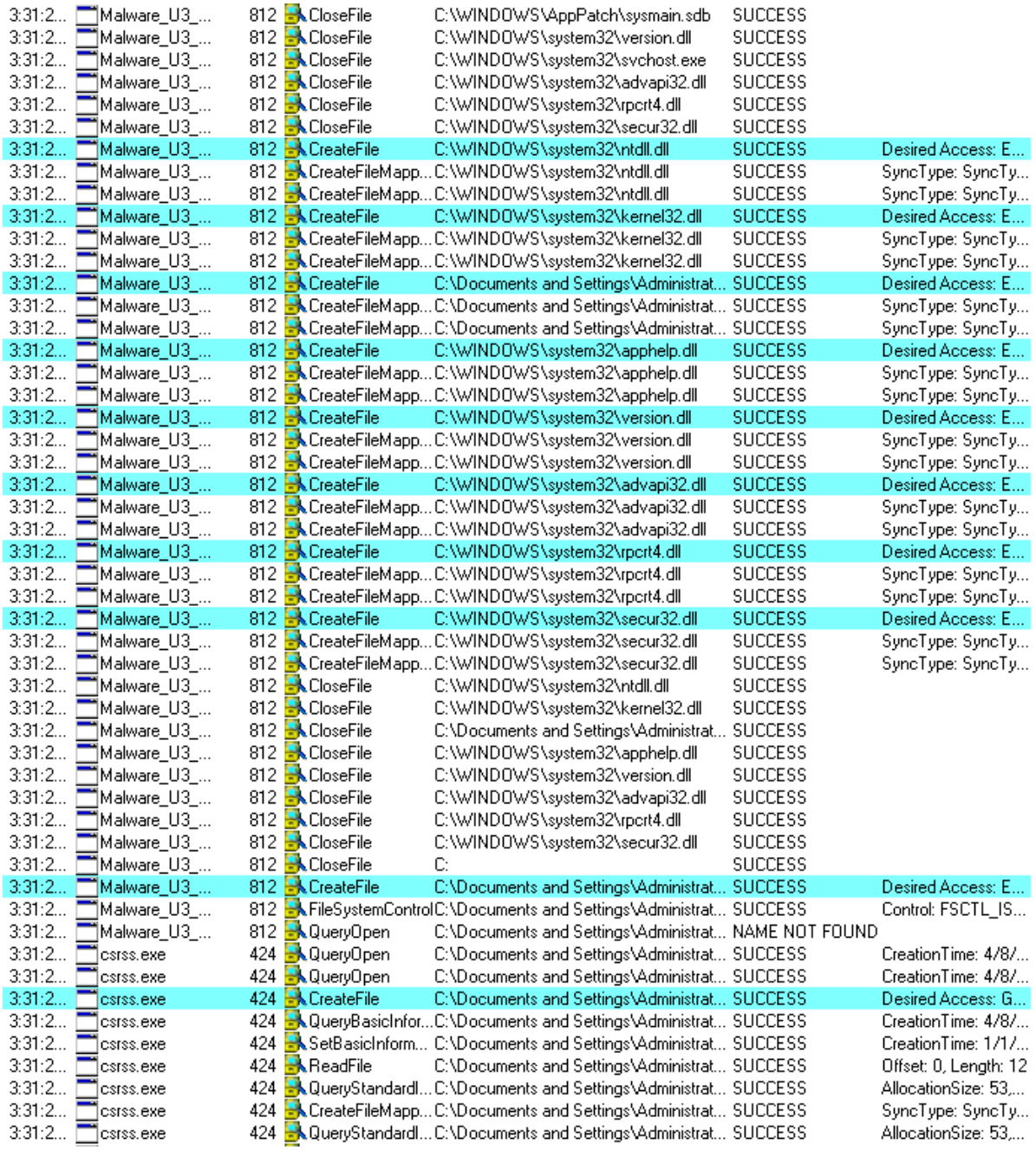
[S10/E2 - Natalino Imbrogno]

Eseguo il malware *Malware_U3_W2_L2* e analizzo il suo comportamento con *procmon*

