

ANALISI DINAMICA BASICA

COME PRIMA COSA SIAMO ANDATI A MONITORARE I PROCESSI PRIMA DELL' AVVIO DEL MALWARE COME IN FOTO SOTTO

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	98.46	0 K	28 K	0		
System	< 0.01	0 K	236 K	4		
Interruptions		0 K	0 K		n/a Hardware Interrupts and DPCs	
smss.exe		168 K	388 K	444	444 Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1.428 K	3.444 K	492	492 Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6.396 K	4.100 K	516	516 Windows NT Logon Applicat...	Microsoft Corporation
services.exe		1.560 K	3.184 K	560	560 Services and Controller app	Microsoft Corporation
svchost.exe		2.936 K	4.680 K	744	744 Generic Host Process for Wi...	Microsoft Corporation
wmpirvse.exe		1.892 K	4.780 K	1716	1716 WMI	Microsoft Corporation
svchost.exe		1.684 K	4.104 K	832	832 Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13.604 K	22.584 K	908	908 Generic Host Process for Wi...	Microsoft Corporation
wscnify.exe		540 K	2.220 K	956	956 Windows Security Center No...	Microsoft Corporation
svchost.exe		1.060 K	2.848 K	1012	1012 Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1.748 K	4.668 K	1068	1068 Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		2.992 K	4.416 K	1188	1188 Spooler SubSystem App	Microsoft Corporation
alg.exe		1.124 K	3.488 K	888	888 Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3.640 K	1.268 K	572	572 LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	21.348 K	27.540 K	1776	Windows Explorer	Microsoft Corporation	
ctfmon.exe		836 K	3.144 K	1100	CTF Loader	Microsoft Corporation
procexp.exe	1.54	9.160 K	12.152 K	984	Sysinternals Process Explorer	Sysinternals - www.sysinter...

Process Monitor - Sysinternals: www.sysinternals.com

Time...	Process Name	PID	Operation	Path	Result	Detail
13.25...	Explorer.EXE	1776	QueryOpen	C:\Documents and Settings\Administrat...	SUCCESS	CreationTime: 05/1...
13.25...	Explorer.EXE	1776	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: E...
13.25...	Explorer.EXE	1776	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
13.25...	Explorer.EXE	1776	QueryStandardI...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 2.1...
13.25...	Explorer.EXE	1776	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
13.25...	Explorer.EXE	Windows Explorer	QueryOpen	C:\Documents and Settings\Administrat...	SUCCESS	
13.25...	Explorer.EXE	Microsoft Corporation	QueryOpen	C:\WINDOWS\Explorer.EXE	SUCCESS	
13.25...	Explorer.EXE	1776	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	CreationTime: 05/1...
13.25...	Explorer.EXE	1776	QueryStandardI...	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: E...
13.25...	Explorer.EXE	1776	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
13.25...	Explorer.EXE	1776	QueryStandardI...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 2.1...
13.25...	Explorer.EXE	1776	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
13.25...	Explorer.EXE	1776	CloseFile	C:\Documents and Settings\Administrat...	SUCCESS	
13.25...	csrss.exe	492	CreateFile	C:\WINDOWS\WinSxS\Policies\x86_P... NAME NOT FOUND	Desired Access: R...	
13.25...	csrss.exe	492	CreateFile	C:\WINDOWS\Assembly\GAC\Policy.6... PATH NOT FOUND	Desired Access: R...	
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\system32\en-US	SUCCESS	CreationTime: 31/0...
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\system32\en	SUCCESS	CreationTime: 31/0...
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\system32	SUCCESS	CreationTime: 31/0...
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\system32	SUCCESS	CreationTime: 31/0...
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\WinSxS\Manifests\x86... NAME NOT FOUND		
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\assembly\GAC\Microsoft... PATH NOT FOUND		
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\system32\en-US\Micro... NAME NOT FOUND		
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\system32\en-US\Micro... PATH NOT FOUND		
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\System32\en-US\Micro... PATH NOT FOUND		
13.25...	csrss.exe	492	CreateFile	C:\WINDOWS\WinSxS\Policies\x86_P... NAME NOT FOUND	Desired Access: R...	
13.25...	csrss.exe	492	CreateFile	C:\WINDOWS\Assembly\GAC\Policy.6... PATH NOT FOUND	Desired Access: R...	
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\WinSxS\Manifests\x86... NAME NOT FOUND		
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\assembly\GAC\Microsoft... PATH NOT FOUND		
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\system32\en\Microsoft... NAME NOT FOUND		
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\system32\en\Microsoft... PATH NOT FOUND		
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\System32\en\Microsoft... PATH NOT FOUND		
13.25...	csrss.exe	492	QueryOpen	C:\WINDOWS\System32\en\Microsoft... PATH NOT FOUND		
Showing 1.095 of 11.401 events (9.%.)	Backed by virtual memory					

