

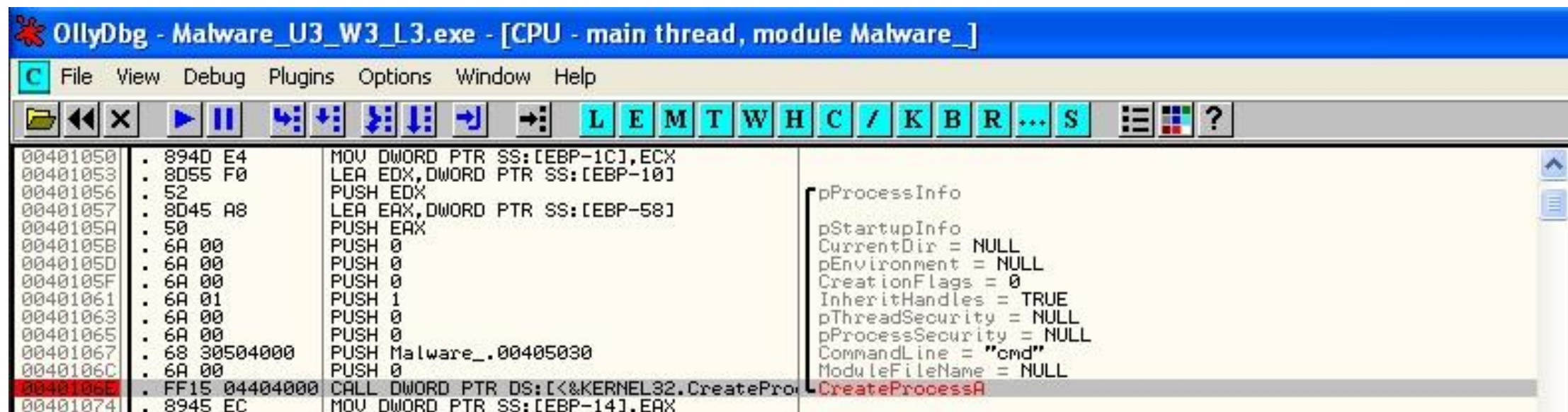
OllyDGB

Malware_U3_W3_L3

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?

Inserimento di un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX, motivando la risposta?

Inserimento di un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguire uno step-into. Qual è ora il valore ECX?
Spiegazione di quale istruzione è stata eseguita



All'indirizzo 0040106E il malware effettua una chiamata di funzione alla funzione *CreateProcess*. Il valore del parametro *CommandLine* che viene passato sullo stack è *cmd*.

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Plugins Options Window Help

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 . 8AD4 MOV DL,AH

Registers (FPU)
EAX 0A280105
ECX 7FFD4000
EDX 00000A28
EBX 7FFD4000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C910208 ntdll.

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Plugins Options Window Help

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 . 8AD4 MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX

Registers (FPU)
EAX 0A280105
ECX 7FFD4000
EDX 00000000
EBX 7FFD4000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C910208 ntdll.
EIP 004015A5 Malware_

Inserimento di un breakpoint software all'indirizzo 004015A3. Il valore del registro EDX, dopo aver cliccato Play, è: 00000A28, ed il programma si ferma all'istruzione: XOR EDX, EDX.

Dopo l'inserimento di uno step-into, il valore del registro EDX è: 00000000 e viene eseguita l'istruzione: XOR EDX, EDX, inizializzando a zero una variabile.

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Plugins Options Window Help

83EC 10 SUB ESP,10
53 PUSH EBX
56 PUSH ESI
57 PUSH EDI
8965 E8 MOV DWORD PTR SS:[EBP-18],ESP
FF15 30404000 CALL DWORD PTR DS:[<&KERNEL32.GetVersion] kernel32.GetVersion
33D2 XOR EDX,EDX
8AD4 MOV DL,AH
8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
8BC8 MOV ECX,EAX
81E1 FF000000 AND ECX,0FF
890D D0524000 MOV DWORD PTR DS:[4052D0],ECX

Registers (FPU)
EAX 0A280105
ECX 0A280105
EDX 00000001
EBX 7FFD4000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C910208 ntdll.
EIP 004015AF Malwar
C 0 ES 0023 32bit

