Analisi del malware

Immagine che contiene testo

Descrizione generata automaticamente

Analisi di un malware in linguaggio assembly.

|  |  |
| --- | --- |
| Istruzioni | Descrizione |
| Push EBP | | Passa EBP come parametro sullo stack. |
| Mov EBP, ESP | Copia il valore di ESP in EBP. |
| Push ECX | Passa ECX come parametro. |
| Push 0 ;Dwreserved | Passa 0 come parametro |
| Push 0 ;Lpdwflags | Passa 0 come parametro |
| Call Ds: Internetgetconnectedstate | Richiama la funzione seguente. |
| Mov [Ebp+Var\_4], Eax | Mette il valore EAX nella posizione dello stack successiva ad EBP. |
| Cmp [Ebp+Var\_4], 0 | Compara ciò che nella posizione successiva a EBP con 0. |
| Jz Short Loc\_40102B | Fa il salto se lo ZF è impostato a 1 e lo fa su un’istruzione locale. |
| Push Offset A Successinterne; “Success: Internet Connection\N” | Manda in output “Success: Internet Connection”. |
| Call Sub\_40105F | Chiama la seguente funzione |
| Add Esp, 4 | Aggiunge a ESP 4. |
| Mov Eax, 1 | Copia 1 in EAX. |
| Jmp Short Loc\_40103A | Esegue un salto in locale. |

Possiamo notare diversi macro blocchi in questo codice come: creazione dello stack, chiamata di una funzione ed un ciclo IF per controllare se c’è una connessione.