

MALWARE ANALYSIS

S11/L3

TABLE OF CONTENT

03. INTRODUCTION

04. PROCEDURE

INTRODUCTION

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).
- BONUS: spiegare a grandi linee il funzionamento del malware

PROCEDURE

1.Task:

| | | | |
|----------|-----------------|---|-------------------------|
| 00401056 | . 52 | PUSH EDX | pProcessInfo |
| 00401057 | . 8D45 A8 | LEA EAX,DWORD PTR SS:[EBP-58] | pStartupInfo |
| 0040105A | . 50 | PUSH EAX | CurrentDir = NULL |
| 0040105B | . 6A 00 | PUSH 0 | pEnvironment = NULL |
| 0040105D | . 6A 00 | PUSH 0 | CreationFlags = 0 |
| 0040105F | . 6A 00 | PUSH 0 | InheritHandles = TRUE |
| 00401061 | . 6A 01 | PUSH 1 | pThreadSecurity = NULL |
| 00401063 | . 6A 00 | PUSH 0 | pProcessSecurity = NULL |
| 00401065 | . 6A 00 | PUSH 0 | CommandLine = "cmd" |
| 00401067 | . 68 30504000 | PUSH Malware_.00405030 | ModuleFileName = NULL |
| 0040106C | . 6A 00 | PUSH 0 | |
| 0040106E | . FF15 04404000 | CALL DWORD PTR DS:[<&KERNEL32.CreatePro | CreateProcessA |
| 00401071 | . 8B45 EC | MOV DWORD PTR EBX,DWORD PTR SS:[EBP-14] | |

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. Task

| | | | |
|----------|------------------|--|---------------------|
| 0040158D | . 64:8925 000000 | MOV DWORD PTR FS:[0],ESP | |
| 00401594 | . 83EC 10 | SUB ESP,10 | |
| 00401597 | . 53 | PUSH EBX | |
| 00401598 | . 56 | PUSH ESI | |
| 00401599 | . 57 | PUSH EDI | |
| 0040159A | . 8965 E8 | MOV DWORD PTR SS:[EBP-18],ESP | |
| 0040159D | . FF15 30404000 | CALL DWORD PTR DS:[<&KERNEL32.GetVersion | kernel32.GetVersion |
| 004015A3 | . 33D2 | XOR EDX,EDX | |
| 004015A5 | . 8AD4 | MOV DL,AH | |
| 004015A7 | . 8915 D4524000 | MOV DWORD PTR DS:[4052D4],EDX | |
| 004015AD | . 8BC8 | MOV ECX,EAX | |
| 004015AF | . 81E1 FF000000 | AND ECX,0FF | |
| 004015B5 | . 89D0 D0524000 | MOV DWORD PTR DS:[4052D0],ECX | |
| 004015B8 | . C1E1 08 | SHL ECX,8 | |
| 004015BE | . 03CA | ADD ECX,EDX | |
| 004015C0 | . 89D0 CC524000 | MOV DWORD PTR DS:[4052CC],ECX | |
| 004015C6 | . C1E8 10 | SHR EAX,10 | |
| 004015C9 | . A3 C8524000 | MOV DWORD PTR DS:[4052C8],EAX | |
| 004015CE | . 6A 00 | PUSH 0 | |
| 004015D0 | . E8 33090000 | CALL Malware_.00401F08 | |
| 004015D5 | . 59 | POP ECX | |

Registers (FPU)
EAX 10B10106
ECX 7EFDE000
EDX 00001DB1
EBX 7EFDE000
ESP 0018FF5C
EBP 0018FF88
ESI 00000000
EDI 00000000
EIP 004015A3 Malware_.004015A3
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
O 0
O 0 LastErr ERROR_SUCCESS (0000)
EFL 00000206 (NO,NB,NE,A,NS,PE,G

Possiamo vedere che EDX ha valore 00001DB1 ma dopo aver eseguito il malware e fatto lo step-into possiamo vedere come il valore passa a 000000.

| | | | |
|----------|------------------|--|---------------------|
| 0040158D | . 64:8925 000000 | MOV DWORD PTR FS:[0],ESP | |
| 00401594 | . 83EC 10 | SUB ESP,10 | |
| 00401597 | . 53 | PUSH EBX | |
| 00401598 | . 56 | PUSH ESI | |
| 00401599 | . 57 | PUSH EDI | |
| 0040159A | . 8965 E8 | MOV DWORD PTR SS:[EBP-18],ESP | |
| 0040159D | . FF15 30404000 | CALL DWORD PTR DS:[<&KERNEL32.GetVersion | kernel32.GetVersion |
| 004015A3 | . 33D2 | XOR EDX,EDX | |
| 004015A5 | . 8AD4 | MOV DL,AH | |
| 004015A7 | . 8915 D4524000 | MOV DWORD PTR DS:[4052D4],EDX | |

Registers (FPU)
EAX 10B10106
ECX 7EFDE000
EDX 00000000
EBX 7EFDE000
ESP 0018FF5C
EBP 0018FF88
ESI 00000000
EDI 00000000

PROCEDURE

3. Task

Dopo aver impostato un secondo breakpoint all'indirizzo 004015AF e aver eseguito il programma, il valore del registro ECX è risultato essere **1DB10106**.

