

# ANALISI DINAMICA BASICA

## Traccia:

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica.

Con riferimento al file eseguibile contenuto nella cartella «**Esercizio\_Pratico\_U3\_W2\_L2**» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul **file system** utilizzando Process Monitor (procmon) oppure se ci sono problemi multimon
- Identificare eventuali azioni del malware su **processi e thread** utilizzando Process Monitor
- Modifiche del registro dopo il malware (**le differenze**)
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

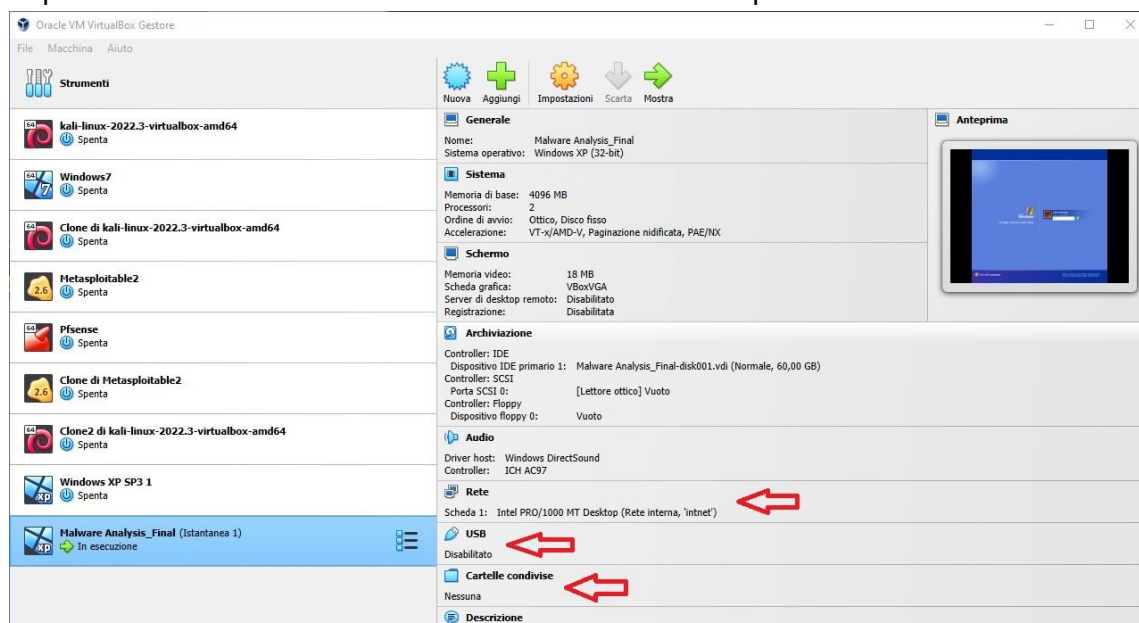
## Suggerimento:

Per quanto riguarda le attività dal malware sul file system, soffermatevi con particolare interesse sulle chiamate alla funzione **Create File** su path noti (ad esempio il path dove è presente l'eseguibile del malware).

