### Analisi Statica AdwereCleaner.exe

### Introduzione

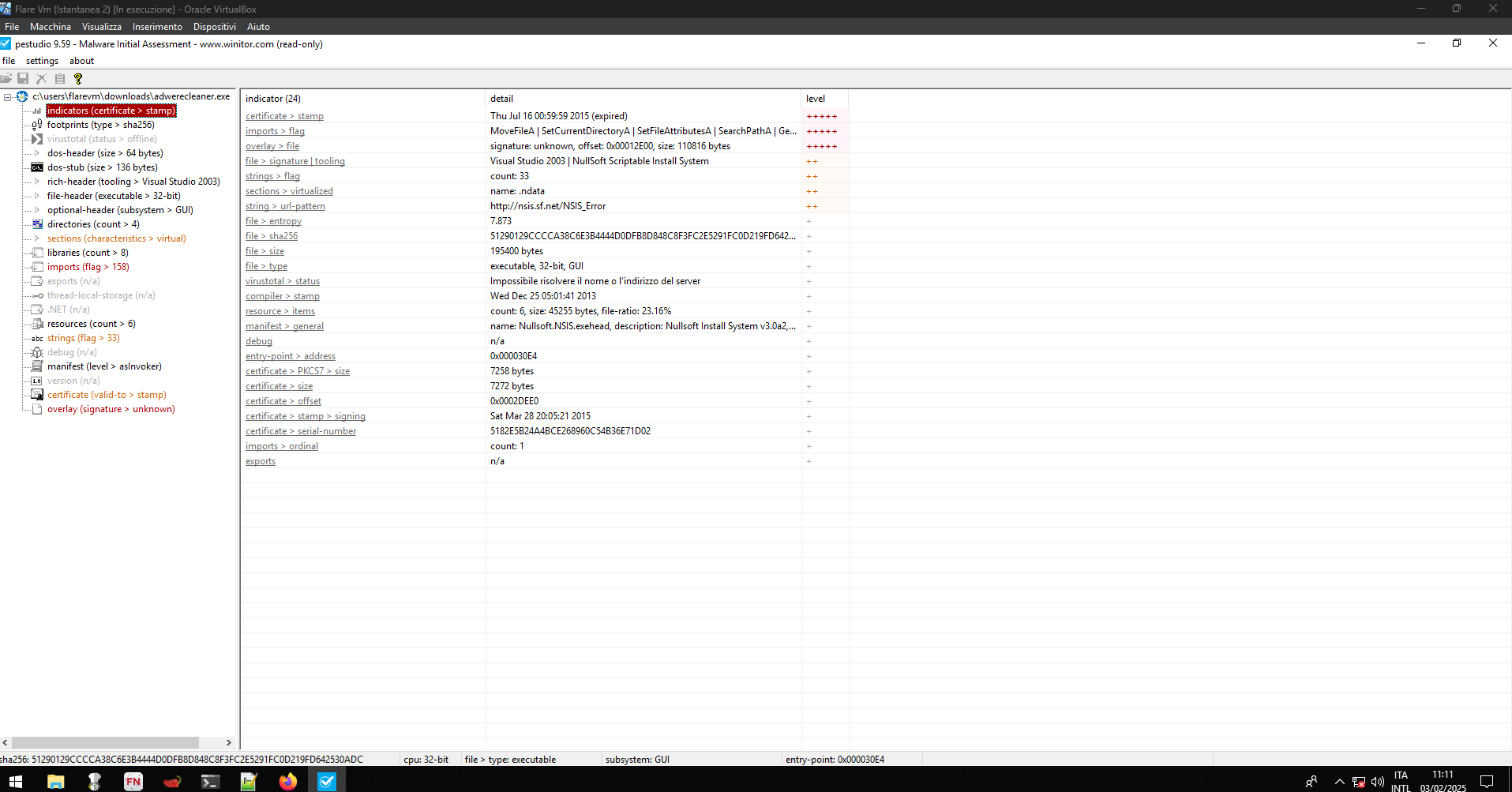
Questa relazione descrive i risultati di un'analisi statica eseguita su un file binario identificato come potenzialmente dannoso. L'analisi è stata effettuata utilizzando diversi strumenti forensi, quali Pestudio, Detect It Easy (DIE), CFF Explorer, Binwalk, File, Unzip/Gunzip, Strings e VirusTotal. L'obiettivo principale è stato quello di determinare caratteristiche anomale, potenziali vettori di attacco e indicazioni di comportamenti sospetti. Nel corso della relazione, i risultati saranno illustrati passo per passo, corredati da esempi visuali tratti dagli strumenti utilizzati.

