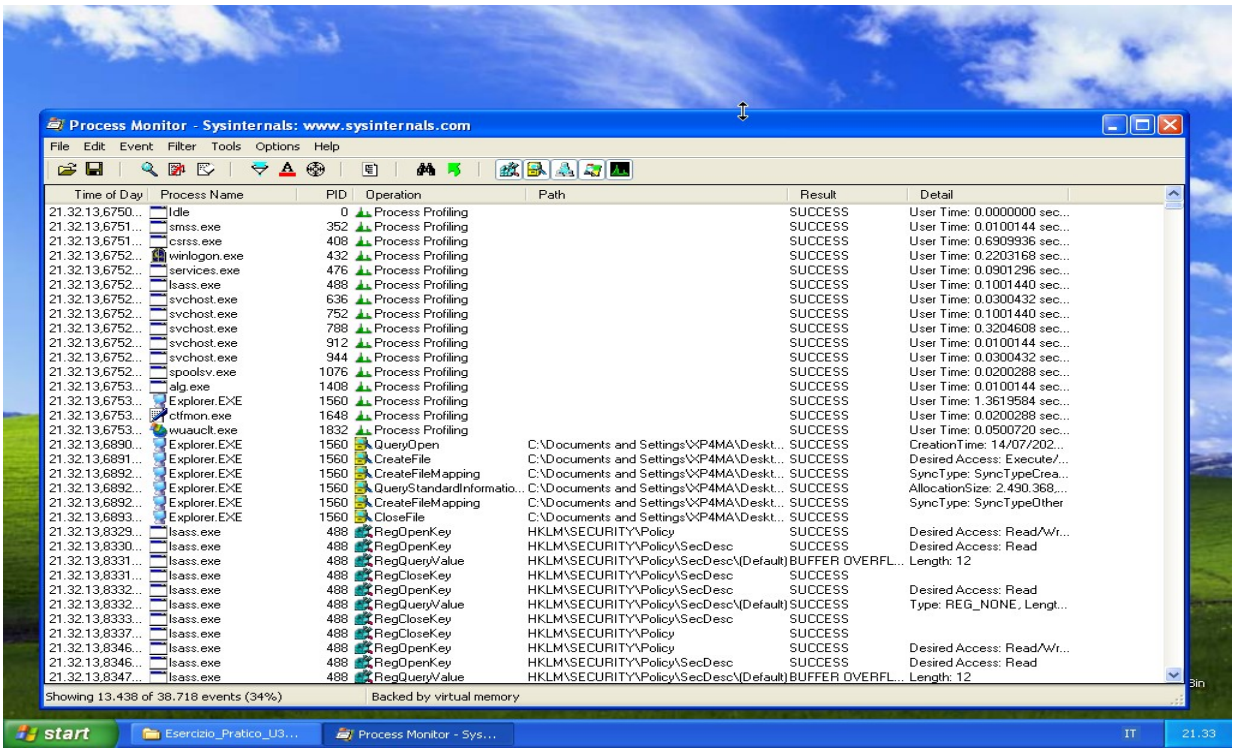
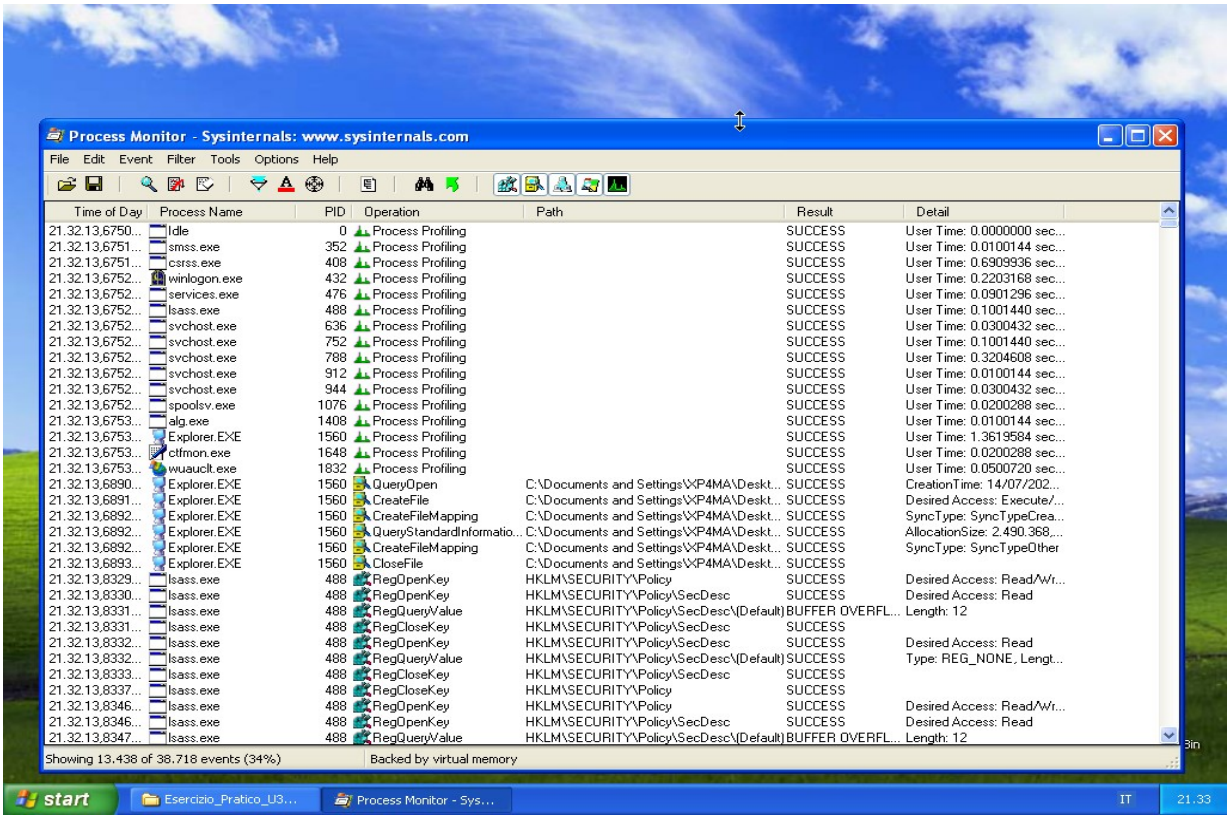
M6 D1

