

# Progetto S11-L3

Studente: Simone Mininni

## Traccia:

Fate riferimento al malware: **Malware\_U3\_W3\_L3**, presente all'interno della cartella

**Esercizio\_Pratico\_U3\_W3\_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware.

Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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**? (1)
- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2)  
Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)
- Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. 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).
- BONUS: spiegare a grandi linee il funzionamento del malware

1)

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	. 69 30504000	PUSH Malware_.00405030	ModuleFileName = NULL
0040106C	. 6A 00	PUSH 0	
0040106E	. FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.CreateProcessA]	CreateProcessA
00401073	. 66 45 50	MOV EBP, PTR DS:[EBP-14]	

Per la chiamata di funzione CreateProcessA, come parametro commandLine viene passato il valore “cmd”(il command prompt di windows)

2)

00401569	. 3907	CHP BYTE PTR DS:[EDI],AL	EDI 004015A3 Malware_.004015A3
0040156B	. 74 04	JE SHORT Malware_.00401571	EIP 004015A3 Malware_.004015A3
0040156D	. 3909	XOR EAX, EAX	EAX 00000000
0040156F	. EB 02	JMP SHORT Malware_.00401573	EAX 00000000
00401571	. 8BC7	MOV EAX, EDI	EDX 000000A28
00401572	. C0	CLO	ESP 0012FF94
00401574	. 5F	POP EDI	ESP 0012FF98
00401575	. C9	LEAVE	ESI 00000000
00401576	. C3	RETN	EDI 7C910208 ntdll.7C910208
00401577	. 55	PUSH EBP	EIP 004015A3 Malware_.004015A3
00401578	. 8BEC	MOV EBP, ESP	C 0 ES 0023 32bit 0(FFFFFFFF)
00401579	. 6A FF	PUSH -1	P 1 CS 0010 32bit 0(FFFFFFFF)
0040157C	. 68 C0404000	PUSH Malware_.004040C0	A 0 SS 0023 32bit 0(FFFFFFFF)
00401581	. 68 3C204000	PUSH Malware_.0040203C	Z 0 DS 0023 32bit 0(FFFFFFFF)
00401586	. 641A1 00000000	MOV EAX, DWORD PTR FS:[0]	S 0 FS 0030 32bit 7FDD0000(FFF)
0040158C	. 50	PUSH EAX	T 0 SS 0000 NULL
00401590	. 641925 000000	MOV DWORD PTR FS:[0],ESP	D 0 0 0 LastErr ERROR_INVALID_HANDLE (00000006)
00401594	. 8BEC 10	SUB ESP, 10	EFL 00000206 (NO,NO,NG,A,NS,PE,GE,G)
00401597	. 59	PUSH EAX	ST0 empty +UNORN BCSC 01050104 005C0050
00401598	. 56	PUSH ESI	ST1 empty +UNORN 0069 006E0069 002E0067
00401599	. 57	PUSH EDI	ST2 empty 0.0
0040159A	. 8B65 E8	MOV DWORD PTR SS:[EBP-18],ESP	ST3 empty 0.0
0040159D	. FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.GetVersion]	ST4 empty 0.0
0040159E	. 39D2	XOR EDX, EDX	ST5 empty 0.0
004015A0	. 8D44	MOV DL, AH	ST6 empty 0.0
004015A2	. 8915 D4524000	MOV DWORD PTR DS:[4052D41],EDX	ST7 empty 0.0
004015A3	. 8BC9	MOV EAX, EAX	
004015A4	. 91E1 FF000000	AND EDI, 0FF	
004015A5	. 89D0 D0524000	MOV DWORD PTR DS:[4052D01],ECX	
004015A6	. C1E1 08	SHL ECX, 8	
004015A8	. 8BC3	MOV ECX, EDX	
004015AD	. 89D0 C0524000	MOV DWORD PTR DS:[4052C01],ECX	
004015B0	. C1E8 10	SHR EAX, 10	
004015B3	. 8B52 4000	MOV DWORD PTR DS:[4052C81],EAX	
004015B5	. 6A 00	PUSH 0	

Inizialmente il valore del registro edx è 0x00000A28, dopo l'istruzione xor edx, edx, il valore del registro è 0.

