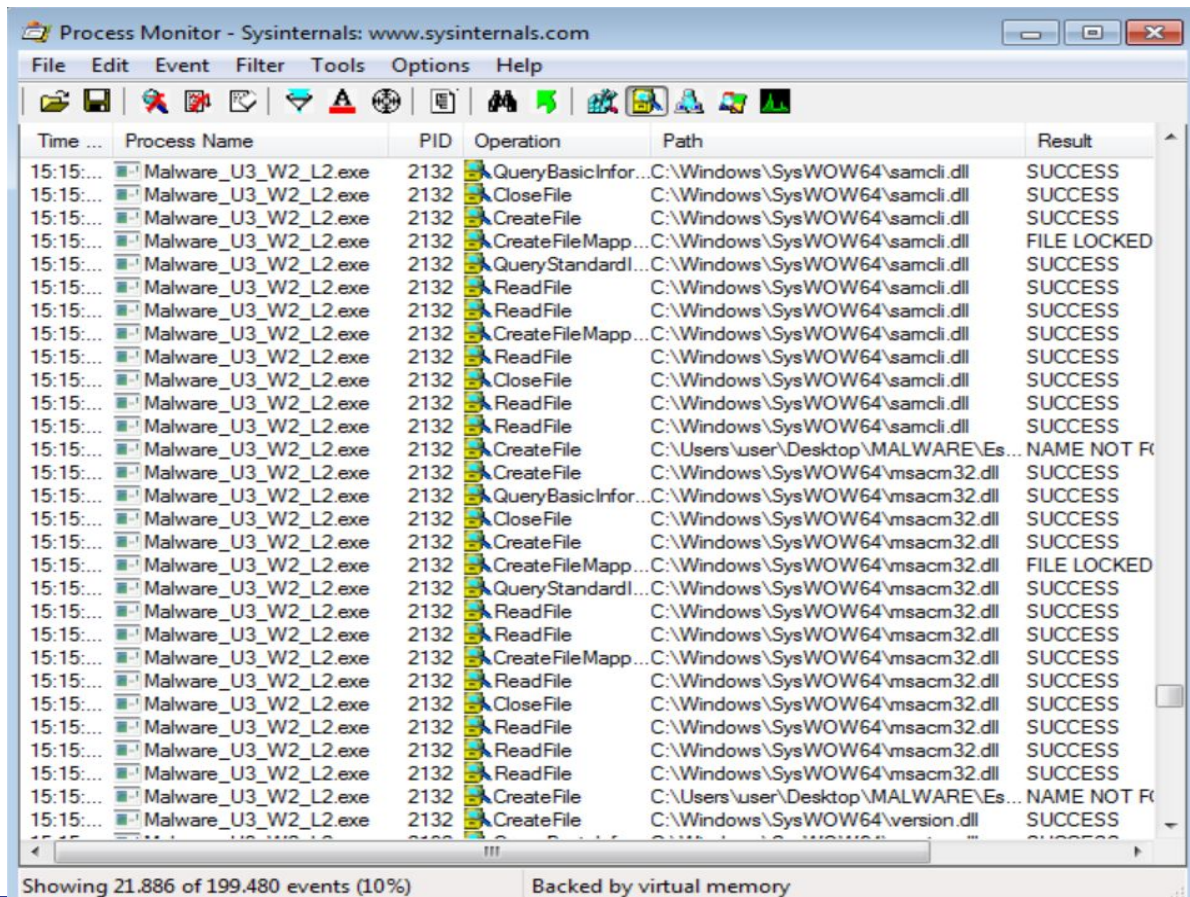


# Unità 3/ Settimana 2/ Compito 2

# Identificazione di malware nel file system

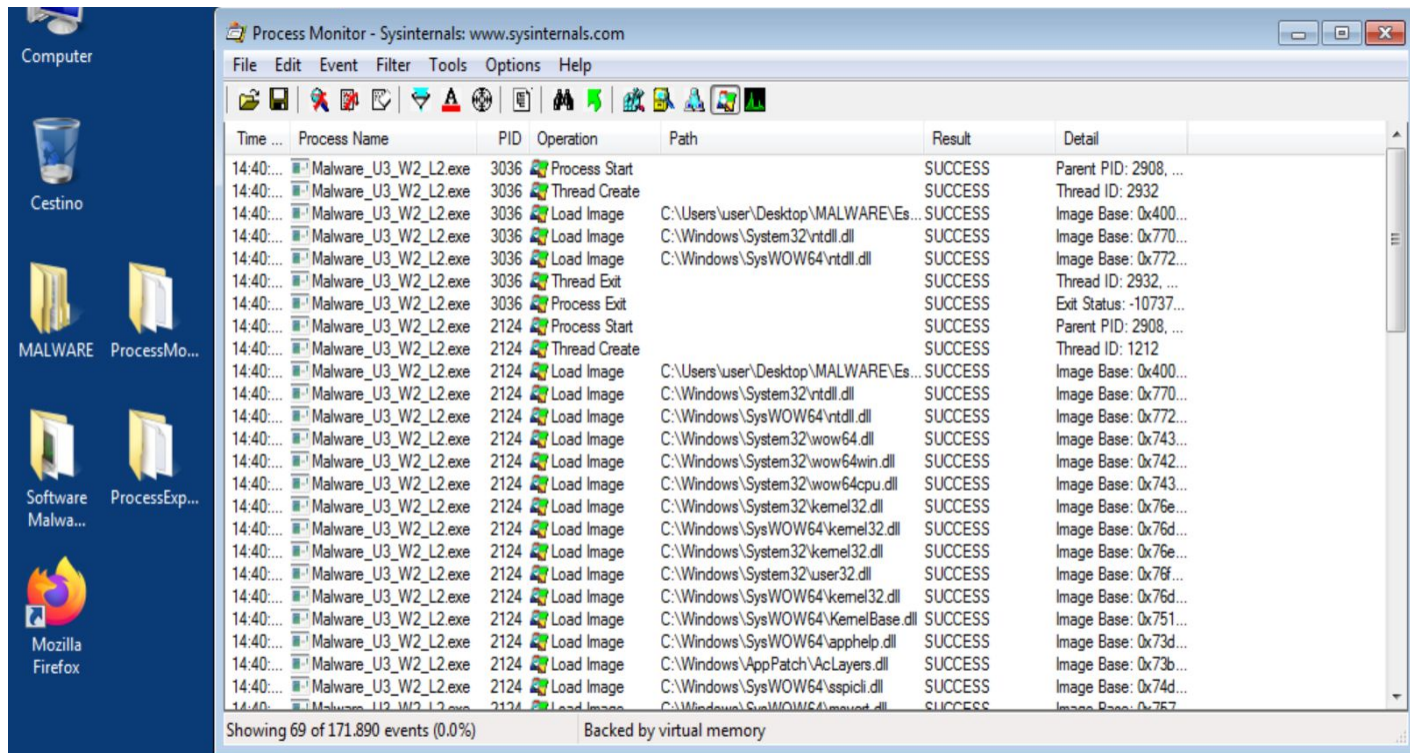


The screenshot displays the Process Monitor application window, titled "Process Monitor - Sysinternals: www.sysinternals.com". The interface includes a menu bar (File, Edit, Event, Filter, Tools, Options, Help) and a toolbar with various icons. The main area is a table of system events. The table has columns for Time, Process Name, PID, Operation, Path, and Result. The data shows a process named "Malware\_U3\_W2\_L2.exe" with PID 2132 performing a series of file operations. The operations include querying basic information, closing files, creating files, creating file mappings, querying standard information, reading files, and creating file mappings. The paths involved are primarily system files in the Windows directory (e.g., C:\Windows\SysWOW64\samcli.dll, C:\Windows\SysWOW64\msacm32.dll) and a file on the desktop (C:\Users\user\Desktop\MALWARE\E...). The results of these operations are mostly "SUCCESS", with some "FILE LOCKED" and "NAME NOT FOUND" errors. The status bar at the bottom indicates "Showing 21.886 of 199.480 events (10%)" and "Backed by virtual memory".

Time ...	Process Name	PID	Operation	Path	Result
15:15:...	Malware_U3_W2_L2.exe	2132	QueryBasicInfor...	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CloseFile	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CreateFile	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CreateFileMapp...	C:\Windows\SysWOW64\samcli.dll	FILE LOCKED