### Analisi dettagliata

#### Pestudio

L'analisi condotta con Pestudio ha evidenziato diversi indicatori di anomalie nel file analizzato. Il certificato digitale associato risulta scaduto, con una firma sconosciuta o assente. Questo può indicare che il file è stato modificato o che non è stato firmato da una fonte affidabile. Inoltre, l'overlay rilevato (signature > unknown) suggerisce la possibile aggiunta di dati non standard al file.

Un aspetto particolarmente interessante è l'entry-point del file, che si trova a 0x000030E4. Questo valore appare anomalo e potrebbe indicare manipolazioni o compressioni del codice. Pestudio ha anche segnalato l'assenza di informazioni di debug, elemento che conferma che il file è stato compilato senza dettagli tecnici per ostacolare ulteriori analisi. L'hash SHA256 del file è stato analizzato tramite VirusTotal, ottenendo risultati che confermano la natura malevola del file.

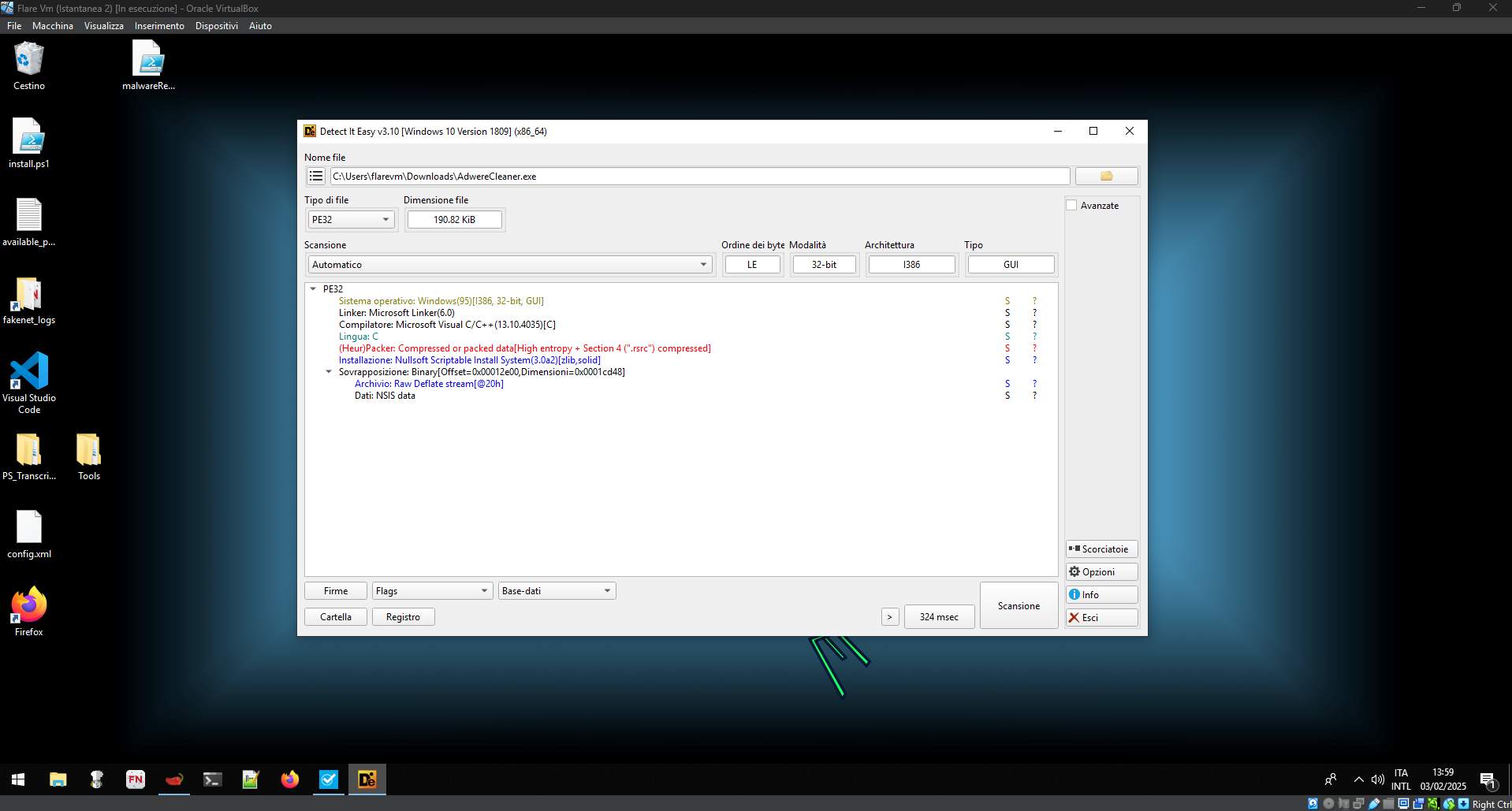
Inoltre, è stato osservato l'uso di API sospette, tra cui ADVAPI32.dll e SHELL32.dll. Queste librerie sono comunemente sfruttate dai malware per attività come la modifica del registro di sistema e l'interazione con il file system. La sezione risorse del file contiene un'icona utilizzata probabilmente per imitare software legittimi. Tuttavia, è stata identificata una risorsa con elevata entropia, denominata instance1 e delle dimensioni di 43.826 byte, che potrebbe contenere dati compressi o cifrati.

