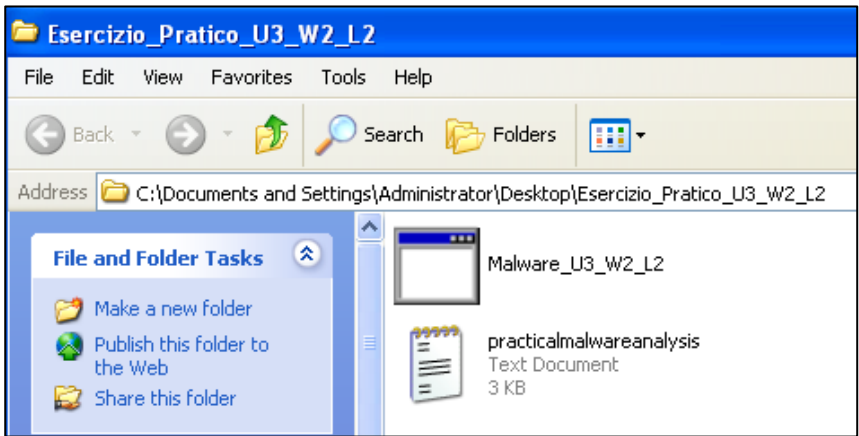


# Analisi dinamica basica

## Sommario

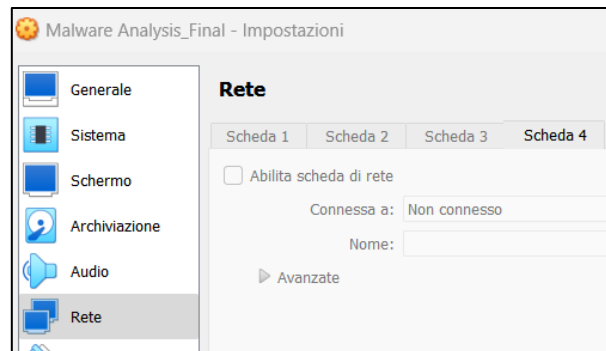
Analisi dinamica basica .....	1
Configurazione ambiente di test .....	2
Analisi con Process Monitor .....	3
Analisi eventi nel file system .....	5
Analisi eventi su processi e thread .....	11
Identificazione modifiche del registro con Regshot .....	14

Analisi dinamica sul malware Malware\_U3\_W2\_L2 su macchina virtuale Windows XP.

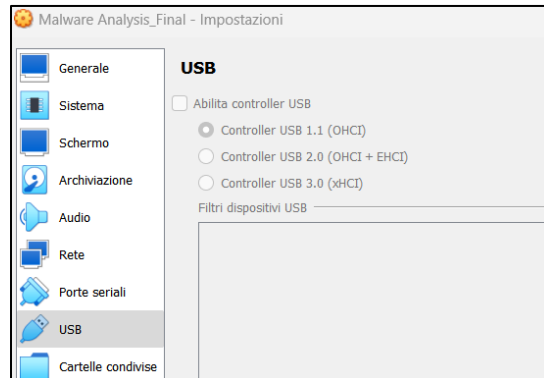
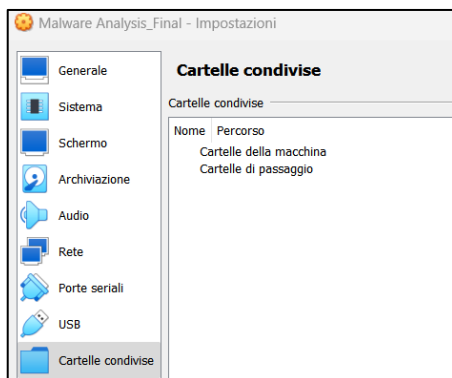


## Configurazione ambiente di test

- ✓ La macchina virtuale su Virtual Box non ha schede di rete abilitate.

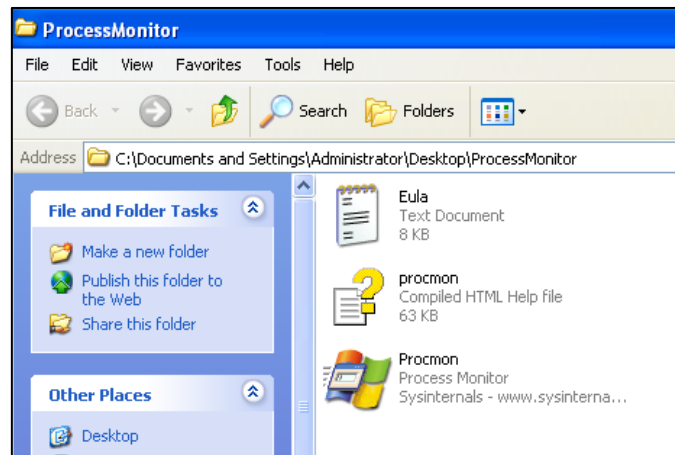


- ✓ Non ci sono cartelle convese con Windows XP né dispositivi USB connessi a Windows XP

