

ANALISI DINAMICA BASICA

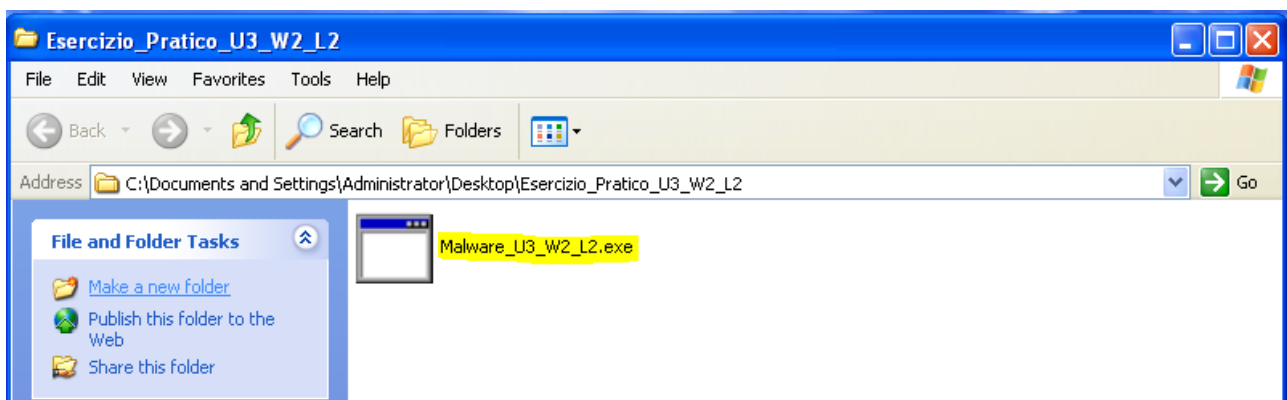
Analisi del malware *Malware_U3_W2_L2.exe*

Tasks:

1. Identificazione di eventuali azioni del malware sul **file system** mediante l'utilizzo del tool "Process Monitor"
2. Identificazione di eventuali azioni del malware su **processi e thread** mediante l'utilizzo del tool "Process Monitor"
3. Identificazione di eventuali modifiche alle **chiavi di registro** da parte del malware (differenze tra prima e dopo l'esecuzione)
4. **Profilazione** del malware in base alla correlazione tra "operation" e "path"

Le attività odierne sono incentrate sull'analisi dinamica basica del file eseguibile di test **Malware_U3_W2_L2.exe**.

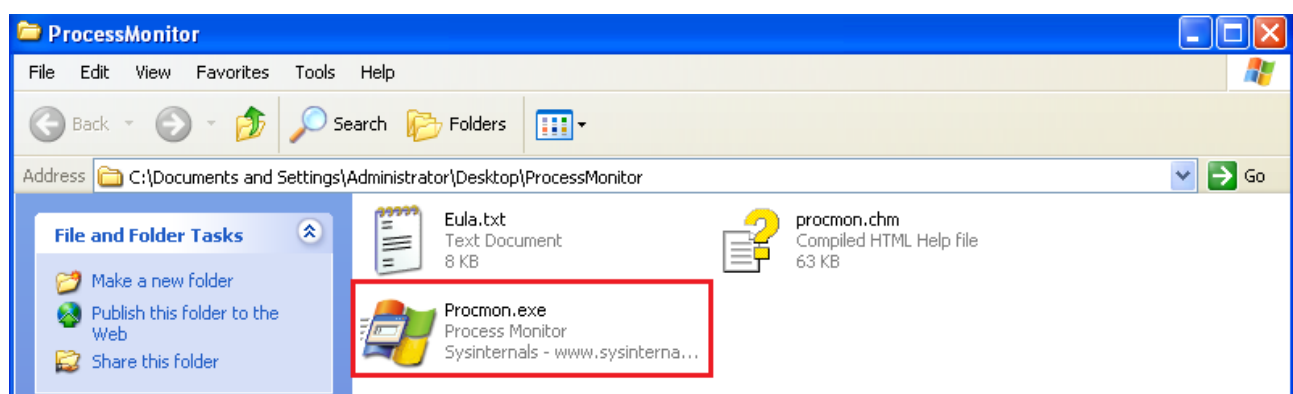
L'**analisi dinamica basica** comprende tutte quelle attività di analisi che presuppongono l'esecuzione del malware in un ambiente dedicato e protetto. È generalmente effettuata DOPO l'analisi statica basica, per sopperire ai limiti di quest'ultima (infatti, al contrario dell'analisi statica, l'analisi dinamica permette di osservare e studiare le vere funzionalità di un malware in esecuzione su un sistema) ed avere una maggiore visibilità sulle attività ed il comportamento del malware in esame.



