

# Report sull'Analisi del Malware Utilizzando OllyDBG

Data 14/02/24

## Introduzione

Nell'ambito dell'analisi del malware "Malware\_U3\_W3\_L3", si è fatto riferimento al debugger OllyDBG per rispondere a una serie di quesiti. Questo strumento è essenziale per eseguire analisi dinamica dei malware, consentendo di esaminare il comportamento del malware in esecuzione e rivelando dettagli importanti sulle sue funzionalità.

## Analisi dei Quesiti

### Valore del Parametro "CommandLine" per la Chiamata alla Funzione "CreateProcess" (Indirizzo 0040106E)

Utilizzando OllyDBG, è stato individuato l'indirizzo 0040106E, dove il malware effettua una chiamata alla funzione "CreateProcess". Analizzando il contenuto dello stack in quel punto, è stato identificato il valore del parametro "CommandLine" passato alla funzione.

Il comando corrispondente è una stringa : "cmd"

|          |                 |   |                     |
|----------|-----------------|---|---------------------|
| 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                                |                     |
| 00401057 | . 8D45 A8       | LEA EAX,DWORD PTR SS:[EBP-58]           |                     |
| 0040105A | . 50            | PUSH EAX                                |                     |
| 0040105B | . 6A 00         | PUSH 0                                  |                     |
| 0040105D | . 6A 00         | PUSH 0                                  |                     |
| 0040105F | . 6A 00         | PUSH 0                                  |                     |
| 00401061 | . 6A 01         | PUSH 1                                  |                     |
| 00401063 | . 6A 00         | PUSH 0                                  |                     |
| 00401065 | . 6A 00         | PUSH 0                                  |                     |
| 00401067 | . 68 30504000   | PUSH Malware_.00405030                  |                     |
| 0040106C | . 6A 00         | PUSH 0                                  |                     |
| 0040106E | . FF15 04404000 | CALL DWORD PTR DS:[<&KERNEL32.CreatePro | CreateProcessA      |
| 00401074 | . 8945 EC       | MOV DWORD PTR SS:[EBP-14],EAX           |                     |
| 00401077 | . 6A FF         | PUSH -1                                 |                     |
| 00401079 | . 8B4D F0       | MOV ECX,DWORD PTR SS:[EBP-10]           |                     |
| 0040107C | . 51            | PUSH ECX                                |                     |
| 0040107D | . FF15 00404000 | CALL DWORD PTR DS:[<&KERNEL32.WaitForSi | WaitForSingleObject |
| 00401083 | . 33C0          | XOR EAX,EAX                             |                     |
| 00401085 | . 8BE5          | MOV ESP,EBP                             |                     |
| 00401087 | . 5D            | POP EBP                                 |                     |
| 00401088 | . C3            | RETN                                    |                     |
| 00401089 | . 55            | PUSH EBP                                |                     |
| 0040108A | . 8BEC          | MOV EBP,ESP                             |                     |
| 0040108C | . 81EC 08010000 | SUB ESP,108                             |                     |
| 00401092 | . 57            | PUSH EDI                                |                     |
| 00401093 | . C785 F0FEFFFF | MOV DWORD PTR SS:[EBP-108],0            |                     |

## Valore del Registro EDX dopo l'Inserimento di un Breakpoint Software (Indirizzo 004015A3)

È stato inserito un breakpoint software all'indirizzo 004015A3 e successivamente è stato osservato il valore del registro EDX. Questo valore fornisce informazioni utili per comprendere lo stato del programma in quel punto.

