

# Analisi Malware

ERNESTO ROBLES



# VirusTotal-Md6deep

```
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep ..\Esercizio
_Pratico_U3_W2_L5\Malware_U3_W2_L5.exe
c0b54534e188e1392f28d17faff3d454 C:\Documents and Settings\Administrator\Desktop
\Esercizio_Pratico_U3_W2_L5\Malware_U3_W2_L5.exe
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>cd ..
```

Il primo passo nell'analisi di un potenziale malware è assicurarsi che di fatto lo sia. Per farlo si calcola l'hash del file, si può utilizzare l'utility md5deep, con l'hash che identifica il file effettuiamo una ricerca su VirusTotal controllerà nei database dei software antivirus e la sua eventuale categorizzazione come malware come in questo caso, abbiamo informazioni come la categoria del virus in quanto Trojan.

39

/ 71

✓

Community Score

39 security vendors and no sandboxes flagged this file as malicious

b71777edbf21167c96d20ff803cbcb25d24b94b3652db2f286dcd6efd3d8416a

Lab06-02.exe

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

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

Security vendors' analysis

Alibaba	Trojan:Win32/Generic.be125c32	Antiy-AVL
Avast	Win32:Trojan-gen	AVG
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason

**VirusTotal inoltre ci fornisce informazioni quali le librerie vengono importate dal file eseguibile e le sezioni che compongono il file eseguibile del malware come è possibile vedere qui nell'immagine affianco.**

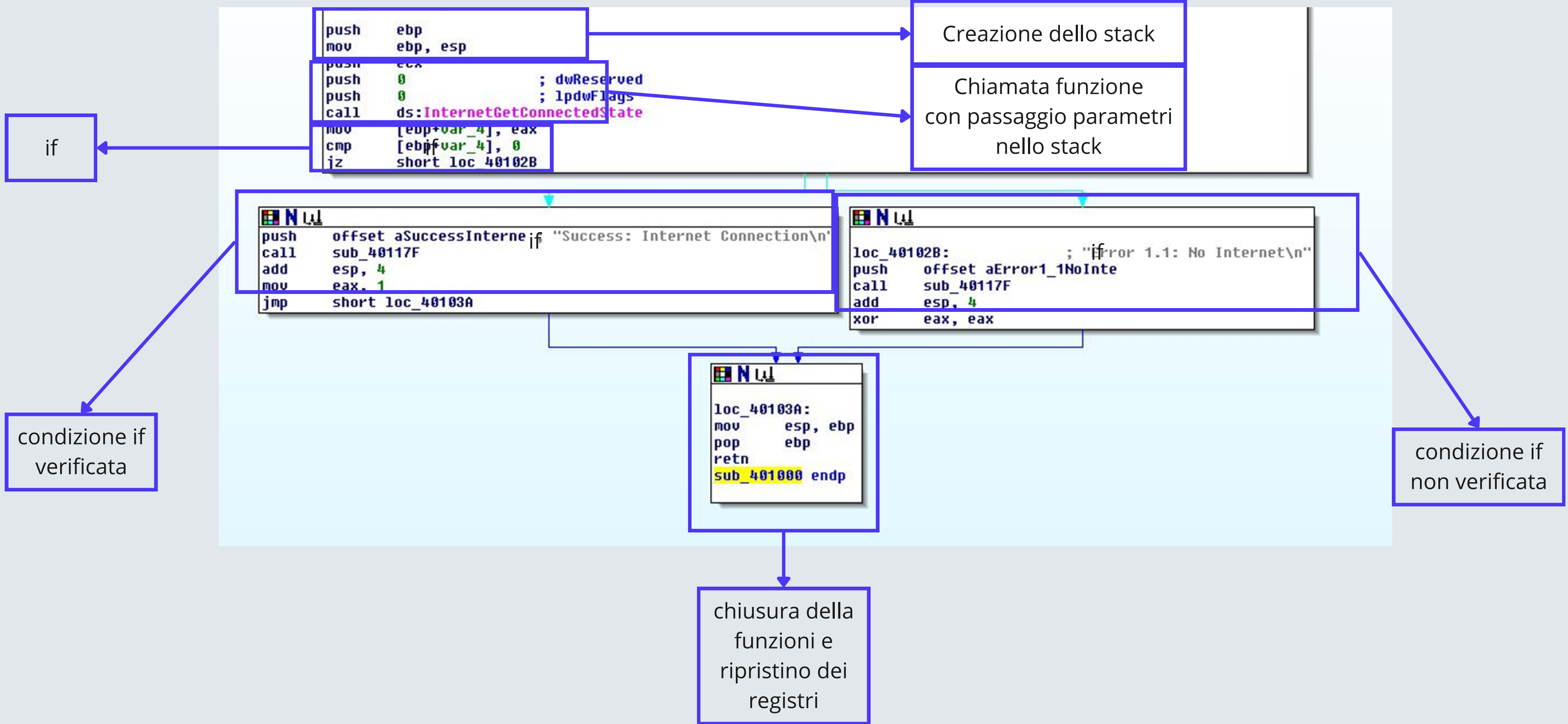
[illegible]

Per un ulteriore controllo delle funzioni importate ed esportate dal malware, possiamo anche utilizzare il toolCFF Explorer, dove vengono confermate le informazioni prima viste su VirusTotal, fra cui librerie come “Kernel32.dll” che contiene le funzioni principali per interagire con il sistema operativo e sezioni come “.rdata” che include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall’eseguibile.

Malware_U3_W2_L5.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000065EC	N/A	000064DC	000064E0	000064E4	000064E8	000064EC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

# Assembly X86





Lo scopo del codice Assembly è la gestione di uno scenario in cui la funzione InternetGetConnectedState attraverso l'uso del costrutto "if" che restituisce un valore diverso da zero "connessione internet riuscita" e in tal caso il programma stampa il messaggio "Success: Internet Connection\n" altrimenti con un valore uguale a zero "connessione internet non riuscita" stampa "Error 1.1: No Internet\n".

Analisi del codice:

```
//.text:00401000  push  ebp      Salva il valore corrente di ebp nello stack
//.text:00401001  mov  ebp, esp  Inizializza il registro ebp con il valore corrente di esp
//.text:00401003  push  ecx      Salva il valore corrente di ecx nello stack
```

```
//.text:00401004  push  0        ; dwReserved
//.text:00401006  push  0        ; lpdwFlags
//.text:00401008  call  ds:InternetGetConnectedState Chiamata a funzione esterna
//.text:0040100E  mov  [ebp+var_4], eax Salva il risultato della funzione nello stack
```

```
//.text:00401011  cmp  [ebp+var_4], 0 Confronta il risultato con 0
//.text:00401015  jz   short loc_40102B Salta a loc_40102B se il risultato è zero
```

```
push offset aSuccessInterne "Success: Internet Connection\n"
call sub_40117F Chiamata a una subroutine per stampare il messaggio
add esp, 4      Pulizia dello stack
mov  eax, 1     Imposta eax a 1 (indicazione di successo)
jmp  short loc_40103A Salto a loc_40103A
```

```
push offset aError1_NoInte "Error 1.1: No Internet\n"
call sub_40117F    Chiamata a una subroutine per stampare il messaggio
add esp, 4        Pulizia dello stack
xor eax, eax      Imposta eax a 0 (indicazione di errore)

mov esp, ebp      Ripristina esp al valore iniziale
pop ebp          Ripristina ebp dallo stack
retn             Ritorna dalla funzione
endp
```