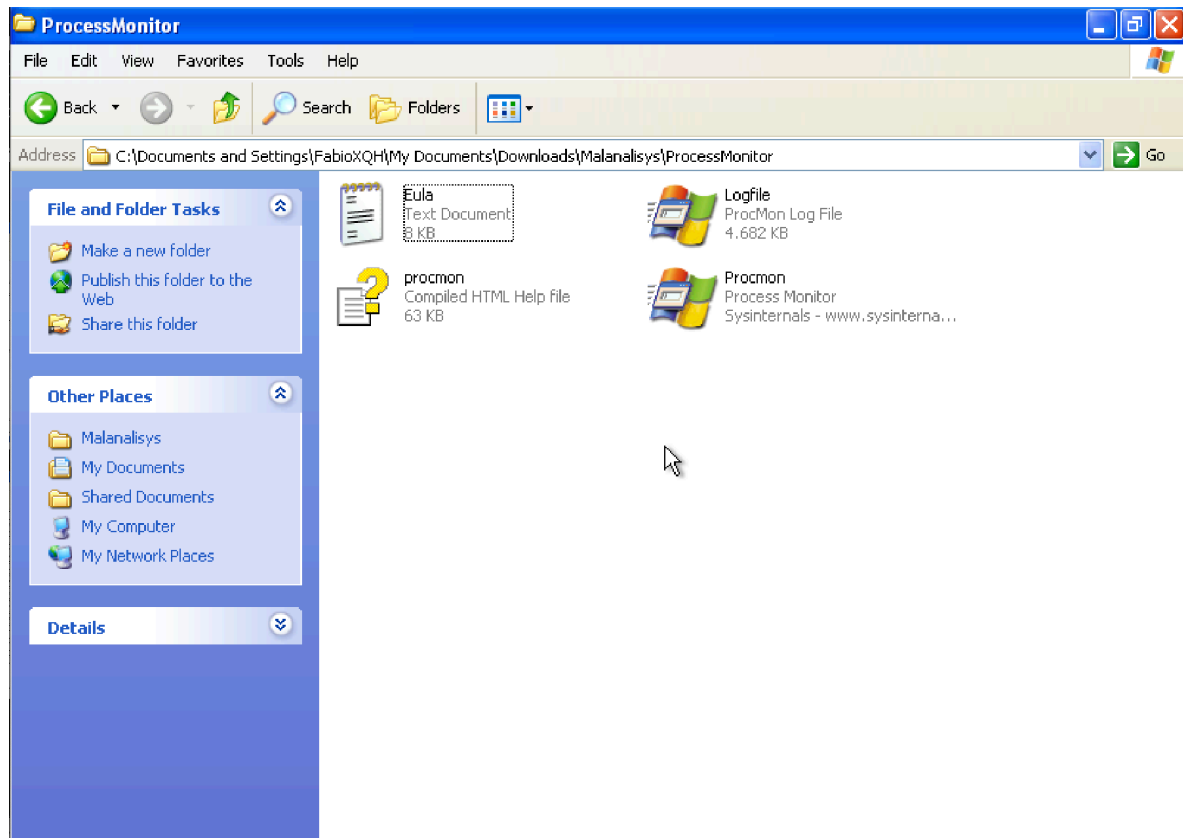


ANALISI DINAMICA BASICA

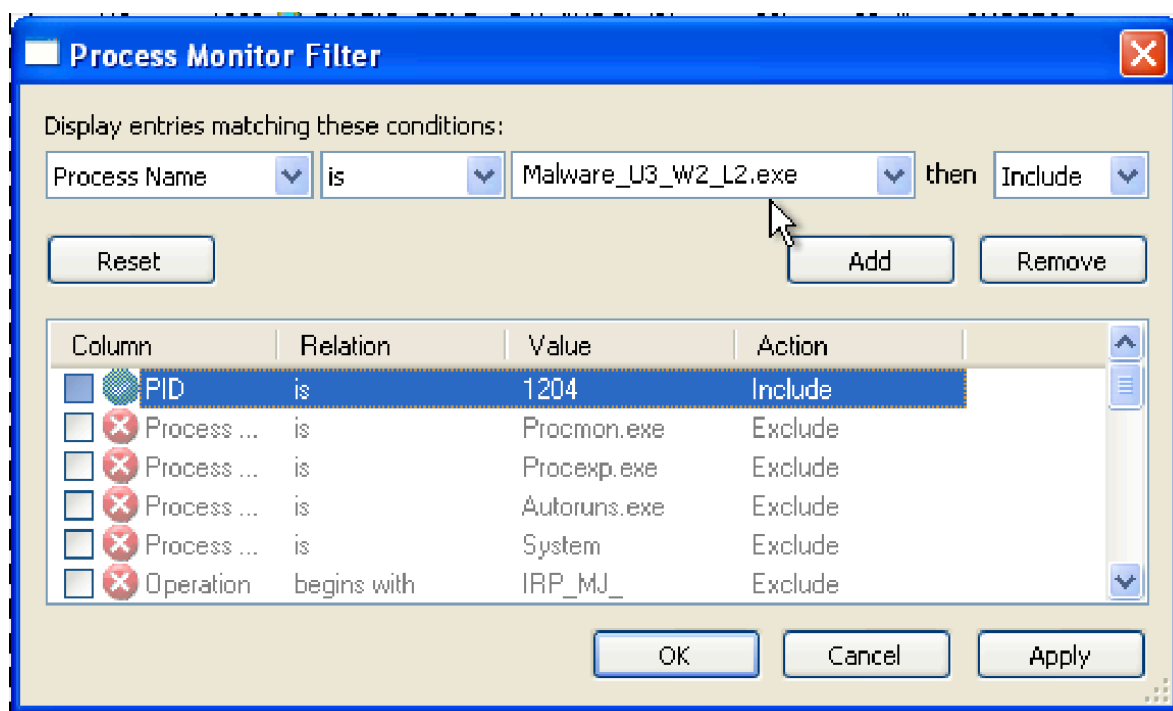
Traccia:

L'esercizio di oggi prevede di effettuare tramite macchina virtuale Windows XP, l'analisi di un malware e identificare la sua identità e processi effettuati tramite programma Process Monitor.

Per Prima cosa andiamo ad aprire il nostro programma "Process Monitor" su macchina virtuale