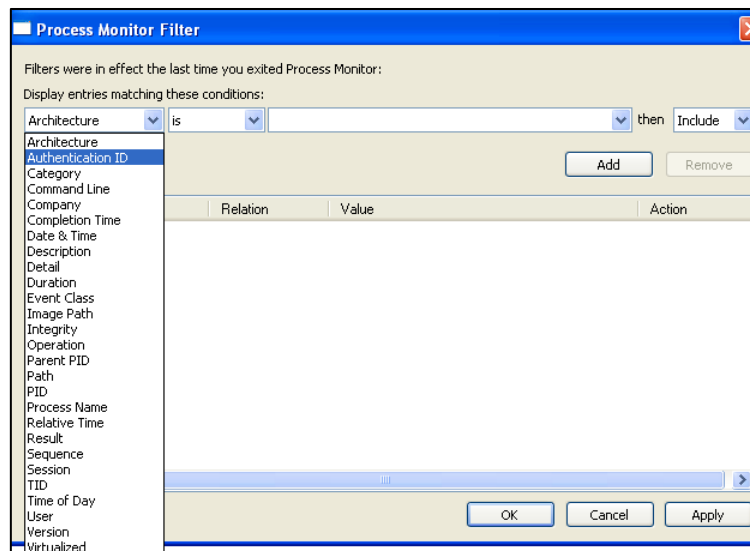


## Analisi con Process Monitor

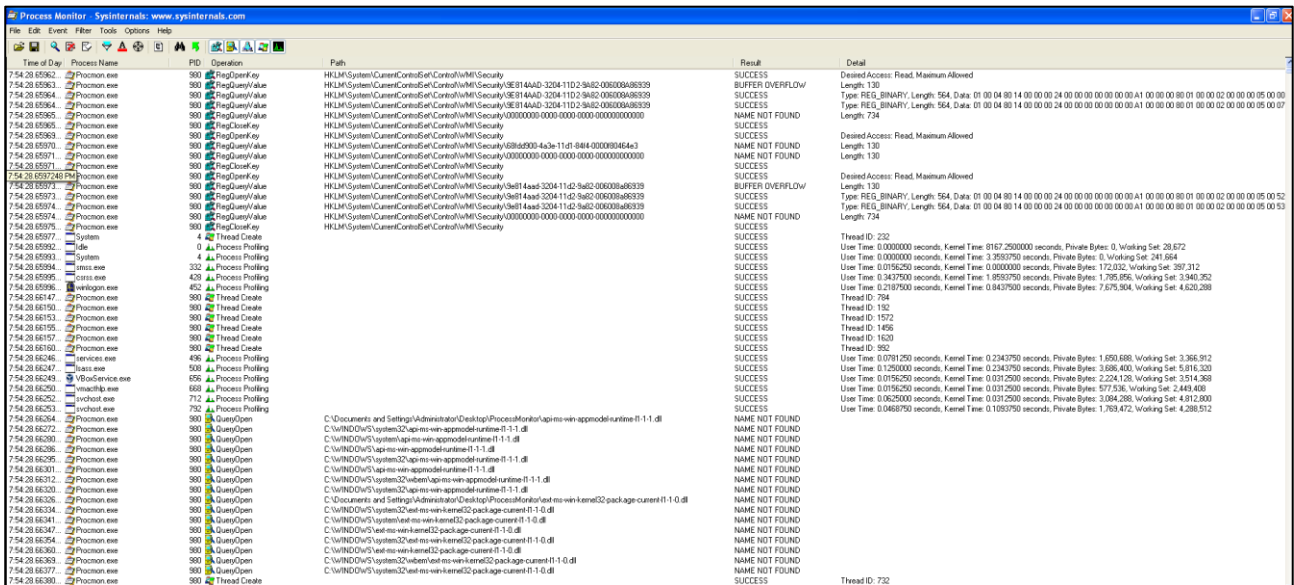
Process Monitor è uno strumento avanzato di monitoraggio per Windows che mostra in tempo reale l'attività del file system, del Registro e dei processi/thread. Combina le funzionalità di due utility Sysinternals di vecchia generazione, Filemon e Regmon, e aggiunge un'ampia lista di miglioramenti tra cui un filtraggio ricco e non distruttivo, dettagliate proprietà degli eventi come ID di sessione e nomi utente, informazioni affidabili sui processi, stack completi dei thread con supporto integrato ai simboli per ogni operazione, registrazione simultanea su un file e molto altro.



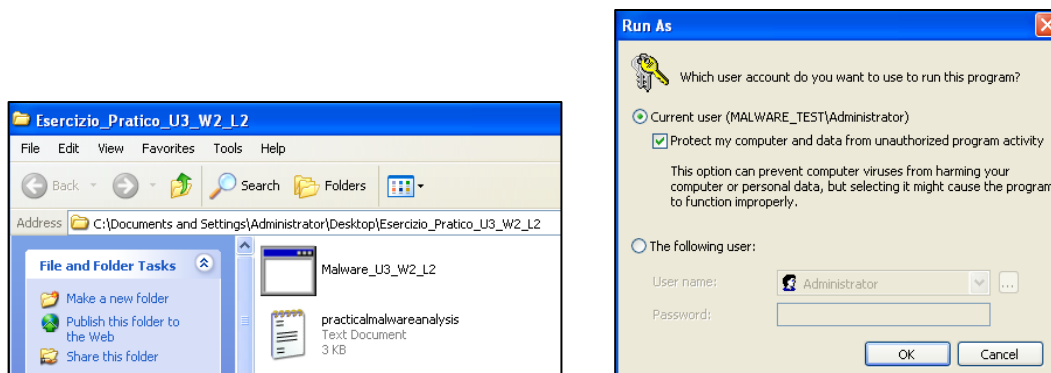
Avviando Process Monitor (procmon.exe) si apre una finestra di impostazione di filtri. Da qua è possibile includere o escludere eventi da monitorare in base a determinati parametri:



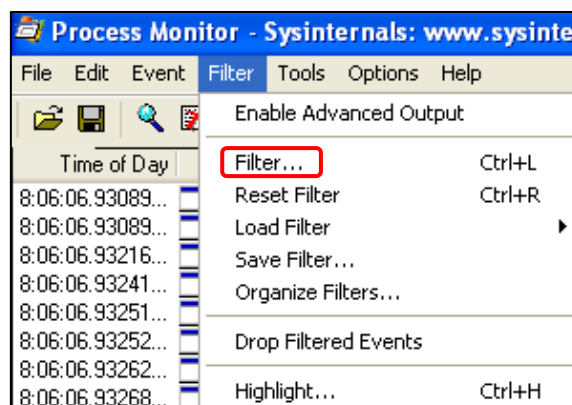
Lasciamo i filtri vuoti in modo da monitorare tutto e chiudiamo la finestra cliccando su “OK”. Vediamo che procmon ha iniziato a catturare i processi del sistema.



Eseguiamo adesso il malware `Malware_U3_W2_L2.exe` come amministratore:

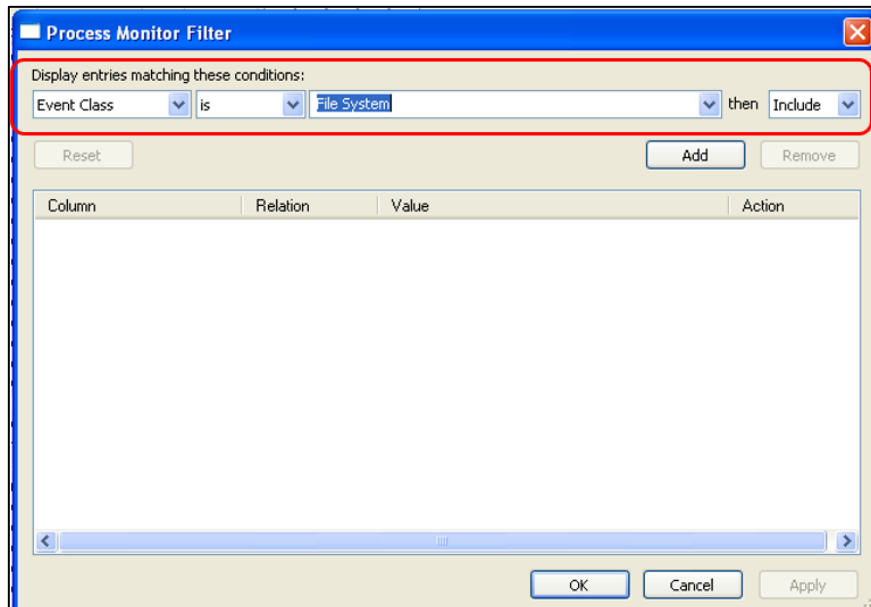


I processi sono moltissimi. Per analizzare più da vicino le azioni del Malware utilizziamo il filtro riaprendo la finestra dal menu “Filter”:

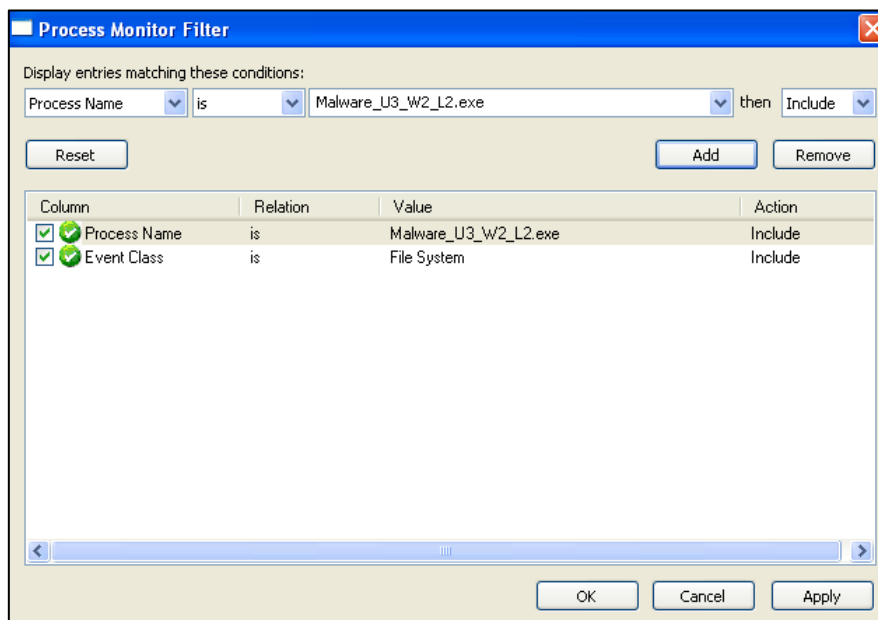


## Analisi eventi nel file system

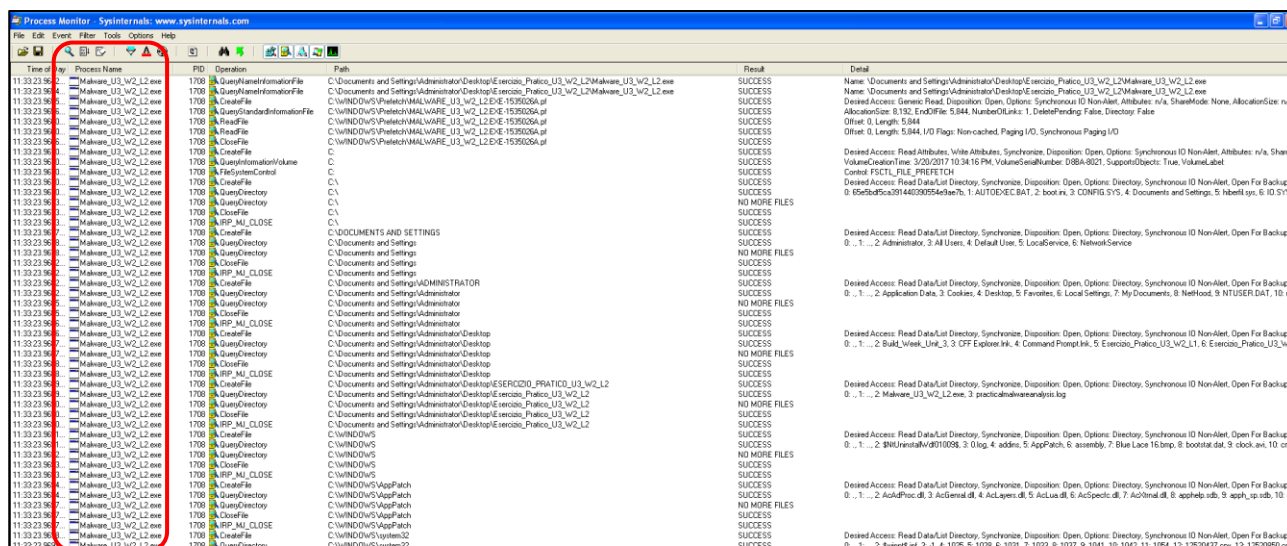
Vediamo le azioni del malware sul **File System** impostando il seguente filtro, e quindi cliccando su “Add” e poi su “Apply”:



I processi sono ancora molti dopo l'applicazione del filtro sul File System, aggiungiamo quindi allo stesso modo un filtro sul **nome processo**, per filtrare gli eventi legati al processo `Malware_U3_W2_L2.exe`:



Vediamo che adesso procmon ha filtrato tutte le azioni eseguite dal malware sul file system:



Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:33:23.962	Malware_U3_W2_L2.exe	1708	QueryNameInformationFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Name: \Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.964	Malware_U3_W2_L2.exe	1708	QueryStandardInformationFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Name: \Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.965	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Windows\System32\MALWARE_U3_W2_L2\EXE-1539206A.pf	SUCCESS	Desired Access: Generic Read; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.966	Malware_U3_W2_L2.exe	1708	ReadFile	C:\Windows\System32\MALWARE_U3_W2_L2\EXE-1539206A.pf	SUCCESS	AllocationSize: 0; 192; EndOfFile: 5,844; NumberOfLinks: 1; DeletePending: False; Directory: False
11:33:23.967	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Windows\System32\MALWARE_U3_W2_L2\EXE-1539206A.pf	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.968	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.969	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.970	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.971	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.972	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.973	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.974	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.975	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.976	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.977	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.978	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.979	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.980	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.981	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.982	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.983	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.984	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.985	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.986	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.987	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.988	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.989	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.990	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.991	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.992	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.993	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.994	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.995	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.996	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:23.997	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O
11:33:23.998	Malware_U3_W2_L2.exe	1708	CreateFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize; Disposition: Open; Options: Synchronous I/O Non-Alert; Attributes: n/a; ShareMode: None; AllocationSize: n/a
11:33:23.999	Malware_U3_W2_L2.exe	1708	QueryInformationVolume	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM; VolumeSerialNumber: D8BA-8021; SupportsObjects: True; VolumeLabel: C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe
11:33:24.000	Malware_U3_W2_L2.exe	1708	CloseFile	C:\Users\Administrator\Desktop\Esecizio_Phaticos_U3_W2_L2\Malware_U3_W2_L2.exe	SUCCESS	Offset: 0; Length: 5,844; I/O Flags: Non-cached, Paging I/O; Synchronous Paging I/O

Possiamo notare nella colonna **Operation** una serie di azioni ripetute più volte su file diversi. Prima di analizzare il comportamento del malware, facciamo una breve descrizione degli eventi principali:

- △ **CreateFile** funzione che serve a creare file ma anche ad aprire file esistenti;
- △ **ReadFile** funzione che serve a leggere dati da un file specifico;
- △ **CloseFile** funzione che serve a chiudere un handle a un file precedentemente aperto;
- △ **QueryNameInformationFile** indica che un processo ha richiesto il nome del file associato a un determinato handle (un riferimento o un identificatore utilizzato per accedere a una risorsa o a un oggetto senza dover fare riferimento ai dettagli interni o alla struttura della risorsa stessa)
- △ **QueryStandardInformationFile** indica che un processo ha richiesto informazioni standard relative a un file associato a un determinato handle. Queste "informazioni standard" includono dettagli come le dimensioni del file, gli attributi, l'allocazione e l'indicatore di eliminazione (cioè se il file è stato segnato per l'eliminazione ma è ancora aperto da qualche processo). Questa chiamata di sistema viene utilizzata per ottenere metadati generali su un file senza necessariamente accedere al contenuto del file stesso;
- △ **CreateFileMapping** è una funzione di sistema di Windows che viene utilizzata per creare o aprire un oggetto di mapping di un file. Questo oggetto di mapping consente a un'applicazione di mappare una vista di un file in uno spazio di indirizzamento di un processo, essenzialmente permettendo al file di essere trattato come se fosse in memoria. Questo è spesso utilizzato per migliorare le prestazioni di lettura/scrittura e per permettere a più processi di condividere lo stesso set di dati in memoria. Questa azione indica che un'applicazione o un componente del sistema sta cercando di creare un mapping in memoria di un file o di un segmento di memoria virtuale;

- △ **FASTIO\_RELEASE\_FOR\_SECTION\_SYNCHRONIZATION** è associato al modello Fast I/O (Input/Output) nel kernel di Windows. Il Fast I/O è un meccanismo che consente alle operazioni di I/O di bypassare la normale routine di creazione di pacchetti I/O e di gestire le operazioni in modo più diretto e veloce. Non tutte le operazioni di I/O possono utilizzare Fast I/O, ma quando è possibile, può offrire prestazioni migliori. Questa azione indica che **un'operazione sta cercando di acquisire l'accesso sincronizzato a una sezione di memoria mappata di un file**. In sostanza, prima che un file possa essere mappato nella memoria (usando funzioni come `CreateFileMapping` e `MapViewOfFile` che abbiamo discusso prima), ogni operazione di I/O in sospeso o in corso sul file deve essere completata.

`FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION` è una delle operazioni Fast I/O che facilita questo processo assicurandosi che il file sia "libero" e pronto per la mappatura;
- △ **FASTIO\_ACQUIRE\_FOR\_CC\_FLUSH** è tipicamente una funzione o un'azione associata alla preparazione di un file per un'operazione di "flush". In termini di I/O, "flushing" si riferisce all'azione di **assicurarsi che tutti i dati in sospeso o memorizzati nella cache siano scritti fisicamente nel disco o nel dispositivo di archiviazione sottostante. Questo assicura l'integrità dei dati**. La parte "ACQUIRE" indica generalmente che una risorsa (in questo caso, probabilmente il file o il buffer associato) viene **acquisita o riservata in modo che l'operazione di flush possa avvenire senza interferenze da altre operazioni simultanee**. In sintesi, `FASTIO_ACQUIRE_FOR_CC_FLUSH` è associato all'acquisizione di una risorsa in preparazione per un'operazione di flushing usando meccanismi di Fast I/O nel kernel di Windows. Questo meccanismo è progettato per migliorare l'efficienza delle operazioni di I/O su file.
- △ **FASTIO\_RELEASE\_FOR\_CC\_FLUSH** mentre `FASTIO_ACQUIRE_FOR_CC_FLUSH` indica l'acquisizione di una risorsa in preparazione per un'operazione di flushing, il complementare **FASTIO\_RELEASE\_FOR\_CC\_FLUSH** indica la **liberazione di tale risorsa dopo l'operazione di flushing**.
- △ **IRP\_MJ\_CLOSE** è un'operazione associata al sistema di I/O (Input/Output) di Windows. Rappresenta una **richiesta per chiudere un handle a un oggetto**, come un file o una chiave del registro. Quando un'applicazione o un componente del sistema operativo apre un file, una chiave del registro o un altro oggetto, ottiene ciò che è noto come "handle" a quell'oggetto. Questo handle viene utilizzato per accedere e interagire con l'oggetto. Quando ha finito di usarlo, l'handle deve essere chiuso. L'operazione `IRP_MJ_CLOSE` indica proprio questa chiusura.

Analizzando i file sui quali il malware ha eseguito le operazioni sopra esplicitate, vediamo alcuni interessanti:

■ **Creazione, richiesta informazioni, lettura e chiusura del file `MALWARE_U3_W2_L2.EXE-1535026A.pf`:**

CreateFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
QueryStandardInformationFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
ReadFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
CloseFile	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf

I file **Prefetch (.pf)** sono utilizzati dal sistema operativo Windows per accelerare il processo di avvio delle applicazioni e il boot del sistema stesso. Quando viene avviata un'applicazione, Windows monitora quali file vengono utilizzati e in che ordine. Queste informazioni vengono quindi salvate nei file .pf nella cartella Prefetch. La prossima volta che viene avviata la stessa applicazione, Windows può riferirsi a queste informazioni per caricare anticipatamente alcuni dati nell'RAM, rendendo il lancio dell'applicazione più veloce.

Questo blocco di azioni ci indica che il malware ha inserito se stesso nella lista dei file prefetch (con l'evento `CreateFile`) in modo da ottimizzare il suo avvio, ha richiesto le informazioni standard del file .pf appena creato (`QueryStandardInformationFile`), lo ha letto (`ReadFile`) e quindi lo ha chiuso (`CloseFile`).

Possiamo vedere i dettagli di queste operazioni nell'immagine seguente:

CreateFile	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous I/O Non-Alert, Attributes: n/a, ShareMode: None, AllocationSize: n/a, OpenResult: Opened
QueryStandardInformationFile	SUCCESS	AllocationSize: 8,192, EndOfFile: 5,844, NumberOfLinks: 1, DeletePending: False, Directory: False
ReadFile	SUCCESS	Offset: 0, Length: 5,844
ReadFile	SUCCESS	Offset: 0, Length: 5,844, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
CloseFile	SUCCESS	

■ **Letture e mappatura di vari file:**

Vediamo diverse azioni di lettura (evento `CreateFile`) e mappatura con accesso sincronizzato (eventi `CreateFileMapping` e `FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION`) su vari file:

1708	CreateFile	C:\WINDOWS\system32\ctype.nls
1708	CreateFileMapping	C:\WINDOWS\system32\ctype.nls
1708	QueryStandardInformationFile	C:\WINDOWS\system32\ctype.nls
1708	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\ctype.nls
1708	CreateFileMapping	C:\WINDOWS\system32\ctype.nls
1708	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\ctype.nls
1708	CreateFile	C:\WINDOWS\system32\sortkey.nls
1708	CreateFileMapping	C:\WINDOWS\system32\sortkey.nls
1708	QueryStandardInformationFile	C:\WINDOWS\system32\sortkey.nls
1708	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\sortkey.nls
1708	CreateFileMapping	C:\WINDOWS\system32\sortkey.nls
1708	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\sortkey.nls
1708	CreateFile	C:\WINDOWS\system32\apphelp.dll
1708	CreateFileMapping	C:\WINDOWS\system32\apphelp.dll
1708	QueryStandardInformationFile	C:\WINDOWS\system32\apphelp.dll
1708	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\apphelp.dll
1708	CreateFileMapping	C:\WINDOWS\system32\apphelp.dll
1708	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\apphelp.dll
1708	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb
1708	CreateFileMapping	C:\WINDOWS\AppPatch\sysmain.sdb
1708	QueryStandardInformationFile	C:\WINDOWS\AppPatch\sysmain.sdb
1708	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\AppPatch\sysmain.sdb
1708	CreateFileMapping	C:\WINDOWS\AppPatch\sysmain.sdb
1708	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\AppPatch\sysmain.sdb
1708	CreateFile	C:\WINDOWS\system32\version.dll
1708	CreateFileMapping	C:\WINDOWS\system32\version.dll
1708	QueryStandardInformationFile	C:\WINDOWS\system32\version.dll
1708	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\version.dll
1708	CreateFileMapping	C:\WINDOWS\system32\version.dll
1708	FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\version.dll



Vediamo i tipi di alcuni di questi file:

**.dll: Dynamic Link Library**, ovvero file “libreria” che contengono dati e risorse che possono essere utilizzati da più programmi contemporaneamente);

**.nls: National Language Support** (Supporto per la lingua nazionale), ovvero file utilizzati per fornire supporto per la codifica di caratteri e altre funzioni legate alla localizzazione in Windows;

**.sdb: file associati a "Application Compatibility Databases"** (Database di Compatibilità delle Applicazioni) nei sistemi operativi Microsoft Windows. Questi file contengono informazioni che permettono a versioni più recenti di Windows di eseguire correttamente software e applicazioni progettati per versioni precedenti di Windows.

■ **Lettura e mappatura dei file `svchost.exe` e `kernel32.dll`, con acquisizione e rilascio per l'operazione di flushing**

Soffermiamoci su questi due file che sono fondamentali per i sistemi Windows, e che il malware ha mappato, bloccato per un'operazione di flushing (`FASTIO_ACQUIRE_FOR_SECTION_SYNCHRONIZATION`), e successivamente rilasciato (`FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION`).

CreateFile	C:\WINDOWS\system32\svchost.exe
CreateFileMapping	C:\WINDOWS\system32\svchost.exe
FASTIO_ACQUIRE_FOR_CC_FLUSH	C:\WINDOWS\system32\svchost.exe
FASTIO_RELEASE_FOR_CC_FLUSH	C:\WINDOWS\system32\svchost.exe
FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\svchost.exe
CreateFileMapping	C:\WINDOWS\system32\svchost.exe
FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\svchost.exe

CreateFile	C:\WINDOWS\system32\kernel32.dll
CreateFileMapping	C:\WINDOWS\system32\kernel32.dll
FASTIO_ACQUIRE_FOR_CC_FLUSH	C:\WINDOWS\system32\kernel32.dll
FASTIO_RELEASE_FOR_CC_FLUSH	C:\WINDOWS\system32\kernel32.dll
FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\kernel32.dll
CreateFileMapping	C:\WINDOWS\system32\kernel32.dll
FASTIO_RELEASE_FOR_SECTION_SYNCHRONIZATION	C:\WINDOWS\system32\kernel32.dll

La presenza di queste due operazioni suggerisce che c'è stata una tentata operazione di flushing. Tuttavia, non essendoci altre operazioni (ad esempio di scrittura o di flushing) intermedie, non sembra che i file siano stati modificati né salvate in memoria le modifiche.

