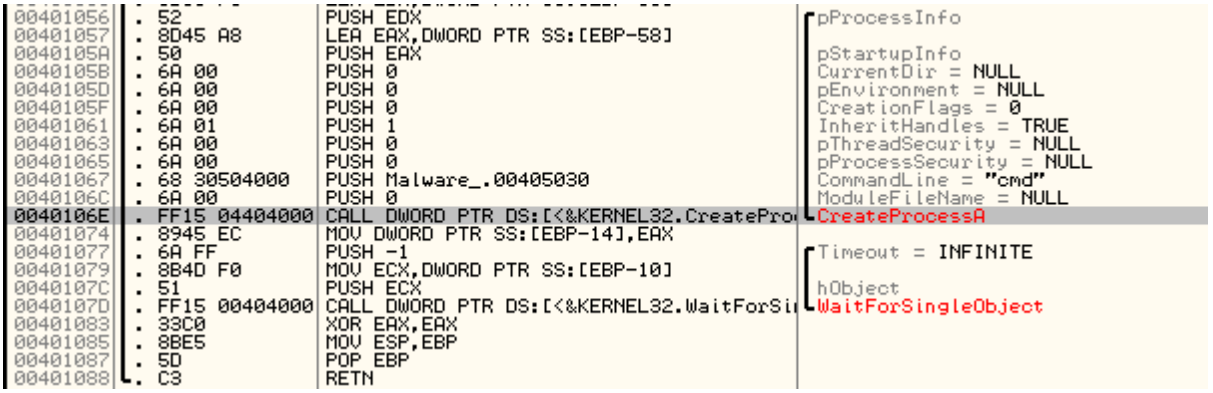
# OllyDBG

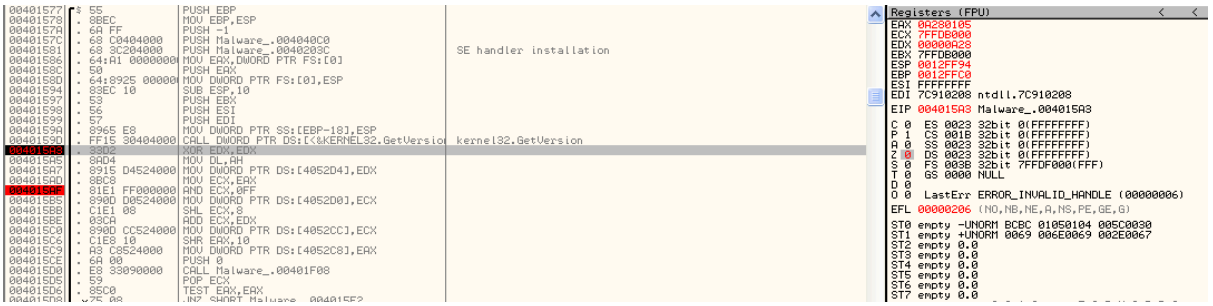
**Traccia:** Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3 sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.
• All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)
• Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)
• Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).

1)

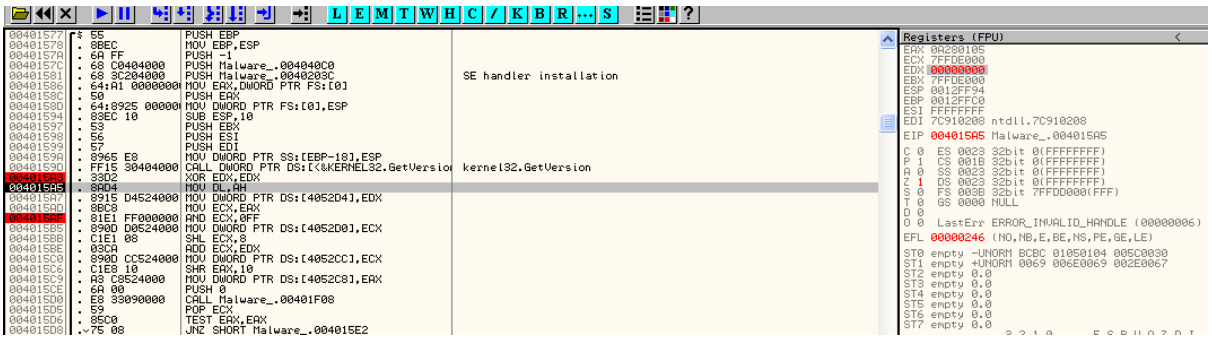



Come possiamo vedere dalla figura il parametro "ComandLine" è "cmd" il che potrebbe indicare l'avvio di una finestra del terminale all'avvio del malware.