Il valore del registro EDX dopo aver effettuato il breakpoint è 00001DB1

|          |                |   |                         |  |  |
|----------|----------------|---|-------------------------|--|--|
| 00401566 | F2:RE          | REPNE SCAS BYTE PTR ES:[EDI]            |                         |  |  |
| 00401568 | 47             | INC EDI                                 |                         |  |  |
| 00401569 | 3907           | CMPS BYTE PTR DS:[EDI],AL               |                         |  |  |
| 0040156B | 74 04          | JE SHORT Malware_.00401571              |                         |  |  |
| 0040156D | 3308           | XOR EAX,EAX                             |                         |  |  |
| 0040156F | EB 02          | JMP SHORT Malware_.00401573             |                         |  |  |
| 00401571 | 8EC7           | MOV EAX,EDI                             |                         |  |  |
| 00401573 | FC             | CLD                                     |                         |  |  |
| 00401574 | 5F             | POP EDI                                 |                         |  |  |
| 00401575 | C9             | LEAVE                                   |                         |  |  |
| 00401576 | C3             | RETN                                    |                         |  |  |
| 00401577 | 55             | PUSH EBP                                |                         |  |  |
| 00401578 | 8BEC           | MOV EBP,ESP                             |                         |  |  |
| 00401579 | 6A FF          | PUSH -1                                 |                         |  |  |
| 0040157C | 68 00404000    | PUSH Malware_.00404000                  |                         |  |  |
| 00401581 | 68 3C204000    | PUSH Malware_.0040203C                  |                         |  |  |
| 00401586 | 64:R1 00000000 | MOV EDI,DWORD PTR FS:[0]                | SE handler installation |  |  |
| 0040158C | 50             | PUSH EAX                                |                         |  |  |
| 0040158D | 64:8925 000000 | MOV DWORD PTR FS:[0],ESP                |                         |  |  |
| 00401594 | 8BEC 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 | 3302           | XOR EDX,EDX                             |                         |  |  |
| 004015A5 | 8004           | MOV DL,AH                               |                         |  |  |
| 004015A7 | 8915 04524000  | MOV DWORD PTR DS:[405204],EDX           |                         |  |  |
| 004015AD | 8BC8           | MOV ECX,EAX                             |                         |  |  |
| 004015AF | 81E1 FF000000  | AND ECX,0FF                             |                         |  |  |

**Registers (FPU)**  
EAX 00010106  
ECX 7E7DE000  
EDX 00001DB1  
EBX 7E7DE000  
ESP 0018FF5C  
EBP 0018FF58  
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)  
D 0  
O 0 LastErr: ERROR\_SUCCESS (00000000)  
EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)  
I00 0000 0000 0000 0000  
I01 0000 0000 0000 0000  
I02 0000 0000 0000 0000  
I03 0000 0000 0000 0000  
I04 0000 0000 0000 0000  
I05 0000 0000 0000 0000  
I06 0000 0000 0000 0000  
I07 0000 0000 0000 0000

Da notare è la funzione al registro di memoria dove abbiamo effettuato il breakpoint. La funzione infatti “ XOR EDX, EDX “ è una condizione booleana che porta il valore del registro EDX a 0.

Eseguito il breakpoint a quel determinato punto del programma il valore del registro EDX corrisponde al valore che ha il registro prima di effettuare la funzione “XOR EDX, EDX”.

## Valore del Registro EDX dopo uno "Step-Into" (Indirizzo 004015A3)

Dopo aver eseguito uno "step-into" dal breakpoint software, è stato verificato il nuovo valore del registro EDX. Questo passaggio è cruciale per comprendere come il malware sta elaborando i dati o le istruzioni in quel punto.

Possiamo subito notare che una volta effettuato lo step-into dopo aver eseguito il breakpoint, il tool ci rimanda alla riga di codice successiva a quella del breakpoint. Per cui la funzione “XOR EDX, EDX” è stata eseguita ed il valore del registro EDX è stato aggiornato e corrisponde a:

- EDX 00000000

|          |                |   |                         |  |  |
|----------|----------------|---|-------------------------|--|--|
| 0040156B | 74 04          | JE SHORT Malware_.00401571              |                         |  |  |
| 0040156D | 3308           | XOR EAX,EAX                             |                         |  |  |
| 0040156F | EB 02          | JMP SHORT Malware_.00401573             |                         |  |  |
| 00401571 | 8EC7           | MOV EAX,EDI                             |                         |  |  |
| 00401573 | FC             | CLD                                     |                         |  |  |
| 00401574 | 5F             | POP EDI                                 |                         |  |  |
| 00401575 | C9             | LEAVE                                   |                         |  |  |
| 00401576 | C3             | RETN                                    |                         |  |  |
| 00401577 | 55             | PUSH EBP                                |                         |  |  |
| 00401578 | 8BEC           | MOV EBP,ESP                             |                         |  |  |
| 00401579 | 6A FF          | PUSH -1                                 |                         |  |  |
| 0040157C | 68 00404000    | PUSH Malware_.00404000                  |                         |  |  |
| 00401581 | 68 3C204000    | PUSH Malware_.0040203C                  |                         |  |  |
| 00401586 | 64:R1 00000000 | MOV EDI,DWORD PTR FS:[0]                | SE handler installation |  |  |
| 0040158C | 50             | PUSH EAX                                |                         |  |  |
| 0040158D | 64:8925 000000 | MOV DWORD PTR FS:[0],ESP                |                         |  |  |
| 00401594 | 8BEC 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 | 3302           | XOR EDX,EDX                             |                         |  |  |
| 004015A5 | 8004           | MOV DL,AH                               |                         |  |  |
| 004015A7 | 8915 04524000  | MOV DWORD PTR DS:[405204],EDX           |                         |  |  |
| 004015AD | 8BC8           | MOV ECX,EAX                             |                         |  |  |
| 004015AF | 81E1 FF000000  | AND ECX,0FF                             |                         |  |  |
| 004015B0 | 8900 00524000  | MOV DWORD PTR DS:[405208],ECX           |                         |  |  |
| 004015B2 | C1E1 00        | SHL ECX,1                               |                         |  |  |
| 004015B3 | 8BCA           | MOV ECX,EDX                             |                         |  |  |

