

## Analisi dinamica avanzata

all'interno del malware, all'indirizzo 0040106E, troviamo il commandLine "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.CreateProcessA>]	CreateProcessA
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	

dopodiche all'indirizzo 004015A3

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	
004015AD	. 8BC8	MOV ECX,EAX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	

troviamo che il valore di edx inizialmente è

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	00000206				(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								
			3 2 1 0		E	S	P	U	O Z D I
FST	0000	Cond	0 0 0 0	Err	0	0	0	0	0 0 0 0 (GT)
FCW	027F	Prec	NEAR,53	Mask		1	1	1	1 1 1 1

questo valore si modifica in

```

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 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 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

```

Viene modificato in 0 in quanto si utilizza l'operatore logico xor che inserisce come valore risultante 1 solo e soltanto se i due valori sono discordi e 0 se sono uguali.

Dato che fa lo xor con se stesso il risultanto è sempre 0 andando così a resettare il valore a 0.

Nel indirizzo 004015AF troviamo invece questo valore di ecx

```
Registers (FPU)
EAX 10B10106
ECX 10B10106
EDX 00000001
EBX 7EFDE000
ESP 0018FF5C
EBP 0018FF88
ESI 00000000
EDI 00000000
EIP 004015AF Malware_.004015AF
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 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 (GT)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1
```

E, vediamo facendo lo step-into che si modifica in

```
Registers (FPU)
EAX 10B10106
ECX 00000006
EDX 00000001
EBX 7EFDE000
ESP 0018FF5C
EBP 0018FF88
ESI 00000000
EDI 00000000
EIP 004015B5 Malware_.004015B5
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)
O 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000206 (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,53 Mask 1 1 1 1 1 1
```

questo in quanto viene eseguita l'operazione end tra i due operatori e il risultante è 6.

a grandi linee questo malware si insinua nel registro di sistema e attraverso un socket client si collega ad un server da cui scarica virus e li va ad attivare sul computer vittima