Epicode
CS-0124
Pratica S10/L1

Francesco Ficetti

1. Traccia..... 3
2. Svolgimento..... 4
2.1 Librerie..... 4
2.2 Sezioni..... 5
3. Conclusioni..... 5

1. Traccia

Con riferimento al malware allegato a questo esercizio, 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 esse.
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte.

2. Svolgimento

2.1 Librerie

Le librerie di Windows sono una serie di file di supporto forniti dal sistema operativo. Esse contengono funzioni per eseguire operazioni specifiche o accedere a funzionalità del sistema operativo.

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

Le librerie importate da questo malware sono 4:

- Kernel32.dll: fornisce una vasta gamma di funzioni di basso livello, necessarie per gestire le risorse di sistema e fornire servizi di base ai programmi in esecuzione su Windows.
- Advapi32.dll: fornisce una serie di funzioni API (Application Programming Interface) relative alla gestione dei servizi, alla sicurezza e alla gestione degli account utente.
- Msvcrt.dll: è una parte fondamentale del runtime di Microsoft Visual C++ (MSVC), il quale è uno degli ambienti di sviluppo più comuni utilizzati per creare software su piattaforma Windows. Essa fornisce un insieme di funzioni standard del linguaggio C.
- Wininet.dll: fornisce funzionalità per la comunicazione via Internet e la gestione delle risorse di rete.

2.2 Sezioni

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 si può vedere dallo screenshot, il vero nome delle sezioni è stato nascosto, non è quindi possibile distinguerle.

3. Conclusioni

Si tratta di un malware avanzato, ciò non ci consente di capirne il funzionamento preciso.