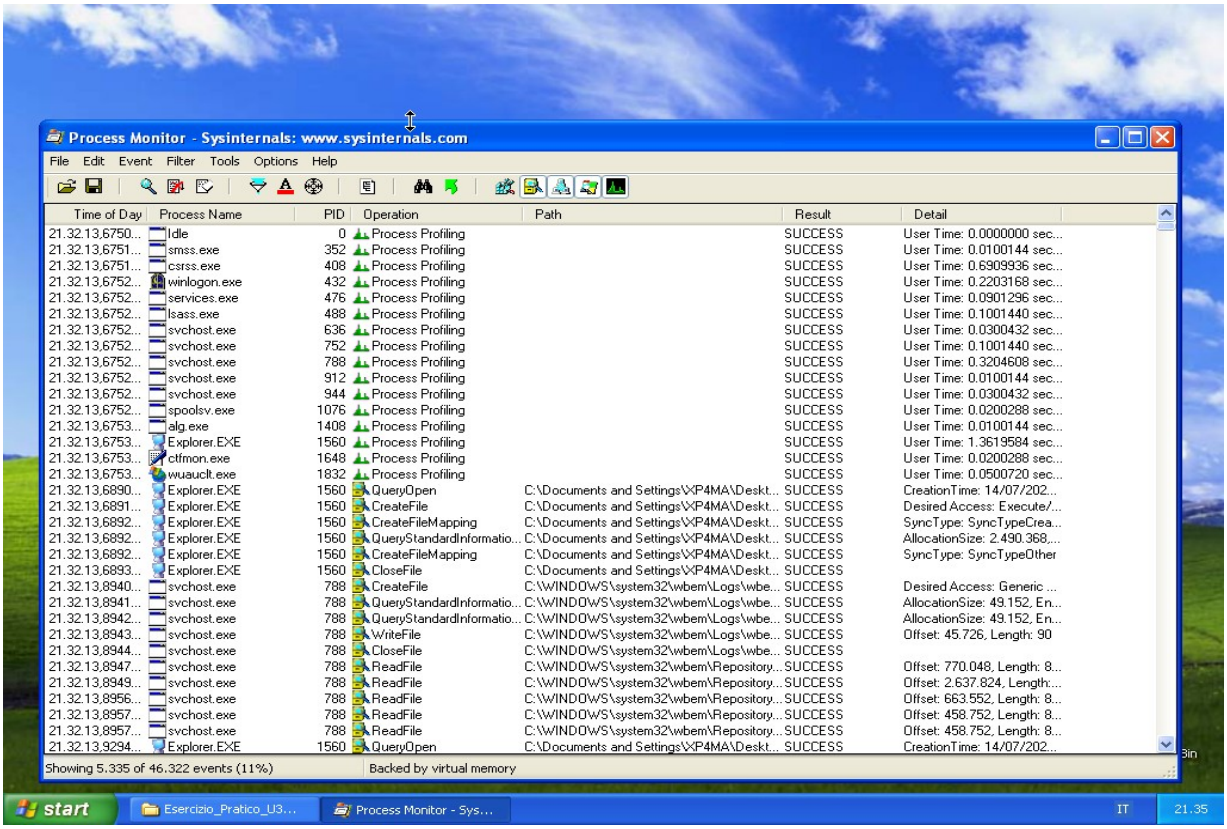
ESERCIZIO 1

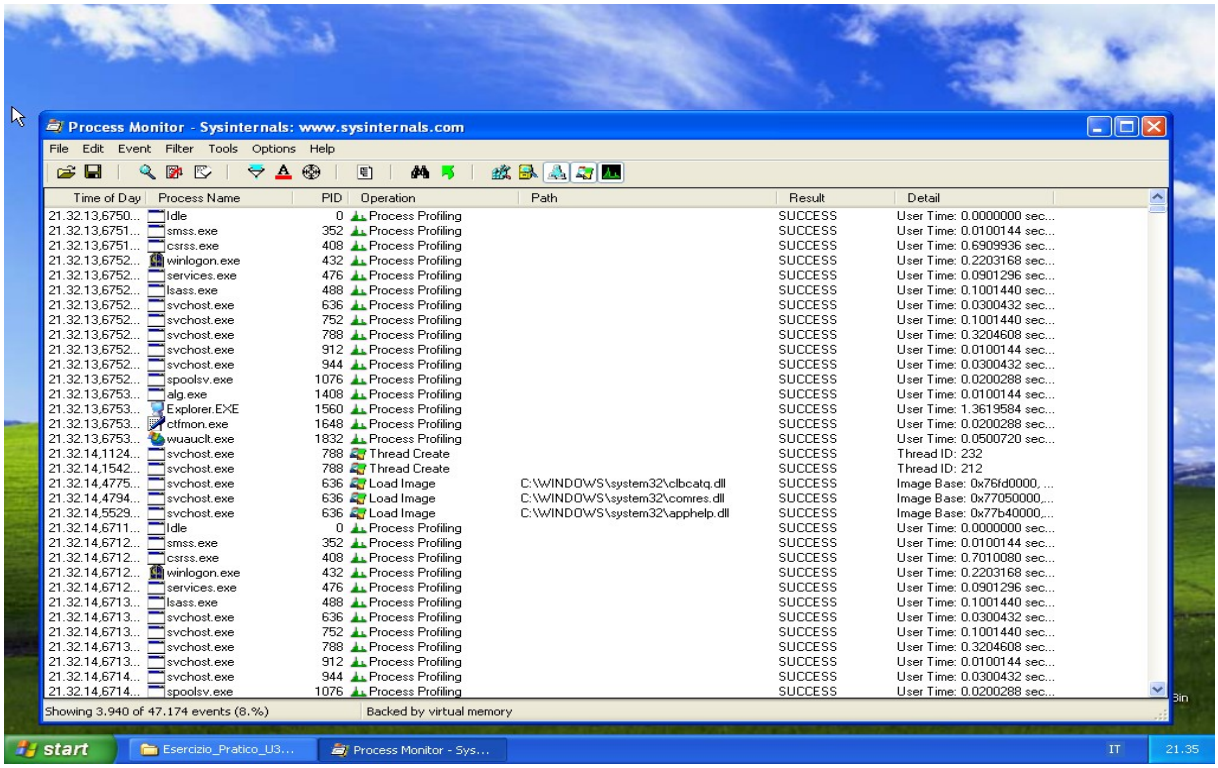
UTILIZZO DEL TOOL PROCMON ---> PROCESS MONITOR

