

# Cyber Security & Ethical Hacking

S10L5

# Introduzione

## Analisi statica basica e dinamica

In questo progetto, è essenziale capire il concetto di analisi statica basica dei Malware. Essa fornisce tecniche e strumenti per analizzare il comportamento di un software malevolo senza la necessità di eseguirlo. Lo scopo di tale analisi è di confermare se un dato file è malevolo e fornire informazioni generiche circa le sue funzionalità. L'analisi statica basica è sicuramente la più intuitiva e semplice da mettere in pratica, ma risulta anche essere la più inefficiente soprattutto contro malware sofisticati. A differenza di quella dinamica a presupporre l'esecuzione del malware in modo tale da osservare il suo comportamento sul sistema infetto al fine di rimuovere l'infezione. I malware devono essere eseguiti in ambiente sicuro e controllato in modo tale da eliminare ogni rischio di arrecare danno a sistemi o all'intera rete.

# Introduzione

## Strumenti

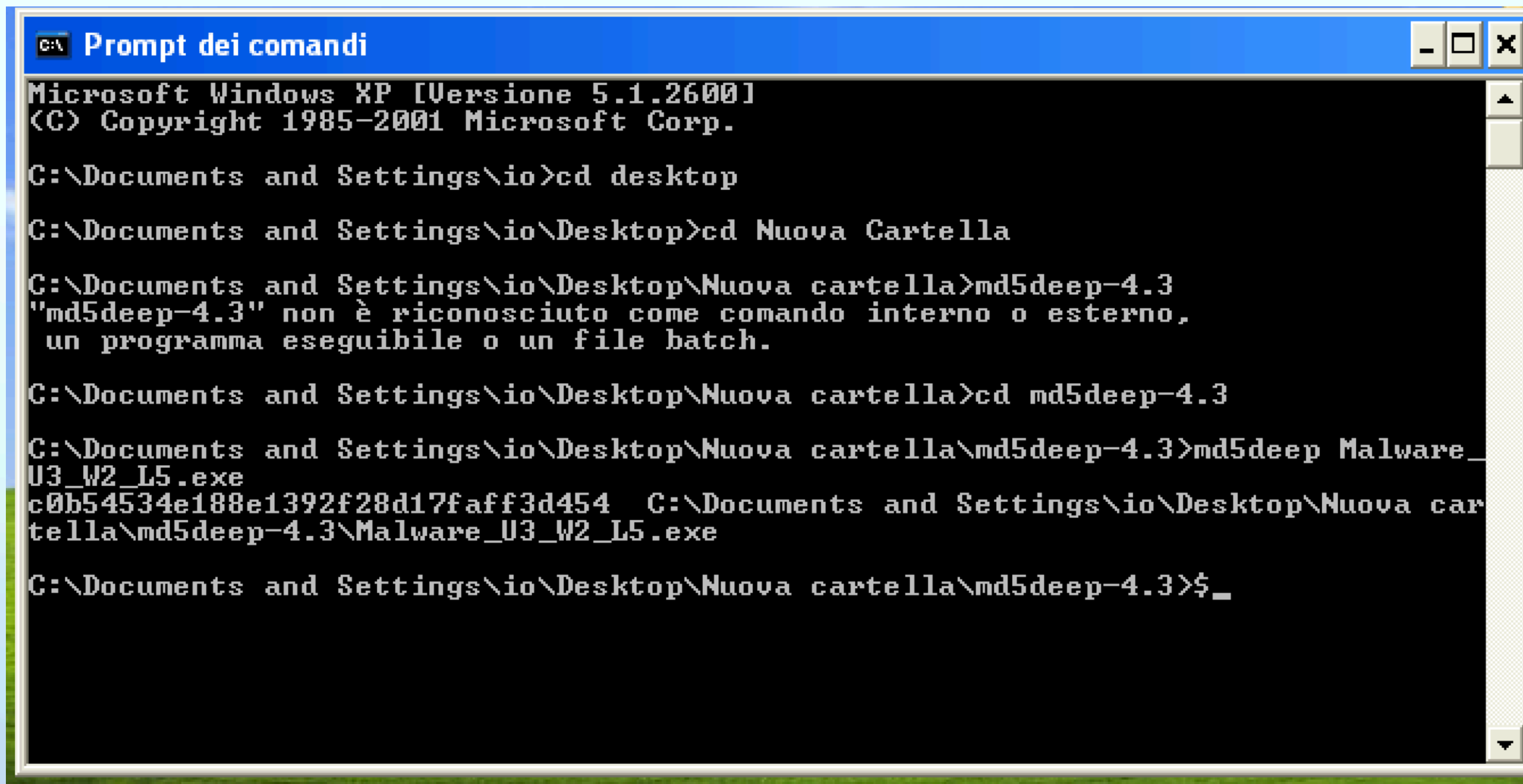
Gli strumenti che utilizziamo per un'analisi statica basica sono:

Virustotal.com: Siti web come questo ci permettono di caricare un file eseguibile e controllare la sua reputazione, tramite la sua firma(hash), in base ad un numero variabile ma consistente di software antivirus.

