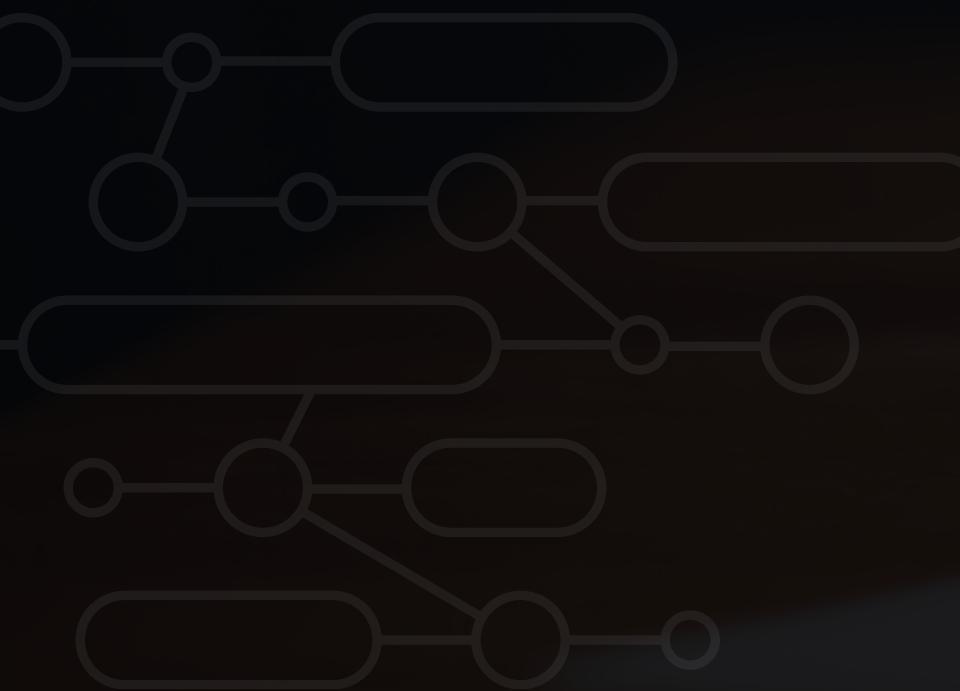


MALWARE ANALYSIS



IDENTIFICARE EVENTUALI AZIONI DEL MALWARE SUL FILE SYSTEM UTILIZZANDO PROCESS MONITOR

Process Monitor è uno strumento avanzato per monitorare l'attività del sistema, inclusi i cambiamenti nel file system e il comportamento dei processi.