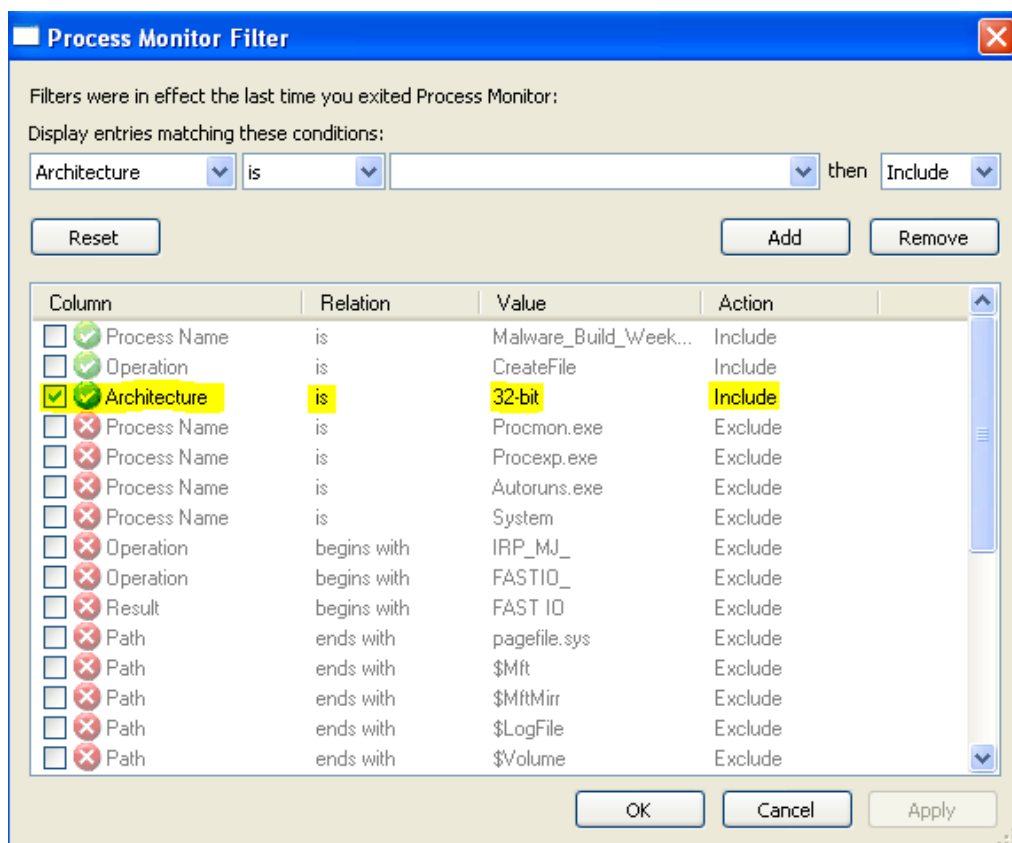
Operazioni preliminari

Process Monitor

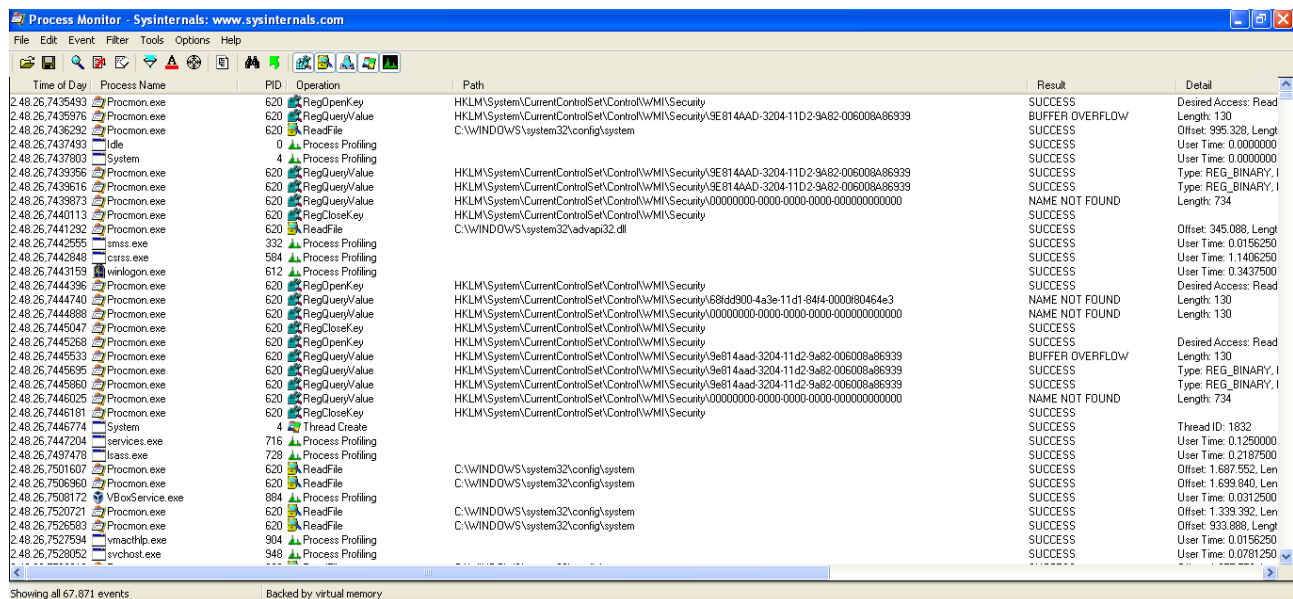
Per l'analisi odierna, ci serviremo di diversi tool per operare un **confronto tra il funzionamento del sistema operativo pre e post-esecuzione del malware oggetto di test**. Uno degli strumenti di cui ci serviremo è **Process Monitor (procmon)**: si tratta di uno strumento avanzato per sistemi operativi Windows che permette di **monitorare i processi** ed i **thread** attivi, l'attività di rete, l'accesso ai file e le chiamate di sistema e il tempo di utilizzo del processore da parte di un determinato processo un sistema operativo.



Avviamo il tool impostando come unico filtro, in una prima fase, **“Architecture is 32-bit”** per avere una panoramica completa della situazione iniziale:



Il filtro produce una lista di eventi relativi all'attività di rete, file system, processi e thread, chiavi di registro e profiling events.