3:31:2...	Explorer.EXE	1528	SetEndOfFileInf...	C:\Documents and Settings\Administrat...	SUCCESS	EndOfFile: 32,768
3:31:2...	Malware_U3_...	812	QueryNameInfo...	C:\Documents and Settings\Administrat...	SUCCESS	Name: \Document...
3:31:2...	Malware_U3_...	812	QueryNameInfo...	C:\Documents and Settings\Administrat...	SUCCESS	Name: \Document...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\Prefetch\MALWARE_U...	SUCCESS	Desired Access: G...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\Prefetch\MALWARE_U...	SUCCESS	AllocationSize: 8,1...
3:31:2...	Malware_U3_...	812	ReadFile	C:\WINDOWS\Prefetch\MALWARE_U...	SUCCESS	Offset: 0, Length: 5...
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\Prefetch\MALWARE_U...	SUCCESS	
3:31:2...	Malware_U3_...	812	CreateFile	C:	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	QueryInformatio...	C:	SUCCESS	VolumeCreationTim...
3:31:2...	Malware_U3_...	812	FileSystemControl	C:	SUCCESS	Control: FSCTL_FI...
3:31:2...	Malware_U3_...	812	CreateFile	C:\	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\	SUCCESS	0: AUTOEXEC.BA...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\	NO MORE FILES	
3:31:2...	Malware_U3_...	812	CloseFile	C:\	SUCCESS	
3:31:2...	Malware_U3_...	812	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\Documents and Settings	SUCCESS	0: ., 1: .., FileInform...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
3:31:2...	Malware_U3_...	812	CloseFile	C:\Documents and Settings	SUCCESS	
3:31:2...	Malware_U3_...	812	CreateFile	C:\Documents and Settings\ADMINIST...	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0: ., 1: .., FileInform...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
3:31:2...	Malware_U3_...	812	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
3:31:2...	Malware_U3_...	812	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\Documents and Settings\Administrat...	SUCCESS	0: ., 1: .., FileInform...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\Documents and Settings\Administrat...	NO MORE FILES	
3:31:2...	Malware_U3_...	812	CloseFile	C:\Documents and Settings\Administrat...	SUCCESS	
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1: .., FileInform...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\WINDOWS	NO MORE FILES	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS	SUCCESS	
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\WINDOWS\AppPatch	SUCCESS	0: ., 1: .., FileInform...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\WINDOWS\AppPatch	NO MORE FILES	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\AppPatch	SUCCESS	
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: ., 1: .., FileInform...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: emptyregdb.dat, ...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: mqise.dll, 1: mql...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: rasmontr.dll, 1: r...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: winmm.dll, 1: win...
3:31:2...	Malware_U3_...	812	QueryDirectory	C:\WINDOWS\system32	NO MORE FILES	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32	SUCCESS	
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	AllocationSize: 708...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	AllocationSize: 991...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\unicode.nls	SUCCESS	Desired Access: R...