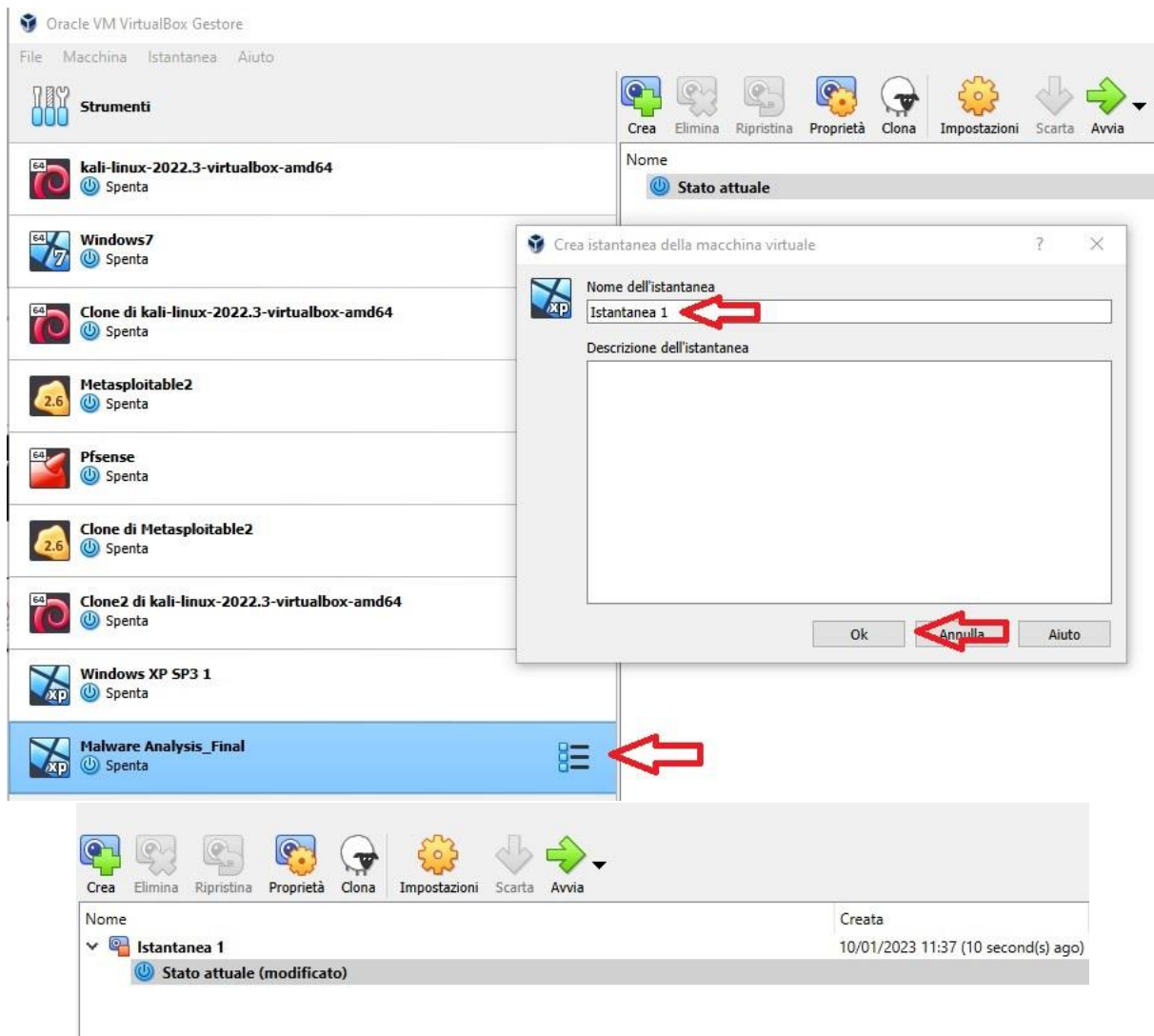
Creare istantanea da Virtualbox della macchina Windows XP prima di iniziare per poter ripristinare in caso di problemi (o al limite fare il clone)

Come da suggerimento della traccia, come prima cosa siamo andati a configurare il nostro ambiente di test in modo appropriato.

Ci siamo assicurati che sulla nostra macchina virtuale fosse attiva un'unica scheda di rete, impostata su "rete interna" e che non fossero abilitati dispositivi USB o cartelle condivise.



Dopodiché siamo andati a creare un'istantanea della macchina virtuale nel suo stato iniziale.