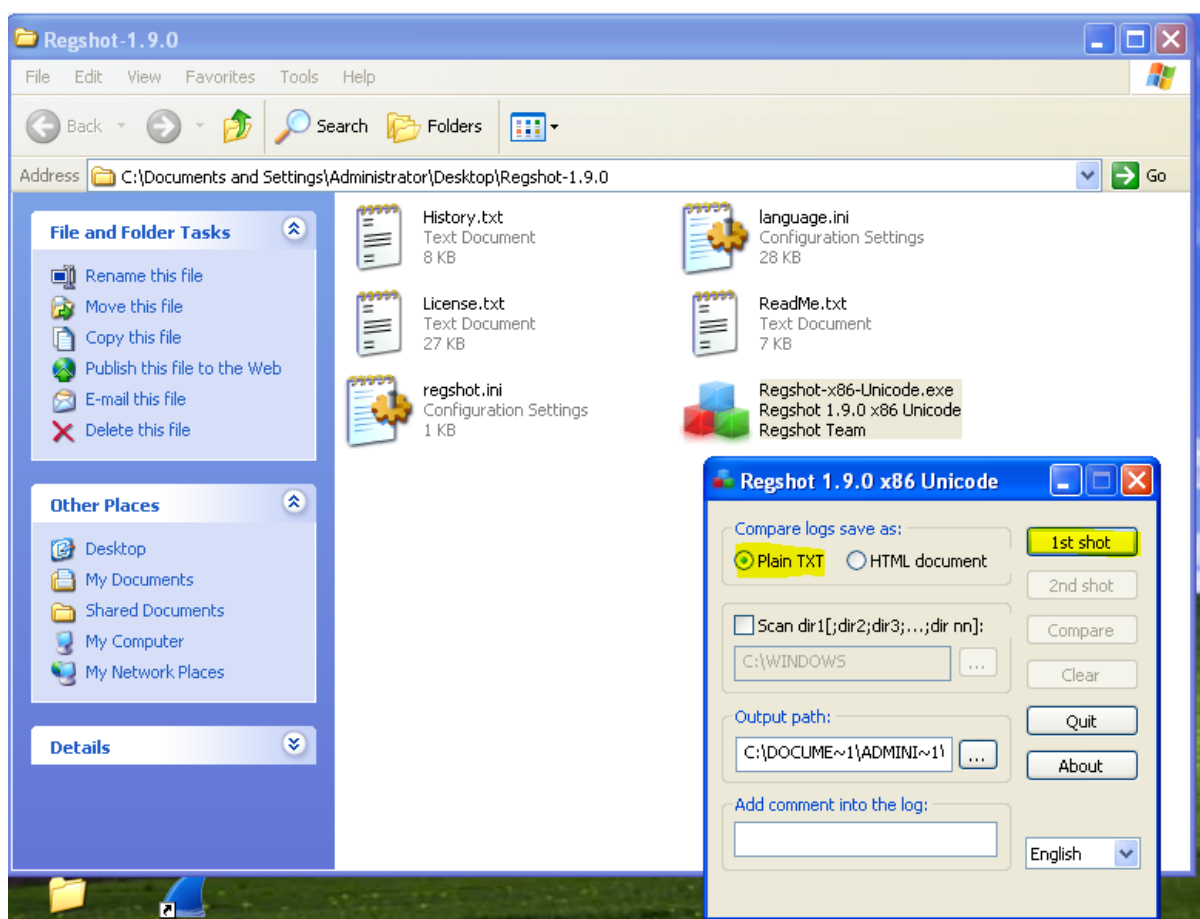


The screenshot shows the Process Monitor application window with a list of events. The columns are Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The events include various system operations like RegOpenKey, RegQueryValue, ReadFile, Process Profiling, and Thread Create, performed by processes like Procton.exe, System, csrss.exe, winlogon.exe, services.exe, iass.exe, vmacthlp.exe, and svchost.exe. The results are mostly SUCCESS, with some BUFFER OVERFLOW and NAME NOT FOUND errors.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
2.48.26.7435493	Procton.exe	620	RegOpenKey	HKLM\System\CurrentControlSet\Control\WMI\Security	SUCCESS	Desired Access: Read Length: 130
2.48.26.7435976	Procton.exe	620	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\9E814AAD-3204-11D2-9A82-006008A86939	SUCCESS	Offset: 995.328, Length: 130
2.48.26.7436292	Procton.exe	620	ReadFile	C:\WINDOWS\system32\config\system	SUCCESS	User Time: 0.0000000
2.48.26.7437493	Idle	0	Process Profiling		SUCCESS	User Time: 0.0000000
2.48.26.7437803	System	4	Process Profiling		SUCCESS	User Time: 0.0000000
2.48.26.7439356	Procton.exe	620	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\9E814AAD-3204-11D2-9A82-006008A86939	SUCCESS	Type: REG_BINARY, Length: 734
2.48.26.7439616	Procton.exe	620	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\9E814AAD-3204-11D2-9A82-006008A86939	SUCCESS	Type: REG_BINARY, Length: 734
2.48.26.7439873	Procton.exe	620	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\00000000-0000-0000-0000-000000000000	NAME NOT FOUND	
2.48.26.7440113	Procton.exe	620	RegCloseKey	HKLM\System\CurrentControlSet\Control\WMI\Security	SUCCESS	
2.48.26.7441292	Procton.exe	620	ReadFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Offset: 345.088, Length: 130
2.48.26.7442555	msiexec.exe	332	Process Profiling		SUCCESS	User Time: 0.0156250
2.48.26.7442848	csrss.exe	584	Process Profiling		SUCCESS	User Time: 1.1406250
2.48.26.7443159	winlogon.exe	612	Process Profiling		SUCCESS	User Time: 0.3437500
2.48.26.7444396	Procton.exe	620	RegOpenKey	HKLM\System\CurrentControlSet\Control\WMI\Security	SUCCESS	Desired Access: Read Length: 130
2.48.26.7444740	Procton.exe	620	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\681dd900-4a3e-11d1-8414-0000080464e3	NAME NOT FOUND	
