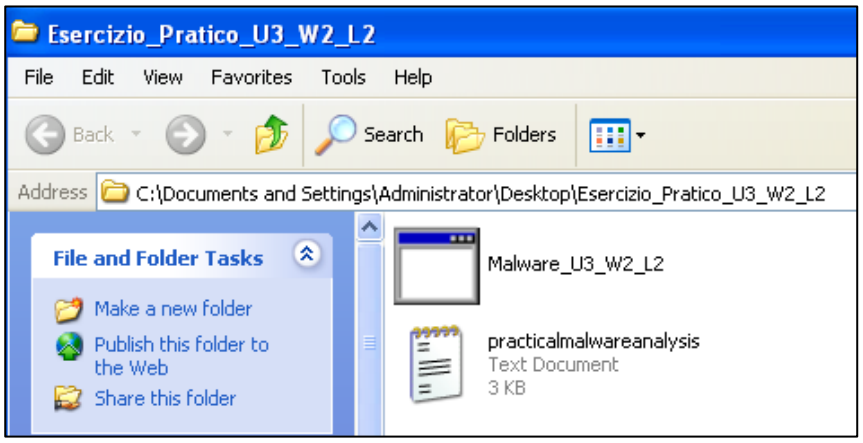
Analisi dinamica basica

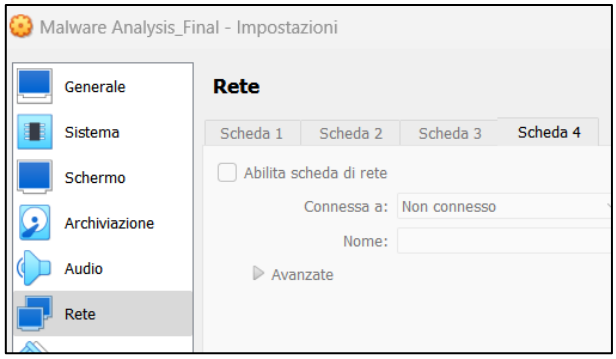
Sommario

Analisi dinamica sul malware `Malware_U3_W2_L2` su macchina virtuale Windows XP.