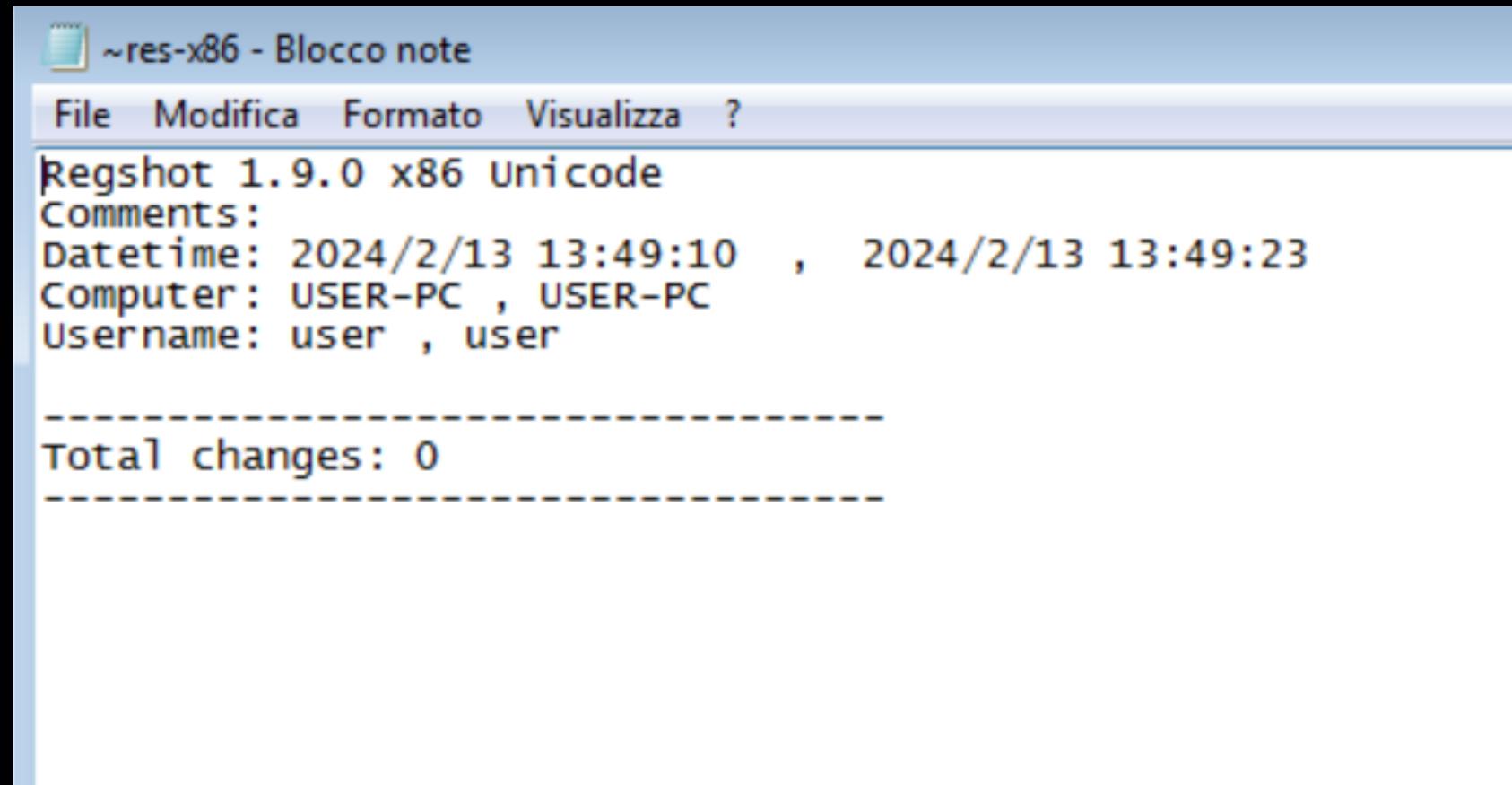
In questa circostanza, abbiamo eseguito un virus all'interno di una macchina virtuale e abbiamo impedito al virus di uscire da quest'ultima. Dopo l'avvio, abbiamo utilizzato Process Monitor per verificare l'attività del virus e lo abbiamo identificato con successo.

Time	Process	Action	Target Path	Result
14:04:42,3229134	svchost.exe	2024	C:\Windows\System32\xmllite.dll	BUFFER OVERFLOW... Creation time: 14/07/...
14:04:42,3229247	svchost.exe	2524	C:\Windows\System32\xmllite.dll	SUCCESS
14:04:42,3240845	Malware_U3_W2_L2.exe	1700	C:\Windows\Prefetch\MALWARE_U3_W2_L2.EXE-06F81ECB.pf	NAME NOT FOUND Desired Access: Gene...
14:04:42,3241616	Malware_U3_W2_L2.exe	1700	C:\Windows\System32\apisetschema.dll	SUCCESS Name: \Windows\Sys...
14:04:42,3241825	Malware_U3_W2_L2.exe	1700	C:\Users\user\Desktop\Malware_U3_W2_L2.exe	SUCCESS Name: \Users\user\De...
14:04:42,3241973	Malware_U3_W2_L2.exe	1700	C:\Windows\System32\ntdll.dll	SUCCESS Name: \Windows\Sys...
14:04:42,3242099	Malware_U3_W2_L2.exe	1700	C:\Windows\SysWOW64\ntdll.dll	SUCCESS Name: \Windows\Sys...
14:04:42,3243442	taskeng.exe	2028	C:\Windows\System32\mpr.dll	SUCCESS Offset: 75.776, Length...
14:04:42,3250366	taskeng.exe	2028	C:\	SUCCESS Desired Access: Sync...

