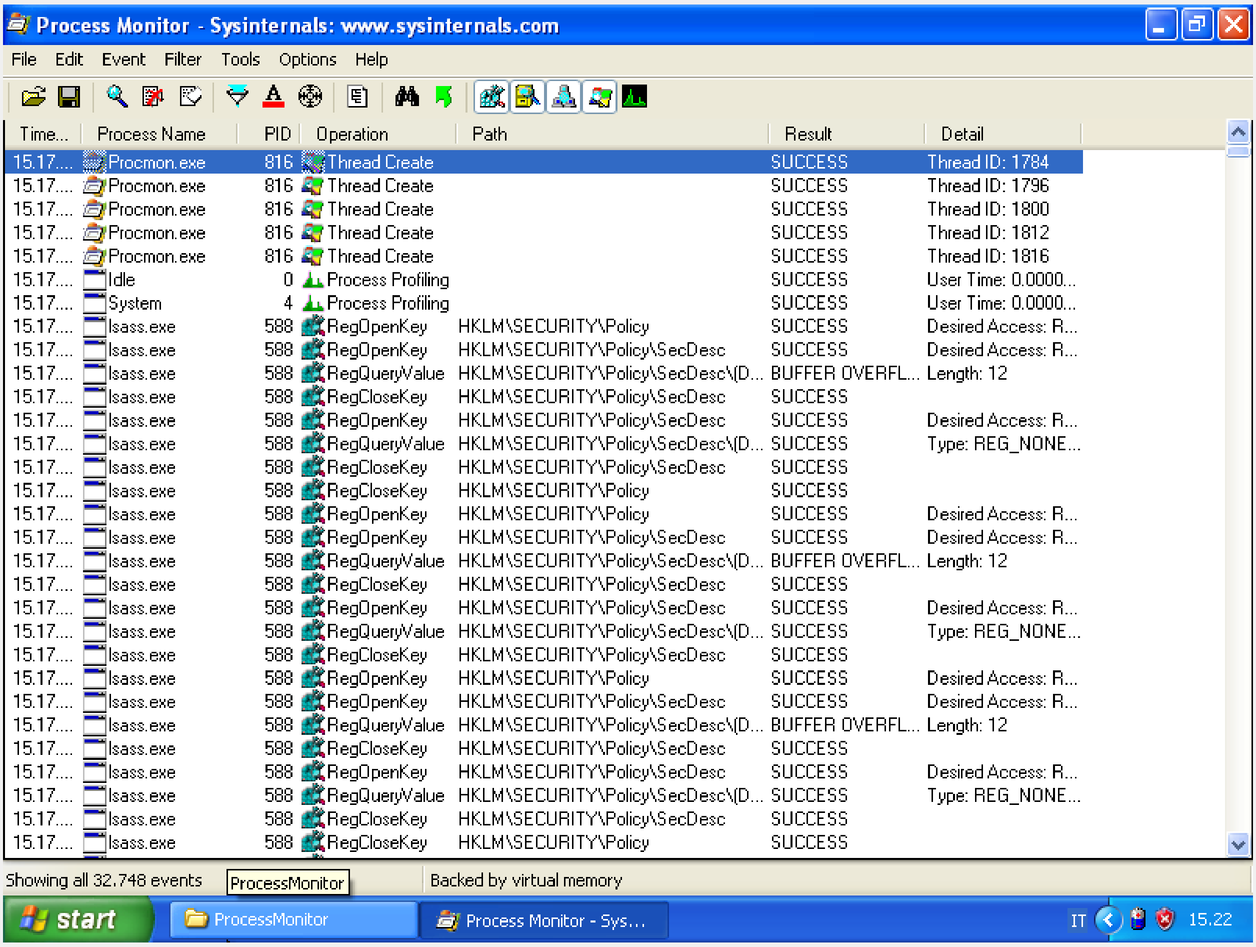
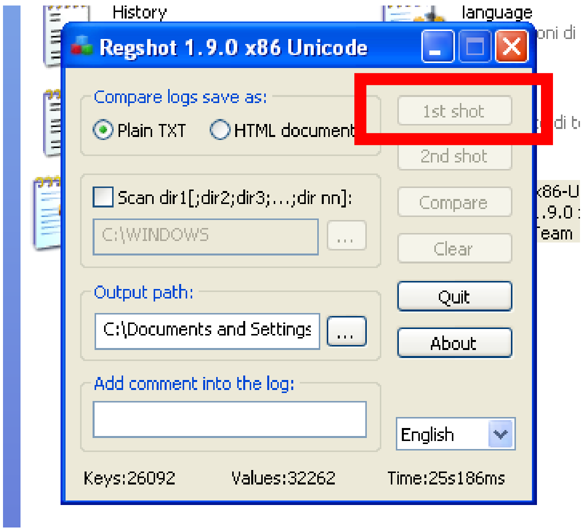

