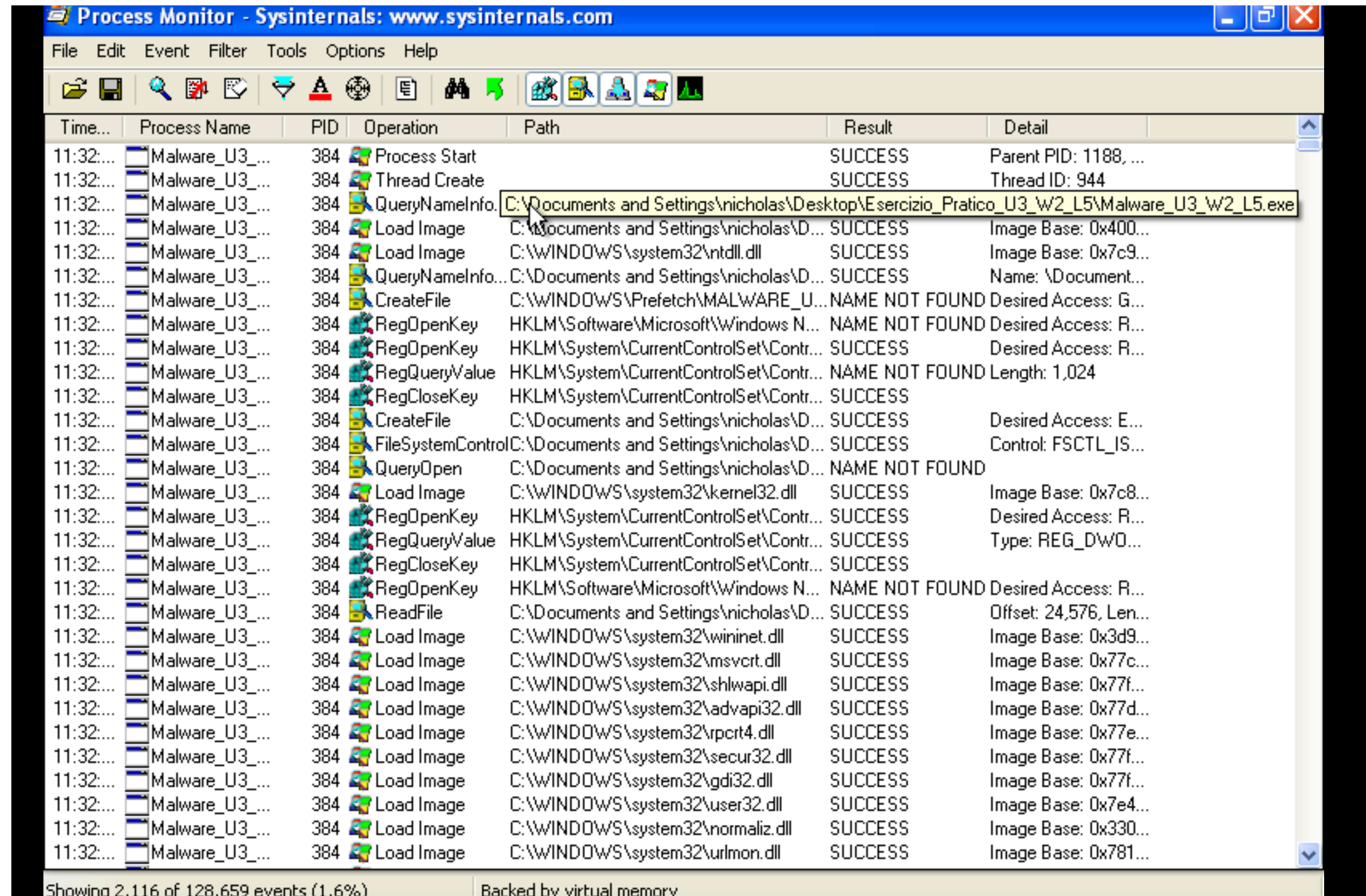


Malware Analysis



Process Monitor - Sysinternals: www.sysinternals.com

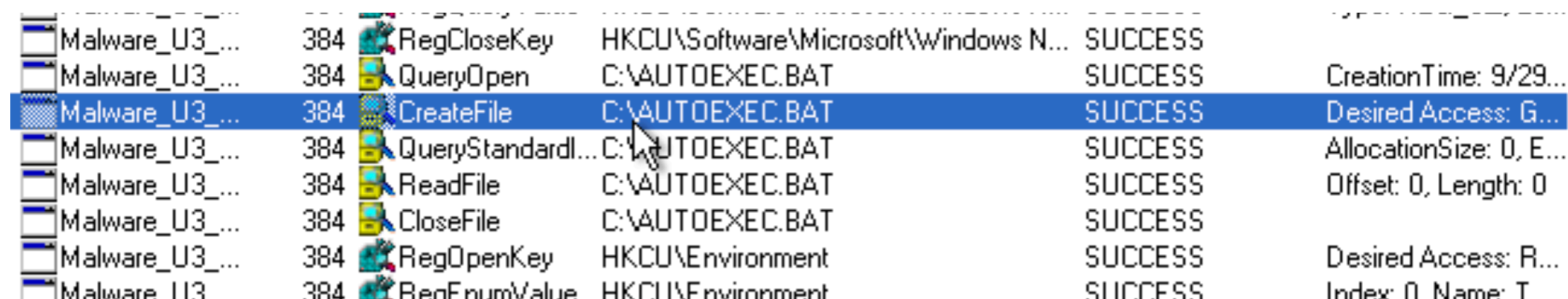
Time...	Process Name	PID	Operation	Path	Result	Detail
11:32:...	Malware_U3_...	384	Process Start		SUCCESS	Parent PID: 1188, ...
11:32:...	Malware_U3_...	384	Thread Create		SUCCESS	Thread ID: 944
11:32:...	Malware_U3_...	384	QueryNameInfo...	C:\Documents and Settings\nicholas\Desktop\Esercizio_Pratico_U3_W2_L5\Malware_U3_W2_L5.exe		
11:32:...	Malware_U3_...	384	Load Image	C:\Documents and Settings\nicholas\D...	SUCCESS	Image Base: 0x400...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
11:32:...	Malware_U3_...	384	QueryNameInfo...	C:\Documents and Settings\nicholas\D...	SUCCESS	Name: \Document...
11:32:...	Malware_U3_...	384	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U...	NAME NOT FOUND	Desired Access: G...
11:32:...	Malware_U3_...	384	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
11:32:...	Malware_U3_...	384	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
11:32:...	Malware_U3_...	384	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1,024
11:32:...	Malware_U3_...	384	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
11:32:...	Malware_U3_...	384	CreateFile	C:\Documents and Settings\nicholas\D...	SUCCESS	Desired Access: E...
11:32:...	Malware_U3_...	384	FileSystemControl	C:\Documents and Settings\nicholas\D...	SUCCESS	Control: FSCTL_IS...
11:32:...	Malware_U3_...	384	QueryOpen	C:\Documents and Settings\nicholas\D...	NAME NOT FOUND	
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
11:32:...	Malware_U3_...	384	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
11:32:...	Malware_U3_...	384	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWD...
11:32:...	Malware_U3_...	384	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
11:32:...	Malware_U3_...	384	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
11:32:...	Malware_U3_...	384	ReadFile	C:\Documents and Settings\nicholas\D...	SUCCESS	Offset: 24,576, Len...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\wininet.dll	SUCCESS	Image Base: 0x3d9...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Image Base: 0x77c...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	Image Base: 0x77f...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 0x77f...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x7e4...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\normaliz.dll	SUCCESS	Image Base: 0x330...
11:32:...	Malware_U3_...	384	Load Image	C:\WINDOWS\system32\urlmon.dll	SUCCESS	Image Base: 0x781...