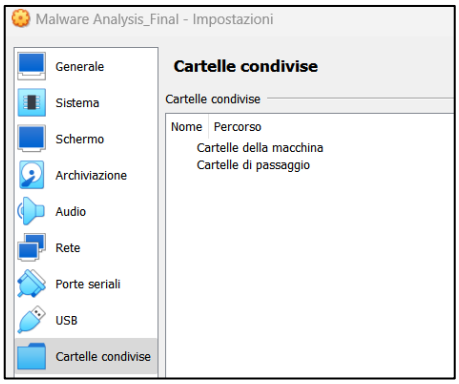


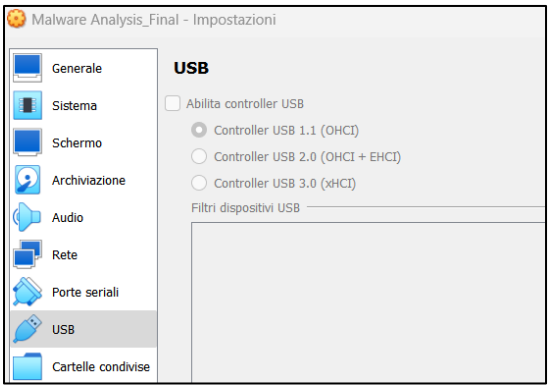
Configurazione ambiente di test

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



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

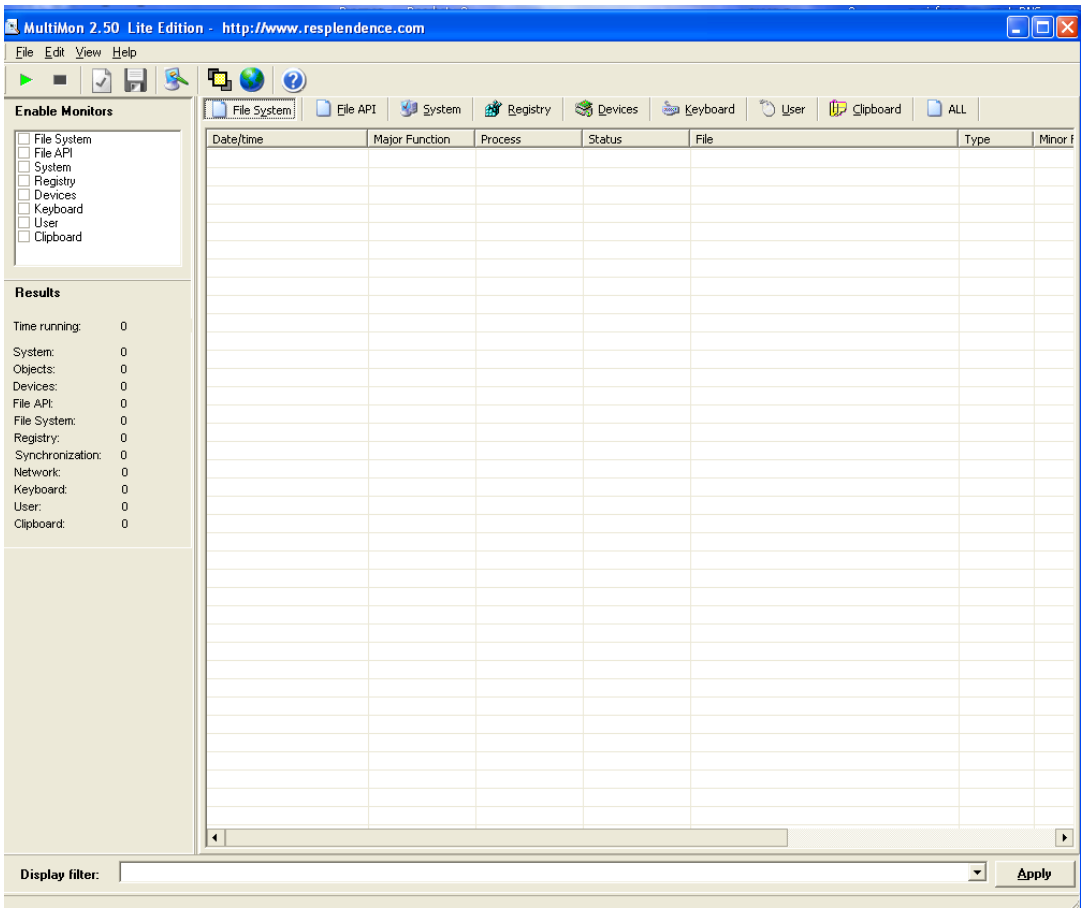




Analisi con MultiMon

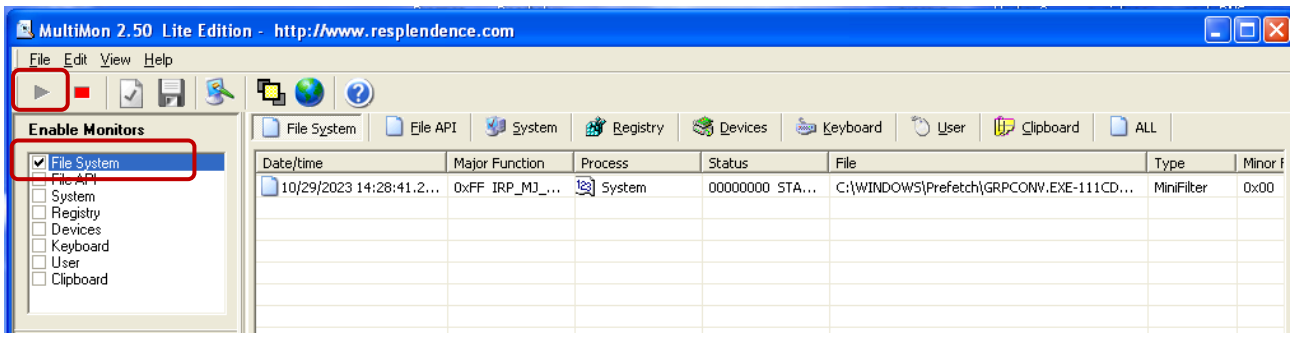
MultiMon è uno strumento avanzato per Windows che monitora una vasta gamma di attività in tempo reale. MultiMon visualizza in tempo reale la creazione di processi e thread, il caricamento di immagini binarie, le attività nel file system e nel registro. Supporta anche il monitoraggio della clipboard, della tastiera e delle attività delle applicazioni.

