BW III:

TRACCIA 3

START MENU

TRACCIA:

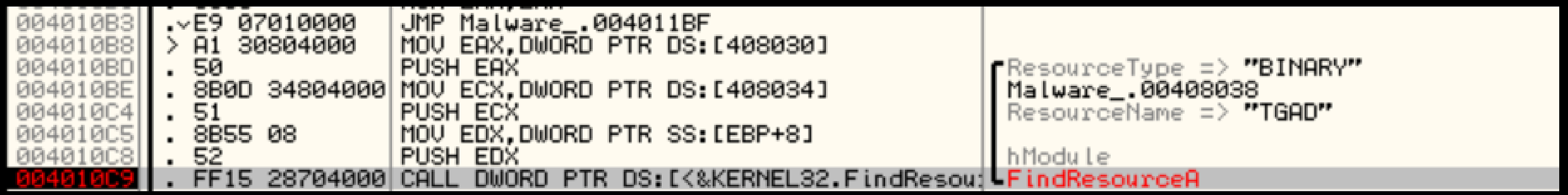
GIORNO 3

Riprendete l'analisi del codice, analizzando le routine tra le locazioni di memoria 00401080 00401128

- Qual è il valore del parametro «ResourceName » passato alla funzione FindResourceA ();
- Il susseguirsi delle chiamate di funzione che effettua il Malware in questa sezione di codice l'abbiamo visto durante le lezioni teoriche. Che funzionalità sta implementando il Malware?
- È possibile identificare questa funzionalità utilizzando l'analisi statica basica ? (dal giorno 1 in pratica)
- In caso di risposta affermativa, elencare le evidenze a supporto.

Entrambe le funzionalità principali del Malware viste finora sono richiamate all'interno della funzione Main()

Disegnare il diagramma di flusso (inserite all'interno dei box solo le informazioni circa le funzionalità principali) che comprenda le 3 funzioni.



Facendo un analisi da Olly DBG nella funzione “FindResourceA” il parametro “ResourceName” ha come valore “TGAD” specificato da hModule, e viene identificato anche il valore di “ResourceType” che sarebbe “BINARY” dove, Il termine "binario" probabilmente si riferisce al codice binario.

Questi tipi di funzioni come:

- FindResource
- LoadResource
- Lock Resource
- SizeofResource

Sono funzioni delle APIs di WIndows che tipicamente vengono utilizzate da Malware di tipo Dropper e permettono di localizzare all’interno della sezione «risorse» il malware da estrarre, e successivamente da caricare in memoria per l’esecuzione o da salvare sul disco per esecuzione futura.

YES NO

Go Back to Agenda Page

È possibile identificare questa funzionalità utilizzando l’analisi statica basica ? (dal giorno 1 in pratica)

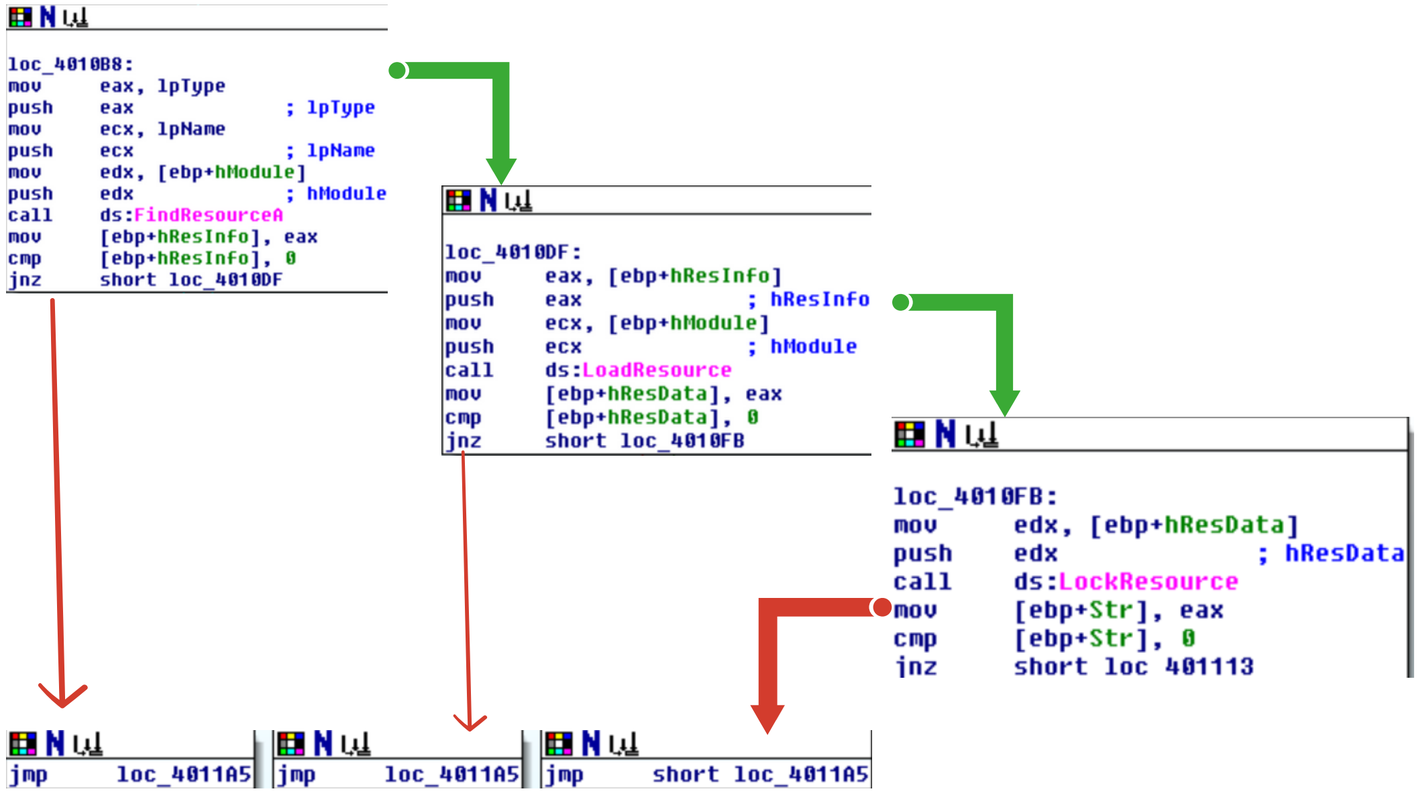
- Si, è possibile determinare la funzionalità del Malware già da una prima analisi statica

Anche senza usare tool come VirusTotal che identificano il Malware dal file signature, è possibile, grazie a CFF Explorer.

.rsrc	00001A70	0000C000	00002000	0000B000	00000000	00000000	0000	0000	40000040

Infatti, come evidenziato in figura controllando le librerie delle funzioni importate su **“Import Directory”** possiamo notare la libreria **.rsrc (resource).** Genericamente un Malware di tipo Dropper è contenuto in questa sezione. Gia da questa prima analisi possiamo iniziare a dedurre che il Malware sia un Dropper.

DIAGRAMMA DI FLUSSO:



GRAZIE PER L'ATTENZIONE