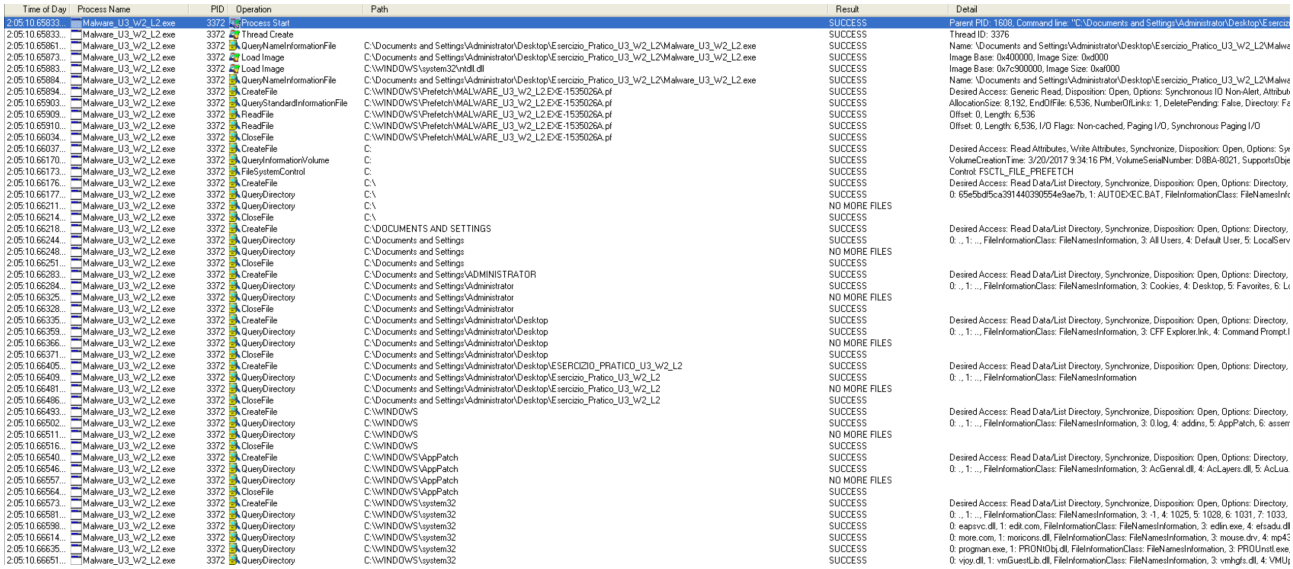
Relazione S10L2

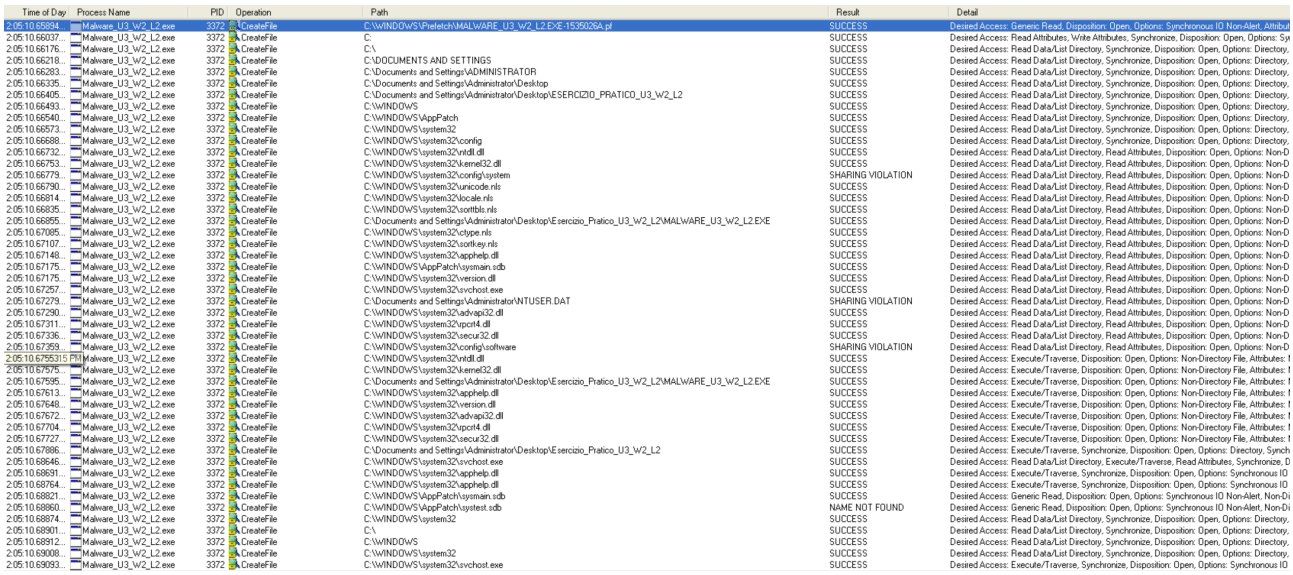
L'obiettivo è analizzare un malware tramite l'analisi dinamica basica utilizzando i diversi softwares che abbiamo a disposizione.