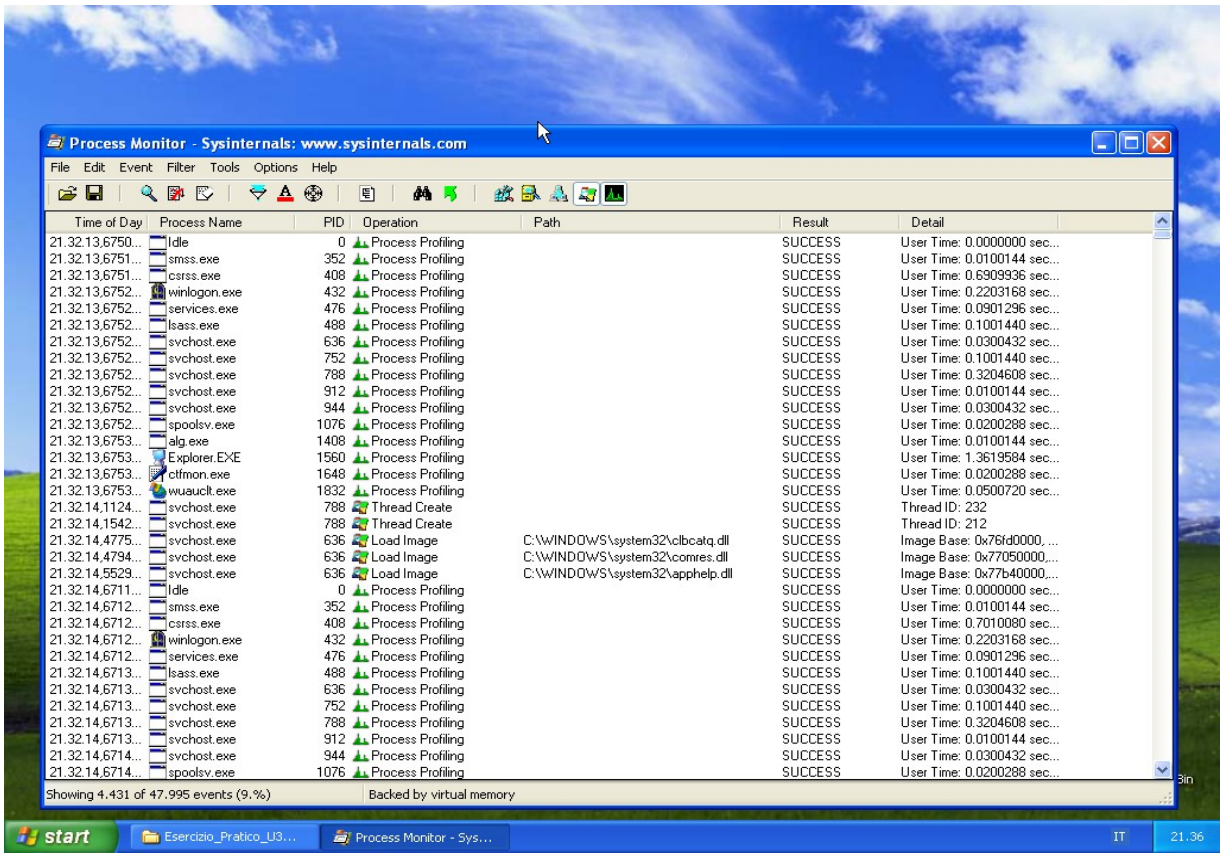
ANALISI PRE ESECUZIONE MALWARE

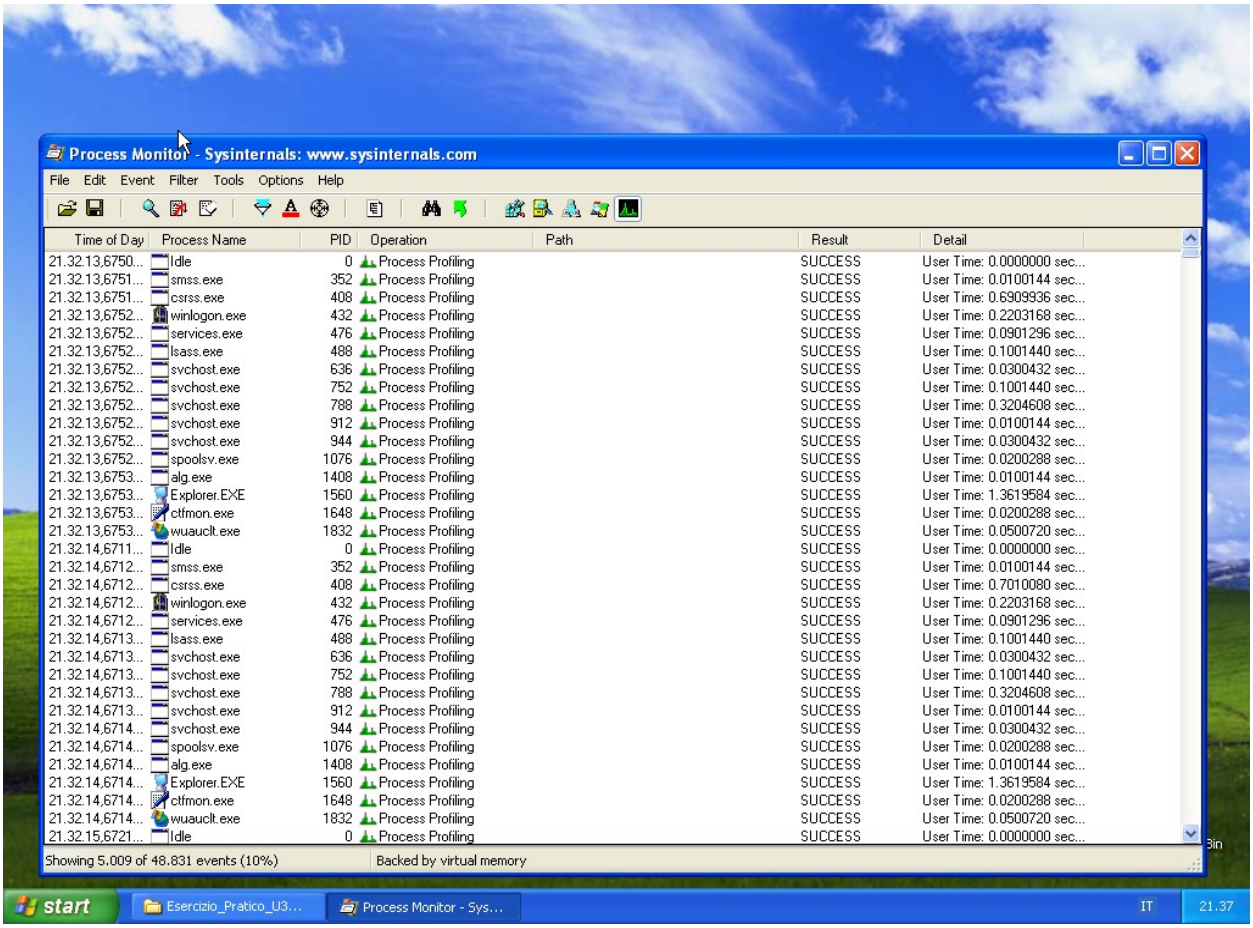





Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result | Detail
21.32.13,6750... Idle 0 Process Profiling SUCCESS User Time: 0.0000000 sec...
21.32.13,6751... smss.exe 352 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6751... csrss.exe 408 Process Profiling SUCCESS User Time: 0.6909936 sec...
21.32.13,6752... winlogon.exe 432 Process Profiling SUCCESS User Time: 0.2203168 sec...
21.32.13,6752... services.exe 476 Process Profiling SUCCESS User Time: 0.0901296 sec...
21.32.13,6752... lsass.exe 488 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.13,6752... svchost.exe 636 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.13,6752... svchost.exe 752 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.13,6752... svchost.exe 788 Process Profiling SUCCESS User Time: 0.3204608 sec...
21.32.13,6752... svchost.exe 912 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6752... svchost.exe 944 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.13,6752... spoolsv.exe 1076 Process Profiling SUCCESS User Time: 0.0200288 sec...
21.32.13,6753... alg.exe 1408 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6753... Explorer.EXE 1560 Process Profiling SUCCESS User Time: 1.3619584 sec...
21.32.13,6753... ctfmon.exe 1648 Process Profiling SUCCESS User Time: 0.0200288 sec...
21.32.13,6753... wuauclt.exe 1832 Process Profiling SUCCESS User Time: 0.0500720 sec...
21.32.13,6890... Explorer.EXE 1560 QueryOpen C:\Documents and Settings\XP4MA\Deskt... SUCCESS CreationTime: 14/07/202...
21.32.13,6891... Explorer.EXE 1560 CreateFile C:\Documents and Settings\XP4MA\Deskt... SUCCESS Desired Access: Execute/...
21.32.13,6892... Explorer.EXE 1560 CreateFileMapping C:\Documents and Settings\XP4MA\Deskt... SUCCESS SyncType: SyncTypeCrea...
21.32.13,6892... Explorer.EXE 1560 QueryStandardInformatio... C:\Documents and Settings\XP4MA\Deskt... SUCCESS AllocationSize: 2.490.368,...
21.32.13,6892... Explorer.EXE 1560 CreateFileMapping C:\Documents and Settings\XP4MA\Deskt... SUCCESS SyncType: SyncTypeOther
21.32.13,6893... Explorer.EXE 1560 CloseFile C:\Documents and Settings\XP4MA\Deskt... SUCCESS
21.32.13,8940... svchost.exe 788 CreateFile C:\WINDOWS\system32\wbem\Logs\wbe... SUCCESS Desired Access: Generic ...
21.32.13,8941... svchost.exe 788 QueryStandardInformatio... C:\WINDOWS\system32\wbem\Logs\wbe... SUCCESS AllocationSize: 49.152, En...
21.32.13,8942... svchost.exe 788 QueryStandardInformatio... C:\WINDOWS\system32\wbem\Logs\wbe... SUCCESS AllocationSize: 49.152, En...
21.32.13,8943... svchost.exe 788 WriteFile C:\WINDOWS\system32\wbem\Logs\wbe... SUCCESS Offset: 45.726, Length: 90
21.32.13,8944... svchost.exe 788 CloseFile C:\WINDOWS\system32\wbem\Logs\wbe... SUCCESS
21.32.13,8947... svchost.exe 788 ReadFile C:\WINDOWS\system32\wbem\Repository... SUCCESS Offset: 770.048, Length: 8...
21.32.13,8949... svchost.exe 788 ReadFile C:\WINDOWS\system32\wbem\Repository... SUCCESS Offset: 2.637.824, Length:...
21.32.13,8956... svchost.exe 788 ReadFile C:\WINDOWS\system32\wbem\Repository... SUCCESS Offset: 663.552, Length: 8...
21.32.13,8957... svchost.exe 788 ReadFile C:\WINDOWS\system32\wbem\Repository... SUCCESS Offset: 458.752, Length: 8...
21.32.13,8957... svchost.exe 788 ReadFile C:\WINDOWS\system32\wbem\Repository... SUCCESS Offset: 458.752, Length: 8...
21.32.13,9294... Explorer.EXE 1560 QueryOpen C:\Documents and Settings\XP4MA\Deskt... SUCCESS CreationTime: 14/07/202...
Showing 5.335 of 46.322 events (11%)
Backed by virtual memory
start
Esercizio_Pratico_U3...
Process Monitor - Sys...
IT
21.35

