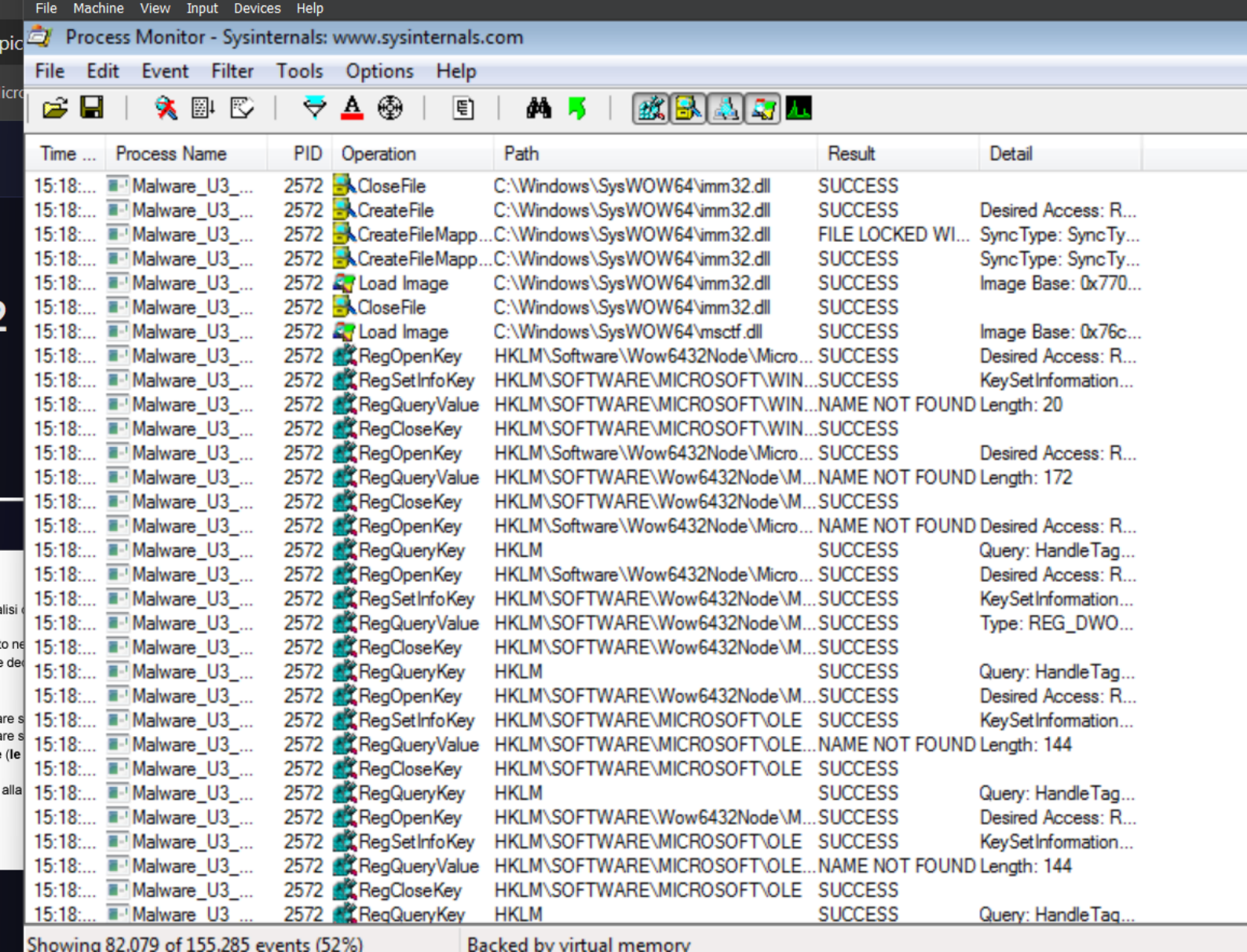
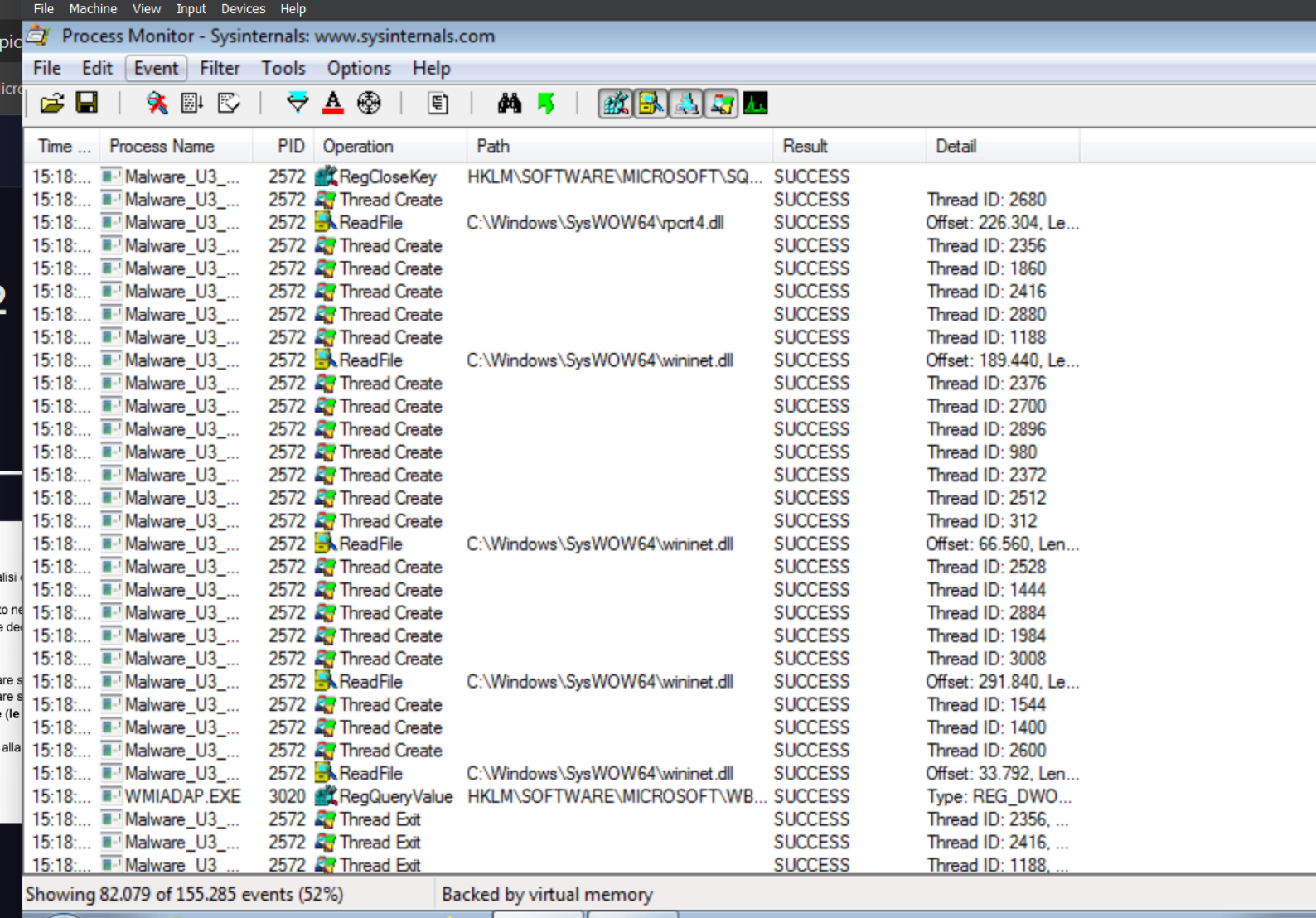
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
15:18:...	Malware_U3_...	2572	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
15:18:...	Malware_U3_...	2572	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x767...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x757...
15:18:...	Malware_U3_...	2572	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: R...
15:18:...	Malware_U3_...	2572	QueryBasicInfor...	C:\Windows\SysWOW64\sechost.dll	SUCCESS	CreationTime: 14/0...
15:18:...	Malware_U3_...	2572	CloseFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	
15:18:...	Malware_U3_...	2572	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: R...
15:18:...	Malware_U3_...	2572	CreateFileMapp...	C:\Windows\SysWOW64\sechost.dll	FILE LOCKED WI...	SyncType: SyncTy...
15:18:...	Malware_U3_...	2572	CreateFileMapp...	C:\Windows\SysWOW64\sechost.dll	SUCCESS	SyncType: SyncTy...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x76e...
15:18:...	Malware_U3_...	2572	CloseFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Image Base: 0x75a...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Image Base: 0x756...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Image Base: 0x756...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Image Base: 0x758...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x759...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x770...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x759...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\lpk.dll	SUCCESS	Image Base: 0x77b...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\usp10.dll	SUCCESS	Image Base: 0x773...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Image Base: 0x774...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x775...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Image Base: 0x76c...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\crypt32.dll	SUCCESS	Image Base: 0x768...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\msasn1.dll	SUCCESS	Image Base: 0x769...
15:18:...	Malware_U3_...	2572	Load Image	C:\Windows\SysWOW64\iertutil.dll	SUCCESS	Image Base: 0x76a...
15:18:...	Malware_U3_...	2572	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
15:18:...	Malware_U3_...	2572	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
15:18:...	Malware_U3_...	2572	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
15:18:...	Malware_U3_...	2572	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...