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
start
ProcessMonitor
Process Monitor - Sys...
IT
15.22

```
Time...   Process Name   PID  Operation      Path                                  Result           Detail
15.17.... Procmon.exe    816  Thread Create                                        SUCCESS          Thread ID: 1784
15.17.... Procmon.exe    816  Thread Create                                        SUCCESS          Thread ID: 1796
15.17.... Procmon.exe    816  Thread Create                                        SUCCESS          Thread ID: 1800
15.17.... Procmon.exe    816  Thread Create                                        SUCCESS          Thread ID: 1812
15.17.... Procmon.exe    816  Thread Create                                        SUCCESS          Thread ID: 1816
15.17.... Idle             0  Process Profiling                                    SUCCESS          User Time: 0.0000...
15.17.... System           4  Process Profiling                                    SUCCESS          User Time: 0.0000...
15.17.... lsass.exe      588  RegOpenKey     HKLM\SECURITY\Policy                  SUCCESS          Desired Access: R...
15.17.... lsass.exe      588  RegOpenKey     HKLM\SECURITY\Policy\SecDesc          SUCCESS          Desired Access: R...
15.17.... lsass.exe      588  RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D...    BUFFER OVERFL... Length: 12
15.17.... lsass.exe      588  RegCloseKey    HKLM\SECURITY\Policy\SecDesc          SUCCESS
15.17.... lsass.exe      588  RegOpenKey     HKLM\SECURITY\Policy\SecDesc          SUCCESS          Desired Access: R...
15.17.... lsass.exe      588  RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D...    SUCCESS          Type: REG_NONE...
15.17.... lsass.exe      588  RegCloseKey    HKLM\SECURITY\Policy\SecDesc          SUCCESS
15.17.... lsass.exe      588  RegCloseKey    HKLM\SECURITY\Policy                  SUCCESS
15.17.... lsass.exe      588  RegOpenKey     HKLM\SECURITY\Policy                  SUCCESS          Desired Access: R...
15.17.... lsass.exe      588  RegOpenKey     HKLM\SECURITY\Policy\SecDesc          SUCCESS          Desired Access: R...
15.17.... lsass.exe      588  RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D...    BUFFER OVERFL... Length: 12
15.17.... lsass.exe      588  RegCloseKey    HKLM\SECURITY\Policy\SecDesc          SUCCESS
15.17.... lsass.exe      588  RegOpenKey     HKLM\SECURITY\Policy\SecDesc          SUCCESS          Desired Access: R...
15.17.... lsass.exe      588  RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D...    SUCCESS          Type: REG_NONE...
15.17.... lsass.exe      588  RegCloseKey    HKLM\SECURITY\Policy\SecDesc          SUCCESS
15.17.... lsass.exe      588  RegOpenKey     HKLM\SECURITY\Policy                  SUCCESS          Desired Access: R...
15.17.... lsass.exe      588  RegOpenKey     HKLM\SECURITY\Policy\SecDesc          SUCCESS          Desired Access: R...
15.17.... lsass.exe      588  RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D...    BUFFER OVERFL... Length: 12
15.17.... lsass.exe      588  RegCloseKey    HKLM\SECURITY\Policy\SecDesc          SUCCESS
15.17.... lsass.exe      588  RegOpenKey     HKLM\SECURITY\Policy\SecDesc          SUCCESS          Desired Access: R...
15.17.... lsass.exe      588  RegQueryValue  HKLM\SECURITY\Policy\SecDesc\(D...    SUCCESS          Type: REG_NONE...
15.17.... lsass.exe      588  RegCloseKey    HKLM\SECURITY\Policy\SecDesc          SUCCESS
15.17.... lsass.exe      588  RegCloseKey    HKLM\SECURITY\Policy                  SUCCESS
```

Showing all 32.748 events   Backed by virtual memory



Compare logs save as:
● Plain TXT ○ HTML document

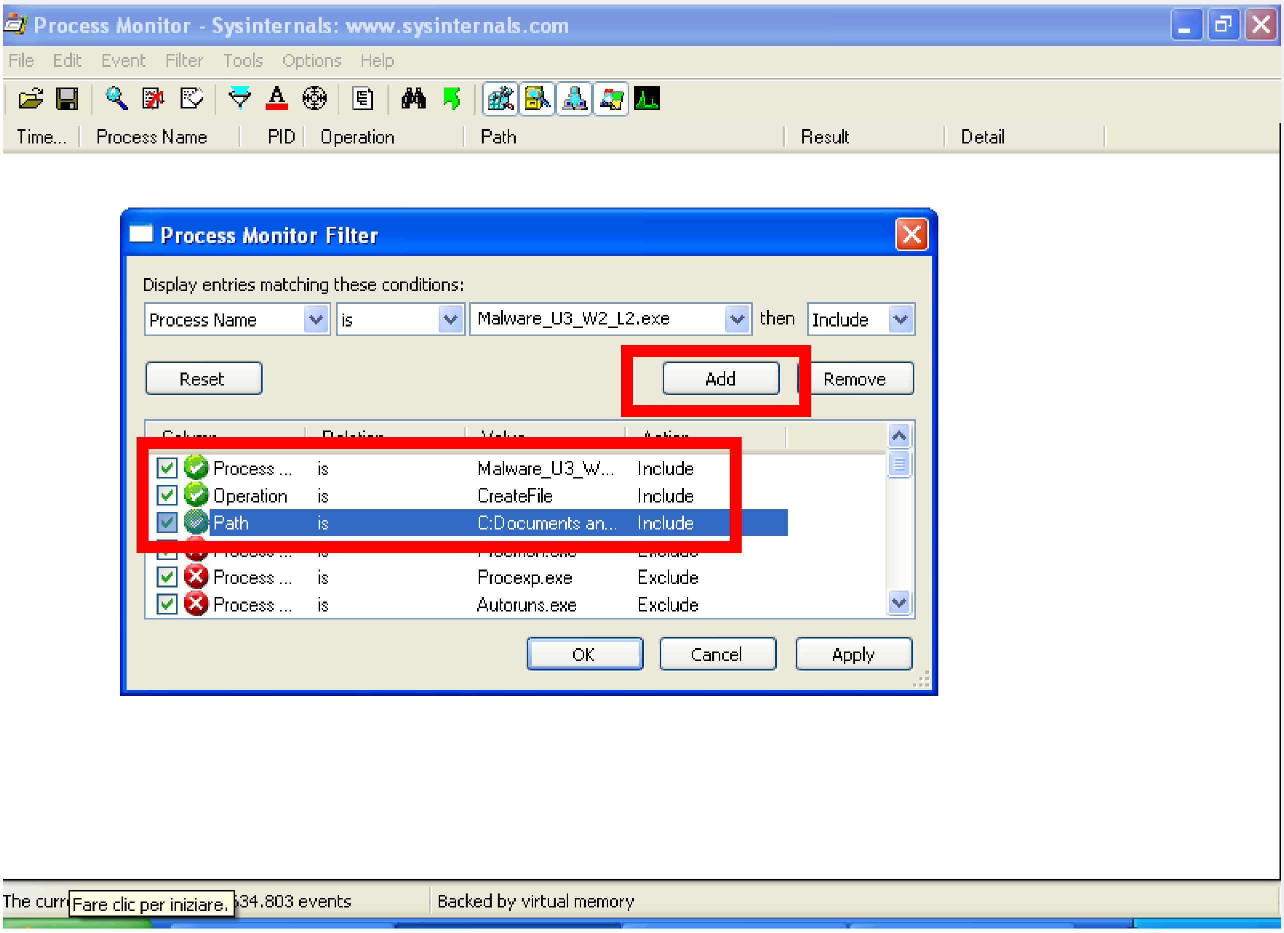
□ Scan dir1[;dir2;dir3;...;dir nn]:
C:\WINDOWS