Dopo abbiamo fatto usato il tool Regshot per paragonare due istantanee delle chiavi di registro.

Il primo shot è stato effettuato prima di avviare il malware mentre il secondo shot è stato effettuato dopo l'avvio del malware, dopo aver fatto tutto ciò andiamo a compare i due file il risultato viene mostrato nelle foto qui di seguito

-res-x86.txt - Notepad

```

File Edit Format View Help
Regshot 1.9.0 x86 Unicode
Commenti:
Dataora:2022/9/20 20:22:42 , 2022/9/20 20:31:09
Computer:LUCA-FC615DFE89 , LUCA-FC615DFE89
Username:Administrator , Administrator

-----
Chiave cancellata:2
-----
HKLM\SYSTEM\ControlSet001\services\PROCMON24\Enum
HKLM\SYSTEM\CurrentControlSet\services\PROCMON24\Enum

-----
Chiave aggiunta:2
-----
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON24\0000\Control
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON24\0000\Control

-----
Valore cancellato:6
-----
HKLM\SYSTEM\ControlSet001\services\PROCMON24\Enum\0: "Root\LEGACY_PROCMON24\0000"
HKLM\SYSTEM\ControlSet001\services\PROCMON24\Enum\Count: 0x00000001
HKLM\SYSTEM\ControlSet001\services\PROCMON24\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON24\Enum\0: "Root\LEGACY_PROCMON24\0000"
HKLM\SYSTEM\CurrentControlSet\services\PROCMON24\Enum\Count: 0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON24\Enum\NextInstance: 0x00000001

-----
Valore aggiunto:8
-----
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON24\0000\Control\ActiveService: "PROCMON24"
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON24\0000\Control\ActiveService: "PROCMON24"
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\Complg32\opensaveMRU\hivu\d: "C:\Documents and Settings\"
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@she1132.d11,-31237: "Creates a new, empty folder in the fc
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\documents and settings\Administrator\Desktop\Esercizio_F
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Sysinternals\Process Monitor\FilterDialog: 2C 00 00 00 00 00 01 00 00 00 FF FF FF FF
HKU\S-1-5-21-1644491937-484763869-299502267-500\Software\Sysinternals\Process Monitor\FilterControlColumns: 64 00 00 00 64 00 00 00 64 00 00 00 C