IDENTIFICARE EVENTUALI AZIONI DEL MALWARE SU PROCESSI E THREAD UTILIZZANDO PROCESS MONITOR

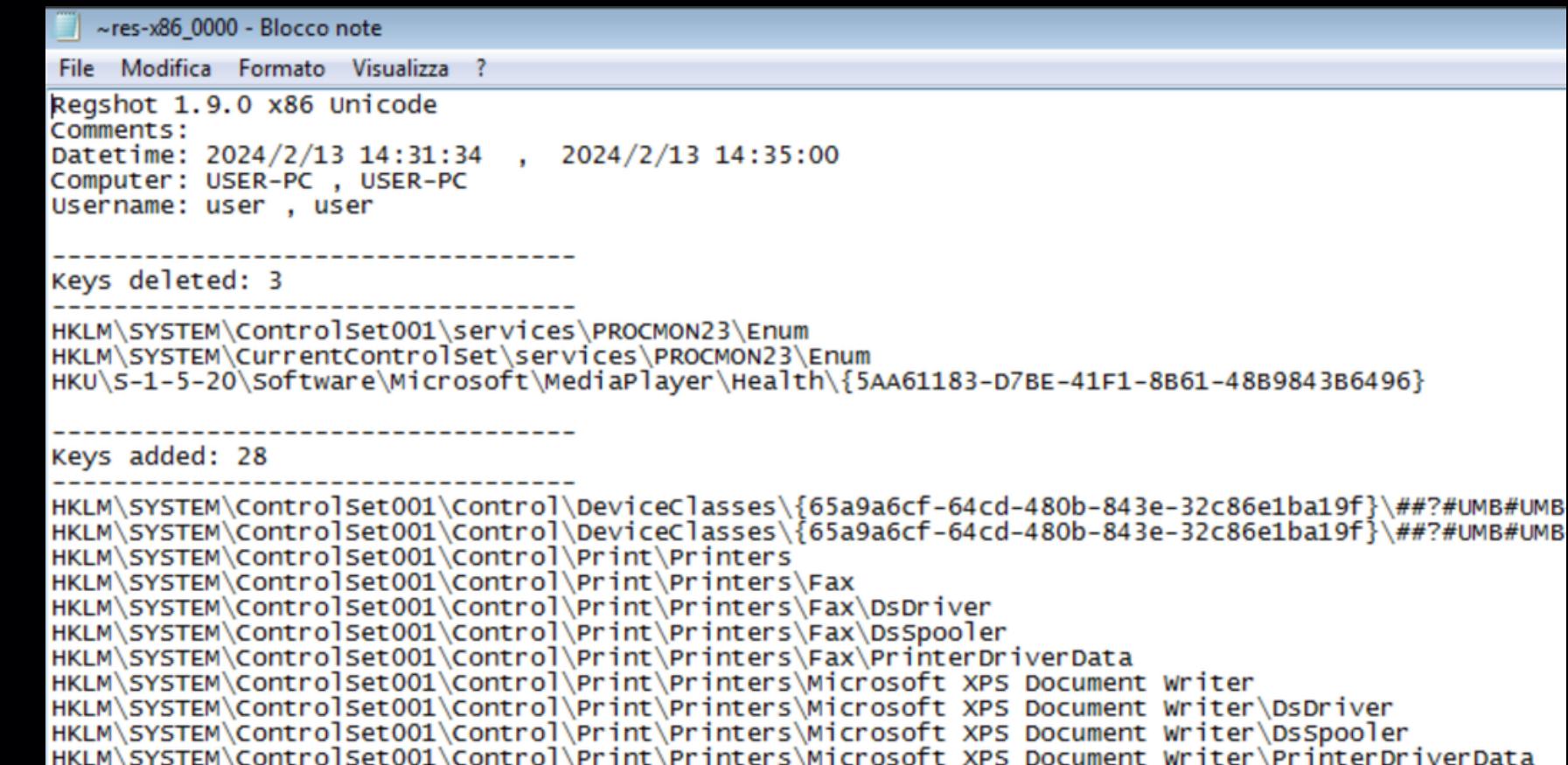
Time of Day	Process Name	PID	Operation	Path	Result	Detail
14:04:42.3217692	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\sspicli.dll		SUCCESS	Name: \Windows\System32\sspicli.dll
14:04:42.3217834	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\cryptbase.dll		SUCCESS	Name: \Windows\System32\cryptbase.dll
14:04:42.3217968	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\KernelBase.dll		SUCCESS	Name: \Windows\System32\KernelBase.dll
14:04:42.3218097	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\clbcatq.dll		SUCCESS	Name: \Windows\System32\clbcatq.dll
14:04:42.3218229	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\lpk.dll		SUCCESS	Name: \Windows\System32\lpk.dll
14:04:42.3218369	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\imm32.dll		SUCCESS	Name: \Windows\System32\imm32.dll
14:04:42.3218501	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\pcrt4.dll		SUCCESS	Name: \Windows\System32\pcrt4.dll
14:04:42.3218630	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\sechost.dll		SUCCESS	Name: \Windows\System32\sechost.dll
14:04:42.3218838	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\svavt.dll		SUCCESS	Name: \Windows\System32\svavt.dll
14:04:42.3218970	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\gd32.dll		SUCCESS	Name: \Windows\System32\gd32.dll
14:04:42.3219097	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\user32.dll		SUCCESS	Name: \Windows\System32\user32.dll
14:04:42.3219227	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\imagehelp.dll		SUCCESS	Name: \Windows\System32\imagehelp.dll
14:04:42.3219366	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\ole32.dll		SUCCESS	Name: \Windows\System32\ole32.dll
14:04:42.3219498	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\msctf.dll		SUCCESS	Name: \Windows\System32\msctf.dll
14:04:42.3219627	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\oleaut32.dll		SUCCESS	Name: \Windows\System32\oleaut32.dll
14:04:42.3219755	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\advapi32.dll		SUCCESS	Name: \Windows\System32\advapi32.dll
14:04:42.3219890	rundll32.exe	2868	QueryNameInfo...C:\Windows\System32\apisetschema.dll		SUCCESS	Name: \Windows\System32\apisetschema.dll
14:04:42.3220401	rundll32.exe	2868	CloseFile C:\Windows\System32		SUCCESS	Name: \Windows\System32
14:04:42.3222840	svchost.exe	2524	CreateFile C:\Windows\System32\svmlite.dll		SUCCESS	Desired Access: Generic Create, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, ShareMode: None, CreateDisposition: 3, CreateOptions: 0x10000, FileAttributes: 0x00000000, Image Base: 0x7ef40000, Image Size: 0x39000
