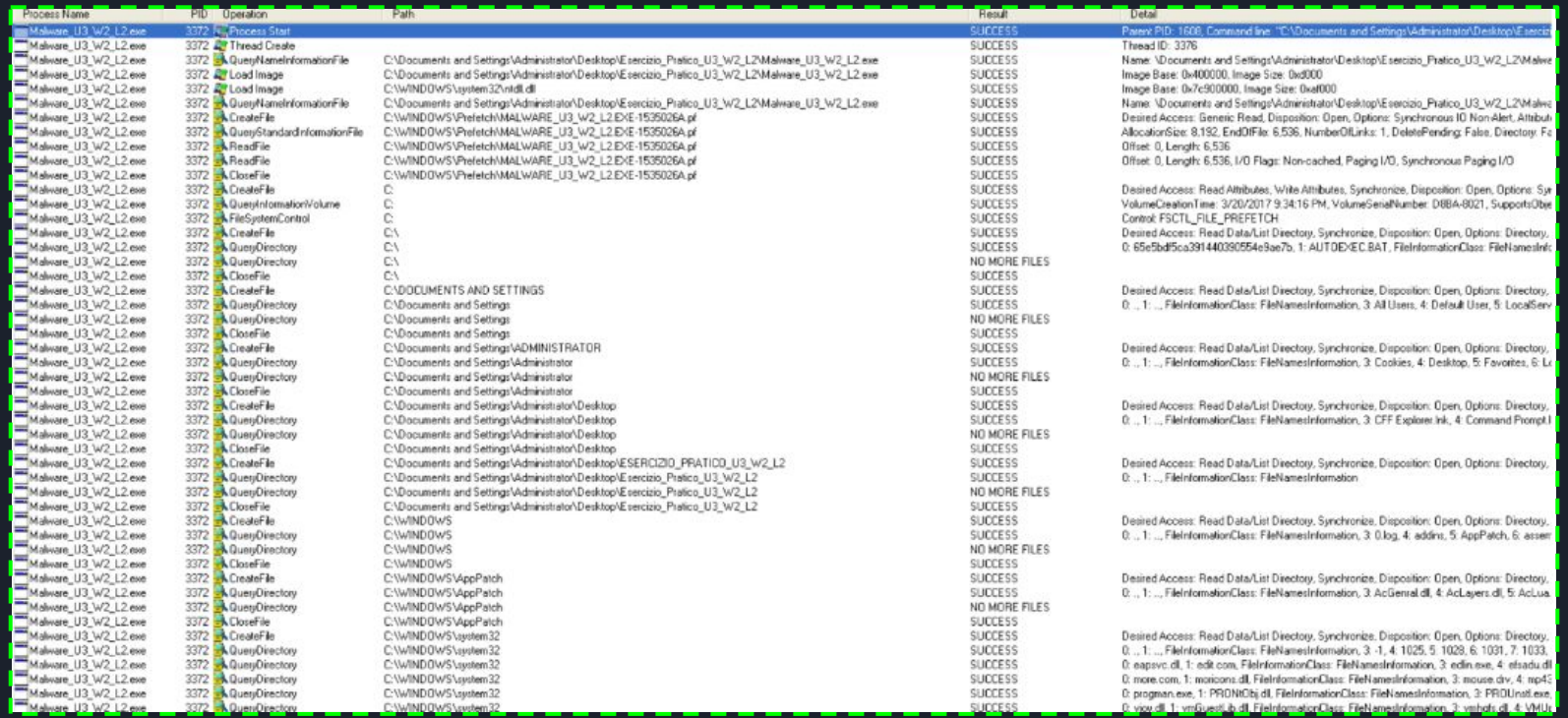
ANALISI DINAMICA MALWARE

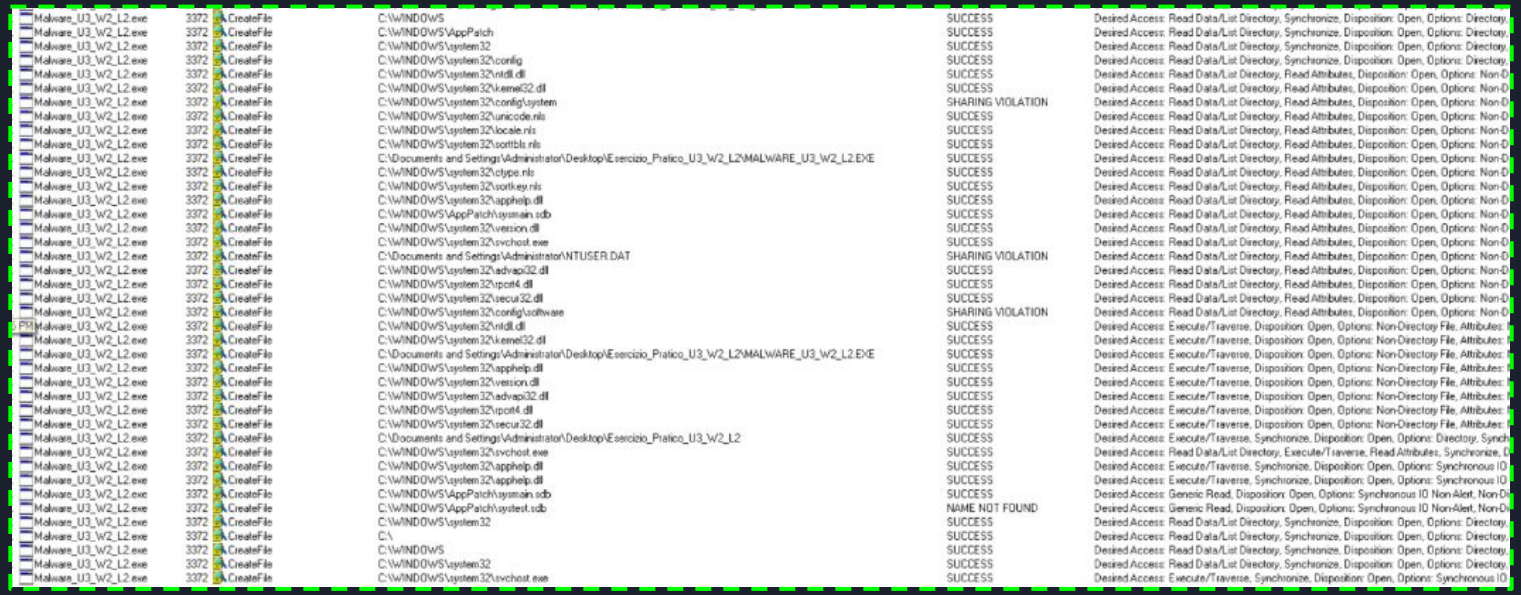
Kamenica Kristiano

Per migliorare l'analisi dinamica di questo malware, abbiamo integrato l'uso di Process Monitor. Questo strumento ci permette di acquisire una visione dettagliata dei processi in esecuzione durante l'attività del malware.
Con questa aggiunta, saremo in grado di individuare comportamenti sospetti o anomalie nel contesto dell'esecuzione del codice dannoso, fornendoci una comprensione più approfondita delle sue azioni e potenziali rischi per il sistema.



Process Name	PID	Operation	Path	Result	Detail
Malware_U3_W2_L2.exe	3372	Process Start		SUCCESS	Parent PID: 1608, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizi
Malware_U3_W2_L2.exe	3372	Thread Create		SUCCESS	Thread ID: 3376
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
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
Malware_U3_W2_L2.exe	3372	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
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
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
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
Malware_U3_W2_L2.exe	3372	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	Offset: 0, Length: 6,536
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
Malware_U3_W2_L2.exe	3372	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf	SUCCESS	
Malware_U3_W2_L2.exe	3372	CreateFile	C:	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Syn
Malware_U3_W2_L2.exe	3372	QueryInformationVolume	C:	SUCCESS	VolumeCreationTime: 3/20/2017 9:34:16 PM, VolumeSerialNumber: D8BA-8021, SupportsObje
Malware_U3_W2_L2.exe	3372	FileSystemControl	C:	SUCCESS	Control: FSCTL_FILE_PREFETCH
Malware_U3_W2_L2.exe	3372	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\	SUCCESS	0: 65e5bdf5ca391440390554e9ae7b, 1: AUTOEXEC.BAT, FileInformationClass: FileNamesInfo
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\	NO MORE FILES	
Malware_U3_W2_L2.exe	3372	CloseFile	C:\	SUCCESS	
Malware_U3_W2_L2.exe	3372	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: All Users, 4: Default User, 5: LocalServ
