

# BUILD WEEK III

MALWARE ANALYSIS



NET.  
REBELS.

# TRACCIA

## GIORNO 4

<https://app.any.run/tasks/371957e1-d960-4b8a-8c68-241ff918517d/>

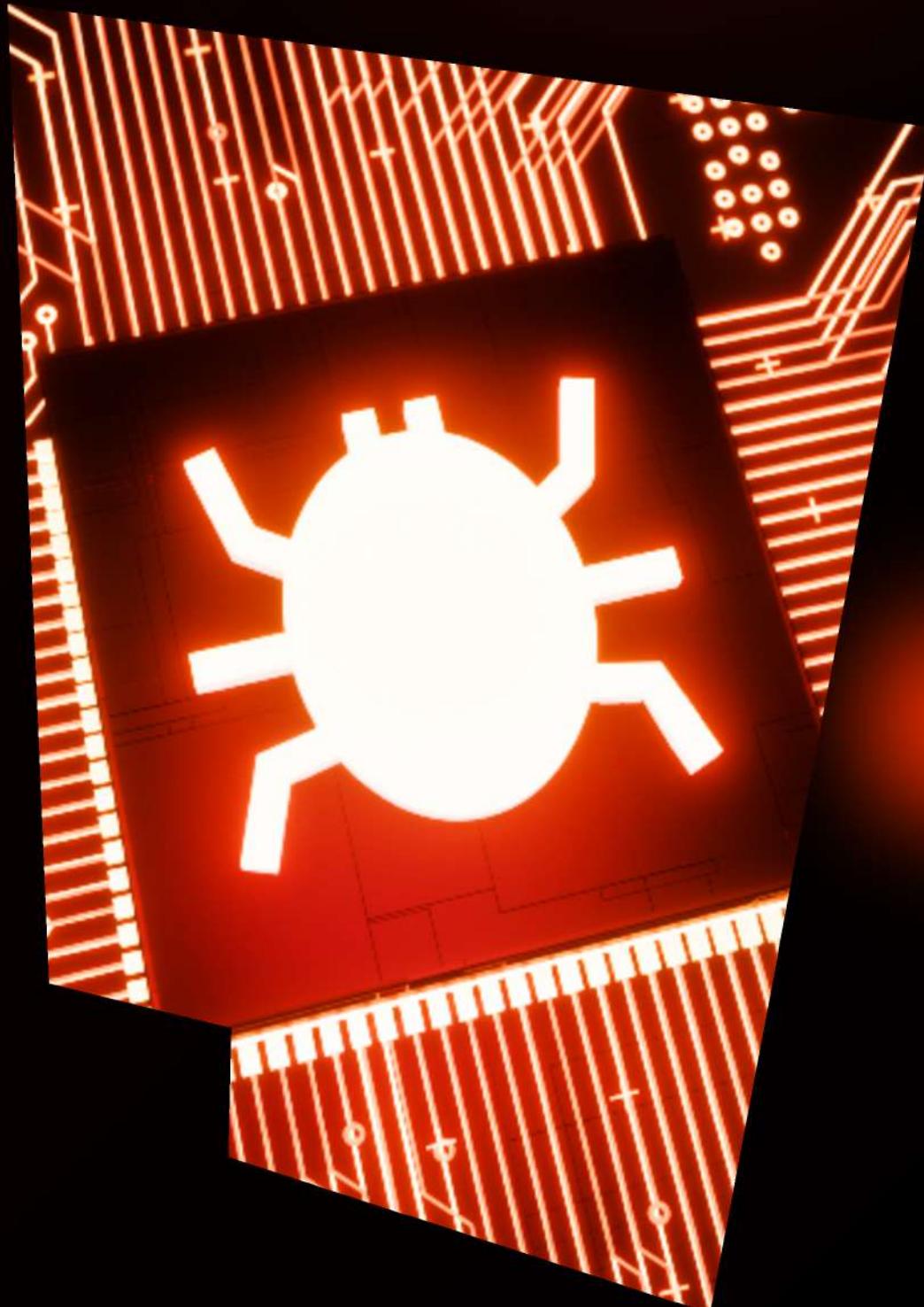
<https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/>

[https://app.any.run/tasks/f1f20828-2222-46fb-a886-09f77581e67b /](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.)



# PARTE 1

## Analisi AnyRun

### IL PRIMO MALWARE ANALIZZATO È VIDAR.EXE

Noto come Infostealer e loader assieme a Lumma.

#### Descrizione dei Processi:

Una volta avviato, il programma eseguirà delle **Query** (delle operazioni che consentono di leggere, cercare o interrogare il registro di sistema di Windows)

- **HKEY\_LOCAL\_MACHINE\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME**

Utilizzato per reperire il Nome del sistema

- **HKEY\_LOCAL\_MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS**

Utilizzato per controllare le lingue supportate

Partiranno anche **svchost.exe** (per le operazioni di rete sul sistema)

**Regasm.exe** (che andremo ad analizzare nella slide successiva)



**Vidar.exe**  
System Infostealer

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

**Regasm.exe**  
Web Infostealer

# PARTE 1

## Analisi AnyRun

**Regasm.exe** è un .NET Framework di windows (è una componente chiave per lo sviluppo e l'esecuzione di applicazioni Windows.)

Ma in questo caso è stato compromesso dall'autore del malware in modo da sostituire la chiave legittima ed ottenere la persistenza

Esso avrà le potenzialità di:

Ottenere le credenziali sui Web Browser

C:\Users\admin\AppData\Roaming\FileZilla\recentservers.xml

Un file contenente informazioni sui server a cui l'utente si è connesso di recente.

Il malintenzionato avrà a disposizione:

- Indirizzi IP dei server visitati recentemente.
- Credenziali di accesso (nomi utente e password).
- Porta utilizzata per la connessione.

Rubare informazioni Personalali

C:\Users\admin\AppData\Local\Google\Chrome\User Data\Local State

Un file contiene le configurazioni del browser in questione(Google).

il malintenzionato avrà a disposizione:

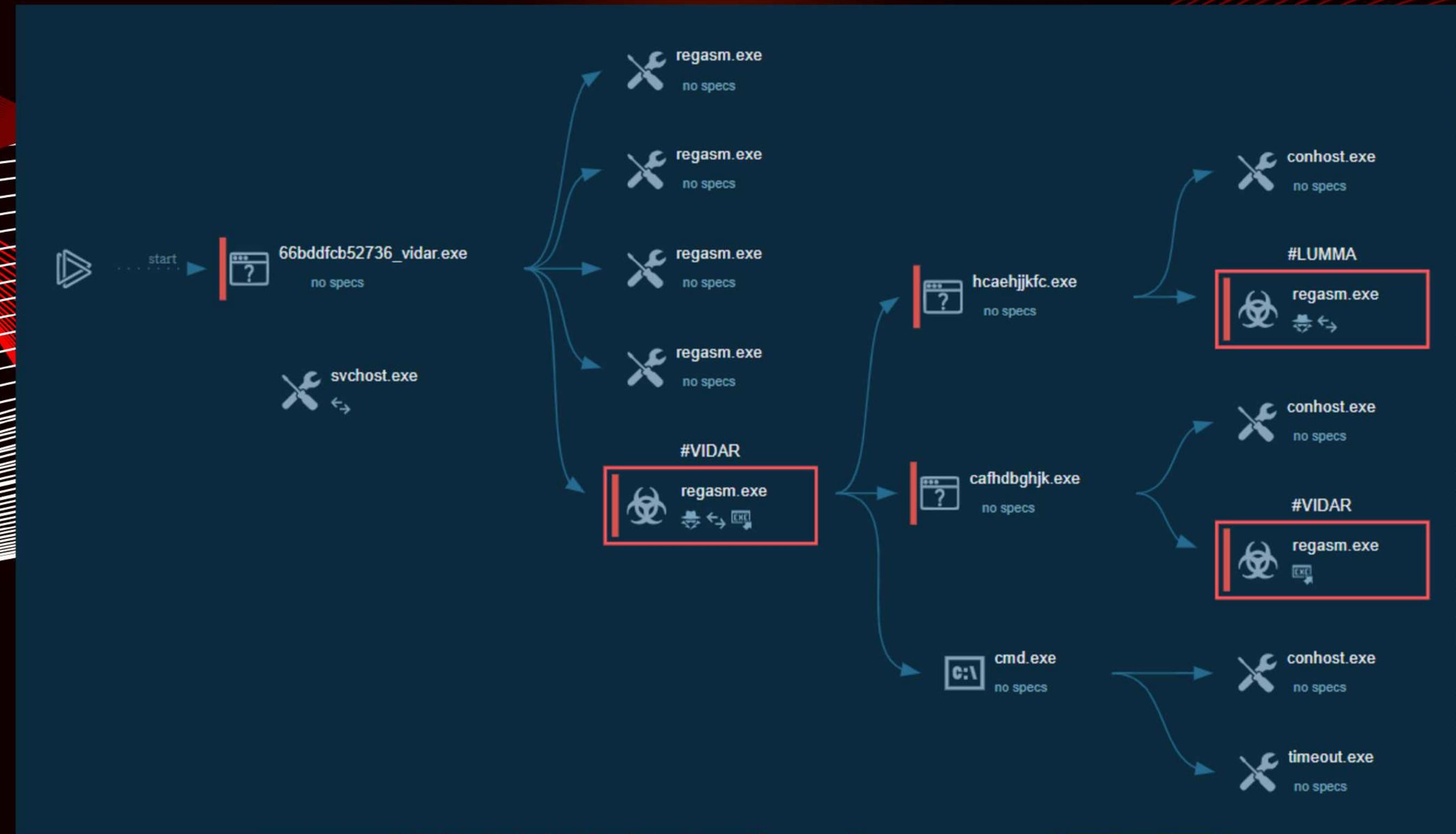
- Chiave di crittografia utilizzata da Chrome per cifrare e decifrare i dati sensibili.
- Informazioni sul profilo: Dati relativi al profilo utente attivo e altre configurazioni.

The screenshot shows the AnyRun analysis interface with a prominent red 'Danger 4' rating at the top. Below it, several threat detections are listed:

- T1555.003 Credentials from Web Browsers (1)**
  - Steals credentials from Web Browsers
- T1552.001 Credentials In Files (2)**
  - Steals credentials from Web Browsers
  - Actions looks like stealing of personal data
- VIDAR has been detected (YARA)**
- T1518 Software Discovery (1)**
  - Actions looks like stealing of personal data

# PARTE I

## Analisi AnyRun



# PARTE 1

## Analisi AnyRun

### CONCLUSIONI

Come abbiamo analizzato, il Malware in questione:

Esegirà delle modifiche ai registri di sistema a fine di Rubare Informazioni e credenziali degli utenti.

### CLASSIFICAZIONE

Vero positivo.

Minaccia Reale.

### SOLUZIONI

Consigliamo:

- **I'isolamento del sistema per prevenire la diffusione ed ulteriori danni.**
- **Eliminazione e Rimozione del file dannoso**
- **Ripristino del sistema da un backup pulito, se disponibile.**



# PARTE 2

## Analisi AnyRun

Il secondo Malware che andremo ad analizzare è un link **GITHUB**  
<https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe>



### Descrizione dei Processi:

Una volta recatoci all'interno, la pagina effettuerà un

#### Download Drive-by:

Visitando il sito in questione effettuerà un download automatico dei file allegati:



### Jvczfhe.exe e Muadnrd.exe

Una volta scaricati ed eseguiti appariranno diversi crash

Andando ad eseguire

cmd.exe

Installutil.exe



# PARTE 2

## Analisi AnyRun

PER OTTENERE LA PERSISTENZA IL MALWARE SFRUTTA:

**CMD.EXE**

Un **CMD.exe** Malevolo viene eseguito (**Andando a sostituire il CMD.exe legittimo ed ottenere così la persistenza**) questo caso il malintenzionato avrà la possibilità di effettuare C2 ovvero azioni di Command and Control

**INSTALLUTIL.EXE**

InstallUtil.exe potrà installare ulteriori payload senza l'intervento diretto dell'utente

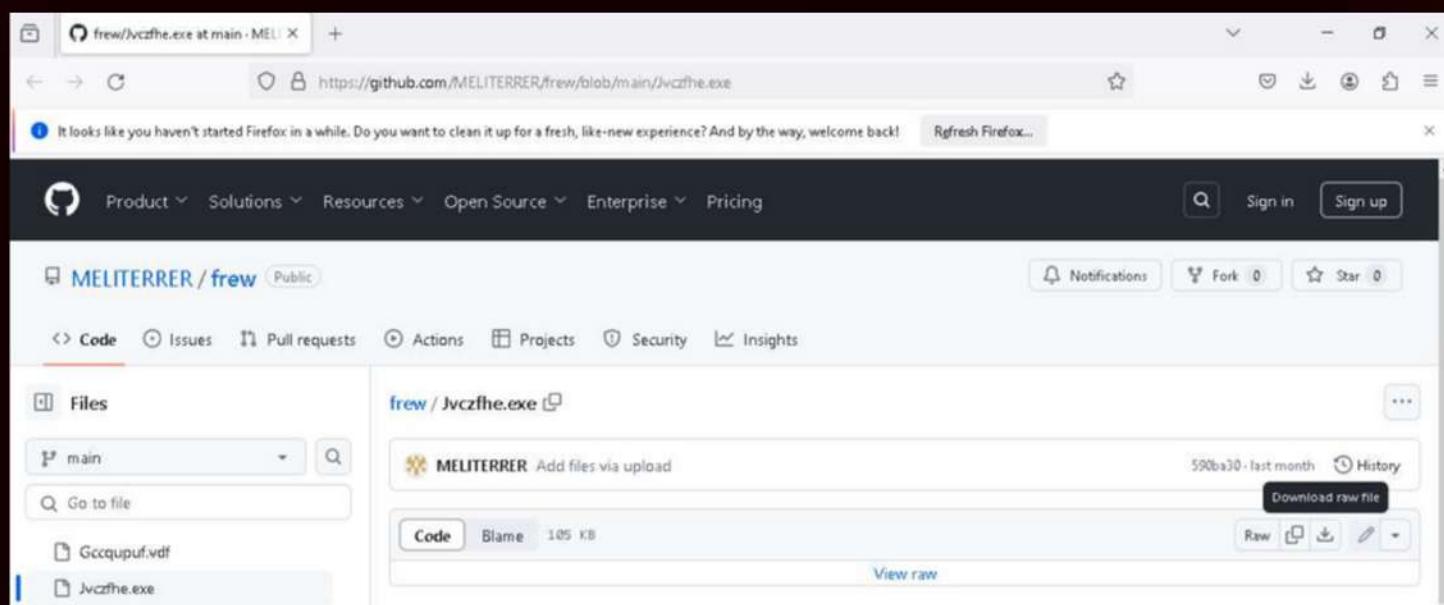
Possiamo reputare questo Malware come una Backdoor di tipo Netreactor.