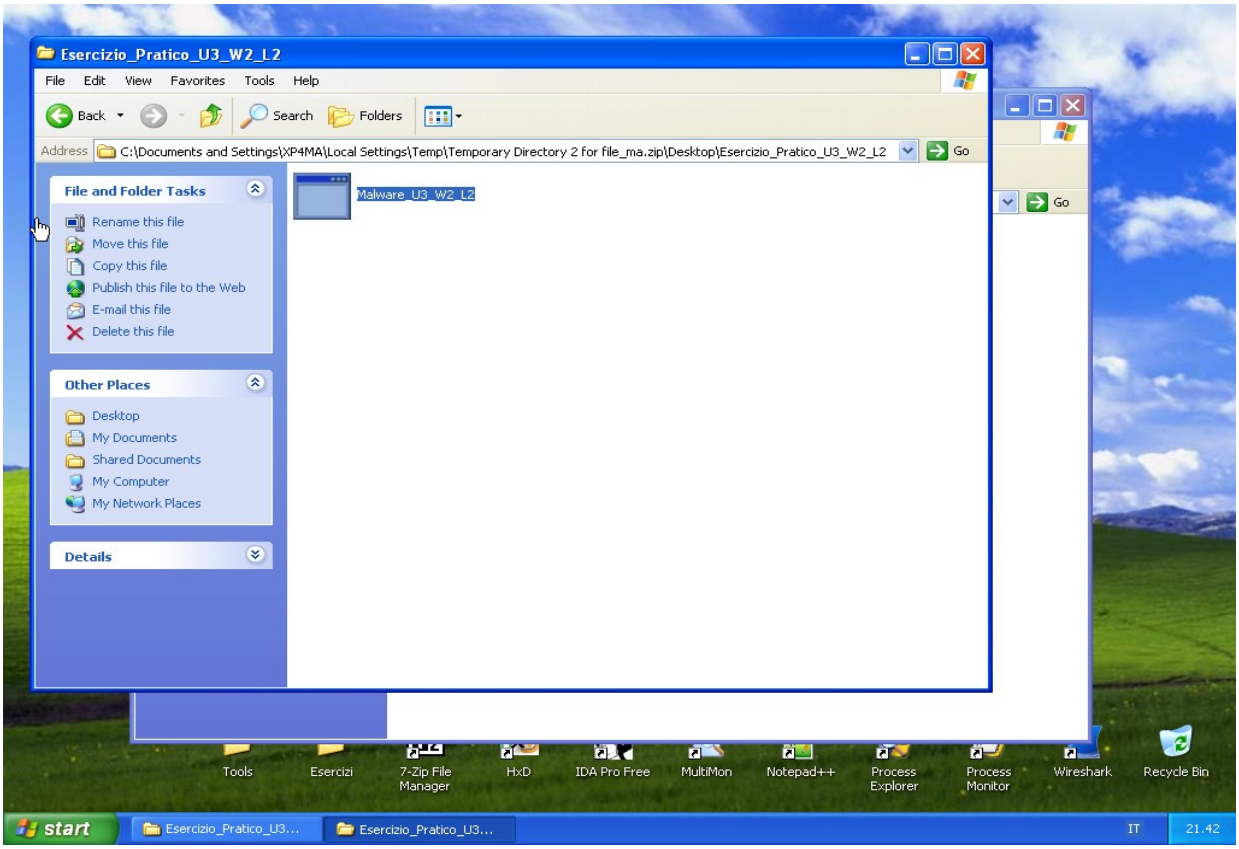

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result | Detail
21.32.13,6750... Idle 0 Process Profiling SUCCESS User Time: 0.0000000 sec...
21.32.13,6751... smss.exe 352 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6751... csrss.exe 408 Process Profiling SUCCESS User Time: 0.6909936 sec...
21.32.13,6752... winlogon.exe 432 Process Profiling SUCCESS User Time: 0.2203168 sec...
21.32.13,6752... services.exe 476 Process Profiling SUCCESS User Time: 0.0901296 sec...
21.32.13,6752... lsass.exe 488 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.13,6752... svchost.exe 636 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.13,6752... svchost.exe 752 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.13,6752... svchost.exe 788 Process Profiling SUCCESS User Time: 0.3204608 sec...
21.32.13,6752... svchost.exe 912 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6752... svchost.exe 944 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.13,6752... spoolsv.exe 1076 Process Profiling SUCCESS User Time: 0.0200288 sec...
21.32.13,6753... alg.exe 1408 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6753... Explorer.EXE 1560 Process Profiling SUCCESS User Time: 1.3619584 sec...
21.32.13,6753... ctfmon.exe 1648 Process Profiling SUCCESS User Time: 0.0200288 sec...
21.32.13,6753... wuauclt.exe 1832 Process Profiling SUCCESS User Time: 0.0500720 sec...
21.32.14,1124... svchost.exe 788 Thread Create SUCCESS Thread ID: 232
21.32.14,1542... svchost.exe 788 Thread Create SUCCESS Thread ID: 212
21.32.14,4775... svchost.exe 636 Load Image C:\WINDOWS\system32\clbcatq.dll SUCCESS Image Base: 0x76fd0000, ...
21.32.14,4794... svchost.exe 636 Load Image C:\WINDOWS\system32\comres.dll SUCCESS Image Base: 0x77050000,...
21.32.14,5529... svchost.exe 636 Load Image C:\WINDOWS\system32\apphelp.dll SUCCESS Image Base: 0x77b40000,...
21.32.14,6711... Idle 0 Process Profiling SUCCESS User Time: 0.0000000 sec...
21.32.14,6712... smss.exe 352 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.14,6712... csrss.exe 408 Process Profiling SUCCESS User Time: 0.7010080 sec...
21.32.14,6712... winlogon.exe 432 Process Profiling SUCCESS User Time: 0.2203168 sec...
21.32.14,6712... services.exe 476 Process Profiling SUCCESS User Time: 0.0901296 sec...
21.32.14,6713... lsass.exe 488 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.14,6713... svchost.exe 636 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.14,6713... svchost.exe 752 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.14,6713... svchost.exe 788 Process Profiling SUCCESS User Time: 0.3204608 sec...
21.32.14,6713... svchost.exe 912 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.14,6714... svchost.exe 944 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.14,6714... spoolsv.exe 1076 Process Profiling SUCCESS User Time: 0.0200288 sec...
Showing 3.940 of 47.174 events (8.%)
Backed by virtual memory
start
Esercizio_Pratico_U3...
Process Monitor - Sys...
IT
21.35

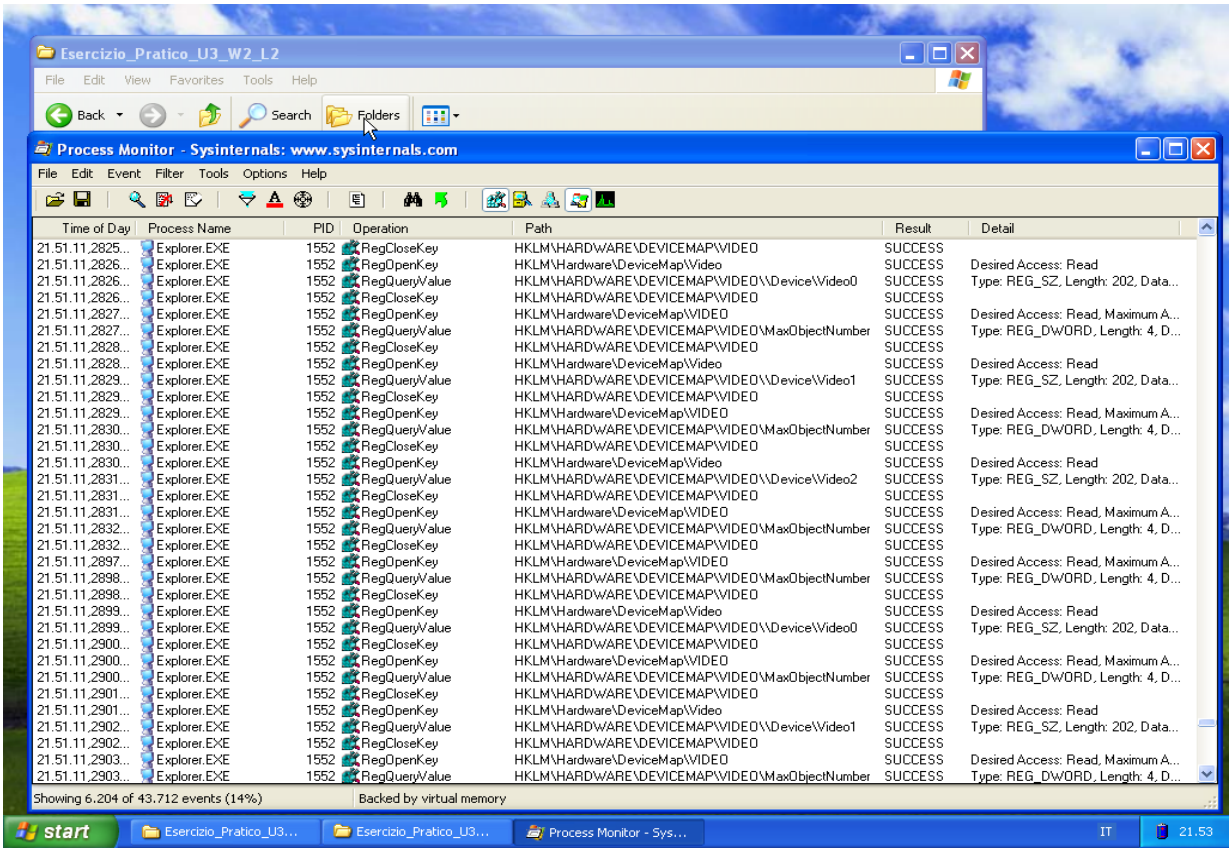

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result | Detail
21.32.13,6750... Idle 0 Process Profiling SUCCESS User Time: 0.0000000 sec...
21.32.13,6751... smss.exe 352 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6751... csrss.exe 408 Process Profiling SUCCESS User Time: 0.6909936 sec...
21.32.13,6752... winlogon.exe 432 Process Profiling SUCCESS User Time: 0.2203168 sec...
21.32.13,6752... services.exe 476 Process Profiling SUCCESS User Time: 0.0901296 sec...
21.32.13,6752... lsass.exe 488 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.13,6752... svchost.exe 636 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.13,6752... svchost.exe 752 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.13,6752... svchost.exe 788 Process Profiling SUCCESS User Time: 0.3204608 sec...
21.32.13,6752... svchost.exe 912 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6752... svchost.exe 944 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.13,6752... spoolsv.exe 1076 Process Profiling SUCCESS User Time: 0.0200288 sec...
21.32.13,6753... alg.exe 1408 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6753... Explorer.EXE 1560 Process Profiling SUCCESS User Time: 1.3619584 sec...
21.32.13,6753... ctfmon.exe 1648 Process Profiling SUCCESS User Time: 0.0200288 sec...
21.32.13,6753... wuauclt.exe 1832 Process Profiling SUCCESS User Time: 0.0500720 sec...
21.32.14,1124... svchost.exe 788 Thread Create SUCCESS Thread ID: 232
21.32.14,1542... svchost.exe 788 Thread Create SUCCESS Thread ID: 212
21.32.14,4775... svchost.exe 636 Load Image C:\WINDOWS\system32\clbcatq.dll SUCCESS Image Base: 0x76fd0000, ...
21.32.14,4794... svchost.exe 636 Load Image C:\WINDOWS\system32\comres.dll SUCCESS Image Base: 0x77050000,...
21.32.14,5529... svchost.exe 636 Load Image C:\WINDOWS\system32\apphelp.dll SUCCESS Image Base: 0x77b40000,...
21.32.14,6711... Idle 0 Process Profiling SUCCESS User Time: 0.0000000 sec...
21.32.14,6712... smss.exe 352 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.14,6712... csrss.exe 408 Process Profiling SUCCESS User Time: 0.7010080 sec...
21.32.14,6712... winlogon.exe 432 Process Profiling SUCCESS User Time: 0.2203168 sec...
21.32.14,6712... services.exe 476 Process Profiling SUCCESS User Time: 0.0901296 sec...
21.32.14,6713... lsass.exe 488 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.14,6713... svchost.exe 636 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.14,6713... svchost.exe 752 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.14,6713... svchost.exe 788 Process Profiling SUCCESS User Time: 0.3204608 sec...
21.32.14,6713... svchost.exe 912 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.14,6714... svchost.exe 944 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.14,6714... spoolsv.exe 1076 Process Profiling SUCCESS User Time: 0.0200288 sec...
Showing 4.431 of 47.995 events (9.%)
Backed by virtual memory
start
Esercizio_Pratico_U3...
Process Monitor - Sys...
IT
21.36

