# Cracking

Dunque, anzi tutto, ben ritrovati...finalmente, ben dopo un mese di straziante lavoro e studio, ora ho tempo, prima dell'inizio dell'apertura delle scuole (non vi preoccupate il tempo ce l'avrò) di tenere aggiornato il mio sito...speravate che fossi morto...non ce l'avete fatta, hahahaha, cmq vi ringrazio ancora per le lettere che mi sono arrivate e che mi arriveranno...spero : ) .

Dunque, in questo mese ho fatto essenzialmente due cose: grattato (ehhh...) e lavorato.

P.s. mi sono dato al Visual Basic, un linguaggio, molto bello e semplice da capire (non esageriamo), molte persone VB non lo definiscono neanche un linguaggio che si dovrebbe imparare, naturalmente sto parlando riguardo al diventare hackerz, o comunque programmatori di alto livello (cosa significa alto livello...bohh?...sono 1:00 a.m. e sto per entrare in standby), io invece sono del parere che il suddetto linguaggio oltre a poter permettere di creare delle interfaccie windows (le finestre, i programmi della microsoft..ok?), è anche facile da programmare e permette di modificare i files, i registri, il S.O, come cacchio pare. Cmq. sto realizzando un prog. di criptaggio...vedremo...chi sa se fungerà bene!

P.s. Un appello ai criptomani, ai programmatori in Visual Basic, o programmatori in grado di creare dei buoni algoritmi, non solo voglio fare un appello a tutti i newbies, ho intenzione di formare un team, che crei programmi di ogni tipo o/e studi tecniche di hacking, cripting, cracking, etc... chi volesse unirsi... tom_newbie@hotmail.com per il momento sono solo...(non è vero..c'è Ernesto...) : ) quindi, se incominciamo ad essere un po' possiamo unirci per studiare, insieme, scambiarci informazioni, testare programmi...insomma cresciamo insieme e anche in fretta!!!! ; )

Dopo questa digressione incominciamo subito con il cracking premetto che io non sono un cracker, per il momento voglio solo dirvi quel poco che sono riuscito a capire e fare nel mese che è appena passato (luglio 2000): crackare, significa (nel nostro specifico) saper corrompere un file, una stringa, quello che c'è..., per riuscire ad avere un qualche genere di vantaggio, nel caso ad es. di un gioco, riuscire a farlo funzionare senza CD o con il cd non originale, nel caso di un programma che richiede la password, riuscire a farlo funzionare inserendo anche una password errata etc. Il cracker non agisce mai per scopo di lucro, la sua è una passione innata, la voglia che ha è semplicemente quella di vincere la sfida lanciata dai programmi, con passwords, protezioni dei cd originali, protezioni a tempo, e tante altre, insomma tutto quello che impedisca ad un software di essere usato e naturalmente distribuito liberamente (sento già i finanzieri che bussano alla porta e mi arrestano per istigazione a delinquere : ), cmq, vi ricordo che il cracking di se e per se non è illegale, perché io del mio software acquistato regolarmente :), dal rivenditore autorizzato : ), ci posso fare quello che voglio, basta che rimanga tutto tra le mura di casa. Quindi fate come credete, allenatevi, e diventate esperti crackatori (magari dopo un quinquegnio di esperienze...)

gli strumenti del cracker:

- HIEW 6.x;
- EDITOR ESADECIMALE (non prendetelo, lo ha direttamente HIEW);
- WDASM 8.x;
- SOFTICE (che non so usare : );

dunque questi bei programmini sono essenziali per il crackaggio, (softice è un pochetto grandicello...a voi la ricerca):

HIEW: essenzialmente permette di fare due cose, vedere codice esadecimale del file eseguibile (non solo eseguibili...), vedere gli off-set e quindi permettere la modifica dei registri.

WDASM: è un debugger e anche decompilatore, cioè traduce in maniera comprensibile (per chi non lo avesse mai fatto provi ad aprire con notepad  un .exe (naturalmente prima lo rinomina .txt) senza WDASM e poi con il sudetto programma) un file eseguibile o una libreria (,dll).

EDITOR ESADECIMALE: permette di vedere il codice esadecimale del file, che non è cosa da poco!

## Seconda parete:

spero che abbiate scaricato i programmi di cui sopra, sono essenziali tools per il cracking. Prima esperienza con il cracking:

Dunque, dopo attente letture su "Xoanon Guide" (data 1997 hahahah), e "newbies", e vari tentativi falliti di crackaggio, mi sono accorto che l'arte del crackaggio si trova essenzialmente nel conoscere e saper manipolare i registri dei file eseguibili. I registri non sono nient'altro che delle semplici righe di comando, che si strutturano come in un algoritmo, queste righe si eseguono, si fanno delle scelte se accadono determinati eventi, etc...