14:04:42.3222840	svchost.exe	2524	QueryInformation C:\Windows\System32\svmlite.dll		SUCCESS	CreationTime: 1/21/2024 11:13:30, VolumeSerialNumber: 88D2-1ECE, SupportsObjects: True, Version: 1.0, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3228765	svchost.exe	2524	QueryInformation C:\Windows\System32\svmlite.dll		BUFFER OVERFL...	CreationTime: 14/07/2009 01:41:27, LastAccessTime: 14/07/2009 01:41:27, LastWriteTime: 14/07/2009 01:41:27, Image Base: 0x7ef40000, Image Size: 0x180000
14:04:42.3228938	svchost.exe	2524	FileSystemControl C:\Windows\System32\svmlite.dll		SUCCESS	Control: FSCTL_READFILE, FILE_USN_DATA, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3229062	svchost.exe	2524	QueryInformation C:\Windows\System32\svmlite.dll		SUCCESS	VolumeCreationTime: 17/01/2024 11:13:30, VolumeSerialNumber: 88D2-1ECE, SupportsObjects: True, Version: 1.0, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3229134	svchost.exe	2524	QueryInformation C:\Windows\System32\svmlite.dll		BUFFER OVERFL...	CreationTime: 14/07/2009 01:41:27, LastAccessTime: 14/07/2009 01:41:27, LastWriteTime: 14/07/2009 01:41:27, Image Base: 0x7ef40000, Image Size: 0x180000
14:04:42.3229247	svchost.exe	2524	CloseFile C:\Windows\System32\svmlite.dll		SUCCESS	Offset: 75,776, Length: 3.072, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3241616	Malware_U3_W2_L2.exe	1700	CreateFile C:\Windows\System32\apisetschema.dll		NONE	NAME NOT FOUND Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, CreateDisposition: 3, CreateOptions: 0x10000, Image Base: 0x7ef40000, Image Size: 0x39000
14:04:42.3241973	Malware_U3_W2_L2.exe	1700	QueryNameInfo...C:\Windows\System32\apisetschema.dll		SUCCESS	Name: \Windows\System32\apisetschema.dll
14:04:42.3241973	Malware_U3_W2_L2.exe	1700	QueryNameInfo...C:\Users\user\Desktop\Malware_U3_W2_L2.exe		SUCCESS	Name: \Users\user\Desktop\Malware_U3_W2_L2.exe
14:04:42.3241973	Malware_U3_W2_L2.exe	1700	QueryNameInfo...C:\Windows\System32\vtndl.dll		SUCCESS	Name: \Windows\System32\vtndl.dll
14:04:42.3242099	Malware_U3_W2_L2.exe	1700	QueryNameInfo...C:\Windows\SysWOW64\vtndl.dll		SUCCESS	Name: \Windows\SysWOW64\vtndl.dll
14:04:42.3243442	taskeng.exe	2028	ReadFile C:\Windows\System32\vrpr.dll		SUCCESS	Offset: 257, Length: 3.072, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3250366	taskeng.exe	2028	CreateFile C:\Windows\System32\vrpr.dll		SUCCESS	Desired Access: Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, CreateDisposition: 3, CreateOptions: 0x10000, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3250504	taskeng.exe	2028	QueryNameInfo...C:\Windows\System32\vrpr.dll		SUCCESS	Name: \Windows\System32\vrpr.dll
