



# Build Week III

## Analisi Malware

# Traccia BW III

giorno 1

**Con riferimento al file eseguibile  
Malware\_Build\_Week\_U3, rispondere ai seguenti  
quesiti utilizzando i tool e le tecniche apprese nelle  
lezioni teoriche:**

- Quanti **parametri** sono passati alla funzione Main()?
- Quante **variabili** sono dichiarate all'interno della funzione Main()?
- Quali **sezioni** sono presenti all'interno del file eseguibile? Descrivete brevemente almeno 2 di quelle identificate
- Quali **librerie** importa il **Malware**? Per ognuna delle librerie importate, fate delle ipotesi sulla base della sola analisi statica delle funzionalità che il Malware potrebbe implementare. Utilizzate le funzioni che sono richiamate all'interno delle librerie per supportare le vostre ipotesi.

**Con riferimento al Malware in analisi, spiegare:**

- Lo scopo della funzione chiamata alla locazione di memoria **00401021**;
- Come vengono passati i parametri alla funzione alla locazione **00401021**;
- Che oggetto rappresenta il parametro alla locazione **00401017**;
- Il significato delle istruzioni comprese tra gli indirizzi **00401027** e **00401029**;
- Con riferimento all'ultimo quesito, **tradurre** il codice **Assembly** nel corrispondente costrutto **C**;
- Valutate ora la chiamata alla locazione **00401047**, qual è il valore del parametro « **ValueName** »?
- Nel complesso delle due funzionalità appena viste, spiegate quale funzionalità sta implementando il Malware in questa sezione

## Quanti parametri sono passati alla funzione Main()?

# Parametri

Come è possibile vedere dallo screen, i parametri passati alla funzione **sono 3**:

**Argc** = **dword ptr 8**

**argv** = **dword ptr 0Ch**

**envp** = **dword ptr 10h**

```
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h
```

# Variabili

Le variabili dichiarate all'interno della funzione Main **sono 5**:

**hModule** = **dword ptr -11Ch**

**Data** = **byte ptr -118h**

**var\_117** = **byte ptr -117h**

**var\_8** = **dword ptr -8**

**var\_4** = **dword ptr -4**

```
hModule= dword ptr -11Ch
Data= byte ptr -118h
var_117= byte ptr -117h
var_8= dword ptr -8
var_4= dword ptr -4
```

Abbiamo capito quali fossero **le Variabili** e quali **i Parametri** grazie all'identificazione del segno (se positivo o negativo), ed esso è determinato dalla sua rappresentazione binaria. Il concetto di numero con segno o senza segno si riferisce a come vengono interpretati i bit che compongono una variabile.

Quali sezioni sono presenti all'interno del file eseguibile?

# Sezioni

Le sezioni presenti all'interno del file eseguibile sono: **.text, .rdata, .data, .rsrc**

Malware_Build_Week_U3.exe										
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics	
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000001FC	
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword	
.text	00005646	00001000	00006000	00001000	00000000	00000000	0000	0000	60000020	
.rdata	000009AE	00007000	00001000	00007000	00000000	00000000	0000	0000	40000040	
.data	00003EA8	00008000	00003000	00008000	00000000	00000000	0000	0000	C0000040	
.rsrc	00001A70	0000C000	00002000	0000B000	00000000	00000000	0000	0000	40000040	

Le sezioni nelle librerie del linguaggio Assembly sono blocchi di codice o dati che vengono organizzati in diverse parti di un file eseguibile. Ogni sezione ha uno scopo specifico e viene trattata non appena il programma viene eseguito

# Sezione .text

.text	00005646	00001000	00006000	00001000	00000000	00000000	0000	0000	60000020	
-------	----------	----------	----------	----------	----------	----------	------	------	----------	--

La sezione **.text** di un file eseguibile PE su Windows **contiene le istruzioni eseguibili del programma**, inclusi funzioni e loop.

Questa sezione è marcata come eseguibile e di sola lettura, il che significa che può essere eseguita e letta ma non modificata una volta caricata in memoria. Le caratteristiche includono gli attributi IMAGE\_SCN\_CNT\_CODE, che indica codice eseguibile, IMAGE\_SCN\_MEM\_EXECUTE, che permette l'esecuzione, e IMAGE\_SCN\_MEM\_READ, che permette la lettura. La dimensione varia a seconda del programma e, quando caricato, il .text è mappato a un indirizzo virtuale specifico. Questa sezione è cruciale per la sicurezza poiché protegge il codice da modifiche malware e è spesso analizzata per comprendere il comportamento del software dannoso.

# Sezione .rdata

.rdata	000009AE	00007000	00001000	00007000	00000000	00000000	0000	0000	40000040	
--------	----------	----------	----------	----------	----------	----------	------	------	----------	--

La sezione **.rdata** nei file PE **contiene dati di sola lettura come stringhe costanti e la tabella delle funzioni importate** (IAT), essenziale per la protezione dei dati in quanto non può essere modificata durante l'esecuzione.

Gli attributi tipici includono IMAGE\_SCN\_CNT\_INITIALIZED\_DATA, che indica dati inizializzati, e IMAGE\_SCN\_MEM\_READ, che permette la lettura della sezione. La dimensione varia in base alla quantità di dati costanti e la sezione è mappata in memoria in modo da essere protetta dal sistema operativo. La .rdata gioca un ruolo cruciale nella sicurezza, proteggendo le informazioni da manipolazioni e fornendo dettagli utili nell'analisi del malware. A differenza della sezione .text, che contiene codice eseguibile, .rdata include solo dati di lettura, non modificabili, offrendo uno sguardo approfondito sulle funzionalità e sulla struttura di un'applicazione, particolarmente utile nel reverse engineering e nella sicurezza informatica.

# Sezione .data



Nell'analisi dei malware, la **sezione .data** di un programma eseguibile è fondamentale per comprendere come il malware gestisce i dati. Contiene variabili globali accessibili da qualsiasi parte del codice, cruciali per mantenere stati e configurazioni del malware. Queste variabili sono persistenti per tutta la durata dell'esecuzione, facilitando la raccolta e la manipolazione di dati sensibili. L'analisi di questa sezione rivela come il malware opera, permettendo agli analisti di scoprire comportamenti specifici e potenziali punti di intervento per neutralizzarlo. Monitorando queste variabili durante l'analisi dinamica, è possibile osservare le reazioni del malware a diversi input o ambienti. Infine, alcune variabili possono agire come indicatori di compromissione, aiutando a identificare attività sospette o la presenza del malware su altri sistemi.

# Sezione .rsrc

La **sezione ".rsrc"** negli eseguibili Windows contiene risorse come icone e stringhe, separate dal codice eseguibile. Nel contesto dell'analisi dei malware, questa sezione può nascondere codice dannoso per eludere l'analisi e le firme antivirus, poiché le soluzioni di sicurezza tendono a concentrarsi più sul codice che sulle risorse. I malware possono anche modificare le risorse per ingannare l'utente o per inserire informazioni che possono aiutare nell'analisi forense. Strumenti come IDA Pro, Ghidra e Resource Hacker sono utili per esaminare queste risorse durante l'analisi del malware, rivelando tattiche e comportamenti del software dannoso.

## Quali librerie importa il Malware?

Per ognuna delle librerie importate, fate delle sola analisi statica delle funzionalità che il Malware potrebbe implementare. Utilizzate le funzioni che sono richiamate all'interno delle librerie per supportare le vostre ipotesi.

# Librerie

Malware_Build_Week_U3.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000769E	N/A	000074EC	000074F0	000074F4	000074F8	000074FC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000

Una libreria di assembly è una raccolta di codice scritto in linguaggio assembly che è stata organizzata e precompilata per essere riutilizzata in diversi programmi

# KERNEL32.dll

KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
--------------	----	----------	----------	----------	----------	----------

**KERNEL32.dll** è una **libreria** essenziale del sistema operativo Windows, ricca di funzioni vitali **per la gestione delle risorse di sistema**. Questa libreria offre strumenti per allocare e liberare memoria, accedere e gestire file e dispositivi, oltre a creare, terminare e sincronizzare processi e thread. Include anche funzioni per il controllo del tempo di sistema e per l'amministrazione di I/O asincroni e dispositivi. **KERNEL32.dll** è quindi un componente fondamentale per il funzionamento efficace e efficiente di Windows, influenzando aspetti cruciali della gestione delle risorse e della sincronizzazione di processi.

# ADVAPI32.dll

ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000
--------------	---	----------	----------	----------	----------	----------

**ADVAPI32.dll** è una libreria essenziale nel sistema operativo Windows, che si occupa di varie funzioni legate alla sicurezza e alla gestione del sistema. Questa libreria gestisce principalmente la sicurezza di Windows, inclusi gli account utente e il controllo degli accessi. Offre funzionalità per la gestione delle credenziali e dei privilegi utente, la manipolazione del Registro di Sistema, e il controllo dei servizi di sistema. Inoltre, **ADVAPI32.dll** supporta funzioni per la crittografia e la gestione delle chiavi di crittografia, rendendola fondamentale per la sicurezza e l'amministrazione del sistema.

## Locazione di memoria 00401021

Alla **locazione di memoria** `00401021`, il codice effettua una chiamata alla **funzione** `RegCreateKeyExA` dalla **libreria** `ADVAPI32.dll`. Questa funzione serve a creare o aprire una chiave di registro nel registro di sistema di Windows. In pratica, garantisce che una chiave specifica esista o la crea se non è già presente, restituendo un handle che può essere utilizzato per altre operazioni sul registro.

00401013	6A 00	PUSH 0	
00401015	6A 00	PUSH 0	
00401017	68 54804000	PUSH Malware_.00400054	ASCII "SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon"
0040101C	68 02000000	PUSH 00000002	
00401021	FF15 04704000	CALL DWORD PTR DS:[<&ADVAPI32.RegCreateKeyExA]	ADVAPI32.RegCreateKeyExA
00401027	85C0	TEST EAX,EAX	
00401029	v74 07	JE SHORT Malware_.00401032	

## Come vengono passati i parametri alla funzione

La **funzione RegCreateKeyExA** usa la convenzione **stdcall** per passare i parametri tramite lo **stack**. Per questa chiamata, i valori sono posizionati sullo **stack** in ordine inverso, partendo dall'ultimo parametro.

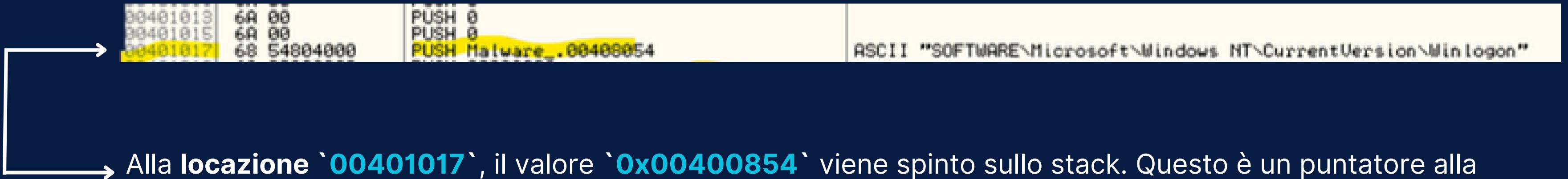
Si inizia **spingendo due valori 0** sullo stack, che indicano rispettivamente che non ci sono attributi di sicurezza specifici (NULL) per **lpSecurityAttributes** e che non si desidera ricevere informazioni sulla creazione o apertura della chiave per **lpdwDisposition**.

Successivamente, viene inserito **l'indirizzo 0x00400854**, che punta alla stringa **"SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"** per il parametro **lpSubKey**.

Poi, viene spinto il valore 2 che specifica che la chiave è **"non volatile"** con l'opzione **REG\_OPTION\_NON\_VOLATILE**. Infine, 0x30 viene spinto sullo stack per indicare le autorizzazioni di lettura e scrittura (KEY\_READ | KEY\_WRITE) per la chiave di registro attraverso **samDesired**.

Questi passaggi **configurano RegCreateKeyExA** per creare o aprire la chiave specificata con le autorizzazioni indicate.

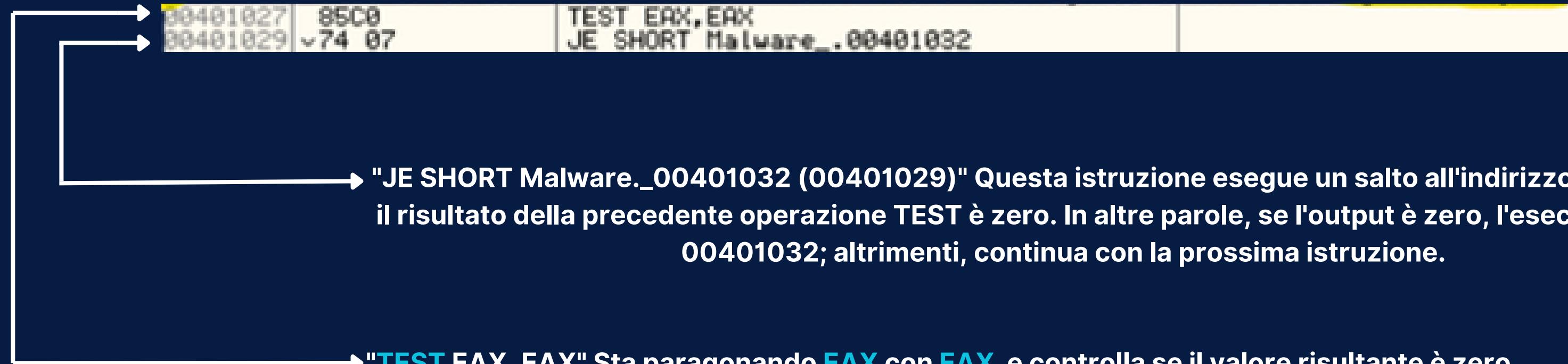
## Cosa Rappresenta l'Oggetto al Parametro alla Locazione `00401017`



```
00401013 6A 00      PUSH 0
00401015 6A 00      PUSH 0
00401017 68 54804000 PUSH Malware_.00400854
              ASCII "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
```

Alla **locazione `00401017`**, il valore **`0x00400854`** viene spinto sullo stack. Questo è un puntatore alla stringa ASCII **``SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon``**, che rappresenta il percorso della chiave di registro da creare o aprire. Questa chiave di registro è utilizzata da Windows per configurare varie impostazioni durante il processo di login, come automatizzare attività o gestire le sessioni degli utenti.

## Il significato delle istruzioni comprese tra gli indirizzi 00401027 e 00401029



Questo diagramma illustra la logica condizionale implementata nell'istruzione TEST EAX, EAX. Se EAX è zero (indicando che la funzione RegCreateKeyExA ha avuto successo), l'esecuzione del codice salterà a 00401032. Se EAX non è zero (indicando un fallimento), l'esecuzione continuerà senza saltare, eseguendo eventuali istruzioni successive.

Con riferimento all'ultimo quesito, tradurre il codice Assembly nel corrispondente costrutto C

00401027	8508	TEST EAX,EAX
00401029	v74 07	JE SHORT Malware...,00401032

COSTRUTTO

**C/C++**

```
if (eax == 0) {  
    goto loc_401032;  
} else {  
    goto lock_0040102B;  
}
```

Se **EAX** è uguale a “0” allora il costrutto passerà alla locazione “**loc\_401032**”, altrimenti andrà alla locazione “**loc\_0040102B**”

# Chiamata alla locazione 00401047

Alla **locazione di memoria 00401047**, viene effettuata una chiamata alla **funzione RegSetValueExA** dalla **libreria ADVAPI32.dll**. Questa funzione è utilizzata per impostare un valore in una chiave del registro di sistema di Windows.

## Valore del Parametro "ValueName"

Per determinare il valore del **parametro ValueName**, dobbiamo esaminare le istruzioni che precedono la chiamata alla **funzione RegSetValueExA** e identificare come vengono preparati i parametri sullo stack.

Le istruzioni pertinenti sono:

- **00401043: MOV EAX, DWORD PTR SS:[EBP-4]** Questa istruzione carica nel registro EAX il valore che si trova all'indirizzo [EBP-4]. Questo valore è presumibilmente l'handle di una chiave di registro ottenuto in una chiamata precedente a RegCreateKeyExA o una simile.
- **00401045: PUSH EAX** L'istruzione successiva spinge il contenuto di EAX sullo stack. Questo sarà il primo parametro per RegSetValueExA, che rappresenta l'handle della chiave di registro aperta.
- **0040103E: PUSH Malware\_.0040094C** Questa istruzione spinge sullo stack l'indirizzo 0x0040094C. Guardando il commento nella colonna di destra, notiamo che questo indirizzo punta alla stringa "ginaDLL".
- Quindi, il valore del parametro ValueName è la stringa "ginaDLL", che rappresenta il nome del valore da impostare all'interno della chiave di registro specificata.

**Nel complesso delle due funzionalità appena viste, spiegate quale funzionalità sta implementando il Malware in questa sezione**

il malware ha la funzionalità di terminazione processi

Utilizzando `TerminateProcess`, il malware può chiudere processi di sicurezza o antivirus che interferiscono con la sua esecuzione, incrementando la sua capacità di evitare la rilevazione e la rimozione.

recupero info sistema

L'impiego di funzioni come `GetCurrentProcess` e `GetVersion` suggerisce che il malware raccoglie dati sull'ambiente di esecuzione, adattando il proprio comportamento in base alle diverse versioni di Windows e alle configurazioni del sistema.

Interazione altri processi

L'uso di funzioni come `ReadProcessMemory` e `WriteProcessMemory` indica che il malware è in grado di interagire con la memoria di altri processi, permettendo così operazioni di iniezione di codice o estrazione di dati.

DLL di monitoraggio nel sistema

il malware sta cercando di inserire una propria DLL di monitoraggio nel sistema. In questo modo tenta di ottenere credenziali, eseguire un codice malevolo al momento del login, oppure alterare altri comportamenti di autenticazione di Windows.

probabilmente il malware è progettato per ottenere persistenza, espandersi e manipolare OS

Il malware sfrutta le funzioni `RegCreateKeyExA` e `RegSetValueExA` per creare e modificare le chiavi di registro, assicurando così l'avvio automatico del sistema. In questo modo, il malware riesce a mantenersi attivo anche dopo il riavvio del computer.

# Traccia

Riprendete l'analisi del codice , analizzando la routine tra le locazioni di memoria **00401080** e **00401128**:

- Qual è il valore del parametro «ResourceName » passato alla funzione FindResourceA ();
- Il susseguirsi delle chiamate di funzione che effettua il Malware in questa sezione di codice l'abbiamo visto durante le lezioni teoriche. **Che funzionalità sta implementando il Malware?**
- **E' possibile identificare questa funzionalità utilizzando l'analisi statica basica?(dal giorno 1 in pratica)**
- In caso di risposta affermativa , elencare le evidenze a supporto.

Entrambe le funzionalità principali del Malware , viste finora sono richiamate all'interno della funzione Main(). Disegnare un diagramma di flusso (inserite al'interno dei box solo le informazioni circa le funzionalità principali ) che comprende le 3 funzioni.

# Risoluzione Tools Utilizzati

Per completare l'esercizio richiesto nella traccia, abbiamo deciso di utilizzare i seguenti tools:

**OllyDBG:** è un debugger a livello di assembly per Windows, utilizzato per l'analisi dinamica di programmi eseguibili. È popolare tra i ricercatori di sicurezza informatica per esaminare e comprendere il comportamento di software, specialmente in contesti come l'analisi di malware e il reverse engineering.

**Procmon :** (Process Monitor) è uno strumento per Windows che monitora in tempo reale l'attività di sistema, come operazioni sui file, registro, processi e thread. Utilizzato principalmente per il troubleshooting e l'analisi di comportamento di applicazioni, è molto utile per identificare attività sospette o indesiderate di programmi e malware.

**IDA :** (Interactive Disassembler) è un potente disassembler e debugger interattivo usato per il reverse engineering di software. Converte il codice binario in assembly leggibile, permettendo agli analisti di esaminare e comprendere il funzionamento interno di un programma. È uno strumento essenziale per l'analisi di malware e la ricerca di vulnerabilità.

# Risoluzione

## Esame Dei Risultati

- Quale è il valore del parametro **ResourceName** passato alla funzione **FindResourceA()**?

Il valore del parametro **Resource Name** passato alla funzione **FindResourceA()** è contenuto all'interno della sezione nella figura. Come possiamo vedere il suo valore è **TGAD**.

- Che funzionalità è implementata dal Malware?

il secondo quesito richiede di identificare la funzionalità implementata dal Malware. Dall'analisi del codice, emerge che il malware sta cercando una risorsa denominata **TGAD** utilizzando le funzioni **FindResourceA()**, **LoadResource()**, **LockResource()** e **SizeofResource()**.

Il codice mostrato utilizza funzioni delle API di Windows per gestire risorse all'interno di un modulo. In particolare, cerca, carica, blocca e ottiene la dimensione di una risorsa specifica, potenzialmente chiamata "TGAD". Queste operazioni potrebbero indicare che il malware sta caricando e utilizzando dati malevoli o codice eseguibile.

