

### 3. Malware analysis: Analisi dinamica avanzata

- 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?

00401056	. 52	PUSH EDX	pProcessInfo
00401057	. 8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]	pStartupInfo
00401058	. 50	PUSH EAX	CurrentDir = NULL
00401059	. 6A 00	PUSH 0	Environment = NULL
0040105A	. 6A 00	PUSH 0	CreationFlags = 0
0040105B	. 6A 00	PUSH 0	InheritHandles = TRUE
0040105C	. 6A 00	PUSH 0	pThreadSecurity = NULL
0040105D	. 6A 00	PUSH 0	pProcessSecurity = NULL
0040105E	. 6A 00	PUSH 0	CommandLine = "cmd"
0040105F	. 6A 00	PUSH 0	ModuleFileName = NULL
00401060	. 6A 00	PUSH 0	
00401061	. 6A 01	PUSH 1	
00401062	. 6A 00	PUSH 0	
00401063	. 6A 00	PUSH 0	
00401064	. 6A 00	PUSH 0	
00401065	. 6A 00	PUSH 0	
00401066	. 68 30504000	PUSH Malware_.00405030	
00401067	. 6A 00	PUSH 0	
00401068	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA>]	CreateProcessA
00401069	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	
0040106A	. 6A FF	PUSH -1	Timeout = INFINITE

Come si nota dalla figura, il valore del parametro è **CMD** (comando prompt Windows).

- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?

0040156F	. 5B 02	JMP SHORT Malware_.00401573	Registers (FPU)
00401570	. 8BC7	MOV EAX,EDI	EAX 0A280105
00401571	. 5F	CLD	ECX 7FFD7000
00401572	. 5F	POP EDI	EDX 00000A28
00401573	. C9	LEAVE	EBX 7FFD7000
00401574	. C3	RETN	ESP 0012FF94
00401575	. 55	PUSH EBP	EBP 0012FFC0
00401576	. 8BEC	MOV EBP,ESP	ESI FFFFFFFF
00401577	. 6A FF	PUSH -1	EDI 7C910208 ntdll.7C910208
00401578	. 68 C0404000	PUSH Malware_.004040C0	EIP 004015A3 Malware_.004015A3
00401579	. 68 3C204000	PUSH Malware_.0040203C	C 0 ES 0023 32bit 0(FFFFFFFF)
0040157A	. 64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	P 1 CS 001B 32bit 0(FFFFFFFF)
0040157B	. 50	PUSH EAX	A 0 SS 0023 32bit 0(FFFFFFFF)
0040157C	. 64:8925 00000000	MOV DWORD PTR FS:[0],ESP	Z 0 DS 0023 32bit 0(FFFFFFFF)
0040157D	. 83EC 10	SUB ESP,10	S 0 FS 003B 32bit 7FFDF000(FFF)
0040157E	. 53	PUSH EBX	T 0 GS 0000 NULL
0040157F	. 56	PUSH ESI	D 0
00401580	. 57	PUSH EDI	O 0 LastErr ERROR_INVALID_HANDLE (00000006)
00401581	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)
00401582	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetUserVers	ST0 empty -UNORM BCBC 01050104 005C0030
00401583	. 33D2	XOR EDX,EDX	
00401584	. 8AD4	MOV DL,AH	
00401585	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	

Come da figura, il valore del registro EDX è **00000A28**.

- Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX.

00401568	. 47	INC EDI	Registers (FPU)
00401569	. 3807	CMPL BYTE PTR DS:[EDI],AL	EAX 0A280105
0040156A	. 74 04	JE SHORT Malware_.00401571	ECX 7FFD4000
0040156B	. 33C0	XOR EAX,EAX	EDX 00000000
0040156C	. 5B 02	JMP SHORT Malware_.00401573	EBX 7FFD4000
0040156D	. 8BC7	MOV EAX,EDI	ESP 0012FF94
0040156E	. 5F	CLD	EBP 0012FFC0
0040156F	. 5F	POP EDI	ESI FFFFFFFF
00401570	. C9	LEAVE	EDI 7C910208 ntdll.7C910208
00401571	. C3	RETN	EIP 004015A5 Malware_.004015A5
00401572	. 55	PUSH EBP	C 0 ES 0023 32bit 0(FFFFFFFF)
00401573	. 8BEC	MOV EBP,ESP	P 1 CS 001B 32bit 0(FFFFFFFF)
00401574	. 6A FF	PUSH -1	A 0 SS 0023 32bit 0(FFFFFFFF)
00401575	. 68 C0404000	PUSH Malware_.004040C0	Z 1 DS 0023 32bit 0(FFFFFFFF)
00401576	. 68 3C204000	PUSH Malware_.0040203C	S 0 FS 003B 32bit 7FFDF000(FFF)
00401577	. 64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	T 0 GS 0000 NULL
00401578	. 50	PUSH EAX	D 0
00401579	. 64:8925 00000000	MOV DWORD PTR FS:[0],ESP	O 0 LastErr ERROR_INVALID_HANDLE (00000006)
0040157A	. 83EC 10	SUB ESP,10	EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
0040157B	. 53	PUSH EBX	ST0 empty -UNORM BCBC 01050104 005C0030
0040157C	. 56	PUSH ESI	ST1 empty -UNORM 0069 006E0069 002E0067
0040157D	. 57	PUSH EDI	ST2 empty 0.0
0040157E	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	ST3 empty 0.0
0040157F	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetUserVers	ST4 empty 0.0
00401580	. 33D2	XOR EDX,EDX	STC empty 0.0
00401581	. 8AD4	MOV DL,AH	
00401582	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	

Il valore di EDX cambia, come è possibile vedere in figura, con il valore 0.