Output path:
C:\Documents and Settings

Add comment into the log:

English

Keys:26092 Values:32262 Time:25s186ms

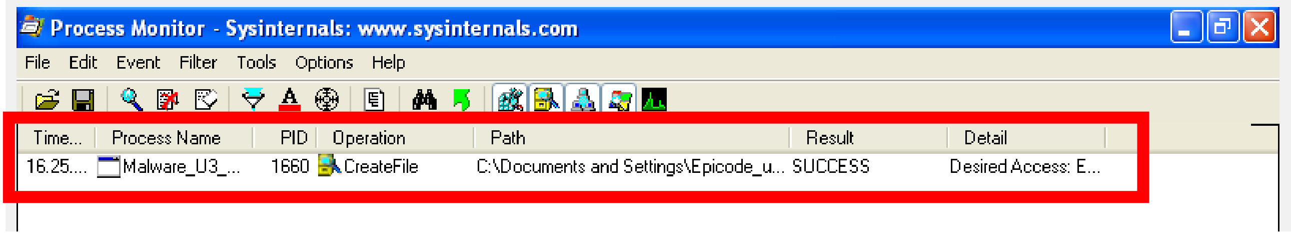

Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Process Monitor Filter
Reset
Add
Remove
OK
Cancel
Apply

Display entries matching these conditions:

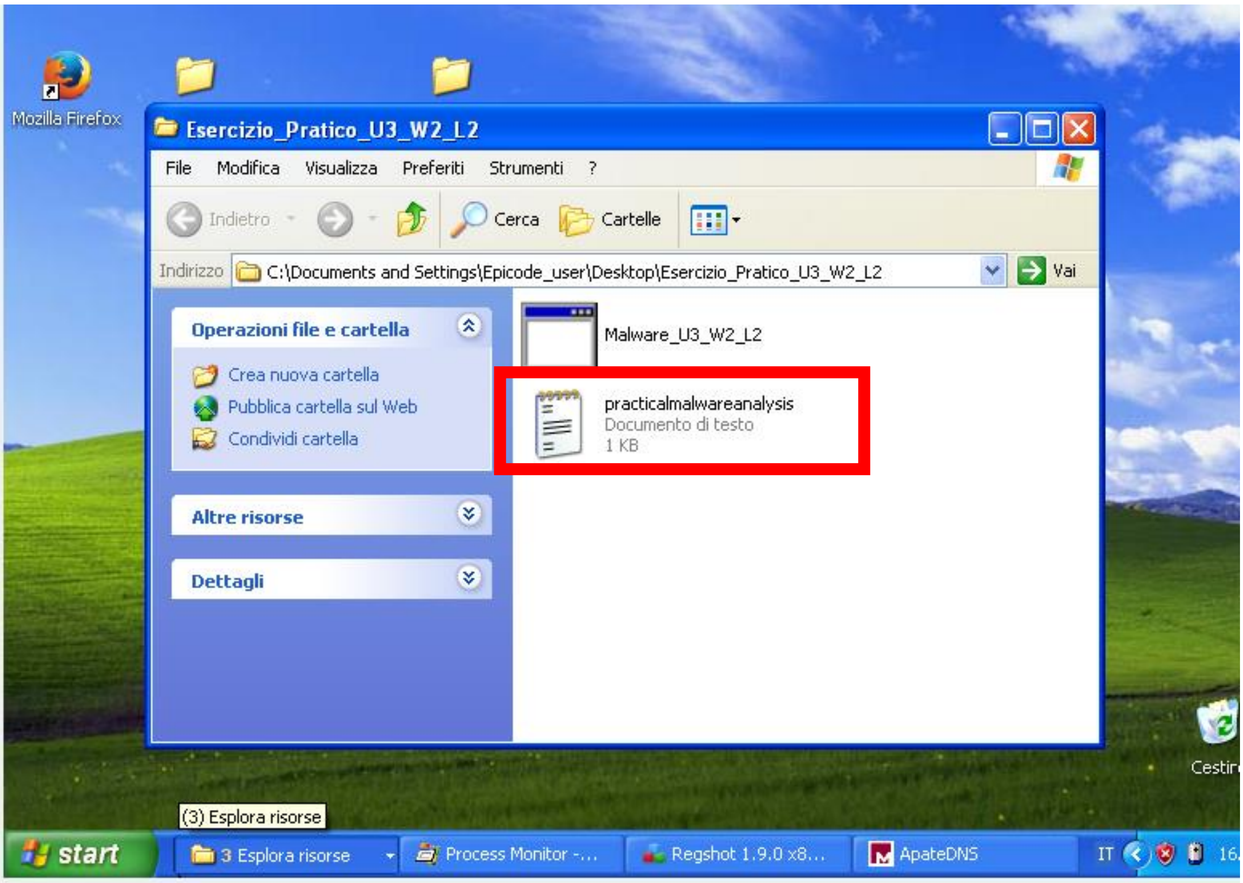
Process Name | is | Malware_U3_W2_L2.exe | then | Include