14:04:42.3250722	taskeng.exe	2028	QueryAttribut... C:\Windows\System32\vrpr.dll		SUCCESS	FileSystemAttributes: Case Preserved, Case Sensitive, Unicode, ACLs, Compression, Named Streams, EFS, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3250809	taskeng.exe	2028	CloseFile C:\Windows\System32\vrpr.dll		SUCCESS	Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3251061	taskeng.exe	2028	CreateFile C:\Windows\System32\vrpr.dll		SUCCESS	Desired Access: Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, CreateDisposition: 3, CreateOptions: 0x10000, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3251173	taskeng.exe	2028	QueryNameInfo...C:\Windows\System32\vrpr.dll		SUCCESS	Name: \Windows\System32\vrpr.dll
14:04:42.3251248	taskeng.exe	2028	QueryAttribut... C:\Windows\System32\vrpr.dll		SUCCESS	FileSystemAttributes: Case Preserved, Case Sensitive, Unicode, ACLs, Compression, Named Streams, EFS, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3251314	taskeng.exe	2028	CloseFile C:\Windows\System32\vrpr.dll		SUCCESS	Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3251491	taskeng.exe	2028	CreateFile C:\Windows\System32\vrpr.dll		SUCCESS	Desired Access: Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, CreateDisposition: 3, CreateOptions: 0x10000, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3251585	taskeng.exe	2028	QueryNameInfo...C:\Windows\System32\vrpr.dll		SUCCESS	Name: \Windows\System32\vrpr.dll
14:04:42.3251655	taskeng.exe	2028	QueryAttribut... C:\Windows\System32\vrpr.dll		SUCCESS	FileSystemAttributes: Case Preserved, Case Sensitive, Unicode, ACLs, Compression, Named Streams, EFS, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3251716	taskeng.exe	2028	CloseFile C:\Windows\System32\vrpr.dll		SUCCESS	Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3253499	svchost.exe	852	ReadFile C:\Windows\System32\appinfo.dll		SUCCESS	Offset: 2, Length: 2.048, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3257700	svchost.exe	852	CreateFile C:\Users\user\Desktop\Malware_U3_W2_L2.exe		SUCCESS	Desired Access: Generic Read/Execute, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, ShareMode: None, CreateDisposition: 3, CreateOptions: 0x10000, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3258355	svchost.exe	852	CreateFile C:\Users\user\Desktop\Malware_U3_W2_L2.exe		SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, ShareMode: None, CreateDisposition: 3, CreateOptions: 0x10000, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3258588	svchost.exe	852	QuerySecurityFile C:\Users\user\Desktop\Malware_U3_W2_L2.exe		SUCCESS	Information: Owner, Group, DACL, SACL, Label
14:04:42.3258715	svchost.exe	852	QueryBasicInfor...C:\Users\user\Desktop\Malware_U3_W2_L2.exe		SUCCESS	CreationTime: 08/04/2011 12:55:00, LastAccessTime: 08/04/2011 12:55:00, LastWriteTime: 17/01/2024 11:13:30, Image Base: 0x7ef40000, Image Size: 0x1a9000
14:04:42.3268517	svchost.exe	852	CreateFileMapping...C:\Users\user\Desktop\Malware_U3_W2_L2.exe		FILE LOCKED WI...	SyntType: SyncTypeCreateSection, PageProtection: 0x00000000, Image Base: 0x7ef40000, Image Size: 0x1a9000

