Funzionalità malware

Traccia

Dato il codice di un malware identificare:

* Tipo di malware
* Funzioni principali
* Metodo utilizzato per ottenere la persistenza

Analizzando il codice del malware sembrerebbe essere un **keylogger** ovvero un tipo di malware che intercetta tutto ciò che l’utente digita sulla tastiera.

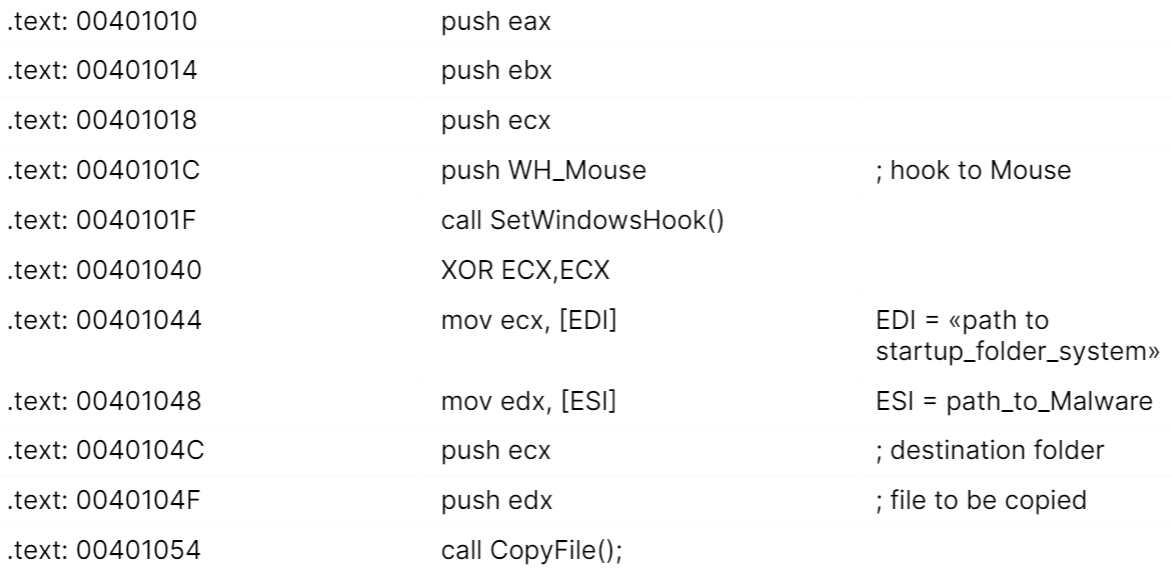
Lo possiamo dedurre dalla funzione **SetWindowsHook**, questa funzione non fa altro che installare un metodo detto **“hook”** dedicato al monitoraggio degli eventi di una periferica, come il mouse in questo caso. Il metodo hook verrà avvisato ogni volta l’utente digiterà un tasto e salverà le informazioni su un file di log.

Mentre la funzione **CopyFile** viene usata dal malware per copiare un file.

Persistenza

Per ottenere la persistenza il malware usa la tecnica di startup folder, ovvero una cartella del sistema operativo controllata all’avvio del sistema operativo, dove all’interno ci sono i programmi che vengono eseguiti. Se il malware riesci a copiare il suo eseguibile all’interno della cartella potrà essere eseguito automaticamente all’avvio del sistema.

Analisi codice



1. Passa eax sullo stack
2. Passa ebx sullo stack
3. Passa ecx sullo stack
4. Passa WH\_Mouse come parametro sullo stack
5. Chiama la funzione SetWindowsHook
6. Setta ecx a 0
7. Copia il percorso della startup folder del sistema operativo (EDI) su ecx
8. Copia il percorso del malware su edx
9. Passa la cartella di destinazione (ECX)
10. Passa il file da copiare (EDX)
11. Chiama la funzione CopyFile