La prima cosa che viene richiesta è di identificare eventuali azioni del malware sul file system. Utilizzando process monitor sono andato a vedere i processi eseguiti dal malware analizzato.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
2:05:10.65833...	Malware_U3_W2_L2.exe	3372	Process Start		SUCCESS	Parent PID: 1608, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizi
2:05:10.65833...	Malware_U3_W2_L2.exe	3372	Thread Create		SUCCESS	Thread ID: 3376
2:05:10.65861...	Malware_U3_W2_L2.exe	3372	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Name: \Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwa
2:05:10.65873...	Malware_U3_W2_L2.exe	3372	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
2:05:10.65883...	Malware_U3_W2_L2.exe	3372	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
2:05:10.65894...	Malware_U3_W2_L2.exe	3372	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Name: \Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malwa
2:05:10.65894...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attribut
2:05:10.65903...	Malware_U3_W2_L2.exe	3372	QueryStandardInformationFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	AllocationSize: 8,192, EndOfFile: 6,536, NumberOfLinks: 1, DeletePending: False, Directory: Fa
2:05:10.65909...	Malware_U3_W2_L2.exe	3372	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	Offset: 0, Length: 6,536
2:05:10.65910...	Malware_U3_W2_L2.exe	3372	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	Offset: 0, Length: 6,536, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
2:05:10.66034...	Malware_U3_W2_L2.exe	3372	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	
2:05:10.66037...	Malware_U3_W2_L2.exe	3372	CreateFile	C:	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Syr
2:05:10.66170...	Malware_U3_W2_L2.exe	3372	QueryInformationVolume	C:	SUCCESS	VolumeCreationTime: 3/20/2017 9:34:16 PM, VolumeSerialNumber: D8BA-8021, SupportsObje
2:05:10.66173...	Malware_U3_W2_L2.exe	3372	FileSystemControl	C:	SUCCESS	Control: FSCTL_FILE_PREFETCH
2:05:10.66176...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66177...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\	SUCCESS	0: 65e5bdf5ca391440390554e9ae7b, 1: AUTOEXEC.BAT, FileInformationClass: FileNamesInfo
2:05:10.66211...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\	NO MORE FILES	
2:05:10.66214...	Malware_U3_W2_L2.exe	3372	CloseFile	C:\	SUCCESS	
2:05:10.66218...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66244...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: All Users, 4: Default User, 5: LocalServ
2:05:10.66248...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
2:05:10.66251...	Malware_U3_W2_L2.exe	3372	CloseFile	C:\Documents and Settings	SUCCESS	
2:05:10.66283...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66284...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: Cookies, 4: Desktop, 5: Favorites, 6: L
2:05:10.66325...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
2:05:10.66328...	Malware_U3_W2_L2.exe	3372	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
2:05:10.66335...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66359...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: CFF Explorer.lnk, 4: Command Prompt.l
2:05:10.66366...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
2:05:10.66371...	Malware_U3_W2_L2.exe	3372	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
2:05:10.66405...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66409...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation
2:05:10.66481...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES	
2:05:10.66486...	Malware_U3_W2_L2.exe	3372	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
2:05:10.66493...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66502...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assem
2:05:10.66511...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS	NO MORE FILES	
2:05:10.66516...	Malware_U3_W2_L2.exe	3372	CloseFile	C:\WINDOWS	SUCCESS	
2:05:10.66540...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66546...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\AppPatch	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: AcGenral.dll, 4: AcLayers.dll, 5: AcLua.
2:05:10.66557...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\AppPatch	NO MORE FILES	
2:05:10.66564...	Malware_U3_W2_L2.exe	3372	CloseFile	C:\WINDOWS\AppPatch	SUCCESS	
2:05:10.66573...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66581...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: 1, 4: 1025, 5: 1028, 6: 1031, 7: 1033,
2:05:10.66598...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: eapsvc.dll, 1: edit.com, FileInformationClass: FileNamesInformation, 3: edlin.exe, 4: efsadu.dll
2:05:10.66614...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: more.com, 1: moricons.dll, FileInformationClass: FileNamesInformation, 3: mouse.drv, 4: mp43
2:05:10.66635...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: progman.exe, 1: PRONtObj.dll, FileInformationClass: FileNamesInformation, 3: PROUnstl.exe
2:05:10.66651...	Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: vjoy.dll, 1: vmGuestLib.dll, FileInformationClass: FileNamesInformation, 3: vmhgfs.dll, 4: VMU