Ora, noi dovremmo anzitutto scaricarci la guida di Xoanon, per imparare un pachettino di assembler (il resto è troppo vecchio...):

dunque, presupposto che la parte sull'assembler l'abbiate già letta, il compito del cracker sta nella maggior parte dei casi (e questo avviene soprattutto nei giochi), nel modificare una riga di comando JUMP, che non è una normale JUMP, ma una di tipo condizionale (quelli che hanno fatto diagrammazione...avranno già un concetto in testa...), cioè una jump che dice: l'evento di tipo "A" si è verificato, se si continua con il codice, se no, salta la parte di codice e eseguine un altra.

Queste JUMP possono essere di due tipi:

JE (JUMP EQUAL)

JNE (JUMP NOT EQUAL)

queste due jump sono una l'opposto dell'altro, dovete guardarle come un istruzione IF (la prima) e IF NOT (la seconda).

Ora vi faccio schematico un esempio di istruzione IF (vuole dire se), così quelli che non la sanno se la imparano.

IF "torni a casa tardi" = VERO

"TUO PADRE TI AMMAZZA"

ELSE

"TUO PADRE NON TI AMMAZZA"

END IF

questo è un banalissimo esempio di quello che accade in un jump.

Primo compito: provare a crackare un gioco, che all'avvio manda la richiesta del cd originale, naturalmente noi di cd originali ne abbiamo 4 o 5 in casa, solo che siamo pigri e non li vogliamo prendere...

CARICAMENTO GIOCO

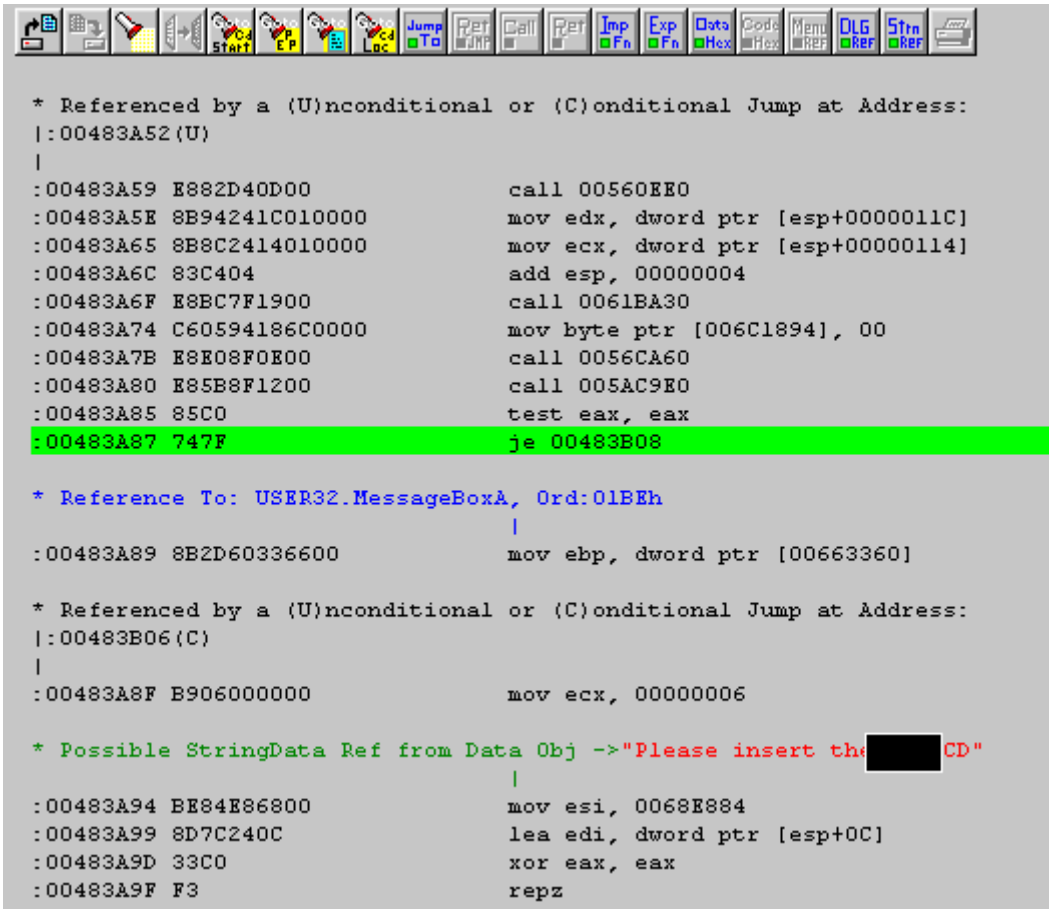
adesso ci servono gli strumenti del mestiere:

WDASM

HIEW

Ci facciamo una copia degli exe nella cartella di HIEW e sul desktop, in modo da non distruggere irrimediabilmente il file (fatevi anche una copia di sicurezza in un'altra cartella), apriamo WDASM, possiamo anche andare a fare un buon pranzo, che intanto prima che carichi...adesso incomincerò molto velocemente con un sacco di procedure, voi non vi preoccupate, se volete davvero intraprendere la strada dei crackrez imparerete tutto molto in fretta : )

Una volta aperto l'eseguibile dovete cliccare il penultimo pulsante alla vostra destra intitolato "String Data references", e vi compariranno tutte le stringhe che ci sono nell'eseguibile: noi casualmente andremo a cercare la stinga intitolata appunto "PLEASE INSERT...", o quello che avete voi!. Ci si posiziona su quella bella stringa e si clicca due volte, così il programma ci spedirà dove appunto risiede nel file la suddetta stringa. Con mezzora di discorso sui JUMP avrete capito cosa dovremmo cercare, immediatamente sopra la stringa ci sarà sicuramente un JUMP condizionale, che può essere JE oppure JNE, a seconda dell'estro dei programmatori : ), in pratica vi troverete di fronte una roba simile



```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00483A52(U)
|
:00483A59 E882D40D00              call 00560EE0
:00483A5E 8B94241C010000          mov edx, dword ptr [esp+0000011C]
:00483A65 8B8C2414010000          mov ecx, dword ptr [esp+00000114]
:00483A6C 83C404                  add esp, 00000004
:00483A6F E8BC7F1900              call 0061BA30
:00483A74 C60594186C0000          mov byte ptr [006C1894], 00
:00483A7B E8E08F0E00              call 0056CA60
:00483A80 E85B8F1200              call 005AC9E0
:00483A85 85C0                    test eax, eax
:00483A87 747F                    je 00483B08

* Reference To: USER32.MessageBoxA, Ord:01BEh
                                  |
:00483A89 8B2D60336600            mov ebp, dword ptr [00663360]

* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00483B06(C)
|
:00483A8F B906000000              mov ecx, 00000006

* Possible StringData Ref from Data Obj ->"Please insert th[redacted]CD"
                                  |
:00483A94 BE84E86800              mov esi, 0068E884
:00483A99 8D7C240C                lea edi, dword ptr [esp+0C]
:00483A9D 33C0                    xor eax, eax
:00483A9F F3                      repz
```

Oh, questo è stato il mio primo gioco crackato...vedete semplicissimo, una volta arrivati qui troviamo un JUMP (JE o JNE), e lo modifichiamo. Molto intuitivamente se troviamo la riga con JE, noi la modifichiamo con JNE e viceversa, adesso come facciamo a modificare il JUMP? per modificare il jump occorre sapere anzitutto il suo OFFSET, che altro non è (da quanto ho capito) l'allocazione del jump (o di qualsiasi altro registro) nel file, l' OFFSET si trova in basso, naturalmente prima il jump deve essere evidenziato in verde, ora vi scrivete, il numero di OFFSET e chiudete WDASM. Adesso tocca a HIEW:

apriamo il programma, cerchiamo il file da modificare:

ci compare il file visto come se lo aprissimo con il notepad, clikiamo invio e ci compare il file visto in esadecimale, clikiamo un'altra volta invio e vediamo i registri : ), questi ultimi sono per ordine di OFFSET, quindi non ci rimane che scorrere tutto il registro...(scherzo scherzo), cliccate F5 (che sarebbe il goto), a dimenticavo...l'OFFSET si scrive senza quegli zeri iniziali e senza l'H finale, poi inseriamo il numero di OFFSET, e clikiamo invio,

_.00483A80: E85B8F1200 call .0005AC9E0 -------- (3)
_.00483A85: 85C0 test eax,eax
_.00483A87: 747F je .000483B08 -------- (4)
_.00483A89: 8B2D60336600 mov ebp,[000663360]
_.00483A8F: B906000000 mov ecx,000000006 ;" "
_.00483A94: BE84E86800 mov esi,00068E884 ;" hÞä"

ora clikiamo F3 per l'edit e potremmo modificare il JUMP da JE a JNE, OK? (p.s. con F3 invio verra tutto più semplice)... se vi siete letti Xoanon avrete già capito e visto quanti jump ci sono, e anche i loro relativi numeri...

quindi noi sappiamo che JE è uguale a 74  e che JNE è uguale a 75, modifichiamo il tutto. Clikiamo F9 per l'updating e F10 pe uscire, copiamo il file nella directory del gioco e incrociamo le dita : )

OHHHH, finito il gioco dovrebbe funzionare...naturalmente non è mai tutto così semplice, il cracking non si limita sono nella modifica dei JUMP, ma cmq, meglio iniziare così che in un altro modo : ).

P.s. fate attenzione ai giochi che contengono il file *.icd, quello è un tipo di protezione un po' difficilotta, che richiede l'uso di SOFTICE...poi se qualche d'uno me lo volesse spiegare !!!!

--- fine seconda parte ---

indietro