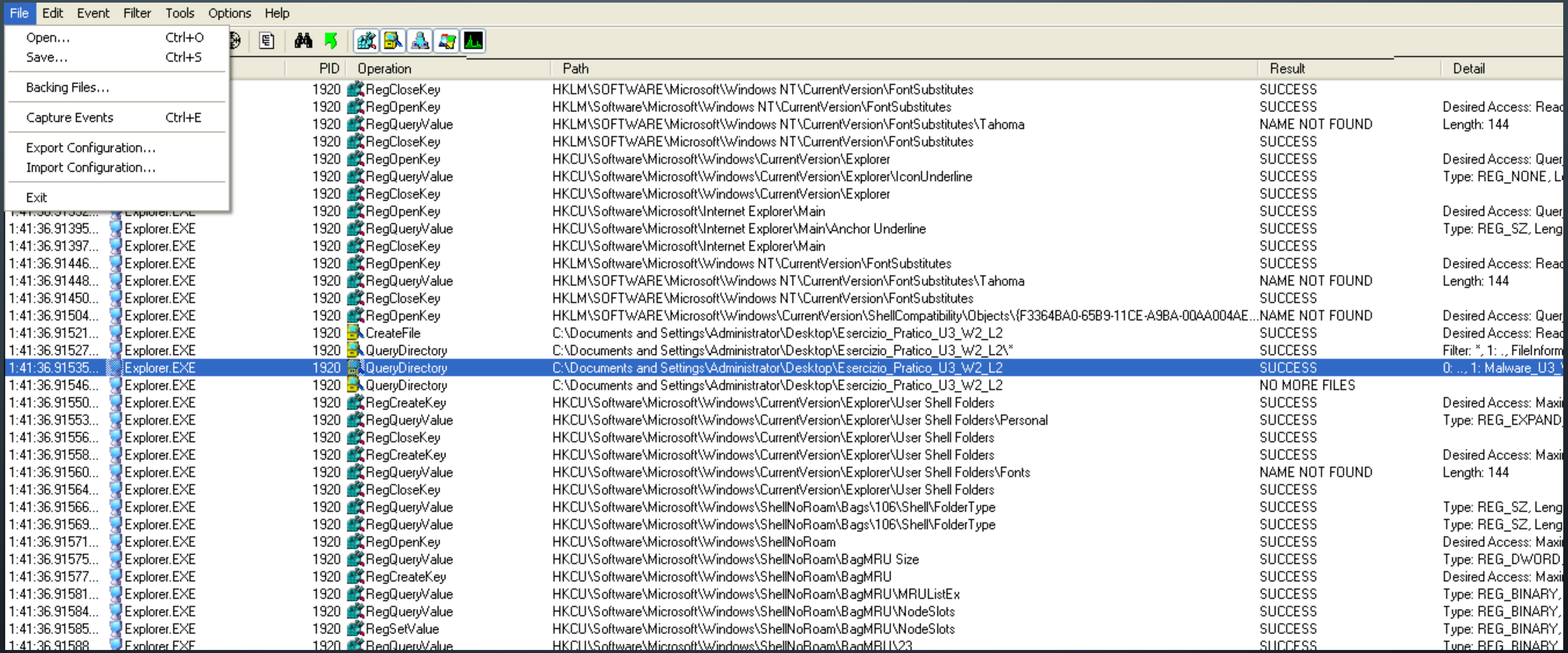
S10L2

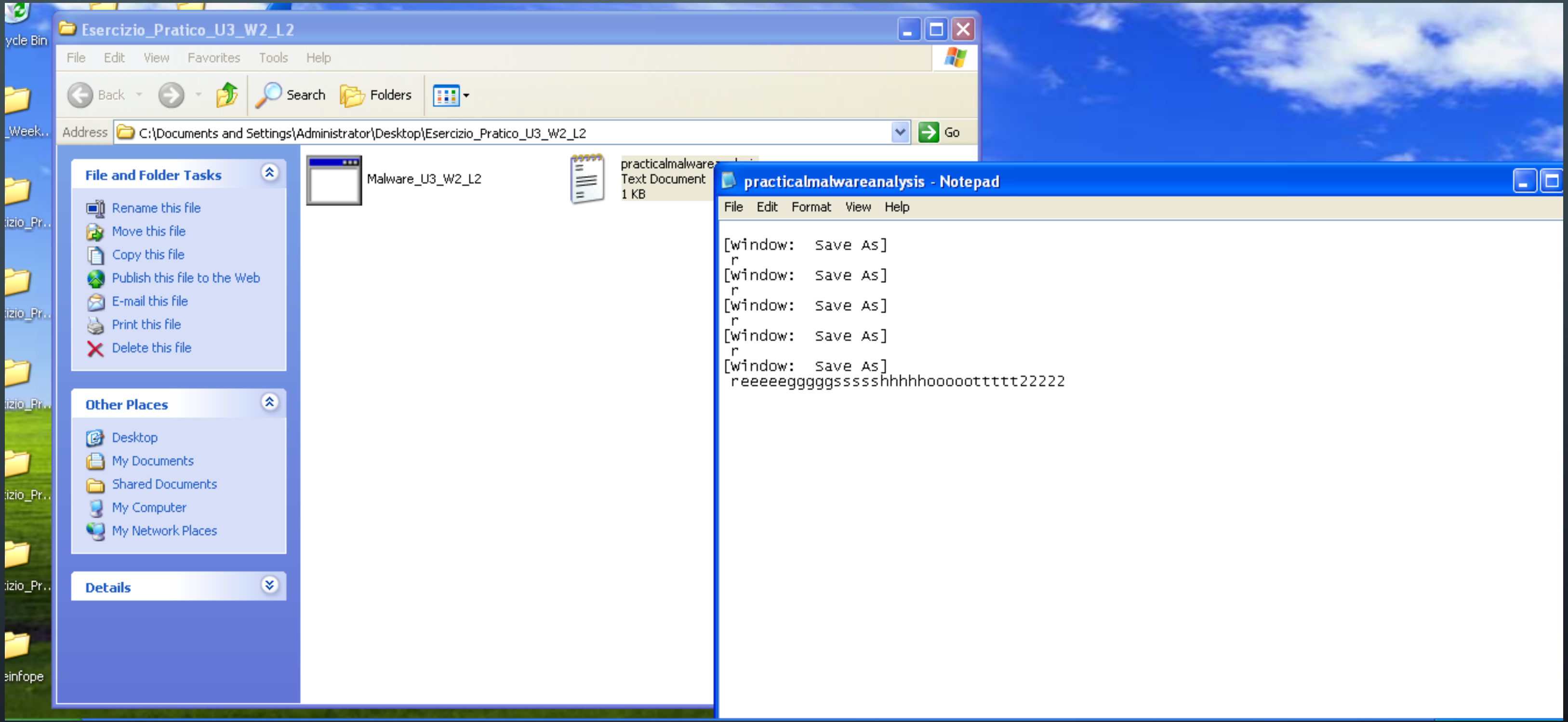
CON RIFERIMENTO AL FILE ESEGUIBILE CONTENUTO NELLA CARTELLA «ESERCIZIO_PRATICO_U3_W2_L2» PRESENTE SUL DESKTOP DELLA VOSTRA MACCHINA VIRTUALE DEDICATA ALL'ANALISI DEI MALWARE, RISPONDERE AI SEGUENTI QUESITI: IDENTIFICARE EVENTUALI AZIONI DEL MALWARE SUL FILE SYSTEM UTILIZZANDO PROCESS MONITOR IDENTIFICARE EVENTUALI AZIONI DEL MALWARE SU PROCESSI E THREAD UTILIZZANDO PROCESS MONITOR PROVARE A PROFILARE IL MALWARE IN BASE ALLA CORRELAZIONE TRA «OPERATION» E PATH

SOLUZIONE – IDENTIFICARE AZIONI SU FILE SYSTEM DEL MALWARE PER PRIMA COSA, FACCIAMO PARTIRE PROCMON PRIMA DI ESEGUIRE IL MALWARE E , SUCCESSIVAMENTE AVVIAMO IL MALWARE E DOPO UN LASSO DI TEMPO TROVEREMO CHE IL FILE TROVATO VIENE REGISTRATO NELLE **QUERY DIRECTORY** OVVERO ATTIVITA' RELATIVE AL FILE SYSTEM



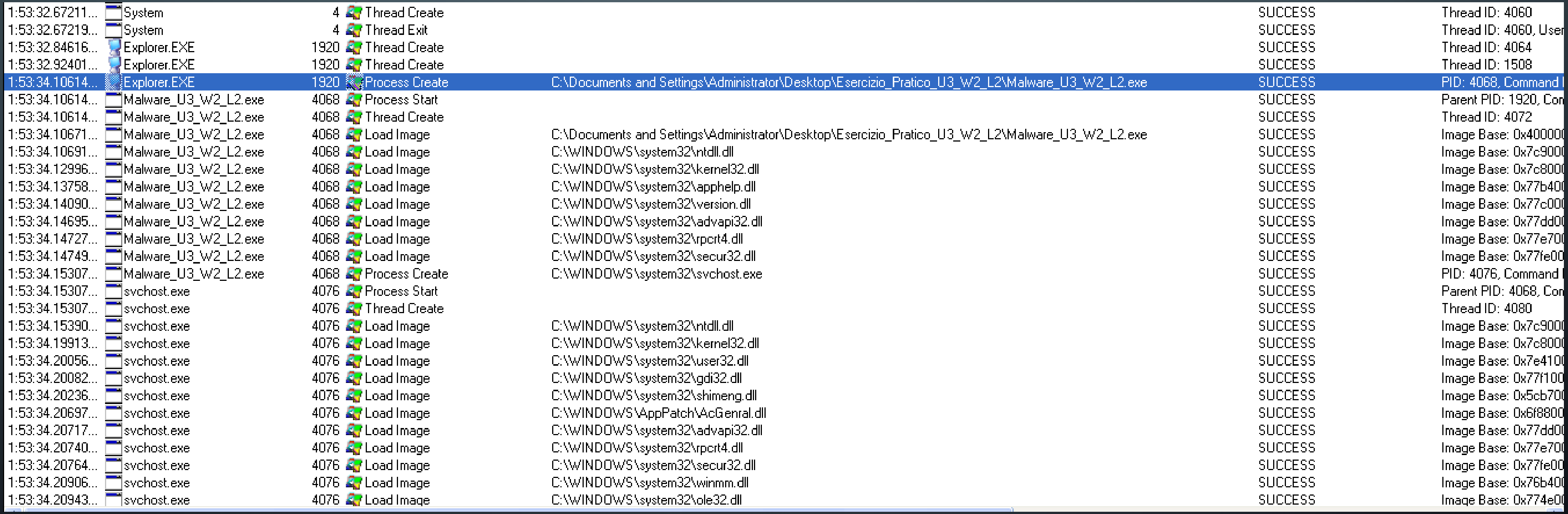
		PID	Operation	Path	Result	Detail
		1920	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	SUCCESS	
		1920	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	SUCCESS	Desired Access: Rea
		1920	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tahoma	NAME NOT FOUND	Length: 144
		1920	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	SUCCESS	
		1920	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	Desired Access: Quer
		1920	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\IconUnderline	SUCCESS	Type: REG_NONE, L
		1920	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer	SUCCESS	
[illegible]	Explorer.EXE	1920	RegOpenKey	HKCU\Software\Microsoft\Internet Explorer\Main	SUCCESS	Desired Access: Quer
1:41:36.91395...	Explorer.EXE	1920	RegQueryValue	HKCU\Software\Microsoft\Internet Explorer\Main\Anchor Underline	SUCCESS	Type: REG_SZ, Leng
1:41:36.91397...	Explorer.EXE	1920	RegCloseKey	HKCU\Software\Microsoft\Internet Explorer\Main	SUCCESS	
1:41:36.91446...	Explorer.EXE	1920	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	SUCCESS	Desired Access: Rea
1:41:36.91448...	Explorer.EXE	1920	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tahoma	NAME NOT FOUND	Length: 144
