

Epicode
CS-0124
Pratica S11/L3
Francesco Ficetti

1. Traccia.....	3
2. Svolgimento.....	4
2.1 Parametro "CommandLine"	4
2.2 Registro EDX.....	4
2.3 Registro ECX.....	5
2.4 Funzionamento del malware.....	5

1. Traccia

Con riferimento al malware allegato, rispondere ai seguenti quesiti utilizzando OllyDBG:

1. All'indirizzo 0040106E il malware effettua una chiamata alla funzione «CreateProcess». Qual è il valore del parametro "CommandLine" che viene passato sullo stack?
2. Inserire un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?
Eseguire uno step-into. Qual è il valore del registro EDX e motivare la risposta. Che istruzione è stata eseguita?
3. Inserire un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?
Eseguire uno step-into. Qual è il valore di ECX? Spiegare quale istruzione è stata eseguita.
4. BONUS. Spiegare a grandi linee il funzionamento del malware.

2. Svolgimento

2.1 Parametro “CommandLine”

Il valore del parametro “CommandLine” è “cmd”.

00401056	. 52	PUSH EDX	pProcessInfo
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	
0040106E	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreatePro	CreateProcessA

2.2 Registro EDX

Il valore del registro EDX, prima che venga eseguita l'istruzione alla riga 004015A3, è “00001DB1”.

Registers (FPU)	
EAX	1DB10106
ECX	7EFDE000
EDX	00001DB1
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
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 7EFDD000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	
O 0	LastErr ERROR_SUCCESS (00000000)
EFL	0000206 (NO,NB,NE,A,NS,PE,GE,G)
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 (GT)
FCW	027F Prec NEAR,S3 Mask 1 1 1 1 1 1

Il valore del registro EDX, dopo che è stata eseguita l'istruzione, è 00000000.

Registers (FPU)	
EAX	1DB10106
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 7EFDD000(FFF)
T 0	GS 002B 32bit 0(FFFFFFFF)
D 0	
O 0	LastErr ERROR_SUCCESS (00000000)
EFL	00010246 (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 (GT)
FCW	027F Prec NEAR,S3 Mask 1 1 1 1 1 1

Il valore del registro EDX è 0, perché è stato effettuato uno *xor* del registro con se stesso. L'operatore logico *xor* restituisce 0, quando i due valori confrontati sono uguali, confrontando quindi un valore con se stesso, il risultato sarà sempre 0. Questa operazione viene effettuata quando si vuole azzerare il valore di un registro.

2.3 Registro ECX

Il valore del registro ECX, prima che venga eseguita l'istruzione alla riga 004015AF, è "1DB10106".

Registers (FPU)	
EAX	1DB10106
ECX	1DB10106
EDX	00000001
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000
EIP	004015AF Malware_.004015AF

Il valore del registro ECX, dopo che è stata eseguita l'istruzione, è 00000006.

Registers (FPU)	
EAX	1DB10106
ECX	00000006
EDX	00000001
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000
EIP	004015B5 Malware_.004015B5

Il valore del registro ECX è 6, perché è stato effettuato un *and* del registro con il numero *Off*. L'operatore logico *and*, restituisce 0, se i due valori confrontati sono diversi, 1 se i due valori confrontati sono uguali.

2.4 Funzionamento del malware

Controllando l'hash del file su VirusTotal, viene segnalato che molto probabilmente si tratta di un trojan.