## - Motivazione della risposta.

Configurando il breakpoint e premendo play, il programma si ferma all'istruzione XOR, dove troviamo il valore 00000A28 prima dell'esecuzione dell'istruzione. Successivamente attraverso lo step-info viene eseguita l'istruzione che è equivalente ad inizializzare a 0 una variabile. In questo caso, il valore di EDX sarà 0.

## - Che istruzione è stata eseguita?

Viene eseguita l'istruzione XOR EDX,EDX

## - Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?

00401568	. 47	INC EDI
00401569	. 3807	CMPL BYTE PTR DS:[EDI],AL
0040156B	. 74 04	JE SHORT Malware_.00401571
0040156D	. 3C00	XOR EAX,EAX
0040156F	. EB 02	JMP SHORT Malware_.00401573
00401571	> 8BC7	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
0040157A	. 6A FF	PUSH -1
0040157C	. 68 C0404000	PUSH Malware_.004040C0
0040157E	. 68 3C204000	PUSH Malware_.0040203C
00401580	. 64:01 00000000	MOV EAX,DWORD PTR FS:[0]
00401582	. 50	PUSH EAX
00401584	. 64:8925 00000000	MOV DWORD PTR FS:[0],ESP
00401586	. 83EC 10	SUB ESP,10
00401588	. 53	PUSH EBX
00401589	. 56	PUSH ESI
0040158A	. 57	PUSH EDI
0040158B	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP
0040158D	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersi
0040158E	. 3302	XOR EDX,EDX
0040158F	. 8AD4	MOV DL,AH
00401590	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX
00401591	. 8BC8	MOV ECX,EAX
00401592	. 81E1 FF000000	AND ECX,0FF
00401593	. 8900 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.7C910208
EIP	004015AF Malware_.004015AF
C 0	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
A 0	SS 0023 32bit 0(FFFFFFFF)
Z 0	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 0038 32bit 7FFDF000(FFF)
T 0	GS 0000 NULL
D 0	
0 0	LastErr ERROR_INVALID_HANDLE (00000006)
EFL	00000246 (NO,OF,DF,IF,OF,OF,OF,OF)
ST0	empty -UNORM BCBC 01050104 005C0030
ST1	empty -UNORM 0069 006E0069 002E0067
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0
ST6	empty 0.0
ST7	empty 0.0

Il valore del registro ECX in questo caso è **0A280105**.

## Eseguite un step-into. Qual è ora il valore di ECX?

00401568	. 47	INC EDI
00401569	. 3807	CMPL BYTE PTR DS:[EDI],AL
0040156B	. 74 04	JE SHORT Malware_.00401571
0040156D	. 3C00	XOR EAX,EAX
0040156F	. EB 02	JMP SHORT Malware_.00401573
00401571	> 8BC7	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
0040157A	. 6A FF	PUSH -1
0040157C	. 68 C0404000	PUSH Malware_.004040C0
0040157E	. 68 3C204000	PUSH Malware_.0040203C
00401580	. 64:01 00000000	MOV EAX,DWORD PTR FS:[0]
00401582	. 50	PUSH EAX
00401584	. 64:8925 00000000	MOV DWORD PTR FS:[0],ESP
00401586	. 83EC 10	SUB ESP,10
00401588	. 53	PUSH EBX
00401589	. 56	PUSH ESI
0040158A	. 57	PUSH EDI
0040158B	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP
0040158D	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersi
0040158E	. 3302	XOR EDX,EDX
0040158F	. 8AD4	MOV DL,AH
00401590	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX
00401591	. 8BC8	MOV ECX,EAX
00401592	. 81E1 FF000000	AND ECX,0FF
00401593	. 8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX

  

Registers (FPU)	
EAX	0A280105
ECX	00000005
EDX	00000001
EBX	7FFD4000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910208
EIP	004015B5 Malware_.004015B5
C 0	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
A 0	SS 0023 32bit 0(FFFFFFFF)
Z 0	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 0038 32bit 7FFDF000(FFF)
T 0	GS 0000 NULL
D 0	
0 0	LastErr ERROR_INVALID_HANDLE (00000006)
EFL	00000206 (NO,OF,DF,IF,OF,OF,OF,OF)
ST0	empty -UNORM BCBC 01050104 005C0030
ST1	empty -UNORM 0069 006E0069 002E0067
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0
ST6	empty 0.0
ST7	empty 0.0

Ora il valore di ECX è cambiato con **00000005**.

## - Spiegate quale istruzione è stata eseguita.

Viene eseguita l'istruzione AND sui bit ECX ed il valore FF (esadecimale). Convertiamo i valori in forma binaria ed eseguiamo l'AND logico.

**0A280105**    0000 1010 0010 1000 0000 0001 0000 0101  
**FF**            0000 0000 0000 0000 0000 0000 1111 1111

**AND logico** 0000 0000 0000 0000 0000 0000 0000 0101  
Che corrisponde all'esadecimale 00000005.

In questo modo possiamo capire il valore di ECX dopo l'istruzione.

- **BONUS: spiegare a grandi linee il funzionamento del malware**  
Il malware è una reverse Shell