Avviamo MultiMon:

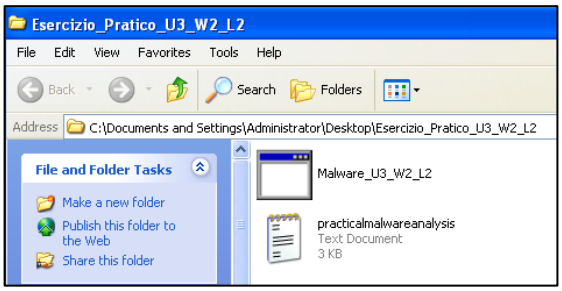


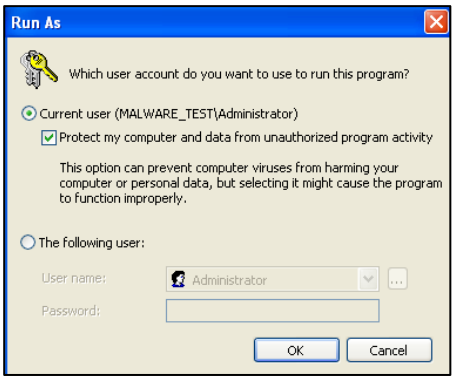
Analisi eventi nel file system

Nel pannello a sinistra selezioniamo “File System” e poi clicchiamo sul tasto “Play” per iniziare la cattura.

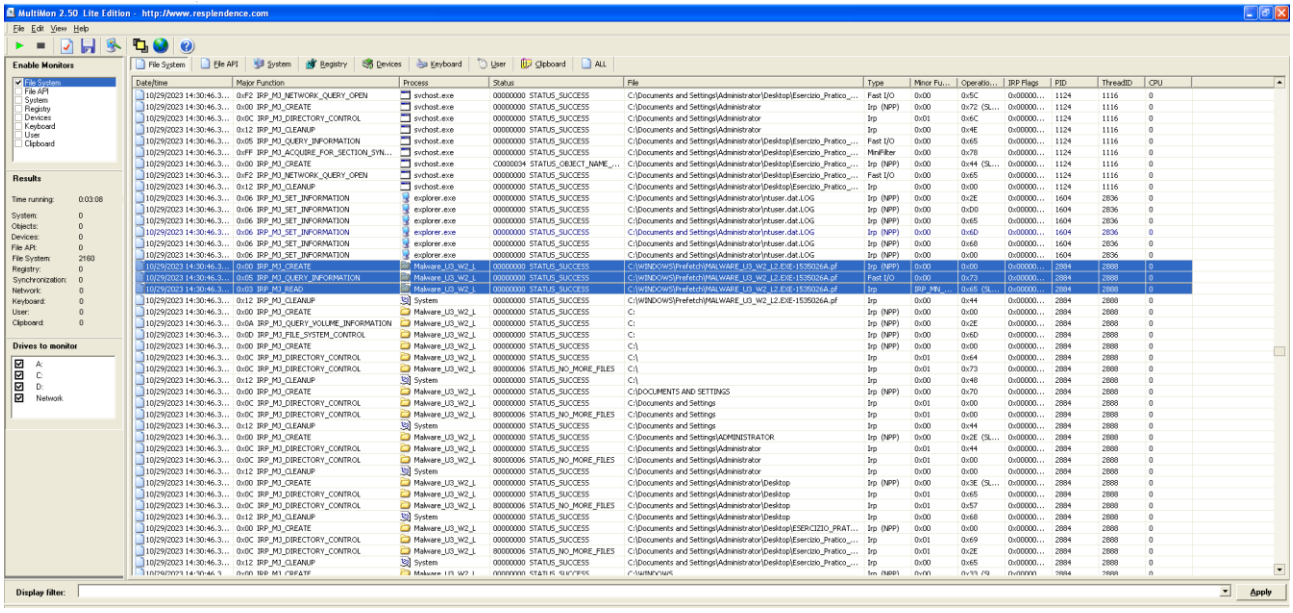


Eseguiamo adesso il malware `Malware_U3_W2_L2.exe` come amministratore:





La versione di prova che stiamo utilizzando non permette di applicare filtri sui risultati. Scorriamo i risultati fino a che non troviamo gli eventi del processo `Malware_U3_W2_L2`



Possiamo notare nella colonna **Major Function** una serie di azioni ripetute più volte su file diversi.

Si tratta di **codici di richiesta di pacchetto I/O (IRP, I/O Request Packet)** all'interno del sistema operativo Windows. Questi codici sono utilizzati dai driver di dispositivo per comunicare con il sistema operativo e gestire le richieste di I/O.

