S10/L1

1) Librerie contenute nel malware:

Kernel32.dll: contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.

Advapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

MSVCRT.dll: contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C.

Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

2) Sezioni di cui si compone il malware:

il malware ha nascosto il vero nome delle sezioni e quindi non siamo in grado di capire che tipo di sezioni sono.

3) Informazioni aggiuntive:

Non è sufficente la sola analisi statica. cercando tra le funzioni troviamo LoadLibrary e GetProcAddres quindi molto probabilmente è un malware che importa le librerie a tempo di esecuzione (runtime) nascondendo di fatto le informazioni circa le librerie importate a monte.