2.48.26.7444888	Procton.exe	620	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\00000000-0000-0000-0000-000000000000	NAME NOT FOUND	
2.48.26.7445047	Procton.exe	620	RegCloseKey	HKLM\System\CurrentControlSet\Control\WMI\Security	SUCCESS	
2.48.26.7445266	Procton.exe	620	RegOpenKey	HKLM\System\CurrentControlSet\Control\WMI\Security	SUCCESS	Desired Access: Read Length: 130
2.48.26.7445533	Procton.exe	620	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\9e814aad-3204-11d2-9a82-006008a86939	BUFFER OVERFLOW	
2.48.26.7445695	Procton.exe	620	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\9e814aad-3204-11d2-9a82-006008a86939	SUCCESS	Type: REG_BINARY, Length: 734
2.48.26.7445880	Procton.exe	620	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\9e814aad-3204-11d2-9a82-006008a86939	SUCCESS	Offset: 1.887.552, Length: 130
2.48.26.7446025	Procton.exe	620	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\00000000-0000-0000-0000-000000000000	NAME NOT FOUND	
2.48.26.7446181	Procton.exe	620	RegCloseKey	HKLM\System\CurrentControlSet\Control\WMI\Security	SUCCESS	
2.48.26.7446774	System	4	Thread Create		SUCCESS	Thread ID: 1832
2.48.26.7447204	services.exe	716	Process Profiling		SUCCESS	User Time: 0.1250000
2.48.26.7497478	iass.exe	728	Process Profiling		SUCCESS	User Time: 0.2167500
2.48.26.7501607	Procton.exe	620	ReadFile	C:\WINDOWS\system32\config\system	SUCCESS	Offset: 1.887.552, Length: 130
2.48.26.7506960	Procton.exe	620	ReadFile	C:\WINDOWS\system32\config\system	SUCCESS	Offset: 1.699.840, Length: 130
2.48.26.7508172	VBOSService.exe	884	Process Profiling		SUCCESS	User Time: 0.0312500
2.48.26.7520721	Procton.exe	620	ReadFile	C:\WINDOWS\system32\config\system	SUCCESS	Offset: 1.339.392, Length: 130
2.48.26.7526583	Procton.exe	620	ReadFile	C:\WINDOWS\system32\config\system	SUCCESS	Offset: 933.888, Length: 130
2.48.26.7527594	vmacthlp.exe	904	Process Profiling		SUCCESS	User Time: 0.0156250
2.48.26.7528052	svchost.exe	948	Process Profiling		SUCCESS	User Time: 0.0781250

RegShot

Questo tool crea un'istantanea dello stato delle chiavi di registro prima e dopo un determinato evento: ci sarà dunque molto utile ai fini dell'analisi delle eventuali modifiche apportate dal malware al sistema operativo. Avviamo il software ed eseguiamo una prima cattura ("1st shot"):

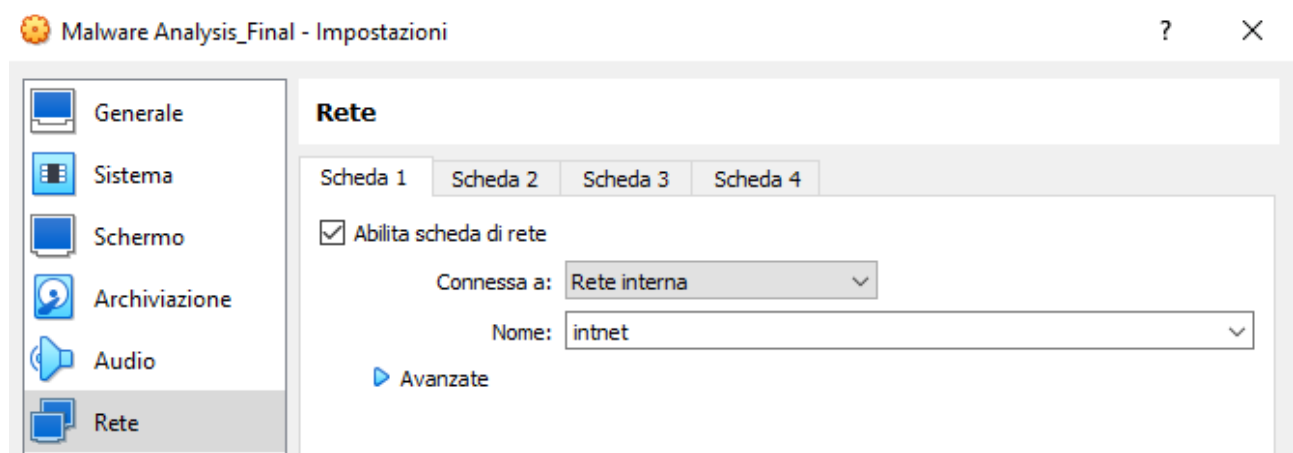


Effettueremo una seconda cattura dopo l'avvio del malware, in modo da procedere con la comparazione.

