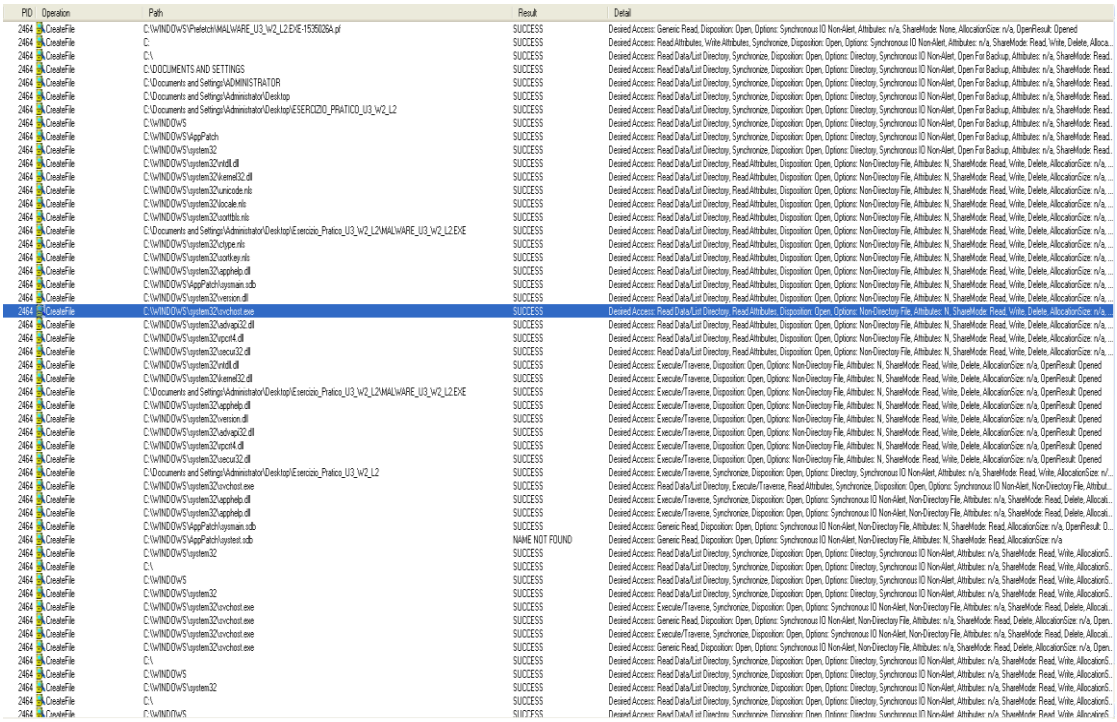
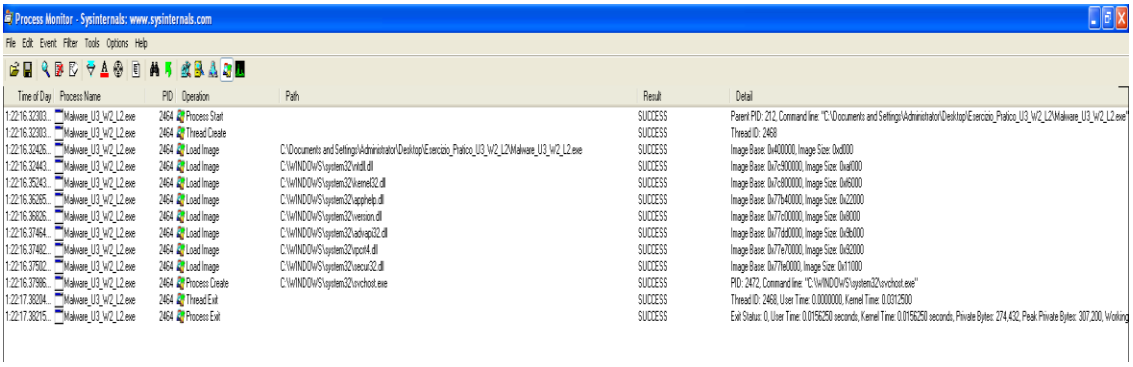
# ANALISI DINAMICA BASICA MALWARE

