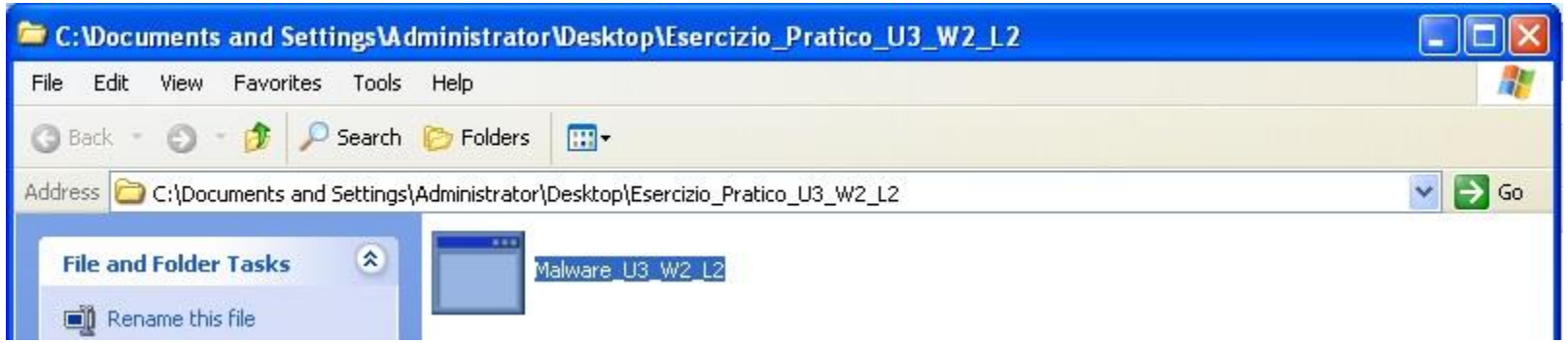
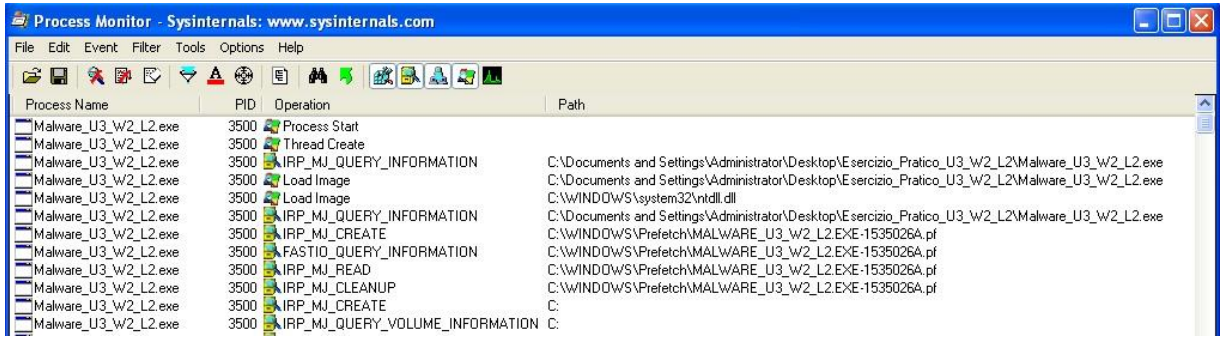
Analisi dinamica basica

Malware_U3_W2_L2

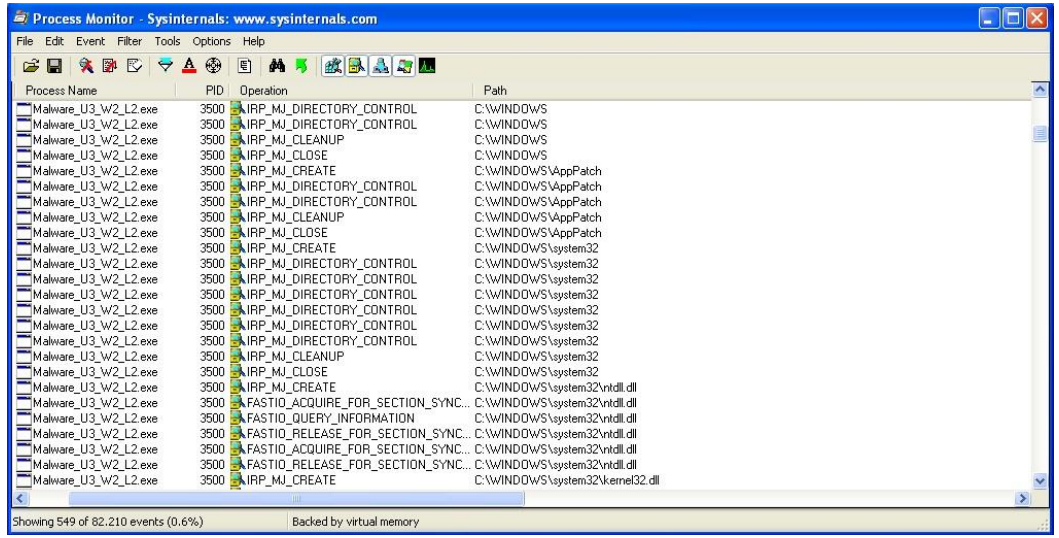
Orlando Tangari



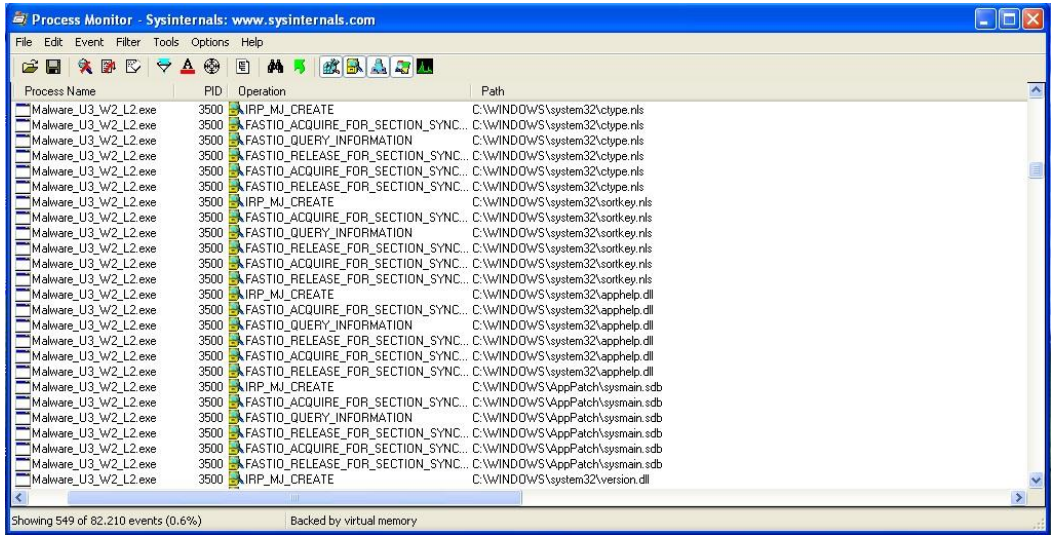
Attraverso il tool Regshot, come mostrato nell'immagine in alto, si effettua un primo shot per verificare lo stato delle chiavi di registro e, successivamente, si avvia Malware_U3_W2_L2, come mostrato nell'immagine in basso.



