S10/L2 Esercizio 28/11/2023

In questo esercizio ci viene richiesto di effettuare un'analisi dinamica eseguendo di fatto il malware e di:

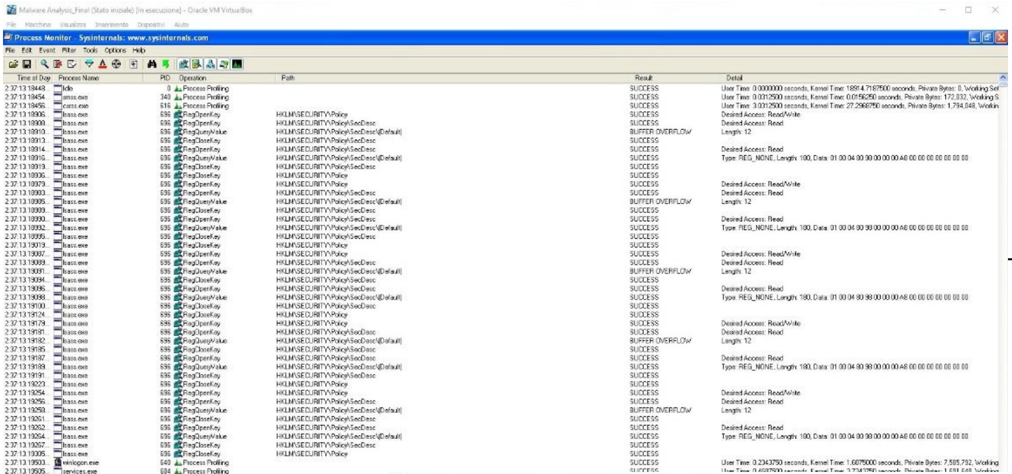
- Identificare eventuali azioni del malware sul file system
- Identificare eventuali azioni del malware su processi e thread
- Identificare le differenze del registro dopo il malware
- Provare a profilare il malware in base alla correlazione tra operation e path

Analisi dinamica

L'analisi dinamica valuta il comportamento di un'applicazione durante l'esecuzione e, a differenza della statica, esegue realmente il programma (il malware in questo specifico caso).
E' utile per comprendere come un'applicazione si comporta in situazioni reali e per identificare problemi che potrebbero non essere evidenti durante un'analisi statica del codice.

Comprende diverse attività quali l'esecuzione del software, che viene rigorosamente eseguito in un ambiente di test; il monitoraggio del comportamento in cui vengono monitorati e registrati diversi aspetti del comportamento dell'applicazione, come ad esempio le chiamate di sistema, le interazioni con il file system o le operazioni di rete e il rilevamento di anomalie o problemi