Showing 82.079 of 155.285 events (52%) Backed by virtual memory


File Machine View Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
15:18:... Malware_U3_... 2572 CloseFile C:\Windows\SysWOW64\imm32.dll SUCCESS
15:18:... Malware_U3_... 2572 CreateFile C:\Windows\SysWOW64\imm32.dll SUCCESS Desired Access: R...
15:18:... Malware_U3_... 2572 CreateFileMapp... C:\Windows\SysWOW64\imm32.dll FILE LOCKED WI... SyncType: SyncTy...
15:18:... Malware_U3_... 2572 CreateFileMapp... C:\Windows\SysWOW64\imm32.dll SUCCESS SyncType: SyncTy...
15:18:... Malware_U3_... 2572 Load Image C:\Windows\SysWOW64\imm32.dll SUCCESS Image Base: 0x770...
15:18:... Malware_U3_... 2572 CloseFile C:\Windows\SysWOW64\imm32.dll SUCCESS
15:18:... Malware_U3_... 2572 Load Image C:\Windows\SysWOW64\msctf.dll SUCCESS Image Base: 0x76c...
15:18:... Malware_U3_... 2572 RegOpenKey HKLM\Software\Wow6432Node\Micro... SUCCESS Desired Access: R...
15:18:... Malware_U3_... 2572 RegSetInfoKey HKLM\SOFTWARE\MICROSOFT\WIN... SUCCESS KeySetInformation...
15:18:... Malware_U3_... 2572 RegQueryValue HKLM\SOFTWARE\MICROSOFT\WIN... NAME NOT FOUND Length: 20
15:18:... Malware_U3_... 2572 RegCloseKey HKLM\SOFTWARE\MICROSOFT\WIN... SUCCESS
15:18:... Malware_U3_... 2572 RegOpenKey HKLM\Software\Wow6432Node\Micro... SUCCESS Desired Access: R...
15:18:... Malware_U3_... 2572 RegQueryValue HKLM\SOFTWARE\Wow6432Node\M... NAME NOT FOUND Length: 172
15:18:... Malware_U3_... 2572 RegCloseKey HKLM\SOFTWARE\Wow6432Node\M... SUCCESS
15:18:... Malware_U3_... 2572 RegOpenKey HKLM\Software\Wow6432Node\Micro... NAME NOT FOUND Desired Access: R...
15:18:... Malware_U3_... 2572 RegQueryKey HKLM SUCCESS Query: HandleTag...
15:18:... Malware_U3_... 2572 RegOpenKey HKLM\Software\Wow6432Node\Micro... SUCCESS Desired Access: R...
15:18:... Malware_U3_... 2572 RegSetInfoKey HKLM\SOFTWARE\Wow6432Node\M... SUCCESS KeySetInformation...
15:18:... Malware_U3_... 2572 RegQueryValue HKLM\SOFTWARE\Wow6432Node\M... SUCCESS Type: REG_DWO...
15:18:... Malware_U3_... 2572 RegCloseKey HKLM\SOFTWARE\Wow6432Node\M... SUCCESS
15:18:... Malware_U3_... 2572 RegQueryKey HKLM SUCCESS Query: HandleTag...
15:18:... Malware_U3_... 2572 RegOpenKey HKLM\SOFTWARE\Wow6432Node\M... SUCCESS Desired Access: R...
15:18:... Malware_U3_... 2572 RegSetInfoKey HKLM\SOFTWARE\MICROSOFT\OLE SUCCESS KeySetInformation...
15:18:... Malware_U3_... 2572 RegQueryValue HKLM\SOFTWARE\MICROSOFT\OLE... NAME NOT FOUND Length: 144
15:18:... Malware_U3_... 2572 RegCloseKey HKLM\SOFTWARE\MICROSOFT\OLE SUCCESS
15:18:... Malware_U3_... 2572 RegQueryKey HKLM SUCCESS Query: HandleTag...
15:18:... Malware_U3_... 2572 RegOpenKey HKLM\SOFTWARE\Wow6432Node\M... SUCCESS Desired Access: R...
15:18:... Malware_U3_... 2572 RegSetInfoKey HKLM\SOFTWARE\MICROSOFT\OLE SUCCESS KeySetInformation...
15:18:... Malware_U3_... 2572 RegQueryValue HKLM\SOFTWARE\MICROSOFT\OLE... NAME NOT FOUND Length: 144
15:18:... Malware_U3_... 2572 RegCloseKey HKLM\SOFTWARE\MICROSOFT\OLE SUCCESS
15:18:... Malware_U3_... 2572 RegQueryKey HKLM SUCCESS Query: HandleTag...
Showing 82,079 of 155,285 events (52%)
Backed by virtual memory