##### 

Il primo screenshot mostra gli indicatori principali identificati con Pestudio, tra cui l'entry-point anomalo e l'assenza di debug.

Il secondo screenshot evidenzia la sezione risorse, con l'icona e la risorsa a elevata entropia.

#### Detect It Easy (DIE)

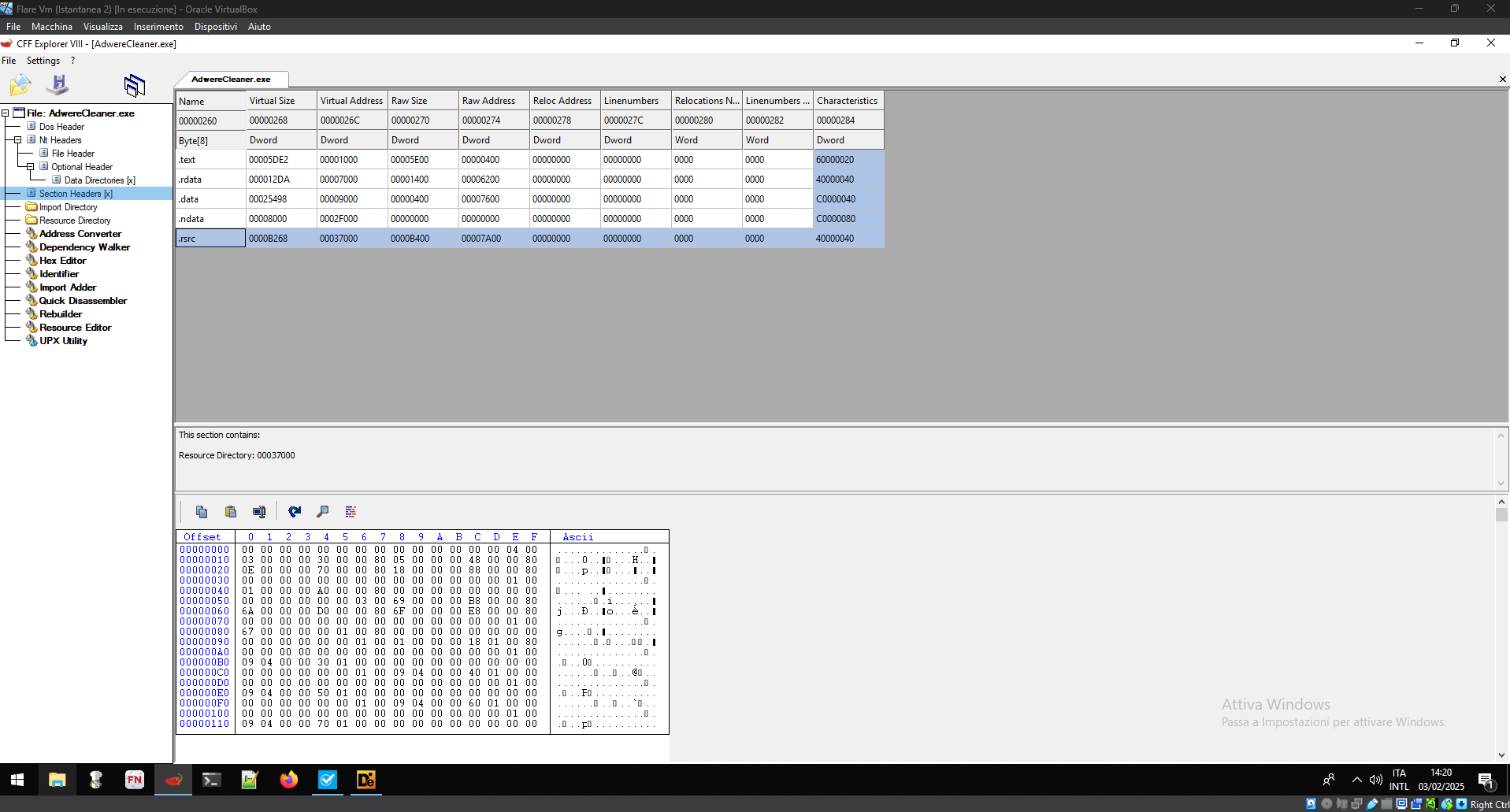
Il file è stato analizzato utilizzando Detect It Easy, che ha confermato che si tratta di un eseguibile PE32 per sistemi Windows a 32 bit. L'analisi ha evidenziato la presenza di HeurPacker, indicando che il file è stato compresso, e una sezione .rsrc con un livello di entropia particolarmente alto, segno che potrebbe contenere dati cifrati o compressi.

Questo screenshot mostra le informazioni estratte tramite DIE, con l'indicazione della compressione e l'alta entropia della sezione .rsrc.