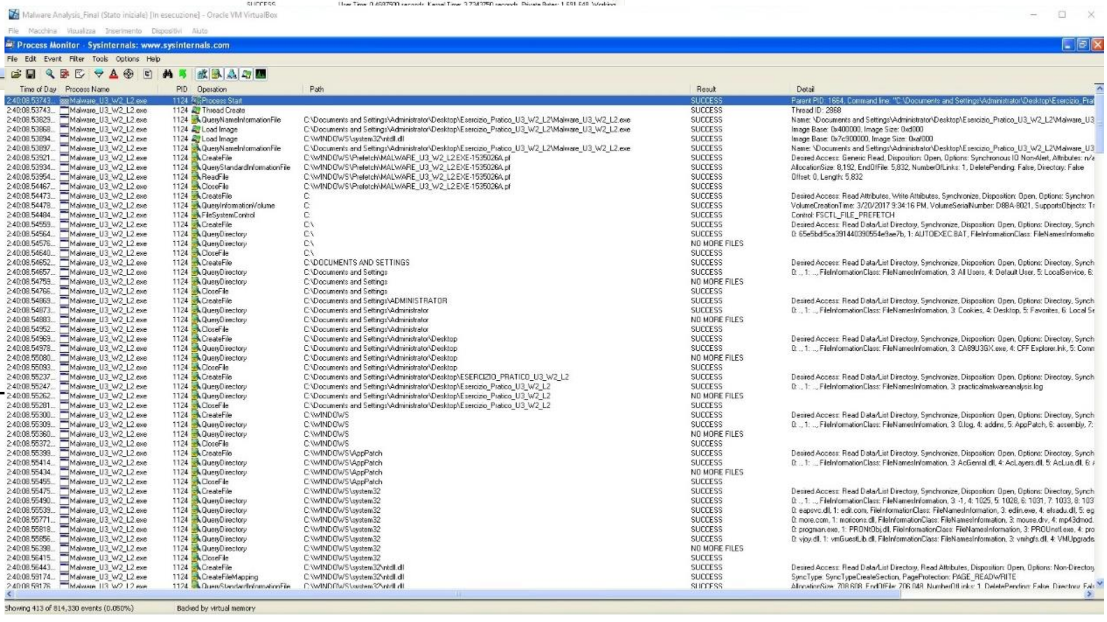
Procmon



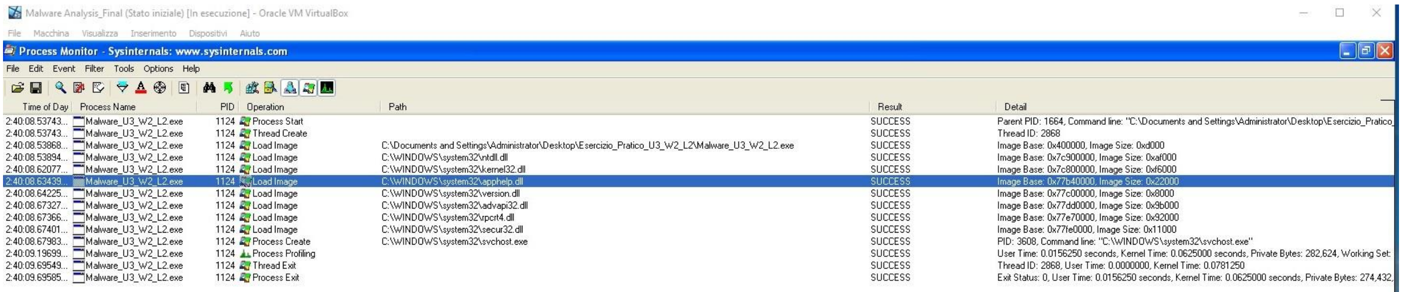
Prima di eseguire il malware

```
Time of Day    Process Name      PID   Operation          Path                                      Result           Detail
2:37:13.18448... Idle              0   Process Profiling                                            SUCCESS          User Time: 0.0000000 seconds, Kernel Time: 18914.7187500 seconds, Private Bytes: 0, Working Set
2:37:13.18454... smss.exe        340   Process Profiling                                            SUCCESS          User Time: 0.0312500 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 172,032, Working S
2:37:13.18456... csrss.exe       616   Process Profiling                                            SUCCESS          User Time: 3.0312500 seconds, Kernel Time: 27.2968750 seconds, Private Bytes: 1,794,048, Workin
2:37:13.18906... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy                      SUCCESS          Desired Access: Read/Write
2:37:13.18908... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy\SecDesc              SUCCESS          Desired Access: Read
2:37:13.18910... lsass.exe       696   RegQueryValue      HKLM\SECURITY\Policy\SecDesc\(Default)    BUFFER OVERFLOW  Length: 12
2:37:13.18913... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy\SecDesc              SUCCESS
2:37:13.18914... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy\SecDesc              SUCCESS          Desired Access: Read
2:37:13.18916... lsass.exe       696   RegQueryValue      HKLM\SECURITY\Policy\SecDesc\(Default)    SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 00 00 00 A8 00 00 00 00 00 00 00
2:37:13.18919... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy\SecDesc              SUCCESS
2:37:13.18936... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy                      SUCCESS
2:37:13.18979... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy                      SUCCESS          Desired Access: Read/Write
2:37:13.18983... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy\SecDesc              SUCCESS          Desired Access: Read
2:37:13.18985... lsass.exe       696   RegQueryValue      HKLM\SECURITY\Policy\SecDesc\(Default)    BUFFER OVERFLOW  Length: 12
2:37:13.18989... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy\SecDesc              SUCCESS
2:37:13.18990... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy\SecDesc              SUCCESS          Desired Access: Read
2:37:13.18992... lsass.exe       696   RegQueryValue      HKLM\SECURITY\Policy\SecDesc\(Default)    SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 00 00 00 A8 00 00 00 00 00 00 00
2:37:13.18995... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy\SecDesc              SUCCESS
2:37:13.19019... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy                      SUCCESS
2:37:13.19087... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy                      SUCCESS          Desired Access: Read/Write
2:37:13.19089... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy\SecDesc              SUCCESS          Desired Access: Read
2:37:13.19091... lsass.exe       696   RegQueryValue      HKLM\SECURITY\Policy\SecDesc\(Default)    BUFFER OVERFLOW  Length: 12
2:37:13.19094... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy\SecDesc              SUCCESS