1:41:36.91450...	Explorer.EXE	1920	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	SUCCESS	
1:41:36.91504...	Explorer.EXE	1920	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{F3364BA0-65B9-11CE-A9BA-00AA004AE...	NAME NOT FOUND	Desired Access: Quer
1:41:36.91521...	Explorer.EXE	1920	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access: Rea
1:41:36.91527...	Explorer.EXE	1920	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\*	SUCCESS	Filter: *, 1: ., FileInform
1:41:36.91535...	Explorer.EXE	1920	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	0: .., 1: Malware_U3_
1:41:36.91546...	Explorer.EXE	1920	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES	
1:41:36.91550...	Explorer.EXE	1920	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	SUCCESS	Desired Access: Maxi
1:41:36.91553...	Explorer.EXE	1920	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Personal	SUCCESS	Type: REG_EXPAND
1:41:36.91556...	Explorer.EXE	1920	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	SUCCESS	
1:41:36.91558...	Explorer.EXE	1920	RegCreateKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	SUCCESS	Desired Access: Maxi
1:41:36.91560...	Explorer.EXE	1920	RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Fonts	NAME NOT FOUND	Length: 144
1:41:36.91564...	Explorer.EXE	1920	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	SUCCESS	
1:41:36.91566...	Explorer.EXE	1920	RegQueryValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\FolderType	SUCCESS	Type: REG_SZ, Leng
1:41:36.91569...	Explorer.EXE	1920	RegQueryValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\FolderType	SUCCESS	Type: REG_SZ, Leng
1:41:36.91571...	Explorer.EXE	1920	RegOpenKey	HKCU\Software\Microsoft\Windows\ShellNoRoam	SUCCESS	Desired Access: Maxi
1:41:36.91575...	Explorer.EXE	1920	RegQueryValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU Size	SUCCESS	Type: REG_DWORD
1:41:36.91577...	Explorer.EXE	1920	RegCreateKey	HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU	SUCCESS	Desired Access: Maxi
1:41:36.91581...	Explorer.EXE	1920	RegQueryValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx	SUCCESS	Type: REG_BINARY,