```
Process Name          PID  Operation                        Path
Malware_U3_W2_L2.exe  3500 Process Start
Malware_U3_W2_L2.exe  3500 Thread Create
Malware_U3_W2_L2.exe  3500 IRP_MJ_QUERY_INFORMATION         C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_U3_W2_L2.exe  3500 Load Image                       C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_U3_W2_L2.exe  3500 Load Image                       C:\WINDOWS\system32\ntdll.dll
Malware_U3_W2_L2.exe  3500 IRP_MJ_QUERY_INFORMATION         C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                    C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
Malware_U3_W2_L2.exe  3500 FASTIO_QUERY_INFORMATION         C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
Malware_U3_W2_L2.exe  3500 IRP_MJ_READ                      C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
Malware_U3_W2_L2.exe  3500 IRP_MJ_CLEANUP                   C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                    C:
Malware_U3_W2_L2.exe  3500 IRP_MJ_QUERY_VOLUME_INFORMATION  C:
```

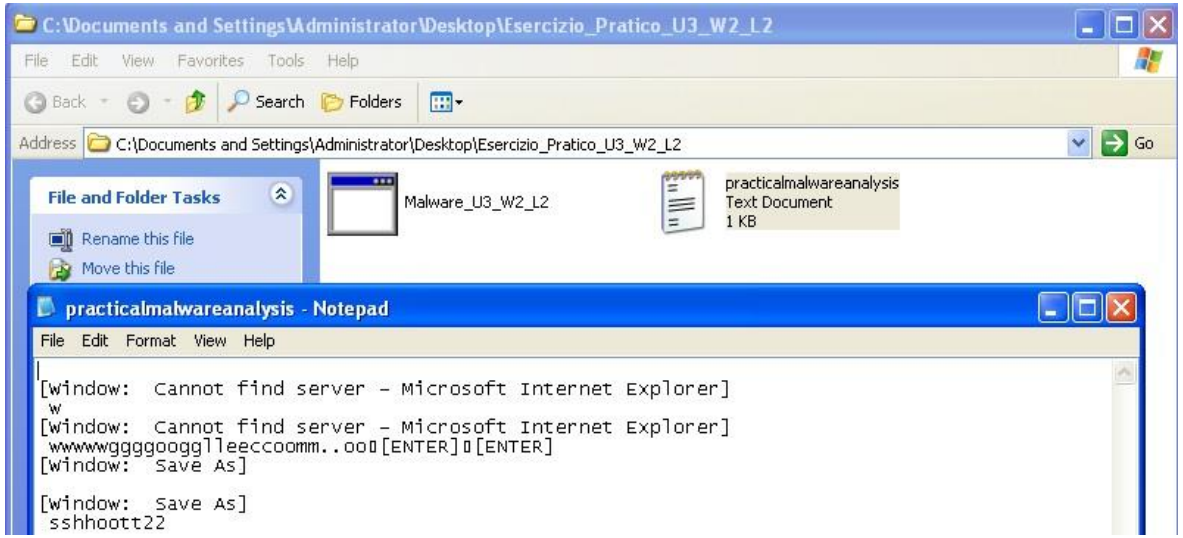


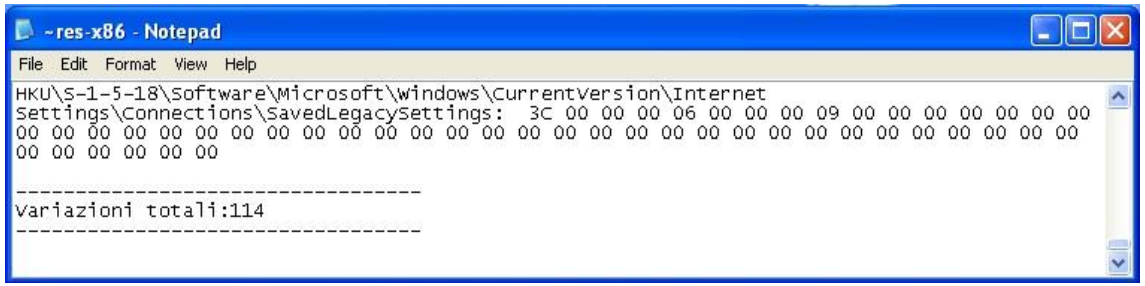
```
Process Name          PID  Operation                         Path
Malware_U3_W2_L2.exe  3500 IRP_MJ_DIRECTORY_CONTROL          C:\WINDOWS
Malware_U3_W2_L2.exe  3500 IRP_MJ_DIRECTORY_CONTROL          C:\WINDOWS
Malware_U3_W2_L2.exe  3500 IRP_MJ_CLEANUP                    C:\WINDOWS
Malware_U3_W2_L2.exe  3500 IRP_MJ_CLOSE                      C:\WINDOWS
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                     C:\WINDOWS\AppPatch
Malware_U3_W2_L2.exe  3500 IRP_MJ_DIRECTORY_CONTROL          C:\WINDOWS\AppPatch
Malware_U3_W2_L2.exe  3500 IRP_MJ_DIRECTORY_CONTROL          C:\WINDOWS\AppPatch
Malware_U3_W2_L2.exe  3500 IRP_MJ_CLEANUP                    C:\WINDOWS\AppPatch
Malware_U3_W2_L2.exe  3500 IRP_MJ_CLOSE                      C:\WINDOWS\AppPatch
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                     C:\WINDOWS\system32
Malware_U3_W2_L2.exe  3500 IRP_MJ_DIRECTORY_CONTROL          C:\WINDOWS\system32
Malware_U3_W2_L2.exe  3500 IRP_MJ_DIRECTORY_CONTROL          C:\WINDOWS\system32
Malware_U3_W2_L2.exe  3500 IRP_MJ_DIRECTORY_CONTROL          C:\WINDOWS\system32
Malware_U3_W2_L2.exe  3500 IRP_MJ_DIRECTORY_CONTROL          C:\WINDOWS\system32