```

-res-x86.txt - Notepad

File Edit Format View Help

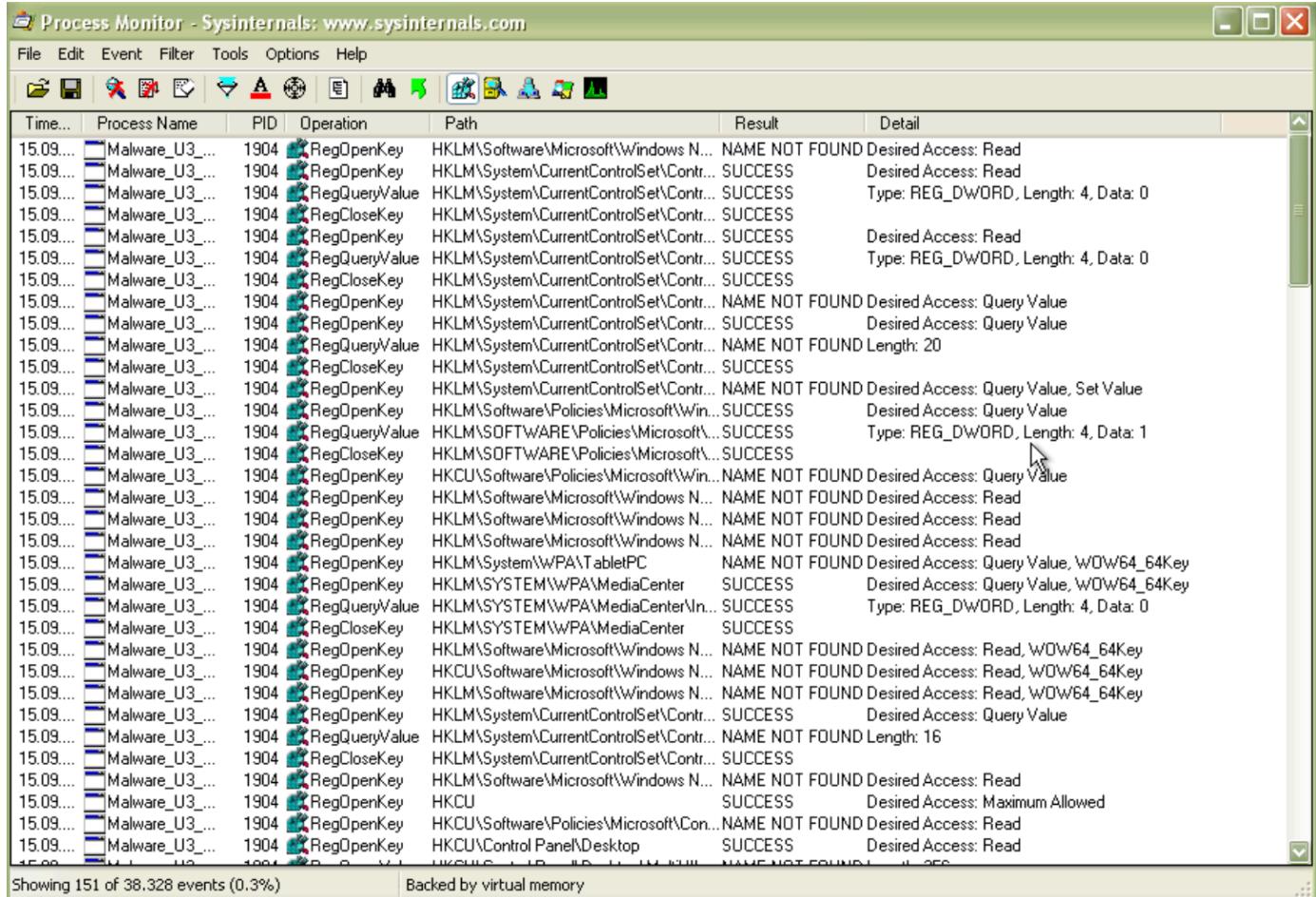
~res-x86.txt - Notepad

www.25-15-21-16111621

HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEAC9\}\Count
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEAC9\}\Count
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEAC9\}\Count
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEAC9\}\Count
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEAC9\}\Count
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEAC9\}\Count
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 46 00 00 00 3
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\Currentversion\Internet settings\Connections\SavedLegacySettings: 46 00 00 00 3
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\Currentversion\Shell Extensions\Cached\{255914F4-21D7-11D4-BDAF-00C4F60B9F0\} [{
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\Currentversion\Shell Extensions\Cached\{255914F4-21D7-11D4-BDAF-00C4F60B9F0\} [{
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\Currentversion\Shell Extensions\Cached\{255914F5-21D7-11D4-BDAF-00C4F60B9F0\} [{
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\She1\Bags\1\Desktop\ColInfo: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\She1\Bags\1\Desktop\ColInfo: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 F
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\She1\Bags\1\Desktop\ItemPos1280x720(1): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 OC
9 00 7A 00 69 00 6F 00 5F 00 50 00 72 00 61 00 74 00 69 00 63 00 6F 00 5F 00 55 00 33 00 5F 00 57 00 33 00 5F 00 4C 00 32 00 00 00 18 00 60 00 00 00 4E 00 00 00 64 00 31 00 00 00 00 C
50 00 72 00 61 00 74 00 69 00 63 00 6F 00 5F 00 55 00 33 00 5F 00 57 00 33 00 5F 00 4C 00 32 00 00 00 18 00 60 00 00 00 4E 00 00 00 64 00 31 00 00 00 00 C
55 0C 5D 34 55 4D 96 14 00 00 00 6D 00 64 00 35 00 64 00 65 00 67 00 70 00 2D 00 34 00 2E 00 33 00 00 00 1A 00 60 00 00 00 7E 01 00 00 3C 00 31 00 00 00 00 C
2_00 00 00 00 18 00 AB 00 00 00 02 00 00 00 4C 00 31 00 00 00 00 00 33 55 06 5D 10 00 50 52 4F 43 45 53 7E 32 00 00 00 34 00 03 04 00 04 EF BE 33 55 06 5D 34 55