File Machine View Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
15:18:... Malware_U3_... 2572 RegCloseKey HKLM\SOFTWARE\MICROSOFT\SQ... SUCCESS
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2680
15:18:... Malware_U3_... 2572 ReadFile C:\Windows\SysWOW64\vpcrt4.dll SUCCESS Offset: 226.304, Le...
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2356
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 1860
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2416
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2880
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 1188
15:18:... Malware_U3_... 2572 ReadFile C:\Windows\SysWOW64\wininet.dll SUCCESS Offset: 189.440, Le...
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2376
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2700
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2896
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 980
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2372
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2512
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 312
15:18:... Malware_U3_... 2572 ReadFile C:\Windows\SysWOW64\wininet.dll SUCCESS Offset: 66.560, Len...
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2528
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 1444
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2884
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 1984
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 3008
15:18:... Malware_U3_... 2572 ReadFile C:\Windows\SysWOW64\wininet.dll SUCCESS Offset: 291.840, Le...
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 1544
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 1400
15:18:... Malware_U3_... 2572 Thread Create SUCCESS Thread ID: 2600
15:18:... Malware_U3_... 2572 ReadFile C:\Windows\SysWOW64\wininet.dll SUCCESS Offset: 33.792, Len...
15:18:... WMIADAP.EXE 3020 RegQueryValue HKLM\SOFTWARE\MICROSOFT\WB... SUCCESS Type: REG_DWO...
15:18:... Malware_U3_... 2572 Thread Exit SUCCESS Thread ID: 2356, ...
15:18:... Malware_U3_... 2572 Thread Exit SUCCESS Thread ID: 2416, ...
15:18:... Malware_U3_... 2572 Thread Exit SUCCESS Thread ID: 1188, ...
Showing 82.079 of 155.285 events (52%)
Backed by virtual memory

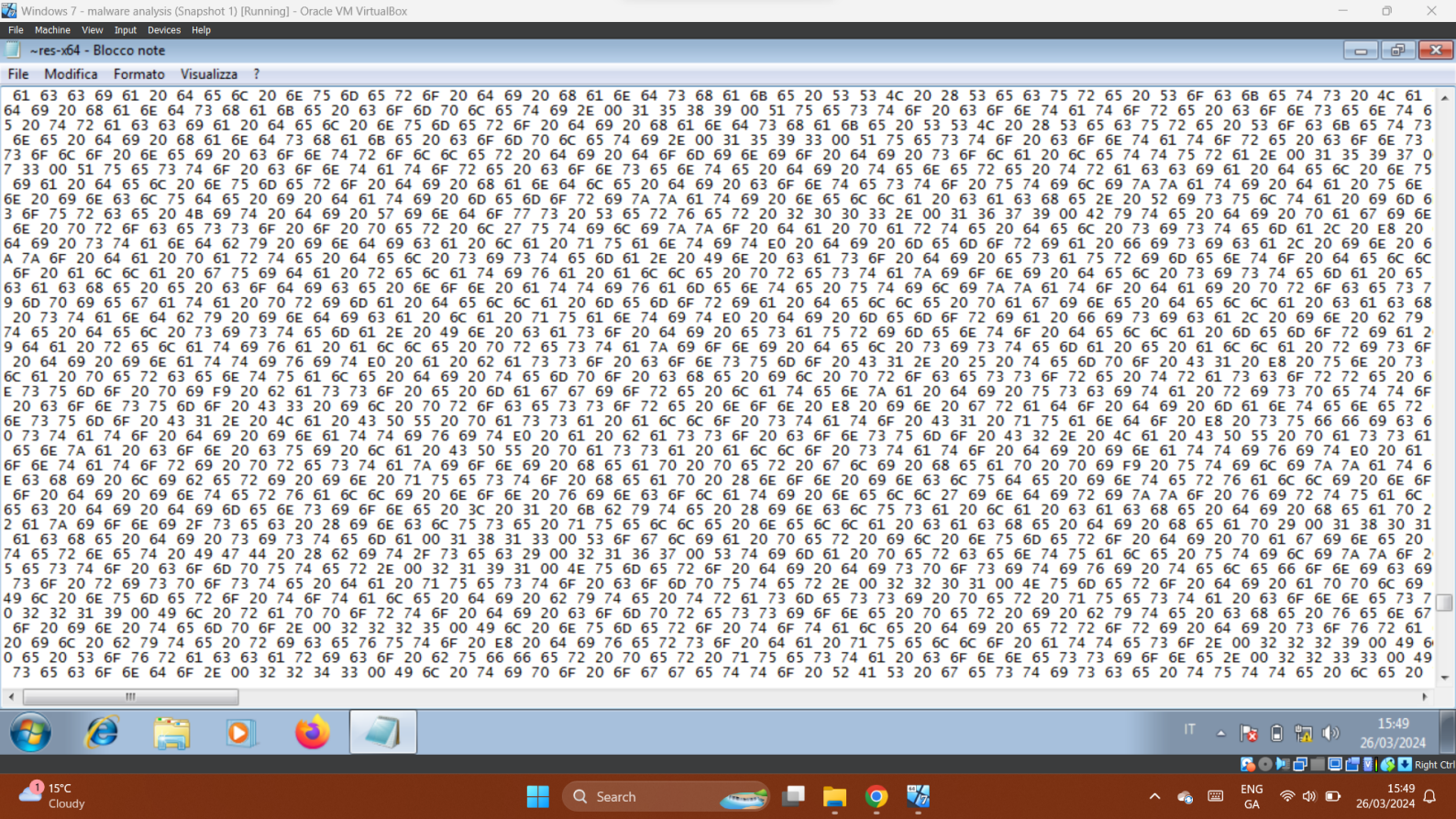
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\user32.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\crypt32.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\msasn1.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\iertutil.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\usp10.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\System32\ntdll.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\lpk.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	QueryNameInfo...	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Name: \Windows\...
15:18:...	Malware_U3_...	2572	Process Exit		SUCCESS	Exit Status: 0, User...
15:18:...	Malware_U3_...	2572	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\WIN...	SUCCESS	
15:18:...	Malware_U3_...	2572	CloseFile	C:\Windows	SUCCESS	
15:18:...	Malware_U3_...	2572	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\WIN...	SUCCESS	
15:18:...	Malware_U3_...	2572	CloseFile	C:\Users\user\Desktop\MALWARE\Es...	SUCCESS	
15:18:...	Malware_U3_...	2572	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15:18:...	Malware_U3_...	2572	RegCloseKey	HKLM	SUCCESS	
15:18:...	Malware_U3_...	2572	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15:18:...	conhost.exe	2964	Thread Exit		SUCCESS	Thread ID: 3036, ...
15:18:...	conhost.exe	2964	Thread Exit		SUCCESS	Thread ID: 2468, ...