Per calcolare la firma di un malware si utilizza un tool chiamato "md5deep".

Un altro tool che utilizziamo per un'analisi statica di base, è CFF explorer, che praticamente ci permette di analizzare le librerie su cui agisce il Malware, e le sezioni da cui è composto.

# Creazione hash



```
C:\> Prompt dei comandi
Microsoft Windows XP [Versione 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\io>cd desktop
C:\Documents and Settings\io\Desktop>cd Nuova Cartella
C:\Documents and Settings\io\Desktop\Nuova cartella>md5deep-4.3
"md5deep-4.3" non è riconosciuto come comando interno o esterno,
un programma eseguibile o un file batch.

C:\Documents and Settings\io\Desktop\Nuova cartella>cd md5deep-4.3
C:\Documents and Settings\io\Desktop\Nuova cartella\md5deep-4.3>md5deep Malware_U3_W2_L5.exe
c0b54534e188e1392f28d17faff3d454 C:\Documents and Settings\io\Desktop\Nuova cartella\md5deep-4.3\Malware_U3_W2_L5.exe
C:\Documents and Settings\io\Desktop\Nuova cartella\md5deep-4.3>$_
```

Tramite il tool m5deep, siamo riusciti a calcolare l'hash del file, così da poterlo utilizzare su Virustotal e capire con che tipo di file abbiamo a che fare.

c0b54534e188e1392f28d17faff3d454



# Virus total / CFF

39 / 71

39 security vendors and no sandboxes flagged this file as malicious

b71777edbf21167c96d20ff803cbcb25d24b94b3652db2f286dcd6efd3d8416a

Lab06-02.exe

Size: 40.00 KB | Last Analysis Date: 5 months ago

peexe checks-network-adapters runtime-modules armadillo direct-cpu-clock-access

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 7

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

Popular threat label: trojan.r002c0pdm21 | Threat categories: trojan | Family labels: r002c0pdm21

Security vendors' analysis

| Vendor             | Detection                         | Category            | Severity |
|--------------------|-----------------------------------|---------------------|----------|
| Alibaba            | Trojan:Win32/Generic.be125c32     | Anti-Virus          | High     |
| Avast              | Win32:Trojan-gen                  | Anti-Virus          | High     |
| CrowdStrike Falcon | Win/malicious_confidence_100% (W) | Endpoint Protection | High     |
| Cylance            | Unsafe                            | Endpoint Protection | High     |
| DeepInstinct       | MALICIOUS                         | Endpoint Protection | High     |
| Elastic            | Malicious (high Confidence)       | Endpoint Protection | High     |
| Fortinet           | W32/Agent.WOOltr                  | Anti-Virus          | High     |
| Google             | Detected                          | Endpoint Protection | High     |
| Ikarus             | Trojan.Win32.Agent                | Anti-Virus          | High     |

Vediamo come appare la ricerca del nostro file hash, su virus total. Da qui possiamo dedurre che è un file malevolo, in particolare un trojan.

CFF Explorer VIII - [Malware\_U3\_W2\_L5.exe]

File Settings ?

Malware\_U3\_W2\_L5.exe

| Module Name  | Imports      | OFs      | TimeStamp | ForwarderChain | ... |
|--------------|--------------|----------|-----------|----------------|-----|
| szAnsi       | (nFunctions) | Dword    | Dword     | Dword          | D   |
| KERNEL32.dll | 44           | 00006518 | 00000000  | 00000000       | 00  |
| WININET.dll  | 5            | 000065CC | 00000000  | 00000000       | 00  |

File: Malware\_U3\_W2\_L5.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

In questa fig. vediamo quali sono le libreria che impatta il Malware.