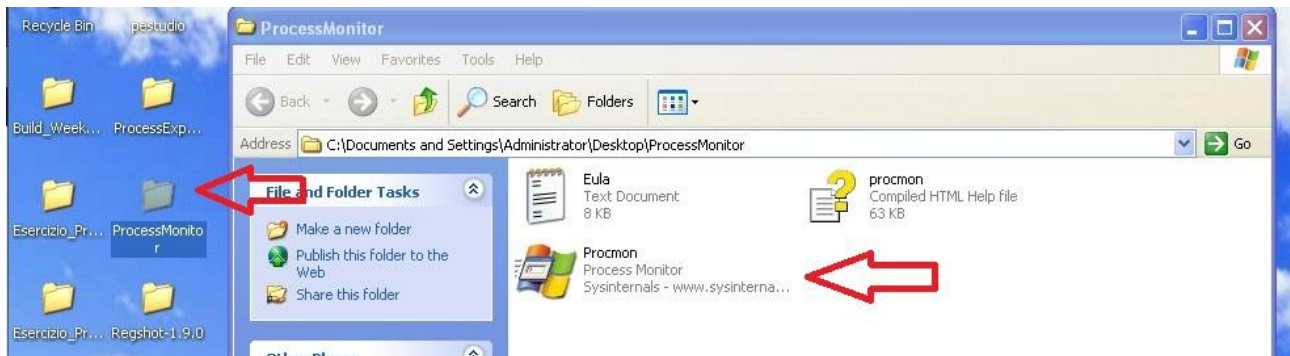


Una volta salvato lo stato della macchina l'abbiamo avviata ed abbiamo seguito la procedura dell'analisi dinamica basica, per recuperare più informazioni possibili sul comportamento del malware in esame utilizzando i tool in nostro possesso.

Il malware in esame sarà presente nella cartella evidenziata sul Desktop della macchina.



Abbiamo quindi avviato **Process Monitor (Procmon)**, un tool avanzato per Windows che permette di monitorare i processi ed i thread attivi, le attività di rete, l'accesso ai file e le chiamate di sistema effettuate su un sistema operativo.



La schermata iniziale di Procmon ci stamperà a schermo tutti i processi in esecuzione sulla nostra macchina.

Il pannello principale mostrerà delle colonne rappresentanti:

- **Time** ovvero il tempo di cattura;
- **Process Name** ovvero il nome del processo;
- **PID** (Process ID) ovvero l'identificativo univoco del processo;
- **Path** ovvero il percorso dove si sta concretizzando l'azione;
- **Result** ovvero il risultato dell'azione dell'operazione;
- **Detail** ovvero il dettaglio della richiesta dell'operazione.