# Risoluzione

## Esame Dei Risultati

004010B1	. 33C0	XOR EAX,EAX	
004010B3	.~E9 07010000	JMP Malware_.004011BF	
004010B8	> A1 30804000	MOU EAX,DWORD PTR DS:[408030]	
004010BD	. 50	PUSH EAX	
004010BE	. 8B0D 34804000	MOV ECX,DWORD PTR DS:[408034]	
004010C4	. 51	PUSH ECX	
004010C5	. 8B55 08	MOV EDX,DWORD PTR SS:[EBP+8]	
004010C8	. 52	PUSH EDX	
004010C9	. FF15 28704000	CALL DWORD PTR DS:[&KERNEL32.FindResourceA]	
004010CF	. 8945 EC	MOU DWORD PTR SS:[EBP-14],EAX	
004010D2	. 837D EC 00	CMP DWORD PTR SS:[EBP-14],0	
004010D6	.~75 07	JNZ SHORT Malware_.004010DF	
004010D8	. 33C0	XOR EAX,EAX	
004010DA	.~E9 E0000000	JMP Malware_.004011BF	
004010DF	> 8B45 EC	MOU EAX,DWORD PTR SS:[EBP-14]	
004010E2	. 50	PUSH EAX	
004010E3	. 8B4D 08	MOV ECX,DWORD PTR SS:[EBP+8]	
004010E6	. 51	PUSH ECX	
004010E7	. FF15 14704000	CALL DWORD PTR DS:[&KERNEL32.LoadResourceA]	
004010ED	. 8945 E8	MOU DWORD PTR SS:[EBP-18],EAX	
004010F0	. 837D E8 00	CMP DWORD PTR SS:[EBP-18],0	
004010F4	.~75 05	JNZ SHORT Malware_.004010FB	
004010F6	.~E9 AA000000	JMP Malware_.004011A5	
004010FB	> 8B55 E8	MOU EDX,DWORD PTR SS:[EBP-18]	
004010FE	. 52	PUSH EDX	
004010FF	. FF15 10704000	CALL DWORD PTR DS:[&KERNEL32.LockResource]	
00401105	. 8945 F8	MOU DWORD PTR SS:[EBP-8],EAX	
00401108	. 837D F8 00	CMP DWORD PTR SS:[EBP-8],0	
0040110C	.~75 05	JNZ SHORT Malware_.00401113	
0040110E	.~E9 92000000	JMP Malware_.004011A5	
00401113	> 8B45 EC	MOU EAX,DWORD PTR SS:[EBP-14]	
00401116	. 50	PUSH EAX	
00401117	. 8B4D 08	MOV ECX,DWORD PTR SS:[EBP+8]	
0040111A	. 51	PUSH ECX	
0040111B	. FF15 0C704000	CALL DWORD PTR DS:[&KERNEL32.SizeofResourceA]	
00401121	. 8945 F0	MOU DWORD PTR SS:[EBP-10],EAX	
00401124	. 837D F0 00	CMP DWORD PTR SS:[EBP-10],0	
00401128	.~77 02	JA SHORT Malware_.0040112C	
0040112A	.~EB 79	JMP SHORT Malware_.004011A5	
0040112C	> 6A 04	PUSH 4	
0040112E	. 68 00100000	PUSH 1000	
00401133	. 8B55 F0	MOU EDX,DWORD PTR SS:[EBP-10]	
00401136	. 52	PUSH EDX	
00401137	. 6A 00	PUSH 0	
00401139	. FF15 18704000	CALL DWORD PTR DS:[&KERNEL32.VirtualAlloc]	
0040113F	. 8945 F4	MOU DWORD PTR SS:[EBP-C],EAX	
00401142	. 837D F4 00	CMP DWORD PTR SS:[EBP-C],0	

ResourceType => "BINARY"  
Malware\_.00408038  
ResourceName => "TGAD"

hModule  
FindResourceA

hResource  
LoadResource

hResource  
LockResource

hResource  
SizeofResource

Protect = PAGE\_READWRITE  
AllocationType = MEM\_COMMIT  
Size  
Address = NULL  
VirtualAlloc

# Risoluzione

## Esame Dei Risultati

E' possibile l'identificazione della Funzionalità mediante analisi statica basica?

Il Malware esegue una sequenza operativa tipica dei dropper, utilizzando le chiamate **API di Windows**: **FindResourceA**, **LoadResource**, e **SizeOfResource**. La funzione **FindResourceA** localizza una risorsa incorporata nell'eseguibile, in questo caso identificata dal nome "**TGAD**". Questo indica che il malware cerca un componente specifico occultato, che potrebbe essere un secondo stadio di un attacco o un payload aggiuntivo. Successivamente, **LoadResource** carica il contenuto della risorsa in memoria, pratica comune dei dropper per eseguire o manipolare componenti dannosi. **SizeOfResource** restituisce la dimensione della risorsa, garantendo una corretta gestione della memoria durante l'estrazione e l'eventuale esecuzione del payload. Queste operazioni di ricerca, caricamento e dimensionamento di componenti nascosti sono utilizzate per eludere la rilevazione basata su firma, poiché il payload non appare come un file separato sul disco ma viene gestito interamente in memoria. L'identificazione di una risorsa con un nome come "**TGAD**" potrebbe implicare l'uso di tecniche di steganografia o compressione per mascherare la natura della risorsa. In sintesi, il malware implementa funzionalità di estrazione di risorse nascoste, allocazione di memoria e manipolazione di dati, e potenzialmente manipolazione di file, indicando un intento di distribuire componenti dannosi nascosti e garantire persistenza sul sistema compromesso.

# Risoluzione

## Esame Dei Risultati

004010B3	.vE9 07610000	JMP <a href="#">Malware_.0040116F</a>
004010B8	> A1 30804000	MOV EAX,DWORD PTR DS:[408030]
004010BD	. 50	PUSH EAX
004010BE	. 8B0D 34804000	MOV ECX,DWORD PTR DS:[408034]
004010C4	. 51	PUSH ECX
004010C5	. 8B55 08	MOV EDX,DWORD PTR SS:[EBP+8]
004010C8	. 52	PUSH EDX
004010C9	. FF15 28704000	CALL DWORD PTR DS:[<&KERNEL32.FindResou: <a href="#">FindResourceA</a> ]
004010CF	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX
004010D2	. 837D EC 00	CMP DWORD PTR SS:[EBP-14],0

ResourceType => "BINARY"  
Malware\_.00408038  
ResourceName => "TGAD"  
hModule  
[FindResourceA](#)

# Risoluzione

## Esame Dei Risultati

**Quali evidenze a ci sono a supporto dell'identificazione della funzionalità: Quando vengono richieste le evidenze a supporto includono le seguenti:**

**FindResourceA:** questa funzione cerca una risorsa specifica in un modulo (di solito un eseguibile o una libreria DLL). Le risorse possono essere elementi come icone, immagini, file di testo, ecc. Viene utilizzata per ottenere un handle (una sorta di puntatore) alla risorsa, che può poi essere utilizzato con altre funzioni per caricare ed utilizzare la risorsa.

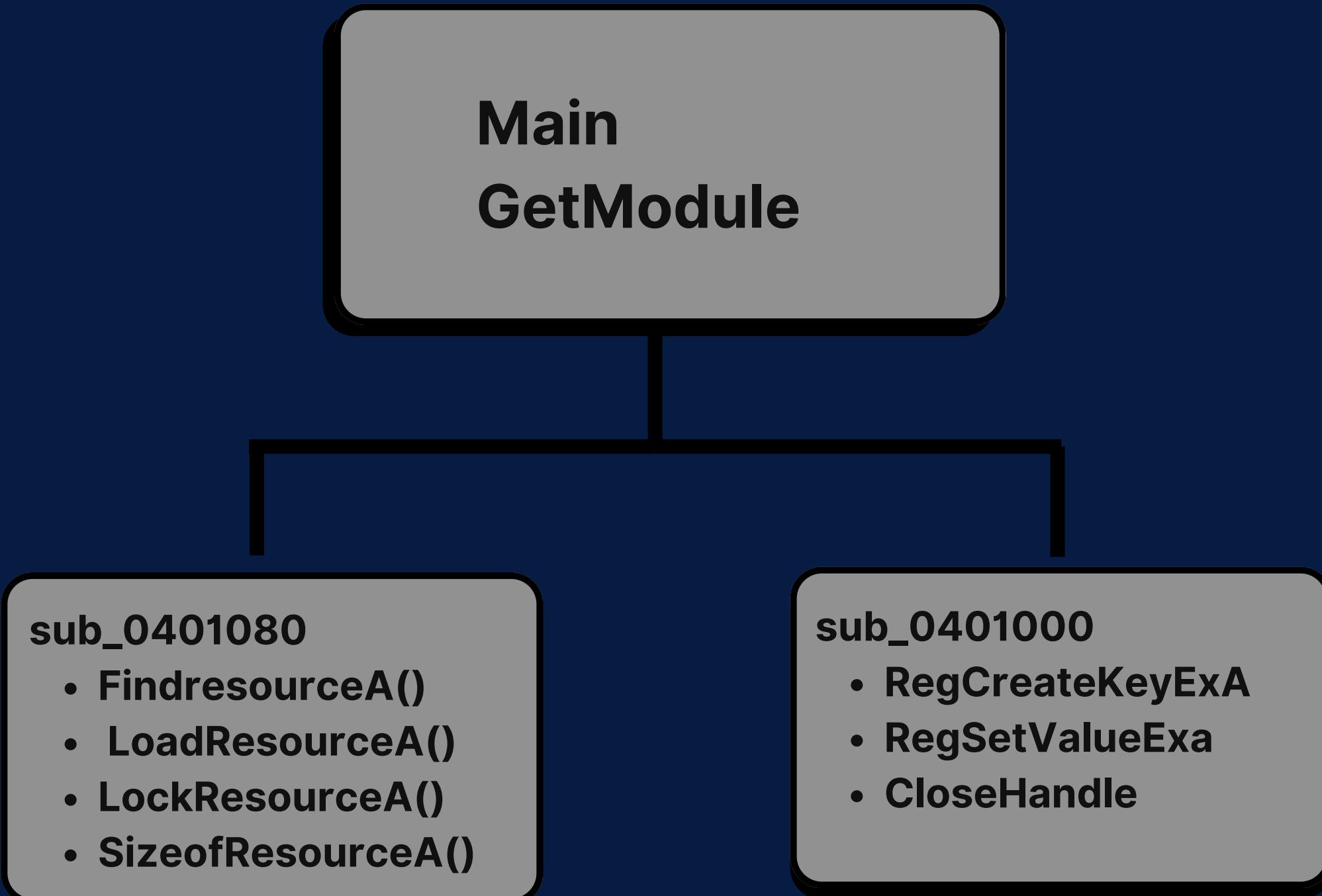
**LoadResource:** questa funzione carica una risorsa specificata da un handle (ottenuto, ad esempio, da FindResourceA) nella memoria. Consente di accedere alla risorsa effettiva in memoria, dopo che è stata trovata con FindResourceA.

**LockResource:** questa funzione blocca la risorsa caricata nella memoria, rendendola accessibile tramite un puntatore. Viene utilizzata per ottenere un puntatore ai dati della risorsa in memoria, in modo da poterli manipolare direttamente.

**SizeofResource:** questa funzione ottiene la dimensione, in byte, di una risorsa specificata. Utilizzata per determinare la quantità di memoria occupata da una risorsa, utile per gestire correttamente lo spazio necessario in memoria.

**VirtualAlloc:** questa funzione riserva e/o impegna una regione di memoria virtuale nel processo chiamante. Viene utilizzata per allocare memoria in modo controllato e gestire direttamente lo spazio di indirizzamento virtuale, importante per operazioni che richiedono alte prestazioni o controllo dettagliato della memoria.

# Diagramma di flusso



# Risoluzione

## Giorno 2

**Preparate l'ambiente ed i tool per l'esecuzione del Malware (suggerimento: avviate principalmente Esercizio Giorno 2 Process Monitor ed assicurate di eliminare ogni filtro cliccando sul tasto «reset» quando richiesto in fase di avvio). Eseguite il Malware , facendo doppio click sull'icona dell'eseguibile**

Procediamo alla preparazione dell'ambiente di lavoro aprendo il software come richiesto dalla traccia. (spesso abbreviato come ProcMon) è uno strumento avanzato per il monitoraggio del sistema operativo Windows, particolarmente utile nell'analisi dinamica dei malware, poiché consente agli analisti di osservare in tempo reale il comportamento dei programmi malevoli nel sistema. Process Monitor traccia tutte le operazioni sui file, le interazioni con il **Registro di sistema**, e le attività dei processi e dei thread, fornendo una visualizzazione dettagliata di tutte le azioni effettuate dal malware. Include anche **filtri avanzati** per isolare attività sospette, log dettagliati per analisi successive e visualizzazione delle stack trace per comprendere il flusso di esecuzione. Dopo aver configurato un ambiente isolato (sandbox), possiamo eseguire il malware in sicurezza e osservare la sua attività in tempo reale.

Possiamo anche utilizzare dei filtri per focalizzarci sulle operazioni rilevanti. Ad esempio, possiamo filtrare le attività di scrittura sui file e le modifiche al registro per individuare rapidamente le azioni dannose.

# Best Practise

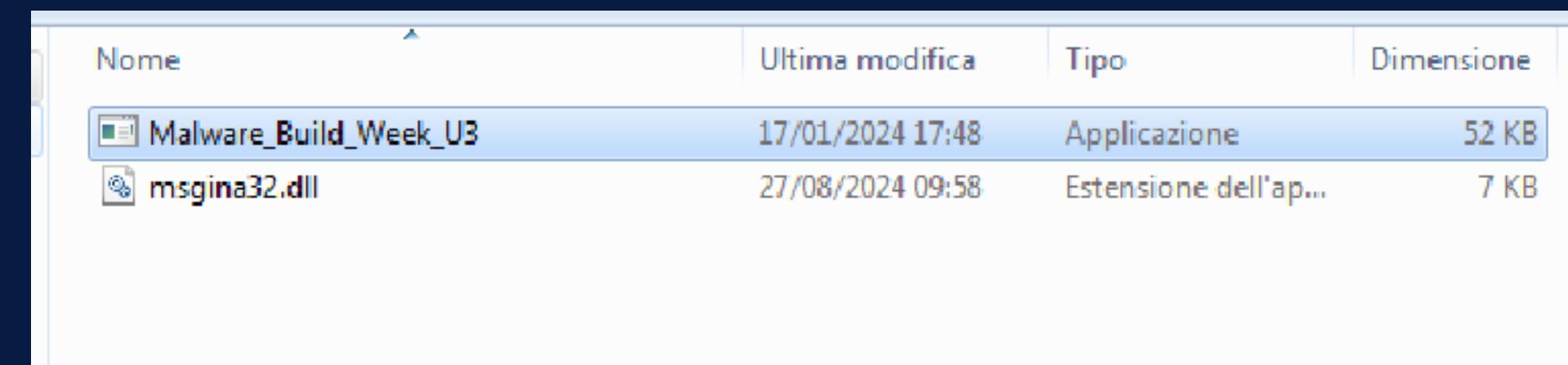
Prima di avviare il malware, settiamo in modo sicuro l'ambiente di lavoro; per farlo eseguiamo le seguenti operazioni:

- **Utilizzo Rete interna:** per evitare che il malware possa comunicare con l'esterno, caricando file malevoli o trasmettere informazioni sulla macchina colpita
- **Disabilitazione porte USB :** spesso un malware è in grado di rilevare dispositivi di archiviazione esterna ed utilizzarli come vettore per propagarsi su altri dispositivi
- **Disabilitazione cartelle condivise tra VM e PC Host :** spesso ce ne dimentichiamo, ma la presenza di queste cartelle permette al malware di agire anche al di fuori della macchina virtuale ed infettare la macchina Host.
- **Creazione di istantanee :** La creazione di istantanee ci permette non solo di capire quali parti del sistema operativo vengono compromesse(attraverso un confronto tra il prima e il dopo l'esecuzione del malware), ma anche di riportare la macchina ad uno stato precedente qualora vi fossero compromissioni importanti.

Possiamo, dunque, eseguire il malware e monitorare i processi ad esso associati tramite il tool Procmon.

# Apertura Malware

Una volta avviato il malware possiamo notare la creazione di un file **msgina32.dll**. La cosa insospettisce il team poichè il file **msgina.dll** è una libreria di sistema di Windows che è responsabile per la gestione del processo di autenticazione utente. In particolare, è associato alla Microsoft Graphical Identification and Authentication (GINA), che è un modulo utilizzato nelle versioni precedenti di Windows (come Windows NT, Windows 2000 e Windows XP) per gestire le operazioni di logon, logoff e gestione della sicurezza.

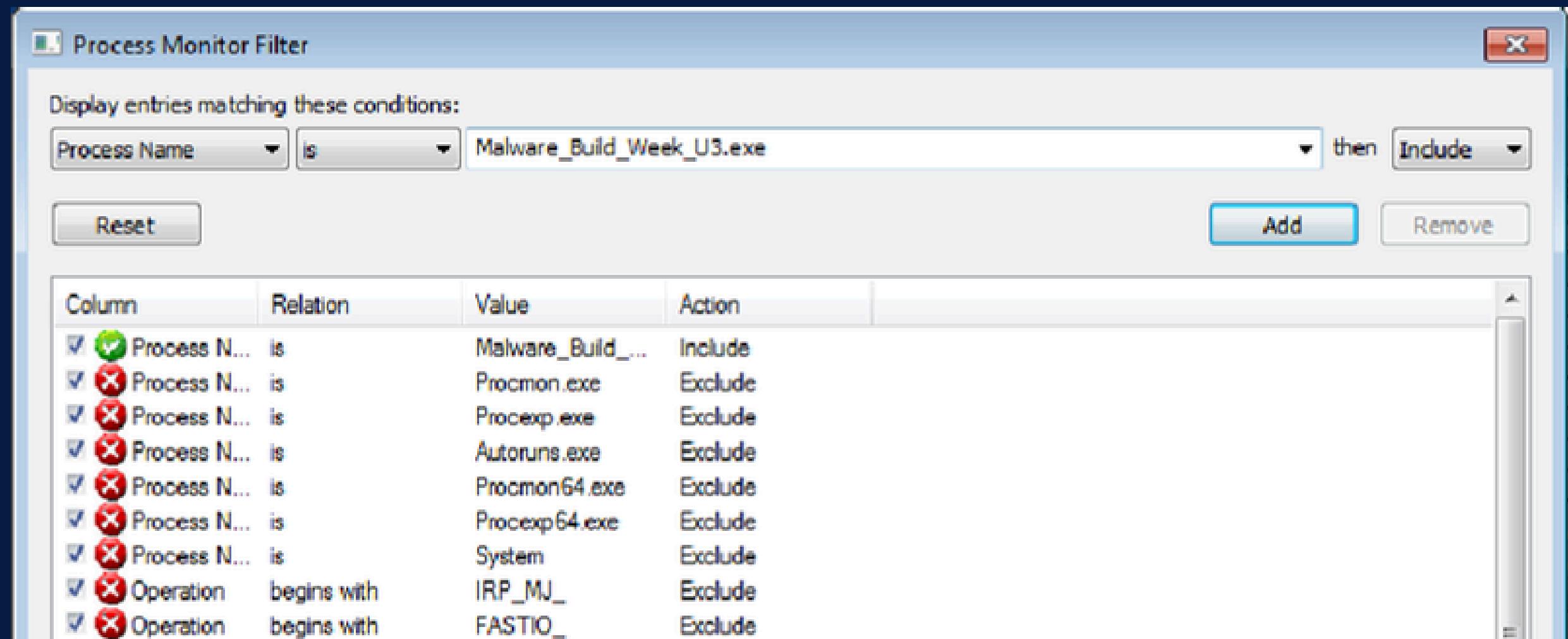


10:59:14.0407...	Malware_Build_Week_U3...	4020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll
10:59:14.0409...	Malware_Build_Week_U3...	4020	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll
10:59:14.0410...	Malware_Build_Week_U3...	4020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll
10:59:14.0421...	Malware_Build_Week_U3...	4020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll
10:59:14.0445...	Malware_Build_Week_U3...	4020	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll
10:59:14.0448...	Malware_Build_Week_U3...	4020	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll

La presenza di questo file può spesso indicare che un eseguibile sta tentando di sostituire una propria libreria con una libreria legittima di windows.

# Chiave di Registro

Apriamo Procmon ed impostiamo i filtri affinchè i risultati possano estrarre solo le modifiche apportate al sistema da parte del malware.



Successivamente filtriamo ulteriormente per visualizzare solamente il registro delle chiavi di sistema.

