

# S11L3

**Traccia:** All'indirizzo 0040106E il Malware Effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «Command Line» che viene passato sullo stack?

|          |                 |   |                         |
|----------|-----------------|---|-------------------------|
| 00401055 | . 3C            | PUSH EAX                                | PROCESSINFO             |
| 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                                  | CreateProcessA          |
| 0040106E | . FF15 04404000 | CALL DWORD PTR DS:[<&KERNEL32.CreatePro |                         |

Sullo stack viene passato Commandline="cmd".

**Traccia:** Inserite un breakpoint software all'indirizzo 004015A3.

Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta . Che istruzione è stata eseguita?

|          |                 |  |                     |  |
|----------|-----------------|--|---------------------|--|
| 0040158C | . 50            | PUSH EAX                                 |                     |  |
| 0040158D | . 64:8925 00000 | 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                              |                     |  |

Registers (FPU)  
EAX 10B10106  
ECX 7EFDE000  
EDX 00001DB1  
EBX 7EFDE000  
ESP 0018FF5C  
EBP 0018FF88  
ESI 00000000  
EDI 00000000  
EIP 004015A5

All'indirizzo 004015A3,EDX=00001DB1.

|          |                  |  |                         |  |
|----------|------------------|--|-------------------------|--|
| 00401577 | . 55             | PUSH EBP                                 |                         |  |
| 00401578 | . 8BEC           | MOV EBP,ESP                              |                         |  |
| 0040157A | . 6A FF          | PUSH -1                                  |                         |  |
| 0040157C | . 68 C0404000    | PUSH Malware_.004040C0                   |                         |  |
| 00401581 | . 68 3C204000    | PUSH Malware_.0040203C                   |                         |  |
| 00401586 | . 64:A1 00000000 | MOV EAX,DWORD PTR FS:[0]                 | SE handler installation |  |
| 0040158C | . 50             | PUSH EAX                                 |                         |  |
| 0040158D | . 64:8925 00000  | 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 | . 80D4           | MOV DL,AH                                |                         |  |
| 004015A7 | . 8915 D4524000  | MOV DWORD PTR DS:[4052D4],EDX            |                         |  |
| 004015AD | . 8BC8           | MOV ECX,EAX                              |                         |  |
| 004015AF | . 81E1 FF000000  | AND ECX,0FF                              |                         |  |
| 004015B5 | . 8900 D0524000  | MOV DWORD PTR DS:[4052D0],ECX            |                         |  |
| 004015B8 | . C1E1 08        | SHL ECX,8                                |                         |  |
| 004015BE | . 03CA           | ADD ECX,EDX                              |                         |  |
| 004015C0 | . 8900 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                                  |                         |  |
| 004015D6 | . 8508           | TEST EAX,EAX                             |                         |  |
| 004015D8 | . 75 08          | JNZ SHORT Malware_.004015E2              |                         |  |
| 004015DA | . 6A 1C          | PUSH 1C                                  |                         |  |
| 004015DC | . E8 9A000000    | CALL Malware_.00401678                   |                         |  |

Registers (FPU)  
EAX 10B10106  
ECX 7EFDE000  
EDX 00000000  
EBX 7EFDE000  
ESP 0018FF5C  
EBP 0018FF88  
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  
LastErr ERROR\_SUCCESS (00000000)  
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)  
ST0 empty 0.0  
ST1 empty 0.0  
ST2 empty 0.0  
ST3 empty 0.0  
ST4 empty 0.0  
ST5 empty 0.0  
ST6 empty 0.0  
ST7 empty 0.0  
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0  
FCW 027F Prec NFAR.53 Mask 1 1 1 1 1 1

Ora EDX viene azzerato,perchè viene eseguito XOR EDX,EDX  
il quale va ad azzerare EDX.

**Traccia:** Inserite un secondo breakpoint all'indirizzo di memoria 004015 AF. 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).

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

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

Il valore di ECX ora è 00000006, questo perchè è stata eseguita l'istruzione AND ECX,OFF.