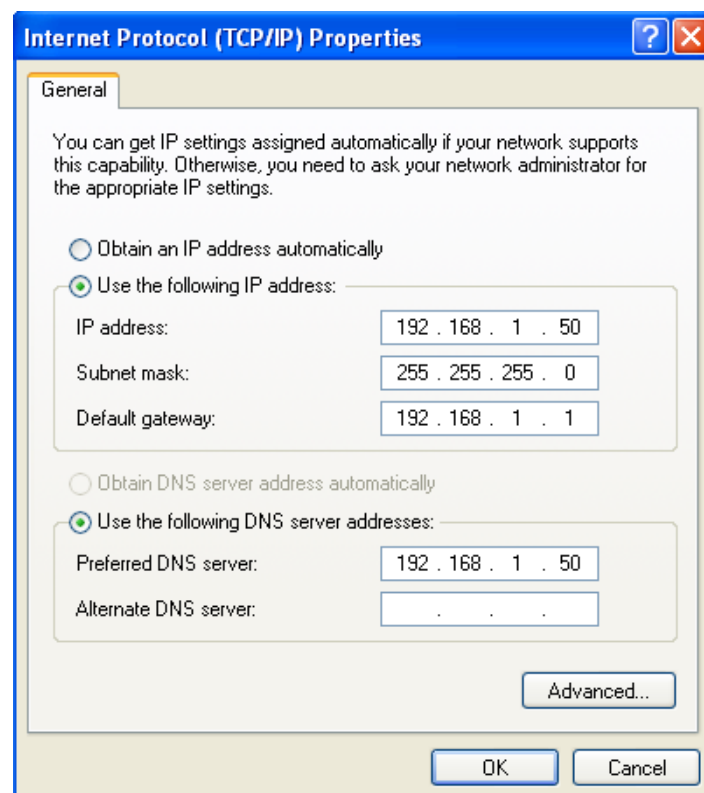
ApateDNS

Con questo tool analizzeremo l'eventuale attività di rete del malware mediante la creazione di un finto server DNS che si occuperà di intercettare le richieste. Ciò risulta particolarmente utile in caso di malware che utilizzano Internet o una rete interna per effettuare il download di file o connettersi a domini infetti.

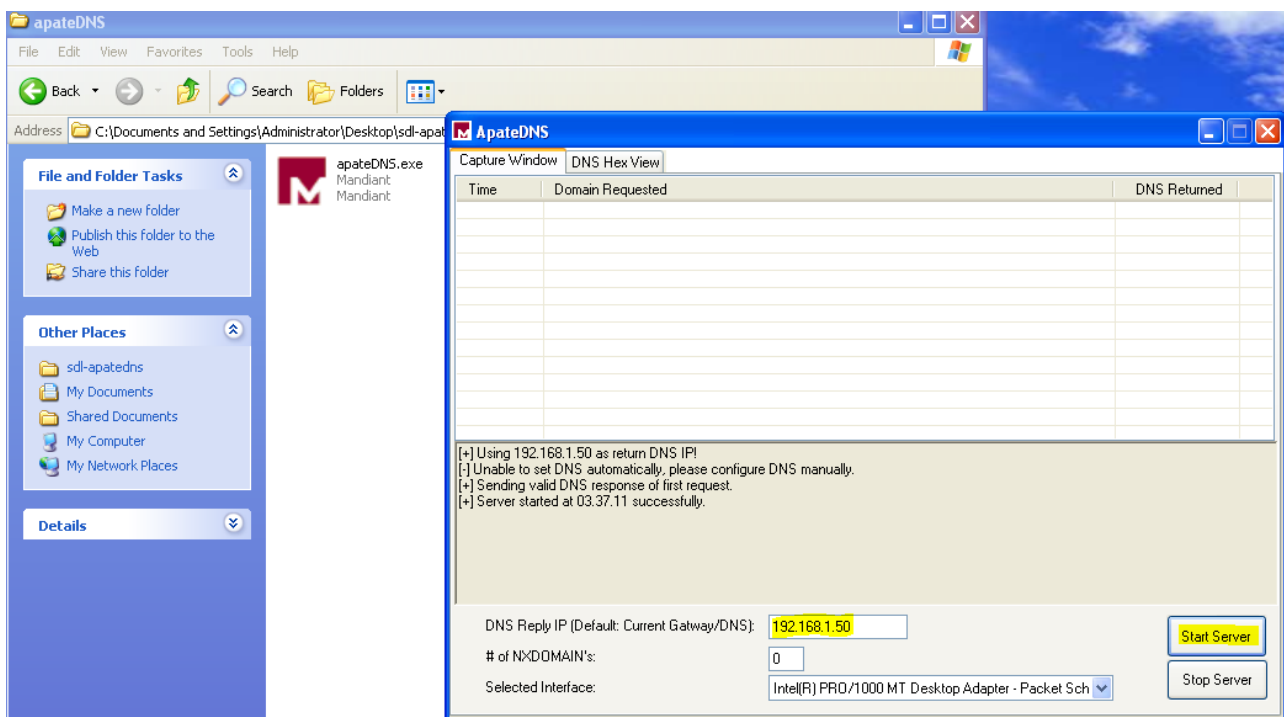
Innanzitutto abilitiamo un'interfaccia di rete, che imposteremo su rete interna:



Adesso ci serviremo dei parametri dell'interfaccia di rete della VM per configurare il finto server DNS.



