REPORT WEEK 2 UNIT 3 ESERCIZIO 1

Nella giornata odierna andiamo ad analizzare sulla nostra VM di windows XP,con il tool CFF Explorer utilizzato per l'analisi statica del codice di un malware,per la precizione andiamo ad analizzare il Malware_U3_W2_L1.exe.

Librerie:

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

All' interno troviamo nella sezione Import Directory troviamo le librerie del malware:

1) KERNEL32 :Utilizzata per interagire col sistema operativo
2) ADVAPI32: Utilizzata per interagire con i servizi e registri di microsoft
3) MSVCRT:Utilizzata per la manipolazione stringhe ,allocazione di memoria e chiamate input/output
4) WININET:Utilizzata per implementare protocolli di rete come HTTP,NTP e FTP

Successivamente nella categoria SECTION HEADERS abbiamo analizzato le varie sezioni di cui si compone il Malware.

Sessioni:

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
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Come vediamo UPX (Ultimate Packer for eXecutables) è un Packer opensource che viene modificato per la creazione di malware,dove il codice viene scompattato e modificato,successivamente vengono riallocate le sezioni in UPX 0,1 e 2.
Questo processo viene chiamato dumping,ovvero viene ricreato l'eseguibile nella sua forma originale.Le sezioni contengono all'interno il codice che la CPU eseguirà una volta avviato il software,le informazioni sulle librerie e funzioni esportate dall'eseguibile e le sue variabili globali .

CONCLUSIONI

Dopo le analisi eseguite con CFF Explorer,abbiamo scoperto che le informazioni per quanto riguarda le librerie sono state manipolate per rielaborare il codice dell'eseguibile,inoltre le sezione sono state rinominate e modificato il codice .Con l'analisi statica non riusciamo ad ottenere ulteriori informazioni.