Showing 82.079 of 155.285 events (52%) | Backed by virtual memory

File Modifica Formato Visualizza ?

```
Process CPU     Private Bytes   Working Set     PID     Description     Company Name
System Idle Process     93.23   0 K     24 K    0
System  0.06    136 K   1.920 K 4
 Interrupts     1.08    0 K     0 K     n/a     Hardware Interrupts and DPCs
 smss.exe               424 K   1.104 K 256
csrss.exe       < 0.01  1.920 K 3.880 K 328
wininit.exe             1.460 K 4.348 K 376
 services.exe           4.520 K 8.340 K 476
  svchost.exe           3.784 K 9.352 K 580     Processo host per servizi di Windows    Microsoft Corporation
   WmiPrvSE.exe         2.508 K 6.564 K 1496
  VBoxService.exe       0.01    2.216 K 7.776 K 640     VirtualBox Guest Additions Service      Oracle Corporation
  svchost.exe           3.820 K 7.528 K 708     Processo host per servizi di Windows    Microsoft Corporation
  svchost.exe           16.384 K        17.552 K        800     Processo host per servizi di Windows    Microsoft Corporation
   audiodg.exe          15.760 K        15.852 K        952
  svchost.exe           5.412 K 13.076 K        844     Processo host per servizi di Windows    Microsoft Corporation
   dwm.exe              1.608 K 4.928 K 1992    Gestione finestre desktop       Microsoft Corporation
  svchost.exe   0.03    17.344 K        31.720 K        876     Processo host per servizi di Windows    Microsoft Corporation
  svchost.exe           5.548 K 10.316 K        112     Processo host per servizi di Windows    Microsoft Corporation
  svchost.exe   0.01    11.368 K        13.012 K        548     Processo host per servizi di Windows    Microsoft Corporation
  spoolsv.exe           6.264 K 11.508 K        1080    Applicazione sottosistema spooler       Microsoft Corporation
  svchost.exe           10.684 K        13.064 K        1108    Processo host per servizi di Windows    Microsoft Corporation
  svchost.exe           6.872 K 13.264 K        1256    Processo host per servizi di Windows    Microsoft Corporation
  taskhost.exe          8.196 K 9.536 K 1592    Processo host per attività di Windows   Microsoft Corporation
  sppsvc.exe            5.880 K 11.540 K        1772    Servizio piattaforma protezione software Microsoft      Microsoft Corporation
  SearchIndexer.exe     < 0.01  18.244 K        14.456 K        1556    Microsoft Windows Search Indexer        Microsoft Corporation
  svchost.exe           63.784 K        22.048 K        2980    Processo host per servizi di Windows    Microsoft Corporation
  wmpnetwk.exe  0.01    10.268 K        4.648 K 2848    Servizio di condivisione in rete Windows Media Player   Microsoft Corporation
 lsass.exe              3.836 K 10.004 K        484     Local Security Authority Process        Microsoft Corporation
 lsm.exe                2.364 K 4.172 K 492
csrss.exe       1.12    2.172 K 6.960 K 384
winlogon.exe            2.708 K 6.776 K 412
explorer.exe    0.06    37.968 K        56.860 K        2016    Esplora risorse Microsoft Corporation
 VBoxTray.exe   0.01    2.400 K 7.604 K 1392    VirtualBox Guest Additions Tray Application     Oracle Corporation
 procexp.exe            2.232 K 7.724 K 2136    Sysinternals Process Explorer   Sysinternals - www.sysinternals.com
  procexp64.exe 4.37    16.420 K        34.436 K        1700    Sysinternals Process Explorer   Sysinternals - www.sysinternals.com
 Regshot-x64-ANSI.exe           177.204 K       184.508 K       2316
  notepad.exe           16.736 K        21.676 K        2720
 Procmon.exe            3.984 K 9.620 K 1604    Process Monitor Sysinternals - www.sysinternals.com
  Procmon64.exe         15.008 K        25.332 K        2384
```


