



SECURE
SENTINELS

BUILD WEEK 3

LAB REPORT

Team Secure Sentinels
CS0424IT

Table of contents

01

Day 1

- 1.1 Parametri passati
- 1.2 Variabili dichiarate
- 1.3 Sezioni presenti
- 1.4 Librerie importate
- 1.5 Funzione chiamata
- 1.6 Parametri passati
- 1.7 Oggetto rappresentato
- 1.8 Istruzioni comprese
- 1.9 Traduzione in costrutto C
- 1.10 Valore del parametro
- 1.11 Funzionalità implementata

02

Day 2

- 2.1 Analisi con IDA Pro
- 2.2 Analisi con OllyDBG
- 2.3 Analisi con CFF Explorer
- 2.4 Analisi delle funzioni del Main()
- 2.5 Analisi dinamica basica
- 2.6 Process Monitor
- 2.7 Creazione chiave malevola
- 2.8 Funzione che crea il file
- 2.9 Conclusioni

03

Day 3

- 3.1 Traccia
- 3.2 Overview GINA.dll
- 3.3 Conseguenze
- 3.4 Diagramma e analisi
- 3.5 Conclusioni

04

Day 4

- 4.1 Analisi Anyrun 1
- 4.2 Analisi Anyrun 2
- 4.3 Analisi Anyrun 3

05

Day 5

- 5.1 Virus Total Malware 2
- 5.2 CFF Explorer Malware 2
- 5.3 Process Monitor Malware 2
- 5.4 Conclusioni

DAY 1

TRACCIA

Il Malware da analizzare è nella cartella Build_Week_Unit_3 presente sul desktop della macchina virtuale dedicata.

Con riferimento al file eseguibile Malware_Build_Week_U3, rispondere ai seguenti quesiti utilizzando i tool e le tecniche apprese nelle lezioni teoriche:

- 1) Quanti parametri sono passati alla funzione Main()?
- 2) Quante variabili sono dichiarate all'interno della funzione Main()?
- 3) Quali sezioni sono presenti all'interno del file eseguibile? Descrivete brevemente almeno 2 di quelle identificate.
- 4) 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.

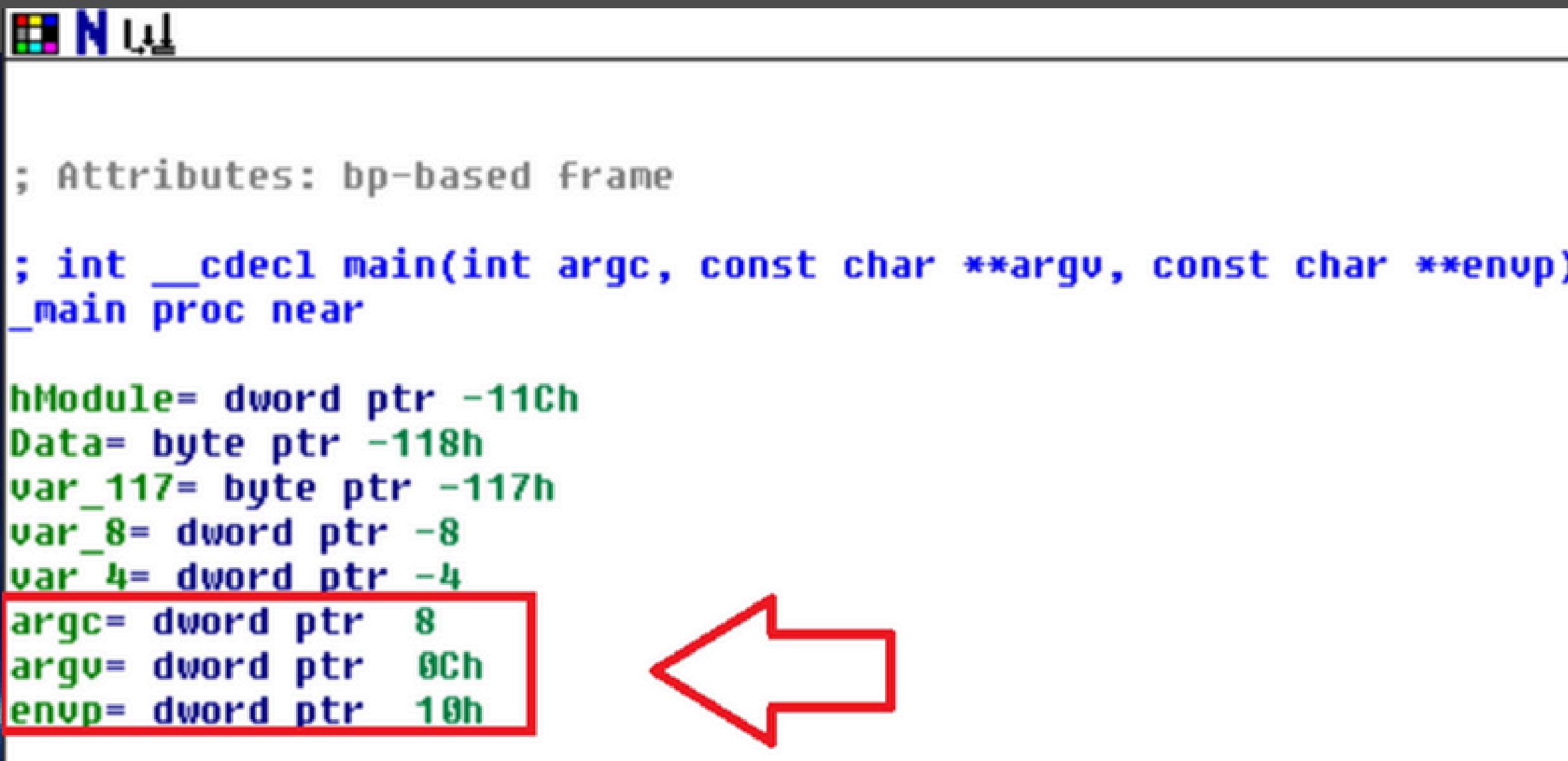
Con riferimento al Malware in analisi, spiegare:

- 5) Lo scopo della funzione chiamata alla locazione di memoria 00401021.
- 6) Come vengono passati i parametri alla funzione alla locazione 00401021.
- 7) Che oggetto rappresenta il parametro alla locazione 00401017.
- 8) Il significato delle istruzioni comprese tra gli indirizzi 00401027 e 00401029 .
(se serve, valutate anche un'altra o altre due righe assembly).
- 9) Con riferimento all'ultimo quesito, tradurre il codice Assembly nel corrispondente costrutto C.
- 10) Valutate ora la chiamata alla locazione 00401047 , qual è il valore del parametro « ValueName»?
- 11) Nel complesso delle due funzionalità appena viste, spiegate quale funzionalità sta implementando il Malware in questa sezione.

1.1. Parametri Passati

Utilizzando il tool IDA Pro possiamo identificare i parametri considerando che essi hanno un offset positivo.

Como abbiamo evidenziato nello screen di seguito, determiniamo che nella funzione Main() sono presenti 3 parametri.



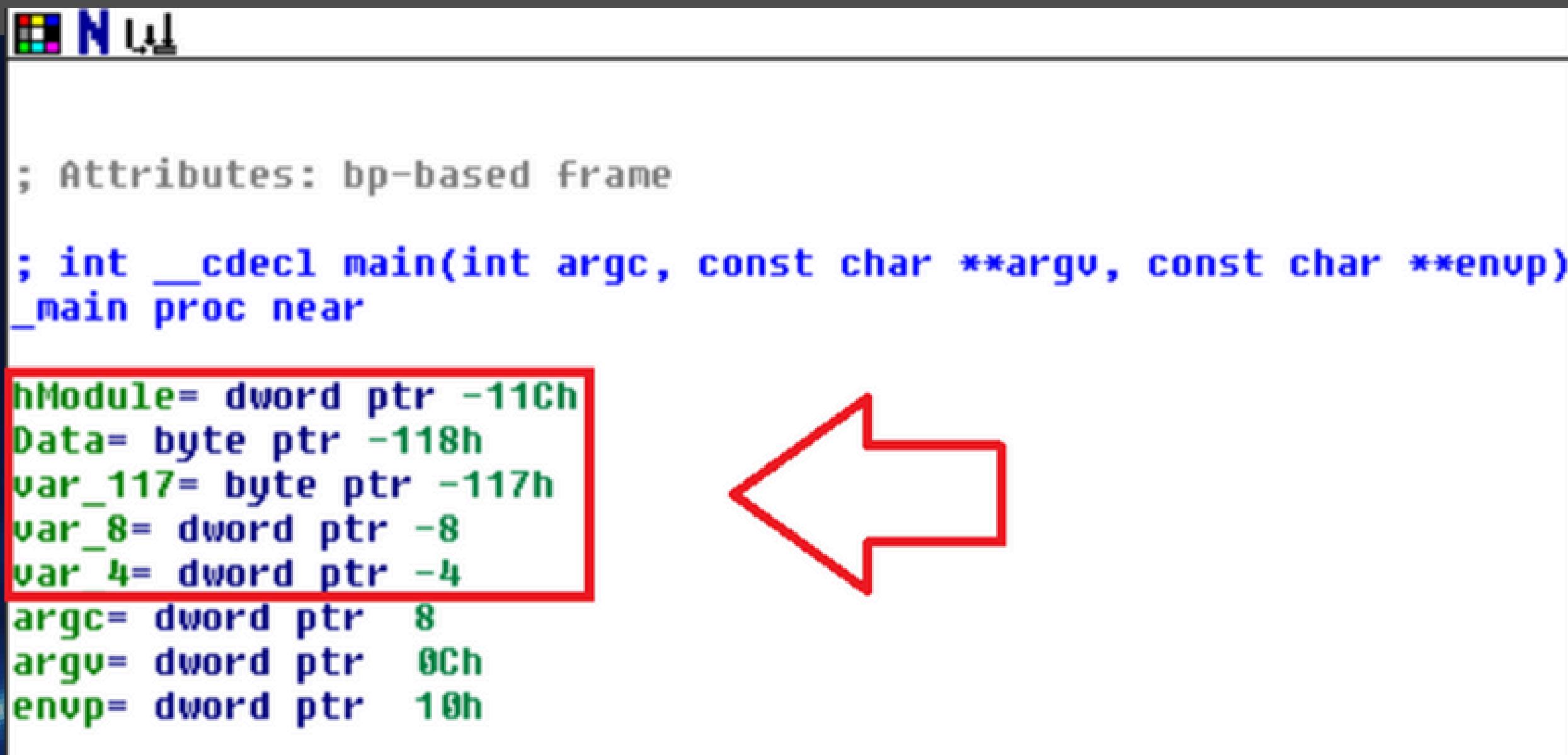
```
; Attributes: bp-based frame
; int __cdecl main(int argc, const char **argv, const char **envp)
_main proc near

hModule= dword ptr -11Ch
Data= byte ptr -118h
var_117= byte ptr -117h
var_8= dword ptr -8
var_4= dword ptr -4
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h
```

1.2. Variabili Dichiarate

Utilizzando il tool IDA Pro possiamo identificare le variabili considerando che esse hanno un offset negativo.

Como abbiamo evidenziato nello screen di seguito, determiniamo che nella funzione Main() sono 5 variabili.



```
; Attributes: bp-based frame
; int __cdecl main(int argc, const char **argv, const char **envp)
_main proc near

hModule= dword ptr -11Ch
Data= byte ptr -118h
var_117= byte ptr -117h
var_8= dword ptr -8
var_4= dword ptr -4
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h
```

1.3. Sezioni Presenti

Utilizzando il tool CFF Explorer possiamo identificare le sezioni del file eseguibile come evidenziamo nello screen di seguito.

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	00005646	00001000	00006000	00001000	00000000	00000000	0000	0000	60000020
.rdata	000009AE	00007000	00001000	00007000	00000000	00000000	0000	0000	40000040
.data	000021A8	00008000	00003000	00008000	00000000	00000000	0000	0000	C0000040
.rsrc	00001A70	0000C000	00002000	0000B000	00000000	00000000	0000	0000	40000040

1.3. Sezioni Presenti

Descrizione delle sezioni identificate:

.text: Questa sezione contiene il codice eseguibile del programma, ossia le istruzioni macchina che verranno eseguite dal processore. È generalmente marcata come di sola lettura ed eseguibile, per prevenire modifiche al codice durante l'esecuzione.

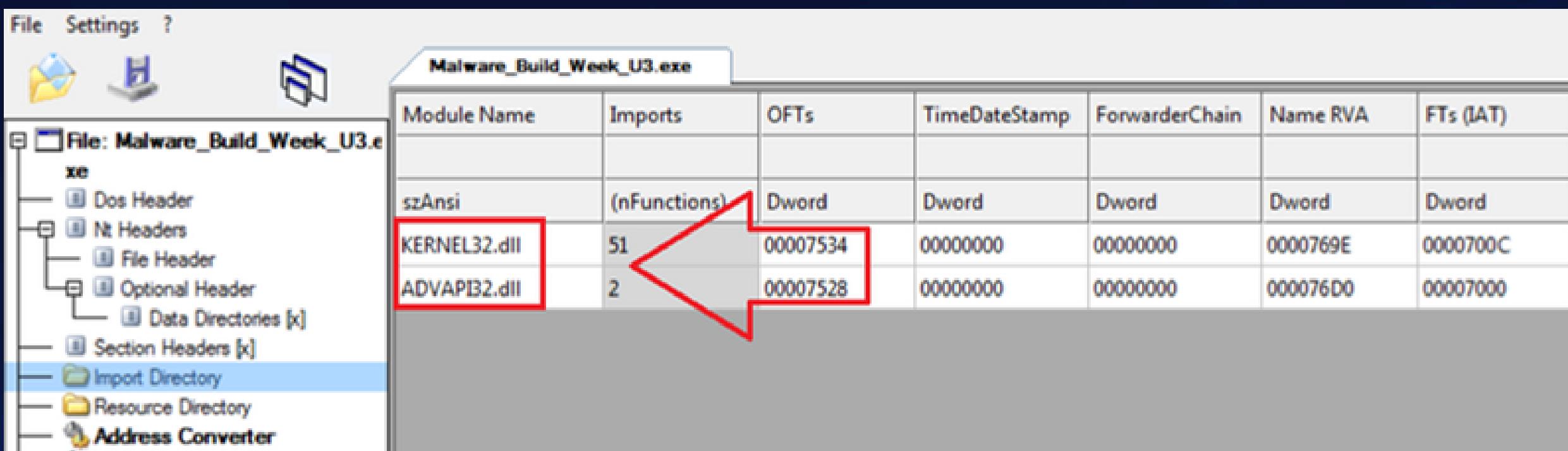
.rdata: Questa sezione .rdata (read-only data) contiene dati di sola lettura, come stringhe costanti, indirizzi di funzione, tabelle di salto, o altre informazioni che il programma utilizza ma non deve modificare durante l'esecuzione.

.data: Questa sezione .data contiene dati modificabili dal programma durante l'esecuzione. In essa si trovano variabili globali e statiche che hanno un valore iniziale definito nel codice. A differenza della sezione .rdata, questa sezione è scrivibile.

.rsrc: Questa sezione .rsrc contiene le risorse del programma, come icone, immagini, stringhe di testo, dialoghi, menu e altre risorse che possono essere utilizzate dal programma durante l'esecuzione. Queste risorse sono generalmente non eseguibili ma leggibili.

1.4. Librerie Importate

Utilizzando il tool CFF Explorer possiamo identificare le librerie importate dal file eseguibile come evidenziamo nello screen di seguito.



Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000

1.4. Librerie Importate

Descrizione delle librerie importate:

KERNEL32.dll: Questa libreria è una delle più essenziali del sistema operativo Windows, responsabile della gestione di molte delle operazioni di base che consentono il funzionamento delle applicazioni. Questa libreria fornisce una serie di funzioni fondamentali come la gestione della memoria, dei processi e dei thread, nonché l'accesso ai file e alle directory. Inoltre, include funzioni per la gestione della console e della sincronizzazione, rendendola cruciale per l'interazione tra il software e l'hardware a basso livello.

ADVAPI32.dll: Questa libreria si occupa di fornire funzioni avanzate per la programmazione delle applicazioni in ambiente Windows, specialmente in ambiti legati alla sicurezza e alla configurazione del sistema. Questa libreria è utilizzata per la gestione delle autorizzazioni e delle politiche di sicurezza, l'accesso e la manipolazione del registro di sistema, la gestione dei servizi di Windows e la criptografia. In sintesi, ADVAPI32.dll è fondamentale per le operazioni che richiedono un controllo più approfondito e sicuro delle risorse del sistema operativo.

1.4. Funzioni Importate

Descrizione delle funzioni importate:

VirtualAlloc / VirtualFree: Queste funzioni sono utilizzate per allocare e liberare memoria in modo dinamico. Un malware potrebbe utilizzare queste funzioni per allocare memoria per il codice dannoso o per nascondere attività malevole.

LoadLibraryA / GetProcAddress: Queste funzioni permettono di caricare dinamicamente altre librerie e ottenere l'indirizzo di funzioni specifiche in esse. Un malware potrebbe caricare librerie aggiuntive per eseguire codice dannoso o ottenere funzioni di sistema critiche.

CreateFileA / WriteFile / ReadFile / SetFilePointer / FlushFileBuffers / SetEndOfFile: Queste funzioni permettono di creare, scrivere, leggere e manipolare file. Un malware potrebbe utilizzarle per modificare file di sistema, rubare informazioni, o installare altri componenti dannosi.

ExitProcess / TerminateProcess: Queste funzioni terminano il processo corrente o un altro processo specificato. Un malware potrebbe utilizzarle per chiudere processi di sicurezza, come antivirus o firewall.

CloseHandle: Questa funzione chiude un handle aperto, che potrebbe essere associato a un file, una risorsa o un processo. Un uso improprio potrebbe portare alla perdita di risorse o all'interruzione di processi critici.

1.4. Funzioni Importate

GetModuleHandleA / GetModuleFileNameA / LoadResource / LockResource / FindResourceA / SizeofResource / FreeResource: Queste funzioni sono utilizzate per gestire moduli e risorse del programma. Un malware potrebbe usarle per manipolare o iniettare codice dannoso in moduli esistenti.

UnhandledExceptionFilter: Questa funzione imposta un gestore per le eccezioni non gestite. Un malware potrebbe utilizzarla per nascondere crash o errori, rendendo più difficile il rilevamento.

HeapCreate / HeapAlloc / HeapReAlloc / HeapFree / HeapDestroy: Queste funzioni gestiscono la memoria heap. Un malware potrebbe usarle per allocare memoria per il proprio codice o per alterare il comportamento del programma.

RegSetValueExA: Questa funzione viene utilizzata per impostare il valore di una chiave di registro. Un malware potrebbe utilizzarla per modificare il registro di sistema in modo da alterare il comportamento del sistema operativo, ad esempio, impostando il malware per eseguire automaticamente all'avvio del sistema, disabilitare funzionalità di sicurezza, o modificare configurazioni critiche.

RegCreateKeyExA: Questa funzione consente di creare una nuova chiave di registro o di aprirne una esistente. Un malware potrebbe usarla per creare nuove chiavi di registro che puntano a codice dannoso, per ottenere persistenza nel sistema, o per modificare impostazioni di sistema in modo dannoso.

1.4. Scansione Virus Total

58 / 75

Community Score

58/75 security vendors flagged this file as malicious

57d8d248a8741176348b5d12dcf29f34c8f48ede0ca13c30d12e5ba0384056d7
Malware_Build_Week_U3.exe

Size: 52.00 KB | Last Analysis Date: 24 days ago | EXE

peaxe checks-user-input spreader armadillo

Detection Details Relations Behavior

Join our Community and enjoy additional community insights & features!

Popular threat label: trojan.doina/totbrick

AhnLab-V3 Trojan/Win32.Agent.C39204 Alibaba Trojan:Win32/Totbrick.48594dcf

AliCloud Trojan:Win/Totbrick.Gen ALYac Gen:Variant.Doina.65814

Anti-AVL Trojan/Win32.Agent Arcabit Trojan.Doina.D10116

Avast Win32:Trojan-gen AVG Win32:Trojan-gen

Avira (no cloud) TR/Agent.53248.465 BitDefender Gen:Variant.Doina.65814

BitDefenderTheta Gen:NN.ZediaF.36810.aq4@a0clrOb Bkav Pro W32.AI Detect Malware

ClamAV Win.Trojan.Agent-595082 CrowdStrike Falcon Win/malicious_confidence_100% (W)

Cybereason Malicious.87a7c5 Cylance Unsafe

Cynet Malicious (score: 99) DeepInstinct MALICIOUS

DrWeb BackDoor.Siggen2.1689 Elastic Malicious (high Confidence)

Emsisoft Gen:Variant.Doina.65814 (B) eScan Gen:Variant.Doina.65814

ESET-NOD32 Win32/Agent.WOU Fortinet W32/Agent.WOU!tr

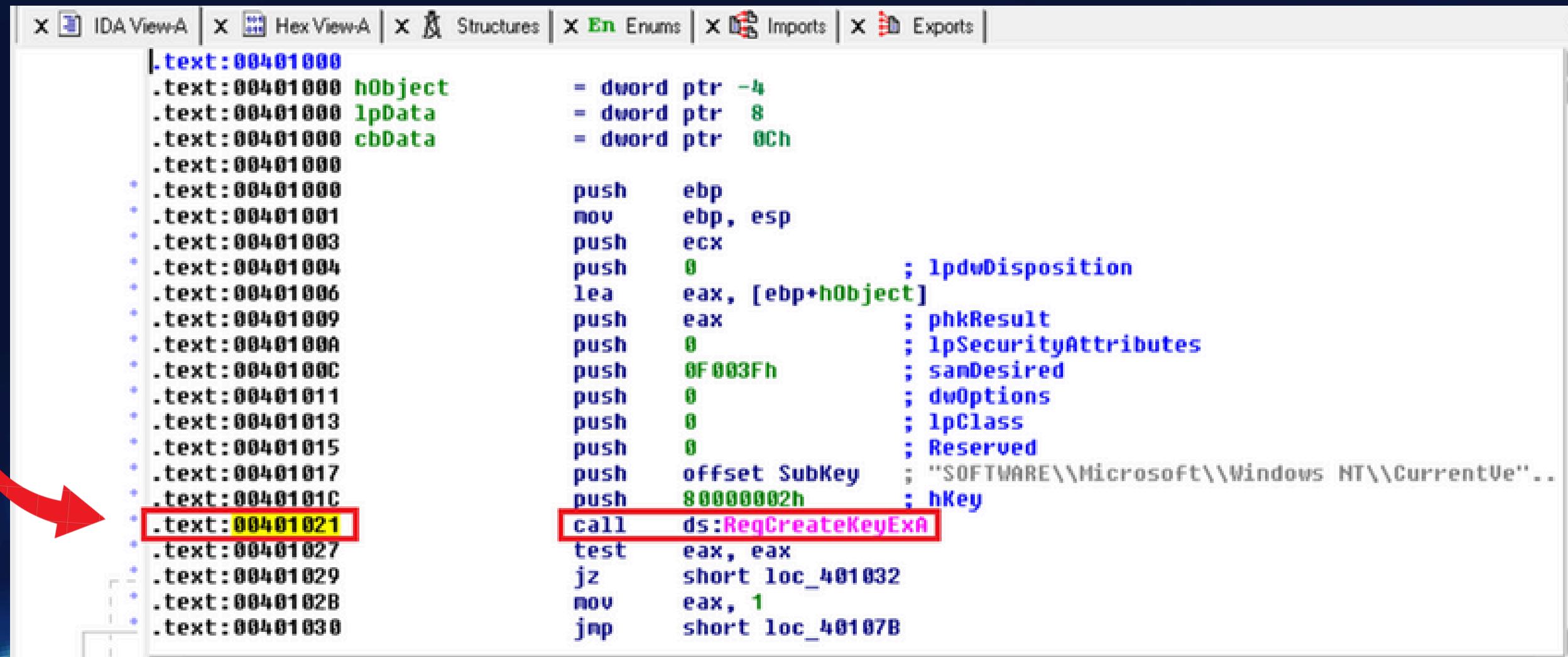


1.4. Ipotesi (in base all'analisi statica):

A seguito di un'analisi delle funzioni importate ed utilizzando Virus Total possiamo ipotizzare che questo malware sembra progettato per iniettarsi in processi o servizi di sistema, assicurandosi di essere sempre attivo (persistente) e difficilmente rilevabile (chiudendo i processi di eventuali FireWall e Antivirus), caricare altri componenti dannosi e manipolare file e processi critici.

1.5. Funzione Chiamata alla Locazione 00401021

La funzione chiamata alla locazione 00401021 è RegCreateKeyExA, un'API di Windows utilizzata per creare o aprire una chiave nel registro di sistema.



The screenshot shows the assembly view of the IDA Pro debugger. The assembly code is as follows:

```
.text:00401000 hObject      = dword ptr -4
.text:00401000 lpData       = dword ptr  8
.text:00401000 cbData       = dword ptr  0Ch
.text:00401000
.text:00401000 push    ebp
.text:00401001 mov     ebp, esp
.text:00401002 push    ecx
.text:00401003 push    0          ; lpdwDisposition
.text:00401004 lea     eax, [ebp+hObject]
.text:00401005 push    eax          ; phkResult
.text:00401006 push    0          ; lpSecurityAttributes
.text:00401007 push    0F003Fh      ; dwDesired
.text:00401008 push    0          ; dwOptions
.text:00401009 push    0          ; lpClass
.text:0040100A push    0          ; Reserved
.text:0040100B push    offset SubKey   ; "SOFTWARE\Microsoft\Windows NT\CurrentVersion\"
.text:0040100C push    80000002h      ; hKey
.text:00401021 call   ds:RegCreateKeyExA
.text:00401022 test   eax, eax
.text:00401023 jz    short loc_401032
.text:00401024 mov    eax, 1
.text:00401025 jnp   short loc_40107B
```

A red arrow points to the instruction at address 00401021, which is a call to the function RegCreateKeyExA.