Column	Relation	Value	Action
☑ Process ...	is	Malware_U3_W...	Include
☑ Operation	is	CreateFile	Include
☑ Path	is	C:Documents an...	Include
☑ Process ...	is	Procmon.exe	Exclude
☑ Process ...	is	Procexp.exe	Exclude
☑ Process ...	is	Autoruns.exe	Exclude

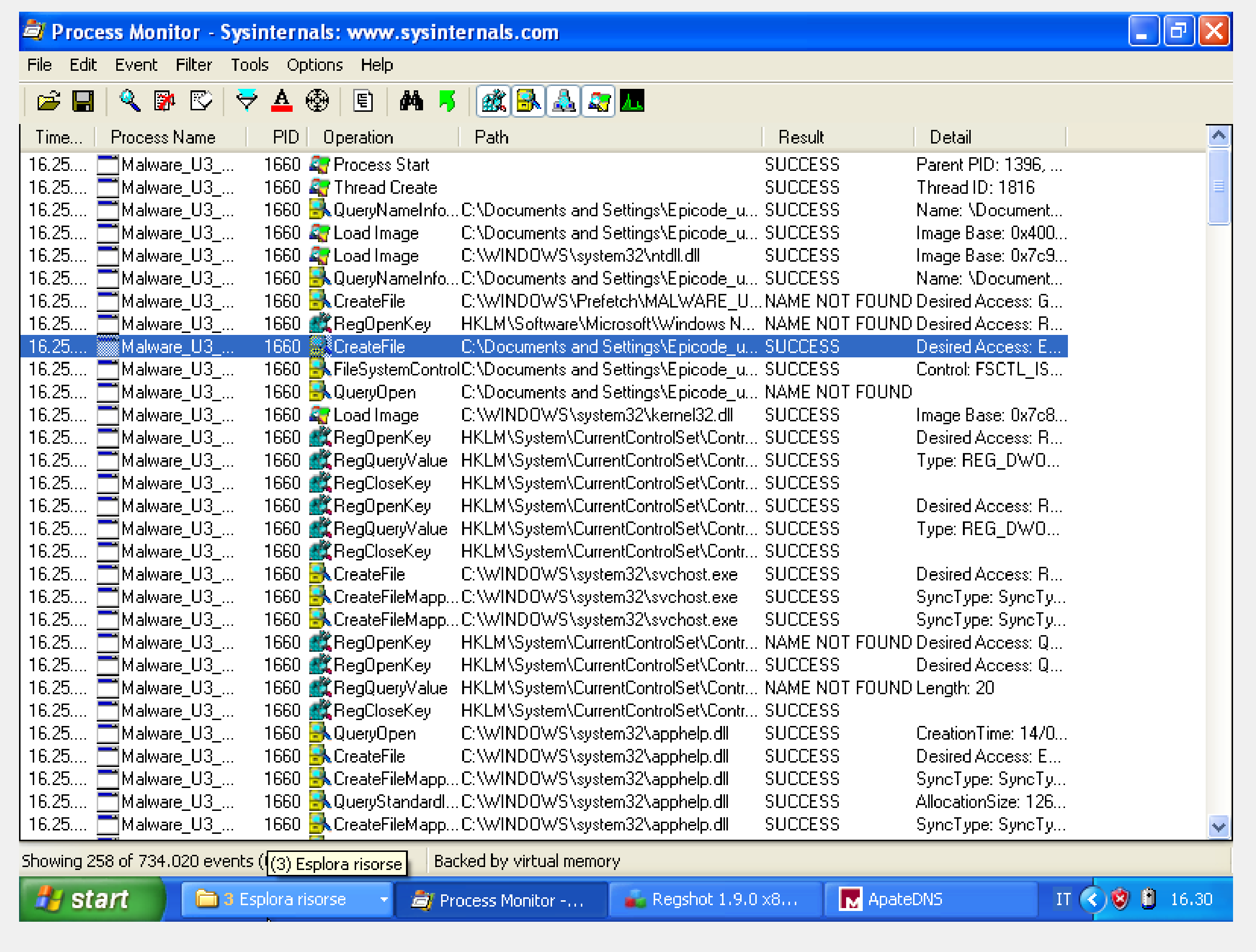
```
The curr Fare clic per iniziare. 34.803 events    Backed by virtual memory
```


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path	Result	Detail
16.25....	Malware_U3_...	1660	CreateFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Desired Access: E...