2)




Possiamo vedere che EDX ha valore 0000A28, ma dopo aver eseguito il malware e fatto lo step-into possiamo vedere come il valore passa a 000000.

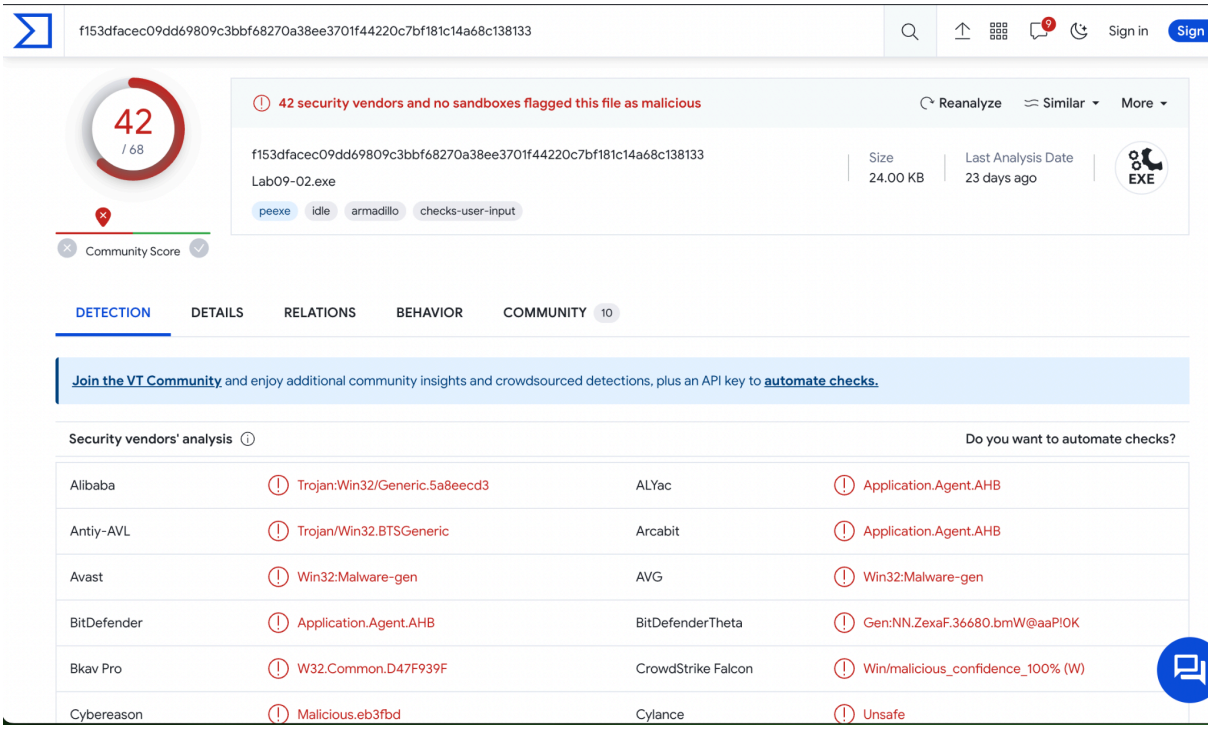


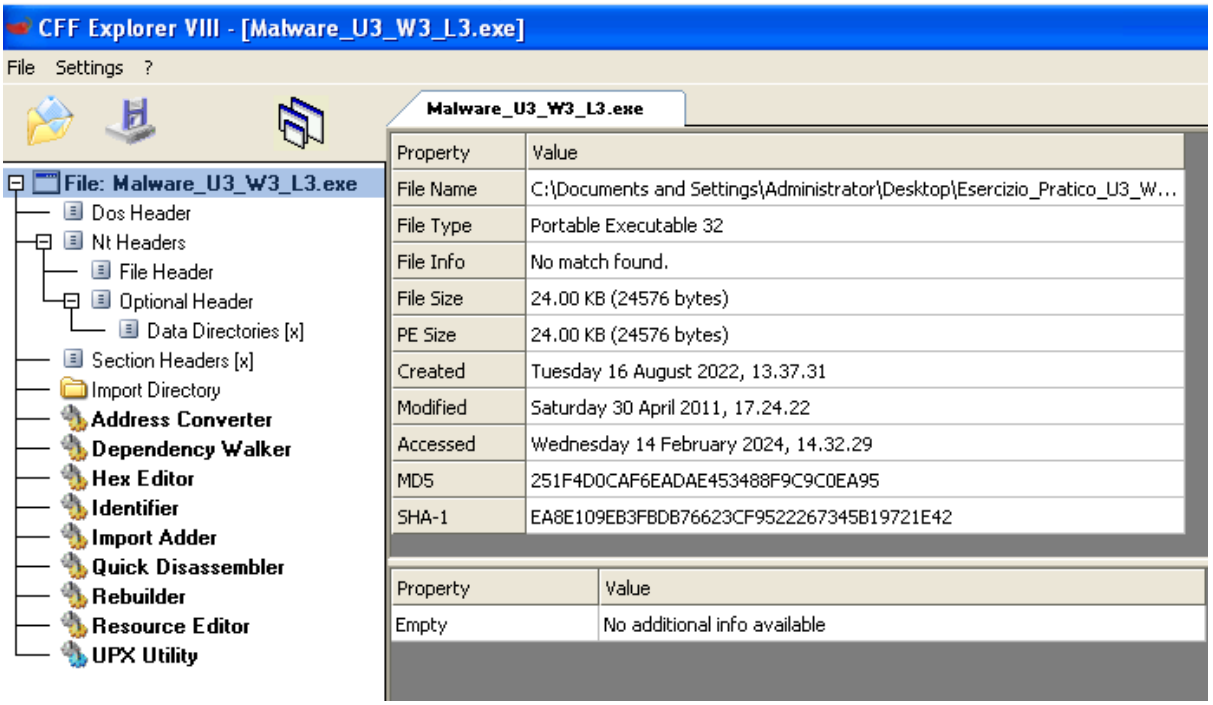
Questo vuol dire che l'operazione XOR è stata eseguita correttamente, ed il malware a modificato il valore del registro.

4)

il valore del registro ECX è 0A280105.
Il valore cambia in quando viene compiuta l'operazione AND con 0FF ( ricordiamo che 0FF in esadecimale equivale a 255). Quindi vengono messi a confronto il registro EAX con il valore 255, bit per bit. Se i bit corrispondono allora il valore è uno se no 0.

**Bonus:**
Dopo essere andato a recuperare MD5 Hash del malware da CFF Explore, ed averlo caricato su Virus Total è risultato evidente che fosse un Trojan.


f153dfacec09dd69809c3bbf68270a38ee3701f44220c7bf181c14a68c138133
Sign in
Sign
42
/ 68
Community Score
42 security vendors and no sandboxes flagged this file as malicious
Reanalyze
Similar
More
f153dfacec09dd69809c3bbf68270a38ee3701f44220c7bf181c14a68c138133
Lab09-02.exe
peexe
idle
armadillo
checks-user-input
Size
24.00 KB