**Registers (FPU)**  
EAX 00010106  
ECX 7E7DE000  
EDX 00000000  
EBX 7E7DE000  
ESP 0018FF5C  
EBP 0018FF58  
ESI 00000000  
EDI 00000000  
EIP 004015A5 Malware\_.004015A5  
C 0 ES 002B 32bit 0(FFFFFFFF)  
P 1 CS 0023 32bit 0(FFFFFFFF)  
A 0 SS 002B 32bit 0(FFFFFFFF)  
Z 1 DS 002B 32bit 0(FFFFFFFF)  
S 0 FS 0053 32bit 7EFD0000(FFF)  
T 0 GS 002B 32bit 0(FFFFFFFF)  
D 0  
O 0 LastErr: ERROR\_SUCCESS (00000000)  
EFL 00010246 (NO,NB,E,SE,NS,PE,GE,LE)  
I00 0000 0000 0000 0000  
I01 0000 0000 0000 0000  
I02 0000 0000 0000 0000  
I03 0000 0000 0000 0000  
I04 0000 0000 0000 0000  
I05 0000 0000 0000 0000  
I06 0000 0000 0000 0000  
I07 0000 0000 0000 0000

## Valore del Registro ECX dopo l'Inserimento di un Breakpoint (Indirizzo 004015AF)

Un secondo breakpoint è stato inserito all'indirizzo di memoria 004015AF per monitorare il valore del registro ECX. Questo indirizzo di memoria corrisponde alla funzione "AND ECX, OFF"

Il procedimento utilizzato è lo stesso di prima. Abbiamo eseguito il breakpoint all'indirizzo di memoria specificato e preso nota del valore del registro ECX che corrisponde a:

- ECX 1DB10106

|          |                |   |                         |
|----------|----------------|---|-------------------------|
| 0040156B | 74 04          | JE SHORT Halware_.00401571              |                         |
| 0040156D | 3BC0           | XOR EAX,EAX                             |                         |
| 0040156F | EB 02          | JMP SHORT Halware_.00401573             |                         |
| 00401571 | 8BC7           | MOV EAX,EDI                             |                         |
| 00401573 | FC             | CLO                                     |                         |
| 00401574 | 5F             | POP EDI                                 |                         |
| 00401575 | C9             | LEAVE                                   |                         |
| 00401576 | C3             | RETN                                    |                         |
| 00401577 | 55             | PUSH EBP                                |                         |
| 00401578 | 8BEC           | MOV EBP,ESP                             |                         |
| 00401579 | 6A FF          | PUSH -1                                 |                         |
| 0040157C | 68 C0404000    | PUSH Halware_.004040C0                  |                         |
| 00401581 | 68 3C204000    | PUSH Halware_.0040203C                  |                         |
| 00401586 | 64:41 00000000 | MOV EDI,DWORD PTR FS:[0]                | SE handler installation |
| 0040158C | 50             | PUSH EAX                                |                         |
| 00401590 | 64:8925 000000 | MOV DWORD PTR FS:[0],ESP                |                         |
| 00401594 | 8BEC 10        | SUB ESP,10                              |                         |
| 00401597 | 53             | PUSH EBX                                |                         |
| 00401598 | 54             | PUSH ESI                                |                         |
| 00401599 | 57             | PUSH EDI                                |                         |
| 0040159A | 9945 E8        | MOV DWORD PTR SS:[EBP-10],ESP           |                         |
| 0040159D | FF15 30404000  | CALL DWORD PTR DS:[<kernel32.GetVersion | kernel32.GetVersion     |
| 004015A3 | 3BD2           | XOR EDX,EDX                             |                         |
| 004015A5 | 804            | MOV DL,AH                               |                         |
| 004015A7 | 8915 D4524000  | MOV DWORD PTR DS:[4052D4],EDX           |                         |
| 004015AC | 8B29           | MOV ECX,EBX                             |                         |
| 004015B5 | 81E1 FF000000  | AND ECX,0FF                             |                         |
| 004015B6 | 8940 D0524000  | MOV DWORD PTR DS:[4052D0],ECX           |                         |
| 004015B8 | C1E1 08        | SHL ECX,8                               |                         |
| 004015BE | 03CA           | ADD ECX,EDX                             |                         |