15:15:...	Malware_U3_W2_L2.exe	2132	QueryStandardI...	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CreateFileMapp...	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CloseFile	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\samcli.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CreateFile	C:\Users\user\Desktop\MALWARE\E...	NAME NOT F...
15:15:...	Malware_U3_W2_L2.exe	2132	CreateFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	QueryBasicInfor...	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CloseFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CreateFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CreateFileMapp...	C:\Windows\SysWOW64\msacm32.dll	FILE LOCKED
15:15:...	Malware_U3_W2_L2.exe	2132	QueryStandardI...	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CreateFileMapp...	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CloseFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	ReadFile	C:\Windows\SysWOW64\msacm32.dll	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	CreateFile	C:\Users\user\Desktop\MALWARE\E...	NAME NOT F...
15:15:...	Malware_U3_W2_L2.exe	2132	CreateFile	C:\Windows\SysWOW64\version.dll	SUCCESS

Showing 21.886 of 199.480 events (10%)      Backed by virtual memory

# Identificazioni di malware su processi e thread



The screenshot displays the Process Monitor application window, titled "Process Monitor - Sysinternals: www.sysinternals.com". The interface includes a menu bar (File, Edit, Event, Filter, Tools, Options, Help) and a toolbar with various icons. The main area is a table of events, with columns for Time, Process Name, PID, Operation, Path, Result, and Detail. The events listed are all for the process "Malware\_U3\_W2\_L2.exe" and occur at 14:40:...