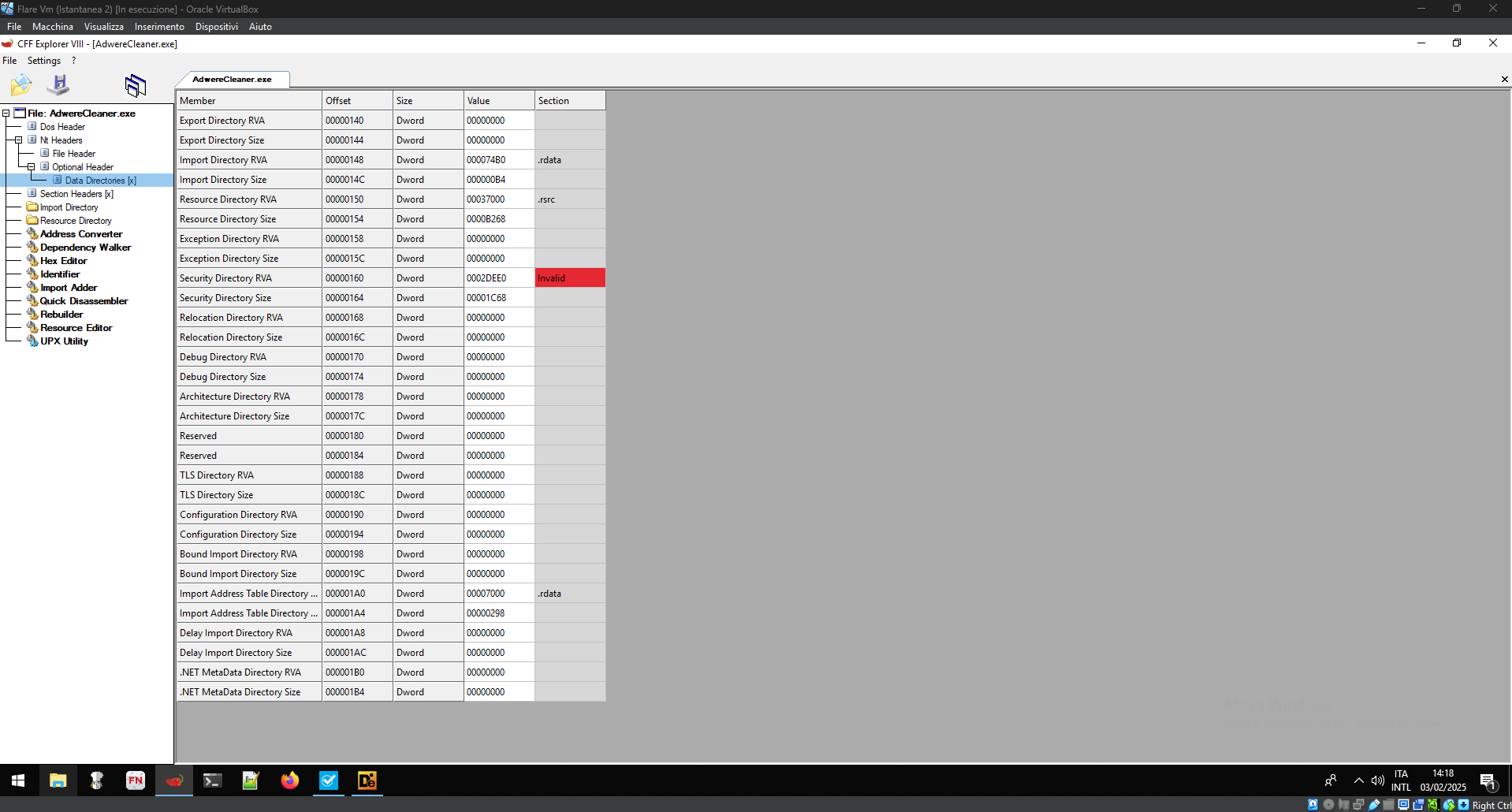
#### CFF Explorer

L'analisi con CFF Explorer ha rivelato ulteriori dettagli interessanti. La directory Security del file presenta un RVA invalido, il che suggerisce una probabile manipolazione della firma digitale. Inoltre, la sezione .rsrc, già segnalata da DIE, conferma un'elevata entropia, potenzialmente indicativa di dati compressi o nascosti.

Un altro elemento critico emerso riguarda la Import Directory, che include riferimenti a librerie come ADVAPI32.dll e SHELL32.dll. Queste librerie sono spesso utilizzate dai malware per garantire persistenza o alterare il registro di sistema.



L'immagine mostra i dettagli delle sezioni, con particolare attenzione alla .rsrc e al suo livello di entropia.



Questo screenshot evidenzia l'RVA invalido della directory Security, che supporta l'ipotesi di manipolazione.

#### Binwalk

L'utilizzo di Binwalk (“-binwalk -e”) ha generato una directory per i file estratti, ma non è stato possibile identificare componenti significativi. Questo potrebbe essere dovuto alla presenza di compressioni o cifrature non standard.