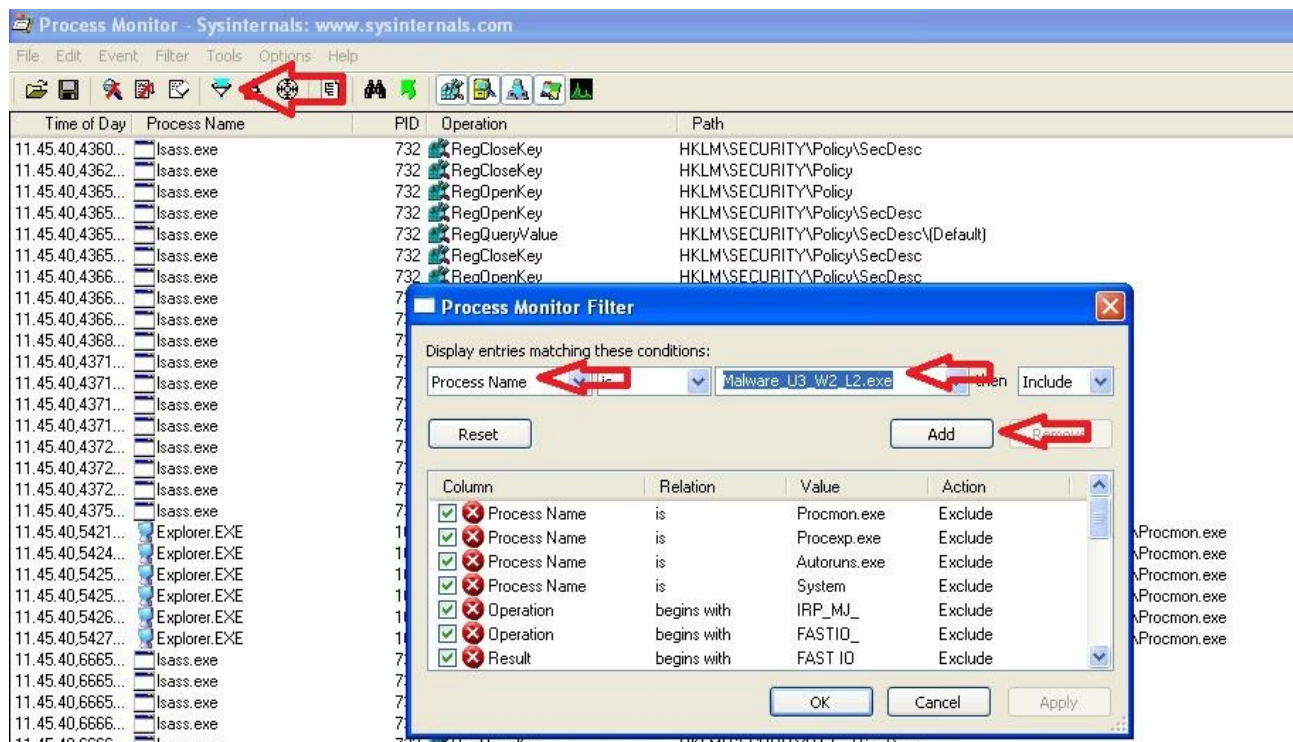
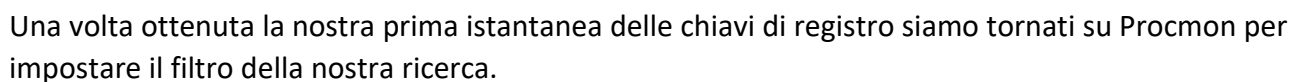
Time of Day	Process Name	PID	Operation	Path	Result	Detail
10.41.31.4134...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: Read/Write
10.41.31.4134...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
10.41.31.4135...	lsass.exe	512	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\Default	BUFFER OVERFLOW	Length: 12
10.41.31.4135...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
10.41.31.4135...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
10.41.31.4136...	lsass.exe	512	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\Default	SUCCESS	Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 00 00 00 A8 00 00 00 00 00 00
10.41.31.4136...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
10.41.31.4139...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: Read/Write
10.41.31.4144...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
10.41.31.4148...	lsass.exe	512	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\Default	BUFFER OVERFLOW	Length: 12
10.41.31.4148...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
10.41.31.4148...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
10.41.31.4148...	lsass.exe	512	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\Default	SUCCESS	Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 00 00 00 A8 00 00 00 00 00 00
10.41.31.4149...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
10.41.31.4156...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy	SUCCESS	
10.41.31.4157...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: Read/Write
10.41.31.4158...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
10.41.31.4158...	lsass.exe	512	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\Default	BUFFER OVERFLOW	Length: 12
10.41.31.4158...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
10.41.31.4158...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
10.41.31.4159...	lsass.exe	512	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\Default	SUCCESS	Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 00 00 00 A8 00 00 00 00 00 00
10.41.31.4159...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
10.41.31.4163...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy	SUCCESS	
10.41.31.4281...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: Read/Write
10.41.31.4281...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
10.41.31.4281...	lsass.exe	512	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\Default	BUFFER OVERFLOW	Length: 12
10.41.31.4283...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
10.41.31.4283...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read
10.41.31.4284...	lsass.exe	512	RegQueryValue	HKLM\SECURITY\Policy\SecDesc\Default	SUCCESS	Type: REG_NONE, Length: 180, Data: 01 00 04 80 98 00 00 00 A8 00 00 00 00 00 00
10.41.31.4284...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	
10.41.31.4288...	lsass.exe	512	RegCloseKey	HKLM\SECURITY\Policy	SUCCESS	
10.41.31.4292...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy	SUCCESS	Desired Access: Read/Write
10.41.31.4292...	lsass.exe	512	RegOpenKey	HKLM\SECURITY\Policy\SecDesc	SUCCESS	Desired Access: Read