00401569	. 8807	CHP BYTE PTR DS:[EDI],AL		
0040156B	< 74 04	JE SHORT Malware_.00401571		
0040156D	> 8B03	XOR EBX,EBX		
0040156F	> EB02	JMP SHORT Malware_.00401573		
00401571	> 8BC7	MOV EAX,EDI		
00401573	> FC	OLD		
00401574	> 5F	POP EDI		
00401576	> C9	LEAVE		
00401577	> 55	PUSH EBP		
00401578	> 56EC	MOV EBP,ESP		
00401579	> 6A FF	PUSH -1		
0040157C	> 68 C0404000	PUSH Malware_.004040C0		
00401581	> 68 3C204000	PUSH Malware_.0040203C		
00401586	> 64A1 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation	
0040158C	> 50	PUSH EAX		
00401590	> 64:8925 000000	MOV DWORD PTR FS:[0],ESP		
00401594	> 5BCD 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	
004015A2	> 8B03	XOR EDX,EDX		
004015A5	> 8B04	MOV DL,AH		
004015A7	> 8915 D4524000	MOV DWORD PTR DS:[405204],EDX		
004015A7	> 8B05	MOV EAX,EDX		

L'istruzione xor mette 1 se i valori confrontati sono diversi, mette 0 se sono uguali, quindi lo xor tra due valori uguali restituirà 0.

3)

0040156D	. 33C0	XOR EAX,EAX		
0040156F	< EB02	JMP SHORT Malware_.00401573		
00401571	> 8B03	MOV EAX,EBX		
00401573	> FC	OLD		
00401574	> 5F	POP EDI		
00401576	> C9	LEAVE		
00401577	> 55	PUSH EBP		
00401578	> 56EC	MOV EBP,ESP		
00401579	> 6A FF	PUSH -1		
0040157C	> 68 C0404000	PUSH Malware_.004040C0		
00401581	> 68 3C204000	PUSH Malware_.0040203C		
00401586	> 64A1 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation	
0040158C	> 50	PUSH EAX		
00401590	> 64:8925 000000	MOV DWORD PTR FS:[0],ESP		
00401594	> 5BCD 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	
004015A2	> 8B03	XOR EDX,EDX		
004015A5	> 8B04	MOV DL,AH		
004015A7	> 8915 D4524000	MOV DWORD PTR DS:[405204],EDX		
004015A7	> 8B05	MOV EAX,EDX		
004015B5	> 81E1 FF000000	AND EAX,0FF		
004015B8	> 8900 D9524000	MOV DWORD PTR DS:[405200],EAX		
004015BB	> D1E1 00	SHL EAX,0		
004015C0	> 8900 C0524000	MOV DWORD PTR DS:[40520C],EAX		
004015C3	> C1E9 10	SHR EAX,10		
004015C9	> 8B C0524000	MOV DWORD PTR DS:[405208],EAX		
004015CE	> 5A 00	PUSH 0		
004015D0	> 58 30900000	CALL Malware_.00401F08		
004015D3	> 59	POP EAX		
004015F2	> 5E90	RET		

Il valore iniziale contenuto nel registro ecx è 0A280105.