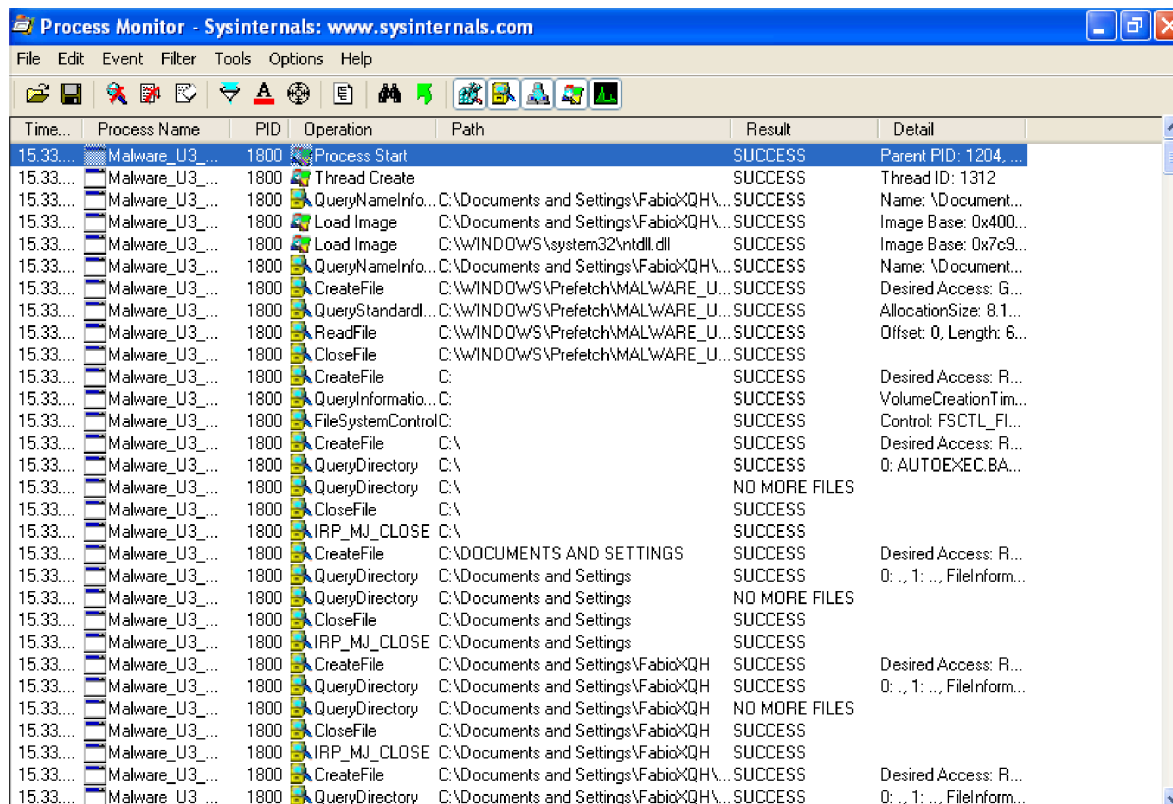


Una volta all'interno del programma andiamo sui filtri e andiamo ad inserire il nome del malware da analizzare (Malware_U3_W2_L2) per poi andarlo ad avviare così da ottenere una scansione completa di tutti effettuati dal software.