1. Identificazione di eventuali azioni del malware sul file system



| PID | Operation | Path | Result | Detail |
|---|---|---|---|---|
| 2464 | CreateFile | C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535B26A.pf | SUCCESS | Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, AllocationSize: n/a, OpenResult: Opened |
| 2464 | CreateFile | C: | SUCCESS | Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, Delete, Alloca... |
| 2464 | CreateFile | C:\ | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read... |
| 2464 | CreateFile | C:\DOCUMENTS AND SETTINGS | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read... |
| 2464 | CreateFile | C:\Documents and Settings\ADMINISTRATOR | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read... |
| 2464 | CreateFile | C:\Documents and Settings\Administrator\Desktop | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read... |
| 2464 | CreateFile | C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2 | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read... |
| 2464 | CreateFile | C:\WINDOWS | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read... |
| 2464 | CreateFile | C:\WINDOWS\AppPatch | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read... |
| 2464 | CreateFile | C:\WINDOWS\system32 | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read... |
| 2464 | CreateFile | C:\WINDOWS\system32\ntdll.dll | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: n/a, ShareMode: Read... |
| 2464 | CreateFile | C:\WINDOWS\system32\kernel32.dll | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\unicode.nls | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\locale.nls | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\sorttbls.nls | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | 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-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\ctype.nls | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\sortkey.nls | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\apphelp.dll | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\AppPatch\sysmain.sdb | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\version.dll | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\vmchost.exe | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\advapi32.dll | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\secur32.dll | SUCCESS | Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ... |
| 2464 | CreateFile | C:\WINDOWS\system32\ntdll.dll | SUCCESS | Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened |
| 2464 | CreateFile | C:\WINDOWS\system32\kernel32.dll | SUCCESS | Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened |
| 2464 | 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: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened |
| 2464 | CreateFile | C:\WINDOWS\system32\apphelp.dll | SUCCESS | Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened |
| 2464 | CreateFile | C:\WINDOWS\system32\version.dll | SUCCESS | Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened |
| 2464 | CreateFile | C:\WINDOWS\system32\advapi32.dll | SUCCESS | Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened |
| 2464 | CreateFile | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS | Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened |
| 2464 | CreateFile | C:\WINDOWS\system32\secur32.dll | SUCCESS | Desired Access: Execute/Traverse, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened |
| 2464 | CreateFile | C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2 | SUCCESS | Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationSize: n/... |
| 2464 | CreateFile | C:\WINDOWS\system32\vmchost.exe | SUCCESS | Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attribut... |
| 2464 | CreateFile | C:\WINDOWS\system32\apphelp.dll | SUCCESS | Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, Allocati... |
| 2464 | CreateFile | C:\WINDOWS\system32\apphelp.dll | SUCCESS | Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, Allocati... |
| 2464 | CreateFile | C:\WINDOWS\AppPatch\sysmain.sdb | SUCCESS | Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, AllocationSize: n/a, OpenResult: O... |
| 2464 | CreateFile | C:\WINDOWS\AppPatch\systest.sdb | NAME NOT FOUND | Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, AllocationSize: n/a |
| 2464 | CreateFile | C:\WINDOWS\system32 | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationS... |
| 2464 | CreateFile | C:\ | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationS... |
| 2464 | CreateFile | C:\WINDOWS | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationS... |
| 2464 | CreateFile | C:\WINDOWS\system32 | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationS... |
| 2464 | CreateFile | C:\WINDOWS\system32\vmchost.exe | SUCCESS | Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, Allocati... |
| 2464 | CreateFile | C:\WINDOWS\system32\vmchost.exe | SUCCESS | Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, Open... |
| 2464 | CreateFile | C:\WINDOWS\system32\vmchost.exe | SUCCESS | Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, Allocati... |
| 2464 | CreateFile | C:\WINDOWS\system32\vmchost.exe | SUCCESS | Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, Open... |
| 2464 | CreateFile | C:\ | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationS... |
| 2464 | CreateFile | C:\WINDOWS | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationS... |
| 2464 | CreateFile | C:\WINDOWS\system32 | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationS... |
| 2464 | CreateFile | C:\ | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationS... |
| 2464 | CreateFile | C:\WINDOWS | SUCCESS | Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, AllocationS... |