Dopo l'istruzione AND il valore restituito è 0x00000005

0040156D	. 33C0	XOR EAX,EAX		
0040156F	< EB02	JMP SHORT Malware_.00401573		
00401571	> 8B03	MOV EAX,EBX		
00401573	> FC	OLD		
00401574	> 5F	POP EDI		
00401576	> C9	LEAVE		
00401577	> 55	PUSH EBP		
00401578	> 56EC	MOV EBP,ESP		
00401579	> 6A FF	PUSH -1		
0040157C	> 68 C0404000	PUSH Malware_.004040C0		
00401581	> 68 3C204000	PUSH Malware_.0040203C		
00401586	> 64A1 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation	
0040158C	> 50	PUSH EAX		
00401590	> 64:8925 000000	MOV DWORD PTR FS:[0],ESP		
00401594	> 5BCD 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	
004015A2	> 8B03	XOR EDX,EDX		
004015A5	> 8B04	MOV DL,AH		
004015A7	> 8915 D4524000	MOV DWORD PTR DS:[405204],EDX		
004015A7	> 8B05	MOV EAX,EDX		
004015B5	> 81E1 FF000000	AND EAX,0FF		
004015B8	> 8900 D9524000	MOV DWORD PTR DS:[405200],EAX		
004015BB	> D1E1 00	SHL EAX,0		

AND mette 0 se i valori confrontati sono diversi, mette 1 se i valori confrontati sono uguali.

3)

Hash: 251F4D0CAF6EADAE453488F9C9C0EA95 md5

Virus Total:

44  
172

Community Score

44 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

f153dfac09dd69809c3bbf68270a38ee3701f44220c7b181c14a68c138133

Lab 6.exe

Size 24.00 KB

Last Analysis Date 1 hour ago

EXE

peexe

idle

armadillo

checks-user-input

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 10

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label 1 trojan.genericxet/neanvzc

Threat categories trojan

Family labels genericxet nearvzc r00zc0pk20

Security vendors' analysis 1

Do you want to automate checks?

Alibaba	1 Trojan:Win32/Generic.5a8eeed3	ALYac	1 Application.Agent.AHB
Antiy-AVL	1 Trojan:Win32.BTSGeneric	Arcabit	1 Application.Agent.AHB
Avast	1 Win32:Malware-gen	AVG	1 Win32:Malware-gen

00401265  
00401266  
00401271  
00401278  
0040127A  
0040127F  
00401284  
00401286  
00401288  
0040128A  
0040128C  
0040128E  
00401290  
00401296  
0040129C  
004012A2  
004012A5  
004012AA  
004012AF  
004012B5  
004012B6  
004012BC  
004012BD  
004012C2  
004012C5  
004012C8  
004012CB  
004012CC  
004012D2  
004012D8  
004012DF  
004012E1  
004012E7  
004012E8  
004012EE  
004012F4  
004012F9  
004012FF  
00401304  
0040130A  
0040130D  
0040130F  
00401311  
00401317  
0040131C  
00401322  
00401329  
00401332  
00401334  
0040133A  
0040133B  
00401341  
00401342  
00401348  
0040134E  
00401355  
00401357  
0040135D  
0040135E  
00401364

FF15 9C404000  
8985 4CFEFFFF  
8980 4CFEFFFF  
74 0A  
B8 01000000  
E9 52010000  
6A 00  
6A 00  
6A 00  
6A 06  
6A 01  
6A 02  
FF15 A0404000  
8985 FCFCFFFF  
8980 FCFCFFFF  
75 0A  
B8 01000000  
E9 27010000  
8080 10FEFFFF  
51  
8095 50FEFFFF  
52  
E8 C7FDFFFF  
83C4 08  
8B45 F8  
8B45 F8  
50  
FF15 A4404000  
8985 44FEFFFF  
8980 44FEFFFF  
75 23  
8980 FCFCFFFF  
51  
FF15 A0404000  
FF15 AC404000  
68 30750000  
FF15 00404000  
E9 48FEFFFF  
8B42 0C  
8B00  
8B11  
8995 38FEFFFF  
68 0F270000  
FF15 00404000  
66 8985 36FEFF  
66 C785 34FEFF  
6A 10  
8085 34FEFFFF  
50  
8980 FCFCFFFF  
51  
FF15 04404000  
8985 4CFEFFFF  
8980 4CFEFFFF  
75 23  
8B95 FCFCFFFF  
52  
FF15 A0404000  
FF15 AC404000