1.5. Funzione Chiamata alla Locazione 00401021

Scopo della Funzione: Lo scopo principale di RegCreateKeyExA è consentire al malware di accedere o creare una chiave di registro specifica all'interno del percorso "SOFTWARE\Microsoft\Windows NT\CurrentVersion". Questa operazione è fondamentale per manipolare le impostazioni del sistema operativo, come ad esempio:

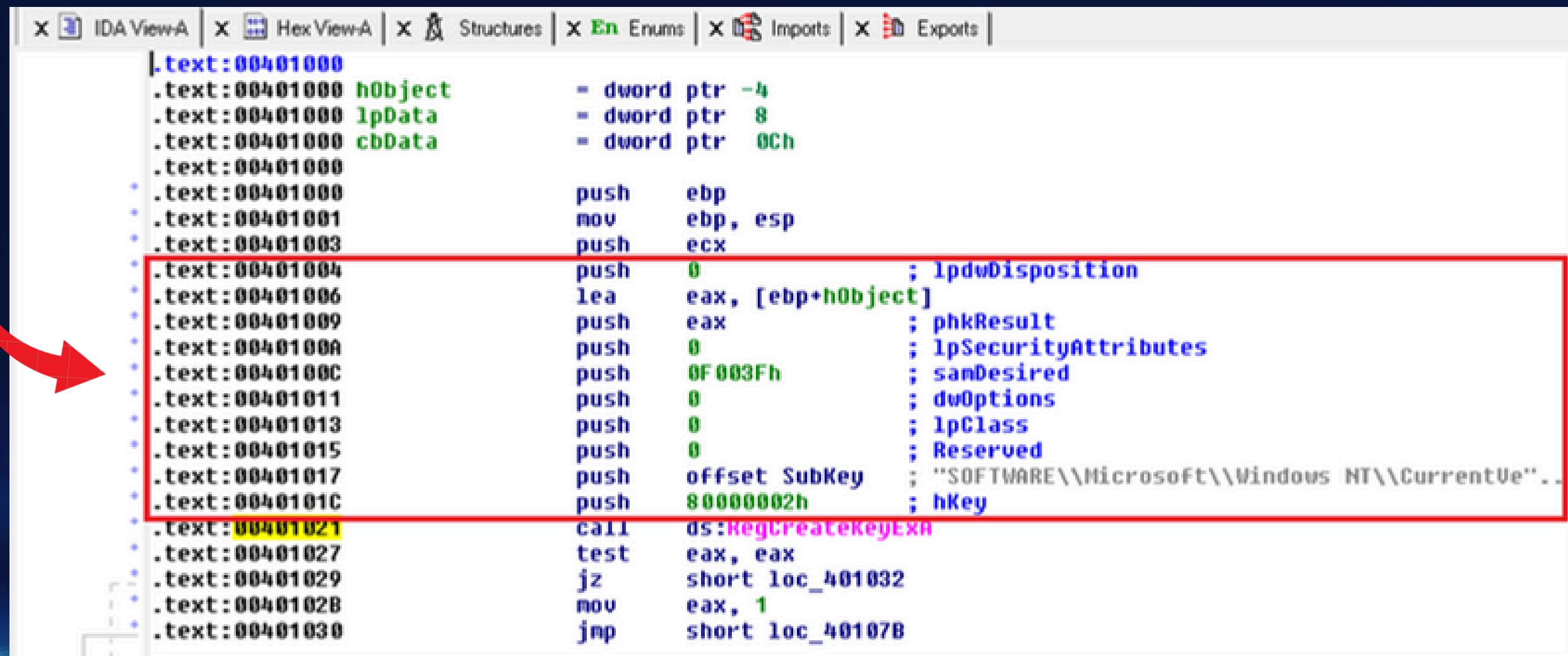
Modificare Configurazioni di Sistema: Creando o aprendo una chiave di registro, il malware può modificare configurazioni critiche del sistema, come il comportamento del processo di autenticazione.

Ottenerе Persistenza: L'accesso a determinate chiavi di registro permette al malware di garantirsi la possibilità di essere eseguito automaticamente ad ogni avvio del sistema, mantenendo così un accesso persistente.

Alterare Comportamenti di Windows: La manipolazione delle chiavi di registro attraverso questa funzione può permettere al malware di alterare il normale funzionamento di Windows, ad esempio iniettando codice malevolo che si attiva durante il login dell'utente.

1.6. Parametri Passati alla Locazione 00401021

Dopo che tutti i parametri sono stati posizionati sullo stack, viene eseguita la chiamata alla funzione RegCreateKeyExA con l'istruzione call ds:RegCreateKeyExA.



```
IDA ViewA | HexViewA | Structures | Enums | Imports | Exports | File | Edit | Search | Help | About | Exit

.Ltext:00401000
.text:00401000 hObject = dword ptr -4
.text:00401000 lpData = dword ptr 8
.text:00401000 cbData = dword ptr 0Ch
.text:00401000
.text:00401000 push    ebp
.text:00401001 mov     ebp, esp
.text:00401003 push    ecx
.text:00401004 push    0          ; lpdwDisposition
.text:00401006 lea     eax, [ebp+hObject]
.text:00401009 push    eax          ; phkResult
.text:0040100A push    0          ; lpSecurityAttributes
.text:0040100C push    0F003Fh    ; samDesired
.text:00401011 push    0          ; dwOptions
.text:00401013 push    0          ; lpClass
.text:00401015 push    0          ; Reserved
.text:00401017 push    offset SubKey ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVer...
.text:0040101C push    80000002h    ; hKey
.text:00401021 call    ds:RegCreateKeyExA
.text:00401027 test    eax, eax
.text:00401029 jz     short loc_401032
.text:0040102B mov     eax, 1
.text:00401030 jnp    short loc_40107B
```

1.6. Parametri Passati alla Locazione 00401021

push 80000002h: Passa hKey con il valore HKEY_LOCAL_MACHINE

push offset SubKey: Passa il puntatore lpSubKey alla stringa "SOFTWARE\Microsoft\Windows NT\CurrentV...",

push 0: Questo valore zero è usato per Reserved, lpClass, e dwOptions, indicando nessuna classe, nessuna opzione speciale.

push 0F003Fh: Questo valore rappresenta il parametro samDesired, che specifica le autorizzazioni richieste sulla chiave di registro. In questo caso, 0F003Fh combina i diritti KEY_READ e KEY_WRITE, che consentono rispettivamente la lettura e la scrittura sulla chiave di registro.

push 0: Questo valore rappresenta il parametro lpSecurityAttributes, che è utilizzato per specificare le attribuzioni di sicurezza della chiave di registro. Essendo impostato a 0, si utilizza il valore predefinito.

lea eax, [ebp+hObject]: L'istruzione lea carica l'indirizzo della variabile hObject nel registro EAX. Questo è il puntatore dove verrà restituito l'handle della chiave di registro creata o aperta.

push eax: Viene passato il valore di EAX come parametro phkResult, che è un puntatore alla variabile dove verrà restituito l'handle della chiave di registro.

push 0: Questo valore rappresenta il parametro lpdwDisposition, che riceverà un valore che indica se la chiave è stata creata o aperta.

1.7. Oggetto rappresentato dal parametro alla locazione 00401017

"SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" rappresenta il percorso di una chiave di registro che il malware sta tentando di modificare. Questo parametro viene passato alla funzione RegCreateKeyExA, che è utilizzata per creare o aprire chiavi di registro.

.text:00401017

push offset SubKey

; "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"



1.8. Istruzioni comprese tra gli indirizzi 00401027 e 00401029

In assembly x86, il comando TEST esegue un'operazione di AND bit a bit tra due operandi e aggiorna i flag di stato senza memorizzare il risultato. L'istruzione JZ (Jump if Zero) salta a una determinata etichetta se il flag ZF (Zero Flag) è impostato, indicando che il risultato dell'operazione precedente era zero. Quindi, TEST è usato per verificare condizioni e JZ per dirigere il flusso del programma basandosi su quei risultati.

In questo caso il comando TEST è eseguito tra due registri identici ovvero EAX, EAX; quindi nel caso $EAX \neq 0$ à $ZF = 0$, nel caso $EAX = 0$ à $ZF = 1$ (è impostato).

```
.text:00401027  
.text:00401029  
.text:0040102B  
.text:00401030
```



```
test    eax, eax  
jz      short loc_401032  
mov    eax, 1  
jmp    short loc_40107B
```

1.9. Traduzione Assembly in costrutto C

```
1 if (a == 0) {  
2 // Corrisponde a Loc_401032  
3 } else {  
4     a = 1; // Imposta a 1 se non lo era già  
5     //Corrisponde a Loc_40107B  
6 }
```

1.10. Valore del parametro « ValueName» alla locazione 00401047

Utilizzando il tool OLLY DBG abbiamo identificato che il valore del parametro “ValueName” è “GinaDLL”

The screenshot shows the OLLY debugger's assembly window and a context menu for a registry value.

Assembly Window:

Address	OpCode	Description
00401032	> 8B40 0C	MOV ECX, DWORD PTR SS:[EBP+C]
00401035	. 51	PUSH ECX
00401036	. 8B55 08	MOV EDX, DWORD PTR SS:[EBP+8]
00401039	. 52	PUSH EDX
0040103A	. 6A 01	PUSH 1
0040103C	. 6A 00	PUSH 0
0040103E	. 68 4C804000	PUSH Malware_.0040804C
00401043	. 8B45 FC	MOV EAX, DWORD PTR SS:[EBP-4]
00401046	. 50	PUSH EAX
00401047	. FF15 00704000	CALL DWORD PTR DS:[<&AUDIOPCI32.RegSetValueExA]

A red arrow points from the assembly line at address 00401047 to the context menu.

Context Menu (ValueName = "GinaDLL"):

- BufSize
- Buffer
- ValueType = REG_SZ
- Reserved = 0
- ValueName = "GinaDLL"** (highlighted in red)
- hKey
- RegSetValueExA

1.11. Funzionalità che sta implementando il Malware in questa sezione

Il malware, nella sezione di codice analizzata, sta implementando una funzionalità di manipolazione dell'autenticazione di Windows. Utilizzando le API RegCreateKeyExA e RegSetValueExA, il malware crea o modifica una chiave di registro (GinaDLL) che è cruciale per il processo di autenticazione del sistema. Questa funzionalità consente al malware di:

Interferire con il processo di login: Installando una propria DLL, il malware può eseguire codice malevolo durante l'autenticazione.

Ottenerne persistenza: Assicurarsi che questa DLL venga caricata ogni volta che l'utente si autentica, garantendo l'esecuzione automatica e il mantenimento dell'accesso al sistema.

Quindi, la funzionalità principale implementata dal malware è la modifica e il controllo del processo di autenticazione di Windows per compromettere la sicurezza del sistema.

DAY 2

Traccia

- Analizzare le routine tra le locazioni di memoria 00401080 e 00401128;
 - Valore del parametro «ResourceName » della funzione FindResourceA ();
 - Che funzionalità sta implementando il malware?
 - Si ottiene lo stesso risultato con l'analisi statica basica ?
 - Se si, elencare le evidenze a supporto.
 - Disegnare un diagramma di flusso che comprenda le 3 funzioni principali del Main().
-
- Preparate l'ambiente ed i tool per l'esecuzione del Malware utilizzando Process Monitor
 - Eseguite il Malware
 - Cosa notate all'interno della cartella dove è situato l'eseguibile? Spiegate cosa è avvenuto, unendo le evidenze che avete raccolto finora per rispondere alla domanda
 - Analizzate ora i risultati di Process Monitor
 - Filtrare includendo solamente l'attività sul Registro di Windows
 - Visualizzare attività sul File System
 - Unire tutte le informazioni e trarre le conclusioni

Analisi con IDA Pro

Abbiamo preso in esame la porzione di codice compresa tra l'indirizzo di memoria 00401080 e l'indirizzo 00401128, come indicato nella traccia. Con IDA Pro si riescono a vedere bene le chiamate a funzione che effettua il programma. Compaiono le seguenti funzioni: FindResourceA, LoadResource, LockResource, SizeOfResource.

Con la visualizzazione a diagramma di flusso (premendo barra spaziatrice) si ottiene anche la visione dei salti che effettua il programma durante l'esecuzione.

The image shows the IDA Pro interface with three main windows. The left window displays assembly code for the range 00401080 to 00401128. The middle window shows a flowchart of the program's execution. Red arrows point from specific assembly instructions in the left window to their corresponding nodes in the flowchart. The right window shows the assembly code for each node in the flowchart.

Left Window (Assembly View):

```
.text:00401080 sub_401080 proc near ; CODE XREF: _main+3F↑p
.text:00401080     = dword ptr -18h
.text:00401080     = dword ptr -14h
.text:00401080     = dword ptr -10h
.text:00401080     = dword ptr -8Ch
.text:00401080     = dword ptr -8
.text:00401080     = dword ptr -4
.text:00401080     = dword ptr 8
.text:00401080
.text:00401080     push    ebp
.text:00401080     mov     ebp, esp
.text:00401080     sub    esp, 18h
.text:00401080     push    esi
.text:00401080     push    edi
.text:00401080     mov    [ebp+hResInfo], 0
.text:00401080     mov    [ebp+hResData], 0
.text:00401080     mov    [ebp+Str], 0
.text:00401080     mov    [ebp+Count], 0
.text:00401080     mov    [ebp+var_C], 0
.text:00401080     cmp    [ebp+hModule], 0
.text:00401080     jnz    short loc_4010B8
.text:00401080     xor    eax, eax
.text:00401080     jmp    loc_4011BF
.text:00401080
.text:00401080 loc_4010B8:
.text:004010B8     mov    eax, lpType
.text:004010B8     push   eax
.text:004010B8     mov    ecx, lpName ; lpName
.text:004010B8     push   ecx
.text:004010C4     mov    edx, [ebp+hModule]
.text:004010C8     push   edx
.text:004010C9     call   ds:FindResourceA
.text:004010CF     mov    [ebp+hResInfo], eax
.text:004010D2     cmp    [ebp+hResInfo], 0
.text:004010D6     jnz    short loc_4010DF
.text:004010D8     xor    eax, eax
.text:004010DA     jmp    loc_4011BF
.text:004010DA
```

Middle Window (Flowchart View):

```
.text:004010DF ; CODE XREF: sub_401080+56↑j
.text:004010DF loc_4010DF:
.text:004010DF     mov    eax, [ebp+hResInfo]
.text:004010E2     push   eax
.text:004010E3     mov    ecx, [ebp+hModule]
.text:004010E6     push   ecx
.text:004010E7     call   ds:LoadResource
.text:004010ED     mov    [ebp+hResData], eax
.text:004010F0     cmp    [ebp+hResData], 0
.text:004010F4     jnz    short loc_4010FB
.text:004010F6     jmp    loc_4011A5
.text:004010FB ; CODE XREF: sub_401080+74↑j
.text:004010FB loc_4010FB:
.text:004010FB     mov    edx, [ebp+hResData]
.text:004010FE     push   edx
.text:004010FF     call   ds:LockResource
.text:00401105     mov    [ebp+Str], eax
.text:00401108     cmp    [ebp+Str], 0
.text:0040110C     jnz    short loc_401113
.text:0040110E     jmp    loc_4011A5
.text:00401113 ; CODE XREF: sub_401080+2F↑j
.text:00401113 loc_401113:
.text:00401113     mov    eax, [ebp+hResInfo]
.text:00401116     push   eax
.text:00401117     mov    ecx, [ebp+hModule]
.text:0040111A     push   ecx
.text:0040111B     call   ds:SizeofResource
.text:00401121     mov    [ebp+Count], eax
.text:00401124     cmp    [ebp+Count], 0
.text:00401128     ja     short loc_40112C
.text:0040112A     jmp    short loc_4011A5
.text:0040112C
```

Right Window (Function View):

```
loc_4010B8:
mov    eax, lpType
push   eax
mov    ecx, lpName ; lpName
push   ecx
mov    edx, [ebp+hModule]
push   edx
call   ds:FindResourceA
mov    [ebp+hResInfo], eax
cmp    [ebp+hResInfo], 0
short loc_4010DF
```

```
loc_4010DF:
mov    eax, [ebp+hResInfo]
push   eax
mov    ecx, [ebp+hModule]
push   ecx
call   ds:LoadResource
mov    [ebp+hResData], eax
cmp    [ebp+hResData], 0
short loc_4010FB
```

```
loc_4010FB:
mov    edx, [ebp+hResData]
push   edx
call   ds:LockResource
mov    [ebp+Str], eax
cmp    [ebp+Str], 0
short loc_401113
```

```
loc_401113:
mov    eax, [ebp+hResInfo]
push   eax
mov    ecx, [ebp+hModule]
push   ecx
call   ds:SizeofResource
mov    [ebp+Count], eax
cmp    [ebp+Count], 0
ja     short loc_40112C
```

Analisi con OllyDBG

```
0040103C > A1 34804000 MOV EAX,DWORD PTR DS:[400030]
004010BD . 50 PUSH EAX
004010BE . 8B0D 34804000 MOV ECX,DWORD PTR DS:[400034]
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
004010CF . 8945 EC MOV 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 FC MOV EBX,DWORD PTR SS:[EBP-14]
```

ResourceType => "BINARY"
Malware_.00400000
ResourceName => "TGAD"
hModule
FindResourceA

Successivamente, possiamo notare che il malware va a chiamare altre funzioni: **LoadResource**, **LockResource** e **SizeOfResource**.

Per svolgere il primo punto della traccia, ci siamo serviti degli strumenti di analisi dinamica avanzata. In questo caso il tool utilizzato è **OllyDBG**. Abbiamo impostato un **breakpoint** all'indirizzo di memoria corrispondente alla chiamata della funzione **FindResourceA**, ovvero l'indirizzo di memoria **004010C9**, ed avviando l'esecuzione del programma da **OllyDBG**, riusciamo ad ottenere il valore del parametro che stavamo cercando. Dopo l'esecuzione della funzione, il parametro **ResourceName** avrà al suo interno il valore “**TGAD**”.

```
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.SizeFResou
00401121 . 8945 F0 MOV DWORD PTR SS:[EBP-10],EHX
00401124 . 837D F0 00 CMP DWORD PTR SS:[EBP-10],0
00401128 .~77 02 JA SHORT Malware_.0040112C
00401129 .~EB 79 JMP SHORT Malware_.004011A5
```

hResource
hModu Le
SizeofResource

```
004010E2 . 50 PUSH EHX
004010E3 . 8B4D 08 MOV ECX,DWORD PTR SS:[EBP+8]
004010E6 . 51 PUSH ECX
004010E7 . FF15 14704000 CALL DWORD PTR DS:[<&KERNEL32.LoadResou
004010ED . 8945 E8 MOV DWORD PTR SS:[EBP-18],EHX
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 MOV EDX,DWORD PTR SS:[EBP-18]
```

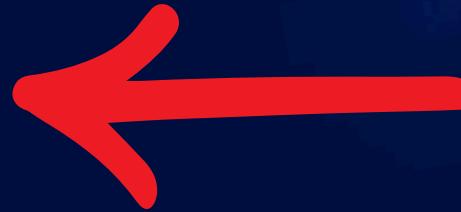
hResource
hModu Le
LoadResource

```
004010FE . 52 PUSH EDX
004010FF . FF15 10704000 CALL DWORD PTR DS:[<&KERNEL32.LockResou
00401105 . 8945 F8 MOV DWORD PTR SS:[EBP-8],EHX
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 FC MOV EBX,DWORD PTR SS:[EBP-14]
```

hResource
LockResource

Analisi con IDA Pro

```
text:004010B8 ;-----  
text:004010B8 loc_4010B8:          ; CODE XREF: sub_401080+2F↑j  
text:004010B8     mov    eax, lpType      ; lpType  
text:004010BD     push   eax           ; lpType  
text:004010BE     mov    ecx, lpName      ; lpName  
text:004010C4     push   ecx           ; lpName  
text:004010C5     mov    edx, [ebp+hModule] ; hModule  
text:004010C8     push   edx           ; hModule  
text:004010C9     call   ds:FindResourceA  
text:004010CF     mov    [ebp+hResInfo], eax  
text:004010D2     cmp    [ebp+hResInfo], 0  
text:004010D6     jnz    short loc_4010DF  
text:004010D8     xor    eax, eax  
text:004010DA     jmp    loc_4011BF  
text:004010DE
```



FindResourceA è una funzione appartente alla libreria KERNEL32 di Microsoft che si occupa di trovare la locazione di una determinata risorsa accettando come parametro il nome ed il tipo della stessa.

```
text:004010DF ;-----  
text:004010DF loc_4010DF:          ; CODE XREF: sub_401080+56↑j  
text:004010DF     mov    eax, [ebp+hResInfo] ; hResInfo  
text:004010E2     push   eax           ; hResInfo  
text:004010E3     mov    ecx, [ebp+hModule] ; hModule  
text:004010E6     push   ecx           ; hModule  
text:004010E7     call   ds:LoadResource  
text:004010ED     mov    [ebp+hResData], eax  
text:004010F0     cmp    [ebp+hResData], 0  
text:004010F4     jnz    short loc_4010FB  
text:004010F6     jmp    loc_4011A5  
text:004010FB
```



LoadResource è una funzione che recupera un handle (passato come parametro) che serve per ottenere il puntatore al primo byte di memoria dove risiede la risorsa desiderata.

```
text:004010FB ;-----  
text:004010FB loc_4010FB:          ; CODE XREF: sub_401080+74↑j  
text:004010FB     mov    edx, [ebp+hResData] ; hResData  
text:004010FE     push   edx           ; hResData  
text:004010FF     call   ds:LockResource  
text:00401105     mov    [ebp+Str], eax  
text:00401108     cmp    [ebp+Str], 0  
text:0040110C     jnz    short loc_401113  
text:0040110E     jmp    loc_4011A5
```



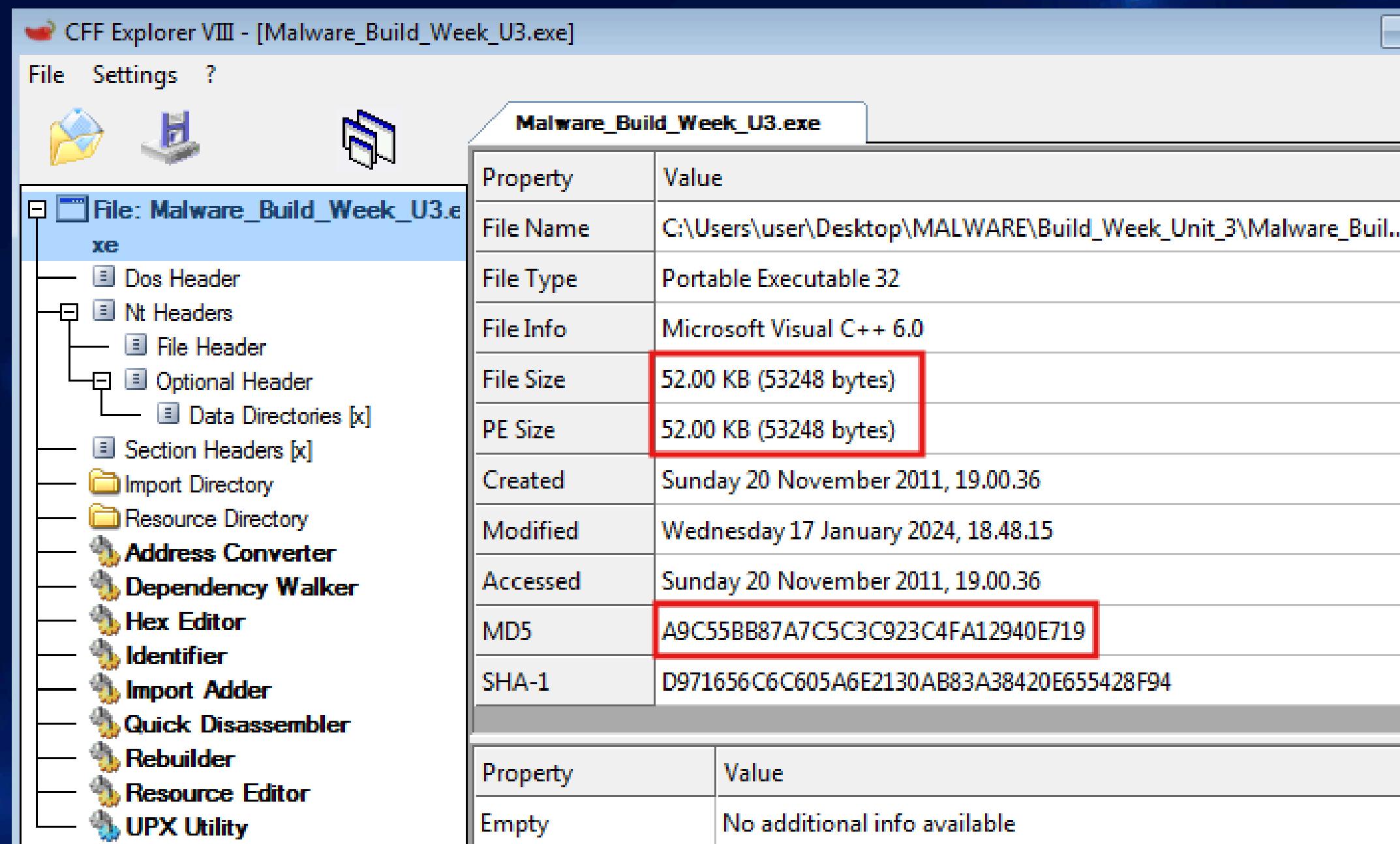
LockResource si occupa di recuperare un puntatore a un indirizzo di memoria specifico.

```
text:00401113 ;-----  
text:00401113 loc_401113:          ; CODE XREF: sub_401080+8C↑j  
text:00401113     mov    eax, [ebp+hResInfo] ; hResInfo  
text:00401116     push   eax           ; hResInfo  
text:00401117     mov    ecx, [ebp+hModule] ; hModule  
text:0040111A     push   ecx           ; hModule  
text:0040111B     call   ds:SizeOfResource  
text:00401121     mov    [ebp+Count], eax  
text:00401124     cmp    [ebp+Count], 0  
text:00401128     ja    short loc_40112C  
text:0040112A     jmp    loc_4011A5
```



SizeOfResource ottiene la dimensione in byte della risorsa specificata.

Analisi con CFF Explorer



CFF Explorer

Analisi con CFF Explorer

Malware_Build_Week_U3.exe				
Module Name	Imports	OFTs	TimeStamp	ForwarderCh
0000769E	N/A	000074EC	000074F0	000074F4
szAnsi	(nFunctions)	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000
ADVAPI32.dll	2	00007528	00000000	00000000

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00007632	00007632	0295	SizeofResource
00007644	00007644	01D5	LockResource
00007654	00007654	01C7	LoadResource
00007622	00007622	02BB	VirtualAlloc
00007674	00007674	0124	GetModuleFileNameA
0000768A	0000768A	0126	GetModuleHandleA
00007612	00007612	00B6	FreeResource
00007664	00007664	00A3	FindResourceA
00007604	00007604	001B	CloseHandle
000076DE	000076DE	00CA	GetCommandLineA
000076F0	000076F0	0174	GetVersion
000076FE	000076FE	007D	ExitProcess



Nella scheda **Import Directory** di **CFF Explorer** si possono trovare tutte le librerie importate dal malware e le funzioni chiamate.

In questo caso si nota che le librerie importate sono **KERNEL32.dll** e **ADVAPI.dll**. Tra le funzioni chiamate troviamo le stesse della porzione di codice appena analizzata con **IDA Pro** e **OllyDBG** in analisi statica avanzata, ovvero: **FindResourceA**, **LoadResource**, **LockResource**, **SizeOfResource**.

Quindi si sarebbe potuto ottenere il medesimo risultato tramite l'analisi statica basica del malware.

L'unica cosa che non si può ricavare con questo tipo di analisi è il valore del parametro **ResourceName** appartenente alla funzione **FindResourceA**.