Di seguito vediamo i dettagli di queste operazioni.

CreateFile	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
CreateFileMapping	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
QueryStandardInformationFile	AllocationSize: 53,248, EndOfFile: 53,248, NumberOfLinks: 1, DeletePending: False, Directory: False

Notiamo nei dettagli di `CreateFile` che l'accesso richiesto è in sola lettura, fatto che conferma che il malware non ha apportato modifiche ai file

Desired Access: Read Data/List Directory, Read Attributes,

Vediamo adesso cosa sono questi due file:

**svchost.exe** è un nome generico che viene assegnato ad un processo Host di Windows. Si tratta di una parte integrante del sistema operativo ed è necessario al corretto funzionamento di vari aspetti del sistema operativo. Questo processo funge da **shell per il caricamento di file DLL (Dynamic-link Library)** che comprendono librerie software che vengono caricate, in modo dinamico, in fase di esecuzione invece di essere collegate staticamente ad un file eseguibile in fase di compilazione. **svchost.exe** nasce, quindi, con l'obiettivo di **utilizzare i file DLL che integrano il codice necessario al corretto funzionamento del sistema operativo**.

Il file **kernel32.dll** è una delle librerie dinamiche (DLL) più fondamentali nei sistemi operativi Windows. Fornisce una vasta gamma di funzioni critiche che permettono alle applicazioni di interagire con il sistema operativo. In particolare, offre funzioni che permettono alle applicazioni di gestire la memoria, creare processi, interagire con il sistema file, e molte altre operazioni essenziali.

#### ■ Chiusura dei file e degli handle agli oggetti

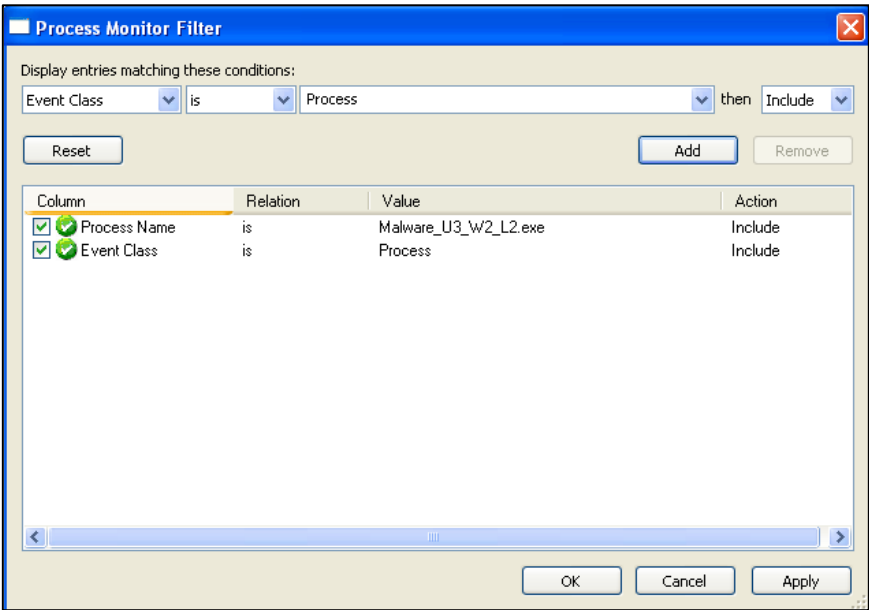
A seguito delle operazioni di lettura e mappatura dei file di sistema, il malware chiude i file (**CloseFile**) e quindi il relativo handle all'oggetto (**IRP\_MJ\_CLOSE**):

CloseFile	C:\WINDOWS\system32\kernel32.dll
IRP_MJ_CLOSE	C:\WINDOWS\system32\kernel32.dll
CloseFile	C:\WINDOWS\system32\unicode.nls
IRP_MJ_CLOSE	C:\WINDOWS\system32\unicode.nls
CloseFile	C:\WINDOWS\system32\locale.nls
IRP_MJ_CLOSE	C:\WINDOWS\system32\locale.nls
CloseFile	C:\WINDOWS\system32\sorttbls.nls
IRP_MJ_CLOSE	C:\WINDOWS\system32\sorttbls.nls
CloseFile	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
IRP_MJ_CLOSE	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe
CloseFile	C:\WINDOWS\system32\ctype.nls
IRP_MJ_CLOSE	C:\WINDOWS\system32\ctype.nls
CloseFile	C:\WINDOWS\system32\sortkey.nls
IRP_MJ_CLOSE	C:\WINDOWS\system32\sortkey.nls
CloseFile	C:\WINDOWS\system32\apphelp.dll
IRP_MJ_CLOSE	C:\WINDOWS\system32\apphelp.dll
CloseFile	C:\WINDOWS\AppPatch\sysmain.sdb
IRP_MJ_CLOSE	C:\WINDOWS\AppPatch\sysmain.sdb
CloseFile	C:\WINDOWS\system32\version.dll
IRP_MJ_CLOSE	C:\WINDOWS\system32\version.dll
CloseFile	C:\WINDOWS\system32\svchost.exe
IRP_MJ_CLOSE	C:\WINDOWS\system32\svchost.exe
CloseFile	C:\WINDOWS\system32\advapi32.dll
IRP_MJ_CLOSE	C:\WINDOWS\system32\advapi32.dll
CloseFile	C:\WINDOWS\system32\rpcrt4.dll

Per quanto riguarda il File System, non sembra che il malware abbia compromesso alcun file, seppure abbia creato una mappatura a diversi file critici, avendo quindi la potenzialità di eseguire operazioni potenzialmente dannose.

Analisi eventi su processi e thread

Impostiamo adesso un filtro di Process Monitor con Event Class is Process



Vediamo il risultato:

Operation	Path	Result	Detail
Process Start		SUCCESS	Parent PID: 956, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pk...
Thread Create		SUCCESS	Thread ID: 640
Load Image	C:\Documents and Settings\Administrator\De...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77fe0000, Image Size: 0x11000
Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 276, Command line: "C:\WINDOWS\system32\svchost.exe"
Thread Exit		SUCCESS	Thread ID: 640, User Time: 0.0000000, Kernel Time: 0.0156250
Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0156250 seconds, Private Bytes: 27...
Process Start		SUCCESS	Parent PID: 1132, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pk...
Thread Create		SUCCESS	Thread ID: 1300
Load Image	C:\Documents and Settings\Administrator\De...	SUCCESS	Image Base: 0x400000, Image Size: 0xd000
Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
Load Image	C:\WINDOWS\system32\apphelp.dll	SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77fe0000, Image Size: 0x11000
Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 2044, Command line: "C:\WINDOWS\system32\svchost.exe"
Thread Exit		SUCCESS	Thread ID: 1300, User Time: 0.0000000, Kernel Time: 0.0000000
Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0000000 seconds, Private Bytes: 27...