Time	Process Name	PID	Operation	Path	Result	Detail
14:40:...	Malware_U3_W2_L2.exe	3036	Process Start		SUCCESS	Parent PID: 2908, ...
14:40:...	Malware_U3_W2_L2.exe	3036	Thread Create		SUCCESS	Thread ID: 2932
14:40:...	Malware_U3_W2_L2.exe	3036	Load Image	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Image Base: 0x400...
14:40:...	Malware_U3_W2_L2.exe	3036	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x770...
14:40:...	Malware_U3_W2_L2.exe	3036	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x772...
14:40:...	Malware_U3_W2_L2.exe	3036	Thread Exit		SUCCESS	Thread ID: 2932, ...
14:40:...	Malware_U3_W2_L2.exe	3036	Process Exit		SUCCESS	Exit Status: -10737...
14:40:...	Malware_U3_W2_L2.exe	2124	Process Start		SUCCESS	Parent PID: 2908, ...
14:40:...	Malware_U3_W2_L2.exe	2124	Thread Create		SUCCESS	Thread ID: 1212
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	Image Base: 0x400...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x770...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x772...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x743...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x742...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x743...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76e...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76d...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x76e...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x76f...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x76d...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x751...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x73d...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\AppPatch\AcLayers.dll	SUCCESS	Image Base: 0x73b...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Image Base: 0x74d...
14:40:...	Malware_U3_W2_L2.exe	2124	Load Image	C:\Windows\SysWOW64\moviest...	SUCCESS	Image Base: 0x767...


Showing 69 of 171.890 events (0.0%) Backed by virtual memory



# Le differenze del registro dopo il malware

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help



Time ...	Process Name	PID	Operation	Path	Result
15:15:...	csrss.exe	320	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS
15:15:...	csrss.exe	320	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS
15:15:...	csrss.exe	320	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT F
15:15:...	Malware_U3_W2_L2.exe	2132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE
15:15:...	Malware_U3_W2_L2.exe	2132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT F
15:15:...	Malware_U3_W2_L2.exe	2132	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT F
15:15:...	Malware_U3_W2_L2.exe	2132	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT F
15:15:...	Malware_U3_W2_L2.exe	2132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE
15:15:...	Malware_U3_W2_L2.exe	2132	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
15:15:...	Malware_U3_W2_L2.exe	2132	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT F
15:15:...	Malware_U3_W2_L2.exe	2132	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
15:15:...	csrss.exe	380	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT F
15:15:...	csrss.exe	380	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT F
15:15:...	conhost.exe	292	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS
15:15:...	conhost.exe	292	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT F
15:15:...	conhost.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE
15:15:...	conhost.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
15:15:...	conhost.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT F
15:15:...	conhost.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
15:15:...	conhost.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE
15:15:...	conhost.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT F
15:15:...	conhost.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE

# Path trovati

Avendo trovato diversi path elencherò e spiegherò solo i primi ovvero quelli in figura:

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 Corpo...	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 Corpo...	6.1.7600.1638...	14/07/2009 02:...	
AcGenral.dll	0x71f40000	0x218000	C:\Windows\AppPatch\AcGenral.dll	Microsoft Corpo...	6.1.7601.1751...	20/11/2010 12:...	

## **C:\Users\user\Desktop\MALWARE\Esercizio\_Pratico\_U3\_W2\_L2\Malware\_U3\_W2\_L2.exe**

- **"C:"** indica che il file si trova sull'unità C del disco rigido, che è una delle unità di archiviazione del computer.
- **"Users"** è il nome della cartella principale che contiene i profili degli utenti su Windows.
- **"user"** è il nome dell'account utente specifico che ha accesso al desktop.
- **"Desktop"** è una cartella all'interno del profilo dell'utente che contiene i file e le icone visualizzate sul desktop.
- **"MALWARE"** è una sottocartella all'interno della cartella Desktop.
- **"Esercizio\_Pratico\_U3\_W2\_L2"** è una sottocartella all'interno della cartella MALWARE.
- **"Malware\_U3\_W2\_L2.exe"** è il nome del file eseguibile. Potrebbe rappresentare un file di malware (come suggerito dal nome "Malware"), ma in un contesto diverso potrebbe essere semplicemente un file con un nome simile per altre ragioni. Tuttavia, è importante essere cauti quando si tratta di file con nomi che includono "malware", poiché potrebbero rappresentare una minaccia per la sicurezza del computer.

