

**Traccia:**

Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica.

A tal proposito, con riferimento al malware chiamato «**Malware\_U3\_W3\_L2**» presente all'interno della cartella «**Esercizio\_Pratico\_U3\_W3\_L2**» sul Desktop della macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.

1. Individuare l'**indirizzo** della funzione **DLLMain** (così com'è, in esadecimale)
2. Dalla scheda «imports» individuare la funzione «**gethostbyname**». Qual è l'indirizzo dell'import? **Cosa fa la funzione?**
3. Quante sono le **variabili locali** della **funzione** alla locazione di memoria 0x10001656?
4. Quanti sono, invece, i **parametri** della funzione sopra?
5. Inserire altre considerazioni macro livello sul malware (comportamento)

- **Indirizzo della funzione DLLMain:**

Attraverso IDA siamo andati ad analizzare il malware, successivamente modificando la visualizzazione in modalità testuale possiamo andare a ricercare la funzione DLLMain.

L'indirizzo della funzione main è 1000D02E.

```
.text:100002B ServiceMain endp
.text:100002B
.text:100002E
.text:100002E ; SUBROUTINE
.text:100002E
.text:100002E ; 800L __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPUVOID lpvReserved)
.text:100002E _DllMain@12 proc near ; CODE XREF: DllEntryPoint+4B1p
.text:100002E ; DATA XREF: sub_100110FF+2D1o
.text:100002E
.text:100002E hinstDLL = dword ptr 4
.text:100002E fdwReason = dword ptr 8
.text:100002E lpvReserved = dword ptr 0Ch
.text:100002E
.text:100002E mov eax, [esp+fdwReason]
.text:1000032 dec eax
.text:1000033 jnz loc_10000107
.text:1000039 mov eax, [esp+hinstDLL]
.text:100003D push ebx
.text:100003E mov ds:hModule, eax
.text:1000043 mov eax, off_10019044
.text:1000048 push esi
.text:1000049 add eax, 00h
```

- Indirizzo e utilizzo della funzione “gethostbyname”:

L'indirizzo della funzione è 100163CC, si tratta di una di una funzione che permette di ottenere l'indirizzo IP inserendo il dominio.

Address	Ordinal	Name	Library
100163AC		waveInClose	WINMM
100163B0		waveInUnprepareHeader	WINMM
100163B4		waveInPrepareHeader	WINMM
100163B8		waveInAddBuffer	WINMM
100163BC		waveInStart	WINMM
100163C4	18	select	WS2_32
100163C8	11	inet_addr	WS2_32
100163CC	52	gethostbyname	WS2_32
100163D0	12	inet_ntoa	WS2_32
100163D4	16	recv	WS2_32
100163D8	19	send	WS2_32
100163DC	4	connect	WS2_32

- Quante sono le variabili locali della funzione all'allocazione di memoria 0x10001656 e i parametri:

Le variabili locali sono 20 tutte con offset negativo, mentre arg\_0 con offset positivo è un parametro.

IDA View-A	Hex View-A	Exports	Imports	N Names	Functions	Strings	Structures	Enums
<pre> .text:10001656 .text:10001656 var_675          = byte ptr -675h .text:10001656 var_674          = dword ptr -674h .text:10001656 hModule         = dword ptr -670h .text:10001656 timeout        = timeval ptr -66Ch .text:10001656 name           = sockaddr ptr -664h .text:10001656 var_654          = word ptr -654h .text:10001656 in             = in_addr ptr -650h .text:10001656 Parameter      = byte ptr -644h .text:10001656 CommandLine    = byte ptr -63Fh .text:10001656 Data           = byte ptr -638h .text:10001656 var_544          = dword ptr -544h .text:10001656 var_50C          = dword ptr -50Ch .text:10001656 var_500          = dword ptr -500h .text:10001656 var_4FC          = dword ptr -4FCh .text:10001656 readfds         = fd_set ptr -48Ch .text:10001656 phkResult       = HKEY__ ptr -388h .text:10001656 var_380          = dword ptr -380h .text:10001656 var_1A4          = dword ptr -1A4h .text:10001656 var_194          = dword ptr -194h .text:10001656 WSADATA         = WSADATA ptr -190h .text:10001656 arg_0            = dword ptr 4 .text:10001656 </pre>								

- Ulteriori considerazioni sul malware:

Inserendo l'hash del malware su Virustotal si può ipotizzare che si tratti di una Backdoor.

59 / 71

59 security vendors and no sandboxes flagged this file as malicious

eb1079bdd96bc9cc19c38b76342113a0966aad47518ff1a7536eebffaadb4a

X-doorc

Size: 130.94 KB | Last Analysis Date: 23 hours ago

pedll corrupt armadillo overlay

Reanalyze Similar More

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 19

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

Popular threat label trojan.idicaf/r06cc0df321 Threat categories trojan Family labels idicaf r06cc0df321

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Backdoor:Win32.Agent.R9408	Alibaba	Backdoor:Win32/Idicaf.9f3a5556
ALYac	Backdoor.XIW	Antiy-AVL	Trojan[Backdoor]/Win32.Agent
Arcabit	Backdoor.XIW	Avast	Win32:Agent-OLH [Trj]
AVG	Win32:Agent-OLH [Trj]	Avira (no cloud)	BDS/Agen.twe.134160
BitDefender	Backdoor.XIW	Bkav Pro	W32.AI DetectMalware
ClamAV	Win.Trojan.Idicaf-9937585-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)