Malware analysis

Immagine che contiene testo

Descrizione generata automaticamente

Analisi di un malware in linguaggio assembly.

|  |  |
| --- | --- |
| Istruzioni | Descrizione |
| Push EBP | | Mette il valore a cui punta EBP in cima allo stack. |
| Mov EBP, ESP | Copia il valore di ESP in EBP. |
| Push ECX | Mette il valore di ECX a cui punta in cima allo stack. |
| Push 0 ;dwReserved | ? |
| Push 0 ;lpdwFlags | ? |
| 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, in qualsiasi caso. |