1:41:36.91584...	Explorer.EXE	1920	RegQueryValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots	SUCCESS	Type: REG_BINARY,
1:41:36.91585...	Explorer.EXE	1920	RegSetValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots	SUCCESS	Type: REG_BINARY,
1:41:36.91588...	Explorer.EXE	1920	RegQueryValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\BagMRU\23	SUCCESS	Type: REG_BINARY

APRIAMO LA CARTELLA SUL DESKTOP DOVE RISIEDE L'ESEGUIBILE DEL MALWARE PER CONFERMARE CHE IN EFFETTI IL MALWARE HA CREATO UN FILE DENOMINATO «PRACTICALMALWAREANALYSIS» APRIAMO IL FILE PER NOTARE CHE IL FILE HA ACQUISITO ALCUNI DEI CARATTERI DA TASTIERA UTILIZZATI DURANTE L'ESECUZIONE DEL MALWARE – QUESTO COMPORTAMENTO È PIUTTOSTO SOLITO DEI MALWARE KEYLOGGER.



```
[Window:  Save As]
 r
[Window:  Save As]
 r
[Window:  Save As]
 r
[Window:  Save As]
 r
[Window:  Save As]
 reeeeegggggssssshhhhhoooootttttt22222
```

VEDIAMO ALCUNE FUNZIONI MOLTO INTERESSANTI COME LOAD IMAGE CHE VIENE UTILIZZATA PER «CARICARE» PER L’ESECUZIONE IL MALWARE E LE LIBRERIE (.DLL) NECESSARIE, E POI VEDIAMO «PROCESS CREATE» CHE SERVE PER CREARE UN PROCESSO. SEMBRA CHE IL NOSTRO MALWARE STIA CREANDO UN PROCESSO CHIAMATO «SVCHOST.EXE» CHE GENERALMENTE È UN PROCESSO VALIDO DI WINDOWS. QUESTO È UN ALTRO COMPORTAMENTO FREQUENTE DEI MALWARE, CERCARE DI CAMUFFARE LA LORO ESECUZIONE SOTTO UN PROCESSO CON UN NOME VALIDO PER ELUDERE EVENTUALI ANTIVIRUS / ANTI MALWARE. ALLA VOCE **SVCHOST.EXE** SAREBBE IL FILE CAMUFFATO DA KEYLOGGER



```
1:53:32.67211... System                4 Thread Create                                                                                        SUCCESS    Thread ID: 4060
1:53:32.67219... System                4 Thread Exit                                                                                          SUCCESS    Thread ID: 4060, User
1:53:32.84616... Explorer.EXE       1920 Thread Create                                                                                        SUCCESS    Thread ID: 4064