2:37:13.19096... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy\SecDesc              SUCCESS          Desired Access: Read
2:37:13.19098... lsass.exe       696   RegQueryValue      HKLM\SECURITY\Policy\SecDesc\(Default)    SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 00 00 00 A8 00 00 00 00 00 00 00
2:37:13.19100... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy\SecDesc              SUCCESS
2:37:13.19124... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy                      SUCCESS
2:37:13.19179... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy                      SUCCESS          Desired Access: Read/Write
2:37:13.19181... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy\SecDesc              SUCCESS          Desired Access: Read
2:37:13.19182... lsass.exe       696   RegQueryValue      HKLM\SECURITY\Policy\SecDesc\(Default)    BUFFER OVERFLOW  Length: 12
2:37:13.19185... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy\SecDesc              SUCCESS
2:37:13.19187... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy\SecDesc              SUCCESS          Desired Access: Read
2:37:13.19189... lsass.exe       696   RegQueryValue      HKLM\SECURITY\Policy\SecDesc\(Default)    SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 00 00 00 A8 00 00 00 00 00 00 00
2:37:13.19191... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy\SecDesc              SUCCESS
2:37:13.19223... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy                      SUCCESS
2:37:13.19254... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy                      SUCCESS          Desired Access: Read/Write
2:37:13.19256... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy\SecDesc              SUCCESS          Desired Access: Read
2:37:13.19258... lsass.exe       696   RegQueryValue      HKLM\SECURITY\Policy\SecDesc\(Default)    BUFFER OVERFLOW  Length: 12
2:37:13.19261... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy\SecDesc              SUCCESS
2:37:13.19262... lsass.exe       696   RegOpenKey         HKLM\SECURITY\Policy\SecDesc              SUCCESS          Desired Access: Read
2:37:13.19264... lsass.exe       696   RegQueryValue      HKLM\SECURITY\Policy\SecDesc\(Default)    SUCCESS          Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 00 00 00 A8 00 00 00 00 00 00 00
2:37:13.19267... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy\SecDesc              SUCCESS
2:37:13.19305... lsass.exe       696   RegCloseKey        HKLM\SECURITY\Policy                      SUCCESS
2:37:13.19503... winlogon.exe    640   Process Profiling                                            SUCCESS          User Time: 0.2343750 seconds, Kernel Time: 1.6875000 seconds, Private Bytes: 7,585,792, Working
2:37:13.19505... services.exe    684   Process Profiling                                            SUCCESS          User Time: 0.4687500 seconds, Kernel Time: 3.7343750 seconds, Private Bytes: 1,691,648, Working
2:37:13.19506... lsass.exe       696   Process Profiling
2:37:13.19508... VBoxService.exe 852   Process Profiling
2:37:13.19512... vmacthlp.exe    872   Process Profiling
2:37:13.19514... svchost.exe     924   Process Profiling
2:37:13.19517... svchost.exe    1004   Process Profiling
2:37:13.20008... svchost.exe    1100   Process Profiling
2:37:13.20011... svchost.exe    1148   Process Profiling

Showing 10,417 of 49,278 events (21%)     Backed by virtual memory
```