Tra le azioni che possiamo vedere abbiamo la creazione dei file:



Time of Day	Process Name	PID	Operation	Path	Result	Detail
2:05:10.65894...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attribut
2:05:10.66037...	Malware_U3_W2_L2.exe	3372	CreateFile	C:	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Syr
2:05:10.66176...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66218...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66283...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66335...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66405...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66493...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66540...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66573...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66688...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\config	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.66732...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.66753...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.66779...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\config\system	SHARING VIOLATION	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.66790...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\unicode.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.66814...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\locale.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.66835...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.66855...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\MALWARE_U3_W2_L2.EXE	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67085...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\ctype.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67107...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67148...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67175...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67175...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67257...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67279...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\Administrator\NTUSER.DAT	SHARING VIOLATION	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67290...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67311...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67336...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67359...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\config\software	SHARING VIOLATION	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-D
2:05:10.67531...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: I
2:05:10.67575...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: I
2:05:10.67595...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\MALWARE_U3_W2_L2.EXE	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: I
2:05:10.67613...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: I
2:05:10.67648...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: I
2:05:10.67672...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: I
2:05:10.67704...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: I
2:05:10.67727...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: I
2:05:10.67886...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synch
2:05:10.68646...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize, D
2:05:10.68691...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO
2:05:10.68764...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO
2:05:10.68821...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Di
2:05:10.68860...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\AppPatch\systest.sdb	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Di
2:05:10.68874...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.68901...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.68912...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.69008...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
2:05:10.69093...	Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO

Per quanto riguarda i processi vediamo questo:

Time of Day	Process Name	PID	Operation	Path	Result	Detail
2:05:10.65833...	Malware_U3_W2_L2.exe	3372	Process Start		SUCCESS	Parent PID: 1608, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_F
2:05:10.69839...	Malware_U3_W2_L2.exe	3372	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 3380, Command line: "C:\WINDOWS\system32\svchost.exe"
2:05:11.68455...	Malware_U3_W2_L2.exe	3372	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 27
3:40:13.42224...	Malware_U3_W2_L2.exe	2908	Process Start		SUCCESS	Parent PID: 1608, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_F
3:40:13.44808...	Malware_U3_W2_L2.exe	2908	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2912, Command line: "C:\WINDOWS\system32\svchost.exe"
3:40:14.43549...	Malware_U3_W2_L2.exe	2908	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 27

Tra le voci di registro modificate troviamo queste:

~res-x86_0017 - Notepad

File Edit Format View Help

```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2023/11/28 15:40:05  ,  2023/11/28 15:40:19
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

----------------------------------
Values modified: 3
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  AE EF 9B 3C 5C 64 E8 EE CB 04 85 C5 B6 FA DE 5B BE E3 24 71 75 94 6B AA D5 22 4B 03 46 97 72 C4 94 77 AB CE 37 48 A
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  3A E0 A4 ED 83 F8 DB 93 9D 3F 14 B1 37 4B 40 79 6D 34 5C C1 2D 7F CB B7 1E C9 71 BE C0 B0 3F 2F C2 8A 92 37 39 5D E
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EH.
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EH.
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EH.
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EH.

----------------------------------
Total changes: 3
----------------------------------
```

In base a quello che vedo non sono in grado di dare ulteriori informazioni. Il malware crea un processo e allo stesso tempo va a creare diversi files all'interno di system32. Per capire cosa faccia nello specifico sono necessarie ulteriori analisi.

Davide Lecci