# Chiave di Registro

Possiamo così notare che la chiave di registro che viene a crearsi è la **REG\_OPENED\_EXISTING\_KEY**

Operation:	RegCreateKey
Result:	SUCCESS
Path:	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon
Duration:	0.0000121
Desired Access:	All Access
Disposition:	REG_OPENED_EXISTING_KEY

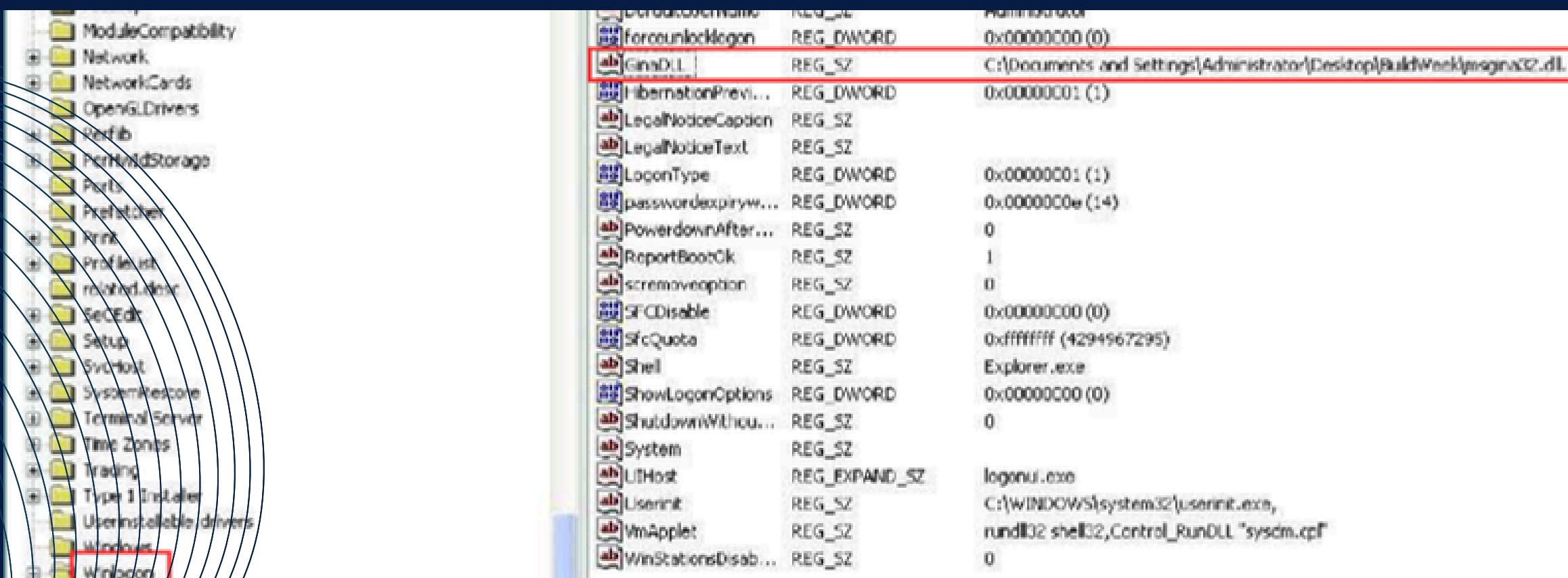
  

Time	Process Name	PID	Operation	Path	Result	Detail
17:51:	Malware_Build_	1968	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Q...
17:51:	Malware_Build_	1968	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	REPARSE	Desired Access: R...
17:51:	Malware_Build_	1968	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	Desired Access: R...
17:51:	Malware_Build_	1968	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	KeySetInformation...
17:51:	Malware_Build_	1968	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\(\Default)	SUCCESS	Type: REG_SZ; Le...
17:51:	Malware_Build_	1968	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: R...
17:51:	Malware_Build_	1968	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
17:51:	Malware_Build_	1968	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	KeySetInformation...
17:51:	Malware_Build_	1968	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	NAME NOT FOUND	Length: 548
17:51:	Malware_Build_	1968	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWO...
17:51:	Malware_Build_	1968	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
17:51:	Malware_Build_	1968	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
17:51:	Malware_Build_	1968	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
17:51:	Malware_Build_	1968	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnos...	NAME NOT FOUND	Desired Access: R...
17:51:	Malware_Build_	1968	RegQueryKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnos...	SUCCESS	Query: HandleTag...
17:51:	Malware_Build_	1968	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All...
17:51:	Malware_Build_	1968	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	KeySetInformation...
17:51:	Malware_Build_	1968	RegQueryKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Query: HandleTag...
17:51:	Malware_Build_	1968	RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	ACCESS DENIED	Type: REG_SZ; Le...
17:51:	Malware_Build_	1968	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	

A questo punto ci dirigiamo tramite il tool di Windows **REGEDIT** nel cercare il valore della chiave di registro . Come possiamo però notare , non riusciamo a trovare **GinaDLL** poichè , come sopracitato , con l'introduzione di Windows Vista e versioni successive, incluso Windows 7 , Microsoft ha sostituito Gina con un nuovo modello di autenticazione. La scrittura della chiave sarà quindi Denied.

# Chiave di Registro

Proviamo dunque a testare il malware su Windows XP. Come si può osservare, è stata correttamente creata la chiave di registro "**HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL**". All'interno di questa chiave, è stato copiato il percorso del DLL msgina32.dll, situato nella stessa directory dell'eseguibile del malware, in questo caso "C:\Documents and Settings\Administrator\Desktop\Buildweek\msgina32.dll". Questo consente di inserire un DLL malevolo che cattura le credenziali di accesso, le quali possono essere poi sfruttate da un utente malintenzionato per prendere il controllo del computer.

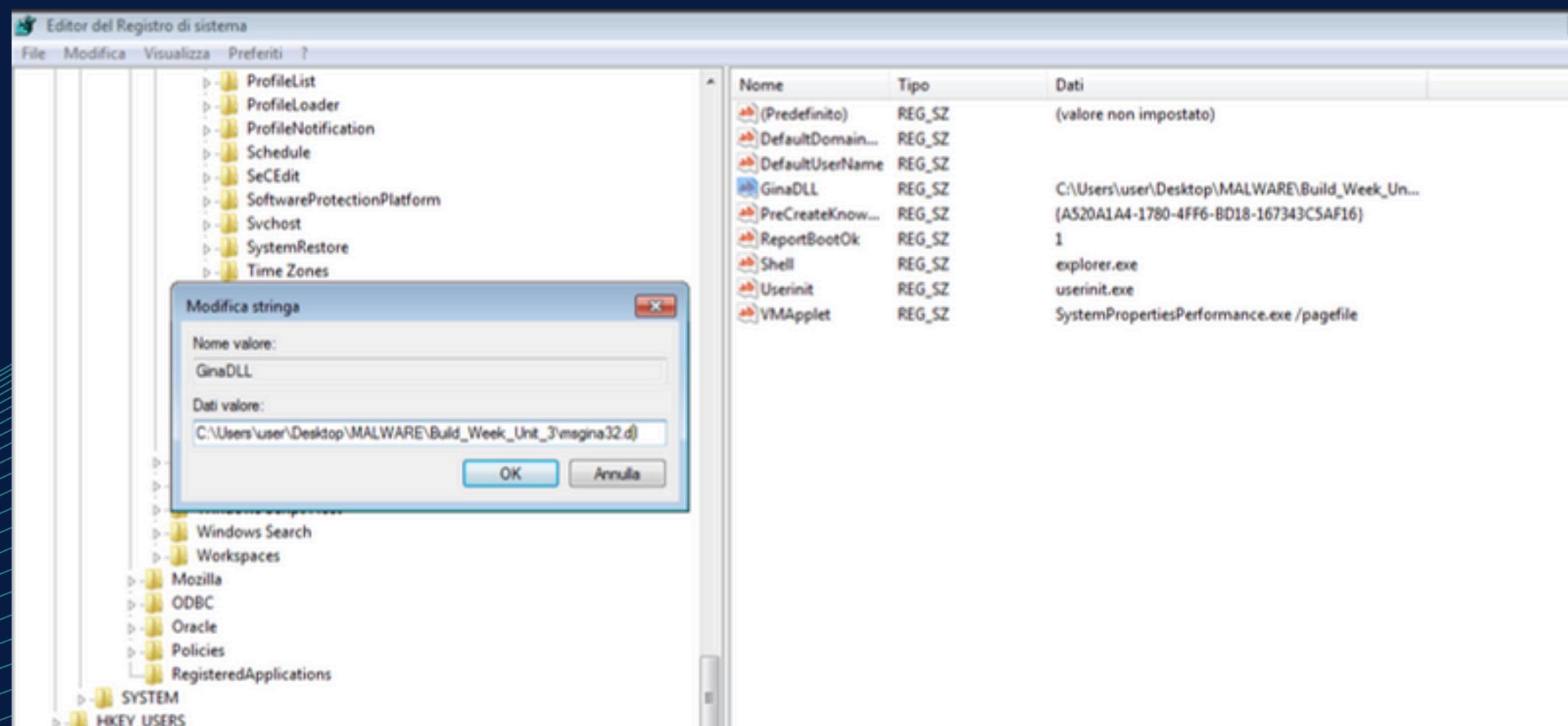


Per ovviare il problema della scrittura denied della chiave di registro su Windows 7 , possiamo avviare il Malware con privilegi d'amministratore.

# Chiave di Registro

Ci rechiamo quindi nel Path trovato tramite Procmon e troviamo il valore della chiave come richiesto dalla traccia.

9:08	Malware_Build...	1976	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnos...	NAME NOT FOUND Desired Access: R...
9:08	Malware_Build...	1976	RegQueryKey	HKLM	SUCCESS Query: HandleTag...
9:08	Malware_Build...	1976	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS Desired Access: All...
9:08	Malware_Build...	1976	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS KeySetInformation...
9:08	Malware_Build...	1976	RegQueryKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS Query: HandleTag...
9:08	Malware_Build...	1976	RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	SUCCESS Type: REG_SZ Le...
9:08	Malware_Build...	1976	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
9:08	Malware_Build...	1976	RegCloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS
9:08	Malware_Build...	1976	RegCloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS
9:08	Malware_Build...	1976	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS
9:08	Malware_Build...	1976	RegCloseKey	HKLM	SUCCESS



# File System

Cambiamo nuovamente i filtri su Procmon per controllare eventuali cambiamenti al file system . Il contenuto della cartella in cui si trova il Malware vien modificato attraverso la chiamata di sistema **CreateFile** come possiamo vedere nell'immagine di seguito. Attraverso questo comando avviene così la creazione del file **msgina.dll**.

Time ...	Process Name	PID	Operation	Path	Result	Detail
18:13:...	Malware_Build_...	1908	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
18:13:...	Malware_Build_...	1908	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
18:13:...	Malware_Build_...	1908	CreateFileMapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
18:13:30,5994728	Malware_Build_...	1908	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
18:13:...	Malware_Build_...	1908	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
18:13:...	Malware_Build_...	1908	QueryBasicInfor...	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 21/1...
18:13:...	Malware_Build_...	1908	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
18:13:...	Malware_Build_...	1908	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
18:13:...	Malware_Build_...	1908	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
18:13:...	Malware_Build_...	1908	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
18:13:...	Malware_Build_...	1908	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
18:13:...	Malware_Build_...	1908	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
18:13:...	Malware_Build_...	1908	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
18:13:...	Malware_Build_...	1908	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
18:13:...	Malware_Build_...	1908	CloseFile	C:\Windows	SUCCESS	
18:13:...	Malware_Build_...	1908	CreateFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3	SUCCESS	Desired Access: E...
18:13:...	Malware_Build_...	1908	CreateFile	C:\Windows\SysWOW64\aechost.dll	SUCCESS	Desired Access: R...
18:13:...	Malware_Build_...	1908	QueryBasicInfor...	C:\Windows\SysWOW64\aechost.dll	SUCCESS	CreationTime: 14/0...
18:13:...	Malware_Build_...	1908	CloseFile	C:\Windows\SysWOW64\aechost.dll	SUCCESS	
18:13:...	Malware_Build_...	1908	CreateFile	C:\Windows\SysWOW64\aechost.dll	SUCCESS	Desired Access: R...
18:13:...	Malware_Build_...	1908	CreateFileMapp...	C:\Windows\SysWOW64\aechost.dll	FILE LOCKED WI...	SyncType: SyncTy...
18:13:...	Malware_Build_...	1908	CreateFileMapp...	C:\Windows\SysWOW64\aechost.dll	SUCCESS	SyncType: SyncTy...
18:13:...	Malware_Build_...	1908	CloseFile	C:\Windows\SysWOW64\aechost.dll	SUCCESS	
18:13:...	Malware_Build_...	1908	CreateFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Desired Access: G...
18:13:...	Malware_Build_...	1908	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 0, Length: 4...
18:13:...	Malware_Build_...	1908	ReadFile	C:	SUCCESS	Offset: 40.595.456...
18:13:...	Malware_Build_...	1908	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 4.096, Leng...
18:13:...	Malware_Build_...	1908	CloseFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	
18:13:...	Malware_Build_...	1908	QueryNameInfo...	C:\Windows\System32\apisetschema.dll	SUCCESS	Name: \Windows\...
18:13:...	Malware_Build_...	1908	QueryNameInfo...	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\Malware_Build_Week_U3.exe	SUCCESS	Name: \Users\user...
18:13:...	Malware_Build_...	1908	QueryNameInfo...	C:\Windows\System32\wow64cpu.dll	SUCCESS	Name: \Windows\...

Notiamo inoltre la presenza della chiamata **CloseFile**; quest'ultima , nel contesto di un Malware , serve a chiudere specifici processi legittimi oppure a chiudere il processo malevolo , quando questo ha finito di operare , per rendersi invisibile.

# Funzionamento del Malware

Il malware descritto è un dropper, un tipo di malware progettato per introdurre e installare ulteriori payload malevoli nel sistema della vittima. In particolare, utilizza la chiave di registro GinaDLL per inserire una DLL malevola che cattura le credenziali di accesso degli utenti. L'inserimento di una DLL malevola tramite la chiave GinaDLL compromette le credenziali di login degli utenti, esponendole a potenziali furti. Una volta che un attaccante avrà accesso alle credenziali, potrà accedere al sistema con i privilegi dell'utente compromesso, potenzialmente eseguendo ulteriori attacchi o installando un altro malware. Inoltre, modificando la chiave di registro per caricare la propria DLL, il malware garantisce la persistenza nel sistema, poiché la DLL verrà caricata ad ogni login dell'utente. Questa tecnica rende difficile la rimozione del malware, poiché anche dopo un riavvio del sistema, il malware rimane attivo. Tuttavia, il malware è progettato per colpire sistemi operativi obsoleti (Windows XP e precedenti), suggerendo che potrebbe essere stato sviluppato in un periodo in cui questi sistemi erano più diffusi o che gli attaccanti stiano prendendo di mira sistemi legacy ancora in uso. Per proteggersi da questo tipo di attacco, è fondamentale aggiornare i sistemi operativi a versioni più recenti e mantenere aggiornati gli strumenti di sicurezza. Inoltre, monitorare e analizzare le modifiche alle chiavi di registro critiche può aiutare a rilevare e prevenire tali attacchi.

# Traccia - Giorno 3

GINA (Graphical identification and authentication ) è un componente lecito di Windows che permette l'autenticazione degli utenti tramite interfaccia grafica utenti di inserire username e password nel classico riquadro Windows, come quello in figura a destra che usate anche voi per accedere alla macchina virtuale.

- Cosa può succedere se il file . dll lecito viene sostituito con un file . dll malevolo, che intercetta i dati inseriti? Sulla base della risposta sopra, delineate il profilo del Utente tutti i punti per creare un grafico che ne rappresenti lo scopo ad alto livello. Esercizio Giorno 3- ovvero permette agli Malware e delle sue funzionalità.



Sostituire la libreria legittima "gina.dll" con una versione malevola può portare a diverse gravi conseguenze:

## FURTO DI CREDENZIALI

Un programma di accesso compromesso potrebbe registrare e inviare le credenziali dell'utente (nome utente e password) a un malintenzionato. Questo permetterebbe all'attaccante di ottenere accesso non autorizzato al sistema, mettendo a rischio sia i dati personali che quelli aziendali.

## ESCALATION DEI PRIVILEGI

Il malware potrebbe tentare di ottenere privilegi elevati per acquisire diritti di amministratore, permettendo così di eseguire operazioni dannose con maggiore autorità e compromettendo ulteriormente la sicurezza del sistema.

## ACCESSO NON AUTORIZZATO

Una volta ottenute le credenziali, l'attaccante potrebbe accedere a risorse sensibili del sistema, come file, database, email e altre informazioni riservate. Questo accesso non autorizzato può causare gravi violazioni della privacy e mettere in pericolo informazioni confidenziali.

## COMPROMISSIONE DEL SISTEMA

Un programma di accesso malevolo potrebbe modificare o eliminare file di sistema critici, causando instabilità o addirittura rendendo il sistema inutilizzabile. Questo tipo di compromissione può portare a periodi di inattività e a significative perdite di produttività.

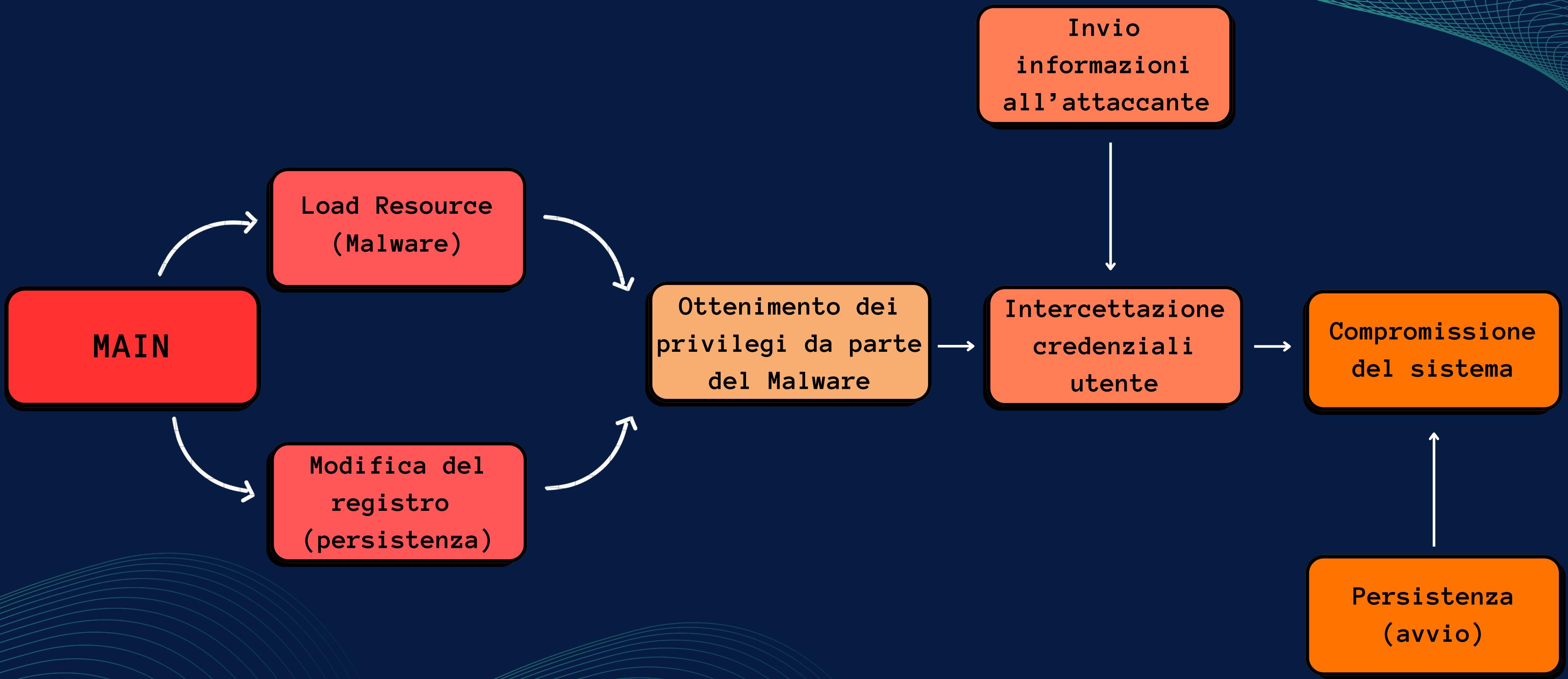
## DIFFUSIONE DI ALTRI MALWARE

Un programma di accesso alterato potrebbe essere utilizzato come veicolo per introdurre ulteriori malware, come trojan, ransomware o keylogger, aumentando il rischio di ulteriori danni al sistema e ai dati.

## MONITORAGGIO E SPIONAGGIO

Il software malevolo potrebbe includere funzionalità di sorveglianza, registrando le attività dell'utente, comprese informazioni sensibili e comunicazioni private, aumentando ulteriormente il rischio di una violazione della sicurezza.

È fondamentale adottare misure preventive per mitigare questi rischi e garantire la sicurezza e l'integrità del sistema.



# GIORNO 4 - TRACCIA

- [https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d /](https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d/)
- [https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281 /](https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/)
- [https://app.any.run/tasks/f1f20828-2222-46fb-a886-09f77581e67b /](https://app.any.run/tasks/f1f20828-2222-46fb-a886-09f77581e67b/)

Studiare queste di anyrun e spiegarle in un piccolo report.

Come output vorrei la spiegazione in italiano per un eventuale cliente / manager (che è poco preparato sulla materia ) di questi malware (o presunti tali).

Anyrun i primi due li segnala come malware , il terzo no. Indicare nei tre casi le vostre scelte (mettere in quarantena, eliminare, blacklist , falso positivo, falso negativo, vero positivo, vero negativo, chiedo al vendor , ecc.)

# ANY.RUN

Any.Run è una sandbox interattiva online per l'analisi di malware.



Consente agli utenti di eseguire file sospetti in un ambiente virtuale controllato per osservarne il comportamento.

Le caratteristiche principali includono:

- Analisi in tempo reale: l'utente può interagire direttamente con il sistema operativo virtuale, aprendo file o eseguendo comandi.
- Monitoraggio di processi: registra tutte le attività dei processi, incluso l'accesso ai file, le modifiche al registro e le connessioni di rete.
- Visualizzazione grafica: fornisce un grafico che mostra le relazioni tra i processi e le attività di rete.
- Report dettagliati: genera report con indicatori di compromissione (IoC) come hash, connessioni IP, e modifiche al sistema.

# TASK 1: VIDAR.EXE

Vidar.exe è un malware invasivo che ruba informazioni sensibili dagli utenti infettati, come credenziali di accesso e criptovalute.

Esso appartiene alla famiglia degli stealer, malware creati per raccogliere informazioni non autorizzate come file, password e criptovalute dagli utenti.

**General Info**

Add for printing

File name: 66bddfc52736\_vidar.exe  
Full analysis: <https://app.any.run/tasks/371957e1-d960-4b8a-8c6b-241ff918517d>  
Verdict: **Malicious activity**  
Threats: Loader Lumma Stealer Vidar

Stealers are a group of malicious software that are intended for gaining unauthorized access to users' information and transferring it to the attacker. The stealer malware category includes various types of programs that focus on their particular kind of data, including files, passwords, and cryptocurrency. Stealers are capable of spying on their targets by recording their keystrokes and taking screenshots. This type of malware is primarily distributed as part of phishing campaigns.