Analisi delle funzioni nel Main()

```
.text:004011D0 ; int __cdecl main(int argc, const char **argv, const char **envp)
.text:004011D0 _main          proc near             ; CODE XREF: start+AF↓p
.text:004011D0
.text:004011D0     hModule        = dword ptr -11Ch
.text:004011D0     Data          = byte ptr -118h
.text:004011D0     var_117       = byte ptr -117h
.text:004011D0     var_8         = dword ptr -8
.text:004011D0     var_4         = dword ptr -4
.text:004011D0     argc          = dword ptr 8
.text:004011D0     argv          = dword ptr 0Ch
.text:004011D0     envp          = dword ptr 10h
.text:004011D0
.text:004011D0     push    ebp    |
.text:004011D1     mov     ebp, esp
.text:004011D3     sub     esp, 11Ch
.text:004011D9     push    ebx
.text:004011DA     push    esi
.text:004011DB     push    edi
.text:004011DC     mov     [ebp+var_4], 0
.text:004011E3     push    0           ; lpModuleName
.text:004011E5     call    ds:GetModuleHandleA
.text:004011EB     mov     [ebp+hModule], eax
.text:004011F1     mov     [ebp+Data], 0
.text:004011F8     mov     ecx, 43h
.text:004011FD     xor     eax, eax
.text:004011FF     lea     edi, [ebp+var_117]
.text:00401205     rep    stosd
.text:00401207     stosb
.text:00401208     mov     eax, [ebp+hModule]
.text:0040120E     push   eax           ; hModule
.text:0040120F     call    sub_401080
.text:00401214     add    esp, 4
.text:00401217     mov     [ebp+var_4], eax
.text:0040121A     push   10Eh          ; nSize
.text:0040121F     lea     ecx, [ebp+Data]
.text:00401225     push   ecx           ; lpFilename
.text:00401226     push   0             ; hModule
.text:00401228     call    ds:GetModuleFileNameA
.text:0040122E     push   5Ch           ; Ch
```

Dichiarazione delle variabili locali e dei parametri del Main()

GetModuleHandleA: recupera l'handle del modulo che deve essere caricato dal processo chiamante.

GetModuleFileNameA: recupera il percorso del modulo specificato che deve esser stato caricato dal processo corrente.

Analisi delle funzioni nel Main()

C++

```
HMODULE GetModuleHandleA(  
    [in, optional] LPCSTR lpModuleName  
)
```



GetModuleHandleA

accetta un parametro di tipo **LPCSTR** nominato **lpModuleName**.

C++

```
DWORD GetModuleFileNameA(  
    [in, optional] HMODULE hModule,  
    [out]          LPSTR   lpFilename,  
    [in]           DWORD    nSize  
)
```



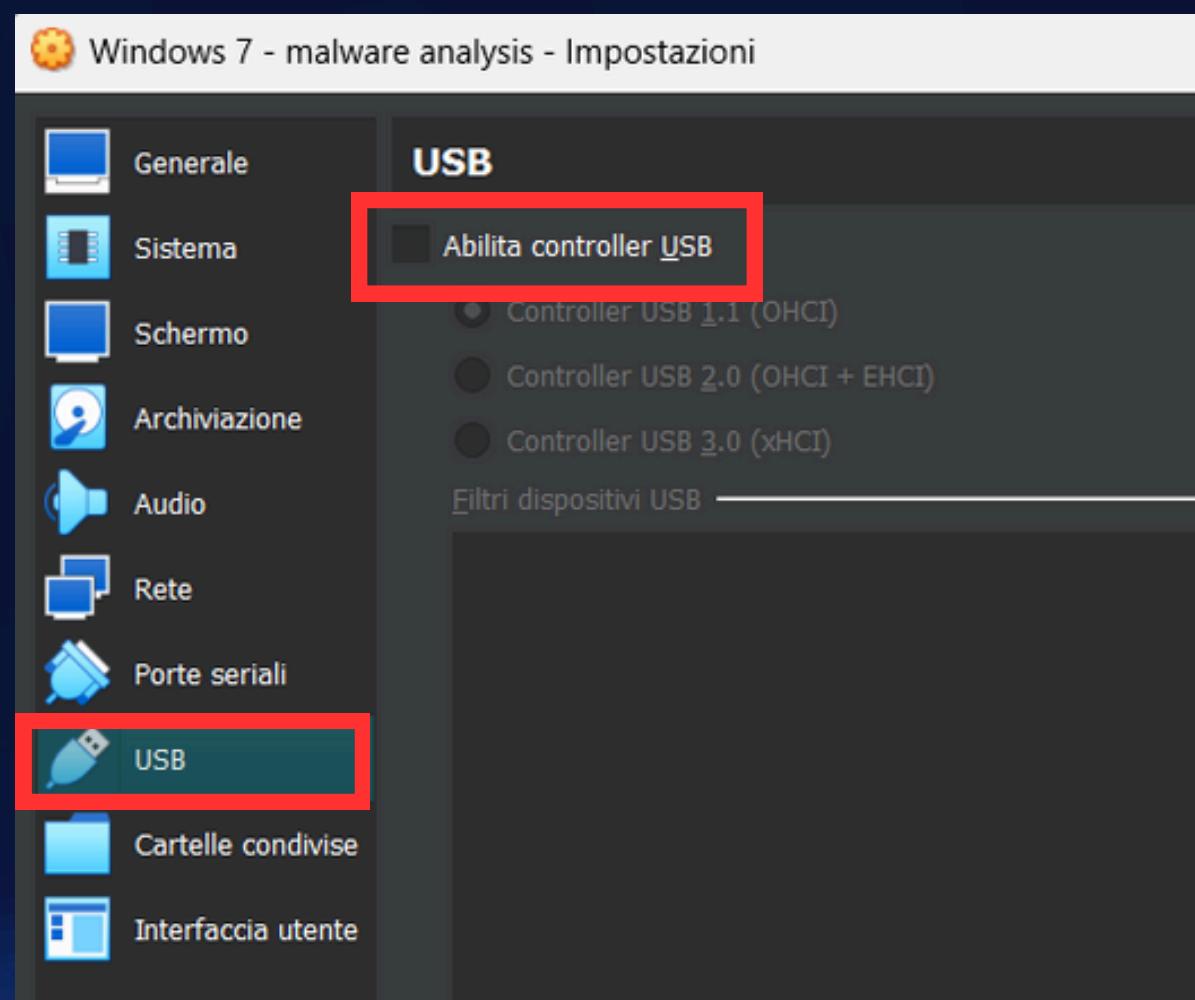
GetModuleFileNameA

accetta 3 parametri:

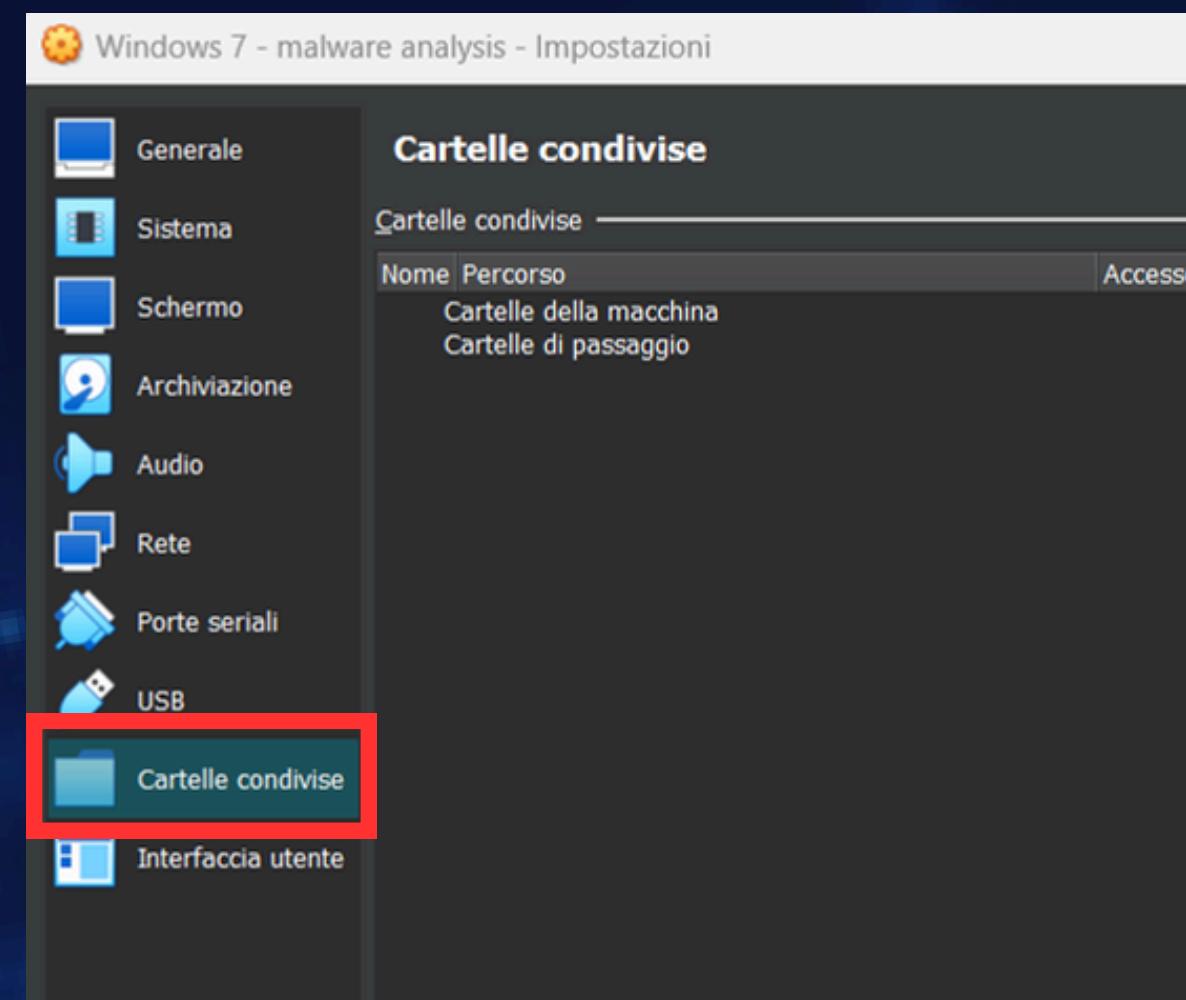
- **hModule** di tipo **HMODULE** (handle)
- **lpFileName** di tipo **LPSTR**
- **nSize** di tipo **DWORD** (intero 32bit)

Analisi dinamica basica

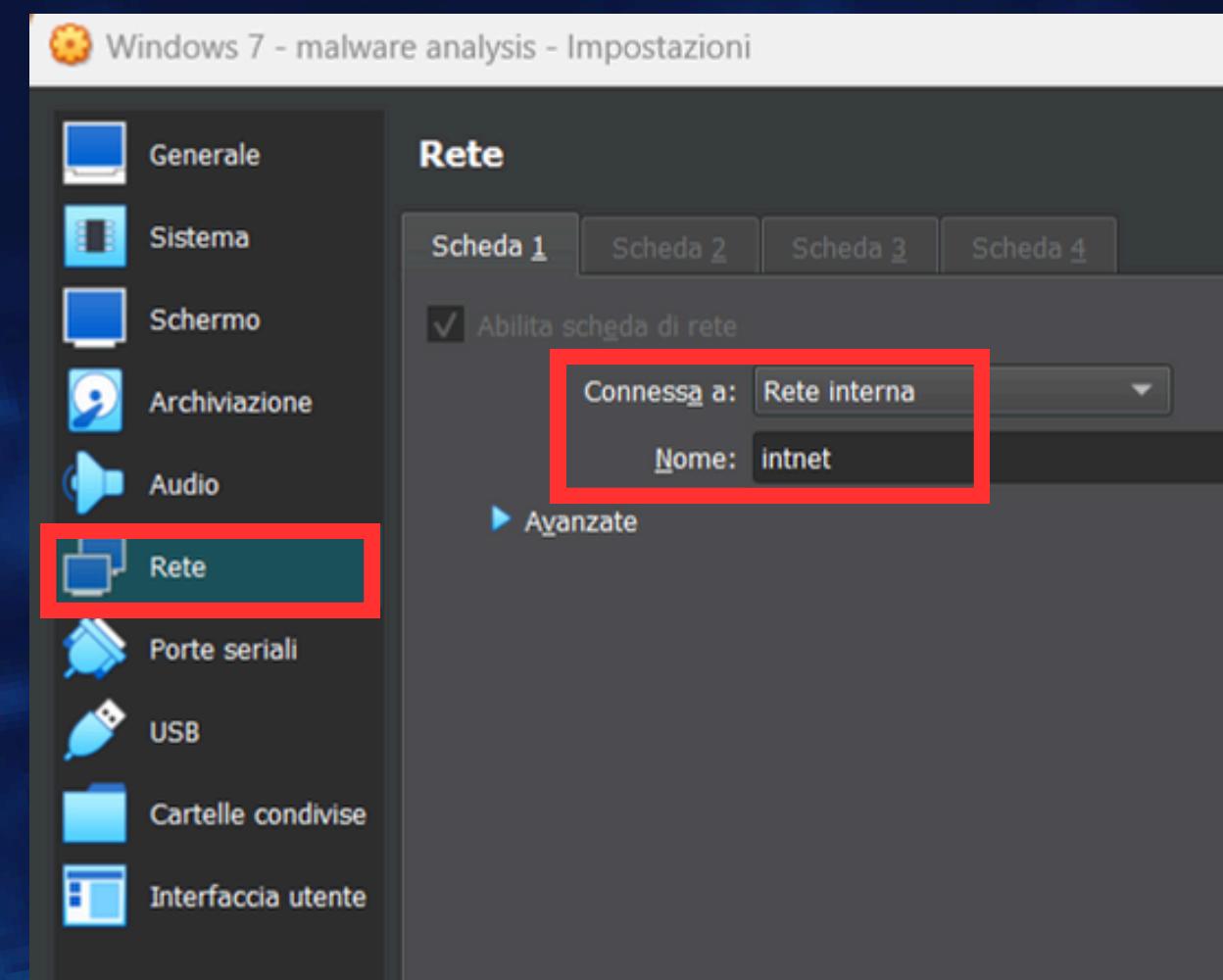
Prima di procedere con l'analisi dinamica basica dobbiamo assicurarci di mettere in sicurezza la macchina virtuale assicurandoci di disabilitare il controller delle porte USB, disattivare le cartelle condivise e metterci in una rete interna.



1-Disabilito controller USB



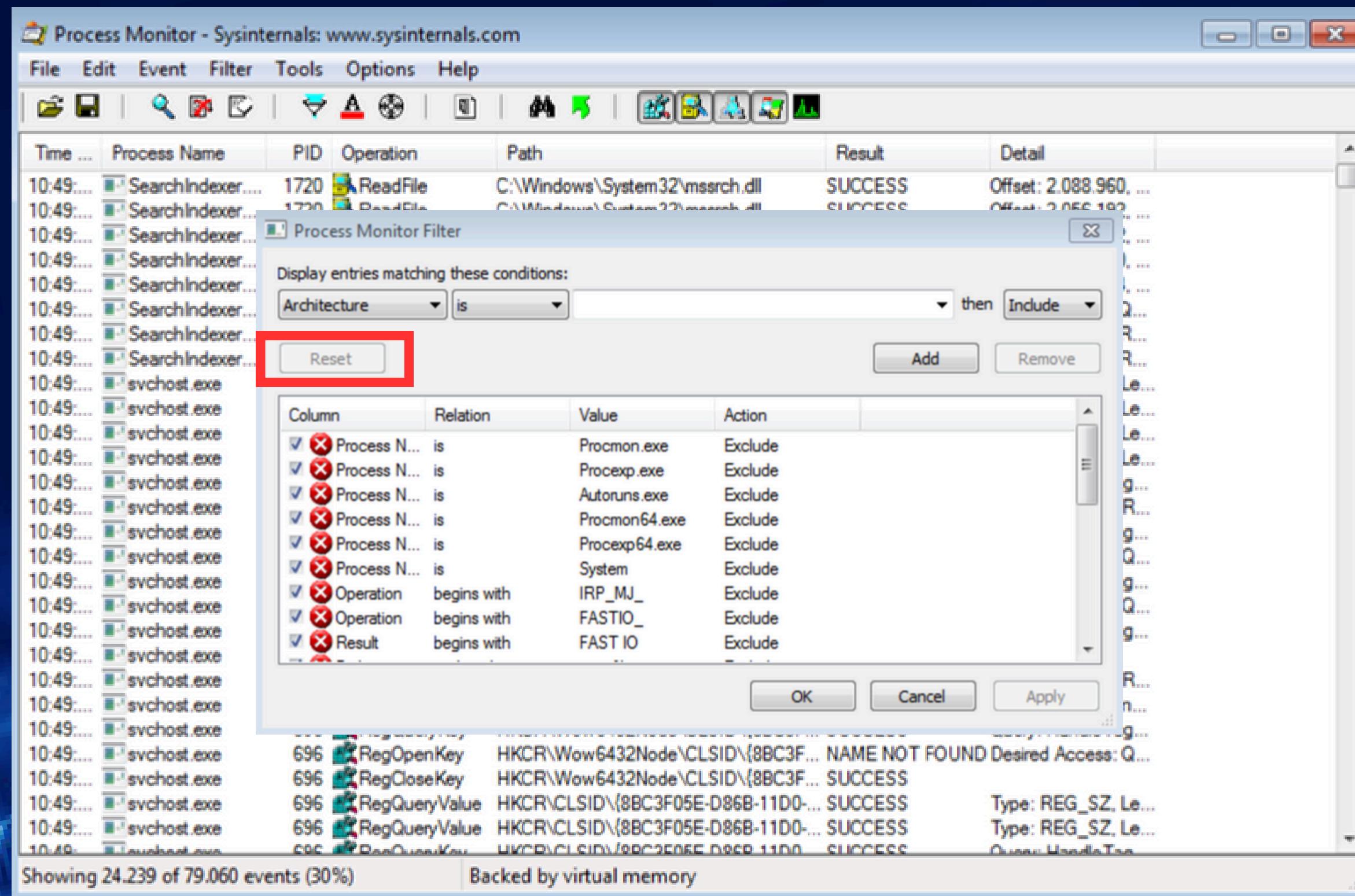
2-Rimuovo cartelle condivise



3- Rete interna

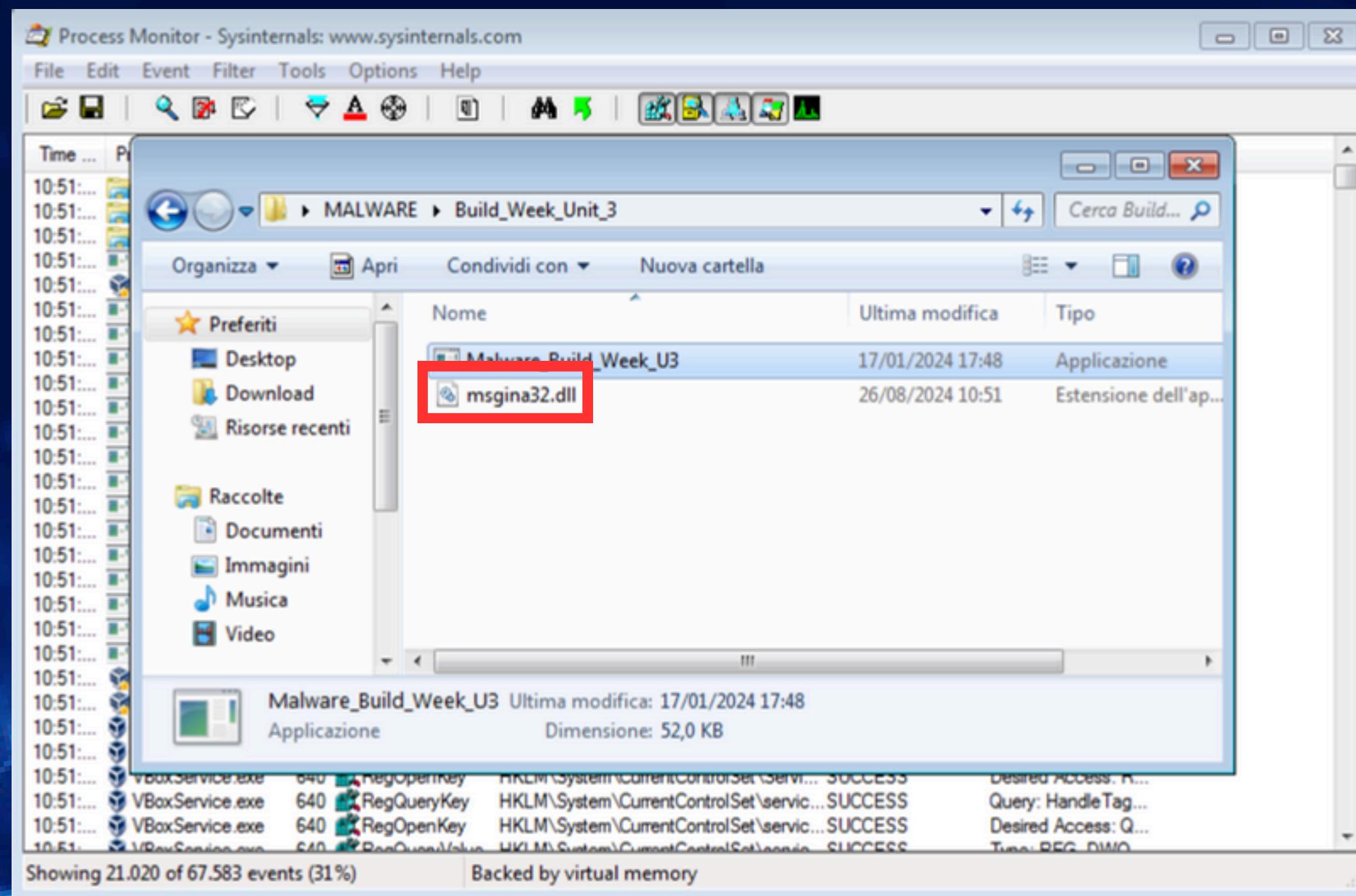
Process Monitor

Appena avviato Process Monitor ci verrà chiesto di resettare tutti i filtri usati in precedenza così andremo a crearne di nuovi per studiare questo malware.



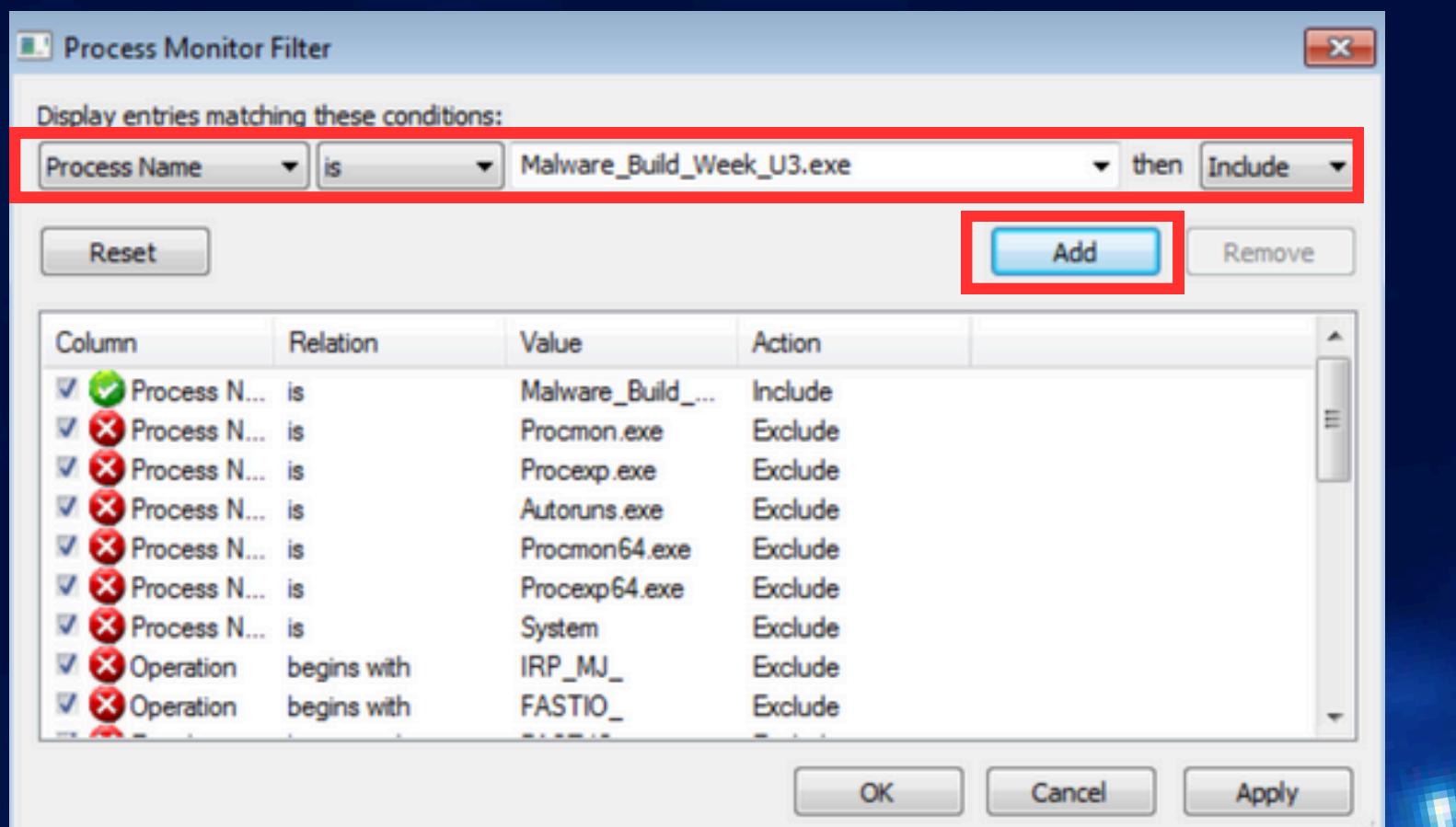
Avvio del malware

Andiamo ora ad avviare il malware, noteremo che si aprirà e chiuderà in pochi millisecondi il prompt dei comandi, dopo di che comparirà un nuovo file con estensione .dll nella stessa cartella dove risiede il malware come ci aspettavamo sulla base delle funzioni viste in precedenza.



