

Identificate:

-Il tipo di Malware in base alle chiamate di funzione utilizzate. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa.

-Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

La funzione setWindowsHookEX sta ad indicare un malware della famiglia dei keylogger.

Questa funzione non fa altro che installare una funzione chiamata «hook» dedicato al monitoraggio degli eventi di una data periferica, come in questo caso il mouse. Il metodo «hook» verrà allertato ogni qualvolta l’utente digiterà un tasto sulla tastiera e salverà le informazioni su un file di log.

La «startup folder» è una particolare cartella del sistema operativo che viene controllata all’avvio del sistema Windows, ed i programmi che sono al suo interno vengono eseguiti.

I sistemi Windows mantengono due tipi di cartelle di startup:

Una dedicata agli utenti, e diversa per ogni utente del sistema

Una generica del sistema operativo, comune a tutti gli utenti del sistema operativo

Se un Malware riesce correttamente a copiare il suo eseguibile all’interno di una delle cartelle sopra, verrà di conseguenza eseguito automaticamente all’avvio del sistema.