73 00 00 00 18 00 AB 00 00 00 32 01 00 00 52 00 31 00 00 00 00 00 33 55 08 5D 10 00 53 59 53 49 4E 54 7E 31 00 00 00 3A 00 03 04 00 04 EF BE 33 55 07 5D 34 55
55 C4 8E 14 00 00 00 64 00 6F 00 77 00 6E 00 6C 00 6F 00 61 00 64 00 2E 00 65 00 78 00 65 00 00 00 1C 00 AB 00 00 00 16 02 00 00 54 00 32 00 92 02 00 00 34
4_55 C9 00 20 00 57 49 52 45 53 48 7E 31 2E 4C 4E 48 00 00 32 00 03 00 04 00 EF BE 34 55 C9 00 34 55 45 98 14 00 00 00 57 00 69 00 72 00 65 00 73 00 68 00
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\She1\Bags\1\Desktop\ItemPos1280x720(1): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 OC
9 00 7A 00 69 00 6F 00 5F 00 50 00 72 00 61 00 74 00 69 00 63 00 6F 00 5F 00 55 00 33 00 5F 00 57 00 32 00 5F 00 4C 00 31 00 00 00 18 00 15 00 00 00 CA 01
50 00 72 00 61 00 74 00 69 00 63 00 6F 00 5F 00 55 00 33 00 5F 00 57 00 33 00 5F 00 4C 00 32 00 00 00 18 00 60 00 00 00 4E 00 00 00 64 00 31 00 00 00 C
55 0C 5D 34 55 4D 96 14 00 00 00 6D 00 64 00 35 00 64 00 65 00 67 00 70 00 2D 00 34 00 2E 00 33 00 00 00 1A 00 15 00 00 00 4E 00 00 00 40 00 31 00 00 00 C
0E 00 31 00 00 00 00 00 33 55 06 5D 10 00 50 52 4F 43 45 53 7E 31 00 00 36 00 03 00 04 EF BE 33 55 05 5D 34 55 AT 95 14 00 00 00 50 00 72 00 6F 00 63 00
00 00 E6 00 00 00 48 00 31 00 00 00 00 33 55 07 5D 10 00 53 44 4C 2D 41 50 7E 31 00 00 30 00 03 00 04 00 EF BE 33 55 07 5D 34 55 A7 95 14 00 00 00 73 C
00 72 00 6F 00 6D 00 70 00 74 00 2E 00 6C 00 6E 00 6B 00 00 00 1C 00 15 00 00 00 9A 00 00 00 4C 00 32 00 E0 A8 97 02 33 55 82 58 20 00 64 6F 77 6E 6C 6F 61
A 52 89 10 34 55 47 48 14 00 00 00 50 00 72 00 6F 00 63 00 65 00 73 00 20 00 48 00 61 00 63 00 6B 00 65 00 72 00 20 00 32 00 2E 00 6C 00 66 00 BH
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\She1\NoRoam\BagMRU\MRUListEX: 0A 00 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 C
HKU\\$-1-5-21-1644491937-484763869-29950267-500\Software\Microsoft\Windows\She1\NoRoam\BagMRU\MRUL1stEX: 06 00 00 00 04 0A 00 00 00 05 00 00 00 09 00 00 00 C
HKU\\$-1-5-21-1644491937-484763869-29950267-500\SessionInformation\ProgramCount: 0x00000002
HKU\\$-1-5-21-1644491937-484763869-29950267-500\SessionInformation\ProgramCount: 0x00000003