Tipologia di Malware avanzato progettato per fornire agli attaccanti un accesso remoto e un controllo completo sui sistemi infetti.

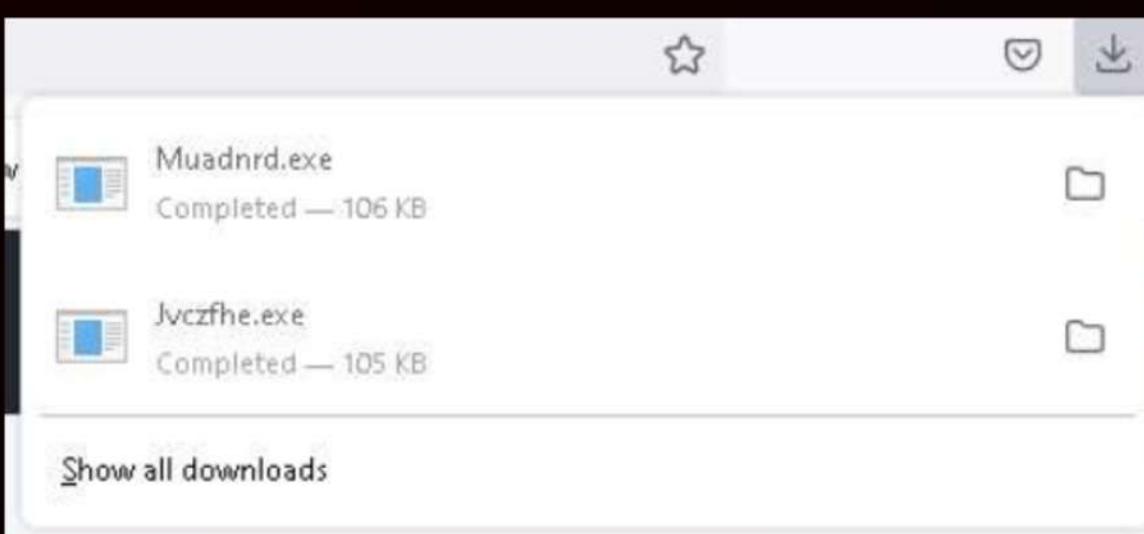
# PARTE 2

## Analisi AnyRun

1. APERTURA LINK [HTTPS://GITHUB.COM/MELITERRER/FREW/BLOB/MAIN/JVCZFHE.EXE](https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe)



2. DOWNLOAD DRIVE-BY: DOWNLOAD AUTOMATICO DEL FILE ALLEGATO (MALWARE)



3. CRASH DELL'APPLICAZIONE ALL'AVVIO DEL MALWARE



4. NEL FRATTEMPO ESEGUE CMD.EXE – INSTALLUTIL.EXE  
OTTENENDO PERSISTENZA E CONTROLLO REMOTO



CMD.exe



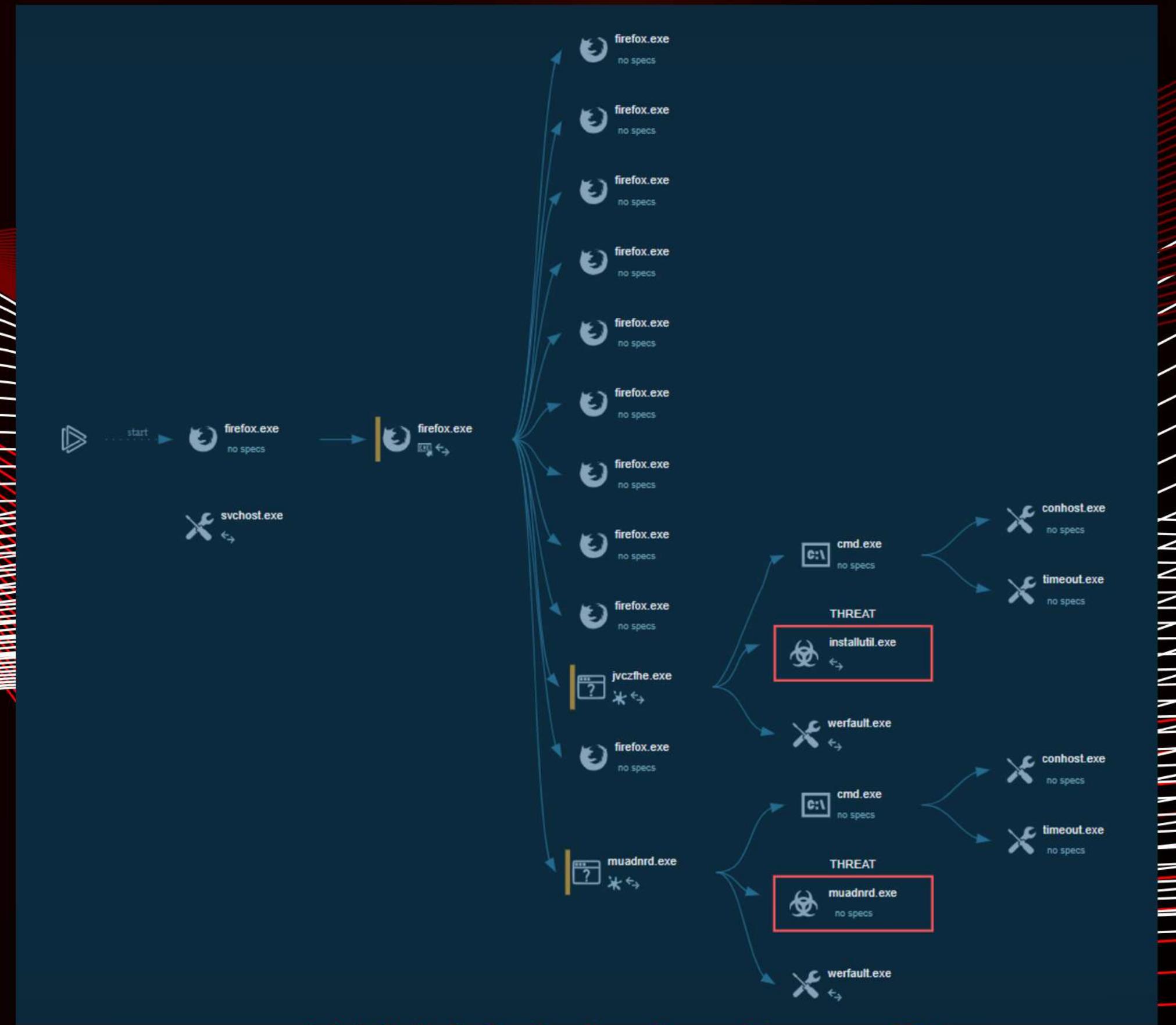
Installutil.exe

5. COMPLETO CONTROLLO DEL SISTEMA DA PARTE DELL'ATTACCANTE C2



# PARTE 2

## Analisi AnyRun



# PARTE 2

## Analisi AnyRun

### CONCLUSIONI

Come abbiamo analizzato, il Malware in questione:

Può essere scaricato da un link apparentemente legittimo (github) con lo scopo di inserire una backdoor  
avendo la possibilità di accedere e controllare il sistema da remoto.

### CLASSIFICAZIONE

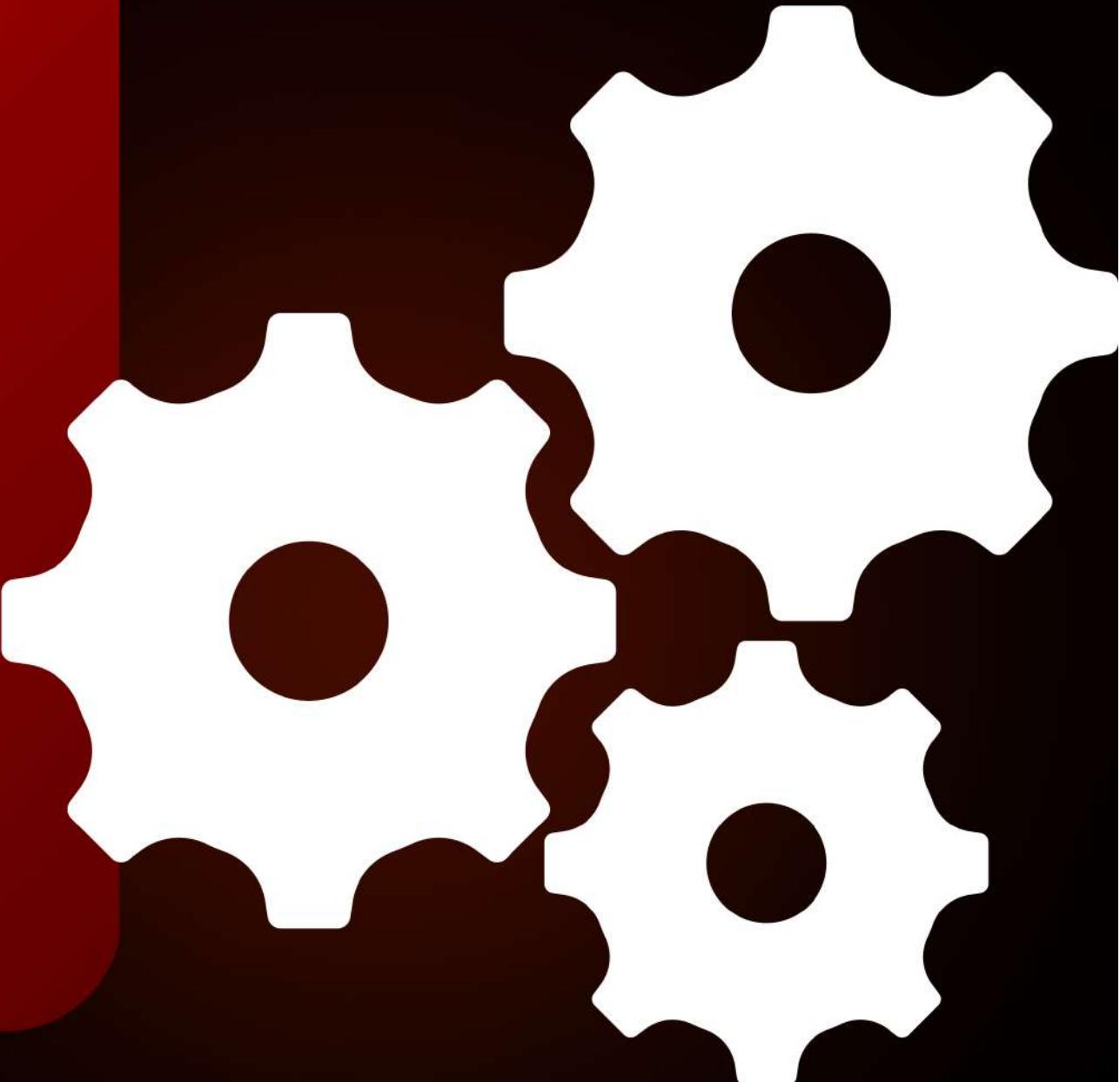
Vero positivo.

Minaccia Reale.