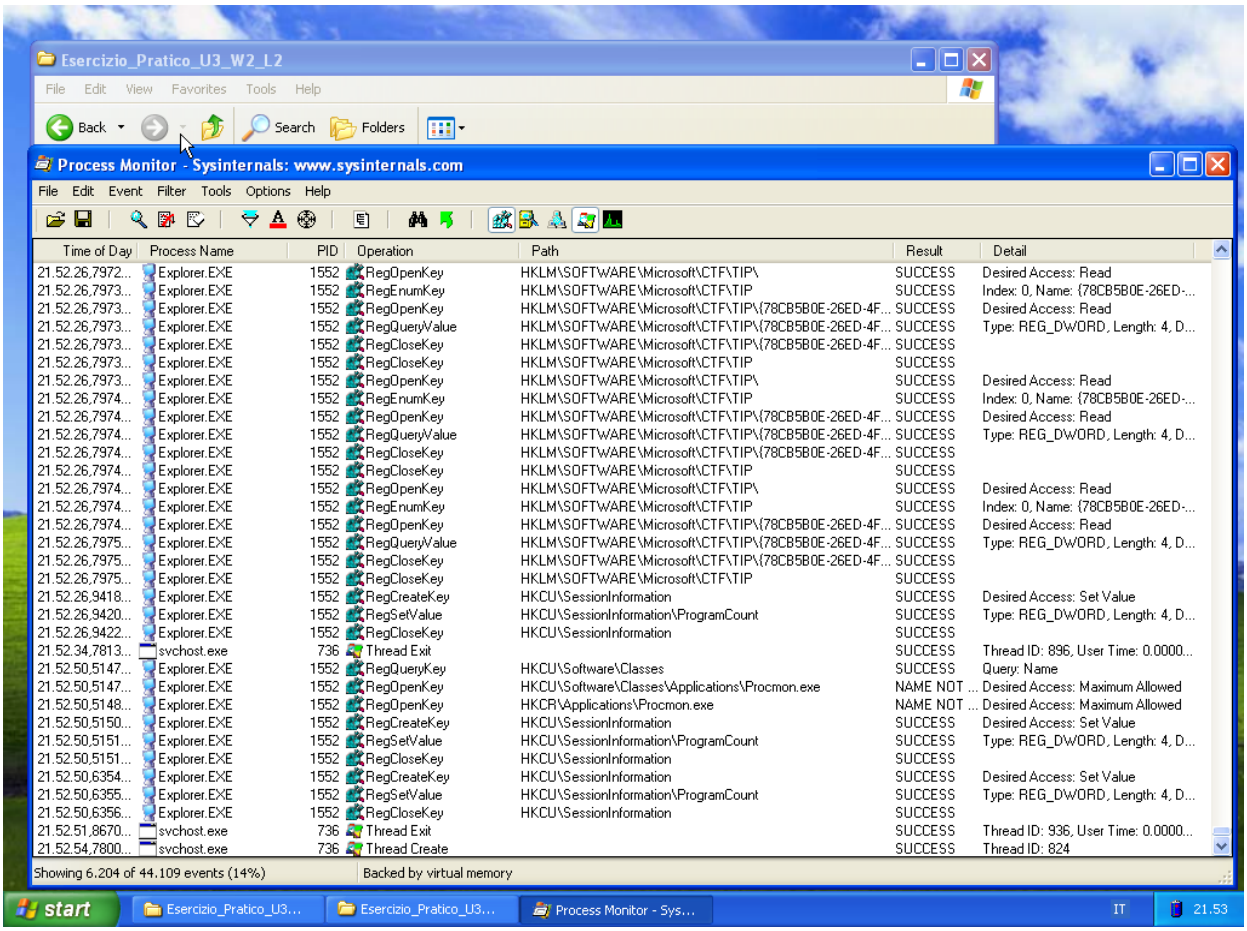

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result | Detail
21.32.13,6750... Idle 0 Process Profiling SUCCESS User Time: 0.0000000 sec...
21.32.13,6751... smss.exe 352 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6751... csrss.exe 408 Process Profiling SUCCESS User Time: 0.6909936 sec...
21.32.13,6752... winlogon.exe 432 Process Profiling SUCCESS User Time: 0.2203168 sec...
21.32.13,6752... services.exe 476 Process Profiling SUCCESS User Time: 0.0901296 sec...
21.32.13,6752... lsass.exe 488 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.13,6752... svchost.exe 636 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.13,6752... svchost.exe 752 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.13,6752... svchost.exe 788 Process Profiling SUCCESS User Time: 0.3204608 sec...
21.32.13,6752... svchost.exe 912 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6752... svchost.exe 944 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.13,6752... spoolsv.exe 1076 Process Profiling SUCCESS User Time: 0.0200288 sec...
21.32.13,6753... alg.exe 1408 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.13,6753... Explorer.EXE 1560 Process Profiling SUCCESS User Time: 1.3619584 sec...
21.32.13,6753... ctfmon.exe 1648 Process Profiling SUCCESS User Time: 0.0200288 sec...
21.32.13,6753... wuauclt.exe 1832 Process Profiling SUCCESS User Time: 0.0500720 sec...
21.32.14,6711... Idle 0 Process Profiling SUCCESS User Time: 0.0000000 sec...
21.32.14,6712... smss.exe 352 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.14,6712... csrss.exe 408 Process Profiling SUCCESS User Time: 0.7010080 sec...
21.32.14,6712... winlogon.exe 432 Process Profiling SUCCESS User Time: 0.2203168 sec...
21.32.14,6712... services.exe 476 Process Profiling SUCCESS User Time: 0.0901296 sec...
21.32.14,6713... lsass.exe 488 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.14,6713... svchost.exe 636 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.14,6713... svchost.exe 752 Process Profiling SUCCESS User Time: 0.1001440 sec...
21.32.14,6713... svchost.exe 788 Process Profiling SUCCESS User Time: 0.3204608 sec...
21.32.14,6713... svchost.exe 912 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.14,6714... svchost.exe 944 Process Profiling SUCCESS User Time: 0.0300432 sec...
21.32.14,6714... spoolsv.exe 1076 Process Profiling SUCCESS User Time: 0.0200288 sec...
21.32.14,6714... alg.exe 1408 Process Profiling SUCCESS User Time: 0.0100144 sec...
21.32.14,6714... Explorer.EXE 1560 Process Profiling SUCCESS User Time: 1.3619584 sec...
21.32.14,6714... ctfmon.exe 1648 Process Profiling SUCCESS User Time: 0.0200288 sec...
21.32.14,6714... wuauclt.exe 1832 Process Profiling SUCCESS User Time: 0.0500720 sec...
21.32.15,6721... Idle 0 Process Profiling SUCCESS User Time: 0.0000000 sec...
Showing 5.009 of 48.831 events (10%)
Backed by virtual memory
start
Esercizio_Pratico_U3...
Process Monitor - Sys...
IT
21.37