Dopo l'esecuzione del malware



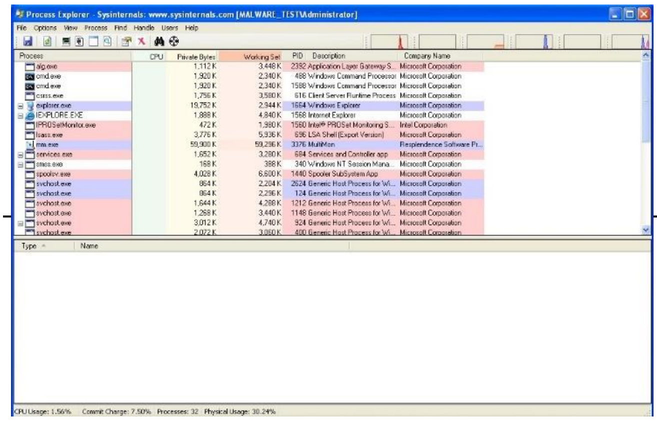
```
Time of Day      Process Name          PID   Operation                       Path                                                                                       Result           Detail
2:40:08.53743... Malware_U3_W2_L2.exe  1124  Process Start                                                                                                              SUCCESS          Parent PID: 1664, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pra
2:40:08.53743... Malware_U3_W2_L2.exe  1124  Thread Create                                                                                                              SUCCESS          Thread ID: 2868
2:40:08.53829... Malware_U3_W2_L2.exe  1124  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\Malware_U3
2:40:08.53868... Malware_U3_W2_L2.exe  1124  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
2:40:08.53894... Malware_U3_W2_L2.exe  1124  Load Image                      C:\WINDOWS\system32\ntdll.dll                                                              SUCCESS          Image Base: 0x7c900000, Image Size: 0xaf000
2:40:08.53897... Malware_U3_W2_L2.exe  1124  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\Malware_U3
2:40:08.53921... Malware_U3_W2_L2.exe  1124  CreateFile                      C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf                                       SUCCESS          Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a
2:40:08.53934... Malware_U3_W2_L2.exe  1124  QueryStandardInformationFile    C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf                                       SUCCESS          AllocationSize: 8,192, EndOfFile: 5,832, NumberOfLinks: 1, DeletePending: False, Directory: False
2:40:08.53954... Malware_U3_W2_L2.exe  1124  ReadFile                        C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf                                       SUCCESS          Offset: 0, Length: 5,832
2:40:08.54467... Malware_U3_W2_L2.exe  1124  CloseFile                       C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf                                       SUCCESS
2:40:08.54473... Malware_U3_W2_L2.exe  1124  CreateFile                      C:                                                                                         SUCCESS          Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Synchron
2:40:08.54478... Malware_U3_W2_L2.exe  1124  QueryInformationVolume          C:                                                                                         SUCCESS          VolumeCreationTime: 3/20/2017 9:34:16 PM, VolumeSerialNumber: D88A-8021, SupportsObjects: Tr
2:40:08.54484... Malware_U3_W2_L2.exe  1124  FileSystemControl               C:                                                                                         SUCCESS          Control: FSCTL_FILE_PREFETCH
2:40:08.54559... Malware_U3_W2_L2.exe  1124  CreateFile                      C:\                                                                                        SUCCESS          Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch
2:40:08.54564... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\                                                                                        SUCCESS          0: 65e5bdf5ca391440390554e9ae7b, 1: AUTOEXEC.BAT, FileInformationClass: FileNamesInformatio
2:40:08.54576... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\                                                                                        NO MORE FILES
2:40:08.54640... Malware_U3_W2_L2.exe  1124  CloseFile                       C:\                                                                                        SUCCESS
2:40:08.54652... Malware_U3_W2_L2.exe  1124  CreateFile                      C:\DOCUMENTS AND SETTINGS                                                                  SUCCESS          Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch
2:40:08.54657... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\Documents and Settings                                                                  SUCCESS          0: ., 1: .., FileInformationClass: FileNamesInformation, 3: All Users, 4: Default User, 5: LocalService, 6:
2:40:08.54759... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\Documents and Settings                                                                  NO MORE FILES
2:40:08.54766... Malware_U3_W2_L2.exe  1124  CloseFile                       C:\Documents and Settings                                                                  SUCCESS
2:40:08.54869... Malware_U3_W2_L2.exe  1124  CreateFile                      C:\Documents and Settings\ADMINISTRATOR                                                    SUCCESS          Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch
2:40:08.54873... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\Documents and Settings\Administrator                                                    SUCCESS          0: ., 1: .., FileInformationClass: FileNamesInformation, 3: Cookies, 4: Desktop, 5: Favorites, 6: Local Se
2:40:08.54883... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\Documents and Settings\Administrator                                                    NO MORE FILES
2:40:08.54952... Malware_U3_W2_L2.exe  1124  CloseFile                       C:\Documents and Settings\Administrator                                                    SUCCESS
2:40:08.54969... Malware_U3_W2_L2.exe  1124  CreateFile                      C:\Documents and Settings\Administrator\Desktop                                            SUCCESS          Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch
2:40:08.54978... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\Documents and Settings\Administrator\Desktop                                            SUCCESS          0: ., 1: .., FileInformationClass: FileNamesInformation, 3: CA89U3GX.exe, 4: CFF Explorer.lnk, 5: Comm
2:40:08.55080... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\Documents and Settings\Administrator\Desktop                                            NO MORE FILES
2:40:08.55093... Malware_U3_W2_L2.exe  1124  CloseFile                       C:\Documents and Settings\Administrator\Desktop                                            SUCCESS
2:40:08.55237... Malware_U3_W2_L2.exe  1124  CreateFile                      C:\Documents and Settings\Administrator\Desktop\ESERCIZIO_PRATICO_U3_W2_L2                 SUCCESS          Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch
2:40:08.55247... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2                 SUCCESS          0: ., 1: .., FileInformationClass: FileNamesInformation, 3: practicalmalwareanalysis.log
2:40:08.55262... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2                 NO MORE FILES
2:40:08.55281... Malware_U3_W2_L2.exe  1124  CloseFile                       C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2                 SUCCESS
2:40:08.55300... Malware_U3_W2_L2.exe  1124  CreateFile                      C:\WINDOWS                                                                                 SUCCESS          Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch
2:40:08.55309... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\WINDOWS                                                                                 SUCCESS          0: ., 1: .., FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7:
2:40:08.55360... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\WINDOWS                                                                                 NO MORE FILES
2:40:08.55372... Malware_U3_W2_L2.exe  1124  CloseFile                       C:\WINDOWS                                                                                 SUCCESS
2:40:08.55399... Malware_U3_W2_L2.exe  1124  CreateFile                      C:\WINDOWS\AppPatch                                                                        SUCCESS          Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch
2:40:08.55414... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\WINDOWS\AppPatch                                                                        SUCCESS          0: ., 1: .., FileInformationClass: FileNamesInformation, 3: AcGenral.dll, 4: AcLayers.dll, 5: AcLua.dll, 6:
2:40:08.55434... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\WINDOWS\AppPatch                                                                        NO MORE FILES
2:40:08.55455... Malware_U3_W2_L2.exe  1124  CloseFile                       C:\WINDOWS\AppPatch                                                                        SUCCESS
2:40:08.55475... Malware_U3_W2_L2.exe  1124  CreateFile                      C:\WINDOWS\system32                                                                        SUCCESS          Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synch
2:40:08.55490... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\WINDOWS\system32                                                                        SUCCESS          0: ., 1: .., FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 103
2:40:08.55539... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\WINDOWS\system32                                                                        SUCCESS          0: eapsvc.dll, 1: edit.com, FileInformationClass: FileNamesInformation, 3: edlin.exe, 4: efsadu.dll, 5: eg
2:40:08.55771... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\WINDOWS\system32                                                                        SUCCESS          0: more.com, 1: moricons.dll, FileInformationClass: FileNamesInformation, 3: mouse.drv, 4: mp43dmod.
2:40:08.55818... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\WINDOWS\system32                                                                        SUCCESS          0: progman.exe, 1: PROMtObj.dll, FileInformationClass: FileNamesInformation, 3: PROUnstl.exe, 4: pro
2:40:08.55856... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\WINDOWS\system32                                                                        SUCCESS          0: vjoy.dll, 1: vmGuestLib.dll, FileInformationClass: FileNamesInformation, 3: vmhgfs.dll, 4: VMUpgrade
2:40:08.56398... Malware_U3_W2_L2.exe  1124  QueryDirectory                  C:\WINDOWS\system32                                                                        NO MORE FILES
2:40:08.56415... Malware_U3_W2_L2.exe  1124  CloseFile                       C:\WINDOWS\system32                                                                        SUCCESS
2:40:08.56443... Malware_U3_W2_L2.exe  1124  CreateFile                      C:\WINDOWS\system32\ntdll.dll                                                              SUCCESS          Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory
2:40:08.59174... Malware_U3_W2_L2.exe  1124  CreateFileMapping               C:\WINDOWS\system32\ntdll.dll                                                              SUCCESS          SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
2:40:08.59176... Malware_U3_W2_L2.exe  1124  QueryStandardInformationFile    C:\WINDOWS\system32\ntdll.dll                                                              SUCCESS          AllocationSize: 708,608, EndOfFile: 706,048, NumberOfLinks: 1, DeletePending: False, Directory: Fals

Showing 413 of 814,330 events (0.050%)     Backed by virtual memory
```



```
Time of Day   Process Name          PID   Operation          Path                                                                                   Result    Detail
2:40:08.53743...  Malware_U3_W2_L2.exe  1124  Process Start                                                                                         SUCCESS   Parent PID: 1664, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_
2:40:08.53743...  Malware_U3_W2_L2.exe  1124  Thread Create                                                                                         SUCCESS   Thread ID: 2868
2:40:08.53868...  Malware_U3_W2_L2.exe  1124  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
2:40:08.53894...  Malware_U3_W2_L2.exe  1124  Load Image     C:\WINDOWS\system32\ntdll.dll                                                          SUCCESS   Image Base: 0x7c900000, Image Size: 0xaf000
2:40:08.62077...  Malware_U3_W2_L2.exe  1124  Load Image     C:\WINDOWS\system32\kernel32.dll                                                       SUCCESS   Image Base: 0x7c800000, Image Size: 0xf6000
2:40:08.63439...  Malware_U3_W2_L2.exe  1124  Load Image     C:\WINDOWS\system32\apphelp.dll                                                        SUCCESS   Image Base: 0x77b40000, Image Size: 0x22000
2:40:08.64225...  Malware_U3_W2_L2.exe  1124  Load Image     C:\WINDOWS\system32\version.dll                                                        SUCCESS   Image Base: 0x77c00000, Image Size: 0x8000
2:40:08.67327...  Malware_U3_W2_L2.exe  1124  Load Image     C:\WINDOWS\system32\advapi32.dll                                                       SUCCESS   Image Base: 0x77dd0000, Image Size: 0x9b000
2:40:08.67366...  Malware_U3_W2_L2.exe  1124  Load Image     C:\WINDOWS\system32\rpcrt4.dll                                                         SUCCESS   Image Base: 0x77e70000, Image Size: 0x92000
2:40:08.67401...  Malware_U3_W2_L2.exe  1124  Load Image     C:\WINDOWS\system32\secur32.dll                                                        SUCCESS   Image Base: 0x77fe0000, Image Size: 0x11000
2:40:08.67983...  Malware_U3_W2_L2.exe  1124  Process Create C:\WINDOWS\system32\svchost.exe                                                        SUCCESS   PID: 3608, Command line: "C:\WINDOWS\system32\svchost.exe"
2:40:09.19699...  Malware_U3_W2_L2.exe  1124  Process Profiling                                                                                     SUCCESS   User Time: 0.0156250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 282,624, Working Set:
2:40:09.69549...  Malware_U3_W2_L2.exe  1124  Thread Exit                                                                                           SUCCESS   Thread ID: 2868, User Time: 0.0000000, Kernel Time: 0.0781250
2:40:09.69585...  Malware_U3_W2_L2.exe  1124  Process Exit                                                                                          SUCCESS   Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0625000 seconds, Private Bytes: 274,432,
```