Assegniamo dunque l'indirizzo IP 192.168.1.50 al nostro server DNS ed avviamolo cliccando su **Start Server**:



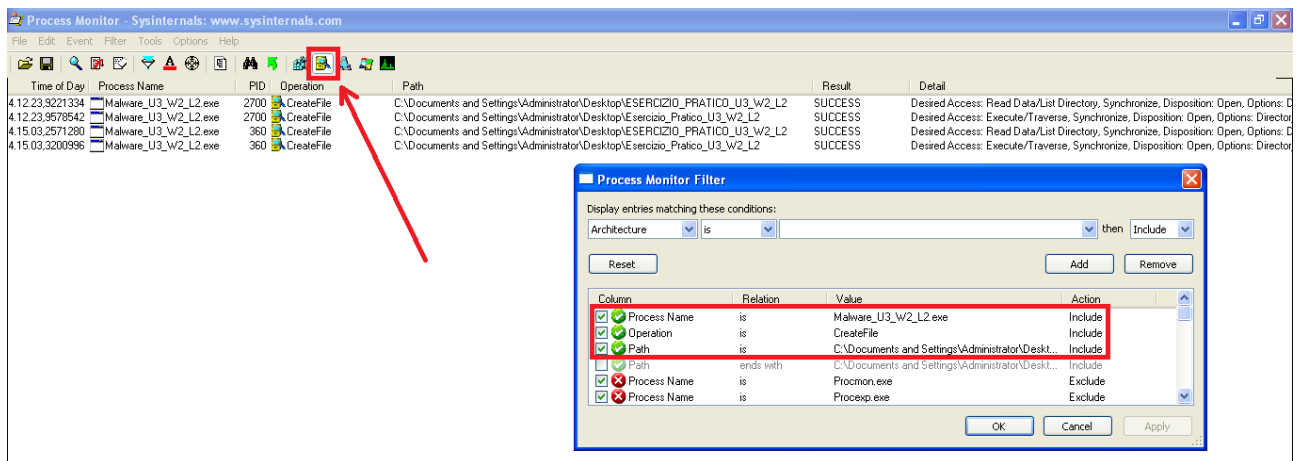
Adesso siamo pronti per avviare il malware e cominciare il test.

1. Identificazione di eventuali azioni del malware sul file system mediante l'utilizzo del tool "Process Monitor"

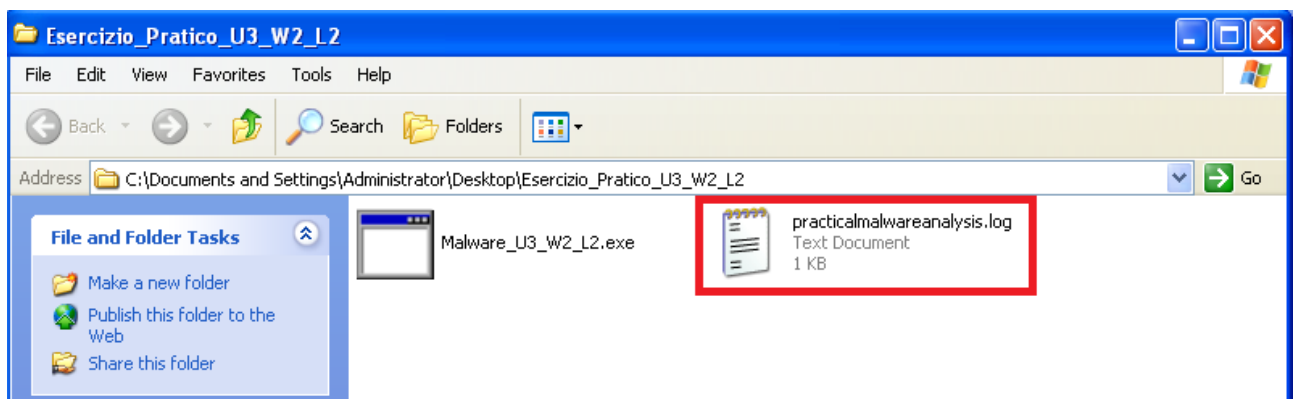
Eseguiamo il malware oggetto di test. Per evidenziare le attività del malware, ci serviremo di alcuni filtri di cattura, da utilizzare individualmente o in combinazione:

- Process Name → **Malware_U3_W2_L2.exe**
- Operation → **CreateFile**
- Path → **C:\Documents and Settings\Administrator\Desktop\Esercizio Pratico U3_W2_L2**

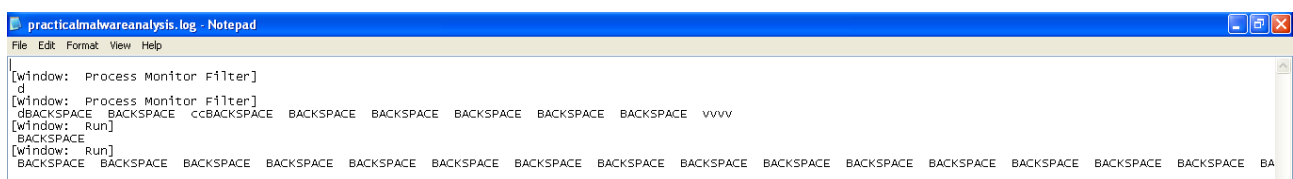
Adesso analizziamo gli eventi di rilievo sul **file system**:



Come si vede, si è scelto di analizzare solo gli eventi relativi al file system (tramite l'icona selezionata in alto) e sono stati applicati tutti e tre i filtri appena menzionati: ciò ci dà modo di vedere che all'interno del path in cui si trova il malware è stato creato un nuovo file. Verifichiamo tale informazione accedendo alla cartella in cui si trova l'eseguibile:



Risulta evidente la creazione del file **practicalmalwareanalysis.log**, il cui contenuto (illustrato nella figura sottostante) consiste nella registrazione dei tasti digitati sulla tastiera a partire dall'avvio del malware. Ciò ci fornisce un indizio fondamentale sulla natura del file malevolo in esame: si tratta di un **keylogger**, ossia un software che cattura gli input immessi a partire da una tastiera, con la finalità di acquisire informazioni sensibili da inviare all'attaccante ed autore del malware.