Analisi con Process Monitor

Andiamo ora ad analizzare nel dettaglio cosa va modificare il malware andando ad inserire dei filtri su Process Monitor, in particolare per vedere nuovi processi eseguiti e i cambiamenti sul registro di sistema e sul File System



Con il filtro mostrato in figura sopra possiamo andare ad evidenziare tutti i processi che riguardano il malware

Time ...	Process Name	PID	Operation	Path	Result	Detail
10:51:	Malware_Build_...	2508	Process Start		SUCCESS	Parent PID: 1972, ...
10:51:	Malware_Build_...	2508	Thread Create		SUCCESS	Thread ID: 2972
10:51:	Malware_Build_...	2508	Load Image	C:\Users\user\Desktop\MALWARE\Bu...	SUCCESS	Image Base: 0x400...
10:51:	Malware_Build_...	2508	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x770...
10:51:	Malware_Build_...	2508	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x772...
10:51:	Malware_Build_...	2508	CreateFile	C:\Windows\Prefetch\MALWARE_BUI...	NAME NOT FOUND	Desired Access: G...
10:51:	Malware_Build_...	2508	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
10:51:	Malware_Build_...	2508	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WIN...	NAME NOT FOUND	Length: 1.024
10:51:	Malware_Build_...	2508	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
10:51:	Malware_Build_...	2508	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
10:51:	Malware_Build_...	2508	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
10:51:	Malware_Build_...	2508	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
10:51:	Malware_Build_...	2508	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
10:51:	Malware_Build_...	2508	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
10:51:	Malware_Build_...	2508	QueryBasicInfor...	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 30/0...
10:51:	Malware_Build_...	2508	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
10:51:	Malware_Build_...	2508	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
10:51:	Malware_Build_...	2508	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
10:51:	Malware_Build_...	2508	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
10:51:	Malware_Build_...	2508	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x73f...
10:51:	Malware_Build_...	2508	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
10:51:	Malware_Build_...	2508	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
10:51:	Malware_Build_...	2508	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 30/0...
10:51:	Malware_Build_...	2508	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
10:51:	Malware_Build_...	2508	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
10:51:	Malware_Build_...	2508	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
10:51:	Malware_Build_...	2508	CreateFileMapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
10:51:	Malware_Build_...	2508	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x72e...

Showing 137 of 69.905 events (0.1%)

Backed by virtual memory

Come possiamo vedere nell'immagine sottostante, una volta avviato il malware vengono fatte molte operazioni di creazione file in una cartella critica per Windows come può essere System32 oppure modifiche alle chiavi di registro.

Operazioni sul registro di Windows

Creazione di diversi files

The screenshot shows the Process Monitor application interface. A red arrow points from the 'Operazioni sul registro di Windows' text to a group of registry-related events in the list. Another red arrow points from the 'Creazione di diversi files' text to a group of file creation events. The table below details the captured events:

Time ...	Process Name	PID	Operation	Path	Result	Detail
10:51...	Malware_Build_...	2508	Process Start		SUCCESS	Parent PID: 1972, ...
10:51...	Malware_Build_...	2508	Thread Create		SUCCESS	Thread ID: 2972
10:51...	Malware_Build_...	2508	Load Image	C:\Users\user\Desktop\MALWARE\Bu...	SUCCESS	Image Base: 0x400...
10:51...	Malware_Build_...	2508	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x770...
10:51...	Malware_Build_...	2508	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x772...
10:51...	Malware_Build_...	2508	CreateFile	C:\Windows\Prefetch\MALWARE_BUI...	NAME NOT FOUND	Desired Access: G...
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
10:51...	Malware_Build_...	2508	RegQueryValue	HKLM\Software\Microsoft\Windows N...	NAME NOT FOUND	Length: 1.024
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
10:51...	Malware_Build_...	2508	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
10:51...	Malware_Build_...	2508	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
10:51...	Malware_Build_...	2508	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
10:51...	Malware_Build_...	2508	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
10:51...	Malware_Build_...	2508	QueryBasicInfor...	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 30/0...
10:51...	Malware_Build_...	2508	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
10:51...	Malware_Build_...	2508	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
10:51...	Malware_Build_...	2508	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
10:51...	Malware_Build_...	2508	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
10:51...	Malware_Build_...	2508	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x73f...
10:51...	Malware_Build_...	2508	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
10:51...	Malware_Build_...	2508	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
10:51...	Malware_Build_...	2508	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 30/0...
10:51...	Malware_Build_...	2508	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
10:51...	Malware_Build_...	2508	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
10:51...	Malware_Build_...	2508	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
10:51...	Malware_Build_...	2508	CreateFileMapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
10:51...	Malware_Build_...	2508	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x72e...

Creazione chiave malevola

Inserendo ora un filtro per evidenziare solo le operazioni fatte sulle chiavi di registro possiamo notare che viene creata con successo una nuova chiave al percorso:
“HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon”

The screenshot shows the Process Monitor application interface. On the left, a 'Process Monitor Filter' dialog is open, with its search bar set to 'Operation contains Reg'. This filter is highlighted with a red box. On the right, the main window displays a list of registry events. One specific event is highlighted with a red box: '10:51: Malware_Build_... 2508 RegCreateKey HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon SUCCESS KeySetInformation...'. This event represents the successful creation of a new key at the specified path.

Time	Process Name	PID	Operation	Path	Result	Detail
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM\Software\Wow6432Node\Polic...	REPARSE	Desired Access: Q...
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	Desired Access: Q...
10:51...	Malware_Build_...	2508	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	KeySetInformation...
10:51...	Malware_Build_...	2508	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND Length: 80	
10:51...	Malware_Build_...	2508	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
10:51...	Malware_Build_...	2508	RegOpenKey	HKCU\Software\Microsoft\Win...	NAME NOT FOUND Desired Access: Q...	
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
10:51...	Malware_Build_...	2508	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
10:51...	Malware_Build_...	2508	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
10:51...	Malware_Build_...	2508	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length: 260	
10:51...	Malware_Build_...	2508	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
10:51...	Malware_Build_...	2508	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
10:51...	Malware_Build_...	2508	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
10:51...	Malware_Build_...	2508	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
10:51...	Malware_Build_...	2508	RegQueryKey	HKLM	SUCCESS	Query: Handle Tag...
10:51...	Malware_Build_...	2508	RegQueryKey	HKLM	SUCCESS	Query: Name
10:51...	Malware_Build_...	2508	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	NAME NOT FOUND Desired Access: R...	
10:51...	Malware_Build_...	2508	RegQueryKey	HKLM\Software\Wow6432Node\Micro...	SUCCESS	Query: Handle Tag...
10:51...	Malware_Build_...	2508	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	
10:51...	Malware_Build_...	2508	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	KeySetInformation...
10:51...	Malware_Build_...	2508	RegQueryKey	HKLM\SOFTWARE\Wow6432Node\VM...	SUCCESS	Query: Handle Tag...
10:51...	Malware_Build_...	2508	RegSetValue	HKLM\SOFTWARE\Wow6432Node\VM...	ACCESS DENIED	Type: REG_SZ, Le...
10:51...	Malware_Build_...	2508	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\VM...	SUCCESS	
10:51...	Malware_Build_...	2508	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\WIN...	SUCCESS	
10:51...	Malware_Build_...	2508	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\WIN...	SUCCESS	
10:51...	Malware_Build_...	2508	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
10:51...	Malware_Build_...	2508	RegCloseKey	HKLM	SUCCESS	

Subito dopo aver creato la chiave nel registro di sistema il malware prova a modificarne il valore in una sotto-chiave, non riuscendoci però per un ACCESS DENIED. A questo punto il malware chiude la chiave appena creata.

Time	Process Name	PID	Operation	Path	Result	Detail
11:32...	Malware_Build...	2688	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	KeySetInformation...
11:32...	Malware_Build...	2688	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND	Length: 80
11:32...	Malware_Build...	2688	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS	
11:32...	Malware_Build...	2688	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND	Desired Access: Q...
11:32...	Malware_Build...	2688	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
11:32...	Malware_Build...	2688	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
11:32...	Malware_Build...	2688	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
11:32...	Malware_Build...	2688	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
11:32...	Malware_Build...	2688	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 260
11:32...	Malware_Build...	2688	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
11:32...	Malware_Build...	2688	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
11:32...	Malware_Build...	2688	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
11:32...	Malware_Build...	2688	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
11:32...	Malware_Build...	2688	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 548
11:32...	Malware_Build...	2688	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_DWO...
11:32...	Malware_Build...	2688	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
11:32...	Malware_Build...	2688	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
11:32...	Malware_Build...	2688	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
11:32...	Malware_Build...	2688	RegQueryKey	HKLM	SUCCESS	Query: Name
11:32...	Malware_Build...	2688	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	NAME NOT FOUND	Desired Access: R...
11:32...	Malware_Build...	2688	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
11:32...	Malware_Build...	2688	RegQueryKey	HKLM	SUCCESS	Query: Name
11:32...	Malware_Build...	2688	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\M...	SUCCESS	Desired Access: All...
11:32...	Malware_Build...	2688	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\M...	SUCCESS	KeySetInformation...
11:32...	Malware_Build...	2688	RegQueryKey	HKLM\SOFTWARE\Wow6432Node\M...	SUCCESS	Query: HandleTag...
11:32...	Malware_Build...	2688	RegSetValue	HKLM\SOFTWARE\Wow6432Node\M...	ACCESS DENIED	Type: REG_SZ, Le...
11:32...	Malware_Build...	2688	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\M...	SUCCESS	
11:32...	Malware_Build...	2688	RegCloseKey	HKLM\SOFTWARE\Microsoft\WIN...	SUCCESS	
11:32...	Malware_Build...	2688	RegCloseKey	HKLM\SOFTWARE\Microsoft\WIN...	SUCCESS	
11:32...	Malware_Build...	2688	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
11:32...	Malware_Build...	2688	RegCloseKey	HKLM	SUCCESS	

Funzione che crea il file

Analizzando ora l'attività sul File System possiamo andare a verificare quale chiamata a sistema ha creato il nuovo file msgina32.dll nella cartella del malware. Per farlo abbiamo inserito un nuovo filtro come mostrato in figura sotto e notiamo subito questa operazione CreateFile seguita subito dopo da due WriteFile proprio sul file di nostro interesse msgina32.dll.

The screenshot shows the Process Monitor application interface. On the left, a 'Process Monitor Filter' dialog is open, with its 'Event Class' dropdown set to 'contains' and 'File System' selected. A red box highlights this configuration. Below the dropdown are several filter rules, also highlighted by a red box. The main window displays a log of system events. A red box highlights a specific sequence of events: a 'CreateFile' operation at 11:32... with PID 2688, followed by two 'WriteFile' operations at the same time. The 'CreateFile' event has a detailed tooltip showing it was successful with generic write/read attributes and overwrite disposition. The 'WriteFile' events show offsets 0 and 4.096 respectively. The log continues with other system calls like 'CloseFile', 'QueryNameInfo', and various 'QueryNameInfo' calls for system DLLs.

Time	Process Name	PID	Operation	Path	Result	Detail
11:32...	Malware_Build_...	2688	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows	SUCCESS	Name: \Windows
11:32...	Malware_Build_...	2688	CloseFile	C:\Windows	SUCCESS	
11:32...	Malware_Build_...	2688	CreateFile	C:\Users\user\Desktop\MALWARE\Bu...	SUCCESS	Desired Access: E...
11:32...	Malware_Build_...	2688	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 338.944, Le...
11:32...	Malware_Build_...	2688	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 330.752, Le...
11:32...	Malware_Build_...	2688	ReadFile	C:\Windows\System32\wow64win.dll	SUCCESS	Offset: 62.464, Len...
11:32...	Malware_Build_...	2688	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: R...
11:32...	Malware_Build_...	2688	QueryBasicInfor...	C:\Windows\SysWOW64\sechost.dll	SUCCESS	CreationTime: 14/0...
11:32...	Malware_Build_...	2688	CloseFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	
11:32...	Malware_Build_...	2688	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: R...
11:32...	Malware_Build_...	2688	CreateFileMapp...	C:\Windows\SysWOW64\sechost.dll	FILE LOCKED WI...	SyncType: SyncTy...
11:32...	Malware_Build_...	2688	CreateFileMapp...	C:\Windows\SysWOW64\sechost.dll	SUCCESS	SyncType: SyncTy...
11:32...	Malware_Build_...	2688	CloseFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	
11:32...	Malware_Build_...	2688	CreateFile	C:\Users\user\Desktop\MALWARE\Bu...	SUCCESS	Desired Access: G...
11:32...	Malware_Build_...	2688	WriteFile	C:\Users\user\Desktop\MALWARE\Bu...	SUCCESS	Offset: 0, Length: 4...
11:32...	Malware_Build_...	2688	WriteFile	C:\Users\user\Desktop\MALWARE\Bu...	SUCCESS	Offset: 4.096, Len...
11:32...	Malware_Build_...	2688	CloseFile	C:\Users\user\Desktop\MALWARE\Bu...	SUCCESS	
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\System32\apisetschema.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Users\user\Desktop\MALWARE\Bu...	SUCCESS	Name: \Users\user...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\System32\wow64win.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\System32\wow64.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\SysWOW64\msvcr.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\SysWOW64\pcre4.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Name: \Windows\...
11:32...	Malware_Build_...	2688	QueryNameInfo	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Name: \Windows\...

Conclusioni

Sulla base di tutte le informazioni raccolte dall'analisi statica e dinamica sia basica che avanzata possiamo trarre le seguenti conclusioni:

Il malware importa due librerie che contengono funzioni critiche su Windows ovvero KERNEL32.dll per la creazione, rimozione o modifica dei file (CreateFile, WriteFile, LoadLibrary, LoadResource...), e ADVAPI32.dll per interagire con il registro (RegCreateKeyExA e RegSetValueExA).
Da questa prima analisi statica ci aspettiamo che il malware faccia delle modifiche alle chiavi del registro e crei nuovi file come abbiamo poi dimostrato nell'analisi dinamica con l'esecuzione del malware.

Nel nostro caso il malware si bloccava nella fase di scrittura della chiave Winlogon con codice di errore ACCESS DENIED quindi non riusciva a completare la sua funzione.

Il malware risulta però essere molto pericoloso nelle versioni di Windows precedenti al 7 dal momento che msgina32.dll non era stata deprecata, quindi modificabile e sostituibile con file malevolo per ottenere l'accesso alle credenziali. Con queste informazioni possiamo classificare il malware come un dropper (crea msgina32.dll e se avesse i permessi TGAD0.exe come confermato da VirusTotal).

Dropped Files (5) 			
Scanned	Detections	File type	Name
2022-04-02	44 / 69	Win32 DLL	msgina32.dll
2024-08-16	55 / 74	Win32 DLL	TGAD0.exe

Conclusioni

Da VirusTotal possiamo notare che il malware effettua anche delle connessioni probabilmente malevole, forse per inviare le credenziali di accesso rubate con il file malevolo. Dall'analisi delle funzioni però non abbiamo notato librerie importate che permettono la connessione ad internet come ad esempio WININET.dll o WS2_32.dll (Winsock). Possiamo supporre che, dal momento che il malware non termina la sua attività di conseguenza non riesca ad arrivare al punto dove crea il file TGAD0.exe che si occupa poi di effettuare le connessioni ed inviare le credenziali rubate all'attaccante.

Contacted URLs (9) ⓘ			
Scanned	Detections	Status	URL
2024-08-23	0 / 96	200	http://crl4.digicert.com/DigiCertGlobalRootCA.crl
2024-02-12	0 / 91	200	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSPwi+rBFUJh18C0nqAFI8du2+GkP0xGIOCEAEF0almGak0

Contacted IP addresses (18) ⓘ			
IP	Detections	Autonomous System	Country
104.85.240.187	0 / 94	16625	US
114.114.114.114	2 / 94	21859	CN
117.18.237.29	0 / 94	15133	US
192.168.0.25	0 / 94	-	-
192.168.0.63	0 / 94	-	-
192.229.211.108	0 / 94	15133	US
20.80.129.13	0 / 94	8075	US

DAY 3

Traccia

GINA

GINA (Graphical identification and authentication) è un componente legato di Windows che permette l'autenticazione degli utenti tramite interfaccia grafica. Esso permette agli utenti di inserire username e password nel classico riquadro Windows.

- Cosa può succedere se il file .dll legato viene sostituito con un file .dll malevolo, che intercetta i dati inseriti?
- Sulla base della risposta sopra, delineate il profilo del malware e delle sue funzionalità.

Unite tutti i punti per creare un grafico che ne rappresenti lo scopo ad alto livello.

Overview GINA

- Componente chiave del processo di autenticazione in Windows 2000, XP (sistemi pre-Vista).
 - Gestisce l'interfaccia grafica per l'inserimento di credenziali.
 - Responsabile della schermata di login degli utenti.
- Funzionalità di GINA.dll:
 - Personalizzazione del processo di login e autenticazione.
 - Supporto per metodi di autenticazione alternativi (smart card, biometria, rete).
 - Ampio utilizzo in ambienti aziendali con esigenze di sicurezza avanzata.
- Rischi associati a GINA.dll:
 - Obiettivo privilegiato per attacchi mirati alla sostituzione della libreria.
 - Potenziale compromissione del processo di autenticazione.
 - Intercettazione delle credenziali degli utenti da parte di malware.



Conseguenze sostituzione con .dll malevolo

La sostituzione di un file legittimo come GINA.dll con una versione malevola può avere conseguenze devastanti per la sicurezza di un sistema Windows, in particolare nelle versioni precedenti a Windows Vista.

Di seguito vengono esaminati in dettaglio i principali impatti che questo tipo di attacco può avere:

- Intercettazione delle credenziali
- Accesso non autorizzato
- Compromissione della sicurezza complessiva del sistema

In sintesi, la sostituzione del file GINA legito con una versione malevola rappresenta una grave minaccia alla sicurezza, poiché permette agli attaccanti di intercettare informazioni sensibili e ottenere accesso non autorizzato al sistema.

Intercettazione credenziali

GINA.dll è un componente critico che gestisce l'autenticazione degli utenti attraverso un'interfaccia grafica. Quando un utente tenta di accedere al sistema, GINA.dll presenta la schermata di login e gestisce l'inserimento di username e password.

- Se GINA.dll viene sostituita con una versione malevola, il malware può intercettare tutte le credenziali inserite dagli utenti. Ogni volta che un utente digita il proprio nome utente e password, queste informazioni vengono registrate dal malware.
- L'intercettazione delle credenziali permette all'attaccante di acquisire informazioni sensibili senza che l'utente o l'amministratore di sistema se ne accorgano. Questa capacità rappresenta una grave violazione della privacy e della sicurezza del sistema.

Accesso non autorizzato

Le credenziali intercettate possono essere utilizzate dagli attaccanti per ottenere accesso non autorizzato al sistema. Questo accesso può avvenire in diverse forme, ognuna con conseguenze potenzialmente gravi:

- **Accesso ai privilegi dell'utente:**

- Con le credenziali rubate, un attaccante può accedere al sistema con i privilegi dell'utente legittimo. Se l'utente compromesso ha diritti amministrativi, l'attaccante può eseguire operazioni di amministrazione, come l'installazione di software, la modifica delle configurazioni di sistema e la creazione di nuovi account utente.

- **Esecuzione di ulteriori attacchi:**

- Una volta ottenuto l'accesso, l'attaccante può eseguire ulteriori attacchi, come l'escalation dei privilegi per ottenere accesso root o amministratore, l'esecuzione di ransomware o il lancio di attacchi DDoS (Distributed Denial of Service) dal sistema compromesso.

- **Modifica delle configurazioni critiche:**

- Con l'accesso non autorizzato, un attaccante può modificare le configurazioni critiche del sistema, compromettendo la stabilità e la sicurezza del sistema stesso. Questo potrebbe includere la disabilitazione delle difese di sicurezza o l'apertura di backdoor per un accesso futuro.

Compromissione della sicurezza

L'accesso non autorizzato e l'intercettazione delle credenziali sono solo il primo passo. Il malware può sfruttare le credenziali rubate per compiere ulteriori azioni dannose che compromettono gravemente la sicurezza del sistema:

- Installazione di software malevolo:
 - Utilizzando le credenziali acquisite, il malware può installare ulteriori software dannosi, come spyware, keylogger o botnet, ampliando il controllo dell'attaccante sul sistema.
- Esecuzione di comandi dannosi:
 - Il malware può eseguire comandi specifici per disabilitare i meccanismi di sicurezza del sistema, cancellare file critici, o criptare dati sensibili in un attacco di ransomware.
- Compromissione della macchina virtuale e dei dati:
 - Se il sistema compromesso è parte di una macchina virtuale o di una rete più ampia, il malware può propagarsi ad altre macchine virtuali, aumentando l'estensione del danno. I dati sensibili presenti sul sistema possono essere rubati, distrutti o resi inaccessibili.

Diagramma di flusso



Analisi ad alto livello

Infezione del sistema:

- Fase iniziale dell'attacco.
- Vettori comuni: email di phishing, download da siti infetti, vulnerabilità del sistema o delle applicazioni.

Esecuzione del malware:

- Il malware viene eseguito nel sistema.
- Modalità di esecuzione: automatica (script/programmi avviati all'accensione) o manuale (utente clicca su file eseguibile apparentemente innocuo).

Creazione di GINA.dll malevolo:

- Il malware sostituisce GINA.dll con una versione malevola.
- Scopo: Intercettare le credenziali di accesso degli utenti.

Analisi ad alto livello

Ottenimento della persistenza:

- Il malware implementa meccanismi per mantenere l'accesso al sistema.
- Modifica delle chiavi di registro per avviare il malware all'accensione del sistema (chiave: "SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon").

Furto delle credenziali di accesso:

- Il malware utilizza la versione malevola di GINA.dll per intercettare le credenziali degli utenti.
- Le credenziali rubate vengono inviate agli attaccanti per ottenere accesso non autorizzato al sistema e ad altre risorse protette.

Conclusioni

Analisi iniziale:

- Analisi del file eseguibile Malware_Build_Week_U3.
- Identificazione di parametri e variabili nella funzione Main().
- Esplorazione delle sezioni principali del file e delle librerie importate.
- Formulazione di ipotesi preliminari sulle funzionalità del malware.

Approfondimento tecnico:

- Analisi della funzione alla locazione 00401021:
 - Studio del passaggio dei parametri.
 - Traduzione delle istruzioni (00401027-00401029) in costrutti C.
- Valutazione del parametro “ValueName” alla locazione 00401047:
- Analisi delle routine tra 00401080 e 00401128:
 - Determinazione del valore del parametro "ResourceName".
 - Comprensione delle funzionalità implementate dal malware.

Conclusioni

Esecuzione in ambiente controllato:

- Utilizzo di Process Monitor per osservare le modifiche al sistema:
 - Attività sul registro di Windows.
 - Modifiche al file system (creazione di chiavi di registro e modifiche delle cartelle).

Esplorazione dell'uso di GINA.dll:

- Analisi dell'impatto della sostituzione di GINA.dll con una versione malevola.
- Identificazione del rischio di intercettazione delle credenziali di accesso.
- Osservazione dei meccanismi per ottenere persistenza nel sistema.

Conclusioni generali:

- Il malware utilizza vari meccanismi per:
 - Infettare il sistema.
 - Eseguire codice malevolo.
 - Ottenere persistenza.
 - Rubare informazioni sensibili.
- Le informazioni ottenute costituiscono una base solida per sviluppare strategie di difesa e mitigazione.
- Miglioramento della sicurezza complessiva del sistema contro tali minacce.

DAY 4

Traccia

- <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/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.)

4.1. Analisi Anyrun - Link 1

Descrizione

Nomi dei File: vidar.exe

Percorso: "C:\Users\admin\Desktop\66bddfcb52736_vidar.exe"

Origine: 66bddfcb52736_vidar.exe

Punteggio di Minaccia:

- **vidar.exe:** 100 su 100 (Malevolo)

The screenshot shows the Anyrun analysis interface. At the top, it displays the file name "66BDDFCB52736_VIDAR.EXE" and its MD5 hash "FEDB687ED23F77925B35623027F799BB". Below this, there are fields for SHA1 ("7F27D0290ECC2C81BF2B2D0FA1026F54FD687C81") and SHA256 ("325396D5FFCA8546730B9A56C2D0ED99238D48B5E1C3C49E7D027505EA1 388D1"). A large red arrow points from the bottom right towards the "Warning / Suspicious" section. This section contains the warning message "Drops the executable file immediately after the start".

The screenshot shows the Anyrun analysis interface. At the top, it displays the process ID "ID 6780" and status "Malicious". The file name "66bddfcb52736_vidar.exe" is shown with a red box around it. To the right, a large red circle highlights the score "100 OUT OF 100". Below this, the "Command line" field shows the path "C:\Users\admin\Desktop\66bddfcb52736_vidar.exe". A red box also surrounds this field. A red arrow points from the bottom left towards the "Warning 1" section. This section contains the warning message "Drops the executable file immediately after the start". Further down, another red box surrounds the "Other 2" section, which lists T1012 Query Registry (2) and T1082 System Information Discovery (2), both of which involve reading the computer name and checking supported languages.

4.1. Analisi Anyrun - Link 1

Comportamento Osservato

Viene catalogato come **loader**, ovvero un eseguibile che rilascia un payload infetto. È capace di analizzare il sistema nel quale si trova per poi installare altri malware come **trojan** o **stealer**. I malware di tipo **loader** di solito si diffondono con le campagne di mail phishing e sfruttando anche l'ingegneria sociale per indurre l'utente inconsapevole ad eseguire i file malevoli. I **loaders** impiegano delle tattiche avanzate di **persistenza nel sistema** ed elusione degli antivirus per non essere rilevati. Gli **stealer** sono un tipo di malware che cercano di effettuare l'accesso non autorizzato al sistema vittima per rubare informazioni dell'utente (credenziali, criptovalute, files) e trasferirle verso l'attaccante. Sono anche in grado di registrare l'attività della tastiera e di fare screenshots.

Attività malevole: furto di dati personali e credenziali del browser.

Attività sospette: esegue il drop dell'eseguibile infetto subito dopo il suo avvio, lettura delle impostazioni di Internet Explorer, accesso alle Trust Settings di Windows, verifica dei programmi installati, esegue un drop di dll del browser Mozilla, drop di dll di C-runtime, sovrascrittura dell'eseguibile originale e rilascio dell'eseguibile Windows legittimo, utilizzo di timeout.exe per ritardare l'esecuzione dell'eseguibile, avvio di cmd.exe per eseguire comandi dal prompt.