variazioni totali:35

DOPO AVER EFFETTUATO QUESTE OPERAZIONI POSSIAMO AVVIARE IL MALWARE



The screenshot shows the Process Monitor application interface. The title bar reads "Process Monitor - Sysinternals: www.sysinternals.com". The menu bar includes File, Edit, Event, Filter, Tools, Options, and Help. Below the menu is a toolbar with various icons. The main window is a table with columns: Time..., Process Name, PID, Operation, Path, Result, and Detail. The table lists 151 events out of 38,328, which is 0.3% of the total. The "Operation" column shows mostly "RegOpenKey" and "RegQueryValue" calls. The "Path" column shows registry keys such as "HKLM\Software\Microsoft\Windows N...", "HKLM\System\CurrentControlSet\Contr...", and "HKCU\Software\Policies\Microsoft\Win...". The "Result" column indicates success for most operations, while the "Detail" column provides specific details like "Desired Access: Read", "Type: REG_DWORD, Length: 4, Data: 0", and "Name NOT FOUND". The table is scrollable, with a vertical scrollbar on the right side.

Time...	Process Name	PID	Operation	Path	Result	Detail
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: Read
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read
15.09...	Malware_U3_...	1904	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
15.09...	Malware_U3_...	1904	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Read
15.09...	Malware_U3_...	1904	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
15.09...	Malware_U3_...	1904	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Query Value
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Query Value
15.09...	Malware_U3_...	1904	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 20
15.09...	Malware_U3_...	1904	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Query Value, Set Value
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\Software\Policy\Microsoft\Win...	SUCCESS	Desired Access: Query Value
15.09...	Malware_U3_...	1904	RegQueryValue	HKLM\SOFTWARE\Policy\Microsoft\Win...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
15.09...	Malware_U3_...	1904	RegCloseKey	HKLM\SOFTWARE\Policy\Microsoft\Win...	SUCCESS	
15.09...	Malware_U3_...	1904	RegOpenKey	HKCU\Software\Policy\Microsoft\Win...	NAME NOT FOUND	Desired Access: Query Value
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: Read
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: Read
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: Read
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\System\WPA\TabletPC	NAME NOT FOUND	Desired Access: Query Value, WOW64_64Key
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\SYSTEM\WPA\MediaCenter	SUCCESS	Desired Access: Query Value, WOW64_64Key
15.09...	Malware_U3_...	1904	RegQueryValue	HKLM\SYSTEM\WPA\MediaCenter\In...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
15.09...	Malware_U3_...	1904	RegCloseKey	HKLM\SYSTEM\WPA\MediaCenter	SUCCESS	
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: Read, WOW64_64Key
15.09...	Malware_U3_...	1904	RegOpenKey	HKCU\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: Read, WOW64_64Key
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: Read, WOW64_64Key
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Query Value
15.09...	Malware_U3_...	1904	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 16
15.09...	Malware_U3_...	1904	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15.09...	Malware_U3_...	1904	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: Read
15.09...	Malware_U3_...	1904	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed
15.09...	Malware_U3_...	1904	RegOpenKey	HKCU\Software\Policy\Microsoft\Con...	NAME NOT FOUND	Desired Access: Read
15.09...	Malware_U3_...	1904	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
15.09...	Malware_U3_...	1904	RegOpenKey	HKCU\Control Panel\Desktop\HKEY...	NAME NOT FOUND	Length: 256