### SOLUZIONI

Consigliamo:

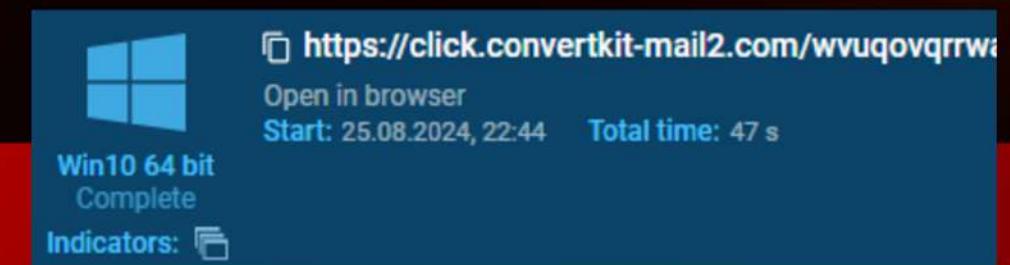
- Isolamento del Sistema dalla rete per prevenire ulteriori danni.
- Rimozione del NetReactor (Malware).
- Ripristino del sistema da un backup pulito, se disponibile.
- Aggiungere il link nella blacklist per ridurre la diffusione del malware



# PARTE 3

## Analisi AnyRun

il terzo link che andremo ad analizzare



[click.convertkit-mail2.com/wvuqovqrwagh50ndddc7hnxdlxuu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2IbnVyc2VyZWNydwI0ZXJz](https://click.convertkit-mail2.com/wvuqovqrwagh50ndddc7hnxdlxuu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2IbnVyc2VyZWNydwI0ZXJz)

viene eseguito all'avvio di Google Chrome

Il link in questione è stato impostato nella fase di avvio del Web Browser tramite linea di comando.  
è possibile che sia stato eseguito accidentalmente

```
"C:\Program Files\Google\Chrome\Application\chrome.exe" --disk-cache-dir=null --disk-cache-size=1 --media-cache-size=1 --disable-gpu-shader-disk-  
cache --disable-background-networking --disable-  
features=OptimizationGuideModelDownloading,OptimizationHintsFetching,OptimizationTargetPrediction,OptimizationHints "https://click.convertkit-  
mail2.com/wvuqovqrwagh50ndddc7hnxdlxuu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2IbnVyc2VyZWNydwI0ZXJz"
```

# PARTE 3

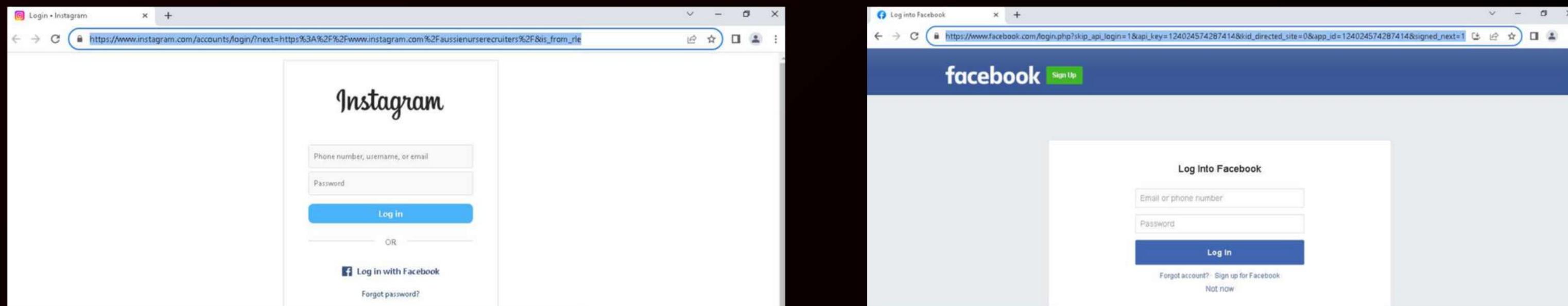
## Analisi AnyRun

Avviando google ci reindirizzerà nelle pagine login dei corrispettivi social

-Instagram

-Facebook

abbiamo potuto verificare che gli URL sono Leggittimi



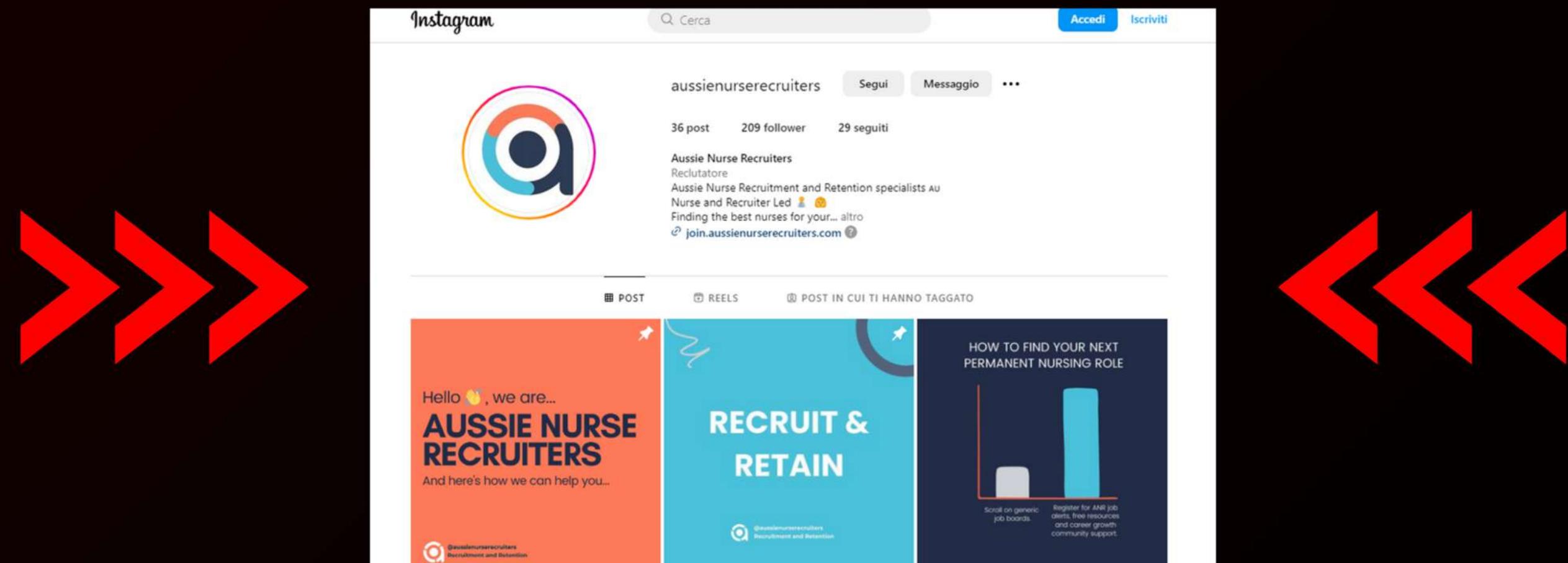
# PARTE 3

## Analisi AnyRun

Qualora andassimo a visitare il link in questione:

[click.convertkit-mail2.com/wvuqovqrwagh50ndddc7hnxdlxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2IibnVyc2VyZWNydwIOZXJz](https://click.convertkit-mail2.com/wvuqovqrwagh50ndddc7hnxdlxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2IibnVyc2VyZWNydwIOZXJz) il Browser

Ci reindirizzerà in una semplice pagina Instagram



# PARTE 3

## Analisi AnyRun

### CONCLUSIONI

L'unico movimento sospetto è l'avvio del link Clickconvertkit-mail2.com la quale non risulta essere dannoso.

Nonostante i collegamenti sono sicuri sarebbe meglio analizzare nel dettaglio il processo

### CLASSIFICAZIONE

Falso positivo

### SOLUZIONI

Consigliamo:

**Mettere il sistema in quarantena**

**Chiedere al vendor per ulteriori informazioni**



# TRACCIA

## GIORNO 5

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

In questo link sono presenti due MALWARE

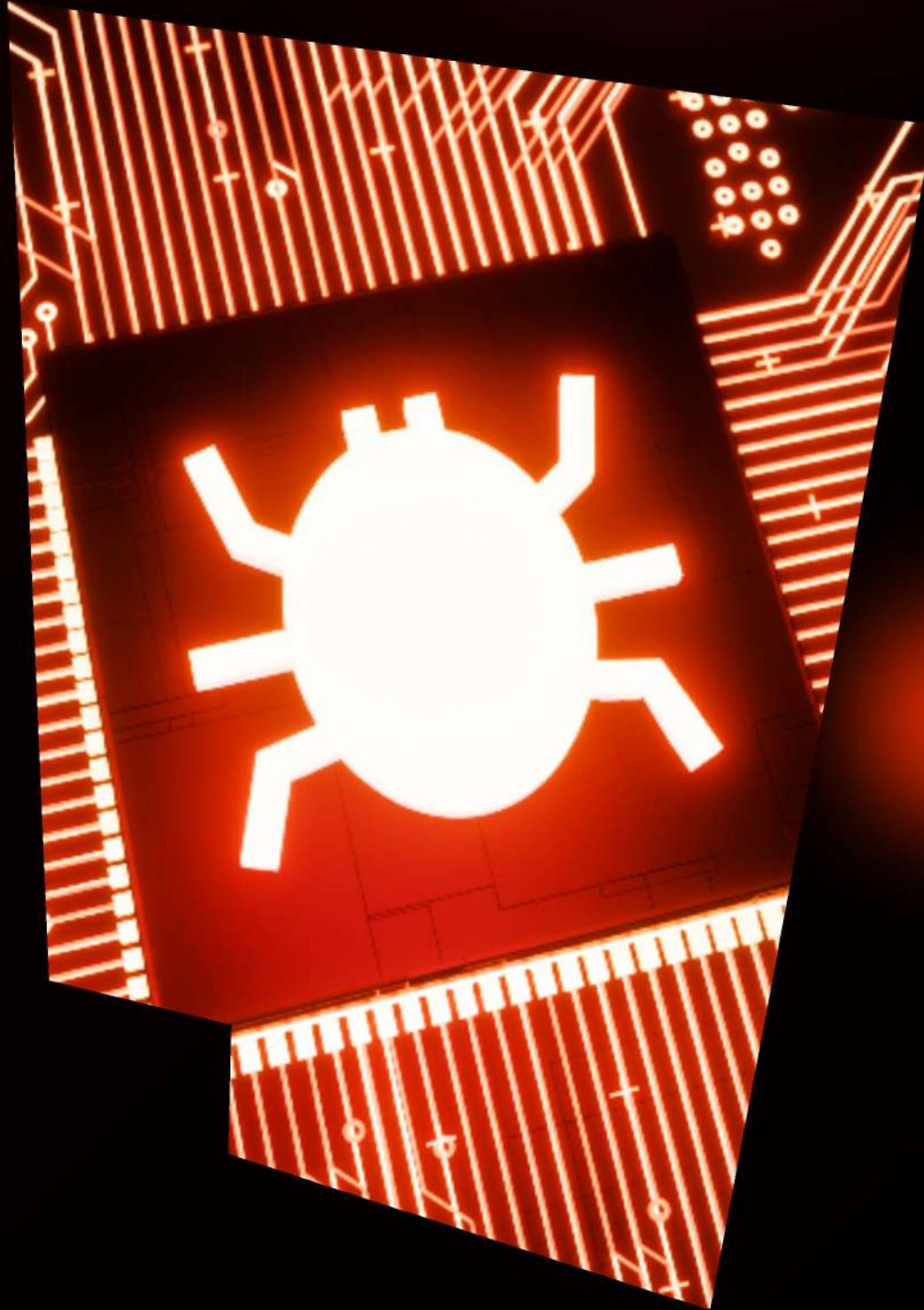
### PARTE 1

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

### PARTE 2

Il solito dipendente "sveglia" 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.



# PARTE 1

## Analisi Statica

Abbiamo eseguito un'indagine approfondita su un software sospetto. È stata eseguita un'analisi sia statica che dinamica per determinare la natura del programma e verificare se si trattasse di un malware.

### CFF EXPLORER

Per iniziare, è stata condotta un'analisi statica utilizzando CFF Explorer, uno strumento specializzato per l'esplorazione dei file eseguibili.

Attraverso questo strumento, sono state **raccolte le seguenti informazioni**:

- **Nome del File e Compagnia:** Sono stati identificati il nome del file eseguibile e il nome della compagnia che lo ha prodotto. Queste informazioni sono state utili per iniziare una prima valutazione dell'affidabilità del software.