Data una accurata ricerca attraverso i risultati ottenuti dalla scansione, possiamo dire che il comportamento del virus inizialmente ha origine dai documenti di sistema.

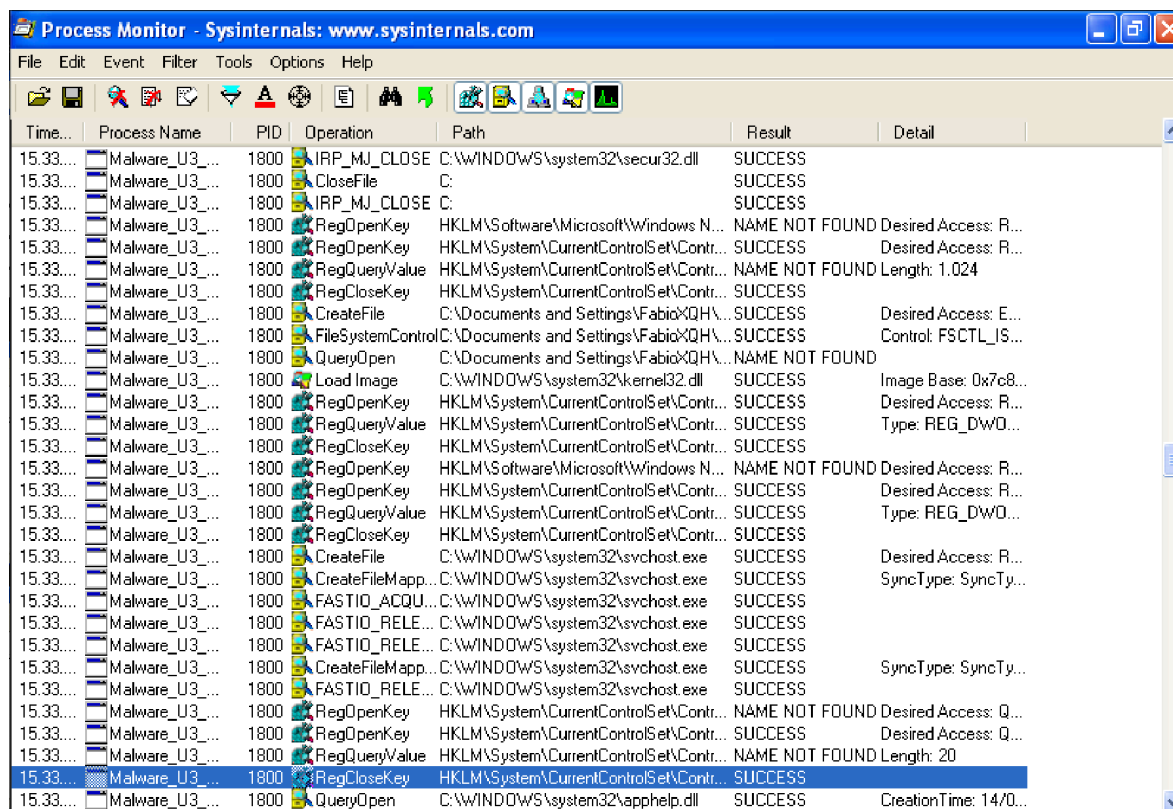
Probabilmente perché ha bisogno di ottenere eventuali informazioni per poi potersi spostare sul sistema operativo.