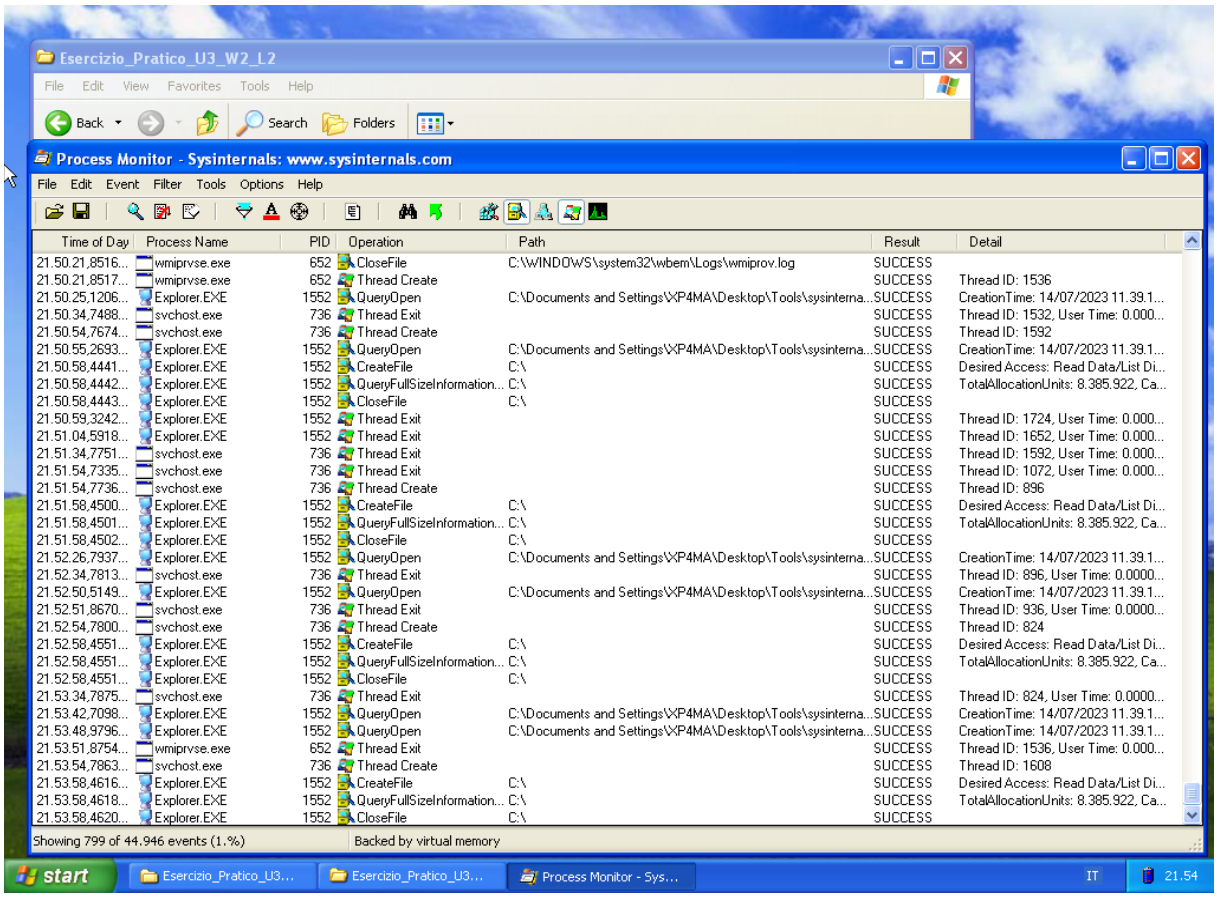
ESECUZIONE DEL MALWARE

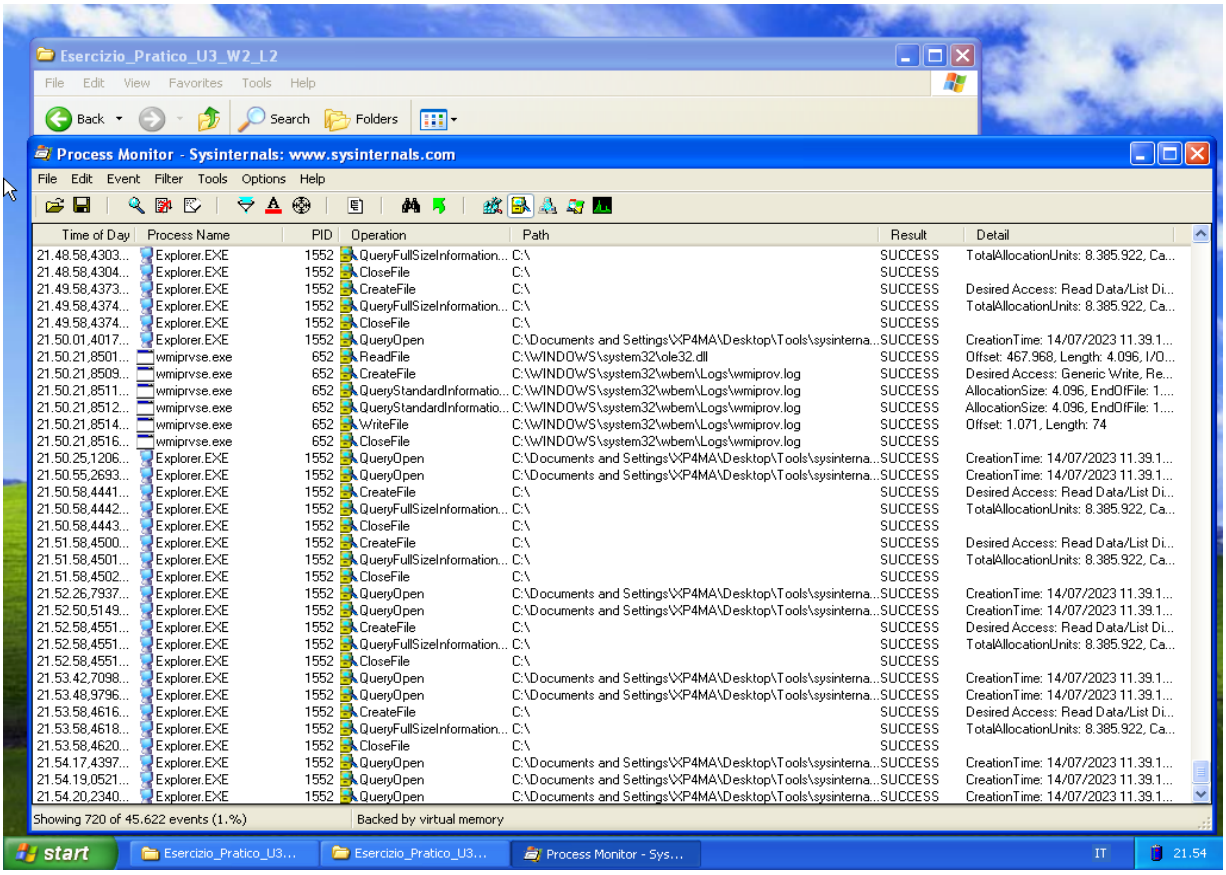
ANALISI POST- ESECUZIONE CON PROCMON

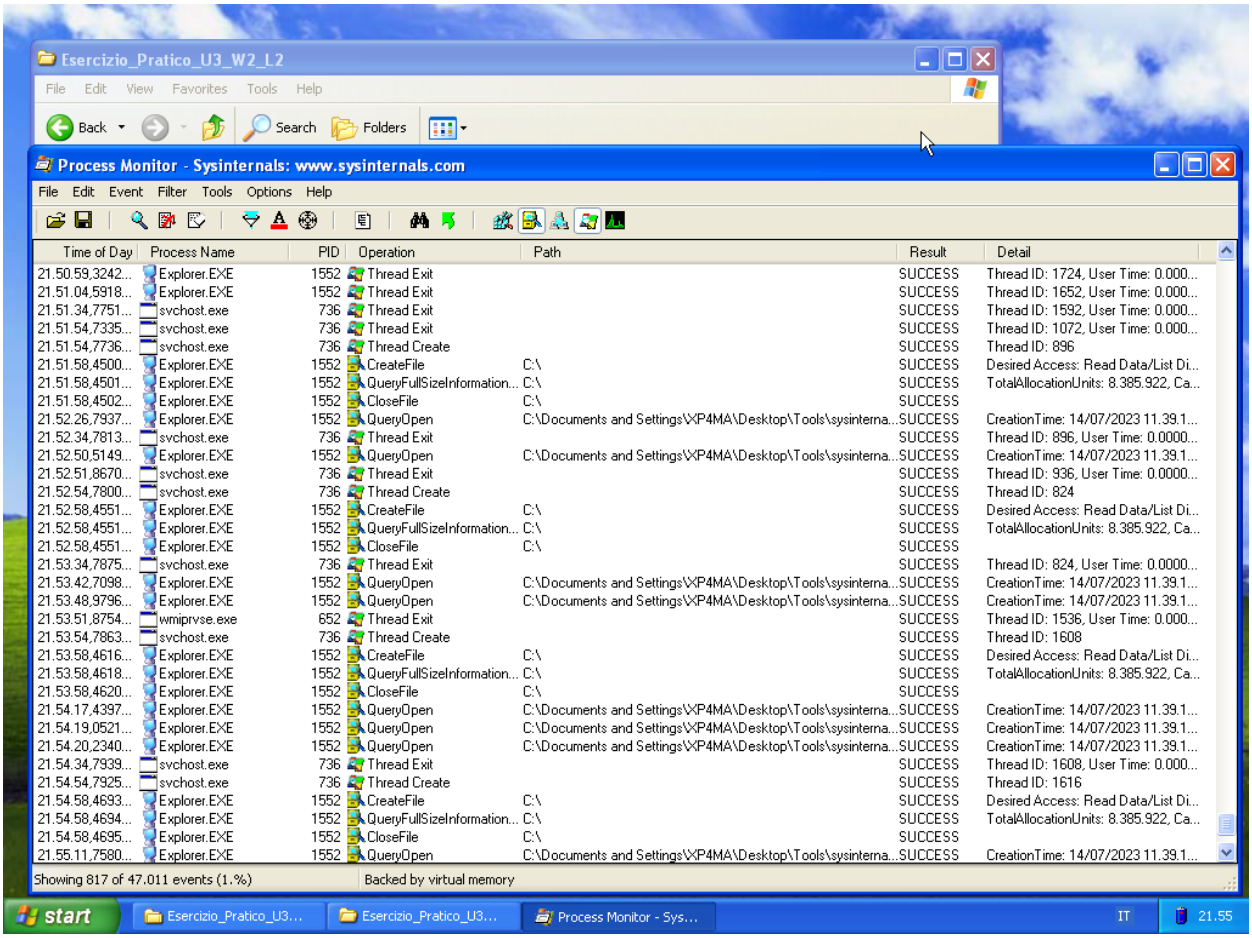


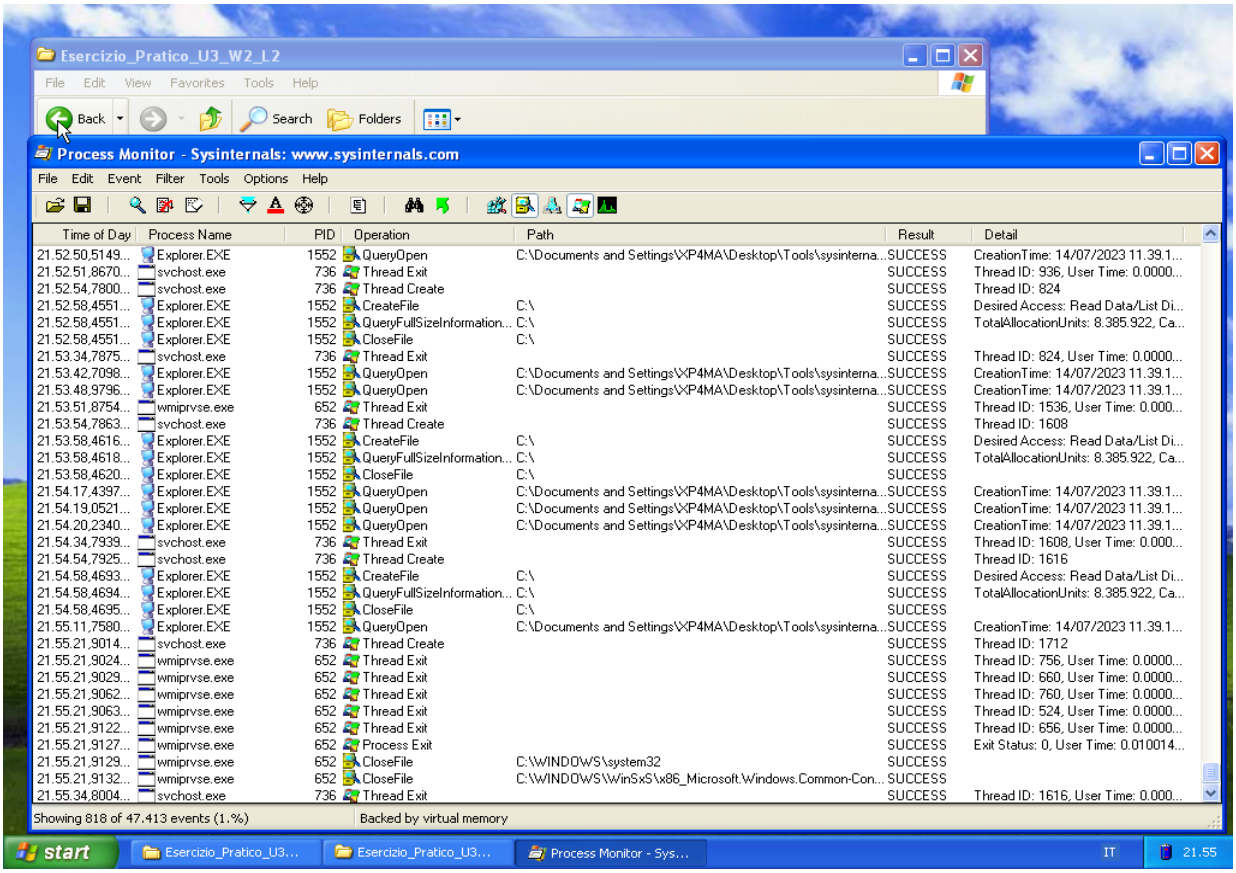



Esercizio_Pratico_U3_W2_L2
File Edit View Favorites Tools Help
Back Search Folders
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result | Detail
21.52.26,7972... Explorer.EXE 1552 RegOpenKey HKLM\SOFTWARE\Microsoft\CTF\TIP\ SUCCESS Desired Access: Read
21.52.26,7973... Explorer.EXE 1552 RegEnumKey HKLM\SOFTWARE\Microsoft\CTF\TIP SUCCESS Index: 0, Name: {78CB5B0E-26ED-...
21.52.26,7973... Explorer.EXE 1552 RegOpenKey HKLM\SOFTWARE\Microsoft\CTF\TIP\{78CB5B0E-26ED-4F... SUCCESS Desired Access: Read
21.52.26,7973... Explorer.EXE 1552 RegQueryValue HKLM\SOFTWARE\Microsoft\CTF\TIP\{78CB5B0E-26ED-4F... SUCCESS Type: REG_DWORD, Length: 4, D...
21.52.26,7973... Explorer.EXE 1552 RegCloseKey HKLM\SOFTWARE\Microsoft\CTF\TIP\{78CB5B0E-26ED-4F... SUCCESS
21.52.26,7973... Explorer.EXE 1552 RegCloseKey HKLM\SOFTWARE\Microsoft\CTF\TIP SUCCESS
21.52.26,7973... Explorer.EXE 1552 RegOpenKey HKLM\SOFTWARE\Microsoft\CTF\TIP\ SUCCESS Desired Access: Read
21.52.26,7974... Explorer.EXE 1552 RegEnumKey HKLM\SOFTWARE\Microsoft\CTF\TIP SUCCESS Index: 0, Name: {78CB5B0E-26ED-...
21.52.26,7974... Explorer.EXE 1552 RegOpenKey HKLM\SOFTWARE\Microsoft\CTF\TIP\{78CB5B0E-26ED-4F... SUCCESS Desired Access: Read
21.52.26,7974... Explorer.EXE 1552 RegQueryValue HKLM\SOFTWARE\Microsoft\CTF\TIP\{78CB5B0E-26ED-4F... SUCCESS Type: REG_DWORD, Length: 4, D...
21.52.26,7974... Explorer.EXE 1552 RegCloseKey HKLM\SOFTWARE\Microsoft\CTF\TIP\{78CB5B0E-26ED-4F... SUCCESS
21.52.26,7974... Explorer.EXE 1552 RegCloseKey HKLM\SOFTWARE\Microsoft\CTF\TIP SUCCESS
21.52.26,7974... Explorer.EXE 1552 RegOpenKey HKLM\SOFTWARE\Microsoft\CTF\TIP\ SUCCESS Desired Access: Read
21.52.26,7974... Explorer.EXE 1552 RegEnumKey HKLM\SOFTWARE\Microsoft\CTF\TIP SUCCESS Index: 0, Name: {78CB5B0E-26ED-...
21.52.26,7974... Explorer.EXE 1552 RegOpenKey HKLM\SOFTWARE\Microsoft\CTF\TIP\{78CB5B0E-26ED-4F... SUCCESS Desired Access: Read
21.52.26,7975... Explorer.EXE 1552 RegQueryValue HKLM\SOFTWARE\Microsoft\CTF\TIP\{78CB5B0E-26ED-4F... SUCCESS Type: REG_DWORD, Length: 4, D...
21.52.26,7975... Explorer.EXE 1552 RegCloseKey HKLM\SOFTWARE\Microsoft\CTF\TIP\{78CB5B0E-26ED-4F... SUCCESS
21.52.26,7975... Explorer.EXE 1552 RegCloseKey HKLM\SOFTWARE\Microsoft\CTF\TIP SUCCESS
21.52.26,9418... Explorer.EXE 1552 RegCreateKey HKCU\SessionInformation SUCCESS Desired Access: Set Value
21.52.26,9420... Explorer.EXE 1552 RegSetValue HKCU\SessionInformation\ProgramCount SUCCESS Type: REG_DWORD, Length: 4, D...
21.52.26,9422... Explorer.EXE 1552 RegCloseKey HKCU\SessionInformation SUCCESS
21.52.34,7813... svchost.exe 736 Thread Exit SUCCESS Thread ID: 896, User Time: 0.0000...
21.52.50,5147... Explorer.EXE 1552 RegQueryKey HKCU\Software\Classes SUCCESS Query: Name
21.52.50,5147... Explorer.EXE 1552 RegOpenKey HKCU\Software\Classes\Applications\Procmon.exe NAME NOT ... Desired Access: Maximum Allowed
21.52.50,5148... Explorer.EXE 1552 RegOpenKey HKCR\Applications\Procmon.exe NAME NOT ... Desired Access: Maximum Allowed
21.52.50,5150... Explorer.EXE 1552 RegCreateKey HKCU\SessionInformation SUCCESS Desired Access: Set Value
21.52.50,5151... Explorer.EXE 1552 RegSetValue HKCU\SessionInformation\ProgramCount SUCCESS Type: REG_DWORD, Length: 4, D...