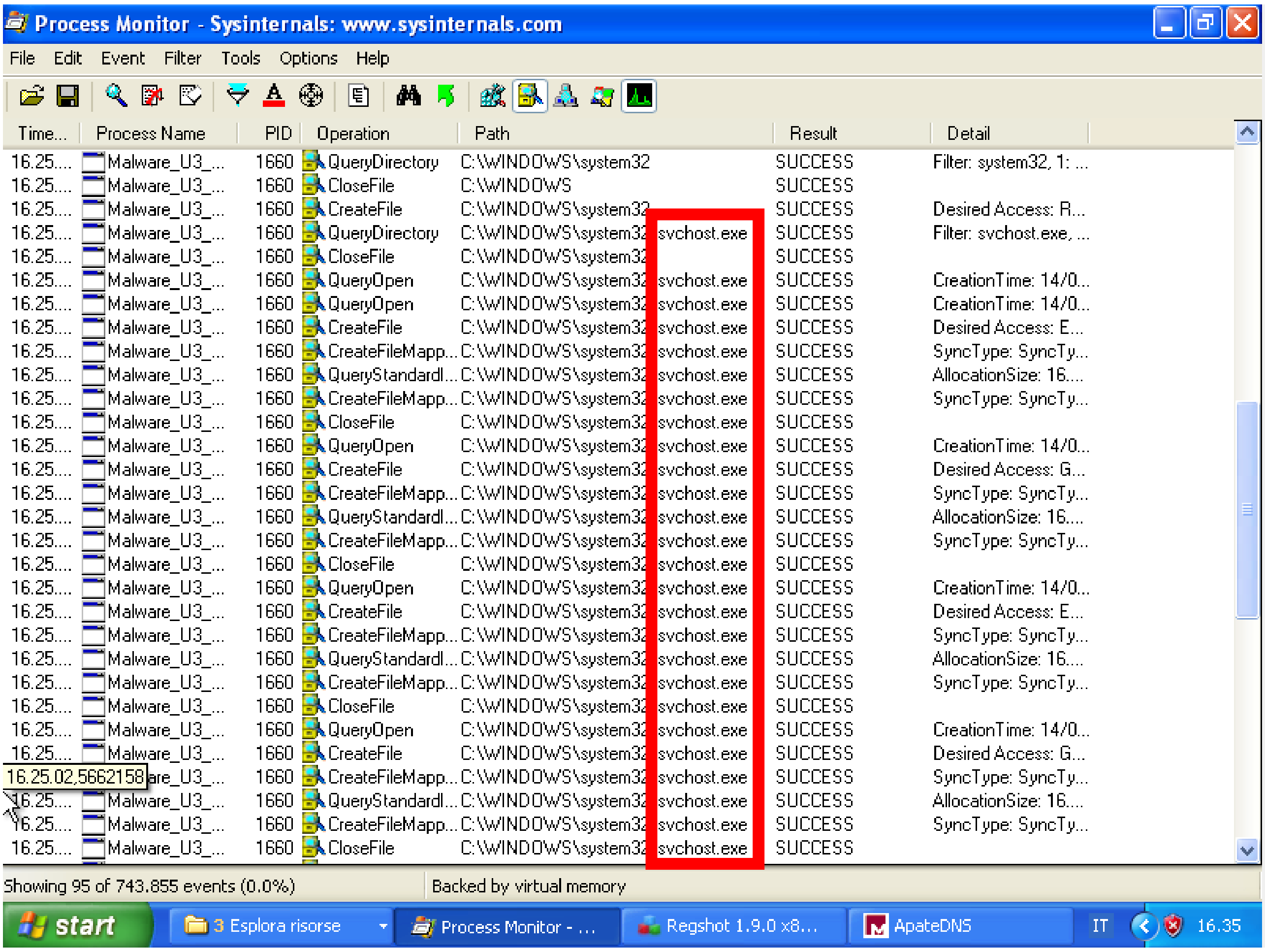


Indirizzo C:\Documents and Settings\Epicode_user\Desktop\Esercizio_Pratico_U3_W2_L2



Time...	Process Name	PID	Operation	Path	Result	Detail
16.25....	Malware_U3_...	1660	Process Start		SUCCESS	Parent PID: 1396, ...
16.25....	Malware_U3_...	1660	Thread Create		SUCCESS	Thread ID: 1816
16.25....	Malware_U3_...	1660	QueryNameInfo...	C:\Documents and Settings\Epicode_u...	SUCCESS	Name: \Document...
16.25....	Malware_U3_...	1660	Load Image	C:\Documents and Settings\Epicode_u...	SUCCESS	Image Base: 0x400...
16.25....	Malware_U3_...	1660	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
16.25....	Malware_U3_...	1660	QueryNameInfo...	C:\Documents and Settings\Epicode_u...	SUCCESS	Name: \Document...
16.25....	Malware_U3_...	1660	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U...	NAME NOT FOUND	Desired Access: G...
16.25....	Malware_U3_...	1660	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
16.25....	Malware_U3_...	1660	CreateFile	C:\Documents and Settings\Epicode_u...	SUCCESS	Desired Access: E...
16.25....	Malware_U3_...	1660	FileSystemControl	C:\Documents and Settings\Epicode_u...	SUCCESS	Control: FSCTL_IS...
16.25....	Malware_U3_...	1660	QueryOpen	C:\Documents and Settings\Epicode_u...	NAME NOT FOUND	
16.25....	Malware_U3_...	1660	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
16.25....	Malware_U3_...	1660	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
16.25....	Malware_U3_...	1660	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
16.25....	Malware_U3_...	1660	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16.25....	Malware_U3_...	1660	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
16.25....	Malware_U3_...	1660	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
16.25....	Malware_U3_...	1660	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16.25....	Malware_U3_...	1660	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: R...
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
16.25....	Malware_U3_...	1660	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
16.25....	Malware_U3_...	1660	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 20
16.25....	Malware_U3_...	1660	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16.25....	Malware_U3_...	1660	QueryOpen	C:\WINDOWS\system32\apphelp.dll	SUCCESS	CreationTime: 14/0...
16.25....	Malware_U3_...	1660	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: E...
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	QueryStandardI...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	AllocationSize: 126...
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...