CALL DWORD PTR DS:[(&WS2\_32.#115)]  
MOV DWORD PTR SS:[EBP-1B4],EAX  
CMP DWORD PTR SS:[EBP-1B4],0  
JE SHORT Malware\_.00401284  
MOV EAX,1  
JMP Malware\_.004013D6  
PUSH 0  
PUSH 0  
PUSH 0  
PUSH 6  
PUSH 1  
PUSH 2  
CALL DWORD PTR DS:[(&WS2\_32.WSASocketA)]  
MOV DWORD PTR SS:[EBP-304],EAX  
CMP DWORD PTR SS:[EBP-304],-1  
JNZ SHORT Malware\_.004012AF  
MOV EAX,1  
JMP Malware\_.004013D6  
LEA ECX,DWORD PTR SS:[EBP-1F0]  
PUSH ECX  
LEA EDI,DWORD PTR SS:[EBP-1B0]  
PUSH EDI  
CALL Malware\_.00401089  
ADD ESP,8  
MOV DWORD PTR SS:[EBP-8],EAX  
MOV EAX,DWORD PTR SS:[EBP-8]  
PUSH EAX  
CALL DWORD PTR DS:[(&WS2\_32.#52)]  
MOV DWORD PTR SS:[EBP-1BC],EAX  
CMP DWORD PTR SS:[EBP-1BC],0  
JNZ SHORT Malware\_.00401304  
MOV ECX,DWORD PTR SS:[EBP-304]  
PUSH ECX  
CALL DWORD PTR DS:[(&WS2\_32.#3)]  
CALL DWORD PTR DS:[(&WS2\_32.#116)]  
PUSH 7530  
CALL DWORD PTR DS:[(&KERNEL32.Sleep)]  
JMP Malware\_.0040124C  
MOV EDI,DWORD PTR SS:[EBP-1BC]  
MOV ECX,DWORD PTR DS:[EDI+C]  
MOV EDI,DWORD PTR DS:[EAX]  
MOV EDI,DWORD PTR DS:[ECX]  
MOV DWORD PTR SS:[EBP-1C8],EDI  
PUSH 270F  
CALL DWORD PTR DS:[(&WS2\_32.#9)]  
MOV WORD PTR SS:[EBP-1CA],AX  
MOV WORD PTR SS:[EBP-1CC],2  
PUSH 10  
LEA EAX,DWORD PTR SS:[EBP-1CC]  
PUSH EAX  
MOV ECX,DWORD PTR SS:[EBP-304]  
PUSH ECX  
CALL DWORD PTR DS:[(&WS2\_32.#4)]  
MOV DWORD PTR SS:[EBP-1B4],EAX  
CMP DWORD PTR SS:[EBP-1B4],-1  
JNZ SHORT Malware\_.0040137A  
MOV EDI,DWORD PTR SS:[EBP-304]  
PUSH EDI  
CALL DWORD PTR DS:[(&WS2\_32.#3)]  
CALL DWORD PTR DS:[(&WS2\_32.#116)]

WSASStartup

Flags = 0  
Group = 0  
pWSAProtocol = NULL  
Protocol = IPPROTO\_TCP  
Type = SOCK\_STREAM  
Family = AF\_INET  
WSASocketA

Arg2  
Arg1  
Malware\_.00401089

Name  
gethostbyname

Socket  
closesocket  
WSACleanup  
Timeout = 30000, ms  
Sleep

NetShout = 270F  
ntohs

AddrLen = 10 (16.)  
pSockAddr  
Socket  
connect

Socket  
closesocket  
WSACleanup

Si può notare la creazione di un socket.

Quindi, considerando anche la funzione “CreateProcessA”, probabilmente si tratta di una backdoor che sfrutta una reverse shell, collegandosi al server attaccante con “connect”.