CS0424IT — ESERCITAZIONE S11L3
ANALISI MALWARE OLLYDBG

Simone La Porta

GitHub

---

21 agosto 2024

INDICE

1 TRACCIA

Fate riferimento al malware `Malware_U3_W3_L3`, presente nella cartella `Esercizio_Pratico_U3_W3_L3` sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando `OllyDBG`:

1. 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?

2. Inserite un breakpoint software all'indirizzo `004015A3`. Qual è il valore del registro `EDX`? Eseguite uno *step-into*. Indicate qual è ora il valore del registro `EDX`, motivando la risposta. Che istruzione è stata eseguita?

3. Inserite un secondo breakpoint all'indirizzo di memoria `004015AF`. Qual è il valore del registro `ECX`? Eseguite uno *step-into*. Qual è ora il valore di `ECX`? Spiegate quale istruzione è stata eseguita.

4. **Bonus:** Spiegare a grandi linee il funzionamento del malware.

2 SVOLGIMENTO

2.1 *Funzione CreateProcess*

All'indirizzo 0040106E, il malware effettua una chiamata di funzione alla funzione `CreateProcess`. Analizzando il parametro `CommandLine` passato alla funzione, visibile nella quarta colonna della finestra di `OllyDbg`, si può osservare che il valore è `cmd`, indicando che il malware tenta di avviare una nuova shell di comando.

```
0040103B | . 66:C745 D8 0000     | MOV WORD PTR SS:[EBP-28],0
00401041 | . 8B55 18             | MOV EDX,DWORD PTR SS:[EBP+18]
00401044 | . 8955 E0             | MOV DWORD PTR SS:[EBP-20],EDX
00401047 | . 8B45 E0             | MOV EAX,DWORD PTR SS:[EBP-20]
0040104A | . 8945 E8             | MOV DWORD PTR SS:[EBP-18],EAX
0040104D | . 8B4D E8             | MOV ECX,DWORD PTR SS:[EBP-18]
00401050 | . 894D E4             | MOV DWORD PTR SS:[EBP-1C],ECX
00401053 | . 8D55 F0             | LEA EDX,DWORD PTR SS:[EBP-10]
00401056 | . 52                  | PUSH EDX                                 | pProcessInfo
00401057 | . 8D45 A8             | LEA EAX,DWORD PTR SS:[EBP-58]            |
0040105A | . 50                  | PUSH EAX                                 | pStartupInfo
0040105B | . 6A 00               | PUSH 0                                   | CurrentDir = NULL
0040105D | . 6A 00               | PUSH 0                                   | pEnvironment = NULL
0040105F | . 6A 00               | PUSH 0                                   | CreationFlags = 0
00401061 | . 6A 01               | PUSH 1                                   | InheritHandles = TRUE
00401063 | . 6A 00               | PUSH 0                                   | pThreadSecurity = NULL
00401065 | . 6A 00               | PUSH 0                                   | pProcessSecurity = NULL
00401067 | . 68 30504000         | PUSH Malware_.00405030                   | CommandLine = "cmd"
0040106C | . 6A 00               | PUSH 0                                   | ModuleFileName = NULL
0040106E | . FF15 04404000       | CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA>] | CreateProcessA
00401074 | . 8945 EC             | MOV DWORD PTR SS:[EBP-14],EAX            |
00401077 | . 6A FF               | PUSH -1                                  | Timeout = INFINITE
00401079 | . 8B4D F0             | MOV ECX,DWORD PTR SS:[EBP-10]            |
0040107C | . 51                  | PUSH ECX                                 | hObject
0040107D | . FF15 00404000       | CALL DWORD PTR DS:[<&KERNEL32.WaitForSingleObject> | WaitForSingleObject
00401083 | . 33C0                | XOR EAX,EAX                              |
00401085 | . 8BE5                | MOV ESP,EBP                              |
```

2.2 *Registro EDX*

2.2.1 Valore del Registro EDX

Dopo aver inserito un breakpoint software all'indirizzo 004015A3 ed eseguito il programma, il valore del registro `EDX` trovato è 00001DB1.