Prima di analizzare il comportamento del malware, facciamo una breve descrizione degli eventi principali:

- **IRP_MJ_CREATE** questo IRP viene inviato quando un'applicazione cerca di aprire un file o una directory. Esso contiene informazioni sul tipo di accesso richiesto (lettura, scrittura, esecuzione, ecc.) e su altri flag e opzioni che influenzano l'apertura;

- **IRP_MJ_READ** questo IRP rappresenta una richiesta di lettura da un file o dispositivo. Il driver di dispositivo legge i dati richiesti e li restituisce al chiamante;

- **IRP_MJ_QUERY_INFORMATION** questo IRP viene utilizzato per recuperare informazioni su un particolare file o directory. Può trattarsi di informazioni come dimensioni del file, attributi, tempi di creazione e modifica, ecc.;

- **IRP_MJ_QUERY_VOLUME_INFORMATION** questo IRP viene utilizzato per interrogare informazioni specifiche sul volume, come la sua capacità, l'ammontare dello spazio libero, il tipo di file system (ad es. NTFS o FAT32) e altre informazioni relative al volume piuttosto che a un singolo file;

- **IRP_MJ_FILE_SYSTEM_CONTROL** questo IRP gestisce varie operazioni di controllo sui file system, come il montaggio o lo smontaggio di un volume o la gestione di punti di analisi (reparse points);

- **IRP_MJ_DIRECTORY_CONTROL** questo IRP gestisce le operazioni sulle directory, come la lettura delle voci di directory o la notifica dei cambiamenti nelle voci di directory;

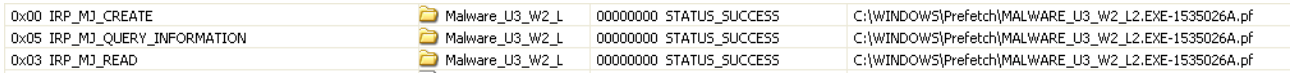
- **IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION** questo IRP viene utilizzato per acquisire una sincronizzazione in vista di operazioni che richiedono un accesso esclusivo o sincronizzato a una sezione di un file. Le sezioni sono essenzialmente viste mappate di un file e questo particolare IRP garantisce che le operazioni che influenzano l'intera sezione (o potenzialmente l'intero file) siano sincronizzate correttamente per evitare conflitti o corruzioni;

- **IRP_MJ_NETWORK_QUERY_OPEN** questo IRP viene utilizzato per interrogare se un file può essere aperto attraverso una rete. Esso fornisce una verifica senza realmente aprire il file, permettendo a un'applicazione o a un driver di sapere se l'operazione di apertura avrebbe successo o no senza effettivamente effettuarla;

- **IRP_MJ_CLEANUP** Questo IRP viene inviato quando un'applicazione o un altro utente del file chiude l'ultimo handle per un file o una directory ma prima che l'oggetto file sia effettivamente deallocato. In pratica, questa richiesta fornisce ai driver l'opportunità di eseguire qualsiasi pulizia necessaria (ad esempio, completare tutte le operazioni pendenti o liberare risorse allocate) in risposta alla chiusura di un file, ma prima che il file stesso venga rimosso dal sistema. È un passaggio intermedio tra la chiusura di un file e la sua effettiva deallocazione.

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

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



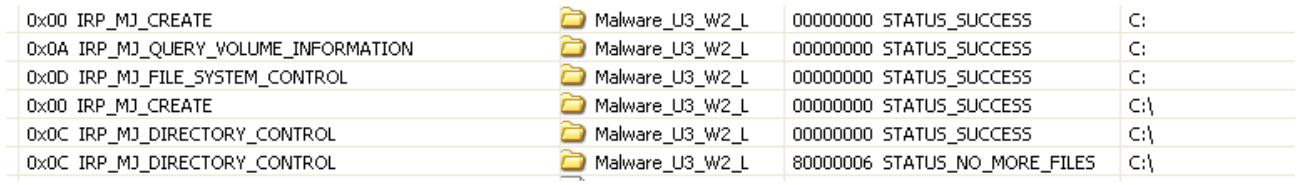
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
0x05 IRP_MJ_QUERY_INFORMATION	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf
0x03 IRP_MJ_READ	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\Prefetch\MALWARE_U3_W2_L2.EXE-1535026A.pf

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 (`IRP_MJ_CREATE`) in modo da ottimizzare il suo avvio, ha richiesto le informazioni standard del file .pf appena creato (`IRP_MJ_QUERY_INFORMATION`), e quindi lo ha letto (`IRP_MJ_READ`).