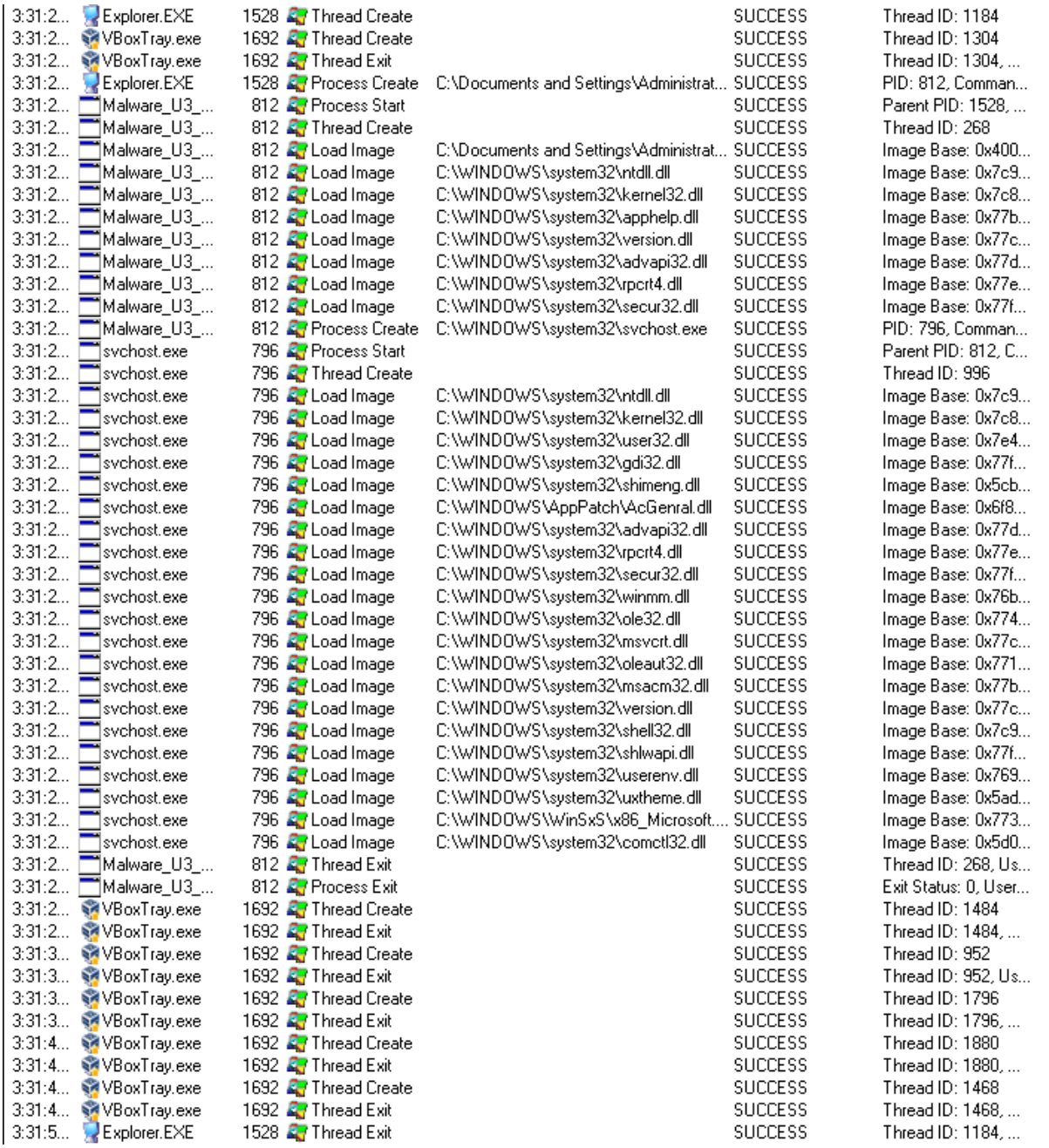
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\unicode.nls	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\unicode.nls	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\unicode.nls	SUCCESS	AllocationSize: 90,...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\unicode.nls	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\locale.nls	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\locale.nls	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\locale.nls	SUCCESS	AllocationSize: 266...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\locale.nls	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	AllocationSize: 24,...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\sorttbls.nls	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 53,...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\ctype.nls	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\ctype.nls	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\ctype.nls	SUCCESS	AllocationSize: 12,...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\ctype.nls	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\sortkey.nls	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\sortkey.nls	SUCCESS	AllocationSize: 266...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\sortkey.nls	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	AllocationSize: 126...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 1,2...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\version.dll	SUCCESS	AllocationSize: 20,...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\svchost.exe	SUCCESS	AllocationSize: 16,...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\svchost.exe	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	AllocationSize: 618...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	AllocationSize: 585...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	Desired Access: R...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	QueryStandardI...	C:\WINDOWS\system32\secur32.dll	SUCCESS	AllocationSize: 57,...