Windows 7 - malware analysis (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~res-x64 - Blocco note
File Modifica Formato Visualizza ?
61 63 63 69 61 20 64 65 6C 20 6E 75 6D 65 72 6F 20 64 69 20 68 61 6E 64 73 68 61 6B 65 20 53 53 4C 20 28 53 65 63 75 72 65 20 53 6F 63 6B 65 74 73 20 4C 61
64 69 20 68 61 6E 64 73 68 61 6B 65 20 63 6F 6D 70 6C 65 74 69 2E 00 31 35 38 39 00 51 75 65 73 74 6F 20 63 6F 6E 74 61 74 6F 72 65 20 63 6F 6E 73 65 74 6
5 20 74 72 61 63 63 69 61 20 64 65 6C 20 6E 75 6D 65 72 6F 20 64 69 20 68 61 6E 64 73 68 61 6B 65 20 53 53 4C 20 28 53 65 63 75 72 65 20 53 6F 63 6B 65 74 73
6E 65 20 64 69 20 68 61 6E 64 73 68 61 6B 65 20 63 6F 6D 70 6C 65 74 69 2E 00 31 35 39 33 00 51 75 65 73 74 6F 20 63 6F 6E 74 61 74 6F 72 65 20 63 6F 6E 73
73 6F 6C 6F 20 6E 65 69 20 63 6F 6E 74 72 6F 6C 6C 65 72 20 64 69 20 64 6F 6D 69 6E 69 6F 20 64 69 20 73 6F 6C 61 20 6C 65 74 74 75 72 61 2E 00 31 35 39 37 0
7 33 00 51 75 65 73 74 6F 20 63 6F 6E 74 61 74 6F 72 65 20 63 6F 6E 73 65 6E 74 65 20 64 69 20 74 65 6E 65 72 65 20 74 72 61 63 63 69 61 20 64 65 6C 20 6E 75
69 61 20 64 65 6C 20 6E 75 6D 65 72 6F 20 64 69 20 68 61 6E 64 6C 65 20 64 69 20 63 6F 6E 74 65 73 74 6F 20 75 74 69 6C 69 7A 7A 61 74 69 20 64 61 20 75 6E
6E 20 69 6E 63 6C 75 64 65 20 69 20 64 61 74 69 20 6D 65 6D 6F 72 69 7A 7A 61 74 69 20 6E 65 6C 6C 61 20 63 61 63 68 65 2E 20 52 69 73 75 6C 74 61 20 69 6D 6
3 6F 75 72 63 65 20 4B 69 73 6F 20 64 69 20 57 69 6E 64 6F 77 73 20 53 65 72 76 65 72 20 32 30 30 33 2E 00 31 36 37 39 00 42 79 74 65 20 64 69 20 70 61 67 69 6E
6E 20 70 72 6F 63 65 73 73 6F 20 6F 20 70 65 72 20 6C 27 75 74 69 6C 69 7A 6F 20 64 61 20 70 61 72 74 65 20 64 65 6C 20 73 69 73 74 65 6D 61 2C 20 E8 20
64 69 20 73 74 61 6E 64 62 79 20 69 6E 64 69 63 61 20 6C 61 20 71 75 61 6E 74 69 74 E0 20 64 69 20 6D 65 6D 6F 72 69 61 20 66 69 73 69 63 61 2C 20 69 6E 20 6
A 7A 6F 20 64 61 20 70 61 72 74 65 20 64 65 6C 20 73 69 73 74 65 6D 2E 20 49 6E 20 63 61 73 6F 20 64 69 20 65 73 61 75 72 69 6D 65 6E 74 6F 20 64 65 6C 6C
6F 20 61 6C 6C 61 20 67 75 69 64 61 20 72 65 6C 61 74 69 76 61 20 61 6C 65 20 70 72 65 73 74 61 7A 69 6F 6E 69 20 64 65 6C 20 73 69 73 74 65 6D 61 20 65
63 61 63 68 65 20 65 20 63 6F 64 69 63 65 20 6E 6F 6E 20 61 74 74 69 76 61 6D 65 6E 74 65 20 75 74 69 6C 69 7A 61 74 6F 20 64 61 69 20 70 72 6F 63 65 73 73
79 6D 70 69 65 67 61 74 61 20 70 72 69 6D 61 20 64 65 6C 61 20 6D 65 6D 6F 72 69 61 20 64 65 6C 65 20 70 61 67 69 6E 65 20 64 65 6C 6C 61 20 63 61 63 68
20 73 74 61 6E 64 62 79 20 69 6E 64 69 63 61 20 6C 61 20 71 75 61 6E 74 69 74 E0 20 64 69 20 6D 65 6D 6F 72 69 61 20 66 69 73 69 63 61 2C 20 69 6E 20 62 79
74 65 20 64 65 6C 20 73 69 73 74 65 6D 61 2E 20 49 6E 20 63 61 73 6F 20 64 69 20 65 73 61 75 72 69 6D 65 6E 74 6F 20 64 65 6C 6C 61 20 72 69 73 6F
29 64 61 20 72 65 6C 61 74 69 76 61 20 61 6C 65 20 70 72 65 73 74 61 7A 69 6F 6E 69 20 64 65 6C 20 73 69 73 74 65 6D 61 20 65 20 61 6C 6C 61 20 72 69 73 6F
20 64 69 20 69 6E 61 74 74 69 76 61 20 74 E0 20 61 20 62 61 73 73 6F 20 63 6F 6E 73 75 6D 6F 20 43 31 2E 20 25 20 74 65 6D 70 6F 20 43 31 20 E8 20 75 6E 20 73
6C 61 20 70 65 72 63 65 6E 74 75 61 6C 65 20 64 69 20 74 65 6D 70 6F 20 63 68 65 20 69 6C 20 70 72 6F 63 65 73 73 6F 72 65 20 74 72 61 73 63 6F 72 72 65 20 6
E 73 75 6D 6F 20 70 69 F9 20 62 61 73 73 6F 20 65 20 6D 61 67 67 6F 72 65 20 6C 61 74 65 6E 7A 61 20 64 69 20 75 73 63 69 74 61 20 72 69 73 70 65 74 74 6F
20 63 6F 6E 73 75 6D 6F 20 43 33 20 69 6C 20 70 72 6F 63 65 73 73 6F 72 65 20 6E 6F 6E 20 E8 20 69 6E 20 67 72 61 64 6F 20 64 69 20 6D 61 6E 74 65 6E 65 72
6E 73 75 6D 6F 20 43 31 2E 20 4C 61 20 43 50 55 20 70 61 73 73 61 20 61 6C 6C 6F 20 73 74 61 74 6F 20 43 31 20 71 75 61 6E 64 6F 20 E8 20 73 75 66 66 69 63 6
0 73 74 61 74 6F 20 64 69 20 69 6E 61 74 74 69 76 69 74 E0 20 61 20 62 61 73 73 6F 20 63 6F 6E 73 75 6D 6F 20 43 32 2E 20 4C 61 20 43 50 55 20 70 61 73 73 61
65 6E 7A 61 20 63 6F 6E 20 63 75 69 20 6C 61 20 43 50 55 20 70 61 73 73 61 20 61 6C 6C 6F 20 73 74 61 74 6F 20 64 69 20 69 6E 61 74 74 69 76 69 74 E0 20 61
6F 6E 74 61 74 6F 72 69 20 70 72 65 73 74 61 7A 69 6F 6E 69 20 68 65 61 70 20 70 65 72 20 67 6C 69 20 68 65 61 70 20 74 65 72 6D 69 6E 61 74 69 6E 63 68 69 20 6C 69 6F 20 69 6E 20 71 75 65 73 74 6F 20 68 65 61 70 20 28 6E 6F 6E 20 69 6E 63 6C 75 64 65 20 69 6E 74 65 72 76 61 6C 6C 69 20 6E 6F
6F 20 64 69 20 69 6E 74 65 72 76 61 6C 6C 69 20 6E 6F 6E 20 76 69 6E 63 6F 6C 61 74 69 20 6E 65 6C 6C 27 69 6E 64 69 72 69 7A 6F 20 76 69 72 74 75 61 6C
65 63 20 64 69 20 64 69 6D 65 6E 73 69 6F 6E 65 20 3C 20 31 20 6B 62 79 74 65 20 28 69 6E 63 6C 75 73 61 20 6C 61 20 63 61 63 68 65 20 64 69 20 68 65 61 70 2
2 61 7A 69 6F 6E 69 2F 73 65 63 20 28 69 6E 63 6C 75 73 65 20 71 75 65 6C 6C 6F 20 6E 65 6C 6C 61 20 63 61 63 68 65 20 64 69 20 68 65 61 70 29 00 31 38 30 31
61 63 68 65 20 64 69 20 73 69 73 74 65 6D 61 00 31 38 31 33 00 53 6F 67 6C 69 20 70 65 72 20 69 6C 20 6E 75 6D 65 72 6F 20 64 69 20 70 61 67 69 6E 65 20
74 65 72 6E 65 74 20 49 47 44 20 28 62 69 74 2F 73 65 63 29 00 32 31 36 37 00 53 74 69 6D 61 20 70 65 72 63 65 6E 74 75 61 6C 65 20 75 74 69 6C 69 7A 7A 6F 2
5 65 73 74 6F 20 63 6F 6D 70 75 74 65 72 2E 00 32 31 39 31 00 4E 75 6D 65 72 6F 20 64 69 20 64 69 73 70 6F 73 69 74 69 6F 6E 69 63 69
73 6F 20 72 69 73 70 6F 73 74 65 20 64 61 20 71 75 65 73 74 6F 20 63 6F 6D 70 75 65 72 2E 00 32 32 30 31 00 4E 75 6D 65 72 6F 20 64 69 20 61 70 6C 69
49 6C 20 6E 75 6D 65 72 6F 20 74 6F 74 61 6C 65 20 64 69 20 62 79 74 65 20 74 72 61 73 6D 65 73 73 69 20 70 65 72 20 71 75 65 73 74 61 20 63 6F 6E 6E 65 73 7
0 32 32 31 39 00 49 6C 20 72 61 70 70 6F 72 74 6F 20 64 69 20 63 6F 6D 70 72 65 73 73 69 6F 6E 65 20 70 65 72 20 69 20 62 79 74 65 20 63 68 65 20 76 65 6E 67
6F 20 69 6E 20 74 65 6D 70 6F 2E 00 32 32 32 35 00 49 6C 20 6E 75 6D 65 72 6F 20 74 6F 74 61 6C 65 20 64 69 20 65 72 72 6F 72 69 20 64 69 20 73 6F 76 65 6E
20 69 6C 20 62 79 74 65 20 72 69 63 65 76 75 74 6F 20 E8 20 64 69 76 65 72 73 6F 20 64 61 20 71 75 65 6C 6F 20 61 74 74 65 73 6F 2E 00 32 32 32 39 00 49 6
0 65 20 53 6F 76 72 61 63 63 61 72 69 63 6F 20 62 75 66 66 65 72 20 70 65 72 20 71 75 65 73 74 61 20 63 6F 6E 6E 65 73 73 69 6F 6E 65 2E 00 32 32 33 33 00 49
73 65 63 6F 6E 64 6F 2E 00 32 32 34 33 00 49 6C 20 74 69 70 6F 20 6F 67 67 65 74 74 6F 20 52 41 53 20 67 65 73 74 69 73 63 65 20 74 75 74 74 65 20 6C 65 20
15:49
26/03/2024
Right Ctrl
15°C
Cloudy
Search
ENG
GA
15:49
26/03/2024

