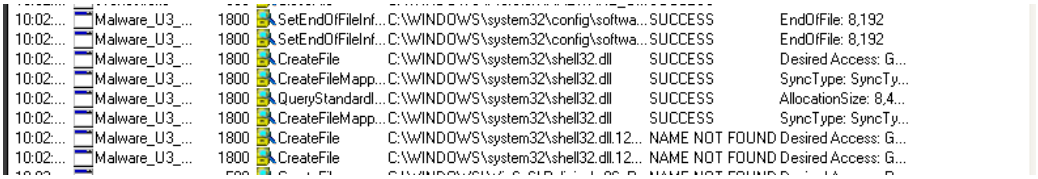
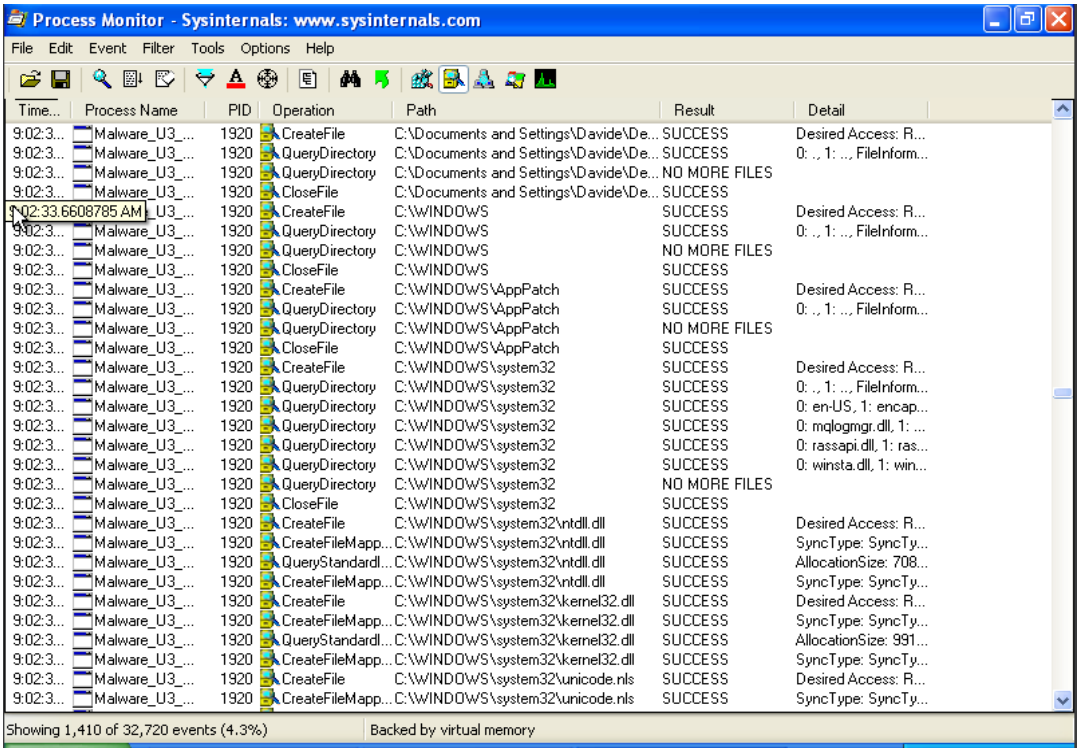
Analizzando le eventuali azioni del malware sul file system possiamo vedere come il malware abbia fatto varie azioni come creare file e fare query directory per leggere gli attributi (come dimensione, data di creazione, data di modifica) di un file o di una cartella ed eseguire operazioni su un gruppo di file, ad esempio copiare, spostare o eliminare file specifici in una directory, per quanto riguarda il “create File” possiamo notare che va a farlo su path che portano alla modifica del sistema di Win come Windows Common Control, shell32 ecc.



10:02:...	Malware_U3_...	1800	SetEndOfFileInf...	C:\WINDOWS\system32\config\softwa...	SUCCESS	EndOfFile: 8,192
10:02:...	Malware_U3_...	1800	SetEndOfFileInf...	C:\WINDOWS\system32\config\softwa...	SUCCESS	EndOfFile: 8,192
10:02:...	Malware_U3_...	1800	CreateFile	C:\WINDOWS\system32\shell32.dll	SUCCESS	Desired Access: G...
10:02:...	Malware_U3_...	1800	CreateFileMapp...	C:\WINDOWS\system32\shell32.dll	SUCCESS	SyncType: SyncTy...
10:02:...	Malware_U3_...	1800	QueryStandardI...	C:\WINDOWS\system32\shell32.dll	SUCCESS	AllocationSize: 8,4...
10:02:...	Malware_U3_...	1800	CreateFileMapp...	C:\WINDOWS\system32\shell32.dll	SUCCESS	SyncType: SyncTy...
10:02:...	Malware_U3_...	1800	CreateFile	C:\WINDOWS\system32\shell32.dll.12...	NAME NOT FOUND	Desired Access: G...
10:02:...	Malware_U3_...	1800	CreateFile	C:\WINDOWS\system32\shell32.dll.12...	NAME NOT FOUND	Desired Access: G...



Le azioni del malware su processi e thread che possiamo notare utilizzando il process monitor sono l’ avvio di processi: caricamento di immagini (load image) e la creazione di thread.