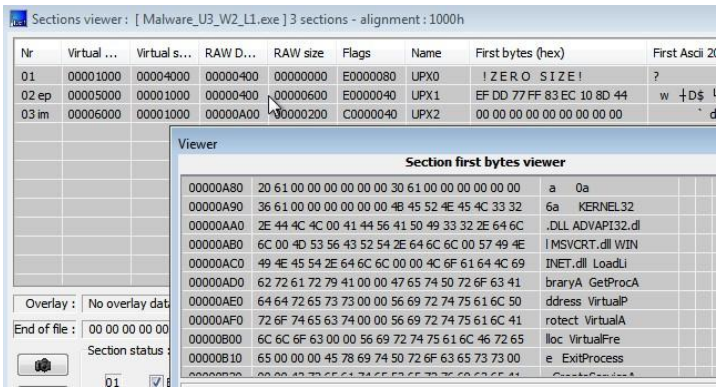

Malware_U3_W2_L1.exe

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

Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address
Byte[8]	Dword	Dword	Dword	Dword
.text	000002DC	00001000	00001000	00001000
.rdata	00000372	00002000	00001000	00002000
.data	0000008C	00003000	00001000	00003000

- **Kernel32.dll**: libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.
- **Advapi32.dll**: libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft
- **.data**: la sezione «data» contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Ricordate che una variabile si dice globale quando non è definita all'interno di un contesto di una funzione, ma bensì è **globalmente dichiarata** ed è di conseguenza accessibile da qualsiasi funzione dell'eseguibile.
- **.text**: la sezione «text» contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.
- **.rdata**: la sezione «rdata» include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.
- **MSVCRT.dll:** libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output in stile linguaggio C.

UPX è un acronimo per "Ultimate Packer for eXecutables", un programma che viene utilizzato per comprimere e proteggere i file eseguibili. Quando si esegue un'analisi delle sezioni di un file eseguibile, UPX0, UPX1 e UPX2 sono nomi delle sezioni utilizzate dal programma UPX per la compressione e la protezione del file. Non posso fornire ulteriori dettagli su come queste sezioni vengono utilizzate nell'analisi delle sezioni senza maggiori informazioni sullo specifico contesto in cui si sta eseguendo l'analisi.

Possiamo notare che questo malware tenti di fare un'accesso verso l'esterno mantenendo la sessione