File Machine View Input Devices Help

~res-x64 - Blocco note

File Modifica Formato Visualizza ?

```
SRegshot 1.9.0 x64 ANSI
Comments:
Datetime: 2024/3/26 14:17:49  ,  2024/3/26 14:20:19
Computer: USER-PC , USER-PC
Username: user , user

----------------------------------
Keys deleted: 2
----------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum

----------------------------------
Keys added: 4
----------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}

----------------------------------
Values deleted: 6
----------------------------------
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum\0: "Root\LEGACY_PROCMON23\0000"
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum\Count: 0x00000001
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum\0: "Root\LEGACY_PROCMON23\0000"
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum\Count: 0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum\NextInstance: 0x00000001

----------------------------------
Values added: 26
----------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control\ActiveService: "PROCMON23"
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control\ActiveService: "PROCMON23"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
```

Windows 7 - malware analysis (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

~res-x64 - Blocco note

File Modifica Formato Visualizza ?


```
 20 64 69 20 63 6F 6E 74 65 6E 75 74 69 20 64 61 20 61 6C 74 72 69 20 70 65 65 72 20 64 65 6C 6C 61 20 73 75 63 63 75 72 73 61 6C 65 2E 00 36 34 35 31 00 4E
72 6F 76 61 74 65 20 65 20 72 69 66 69 75 74 61 74 65 20 61 6C 20 73 65 63 6F 6E 64 6F 20 69 6E 76 69 61 74 65 20 64 61 20 75 74 65 6E 74 69 20 61 75 74 6F 7
0 67 6C 69 20 75 74 65 6E 74 69 2E 00 35 32 36 31 00 56 69 73 75 61 6C 69 7A 7A 61 20 69 6C 20 6E 75 6D 65 72 6F 20 63 6F 72 72 65 6E 74 65 20 64 69 20 75 74
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3771313050-58705377-3452663501-1001\RefCount: 0x00000005
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-3771313050-58705377-3452663501-1001\RefCount: 0x00000006
HKLM\SYSTEM\RNG\Seed:  53 65 65 64 46 69 6C 65 01 00 00 00 D9 55 CE 46 DF 57 E5 FF 0F C0 B5 94 2C 66 9D 79 6C 6C 72 33 6B BE BE 6B B6 AB E2 0C A4 C2 25 9D 49
HKLM\SYSTEM\RNG\Seed:  53 65 65 64 46 69 6C 65 D2 6C 04 00 D6 82 48 E8 6F 31 99 56 B2 EC 8E 91 9B A1 A4 E0 35 03 6D B1 8F 49 E2 E9 D2 E8 7F C3 28 7C FB 4F EA
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\H
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2B 29 00 00 00 00 00 B5 77 C1 72 00 00 00 00
 00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 00 32 00 33 00 7D 00 5C 00 65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 00 65 00 78 00 65
43 00 00 00 00 00 78 7F CC C9 F0 1C F9 41 A1 1A 99 4B A5 A9 A5 4D 0D 00 00 00 01 00 00 00 72 7F 03 00 1C 04 00 00 E0 07 00 00 00 00 00 00 06 44 CE F1 87 7F 0
8 00 00 00 00 00 00 00 00 00 00 00 00 60 DF 0D 03 00 00 00 00 82 15 9A FD FE 07 00 00 50 BB 2F 08 00 00 00 00 30 35 04 08 00 00 00 00 90 73 42 08 00 00 00 00
 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\H
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2B 29 00 00 00 00 00 B5 77 C1 72 00 00 00 00
 00 36 00 37 00 44 00 45 00 30 00 42 00 32 00 38 00 46 00 43 00 32 00 33 00 7D 00 5C 00 65 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 2E 00 65 00 78 00 65
00 00 00 00 00 00 18 19 61 03 00 00 00 00 01 00 00 00 00 00 00 00 04 08 01 87 FF FF FF FF C8 3D FE FD FE 07 00 00 00 10 00 00 00 00 00 00 0C 00 00 00 00 00 0
F FE 07 00 00 48 43 8B 02 00 00 00 00 01 00 00 00 00 00 00 00 00 43 00 00 00 00 00 6E 00 02 00 00 00 00 00 01 00 00 00 00 00 00 00 0F 00 00 C0 00 00 00 00
 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  0B 00 00 00 01 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  0A 00 00 00 0B 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  0B 00 00 00 01 00 00 00 0A 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx:  0A 00 00 00 0B 00 00 00 01 00 00
```


```
----------------------------------
Total changes: 58
----------------------------------
```

IT 15:50 26/03/2024

15°C Cloudy Search ENG GA 15:50 26/03/2024

Windows 7 - malware analysis (Snapshot 1) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

~res-x64 - Blocco note

File Modifica Formato Visualizza ?

```
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum\Count: 0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum\NextInstance: 0x00000001

----------------------------------
Values added: 26
----------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control\ActiveService: "PROCMON23"
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control\ActiveService: "PROCMON23"
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11D
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-3771313050-58705377-345263501-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\90\Shell\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}

----------------------------------
Values modified: 20
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x00000003
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\010\Counter:  31 00 31 38 34 37 00 32 00 53 69 73 74 65 6D 61 00 34 00 4D 65 6D 6F 72 69 61 00 36 0
6 69 6E 63 6F 6C 61 74 61 00 33 32 00 53 63 72 69 74 74 75 72 65 20 69 6E 20 63 6F 70 69 61 2F 73 65 63 00 33 34 00 45 72 72 6F 72 69 20 69 6E 20 74 72 61 6E
```