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®

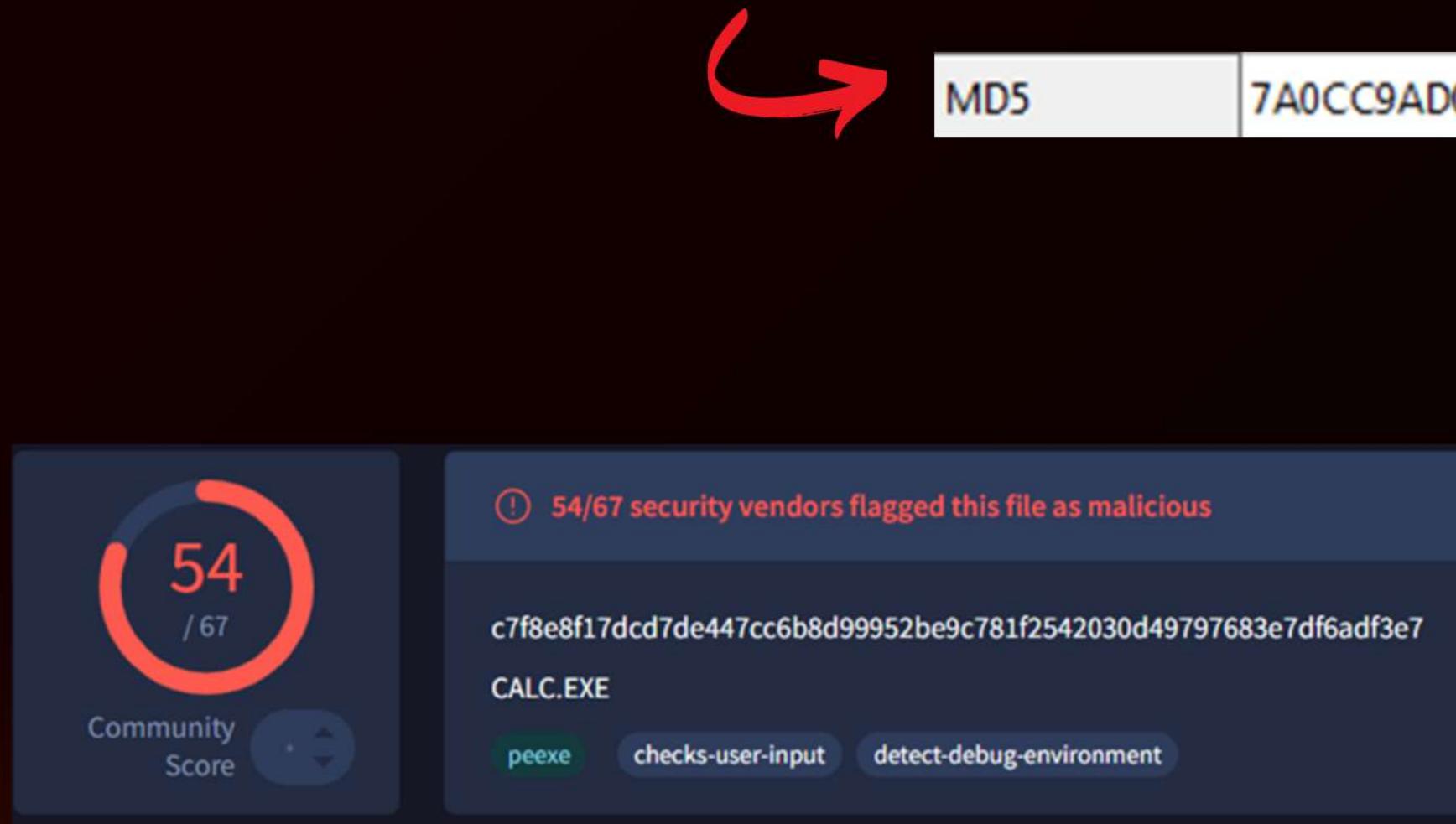
Alcune informazioni sul file sono scritte in cirillico. Usando un traduttore scopriamo che il nome della compagnia indicato è “**Microsoft Corporation**” e la descrizione del file è “**Calcolatrice per Windows**”. Queste informazioni sembrano puntare ad un file legittimo. Infatti, Microsoft è nota per localizzare completamente i propri prodotti, inclusi i nomi delle compagnie e le descrizioni, nella lingua dell'utente finale. Ciò nonostante, **possiamo osservare che il nome originale del file (CALC) differisce da quello attuale**. Questo è un **segnale d'allarme** perché spesso i malware cambiano il loro nome per mascherarsi come software legittimi o per evitare di essere rilevati da strumenti di sicurezza.

# PARTE 1

## Analisi Statica

### VIRUS TOTAL

- **Calcolo dell'Hash:** È stato calcolato l'hash del file utilizzando CFF Explorer. L'hash è una rappresentazione univoca del contenuto del file e serve come "impronta digitale" per identificare il software in modo preciso.



A screenshot of a VirusTotal analysis page. On the left, there's a circular progress bar with the number '54' in red, indicating the number of hits. Next to it, the text 'Community Score' is visible. In the center, the MD5 hash of the file is shown as '7A0CC9AD09AC127C2B82FC953E8AFC8D'. Above this hash, the text 'MD5' is displayed. Below the hash, there's a warning message: '① 54/67 security vendors flagged this file as malicious'. Underneath the hash, the file name 'CALC.EXE' is listed, along with several tags: 'peexe', 'checks-user-input', and 'detect-debug-environment'. A large red arrow points from the 'MD5' label on the right towards the highlighted MD5 hash in the center of the screenshot.

L'hash calcolato è stato successivamente utilizzato per effettuare una ricerca su VirusTotal, un servizio online che aggrega i risultati di numerosi motori antivirus per fornire una valutazione del rischio associato a un file specifico.

Su un totale di 67 motori antivirus, 54 vendor hanno rilevato il file come malware. Questo risultato indica con alta probabilità che il software in questione presenta caratteristiche tipiche di un programma malevolo.

# PARTE 1

## Analisi Statica

- **Librerie Utilizzate e API Sospette:** Durante l'analisi, sono state esaminate le librerie utilizzate dal software. È emersa la presenza di diverse API sospette, tipicamente associate a comportamenti malevoli, come l'accesso a funzioni di sistema critiche, la manipolazione del registro di sistema, la creazione di processi secondari e l'interazione con la clipboard. Tali attività sono spesso indicative di azioni tipiche dei malware, quali la raccolta di informazioni sensibili, l'evasione di controlli di sicurezza e l'iniezione di codice.

Di seguito una valutazione dettagliata delle API principali utilizzate:

**RegOpenKeyExA, RegCloseKey:** Queste funzioni sono utilizzate per aprire e chiudere chiavi del registro di sistema. L'accesso al registro di sistema non è tipico per una semplice calcolatrice. Se queste API vengono usate per accedere a chiavi sensibili o modificarle, potrebbe indicare un comportamento sospetto, come la persistenza del malware (es. inserendosi nelle chiavi di esecuzione automatica) o l'alterazione di configurazioni di sistema.

**LoadLibraryA, GetProcAddress:** Queste API sono utilizzate per caricare dinamicamente librerie e ottenere indirizzi di funzioni in esse contenute. È comune in molti programmi legittimi per caricare funzionalità esterne. Tuttavia, un uso frequente e non documentato di queste API può suggerire l'intenzione di caricare codice potenzialmente dannoso o librerie non autorizzate.

# PARTE 1

## Analisi Statica

**GetStartupInfoA, GetCommandLineW:** Queste API ottengono informazioni sul processo di avvio e sulla linea di comando passata al programma. Anche se possono essere utilizzate legittimamente, in combinazione con altre API sospette potrebbero indicare che il programma sta cercando di modificare il proprio comportamento in base a come è stato avviato o ai parametri passati, magari per eseguire tecniche di offuscamento.

**CreateThread:** Questa API permette di creare nuovi thread di esecuzione. L'uso di thread multipli non è necessariamente sospetto, ma può essere utilizzato da malware per eseguire operazioni in background, come la raccolta di informazioni o l'esecuzione di payload malevoli.

**GetClipboardData:** Accede ai dati presenti nella clipboard di Windows. Un'applicazione calcolatrice non ha normalmente bisogno di accedere alla clipboard. L'accesso alla clipboard potrebbe essere usato per rubare dati sensibili (ad esempio, password o informazioni bancarie copiate negli appunti dall'utente).

**Sleep:** Fa sì che il thread corrente si metta in attesa per un determinato intervallo di tempo. Sebbene non sia di per sé sospetta, Sleep può essere usata per ritardare l'esecuzione di azioni dannose o per bypassare alcuni controlli di sicurezza temporizzati.

**Per concludere, un eseguibile chiamato "calcolatrice" che utilizza queste API può essere considerato sospetto.**

# PARTE 1

## Analisi Statica

### STRINGS

- Abbiamo cercato di estrapolare ulteriori informazioni andando a cercare delle stringhe visibili nel codice. Per farlo abbiamo usato il tool strings e il risultato è stato salvato su un txt



```
C:\Users\user\Desktop\Software Malware analysis\SysinternalsSuite>strings C:\Users\user\Downloads\BuildWeek\calcolatriceinnovativa50.exe > strings.txt
```

Oltre ad aver trovato riferimenti ad alcune API già viste in precedenza, abbiamo trovato un riferimento ad una **Windows Shell**.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
  name="Microsoft.Windows.Shell.calc"
  processorArchitecture= x86
  version="5.1.0.0"
  type="win32"/>
<description>windows Shell</description>
<dependency>
  <dependentAssembly>
    <assemblyIdentity
      type="win32"
      name="Microsoft.windows.Common-Controls"
      version="6.0.0.0"
      processorArchitecture="x86"
      publicKeyToken="6595b64144ccf1df"
      language="*"
    />
  </dependentAssembly>
</dependency>
</assembly>
```

# PARTE 1

## Analisi Statica

IDA PRO

Arrivati a questo punto abbiamo deciso di analizzare il codice assembly tramite l'uso di IDA Pro.

Sfortunatamente ci siamo trovati davanti un codice difficile da interpretare perché non presenta nessun chiaro riferimento alle API che abbiamo trovato o ad altre funzioni. Inoltre, in diversi parti del codice notiamo questo errore da parte di IDA Pro:



sub\_1004150 endp ; sp-analysis failed

Questo indica che IDA Pro non è riuscito a completare l'analisi automatica della funzione. Questo potrebbe essere dovuto problemi con la struttura del codice o difficoltà con l'analisi statica, ma anche **tecniche di offuscamento**.

Infatti, se un malware utilizza API specifiche ma non si riesce a trovarle tramite analisi statica, il problema potrebbe risiedere nell'uso dinamico delle API (che potrebbe fare tramite l'uso di API viste in precedenza come GetStartupInfoA, GetCommandLineW), tecniche di offuscamento (come lo **String Encryption** che va cifrare i nomi delle API per poi decifrarle a runtime), o anti-debugging.

Altra anomalia è la seguente istruzione:

```
NUL  
aaa  
fisttp word ptr [esi+79898196h]  
mov esp, ds:87D0DE0Ah  
pop ebx
```



L'istruzione sembra anomala poiché esp è generalmente usato come puntatore allo stack e non viene solitamente modificato direttamente in questo modo. Questo potrebbe indicare un comportamento non convenzionale, manipolazione dello stack, o codice che tenta di eseguire operazioni non standard.

# PARTE 1

## Analisi Dinamica

Per effettuare l'analisi dinamica abbiamo usato i tools OllyDbg, ApateDNS, Regshot e Process Monitor.

OLLYDBG

Dopo aver messo in sicurezza la macchina, abbiamo aperto il malware con il software OllyDBG

Durante l'analisi del malware abbiamo riscontrato il seguente errore: **Access violation when writing to [000D0003]**.

La violazione di accesso potrebbe essere intenzionale come meccanismo di offuscamento o come tecniche per rilevare la presenza di un debugger e provocare errori come le violazioni di accesso per interrompere il debug.

Access violation when writing to [000D0003] .

# PARTE 1

## Analisi Dinamica

Per la prossima fase dell'analisi abbiamo usato e preparato i seguenti tools:

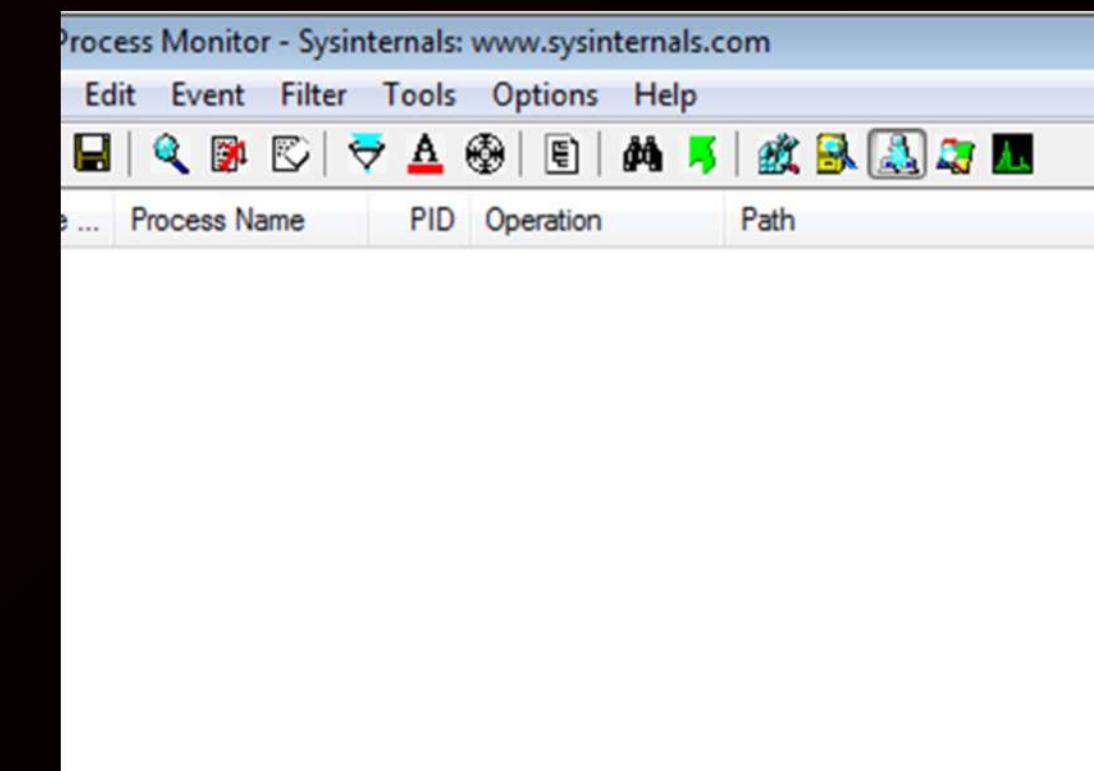
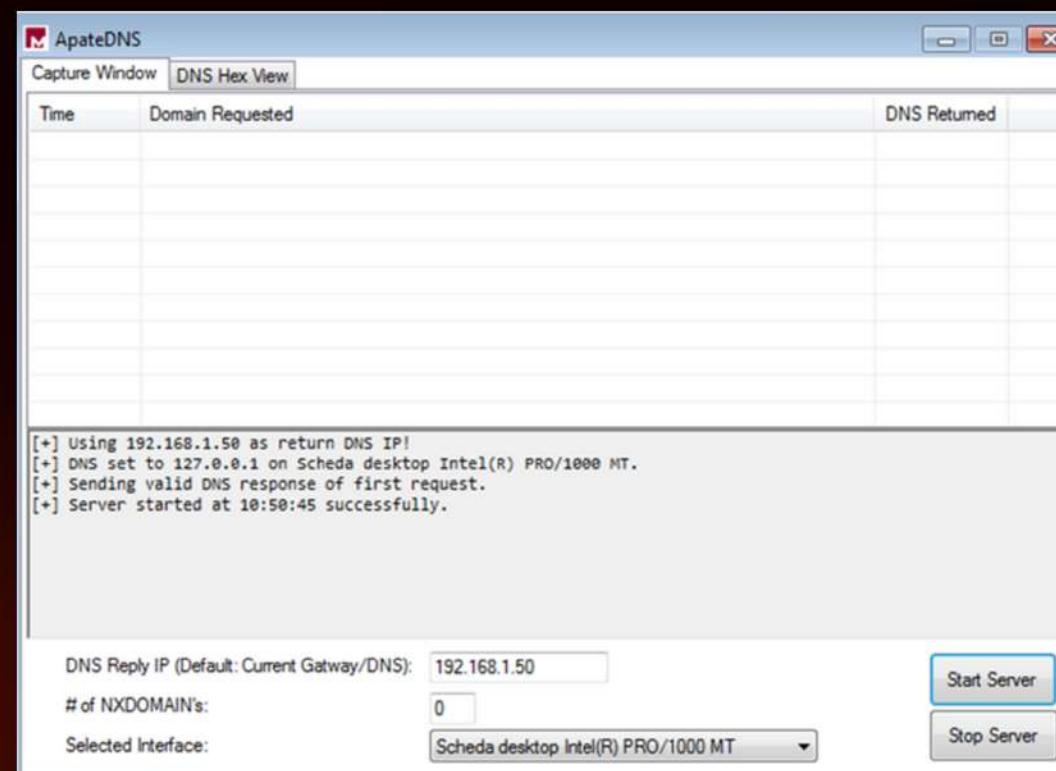
**ApateDNS**, per poter intercettare eventuali tentativi di connessione alla rete;

**Regshot**, per eseguire uno shot dei registri;

**Process Monitor**, per tenere traccia delle attività del malware.

### APATEDNS

Con ApateDNS non abbiamo trovato evidenze relative a tentativi di connessioni da parte del malware, elemento confermato anche dall'analisi con Process Monitor applicando il solo filtro di “Show Network Activity”.



# PARTE 1

## Analisi Dinamica

### ANALISI FILE SYSTEM

Tramite Process Monitor abbiamo analizzato il comportamento del malware sul file system.

**Accesso a File di Sistema Critici:** Il programma tenta di accedere e mappare in memoria diversi file DLL critici situati nelle directory di sistema (C:\Windows\System32\ e C:\Windows\SysWOW64\), come wow64.dll, wow64win.dll, wow64cpu.dll, sechost.dll, e imm32.dll. Questi file sono utilizzati per funzioni di sistema importanti, come la gestione dell'architettura a 32/64 bit e la sicurezza del sistema.

**Creazione di Mappature di File:** Il malware utilizza operazioni di CreateFileMapping, che possono essere utilizzate per modificare o manipolare il contenuto di file in memoria. In diversi casi, i file vengono bloccati con accesso di sola lettura (FILE LOCKED WITH ONLY READERS), suggerendo che il malware potrebbe essere progettato per leggere e potenzialmente alterare o analizzare questi file in modo non autorizzato.

**Tentativo di Accesso alla Prefetch:** L'accesso al percorso C:\Windows\Prefetch\CALCOLATRICEINNOVATIVA50.EXE-950054E1(pf indica che il malware potrebbe tentare di analizzare o modificare file di prefetch. I file di prefetch contengono informazioni su come le applicazioni vengono eseguite, e possono essere utilizzati per migliorare le prestazioni dell'applicazione. L'accesso a questi file potrebbe suggerire un tentativo di elusione o nascondere tracce di attività malevola.

# PARTE 1

## Analisi Dinamica

### ANALISI REGISTRI

Dall'analisi dei registri di sistema, eseguita incrociando i dati ottenuti da Regshot e Process Monitor, sembrano emergere diverse attività che indicano il comportamento del malware.

#### 1. Modifiche alle Attività Pianificate

##### Chiavi Eliminate:

- `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain\{9AA8DB49-6DD1-41ED-BA2C-F6DE78EB5E7E}`
- `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{9AA8DB49-6DD1-41ED-BA2C-F6DE78EB5E7E}`
- La chiave eliminata «MP Scheduled Scan» si riferisce a un'attività programmata legata a Windows Defender per effettuare scansioni periodiche. La sua rimozione potrebbe suggerire un tentativo del malware di disabilitare o evitare scansioni di sicurezza che potrebbero rilevarlo.

##### Chiavi Aggiunte:

- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain\{F88955AD-F670-4D1D-968B-6BE4E2E458AA}
- HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{F88955AD-F670-4D1D-968B-6BE4E2E458AA}
- Una nuova attività programmata è stata aggiunta sotto un GUID differente. Questo potrebbe significare che il malware ha creato una nuova attività pianificata per eseguire codici o payload dannosi in modo regolare o persistente.

# PARTE 1

## Analisi Dinamica

### 2. Modifiche al Registro di Windows Search

#### Chiavi Eliminate:

- HKLM\SOFTWARE\Microsoft\Windows Search\Gather\Windows\SystemIndex\Crawls\12

La rimozione di chiavi legate a Windows Search potrebbe indicare un tentativo di interferire con il servizio di indicizzazione, forse per evitare che certi file o directory siano indicizzati e quindi potenzialmente rilevati dagli strumenti di sicurezza.

### 3. Modifiche alla Shell di Windows e alla Configurazione dell'Esplora Risorse

#### Chiavi Aggiunte:

Modifiche in percorsi come HKU\S-1-5-21-3771313050-58705377-3452663501

1001\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\...` e simili suggeriscono che il malware potrebbe essere interessato a manipolare la configurazione dell'utente per la shell di Windows o per tracciare le attività dell'utente

### 4. Modifiche legate a WBEM/WMI

#### Chiavi Aggiunte:

Modifiche a HKLM\SOFTWARE\Microsoft\WBEM\WDM\DRDGE\... indicano interazioni con il Windows Management Instrumentation (WMI), che potrebbero essere utilizzate dal malware per raccogliere informazioni sul sistema o per stabilire la persistenza.

# PARTE 1



## INTERPRETAZIONE COMPLESSIVA DEL COMPORTAMENTO DEL MALWARE



- **Persistenza e Evasione della Rilevazione:** Il malware sembra adottare tecniche per stabilire la persistenza (attraverso nuove attività pianificate) e per evitare di essere rilevato, disabilitando le scansioni di sicurezza e manipolando configurazioni di sistema che potrebbero consentire di rilevare la sua presenza.
- **Raccolta di Informazioni e Manipolazione dell'Utente:** Modifiche alle chiavi di registro che gestiscono la shell di Windows e le impostazioni dell'Esplora Risorse suggeriscono che il malware potrebbe raccogliere informazioni sulle attività dell'utente o manipolare il comportamento della shell per scopi malevoli.

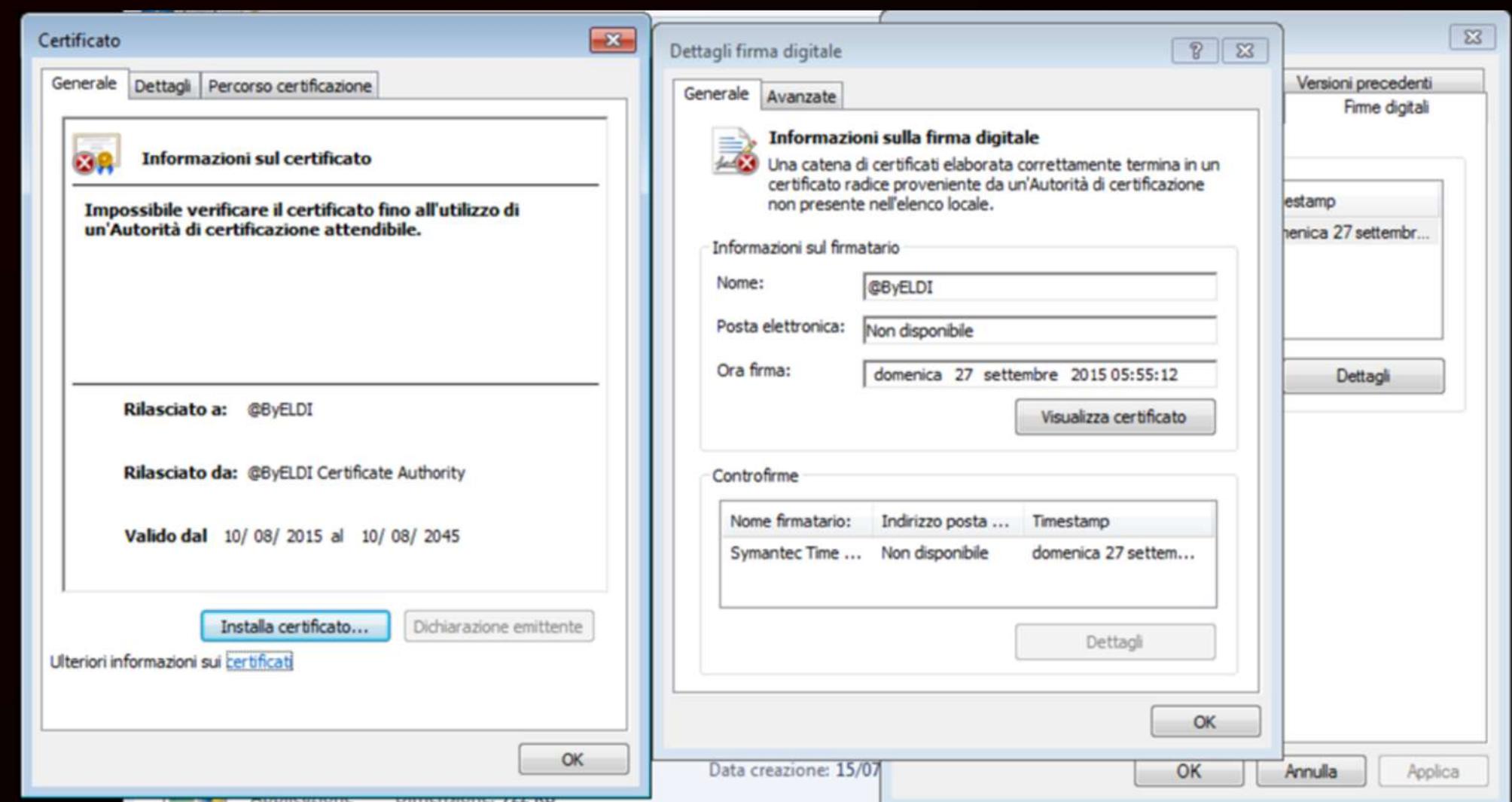
Questi comportamenti sono tipici di malware di tipo Trojan che cercano di mantenere un basso profilo mentre stabiliscono una presenza persistente nel sistema, eludendo la rilevazione e la rimozione da parte di strumenti di sicurezza.

# PARTE 2

## Analisi Statica

### 1] Controllo Firma Digitale

Per prima cosa abbiamo provato, prima ancora di aprire qualsiasi strumento di analisi, a vedere se il file avesse o meno una firma digitale valida per confermarne l'autenticità e l'integrità. Quindi, con un semplice click del tasto destro sull'eseguibile e andando nella sezione “**Firme digitali**” abbiamo potuto notare, come si vede dall'immagine, che **la firma digitale non è considerata attendibile** perché non è presente nell'archivio delle autorità di certificazione.

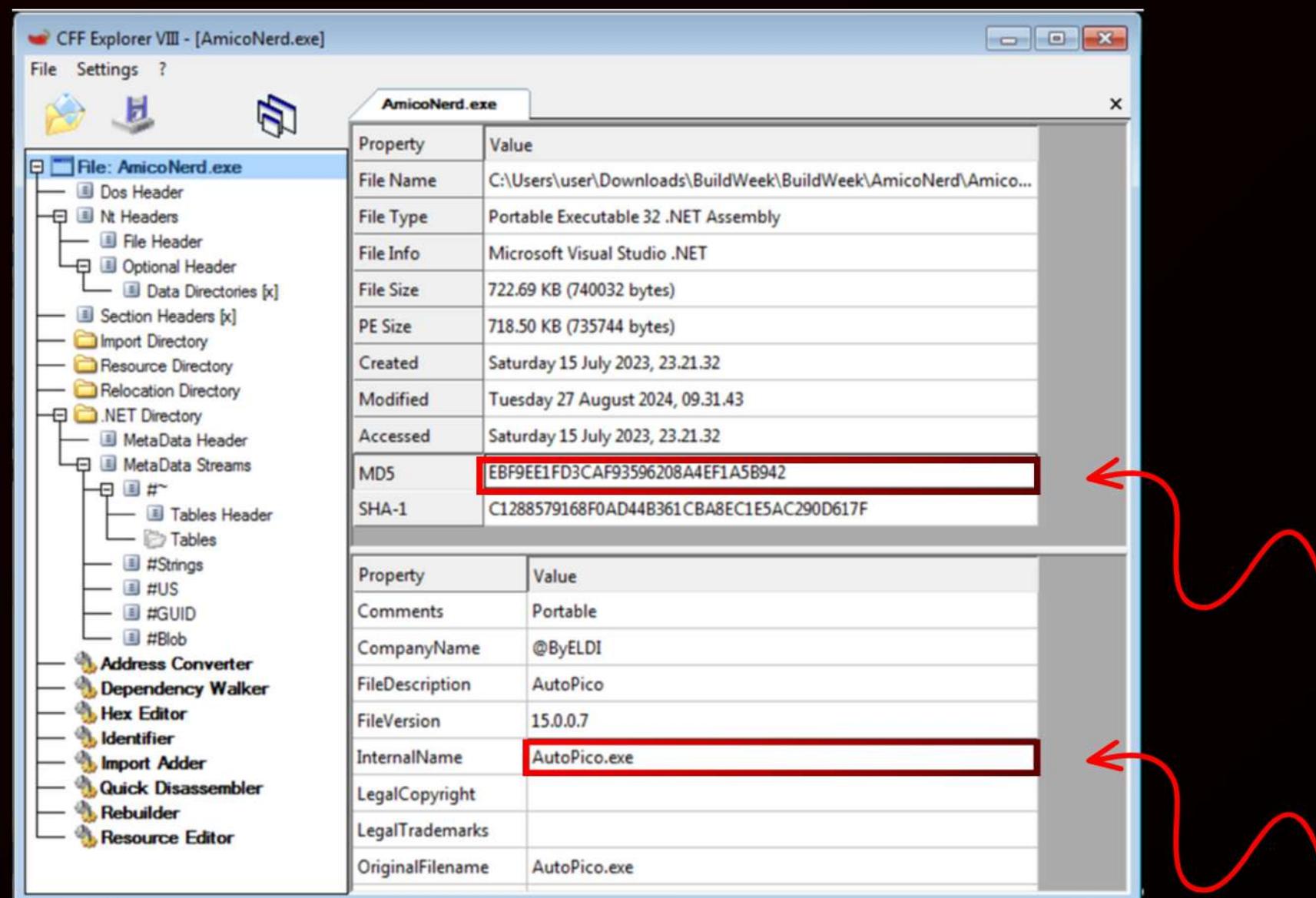


# PARTE 2

## Analisi Statica

### 2] Analisi con CFF Explorer

Da una prima analisi statica con **CFF Explorer**, a colpo d'occhio, si può notare come il vero nome dell'eseguibile non è AmicoNerd.exe ma bensì AutoPico.exe e che l'**hash è EBF9EE1FD3CAF93596208A4EF1A5B942** che ci servirà in seguito per cercare, quest'ultimo, online per confermare che sia un malware e, magari, per trovare delle informazioni circa il suo comportamento.

