

# Esercizio S10L1

## Analisi statica basica

*Samuele Conti*

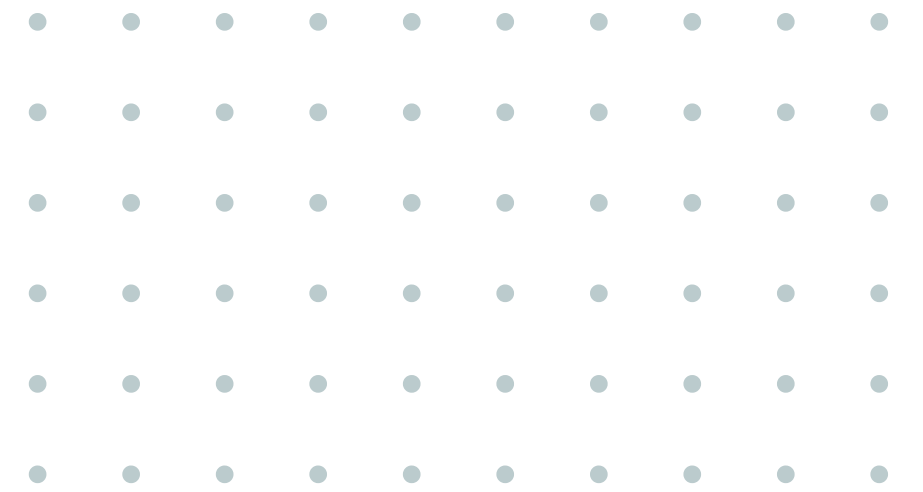


## Task

L'esercizio ci chiede di recuperare info su un Malware tramite l'analisi statica

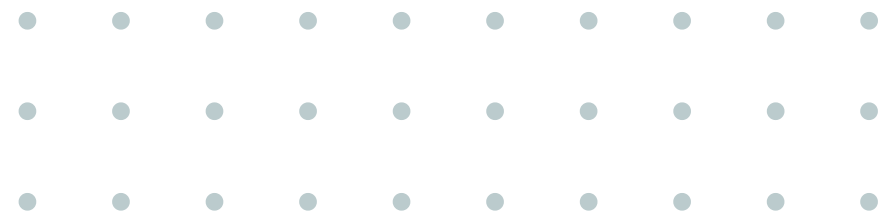
## Side Tasks

- Indicare le librerie importate dal malware
- Indicare le sezioni di cui si compone il malware
- Aggiungere una considerazione finale