- **Lettura, rischiesta informazioni e lettura delle directory del disco C:**

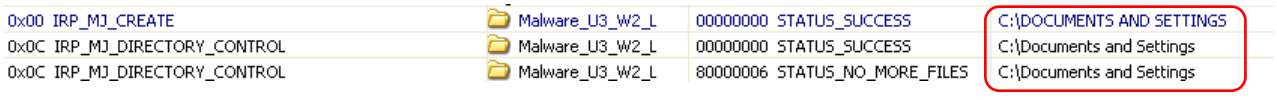
Vediamo successivamente diverse azioni sul disco `C`:



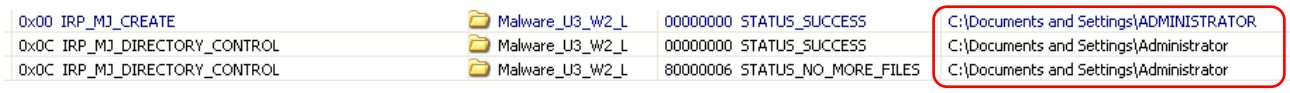
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:
0x0A IRP_MJ_QUERY_VOLUME_INFORMATION	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:
0x0D IRP_MJ_FILE_SYSTEM_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	80000006 STATUS_NO_MORE_FILES	C:\

Il malware ha avuto accesso al disco `C:` (`IRP_MJ_CREATE`), ne ha richiesto informazioni specifiche (`IRP_MJ_QUERY_VOLUME_INFORMATION`), e quindi ne ha catalogato il contenuto (`IRP_MJ_DIRECTORY_CONTROL`)

Queste operazioni sono state eseguite anche su altre cartelle di sistema, di cui si riportano di seguito alcuni esempi:



0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\DOCUMENTS AND SETTINGS
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\Documents and Settings
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	80000006 STATUS_NO_MORE_FILES	C:\Documents and Settings



0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\Documents and Settings\ADMINISTRATOR
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\Documents and Settings\Administrator
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	80000006 STATUS_NO_MORE_FILES	C:\Documents and Settings\Administrator

0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	80000006 STATUS_NO_MORE_FILES	C:\WINDOWS\system32

Notiamo che lo status finale restituito è sempre `STATUS_NO_MORE_FILES`, che sta ad indicare che la lettura è stata completata.

- **Lettura, acquisizione di sincronizzazione di file `.dll`, `.nls`, `.sdb` e `svchost.exe` con interrogazione sulla possibilità di apertura attraverso una rete e chiusura dell'handle**

Vediamo che il malware ha letto (`IRP_MJ_CREATE`) e acquisito la sincronizzazione (`IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION`) di una serie di file di sistema. Oltre a questo, su questi file ill malware ha richiesto se i file possono essere aperti attraverso una rete (`IRP_MJ_NETWORK_QUERY_OPEN`) e quindi ha richiesto la chiusura dell'handle. L'handle è un identificatoree univoco che serve ad accedere a una risorsa o a un oggetto senza dover fare riferimento ai dettagli interni o alla struttura della risorsa stessa.

0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0xFF IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0xF2 IRP_MJ_NETWORK_QUERY_OPEN	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\apphelp.dll
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\apphelp.dll
0xFF IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\apphelp.dll
0x12 IRP_MJ_CLEANUP	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\apphelp.dll
0xF2 IRP_MJ_NETWORK_QUERY_OPEN	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\apphelp.dll
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\apphelp.dll
0xFF IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\apphelp.dll
0x12 IRP_MJ_CLEANUP	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\apphelp.dll
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\AppPatch\sysmain.sdb
0x05 IRP_MJ_QUERY_INFORMATION	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\AppPatch\sysmain.sdb
0xFF IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\AppPatch\sysmain.sdb
0x05 IRP_MJ_QUERY_INFORMATION	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\AppPatch\sysmain.sdb
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	C0000034 STATUS_OBJECT_NAME_...	C:\WINDOWS\AppPatch\systest.sdb
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0x12 IRP_MJ_CLEANUP	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0xF2 IRP_MJ_NETWORK_QUERY_OPEN	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\
0x12 IRP_MJ_CLEANUP	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS
0x12 IRP_MJ_CLEANUP	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0x0C IRP_MJ_DIRECTORY_CONTROL	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0x12 IRP_MJ_CLEANUP	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32
0xF2 IRP_MJ_NETWORK_QUERY_OPEN	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0xF2 IRP_MJ_NETWORK_QUERY_OPEN	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0xFF IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0x12 IRP_MJ_CLEANUP	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0xF2 IRP_MJ_NETWORK_QUERY_OPEN	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0xFF IRP_MJ_ACQUIRE_FOR_SECTION_SYNCHRONIZATION	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0x12 IRP_MJ_CLEANUP	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0xF2 IRP_MJ_NETWORK_QUERY_OPEN	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe
0x00 IRP_MJ_CREATE	Malware_U3_W2_L	00000000 STATUS_SUCCESS	C:\WINDOWS\system32\svchost.exe

Vediamo cosa sono le tipoloigie 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.