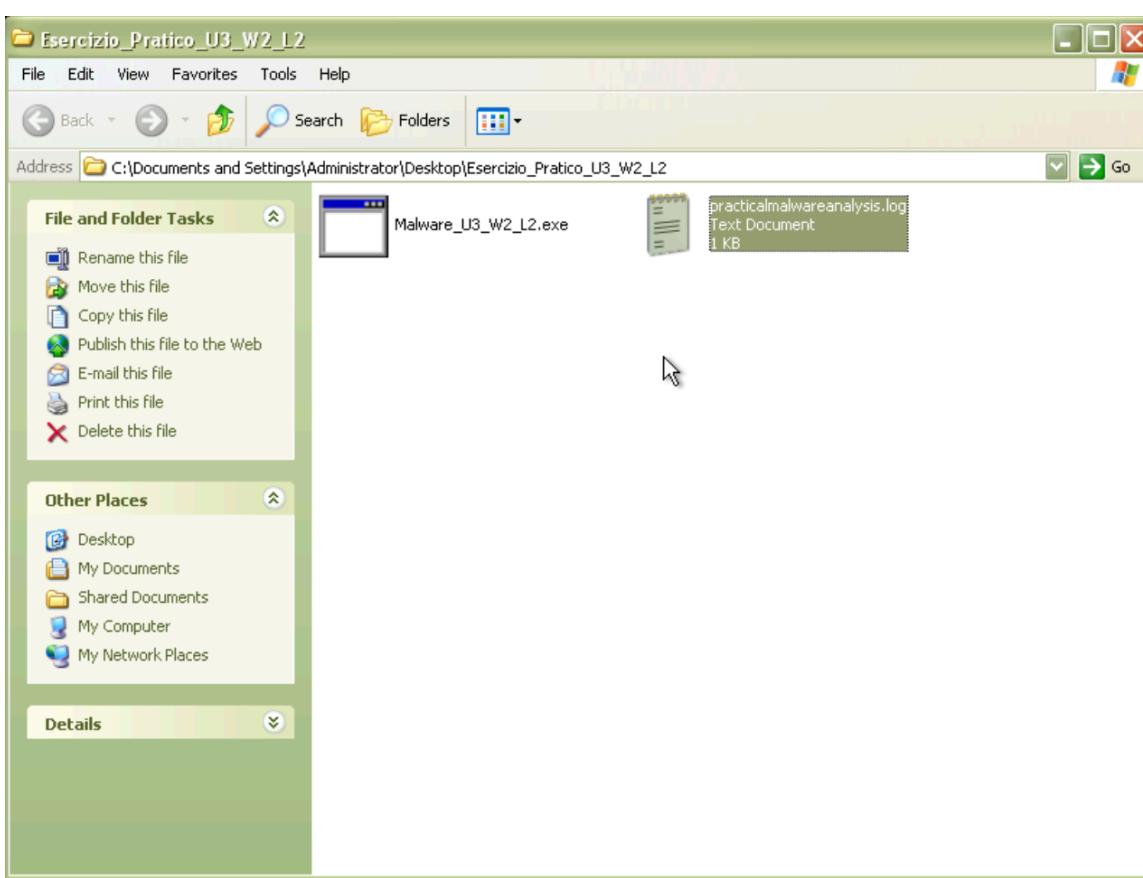
COME POSSIAMO VEDERE DALLA FOTO SOPRA QUI IL MALWARE STA PROVANDO AD APRIRE (REGOPENKEY) UNA CHIAVE DI REGISTRO E QUINDI IL MALWARE STA FACENDO UNA CHIAMATA AD UNA FUNZIONE CONTENUTA IN UNA DATA LIBRERIA