##### 

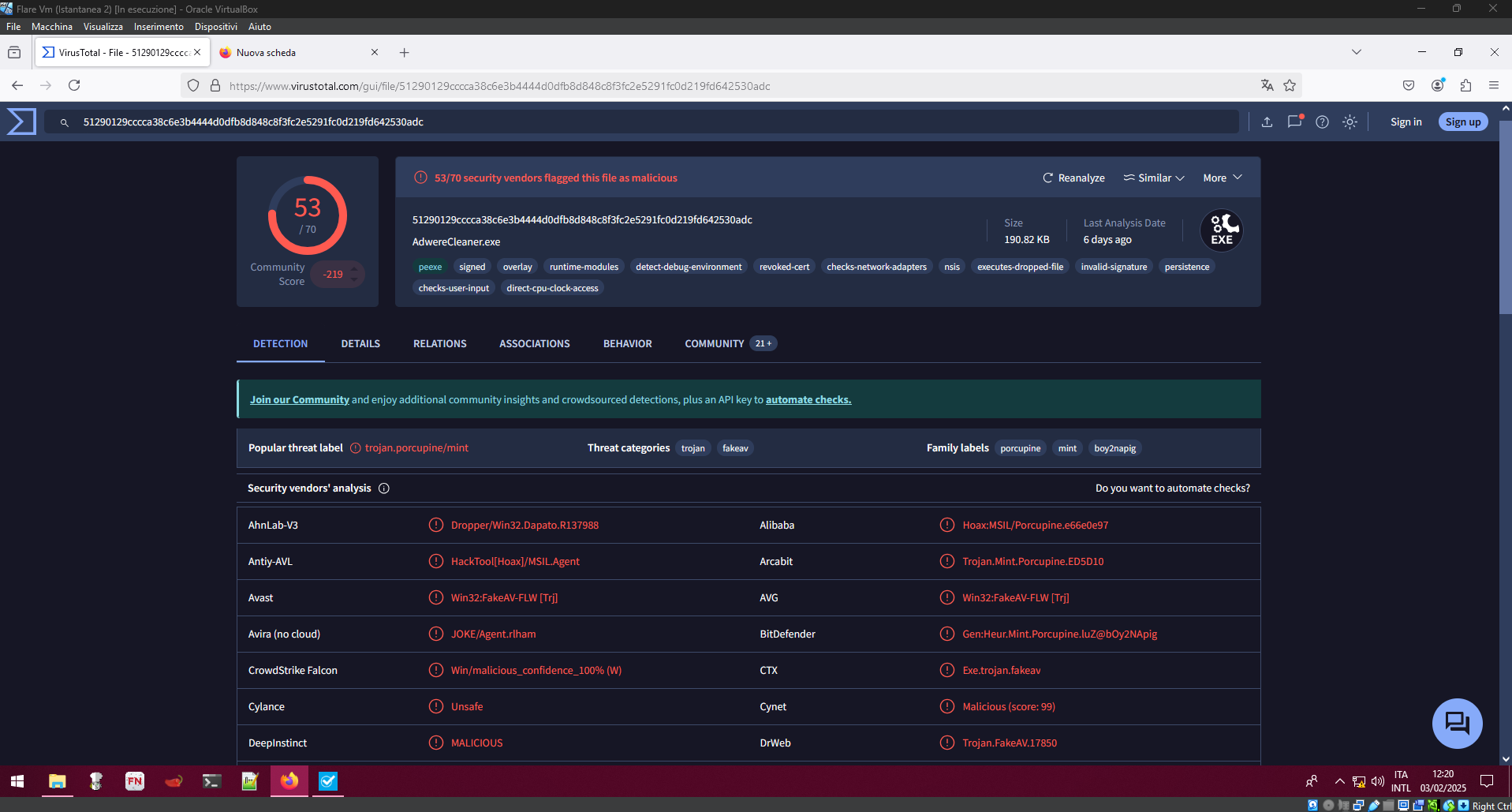
Lo screenshot illustra l'output di Binwalk durante il tentativo di estrazione dei file.

