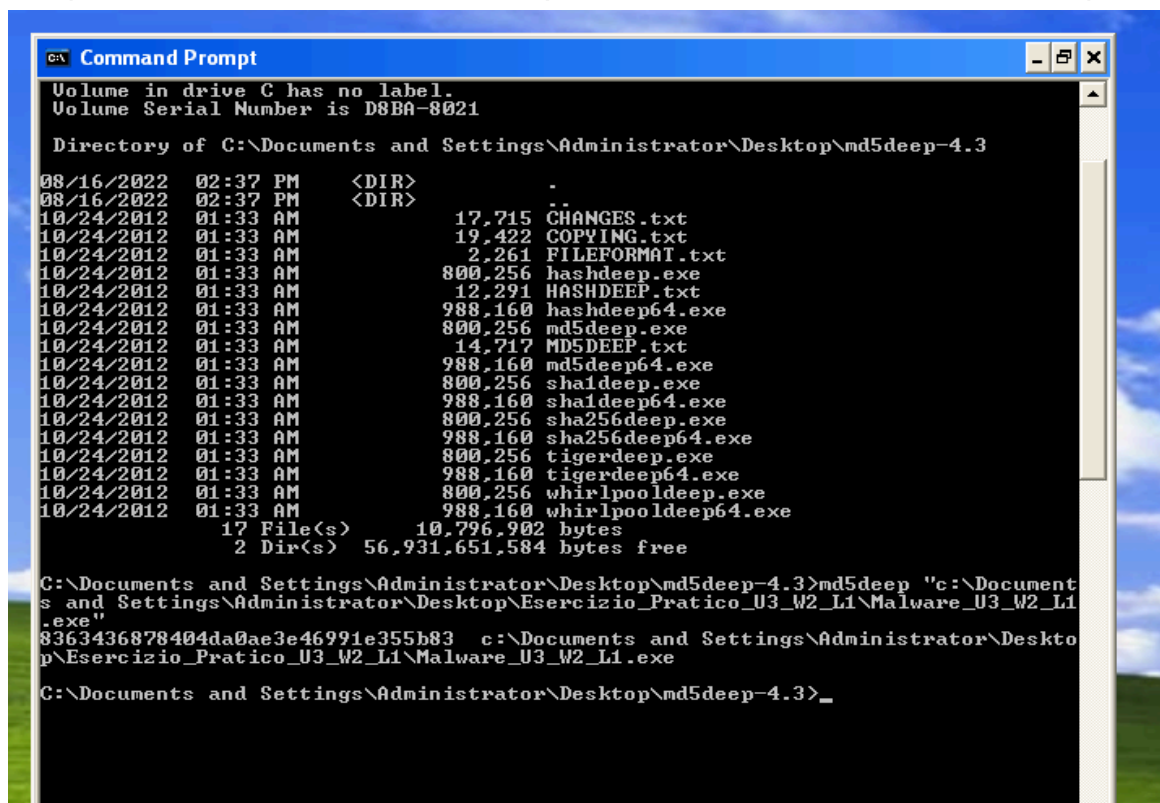


S10L1

Traccia: Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi statica basica. Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti: Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.

Per prima cosa sono andato a recuperare l'hash tramite il tool md5deep.



```
CA Command Prompt
Volume in drive C has no label.
Volume Serial Number is D8BA-8021

Directory of C:\Documents and Settings\Administrator\Desktop\md5deep-4.3

08/16/2022 02:37 PM <DIR> .
08/16/2022 02:37 PM <DIR> ..
10/24/2012 01:33 AM 17,715 CHANGES.txt
10/24/2012 01:33 AM 19,422 COPYING.txt
10/24/2012 01:33 AM 2,261 FILEFORMAT.txt
10/24/2012 01:33 AM 800,256 hashdeep.exe
10/24/2012 01:33 AM 12,291 HASHDEEP.txt
10/24/2012 01:33 AM 988,160 hashdeep64.exe
10/24/2012 01:33 AM 800,256 md5deep.exe
10/24/2012 01:33 AM 14,717 MD5DEEP.txt
10/24/2012 01:33 AM 988,160 md5deep64.exe
10/24/2012 01:33 AM 800,256 sha1deep.exe
10/24/2012 01:33 AM 988,160 sha1deep64.exe
10/24/2012 01:33 AM 800,256 sha256deep.exe
10/24/2012 01:33 AM 988,160 sha256deep64.exe
10/24/2012 01:33 AM 800,256 tigerdeep.exe
10/24/2012 01:33 AM 988,160 tigerdeep64.exe
10/24/2012 01:33 AM 800,256 whirlpooldeep.exe
10/24/2012 01:33 AM 988,160 whirlpooldeep64.exe
17 File(s) 10,796,902 bytes
2 Dir(s) 56,931,651,584 bytes free

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep "c:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe"
8363436878404da0ae3e46991e355b83 c:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>
```

Ottenuto il codice hash ho proceduto ad inserirlo su VirusTotal per vedere se era un malware già noto e risulta essere un trojan di tipo downloader.

56

172

56 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

c876a332d7dd8da331cb8ee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Size3.00 KB

Last Analysis Date2 days ago

EXE

peexe checks-disk-space via-tor detect-debug-environment idle long-sleeps upx checks-user-input

Community Score

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
30

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

Popular threat label Trojan:ulise/startpage

Threat categories trojan downloader

Family labels ulise startpage trojanclicker

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan:Win32.StartPage.C26214	Alibaba	TrojanClicker:Win32/Generic.47e7b5e4
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan:Win32.SGeneric
Arcabit	Trojan.Ser.Ulise.216	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/Downloader.Gen
Baidu	Win32:Trojan-Clicker.Agent.ad	BitDefender	Gen:Variant.Ser.Ulise.216

Mi sono servito in seguito del tool CFF Explorer per vedere da quali librerie è composto il malware.

Malware_U3_W2_L1.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000	40000040
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040

Qui possiamo vedere come il file sia diviso in 3 sezioni: .text, .rdata e .data e contengono rispettivamente il codice con le istruzioni per la CPU, le informazioni sulle librerie importate ed esportate dal file e le variabili globali del programma.

Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

Qui inoltre sono presenti le quattro librerie importate dal malware.

In conclusione, dalle informazioni ottenute dall'analisi possiamo dire che si tratta di un malware downloader progettato per scaricare altri malware su sistemi infetti.