IT 15:53 26/03/2024

Right Ctrl

15°C Cloudy

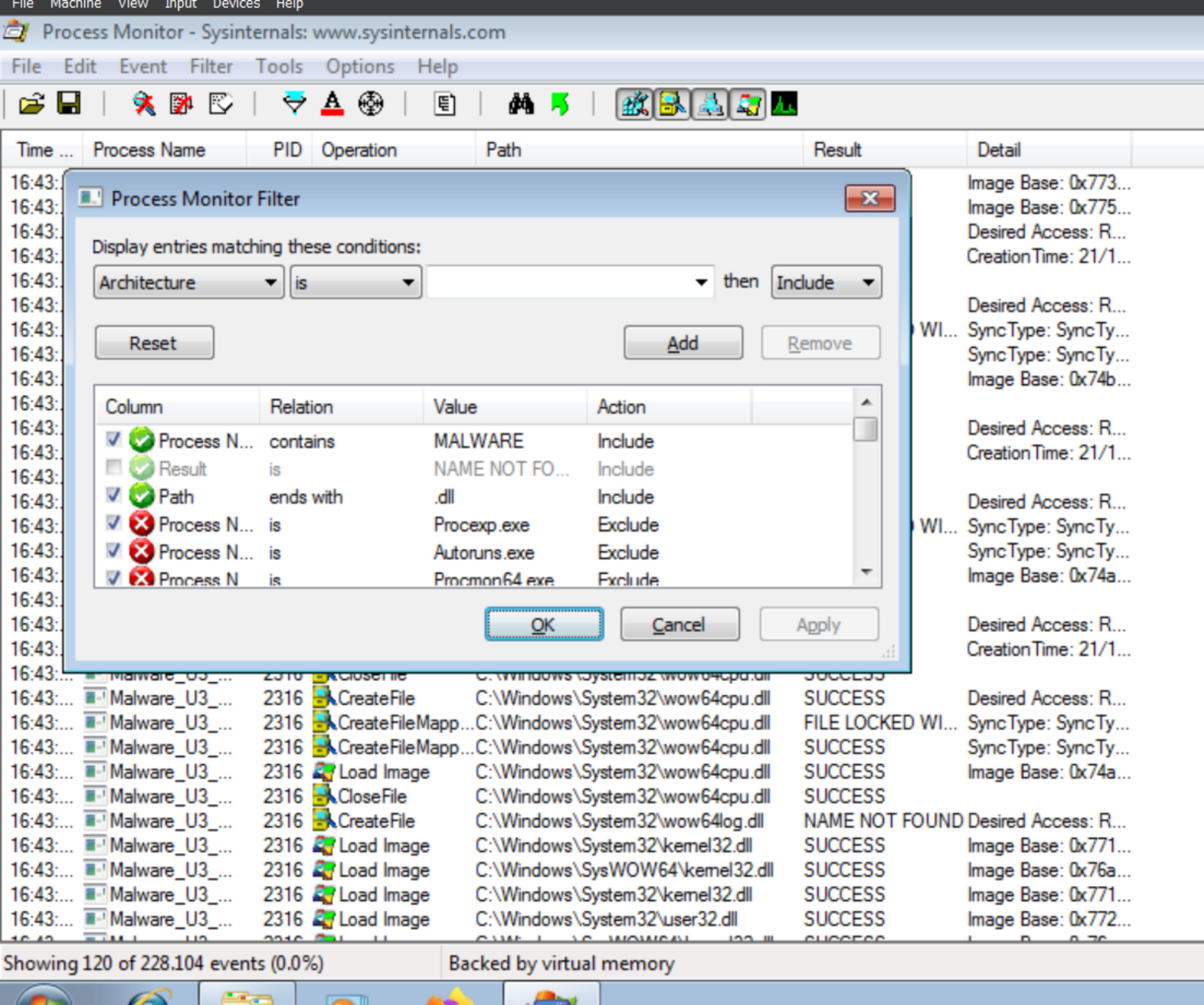
Search

ENG GA 15:53 26/03/2024

16:44:...	svchost.exe	452	QueryStandardI...	C:\Windows\System32\rsaenh.dll	SUCCESS	AllocationSize: 282...
16:44:...	svchost.exe	452	CreateFileMapp...	C:\Windows\System32\rsaenh.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:44:...	svchost.exe	452	QueryStandardI...	C:\Windows\System32\rsaenh.dll	SUCCESS	AllocationSize: 282...
16:44:...	svchost.exe	452	CreateFileMapp...	C:\Windows\System32\rsaenh.dll	SUCCESS	SyncType: SyncTypeOther
16:44:...	svchost.exe	452	CloseFile	C:\Windows\System32\rsaenh.dll	SUCCESS	
16:44:...	svchost.exe	452	CreateFile	C:\Windows\System32\rsaenh.dll	SUCCESS	Desired Access: R...
16:44:...	svchost.exe	452	QueryBasicInfor...	C:\Windows\System32\rsaenh.dll	SUCCESS	CreationTime: 14/0...
16:44:...	svchost.exe	452	CloseFile	C:\Windows\System32\rsaenh.dll	SUCCESS	
16:44:...	svchost.exe	452	CreateFile	C:\Windows\System32\rsaenh.dll	SUCCESS	Desired Access: R...
16:44:...	svchost.exe	452	CreateFileMapp...	C:\Windows\System32\rsaenh.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:44:...	svchost.exe	452	CreateFileMapp...	C:\Windows\System32\rsaenh.dll	SUCCESS	SyncType: SyncTy...
16:44:...	svchost.exe	452	Load Image	C:\Windows\System32\rsaenh.dll	SUCCESS	Image Base: 0x7fef...
16:44:...	svchost.exe	452	CloseFile	C:\Windows\System32\rsaenh.dll	SUCCESS	
16:44:...	svchost.exe	452	CreateFile	C:\Windows\System32\cryptbase.dll	SUCCESS	Desired Access: R...
16:44:...	svchost.exe	452	QueryBasicInfor...	C:\Windows\System32\cryptbase.dll	SUCCESS	CreationTime: 14/0...
16:44:...	svchost.exe	452	CloseFile	C:\Windows\System32\cryptbase.dll	SUCCESS	
16:44:...	svchost.exe	452	CreateFile	C:\Windows\System32\cryptbase.dll	SUCCESS	Desired Access: R...
16:44:...	svchost.exe	452	CreateFileMapp...	C:\Windows\System32\cryptbase.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:44:...	svchost.exe	452	CreateFileMapp...	C:\Windows\System32\cryptbase.dll	SUCCESS	SyncType: SyncTy...
16:44:...	svchost.exe	452	Load Image	C:\Windows\System32\cryptbase.dll	SUCCESS	Image Base: 0x7fef...
16:44:...	svchost.exe	452	CloseFile	C:\Windows\System32\cryptbase.dll	SUCCESS	
16:44:...	svchost.exe	452	ReadFile	C:\program files\windows defender\Mp...	SUCCESS	Offset: 480.256, Le...
16:44:...	svchost.exe	452	ReadFile	C:\program files\windows defender\Mp...	SUCCESS	Offset: 472.064, Le...
16:44:...	svchost.exe	452	ReadFile	C:\program files\windows defender\Mp...	SUCCESS	Offset: 398.336, Le...
16:44:...	svchost.exe	452	ReadFile	C:\program files\windows defender\Mp...	SUCCESS	Offset: 398.336, Le...
16:44:...	wmpnetwk.exe	2460	ReadFile	C:\Windows\System32\wtsapi32.dll	SUCCESS	Offset: 50.176, Len...
16:44:...	wmpnetwk.exe	2460	CreateFile	C:\Program Files\Windows Media Player...	NAME NOT FOUND	Desired Access: R...
16:44:...	wmpnetwk.exe	2460	CreateFile	C:\Windows\System32\winsta.dll	SUCCESS	Desired Access: R...
16:44:...	wmpnetwk.exe	2460	QueryBasicInfor...	C:\Windows\System32\winsta.dll	SUCCESS	CreationTime: 21/1...
16:44:...	wmpnetwk.exe	2460	CloseFile	C:\Windows\System32\winsta.dll	SUCCESS	
16:44:...	wmpnetwk.exe	2460	CreateFile	C:\Windows\System32\winsta.dll	SUCCESS	Desired Access: R...

