**Floriana Feminò**

**10/01/2023**

**ANALISI DINAMICA BASICA**

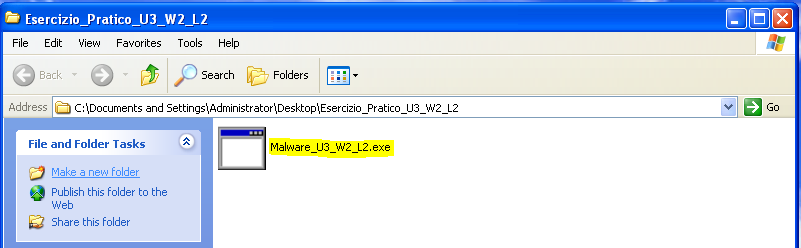
**Analisi del malware *Malware\_U3\_W2\_L2.exe***

**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**.

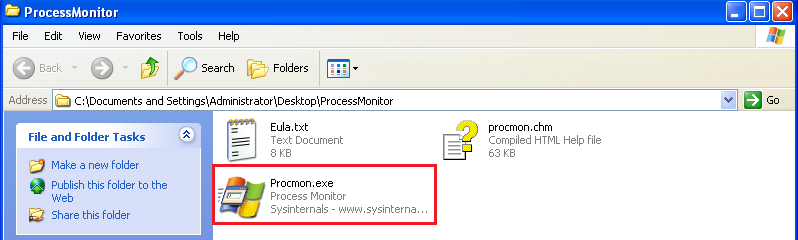
**L’analisi dinamica basica** comprende tutte quelle attività di analisi che presuppongono **l’esecuzione del malware in un ambiente dedicato e protetto**. È generalmente effettuata DOPO l’analisi statica basica, per sopperire ai limiti di quest’ultima (infatti, al contrario dell’analisi statica, l’analisi 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.