Last Analysis Date
23 days ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 10
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Alibaba
Trojan:Win32/Generic.5a8eecd3
ALYac
Application.Agent.AHB
Antiy-AVL
Trojan/Win32.BTSGeneric
Arcabit
Application.Agent.AHB
Avast
Win32:Malware-gen
AVG
Win32:Malware-gen
BitDefender
Application.Agent.AHB
BitDefenderTheta
Gen:NN.ZexaF.36680.bmW@aaP!0K
Bkav Pro
W32.Common.D47F939F
CrowdStrike Falcon
Win/malicious_confidence_100% (W)
Cybereason
Malicious.eb3fbd
Cylance
Unsafe


CFF Explorer VIII - [Malware_U3_W3_L3.exe]
File
Settings
?
File: Malware_U3_W3_L3.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
Malware_U3_W3_L3.exe
Property
Value
File Name
C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W...
File Type
Portable Executable 32
File Info
No match found.
File Size
24.00 KB (24576 bytes)
PE Size
24.00 KB (24576 bytes)
Created
Tuesday 16 August 2022, 13.37.31
Modified
Saturday 30 April 2011, 17.24.22
Accessed
Wednesday 14 February 2024, 14.32.29
MD5
251F4D0CAF6EADAE453488F9C9C0EA95
SHA-1
EA8E109EB3FBDB76623CF9522267345B19721E42
Property
Value
Empty
No additional info available