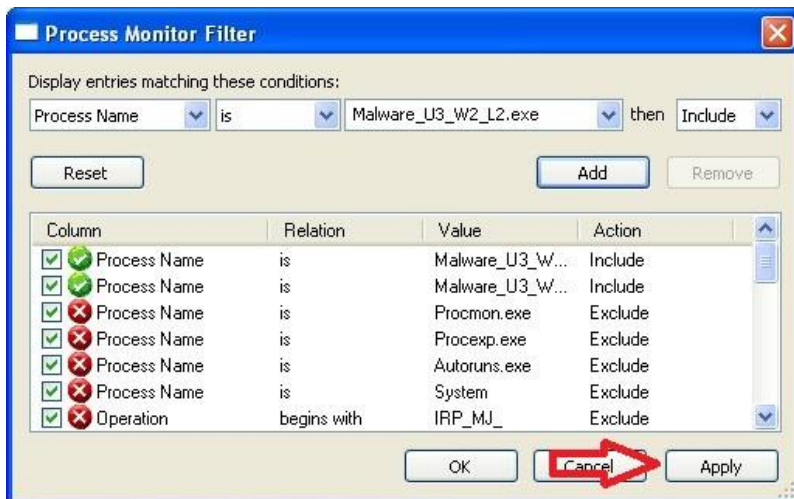
Showing 66,520 of 114,929 events (57%)

Backed by virtual memory



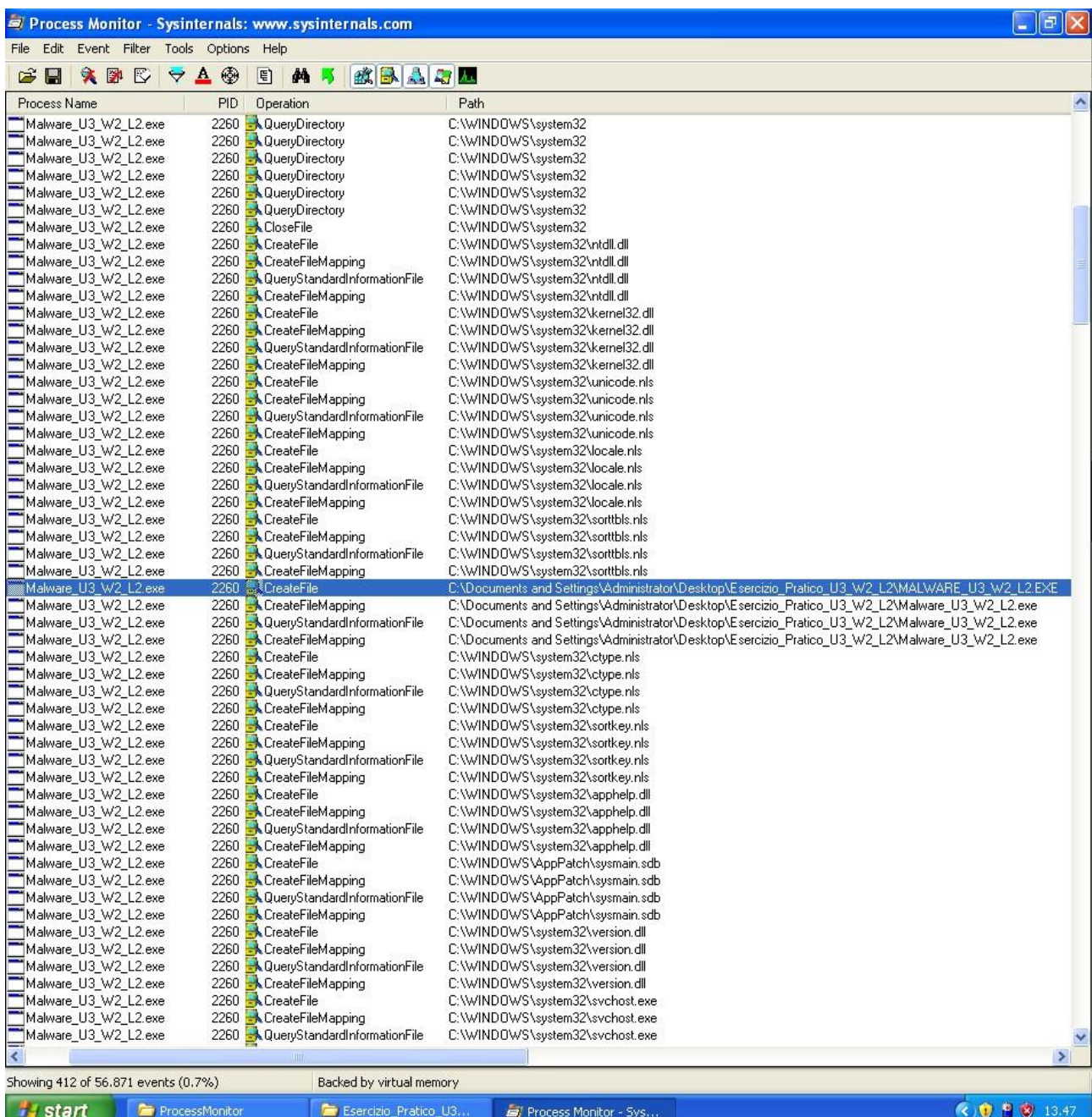
Una volta avviato siamo andati a cliccare su **First Shot** e successivamente su **Shot**.