Successivamente, eseguendo un'istruzione step-into, il valore di ECX è cambiato in **00000006**.

L'istruzione eseguita è stata un'operazione AND bit a bit tra il valore corrente di ECX e 0FF. Questa operazione AND ha permesso di mantenere soltanto gli 8 bit meno significativi di ECX, producendo così il nuovo valore del registro.

| Address | Disassembly | Registers (FPU) |
|----------|---|-----------------|
| 004015AF | 81E1 FF000000 AND ECX,0FF | EAX 1DB10106 |
| 004015B5 | 8900 D0524000 MOV DWORD PTR DS:[4052D0],ECX | ECX 1DB10106 |
| 004015B8 | C1E1 08 SHL ECX,8 | EDX 00000001 |
| 004015BE | 03CA ADD ECX,EDX | EBX 7EFDE000 |
| 004015C0 | 8900 CC524000 MOV DWORD PTR DS:[4052CC],ECX | ESP 0018FF5C |
| 004015C2 | 81E1 00000000 AND ECX,0 | EBP 0018FF88 |
| 004015C4 | 8900 00000000 MOV DWORD PTR DS:[4052D0],ECX | ESI 00000000 |
| 004015C6 | 81E1 00000000 AND ECX,0 | EDI 00000000 |

| Registers (FPU) | |
|-----------------|----------|
| EAX | 1DB10106 |
| ECX | 00000006 |
| EDX | 00000001 |
| EBX | 7EFDE000 |
| ESP | 0018FF5C |
| EBP | 0018FF88 |
| ESI | 00000000 |
| EDI | 00000000 |

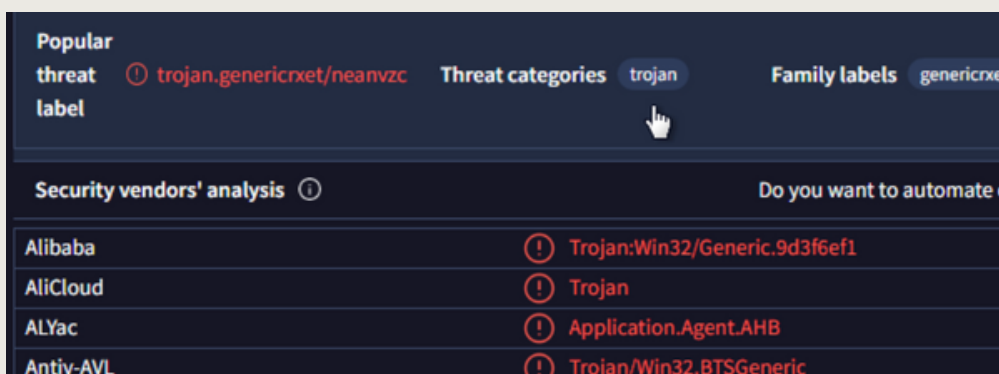
4. Task

Analizzando il flusso del programma, si osserva che il malware impiega diverse tecniche avanzate, come la creazione di processi tramite **CreateProcess**, l'instaurazione di connessioni di rete (tramite la creazione di socket) e la manipolazione dell'interfaccia utente.

Questi elementi indicano che il malware è multifunzionale e probabilmente progettato per svolgere una serie di attività dannose, come comunicare con un server remoto o alterare l'interfaccia utente per ingannare l'utente.

Inoltre, il malware sembra essere stato sviluppato per evitare il rilevamento da parte dei software antivirus, utilizzando tecniche come l'offuscamento, la crittografia o misure anti-analisi.

Confrontando l'hash del malware con i database di VirusTotal, è stato identificato come un **Trojan**, una tipologia di malware in grado di consentire l'accesso remoto non autorizzato al sistema compromesso.



The screenshot shows the VirusTotal interface for a specific threat. At the top, the threat is identified as 'trojan.genericxet/neanvzc' with a 'trojan' category label. Below this, a table titled 'Security vendors' analysis' lists detections from various vendors. Each entry includes a red warning icon, the vendor name, and the specific malware name detected.

| Popular threat label | | | Threat categories | trojan | Family labels | genericxet |
|----------------------------|---|-------------------------------|-------------------------|--------|---------------|------------|
| Security vendors' analysis | | | Do you want to automate | | | |
| Alibaba | ! | Trojan:Win32/Generic.9d3f6ef1 | | | | |
| AliCloud | ! | Trojan | | | | |
| ALYac | ! | Application.Agent.AHB | | | | |
| Antiy-AVL | ! | Trojan/Win32.BTSGeneric | | | | |