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
Malware_U3_W2_L2.exe	3372	CloseFile	C:\Documents and Settings	SUCCESS	
Malware_U3_W2_L2.exe	3372	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: Cookies, 4: Desktop, 5: Favorites, 6: Lo
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
Malware_U3_W2_L2.exe	3372	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
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,
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
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
Malware_U3_W2_L2.exe	3372	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
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,
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	NO MORE FILES	
Malware_U3_W2_L2.exe	3372	CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2	SUCCESS	
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: asser
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS	NO MORE FILES	
Malware_U3_W2_L2.exe	3372	CloseFile	C:\WINDOWS	SUCCESS	
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\AppPatch	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: AcGenral.dll, 4: AcLayers.dll, 5: AcLua
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\AppPatch	NO MORE FILES	
Malware_U3_W2_L2.exe	3372	CloseFile	C:\WINDOWS\AppPatch	SUCCESS	
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: ., 1: .., FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1029, 6: 1031, 7: 1033,
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: eapsvc.dll, 1: edit.com, FileInformationClass: FileNamesInformation, 3: edlin.exe, 4: elsadu.dll
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: more.com, 1: moricons.dll, FileInformationClass: FileNamesInformation, 3: mouse.drv, 4: mp43
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: progman.exe, 1: PRONICfg.dll, FileInformationClass: FileNamesInformation, 3: PROUninst.exe
Malware_U3_W2_L2.exe	3372	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: vga.dll, 1: vmGuestLib.dll, FileInformationClass: FileNamesInformation, 3: vmhgfs.dll, 4: VMUp