Avremo così la possibilità di monitorare i comportamenti del malware in esecuzione, come eventuali processi o attività create dal malware in esecuzione sul sistema.

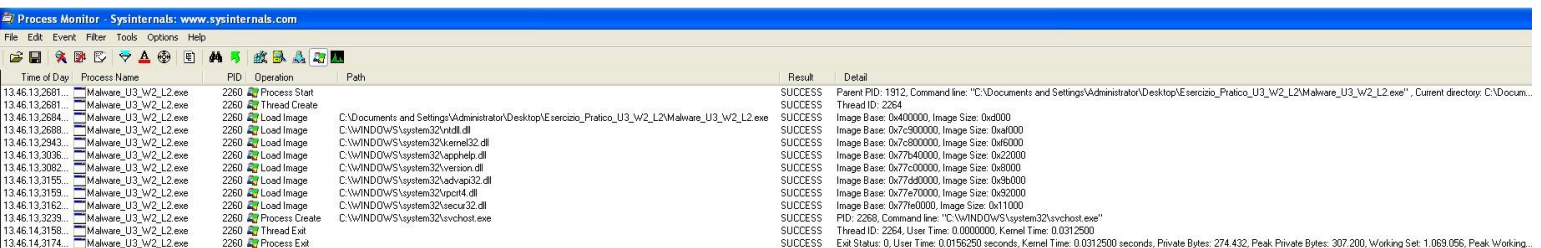
Come suggerito dalla traccia ci siamo soffermati sulle chiamate alla funzione **Create File** su path noti (dove è presente l'eseguibile del malware), per identificare le azioni del malware sul **file system**.



