Analisi Malware

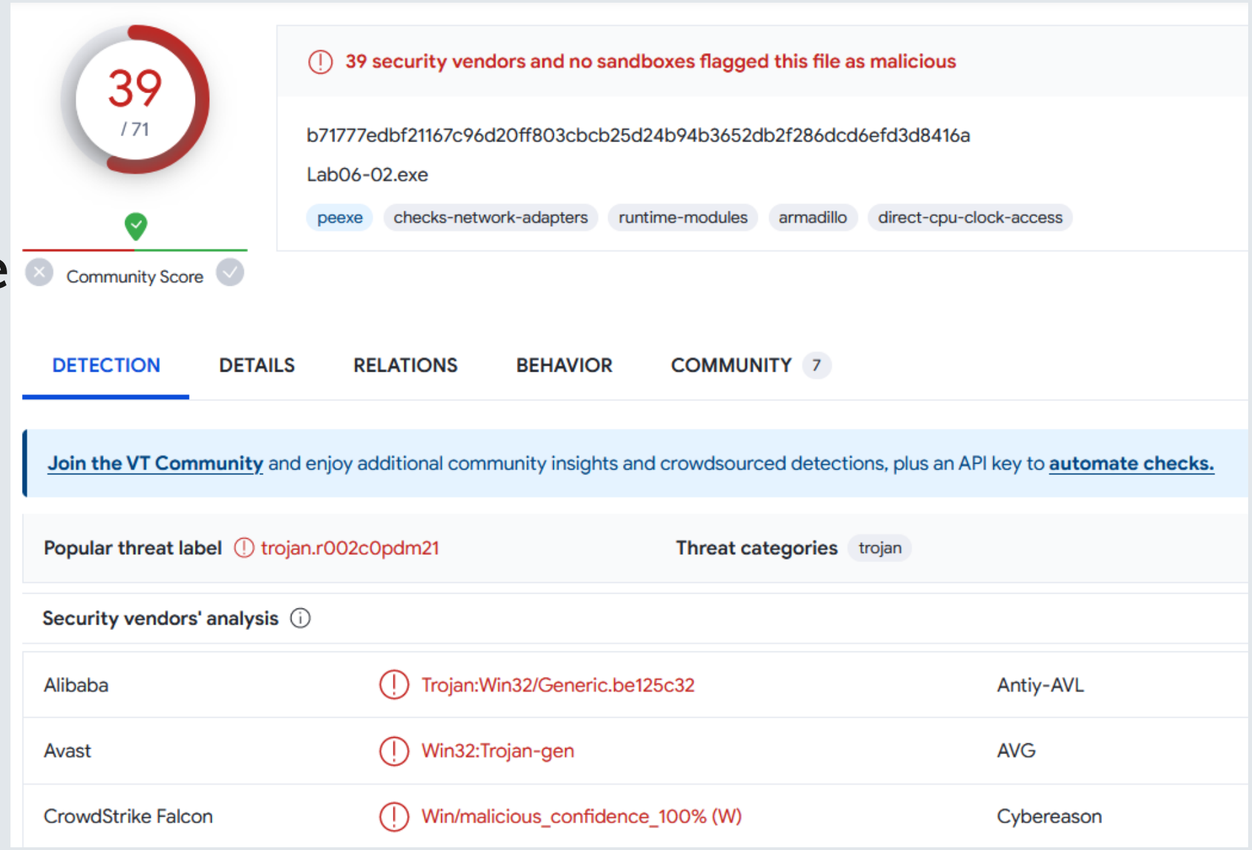
ERNESTO ROBLES

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\Deskto
p\Esercizio_Pratico_U3_W2_L5\Malware_U3_W2_L5.exe

