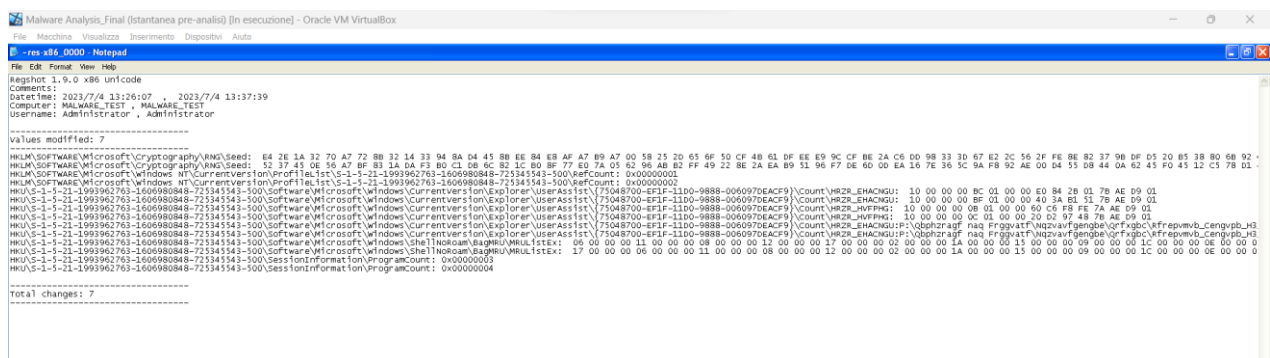


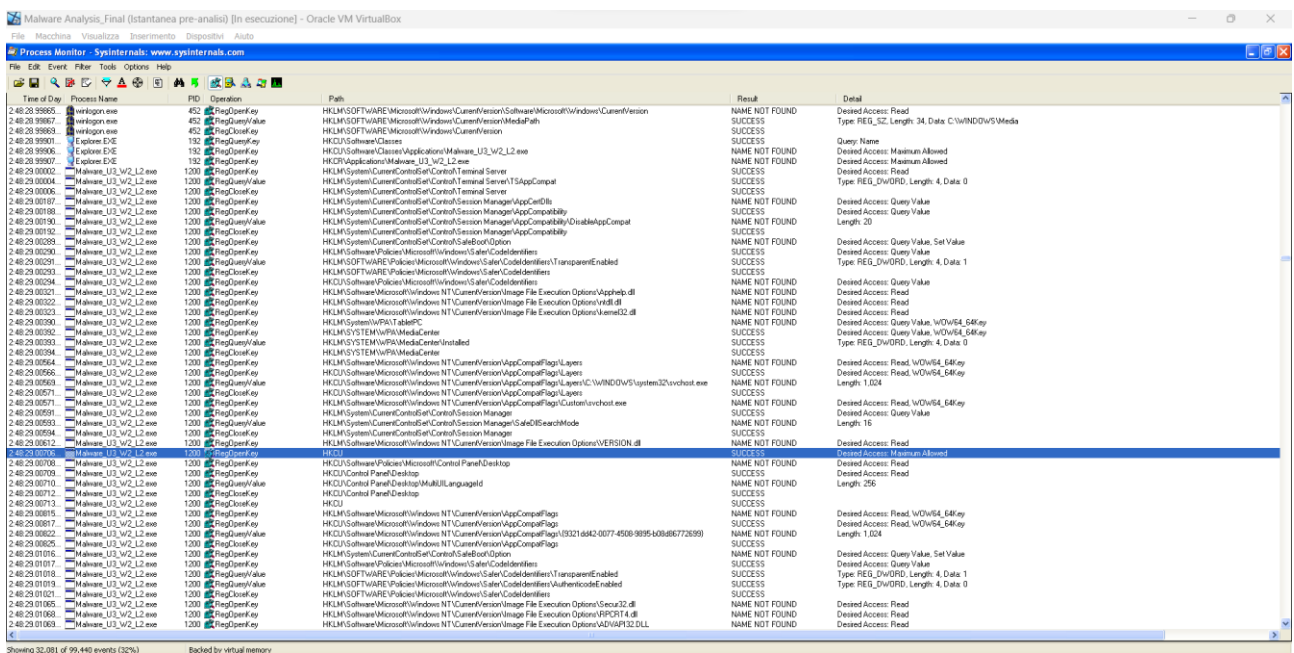
Dynamic Basic Analysis

Nell'esercitazione odierna è richiesto allo studente di analizzare il comportamento di un Malware durante la sua esecuzione.

Si procede dunque con l'avvio di Procmon per effettuare tale analisi, iniziando con lo studio di eventuali modifiche alle chiavi di registro, anche eseguendo una comparazione con Regshot.



Il tool evidenzia sette differenze tra lo stato della macchina prima e dopo l'avvio dell'eseguibile da studiare. Si procede dunque allo studio di tali modifiche applicando il filtro dei registri al tool Process Monitor.



Si procede dunque con lo studio del File System di Windows per cercare di individuare eventuali comportamenti dell'eseguibile.