Malware_U3_W2_L2.exe  3500 IRP_MJ_DIRECTORY_CONTROL          C:\WINDOWS\system32
Malware_U3_W2_L2.exe  3500 IRP_MJ_DIRECTORY_CONTROL          C:\WINDOWS\system32
Malware_U3_W2_L2.exe  3500 IRP_MJ_CLEANUP                    C:\WINDOWS\system32
Malware_U3_W2_L2.exe  3500 IRP_MJ_CLOSE                      C:\WINDOWS\system32
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                     C:\WINDOWS\system32\ntdll.dll
Malware_U3_W2_L2.exe  3500 FASTIO_ACQUIRE_FOR_SECTION_SYNC... C:\WINDOWS\system32\ntdll.dll
Malware_U3_W2_L2.exe  3500 FASTIO_QUERY_INFORMATION          C:\WINDOWS\system32\ntdll.dll
Malware_U3_W2_L2.exe  3500 FASTIO_RELEASE_FOR_SECTION_SYNC... C:\WINDOWS\system32\ntdll.dll
Malware_U3_W2_L2.exe  3500 FASTIO_ACQUIRE_FOR_SECTION_SYNC... C:\WINDOWS\system32\ntdll.dll
Malware_U3_W2_L2.exe  3500 FASTIO_RELEASE_FOR_SECTION_SYNC... C:\WINDOWS\system32\ntdll.dll
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                     C:\WINDOWS\system32\kernel32.dll

Showing 549 of 82.210 events (0.6%)        Backed by virtual memory
```



```
Process Name          PID  Operation                         Path
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                     C:\WINDOWS\system32\ctype.nls
Malware_U3_W2_L2.exe  3500 FASTIO_ACQUIRE_FOR_SECTION_SYNC... C:\WINDOWS\system32\ctype.nls
Malware_U3_W2_L2.exe  3500 FASTIO_QUERY_INFORMATION          C:\WINDOWS\system32\ctype.nls
Malware_U3_W2_L2.exe  3500 FASTIO_RELEASE_FOR_SECTION_SYNC... C:\WINDOWS\system32\ctype.nls
Malware_U3_W2_L2.exe  3500 FASTIO_ACQUIRE_FOR_SECTION_SYNC... C:\WINDOWS\system32\ctype.nls
Malware_U3_W2_L2.exe  3500 FASTIO_RELEASE_FOR_SECTION_SYNC... C:\WINDOWS\system32\ctype.nls
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                     C:\WINDOWS\system32\sortkey.nls
Malware_U3_W2_L2.exe  3500 FASTIO_ACQUIRE_FOR_SECTION_SYNC... C:\WINDOWS\system32\sortkey.nls
Malware_U3_W2_L2.exe  3500 FASTIO_QUERY_INFORMATION          C:\WINDOWS\system32\sortkey.nls
Malware_U3_W2_L2.exe  3500 FASTIO_RELEASE_FOR_SECTION_SYNC... C:\WINDOWS\system32\sortkey.nls
Malware_U3_W2_L2.exe  3500 FASTIO_ACQUIRE_FOR_SECTION_SYNC... C:\WINDOWS\system32\sortkey.nls
Malware_U3_W2_L2.exe  3500 FASTIO_RELEASE_FOR_SECTION_SYNC... C:\WINDOWS\system32\sortkey.nls