# Librerie importate

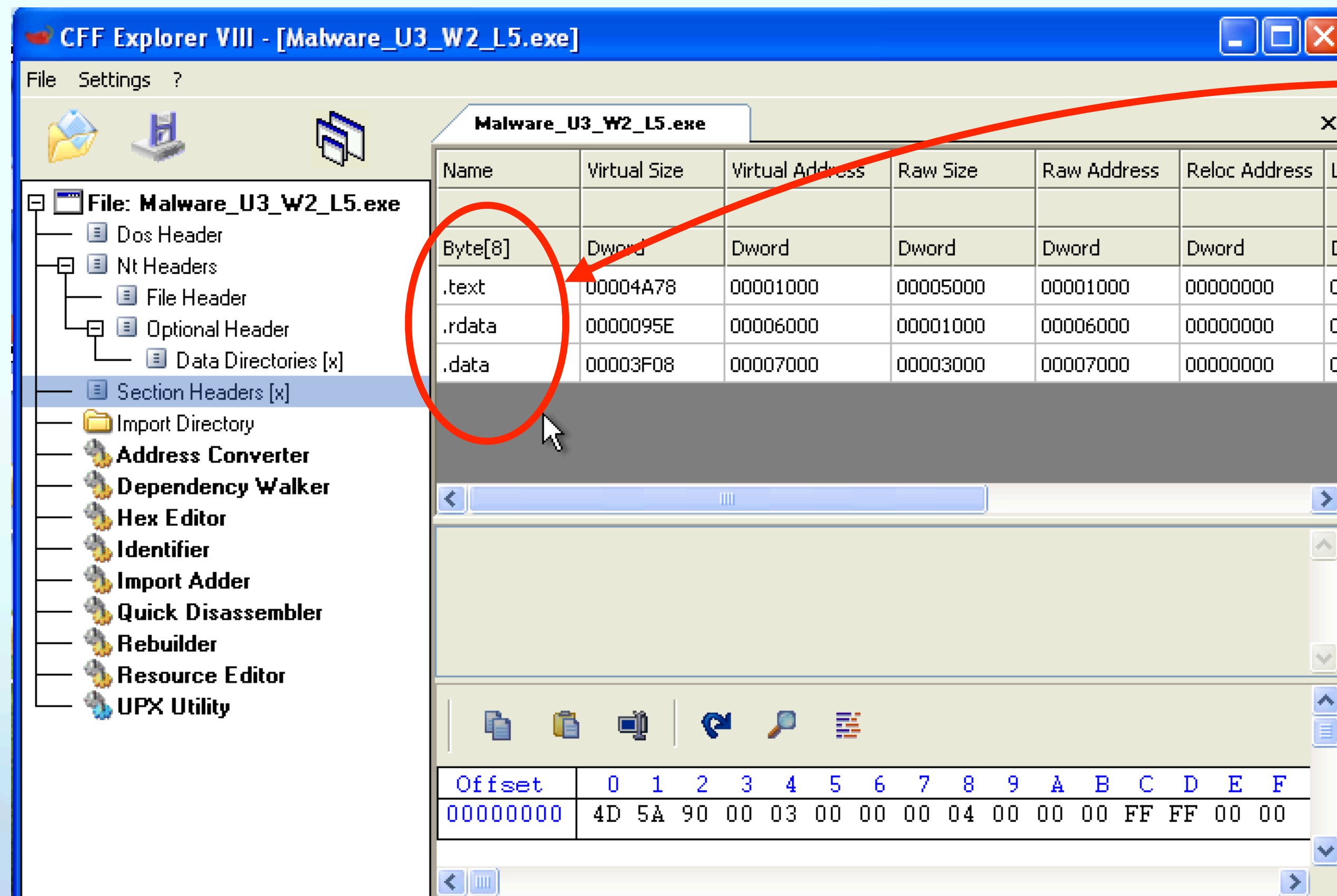
Come abbiamo visto nelle slide precedenti il malware importa 2 librerie:

KERNEL32.dll: contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

| szAnsi       | (nFunctions) | Dword    | Dword    | Dword    |
|--------------|--------------|----------|----------|----------|
| KERNEL32.dll | 44           | 00006518 | 00000000 | 00000000 |
| WININET.dll  | 5            | 000065CC | 00000000 | 00000000 |
|              |              |          |          |          |

# Sezioni



Le sezioni di un malware sono parti specifiche che compongono il codice del software dannoso. Queste sezioni sono progettate per svolgere varie funzioni all'interno del programma dannoso stesso. Le sezioni che analizziamo oggi sono:

**.rdata:** include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.

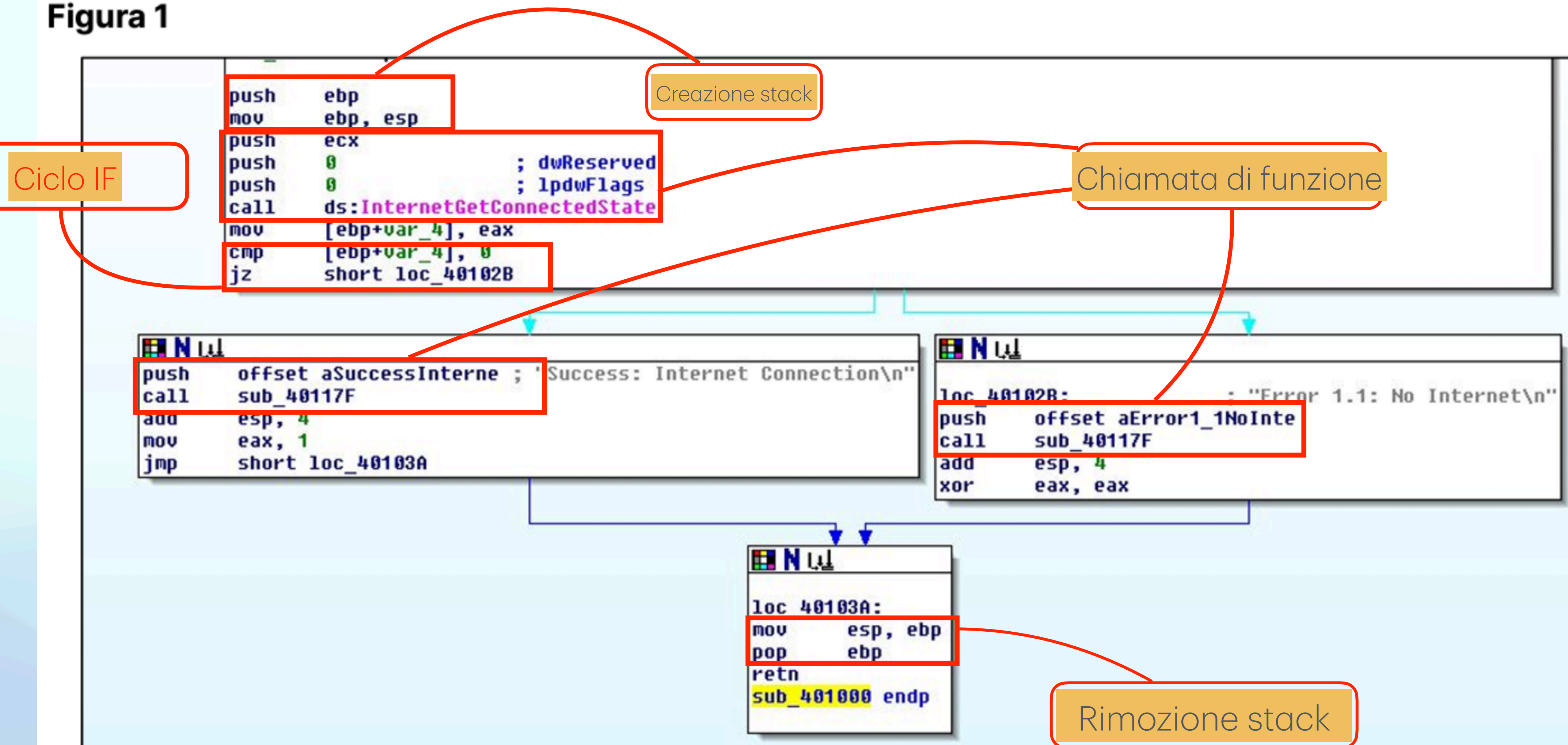
**.text:** contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.

**.data:** contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Una variabile si dice globale quando non è definita all'interno di un contesto di una funzione, ma bensì è globalmente dichiarata ed è di conseguenza accessibile da qualsiasi funzione all'interno dell'eseguibile.



# Identificazione dei costrutti noti

Figura 1





# Analisi dei costrutti noti

Figura 1

```
push    ebp
mov     ebp, esp
push    ecx           ; dwReserved
push    0             ; lpdwFlags
call    ds:InternetGetConnectedState
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jz      short loc_40102B
```

Creazione stack

Chiamata di funzione

Ciclo IF

Nella sezione di codice evidenziato il malware chiama la funzione "internetgetconnectedstate"

Con il ciclo if, c'è la verifica di una condizione, ovvero se c'è o meno una connessione internet attiva. Se il valore di ritorno della funzione è diverso da 0, allora vuol dire c'è una connessione attiva. Viceversa ci darà in output "Error", quindi in mancanza di connessione il malware non è in grado di sfruttare completamente le sue potenzialità.

```
push    offset aSuccessInterne ; "Success: Internet Connection\n"
call    sub_40117F
add     esp, 4
mov     eax, 1
jmp     short loc_40103A
```

```
loc_40102B:
push    offset aError1_1NoInte
call    sub_40117F
add     esp, 4
xor     eax, eax
```

# Ipotesi finali

Se ipotizziamo che questo codice sia parte di un malware, potrebbe essere progettato per controllare lo stato della connessione a Internet sulla macchina bersaglio. In base alla presenza o all'assenza di una connessione Internet, potrebbe eseguire azioni specifiche:

Se la connessione risultasse attiva potrebbe eseguire operazioni legate alla presenza di una connessione, come inviare dati a un server remoto, scaricare aggiornamenti o eseguire altre operazioni di rete, o magari creare una backdoor.

Viceversa se la connessione non risulta attiva potrebbe mostrare un messaggio di errore o eseguire azioni per tentare di ripristinare la connessione, o potrebbe avviare un'altra sequenza di azioni per il funzionamento offline.

Fin.