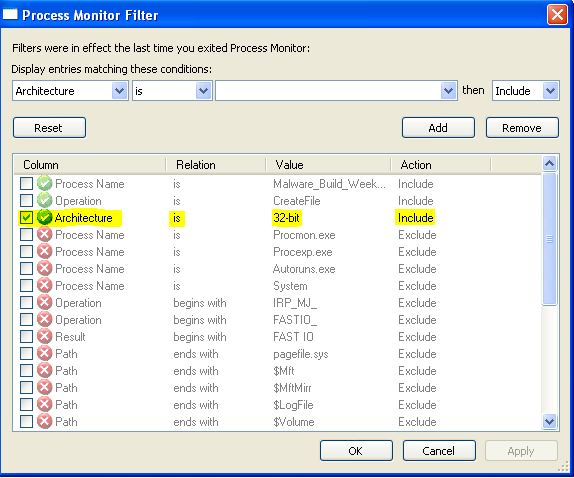
**Operazioni preliminari**

**Process Monitor**

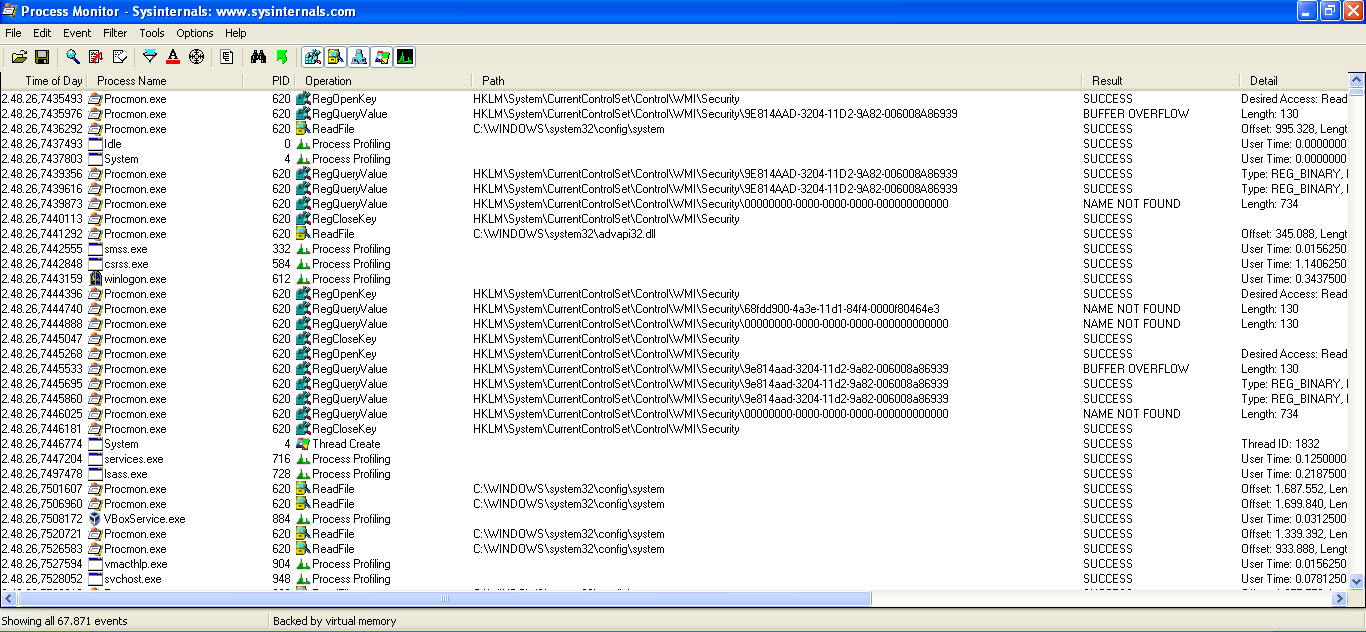
Per l’analisi odierna, ci serviremo di diversi tool per operare un **confronto tra il funzionamento del sistema operativo pre e post-esecuzione del malware oggetto di test**. Uno degli strumenti di cui ci serviremo è **Process Monitor (procmon)**: si tratta di uno strumento avanzato per sistemi operativi 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:

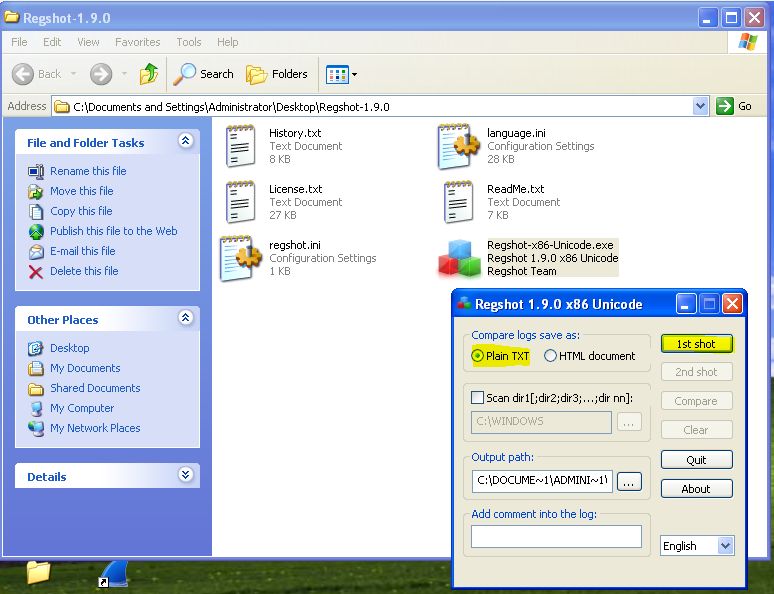


Il filtro produce una lista di eventi relativi all’attività di rete, file system, processi e thread, chiavi di registro e profiling events.



**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”):

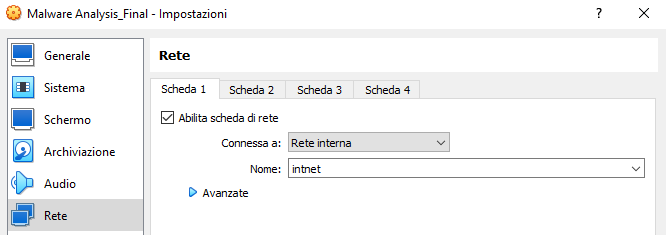


Effettueremo una seconda cattura dopo l’avvio del malware, in modo da procedere con la comparazione.