1:53:32.92401... Explorer.EXE       1920 Thread Create                                                                                        SUCCESS    Thread ID: 1508
1:53:34.10614... Explorer.EXE       1920 Process Create  C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe  SUCCESS    PID: 4068, Command l
1:53:34.10614... Malware_U3_W2_L2.exe 4068 Process Start                                                                                      SUCCESS    Parent PID: 1920, Con
1:53:34.10614... Malware_U3_W2_L2.exe 4068 Thread Create                                                                                      SUCCESS    Thread ID: 4072
1:53:34.10671... Malware_U3_W2_L2.exe 4068 Load Image    C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe  SUCCESS    Image Base: 0x40000(
1:53:34.10691... Malware_U3_W2_L2.exe 4068 Load Image    C:\WINDOWS\system32\ntdll.dll                                                SUCCESS    Image Base: 0x7c900(
1:53:34.12996... Malware_U3_W2_L2.exe 4068 Load Image    C:\WINDOWS\system32\kernel32.dll                                             SUCCESS    Image Base: 0x7c800(
1:53:34.13758... Malware_U3_W2_L2.exe 4068 Load Image    C:\WINDOWS\system32\apphelp.dll                                              SUCCESS    Image Base: 0x77b40(
1:53:34.14090... Malware_U3_W2_L2.exe 4068 Load Image    C:\WINDOWS\system32\version.dll                                              SUCCESS    Image Base: 0x77c00(
1:53:34.14695... Malware_U3_W2_L2.exe 4068 Load Image    C:\WINDOWS\system32\advapi32.dll                                             SUCCESS    Image Base: 0x77dd0(
1:53:34.14727... Malware_U3_W2_L2.exe 4068 Load Image    C:\WINDOWS\system32\rpcrt4.dll                                               SUCCESS    Image Base: 0x77e70(
1:53:34.14749... Malware_U3_W2_L2.exe 4068 Load Image    C:\WINDOWS\system32\secur32.dll                                              SUCCESS    Image Base: 0x77fe0(
1:53:34.15307... Malware_U3_W2_L2.exe 4068 Process Create C:\WINDOWS\system32\svchost.exe                                             SUCCESS    PID: 4076, Command l