Analysis date: August 25, 2024 at 22:11:02  
OS: Windows 10 Professional (build: 19045, 64 bit)  
Tags: [vidar](#) [lumma](#) [stealer](#) [loader](#)  
Indicators:   
MIME: application/x-dosexec  
File info: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows  
MD5: FEDB687ED23F77925B35623027F799BB  
SHA1: 7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81  
SHA256: 325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA13B8D1  
SSDEEP: 6144:yZIGEaS7npmSNlfI330znhlBf4hJYBaZaH55B:rGEaSVmSmI30znhSYaZa5

Malware Trends Tracker >>>

# TASK 1: VIDAR.EXE

Per avere una conferma abbiamo cercato il file su **VirusTotal** tramite hash e 61 vendors lo ritengono malevolo.

The screenshot shows the VirusTotal analysis interface for the file 325396d5ffca8546730b9a56c2d0ed99238d48b5e1c3c49e7d027505ea13b8d1. The main summary indicates that 61 out of 75 security vendors flagged the file as malicious. The file is identified as MSG.exe and is an EXE file. It was analyzed a moment ago and has a size of 190.00 KB. The interface includes a community score bar and various detection tags such as 'peexe', 'spreader', 'long-sleeps', 'persistence', 'checks-user-input', 'checks-cpu-name', 'assembly', 'calls-wmi', and 'detect-debug-environment'. Below the summary, a detailed table lists 61 vendor detections:

Vendor	Detection	Vendor	Detection
CrowdStrike Falcon	Win/malicious_confidence_90% (D)	Cybereason	Malicious.ed23f7
Cylance	Unsafe	DeepInstinct	MALICIOUS
DrWeb	Trojan.PWS.Steam.37520	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Jalapeno.18063 (B)	eScan	Gen:Variant.Jalapeno.18063
ESET-NOD32	A Variant Of MSIL/GenKryptik.HARO	Fortinet	MSIL/Kryptik.AKRFItr
GData	Gen:Variant.Jalapeno.18063	Google	Detected
Gridinsoft (no cloud)	Spy.Win32.Vidar.tr	Huorong	Trojan/MSIL.Agent.li
Ikarus	Trojan.MSIL.Krypt	K7AntiVirus	Trojan (005b96981)
K7GW	Trojan (005b96981)	Kaspersky	HEUR:Trojan-PSW.MSIL.Stalerc.gen
Kingsoft	MSIL.Trojan-PSW.Stalerc.gen	Lionic	Trojan.Win32.Stalerc.1m/c
Malwarebytes	Spyware.Stalc	MAX.	Malware (ai Score=88)
MaxSecure	Trojan.Malware.204074003.susgen	McAfee Scanner	Real Protect-LS/FEDB687ED23F
Microsoft	Trojan:MSIL/LummaC.MERIMTB	NANO-Antivirus	Trojan.Win32.Steam.kqyfae
Palo Alto Networks	Generic.ml	Panda	Trj/GdSda.A
QuickHeal	Trojan.Lummac	Rising	Malware.Obfus/MSIL@AI.100 (RDM.MSIL...)
Sangfor Engine Zero	Infostealer.Msll.Stalerc.Vru1	SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Suspicious PE	Skyhigh (SWG)	Artemis!Trojan
Sophos	Mal/MSIL-KC	Symantec	ML.Attribute.HighConfidence
TACHYON	Trojan-PWS/W32.DN-Stalerc.194560	Tencent	Malware.Win32.Gencirc.1416eb8e
Trellix (ENS)	Artemis!FEDB687ED23F	Trellix (HX)	Generic.mg.fedb687ed23f7792
TrendMicro	Trojan.Win32.PRIVATELOADER.YXEHQZ	TrendMicro-HouseCall	Trojan.Win32.PRIVATELOADER.YXEHQZ
Varist	W32/MSIL_Kryptik.LKR.gen Eldorado	VIPRE	Gen:Variant.Jalapeno.18063

Nell'analisi di Any.Run troviamo queste principali minacce:

**Loader**: un software che installa altri tipi di malware nel sistema infetto, essi vengono spesso distribuiti attraverso tecniche di phishing e social engineering, cioè ingannando l'utente a scaricare ed eseguire il file infetto.

**Stealer**: sono malware progettati per rubare informazioni sensibili degli utenti, come file, password e criptovalute, e inviarle agli attaccanti. Possono spiare gli utenti registrando tastiere e schermate, e vengono diffusi principalmente tramite campagne di phishing.

- **Vidar**: un noto stealer che prende il nome dal dio della vendetta della mitologia scandinava. Attivo dal 2018, Vidar è progettato per rubare informazioni personali, incluse credenziali di accesso e portafogli di criptovalute.
- **Lumma**: un altro stealer che si concentra sul furto di dati, in particolare di criptovalute e password. In particolare è offerto come "malware-as-a-service", cioè venduto a criminali informatici per scopi malevoli.

Di solito Vidar viene distribuito tramite email o link fraudolenti, in cui gli utenti sono indotti ad eseguire un file infetto; inoltre il malware utilizza tecniche avanzate per evitare la rilevazione da parte dei software di sicurezza e per mantenere una presenza attiva nel sistema infetto.

Nel nostro caso specifico il file eseguibile "**vidar.exe**" avvia per l'appunto diversi processi malevoli, inclusi tentativi di lettura delle credenziali da browser web, scansione del sistema e creazione di file nei directory di sistema e utente.

Inoltre utilizza strumenti legittimi di Windows (come **RegAsm.exe**) per eseguire attività malevole, come la lettura di impostazioni di sicurezza o di informazioni sul sistema.

**RegAsm.exe** è uno strumento di Windows che fa parte di .NET Framework.

Serve a rendere le librerie create con .NET (file .DLL) utilizzabili da altri programmi, specialmente quelli più vecchi che usano la tecnologia COM (Component Object Model).

In pratica, **RegAsm.exe** aiuta i programmi a "**vedere**" e usare questi tipi di librerie, ulteriormente serve a "**registrare**" questi file in modo che i programmi possano trovarli e utilizzarli.

Come da foto possiamo osservare l'utilizzo di RegAsm.exe

Connections						
PID	Process	IP	Domain	ASN	CN	Reputation
5468	svchost.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3584	svchost.exe	20.73.194.208:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6908	RegAsm.exe	147.45.44.104:80	-	000 FREEnet Group	RU	malicious
4704	RegAsm.exe	72.67.215.62:443	caffegclasiqwp.shop	CLOUDFLARENET	US	unknown
6344	SIHClient.exe	27.169.103:443	slscr.update.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	IE	unknown
6344	SIHClient.exe	23.35.229.160:80	www.microsoft.com	AKAMAI-AS	DE	whitelisted
6344	SIHClient.exe	13.95.31.18:443	fe3cr.delivery.mp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted

Threats			
PID	Process	Class	Message
6908	RegAsm.exe	Potentially Bad Traffic	ET INFO Executable Download from dotted-quad Host
6908	RegAsm.exe	Potential Corporate Privacy Violation	ET POLICY PE EXE or DLL Windows file download HTTP
6908	RegAsm.exe	Potentially Bad Traffic	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response
6908	RegAsm.exe	Misc Attack	ET DROP Spamhaus DROP Listed Traffic Inbound group 23
6908	RegAsm.exe	Potentially Bad Traffic	ET INFO Executable Download from dotted-quad Host
4704	RegAsm.exe	A Network Trojan was detected	STEALER [ANY.RUN] Lumma Stealer TLS Connection
2256	svchost.exe	Potentially Bad Traffic	ET POLICY DNS Query to DynDNS Domain *.zapto .org
6908	RegAsm.exe	Potentially Bad Traffic	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response

Inoltre dal comportamento abbiamo dedotto che il Malware estrae informazioni sensibili tramite comando (cmd.exe) e quindi potrebbe inviare questi dati a server remoti come quello in esempio di seguito:



Come da report di Any.run il malware forza una connessione tra l'host e i server aventi ip 172.67.215.62 e 104.21.16.180.

In conclusione possiamo confermare che il malware è un vero positivo ed è consigliabile eliminarlo.

# TASK 2: JVCZFHE.EXE

The screenshot shows the ANY.RUN malware analysis interface. At the top, there's a banner with the ANY.RUN logo, the text "ANALYZE MALWARE", and links for "Huge database of samples and IOCs", "Unlimited submissions", "Custom VM setup", and "Interactive approach". A "Sign up, it's free" button is also present. Below the banner, the main interface has tabs for "General", "Behavior", "MalConf", "Static information", "Video", "Screenshots", "System events", and "Network". A "Print" icon and a "Download" icon are also visible. The "General Info" section contains the following details:

URL:	<a href="https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe">https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe</a>
Full analysis:	<a href="https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281">https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281</a>
Verdict:	Malicious activity
Analysis date:	August 25, 2024 at 22:38:59
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	github netreactor
Indicators:	* * * *
MDS:	00B5E91B42712471C0FB0B37B715670C
SHA1:	D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
SHA256:	0307EE805DF8B94733598D5C3D62828678EAEDBF1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3fJMERCNuN:2uRQyQ3zMsCNa

A note at the bottom states: "ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content."

Below this is a "Software environment set and analysis options" dropdown menu, and at the bottom, a "Behavior activities" section.

## Behavior activities

### MALICIOUS

No malicious indicators.

### SUSPICIOUS

Process drops legitimate windows executable

- firefox.exe (PID: 6596)

Uses TIMEOUT.EXE to delay execution

- cmd.exe (PID: 7520)
- cmd.exe (PID: 7876)

Reads security settings of Internet Explorer

- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)

Checks Windows Trust Settings

- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)

Starts CMD.EXE for commands execution

- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)

Executes application which crashes

- Jvczfhe.exe (PID: 7492)
- Muadnrd.exe (PID: 7824)

Connects to unusual port

- InstallUtil.exe (PID: 5152)

Application launched itself

- Muadnrd.exe (PID: 7824)

In quest'analisi prendiamo in considerazione 3 principali file sospetti: **Jvczfhe.exe**, **Muadnrd.exe** e **InstallUtil.exe**

Dunque andiamo a vedere nel dettaglio:

## 1. Muadnrd.exe

7248	"C:\Users\admin\Downloads\Muadnrd.exe"	C:\Users\admin\Downloads\Muadnrd.exe		Muadnrd.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Microsoft Edge	
Exit code:	0	Version:	126.0.2592.113	

Questo file è risultato sospetto durante l'analisi poiché mostra un comportamento simile ad un malware, di fatti ha eseguito operazioni insolite, come:

- **Modifica delle impostazioni di rete:** modifica le impostazioni di rete relative alla gestione dei proxy e delle connessioni intranet, un altro indicatore di possibili tentativi di esfiltrazione di dati o connessioni non autorizzate.

Key: HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap  
Name: ProxyBypass

- **Disabilitazione di tracciamenti:** scrive nei registri di sistema per disabilitare diverse forme di tracciamento, come la registrazione delle attività di rete **RASAPI32** e **RASMANCS**. Questi ultimi sono dei componenti di Windows associati ai servizi di rete e alla gestione delle connessioni da remoto attivi in background (RAS).

(PID) Process: (7824) Muadnrd.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write	Name: EnableFileTracing
Value: 0	
(PID) Process: (7824) Muadnrd.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write	Name: EnableAutoFileTracing
Value: 0	
(PID) Process: (7824) Muadnrd.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write	Name: EnableConsoleTracing
Value: 0	
(PID) Process: (7824) Muadnrd.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write	Name: FileTracingMask
Value:	
(PID) Process: (7824) Muadnrd.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write	Name: ConsoleTracingMask
Value:	
(PID) Process: (7824) Muadnrd.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write	Name: MaxFileSize
Value: 1048576	
(PID) Process: (7824) Muadnrd.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd_RASAPI32
Operation: write	Name: FileDirectory

Nello specifico possiamo vedere come il malware ottiene la persistenza:

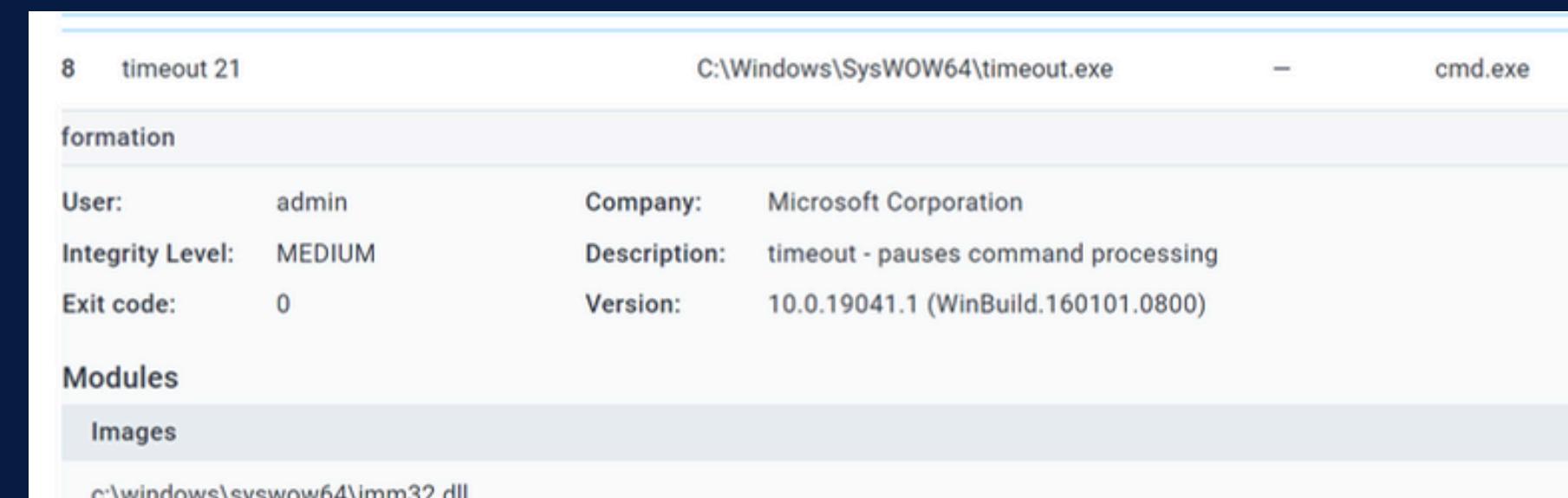
- **HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Muadnrd\_RASAPI32**

In questa chiave, il malware effettua diverse operazioni di scrittura per configurare la traccia del file e impostazioni relative al tracciamento e alla persistenza.

Questa chiave di registro è utilizzata per eseguire operazioni di monitoraggio e configurazione di tracce, che possono includere elementi di persistenza per assicurare che il malware rimanga attivo sul sistema compromesso.

- **Esecuzione di Comandi:**

Utilizzo di **cmd.exe**: avvia il processo cmd.exe per eseguire comandi specifici, come l'uso di **timeout.exe** per ritardare l'esecuzione. Questo può essere un tentativo di ritardare l'attività malevola per evitare la rilevazione immediata.



Come Best Practise consigliamo l'eliminazione del file.

Anche se il comportamento non è così chiaro come nel caso precedente, la sicurezza del sistema potrebbe essere compromessa e il file andrebbe rimosso per prevenire eventuali danni futuri.

Si può affermare quindi , anche in questo caso , che il file rappresenti un vero positivo (molto probabilmente un malware).

## 2. Jvczfhe.exe

7492	"C:\Users\admin\Downloads\Jvczfhe.exe"	C:\Users\admin\Downloads\Jvczfhe.exe	*	firefox.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Microsoft Edge	
Exit code:	3762504530	Version:	126.0.2592.113	

Durante l'analisi, anche questo file ha mostrato comportamenti malevoli.

Sono state rilevate attività che possono compromettere la sicurezza del sistema, come l'accesso a informazioni sensibili, la modifica delle impostazioni di sicurezza e l'esecuzione di comandi nascosti.

- **Rischi principali:**

- Tentativi di aggirare le difese del sistema.
- Connessioni a server esterni per potenziali furti di dati.
- Modifiche non autorizzate al sistema operativo.

Vediamo in dettaglio quello che fa questo malware:

## Modifica delle impostazioni di sicurezza:

il malware scrive nelle chiavi di registro legate al tracing (tracciamento) del sistema, che includono:

- **HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe\_RASAPI32**
- **HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe\_RASMANCS**

Vengono disabilitate funzionalità di tracciamento, come **EnableFileTracing**, **EnableAutoFileTracing**, e **EnableConsoleTracing**.

Modifica altre impostazioni del tracing come **FileTracingMask**, **ConsoleTracingMask**, **MaxFileSize**, e **FileDirectory** per nascondere la propria attività.

(PID) Process: (7492) Jvczfhe.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write	Name: EnableFileTracing
Value: 0	
(PID) Process: (7492) Jvczfhe.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write	Name: EnableAutoFileTracing
Value: 0	
(PID) Process: (7492) Jvczfhe.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write	Name: EnableConsoleTracing
Value: 0	
(PID) Process: (7492) Jvczfhe.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write	Name: FileTracingMask
Value:	
(PID) Process: (7492) Jvczfhe.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write	Name: ConsoleTracingMask
Value:	
(PID) Process: (7492) Jvczfhe.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write	Name: MaxFileSize
Value: 1048576	
(PID) Process: (7492) Jvczfhe.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASAPI32
Operation: write	Name: FileDirectory
Value: %windir%\tracing	
(PID) Process: (7492) Jvczfhe.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write	Name: EnableFileTracing
Value: 0	
(PID) Process: (7492) Jvczfhe.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write	Name: EnableAutoFileTracing
Value: 0	
(PID) Process: (7492) Jvczfhe.exe	Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\Jvczfhe_RASMANCS
Operation: write	Name: EnableConsoleTracing
Value: 0	

## IP MALEVOLO:

**91.92.253.47** - Associato al dominio egehdehbjtre.duckdns.org, un dominio spesso utilizzato per attività malevole come il controllo remoto di malware. Questo indirizzo IP è probabilmente utilizzato per comunicare con un server di comando e controllo (C2).

Il dominio duckdns.org è noto per fornire servizi di DNS dinamico che vengono spesso abusati dai cybercriminali per gestire i loro server C2.



## Alterazioni delle impostazioni di Internet:

Modifica le impostazioni di sicurezza di Internet Explorer e della gestione della rete, scrivendo nelle chiavi:

**HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap**

Viene abilitato il bypass del proxy (**ProxyBypass**), viene considerato l'intranet (**IntranetName** e **UNCAsIntranet**), e disabilitato l'auto-rilevamento (**AutoDetect**).

Queste modifiche indicano un tentativo di mantenere la persistenza, nascondere l'attività del malware e modificare il comportamento del sistema per evitare il rilevamento o l'interferenza da parte di strumenti di sicurezza.

(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		
(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		
(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet
Value:	1		
(PID) Process:	(7492) Jvczfhe.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	AutoDetect
Value:	0		

## FURTO DI DATI:

Il malware Jvczfhe.exe ha stabilito diverse connessioni a server esterni che potrebbero essere utilizzate per il furto di dati.

Abbiamo notato:

- **Connessioni a porte insolite:**

il malware ha stabilito connessioni su porte insolite, che potrebbero essere utilizzate per comunicare con server di comando e controllo (C2) o per esfiltrare dati. Queste connessioni su porte non standard sono spesso utilizzate dai malware per bypassare le regole di sicurezza e mascherare il traffico malevolo.

- **Modifiche alle impostazioni di sicurezza di Internet Explorer:**

Jvczfhe.exe ha modificato le impostazioni di sicurezza di Internet Explorer, che potrebbero essere utilizzate per facilitare il download di ulteriori payload o per inviare dati rubati a server remoti.

- **Controllo delle impostazioni del proxy:**

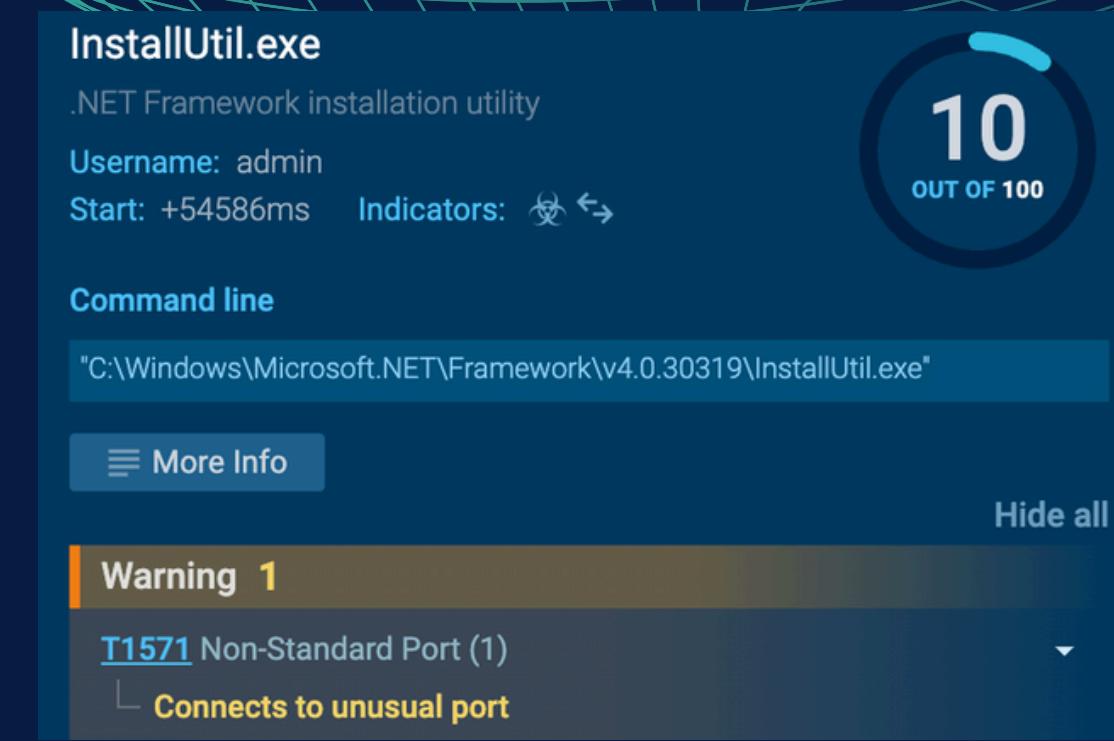
il malware ha controllato e modificato le impostazioni del proxy del sistema.