NELLA FOTO QUI DI SEGUITO POSSIAMO VEDERE COME MALWARE VA AD INTERAGIRE CON IL FILE SYSTEM, NEL NOSTRO CASO IL MALWARE CREA UN FILE

Process Monitor - Sysinternals: www.sysinternals.com						
Time...	Process Name	PID	Operation	Path	Result	Detail
13.28...	Malware_U3_...	1144	QueryNameInfo...	C:\Documents and Settings\Administrat...	SUCCESS	Name: \Documents and Settings\Administrat...
13.28...	Malware_U3_...	1144	QueryNameInfo...	C:\Documents and Settings\Administrat...	SUCCESS	Name: \Documents and Settings\Administrat...
13.28...	Malware_U3_...	1144	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U... NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open...	
13.28...	Malware_U3_...	1144	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: Execute/Traverse, Synchronize, ...
13.28...	Malware_U3_...	1144	FileSystemControl	C:\Documents and Settings\Administrat...	SUCCESS	Control: FSCTL_IS_VOLUME_MOUNTED
13.28...	Malware_U3_...	1144	QueryOpen	C:\Documents and Settings\Administrat...	NAME NOT FOUND	
13.28...	Malware_U3_...	1144	ReadFile	C:\Documents and Settings\Administrat...	SUCCESS	Offset: 16.384, Length: 4.096, I/O Flags: Non-cac...
13.28...	Malware_U3_...	1144	ReadFile	C:\Documents and Settings\Administrat...	SUCCESS	Offset: 4.096, Length: 12.288, I/O Flags: Non-cac...
13.28...	Malware_U3_...	1144	ReadFile	C:\Documents and Settings\Administrat...	SUCCESS	Offset: 20.480, Length: 4.096, I/O Flags: Non-cac...
13.28...	Malware_U3_...	1144	ReadFile	C:\Documents and Settings\Administrat...	SUCCESS	Offset: 40.960, Length: 12.288, I/O Flags: Non-ca...
13.28...	Malware_U3_...	1144	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: Read Data/List Directory, Execut...
13.28...	Malware_U3_...	1144	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTypeCreateSection, PageProtecti...
13.28...	Malware_U3_...	1144	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTypeOther
13.28...	Malware_U3_...	1144	QueryOpen	C:\WINDOWS\system32\apphelp.dll	SUCCESS	CreationTime: 14/04/2008 5.00.00, LastAccessTi...
13.28...	Malware_U3_...	1144	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, ...
13.28...	Malware_U3_...	1144	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtecti...
13.28...	Malware_U3_...	1144	QueryStandardI...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	AllocationSize: 126.976, EndOfFile: 125.952, Num...
13.28...	Malware_U3_...	1144	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTypeOther
13.28...	Malware_U3_...	1144	CloseFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	
13.28...	Malware_U3_...	1144	QueryOpen	C:\WINDOWS\system32\apphelp.dll	SUCCESS	CreationTime: 14/04/2008 5.00.00, LastAccessTi...
13.28...	Malware_U3_...	1144	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, ...
13.28...	Malware_U3_...	1144	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtecti...
13.28...	Malware_U3_...	1144	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTypeOther
13.28...	Malware_U3_...	1144	CloseFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	
13.28...	Malware_U3_...	1144	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Open...
13.28...	Malware_U3_...	1144	QueryStandardI...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 1.204.224, EndOfFile: 1.202.774, ...
13.28...	Malware_U3_...	1144	CreateFileMapp...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTypeCreateSection, PageProtecti...
13.28...	Malware_U3_...	1144	QueryStandardI...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 1.204.224, EndOfFile: 1.202.774, ...
13.28...	Malware_U3_...	1144	CreateFileMapp...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTypeOther
13.28...	Malware_U3_...	1144	QueryStandardI...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 1.204.224, EndOfFile: 1.202.774, ...
13.28...	Malware_U3_...	1144	CreateFile	C:\WINDOWS\AppPatch\sysstest.sdb	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open...
13.28...	Malware_U3_...	1144	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchron...