4.1. Analisi Anyrun - Link 1

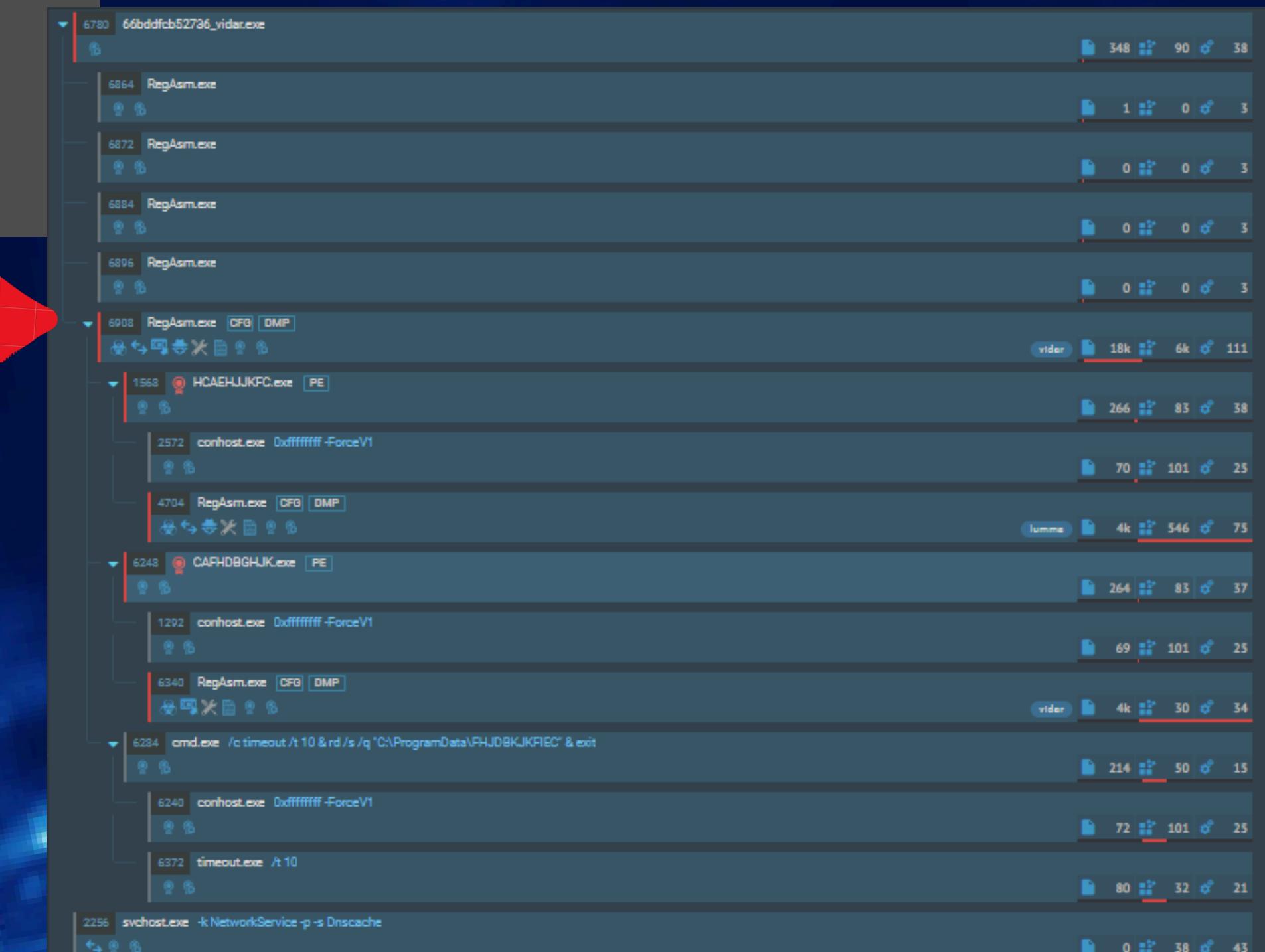
Attività generiche: verifica delle lingue supportate nel sistema e del nome della macchina, verifica del proxy server, lettura del GUID della macchina, creazione di file nella directory dell'eseguibile, lettura delle software policy settings, lettura delle info sul processore e variabili d'ambiente, creazione di file nella cartella temporanea.

Processi Attivati:

- hcaejjkfc.exe: processo malevolo creato dal malware che si occupa di recuperare informazioni sulla macchina vittima dalle chiavi di registro di Windows
(**HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions**,
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName). Il percorso dell'eseguibile è "C:\ProgramData\HCAEHJJKFC.exe".
- regasm.exe: Si tratta dell'**Assembly Registration Tool** di Microsoft. Esso legge i metadati all'interno dell'assembly e aggiunge le entrate necessarie nel registro di sistema per permettere ai client COM di creare classi .NET in modo trasparente.
- cmd.exe: La shell dei comandi di Windows, usata per eseguire script e comandi specifici. Il malware sfrutta questo processo per eseguire comandi in modo nascosto.
- timeout.exe: Si tratta di un eseguibile legittimo di Windows che risiede al percorso **C:\Windows\System32**. Di fatto è una command-line utility che serve per mettere in pausa per un certo numero di secondi un processo, ad esempio, per attendere l'esecuzione di un'altra applicazione. Accade che ci siano malware che utilizzino questo eseguibile per camuffarsi.

4.1. Analisi Anyrun - Link 1

- CAFHDBGHJK.exe: eseguibile malevolo droppato dal malware che si occupa di recuperare informazioni sulla macchina vittima dalle chiavi di registro di Windows. Percorso dell'eseguibile "C:\ProgramData\CAFHDBGHJK.exe".



4.1. Analisi Anyrun - Link 1

- conhost.exe: Il nome del file è un acronimo che sta per **Console Window Host**, è un processo Microsoft legittimo che gestisce le richieste di input/output per le applicazioni della console (riga di comando).
- timeout.exe: Si tratta di un eseguibile legittimo di Windows che risiede al percorso “**C:\Windows\System32**”. Di fatto è una command-line utility che serve per mettere in pausa per un certo numero di secondi un processo, ad esempio , per attendere l'esecuzione di un'altra applicazione.
- svchost.exe: È una categoria di processi Windows usati per svolgere le funzioni generiche del sistema operativo. In genere è un processo legittimo, e il suo eseguibile si trova in “**C:\Windows\System32**”.

Process details ID 1292 No verdict

conhost.exe
Console Window Host
Username: admin
Start: +21362ms

Command line
\\??(C:\\WINDOWS\\system32\\conhost.exe 0xffffffff -ForceV1)

More Info

No suspicious events

Process details ID 6372 No verdict

timeout.exe
timeout - pauses command processing
Username: admin
Start: +22938ms

Command line
timeout /t 10

More Info

Process details ID 6372 No verdict

timeout.exe
timeout - pauses command processing
Username: admin
Start: +22938ms

Command line
timeout /t 10

More Info

4.1. Analisi Anyrun - Link 1

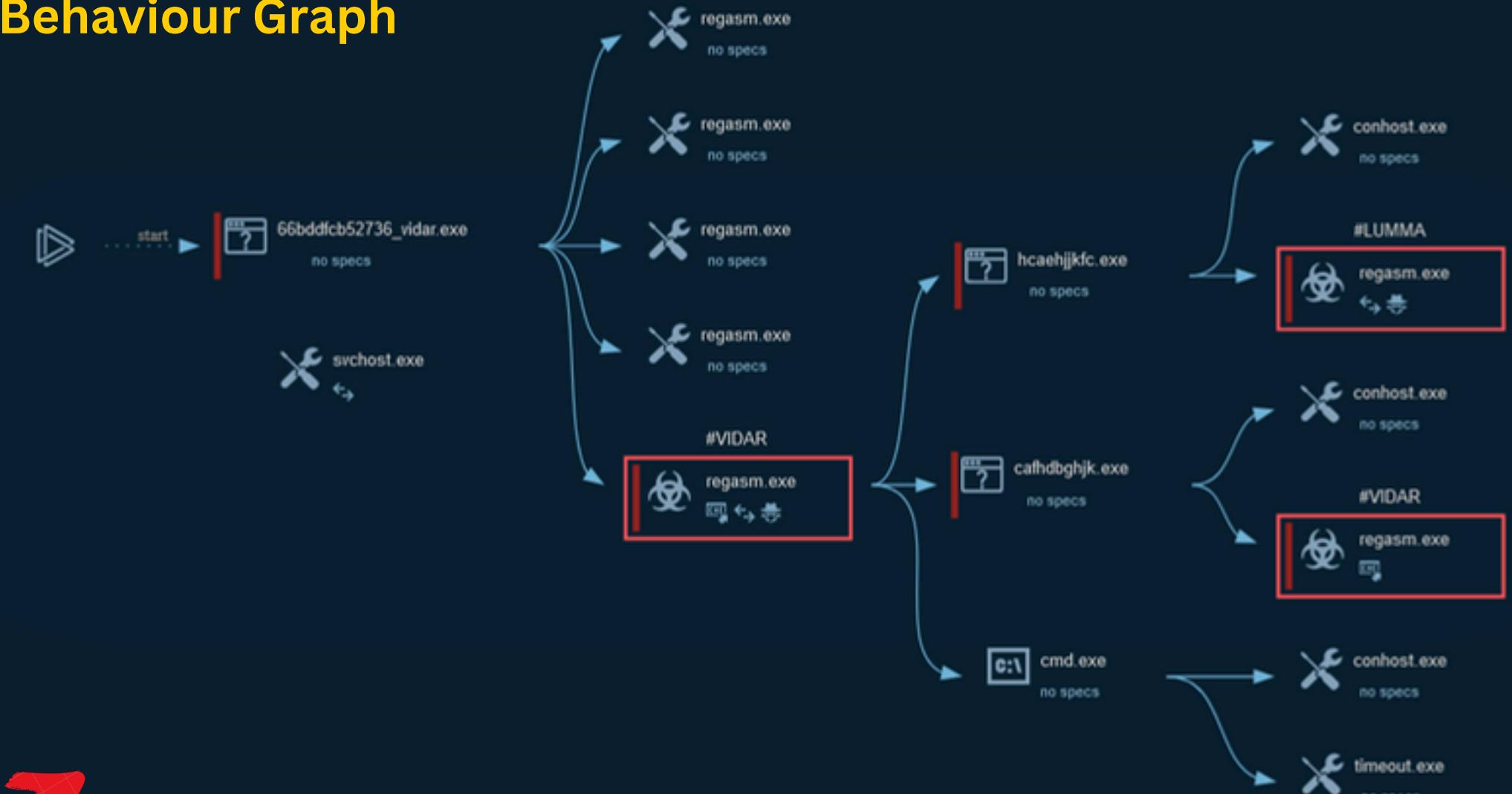
Conclusioni

vidar.exe

Si tratta di un malware di tipo **loader** che fa il drop di altri malware scaricati da URL infetti come gli **stealer**.

Raccomandazioni per l'utente: **Eliminazione** immediata del file. Se il malware è già in esecuzione provvedere ad una scansione antivirus completa del sistema o eventualmente se necessario ad un ripristino del sistema ad uno stato precedente all'infezione.

Behaviour Graph



4.1. Analisi Anyrun - Link 1

regasm.exe

Può accadere che qualche malware si camuffi usando il nome di questo strumento di Microsoft. Per evitare che ciò accada serve installare sempre software Microsoft autentico.

In questo caso, come descritto in precedenza, avviene che uno di questi eseguibili che sono parte di Windows venga usato dal malware per scopi malevoli. Qui verrà usato per agire come uno stealer (tipo di malware descritto in precedenza), cioè tenterà di accedere alle informazioni utente memorizzate nel sistema per poi trasferirle verso l'esterno, magari all'IP di chi ha organizzato l'attacco.

Raccomandazioni per l'utente: Capita che possa trattarsi anche di **falso positivo**, ma per una maggiore sicurezza si consiglia di mettere l'eseguibile in quarantena per studiarne meglio il comportamento. Se l'analisi risulta positiva allora procedere all'**eliminazione**, altrimenti non si corre alcun rischio.



4.1. Analisi Anyrun - Link 1

HCAEHJJKFC.exe

Raccomandazioni per l'utente: **Eliminazione** immediata del file. Se il malware è già in esecuzione provvedere ad una scansione antivirus completa del sistema o eventualmente se necessario ad un ripristino del sistema ad uno stato precedente all'infezione.

The screenshot shows the Anyrun analysis interface for the file HCAEHJJKFC.exe. The process details panel indicates the file is Malicious (ID 1568). The command line is listed as "C:\ProgramData\HCAEHJJKFC.exe". Under the 'Other' section, two T1012 indicators are shown: "Query Registry (2)" which includes "Reads the computer name" and "Checks supported languages", and "System Information Discovery (2)" which also includes "Reads the computer name" and "Checks supported languages". A large red arrow points from the 'Command line' section to the '100 OUT OF 100' score in the bottom right corner. Another red arrow points from the 'Other' section back towards the top left of the interface.

Process details ID 1568 Malicious

HCAEHJJKFC.exe

AUTO File System Format Utility

Username: admin Start: +20553ms Indicators: ⓘ

Command line

"C:\ProgramData\HCAEHJJKFC.exe"

More Info

Other 2

T1012 Query Registry (2)
Reads the computer name
Checks supported languages

T1082 System Information Discovery (2)
Reads the computer name
Checks supported languages

100 OUT OF 100

4.1. Analisi Anyrun - Link 1

CAFHDBGHJK.exe

Raccomandazioni per l'utente: **Eliminazione** immediata del file. Se il malware è già in esecuzione provvedere ad una scansione antivirus completa del sistema o eventualmente se necessario ad un ripristino del sistema ad uno stato precedente all'infezione.

Process details ID 6248 Malicious

CAFHDBGHJK.exe
Auto File System Format Utility

Username: admin Start: +21335ms Indicators: ⓘ

Command line
"C:\ProgramData\CAFHDBGHJK.exe"

[More Info](#)

Other 2

- T1012 Query Registry (2)
 - Checks supported languages
 - Reads the computer name
- T1082 System Information Discovery (2)
 - Checks supported languages
 - Reads the computer name

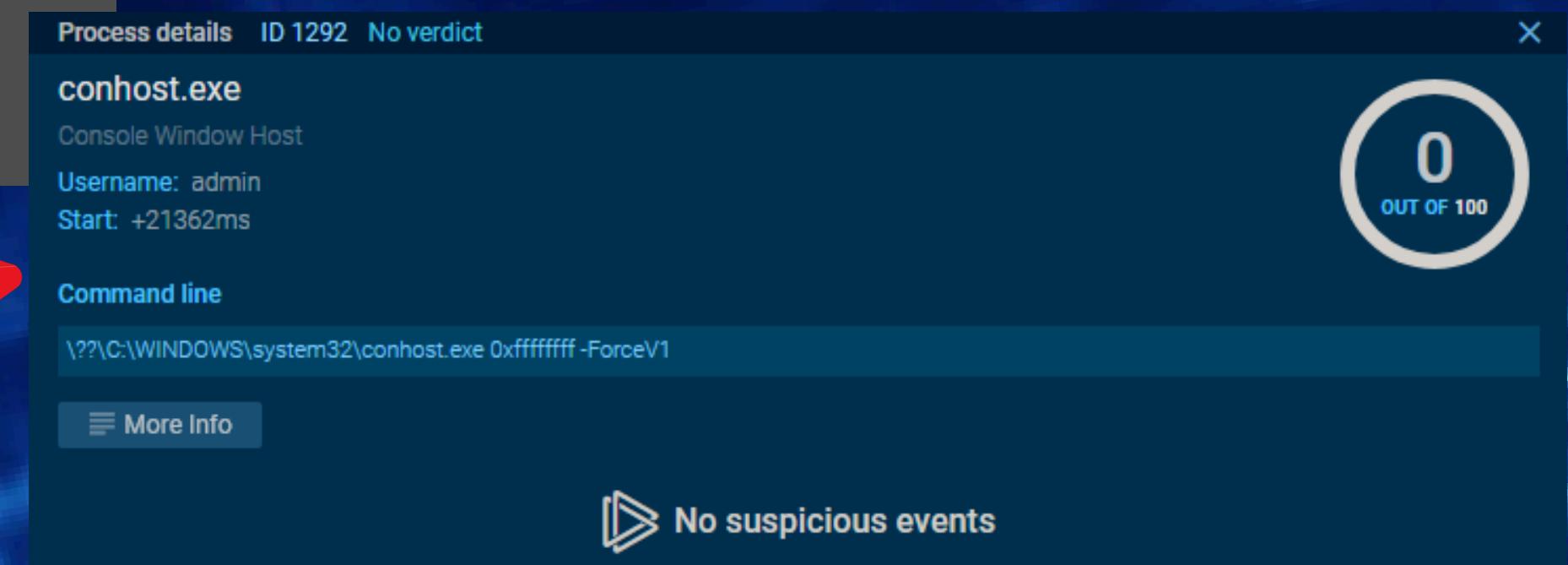
100 OUT OF 100

Hide all

4.1. Analisi Anyrun - Link 1

conhost.exe

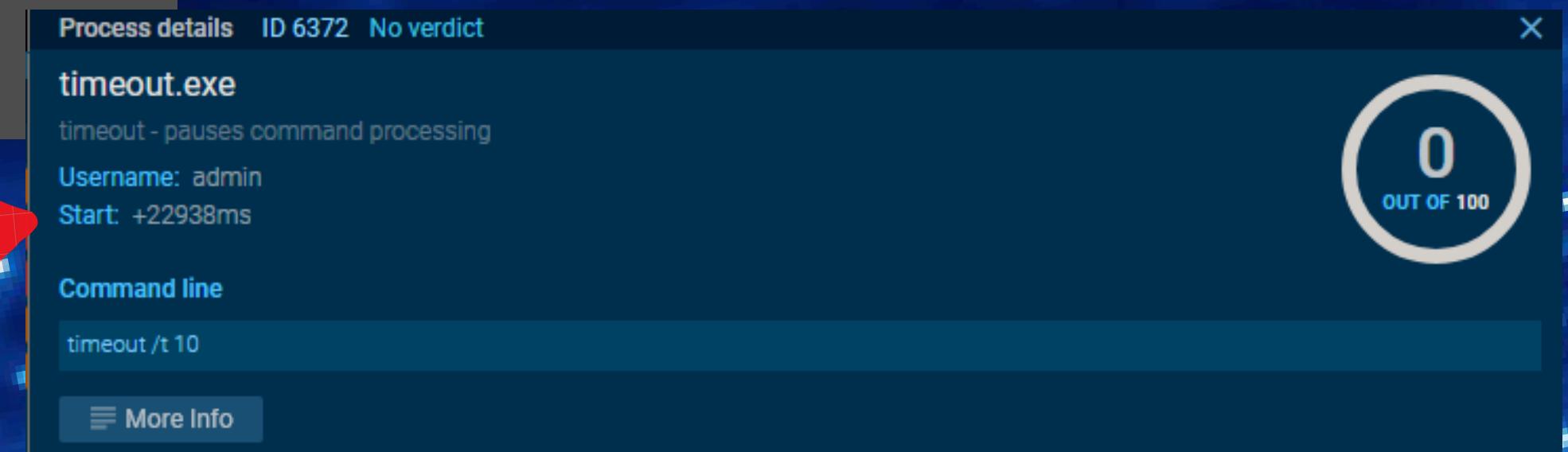
Raccomandazioni per l'utente: Si tratta di un processo di sistema appartenente a Windows che non presenta alcun rischio legato alla sua esecuzione. Purtroppo in alcuni casi, come in questo che stiamo analizzando, è possibile che un malware lo avvii per svolgere pratiche poco lecite, quindi potrebbe trattarsi di un falso negativo.



4.1. Analisi Anyrun - Link 1

timeout.exe

Raccomandazioni per l'utente: Accade che ci siano malware che utilizzino questo eseguibile per camuffarsi. Nella maggioranza dei casi trattasi di un eseguibile legittimo. Ma se il software antivirus lo segnala come una possibile minaccia, allora provvedere subito a metterlo in **quarantena** per analisi più approfondite e, se necessario, provvedere all'**eliminazione**.



A screenshot of the Anyrun analysis interface showing the process details for 'timeout.exe'. The window title is 'Process details ID 6372 No verdict'. The process name is 'timeout.exe' with the description 'timeout - pauses command processing'. The user is 'admin' and the start time is '+22938ms'. The command line is 'timeout /t 10'. A large red arrow points from the text above to this window. In the top right corner of the window, there is a circular progress bar with the number '0' and the text 'OUT OF 100'.

Process details ID 6372 No verdict

timeout.exe
timeout - pauses command processing

Username: admin
Start: +22938ms

Command line
timeout /t 10

More Info

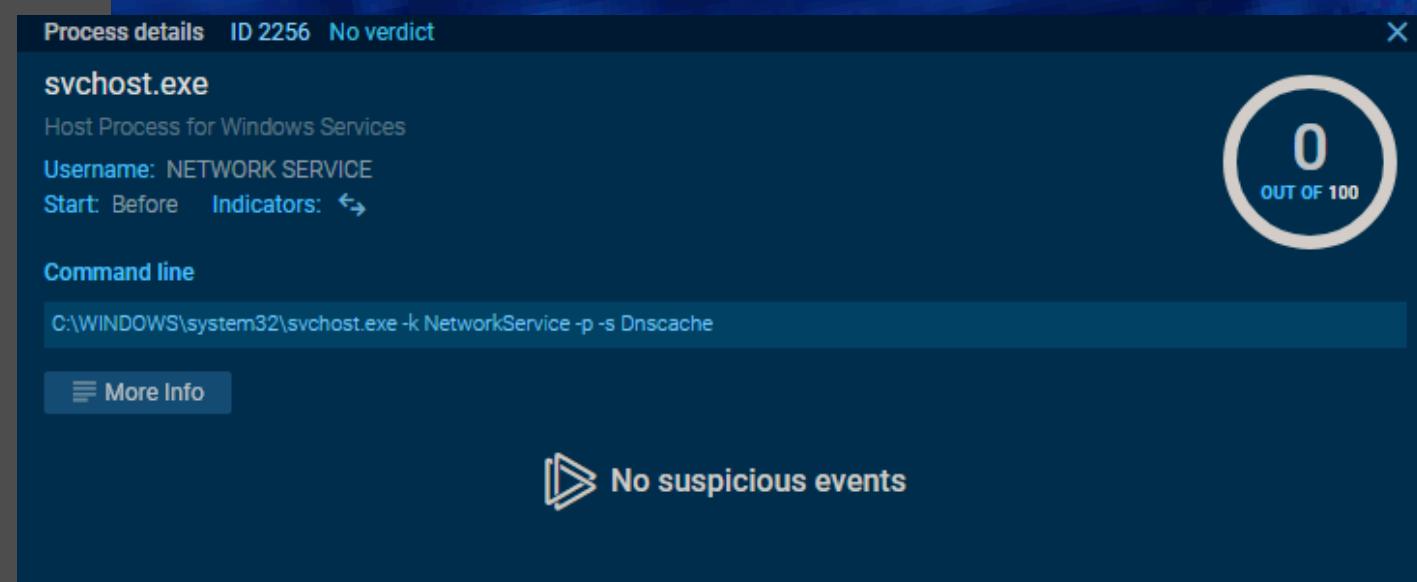
0 OUT OF 100

4.1. Analisi Anyrun - Link 1

svhost.exe

Di fatto è un nome che viene assegnato ai processi host all'interno del sistema operativo. Infatti, aprendo Gestione Attività di Windows, si può vedere come siano in esecuzione numerosi servizi di sistema che sono identificati per mezzo di questo appellativo. Questi processi servono per caricare file dll (Dynamic Link Libraries), ovvero, librerie dinamiche (non collegate staticamente all'eseguibile) utili alle varie applicazioni per usufruire delle funzionalità principali del sistema. Se si fa clic sul processo nella scheda Processi di Gestione Attività, comparirà il nome del servizio che sta sfruttando il processo host per essere eseguito.

Raccomandazioni per l'utente: i processi host di Windows non sono altro che servizi di sistema eseguiti sotto un nome di processo generico, appunto svhost.exe. Ma alcuni malware possono sfruttare questo tipo di funzionamento per camuffarsi all'interno del sistema e rendersi invisibili sia all'utente che ai sistemi antivirus. Se ci si accorge che uno di questi servizi sta usando più risorse del normale, procedere subito a controllare il nome del servizio associato a quel processo host e se si ritiene opportuno, previa scansione antivirus, cessarne l'esecuzione e metterlo in quarantena.



4.2. Analisi Anyrun - Link 2

Descrizione

Nomi dei File: Jvczfhe.exe e Muadnrd.exe

Origine: Entrambi i file sono stati eseguiti e analizzati tramite AnyRun. I file sono stati scaricati da un repository GitHub <https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe>

Punteggio di Minaccia:

- Jvczfhe.exe: 51 su 100 (Sospetto)
- Muadnrd.exe: 62 su 100 (Sospetto)

The screenshot shows the AnyRun interface with two main windows. On the left, a GitHub repository page for 'MELITERRER/kioluu' is displayed, showing files 'Muadnrd.exe' and 'Jvczfhe.exe'. A large red arrow points from the top-left towards this window. On the right, the AnyRun analysis results are shown. The title bar says 'Malicious activity' with the URL 'https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe'. Below it, a 'Processes' section lists several Firefox processes. The first process is highlighted with a red border and shows details: 'Process ID: 4552', 'File: firefox.exe', 'URL: https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe', 'CPU usage: 154 %', 'Memory usage: 74 MB of 25 MB'. Other processes listed include '4550', '4551', '4553', '4554', '4555', and '7048'. The bottom of the interface features a navigation bar with links like 'Home', 'About', 'Help', 'Logout', and 'Sign up'.

4.2. Analisi Anyrun - Link 2

Comportamento Osservato

Processi Attivati:

Entrambi i file utilizzano il processo legittimo firefox.exe per mascherare le loro attività malevoli, avviando una serie di processi tra cui cmd.exe, timeout.exe, Conhost.exe, WerFault.exe e InstallUtil.exe, in particolare, è segnalato come una possibile minaccia.

Nel dettaglio:

- **cmd.exe:** La shell dei comandi di Windows, usata per eseguire script e comandi specifici. Il malware sfrutta questo processo per eseguire comandi in modo nascosto.
- **timeout.exe:** Comando utilizzato per introdurre ritardi nell'esecuzione, spesso usato dai malware per sfuggire alle analisi automatizzate che si concentrano sui primi momenti dopo l'esecuzione.

The screenshot shows a detailed analysis of a threat's techniques. The main title is "Techniques details" with a subtitle "Get to know what this threat is about". It lists "Subtechniques" as T1059.003 and "«Windows Command Shell»". Below this, it specifies "Permissions required: User" and "Data sources: Process: Process Creation, Command: Command Execution". On the right, there is a "Warning (4)" section. Two specific subtechniques are highlighted with red boxes:

- Uses TIMEOUT.EXE to delay execution (2)
 - 7520 cmd.exe (1)
 - 7876 cmd.exe (1)
- Starts CMD.EXE for commands execution (2)
 - 7492 Jscript.exe (1)
 - 7824 Msasnpl.exe (1)

4.2. Analisi Anyrun - Link 2

- **InstallUtil.exe**: Uno strumento di Microsoft utilizzato per l'installazione e la configurazione di applicazioni. Il malware lo usa per eseguire o configurare componenti malevoli, rendendo più difficile il rilevamento.
- **WerFault.exe**: Processo legato alla gestione degli errori di Windows. La sua esecuzione in questo contesto può indicare che il malware sta cercando di manipolare o sfruttare i crash di sistema per ottenere un vantaggio.
- **conhost.exe**: Il processo Console Window Host è legato alla gestione delle finestre della console nei sistemi Windows. In questo caso, il malware utilizza conhost.exe in combinazione con cmd.exe per eseguire comandi di shell in background, mascherando ulteriormente le sue operazioni.



4.2. Analisi Anyrun - Link 2

Attività del Registro di Sistema:

- I malware hanno effettuato letture e modifiche al registro, in particolare alle chiavi relative a Microsoft Office e alle impostazioni di sicurezza di Internet Explorer e Windows. Queste modifiche riducono le difese del sistema contro altre potenziali minacce.
- È stata tentata la disabilitazione della registrazione degli eventi di Windows, una tecnica comune per nascondere le tracce delle attività malevoli.