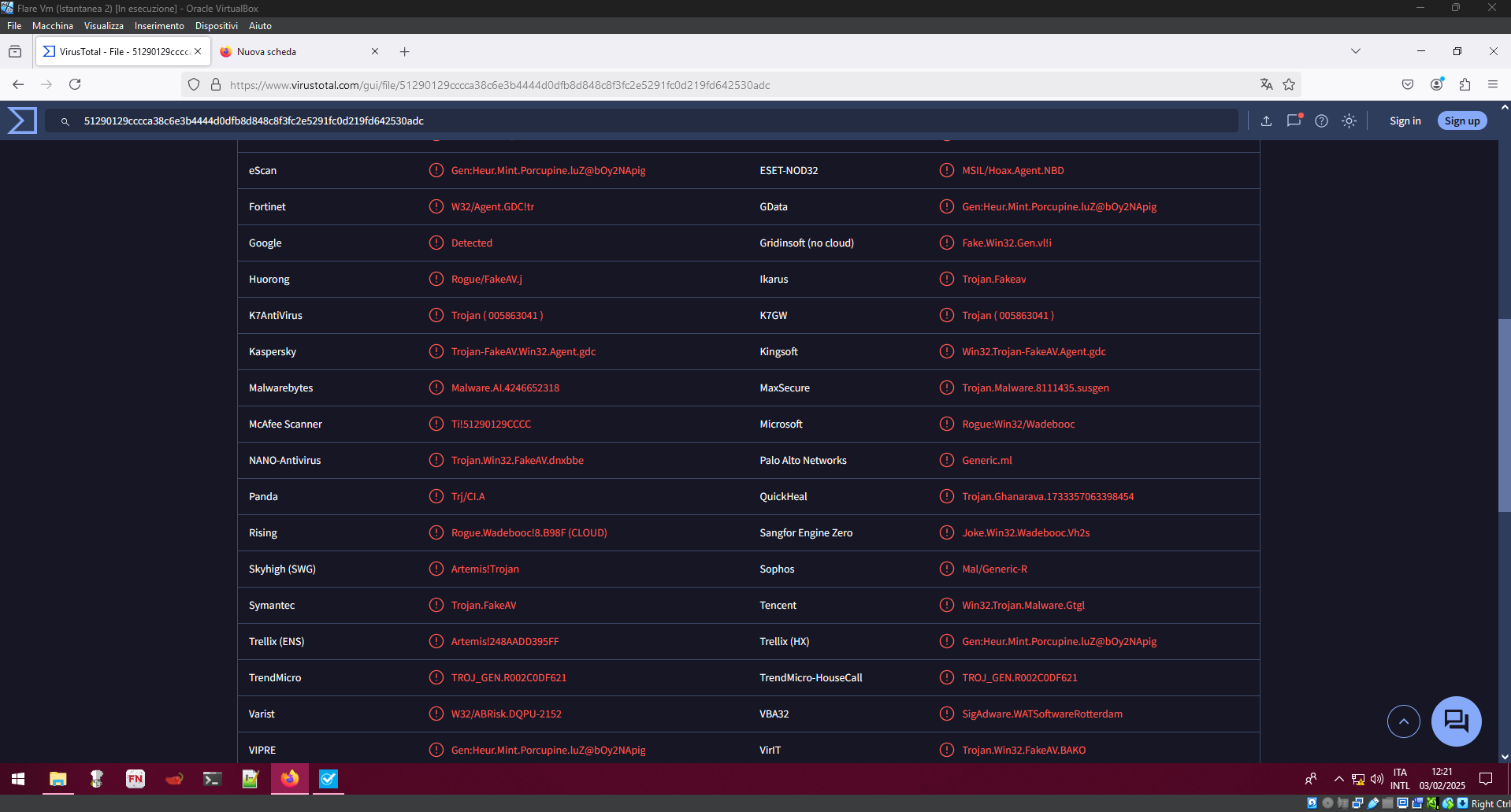
#### Strings

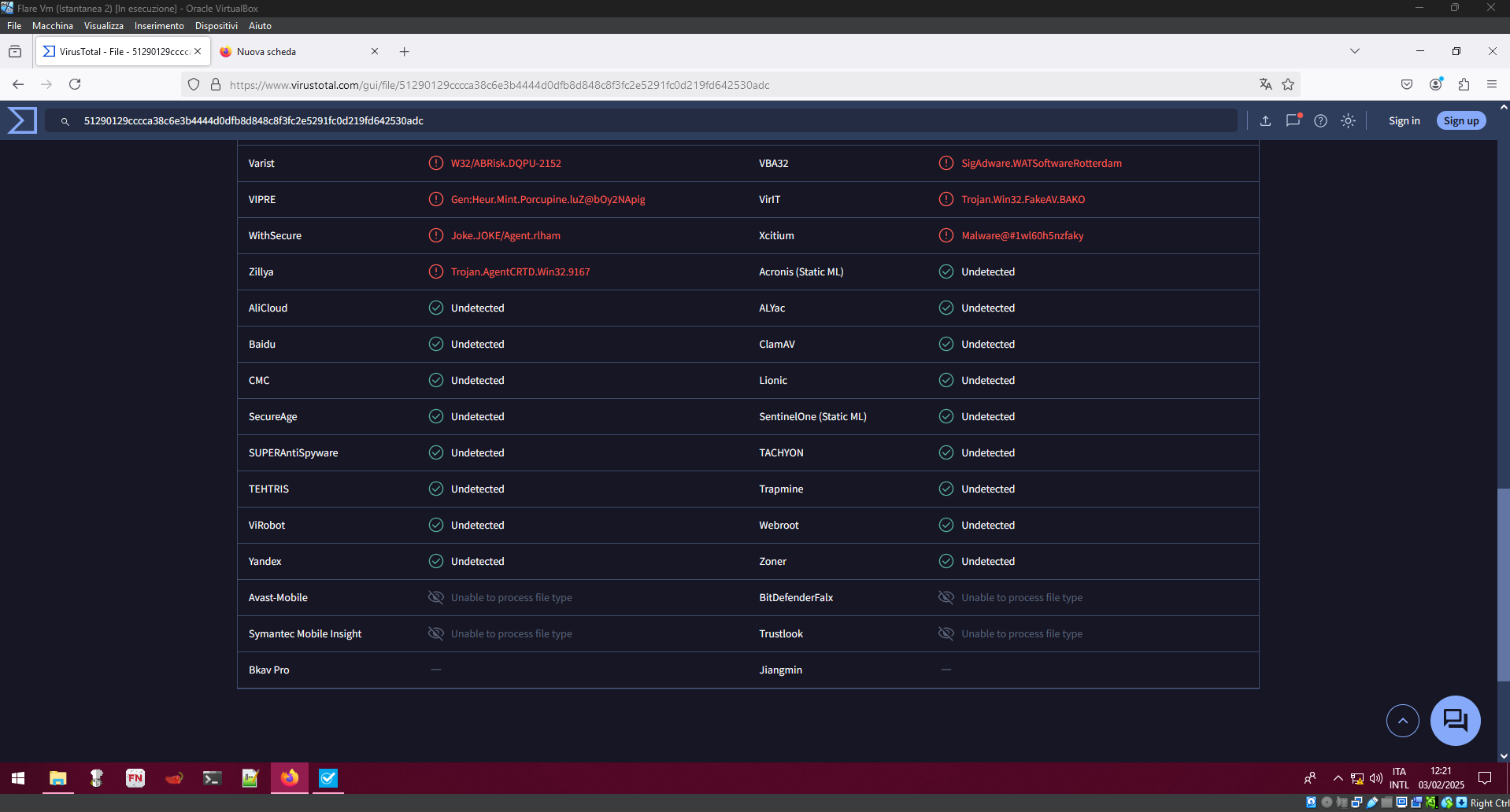
Con il comando strings, è stato possibile estrarre stringhe leggibili dal file. Tra queste, sono stati individuati riferimenti a XML, descrizioni di sistema e alcune stringhe potenzialmente offuscate. Nonostante l’offuscamento, alcune di queste stringhe potrebbero rappresentare URL o comandi utilizzati dal malware.

#### VirusTotal

Infine, il file è stato caricato su VirusTotal, dove 53 motori antivirus su 70 lo hanno classificato come malevolo. L'analisi ha identificato il file come un Dropper o un Trojan, con riferimenti a categorie come FakeAV e Porcupine. Gli indicatori di comportamento, come “execute-dropped-file” e “invalid-signature”, confermano la natura sospetta del file.







Le immagini evidenziano i risultati dell'analisi su VirusTotal, con il tasso di rilevamento e i dettagli comportamentali.

### Conclusioni

L'analisi statica del file ha evidenziato numerosi indicatori di comportamenti malevoli. I dettagli tecnici confermano che il file presenta caratteristiche tipiche di un dropper o trojan, con potenziale capacità di persistenza, modifica del registro e distribuzione di payload nascosti.