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:44:...	svchost.exe	900	QueryBasicInfor...	C:\Windows\System32\bitsigd.dll	SUCCESS	CreationTime: 14/0...
16:44:...	svchost.exe	900	CloseFile	C:\Windows\System32\bitsigd.dll	SUCCESS	
16:44:...	svchost.exe	900	CreateFile	C:\Windows\System32\bitsigd.dll	SUCCESS	Desired Access: R...
16:44:...	svchost.exe	900	CreateFileMapp...	C:\Windows\System32\bitsigd.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:44:...	svchost.exe	900	QueryStandardI...	C:\Windows\System32\bitsigd.dll	SUCCESS	AllocationSize: 57....
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\bitsigd.dll	SUCCESS	Offset: 0, Length: 4...
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\bitsigd.dll	SUCCESS	Offset: 56.320, Len...
16:44:...	svchost.exe	900	CreateFileMapp...	C:\Windows\System32\bitsigd.dll	SUCCESS	SyncType: SyncTy...
16:44:...	svchost.exe	900	Load Image	C:\Windows\System32\bitsigd.dll	SUCCESS	Image Base: 0x7fef...
16:44:...	svchost.exe	900	CloseFile	C:\Windows\System32\bitsigd.dll	SUCCESS	
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\bitsigd.dll	SUCCESS	Offset: 54.784, Len...
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\bitsigd.dll	SUCCESS	Offset: 21.504, Len...
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\bitsigd.dll	SUCCESS	Offset: 1.024, Leng...
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\bitsigd.dll	SUCCESS	Offset: 52.224, Len...
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\bitsigd.dll	SUCCESS	Offset: 51.200, Len...
16:44:...	svchost.exe	900	CreateFile	C:\Windows\System32\upnp.dll	SUCCESS	Desired Access: R...
16:44:...	svchost.exe	900	QueryBasicInfor...	C:\Windows\System32\upnp.dll	SUCCESS	CreationTime: 21/1...
16:44:...	svchost.exe	900	CloseFile	C:\Windows\System32\upnp.dll	SUCCESS	
16:44:...	svchost.exe	900	CreateFile	C:\Windows\System32\upnp.dll	SUCCESS	Desired Access: R...
16:44:...	svchost.exe	900	CreateFileMapp...	C:\Windows\System32\upnp.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:44:...	svchost.exe	900	QueryStandardI...	C:\Windows\System32\upnp.dll	SUCCESS	AllocationSize: 266...
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\upnp.dll	SUCCESS	Offset: 0, Length: 4...
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\upnp.dll	SUCCESS	Offset: 259.584, Le...
16:44:...	svchost.exe	900	CreateFileMapp...	C:\Windows\System32\upnp.dll	SUCCESS	SyncType: SyncTy...
16:44:...	svchost.exe	900	Load Image	C:\Windows\System32\upnp.dll	SUCCESS	Image Base: 0x7fef...
16:44:...	svchost.exe	900	CloseFile	C:\Windows\System32\upnp.dll	SUCCESS	
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\upnp.dll	SUCCESS	Offset: 239.616, Le...
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\upnp.dll	SUCCESS	Offset: 194.048, Le...
16:44:...	svchost.exe	900	ReadFile	C:\Windows\System32\upnp.dll	SUCCESS	Offset: 1.536, Leng...
16:44:...	svchost.exe	900	CreateFile	C:\Windows\System32\winhttp.dll	SUCCESS	Desired Access: R...
16:44:...	svchost.exe	900	QueryBasicInfor...	C:\Windows\System32\winhttp.dll	SUCCESS	CreationTime: 21/1...

Showing 7.736 of 228.104 events (3.%) | Backed by virtual memory


File Machine View Input Devices Help
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path Result Detail
Process Monitor Filter
Display entries matching these conditions:
Architecture is then Include
Reset Add Remove
Column Relation Value Action
Process N... contains MALWARE Include
Result is NAME NOT FO... Include
Path ends with .dll Include
Process N... is Procexp.exe Exclude
Process N... is Autoruns.exe Exclude
Process N is Procmon64.exe Exclude
OK Cancel Apply
16:43:... Malware_U3_... 2316 CreateFile C:\Windows\System32\wow64cpu.dll SUCCESS Desired Access: R...
16:43:... Malware_U3_... 2316 CreateFileMapp... C:\Windows\System32\wow64cpu.dll FILE LOCKED WI... SyncType: SyncTy...
16:43:... Malware_U3_... 2316 CreateFileMapp... C:\Windows\System32\wow64cpu.dll SUCCESS SyncType: SyncTy...
16:43:... Malware_U3_... 2316 Load Image C:\Windows\System32\wow64cpu.dll SUCCESS Image Base: 0x74a...
16:43:... Malware_U3_... 2316 CloseFile C:\Windows\System32\wow64cpu.dll SUCCESS
16:43:... Malware_U3_... 2316 CreateFile C:\Windows\System32\wow64log.dll NAME NOT FOUND Desired Access: R...
16:43:... Malware_U3_... 2316 Load Image C:\Windows\System32\kernel32.dll SUCCESS Image Base: 0x771...
16:43:... Malware_U3_... 2316 Load Image C:\Windows\SysWOW64\kernel32.dll SUCCESS Image Base: 0x76a...
16:43:... Malware_U3_... 2316 Load Image C:\Windows\System32\kernel32.dll SUCCESS Image Base: 0x771...
16:43:... Malware_U3_... 2316 Load Image C:\Windows\System32\user32.dll SUCCESS Image Base: 0x772...
Showing 120 of 228,104 events (0.0%)
Backed by virtual memory