3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\version.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\svchost.exe	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Desired Access: E...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\ntdll.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Desired Access: E...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\kernel32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: E...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Desired Access: E...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\apphelp.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\version.dll	SUCCESS	Desired Access: E...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\version.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Access: E...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Desired Access: E...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	Desired Access: E...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CreateFileMapp...	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: SyncTy...
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\ntdll.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\Documents and Settings\Administrat...	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\apphelp.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\version.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	
3:31:2...	Malware_U3_...	812	CloseFile	C:	SUCCESS	
3:31:2...	Malware_U3_...	812	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: E...
3:31:2...	Malware_U3_...	812	FileSystemControl	C:\Documents and Settings\Administrat...	SUCCESS	Control: FSCTL_IS...
3:31:2...	Malware_U3_...	812	QueryOpen	C:\Documents and Settings\Administrat...	NAME NOT FOUND	
3:31:2...	csrss.exe	424	QueryOpen	C:\Documents and Settings\Administrat...	SUCCESS	CreationTime: 4/8/...
3:31:2...	csrss.exe	424	QueryOpen	C:\Documents and Settings\Administrat...	SUCCESS	CreationTime: 4/8/...
3:31:2...	csrss.exe	424	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: G...
3:31:2...	csrss.exe	424	QueryBasicInfor...	C:\Documents and Settings\Administrat...	SUCCESS	CreationTime: 4/8/...
3:31:2...	csrss.exe	424	SetBasicInform...	C:\Documents and Settings\Administrat...	SUCCESS	CreationTime: 1/1/...
3:31:2...	csrss.exe	424	ReadFile	C:\Documents and Settings\Administrat...	SUCCESS	Offset: 0, Length: 12
3:31:2...	csrss.exe	424	QueryStandardI...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 53,...
3:31:2...	csrss.exe	424	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
3:31:2...	csrss.exe	424	QueryStandardI...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 53,...

Le seguenti azioni effettuate sul file system suggeriscono che si tratta di un malware che sta tentando di accedere a diversi file sul sistema. Probabilmente sta cercando informazioni sensibili, come password o dati finanziari, o forse cerca di installare altre parti di malware sul sistema. In definitiva, probabilmente questo malware sta cercando di ottenere un controllo completo del sistema.

Spostando l’attenzione su processi e thread, invece



3:31:2...	Explorer.EXE	1528	Thread Create		SUCCESS	Thread ID: 1184
3:31:2...	VBoxTray.exe	1692	Thread Create		SUCCESS	Thread ID: 1304
3:31:2...	VBoxTray.exe	1692	Thread Exit		SUCCESS	Thread ID: 1304, ...
3:31:2...	Explorer.EXE	1528	Process Create	C:\Documents and Settings\Administrat...	SUCCESS	PID: 812, Comman...
3:31:2...	Malware_U3_...	812	Process Start		SUCCESS	Parent PID: 1528, ...
3:31:2...	Malware_U3_...	812	Thread Create		SUCCESS	Thread ID: 268
3:31:2...	Malware_U3_...	812	Load Image	C:\Documents and Settings\Administrat...	SUCCESS	Image Base: 0x400...
3:31:2...	Malware_U3_...	812	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
3:31:2...	Malware_U3_...	812	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
3:31:2...	Malware_U3_...	812	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b...
3:31:2...	Malware_U3_...	812	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c...
3:31:2...	Malware_U3_...	812	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
3:31:2...	Malware_U3_...	812	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e...
3:31:2...	Malware_U3_...	812	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
3:31:2...	Malware_U3_...	812	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 796, Comman...
3:31:2...	svchost.exe	796	Process Start		SUCCESS	Parent PID: 812, C...
3:31:2...	svchost.exe	796	Thread Create		SUCCESS	Thread ID: 996
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x7e4...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 0x77f...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\shimeng.dll	SUCCESS	Image Base: 0x5cb...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\AppPatch\AcGenral.dll	SUCCESS	Image Base: 0x6f8...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\winmm.dll	SUCCESS	Image Base: 0x76b...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x774...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Image Base: 0x77c...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	Image Base: 0x771...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\msacm32.dll	SUCCESS	Image Base: 0x77b...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\shell32.dll	SUCCESS	Image Base: 0x7c9...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	Image Base: 0x77f...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\userenv.dll	SUCCESS	Image Base: 0x769...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\uxtheme.dll	SUCCESS	Image Base: 0x5ad...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\WinSxS\x86_Microsoft....	SUCCESS	Image Base: 0x773...
3:31:2...	svchost.exe	796	Load Image	C:\WINDOWS\system32\comctl32.dll	SUCCESS	Image Base: 0x5d0...
3:31:2...	Malware_U3_...	812	Thread Exit		SUCCESS	Thread ID: 268, Us...
3:31:2...	Malware_U3_...	812	Process Exit		SUCCESS	Exit Status: 0, User...
3:31:2...	VBoxTray.exe	1692	Thread Create		SUCCESS	Thread ID: 1484
3:31:2...	VBoxTray.exe	1692	Thread Exit		SUCCESS	Thread ID: 1484, ...
3:31:3...	VBoxTray.exe	1692	Thread Create		SUCCESS	Thread ID: 952
3:31:3...	VBoxTray.exe	1692	Thread Exit		SUCCESS	Thread ID: 952, Us...
3:31:3...	VBoxTray.exe	1692	Thread Create		SUCCESS	Thread ID: 1796
3:31:3...	VBoxTray.exe	1692	Thread Exit		SUCCESS	Thread ID: 1796, ...
3:31:4...	VBoxTray.exe	1692	Thread Create		SUCCESS	Thread ID: 1880
3:31:4...	VBoxTray.exe	1692	Thread Exit		SUCCESS	Thread ID: 1880, ...
3:31:4...	VBoxTray.exe	1692	Thread Create		SUCCESS	Thread ID: 1468
3:31:4...	VBoxTray.exe	1692	Thread Exit		SUCCESS	Thread ID: 1468, ...
3:31:5...	Explorer.EXE	1528	Thread Exit		SUCCESS	Thread ID: 1184, ...