Questo potrebbe essere un tentativo di reindirizzare il traffico di rete attraverso server controllati dagli attaccanti, consentendo il furto di dati senza essere rilevati dalle misure di sicurezza standard.

Concludendo consigliamo un'eliminazione immediata poiché questo file è confermato come dannoso e potrebbe portare a gravi conseguenze per la sicurezza, come detto nelle pagine precedenti.

Possiamo confermare che questo è **vero positivo**.

### 3. InstallUtil.exe



**InstallUtil.exe** è uno strumento di Windows legittimo, usato per installare e disinstallare software.

In alcuni casi, è stato notato che i criminali informatici lo utilizzano per scopi malevoli, mascherando le loro attività. Durante l'analisi, questo file ha mostrato comportamenti sospetti, di fatti in questo contesto, sembra che **Jvczfhe.exe** sia stato lanciato tramite **InstallUtil.exe**.

Questo può essere indicativo di un potenziale abuso di **InstallUtil.exe**, una tecnica che i malware a volte utilizzano per eseguire codice malevolo fingendosi un programma legittimo.

Quest'analisi ci fa comprendere che il file **Jvczfhe.exe** è un **dropper**, ovvero un tipo di malware che ha come scopo quello di "**droppare**" (rilasciare) altri tipi di malware su un sistema bersaglio. In questo caso, il file sembra eseguire vari comandi, disabilitare log, e sfruttare tecniche di offuscamento, tutti comportamenti che possono indicare un dropper.

Dunque il malware che utilizza **InstallUtil.exe** adotta diverse tecniche di occultamento per evadere la rilevazione e mantenere la sua presenza nel sistema tra cui:

- **Utilizzo di un file legittimo per eseguire codice malevolo:** InstallUtil.exe viene lanciato dal malware Jvczfhe.exe

5152	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.e xe"	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.ex	Jvczfhe.exe
<b>Information</b>			
User:	admin	Company:	Microsoft Corporation
Integrity Level:	MEDIUM	Description:	.NET Framework installation utility
Version:	4.8.9037.0 built by: NET481REL1		

- **Tecniche di anti-debugging e anti-analisi:**

ovvero offuscamento del codice o anti-debugging per rendere difficile l'analisi da parte di ricercatori di sicurezza e strumenti di analisi automatizzati come per esempio l'utilizzo di **timeout.exe**.

- **Persistenza tramite registrazione come servizio:**

InstallUtil.exe può essere utilizzato per registrare un servizio Windows che si avvia automaticamente all'avvio del sistema, garantendo la persistenza del malware.

- **Evasione delle difese di sicurezza:**

Il malware può sfruttare le funzionalità di InstallUtil.exe per eseguire codice in modo silente, evitando di generare comportamenti sospetti che potrebbero attivare le difese di sicurezza come antivirus e firewall.

- **Disabilitazione della Tracciatura:**

Il report descrive che il malware disabilita la tracciatura dei log attraverso InstallUtil.exe, specificamente disabilitando le impostazioni come EnableFileTracing, EnableAutoFileTracing, e EnableConsoleTracing come visto anche in precedenza.

Infine in questo caso consigliamo di tenere costantemente monitorato InstallUtil.exe e altre utilità simili per comportamenti insoliti.

Oltre che esaminare eventuali altri comportamenti sospetti associati a Jvczfhe.exe o attività insolite nel sistema per determinare l'estensione della potenziale infezione; si può configurare il sistema per limitare o bloccare l'uso di InstallUtil.exe da directory non autorizzate, questo può essere fatto tramite regole di gruppo (**GPO**) o soluzioni come AppLocker o Software Restriction Policies (**SRP**).

In questo caso particolare InstallUtil.exe può essere considerato uno strumento di **Living-off-the-Land** (programmi di sistema legittimi che vengono utilizzati dai cybercriminali per evitare di essere rilevati dai software di sicurezza, proprio perché non sono di per sé dannosi).

Possiamo dire che è un **vero positivo** perché Any.Run ha correttamente individuato la minaccia.

Una particolarità che abbiamo notato è il confronto con VirusTotal che non segna alcuna minaccia:

The screenshot shows the VirusTotal analysis interface for the file `Jvcfhe.exe` from the GitHub URL `https://github.com/MELITERRER/frew/blob/main/Jvcfhe.exe`. The main summary indicates that 0 out of 95 security vendors flagged the URL as malicious. Key details include a status of 404, a content type of `text/html; charset=utf-8`, and a last analysis date of 12 minutes ago. Below the summary, there are tabs for DETECTION, DETAILS, and COMMUNITY, with the DETECTION tab currently selected. A green banner encourages users to join the community for additional insights and automation features. The security vendors' analysis section lists 15 vendors, all of which have flagged the file as "Clean". A link to automate checks is also present in this section.

Security vendor	Result
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Antiy-AVL	Clean
benkow.cc	Clean
BlockList	Clean
Certeza	Clean
Acronis	Clean
AI Labs (MONITORAPP)	Clean
alphaMountain.ai	Clean
Artists Against 419	Clean
BitDefender	Clean
Blueliv	Clean
Chong Lua Dao	Clean

Senza l'analisi di Any.Run questo sarebbe stato un falso negativo.

# TASK 3: clic.convertkit-mail2

Win10 64 bit  
Complete  
Indicators:

IOC MalConf Restart

Text report Graph ATT&CK ChatGPT Export ▾

Processes Filter by PID or name Only important

Questo URL è stato sottoposto ad verifica per potenziali attività malevoli, poiché è spesso utilizzato e associato a campagne di phishing o per distribuire software dannosi attraverso download nascosti.

Possiamo notare subito che secondo l'analisi di Any.Run non ci sono attività particolarmente sospette ed infatti Any.Run non ha rilevato nessuna minaccia.

**General Info**

Add for printing

URL: <https://click.convertkit-mail2.com/wvuqovqmwagh50nddc7hnxdlxxcu8/48hvhehr87opxbux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2lbnVyc2VyZWNydwI0ZXJz>

Full analysis: <https://app.any.run/tasks/1f20808-2222-46fb-a8b6-0f177581e67b>

Verdict: **No threats detected** 

Analysis date: August 25, 2024 at 22:44:49

OS: Windows 10 Professional (build: 19045, 64 bit)

Indicators:

MDS: 4C091ASA8C03EBC2EA267980D0DA9F8D

SHA1: F52C878B7F23559FFCE5D1125EFD7B399165DFFC

SHA256: 60F8AB4ACFC5C751F09F2C8632464C8C5E6DA9D04539A69EDB0FC53C8561DFBC

SSDEEP: 3.NIUUE00y0ISibdiJTQTT4SDf0SNicTNKdSVKbf0b/FizfaLzw/y@ax.2UELmtQTT4SB0+su0Sgh0b/FizAiaX

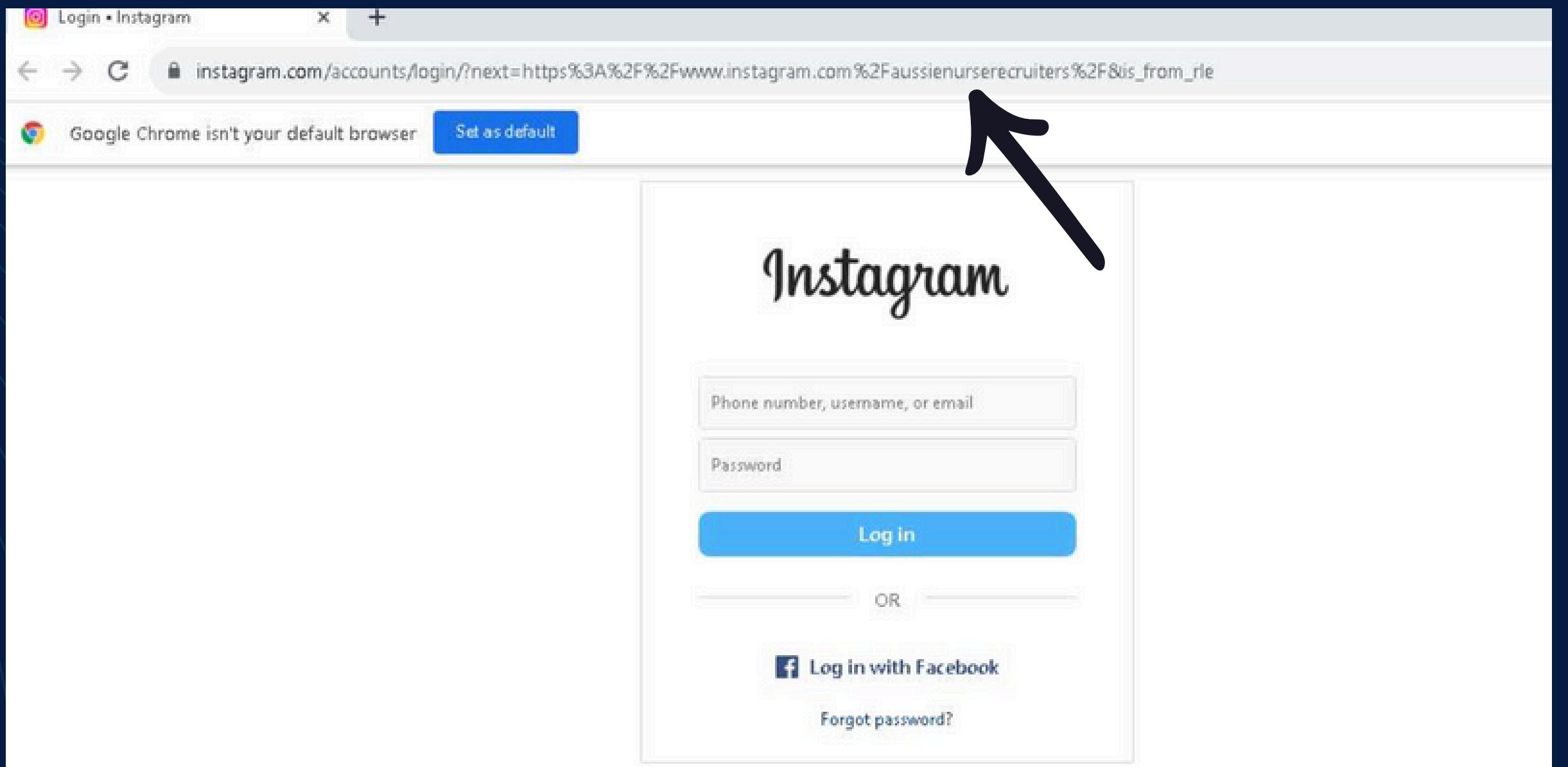
● **ANY.RUN** is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. **ANY.RUN** does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Behavior activities

Add for printing

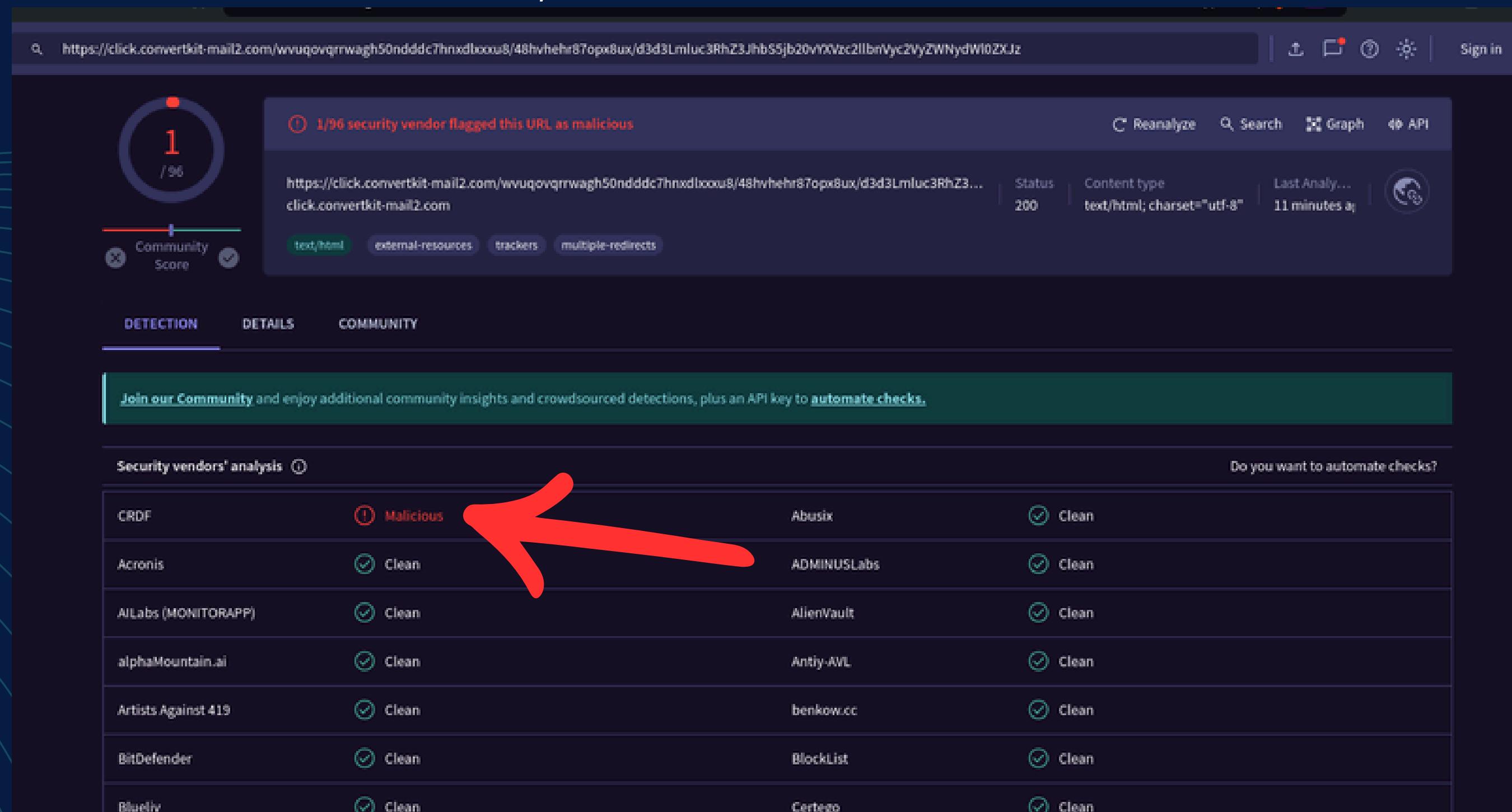
Sembrerebbe solo reindirizzare ad una pagina instagram di recruiter australiani:



#### Redirection chain ⓘ

<https://click.convertkit-mail2.com/wvuqovqrrwagh50ndddc7hnxdlxoxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2lbnVyc2VyZWNydwI0ZXJz>  
<http://www.instagram.com/aussienurseresrecruiters>  
<https://www.instagram.com/aussienurseresrecruiters>  
<https://www.instagram.com/aussienurseresrecruiters/>

Provando a fare un controllo incrociato con VirusTotal si può constatare come quasi tutti i vendor lo classificano come sicuro, tranne CRDF:



The screenshot shows the VirusTotal analysis interface for the URL <https://click.convertkit-mail2.com/wvuqovqrwagh50ndddc7hnxdxxxx8/48hwhehr87opx8ux/d3d3Lmluc3RhZ3JhbSSjb20vY2Vzc2lbnVyc2VyZWNydwI0ZXJz>. The main summary indicates 1/96 security vendors flagged the URL as malicious. Below this, a table lists the vendor analysis results. A red arrow points to the CRDF row, which is marked as 'Malicious'. All other vendors listed (Acronis, AI Labs, alphaMountain.ai, Artists Against 419, BitDefender, Blueliv, Abusix, ADMINUSLabs, AlienVault, Antiy-AVL, benkow.cc, BlockList, Certesoo) are marked as 'Clean'.

Vendor	Analysis	Vendor	Analysis
CRDF	Malicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean
AI Labs (MONITORAPP)	Clean	AlienVault	Clean
alphaMountain.ai	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certesoo	Clean

In questo caso la Best Practice sarebbe contattare il vendor, perché molto probabilmente è un **falso positivo**, l'URL era sospetto, ma non sono stati trovati segni di malware.

# GIORNO 5 - TRACCIA

- [https:// mega.nz/folder/ASgWmZpD#vZdDbQXLW8tOEoC8npglyg](https://mega.nz/folder/ASgWmZpD#vZdDbQXLW8tOEoC8npglyg)

In questo link sono presenti due MALWARE

- Parte 1 Analizzare il contenuto del file compresso “calcolatriceinnovativa50.exe.zip” andando a confermare che è un malware (totalmente innoquo)
- Parte 2 Il solito dipendente "sveglio" dice al SOC (che siamo noi) che un suo amico, che qui chiameremo "AmicoNerd" ha avviato in un PC aziendale il contenuto di questo archivio “AmicoNerd.zip”

Il nostro compito è convincere il dipendente che il file è malevolo. Dopo l'analisi, pulire le eventuali tracce / gli effetti del malware dalla macchina virtuale di test.

Considerata la richiesta della traccia andremo ad effettuare delle analisi statiche e dinamiche, così da ottenere più risultati che ci consentiranno di rilasciare una conclusione esplicita e dimostrativa.

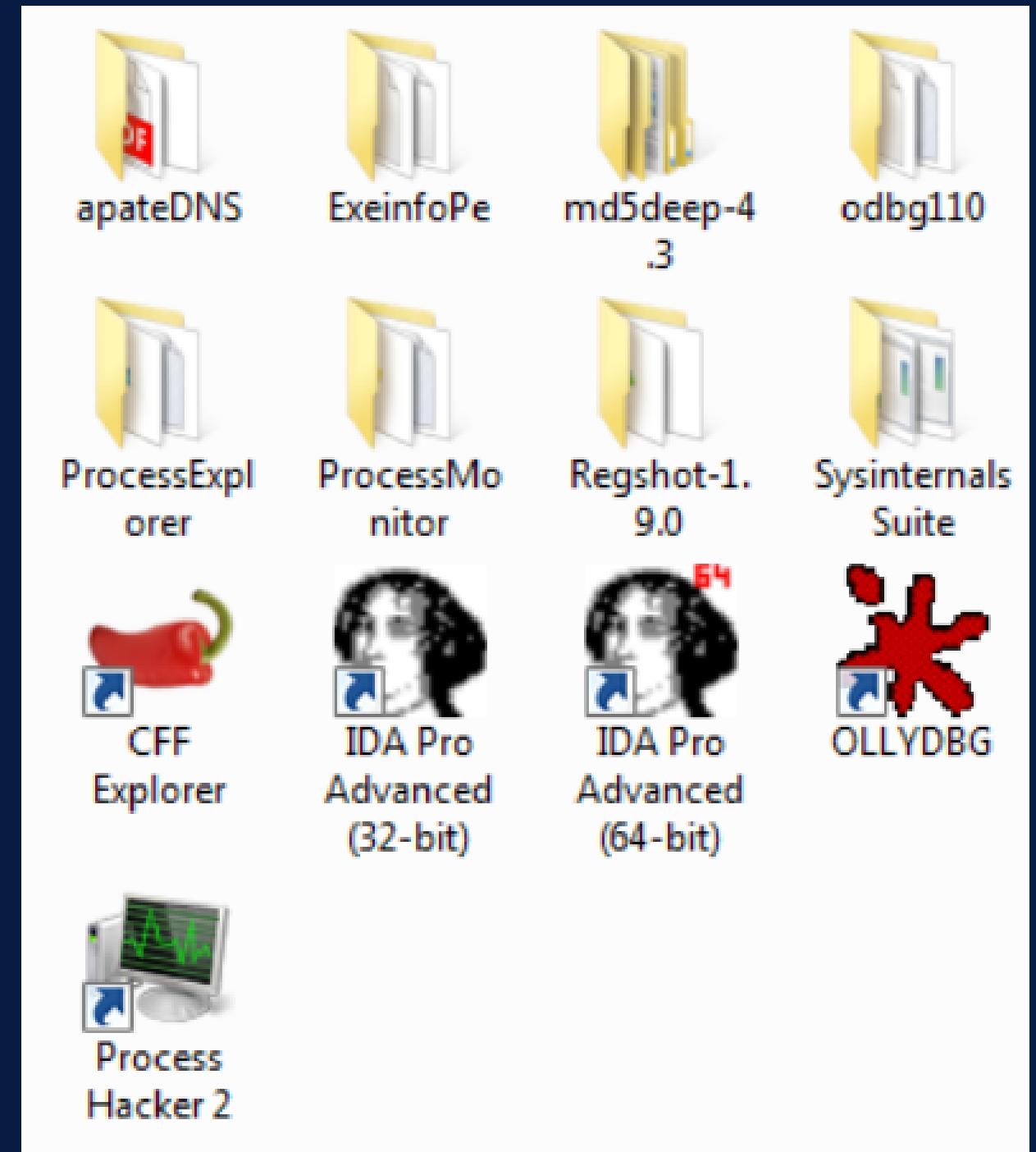
Andremo ad utilizzare vari servizi e software quali:

#### ANALISI STATICÀ

- CFF Explorer
- VirusTotal

#### ANALISI DINAMICA

- RegShot
- ApateDns
- ProcMon
- Process Explorer



Nel primo step di analisi che abbiamo affrontato, abbiamo utilizzare il servizio che offre “VirusTotal”, in modo tale da poter avere un riscontro basato sui feedback degli esperti del settore, sul file oggetto di analisi. Utilizzando il software CFF Explorer, possiamo ottenere l’hash, nell’algoritmo SHA256, per effettuare la ricerca del file in questione, “**calcolatriceinnovativa50.exe**”, che inserendolo nel sito di VirusTotal ci da come riscontro queste informazioni:

The screenshot shows the VirusTotal analysis interface for the file `c7f8e8f17dcd7de447cc6b8d99952be9c781f2542030d49797683e7d5ad5e7`, which is identified as `CALC.EXE`. The file size is 112.50 KB and was last analyzed 1 year ago. A prominent red circle highlights the **Community Score** of **54 / 67**. The vendor analysis table lists 67 entries, showing various detections across different security vendors. The table includes columns for vendor name, detection name, and malware family. Some detections include additional context like file hashes or specific threat names.