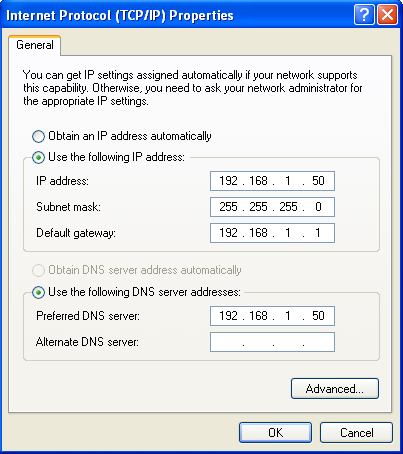
**ApateDNS**

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.

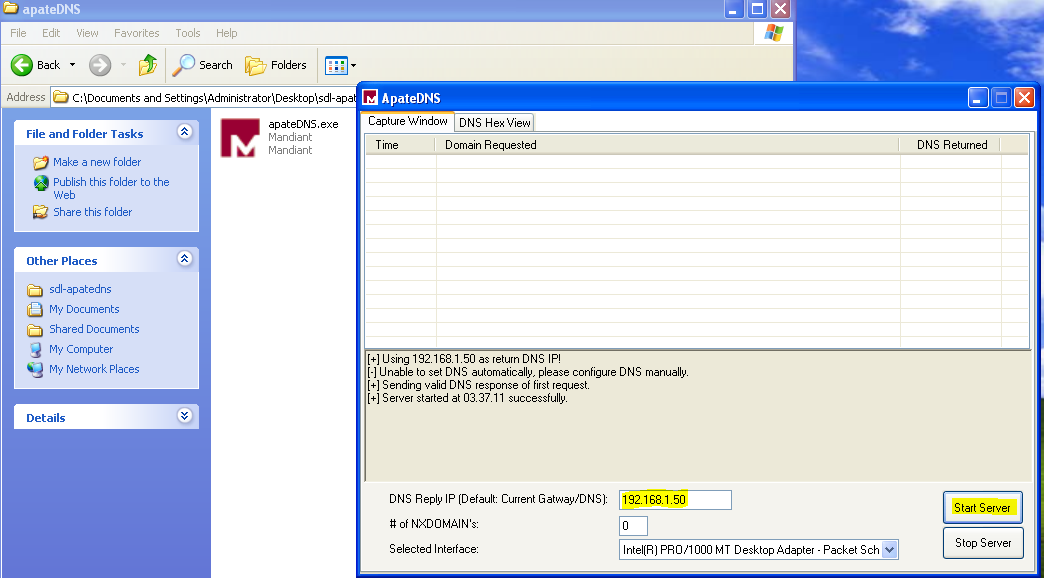
Innanzitutto abilitiamo un’interfaccia di rete, che imposteremo su rete interna:



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**:



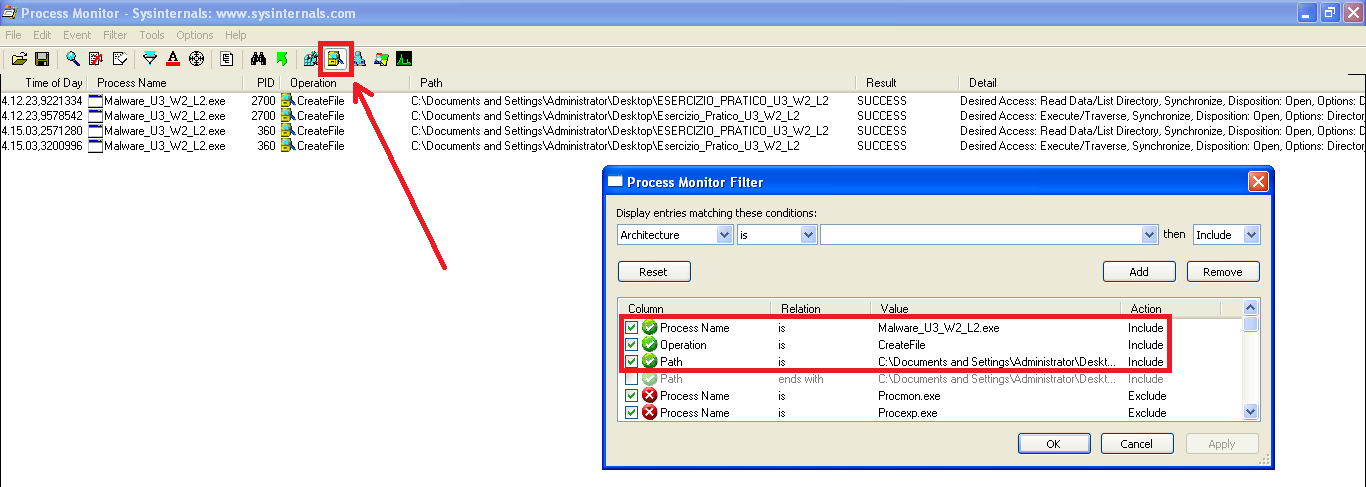
Adesso siamo pronti per avviare il malware e cominciare il test.

1. **Identificazione di eventuali azioni del malware sul file system mediante l’utilizzo del tool “Process Monitor”**

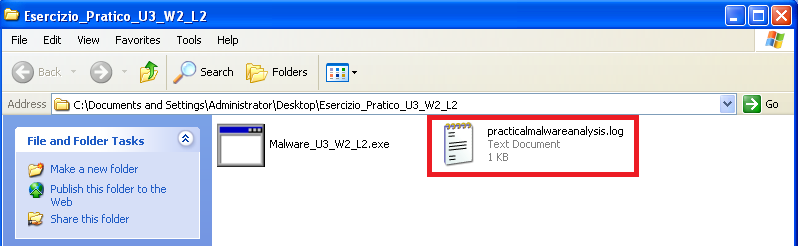
Eseguiamo il malware oggetto di test. Per evidenziare le attività del malware, ci serviremo di alcuni filtri di cattura, da utilizzare individualmente o in combinazione:

* Process Name 🡪 **Malware\_U3\_W2\_L2.exe**
* Operation 🡪 **CreateFile**
* Path 🡪 **C:\Documents and Settings\Administrator\Desktop\Esercizio\_Pratico\_U3\_W2\_L2**

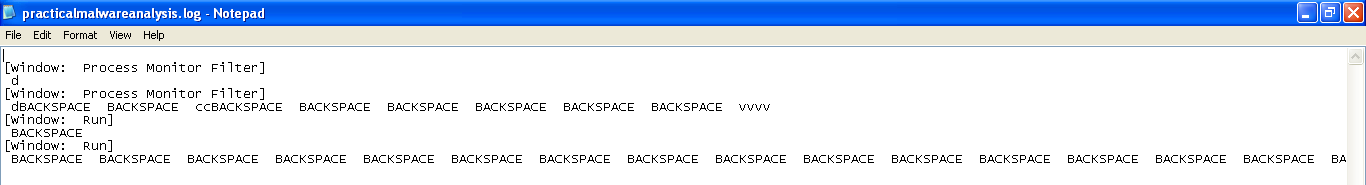
Adesso analizziamo gli eventi di rilievo sul **file system**:



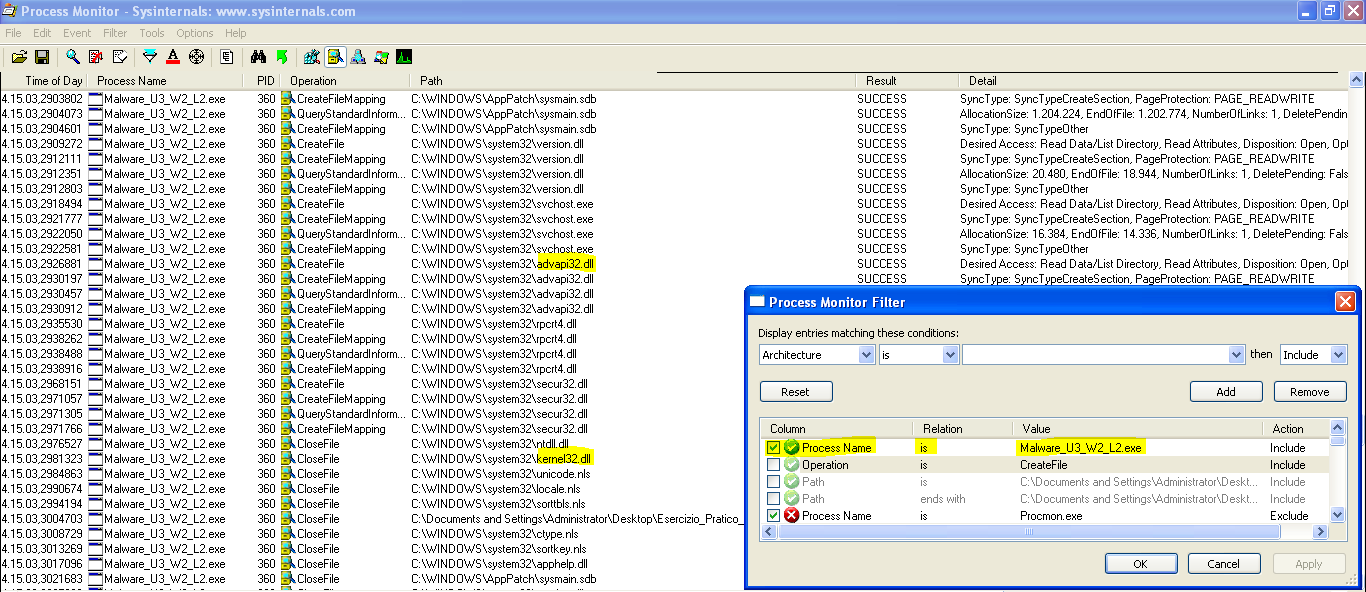
Come si vede, si è scelto di analizzare solo gli eventi relativi al file system (tramite l’icona selezionata in alto) e sono stati applicati tutti e tre i filtri appena menzionati: ciò ci dà modo di vedere che all’interno del path in cui si trova il malware è stato creato un nuovo file. Verifichiamo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



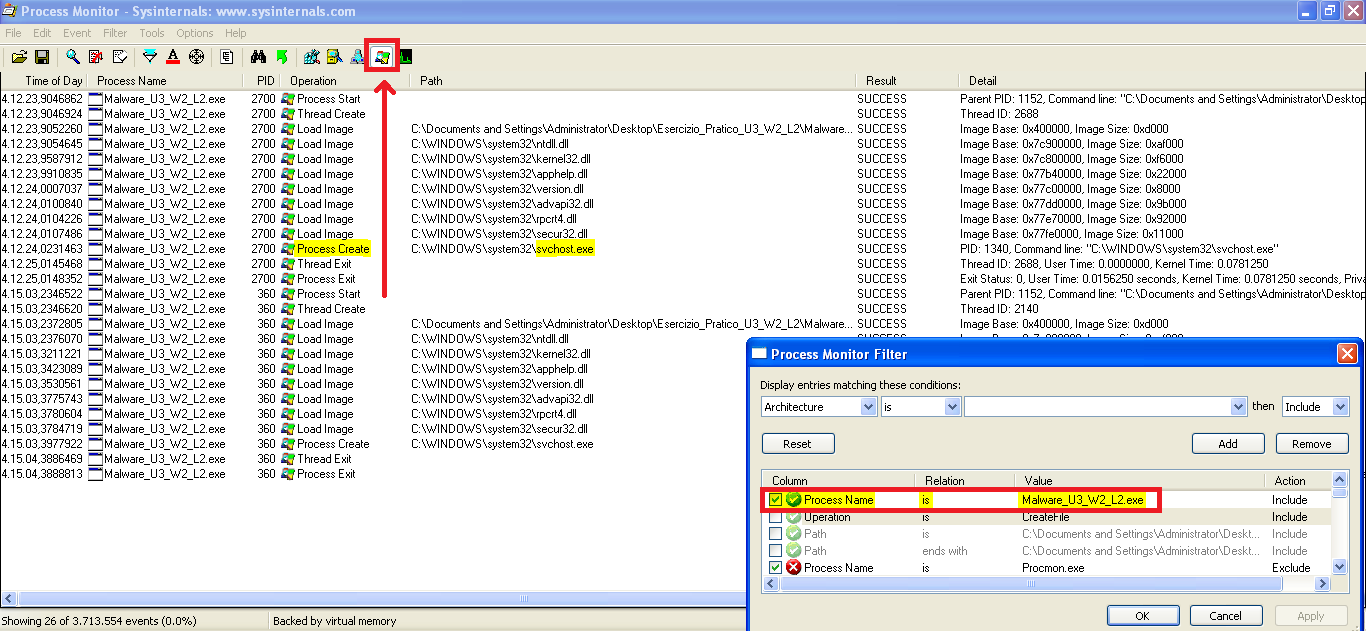
Adesso, per verificare più da vicino ogni interazione del processo relativo al malware con il file system, lasciamo attivo solamente il filtro relativo al nome del processo (*Process Name*) ed osserviamo le attività:



Possiamo notare che il malware interagisce con alcune importanti librerie come **kernel32.dll** (al cui interno sono contenute le funzioni principali per interagire con il sistema operativo, es. manipolazione del file, gestione della memoria) e **advapi.dll** (al cui interno sono contenute le funzioni per interagire con i servizi ed i **registri** del sistema operativo Microsoft).

1. **Identificazione di eventuali azioni del malware su processi e thread mediante l’utilizzo del tool “Process Monitor”**

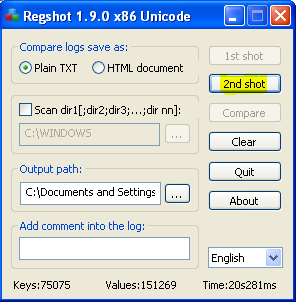
Adesso spostiamo il focus sugli eventi relativi ai **processi e thread**, mantenendo il filtro attivo sulle attività create dal processo relativo al malware in esecuzione (*Process Name is Malware\_U3\_W2\_L2.exe***):**

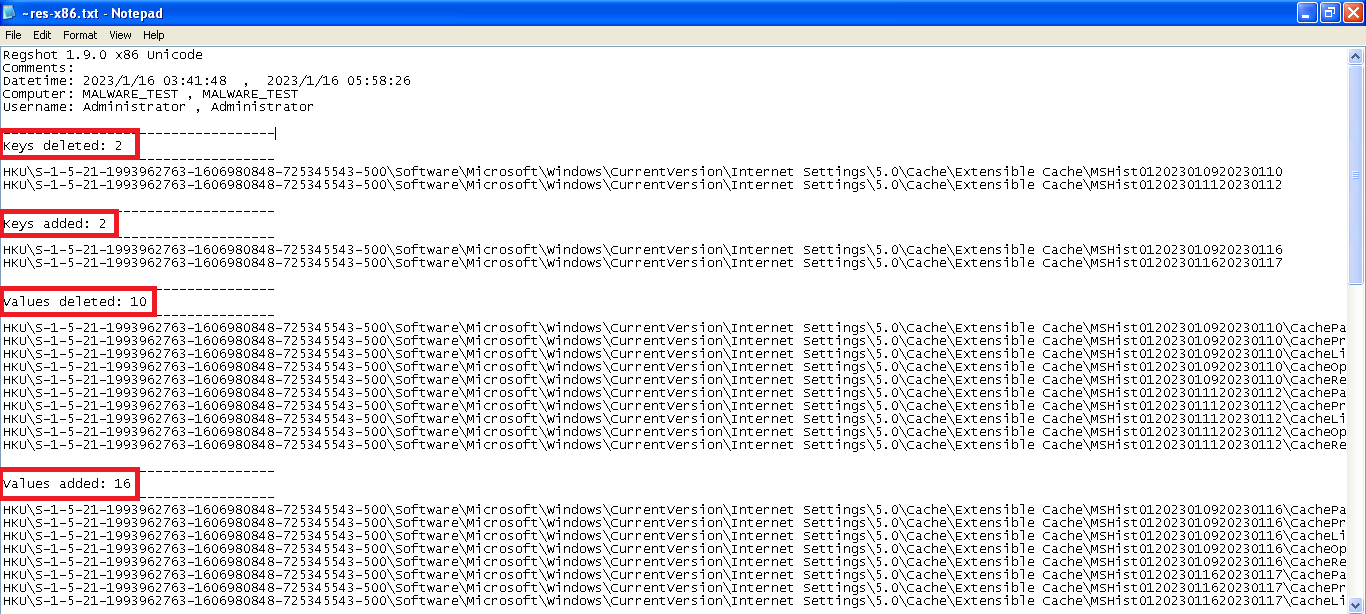


Come possiamo notare, il malware ha creato un processo “**svchost.exe**” tramite la operation “Process Create”. Tale processo ha la finalità di emulare l’omonimo processo legittimo di Windows (presente di default nella cartella System32 di Windows), al fine di non essere rilevato dall’utente e poter così agire indisturbato sul sistema vittima.

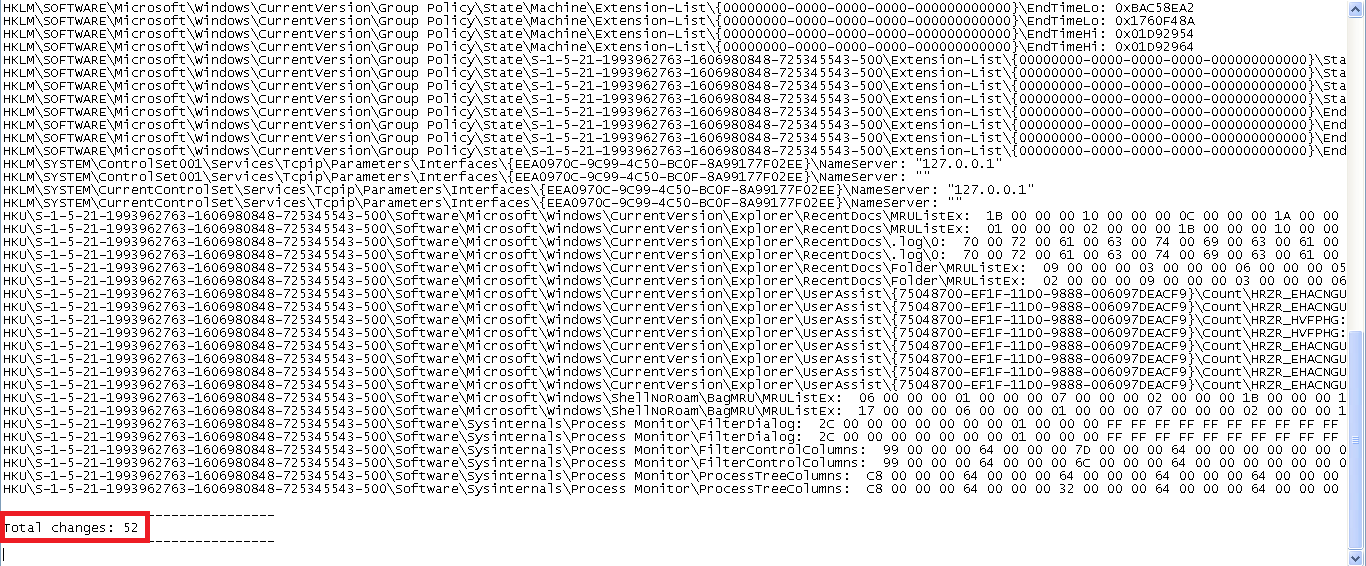
1. **Identificazione di eventuali modifiche alle chiavi di registro da parte del malware (differenze tra prima e dopo l’esecuzione)**

Eseguiamo adesso una seconda istantanea dello stato delle chiavi di registro, e confrontiamola con la prima (scattata prima dell’esecuzione del malware) attraverso la funzione *Compare* di RegShot:









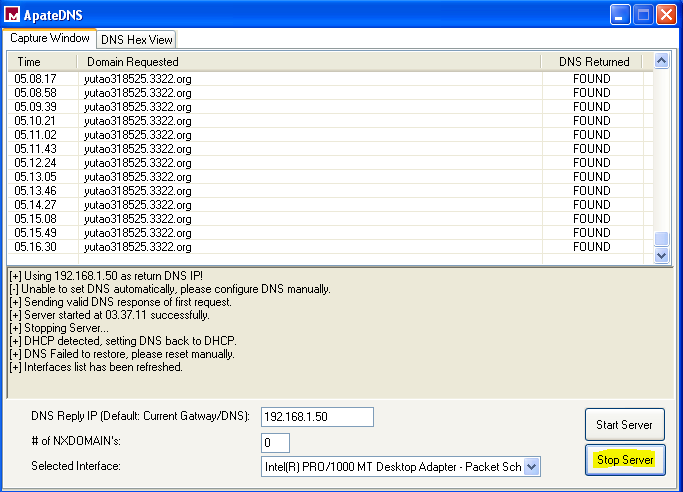
Come si nota, il malware ha

* Eliminato 2 chiavi di registro
* Creato 2 nuove chiavi di registro
* Eliminato 10 valori
* Creato 16 nuovi valori
* Modificato 22 valori

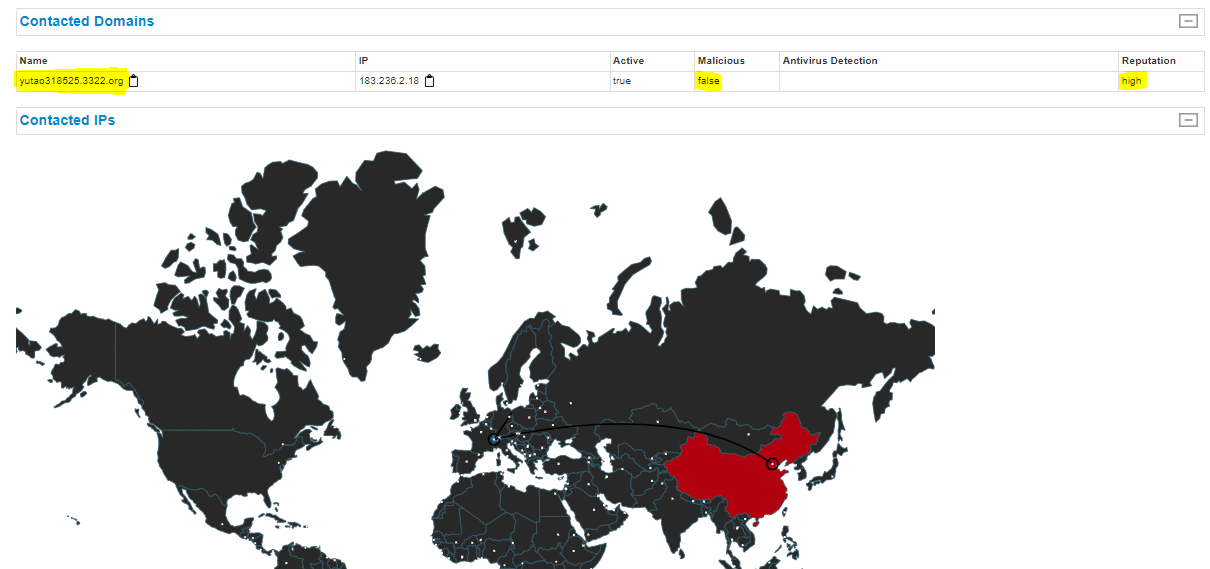
Producendo un totale di 52 cambiamenti.

**Esito della verifica dell’eventuale attività di rete con ApateDNS**

Stoppiamo il server DNS fittizio precedentemente avviato dal software ApateDNS ed osserviamo i risultati della cattura:



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



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

1. **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’eseguibile in mezzo a thread legittimi naturalmente presenti su Windows.

