S10-L1 Emanuele Di Stefano

Preparazione

Strumenti utilizzati: PE Explorer, Dependency Walker, CFF Explorer

File analizzato: Malware_U3_W2_L1.exe

Librerie Importate:

kernel32.dll

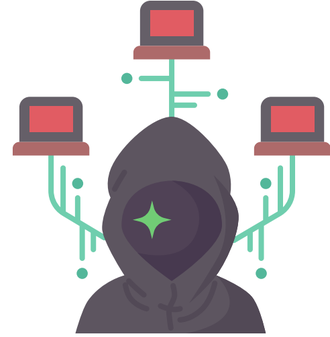
Descrizione: questa libreria fornisce l'accesso alle funzioni di sistema di base, come la gestione della memoria, la gestione dei file e le operazioni I/O.

user32.dll

Descrizione: contiene le funzioni per la gestione dell'interfaccia utente, come la gestione delle finestre, i messaggi delle finestre, e le interazioni dell'utente.

gdi32.dll

Descrizione: gestisce le operazioni grafiche, come il disegno di testo e forme, ed è utilizzato per la rappresentazione grafica di base.



Sezioni del Malware:

text
Descrizione: questa sezione contiene il codice eseguibile del malware. È la sezione principale dove risiede la logica del malware.

.data
Descrizione: contiene i dati inizializzati utilizzati dal malware. Questi dati possono includere variabili globali e strutture utilizzate durante l'esecuzione.

.rdata
Descrizione: contiene dati di sola lettura, come stringhe, puntatori a funzioni, e altre informazioni di runtime che non vengono modificate durante l'esecuzione.

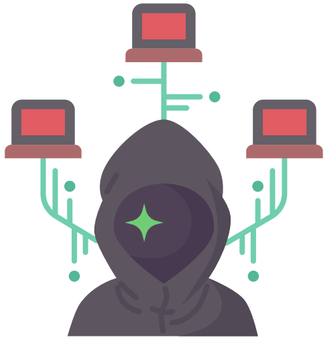
.rsrc
Descrizione: contiene le risorse del programma, come icone, immagini, e file di dialogo che il malware può utilizzare per presentare interfacce all'utente.

.bss
Descrizione: contiene i dati non inizializzati. Questa sezione è generalmente utilizzata per variabili globali non inizializzate che vengono impostate a zero all'inizio dell'esecuzione del programma.

Considerazione Finale

In base alle informazioni raccolte, il malware sembra interagire con il sistema operativo a un livello piuttosto basso, utilizzando funzioni di sistema fondamentali per operazioni di I/O, gestione delle finestre e rappresentazione grafica. La presenza di sezioni standard (.text, .data, .rdata, .rsrc, .bss) indica una struttura tipica di un programma eseguibile, ma l'uso di tali sezioni suggerisce che il malware può:

- eseguire codice dannoso contenuto nella sezione .text.
- utilizzare variabili e dati inizializzati nella sezione .data.
- contenere stringhe e puntatori di sola lettura nella sezione .rdata.
- utilizzare risorse come icone e file di dialogo dalla sezione .rsrc.
- lavorare con dati non inizializzati nella sezione .bss.



Report di Analisi Statica

Librerie Importate

kernel32.dll
Descrizione: fornisce accesso alle funzioni di sistema di base come gestione della memoria, gestione dei file e operazioni I/O.

user32.dll
Descrizione: contiene le funzioni per la gestione dell'interfaccia utente, come la gestione delle finestre e delle interazioni dell'utente.

gdi32.dll
Descrizione: gestisce le operazioni grafiche, come il disegno di testo e forme.

Sezioni del Malware

.text
Descrizione: contiene il codice eseguibile del malware.

.data
Descrizione: contiene i dati inizializzati utilizzati dal malware.

.rdata
Descrizione: contiene dati di sola lettura, come stringhe.

.rsrc
Descrizione: contiene le risorse del programma, come icone e file di dialogo.

.bss
Descrizione: contiene i dati non inizializzati.