2. Identificazione eventuali azioni del malware su processi e thread



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time of Day | Process Name | PID | Operation | Path | Result | Detail |
|---|---|---|---|---|---|---|
| 1:22:16.32383... | Malware_U3_W2_L2.exe | 2464 | Process Start | | SUCCESS | Parent PID: 212, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe" |
| 1:22:16.32383... | Malware_U3_W2_L2.exe | 2464 | Thread Create | | SUCCESS | Thread ID: 2468 |
| 1:22:16.32426... | Malware_U3_W2_L2.exe | 2464 | 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 |
| 1:22:16.32443... | Malware_U3_W2_L2.exe | 2464 | Load Image | C:\WINDOWS\system32\ntdll.dll | SUCCESS | Image Base: 0x7c900000, Image Size: 0xaf000 |
| 1:22:16.35243... | Malware_U3_W2_L2.exe | 2464 | Load Image | C:\WINDOWS\system32\kernel32.dll | SUCCESS | Image Base: 0x7c800000, Image Size: 0xf6000 |
| 1:22:16.36295... | Malware_U3_W2_L2.exe | 2464 | Load Image | C:\WINDOWS\system32\apphelp.dll | SUCCESS | Image Base: 0x77b40000, Image Size: 0x22000 |
| 1:22:16.36826... | Malware_U3_W2_L2.exe | 2464 | Load Image | C:\WINDOWS\system32\version.dll | SUCCESS | Image Base: 0x77c00000, Image Size: 0x8000 |
| 1:22:16.37464... | Malware_U3_W2_L2.exe | 2464 | Load Image | C:\WINDOWS\system32\advapi32.dll | SUCCESS | Image Base: 0x77dd0000, Image Size: 0x9b000 |
| 1:22:16.37492... | Malware_U3_W2_L2.exe | 2464 | Load Image | C:\WINDOWS\system32\rpcrt4.dll | SUCCESS | Image Base: 0x77e70000, Image Size: 0x92000 |
| 1:22:16.37592... | Malware_U3_W2_L2.exe | 2464 | Load Image | C:\WINDOWS\system32\secur32.dll | SUCCESS | Image Base: 0x77fe0000, Image Size: 0x11000 |
| 1:22:16.37986... | Malware_U3_W2_L2.exe | 2464 | Process Create | C:\WINDOWS\system32\vmchost.exe | SUCCESS | PID: 2472, Command line: "C:\WINDOWS\system32\vmchost.exe" |
| 1:22:17.38204... | Malware_U3_W2_L2.exe | 2464 | Thread Exit | | SUCCESS | Thread ID: 2468, User Time: 0.0000000, Kernel Time: 0.0312500 |
| 1:22:17.39215... | Malware_U3_W2_L2.exe | 2464 | Process Exit | | SUCCESS | Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 274,432, Peak Private Bytes: 307,200, Working |

3. Modifiche del registro dopo l'esecuzione del malware

```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2023/1/10 13:18:04   ,   2023/1/10 13:29:38
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

----------------------------------
Keys deleted: 2
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\PROCMON24\Enum
HKLM\SYSTEM\CurrentControlSet\Services\PROCMON24\Enum

----------------------------------
Keys added: 2
----------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON24\0000\Control
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON24\0000\Control

----------------------------------
Values deleted: 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

----------------------------------
Values added: 24
----------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON24\0000\Control\ActiveService: "PROCMON24"
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON24\0000\Control\ActiveService: "PROCMON24"
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\MinPos1920x940(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\MinPos1920x940(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\MaxPos1920x940(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\MaxPos1920x940(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\WinPos1920x940(1).left: 0x0000009A
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\WinPos1920x940(1).top: 0x000000CB
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\WinPos1920x940(1).right: 0x000003BA
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\WinPos1920x940(1).bottom: 0x00000323
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\ScrollPos1920x940(1).x: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\106\Shell\ScrollPos1920x940(1).y: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\26\Shell\ScrollPos1920x940(1).x: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\26\Shell\ScrollPos1920x940(1).y: 0x00000000
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\26\Shell\MinPos1920x940(1).x: 0xFFFF8300
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\26\Shell\MinPos1920x940(1).y: 0xFFFF8300
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\26\Shell\MaxPos1920x940(1).x: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\26\Shell\MaxPos1920x940(1).y: 0xFFFFFFFF
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\26\Shell\WinPos1920x940(1).left: 0x00000016
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\26\Shell\WinPos1920x940(1).top: 0x0000001D
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\26\Shell\WinPos1920x940(1).right: 0x00000336
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\Bags\26\Shell\WinPos1920x940(1).bottom: 0x00000275

----------------------------------
Values modified: 21
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  A3 D5 BD 91 DC 89 D6 BF 7E 81 AE 12 FB 6C F5 03 91 D1 5F 8F 58 DC 72 59 67 C5 35 93 F8 83 C3 D
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  E4 5C FA 49 9A E8 C8 D1 AF 0D 5D 40 04 63 04 FB A6 57 3D BC 90 BB F0 9D E0 15 C5 E6 34 15 0D 7
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\Count: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\Count: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInstance: 0x00000000
```