|                 |                                   |
|-----------------|-----------------------------------|
| Registers (FPU) |                                   |
| EAX             | 1DB10106                          |
| ECX             | 00000006                          |
| EDX             | 00000001                          |
| EBX             | 7EFD0000                          |
| ESP             | 0018FFC0                          |
| EBP             | 0018FF80                          |
| ESI             | 00000000                          |
| EDI             | 00000000                          |
| EIP             | 004015AF Halware_.004015AF        |
| C 0             | ES 002B 32bit 0(FFFFFFFF)         |
| F 1             | CS 0023 32bit 0(FFFFFFFF)         |
| D 0             | DS 002B 32bit 0(FFFFFFFF)         |
| Z 1             | OS 002B 32bit 0(FFFFFFFF)         |
| S 0             | FS 0053 32bit 7EFD0000(FFF)       |
| T 0             | GS 002B 32bit 0(FFFFFFFF)         |
| D 0             |                                   |
| O 0             | LastErr ERROR_SUCCESS (00000000)  |
| EFL             | 00000246 (NO,OF,E,GE,NS,PE,GE,LE) |
| MM0             | 0000 0000 0000 0000               |
| MM1             | 0000 0000 0000 0000               |
| MM2             | 0000 0000 0000 0000               |
| MM3             | 0000 0000 0000 0000               |
| MM4             | 0000 0000 0000 0000               |
| MM5             | 0000 0000 0000 0000               |
| MM6             | 0000 0000 0000 0000               |
| MM7             | 0000 0000 0000 0000               |

## Valore del Registro ECX dopo uno "Step-Into" (Indirizzo 004015AF)

Dopo aver eseguito uno "step-into" dal secondo breakpoint, è stato osservato il nuovo valore del registro ECX. Il valore del registro ECX è cambiato e corrisponde a :

- ECX 00000006

|          |                |   |                         |
|----------|----------------|---|-------------------------|
| 0040156B | 74 04          | JE SHORT Halware_.00401571              |                         |
| 0040156D | 3BC0           | XOR EAX,EAX                             |                         |
| 0040156F | EB 02          | JMP SHORT Halware_.00401573             |                         |
| 00401571 | 8BC7           | MOV EAX,EDI                             |                         |
| 00401573 | FC             | CLO                                     |                         |
| 00401574 | 5F             | POP EDI                                 |                         |
| 00401575 | C9             | LEAVE                                   |                         |
| 00401576 | C3             | RETN                                    |                         |
| 00401577 | 55             | PUSH EBP                                |                         |
| 00401578 | 8BEC           | MOV EBP,ESP                             |                         |
| 00401579 | 6A FF          | PUSH -1                                 |                         |
| 0040157C | 68 C0404000    | PUSH Halware_.004040C0                  |                         |
| 00401581 | 68 3C204000    | PUSH Halware_.0040203C                  |                         |
| 00401586 | 64:41 00000000 | MOV EDI,DWORD PTR FS:[0]                | SE handler installation |
| 0040158C | 50             | PUSH EAX                                |                         |
| 00401590 | 64:8925 000000 | MOV DWORD PTR FS:[0],ESP                |                         |
| 00401594 | 8BEC 10        | SUB ESP,10                              |                         |
| 00401597 | 53             | PUSH EBX                                |                         |
| 00401598 | 54             | PUSH ESI                                |                         |
| 00401599 | 57             | PUSH EDI                                |                         |
| 0040159A | 9945 E8        | MOV DWORD PTR SS:[EBP-10],ESP           |                         |
| 0040159D | FF15 30404000  | CALL DWORD PTR DS:[<kernel32.GetVersion | kernel32.GetVersion     |
| 004015A3 | 3BD2           | XOR EDX,EDX                             |                         |
| 004015A5 | 804            | MOV DL,AH                               |                         |
| 004015A7 | 8915 D4524000  | MOV DWORD PTR DS:[4052D4],EDX           |                         |
| 004015AC | 8B29           | MOV ECX,EBX                             |                         |
| 004015B5 | 81E1 FF000000  | AND ECX,0FF                             |                         |
| 004015B6 | 8940 D0524000  | MOV DWORD PTR DS:[4052D0],ECX           |                         |
| 004015B8 | C1E1 08        | SHL ECX,8                               |                         |
| 004015BE | 03CA           | ADD ECX,EDX                             |                         |