Showing 2,116 of 128,659 events (1.6%) Backed by virtual memory

- Avviando il programma Procmon è possibile visualizzare tutti i processi attivi sul pc e tutto ciò che stanno facendo
- Nel caso di questo test ho sestetato il filtro per l'unico processo che interessava a me ovvero il malware installato sulla macchina xp, per poterne studiare il comportamento
- Dalla figura a sinistra si evince la panoramica delle azioni che una volta avviato, il malware ha eseguito

Malware_U3_...	384	QueryNameInfo...	C:\Documents and Settings\nicholas\D...	SUCCESS	Name: \Document...
Malware_U3_...	384	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L5.EXE-1CF2978C.pf	Desired Access: G...	
Malware_U3_...	384	RegOpenKey	HKLM\Software\Microsoft\Windows	NAME NOT FOUND	Desired Access: R...
Malware_U3_...	384	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
Malware_U3_...	384	RegQueryValue	HKLM\System\CurrentControlSet\Contr	NAME NOT FOUND	Length: 1,024

- Acquisisce significativa importanza l'azione 'CreateFile' in quando ci dice che è stato appunto creato un file che potrebbe essere ancora più dannoso per il pc



Malware_U3_...	384	RegCloseKey	HKCU\Software\Microsoft\Windows N...	SUCCESS	
Malware_U3_...	384	QueryOpen	C:\AUTOEXEC.BAT	SUCCESS	CreationTime: 9/29...
Malware_U3_...	384	CreateFile	C:\AUTOEXEC.BAT	SUCCESS	Desired Access: G...
Malware_U3_...	384	QueryStandardl...	C:\AUTOEXEC.BAT	SUCCESS	AllocationSize: 0, E...
Malware_U3_...	384	ReadFile	C:\AUTOEXEC.BAT	SUCCESS	Offset: 0, Length: 0
Malware_U3_...	384	CloseFile	C:\AUTOEXEC.BAT	SUCCESS	
Malware_U3_...	384	RegOpenKey	HKCU\Environment	SUCCESS	Desired Access: R...
Malware_U3_...	384	RegEnumValue	HKCU\Environment	SUCCESS	Index: 0 Name: T...

Regshot

```
Regshot 1.9.0 x86 Unicode
Commenti:
Dataora:2023/11/1 10:43:43 , 2023/11/1 10:44:24
Computer:NICHOLAS-EDB25A , NICHOLAS-EDB25A
Username:nicholas , nicholas

-----
Variazioni totali:0
-----
```

```
Commenti:
Dataora:2023/11/1 10:41:07 , 2023/11/1 10:41:40
Computer:NICHOLAS-EDB25A , NICHOLAS-EDB25A
Username:nicholas , nicholas

-----
Valore modificato:3
-----
HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed: 0F 0B 6C 71 24 E8 CB 64 DD 6B 18 45 36 30 B7 B2 F:
HKLM\SOFTWARE\Microsoft\Cryptography\ RNG\Seed: C6 1B 74 85 0F F6 E6 06 D7 4C FA 4F 4E 5F 5A 66 5
HKU\S-1-5-21-1645522239-725345543-1614895754-1003\Software\Microsoft\windows\CurrentVersion\Explo
HKU\S-1-5-21-1645522239-725345543-1614895754-1003\Software\Microsoft\windows\CurrentVersion\Explo
HKU\S-1-5-21-1645522239-725345543-1614895754-1003\Software\Microsoft\windows\CurrentVersion\Explo
HKU\S-1-5-21-1645522239-725345543-1614895754-1003\Software\Microsoft\windows\CurrentVersion\Explo

-----
File [attributi?] modificato:3
-----
C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-05897C23.pf
C:\WINDOWS\Prefetch\SVCHOST.EXE-3530F672.pf
C:\WINDOWS\system32\config\software.LOG

-----
Variazioni totali:6
-----
```

- Grazie all' applicativo Regshot ho potuto confrontare due istantanee che ho creato riguardo alle chiavi di registro del pc prima dell' esecuzione del malware e il risultato è stato che variazioni, come è corretto che sia, non ce ne sono state. A volte capita che ci siano normali variazioni poiché ogni pc esegue sempre azioni predefinite
- Quello che per noi è importante è la verifica dopo aver eseguito il malware, e come mostrato in slide si evincono alcune modifiche delle chiavi di registro, e questa è un informazione importantissima in quanto ci dice qual'è il suo comportamento e cosa va a modificare