Vendor	Detection	Malware Family
AhnLab-V3	Backdoor/Win32.Bifrose.C64906	Alibaba
Antiy-AVL	Trojan/Win32.Rozena	Arcabit
Avast	Win32:SwPatch [Wrm]	AVG
Avira (no cloud)	TR/Patched.Gen2	BitDefender
BitDefenderTheta	Gen:NN_ZexAF.36350.hm0@a0QzbzfC	Bkav Pro
ClamAV	Win.Trojan.MSShellcode-6360730-0	CrowdStrike Falcon
Cybureau	Malicious.138f26	Cylance

The screenshot shows a malware analysis interface. At the top left is a circular 'Community Score' meter with a red needle pointing to 54 out of 67. To its right, a message indicates that 54/67 security vendors flagged the file as malicious. Below this are the file's SHA256 hash (c7f8e0f17dcd7de447cc6b8d99952be9c781f2542030d49797683e7df6ad93e7), name (CALC.EXE), and tags (peexe, checks-user-input, detect-debug-environment). On the right, it shows a file size of 112.50 KB and a last analysis date of 1 year ago. Below this is a navigation bar with tabs: DETECTION (selected), DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with a count of 1). A green banner below the tabs encourages joining the community. The main content area displays a table titled 'Security vendors' analysis' with 14 rows. Each row contains the vendor name, detection name, and a brief description. The vendors listed are AhnLab-V3, Antiy-AVL, Avast, Avira (no cloud), BitDefenderTheta, ClamAV, and Cybereason. The detections include Backdoor/Win32.Bifrose.C64906, Trojan/Win32.Rozena, Win32:SwPatch [Wrm], TR/Patched.Gen2, Gen:NN.Zexaf.36350.hm0@a0Qzbzfc, Win.Trojan.MSShellcode-6360730-0, and Malicious.138f26. The descriptions mention various malware types like CobaltStrike, CryptZ, and W32.AIDetectMalware.

Vendor	Detection	Description
AhnLab-V3	Backdoor/Win32.Bifrose.C64906	Alibaba
Antiy-AVL	Trojan/Win32.Rozena	Arcabit
Avast	Win32:SwPatch [Wrm]	AVG
Avira (no cloud)	TR/Patched.Gen2	BitDefender
BitDefenderTheta	Gen:NN.Zexaf.36350.hm0@a0Qzbzfc	Bkav Pro
ClamAV	Win.Trojan.MSShellcode-6360730-0	CrowdStrike Falcon
Cybereason	Malicious.138f26	Cylance

Come possiamo vedere i feedback dei vendor ci danno informazioni univoche che considerano il file oggetto un file malevolo e sconsigliano l'utilizzo poichè reputato nella maggior parte dei casi come un "Trojan", tipologia di Malware molto nota e diffusa.

Abbiamo effettuato anche un'ulteriore analisi del file utilizzandolo con l'estensione **.zip**, abbiamo preso questa decisione poichè cambiando l'estensione siamo andati ad alterare la sequenza di byte del file, ottenendo hash differenti. Analizzando questo nuovo hash abbiamo ottenuto più informazioni.

The screenshot shows the VirusTotal analysis interface for the file `calcolatriceinnovativa50.exe.zip`. The top bar indicates 55/71 security vendors flagged it as malicious. The file size is 73.26 KB, and the last analysis date was 42 minutes ago. The file type is identified as ZIP. Below the header, there are tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The DETECTION tab is selected, showing a green banner encouraging community membership. Below the banner, threat labels include `trojan.swbot/cryptz`, threat categories like trojan, and family labels such as `swbot`, `cryptz`, and `marte`. The SECURITY VENDORS' ANALYSIS section lists detections from various vendors:

Vendor	Detection	Vendor	Detection
AhnLab-V3	Backdoor/Win32_Bifrose.C64906	Alibaba	Trojan/Win32/CobaltStrike.Sc89
ALYac	Trojan.CryptZ.Marte.1.Gen	Anti-AVL	Trojan/Win32.Rozena
Arcabit	Trojan.CryptZ.Marte.1.Gen	Avast	Win32:SwPatch [Wrm]
AVG	Win32:SwPatch [Wrm]	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Marte.1.Gen	BitDefenderTheta	GenCN_ZetaF.36812.hm0@isQzbzlc
ClamAV	Win.Trojan.MSShellCode-6360730-0	Cynet	Malicious (score: 99)
Deepinstinct	MALICIOUS	DrWeb	Trojan.Swbot.1

Qui riportate le informazioni ottenute dalla seconda analisi.

- **Rilevamenti Antivirus:**

- 55 su 71 motori antivirus hanno rilevato il file come malevolo.
  - **Etichette comuni:** Trojan.CryptZ.Marte.1.Gen, Backdoor/Win32.Bifrose.C64906, Trojan/CobaltStrike.5c89, Win32[Wrm].

- **Categorie di Minacce:**

- **Trojan:** il file è stato classificato principalmente come trojan, un tipo di malware che si maschera come un programma legittimo per infettare il sistema.

- **Etichette di Famiglia:**

- **swort, cryptz, marte:** queste etichette indicano la possibile associazione del file con famiglie di malware note per il furto di informazioni o l'infiltrazione.

Possiamo quindi concludere affermando che il file è fortemente malevolo, con il 77% dei motori antivirus che lo classificano come tale. Si consiglia vivamente di eliminare il file e di evitare di eseguirlo.

History ⓘ	
Creation Time	2001-07-18 07:04:41 UTC
First Submission	2023-07-18 08:14:15 UTC
Last Submission	2024-08-29 10:37:21 UTC
Last Analysis	2024-08-29 10:37:32 UTC
Names ⓘ	
CALC	
CALC.EXE	
calcolatriceinnovativa50.exe	
anyrun.bin	
calcprof.exe	
Signature info ⓘ	
Signature Verification	
⚠ File is not signed	
File Version Information	
Copyright	© Корпорация Майкрософт. Все права защищены.
Product	Операционная система Microsoft® Windows®
Description	Калькулятор для Windows
Original Name	CALC.EXE
Internal Name	CALC
File Version	5.1.2600.0 (xpclient.010817-1148)

Abbiamo inoltre avuto come risultato che il Malware oggetto ci porta ad avere 9 “Dropped File”, tra cui **malware.exe** che abbiamo successivamente analizzato

The screenshot shows a malware analysis interface. At the top, a circular progress bar indicates a 'Community Score' of 26/59, with 26 in red and 59 in grey. Below the bar, a message states '26/59 security vendors flagged this file as malicious'. The file name 'malware.exe' is shown with its MD5 hash: 41256d5fddc40fc65b83e6a8aa7bdb79001aeeef49de8a33d658649d42cf22a0c. The file was scanned on 2021-03-12 and has a size of 341 B, last analyzed 3 years ago. The 'DETECTION' tab is selected, showing a table of vendor detections:

Vendor	Detection
Ad-Aware	Generic.RozenaA.70A560A6
AhnLab-V3	BinImage/Shellcode
Anti-AVL	Trojan/Win32.Rozena.ed
Avast	Win32.Swbot-S [Tr]
BitDefender	Generic.RozenaA.70A560A6
AegisLab	Trojan.Win32.Shelma.4ic
ALYac	Generic.RozenaA.70A560A6
Arcabit	Generic.RozenaA.70A560A6
AVG	Win32.Swbot-S [Tr]
ClamAV	Win.Trojan.MSShellcode-7

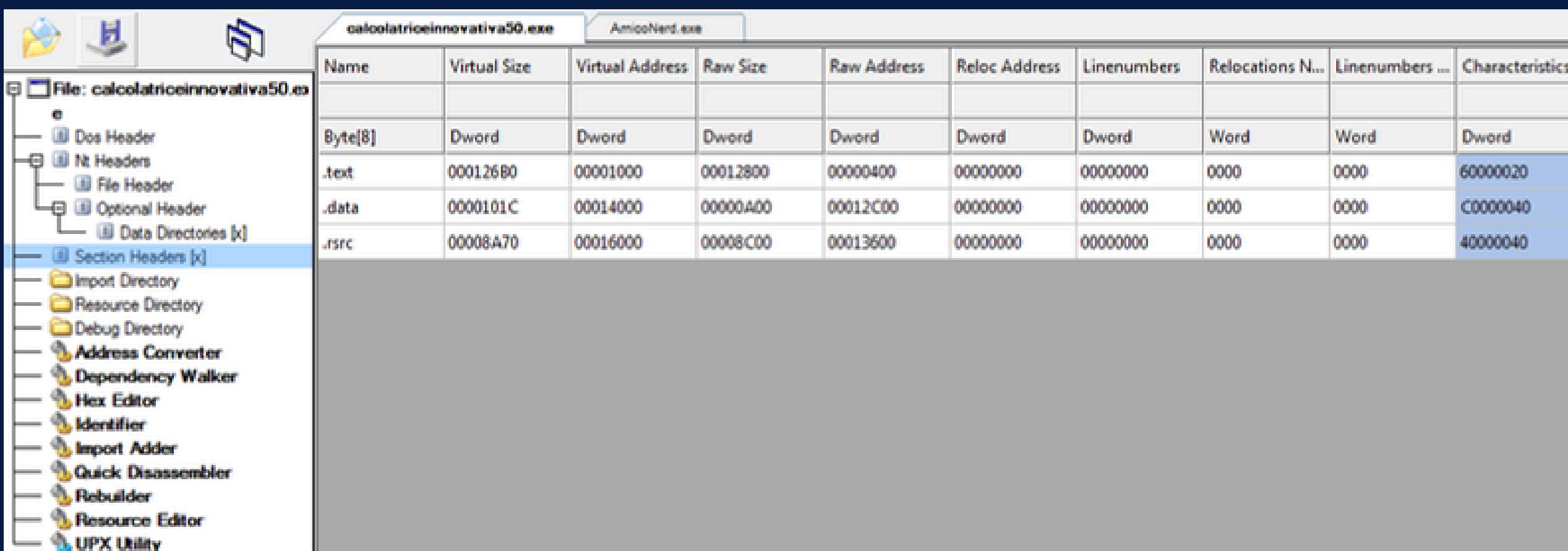
Scanned	Detections	File type	Name
?	?	file	318df61c672561c5214a730e068e37070c81f73e641dfac4708863572e16145c
?	?	file	4107c91e85eff4a480edeb934c23def815156b096b4cdffb81eb3ac98f879b32
?	?	file	8e7f0ad3800a3315c722e576a395300b4233fb848333314102626d1d43fe22d3
?	?	file	925a63af2db7b90d607a57ad91b43dbbb4a9d35533e39fe96dcba4e26b69b93f
?	?	file	b12c3d2dca1008db344092d366e916f3805492493841699e2e1c3e04cc089414
?	?	file	b63c86a02be4dc61c5d7d18257ec8d14075610a715fd78e3be2d0fa7f54480987
?	?	file	b60c34503b1f5585efb89a0e6d72309116efc37bd6a5585848cd7bf73f21459c
?	?	file	e1d3e1a9faa854f90ffed933189900e50c7fd8f6ad5486ffda292bec3b6f3ee3
?	?	?	malware.exe

Il file identificato come **malware.exe** è associato a più file generati o scaricati che presentano nomi di file hashati. Questi file sono molto probabilmente correlati al comportamento del malware, che potrebbe scaricarli, generarli o utilizzarli durante la sua esecuzione.

Tramite il software di CFF Explorer, andiamo a caricare il file **calcolatriceinnovativa50.exe**, procediamo con un'analisi statica andando ad analizzare le sezioni e le directory che il file malevolo contiene.

Come possiamo vedere nell'immagine allegata, il file malevolo contiene queste tre sezioni:

- **.text**: contiene il codice eseguibile del programma, rappresentando la logica principale e le istruzioni operative.
- **.data**: ospita i dati inizializzati, come variabili globali e statiche, essenziali per il funzionamento del programma.
- **.rsrc**: include le risorse dell'applicazione, quali immagini, icone e elementi dell'interfaccia grafica.



L'immagine mostra la Import Directory del file eseguibile, evidenziando le principali librerie dinamiche (DLL) e le funzioni importate dal programma:

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
SHELL32.dll	1	00012CA8	FFFFFFF	FFFFFFF	00012E42	0000109C
msvcrt.dll	26	00012DC8	FFFFFFF	FFFFFFF	00012F60	000011BC
ADVAPI32.dll	3	00012C0C	FFFFFFF	FFFFFFF	00012FFC	00001000
KERNEL32.dll	30	00012C2C	FFFFFFF	FFFFFFF	000131D4	00001020
GDI32.dll	3	00012C1C	FFFFFFF	FFFFFFF	0001320C	00001010
USER32.dll	69	00012CB0	FFFFFFF	FFFFFFF	000136A4	000010A4

1. **SHELL32.dll**: utilizzata per operazioni legate alla shell di Windows, come la gestione di file e cartelle.

2. **msvcrt.dll**: fornisce funzioni della libreria runtime C di Microsoft, essenziali per operazioni matematiche, gestione della memoria e manipolazione di stringhe.

3. **ADVAPI32.dll**: offre accesso a funzionalità avanzate del sistema operativo, come la gestione del registro e dei servizi di sicurezza.

4. **KERNEL32.dll**: una delle librerie core di Windows, utilizzata per operazioni fondamentali come gestione della memoria, processi e thread.

5. **GDI32.dll**: gestisce funzioni grafiche di base, come il rendering di testi e grafica.

6. **USER32.dll**: fornisce le funzioni necessarie per l'interazione con l'interfaccia utente, inclusa la gestione delle finestre e dei controlli.

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
000131AE	77E79F93	0167	GetModuleHandleA
0001319E	77E805D8	022E	LoadLibraryA
0001318C	77E7A5FD	0189	GetProcAddress
0001317C	77E9A9AD	01D8	GlobalCompact
0001316E	77E736A3	01D7	GlobalAlloc
00013160	77E73803	01DE	GlobalFree
00013150	77E6E341	01E5	GlobalReAlloc
00013144	77E78D60	0393	IstrcmpW
0001313C	77E61BE6	0329	Sleep
00013126	77E72A2B	0383	WriteProfileStringW
000131C2	77E6177A	019C	GetStartupInfoA
0001310A	77E6C879	01E6	GlobalSize
000130FA	77E71B14	01E9	GlobalUnlock
000130EA	77E730C1	0047	CreateEventW
000130DA	77E7AC37	0065	CreateThread
000130CC	77E74A69	02A9	ResetEvent
000130C0	77E6F65E	039C	IstrcpynW
000130B4	77E74A3B	02EC	SetEvent
0001309E	77E79D5B	0365	WaitForSingleObject
00013090	77E77963	002C	CloseHandle
00013084	77E73640	0390	IstrcatW
00013078	77E77EF1	039F	IstrlenW
00013068	77E73458	023B	LocalReAlloc
0001305C	77E79A45	0238	LocalFree
00013028	77E79881	0234	LocalAlloc
00013036	77E67FD7	0198	GetProfileStringW
00013118	77E7166F	01E2	GlobalLock
0001300A	77E7C9DB	00FE	GetCommandLineW
0001301C	77E73679	0399	IstrcpyW
0001304A	77E641D5	0194	GetProfileIntW

## LIBRERIA KERNEL

è una libreria di sistema essenziale di Windows che gestisce funzioni di basso livello relative alla gestione della memoria, thread, processi e input/output. Qui di seguito possiamo focalizzarci sulle funzioni più rilevanti:

- **GetModuleHandleA**: restituisce un handle al modulo specificato, utile per ottenere informazioni su moduli già caricati.
- **LoadLibraryA**: carica una libreria DLL nel processo chiamante, permettendo di utilizzare funzioni esterne.
- **GetProcAddress**: recupera l'indirizzo di una funzione esportata da una DLL caricata.
- **GlobalAlloc**: alloca memoria globale.
- **GlobalFree**: libera memoria globale precedentemente allocata.
- **CreateThread**: crea un nuovo thread, permettendo operazioni parallele all'interno di un'applicazione.
- **CreateEventW**: crea o apre un evento utilizzato per la sincronizzazione tra thread o processi.
- **WaitForSingleObject**: sospende l'esecuzione del thread finché un oggetto non diventa disponibile.
- **CloseHandle**: chiude un handle aperto, prevenendo perdite di risorse.
- **Sleep**: sospende l'esecuzione del thread per un periodo specificato.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderC
00012360	N/A	00011F94	00011F98	00011F9C
szAnsi	(nFunctions)	Dword	Dword	Dword
msvcrt.dll	26	00012DC8	FFFFFFFF	FFFFFFFF
ADVAPI32.dll	3	00012C0C	FFFFFFFF	FFFFFFFF
OFTs	FTs (IAT)	Hint	Name	
Dword	Dword	Word	szAnsi	
00012E4E	77C11AD8	0052	<a href="#">_CxxFrameHandler</a>	
00012E62	77C119F5	0047	<a href="#">_CxxThrowException</a>	
00012E78	77C0D7F9	0338	<a href="#">wcstoul</a>	
00012E82	77C0C7E6	031A	<a href="#">toupper</a>	
00012E8C	77C33CCE	0326	<a href="#">wcschr</a>	
00012E96	77C33150	02DE	<a href="#">memmove</a>	
00012EA0	77C33DBC	032C	<a href="#">wcslen</a>	
00012EAA	77C32B40	022F	<a href="#">_wcsrev</a>	
00012EB4	77C27B11	00C5	<a href="#">_c_exit</a>	
00012EBE	77C27AEE	00F6	<a href="#">_exit</a>	
00012EC6	77C21269	004E	<a href="#">_XcptFilter</a>	
00012ED4	77C27B00	00C8	<a href="#">_cexit</a>	
00012EDE	77C27ADC	028F	<a href="#">exit</a>	
00012EE6	77C4C7A8	00A8	<a href="#">_acmdln</a>	
00012EF0	77C0E909	006D	<a href="#">_getmainargs</a>	
00012F00	77C279DB	013A	<a href="#">_initterm</a>	
00012F0C	77C38F60	009A	<a href="#">_setusermatherr</a>	
00012F20	77C4D388	00B6	<a href="#">_adjust_fdiv</a>	
00012F30	77C0EB4A	0080	<a href="#">_p_commode</a>	
00012F40	77C0EB68	0085	<a href="#">_p_fmode</a>	
00012F4E	77C23632	0098	<a href="#">_set_app_type</a>	
00012F6C	77C18933	0012	<a href="#">??3@YAXPAX@Z</a>	
00012F7C	77C10C58	0010	<a href="#">??1type_info@@UAE@XZ</a>	
00012F94	77C3A658	00D6	<a href="#">_controlfp</a>	
00012FA2	77C23EB0	00ED	<a href="#">_except_handler3</a>	
00012FB6	77C1197B	0034	<a href="#">?terminate@@YAXXZ</a>	

## LIBRERIA MSVCRT

è una libreria che contiene funzioni della libreria runtime del linguaggio C, utilizzate da molte applicazioni per compiti comuni come la gestione delle stringhe, l'allocazione di memoria, la gestione delle eccezioni, e altro ancora.

Qui sotto elenchiamo le funzioni più importanti contenute in essa:

- **memmove**: copia sicura di memoria che gestisce sovrapposizioni tra sorgente e destinazione, cruciale per la manipolazione della memoria.
- **wcstoul**: converte stringhe in numeri, utile per gestire dati numerici in Unicode, ovvero che assegna un numero univoco a ogni carattere, simbolo, o elemento di testo.
- **Funzioni di gestione dell'errore:**
  - **\_CxxFrameHandler / \_CxxThrowException**: gestione delle eccezioni in C++, fondamentali per il controllo degli errori nelle applicazioni C++.
  - **\_XcptFilter**: filtra e gestisce eccezioni specifiche, importante per un controllo preciso sugli errori.
- **Funzioni di chiusura:**
  - **\_exit**: termina immediatamente il programma senza pulire risorse, usato per chiusure rapide.
  - **exit**: termina il programma dopo aver eseguito operazioni di pulizia come chiudere file aperti. Essenziale per una terminazione pulita.
  - **terminate**: termina il programma in modo anomalo, utilizzato in caso di eccezioni non gestite.