Probabilmente il malware sta cercando di eseguire dei comandi tramite la shell di Windows. Questo può essere un modo per sfruttare le vulnerabilità del sistema, installare altri programmi dannosi o rubare informazioni sensibili.

Dopo il malware, ecco come appare il registro

4:33:2...	Explorer.EXE	1528	QueryOpen	C:\Documents and Settings\Administrat...	SUCCESS	CreationTime: 11/5...
4:33:2...	Explorer.EXE	1528	CreateFile	C:\Documents and Settings\Administrat...	SUCCESS	Desired Access: E...
4:33:2...	Explorer.EXE	1528	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
4:33:2...	Explorer.EXE	1528	QueryStandardI...	C:\Documents and Settings\Administrat...	SUCCESS	AllocationSize: 2,1...
4:33:2...	Explorer.EXE	1528	CreateFileMapp...	C:\Documents and Settings\Administrat...	SUCCESS	SyncType: SyncTy...
4:33:2...	Explorer.EXE	1528	CloseFile	C:\Documents and Settings\Administrat...	SUCCESS	
4:34:1...	Explorer.EXE	1528	CreateFile	C:\	SUCCESS	Desired Access: R...
4:34:1...	Explorer.EXE	1528	QueryFullSizeIn...	C:\	SUCCESS	TotalAllocationUnit...
4:34:1...	Explorer.EXE	1528	CloseFile	C:\	SUCCESS	

4:33:2...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 896
4:33:2...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 896, Us...
4:33:2...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1888
4:33:2...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1888, ...
4:33:3...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1432
4:33:3...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1432, ...
4:33:3...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1232
4:33:3...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1232, ...
4:33:4...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1240
4:33:4...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1240, ...
4:33:4...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1864
4:33:4...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1864, ...
4:33:5...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1048
4:33:5...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1048, ...
4:33:5...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 844
4:33:5...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 844, Us...
4:34:0...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1896
4:34:0...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1896, ...
4:34:0...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1964
4:34:0...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1964, ...
4:34:1...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1112
4:34:1...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1112, ...
4:34:1...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1924
4:34:1...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1924, ...
4:34:2...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1016
4:34:2...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1016, ...
4:34:2...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1656
4:34:2...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1656, ...
4:34:3...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1036
4:34:3...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1036, ...
4:34:3...	svchost.exe	1084	Thread Create	SUCCESS	Thread ID: 1244
4:34:3...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1684
4:34:3...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1684, ...
4:34:4...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 908
4:34:4...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 908, Us...
4:34:4...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1344
4:34:4...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1344, ...
4:34:5...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1948
4:34:5...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1948, ...
4:34:5...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 876
4:34:5...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 876, Us...
4:35:0...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1544
4:35:0...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1544, ...
4:35:0...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 364
4:35:0...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 364, Us...
4:35:1...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1308
4:35:1...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1308, ...
4:35:1...	svchost.exe	1084	Thread Exit	SUCCESS	Thread ID: 1244, ...
4:35:1...	VBoxTray.exe	1692	Thread Create	SUCCESS	Thread ID: 1032
4:35:1...	VBoxTray.exe	1692	Thread Exit	SUCCESS	Thread ID: 1032, ...