The screenshot shows the Anyrun analysis interface. On the left, there is a list of detected behaviors:

- Other / Environment: Reads Microsoft Office registry keys (T1012 Query Registry)
- Operation: READ
- Name: HTTP
- Value:
- Key: HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\OFFICE\16.0\ACCESS\CAPABILITIES\URLASSOCIATIONS

On the right, a tooltip provides detailed information about a specific registry operation:

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

A large red arrow points from the bottom-left towards the tooltip, highlighting the 'ProxyBypass' entry.

4.2. Analisi Anyrun - Link 2

Raccolta di Informazioni di Sistema:

- Entrambi i file hanno raccolto informazioni critiche sul sistema, come il GUID della macchina e altri valori relativi all'ambiente di sistema. Queste informazioni possono essere utilizzate per personalizzare ulteriori attacchi o per esfiltrare dati sensibili.

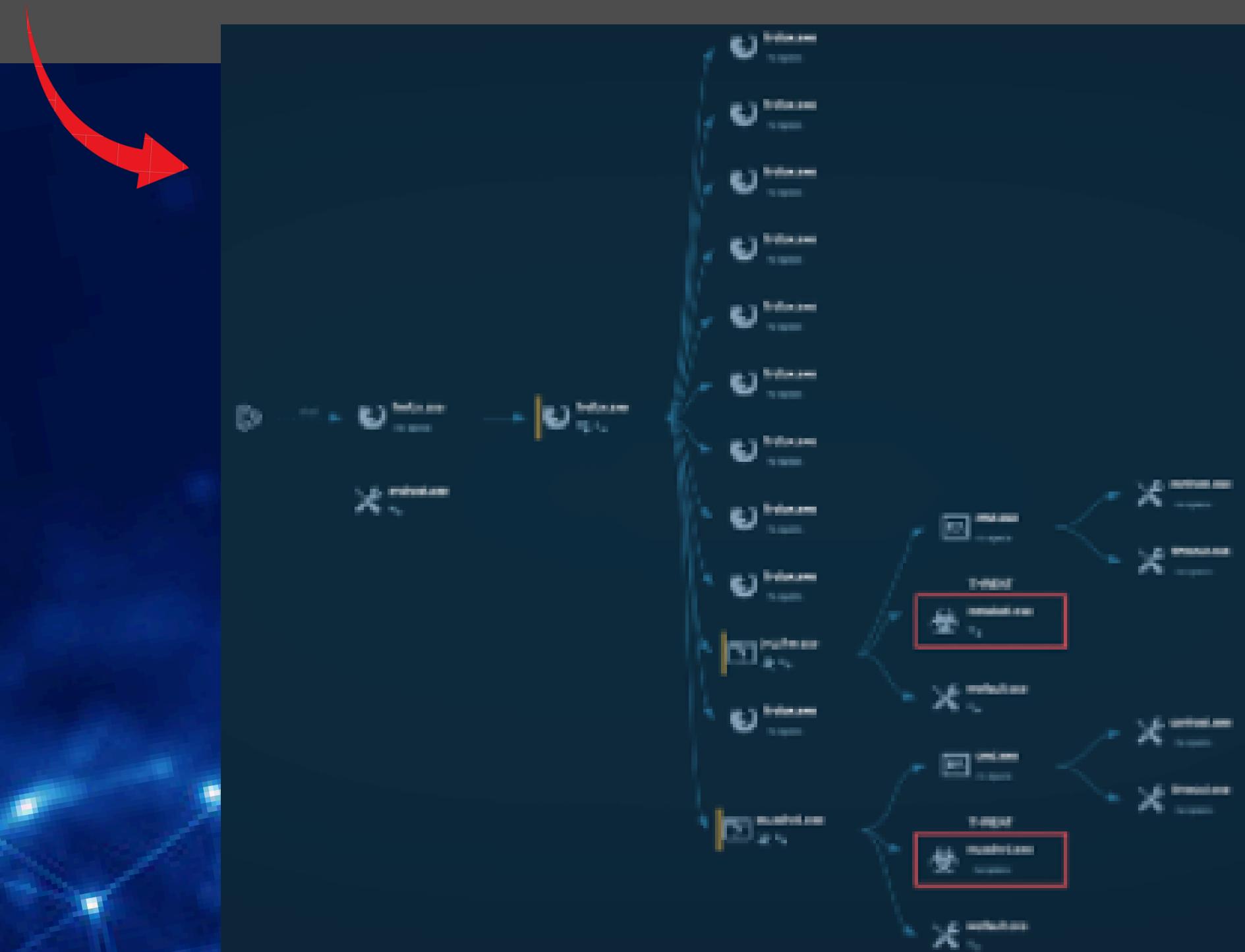
Utilizzo di NetReactor:

- NetReactor è stato identificato come parte del processo di protezione e offuscamento del codice. Questo strumento è utilizzato dai creatori del malware per rendere difficile l'analisi del codice e ritardare il rilevamento da parte dei software di sicurezza. L'offuscamento avanzato che offre NetReactor indica che il malware è progettato per evitare l'analisi forense e complicare il reverse engineering.

4.2. Analisi Anyrun - Link 2

Behavior Graph

Il flusso di esecuzione mostra che i malware operano utilizzando una struttura a catena, avviando numerosi processi legittimi per eseguire operazioni malevole e mantenere la persistenza nel sistema.



4.2. Analisi Anyrun - Link 2

Classificazione:

- **Vero Positivo:** I comportamenti osservati in entrambi i file indicano chiaramente che si tratta di malware. Le tecniche di evasione utilizzate, la manipolazione delle impostazioni di sistema, l'offuscamento tramite NetReactor, e il tentativo di nascondere le attività mediante la disabilitazione dei log, confermano la natura malevola dei file.

Raccomandazioni:

1. Quarantena dei File:

Jvczfhe.exe e Muadnrd.exe dovrebbero essere immediatamente messi in quarantena. Questo passaggio è cruciale per evitare che i file possano continuare a operare o propagarsi all'interno del sistema. La quarantena permette inoltre di preservare i file per ulteriori analisi forensi, se necessario.

2. Eliminazione dei File:

Dopo la quarantena e le analisi necessarie, se confermati come malevoli, Jvczfhe.exe e Muadnrd.exe devono essere eliminati dal sistema. È importante usare strumenti di sicurezza che possano garantire la completa rimozione del malware, comprese le modifiche fatte al registro e alle impostazioni di sistema.

4.2. Analisi Anyrun - Link 2

3. Monitoraggio Continuo del Sistema:

Dopo la rimozione dei malware, è necessario implementare un monitoraggio continuo del sistema per rilevare eventuali attività anomale o segni di persistenza. Questo include il controllo regolare dei log di sistema, l'analisi dei processi in esecuzione, e la verifica delle modifiche non autorizzate al registro.

4. Analisi Forense Approfondita:

A causa dell'uso di NetReactor, è necessario un approccio di analisi forense avanzata per deoffuscare il codice e comprendere pienamente le capacità del malware. Strumenti specializzati in reverse engineering dovrebbero essere impiegati per tentare di decodificare il codice offuscato.



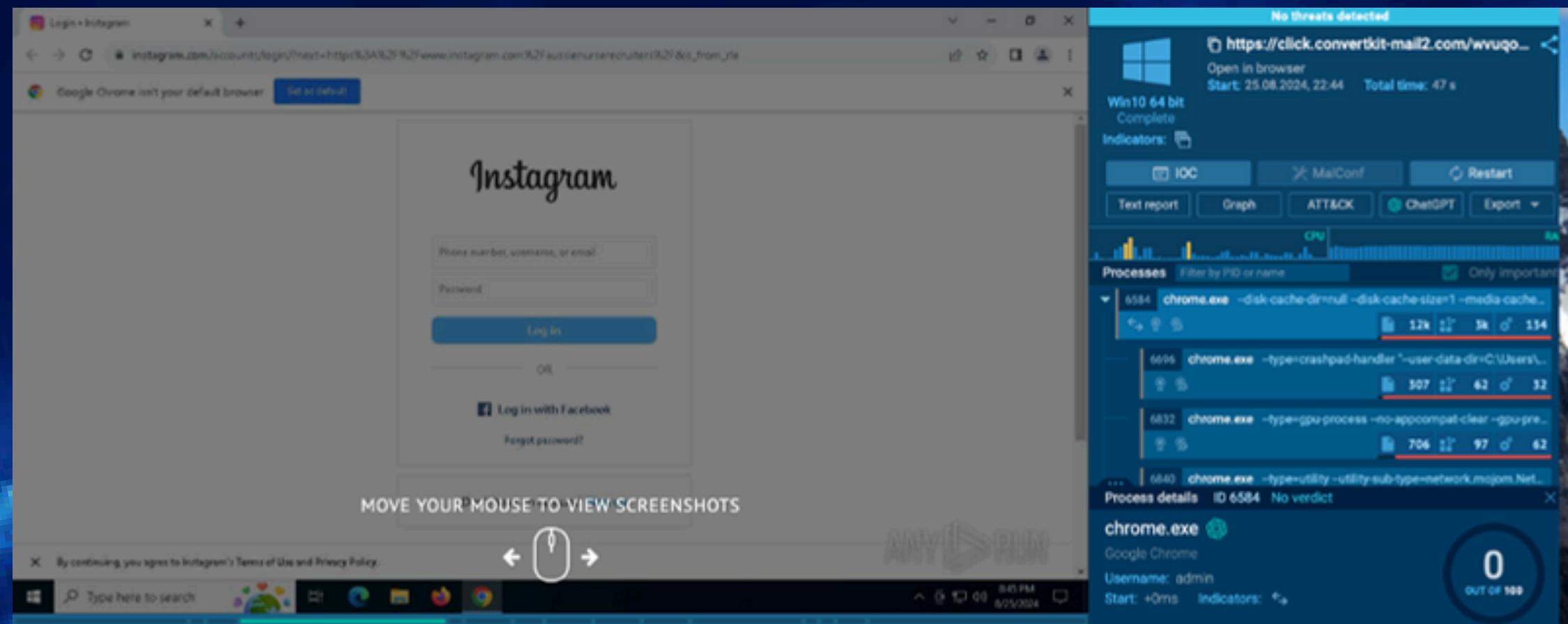
4.2. Analisi Anyrun - Link 3

Descrizione

Abbiamo condotto un'analisi dettagliata di un file sospetto utilizzando Anyrun per determinare se rappresenti una minaccia per il sistema. Anyrun ha analizzato il comportamento del file su un sistema operativo Windows 10 Professional. Il file è stato eseguito e monitorato per individuare eventuali attività sospette o malevole.

Punteggio di Minaccia:

- 0 su 100 (No threats detected)

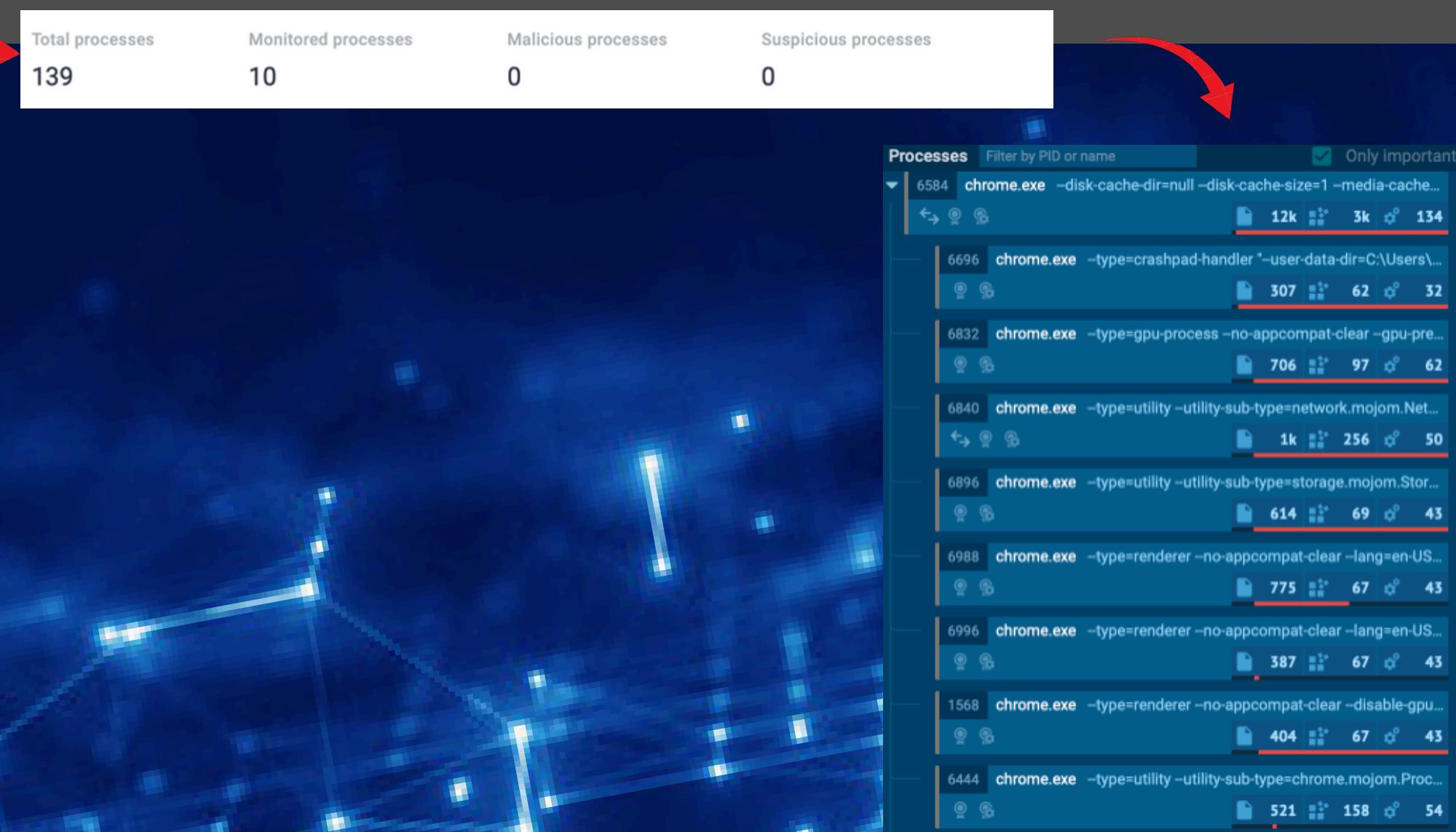


4.2. Analisi Anyrun - Link 3

Comportamento Osservato

Processi Attivati:

Il file analizzato ha avviato diversi processi legati al browser Google Chrome. In totale, sono stati monitorati 139 processi, di cui 10 sono stati osservati attentamente. Tuttavia, nessuno di questi processi è stato identificato come malevolo o sospetto.



4.2. Analisi Anyrun - Link 3

Behavior Graph

Il grafico comportamentale (Behavior Graph) ha mostrato che i processi monitorati sono tipici del funzionamento normale di un browser web, senza alcun comportamento anomalo o sospetto.



4.2. Analisi Anyrun - Link 3

Attività di Rete:

Il file ha generato diverse richieste HTTP e connessioni di rete, in particolare:

- **Richieste HTTP:** Sono state osservate tre richieste GET, tutte con codice di risposta 200 (OK), il che indica che le richieste sono state completate con successo. Le richieste erano indirizzate a:
 1. ocsp.digicert.com (gestito da svchost.exe)
 2. www.microsoft.com (gestito da SIHClient.exe)
- **Connessioni di Rete:** Sono state stabilite 48 connessioni di rete e sono state effettuate 33 richieste DNS. Tutte queste attività sono state classificate come legittime e non hanno indicato comportamenti sospetti o malevoli.
- **Accesso a Facebook e Instagram:** Sono stati osservati accessi a pagine di login di Facebook e Instagram, il che potrebbe indicare una normale navigazione web.

Attività del Registro di Sistema:

Durante l'analisi, è stato rilevato che il processo chrome.exe ha interagito con il registro di sistema di Windows. In particolare, ha letto una chiave di registro associata a Microsoft Office. Questa operazione è comune per i browser, che utilizzano queste informazioni per determinare quali applicazioni sono associate all'apertura di specifici tipi di file o URL.

The screenshot shows a red arrow pointing from the text above to the 'Techniques details' section of the AnyRun interface. The 'Techniques details' section includes a 'Get to know what this threat is about' link, a T1012 indicator, a 'Query Registry' link, and a list of actions: 'Reads Microsoft Office registry keys (1)', 'chrome.exe (1)', and 'Other (1)'.

Action	Count
Reads Microsoft Office registry keys	1
chrome.exe	1
Other	1

4.2. Analisi Anyrun - Link 3

Classificazione:

- **Falso Positivo:** È possibile che il file fosse stato precedentemente segnalato come sospetto in modo erroneo (falso positivo). Tuttavia, l'analisi dettagliata condotta non ha rilevato alcuna minaccia concreta. Nessun processo è stato classificato come una minaccia, e l'interazione con il registro di sistema è risultata essere parte del normale funzionamento del browser Google Chrome. Di conseguenza, il file può essere considerato sicuro e non rappresenta un rischio per il sistema.

Raccomandazioni:

- Non sono necessarie ulteriori azioni immediate.
- Si consiglia di continuare a monitorare il sistema e di mantenere aggiornati i software di sicurezza per garantire la protezione continua.



DAY 5

Analisi Malware 1 giorno 5

Analizzare il contenuto del file compresso calcolatriceinnovativa50.exe.zip andando a confermare che è un malware

Per prima cosa effettuiamo un'analisi statica sia basica che avanzata.

Inserendo il file su virusTotal abbiamo la conferma che il file calcolatriceinnovativa50 sia in realtà un malware classificato come trojan/cryptz che sta ad indicare che il malware ha a che fare con la crittografia dei dati.

VIRUSTOTAL

SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

55/71 security vendors flagged this file as malicious

Community Score 55 / 71



VIRUSTOTAL

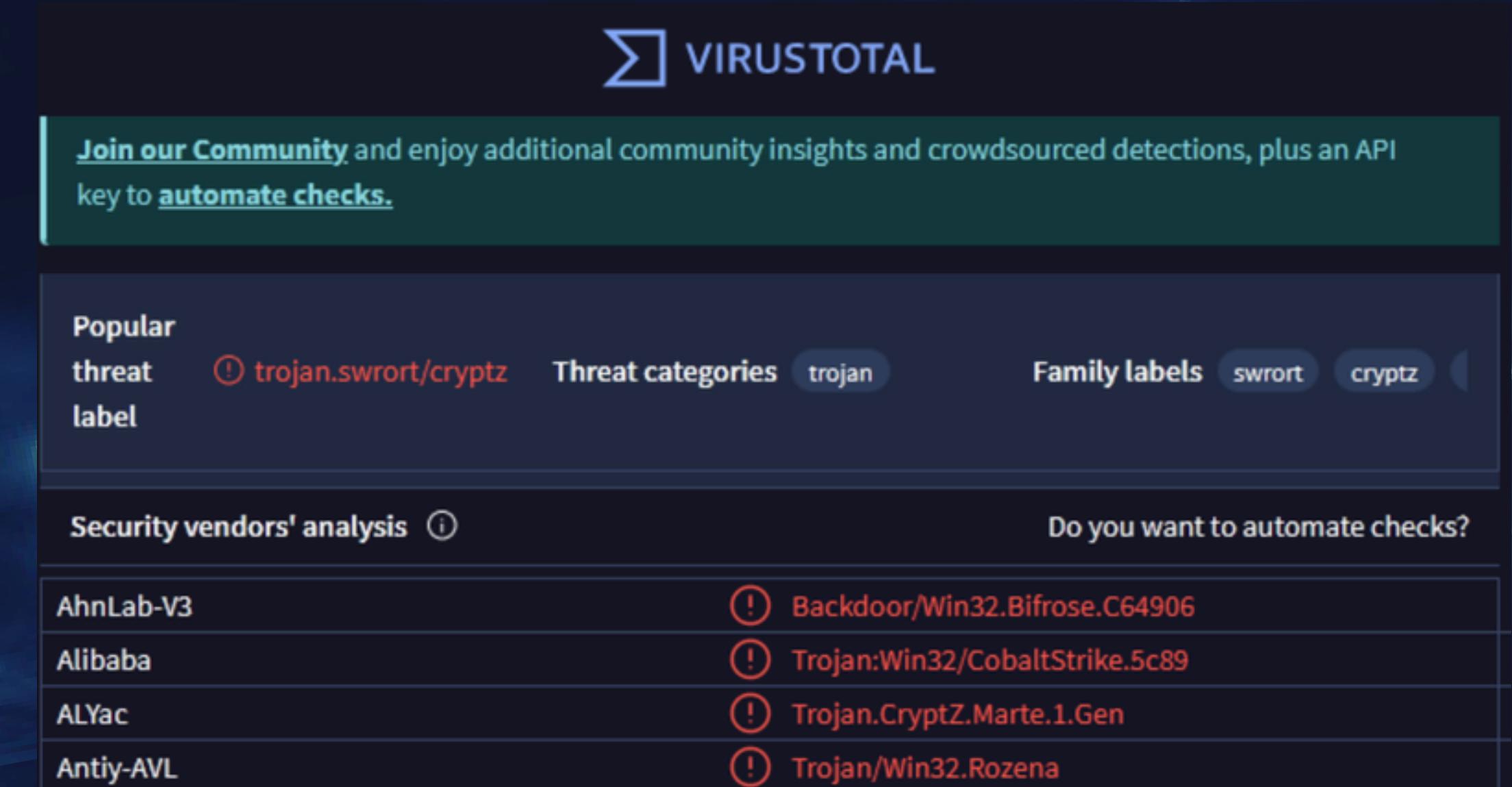
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label ! trojan.swort/cryptz Threat categories trojan Family labels swort cryptz

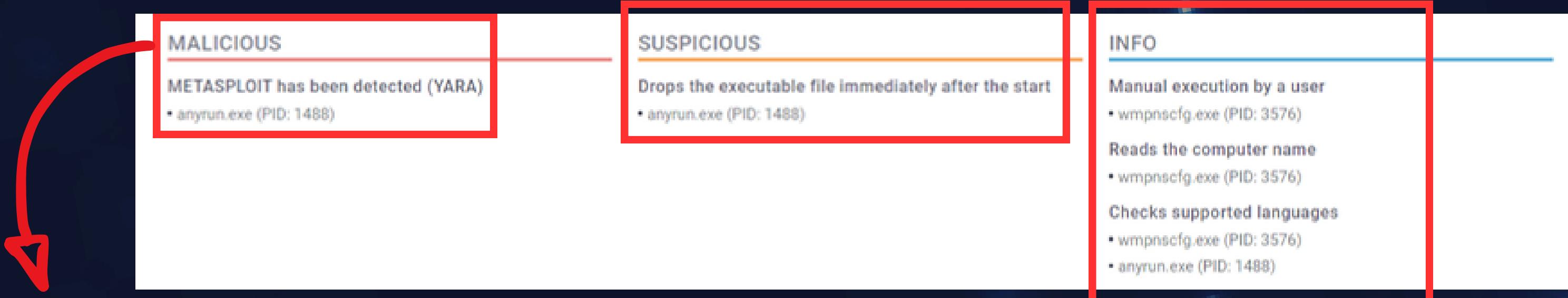
Security vendors' analysis ⓘ

AhnLab-V3	! Backdoor/Win32.Bifrose.C64906
Alibaba	! Trojan:Win32/CobaltStrike.5c89
ALYac	! Trojan.CryptZ.Marte.1.Gen
Antiy-AVL	! Trojan/Win32.Rozena

Do you want to automate checks?



Analisi basica



Se un sistema rileva "METASPLOIT" tramite una regola YARA, significa che è stato trovato un modello o una firma associata al framework Metasploit. Metasploit è uno strumento popolare utilizzato per il penetration testing, ma può essere anche sfruttato da attaccanti per sfruttare vulnerabilità. La rilevazione YARA suggerisce che alcuni file o attività sul sistema corrispondono a caratteristiche note di Metasploit, indicando possibili attività di penetration testing non autorizzate o un attacco attivo.

YARA è uno strumento utilizzato per identificare e classificare file sospetti o dannosi attraverso la creazione di regole personalizzate basate su modelli. È ampiamente utilizzato in ambito di sicurezza informatica per la rilevazione di malware, permettendo di scrivere regole che descrivono i comportamenti o le caratteristiche di file specifici. Queste regole vengono poi utilizzate per scansionare file, processi e memoria, identificando così potenziali minacce. In sintesi, YARA aiuta a individuare e contrastare il malware.

Informazioni sul malware

- Defense Evasion TA0005
 - Obfuscated Files or Information T1027
 - Binary may include packed or encrypted data
 - Software Packing T1027.002
 - Binary may include packed or encrypted data
 - PE file has an executable .text section which is very likely to contain packed code (zlib compression ratio < 0.3)
 - Virtualization/Sandbox Evasion T1497
 - Contains medium sleeps (>= 30s)
 - Contains long sleeps (>= 3 min)
 - May sleep (evasive loops) to hinder dynamic analysis

- Impair Defenses T1562
- Disable or Modify Tools T1562.001
 - Creates guard pages, often used to prevent reverse engineering and debugging

Malware Behavior Catalog Tree

- Communication OC0006
 - HTTP Communication C0002
 - WinINet C0005
 - InternetConnect C0005.001

- Credential Access TA0006
 - Input Capture T1056
 - Creates a DirectInput object (often for capturing keystrokes)
- Discovery TA0007
 - System Information Discovery T1082
 - Queries the cryptographic machine GUID
 - Reads software policies
 - Queries the volume information (name, serial number etc) of a device
 - Virtualization/Sandbox Evasion T1497
 - Contains medium sleeps (>= 30s)
 - Contains long sleeps (>= 3 min)
 - May sleep (evasive loops) to hinder dynamic analysis
 - Software Discovery T1518
 - Security Software Discovery T1518.001
 - AV process strings found (often used to terminate AV products)
 - May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)

- Command and Control TA0011
 - Application Layer Protocol T1071
 - Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic.

CFF Explorer

The screenshot shows the CFF Explorer interface. On the left is a navigation pane with various tools like Address Converter, Dependency Walker, Hex Editor, etc. The main area shows the file structure of 'calcolatriceinnovativa50.exe' with sections like Dos Header, Nt Headers, File Header, Optional Header, Data Directories, Section Headers, Import Directory, Resource Directory, and Debug Directory. Below this is a table of properties:

Property	Value
File Name	C:\Users\user\Downloads\calcolatriceinnovativa50.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	112.50 KB (115200 bytes)
PE Size	112.50 KB (115200 bytes)
Created	Thursday 29 August 2024, 11.07.34
Modified	Tuesday 12 January 2021, 12.07.30
Accessed	Thursday 29 August 2024, 16.09.29
MD5	7A0CC9AD09AC127C2B82FC953E8AFC8D
SHA-1	68BB74C138F26D2E61E055D87582C98775BF3C7B

Below this is another table of properties, highlighted with a red box:

Property	Value
CompanyName	Корпорация Майкрософт
FileDescription	Калькулятор для Windows
FileVersion	5.1.2600.0 (xpclient.010817-1148)
InternalName	CALC
LegalCopyright	© Корпорация Майкрософт. Все права защищены.
OriginalFilename	CALC.EXE
ProductName	Операционная система Microsoft® Windows®

Da CFF Explorer possiamo notare che le proprietà del file come il copyright risultano essere scritto in russo e non sembrano essere lecite. Queste informazioni ci dicono che il software potrebbe non essere legittimo, ma si spaccia per tale.