1:53:34.15307... svchost.exe        4076 Process Start                                                                                        SUCCESS    Parent PID: 4068, Con
1:53:34.15307... svchost.exe        4076 Thread Create                                                                                        SUCCESS    Thread ID: 4080
1:53:34.15390... svchost.exe        4076 Load Image      C:\WINDOWS\system32\ntdll.dll                                                SUCCESS    Image Base: 0x7c900(
1:53:34.19913... svchost.exe        4076 Load Image      C:\WINDOWS\system32\kernel32.dll                                             SUCCESS    Image Base: 0x7c800(
1:53:34.20056... svchost.exe        4076 Load Image      C:\WINDOWS\system32\user32.dll                                               SUCCESS    Image Base: 0x7e410(
1:53:34.20082... svchost.exe        4076 Load Image      C:\WINDOWS\system32\gdi32.dll                                                SUCCESS    Image Base: 0x77f10(
1:53:34.20236... svchost.exe        4076 Load Image      C:\WINDOWS\system32\shimeng.dll                                              SUCCESS    Image Base: 0x5cb70(
1:53:34.20697... svchost.exe        4076 Load Image      C:\WINDOWS\AppPatch\AcGenral.dll                                             SUCCESS    Image Base: 0x6f880(
1:53:34.20717... svchost.exe        4076 Load Image      C:\WINDOWS\system32\advapi32.dll                                             SUCCESS    Image Base: 0x77dd0(
1:53:34.20740... svchost.exe        4076 Load Image      C:\WINDOWS\system32\rpcrt4.dll                                               SUCCESS    Image Base: 0x77e70(
1:53:34.20764... svchost.exe        4076 Load Image      C:\WINDOWS\system32\secur32.dll                                              SUCCESS    Image Base: 0x77fe0(
1:53:34.20906... svchost.exe        4076 Load Image      C:\WINDOWS\system32\winmm.dll                                                SUCCESS    Image Base: 0x76b40(
1:53:34.20943... svchost.exe        4076 Load Image      C:\WINDOWS\system32\ole32.dll                                                SUCCESS    Image Base: 0x774e0(
```