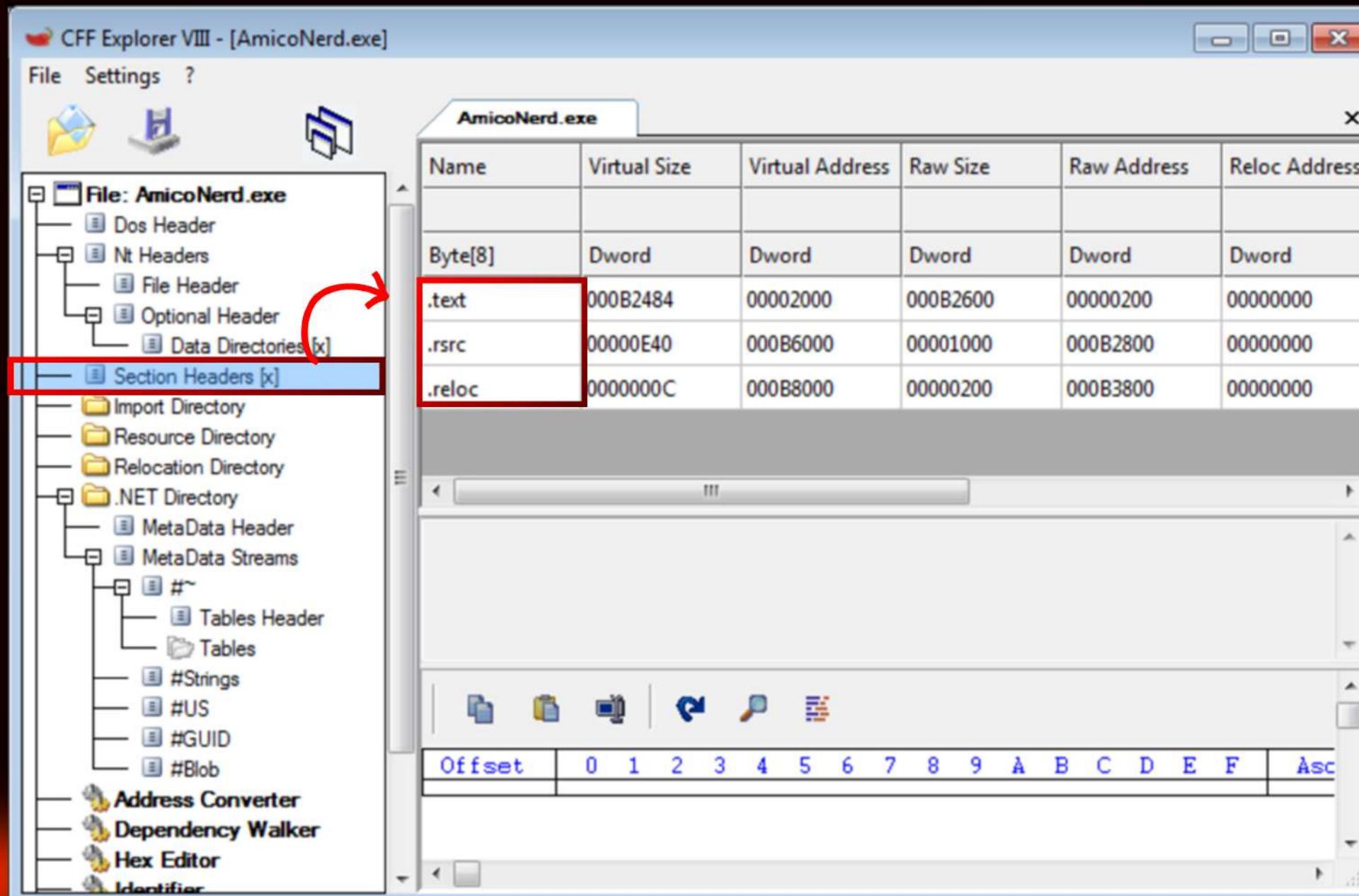


# PARTE 2

## Analisi Statica

### 2] Analisi con CFF Explorer

Sono state controllate le sezioni dell'eseguibile.



Non è stato notato nulla di insolito, solitamente i malware cercano di nascondere le sezioni come .text e .rsrc, inoltre spesso i malware sono difficilmente leggibili o si trovano attività sospette.

Le sezioni di cui è composto l'eseguibile sono:

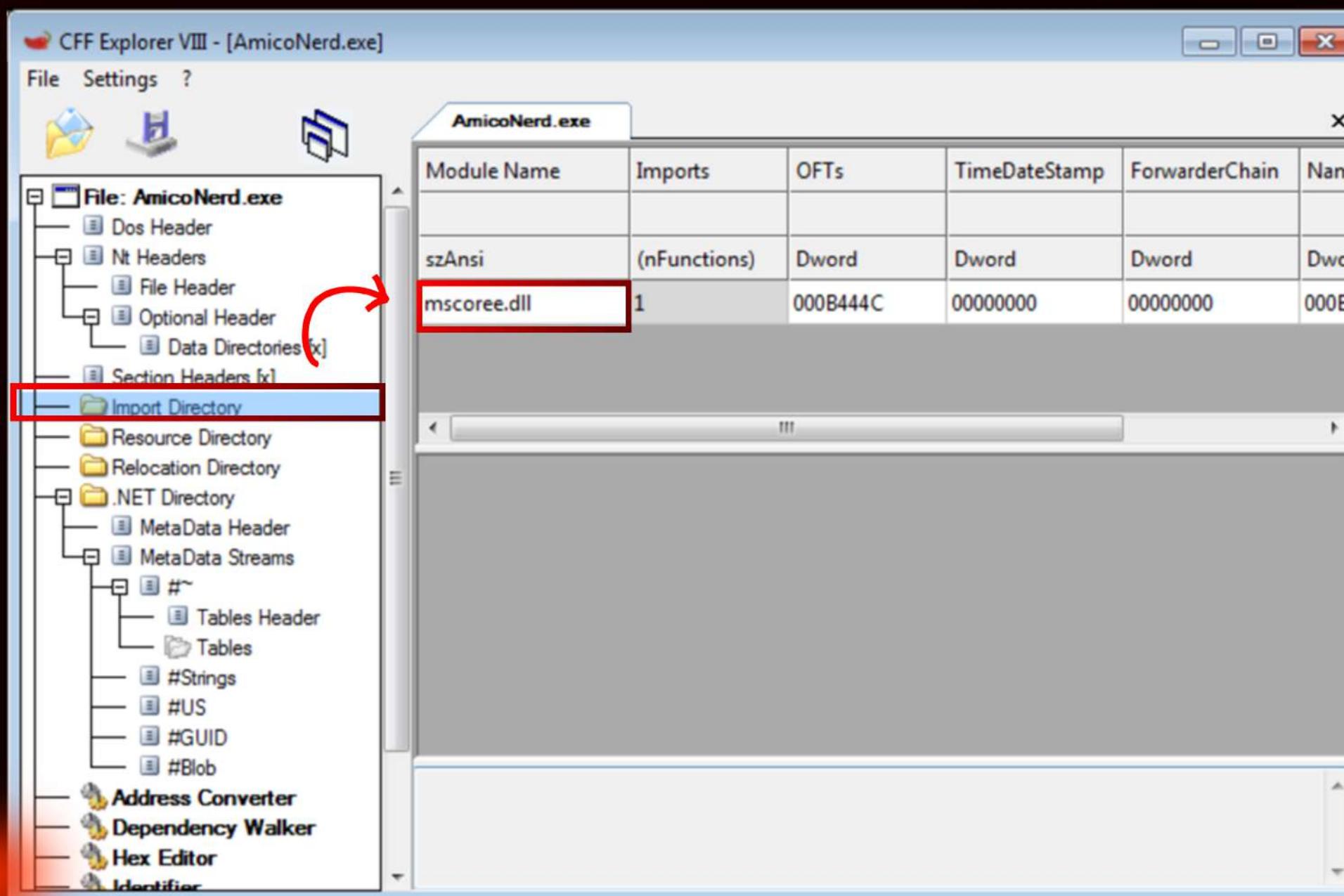
- **.text:** contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.
- **.rsrc:** include le risorse utilizzate dall'eseguibile come ad esempio icone, immagini, menu e stringhe che non sono parte dell'eseguibile stesso.
- **.reloc:** contiene la tabella delle relocation. Queste relocation sono necessarie quando l'eseguibile o la DLL non può essere caricato all'indirizzo di memoria preferito e deve invece essere caricato in un altro indirizzo.

# PARTE 2

## Analisi Statica

### 2] Analisi con CFF Explorer

Infine sono state controllate le **librerie importate dall'eseguibile**.



E si può notare che viene importata una sola libreria per l'esattezza **mscoree.dll**. L'importazione di una sola libreria da parte di un eseguibile non è automaticamente considerata un'attività sospetta, ma può essere un segnale che merita attenzione.



# PARTE 2

Analisi Statica

## 2] Analisi con CFF Explorer

**mscoree.dll** contiene funzioni per l'avvio e la gestione del runtime .NET, inclusa l'esecuzione di codice gestito, la gestione automatica della memoria e la sicurezza del codice. È utilizzata per eseguire applicazioni sviluppate con il .NET Framework, fornendo un ambiente di esecuzione e servizi come la **garbage collection e l'isolamento del codice**.

Se si tratta di un'applicazione semplice, potrebbe aver bisogno di importare solo una libreria per eseguire la loro funzione ma visto che la libreria in questione è mscoree.dll, potrebbe suggerire che l'eseguibile è un modulo gestito .NET, il che **può indicare la presenza di codice offuscato o dinamico, spesso utilizzato dai malware per evitare la rilevazione**.

L'importazione di **una sola libreria** non è necessariamente sospetta da sola, ma **deve essere valutata nel contesto complessivo dell'analisi**.

Se altri segnali indicano comportamenti sospetti (ad esempio il controllo dell'hash su VirusTotal, o un nome di file ingannevole), l'importazione di una singola libreria potrebbe essere un ulteriore indicatore di possibili attività malevoli.

# PARTE 2

## Analisi Statica

### 3] Analisi con VIRUS TOTAL

Torniamo all'**hash** che abbiamo trovato prima e proviamo a caricarlo **su Virus Total** e vediamo cosa riusciamo a vedere.

Dopo aver inserito l'hash sul sito ci si presenta subito la seguente schermata:

57 / 74 security vendors flagged this file as malicious

c6603d416dfc48894eda35d9a9a8523bd9823e215ab926783ce684aa8a62c4

AutoPico.exe

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

checks-network-adapters calls-wmi

Community Score 57 / 74

REANALYZE SIMILAR More

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 20+

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

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

Security vendors' analysis

Vendor	Analysis Result	Vendor	Analysis Result
AhnLab-V3	HackTool/Win.AutoKMS.C948312	AliCloud	Hacktool:MSIL/Idlekms.C
AIYac	Application.Hacktool.KMSActivator.AQ	Anti-AVL	RiskWare[NetTool]/Win64.RPCHook
Arcabit	Application.Hacktool.KMSActivator.AQ	Avast	Win32:MicX-gen [PUP]
AVG	Win32:MicX-gen [PUP]	BitDefender	Application.Hacktool.KMSActivator.AQ
BitDefenderTheta	Gen:NN.ZemsilF.36810.Tm1@a8vJERd	Bkav Pro	W32.AIDetectMalware.CS
ClamAV	Win.Tool.Kmsactivator-9811695-0	CrowdStrike Falcon	Win/grayware_confidence_100% (W)
Cybereason	Malicious.fd3caf	Cylance	Unsafe
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

Dove ci viene detto che su 74 compagnie di sicurezza in 57 hanno rivelato che il file in questione è malevolo. Andando ad analizzare il report fatto da Virus Total possiamo anche vedere altri siti di analisi o sandbox che hanno già analizzato questo file e il loro report, come tria.ge

# PARTE 2

## Analisi Statica

### 3] Analisi con VIRUS TOTAL

Da quest'ultimo possiamo avere un'ottima analisi molto approfondita

Targets

Target  
ebf9ee1fd3caf93596208a4ef1a5b942

Size  
722KB

MD5  
ebf9ee1fd3caf93596208a4ef1a5b942

SHA1  
c1288579168f0ad44b361cba8ec1e5ac290d617f

SHA256  
c6603d416dfc48894eda35d9a9a8523bd9823e215ab926783ce6848aa8a62c4

SHA512  
070ba2b5e5ee7af04d4e4718b1f80baaa4d1870cf1a6d4e87549a5aaa2eacc0b95e1a80e3355a3428f7  
a282ec3beb1a63180e7c97dcdb1ae11494736866c9b19

Creates new service(s)  
PERSISTENCE

Sets file execution options in registry  
PERSISTENCE

Stops running service(s)  
EVASION

Loads dropped DLL

Score  
8 /10

EVASION PERSISTENCE

A screenshot of the VirusTotal analysis interface. On the left, there's a list of hashes and their corresponding file types (represented by icons like document, image, and executable). To the right, a large red box highlights a 'Score' section showing '8 /10'. Below the score are two tabs: 'EVASION' and 'PERSISTENCE'. A red arrow points from this highlighted area to a callout box on the right.

Ci viene mostrato di che tipo è il malware e anche semplice una mappa concettuale che ci mostra come il malware si comporta all'interno del sistema.

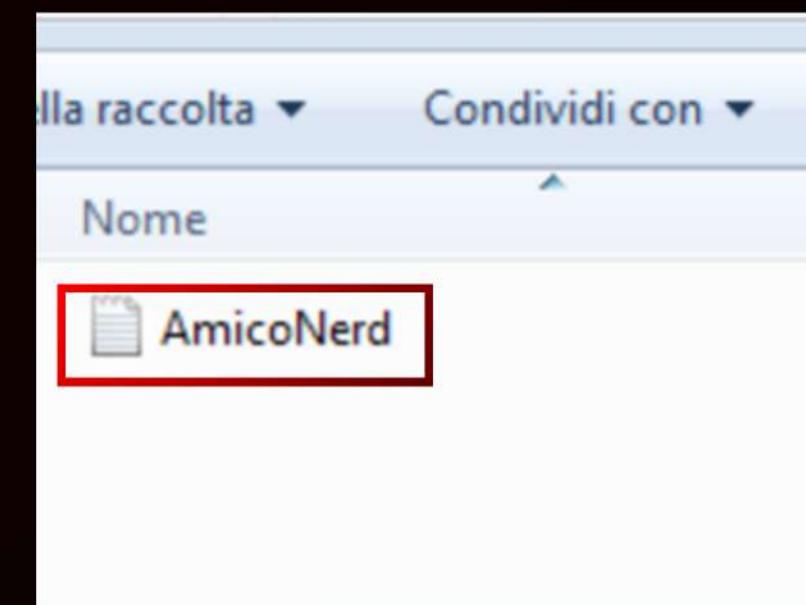
# PARTE 2

## Analisi Dinamica

Abbiamo appurato che il nostro “**Amico Nerd**” è un malware. L'unica cosa che vorremmo sapere è cosa fa esattamente questo malware?

Per questo abbiamo messo in sicurezza la nostra macchina virtuale per la analisi dinamica e, **dopo aver lanciato il malware**, ci siamo accorti che nella cartella dove c'era l'eseguibile ne era apparsa un'altra (logs) con un file di testo all'interno. Andandolo a controllare **era il log** che il malware stesso ha fatto dopo esser stato eseguito, descrivendo tutto ciò che ha fatto.

 logs	28/08/2024 10:03	Cartella di file
 AmicoNerd	27/08/2024 09:31	Applicazione 723 KB
 DM.bin	28/08/2024 10:03	File BIN 0 KB



AmicoNerd - Blocco note

File	Modifica	Formato	Visualizza	?
10:03:42:331 Checking Internet Connection...				
10:03:42:331 2024.08.28 AutoPico 15.0.0.7				
official site:				
<a href="http://forums.mydigitallife.info/threads/491">http://forums.mydigitallife.info/threads/491</a>				
Time Start: 28/08/2024 10:03:41				
10:03:42:566 windows Detected: Windows 7 Pro				
10:03:42:581 Using host: 127.102.167.77:1688				
10:03:42:659 Opening Firewall Port...				

# PARTE 2

## Analisi Dinamica

Andando ad analizzare il log possiamo dire cosa ha fatto il malware durante la sua esecuzione.

### 1) Connessione Internet e Informazioni di Sistema

**Checking Internet Connection...**

Il malware cerca la connessione a Internet, che non riesce a stabilire (perché la macchina era sola su una rete locale).

**Windows Detected: Windows 7 Professional...**

Il malware rileva la versione del sistema operativo, in questo caso Windows 7 Professional.

### 2) Configurazione del Servizio KMS

**Using host: 127.102.167.77:1688**

Configura l'indirizzo IP del server KMS (Key Management Service) per l'attivazione del software. L'indirizzo IP e la porta 1688 sono usati per comunicare con un server KMS simulato.

**KMSEmulator Port: 1688**

Viene avviato un emulatore KMS sulla porta 1688

### 3) Interazioni con il Firewall

**Opening Firewall Port...**

Tenta di aprire una porta nel firewall per facilitare la comunicazione del servizio KMS.