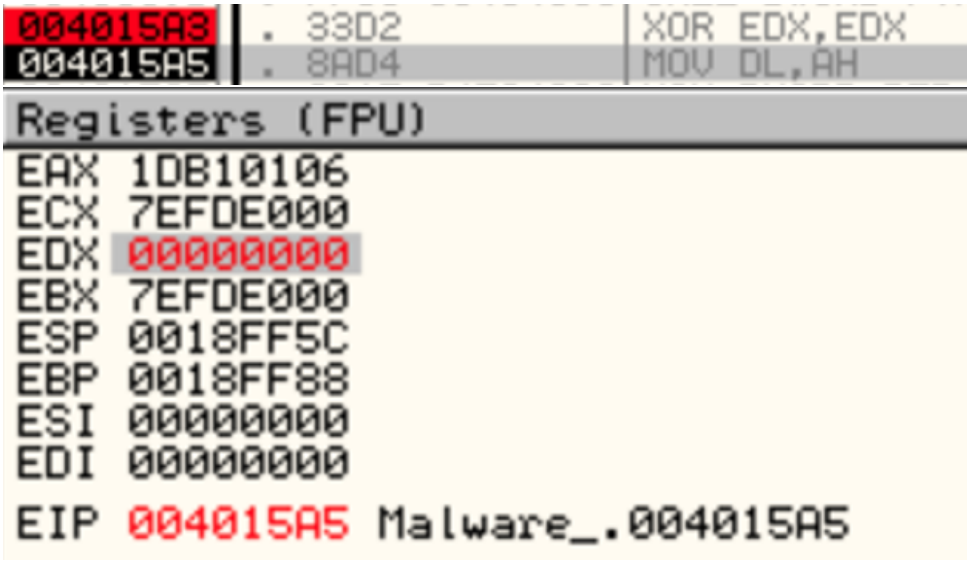
```
004015A3 | . 33D2 | XOR EDX,EDX

Registers (FPU)
EAX 1DB10106
ECX 7EFDE000
EDX 00001DB1
EBX 7EFDE000
ESP 0018FF5C
EBP 0018FF88
ESI 00000000
EDI 00000000

EIP 004015A3 Malware_.004015A3
```

2.2.2 Step-into e analisi dell'istruzione

Eseguendo uno *step-into*, il valore del registro `EDX` cambia in 00000000. L'istruzione eseguita è `XOR EDX, EDX`, un'operazione logica XOR che azzera il contenuto del registro `EDX`. Tale operazione ritorna in output il valore 1 nel caso in cui i due valori di input siano diversi tra loro. Siccome l'operatore XOR è usato con gli input EDX ed EDX, l'output sarà sempre 0. Da cui il nuovo valore del registro EDX.



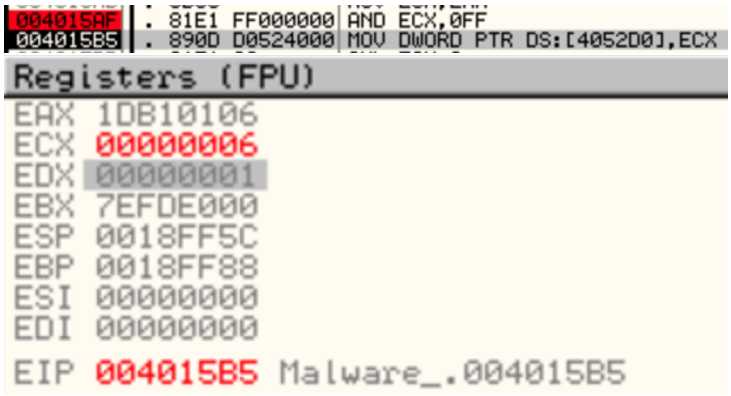
2.3 *Registro ECX*

2.3.1 Valore del Registro ECX

Dopo aver inserito un secondo breakpoint all'indirizzo `004015AF` ed eseguito il programma, il valore del registro `ECX` trovato è `1DB10106`.

2.3.2 Step-into e analisi dell'istruzione

Eseguendo uno *step-into*, il valore di `ECX` cambia in `00000006`. L'istruzione eseguita è `AND ECX, 0FF`, che effettua un'operazione AND bit a bit tra il contenuto di `ECX` e il valore esadecimale `0FF`, mantenendo solo gli 8 bit meno significativi di `ECX`. Il nuovo valore del contenuto del registro



ECX è il risultato dell'operazione mostrata nella tabella seguente:

Operazione	Hex	Bin
AND	1DB1 0106	0001 1101 1011 0001 0000 0001 0000 0110
	FF	1111 1111
	0000 0006	0000 0000 0000 0000 0000 0000 0000 0110

2.4 *Funzionamento generale del Malware*

Esaminando il flusso del programma, si nota che il malware utilizza diverse tecniche avanzate, come la creazione di processi (`CreateProcess`), la creazione di connessioni di rete (creazione di socket) e la manipolazione dell'interfaccia utente. Questo suggerisce che il malware sia multifunzionale, potenzialmente progettato per eseguire più compiti dannosi, come comunicare con un server remoto o manipolare l'interfaccia utente per ingannare l'utente.

Utilizzando tecniche come offuscamento, crittografia o anti-analisi, il malware sembra progettato per evitare la rilevazione da parte dei software antivirus. Confrontando l'hash del

malware con i database di Virus Total, è stato identificato come un Trojan, un tipo di malware che può permettere l'accesso remoto non autorizzato al sistema compromesso.