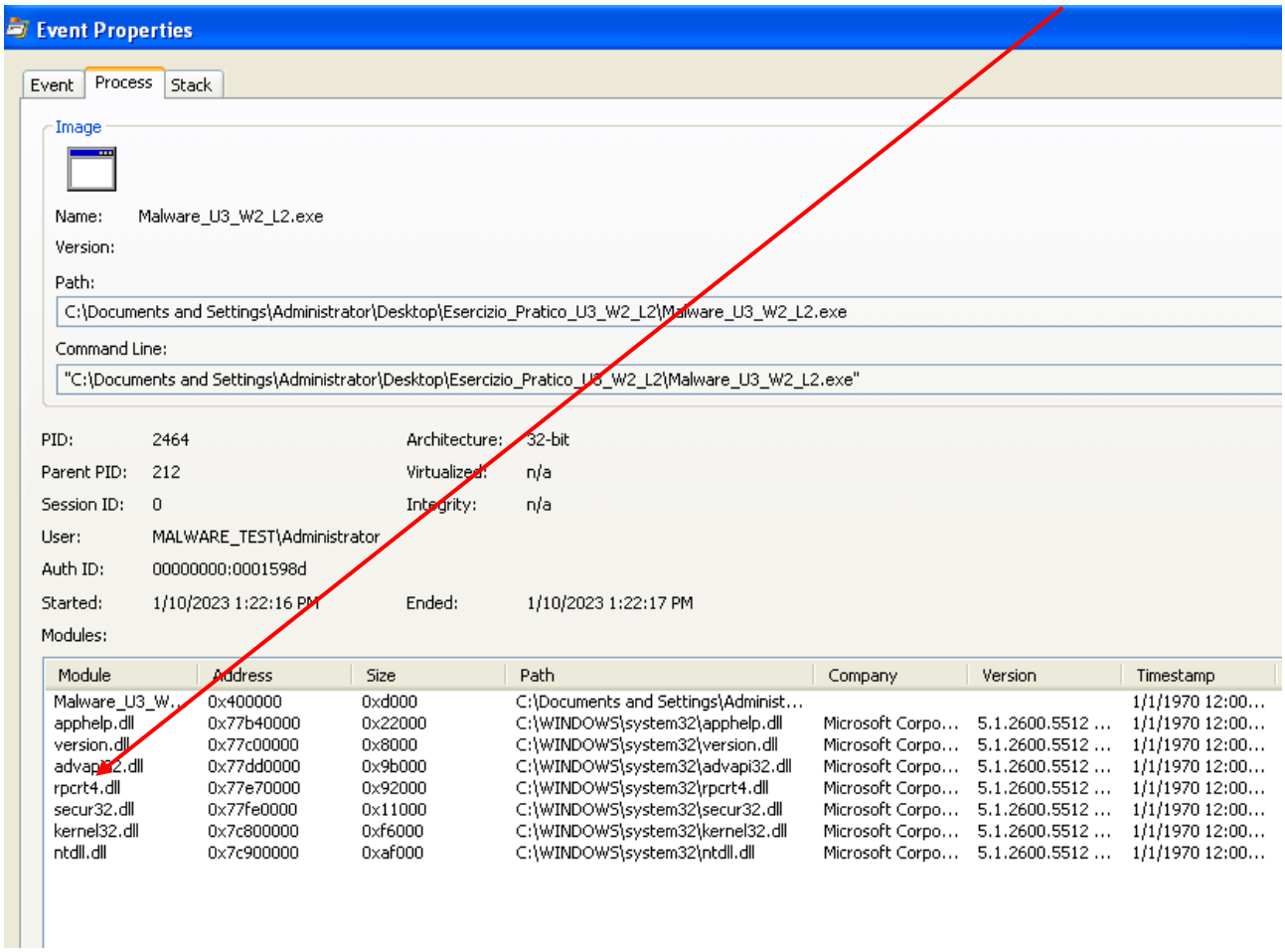
```
----------------------------------
Files added: 1
----------------------------------
C:\Documents and Settings\Administrator\Desktop\1st shot.hivu

----------------------------------
Files deleted: 1
----------------------------------
C:\WINDOWS\SoftwareDistribution\DataStore\Logs\tmp.edb

----------------------------------
Files [attributes?] modified: 17
----------------------------------
C:\WINDOWS\Prefetch\APATEDNS.EXE-02BC24A6.pf
C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
C:\WINDOWS\Prefetch\PROCMON.EXE-0D936DEE.pf
C:\WINDOWS\Prefetch\REGSHOT-X86-UNICODE.EXE-32EDD4BA.pf
C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf
C:\WINDOWS\Prefetch\TASKMGR.EXE-20256C55.pf
C:\WINDOWS\Prefetch\VERCLSID.EXE-3667BD89.pf
C:\WINDOWS\Prefetch\WMIPRVSE.EXE-28F301A9.pf
C:\WINDOWS\SoftwareDistribution\DataStore\DataStore.edb
C:\WINDOWS\SoftwareDistribution\DataStore\Logs\edb.chk
C:\WINDOWS\SoftwareDistribution\DataStore\Logs\edb.log
C:\WINDOWS\system32\config\SECURITY.LOG
C:\WINDOWS\system32\config\software.LOG
C:\WINDOWS\system32\config\system.LOG
C:\WINDOWS\system32\wbem\Logs\wbemcore.log
C:\WINDOWS\system32\wbem\Logs\wmiprov.log
C:\WINDOWS\WindowsUpdate.log

----------------------------------
Total changes: 74
----------------------------------
```