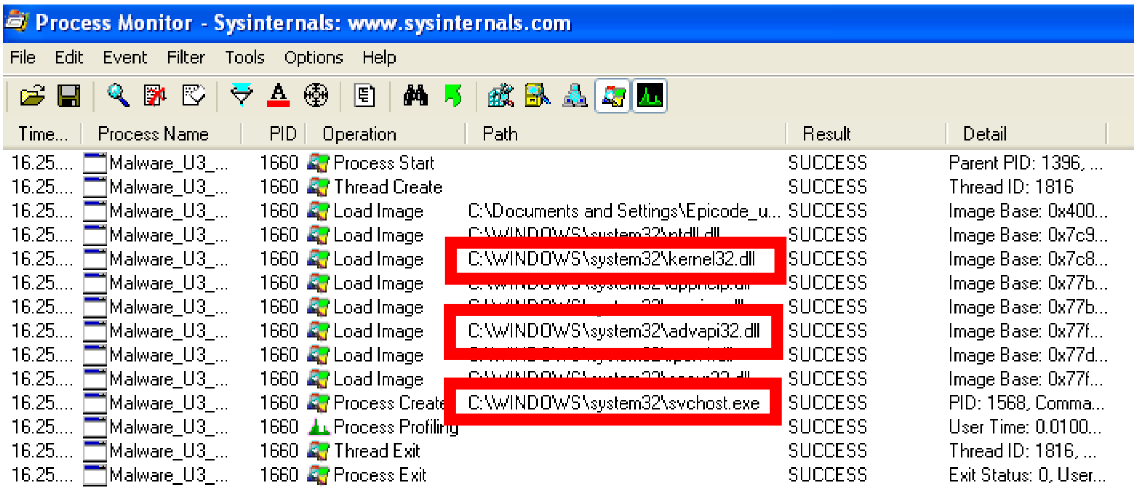
Showing 258 of 734.020 events (| (3) Esplora risorse | Backed by virtual memory


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

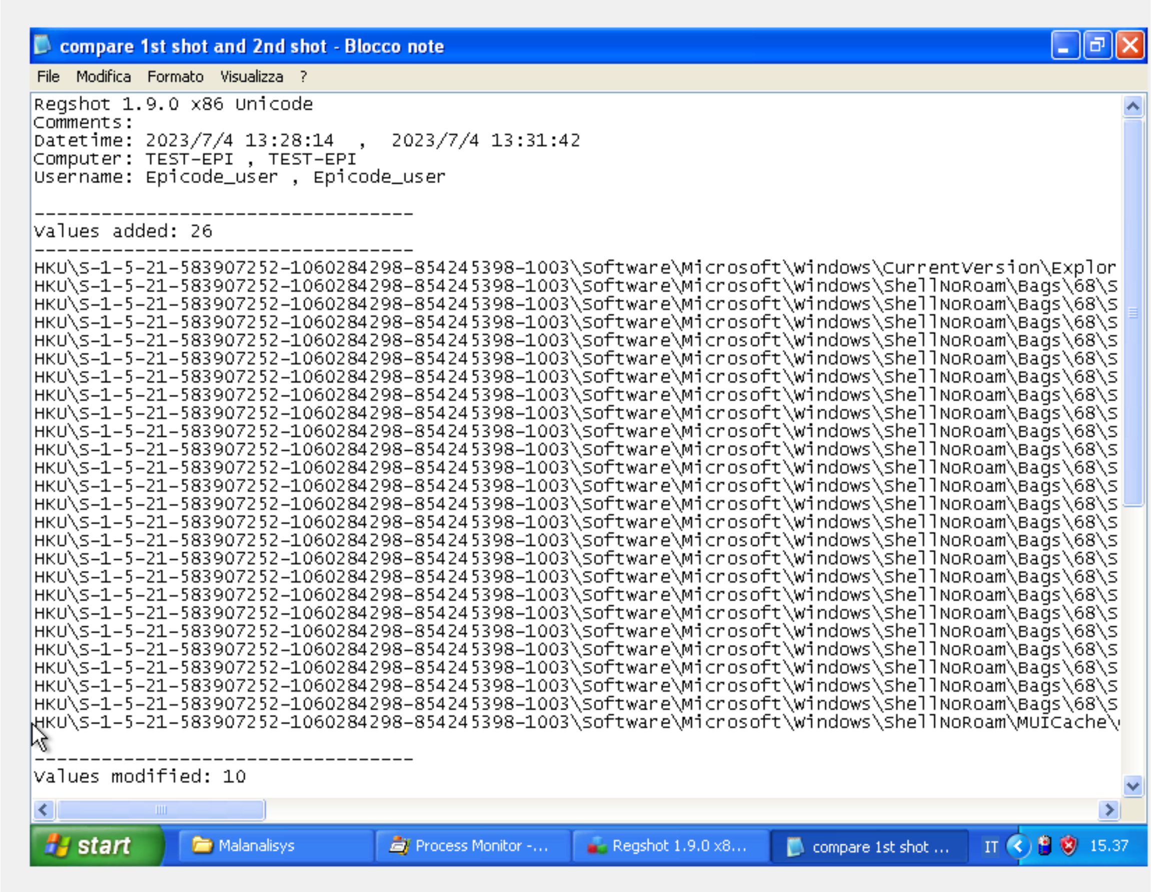
Time...	Process Name	PID	Operation	Path	Result	Detail
16.25....	Malware_U3_...	1660	QueryDirectory	C:\WINDOWS\system32	SUCCESS	Filter: system32, 1: ...
16.25....	Malware_U3_...	1660	CloseFile	C:\WINDOWS	SUCCESS	
16.25....	Malware_U3_...	1660	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: R...
16.25....	Malware_U3_...	1660	QueryDirectory	C:\WINDOWS\system32\svchost.exe	SUCCESS	Filter: svchost.exe, ...
16.25....	Malware_U3_...	1660	CloseFile	C:\WINDOWS\system32	SUCCESS	
16.25....	Malware_U3_...	1660	QueryOpen	C:\WINDOWS\system32\svchost.exe	SUCCESS	CreationTime: 14/0...
16.25....	Malware_U3_...	1660	QueryOpen	C:\WINDOWS\system32\svchost.exe	SUCCESS	CreationTime: 14/0...
16.25....	Malware_U3_...	1660	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: E...
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	QueryStandardI...	C:\WINDOWS\system32\svchost.exe	SUCCESS	AllocationSize: 16....
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	CloseFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	
16.25....	Malware_U3_...	1660	QueryOpen	C:\WINDOWS\system32\svchost.exe	SUCCESS	CreationTime: 14/0...
16.25....	Malware_U3_...	1660	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: G...
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	QueryStandardI...	C:\WINDOWS\system32\svchost.exe	SUCCESS	AllocationSize: 16....
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	CloseFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	
16.25....	Malware_U3_...	1660	QueryOpen	C:\WINDOWS\system32\svchost.exe	SUCCESS	CreationTime: 14/0...
16.25....	Malware_U3_...	1660	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: E...
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	QueryStandardI...	C:\WINDOWS\system32\svchost.exe	SUCCESS	AllocationSize: 16....
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	CloseFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	
16.25....	Malware_U3_...	1660	QueryOpen	C:\WINDOWS\system32\svchost.exe	SUCCESS	CreationTime: 14/0...
16.25....	Malware_U3_...	1660	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: G...
16.25.02,5662158	are_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	QueryStandardI...	C:\WINDOWS\system32\svchost.exe	SUCCESS	AllocationSize: 16....
16.25....	Malware_U3_...	1660	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
16.25....	Malware_U3_...	1660	CloseFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	