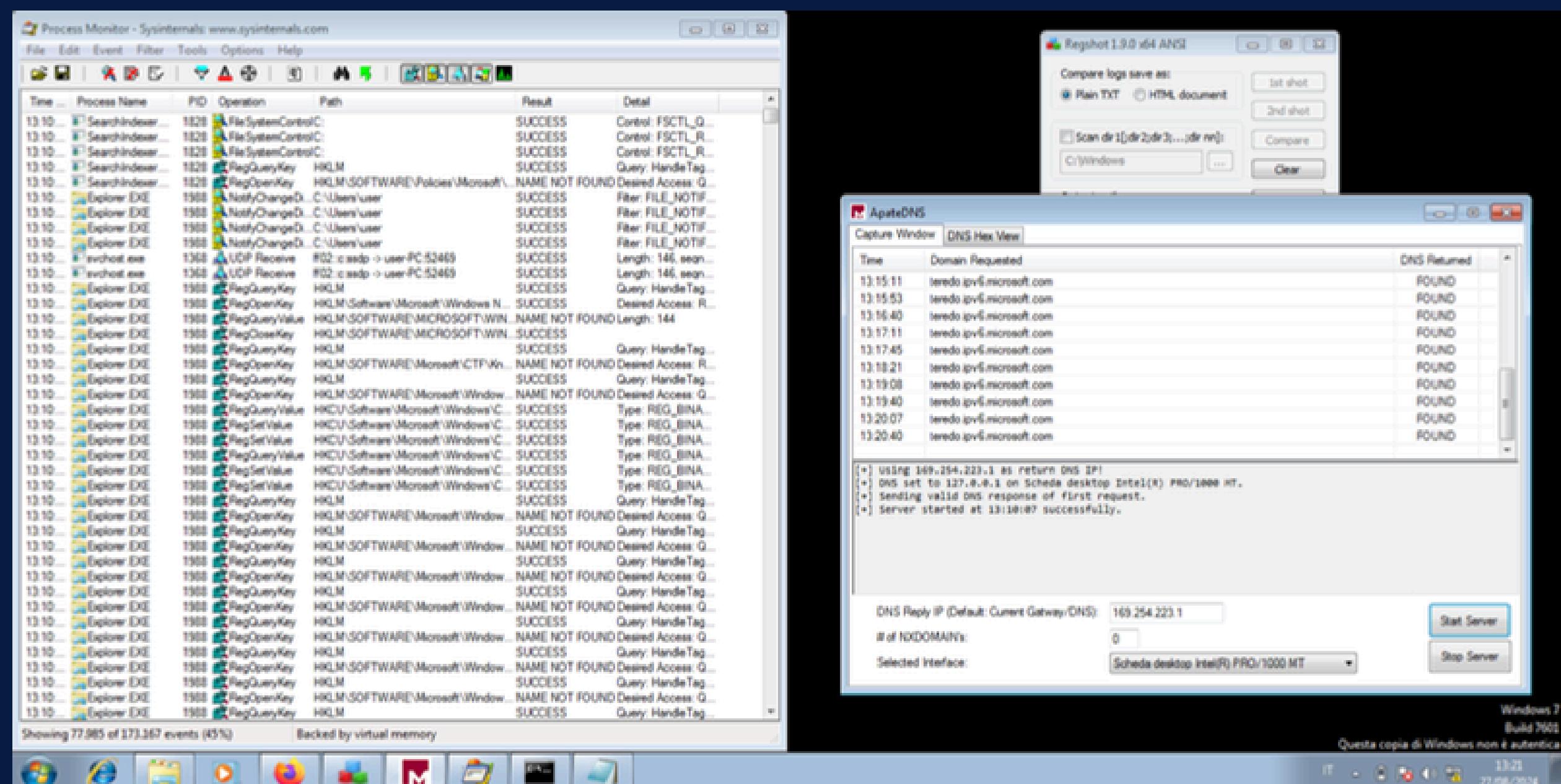
## LIBRERIA ADVAPI32

è una libreria che contiene funzioni che sono fondamentali per la gestione del registro di sistema di Windows. Nello specifico:

- **RegOpenKeyExA**: apre una chiave del registro specificata, è utilizzata per ottenere un handle a una chiave del registro, necessario per leggere o modificare le sue voci.
- **RegQueryValueExA**: recupera i dati associati a un valore specifico all'interno di una chiave del registro aperta, serve per leggere il contenuto delle voci di registro.
- **RegCloseKey**: chiude una chiave del registro aperta, rilasciando l'handle associato, è importante per prevenire perdite di risorse.

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
000123FC	N/A	00011FA8	00011FAC	00011FB0	00011FB4	00011FB8
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
msvcrt.dll	26	00012DC8	FFFFFFFF	FFFFFFFF	00012F60	000011BC
ADVAPI32.dll	3	00012C0C	FFFFFFFF	FFFFFFFF	00012FFC	00001000
KERNEL32.dll	30	00012C2C	FFFFFFFF	FFFFFFFF	000131D4	00001020
CORE32.dll	2	00012C1C	FFFFFFFF	FFFFFFFF	0001320C	00001010
OFTs	FTs (IAT)	Hint	Name			
Dword	Dword	Word	szAnsi			
00012FEC	77DC22EA	01E1	RegOpenKeyExA			
00012FD8	77DC23D7	01EB	RegQueryValueExA			
00012FCA	77DC189A	01C8	RegCloseKey			

Nel secondo step andremo ad eseguire un'analisi dinamica sfruttando la combo di tre software: ProcMon, RegShot ed Apate DNS. Il primo software viene utilizzato per visualizzare lo sviluppo di processi all'interno del registro di sistema, il secondo viene utilizzato per analizzare il funzionamento di eseguibili attraverso il compare di due screenshot di registro, ante e post esecuzione del file, ed il terzo software invece viene utilizzato per creare un ambiente di test isolato volto a manipolare le richieste DNS del Malware ad un applicazione durante l'analisi.



Mentre con Apate DNS, non abbiamo potuto visionare il download di **malware.exe**, con ProcMon abbiamo catturato tutti i processi catturati dal Malware.

Con RegShot abbiamo invece catturato, tramite comparazione degli screenshot, tutte le modifiche di registro effettuate dal Malware.

Time ...	Process Name	PID	Operation	Path	Result	Detail
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	Access: Q...	
18:58:...	calcolatriceinnovativa50.exe	3588	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVers... NAME NOT FOUND Length: 1.024		
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Mana...	REPARSE	Desired Access: R...
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Mana...	SUCCESS	Desired Access: R...
18:58:...	calcolatriceinnovativa50.exe	3588	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MA...	NAME NOT FOUND Length: 1.024	
18:58:...	calcolatriceinnovativa50.exe	3588	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MA...	SUCCESS	
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\hivelist	REPARSE	Desired Access: R...
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\hivelist	SUCCESS	Desired Access: R...
18:58:...	calcolatriceinnovativa50.exe	3588	RegQueryValue	HKLM\System\CurrentControlSet\Control\hivelist\Regist...	SUCCESS	Type: REG_SZ, Le...
18:58:...	calcolatriceinnovativa50.exe	3588	RegCloseKey	HKLM\System\CurrentControlSet\Control\hivelist	SUCCESS	
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT FOUND Desired Access: Q...	
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\... REPARSE		Desired Access: Q...
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVers...	SUCCESS	Desired Access: Q...
18:58:...	calcolatriceinnovativa50.exe	3588	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVers...	SUCCESS	KeySetInformation...
18:58:...	calcolatriceinnovativa50.exe	3588	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVers... NAME NOT FOUND Length: 1.024		
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Mana...	REPARSE	Desired Access: R...
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Mana...	SUCCESS	Desired Access: R...
18:58:...	calcolatriceinnovativa50.exe	3588	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\SESSION MA...	SUCCESS	KeySetInformation...
18:58:...	calcolatriceinnovativa50.exe	3588	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MA... NAME NOT FOUND Length: 1.024		
18:58:...	calcolatriceinnovativa50.exe	3588	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MA...	SUCCESS	
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Q...
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND Desired Access: Q...	
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srv\GP\DLL	REPARSE	Desired Access: R...
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srv\GP\DLL	NAME NOT FOUND Desired Access: R...	
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Win...	REPARSE	Desired Access: Q...
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\...	SUCCESS	Desired Access: Q...
18:58:...	calcolatriceinnovativa50.exe	3588	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\...	SUCCESS	KeySetInformation...
18:58:...	calcolatriceinnovativa50.exe	3588	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\... NAME NOT FOUND Length: 80		
18:58:...	calcolatriceinnovativa50.exe	3588	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\...	SUCCESS	
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\Cod...	NAME NOT FOUND Desired Access: Q...	
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Ve...	REPARSE	Desired Access: R...
18:58:...	calcolatriceinnovativa50.exe	3588	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Ve...	SUCCESS	Desired Access: R...

## CHIAVI AGGIUNTE

Durante il periodo di osservazione, sono state aggiunte 21 chiavi al registro di sistema.

Le principali aggiunte includono:

- **Configurazioni di Windows Error Reporting:** creazione di una nuova chiave in HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\Debug.
- **Preferenze di Explorer:** creazione di chiavi relative alla gestione di file con estensione .hiv, comprese associazioni di file e liste di file recenti.
- **Shell Bags:** aggiunta di diverse chiavi relative alle preferenze di visualizzazione delle cartelle in Explorer.

## VALORI AGGIUNTI

Sono stati introdotti 81 nuovi valori nel registro di sistema. Tra i più rilevanti:

- **Regole del Firewall:** aggiunte regole per permettere l'esecuzione del programma apatedns.exe, situato in C:\users\user\Desktop\software malware analysis\apatedns\apatedns.exe.
- **Preferenze di Explorer:** inserimento di valori riguardanti la gestione delle finestre di dialogo per l'apertura e il salvataggio dei file, con registrazione di percorsi visitati e dimensioni delle finestre.



Il file malevolo potrebbe comportare rischi significativi per la stabilità e la sicurezza del sistema legata alla modifica delle chiavi.

I principali problemi includono:

- **Modifiche Involontarie o Malintenzionate:** le modifiche possono essere introdotte da software dannoso o in modo non intenzionale, esponendo il sistema a vulnerabilità. Per evitare eventuali problemi possiamo confrontare le modifiche con configurazioni sicure conosciute ed ignorare quelle sospette eseguendo un'analisi di sicurezza approfondita.
- **Conflitti con Software Esistente:** le nuove chiavi o valori possono entrare in conflitto con configurazioni esistenti, causando malfunzionamenti. In questo caso è consigliato verificare la compatibilità delle modifiche e monitorare il sistema per eventuali anomalie verificatesi.
- **Modifiche non Documentate:** senza una documentazione adeguata, le modifiche possono risultare difficili da tracciare e gestire a lungo termine. Per evitare ciò possiamo documentare dettagliatamente tutte le modifiche, inclusi i motivi e gli impatti previsti, per facilitare la gestione futura del sistema.

Proseguiamo analizzando il secondo file indicato nella traccia, “**AmicoNerd.exe**”, l’iter che andremo a seguire è lo stesso visto pocanzi nell’analisi del file precedente.  
Come primo passo andiamo ad analizzare il file tramite hash con il portale **VirusTotal**.

57 / 74

Community Score -27

57/74 security vendors flagged this file as malicious

c6603d416dfc48894eda35d9a9a8523bd9823e215ab926783ce6848aa8a62c4

AutoPico.exe

Size 722.69 KB | Last Analysis Date 1 month ago | EXE

peexe revoked-cert runtime-modules via-tor signed overlay invalid-signature direct-cpu-clock-access assembly long-sleeps detect-debug-environment checks-network-adapters calls-wmi

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 20+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: hacktool.autokms/rpchook Threat categories: hacktool trojan pua Family labels: autokms rpchook kmsactivator

Security vendors' analysis	Do you want to automate checks?		
AhnLab-V3	HackTool/Win.AutoKMS.C948312	AllCloud	Hacktool:MSIL/Idlekms.C
ALYac	Application.Hacktool.KMSActivator.AQ	Antiy-AVL	RiskWare[NetTool]/Win64.RPCHook
Arcabit	Application.Hacktool.KMSActivator.AQ	Avast	Win32:MiscX-gen [PUP]
AVG	Win32:MiscX-gen [PUP]	BitDefender	Application.Hacktool.KMSActivator.AQ
BitDefenderTheta	Gen:NN.ZemsilF.36810.Tm1@a8vJERd	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Tool.Kmsactivator-9811695-0	CrowdStrike Falcon	Win/grayware_confidence_100% (W)
Cybereason	Malicious.fd3caf	Cylance	Unsafe

Come possiamo vedere i feedback dei vendor ci danno informazioni univoche anche in questo caso.

Anche in questo caso abbiamo deciso di eseguire una seconda analisi del file utilizzando l'estensione **.zip**. Inserendo il secondo hash nel portale abbiamo avuto questi risultati che ci mostrano risultati differenti da quelli visti pocanzi.

The screenshot shows a VirusShare analysis interface for the file `AmicoNerd.zip`. The file has a **Community Score** of **48 / 69**, with **48/69 security vendors flagged this file as malicious**. The file hash is `9e3f672d0de2ae92ea109cab0688efc35bf93304b8112d481afa7975fa15f56`. It was last analyzed **34 minutes ago** and is **310.80 KB** in size. The file is identified as a **ZIP** file. Below the file details, there are tabs for **DETECTION**, **DETAILS**, **RELATIONS**, **BEHAVIOR**, and **COMMUNITY**. The **DETECTION** tab is selected, showing a message to join the community for additional insights. Below this, it lists popular threat labels, threat categories, and family labels. The **Security vendors' analysis** section lists vendor detections and their corresponding threat labels. A link to automate checks is also present.

Vendor	Detection	Threat Label	Family Label
AhnLab-V3	HackTool/Win.AutoKMS.C948312	ALYac	Application.Hacktool.KMSActivator.AQ
Antiy-AVL	RiskWare[NetTool]/Win64.RPCHook	Arcabit	Application.Hacktool.KMSActivator.AQ
Avast	Win32:MiscX-gen [PUP]	AVG	Win32:MiscX-gen [PUP]
BitDefender	Application.Hacktool.KMSActivator.AQ	BitDefenderTheta	Gen:NN.Zemniff.36812.Tm1@abv.JERd
ClamAV	Win.Tool.Kmsactivator-9811695-0	DeepInstinct	MALICIOUS
Elastic	Malicious (high Confidence)	Emsisoft	Application.Hacktool.KMSActivator.AQ (B)
eScan	Application.Hacktool.KMSActivator.AQ	ESET-NOD32	A Variant Of MSIL/HackToolIdleKMS.E P...
Fortinet	Riskware/RPCHook	GData	MSIL.Application.HackKMS.X

Ecco le informazioni ottenute dalla seconda analisi:

- **RILEVAMENTI ANTIVIRUS:**
  - 48 su 69 motori antivirus hanno rilevato il file come malevolo.
- **CATEGORIE DI MINACCE:**
  - **Hacktool**: strumenti progettati per bypassare la sicurezza, come attivatori di software o strumenti per ottenere accesso non autorizzato.
  - **Trojan**: Malware che si maschera da software legittimo per ingannare l'utente ed eseguire attività malevole.
  - **PUA** (Potentially Unwanted Application): software che, pur non essendo necessariamente malevolo, può eseguire attività indesiderate come pubblicità invasive o modifiche alle impostazioni del sistema.
- **ETICHETTE DI FAMIGLIA:**
  - **kmsactivator**: fa riferimento a strumenti utilizzati per attivare illegalmente software Microsoft tramite **KMS** (Key Management Service).
  - **autokms**: una variante di *hacktool* che automatizza l'attivazione del software tramite KMS.
  - **rpchook**: indica la presenza di strumenti che possono manipolare o intercettare chiamate di procedura remota (RPC), spesso utilizzati in contesti di attacco.

Possiamo quindi dire che il file è considerato altamente sospetto e pericoloso, associato a strumenti di hacking e potenziali Trojan. Si raccomanda vivamente di eliminare il file e di non eseguirlo, in quanto potrebbe compromettere la sicurezza del sistema.

Altre informazioni relative al malware sono i Dropped Files (nella prima immagine) ed informazioni generiche inerenti l'History ed i vari nomi affibbiati allo stesso (seconda immagine).

Dropped Files (12) ⓘ				History ⓘ	Names ⓘ
Scanned	Detections	File type	Name		
2024-08-28	43 / 75	Win32 DLL	SECOH-QAD.dll		
2024-07-19	0 / 64	Text	software.log		
2024-08-28	45 / 74	Win32 EXE	SECOH-QAD.exe		
?	?	file	0398221231CFF97E1FDC03D357AC4610AFB8F3CDDE4C90A9EC4	Creation Time	2015-09-27 03:54:08 UTC
?	?	file	246d63c252011537a5079fa68a29570905c8718f3379158f2f51a63	Signature Date	2015-09-27 03:55:00 UTC
?	?	file	564f08220cdab8837ce130cdeef8a399d3d3e24e0e109c1e08613	First Seen In The Wild	2015-03-10 15:50:41 UTC
?	?	file	9896A6FCB9BB5AC1EC5297B4A65BE3F647589ADF7C37B45F3F7	First Submission	2015-09-27 08:33:35 UTC
?	?	file	9896A6FCB9BB5AC1EC5297B4A65BE3F647589ADF7C37B45F3F7	Last Submission	2024-08-29 07:50:20 UTC
?	?	file	cffba1abe8b970c7f49c9a6010fd3e421678a079ed88cb6d52837ee6	Last Analysis	2024-07-19 18:57:24 UTC
?	?	file	fcde47d984458d9b8c0e3e4f5d00318648cb83a7ae1f02694b5901		
2024-05-21	50 / 74	Win32 EXE	aquel.bin		AmicoNerd.exe
2024-01-28	2 / 70	Win32 DLL	aquel64.bin		AutoPico.exe
2024-02-17	3 / 66	Win32 DLL	aquel32.exe		AutoPico.exe (copy)
					autopico.exe
					svchost.exe
					_cache_%SAMPLENAME%
					_cache_pPvKPUSm1N.exe
					_cache_b8b8eefb760dce0c52a39fa63edc0c67.exe
					c6603d416dfc48894eda35d9a9a8523bdf9823e215ab926783ce6848aa8a62c4-dropped.bin
					setup.exe

Infine, possiamo anche analizzare gli Execution Parents e PE Resource Parents. Ecco cosa significano e cosa fanno queste sezioni:

- **Execution Parents:**

- Questa sezione elenca i file o i processi che hanno avviato o eseguito il file in questione. In altre parole, mostra quali sono i "genitori" del processo analizzato, cioè quali altri file o applicazioni hanno eseguito o lanciato il file analizzato.
- Gli "Execution Parents" sono cruciali per comprendere la catena di esecuzione e come un file potenzialmente malevolo è stato eseguito sul sistema. Se un file sospetto è stato lanciato da un archivio .rar o da un altro file .exe con una cattiva reputazione, questo può essere un indicatore che il file stesso è malevolo o è parte di una catena di infezione.

- **PE Resource Parents:**

- Questa sezione riguarda le risorse di codice o i componenti utilizzati all'interno del file eseguibile analizzato. "PE" sta per Portable Executable, che è il formato dei file eseguibili su Windows. I "PE Resource Parents" indicano i file o le risorse da cui il file eseguibile ha ereditato o utilizzato porzioni di codice o risorse.
- L'analisi delle risorse PE può rivelare se il file utilizza risorse note per essere associate a malware. Se un file ha utilizzato risorse da un eseguibile già noto per essere malevolo (come Synaptics.exe nell'immagine), questo aumenta la probabilità che il file analizzato possa essere compromesso o malevolo.

### Execution Parents (83) ⓘ

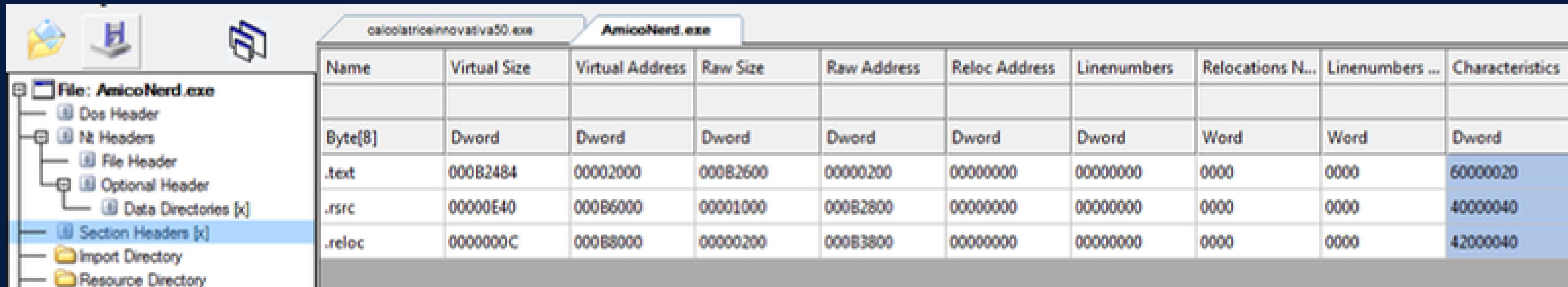
Scanned	Detections	Type	Name
2021-01-22	38 / 59	RAR	KMSpico Portable.rar
2024-04-04	62 / 72	Win32 EXE	02a61c55e9840488143d5afb0612aaef2e0345369cef19af57b12ceaadc532604
2022-05-09	56 / 69	Win32 EXE	9ebac1194004bfa09417a09670620ebe.virus
2024-08-05	45 / 71	ZIP	KMSpicoACTIVAWINDOS10JULIO2024.zip
2023-08-25	46 / 71	Win32 EXE	unknown
2021-04-30	38 / 58	RAR	11-KMSpico Portable.rar
2022-08-22	38 / 61	RAR	KMSpico 10.1.7 Portable - mhktbbricks.net.rar
2020-02-15	35 / 61	RAR	50076326
2022-12-29	32 / 59	RAR	KMSpico Portable.rar
2024-08-04	52 / 73	Win32 EXE	KMSpico_setup.exe

• • •

### PE Resource Parents (1) ⓘ

Scanned	Detections	Type	Name
2023-02-02	63 / 70	Win32 EXE	Synaptics.exe

Continuiamo l'analisi con **CFF Explorer**, andando ad esaminare il contenuto del file.