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

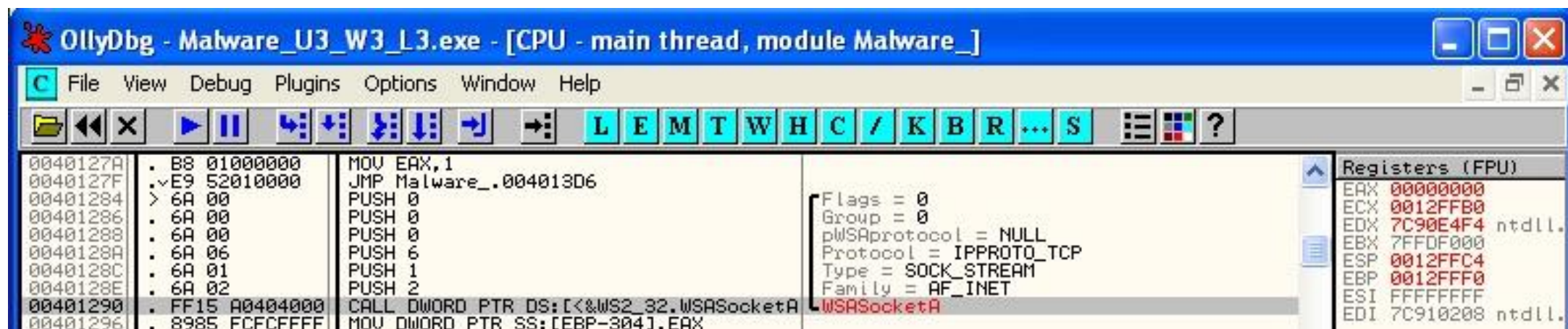
File View Debug Plugins Options Window Help

83EC 10 SUB ESP,10
53 PUSH EBX
56 PUSH ESI
57 PUSH EDI
8965 E8 MOV DWORD PTR SS:[EBP-18],ESP
FF15 30404000 CALL DWORD PTR DS:[<&KERNEL32.GetVersion] kernel32.GetVersion
33D2 XOR EDX,EDX
8AD4 MOV DL,AH
8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
8BC8 MOV ECX,EAX
81E1 FF000000 AND ECX,0FF
890D D0524000 MOV DWORD PTR DS:[4052D0],ECX
C1E1 08 SHL ECX,8

Registers (FPU)
EAX 0A280105
ECX 00000005
EDX 00000001
EBX 7FFD4000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C910208 ntdll.
EIP 004015B5 Malwar
C 0 ES 0023 32bit
P 1 CS 001B 32bit

Inserimento di un secondo breakpoint all'indirizzo di memoria 004015AF. Il valore del registro ECX, dopo aver cliccato Play è:
0A280105

Dopo l'inserimento di uno step-into, il valore ECX è: 00000005, essendo stata eseguita l'istruzione: AND ECX, 0FF.



The screenshot shows the OllyDbg interface with the title bar "OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]". The menu bar includes File, View, Debug, Plugins, Options, Window, and Help. The toolbar contains various debugging icons. The assembly window displays the following code:

Address	Disassembly	Comment
0040127A	. B8 01000000	MOV EAX,1
0040127F	.vE9 52010000	JMP Malware_.004013D6
00401284	> 6A 00	PUSH 0
00401286	. 6A 00	PUSH 0
00401288	. 6A 00	PUSH 0
0040128A	. 6A 06	PUSH 6
0040128C	. 6A 01	PUSH 1
0040128E	. 6A 02	PUSH 2
00401290	. FF15 A0404000	CALL DWORD PTR DS:[<&WS2_32.WSASocketA
00401296	. 8985 FCFCFFFF	MOV DWORD PTR SS:[EBP-304],EAX

On the right, the "Registers (FPU)" window shows the following values:

Register	Value	Comment
EAX	00000000	
ECX	0012FFB0	
EDX	7C90E4F4	ntdll.
EBX	7FFDF000	
ESP	0012FFC4	
EBP	0012FFF0	
ESI	FFFFFFFF	
EDI	7C910208	ntdll.

Below the assembly window, a data window shows the following information:

Flags = 0
Group = 0
pWSAprotocol = NULL
Protocol = IPPROTO_TCP
Type = SOCK_STREAM
Family = AF_INET

La funzione del malware, potrebbe essere, dalla lettura delle righe di codice, quella di creare una backdoor.
Si può dedurre dal fatto che il malware crei un socket per connettersi ad esso.