Con filtri (nome malware e attività processi e thread)

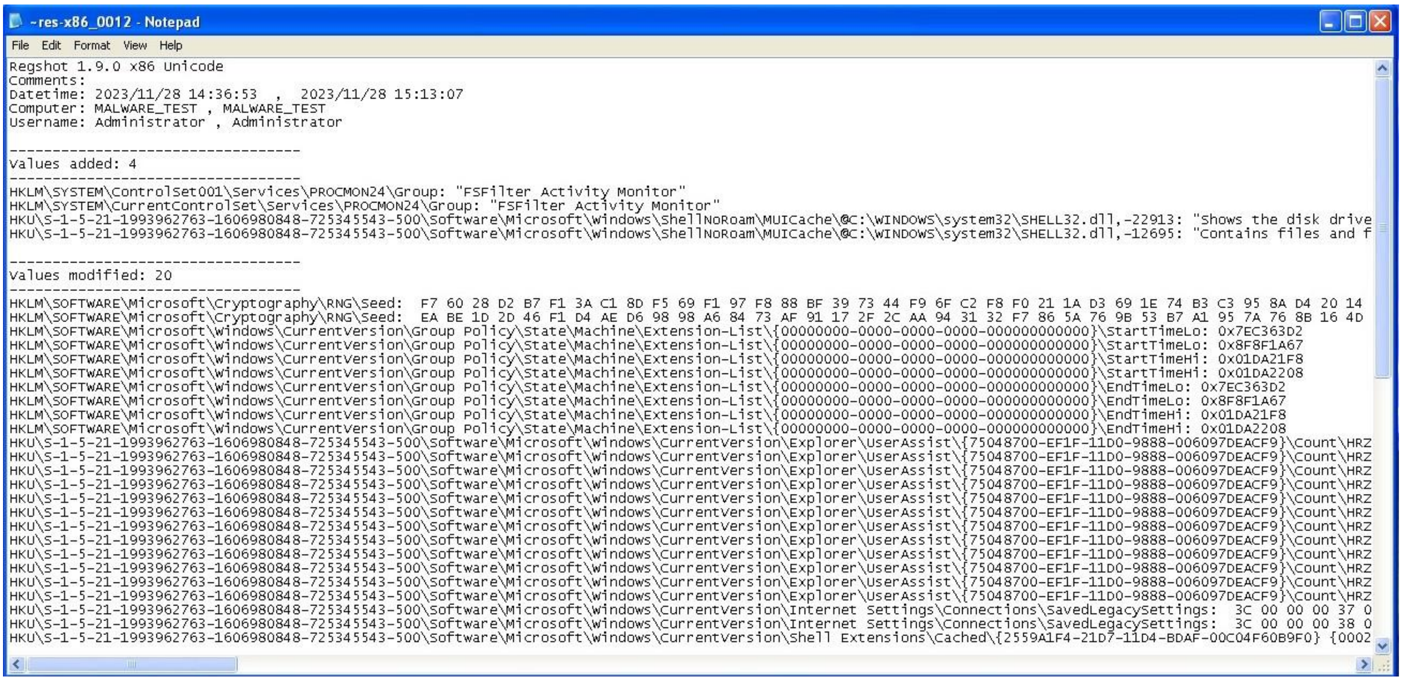
Come possiamo notare da Procmon il malware risulta eseguito ("process start", prima riga) e tra le varie righe si scorge un malware di tipo "svchost" che può eseguire attività dannose come raccolta di informazioni sensibili, installazione di altri componenti del malware ed essere utilizzato come vettore di infezione cercando di infiltrarsi in altri sistemi o dispositivi e andare a gestire anche le connessioni di rete



```
Process            CPU  Private Bytes  Working Set  PID   Description                     Company Name
alg.exe                      1,112 K      3,448 K   2392 Application Layer Gateway S...  Microsoft Corporation
cmd.exe                      1,920 K      2,340 K    488 Windows Command Processor       Microsoft Corporation
cmd.exe                      1,920 K      2,340 K   1588 Windows Command Processor       Microsoft Corporation
csrss.exe                    1,756 K      3,580 K    616 Client Server Runtime Process   Microsoft Corporation
explorer.exe                19,752 K      2,944 K   1664 Windows Explorer                Microsoft Corporation
IEXPLORE.EXE                 1,888 K      4,840 K   1568 Internet Explorer               Microsoft Corporation
IPROSetMonitor.exe             472 K      1,980 K   1560 Intel® PROSet Monitoring S...   Intel Corporation
lsass.exe                    3,776 K      5,936 K    696 LSA Shell (Export Version)      Microsoft Corporation
mm.exe                      59,900 K     59,296 K   3376 MultiMon                        Resplendence Software Pr...
services.exe                 1,652 K      3,280 K    684 Services and Controller app     Microsoft Corporation
smss.exe                       168 K        388 K    340 Windows NT Session Mana...      Microsoft Corporation
spoolsv.exe                  4,028 K      6,600 K   1440 Spooler SubSystem App           Microsoft Corporation
svchost.exe                    864 K      2,204 K   2624 Generic Host Process for Wi...  Microsoft Corporation
svchost.exe                    864 K      2,296 K    124 Generic Host Process for Wi...  Microsoft Corporation
svchost.exe                  1,644 K      4,288 K   1212 Generic Host Process for Wi...  Microsoft Corporation
svchost.exe                  1,268 K      3,440 K   1148 Generic Host Process for Wi...  Microsoft Corporation
svchost.exe                  3,012 K      4,740 K    924 Generic Host Process for Wi...  Microsoft Corporation
svchost.exe                  2,072 K      3,060 K    400 Generic Host Process for Wi...  Microsoft Corporation

CPU Usage: 1.56%   Commit Charge: 7.50%   Processes: 32   Physical Usage: 30.24%
```

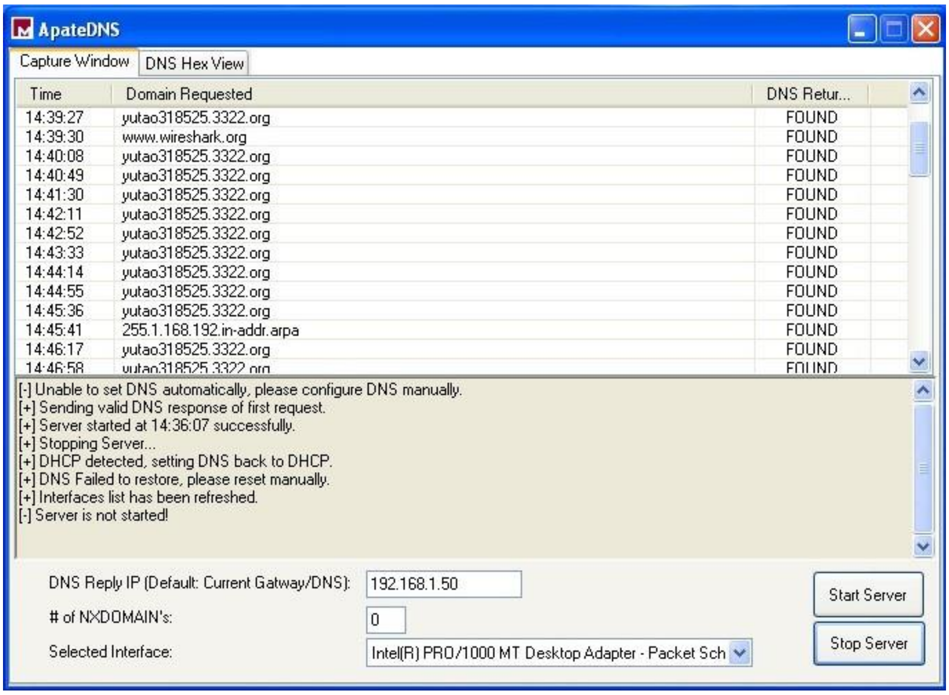
"Svchost" rilevato anche su process explorer

