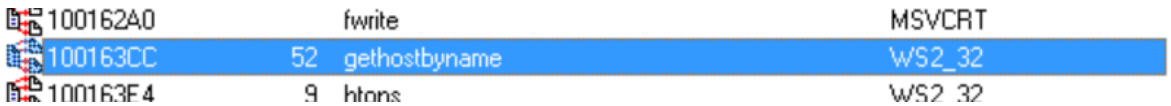
Analisi malware usando IDA Pro

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.

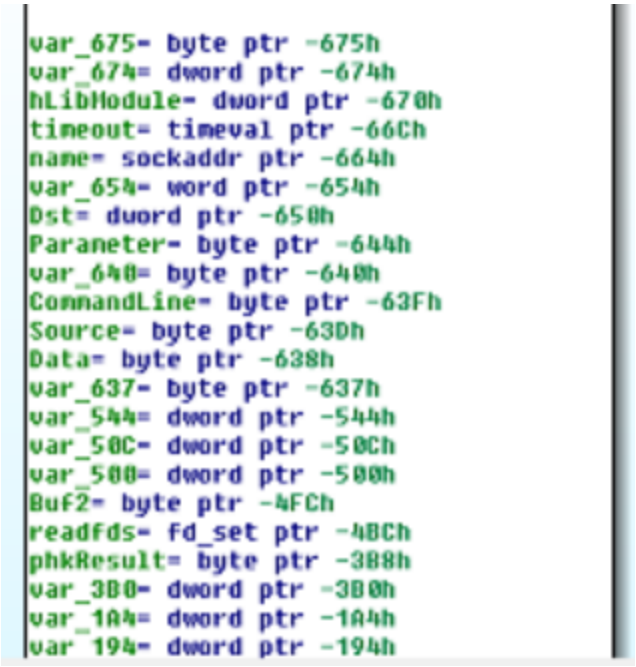
Svolgimento

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?



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

Per effettuare una corretta analisi del malware, questo caso ci basterà verificare le funzioni che lo stesso importa da windows . tra le librerie utilizzate a prima che salta all'occhio è la WS2_32 questa libreria richiama l'omonima dll che viene utilizzata quando si trattano collegamenti di rete.

18	select	WS2_32
11	inet_addr	WS2_32
52	gethostbyname	WS2_32
12	inet_ntoa	WS2_32
16	recv	WS2_32
19	send	WS2_32
4	connect	WS2_32
15	ntohs	WS2_32
9	htons	WS2_32
21	setsockopt	WS2_32
116	WSACleanup	WS2_32
115	WSAStartup	WS2_32
3	closesocket	WS2_32
23	socket	WS2_32
111	WSAGetLastError	WS2_32

Kernell32 espone alle applicazioni la maggiorparte delle API basate su win32 quali la gestione della memoria , dell'imput/output, la creazione di processi e thread.

Analizzando le librerie si potrebbe dire che questo malware è una backdoor , ed effettivamente dopo aver estratto l'hash dello stesso, averla inserita su virus total per un confronto effettivamente si può avere conferma della tesi

Security vendors' analysis			Do you want to automate checks?
AhnLab-V3	Backdoor/Win32.Agent.R9408	Alibaba	Backdoor:Win32/Idicaf.9f3a5556
AliCloud	Backdoor:Win/Idicaf.C	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.Common.9B3E4E7C	ClamAV	Win.Trojan.Idicaf-9937585-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	BackDoor.Siggen.47995	Elastic	Malicious (high Confidence)
Emsisoft	Backdoor.XIW (B)	eScan	Backdoor.XIW
ESET-NOD32	A Variant Of Win32/Idicaf.C	Fortinet	W32/Idicaf.K!tr
GData	Backdoor.XIW	Google	Detected
Gridinsoft (no cloud)	Trojan.Heur!.02016020	Ikarus	Virus.Win32.Agent.OLH
Jiangmin	Backdoor/Agent.cejo	K7AntiVirus	Trojan (004c48271)
K7GW	Trojan (004c48271)	Kaspersky	Backdoor.Win32.Agent.kwa
Kingsoft	Win32.Hack.Agent.kwa	Lionic	Trojan.Win32.QQPass.looG

Basic properties

MD5	1a9fd80174aafecd9a52fd908cb82637
SHA-1	fbe285b8b7fe710724ea35d15948969a709ed33b
SHA-256	eb1079bdd96bc9cc19c38b76342113a09666aad47518ff1a7536eebff8aadb4a
Vhash	115066655d7d5515525z110059345z502028z1a3z70f6z9
Authentihash	9cfb17b8ae79aa81973b06383b3c2c33495cd5f1f009b98823b96dad75f2e995
Imphash	b24a23067c1966f0842b1f450772172c
Rich PE header hash	1539488e7208f95865a6d5e8ce0e1e87
SSDEEP	3072:6gAP9p3D0+fnD0Mx72ZeJ3u1qLOrPFuDa9ZX2P8HAmqx0x:LAP9p3l62ZeJ3u16Or9u2P2P8gmF
TLSH	T144D37D47B255C4B2D4C3003C209D77367BBF9E356465A893FB58CEC63AB5A9AEA14303
File type	Win32 DLL executable windows win32 pe pedll
Magic	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (38.8%) | Microsoft Visual C++ compiled executable (generic) (20.5%) | Win64 Executable (generic) (13%) | Win32 Dynamic ...
DetectItEasy	PE32 | Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-8966)) [DLL32] | Compiler: Microsoft Visual C/C++ (13.00.9178) [C] | Linker: Microsoft Linker (6.00.8168) | Tool:...
File size	130.94 KB (134085 bytes)
PEiD packer	Microsoft Visual C++ v6.0 DLL