**Error: Opening Firewall App**

Fallisce nell'apertura del firewall, probabilmente perché il firewall su questo Windows è disabilitato

### 4) Accedere e Modificare Chiavi di Registro

**SYSTEM\CurrentControlSet\Services\sppsvc**

Qui il malware accede alla chiave di registro legata al servizio di protezione software (sppsvc), che è responsabile della gestione delle licenze di Windows. Il valore Start in questa chiave determina come e quando il servizio viene avviato.

### 5) Gestione delle Chiavi di Licenza di Office

**Loading OEM Key Dumper...** Il malware carica uno strumento che cerca chiavi di licenza OEM, probabilmente per manipolarle.

**Office 2013/2016/2010 Skipped:** Il malware salta l'attivazione delle versioni di Office menzionate. Questo suggerisce che l'obiettivo principale è l'attivazione di Windows.

### 6) Gestione delle Chiavi di Licenza di Windows

**KMSEmulator running port: 1688:** L'emulatore KMS viene avviato sulla porta 1688, il che permette di simulare un server KMS locale per l'attivazione delle licenze.

**None MSDM table found:** Non trova una tabella MSDM, che normalmente contiene chiavi di licenza OEM nei dispositivi che supportano l'attivazione automatica.

**Found Windows Products:** Il malware identifica la versione di Windows installata (Windows 7 Professional) e i dettagli associati come la modalità di licenza (RETAIL channel) e la chiave di prodotto parziale.

### 7) Installazione e Conversione della Chiave di Prodotto:

**Installing Key: -GPDD4:** Tenta di installare una nuova chiave di prodotto (-GPDD4).

**Converting: Windows(R) 7, Professional edition:** Converte l'edizione di Windows da un canale RETAIL (vendita al dettaglio) a un canale VOLUME\_KMSCLIENT, che è tipicamente usato per le attivazioni via KMS.

**UnInstalling Key - Error: C004F012:** L'errore durante la disininstallazione della chiave di prodotto (C004F012) indica che qualcosa è andato storto nel tentativo di rimuovere la chiave precedente.

# PARTE 2

## Analisi Dinamica

Andando ad analizzare il log possiamo dire cosa ha fatto il malware durante la sua esecuzione.

### 8) Attivazione:

Dopo aver convertito l'edizione di Windows al canale VOLUME\_KMSCLIENT, il malware continua a manipolare il registro di sistema per impostare il nome e la porta del servizio KMS, tentando infine di attivare Windows usando il server KMS emulato.

### 9) Disabilitazione della Cache del Servizio KMS:

**DisableKeyManagementServiceHostCaching 0:** Disabilita la cache per il servizio KMS sul sistema. Questo passo potrebbe essere fatto per assicurarsi che il sistema non memorizzi nella cache le informazioni del KMS precedente, garantendo così che le nuove impostazioni siano applicate correttamente.

### 10) Impostazioni del Registro di Sistema per il Servizio KMS:

#### Set Registry : SoftwareProtectionPlatform:

Il malware modifica il registro di sistema per impostare il nome del server KMS.

Modifica il registro per impostare la porta del server KMS, che di solito è 1688.

### 11) Attivazione di Windows:

**Activating Windows:** Il malware tenta di attivare Windows usando le nuove impostazioni KMS (server e porta) che ha appena configurato.

### 12) Connessione al Server KMS Emulato:

**SetKeyManagementServiceMachine: 0: 127.246.23.93:** Imposta l'indirizzo IP del server KMS a 127.246.23.93. Questo è l'IP del server KMS emulato a cui il malware si connette per tentare l'attivazione.

**Connection accepted from [::ffff:127.0.0.1]:49159:** Una connessione viene stabilita localmente, suggerendo che l'attivazione avviene sullo stesso sistema (localhost).

### 13) Processo di Attivazione:

**Received request: v4, AppID: 55c92734-d682-4d71-983e-d6ec3f16059f, Machine: user-PC:** Il sistema invia una richiesta di attivazione al server KMS. L'AppID corrisponde al tipo di software che il KMS sta tentando di attivare (in questo caso, Windows).

**Sending response: v4, PID: 06401-00142-234-876517-03-1040-9600.0000-0052024:** Il server KMS emulato invia una risposta di attivazione, generando un Product ID (PID) che fa sembrare che l'attivazione sia andata a buon fine.

**Connection closed:** La connessione al server KMS viene chiusa dopo l'invio della risposta

### 14) Attivazione di Windows:

**Windows(R) 7, Professional edition Activated 0:** Conferma che l'attivazione di Windows 7 Professional è riuscita. Questo indica che il processo di emulazione del server KMS e l'installazione della chiave sono stati completati con successo.

### 15) Configurazione delle Impostazioni del Registro per Office:

**Set Registry : OfficeSoftwareProtectionPlatform...:** Il malware procede a configurare diverse chiavi di registro sotto OfficeSoftwareProtectionPlatform. Queste chiavi riguardano il nome del server KMS e la porta da utilizzare per l'attivazione dei prodotti Office. Le chiavi di registro aggiornate specificano il server KMS da usare per attivare diverse versioni e componenti di Microsoft Office. Viene utilizzato lo stesso server KMS emulato che è stato usato per attivare Windows.

# PARTE 2

## Analisi Dinamica

Andando ad analizzare il log possiamo dire cosa ha fatto il malware durante la sua esecuzione.

### 16) Pulizia e Chiusura delle Porte:

**ClearKeyManagementServiceMachine 0 e ClearKeyManagementServicePort 0:** Il malware ripristina le impostazioni di registro riguardanti il server KMS, probabilmente per nascondere le tracce del server KMS emulato che è stato utilizzato.

**Closing Firewall Port...:** Chiude la porta del firewall che era stata aperta per consentire il traffico verso il server KMS emulato. Questo è un tentativo di ripristinare lo stato del sistema per evitare il rilevamento.

---

### 17) Modifica Estetica del Sistema:

**Set Registry : HKEY\_CURRENT\_USER\Control Panel\Desktop**

Modifica una chiave di registro che riguarda la visualizzazione della versione di Windows sul desktop. Questo potrebbe essere un tentativo di disabilitare la visualizzazione della versione di Windows o di manipolarla in qualche modo.

---

### 18) Chiusura del Malware:

**Client listener shut down:** Il malware termina le sue operazioni, chiudendo eventuali processi aperti durante l'esecuzione.



In sintesi ,da quanto riportato dal log, questo malware è progettato per attivare illegalmente copie di Windows e Office, modificando il registro di sistema e utilizzando un server KMS emulato per completare il processo di attivazione senza l'uso di chiavi di licenza legittime

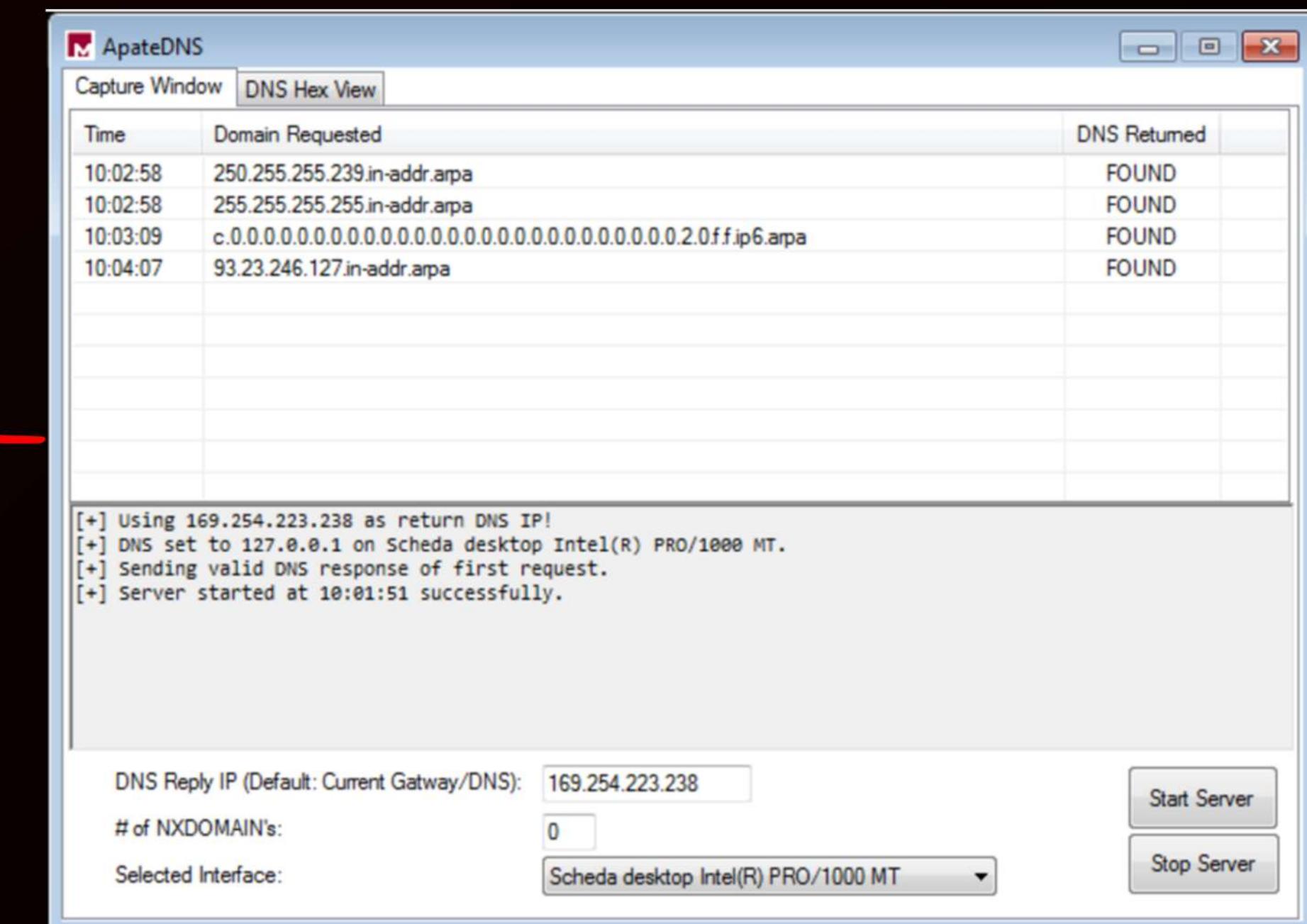
# PARTE 2

Analisi Dinamica

Per essere sicuri che il log sia veritiero possiamo confrontarlo con i dati raccolti dall'analisi dinamica.

Possiamo notare con ApateDNS, che cattura le richieste DNS fatte dal sistema, che ci sono alcuni aspetti che potrebbero sembrare sospetti:

- 1) Le prime due richieste DNS sono per indirizzi IP non validi o di broadcast. Queste richieste potrebbero indicare tentativi di connessione a indirizzi non convenzionali o risposte automatiche.
  - 2) La terza richiesta sembra correlata a un indirizzo IPv6, ma l'indirizzo non sembra corrispondere a un indirizzo IPv6 valido. Questo potrebbe essere un tentativo di camuffare attività sospette.
  - 3) L'ultima richiesta sembra puntare a un indirizzo IP specifico. Questo indirizzo non appartiene a un servizio noto o affidabile, quindi potrebbe essere un altro segnale di attività sospetta.



# PARTE 2

## Analisi Dinamica

Poi possiamo anche vedere che, grazie al report di **regshot**, vengono cancellate 2 chiavi