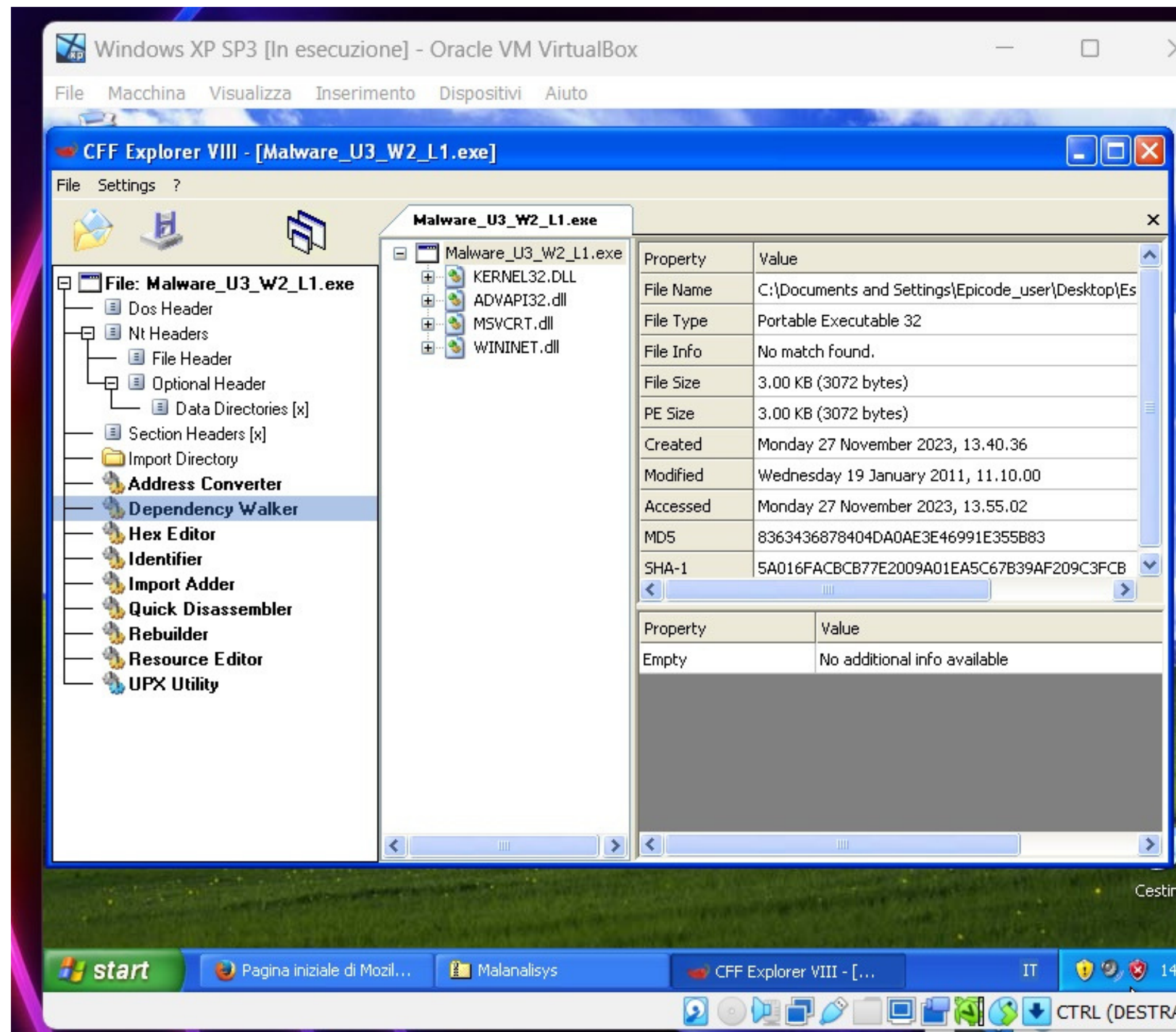
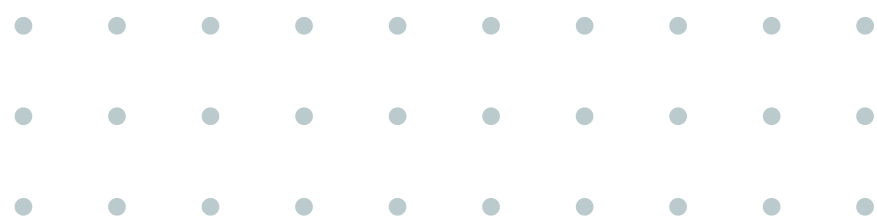
# Analisi statica basica

Lo scopo dell'analisi statica basica è se un dato file è malevolo e fornire informazioni riguardo le sue funzionalità



Caricando il malware datoci dall'esercizio tramite CFF Explorer, vediamo che il malware ha importato le seguenti librerie:

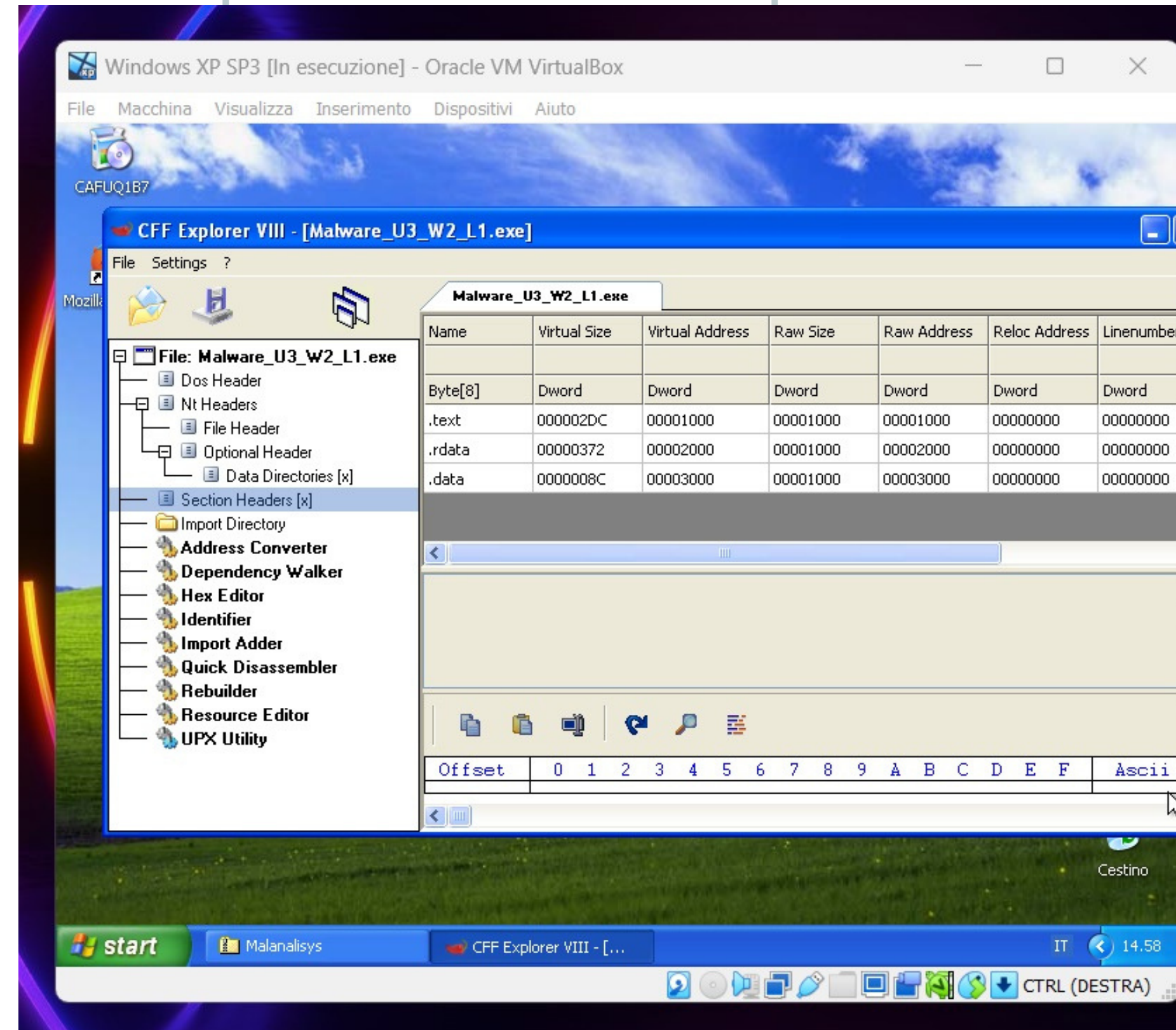
- Kernel32.dll (contiene funzioni principali per interagire con S.O.)
- Advapi32.dll (contiene funzioni principali per interagire con S.O Microsoft)
- MSVCRT.dll (funzioni che manipolano stringhe, allocazione memorie e servizi in/out in stile C)
- Wininet.dll (funzioni che implementano protocolli di rete)





Abbiamo spaccettato il file ed abbiamo potuto vedere le varie sezioni di cui si compone il malware:

- .text ( contengono istruzioni che la CPU eseguirà una volta che il malware sarà avviato)
- .rdata (include info sulle librerie e le funzioni importate ed esportate dall'eseguibile)
- .data (contiene dati/variabili globali del malware, che devono essere disponibili da qualsiasi parte del programma)



Come verifica finale ho controllato il codice hash sul sito VirusTotal il il quale mi ha fornito che probabilmente l'entità di questo malware è un Trojan

57  
/ 72

Community Score

57 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Size  
3.00 KB

Last Analysis Date  
21 hours ago

EXE

Lab01-02.exe

peexe checks-disk-space checks-user-input detect-debug-environment idle long-sleeps upx via-tor

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY30+

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

Popular threat labeltrojan.ulise/startpageThreat categoriestrojan downloaderFamily labelsulise startpage trojanclicker

Security vendors' analysisDo you want to automate checks?

AhnLab-V3	Trojan.Win32.StartPage.C26214	Alibaba	TrojanClicker:Win32/Generic.47e7b5e4
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan/Win32.SGeneric
Arcabit	Trojan.Ser.Ulise.216	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TB/Downloader.Gen