Showing 95 of 743.855 events (0.0%) Backed by virtual memory

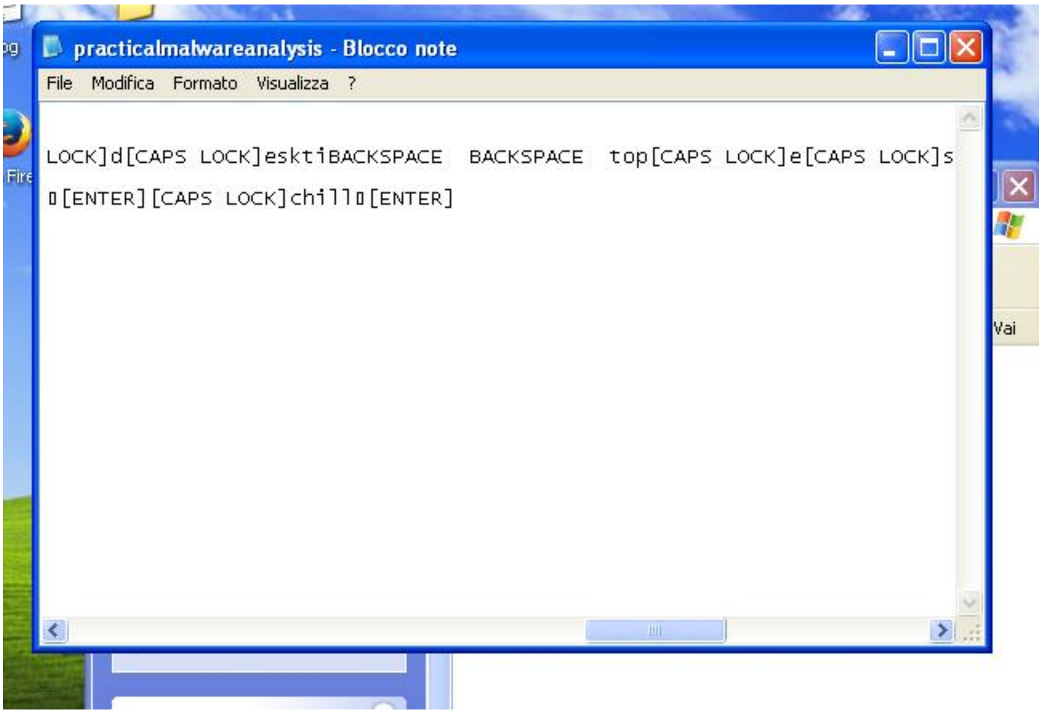
THREAD E PROCESSI


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path	Result	Detail
16.25....	Malware_U3_...	1660	Process Start		SUCCESS	Parent PID: 1396, ...
16.25....	Malware_U3_...	1660	Thread Create		SUCCESS	Thread ID: 1816
16.25....	Malware_U3_...	1660	Load Image	C:\Documents and Settings\Epicode_u...	SUCCESS	Image Base: 0x400...
16.25....	Malware_U3_...	1660	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
16.25....	Malware_U3_...	1660	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
16.25....	Malware_U3_...	1660	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b...
16.25....	Malware_U3_...	1660	Load Image	C:\WINDOWS\system32\[illegible].dll	SUCCESS	Image Base: 0x77b...
16.25....	Malware_U3_...	1660	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77f...
16.25....	Malware_U3_...	1660	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77d...
16.25....	Malware_U3_...	1660	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
16.25....	Malware_U3_...	1660	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1568, Comma...
16.25....	Malware_U3_...	1660	Process Profiling		SUCCESS	User Time: 0.0100...