```
-----  
Keys deleted: 2  
-----  
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Plain\{B3F71B04-A05D-4AE0-96B4-BCEC2723B665}  
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{B3F71B04-A05D-4AE0-96B4-BCEC2723B665}
```

Per poi aggiungerne 27

```
-----  
Keys added: 27  
-----
```

Poi i valori associati alle chiavi del registro di sistema di Windows vengono infine cancellati per poi aggiungerne degli altri valori e, infine, modificati. Il registro di sistema è una parte fondamentale del sistema operativo, dove vengono memorizzate configurazioni e impostazioni per il sistema operativo stesso, il software, i driver, e altro.

```
-----  
values added: 43  
-----
```

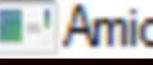
```
-----  
values deleted: 16  
-----
```

```
-----  
values modified: 44  
-----
```

# PARTE 2

## Analisi Dinamica

Per l'ultimo confronto con il log fornito dal malware, possiamo guardare il report di **ProcMon (Process Monitor)**  
Da quest'ultima analisi possiamo vedere come appunto vengano create delle chiavi e modificati molti valori:

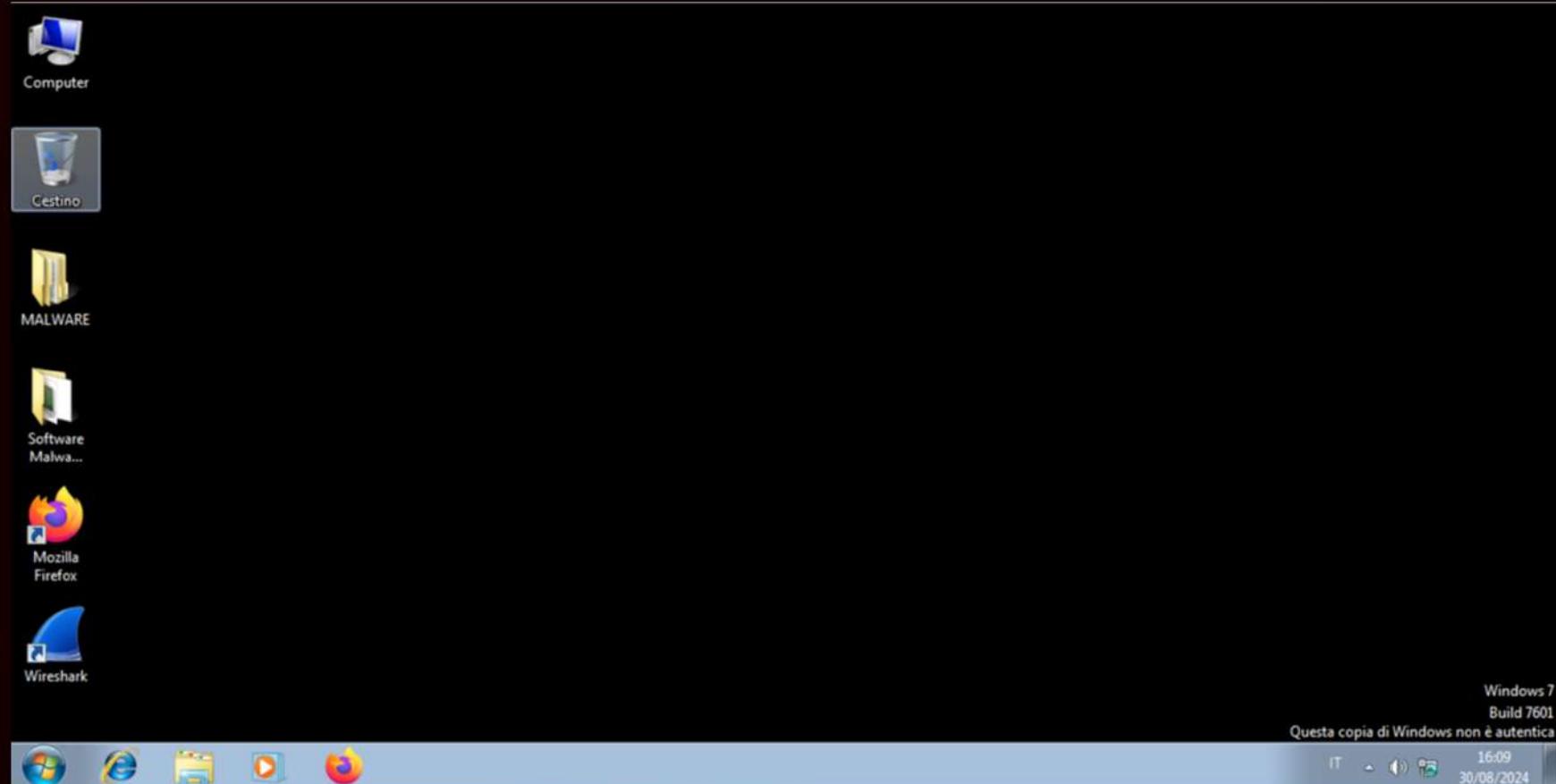
 AmicoNerd.exe	3784	 RegCreateKey	HKLM\Software\Microsoft\Fusion\GACChangeNotification\Default
 AmicoNerd.exe	3784	 RegCreateKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\IL\5a99e5c...
3784	 RegCloseKey	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64\NI\181938c...
3784	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\Fusion\NativeImagesIndex\v4.0.30319_64

# PARTE 2

## Analisi Dinamica

A dimostrazione che quello che abbiamo visto è vero ecco 2 screenshot prima e dopo aver fatto partire il malware



PRIMA



DOPO

# CONCLUSIONE

Con tutte le prove a nostro favore posso tranquillamente dire al nostro dipendente "sveglio" che **"Amico Nerd.exe è un malware progettato per attivare illegalmente copie di Windows e Office, senza l'uso di chiavi di licenza legittime"**





THANK YOU