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>cd ..
```

Il prima 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.



VirusTotal inoltre ci fornice 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.

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	19064	20480	6.37	4b8aaeb128744c00b1f9b29dd120616e	196535.5
.rdata	24576	2398	4096	3.66	e5e39acc53e64c50fa5a35693a911478	304856
.data	28672	16136	12288	0.7	305514f6ece00473b7ff8bc023f57e15	2765274

Imports

— KERNEL32.dll

- CloseHandle
- ExitProcess
- FlushFileBuffers
- FreeEnvironmentStringsA
- FreeEnvironmentStringsW
- GetACP
- GetCommandLineA
- GetCPInfo
- GetCurrentProcess
- GetEnvironmentStrings

— WININET.dll

- InternetCloseHandle
- InternetGetConnectedState
- InternetOpenA
- InternetOpenUrlA
- InternetReadFile

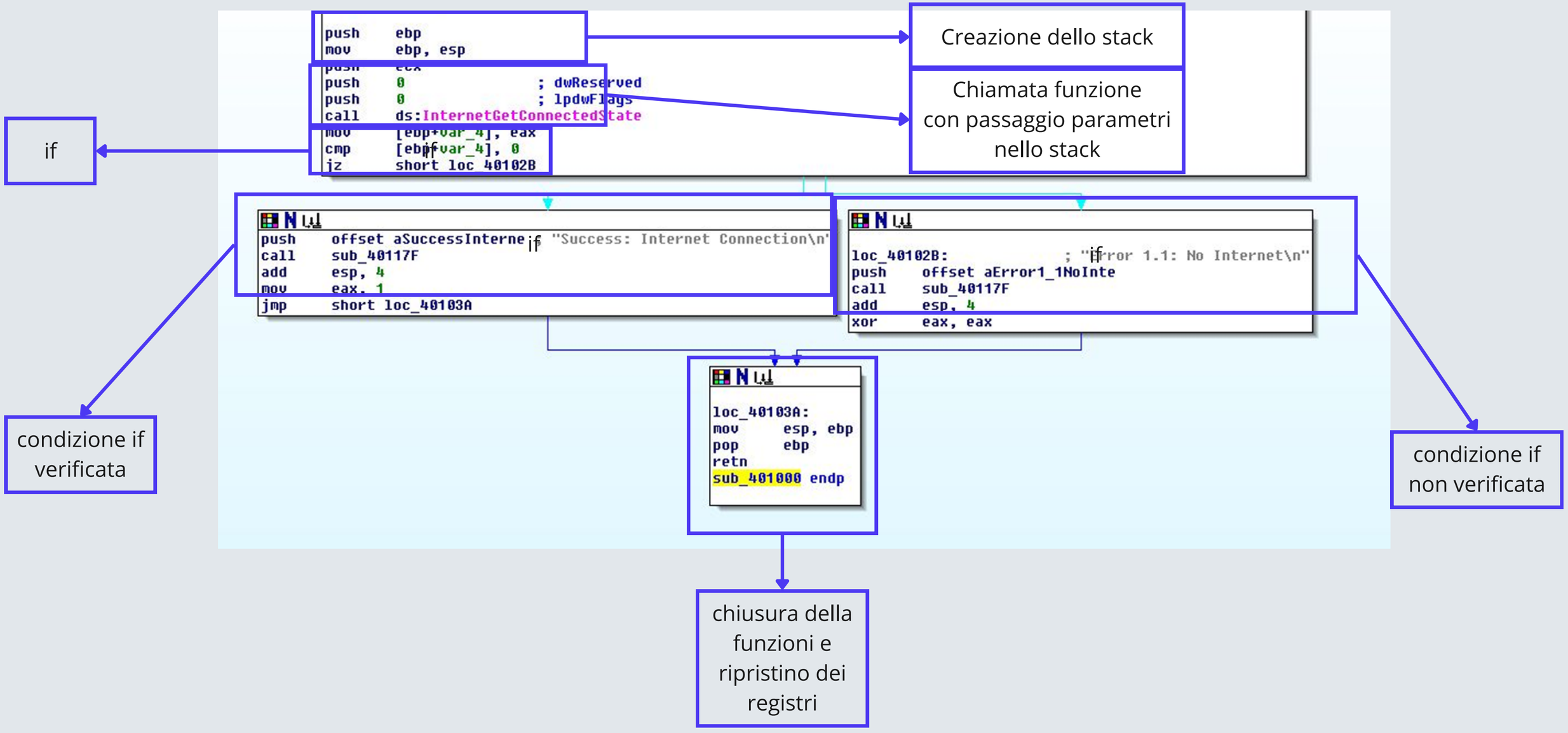
Per un ulteriore controllo delle funzioni importate ed esportate dal malware, possiamo anche utilizzare il toolCFF Explorer, dove vengono confermate le informazioni prima viste su VirusTotal, fra cui librerie come “Kernel32.dll” che contiene le funzioni principali per interagire con il sistema operativo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



Ilcodice assembly raffigurato controlla lo stato della connessione internet stampando un messaggio di successo se la connessione è attiva e un messaggio di errore se disattiva.

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
```