21.52.50,5151... Explorer.EXE 1552 RegCloseKey HKCU\SessionInformation SUCCESS
21.52.50,6354... Explorer.EXE 1552 RegCreateKey HKCU\SessionInformation SUCCESS Desired Access: Set Value
21.52.50,6355... Explorer.EXE 1552 RegSetValue HKCU\SessionInformation\ProgramCount SUCCESS Type: REG_DWORD, Length: 4, D...
21.52.50,6356... Explorer.EXE 1552 RegCloseKey HKCU\SessionInformation SUCCESS
21.52.51,8670... svchost.exe 736 Thread Exit SUCCESS Thread ID: 936, User Time: 0.0000...
21.52.54,7800... svchost.exe 736 Thread Create SUCCESS Thread ID: 824
Showing 6.204 of 44.109 events (14%)
Backed by virtual memory
start
Esercizio_Pratico_U3...
Esercizio_Pratico_U3...
Process Monitor - Sys...
IT
21.53


Esercizio_Pratico_U3_W2_L2
File Edit View Favorites Tools Help
Back Search Folders
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result | Detail
21.50.21,8516... wmiprvse.exe 652 CloseFile C:\WINDOWS\system32\wbem\Logs\wmiprov.log SUCCESS
21.50.21,8517... wmiprvse.exe 652 Thread Create SUCCESS Thread ID: 1536
21.50.25,1206... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.50.34,7488... svchost.exe 736 Thread Exit SUCCESS Thread ID: 1532, User Time: 0.000...
21.50.54,7674... svchost.exe 736 Thread Create SUCCESS Thread ID: 1592
21.50.55,2693... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.50.58,4441... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.50.58,4442... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.50.58,4443... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.50.59,3242... Explorer.EXE 1552 Thread Exit SUCCESS Thread ID: 1724, User Time: 0.000...
21.51.04,5918... Explorer.EXE 1552 Thread Exit SUCCESS Thread ID: 1652, User Time: 0.000...
21.51.34,7751... svchost.exe 736 Thread Exit SUCCESS Thread ID: 1592, User Time: 0.000...
21.51.54,7335... svchost.exe 736 Thread Exit SUCCESS Thread ID: 1072, User Time: 0.000...
21.51.54,7736... svchost.exe 736 Thread Create SUCCESS Thread ID: 896
21.51.58,4500... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.51.58,4501... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.51.58,4502... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.52.26,7937... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.52.34,7813... svchost.exe 736 Thread Exit SUCCESS Thread ID: 896, User Time: 0.0000...
21.52.50,5149... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.52.51,8670... svchost.exe 736 Thread Exit SUCCESS Thread ID: 936, User Time: 0.0000...
21.52.54,7800... svchost.exe 736 Thread Create SUCCESS Thread ID: 824
21.52.58,4551... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.52.58,4551... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.52.58,4551... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.53.34,7875... svchost.exe 736 Thread Exit SUCCESS Thread ID: 824, User Time: 0.0000...
21.53.42,7098... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.53.48,9796... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.53.51,8754... wmiprvse.exe 652 Thread Exit SUCCESS Thread ID: 1536, User Time: 0.000...
21.53.54,7863... svchost.exe 736 Thread Create SUCCESS Thread ID: 1608
21.53.58,4616... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.53.58,4618... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.53.58,4620... Explorer.EXE 1552 CloseFile C:\ SUCCESS
Showing 799 of 44.946 events (1.%)
Backed by virtual memory
start
Esercizio_Pratico_U3...
Esercizio_Pratico_U3...
Process Monitor - Sys...
IT
21.54