[illegible]

Come si può notare ancora prima di analizzare i processi nello specifico, il malware crea numerosi file sia su path “nascosti” o specifici del File System Windows, sia nello stesso path in cui esso stesso si trova, tanto che si può notare che dopo l’avvio dell’eseguibile un documento appare nella stessa cartella (Si può dunque pensare ad un probabile Spyware o Keylogger).

Analizzando più nello specifico i processi, inoltre, possiamo anche individuare ulteriori informazioni circa le azioni e le librerie usate per la creazione dei file, andando via via ricostruendo il comportamento del programma. Si noti in particolare la creazione di `SVChost.exe`, molto spesso utilizzato dai Malware Programmer per celare i processi malevoli dei loro programmi.

The screenshot shows the Windows Event Viewer interface. The main pane displays the properties of a process named 'Malware_U3_W2_12.exe'. The 'Image' tab is selected, showing the process icon and details. The 'Path' is 'C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_12\Malware_U3_W2_12.exe'. The 'Command Line' is 'C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_12\Malware_U3_W2_12.exe*'. The 'PID' is 1200, 'Architecture' is 32-bit, 'Parent PID' is 192, 'Virtualized' is n/a, 'Session ID' is 0, 'Integrity' is n/a, 'User' is 'MALWARE_TEST\Administrator', 'Auth ID' is '00000000:0001481f', 'Started' is '7/4/2023 2:48:28 PM', and 'Ended' is '7/4/2023 2:48:30 PM'. Below this, a table lists the loaded modules.

The 'Module Properties' dialog box is open, showing details for 'kernel32.dll'. The 'Module' is 'kernel32.dll', 'Path' is 'C:\WINDOWS\system32\kernel32.dll', 'Description' is 'Windows NT BASE API Client DLL', 'Version' is '5.1.2600.5512 (xssp.080413-2111)', 'Company' is 'Microsoft Corporation', and 'Timestamp' is '1/1/1970 1:00:00 AM'. A 'Close' button is visible at the bottom right of the dialog.

Module	Address	Size	Path	Company	Version	Timestamp
Malware_U3_W...	0x400000	0x2000	C:\Documents and Settings\Admin...			1/1/1970 1:00:...
apphelp.dll	0x7640000	0x22000	C:\WINDOWS\system32\apphelp.dll	Microsoft Corpo...	5.1.2600.5512 ...	1/1/1970 1:00:...
kernel32.dll	0x7600000	0xF6000	C:\WINDOWS\system32\kernel32.dll	Microsoft Corpo...	5.1.2600.5512 ...	1/1/1970 1:00:...
ntdll.dll	0x7C90000	0x4F600	C:\WINDOWS\system32\ntdll.dll	Microsoft Corpo...	5.1.2600.5512 ...	1/1/1970 1:00:...

In ultima battuta si procede con l'analisi dei Thread. Utilizzando l'apposito filtro di Process Monitor si può giungere al risultato mostrato nello screen successivo.

2.50.02.76144	Malware_U3_W2_L2.exe	1968	Process Start	SUCCESS	Parent PID: 1576; Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Phatico_U3_W2_L2\Malware_U3_W2_L2.exe"
2.50.02.76116	Malware_U3_W2_L2.exe	1968	Thread Create	SUCCESS	Thread ID: 1576
2.50.02.76266	Malware_U3_W2_L2.exe	1968	Load Image	SUCCESS	Image Base: 0x400000; Image Size: 0x4000
2.50.02.76291	Malware_U3_W2_L2.exe	1968	Load Image	SUCCESS	Image Base: 0x7c800000; Image Size: 0x40000
2.50.02.77704	Malware_U3_W2_L2.exe	1968	Load Image	SUCCESS	Image Base: 0x7c800000; Image Size: 0x40000
2.50.02.76304	Malware_U3_W2_L2.exe	1968	Load Image	SUCCESS	Image Base: 0x77640000; Image Size: 0x20000
2.50.02.76469	Malware_U3_W2_L2.exe	1968	Load Image	SUCCESS	Image Base: 0x77650000; Image Size: 0x4000
2.50.02.76974	Malware_U3_W2_L2.exe	1968	Load Image	SUCCESS	Image Base: 0x776d0000; Image Size: 0x6000
2.50.02.76983	Malware_U3_W2_L2.exe	1968	Load Image	SUCCESS	Image Base: 0x77670000; Image Size: 0x5000
2.50.02.79182	Malware_U3_W2_L2.exe	1968	Load Image	SUCCESS	Image Base: 0x77640000; Image Size: 0x10000
2.50.02.79675	Malware_U3_W2_L2.exe	1968	Process Create	SUCCESS	PID: 848; Command line: "C:\Windows\system32\cmd.exe"

Come si può notare, in seguito alla creazione del processo ed ad una serie di “load image”, il nuovo processo inizializzato dal malware viene lanciato (“process Start”).

Conclusioni:

Alla luce di quanto analizzato, in particolare le modifiche delle chiavi di registro, la creazione del file nel path del malware, il costante aumento dei processi come segnalato da Procmon, potremmo ipotizzare che l'eseguibile in questione sia un worm in continua replicazione. Quello che è sicuro, alla luce del file creato e costantemente aggiornato nel path del malware, è che tale programma funzioni anche come keylogger.

```
[window: Errore caricamento pagina - Mozilla Firefox]
edoardo0[ENTER]
```