The screenshot shows the CFF Explorer interface. On the left, a tree view displays the file structure of 'AmicoNerd.exe' with nodes for Dos Header, NT Headers, File Header, Optional Header, Data Directories, Section Headers, Import Directory, and Resource Directory. The 'Section Headers' node is currently selected. On the right, a table provides detailed information for each section:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000B2484	00002000	000B2600	00000200	00000000	00000000	0000	0000	60000020
.rsrc	00000E40	000B6000	00001000	000B2800	00000000	00000000	0000	0000	40000040
.reloc	0000000C	000B8000	00000200	000B3800	00000000	00000000	0000	0000	42000040

Queste che vediamo nell'immagine sono le sezioni presenti nel file che in questo caso vedono:

- **.text**: contiene il codice eseguibile. È la sezione principale del programma, con istruzioni eseguibili;
- **.rsrc**: contiene le risorse dell'applicazione, come icone e stringhe;
- **.reloc**: gestisce le informazioni per la rilocazione del codice in memoria.

Visualizziamo ora le directory contenenti le librerie importate dal file.

calcolatriceinnovativa50.exe		AmicoNerd.exe					
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)	
000B266E	N/A	000B2624	000B2628	000B262C	000B2630	000B2634	
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword	
mscoree.dll	1	000B444C	00000000	00000000	000B446E	00002000	

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
000B4460	000B4460	0000	_CorExeMain

L'immagine qui sopra elenca le librerie esterne necessarie per l'esecuzione dell'applicazione.

In questo caso, viene importata una sola libreria:

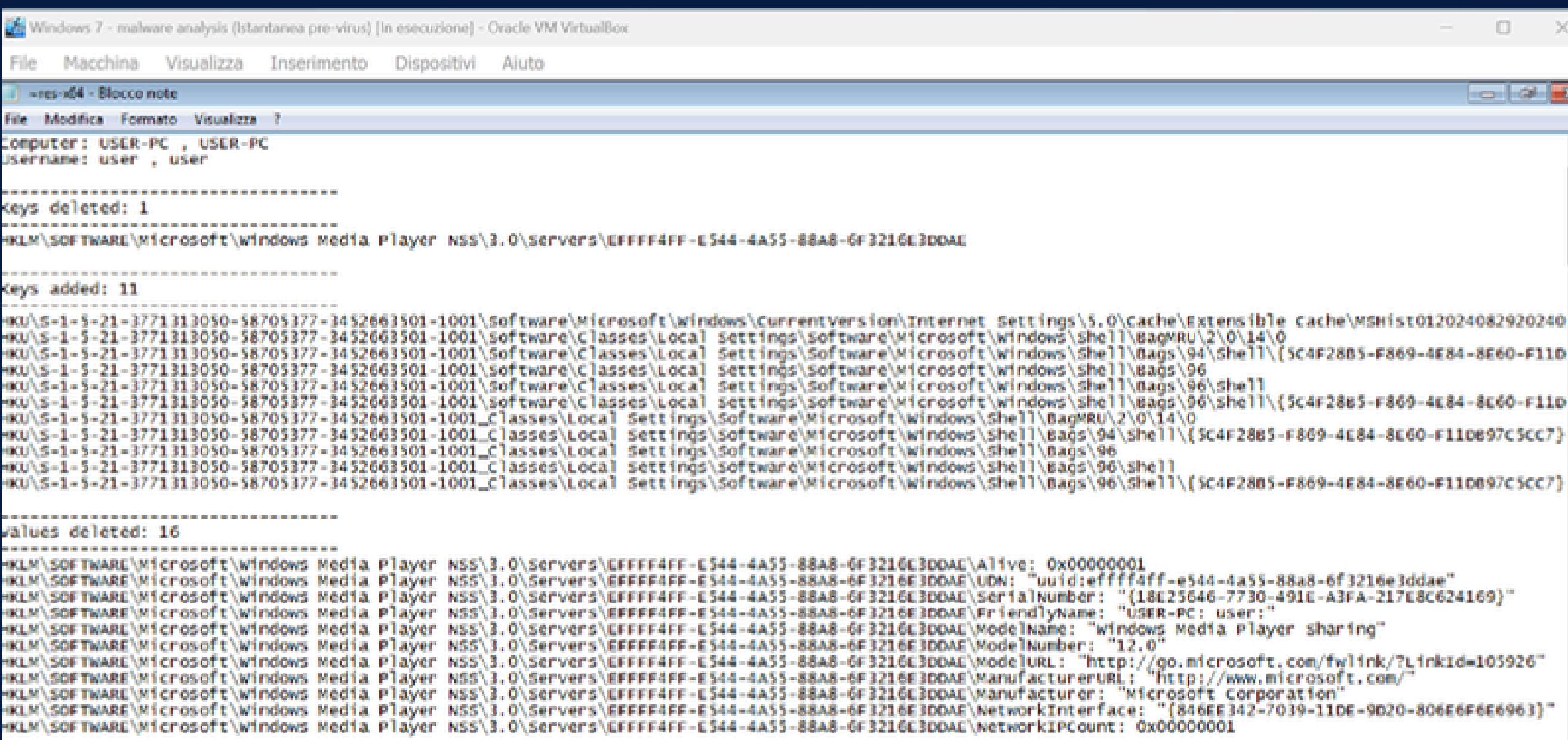
- **mscoree.dll**: questa è una libreria essenziale per l'esecuzione di applicazioni .NET. La funzione principale importata, \_CorExeMain, è il punto di ingresso per le applicazioni gestite (.NET), avviando il Common Language Runtime (CLR) per l'esecuzione del codice.

Quando un'applicazione .NET viene eseguita, il sistema operativo utilizza questa funzione per avviare l'esecuzione del codice gestito, passando dal codice nativo al codice gestito.

"\_CorExeMain" avvia l'applicazione .NET preparando l'ambiente di esecuzione e invocando il metodo Main() dell'applicazione.

In sostanza, questa funzione è cruciale per l'inizializzazione e l'esecuzione delle applicazioni .NET all'interno del runtime gestito.

Proseguiamo, anche con questo file malevolo, con il secondo step di analisi utilizzando la combinazione di software vista precedentemente; dopo aver effettuato entrambi gli screenshot del registro di sistema siamo passati a confrontarli ed abbiamo potuto valutare le modifiche effettuate dal Malware.



The screenshot shows a Windows 7 desktop with a VirtualBox window titled "Windows 7 - malware analysis (Instantanea pre-virus) [In esecuzione] - Oracle VM VirtualBox". Inside the window, a Notepad application is open with the title "-res-x64 - Blocco note". The content of the Notepad is a registry dump from the registry key "HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Server\{EFFFF4FF-E544-4A55-88A8-6F3216E3DDAE}":

```
Computer: USER-PC , USER-PC
Username: user , user

-----
keys deleted: 1
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240

-----
keys added: 11
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Shell\BagMRU\2\0\14\0
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Shell\Bags\94\Shell\{(5C4F28B5-F869-4E84-8E60-F11D
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Shell\Bags\96\Shell\{(5C4F28B5-F869-4E84-8E60-F11D

-----
values deleted: 16
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\Alive: 0x00000001
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\UDN: "uuid:effff4ff-e544-4a55-88a8-6f3216e3ddae"
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\SerialNumber: "(18E25646-7730-491E-A3FA-217E8C624169)"
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\FriendlyName: "USER-PC: user"
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\ModelName: "Windows Media Player Sharing"
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\ModelNumber: "12.0"
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\ModelURL: "http://go.microsoft.com/fwlink/?LinkId=105926"
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\ManufacturerURL: "http://www.microsoft.com/"
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\Manufacturer: "Microsoft Corporation"
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\NetworkInterface: "{846FF342-7039-11DE-9D20-806E6F6E6963}"
-HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible cache\MSHist012024082920240\NetworkIPCount: 0x00000001
```

Nello specifico possiamo identificare le modifiche chiave e rilevanti.

- **CHIAVI DI REGISTRO ELIMINATE**

È stata eliminata una chiave di registro situata in HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Servers\. Questa chiave è specificamente associata a un server identificato dal GUID EFFFF4FF-E544-4A55-88A8-6F3216E3DDAE.

- **CHIAVI DI REGISTRO AGGIUNTE**

Sono state aggiunte 11 nuove chiavi di registro sotto l'hive HKU (HKEY\_USERS). Queste chiavi riguardano principalmente configurazioni di Windows, come le impostazioni della shell e della cronologia di navigazione (Shell\Bags e Shell\BagMRU). Questi percorsi indicano modifiche ai dati dell'interfaccia utente e alle configurazioni personalizzate dell'utente.

- **VALORI DI REGISTRO ELIMINATI**

Sono stati eliminati 16 valori di registro, tutti associati alla chiave HKLM\SOFTWARE\Microsoft\Windows Media Player NSS\3.0\Servers\. I valori eliminati includevano dettagli specifici del server, come lo stato di attività (Alive), il numero di serie (SerialNumber), e informazioni sul modello (ModelName), tra gli altri. Queste eliminazioni suggeriscono un tentativo di rimuovere tracce di configurazioni legate a Windows Media Player.

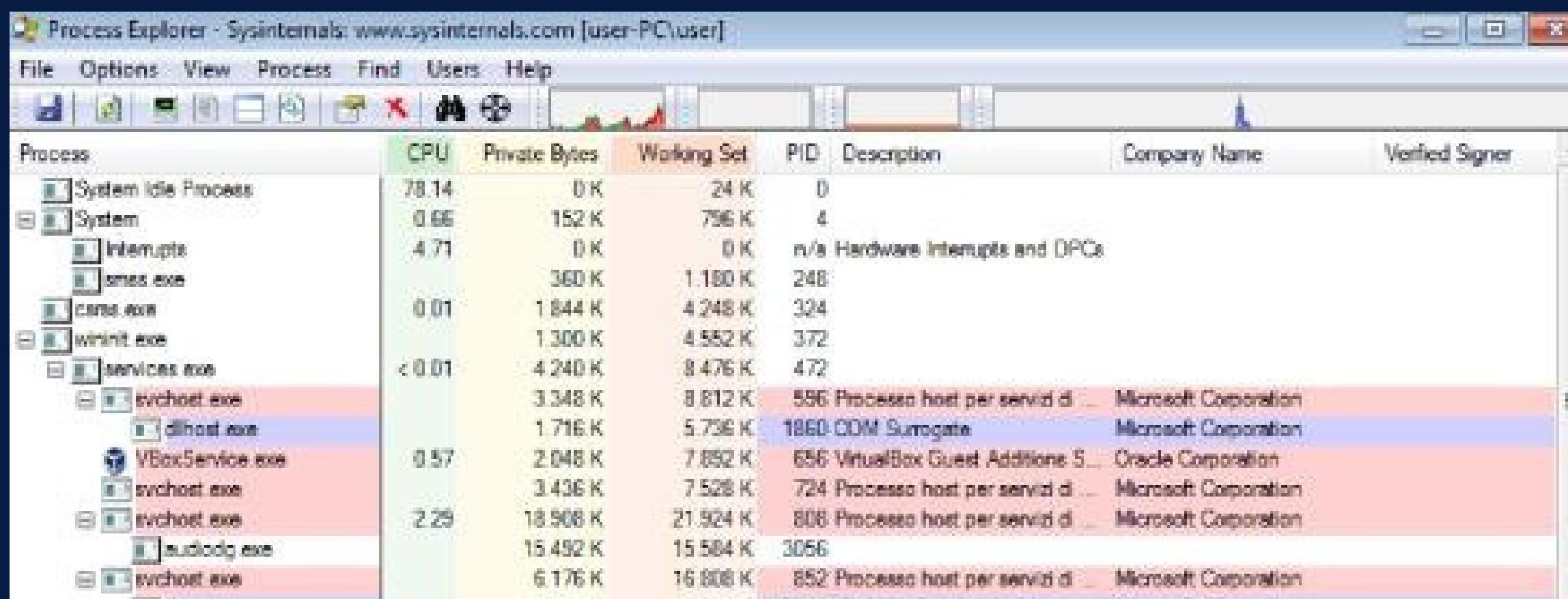
In conclusione possiamo conferare che, le modifiche evidenziate indicano che il malware ha tentato di manipolare il sistema attraverso la rimozione di informazioni cruciali e l'aggiunta di nuove configurazioni nel registro. Le chiavi e i valori modificati sono associati a componenti essenziali di Windows Media Player e a configurazioni dell'interfaccia utente, suggerendo un tentativo di mascherare attività malevole e di garantire la persistenza del malware nel sistema.

Analizzando il malware con ProcMon possiamo raccogliere altre informazioni utili a comprendere il funzionamento del malware:

Time	Process Name	PID	Operation	Path	Result
11:25...	AmicoNerd.exe	3788	RegQueryKey	HKLM	SUCCESS
11:25...	AmicoNerd.exe	3788	RegOpenKey	HKLM\Software\Microsoft\.NETFramework	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryValue	HKLM\SOFTWARE\Microsoft\.NETFramework\InstallRoot	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryValue	HKLM\SOFTWARE\Microsoft\.NETFramework\InstallRoot	SUCCESS
11:25...	AmicoNerd.exe	3788	RegCloseKey	HKLM\SOFTWARE\Microsoft\.NETFramework	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryKey	HKLM	SUCCESS
11:25...	AmicoNerd.exe	3788	RegOpenKey	HKLM\Software\Microsoft\.NETFramework	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryValue	HKLM\SOFTWARE\Microsoft\.NETFramework\InstallRoot	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryValue	HKLM\SOFTWARE\Microsoft\.NETFramework\InstallRoot	SUCCESS
11:25...	AmicoNerd.exe	3788	RegCloseKey	HKLM\SOFTWARE\Microsoft\.NETFramework	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryKey	HKLM	SUCCESS
11:25...	AmicoNerd.exe	3788	RegOpenKey	HKLM\Software\Microsoft\.NETFramework	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryValue	HKLM\SOFTWARE\Microsoft\.NETFramework\CLRLoadLogDir	NAME NOT FOUND
11:25...	AmicoNerd.exe	3788	RegCloseKey	HKLM\SOFTWARE\Microsoft\.NETFramework	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryKey	HKLM	SUCCESS
11:25...	AmicoNerd.exe	3788	RegOpenKey	HKLM\Software\Microsoft\.NETFramework	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryValue	HKLM\SOFTWARE\Microsoft\.NETFramework\InstallRoot	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryValue	HKLM\SOFTWARE\Microsoft\.NETFramework\InstallRoot	SUCCESS
11:25...	AmicoNerd.exe	3788	RegCloseKey	HKLM\SOFTWARE\Microsoft\.NETFramework	SUCCESS
11:25...	AmicoNerd.exe	3788	RegOpenKey	HKLM\System\CurrentControlSet\Control\Error Message Instrument\	REPARSE
11:25...	AmicoNerd.exe	3788	RegOpenKey	HKLM\System\CurrentControlSet\Control\Error Message Instrument	NAME NOT FOUND
11:25...	AmicoNerd.exe	3788	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\GРЕ_Initialize	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GРЕ_Initialize\DisableMetaFiles	NAME NOT FOUND
11:25...	AmicoNerd.exe	3788	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GРЕ_Initialize	SUCCESS
11:25...	AmicoNerd.exe	3788	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS
11:25...	AmicoNerd.exe	3788	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\AmicoNerd	NAME NOT FOUND
11:25...	AmicoNerd.exe	3788	RegCloseKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS
11:25...	AmicoNerd.exe	3788	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\VME Compatibility	NAME NOT FOUND
11:25...	AmicoNerd.exe	3788	RegCloseKey	HKLM	SUCCESS

- **ACCESSO AL REGISTRO DI SISTEMA:**
  - Il processo esegue numerose operazioni di lettura (RegQueryKey, RegQueryValue) e apertura (RegOpenKey) di chiavi di registro relative a vari componenti del sistema, in particolare legate a .NET Framework.
  - Sta leggendo le chiavi sotto il percorso HKLM\Software\Microsoft\.NETFramework\InstallRoot, che è tipicamente usato per verificare l'installazione e la configurazione di .NET Framework sul sistema.
- **TENTATIVI DI ACCESSO A CHIAVI NON ESISTENTI:**
  - Alcune delle operazioni falliscono con il risultato “NAME NOT FOUND”, indicando che il processo sta cercando chiavi di registro che non esistono, come “CLRLoadLogDir”, che potrebbe essere un tentativo di verificare la configurazione o lo stato del sistema in relazione a .NET Framework.
- **COMPATIBILITÀ E INIZIALIZZAZIONE DI GRE (GRAPHICS RENDERING ENGINE):**
  - Il processo accede a chiavi di registro relative alla compatibilità (Compatibility32) e alla disabilitazione di file di metafile (DisableMetaFiles) sotto HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE\_Initialize. Queste operazioni possono essere indicative di un tentativo di manipolare la configurazione di compatibilità o altri aspetti legati alla grafica del sistema.
- **COMPORTAMENTO TIPICO O SOSPETTO:**
  - Questo comportamento potrebbe essere parte del normale funzionamento di un'applicazione legittima che sta verificando la configurazione del sistema prima di eseguire. Tuttavia, se AmicoNerd.exe è un malware, queste operazioni potrebbero indicare un tentativo di raccogliere informazioni sul sistema, in particolare riguardo alla configurazione del .NET Framework, o di manipolare impostazioni critiche per compromettere il sistema.

Per dimostrare al nostro collega che il file **amiconerd.exe** sia veramente un file malevolo, abbiamo deciso di eseguire un'analisi extra utilizzando il software **Process Explorer**, che è uno strumento avanzato di monitoraggio per Windows che fornisce dettagli sui processi in esecuzione, incluso l'uso di CPU, memoria e risorse di sistema.



The screenshot shows the Process Explorer interface with the following data:

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Verified Signer
System Idle Process	78.14	0 K	24 K	0			
System	0.66	152 K	796 K	4			
Interrupt	4.71	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		360 K	1.180 K	248			
csrss.exe	0.01	1.844 K	4.248 K	324			
wininit.exe		1.300 K	4.552 K	372			
services.exe	< 0.01	4.240 K	8.476 K	472			
svchost.exe		3.348 K	8.812 K	586	Processo host per servizi di	Microsoft Corporation	
clhost.exe		1.716 K	5.736 K	1860	COM Surrogate	Microsoft Corporation	
VBoxService.exe	0.57	2.048 K	7.892 K	656	VirtualBox Guest Additions S...	Oracle Corporation	
svchost.exe		3.436 K	7.528 K	724	Processo host per servizi di	Microsoft Corporation	
svchost.exe	2.29	18.508 K	21.924 K	806	Processo host per servizi di	Microsoft Corporation	
audiodg.exe		15.452 K	15.584 K	3056			
svchost.exe		6.176 K	16.808 K	852	Processo host per servizi di	Microsoft Corporation	



Come possiamo vedere dal ritaglio di screenshot, all'avvio del file malevolo oggetto di analisi si crea un processo chiamato **dllhost.exe** che ha come descrizione **COM Surrogate**.

**COM Surrogate** è un processo legittimo su sistemi Windows, identificato come dllhost.exe, utilizzato per eseguire componenti software non integrati direttamente nel sistema operativo, come estensioni per la gestione di file multimediali. Sebbene COM Surrogate non sia di per sé un malware, può essere sfruttato da codice malevolo per eseguire azioni dannose sotto le spoglie di un processo legittimo.

I rischi associati all'uso di COM Surrogate da parte di malware includono l'esecuzione di codice malevolo, la persistenza del malware nel sistema, la compromissione del sistema con privilegi elevati, e il furto di informazioni sensibili.

Per mitigare questi rischi, è essenziale monitorare la posizione del file **dllhost.exe** e utilizzare strumenti di sicurezza per analizzare e verificare i processi associati a COM Surrogate.

## CONCLUSIONI

Attraverso l'uso di strumenti di monitoraggio come ProcMon, è emerso che il malware interagisce intensivamente con il registro di sistema, eseguendo numerose operazioni di lettura e scrittura che possono indicare un tentativo di monitorare o manipolare configurazioni di sistema critiche. Questo comportamento è tipico di malware che cercano di stabilire un controllo persistente sul sistema compromesso.

Il malware effettua modifiche significative al registro di sistema, inclusa l'eliminazione di chiavi e valori critici, suggerendo un tentativo di mascherare la propria presenza e garantire la persistenza nel sistema. In particolare, le modifiche riguardano componenti cruciali come Windows Media Player, alterando configurazioni e rimuovendo tracce di attività, il che potrebbe compromettere la stabilità e la sicurezza del sistema.

Il malware "AmicoNerd.exe" rappresenta una minaccia significativa per la sicurezza del sistema, con funzionalità che spaziano dal bypass delle protezioni di sicurezza alla manipolazione del registro di sistema, fino all'interazione con il runtime di applicazioni .NET, rendendolo un rischio elevato per qualsiasi ambiente in cui venga eseguito.

**Raccomandiamo** quindi, nel caso in cui si entrasse in contatto con questo file, di rimuovere prontamente il Malware e di effettuare scansioni complete del sistema con relative operazioni per garantire la sicurezza dell'uso del device.