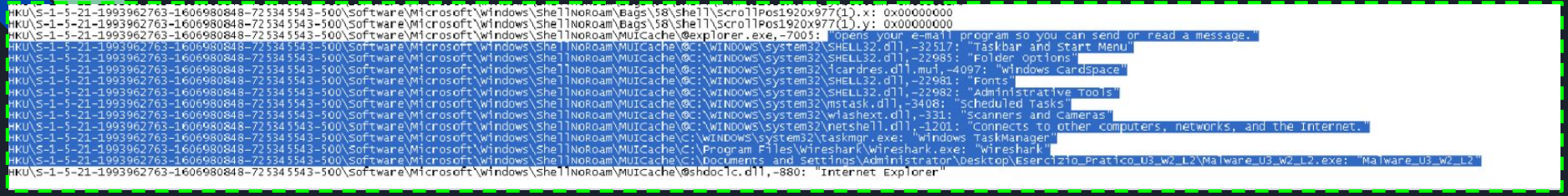
Per arricchire l'analisi delle azioni intraprese dal malware, è interessante notare che, tra le sue attività, si osserva la creazione di file, soprattutto all'interno della directory di sistema.
Questo comportamento solleva ulteriori interrogativi sulla natura e gli obiettivi del malware, poiché la manipolazione dei file di sistema potrebbe indicare un tentativo di compromettere l'integrità del sistema operativo o di installare componenti dannosi in posizioni critiche.



Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\config	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes:
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes:
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:
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes:
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes:
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes:
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes:
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes:
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
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
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO
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
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
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory,
Malware_U3_W2_L2.exe	3372	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO

Per ampliare la nostra comprensione delle tattiche impiegate dal malware, è rilevante evidenziare che, attraverso l'analisi con Process Explorer, è emerso che i processi utilizzati dal codice dannoso si camuffano sotto i nomi "explorer.exe" e "svchost.exe". Questa strategia è finalizzata a mimetizzarsi all'interno di processi legittimi del sistema operativo, rendendo così più arduo rilevare la sua esecuzione in background. Questa mascheratura rappresenta una sfida aggiuntiva per gli investigatori della sicurezza informatica, poiché richiede un'analisi più approfondita per individuare e contrastare l'attività del malware senza compromettere il funzionamento normale del sistema. Incorporando questa osservazione nella nostra analisi, possiamo concentrarci su metodi più sofisticati per rilevare e neutralizzare questa minaccia.

IEXPLORE.EXE		1,888 K	4,552 K	1588 Internet Explorer	Microsoft Corporation
IPROSetMonitor.exe		472 K	1,980 K	1692 Intel® PROSet Monitoring S...	Intel Corporation
explorer.exe		11,196 K	18,040 K	1700 Windows Explorer	Microsoft Corporation
wmiprvse.exe		1,748 K	4,708 K	1732 WMI	Microsoft Corporation
alg.exe		1,108 K	3,424 K	1736 Application Layer Gateway S...	Microsoft Corporation
Wireshark.exe	1.56	95,536 K	16,160 K	1824	
VGAuthService.exe		6,256 K	8,992 K	1836 VMware Guest Authenticatio...	VMware, Inc.
VBoxTray.exe		1,964 K	3,540 K	1848 VirtualBox Guest Additions Tr...	Oracle Corporation
Procmon.exe		13,632 K	3,360 K	1976 Process Monitor	Sysinternals - www.sysinter...
svchost.exe		864 K	2,264 K	3148 Generic Host Process for Wi...	Microsoft Corporation
dumpcap.exe		1,928 K	4,644 K	3624 Dumpcap	The Wireshark developer ...
procexp.exe		11,732 K	7,504 K	3824 Sysinternals Process Explorer	Sysinternals - www.sysinter...
wuauclt.exe		5,556 K	5,060 K	3948 Automatic Updates	Microsoft Corporation



Per arricchire ulteriormente la nostra indagine, dopo l'analisi dinamica con Process Monitor, abbiamo eseguito un controllo aggiuntivo tramite Regshot.
Questo ci ha permesso di catturare e confrontare lo stato del Registro di sistema prima e dopo l'esecuzione del malware.
Attraverso questa procedura, possiamo identificare eventuali modifiche o aggiunte sospette al Registro di sistema, fornendo così un'ulteriore traccia per comprendere l'impatto e le intenzioni del malware. Integrando questo passaggio nel nostro processo di analisi, siamo in grado di ottenere una panoramica più completa delle azioni del malware e delle sue possibili implicazioni per la sicurezza del sistema.