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                     C:\WINDOWS\system32\apphelp.dll
Malware_U3_W2_L2.exe  3500 FASTIO_ACQUIRE_FOR_SECTION_SYNC... C:\WINDOWS\system32\apphelp.dll
Malware_U3_W2_L2.exe  3500 FASTIO_QUERY_INFORMATION          C:\WINDOWS\system32\apphelp.dll
Malware_U3_W2_L2.exe  3500 FASTIO_RELEASE_FOR_SECTION_SYNC... C:\WINDOWS\system32\apphelp.dll
Malware_U3_W2_L2.exe  3500 FASTIO_ACQUIRE_FOR_SECTION_SYNC... C:\WINDOWS\system32\apphelp.dll
Malware_U3_W2_L2.exe  3500 FASTIO_RELEASE_FOR_SECTION_SYNC... C:\WINDOWS\system32\apphelp.dll
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                     C:\WINDOWS\AppPatch\sysmain.sdb
Malware_U3_W2_L2.exe  3500 FASTIO_ACQUIRE_FOR_SECTION_SYNC... C:\WINDOWS\AppPatch\sysmain.sdb
Malware_U3_W2_L2.exe  3500 FASTIO_QUERY_INFORMATION          C:\WINDOWS\AppPatch\sysmain.sdb
Malware_U3_W2_L2.exe  3500 FASTIO_RELEASE_FOR_SECTION_SYNC... C:\WINDOWS\AppPatch\sysmain.sdb
Malware_U3_W2_L2.exe  3500 FASTIO_ACQUIRE_FOR_SECTION_SYNC... C:\WINDOWS\AppPatch\sysmain.sdb
Malware_U3_W2_L2.exe  3500 FASTIO_RELEASE_FOR_SECTION_SYNC... C:\WINDOWS\AppPatch\sysmain.sdb
Malware_U3_W2_L2.exe  3500 IRP_MJ_CREATE                     C:\WINDOWS\system32\version.dll

Showing 549 of 82.210 events (0.6%)        Backed by virtual memory
```

Attraverso il tool avanzato di Windows, Process Monitor, si monitorano i processi ed i thread attivi create dal malware in esecuzione. Nella prima immagine in alto a sinistra, si nota, alla quinta riga, come si carica nella cartella system32 e nella seconda immagine in alto a destra, come assume il controllo di essa e di alcune librerie. Scorrendo ancora l’elenco di *procmon*, come si nota nell’immagine in basso, si nota come, il malware, acquisisca informazioni da softkey.nls, presumendo che esso si un keylogger.





Aprendo il browser Internet Explorer, come mostrato nell'immagine in alto, si inserisce l'URL di google.com per verificare se, il malware, sia proprio un keylogger. Ed aprendo la cartella del malware, si nota, nell'immagine in basso a sinistra, un nuovo file txt, che, aprendolo, mostra effettivamente i tasti digitati per l'URL di Google. Ed, infine, come si nota nell'immagine in basso a destra, dopo il secondo shot effettuato con Regshot e comparato con il primo, si nptano 114 variazioni tra chiavi e valori cancellati e aggiunti.