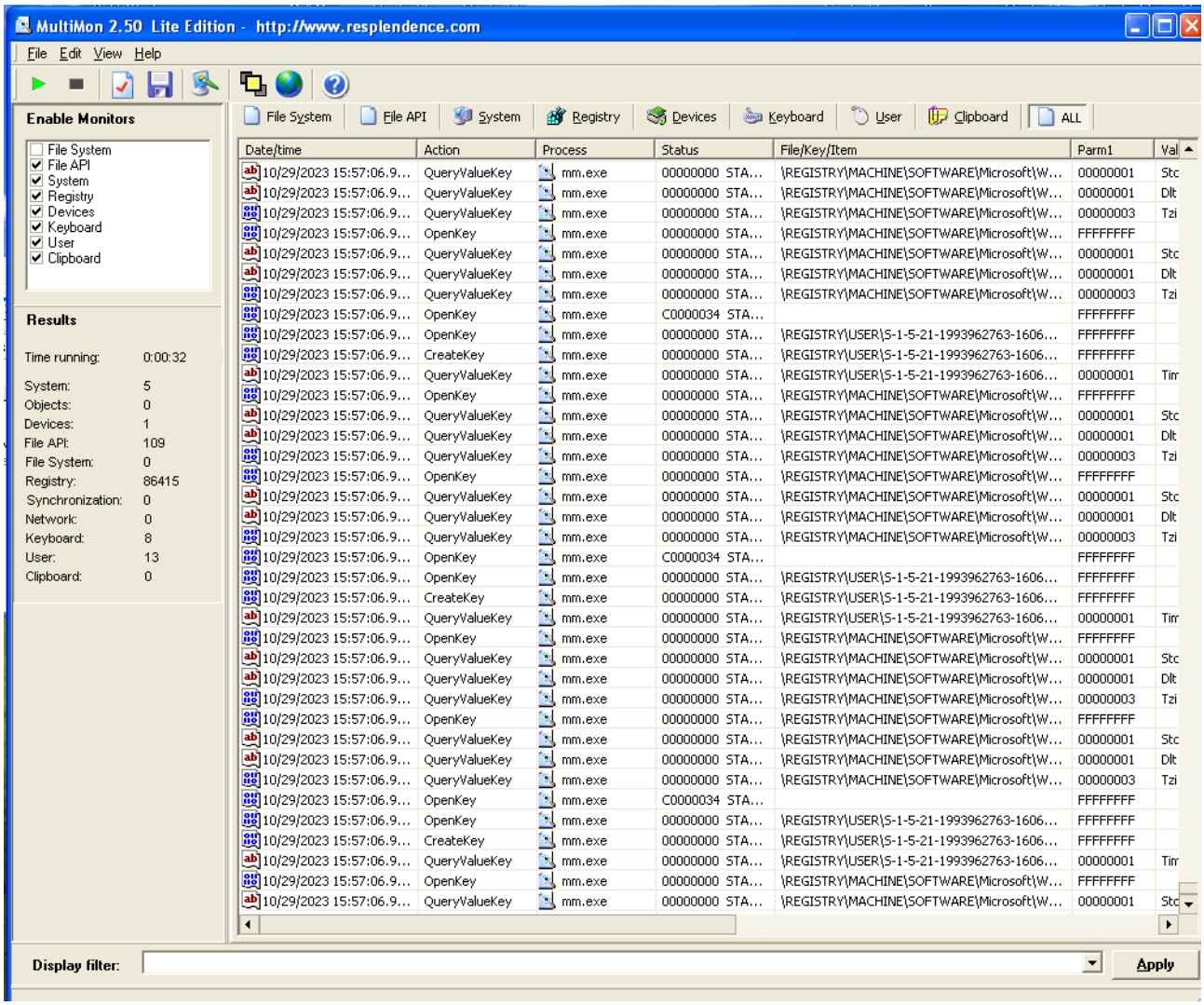
Vediamo anche cosa è il file **`svchost.exe`**

`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**.

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.

Identificazione di altre azioni del malware

Spuntiamo le caselle a sinistra relative agli altri tipi di monitoraggio, avviamo la cattura ed eseguiamo nuovamente il malware.



Categoria File API

I **file API (Application Programming Interfaces)** permettono alle applicazioni di interagire con i file a livello di sistema operativo.