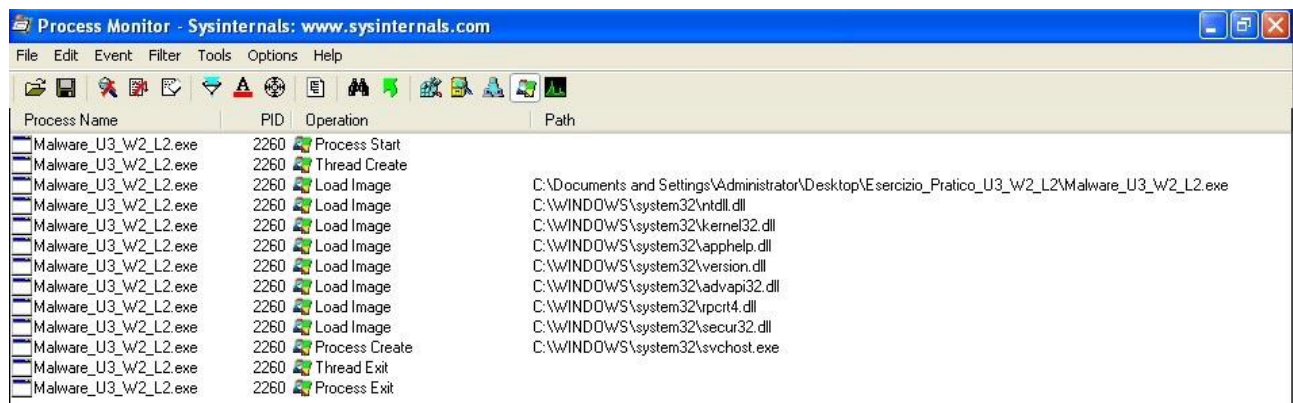


Siamo poi andati a filtrare ulteriormente la ricerca andando a mostrare solo gli eventi relativi ai processi cliccando su **“Show Process and Thread Activity”**.

Gli eventi di questa categoria aiutano ad identificare eventuali processi aggiuntivi creati dal malware per propagarsi sul sistema o per rendere se stesso non identificabile, ad esempio creando nuovi processi con nomi comuni o innocui. Le funzioni sfruttate dai malware più comuni sono **“Load Image”**, come nel nostro caso, per caricare eseguibili e librerie per esecuzione in memoria e attività sui processi e thread.



Time of Day	Process Name	PID	Operation	Path	Result	Detail
13.46.13.2681	Malware_U3_W2_L2.exe	2260	Process Start		SUCCESS	Parent PID: 1912, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe", Current directory: C:\Docum...
13.46.13.2681	Malware_U3_W2_L2.exe	2260	Thread Create		SUCCESS	Thread ID: 2264
13.46.13.2684	Malware_U3_W2_L2.exe	2260	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
13.46.13.2688	Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xa000
13.46.13.2943	Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
13.46.13.3036	Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
13.46.13.3082	Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
13.46.13.3155	Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d90000, Image Size: 0x8b000
13.46.13.3159	Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\iprt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x52000
13.46.13.3162	Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77fd0000, Image Size: 0x11000
13.46.13.3239	Malware_U3_W2_L2.exe	2260	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2268, Command line: "C:\WINDOWS\system32\svchost.exe"
13.46.14.3158	Malware_U3_W2_L2.exe	2260	Thread Exit		SUCCESS	Thread ID: 2264, User Time: 0.0000000, Kernel Time: 0.0312500
13.46.14.3174	Malware_U3_W2_L2.exe	2260	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0312500 seconds, Private Bytes: 274.432, Peak Private Bytes: 307.200, Working Set: 1.069.056, Peak Working...