Time of Day	Process Name	PID	Operation	Path	Result	Detail
14:04:42.2378058	rundll32.exe	2868	Load Image	C:\Windows\System32\clbcatq.dll	SUCCESS	Image Base: 0x7ef40000, Image Size: 0x39000
14:04:42.2378803	rundll32.exe	2868	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7ef080000, Image Size: 0xd0000
14:04:42.2468780	rundll32.exe	2868	Load Image	C:\Windows\System32\sechost.dll	SUCCESS	Image Base: 0x7ef710000, Image Size: 0xf0000
14:04:42.2483526	rundll32.exe	2868	Load Image	C:\Windows\System32\taskschd.dll	SUCCESS	Image Base: 0x7efac50000, Image Size: 0x127000
14:04:42.2494278	rundll32.exe	2868	Load Image	C:\Windows\System32\sspicl.dll	SUCCESS	Image Base: 0x7efcc00000, Image Size: 0x25000
14:04:42.2821024	rundll32.exe	2868	Load Image	C:\Windows\System32\vmmlite.dll	SUCCESS	Image Base: 0x7efb0e0000, Image Size: 0x35000
14:04:42.3134505	rundll32.exe	2868	Thread Create		SUCCESS	Thread ID: 2568
14:04:42.3139465	taskeng.exe	2028	Thread Create		SUCCESS	Thread ID: 2196
14:04:42.3146770	rundll32.exe	2868	Thread Exit		SUCCESS	Thread ID: 2988, User Time: 0.000000 seconds, Kernel Time: 0.0156 seconds
14:04:42.3147502	rundll32.exe	2868	Thread Exit		SUCCESS	Thread ID: 2568, User Time: 0.000000 seconds, Kernel Time: 0.000000 seconds
14:04:42.3151604	taskeng.exe	2028	Process Create	C:\Users\user\Desktop\Malware_U3_W2_L2.exe	SUCCESS	PID: 1700, Command line: C:\Users\user\Desktop\Malware_U3_W2_L2.exe
14:04:42.3151654	Malware_U3_W2_L2.exe	1700	Process Start		SUCCESS	Parent PID: 2028, Command line: C:\Users\user\Desktop\Malware_U3_W2_L2.exe
14:04:42.3151692	Malware_U3_W2_L2.exe	1700	Thread Create		SUCCESS	Thread ID: 2944
14:04:42.3220182	rundll32.exe	2868	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.000000 seconds, Kernel Time: 0.000000 seconds
14:04:42.3238391	Malware_U3_W2_L2.exe	1700	Load Image	C:\Users\user\Desktop\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000,



Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2024/2/13 13:49:10 , 2024/2/13 13:49:23
Computer: USER-PC , USER-PC
Username: user , user

Total changes: 0



Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2024/2/13 14:31:34 , 2024/2/13 14:35:00
Computer: USER-PC , USER-PC
Username: user , user

Keys deleted: 3

HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum
HKU\S-1-5-20\software\Microsoft\MediaPlayer\Health\{5AA61183-D7BE-41F1-8B61-48B9843B6496}

Keys added: 28

HKLM\SYSTEM\ControlSet001\control\DeviceClasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB
HKLM\SYSTEM\ControlSet001\control\DeviceClasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB
HKLM\SYSTEM\ControlSet001\control\Print\Printers
HKLM\SYSTEM\ControlSet001\control\Print\Printers\Fax
HKLM\SYSTEM\ControlSet001\control\Print\Printers\Fax\DsDriver
HKLM\SYSTEM\ControlSet001\control\Print\Printers\Fax\DsSpooler
HKLM\SYSTEM\ControlSet001\control\Print\Printers\Fax\PrinterDriverData
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

MODIFICHE DEL REGISTRO DOPO IL MALWARE

Per determinare eventuali modifiche apportate dal virus, abbiamo impiegato RegShot, un'applicazione che ci ha richiesto di eseguire un "PrimoShot" del sistema in uno stato privo del virus, seguito da un "SecondoShot" con il virus attivo. Durante questa procedura, abbiamo identificato variazioni nel registro di sistema. Il malware ha influenzato chiavi e valori di rilevanza fondamentale, minando la stabilità e la sicurezza del sistema.

PROVARE A PROFILARE IL MALWARE IN BASE ALLA CORRELAZIONE TRA «OPERATION» E PATH.

Image						
Name:	Malware_U3_W2_L2.exe	Architecture:	32-bit	Company:	Microsoft Corporation	Version:
Version:		Virtualized:	False	File Version:	6.1.7600.16384	Timestamp:
Path:	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	Processor:	x64	File Hash (SHA-1):	314E8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A	Last Write Time:
Command Line:	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	Start Type:	0x00000000	File Hash (MD5):	314E8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A	File Size:
PID:	2132	Architecture:	32-bit	File Hash (SHA-256):	314E8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A	File Extension:
Parent PID:	2540	Virtualized:	False	File Hash (CRC32):	314E8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A	File Type:
Session ID:	1	Integrity:	Etichetta obbligatoria\Livello obbligatorio alto	File Hash (SSDeep):	314E8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A	File Path:
User:	user-PC\user	Processor:	x64	File Hash (DST):	314E8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A	File Name:
Auth ID:	00000000:0000eb7e	Start Type:	0x00000000	File Hash (SSDeep):	314E8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A	File Extension:
Started:	13/02/2024 15:15:54	Ended:	13/02/2024 15:15:56	File Hash (DST):	314E8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A8A	File Path:
Modules:						
Module	Address	Size	Path	Company	Version	Timestamp
Malware_U3_W... 0x30000	0xd000	C:\Users\user\Desktop\MALWARE\E...			08/04/2011 18:...	
svchost.exe 0x320000	0x8000	C:\Windows\SysWOW64\svchost.exe	Microsoft Corpor...	6.1.7600.1638...	14/07/2009 00:...	
Malware_U3_W... 0x400000	0xd000	C:\Users\user\Desktop\MALWARE\E...			08/04/2011 18:...	
AcXtrnal.dll 0x71ce0000	0x259000	C:\Windows\AppPatch\AcXtrnal.dll	Microsoft Corpor...	6.1.7600.1638...	14/07/2009 02:...	
AcGenral.dll 0x71f40000	0x218000	C:\Windows\AppPatch\AcGenral.dll	Microsoft Corpor...	6.1.7601.1751...	20/11/2010 12:...	

Sechost.dll

Sechost.dll è una libreria di collegamento dinamico (DLL) di sistema in ambienti Windows. Questa DLL è associata ai servizi di hosting della sicurezza del sistema operativo. La sua presenza è fondamentale per il corretto funzionamento del sistema e per garantire la sicurezza delle operazioni.

kernel32.dll

La kernel32.dll è una delle librerie di collegamento dinamico (DLL) essenziali nei sistemi operativi Windows. Questa DLL svolge un ruolo cruciale nel kernel del sistema operativo e offre una vasta gamma di funzioni di base per le applicazioni e il sistema stesso.