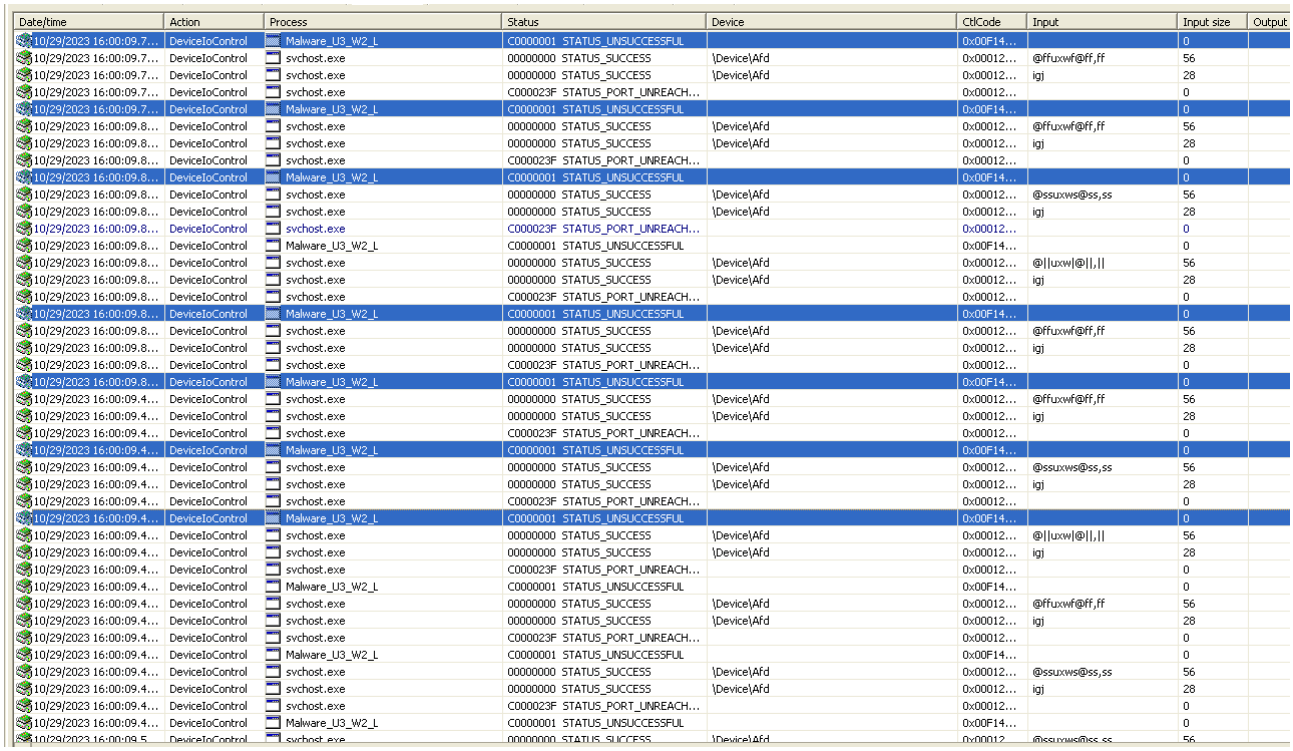
Per quanto riguarda questo tipo di file, vediamo che il malware ha esguito l' operazione `QueryInformationFile` per richiedere informazioni sui file temporanei del browser Internet Explorer.

Action	Process	Status	File
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
QueryInformationFile	Malware_U3_W2_L	00000000 STATUS_SUCCESS	\Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat

Categoria Devices

In questa categoria vediamo che il malware ha tentato senza successo (come indica lo stato `STATUS_UNSUCCESFUL`) di inviare comandi direttamente a driver di dispositivo.

`DeviceIoControl` è una funzione delle API Win32 di Windows utilizzata per inviare comandi direttamente a driver di dispositivo. Essa consente alle applicazioni di comunicare e inviare richieste specifiche a driver, che possono riguardare periferiche hardware (come dischi rigidi, dispositivi USB, schede grafiche) o driver virtuali/software.



