Analisi Assembly x86

.text:00401000 push ebp

.text:00401001 mov ebp, esp

.text:00401003 push ecx

.text:00401004 push 0 ;dwReserved

.text:00401006 push 0 ;lpdwFlags

.text:00401008 call ds:InternetGetConnectedState

.text:0040100E mov [ebp+var\_4], eax

.text:00401011 cmp [ebp+var\_4], 0

.text:00401015 jz short loc\_40102B

.text:00401017 push offset aSuccessInterne ; “Success: Internet Connection\n”

.text:0040101C call sub\_40105F

.text:00401021 add esp, 4

.text:00401024 inc eax, 1

.text:00401029 jmp short loc\_40103A

Di questo frammento di malware cerchiamo di identificare i costrutti del codice come (while, For, If).

Analizziamo passo a passo le varie righe di codice:

.text:00401000 push ebp

.text:00401001 mov ebp, esp

Queste istruzioni iniziano la funzione e impostano il frame di stack.

.text:00401003 push ecx

Viene salvato il contenuto del registro ECX nello stack.

.text:00401004 push 0 ;dwReserved

.text:00401006 push 0 ;lpdwFlags

.text:00401008 call ds:InternetGetConnectedState

Si chiama la funzione InternetGetConnectedState per verificare lo stato della connessione Internet. I risultati della funzione vengono memorizzati in EAX.

.text:0040100E mov [ebp+var\_4], eax

Il risultato della chiamata viene memorizzato nella variabile locale [ebp+var\_4].

.text:00401011 cmp [ebp+var\_4], 0

.text:00401015 jz short loc\_40102B

Queste istruzioni confrontano il valore memorizzato con zero e saltano a loc\_40102B se è uguale a zero. Questo potrebbe significare che il malware sta verificando se la connessione Internet è disponibile o meno.

.text:00401017 push offset aSuccessInterne ; “Success: Internet Connection\n”

.text:0040101C call sub\_40105F

.text:00401021 add esp, 4

Se la connessione Internet è disponibile, viene chiamata la subroutine sub\_40105F con un messaggio di successo come argomento. La stringa "Success: Internet Connection\n" viene passata come argomento alla subroutine.

.text:00401024 inc eax, 1

Il valore in EAX viene incrementato di 1.

.text:00401029 jmp short loc\_40103A

Salta incondizionatamente a loc\_40103A.

Dall'analisi del codice, sembra che il malware stia verificando la connessione Internet e, se disponibile, esegue alcune azioni, altrimenti continua con l'esecuzione del programma senza fare nulla di significativo riguardo alla connessione Internet.

Riguardo alla struttura del codice, sembra che sia implementato un costrutto "if".

In particolare, la parte chiave è:

.text:00401011 cmp [ebp+var\_4], 0

.text:00401015 jz short loc\_40102B