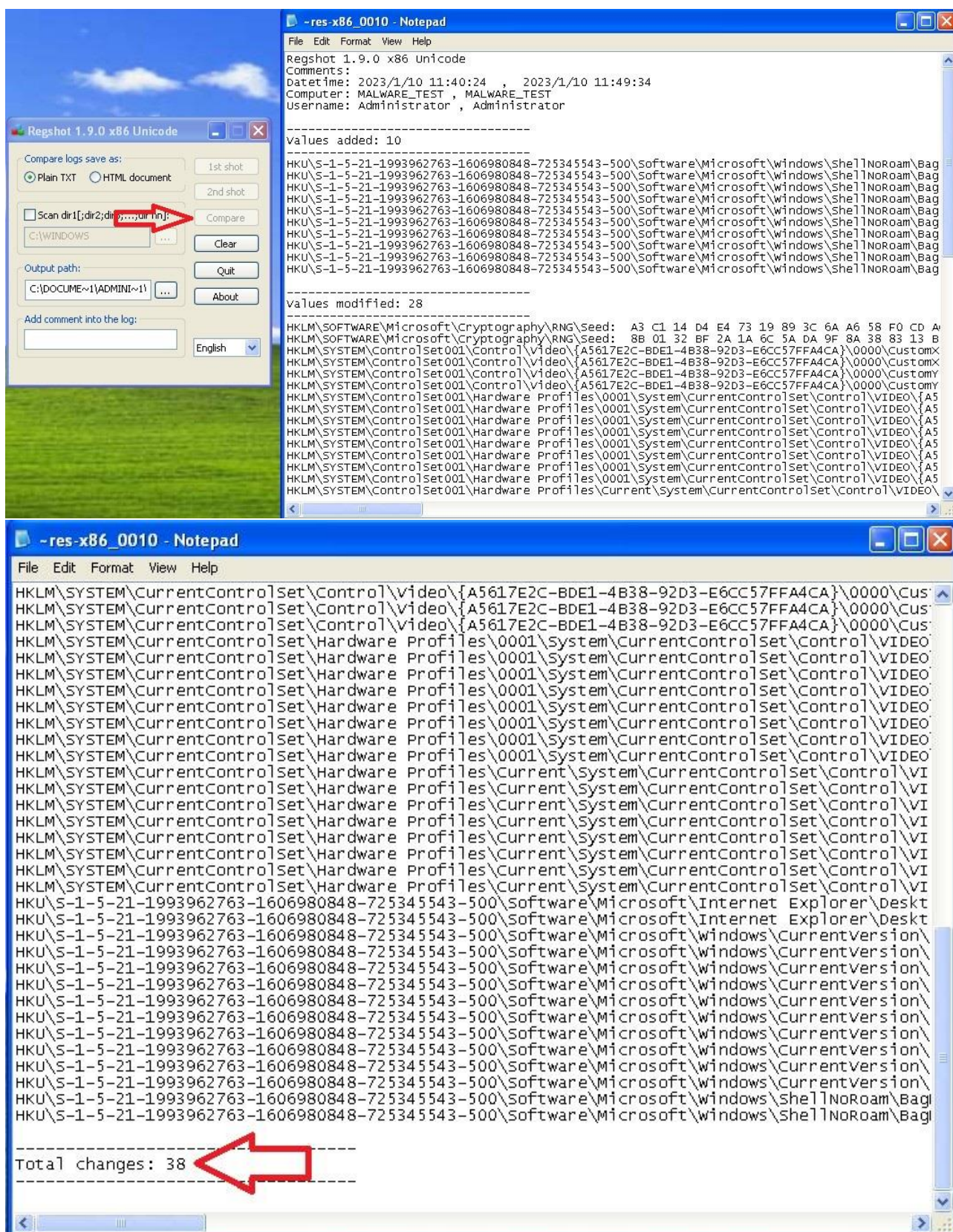
Process Name	PID	Operation	Path
Malware_U3_W2_L2.exe	2260	Process Start	
Malware_U3_W2_L2.exe	2260	Thread Create	
Malware_U3_W2_L2.exe	2260	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\ntdll.dll
Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\kernel32.dll
Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\apphelp.dll
Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\version.dll
Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\advapi32.dll
Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\iprt4.dll
Malware_U3_W2_L2.exe	2260	Load Image	C:\WINDOWS\system32\secur32.dll
Malware_U3_W2_L2.exe	2260	Process Create	C:\WINDOWS\system32\svchost.exe
Malware_U3_W2_L2.exe	2260	Thread Exit	
Malware_U3_W2_L2.exe	2260	Process Exit	

Come potremo vedere il malware in analisi utilizza delle librerie conosciute come kernel32.dll e advapi32.dll, oltre che creare dei processi come svchost.exe, processo non dannoso di per sé ma sarebbe plausibile sospettare che abbia file malevoli al suo interno.



Per concludere siamo andati a catturare la seconda istantanea con RegShot.

Per poi andare a comparare le due istantanee cliccando su **“compare”**.



Stando alle nostre ricerche tramite i tool sopracitati siamo arrivati alla conclusione che ci sia la possibilità che si tratti di un Trojan, in quanto il malware ha un comportamento sospetto che potrebbe ingannare le difese della macchina rendendosi non identificabile come minaccia.