16.25....	Malware_U3_...	1660	Thread Exit		SUCCESS	Thread ID: 1816, ...
16.25....	Malware_U3_...	1660	Process Exit		SUCCESS	Exit Status: 0, User...

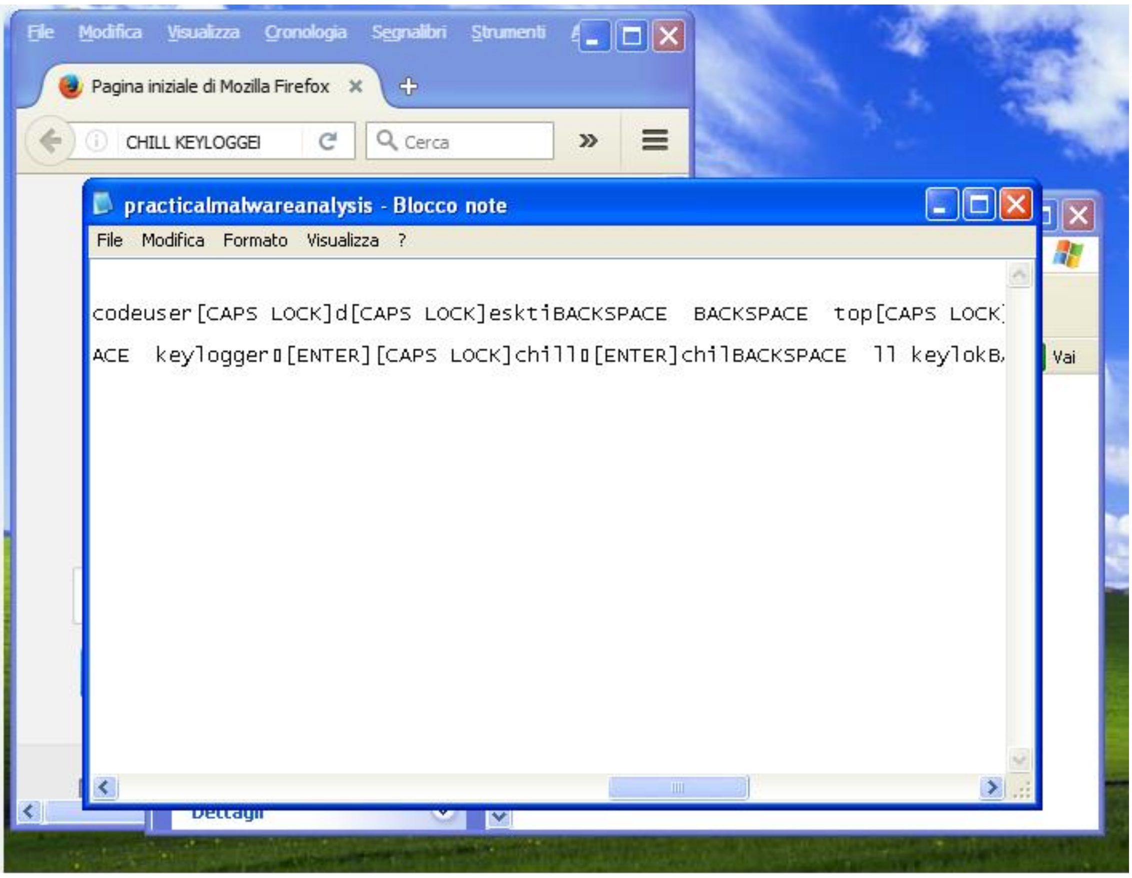


```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2023/7/4 13:28:14  ,  2023/7/4 13:31:42
Computer: TEST-EPI , TEST-EPI
Username: Epicode_user , Epicode_user

----------------------------------
Values added: 26
----------------------------------
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\CurrentVersion\Explor
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\68\S
HKU\S-1-5-21-583907252-1060284298-854245398-1003\Software\Microsoft\Windows\ShellNoRoam\MUICache\

----------------------------------
Values modified: 10
```



practicalmalwareanalysis - Blocco note
File Modifica Formato Visualizza ?
Fire
Vai

```
LOCK]d[CAPS LOCK]esktiBACKSPACE  BACKSPACE  top[CAPS LOCK]e[CAPS LOCK]s

▯[ENTER][CAPS LOCK]chill▯[ENTER]
```


File Modifica Visualizza Cronologia Segnalibri Strumenti
Pagina iniziale di Mozilla Firefox
CHILL KEYLOGGEI
Cerca
practicalmalwareanalysis - Blocco note
File Modifica Formato Visualizza ?
Vai
Dettagli

```
codeuser[CAPS LOCK]d[CAPS LOCK]esktiBACKSPACE  BACKSPACE  top[CAPS LOCK]
ACE  keylogger□[ENTER][CAPS LOCK]chill□[ENTER]chilBACKSPACE  ll keylokB
```