The screenshot displays the Windows Process Monitor (ProcMon) application. The main window shows a list of system events with columns for Time of Day, Process Name, PID, Operation, Path, Result, and Detail. The 'Process Name' column is filtered to show only 'Malware_U3_W2_L2.exe'. The 'Operation' column is filtered to show 'CreateFile' and 'QueryStandardInformation'. The 'Path' column is filtered to show 'C:\Windows\System32\advapi32.dll' and 'C:\Windows\System32\advapi32.dll'. The 'Result' column is filtered to show 'SUCCESS' and 'SUCCESS'. The 'Detail' column is filtered to show 'SyntheticTypeCreateSection, PageProtection: PAGE_READWRITE' and 'AllocationSize: 1,204,224, EndOfFile: 1,202,774, NumberOfLinks: 1, DeletePending: False'.

The 'Process Monitor Filter' dialog box is open, showing the filter criteria. The 'Display entries matching these conditions:' section contains the following filter rules:

- Architecture is then Include
- Process Name is Malware_U3_W2_L2.exe
- Operation is CreateFile
- Path ends with C:\Windows\System32\advapi32.dll
- Process Name is Promcon.exe

The 'Add' button is highlighted, indicating that the filter rules are being applied.

2. Identificazione di eventuali azioni del malware su **processi e thread** mediante l'utilizzo del tool "Process Monitor"

The screenshot shows the Process Monitor application window. The main pane displays a list of events for the process Malware_U3_W2_L2.exe. A red arrow points to the 'Process Create' event at 12:24.0107486. A red box highlights the 'Process Name' column and the value 'Malware_U3_W2_L2.exe' in the 'Process Monitor Filter' dialog box.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
12.23.3046882	Malware_U3_W2_L2.exe	2700	Process Start		SUCCESS	Parent PID: 1152, Command line: "C:\Documents and Settings\Administrator\Desktop\...
12.23.3046320	Malware_U3_W2_L2.exe	2700	Thread Create		SUCCESS	Thread ID: 2680
12.23.3056260	Malware_U3_W2_L2.exe	2700	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware...	SUCCESS	Image Base: 0x400000, Image Size: 0x0000
12.23.3056465	Malware_U3_W2_L2.exe	2700	Load Image	C:\WINDOWS\system32\ntldr.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0x0000
12.23.3587912	Malware_U3_W2_L2.exe	2700	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf60000
12.23.3910835	Malware_U3_W2_L2.exe	2700	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x02000
12.23.4007037	Malware_U3_W2_L2.exe	2700	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x0000
12.24.0100840	Malware_U3_W2_L2.exe	2700	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d00000, Image Size: 0x06000
12.24.0104226	Malware_U3_W2_L2.exe	2700	Load Image	C:\WINDOWS\system32\ipcch.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x04000
12.24.0107486	Malware_U3_W2_L2.exe	2700	Load Image	C:\WINDOWS\system32\secu32.dll	SUCCESS	Image Base: 0x77f00000, Image Size: 0x11000
12.24.0231463	Malware_U3_W2_L2.exe	2700	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1340, Command line: "C:\WINDOWS\system32\svchost.exe"
12.25.0145468	Malware_U3_W2_L2.exe	2700	Thread Exit		SUCCESS	Thread ID: 2688, User Time: 0.0000000, Kernel Time: 0.0781250
12.25.0149352	Malware_U3_W2_L2.exe	2700	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0781250 seconds, Priv...
15.03.2346522	Malware_U3_W2_L2.exe	360	Process Start		SUCCESS	Parent PID: 1152, Command line: "C:\Documents and Settings\Administrator\Desktop\...
15.03.2346520	Malware_U3_W2_L2.exe	360	Thread Create		SUCCESS	Thread ID: 2140
15.03.2372005	Malware_U3_W2_L2.exe	360	Load Image	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware...	SUCCESS	Image Base: 0x400000, Image Size: 0x0000
15.03.2376070	Malware_U3_W2_L2.exe	360	Load Image	C:\WINDOWS\system32\ntldr.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0x0000
15.03.3211221	Malware_U3_W2_L2.exe	360	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf60000
15.03.3423089	Malware_U3_W2_L2.exe	360	Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x02000
15.03.3530561	Malware_U3_W2_L2.exe	360	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x0000
15.03.3775743	Malware_U3_W2_L2.exe	360	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d00000, Image Size: 0x06000
15.03.3780864	Malware_U3_W2_L2.exe	360	Load Image	C:\WINDOWS\system32\ipcch.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x04000
15.03.3784719	Malware_U3_W2_L2.exe	360	Load Image	C:\WINDOWS\system32\secu32.dll	SUCCESS	Image Base: 0x77f00000, Image Size: 0x11000
15.03.3977922	Malware_U3_W2_L2.exe	360	Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 1340, Command line: "C:\WINDOWS\system32\svchost.exe"
15.04.3886469	Malware_U3_W2_L2.exe	360	Thread Exit		SUCCESS	Thread ID: 2140
15.04.3888813	Malware_U3_W2_L2.exe	360	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0781250 seconds, Priv...