Altri strumenti utilizzati sono **Regshot**, un tool che permette di paragonare due istantanee delle chiavi di registro salvate in due momenti separati tra di loro e qui possiamo osservare la modifica che il malware ha apportato alle chiavi di registro



```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2023/11/28 14:36:53  ,  2023/11/28 15:13:07
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

----------------------------------
Values added: 4
----------------------------------
HKLM\SYSTEM\ControlSet001\Services\PROCMON24\Group: "FSFilter Activity Monitor"
HKLM\SYSTEM\CurrentControlSet\Services\PROCMON24\Group: "FSFilter Activity Monitor"
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\SHELL32.dll,-22913: "Shows the disk drive
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\SHELL32.dll,-12695: "Contains files and f

----------------------------------
Values modified: 20
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  F7 60 28 D2 B7 F1 3A C1 8D F5 69 F1 97 F8 88 BF 39 73 44 F9 6F C2 F8 F0 21 1A D3 69 1E 74 B3 C3 95 8A D4 20 14
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  EA BE 1D 2D 46 F1 D4 AE D6 98 98 A6 84 73 AF 91 17 2F 2C AA 94 31 32 F7 86 5A 76 9B 53 B7 A1 95 7A 76 8B 16 4D
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-000000000000}\StartTimeLo: 0x7EC363D2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-000000000000}\StartTimeLo: 0x8F8F1A67
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-000000000000}\StartTimeHi: 0x01DA21F8
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-000000000000}\StartTimeHi: 0x01DA2208
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-000000000000}\EndTimeLo: 0x7EC363D2
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-000000000000}\EndTimeLo: 0x8F8F1A67
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-000000000000}\EndTimeHi: 0x01DA21F8
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\State\Machine\Extension-List\{00000000-0000-0000-0000-000000000000}\EndTimeHi: 0x01DA2208
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZ
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings:  3C 00 00 00 37 0
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings:  3C 00 00 00 38 0
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{2559A1F4-21D7-11D4-BDAF-00C04F60B9F0} {0002
```

Quindi abbiamo utilizzato **ApateDNS** che simula un server DNS e può intercettare tutte le richieste effettuate dai malware verso i domini Internet

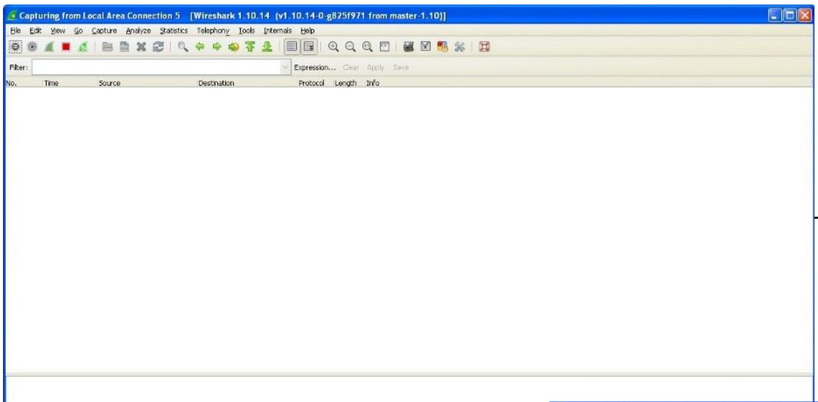


Time	Domain Requested	DNS Retur...
14:39:27	yutao318525.3322.org	FOUND
14:39:30	www.wireshark.org	FOUND
14:40:08	yutao318525.3322.org	FOUND
14:40:49	yutao318525.3322.org	FOUND
14:41:30	yutao318525.3322.org	FOUND
14:42:11	yutao318525.3322.org	FOUND
14:42:52	yutao318525.3322.org	FOUND
14:43:33	yutao318525.3322.org	FOUND
14:44:14	yutao318525.3322.org	FOUND
14:44:55	yutao318525.3322.org	FOUND
14:45:36	yutao318525.3322.org	FOUND
14:45:41	255.1.168.192.in-addr.arpa	FOUND
14:46:17	yutao318525.3322.org	FOUND
14:46:58	yutao318525.3322.org	FOUND

```
[-] Unable to set DNS automatically, please configure DNS manually.
[+] Sending valid DNS response of first request.
[+] Server started at 14:36:07 successfully.
[+] Stopping Server...
[+] DHCP detected, setting DNS back to DHCP.
[+] DNS Failed to restore, please reset manually.
[+] Interfaces list has been refreshed.
[-] Server is not started!
```