CFF Explorer

The screenshot shows three windows of the CFF Explorer tool. The top window displays the section headers for the executable 'calcolatriceinnovativa50.exe'. The middle window shows the file structure of the executable, with the 'Import Directory' selected. The bottom window shows the imported DLLs and their function counts.

Section Headers (Top Window):

Name	Virtual Size	Virtual Address
Byte[8]	Dword	Dword
.text	000126B0	00001000
.data	0000101C	00014000
.rsrc	00008A70	00016000

File Structure (Middle Window):

- File: calcolatriceinnovativa50.exe
 - Dos Header
 - Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]
 - Import Directory
 - Resource Directory
 - Debug Directory
 - Address Converter

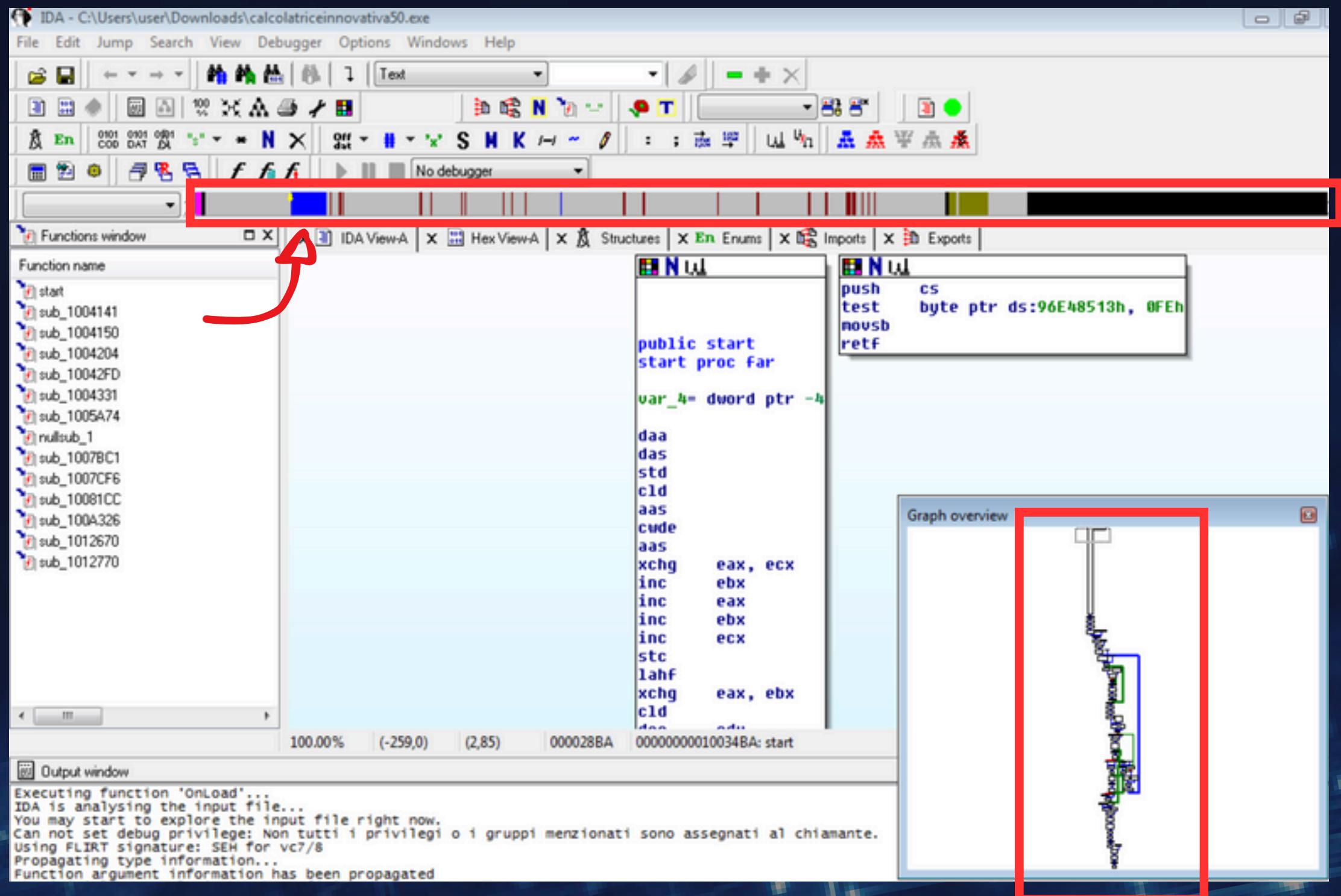
Imports (Bottom Window):

Module Name	Imports
SHELL32.dll	1
msvcrt.dll	26
ADVAPI32.dll	3
KERNEL32.dll	30
GDI32.dll	3
USER32.dll	69

Da CFF Explorer possiamo anche notare le librerie importate dal malware, alcune critiche per Windows ad esempio:

- SHELL32.dll: Gestisce operazioni legate all'interfaccia utente, come l'apertura di file e cartelle, oltre a comandi di sistema.
- mservcrt.dll: È la libreria runtime di Microsoft C che contiene funzioni standard per la gestione di stringhe, memoria, file, ecc.
- ADVAPI32.dll: Fornisce funzioni avanzate per la gestione di sicurezza e registri di Windows.
- KERNEL32.dll: Contiene funzioni di gestione della memoria, file, processi e thread, fondamentali per il sistema operativo.
- GDI32.dll: Gestisce le funzioni grafiche e l'interfaccia con l'hardware grafico.
- USER32.dll: Fornisce funzioni per la gestione delle finestre, input da tastiera/mouse e altre interfacce utente.

Analisi con IDA



Inserendo il malware su IDA possiamo vedere come mostrato nell'immagine a fianco che il codice scritto dal malware è molto poco (parte blu) nonostante il programma risulti essere molto lungo da analizzare

Analisi con IDA

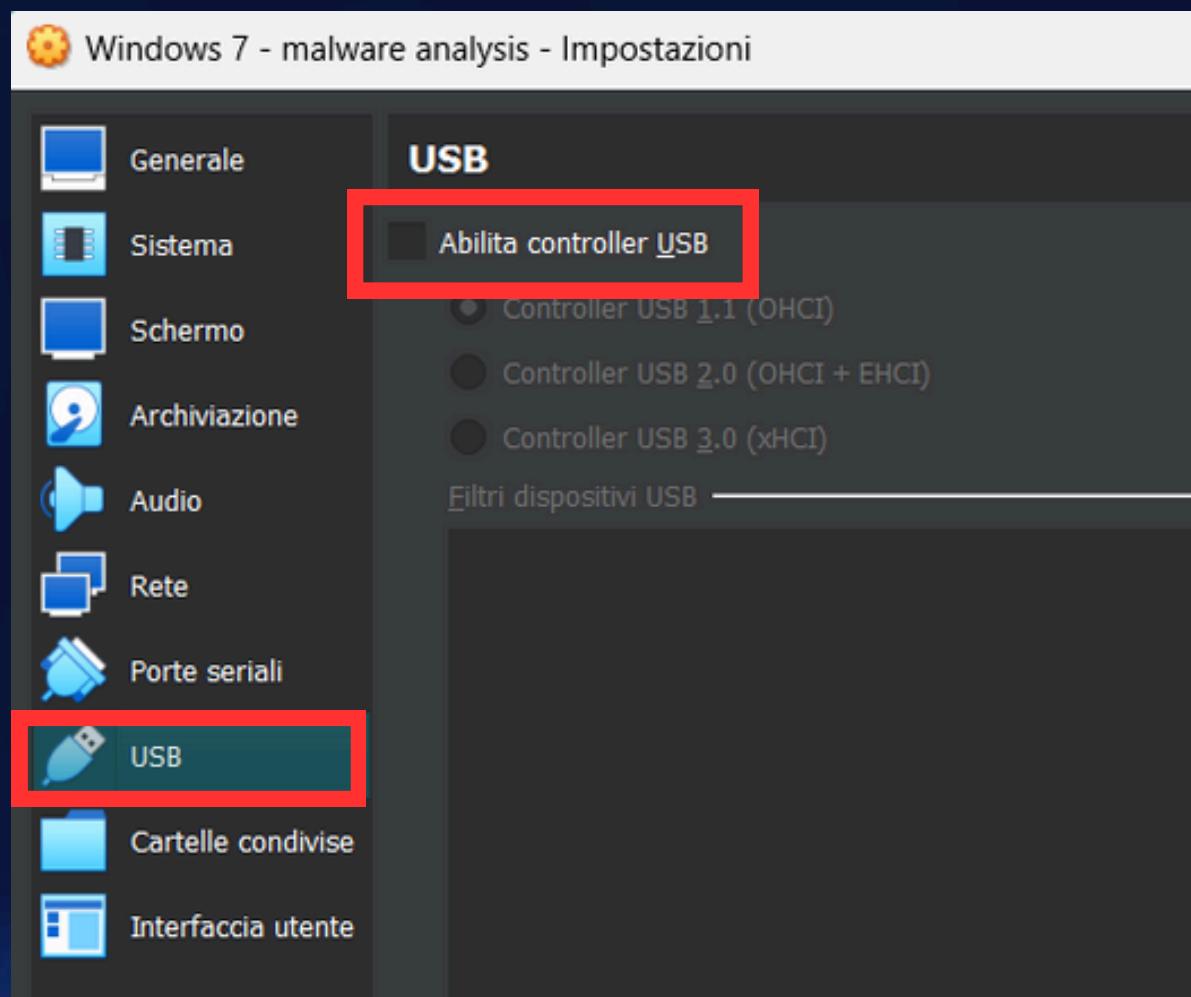
The screenshot shows the IDA Pro interface with the following assembly code snippet:

```
.text:01004126 nov    edx, [edx]
.text:01004128 nop
.text:01004129 jnp    loc_100413C
.text:01004129 ; dw 0C42Ah
.text:0100412E dd 38BD1F0h, 0AB9AE4FFh, 566A9FA2h
.text:01004130 ; dd 00000000, 00000000, 00000000
.text:0100413C ; dw 75F5h
.text:0100413C ; dd 28FD9FB3h, 0DA99C116h
.text:0100413C start    jnp    loc_1003E9E
.text:0100413C start    endp   ; sp-analysis Failed
.text:0100413C ; dw 00000000
.text:01004141 ; ----- SUBROUTINE -----
.text:01004141 ; Attributes: thunk
.text:01004141 sub_1004141 proc near
.text:01004141 sub_1004141 jnp    sub_1004150
.text:01004141 sub_1004141 endp
.text:01004141 ; dw 00000000
.text:01004146 dd 00000000, 00000000, 00000000
.text:01004148 .text:01004150 ; dw 75F5h
.text:01004150 ; dd 28FD9FB3h, 0DA99C116h
0000353C 000000000100413C: start:loc_100413C
```

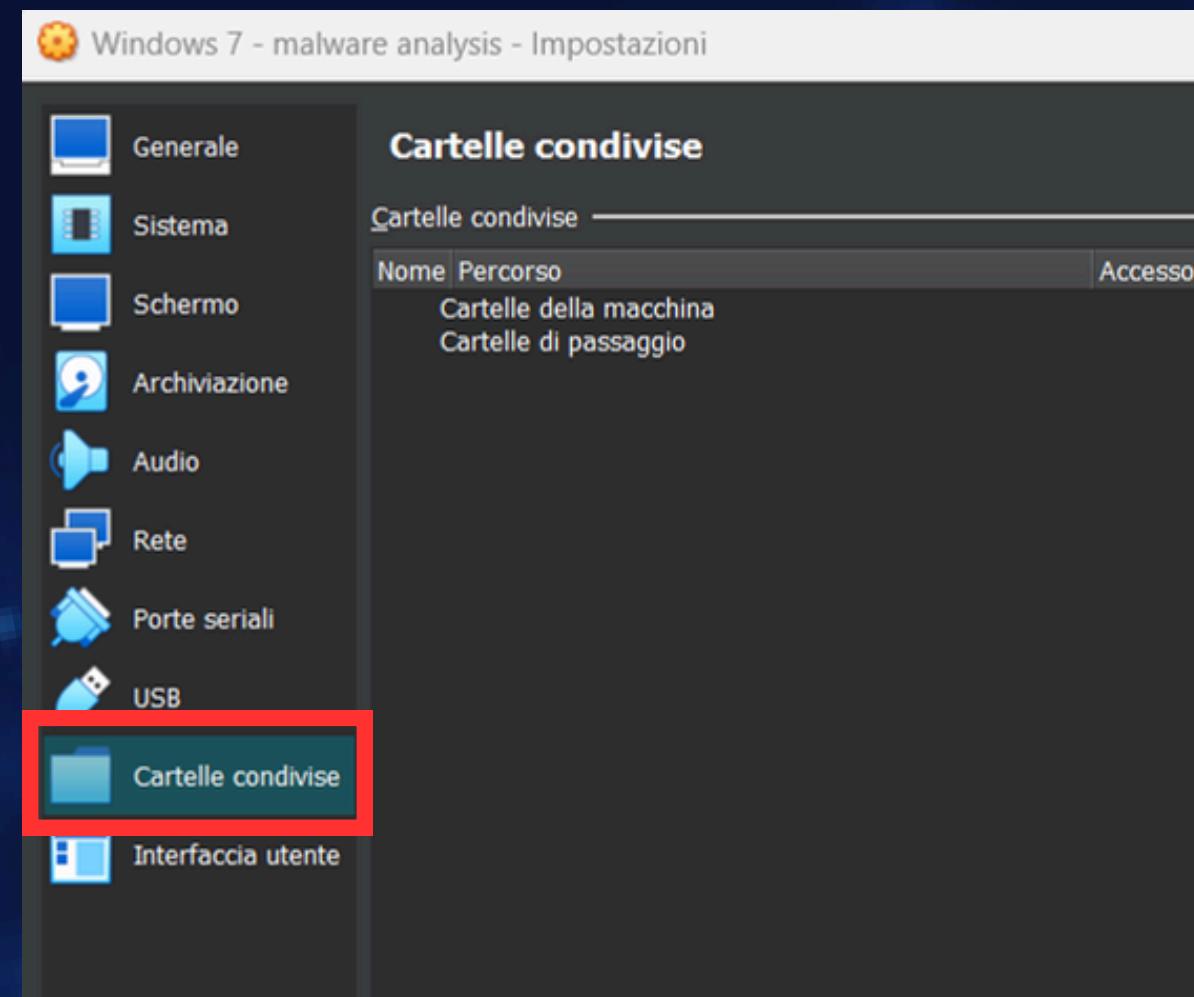
Nella parte di codice malevola il programma IDA non è riuscito ad analizzare completamente le istruzioni come nel caso evidenziato in figura dove è avvenuto un errore nell'analisi dello stack pointer. Inoltre la maggior parte del codice non viene nemmeno commentata da IDA o non si vedono le chiamate a funzioni che solitamente abbiamo visto. Questo potrebbe essere dovuto al fatto che il codice del malware è stato opportunamente offuscato per renderne difficile l'analisi e quindi la comprensione.

Analisi dinamica

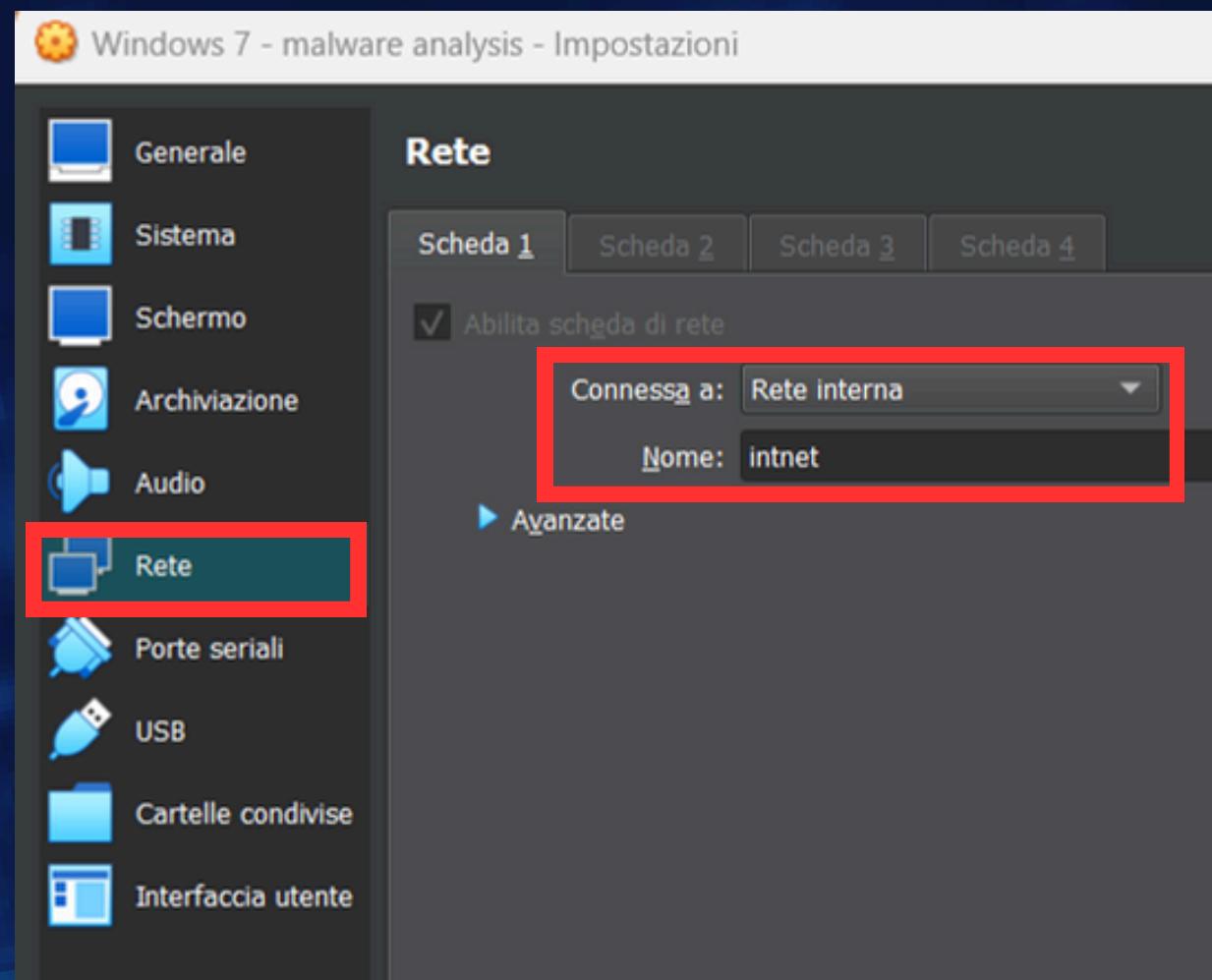
Prima di procedere con l'analisi dinamica basica dobbiamo assicurarci di mettere in sicurezza la macchina virtuale assicurandoci di disabilitare il controller delle porte USB, disattivare le cartelle condivise e metterci in una rete interna.



1-Disabilito controller USB



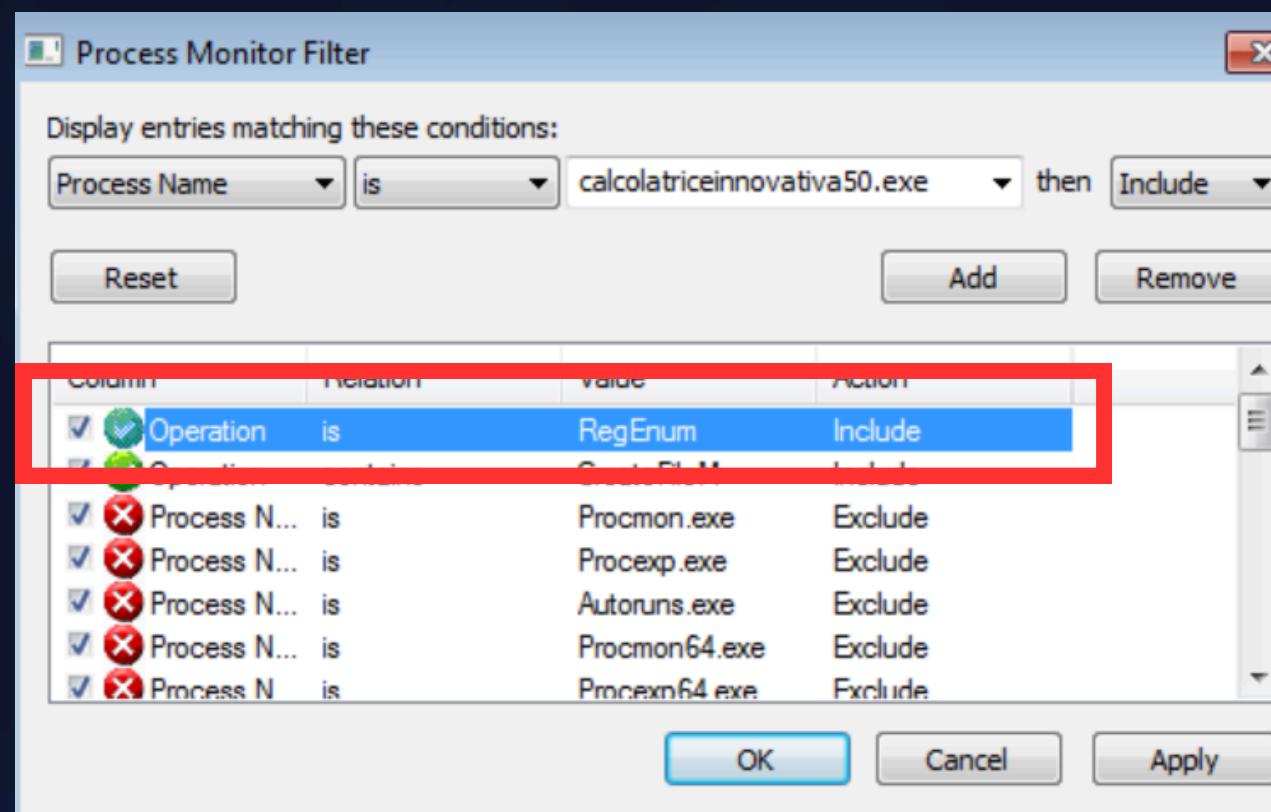
2-Rimuovo cartelle condivise



3- Rete interna

Process Monitor

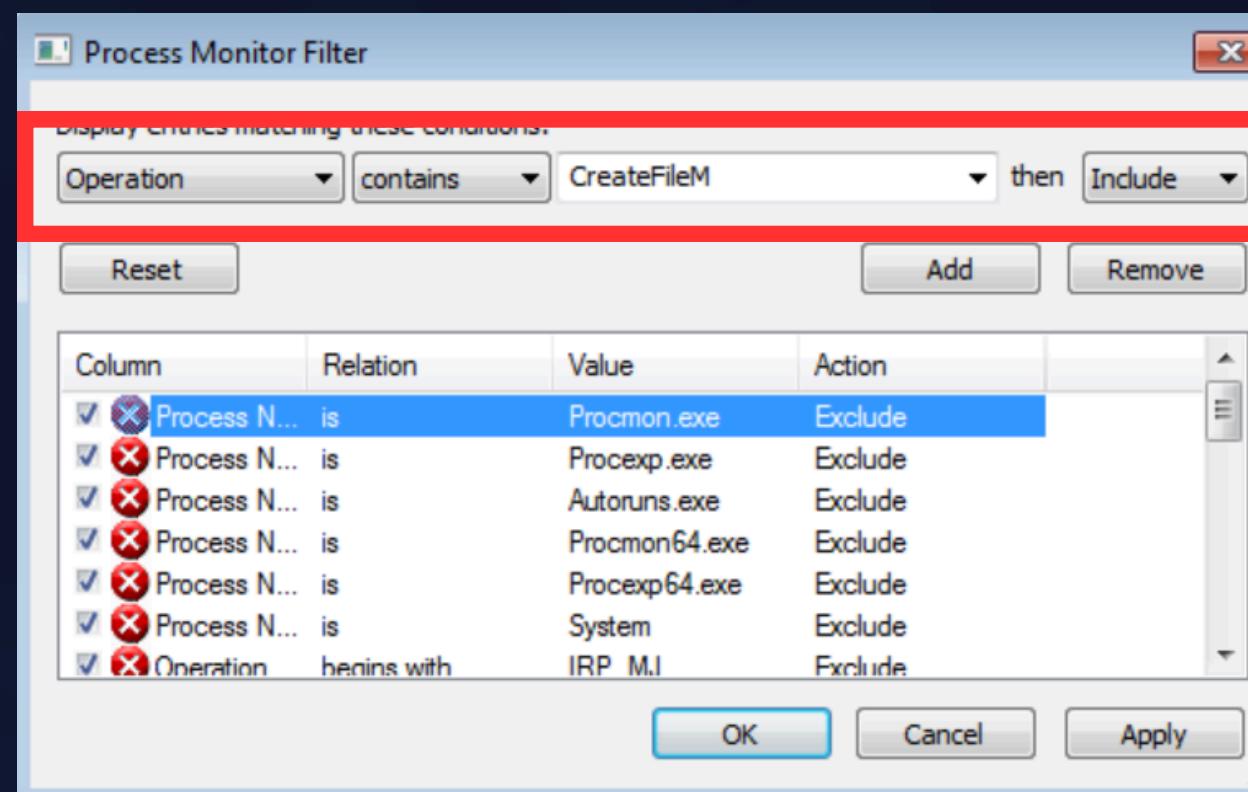
Appena avviato Process Monitor inseriamo un filtro per andare ad evidenziare solo le operazioni effettuate dal processo del malware. Come possiamo notare il malware effettua molte operazioni sul file system in particolare con operazioni di creazione file



Time ...	Process Name	PID	Operation	Path	Result	Detail
16:09:	calcolatriceinnova...	1592	Thread Create		SUCCESS	Thread ID: 3232
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\Prefetch\CALCOLATRICE...	NAME NOT FOUND	Desired Access: G...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Users\user\Downloads	SUCCESS	Desired Access: E...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\SysWOW64\sechost.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\SysWOW64\sechost.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFileMapp...	C:\Windows\SysWOW64\imm32.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinnova...	1592	CreateFile	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Desired Access: R...

Process Monitor

Inserendo questo filtro vediamo che il malware effettua molta attività nel creare File di mapping, probabilmente questi file gli servono a scansionare il nostro sistema e a rubare informazioni



The main window displays a log of 106,473 events, showing numerous 'CreateFileMapp.' operations by process 'calcolatriceinno...' with PID 1592. These operations are primarily directed at system DLLs like 'C:\Windows\System32\wow64.dll' and 'C:\Windows\System32\wow64cpu.dll'. The log also includes entries for 'sechost.dll' and 'vmm32.dll'. Most operations result in 'SUCCESS' or are 'FILE LOCKED'.