Una volta all'interno del sistema operativo possiamo vedere come esso cerchi

disperatamente di accedere al sistema per prenderne il controllo e modificare le varie policy.

Detto ciò, e stando a questi dati raccolti presumo che questo sia un tipo di malware di categoria Trojan, il quale si insedia nel sistema operativo in modo innocuo per poi prenderne il controllo ed eliminare file e mettere K.O il sistema informatico.



Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time...	Process Name	PID	Operation	Path	Result	Detail
15.33...	Malware_U3...	1800	IRP_MJ_CLOSE	C:\WINDOWS\system32\secur32.dll	SUCCESS	
15.33...	Malware_U3...	1800	CloseFile	C:	SUCCESS	
15.33...	Malware_U3...	1800	IRP_MJ_CLOSE	C:	SUCCESS	
15.33...	Malware_U3...	1800	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
15.33...	Malware_U3...	1800	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
15.33...	Malware_U3...	1800	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
15.33...	Malware_U3...	1800	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15.33...	Malware_U3...	1800	CreateFile	C:\Documents and Settings\Fabio\QH\...	SUCCESS	Desired Access: E...
15.33...	Malware_U3...	1800	FileSystemControl	C:\Documents and Settings\Fabio\QH\...	SUCCESS	Control: FSCTL_IS...
15.33...	Malware_U3...	1800	QueryOpen	C:\Documents and Settings\Fabio\QH\...	NAME NOT FOUND	
15.33...	Malware_U3...	1800	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
15.33...	Malware_U3...	1800	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
15.33...	Malware_U3...	1800	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWD...
15.33...	Malware_U3...	1800	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15.33...	Malware_U3...	1800	RegOpenKey	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Desired Access: R...
15.33...	Malware_U3...	1800	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
15.33...	Malware_U3...	1800	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWD...
15.33...	Malware_U3...	1800	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15.33...	Malware_U3...	1800	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: R...
15.33...	Malware_U3...	1800	CreateFileMap...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
15.33...	Malware_U3...	1800	FASTIO_ACQU...	C:\WINDOWS\system32\svchost.exe	SUCCESS	
15.33...	Malware_U3...	1800	FASTIO_RELE...	C:\WINDOWS\system32\svchost.exe	SUCCESS	
15.33...	Malware_U3...	1800	FASTIO_RELE...	C:\WINDOWS\system32\svchost.exe	SUCCESS	
15.33...	Malware_U3...	1800	CreateFileMap...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
15.33...	Malware_U3...	1800	FASTIO_RELE...	C:\WINDOWS\system32\svchost.exe	SUCCESS	
15.33...	Malware_U3...	1800	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
15.33...	Malware_U3...	1800	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
15.33...	Malware_U3...	1800	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 20
15.33...	Malware_U3...	1800	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15.33...	Malware_U3...	1800	QueryOpen	C:\WINDOWS\system32\apphelp.dll	SUCCESS	CreationTime: 14/0...