Date/time	Action	Process	Status	Device	CtlCode	Input	Input size	Output
10/29/2023 16:00:09.7...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.7...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@ffuxwf@ff,ff	56	
10/29/2023 16:00:09.7...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	igj	28	
10/29/2023 16:00:09.7...	DeviceIoControl	svchost.exe	C000023F STATUS_PORT_UNREACH...		0x00012...		0	
10/29/2023 16:00:09.7...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@ffuxwf@ff,ff	56	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	igj	28	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	C000023F STATUS_PORT_UNREACH...		0x00012...		0	
10/29/2023 16:00:09.8...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@ssuxws@ss,ss	56	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	igj	28	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	C000023F STATUS_PORT_UNREACH...		0x00012...		0	
10/29/2023 16:00:09.8...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@||uxw|@||,||	56	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	igj	28	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	C000023F STATUS_PORT_UNREACH...		0x00012...		0	
10/29/2023 16:00:09.8...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@ffuxwf@ff,ff	56	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	igj	28	
10/29/2023 16:00:09.8...	DeviceIoControl	svchost.exe	C000023F STATUS_PORT_UNREACH...		0x00012...		0	
10/29/2023 16:00:09.8...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@ffuxwf@ff,ff	56	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	igj	28	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	C000023F STATUS_PORT_UNREACH...		0x00012...		0	
10/29/2023 16:00:09.4...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@ssuxws@ss,ss	56	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	igj	28	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	C000023F STATUS_PORT_UNREACH...		0x00012...		0	
10/29/2023 16:00:09.4...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@||uxw|@||,||	56	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	igj	28	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	C000023F STATUS_PORT_UNREACH...		0x00012...		0	
10/29/2023 16:00:09.4...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@ffuxwf@ff,ff	56	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	igj	28	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	C000023F STATUS_PORT_UNREACH...		0x00012...		0	
10/29/2023 16:00:09.4...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@ssuxws@ss,ss	56	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	igj	28	
10/29/2023 16:00:09.4...	DeviceIoControl	svchost.exe	C000023F STATUS_PORT_UNREACH...		0x00012...		0	
10/29/2023 16:00:09.4...	DeviceIoControl	Malware_U3_W2_L	C0000001 STATUS_UNSUCCESSFUL		0x00F14...		0	
10/29/2023 16:00:09.5...	DeviceIoControl	svchost.exe	00000000 STATUS_SUCCESS	\Device\Afd	0x00012...	@ssuxws@ss,ss	56	

Oltre a questo, non si rilevano altre azioni eseguite dal malware nelle altre categorie.

Profilazione del malware

Di seguito riportiamo una panoramica dei tipi di malware e delle operazioni principali che esguono e che li identificano.

1. **Virus**:
    - Si attacca a file eseguibili e si propaga quando l'eseguibile infetto viene lanciato.
    - Modifica il codice dei file o inserisce se stesso nel file.

2. **Worm**:
    - Si propaga autonomamente attraverso reti o sfruttando vulnerabilità software.
    - Può consumare larghezza di banda o causare overload sui sistemi.

3. **Trojan**:
    - Si maschera come software legittimo o viene incorporato in software legittimo.
    - Può fornire un backdoor al sistema, permettendo ad un attaccante di accedervi.

4. **Rootkit**:
    - Si nasconde profondamente nel sistema per evitare la rilevazione.
    - Interferisce con le API di sistema, driver o processi di avvio per rimanere nascosto.
    - Utilizza spesso funzioni come `DeviceIoControl` per interagire a basso livello con il sistema.

5. **Ransomware**:
    - Cripta file dell'utente e richiede un riscatto per la decrittazione.
    - Modifica l'accesso ai file e mostra spesso notifiche o schermate di blocco.

6. **Adware**:
    - Mostra pubblicità non desiderate all'utente.
    - Modifica le impostazioni del browser o installa estensioni/plugin.

7. **Spyware**:
    - Raccoglie informazioni sull'utente senza il suo consenso.
    - Monitora attività come la digitazione, la cronologia del browser e altre attività personali.

8. **Keylogger**:
    - Registra i tasti premuti dall'utente.
    - Può utilizzare API di sistema per monitorare l'input della tastiera.

9. **Botnet**:
    - Trasforma il sistema infetto in un "bot" controllato da un server centrale.
    - Esegue attacchi DDoS, invia spam o propaga ulteriormente il malware.

10. **Downloader/ Dropper**:
    - Scarica e installa altri malware o componenti aggiuntivi.
    - Comunica spesso con server remoti per scaricare payload.

Nel nostro caso, facciamo alcune considerazioni:

- il malware non sembra avere modificato file né aver effettuato connessioni di qualsiasi tipo. Questo lo esclude dalle categorie: Virus, Worm, Adware, Botnet, Downloader/Dropper;

- Inoltre, non era nascosto in nessun altro file, ma consisteva in un eseguibile a sé stante. Questo lo esclude dalla categoria Trojan;

- Non sono stati crittati file, quindi non è neanche un Ransomware.

A seguito di quanto detto, il nostro malware potrebbe rientrare nelle seguenti categorie: Rootkit, Spyware, Keylogger.

Non sono stati rilevati specifici tentativi di registrazione degli input utente (se pure ci sono stati tentativi falliti di invio comandi ai driver del dispositivo), il che farebbe escludere che possa trattarsi di un Keylogger.

Il fatto che un Rootkit utilizzi spesso funzioni come `DeviceIoControl` per interagire a basso livello con il sistema fa pensare che possa trattarsi proprio di un **Rootkit**. In alternativa, poiché le attività principali sono state di lettura e mappatura dei file di sistema, potrebbe trattarsi di uno **Spyware**.