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\SysWOW64\sechost.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\SysWOW64\sechost.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\SysWOW64\vmm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\SysWOW64\vmm32.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\SysWOW64\vmm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\SysWOW64\vmm32.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\SysWOW64\vmm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\SysWOW64\vmm32.dll	SUCCESS	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\SysWOW64\vmm32.dll	FILE LOCKED WI...	SyncType: SyncTy...
16:09:	calcolatriceinno...	1592	CreateFileMapp.	C:\Windows\SysWOW64\vmm32.dll	SUCCESS	SyncType: SyncTy...

Process Monitor

Possiamo vedere inoltre che tra le attività sulle chiavi di registro non ce ne sono di create o modificate, ma anche qui vengono fatte operazioni di enumerazione sia delle chiavi sia dei valori che contengono, come mostrato nella figura sotto

The screenshot shows the Process Monitor application interface. On the left, a 'Process Monitor Filter' dialog is open, with its title bar highlighted by a red box. The filter criteria are set to 'Operation' is 'RegEnum'. The main window displays a list of registry operations. A red box highlights the 'Operation' column header and the first few rows of the table, which show multiple entries for 'RegEnumKey' and 'RegEnumValue' operations performed by process ID 1592.

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:09:...	calcolatriceinno...	1592	RegEnumKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Index: 0, Name: it-IT
16:09:...	calcolatriceinno...	1592	RegEnumKey	HKLM\System\CurrentControlSet\Contr...	NO MORE ENTRI...	Index: 1, Length: 5...
16:09:...	calcolatriceinno...	1592	RegEnumValue	HKLM\System\CurrentControlSet\Contr...	NO MORE ENTRI...	Index: 0, Length: 5...
16:09:...	calcolatriceinno...	1592	RegEnumValue	HKCU\Control Panel\Desktop\Langu...	NO MORE ENTRI...	Index: 0, Length: 5...

Conclusioni

01001029	12FE	ADC BH,DH	
0100102B	v74 4A	JE SHORT calcolat.01001077	
0100102D	FF05 75D651FE	INC DWORD PTR DS:[FE51D675]	
01001033	v74 48	JE SHORT calcolat.0100107D	
01001035	5F	POP EDI	
01001036	FE	???	
01001037	v74 1E	JE SHORT calcolat.01001057	
01001039	E5 FF	IN EAX,0FF	
0100103B	v74 71	JE SHORT calcolat.010010AE	
0100103D	52	PUSH EDV	
0100103E	FE	???	Unknown command
0100103F	v74 FF	JE SHORT <&KERNEL32.Sleep>	I/O command
01001041	10FE	ADC DH,BH	Unknown command
01001043	v74 EC	JE SHORT calcolat.01001091	
01001045	6900 75000EFE	IMUL ERX,DWORD PTR DS:[ERX],FE0E0075	
0100104B	^74 CF	JE SHORT calcolat.0100101C	
0100104D	D1FF	SAR EDI,1	
0100104F	v74 44	JE SHORT calcolat.01001095	
01001051	D0FF	SAR BH,1	
01001053	v74 1A	JE SHORT calcolat.0100106F	
01001055	18FE	SBB DH,BH	
01001057	^74 E4	JE SHORT calcolat.0100103D	
01001059	24 FE	AND AL,0FE	
0100105B	^74 B9	JE SHORT calcolat.01001016	
0100105D	16	PUSH SS	
0100105E	FE	???	
0100105F	-74 FE	JE SHORT calcolat.0100105F	Unknown command
01001061	BF 0075A116	MOU EDI,16A17500	
01001066	FE	???	Unknown command
01001067	v74 36	JE SHORT calcolat.0100109F	
01001069	11FE	ADC ESI,EDI	
0100106B	^74 F0	JE SHORT calcolat.0100105D	
0100106D	13FE	ADC EDI,ESI	
0100106F	^74 EE	JE SHORT calcolat.0100105F	
01001071	8300 75	ADD DWORD PTR DS:[EAX],75	
01001074	DC16	FCOM QWORD PTR DS:[ESI]	
01001076	FE	???	
01001077	v74 07	JE SHORT <&KERNEL32.LocalAlloc>	Unknown command
01001079	53	PUSH EBX	
0100107A	FE	???	Unknown command
0100107B	v74 4C	JE SHORT calcolat.010010C9	
0100107D	2F	DAS	
0100107E	FE	???	Unknown command
0100107F	v74 68	JE SHORT calcolat.010010E9	
01001081	16	PUSH SS	
01001082	FE	???	Unknown command
01001083	v74 54	JE SHORT calcolat.010010D9	
01001085	C000 75	ROL BYTE PTR DS:[EAX],75	Shift constant out of range 1..31
01001088	07	POP ES	Modification of segment register

Sulla base delle analisi effettuate possiamo affermare che il malware in questione sia un mapper o scanner dal momento che effettua l'enumerazione delle chiavi di registro o crea file per avere informazioni sul nostro sistema, inoltre il codice è opportunamente offuscato e utilizza tecniche non invasive come la funzione sleep per non essere individuato, nonostante questo risulta essere innocuo su Windows 7 ma potrebbe essere molto dannoso su sistemi operativi precedenti.

Analisi Secondo Malware

Traccia:

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.

Link:

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

Setup Macchina Virtuale

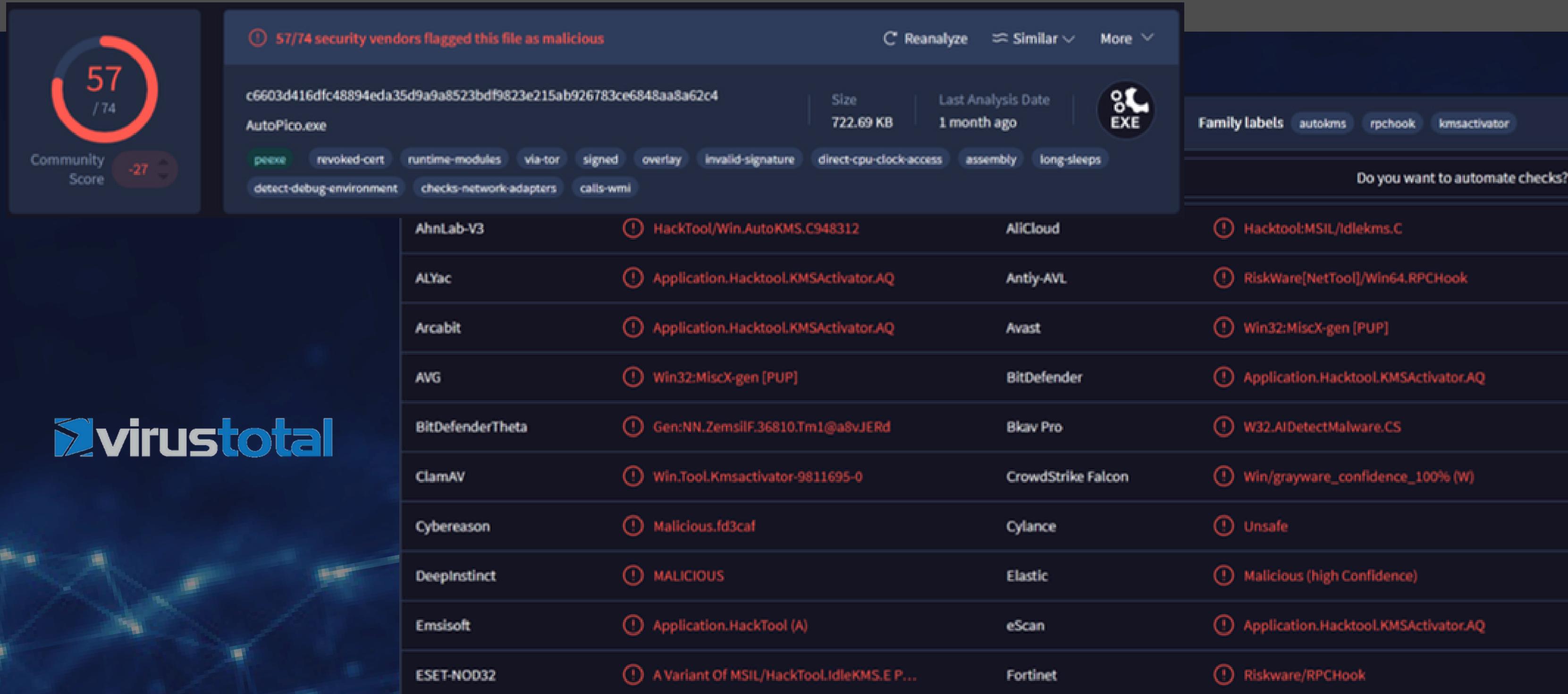
La macchina Windows 7 dove analizzeremo il file è una macchina virtuale configurata per fare una analisi in tutta sicurezza.

Nel caso in cui volessimo eseguire il file per effettuare una analisi dinamica configureremo la macchina in un ambiente isolato, senza connessione ad internet o alla nostro stesso computer. (Come abbiamo già visto in precedenza)



Virus Total

Come prima cosa andiamo ad analizzare il file con il tool Virus Total. E' molto semplice da utilizzare e ti da risultati immediati senza dover scaricare alcuna applicazione direttamente dal tuo browser.



The screenshot shows the VirusTotal analysis interface for the file `c6603d416dfc48894eda35d9a9a8523bdf9823e215ab926783ce6848aa8a62c4`. The file is identified as `AutoPico.exe`. The analysis results indicate that 57 out of 74 security vendors flagged the file as malicious. The file is an EXE file, weighs 722.69 KB, and was last analyzed a month ago. The interface lists various vendor names and their findings, such as AhnLab-V3, HackTool/Win.AutoKMS.C948312, AliCloud, and many others. A large red circle highlights the '57 / 74' malicious count. The overall community score is shown as -27.

Vendor	Signature	Analysis Result	Family Labels
AhnLab-V3	HackTool/Win.AutoKMS.C948312	AliCloud	Hacktool:MSIL/Idlekms.C
ALYac	Application.Hacktool.KMSActivator.AQ	Antly-AVL	RiskWare[NetTool]/Win64.RPCHook
Arcabit	Application.Hacktool.KMSActivator.AQ	Avast	Win32:MisX-gen [PUP]
AVG	Win32:MisX-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.Id3caf	Cylance	Unsafe
DeepInstinct	MALICIOUS	Elastic	Malicious (high Confidence)
Emsisoft	Application.HackTool (A)	eScan	Application.Hacktool.KMSActivator.AQ
ESET-NOD32	A Variant Of MSIL/HackTool.IdleKMS.E P...	Fortinet	Riskware/RPCHook

Virus Total



57/74, significa che 57 motori antivirus su un totale di 74 hanno rilevato il file come potenzialmente dannoso o infetto.

Questo punteggio suggerisce che il file è altamente sospetto e molto probabilmente contiene un malware o un'altra forma di codice dannoso, poiché la maggior parte degli antivirus lo ha identificato come tale.

Ma...

Nonostante ci sia un grande possibilità che sia un malware è sempre consigliabile esaminare ulteriormente il file per avere un'idea più chiara della natura della minaccia.

CFF Explorer

Continuiamo l'analisi del file partendo dall'analisi statica basica. Andando ad identificare le librerie importate e le sezioni di cui si compone il probabile malware.

Screenshot of CFF Explorer showing the analysis of AmicoNerd.exe. The interface includes a navigation tree on the left and two tables on the right.

Navigation Tree:

- File: AmicoNerd.exe
 - Dos Header
 - Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]
 - Import Directory
 - Resource Directory
 - Relocation Directory
 - .NET Directory
 - MetaData Header
 - MetaData Streams
 - #~
 - Tables Header
 - Tables
 - #Strings
 - #IIS

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

A red arrow points upwards from the 'szAnsi' entry in the table to the 'szAnsi' entry in the 'Name' column of the second table.

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

CFF Explorer



La libreria “mscoree.dll” è un componente essenziale del .NET Framework di Microsoft. Il suo nome sta per “Microsoft Common Language Runtime Execution Engine”.

Poiché “mscoree.dll” gestisce l'esecuzione di codice .NET, un malware può fare leva su questa libreria per caricare e avviare il codice malevolo all'interno di un'applicazione .NET legittima. Il malware potrebbe chiamare API attraverso mscoree.dll per ottenere informazioni sul sistema, eseguire comandi, o manipolare dati. E potrebbe anche ottenere la persistenza.



La funzione “_CorExeMain” è una funzione centrale nel runtime del .NET Framework, ed è particolarmente importante per l'avvio di applicazioni .NET.

E' responsabile della gestione del processo di inizializzazione del runtime .NET e dell'avvio dell'applicazione quindi un malware potrebbe sfruttare la sua funzionalità per eseguire codice malizioso.

CFF Explorer

Come possiamo vedere le sezioni sono: .text , .rsrc e .reloc.

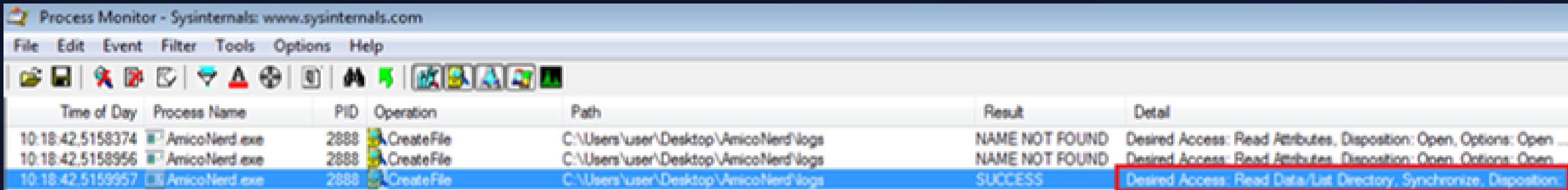
Visto che abbiamo già parlato delle prime 2 mi soffermerei a descrivere quest'ultima:

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	00008240	00002000	000082600	000000200	000000000	000000000	0000	0000	60000020
.rsrc	000000E40	000036000	00001000	000B2800	000000000	000000000	0000	0000	40000040
.reloc	000000A0	000068000	00000200	000B3800	000000000	000000000	0000	0000	42000040

La sezione “.reloc” può essere sfruttata dal malware per alterare gli indirizzi di memoria e dirigere l'esecuzione verso il codice dannoso, nascondendo la sua presenza e rendendo più difficile la rilevazione da parte dei software di sicurezza.

Process Monitor

Process Monitor è uno strumento di diagnostica per Windows che monitora in tempo reale tutte le attività di sistema legate a processi, file di sistema, registro di sistema e thread, utile per identificare problemi e comportamenti anomali.



The screenshot shows two instances of Process Monitor. The top instance displays three events for the process AmicoNerd.exe (PID 2888) performing CreateFile operations on files named 'logs' located at C:\Users\user\Desktop\AmicoNerd\logs. The first two events result in 'NAME NOT FOUND' and the third results in 'SUCCESS'. The bottom instance shows two events for the same process attempting to create files named 'DM.bin' at C:\Users\user\Desktop\AmicoNerd\DM.bin. The first event fails ('NAME NOT FOUND'), and the second succeeds ('SUCCESS'). The 'Detail' column provides more specific information about the access desired by the process.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:18:42.5158374	AmicoNerd.exe	2888	CreateFile	C:\Users\user\Desktop\AmicoNerd\logs	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
10:18:42.5158356	AmicoNerd.exe	2888	CreateFile	C:\Users\user\Desktop\AmicoNerd\logs	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
10:18:42.5158957	AmicoNerd.exe	2888	CreateFile	C:\Users\user\Desktop\AmicoNerd\logs	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Dispositio...

Time of Day	Process Name	PID	Operation	Path	Result	Detail
10:18:42.9607702	AmicoNerd.exe	2888	CreateFile	C:\Users\user\Desktop\AmicoNerd\DM.bin	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open ...
10:18:42.9848938	AmicoNerd.exe	2888	CreateFile	C:\Users\user\Desktop\AmicoNerd\DM.bin	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Overwrit...

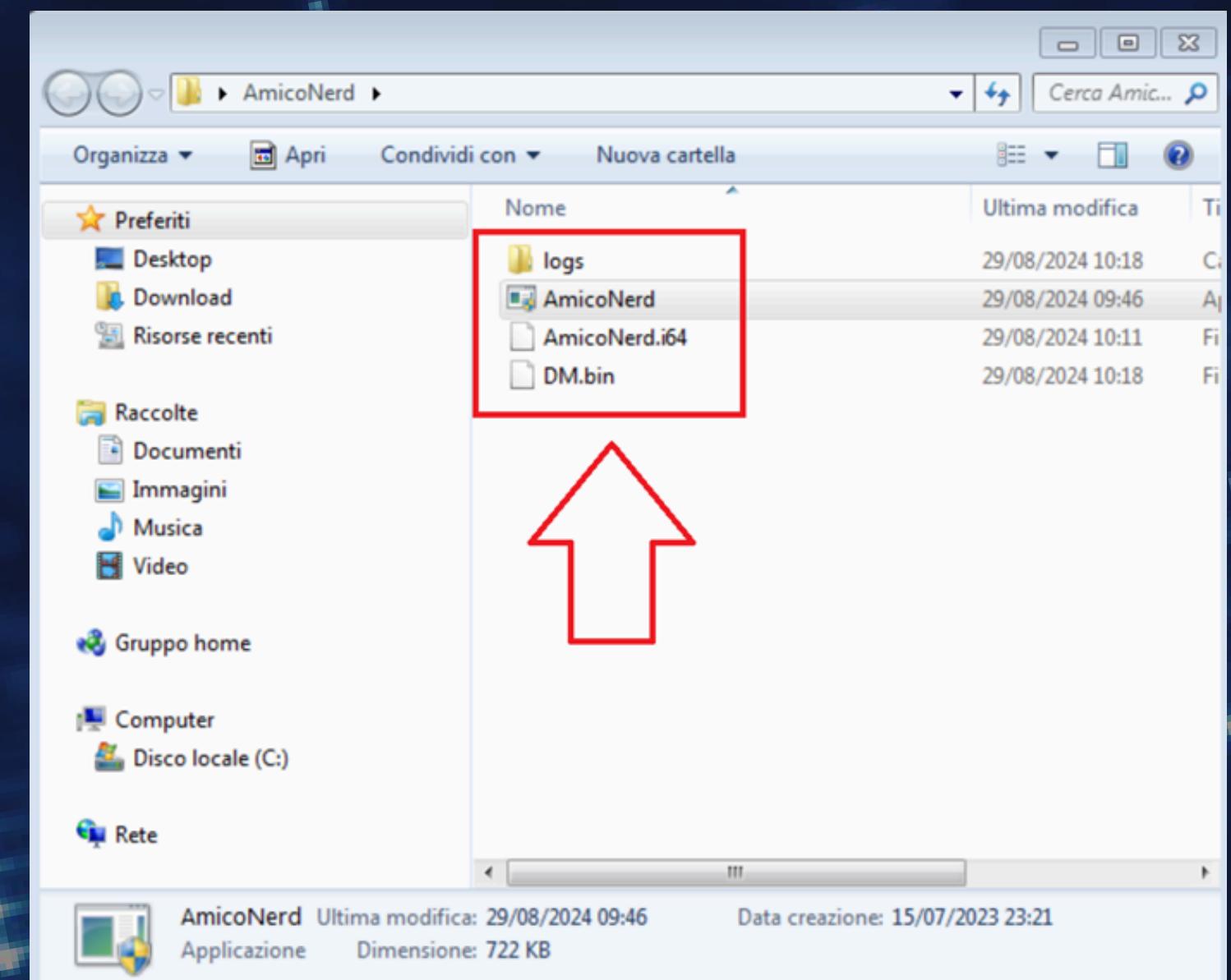
Tramite Process Monitor possiamo identificare che vengono creati dei file all'interno della cartella dove è presente il malware.

Process Monitor

E sempre Tramite Process Monitor abbiamo identificato anche una funzione del kernel di Windows “QueryNetworkOpenInformationFile” che può essere sfruttata dal malware per esplorare, identificare e raccogliere informazioni sui file e le directory su una rete, facilitando attività come la raccolta di dati.

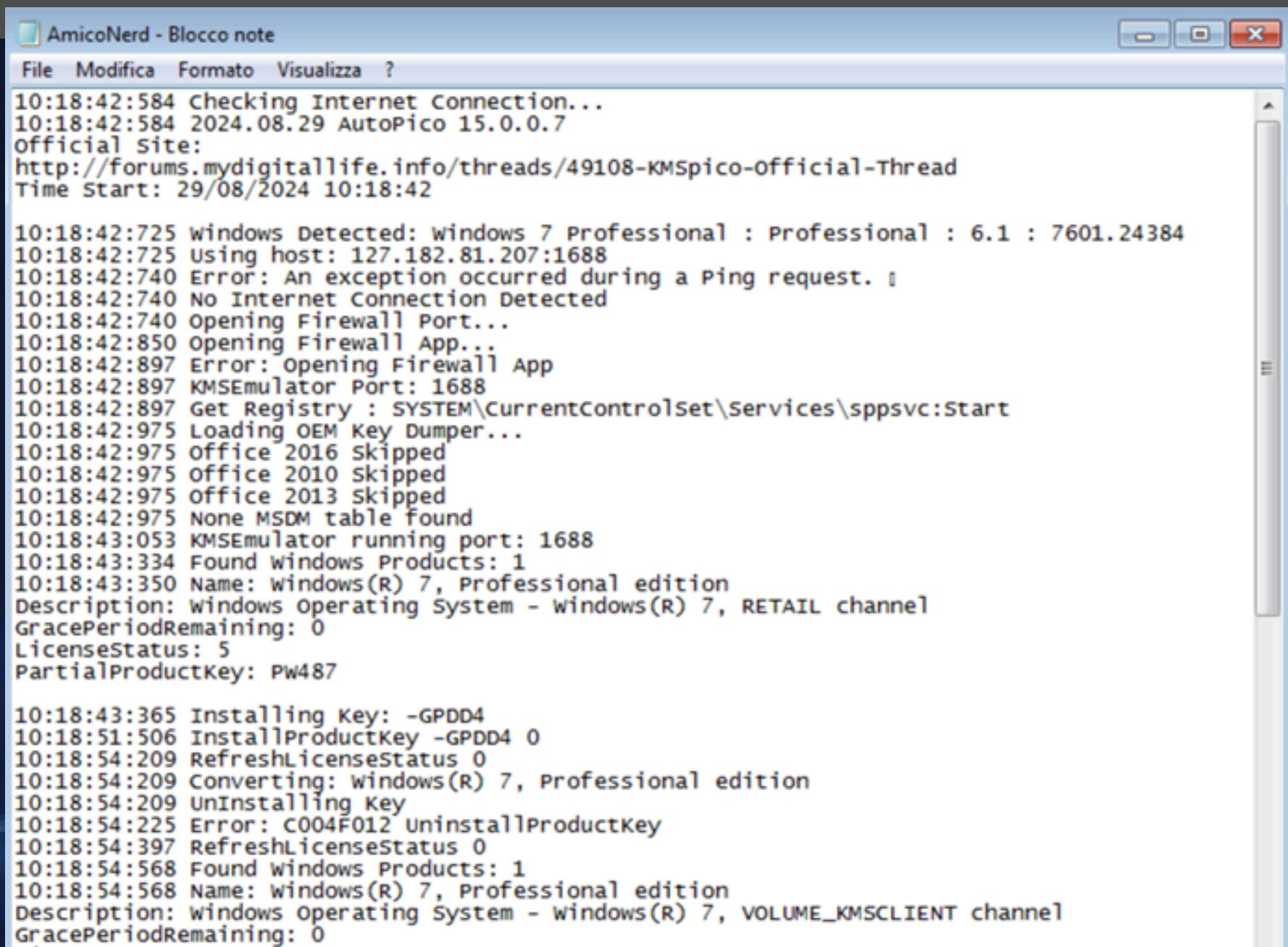
A screenshot of the Process Monitor application. The main window displays a list of events. One event is highlighted with a red box: "11/05/2024, 10:48:48 2732 AmicoNerd.exe CreateFile C:\Users\user\Desktop\AmicoNerd\DM.bin". Below it, another event shows "QueryNetworkOpenInformationFile" being performed on the same path. A third event shows "CloseFile" on the same path. The interface includes a menu bar (File, Edit, Event, Filter, Tools, Options, Help) and a toolbar with various icons.

Infatti come possiamo vedere la cartella dove è presente il malware si popola di altri file al momento dell'esecuzione.



Process Monitor

All'interno della cartella “logs” viene creato per l'appunto il file “AmicoNerd” dove sono state registrate le configurazioni del sistema vittima.
Possiamo dunque affermare che l'eseguibile è un malware



```
AmicoNerd - Blocco note
File Modifica Formato Visualizza ?
10:18:42:584 Checking Internet Connection...
10:18:42:584 2024.08.29 AutoPico 15.0.0.7
official Site:
http://forums.mydigitallife.info/threads/49108-KMSpico-official-Thread
Time Start: 29/08/2024 10:18:42

10:18:42:725 windows Detected: windows 7 Professional : Professional : 6.1 : 7601.24384
10:18:42:725 Using host: 127.182.81.207:1688
10:18:42:740 Error: An exception occurred during a Ping request. !
10:18:42:740 No Internet Connection Detected
10:18:42:740 Opening Firewall Port...
10:18:42:850 Opening Firewall App..
10:18:42:897 Error: Opening Firewall App
10:18:42:897 KMSEmulator Port: 1688
10:18:42:897 Get Registry : SYSTEM\CurrentControlSet\Services\sppsvc:Start
10:18:42:975 Loading OEM Key Dumper...
10:18:42:975 office 2016 Skipped
10:18:42:975 office 2010 Skipped
10:18:42:975 office 2013 Skipped
10:18:42:975 None MSDM table found
10:18:43:053 KMSEmulator running port: 1688
10:18:43:334 Found windows Products: 1
10:18:43:350 Name: Windows(R) 7, Professional edition
Description: windows Operating System - Windows(R) 7, RETAIL channel
GracePeriodRemaining: 0
LicenseStatus: 5
PartialProductKey: Pw487

10:18:43:365 Installing Key: -GPDD4
10:18:51:506 InstallProductKey -GPDD4 0
10:18:54:209 RefreshLicenseStatus 0
10:18:54:209 Converting: Windows(R) 7, Professional edition
10:18:54:209 UnInstalling Key
10:18:54:225 Error: C004F012 UninstallProductKey
10:18:54:397 RefreshLicenseStatus 0
10:18:54:568 Found windows Products: 1
10:18:54:568 Name: Windows(R) 7, Professional edition
Description: windows Operating System - Windows(R) 7, VOLUME_KMSCLIENT channel
GracePeriodRemaining: 0
```

Conclusione

Per evitare di incorrere in problemi di sicurezza, è sempre una buona pratica:

1. Scaricare software solo da fonti affidabili e verificate.
2. Utilizzare un buon antivirus e fare scansioni regolari.
3. Verificare la reputazione del software attraverso recensioni e raccomandazioni.

Per evitare di danneggiare la macchina (seppur macchina virtuale) dove ho analizzato il malware ho precedentemente effettuato una istantanea su VirtualBox in modo tale che io possa “tornare indietro” a prima che il file malevolo venisse eseguito.



Thank you!



Our Team

