UIC packer Project
Killing Neolite 2

Data	by "-Death_Reaver-"	
07/09/2005	***UIC's Home Page***	**Published by Quequero**
::::::::::::::::::::::::::::::::::::	*Dannato Neolite, grazie Death!*	::::::::::::::::::::::::::::::::::::
....	**E-mail: death.reaver@virgilio.it** **Nick, UIN, canale IRC/EFnet frequentato**	....
Difficolt	**( )NewBies (*)Intermedio ( )Avanzato ( )Master**	

Introduzione

Il titolo dice tutto: buona lettura!

Tools usati

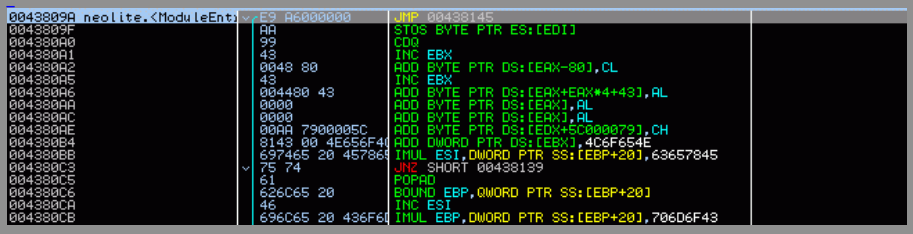
OllyDbg
Plugins per Olly
ImportRec
Un qualsiasi PeEditor e HexEditor

URL o FTP del programma

Il programma packato in allegato
ALLEGATO

Essay

Prima di cominciare vi faccio notare una cosa:
Se andate (sotto XP) in C:\Documents and settings\<nome utente>\SendTO (una cartella nascosta) e ci mettete dentro un collegamento a Olly e/o a IDA etc. potete, facendo click con il destro su un file exe e scegliendo invia a e successivamente OllyDBG, caricare direttamente il file exe dentro olly senza la solita Olly->File->Open Fico no!?
Ora cominciamo:
Prima di tutto caricate il programma in allegato con Olly (potete farlo anche con il metodo sopra citato) e vi ritroverete dinanzi a questo codice:



Come potete vedere la prima istruzione un JMP. Eseguitelo e vi ritroverete qui:

La prima cosa che salta all occhio quella call: non prende parametri a quanto pare, ma prima di essere eseguita il programma fa dei lavoretti con eax. E a quanto si vede dopo, la call restituisce lindirizzo a cui JMP a 0043815A ci spedir.
Per: Molti come me sanno che un JMP EAX in un programma packato MOLTO sospetto. Infatti se lo si esegue si ci ritrova a 004012A5 che come potete immaginare il nostro OEP (Naturalmente in tutti i programmi cavia di Que lOEP questo, cambia solo il codice del packer)
Ora che siamo posizionati sull indirizzo 004012A5 siamo pronti a fare un po di dumping:
Aprite OllyDump e deselezionate la casella Rebuild Import in basso e Dumpate il processo. ORA NON CHIUDETE OLLY!!!
Sicuramente limport table disintegrata o come minimo contiene i dati relativi agli import del packer E NON del programma packato. Quindi ora apriamo ImportRec (anche se il lavoro di rebuilding si pu fare benissimo con un HexEditor*) e per prima cosa scegliamo il processo chiamato in questo caso Neolite.exe. Ora premiamo il pulsante IAT autosearch che far trovare la iat a ImportRec il quale scriver il relativo indirizzo nel box affianco. Ora che Abbiamo l indirizzo della IAT Premiamo Get Import e I mportRec Ci mostrer i suoi risultati. In questo caso troviamo due risultati positivi (Kernel32 e User32). Che culo!. Ok ora possiamo premere il fatidico pulsante Fix Dump che corregger un dump con i dati trovati. Scegliamo quindi il nostro dump e avremo un bel programmino funzionante!!!!

---

*Guardando il risultato con un PeEditor (o con l HexEditor) si nota che ImportRec non ha fatto altro che aggiungere una sezione chiamata mackt dove ha posizionato una nuova IT con le sue varie tavole (nomi, thunk etc.).
Volendo fare a mano (che devo dire d pi soddisfazione ☺) basta fare:

1) incrementare il valore di *NumberOfSection* nel FileHeader
2) Modificare il valore di *SizeOfImage* nellOptional Header secondo lallineamento delle sezioni (se lallineamento perfetto basta aggiungere 1000)
3) Aggiungere una entry nella section table
4) Aggiungere X byte a fine file (dove X pari in questo caso a 1000)

In questo modo abbiamo aggiunto una sezione. Ora basta preservarsi 15 Dword: 5 per Kernel32, 5 per User32 e 5 NULL per indicare la fine dell IT. Quindi scrivere i nome degli import da qualche parte e fategli puntare i rispettivi membri name delle entry della import table. Poi bisogna armarsi di pazienza e riempire le thunk data puntate degli OFT con gli indirizzi che puntano alle strutture Import_By_Name o azzerare il valore degli OFT nellIT e riempire la IAT (FT) con gli indirizzi delle funzioni importare.

PS. Se volete sapere i miei gusti, io non mi piace tanto usare sia i PeEditor che ImportRec(anche se a volte necessario ☺). Preferisco un buon HexEditor

-Death_Reaver-

Note finali

Ringrazio tutti quelli del forum e della mailing list.

Disclaimer