|                 |                                  |
|-----------------|----------------------------------|
| Registers (FPU) |                                  |
| EAX             | 1DB10106                         |
| ECX             | 00000006                         |
| EDX             | 00000001                         |
| EBX             | 7EFD0000                         |
| ESP             | 0018FFC0                         |
| EBP             | 0018FF80                         |
| ESI             | 00000000                         |
| EDI             | 00000000                         |
| EIP             | 004015B5 Halware_.004015B5       |
| C 0             | ES 002B 32bit 0(FFFFFFFF)        |
| F 1             | CS 0023 32bit 0(FFFFFFFF)        |
| D 0             | DS 002B 32bit 0(FFFFFFFF)        |
| Z 0             | OS 002B 32bit 0(FFFFFFFF)        |
| S 0             | FS 0053 32bit 7EFD0000(FFF)      |
| T 0             | GS 002B 32bit 0(FFFFFFFF)        |
| D 0             |                                  |
| O 0             | LastErr ERROR_SUCCESS (00000000) |
| EFL             | 00010206 (NO,OF,OF,A,NS,PE,GE,G) |
| MM0             | 0000 0000 0000 0000              |
| MM1             | 0000 0000 0000 0000              |
| MM2             | 0000 0000 0000 0000              |
| MM3             | 0000 0000 0000 0000              |
| MM4             | 0000 0000 0000 0000              |
| MM5             | 0000 0000 0000 0000              |
| MM6             | 0000 0000 0000 0000              |
| MM7             | 0000 0000 0000 0000              |

La funzione AND ECX, OFF è un'operazione booleana di confronto bit a bit dove due bit a confronto daranno 1 come risultato solo se si confrontano 1 con 1, tutti gli altri confronti "0 e 1" o "0 e 0" avranno come risultato 0. Di conseguenza per ottenere il valore 00000006 mettendo a confronto il valore che aveva ECX con OFF il valore di OFF sarà uguale a 00000006.

## Conclusioni

L'analisi dinamica del malware "Malware\_U3\_W3\_L3" utilizzando OllyDBG ha consentito di rispondere con successo ai quesiti posti. Attraverso l'identificazione dei valori dei registri, l'analisi delle istruzioni eseguite e l'esame dei dati nello stack, è stato possibile ottenere una visione dettagliata del comportamento del malware in esecuzione.

### BONUS: Spiegazione a Grandi Linee

Il debugger OllyDBG è uno strumento potente per l'analisi dei malware, consentendo agli analisti di esaminare il comportamento del malware in tempo reale, monitorare lo stato dei registri e delle variabili, e comprendere il flusso di esecuzione del codice. Utilizzando funzionalità come i breakpoint e gli step-into, è possibile eseguire un'analisi dettagliata del malware e rispondere a domande specifiche sulla sua funzionalità e comportamento. Questo approccio dinamico all'analisi dei malware è complementare all'analisi statica e fornisce informazioni cruciali per comprendere appieno le minacce e sviluppare contro-misure efficaci. Purtroppo però basandoci su quanto appreso durante l'esercitazione abbiamo capito che il programma crea una shell.

Abbiamo caricato l'hash MD5 del malware su virustotal per avere un'idea sul tipo di malware in esame ed è risultato che il file in questione è un Trojan, probabilmente capace di aprire una shell di comandi da remoto.