## C:\Windows\SysWOW64\svchost.exe

- "C:" indica che il file si trova sull'unità C del disco rigido, che è una delle unità di archiviazione del computer.
- "Windows" è la cartella principale del sistema operativo Windows, che contiene molti file e cartelle essenziali per il funzionamento del sistema.
- "SysWOW64" è una sottocartella all'interno della cartella "Windows". Questa cartella contiene file di sistema a 32 bit su sistemi operativi Windows a 64 bit. Il nome "SysWOW64" significa "System Windows on Windows 64-bit".
- "svchost.exe" è il nome del file eseguibile. Questo file è parte del sistema operativo Windows ed è utilizzato per ospitare servizi di sistema. Tuttavia, vale la pena notare che i malware possono a volte mascherarsi come "svchost.exe" per nascondersi e danneggiare il sistema. Pertanto, è importante verificare l'autenticità di questo file, specialmente se si sospetta di attività sospette sul computer.

# C:\Users\user\Desktop\MALWARE\Esercizio\_Pratico\_U3\_W2\_L2\Malware\_U3\_W2\_L2.exe

- "C:" indica che il file si trova sull'unità C del disco rigido, che è una delle unità di archiviazione del computer.

- "Users" è il nome della cartella principale che contiene i profili degli utenti su Windows.

- "user" è il nome dell'account utente specifico che ha accesso al desktop.

- "Desktop" è una cartella all'interno del profilo dell'utente che contiene i file e le icone visualizzate sul desktop.

- "MALWARE" è una sottocartella all'interno della cartella Desktop.


- "Esercizio\_Pratico\_U3\_W2\_L2" è una sottocartella all'interno della cartella MALWARE. - "Malware\_U3\_W2\_L2.exe" è il nome del file eseguibile. Potrebbe rappresentare un file di malware, ma in un contesto diverso potrebbe essere semplicemente un file con un nome simile per altre ragioni. Tuttavia, è importante essere cauti quando si tratta di file con nomi che includono "malware", poiché potrebbero rappresentare una minaccia per la sicurezza del computer. Se hai ulteriori domande o



## C:\Windows\AppPatch\AcXtrnal.dll

- "C:" indica che il file si trova sull'unità C del disco rigido, che è una delle unità di archiviazione del computer.
- "Windows" è la cartella principale del sistema operativo Windows, che contiene molti file e cartelle essenziali per il funzionamento del sistema.
- "AppPatch" è una sottocartella all'interno della cartella "Windows". Questa cartella contiene patch (aggiornamenti e correzioni) per le applicazioni installate nel sistema.
- "AcXtrnal.dll" è il nome del file DLL. Le DLL sono librerie di funzioni che vengono utilizzate da diversi programmi. In questo caso specifico, "AcXtrnal.dll" potrebbe essere associato a un'applicazione o a un componente del sistema operativo.

## **C:\Windows\AppPatch\AcGenral.dll**

- "C:" indica che il file si trova sull'unità C del disco rigido, che è una delle unità di archiviazione del computer.**
  - "Windows" è la cartella principale del sistema operativo Windows, contenente file essenziali per il funzionamento del sistema.**
  - "AppPatch" è una sottocartella all'interno della cartella "Windows". Contiene patch e correzioni per le applicazioni installate nel sistema.**
  - "AcGenral.dll" è il nome del file DLL (Dynamic Link Library). Le DLL sono librerie di funzioni utilizzate da vari programmi o componenti del sistema operativo.**
- 

# Shot fatto prima e dopo

Windows 7 - malware analysis (progetto del martedì) [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

~res-x86\_0000 - Blocco note

File Modifica Formato Visualizza ?

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#1&841921d&0&PrinterBusEnumerator#{65a9a6cf-64cd-480b-843e-

HKLM\SYSTEM\ControlSet001\Control\DeviceClasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1&841921d&0&PrinterBusEnumerator#{65a9a6cf-64cd-480b-843e-

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

HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY\_PROCMON23\0000\Control

HKLM\SYSTEM\ControlSet001\Enum\UMB\UMB#1&841921d&0&PrinterBusEnumerator\Control

HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1&841921d&0&PrinterBusEnumerator#{65a9a6cf-64cd-480b-8-

HKLM\SYSTEM\CurrentControlSet\Control\DeviceClasses\{65a9a6cf-64cd-480b-843e-32c86e1ba19f}\##?#UMB#UMB#1&841921d&0&PrinterBusEnumerator#{65a9a6cf-64cd-480b-8-

HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers

HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax

HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax\DsDriver

HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax\DsSpooler

HKLM\SYSTEM\CurrentControlSet\Control\Print\Printers\Fax\PrinterDriverData

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

111



IT 15:38

13/02/2024

CTRL (DESTRA)