Analisi comportamentale delle categorie dei malware più note

A screenshot of a computer program

Description automatically generated

**Traccia:** La figura nella slide successiva mostra un estratto del codice di un malware. 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

Il codice fornito sembra essere un frammento di un malware che sta cercando di ottenere la persistenza nel sistema operativo. Ecco un'analisi delle parti principali del codice:

**Tipo di Malware:**

Possiamo vedere che il malware sta cercando di ottenere la persistenza nel sistema operativo, il che potrebbe indicare un malware di tipo **Keylogger**.

Ciò è stato dedotto (ipotizzato) tramite le chiamate di funzione che andremo ad analizzare successivamente:

**Chiamate di Funzione Principali:**

di seguito elenchiamo le chiamate di funzione principali del codice precedentemente riportato:

**SetWindowsHook** (a 0040101F):

Questa chiamata di funzione sembra essere utilizzata per impostare un hook al mouse (che precedentemente viene richiamata da un push).

Questa è una funzione principale di un **keylogger** utilizzato per il monitoraggio delle attività dell'utente.

**CopyFile** (a 00401054):

Questa chiamata di funzione è utilizzata per copiare un file da una posizione all'altra. Nel contesto del malware, potrebbe essere utilizzata per copiare il malware stesso o altri file necessari per la sua esecuzione.

**Metodo di Persistenza:**

Possiamo vedere che il malware sta cercando di copiare un file (path\_to\_Malware) nella cartella di avvio path to startup\_folder\_system.

**startup\_folder.**

in un sistema operativo Windows è copiare il suo eseguibile in una delle cartelle di startup (che sia la cartella dedicata ad un utente specifico oppure la cartella di startup comune a tutti gli utenti)

Questa potrebbe essere una tecnica per garantire che il malware venga eseguito ogni volta che il sistema operativo si avvia.