Anche in questo caso, andiamo a descrivere il significato delle azioni presenti nei risultati di Process Monitor:

- △ **ProcessStart** indica l'inizio dell'esecuzione di un nuovo processo. Un processo è un'entità in esecuzione che rappresenta un'applicazione o un servizio;
- △ **ProcessCreate** analogamente a **ProcessStart**, indica la creazione di un nuovo processo;
- △ **ProcessExit** indica che un processo ha completato la sua esecuzione e sta terminando. Tutte le risorse associate al processo vengono in genere rilasciate dal sistema operativo;
- △ **ThreadCreate** Indica la creazione di un nuovo thread all'interno di un processo esistente. I thread sono le unità di base di esecuzione all'interno di un processo e permettono l'esecuzione concorrente di compiti all'interno dello stesso processo;
- △ **ThreadExit** indica che un thread all'interno di un processo ha terminato la sua esecuzione. Un thread può concludersi prima del processo padre;
- △ **LoadImage** si riferisce al caricamento di un'immagine eseguibile (come un file .exe o .dll) nella memoria di un processo. Questo accade quando un'applicazione o una libreria viene inizialmente caricata o quando vengono caricate delle DLL supplementari.

Vediamo adesso le azioni eseguite dal malware.

#### ■ **Avvio del malware :**

Il primo evento, **ProcessStart** sul file **Malware\_U3\_W2\_L2.exe** (come vediamo bene nel dettaglio sotto), indica l'avvio del malware:

PID	Operation	Result	Detail
1708	Process Start	SUCCESS	Parent PID: 956, Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L2\Malware_U3_W2_L2.exe"

**Event** | Process | Stack

Date: 10/28/2023 11:33:23 AM  
Thread: 240  
Class: Process  
**Operation: Process Start**  
**Result: SUCCESS**  
Path:  
Duration: 0.0000000

Parent PID: 956  
Command line: "C:\Documents and Settings\Administrator\Desktop\Esercizio\_Pratico\_U3\_W2\_L2\Malware\_U3\_W2\_L2.exe"  
Current directory: C:\Documents and Settings\Administrator\Desktop\Esercizio\_Pratico\_U3\_W2\_L2  
Environment:

==:={}  
ALLUSERPROFILE=C:\Documents and Settings\All Users  
APPDATA=C:\Documents and Settings\Administrator\Application Data  
CommonProgramFiles=C:\Program Files\Common Files  
COMPUTERNAME=MALWARE\_TEST  
ComSpec=C:\WINDOWS\system32\cmd.exe  
FP\_NO\_HOST\_CHECK=NO  
HOMEDRIVE=C:  
HOMEPATH=C:\Documents and Settings\Administrator  
LOGONSERVER={MALWARE\_TEST  
NUMBER\_OF\_PROCESSORS=1  
OS=Windows\_NT  
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32;Wbem  
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH  
PROCESSOR\_ARCHITECTURE=x86  
PROCESSOR\_IDENTIFIER=x86 Family 6 Model 140 Stepping 1, GenuineIntel  
PROCESSOR\_LEVEL=6  
PROCESSOR\_REVISION=8c01  
ProgramFiles=C:\Program Files  
SESSIONNAME=Console  
SystemDrive=C:  
SystemRoot=C:\WINDOWS  
TEMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp  
TMP=C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp  
USERDOMAIN=MALWARE\_TEST  
USERNAME=Administrator  
USERPROFILE=C:\Documents and Settings\Administrator  
windir=C:\WINDOWS

## ■ Creazione di thread e caricamento di dll

Dopo l'avvio, vediamo che il malware ha creato il thread 640 e ha caricato alcune dll:

Thread Create	SUCCESS	Thread ID: 640
Load Image	C:\Documents and Settings\Administrator\D... SUCCESS	Image Base: 0x400000, Image Size: 0xd000
Load Image	C:\WINDOWS\system32\ntdll.dll SUCCESS	Image Base: 0x7c900000, Image Size: 0xaf000
Load Image	C:\WINDOWS\system32\kernel32.dll SUCCESS	Image Base: 0x7c800000, Image Size: 0xf6000
Load Image	C:\WINDOWS\system32\apphelp.dll SUCCESS	Image Base: 0x77b40000, Image Size: 0x22000
Load Image	C:\WINDOWS\system32\version.dll SUCCESS	Image Base: 0x77c00000, Image Size: 0x8000
Load Image	C:\WINDOWS\system32\advapi32.dll SUCCESS	Image Base: 0x77dd0000, Image Size: 0x9b000
Load Image	C:\WINDOWS\system32\rpcrt4.dll SUCCESS	Image Base: 0x77e70000, Image Size: 0x92000
Load Image	C:\WINDOWS\system32\secur32.dll SUCCESS	Image Base: 0x77fe0000, Image Size: 0x11000

## ■ Avvio del processo svchost.exe, chiusura del thread e chiusura del malware

Vediamo che successivamente il malware avvia il processo svchost.exe (ProcessCreate)

Process Create	C:\WINDOWS\system32\svchost.exe	SUCCESS	PID: 276, Command line: "C:\WINDOWS\system32\svchost.exe"
Thread Exit		SUCCESS	Thread ID: 640, User Time: 0.0000000, Kernel Time: 0.0156250
Process Exit		SUCCESS	Exit Status: 0, User Time: 0.0156250 seconds, Kernel Time: 0.0156250

L'azione seguente indica la chiusura del thread 640 e quindi del processo relativo al malware, come mostrano le immagini di dettaglio seguenti:

Event	Process	Stack
Date:	10/28/2023 11:33:25 AM	
Thread:	640	
Class:	Process	
Operation:	Thread Exit	
Result:	SUCCESS	
Path:		
Duration:	0.0000000	
Thread ID:	640	
User Time:	0.0000000	
Kernel Time:	0.0156250	

Event	Process	Stack
Date:	10/28/2023 11:33:25 AM	
Thread:	640	
Class:	Process	
Operation:	Process Exit	
Result:	SUCCESS	
Path:		
Duration:	0.0000000	
Exit Status:	0	
User Time:	0.0156250 seconds	
Kernel Time:	0.0156250 seconds	
Private Bytes:	274,432	
Peak Private Bytes:	307,200	
Working Set:	1,052,672	
Peak Working Set:	1,081,344	

Image

Name: Malware\_U3\_W2\_L2.exe

Version:

Path: C:\Documents and Settings\Administrator\Desktop\Esercizio\_Pratico\_U3\_W2\_L2\Malware\_U3\_W2\_L2.exe

Command Line: "C:\Documents and Settings\Administrator\Desktop\Esercizio\_Pratico\_U3\_W2\_L2\Malware\_U3\_W2\_L2.exe"

PID: 1708 Architecture: 32-bit

Parent PID: 956 Virtualized: n/a

Session ID: 0 Integrity: n/a

User: MALWARE\_TEST\Administrator

Auth ID: 00000000:000185bd

Started: 10/28/2023 11:33:23 AM Ended: 10/28/2023 11:33:25 AM

Modules:

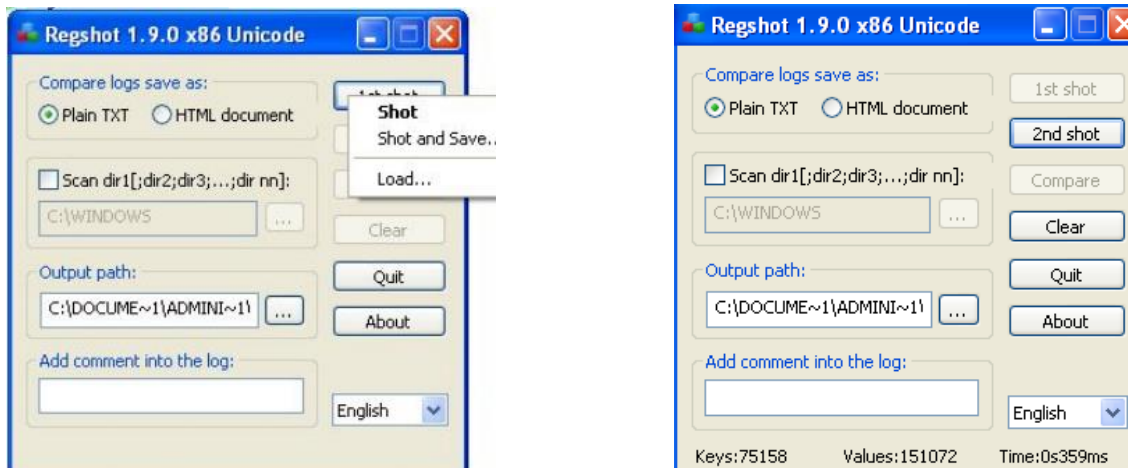
Module	Address	Size	Path	Company	Version	Timestamp
Malware_U3_W...	0x400000	0xd000	C:\Documents and Settings\Administr...			1/1/1970 1:00:...
apphelp.dll	0x77b40000	0x22000	C:\WINDOWS\system32\apphelp.dll	Microsoft Corpo...	5.1.2600.5512 ...	1/1/1970 1:00:...
version.dll	0x77c00000	0x8000	C:\WINDOWS\system32\version.dll	Microsoft Corpo...	5.1.2600.5512 ...	1/1/1970 1:00:...
advapi32.dll	0x77dd0000	0x9b000	C:\WINDOWS\system32\advapi32.dll	Microsoft Corpo...	5.1.2600.5512 ...	1/1/1970 1:00:...
rpcrt4.dll	0x77e70000	0x92000	C:\WINDOWS\system32\rpcrt4.dll	Microsoft Corpo...	5.1.2600.5512 ...	1/1/1970 1:00:...
secur32.dll	0x77fe0000	0x11000	C:\WINDOWS\system32\secur32.dll	Microsoft Corpo...	5.1.2600.5512 ...	1/1/1970 1:00:...
kernel32.dll	0x7c800000	0xf6000	C:\WINDOWS\system32\kernel32.dll	Microsoft Corpo...	5.1.2600.5512 ...	1/1/1970 1:00:...
ntdll.dll	0x7c900000	0xaf000	C:\WINDOWS\system32\ntdll.dll	Microsoft Corpo...	5.1.2600.5512 ...	1/1/1970 1:00:...

Anche per quanto riguarda i processi, non sembrano essere state eseguite operazioni particolarmente dannose da parte di questo malware.

## Identificazione modifiche del registro con Regshot

**Regshot** è un tool che permette di paragonare due istantanee delle chiavi di registro salvate in due momenti separati tra di loro.

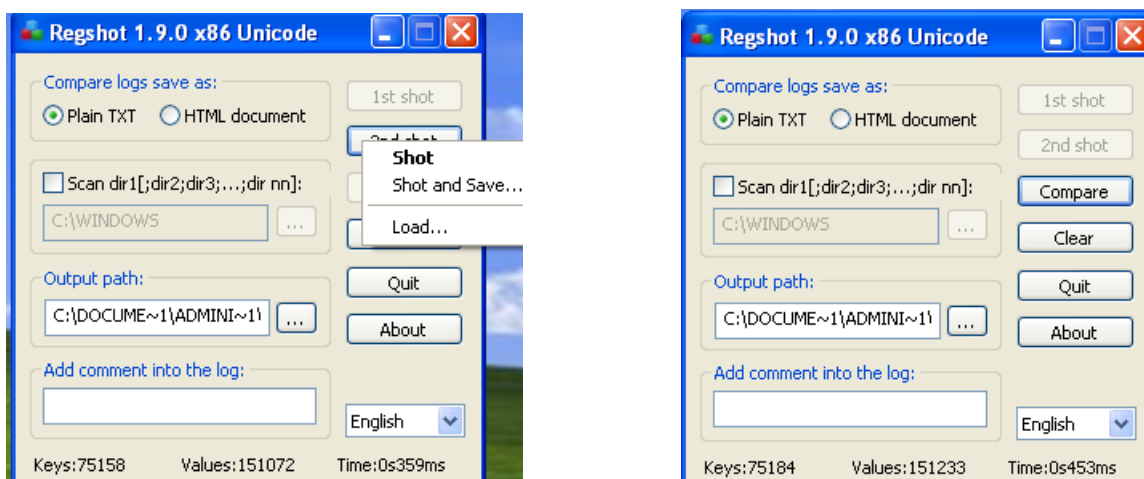
Avviamo quindi Regshot e clicchiamo sul tasto **1st shot** per salvare un'istantanea dello stato delle chiavi di registro prima dell'esecuzione del malware :



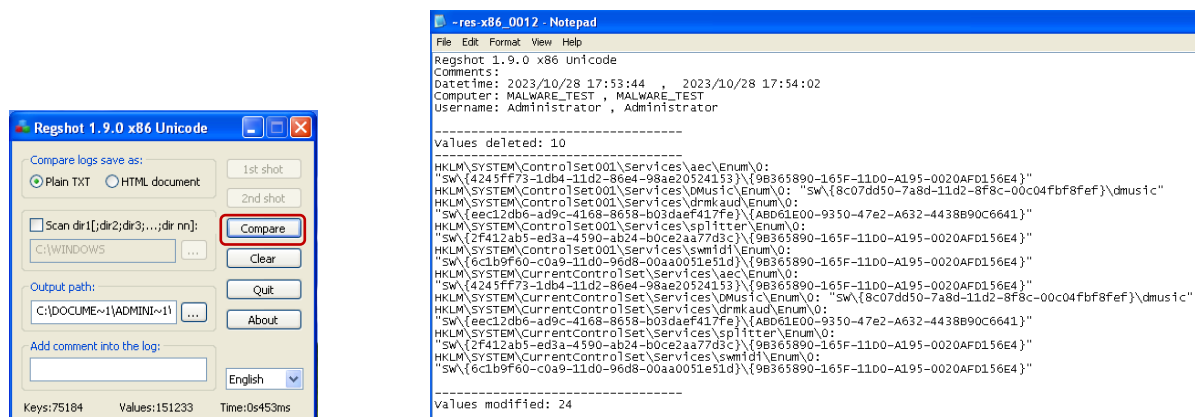
Avviamo poi il malware con doppio click sul file eseguibile:



Successivamente scattiamo una seconda istantanea cliccando su **2nd shot** per salvare lo stato delle chiavi di registro dopo l'esecuzione del malware:



Clicchiamo quindi su **Compare**: Regshot presenterà un file di testo dove sono riportate tutte le modifiche apportate alle chiavi di registro come ad esempio: chiavi modificate, chiavi eliminate, chiavi aggiunte.



Vediamo in dettaglio il file: non tutte le modifiche rilevate sono necessariamente da attribuire al malware. Vediamo evidenziati in giallo i riepiloghi: sono state rilevate 34 modifiche di cui 10 riguardano chiavi di registro eliminate e 14 sono relative a chiavi di registro modificate.