4. Spiegazione del malware in base a quanto visto

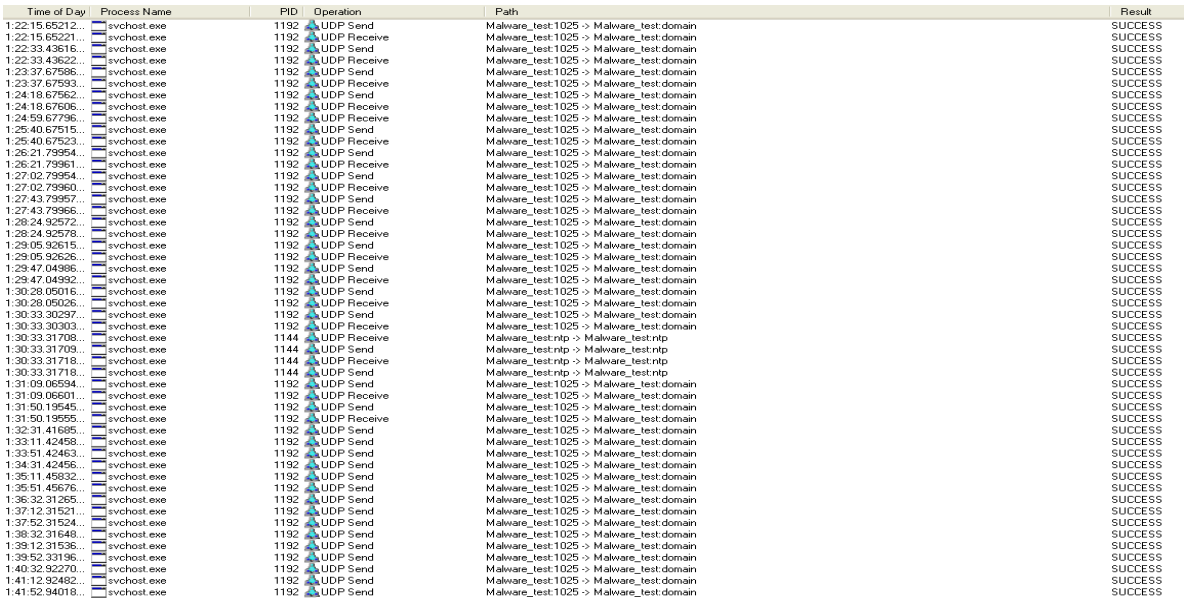
Il malware ha attaccato il processo svchost.exe

... Malware U3 W2 L2.exe 2464 Process Create C:\WINDOWS\system32\svchost.exe SUCCESS

che è usato da Microsoft per nascondere più servizi dietro ad un unico processo, quindi bisogna capire intanto quale servizio è stato attaccato; andando a cercare i moduli usati, ci siamo accorti che il processo usava la libreria rpcrt4.dll




che è usata per la comunicazione di rete e internet; cercando sempre su ProcMon nella sezione network activity, possiamo vedere infatti che il processo svchost tenta una connessione sia TCP che UDP ad un server esterno



in questo caso possiamo ipotizzare si tratti di un Trojan in quanto il comportamento appena evidenziato fa parte dell'attività del suddetto, che può essere programmato appunto per trasformare il pc infetto in un computer zombie da utilizzare in una botnet.