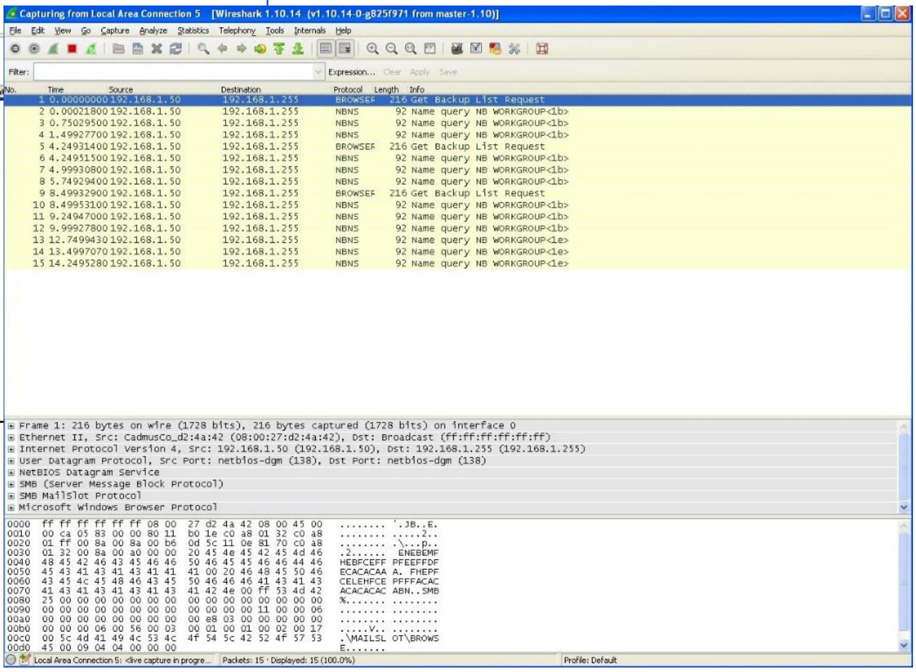
DNS Reply IP (Default: Current Gatway/DNS): 192.168.1.50
# of NXDOMAIN's: 0
Selected Interface: Intel(R) PRO/1000 MT Desktop Adapter - Packet Sch

Ed infine **wireshark**, uno strumento di analisi del traffico di rete che, come possiamo vedere dalla figura sottostante, ha rilevato attività solo una volta eseguito il malware



Prima dell'esecuzione del malware

Dopo l'esecuzione del malware



```
No.  Time       Source         Destination     Protocol Length Info
   1 0.00000000 192.168.1.50   192.168.1.255   BROWSER   216 Get Backup List Request
   2 0.00021800 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1b>
   3 0.75029500 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1b>
   4 1.49927700 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1b>
   5 4.24931400 192.168.1.50   192.168.1.255   BROWSER   216 Get Backup List Request
   6 4.24951500 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1b>
   7 4.99930800 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1b>
   8 5.74929400 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1b>
   9 8.49932900 192.168.1.50   192.168.1.255   BROWSER   216 Get Backup List Request
  10 8.49953100 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1b>
  11 9.24947000 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1b>
  12 9.99927800 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1b>
  13 12.7499430 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1e>
  14 13.4997070 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1e>
  15 14.2495280 192.168.1.50   192.168.1.255   NBNS       92 Name query NB WORKGROUP<1e>
```

```
⊞ Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
⊞ Ethernet II, Src: CadmusCo_d2:4a:42 (08:00:27:d2:4a:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 192.168.1.50 (192.168.1.50), Dst: 192.168.1.255 (192.168.1.255)
⊞ User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
⊞ NetBIOS Datagram Service
⊞ SMB (Server Message Block Protocol)
⊞ SMB MailSlot Protocol
⊞ Microsoft Windows Browser Protocol
```

```
0000  ff ff ff ff ff ff 08 00  27 d2 4a 42 08 00 45 00   ........ '.JB..E.
0010  00 ca 05 83 00 00 80 11  b0 1e c0 a8 01 32 c0 a8   ........ .....2..
0020  01 ff 00 8a 00 8a 00 b6  0d 5c 11 0e 81 70 c0 a8   ........ .\...p..
0030  01 32 00 8a 00 a0 00 00  20 45 4e 45 42 45 4d 46   .2......  ENEBEMF
0040  48 45 42 46 43 45 46 46  50 46 45 45 46 46 44 46   HEBFCEFF PFEEFFDF
0050  45 43 41 43 41 43 41 41  41 00 20 46 48 45 50 46   ECACACAA A. FHEPF
0060  43 45 4c 45 48 46 43 45  50 46 46 46 41 43 41 43   CELEHFCE PFFFACAC
0070  41 43 41 43 41 43 41 43  41 42 4e 00 ff 53 4d 42   ACACACAC ABN..SMB
0080  25 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   %....... ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 11 00 00 06   ........ ........
00a0  00 00 00 00 00 00 00 00  00 e8 03 00 00 00 00 00   ........ ........
00b0  00 00 00 06 00 56 00 03  00 01 00 01 00 02 00 17   .....V.. ........
00c0  00 5c 4d 41 49 4c 53 4c  4f 54 5c 42 52 4f 57 53   .\MAILSL OT\BROWS
00d0  45 00 09 04 04 00 00 00                            E.......
```

Local Area Connection 5: <live capture in progre... Packets: 15 · Displayed: 15 (100.0%)