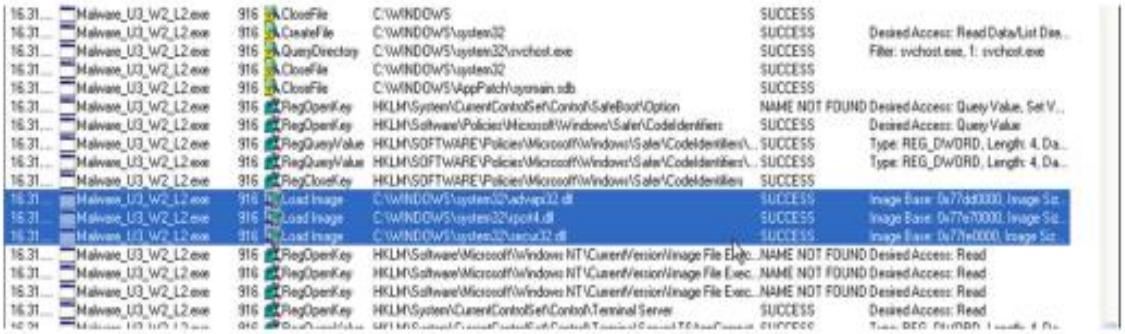

Esercizio_Pratico_U3_W2_L2
File Edit View Favorites Tools Help
Back Search Folders
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result | Detail
21.48.58,4303... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.48.58,4304... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.49.58,4373... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.49.58,4374... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.49.58,4374... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.50.01,4017... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.50.21,8501... wmiprvse.exe 652 ReadFile C:\WINDOWS\system32\ole32.dll SUCCESS Offset: 467.968, Length: 4.096, I/O...
21.50.21,8509... wmiprvse.exe 652 CreateFile C:\WINDOWS\system32\wbem\Logs\wmiprov.log SUCCESS Desired Access: Generic Write, Re...
21.50.21,8511... wmiprvse.exe 652 QueryStandardInformatio... C:\WINDOWS\system32\wbem\Logs\wmiprov.log SUCCESS AllocationSize: 4.096, EndOfFile: 1....
21.50.21,8512... wmiprvse.exe 652 QueryStandardInformatio... C:\WINDOWS\system32\wbem\Logs\wmiprov.log SUCCESS AllocationSize: 4.096, EndOfFile: 1....
21.50.21,8514... wmiprvse.exe 652 WriteFile C:\WINDOWS\system32\wbem\Logs\wmiprov.log SUCCESS Offset: 1.071, Length: 74
21.50.21,8516... wmiprvse.exe 652 CloseFile C:\WINDOWS\system32\wbem\Logs\wmiprov.log SUCCESS
21.50.25,1206... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.50.55,2693... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.50.58,4441... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.50.58,4442... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.50.58,4443... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.51.58,4500... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.51.58,4501... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.51.58,4502... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.52.26,7937... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.52.50,5149... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.52.58,4551... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.52.58,4551... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.52.58,4551... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.53.42,7098... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.53.48,9796... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.53.58,4616... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.53.58,4618... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.53.58,4620... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.54.17,4397... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.54.19,0521... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.54.20,2340... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
Showing 720 of 45.622 events (1.%)
Backed by virtual memory
start
Esercizio_Pratico_U3...
Esercizio_Pratico_U3...
Process Monitor - Sys...
IT
21.54


Esercizio_Pratico_U3_W2_L2
File Edit View Favorites Tools Help
Back Search Folders
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day | Process Name | PID | Operation | Path | Result | Detail
21.50.59,3242... Explorer.EXE 1552 Thread Exit SUCCESS Thread ID: 1724, User Time: 0.000...
21.51.04,5918... Explorer.EXE 1552 Thread Exit SUCCESS Thread ID: 1652, User Time: 0.000...
21.51.34,7751... svchost.exe 736 Thread Exit SUCCESS Thread ID: 1592, User Time: 0.000...
21.51.54,7335... svchost.exe 736 Thread Exit SUCCESS Thread ID: 1072, User Time: 0.000...
21.51.54,7736... svchost.exe 736 Thread Create SUCCESS Thread ID: 896
21.51.58,4500... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.51.58,4501... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.51.58,4502... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.52.26,7937... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.52.34,7813... svchost.exe 736 Thread Exit SUCCESS Thread ID: 896, User Time: 0.0000...
21.52.50,5149... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.52.51,8670... svchost.exe 736 Thread Exit SUCCESS Thread ID: 936, User Time: 0.0000...
21.52.54,7800... svchost.exe 736 Thread Create SUCCESS Thread ID: 824
21.52.58,4551... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.52.58,4551... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.52.58,4551... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.53.34,7875... svchost.exe 736 Thread Exit SUCCESS Thread ID: 824, User Time: 0.0000...
21.53.42,7098... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.53.48,9796... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.53.51,8754... wmiprvse.exe 652 Thread Exit SUCCESS Thread ID: 1536, User Time: 0.000...
21.53.54,7863... svchost.exe 736 Thread Create SUCCESS Thread ID: 1608
21.53.58,4616... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.53.58,4618... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.53.58,4620... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.54.17,4397... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.54.19,0521... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.54.20,2340... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.54.34,7939... svchost.exe 736 Thread Exit SUCCESS Thread ID: 1608, User Time: 0.000...
21.54.54,7925... svchost.exe 736 Thread Create SUCCESS Thread ID: 1616
21.54.58,4693... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.54.58,4694... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.54.58,4695... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.55.11,7580... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
Showing 817 of 47.011 events (1.%)
Backed by virtual memory
start
Esercizio_Pratico_U3...
Esercizio_Pratico_U3...
Process Monitor - Sys...
IT
21.55


Esercizio_Pratico_U3_W2_L2
File Edit View Favorites Tools Help
Back Search Folders
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time of Day Process Name PID Operation Path Result Detail
21.52.50,5149... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.52.51,8670... svchost.exe 736 Thread Exit SUCCESS Thread ID: 936, User Time: 0.0000...
21.52.54,7800... svchost.exe 736 Thread Create SUCCESS Thread ID: 824
21.52.58,4551... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.52.58,4551... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.52.58,4551... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.53.34,7875... svchost.exe 736 Thread Exit SUCCESS Thread ID: 824, User Time: 0.0000...
21.53.42,7098... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.53.48,9796... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.53.51,8754... wmiprvse.exe 652 Thread Exit SUCCESS Thread ID: 1536, User Time: 0.000...
21.53.54,7863... svchost.exe 736 Thread Create SUCCESS Thread ID: 1608
21.53.58,4616... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.53.58,4618... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.53.58,4620... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.54.17,4397... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.54.19,0521... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.54.20,2340... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.54.34,7939... svchost.exe 736 Thread Exit SUCCESS Thread ID: 1608, User Time: 0.000...
21.54.54,7925... svchost.exe 736 Thread Create SUCCESS Thread ID: 1616
21.54.58,4693... Explorer.EXE 1552 CreateFile C:\ SUCCESS Desired Access: Read Data/List Di...
21.54.58,4694... Explorer.EXE 1552 QueryFullSizeInformation... C:\ SUCCESS TotalAllocationUnits: 8.385.922, Ca...
21.54.58,4695... Explorer.EXE 1552 CloseFile C:\ SUCCESS
21.55.11,7580... Explorer.EXE 1552 QueryOpen C:\Documents and Settings\XP4MA\Desktop\Tools\sysinterna... SUCCESS CreationTime: 14/07/2023 11.39.1...
21.55.21,9014... svchost.exe 736 Thread Create SUCCESS Thread ID: 1712
21.55.21,9024... wmiprvse.exe 652 Thread Exit SUCCESS Thread ID: 756, User Time: 0.0000...
21.55.21,9029... wmiprvse.exe 652 Thread Exit SUCCESS Thread ID: 660, User Time: 0.0000...
21.55.21,9062... wmiprvse.exe 652 Thread Exit SUCCESS Thread ID: 760, User Time: 0.0000...
21.55.21,9063... wmiprvse.exe 652 Thread Exit SUCCESS Thread ID: 524, User Time: 0.0000...
21.55.21,9122... wmiprvse.exe 652 Thread Exit SUCCESS Thread ID: 656, User Time: 0.0000...
21.55.21,9127... wmiprvse.exe 652 Process Exit SUCCESS Exit Status: 0, User Time: 0.010014...
21.55.21,9129... wmiprvse.exe 652 CloseFile C:\WINDOWS\system32 SUCCESS
21.55.21,9132... wmiprvse.exe 652 CloseFile C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Con... SUCCESS
21.55.34,8004... svchost.exe 736 Thread Exit SUCCESS Thread ID: 1616, User Time: 0.000...
Showing 818 of 47.413 events (1.%)
Backed by virtual memory
start
Esercizio_Pratico_U3...
Esercizio_Pratico_U3...
Process Monitor - Sys...
IT
21.55

La prima azione da compiere è creare una istantanea del registro di sistema tramite RegShot prima dell'analisi del malware. Questo ci permetterà di identificare eventuali modifiche che si potrebbero andare a creare dopo l'esecuzione del malware.

Lanciamo poi ProcMon utilizzando come filtro il nome del file infetto compreso di estensione, lanciamo il malware, lasciamo che l'output si popoli e creiamo poi una seconda istantanea tramite RegShot da utilizzare come confronto a fine processo.



Analizzando la cattura di ProcMon notiamo che il malware ha richiamato diverse librerie di sistema per poi andare a creare un processo svchost.exe all'interno della directory di sistema (system32).