Showing 98 of 62.093 events (0.1%)

Backed by virtual memory



DA QUESTA FOTO POSSIAMO VEDERE COME IL MALWARE INTERAGISCE SUI PROCESSI E THREAD

Process Monitor - Sysinternals: www.sysinternals.com						
Time...	Process Name	PID	Operation	Path	Result	Detail
13.28...	Malware_U3...	1144	Process Start		SUCCESS	Parent PID: 1776, Command line: "C:\Documents ...
13.28...	Malware_U3...	1144	Thread Create		SUCCESS	Thread ID: 536
13.28...	Malware_U3...	1144	Load Image	C:\Documents and Settings\Administrat...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
13.28...	Malware_U3...	1144	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
13.28...	Malware_U3...	1144	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7cb00000, Image Size: 0xf6000
13.28...	Malware_U3...	1144	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
13.28...	Malware_U3...	1144	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
13.28...	Malware_U3...	1144	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0xb0000
13.28...	Malware_U3...	1144	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
13.28...	Malware_U3...	1144	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77e00000, Image Size: 0x11000
13.28...	Malware_U3...	1144	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1484, Command line: "C:\WINDOWS\syste...
13.28...	Malware_U3...	1144	Thread Exit		SUCCESS	Thread ID: 536, User Time: 0.0000000, Kernel Ti...
13.28...	Malware_U3...	1144	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Ke...

COME POSSIAMO NOTARE QUI IL MALWARE VA A CREARE DELLE FUNZIONI (LOAD IMAGE) CHE SERVONO PER CARICARE ESEGUIBILI E LIBRERIE PER ESECUZIONE IN MEMORIA E ATTIVITA' SUI PROCESSI E THREAD COME CREATE PROCESS, CREATE THREAD

Process Explorer - Sysinternals: www.sysinternals.com [LUCA-FC615DFE89\Administrator]						
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		1.668 K	4.120 K	832	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1.49	13.556 K	22.656 K	908	Generic Host Process for Wi...	Microsoft Corporation
wscnify.exe		540 K	2.220 K	956	Windows Security Center No...	Microsoft Corporation
svchost.exe		1.188 K	3.408 K	1012	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1.748 K	4.668 K	1068	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		2.992 K	4.424 K	1188	Spooler SubSystem App	Microsoft Corporation
alg.exe		1.124 K	3.488 K	888	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3.552 K	700 K	572	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	0.75	37.360 K	13.628 K	1776	Windows Explorer	Microsoft Corporation
ctfmon.exe		836 K	3.172 K	1100	CTF Loader	Microsoft Corporation
procexp.exe	0.75	9.960 K	5.172 K	984	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon.exe		6.332 K	744 K	1324	Process Monitor	Sysinternals - www.sysinter...
Wireshark.exe		88.312 K	4.020 K	1460	Wireshark	The Wireshark developer ...
notepad.exe		1.288 K	568 K	1280	Notepad	Microsoft Corporation
procexp.exe	2.99	9.632 K	12.800 K	388	Sysinternals Process Explorer	Sysinternals - www.sysinter...
svchost.exe		872 K	2.384 K	1484	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		892 K	2.500 K	944	Generic Host Process for Wi...	Microsoft Corporation

Type	Name
Directory	\KnownDlls
Directory	Wwindows
Directory	\BaseNamedObjects
Event	\BaseNamedObjects\userenv: User Profile setup event
File	C:\Documents and Settings\Administrator\Desktop
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0...
File	\Device\KsecDD
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32
Key	HKCU

CPU Usage: 5.97% | Commit Charge: 8.01% | Processes: 25 | Physical Usage: 13.21%

SECONDO ME IL MALWARE VA A COMPROMETTERE IL SITEMA OPERATIVO IN MODO TALE DA NON PERMETTE IL NORMALE FUNZIONAMENTO