Regshot 1.9.0 x86 Unicode

Comments:

Datetime: 2023/10/28 17:53:44 , 2023/10/28 17:54:02

Computer: MALWARE\_TEST , MALWARE\_TEST

Username: Administrator , Administrator

Values deleted: 10

HKLM\SYSTEM\ControlSet001\Services\aec\Enum\0: "SW\{4245ff73-1db4-11d2-86e4-98ae20524153}\{9B365890-165F-11D0-A195-0020AFD156E4}"

HKLM\SYSTEM\ControlSet001\Services\DMusic\Enum\0: "SW\{8c07dd50-7a8d-11d2-8f8c-00c04fbf8fef}\dmusic"

HKLM\SYSTEM\ControlSet001\Services\drmkaud\Enum\0: "SW\{eec12db6-ad9c-4168-8658-b03daef417fe}\{ABD61E00-9350-47e2-A632-4438B90C6641}"

HKLM\SYSTEM\ControlSet001\Services\splitter\Enum\0: "SW\{2f412ab5-ed3a-4590-ab24-b0ce2aa77d3c}\{9B365890-165F-11D0-A195-0020AFD156E4}"

HKLM\SYSTEM\ControlSet001\Services\swmidi\Enum\0: "SW\{6c1b9f60-c0a9-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"

HKLM\SYSTEM\CurrentControlSet\Services\aec\Enum\0: "SW\{4245ff73-1db4-11d2-86e4-98ae20524153}\{9B365890-165F-11D0-A195-0020AFD156E4}"

HKLM\SYSTEM\CurrentControlSet\Services\DMusic\Enum\0: "SW\{8c07dd50-7a8d-11d2-8f8c-00c04fbf8fef}\dmusic"

HKLM\SYSTEM\CurrentControlSet\Services\drmkaud\Enum\0: "SW\{eec12db6-ad9c-4168-8658-b03daef417fe}\{ABD61E00-9350-47e2-A632-4438B90C6641}"

HKLM\SYSTEM\CurrentControlSet\Services\splitter\Enum\0: "SW\{2f412ab5-ed3a-4590-ab24-b0ce2aa77d3c}\{9B365890-165F-11D0-A195-0020AFD156E4}"

HKLM\SYSTEM\CurrentControlSet\Services\swmidi\Enum\0: "SW\{6c1b9f60-c0a9-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"

-----  
Values modified: 24  
-----

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: BE 37 E8 9F A9 50 07 FE 1D C8 CB 71 D4 4A 6F 2A 78 99 F3 D0 65 25  
F0 0B D6 A5 5A 77 12 D1 DB 64 32 BB E0 5A DD EB BA 8C FC A9 03 D3 20 1C 93 CE 08 19 8E 48 75 FB 7B C2 E6 23 2D 97  
E8 27 DB 3E 03 6D A5 6D 44 DB 0D F8 51 A6 F6 7C 09 FD 8F 34

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 76 AE CD D8 8A 73 D6 87 42 57 E1 37 29 AF B8 8C 29 09 6E C7 6E BF  
E5 34 2C 95 94 BC D0 43 D9 EB 60 FD 1E 0D 3C 9F 1C 59 95 08 40 5C 2B 9C 4F 37 32 01 E5 76 91 D5 6C 1F 92 58 AB B6  
96 59 42 42 F6 D0 F4 D7 40 91 DE 37 A8 4D C8 19 17 28 19 42

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1993962763-1606980848-725345543-  
500\RefCount: 0x00000001

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1993962763-1606980848-725345543-  
500\RefCount: 0x00000002

HKLM\SYSTEM\ControlSet001\Services\aec\Enum\Count: 0x00000001

HKLM\SYSTEM\ControlSet001\Services\aec\Enum\Count: 0x00000000

HKLM\SYSTEM\ControlSet001\Services\aec\Enum\NextInstance: 0x00000001

HKLM\SYSTEM\ControlSet001\Services\aec\Enum\NextInstance: 0x00000000

HKLM\SYSTEM\ControlSet001\Services\DMusic\Enum\Count: 0x00000001

HKLM\SYSTEM\ControlSet001\Services\DMusic\Enum\Count: 0x00000000

HKLM\SYSTEM\ControlSet001\Services\DMusic\Enum\NextInstance: 0x00000001

HKLM\SYSTEM\ControlSet001\Services\DMusic\Enum\NextInstance: 0x00000000

HKLM\SYSTEM\ControlSet001\Services\drmkaud\Enum\Count: 0x00000001

HKLM\SYSTEM\ControlSet001\Services\drmkaud\Enum\Count: 0x00000000

HKLM\SYSTEM\ControlSet001\Services\drmkaud\Enum\NextInstance: 0x00000001

HKLM\SYSTEM\ControlSet001\Services\drmkaud\Enum\NextInstance: 0x00000000

HKLM\SYSTEM\ControlSet001\Services\splitter\Enum\Count: 0x00000001

HKLM\SYSTEM\ControlSet001\Services\splitter\Enum\Count: 0x00000000

HKLM\SYSTEM\ControlSet001\Services\splitter\Enum\NextInstance: 0x00000001

HKLM\SYSTEM\ControlSet001\Services\splitter\Enum\NextInstance: 0x00000000

HKLM\SYSTEM\ControlSet001\Services\swmidi\Enum\Count: 0x00000001

HKLM\SYSTEM\ControlSet001\Services\swmidi\Enum\Count: 0x00000000

HKLM\SYSTEM\ControlSet001\Services\swmidi\Enum\NextInstance: 0x00000001

HKLM\SYSTEM\ControlSet001\Services\swmidi\Enum\NextInstance: 0x00000000

HKLM\SYSTEM\CurrentControlSet\Services\aec\Enum\Count: 0x00000001

HKLM\SYSTEM\CurrentControlSet\Services\aec\Enum\Count: 0x00000000

HKLM\SYSTEM\CurrentControlSet\Services\aec\Enum\NextInstance: 0x00000001

HKLM\SYSTEM\CurrentControlSet\Services\aec\Enum\NextInstance: 0x00000000

HKLM\SYSTEM\CurrentControlSet\Services\DMusic\Enum\Count: 0x00000001

HKLM\SYSTEM\CurrentControlSet\Services\DMusic\Enum\Count: 0x00000000

HKLM\SYSTEM\CurrentControlSet\Services\DMusic\Enum\NextInstance: 0x00000001

HKLM\SYSTEM\CurrentControlSet\Services\DMusic\Enum\NextInstance: 0x00000000

HKLM\SYSTEM\CurrentControlSet\Services\drmkaud\Enum\Count: 0x00000001

HKLM\SYSTEM\CurrentControlSet\Services\drmkaud\Enum\Count: 0x00000000

HKLM\SYSTEM\CurrentControlSet\Services\drmkaud\Enum\NextInstance: 0x00000001

HKLM\SYSTEM\CurrentControlSet\Services\drmkaud\Enum\NextInstance: 0x00000000

HKLM\SYSTEM\CurrentControlSet\Services\splitter\Enum\Count: 0x00000001



```
HKLM\SYSTEM\CurrentControlSet\Services\splitter\Enum\Count: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\splitter\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\splitter\Enum\NextInstance: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\swmidi\Enum\Count: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\swmidi\Enum\Count: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\swmidi\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\swmidi\Enum\NextInstance: 0x00000000

HKU\S-1-5-21-1993962763-1606980848-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU: 10 00 00 00 EA 01 00 00 A0 08 CB AC C7 09 DA 01

HKU\S-1-5-21-1993962763-1606980848-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU: 10 00 00 00 EB 01 00 00 C0 4C D2 B9 C7 09 DA 01

HKU\S-1-5-21-1993962763-1606980848-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbphzragf naq
Frggvatf\Nqzvavfgengbe\Qrfxgbc\Rfrepvmvb_Cengvpb_H3_J2_Y2\Znyjner_H3_J2_Y2.rkr: 10 00 00 00 13 00 00 00 60 AB BF
78 C7 09 DA 01

HKU\S-1-5-21-1993962763-1606980848-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-
006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbphzragf naq
Frggvatf\Nqzvavfgengbe\Qrfxgbc\Rfrepvmvb_Cengvpb_H3_J2_Y2\Znyjner_H3_J2_Y2.rkr: 10 00 00 00 14 00 00 00 C0 4C D2
B9 C7 09 DA 01
```

-----

Total changes: 34

-----