Process Monitor Filter

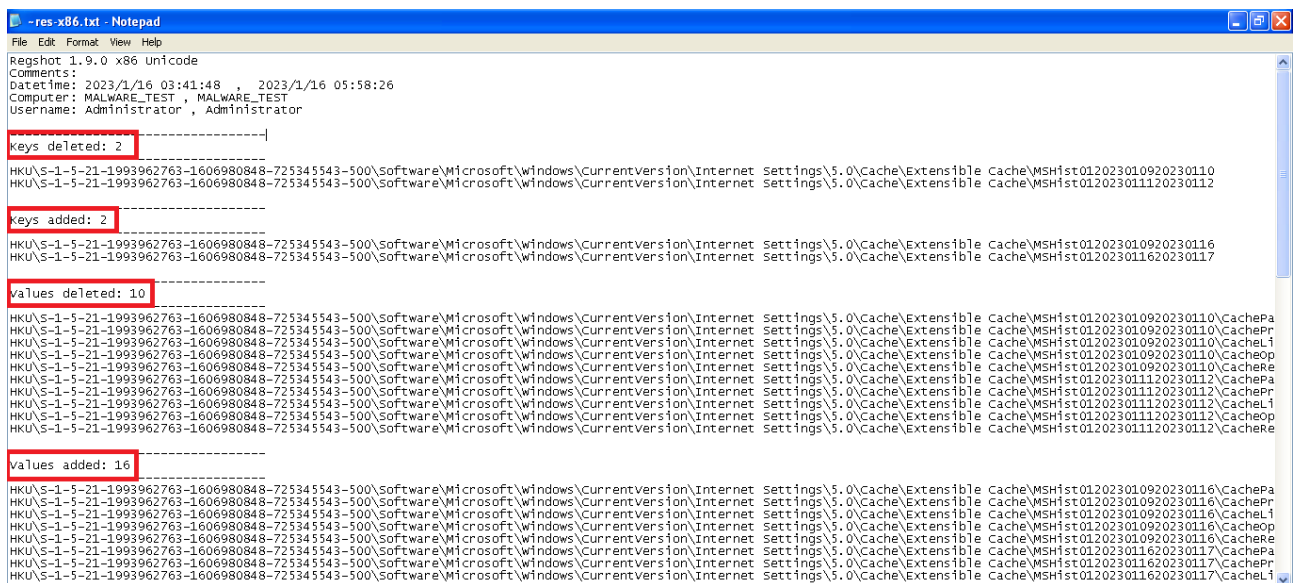
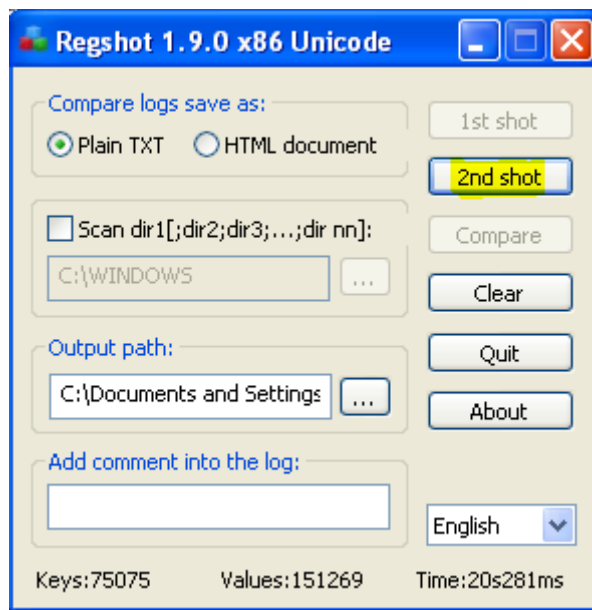
Display entries matching these conditions:

Architecture is then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process Name	is	Malware_U3_W2_L2.exe	Include
<input checked="" type="checkbox"/> Operation	is	Create file	Include
<input checked="" type="checkbox"/> Path	ends with	C:\Documents and Settings\Administrator\Desktop\...	Include
<input checked="" type="checkbox"/> Process Name	is	Procmon.exe	Exclude

OK Cancel Apply



ApateDNS

Capture Window DNS Hex View

Time	Domain Requested	DNS Returned
05.08.17	yutao318525.3322.org	FOUND
05.08.58	yutao318525.3322.org	FOUND
05.09.39	yutao318525.3322.org	FOUND
05.10.21	yutao318525.3322.org	FOUND
05.11.02	yutao318525.3322.org	FOUND
05.11.43	yutao318525.3322.org	FOUND
05.12.24	yutao318525.3322.org	FOUND
05.13.05	yutao318525.3322.org	FOUND
05.13.46	yutao318525.3322.org	FOUND
05.14.27	yutao318525.3322.org	FOUND
05.15.08	yutao318525.3322.org	FOUND
05.15.49	yutao318525.3322.org	FOUND
05.16.30	yutao318525.3322.org	FOUND

[+] Using 192.168.1.50 as return DNS IP!
 [-] Unable to set DNS automatically, please configure DNS manually.
 [+] Sending valid DNS response of first request.
 [+] Server started at 03.37.11 successfully.
 [+] Stopping Server...
 [+] DHCP detected, setting DNS back to DHCP.
 [+] DNS Failed to restore, please reset manually.
 [+] Interfaces list has been refreshed.

DNS Reply IP (Default: Current Gateway/DNS):

of NXDOMAIN's:

Selected Interface:

Emergono numerose chiamate DNS all'indirizzo yutao318525.3322.org, che è stato identificato dal database JoeSandbox come un dominio legittimo con sede in Cina:

Contacted Domains					
Name	IP	Active	Malicious	Antivirus Detection	Reputation
yutao318525.3322.org	183.236.2.18	true	false		high

Contacted IPs					
---------------	--	--	--	--	--



Fonte: <https://www.joesandbox.com/analysis/223589/0/html>

4. **Profilazione** del malware in base alla correlazione tra “operation” e “path”

Al netto dell’analisi appena eseguita, possiamo affermare che il malware in oggetto è un **keylogger** che cattura gli input della tastiera all’interno del file di log **practicalmalwareanalysis.log**; altra peculiarità importante è, come abbiamo visto, la creazione di un processo addizionale “**svchost.exe**” allo scopo di rendere il malware difficilmente rilevabile e mimetizzarne l’attività malevola dell’eleguibile in mezzo a thread legittimi naturalmente presenti su Windows.

