Bitmap to Icon 3.5 (serial fishing)		
Data	by "occasus"	
11/02/2004	***UIC's Home Page***	**Published by Quequero**
:share your knowledge=	*Grazie tante occasus, e continua cosi*	=ever:
....	**E-mail:** angelreaper84@hotmail.com	....
Difficoltà	(X)**NewBies** ( )**Intermedio** ( )**Avanzato** ( )**Master**	

Con questo tutorial cercheró di mostrarvi come trovare il numero di serie (di registrazione ovviamente) per questo piccolo programma. Vi dico subito sinceramente di non aspettarvi troppo, é il mio primo tutorial.

Bitmap to Icon 3.5 (serial fishing)

Written by occasus

Introduzione

Questo é il mio primo tutorial e come introduzione non saprei cosa scrivere, quindi bando alle ciance. Comunque spero che qualcuno nella rete mi criticherá sia nel bene (poco probabile) che nel male (molto probabile). Ho ancora molto da imparare e non vivró abbastanza.

Tools usati

Tools usati per il ns. scopo:
SoftIce 4.05 (purtroppo sul sito di Quequero non c'é abbastanza banda, cmq si puó trovare facilmente in rete)
- un minimo di conoscenza assembly (sapere cosé una call, je, jnz, mov, cmp, ...)

URL o FTP del programma

Nome del programma: [Bitmap to Icon 3.5]
Reperibile: [http://www.qtam-computer.com/]
Nome file: [bmp2ico35.zip]
Dimensione: [511 kb]

Notizie sul programma

"QTam Bitmap to Icon é una piccola utility che converte file BMP in file ICO e viceversa. La versione registrata supporta anche i formati GIF, JPG e formati multi-source ICO. Con un interfaccia grafica e il wizard non é mai stato cosí facile creare icone." Protezione: nome serial

Essay

Salve a tutti, iniziamo subito: scarichiamo il programma, installiamolo e andiamo a cercarci un menu o qualche pulsante per la registrazione del programma. Andiamo sul pulsante "More" --> "About program" e ci appare una bella finestra che ci chiede NOME e CODICE. Io ho messo NOME: occasus e CODICE: 123456, premiamo "Enter Code" e ... non succede niente. Ripetiamo il tutto ma prima di clickare "Enter Code" entriamo in SoftIce (Ctrl+D) e settiamo un -break point on execution- (bpx) (per interrompere il flusso del programma e visionare cosa succede in ogni singola esecuzione). Allora settiamo un bpx sulla funzione hmemcpy, molto famosa e spiegata in tanti tutorial; uno piú bello dell'altro. In poche parole bpx hmemcpy --> enter e usciamo dal SI (F5). Adesso clickiamo su "Enter Code" e ... il SI si avvia bloccando tutte le altre applicazioni. Premiamo una volta F5 per uscire da SI e ritorna sullo schermo una seconda volta. (Perché? Perché la prima volta che poppa, il programma prende il nome (i char) che abbiamo immesso; la seconda volta poppa perché il programma prende il codice da noi inserito, ed é questa parte di codice che ci interessa.) ... SI ritorna la seconda volta. Ora premiamo una volta F11 per ritornare dalla call e premiamo F12, per spostarci al processo del programma in questione, un paio di volte fino ad arrivare li, dove c'é la scritta verde -BMP2ICO!CODE+00032141- sulla linea intermedia in basso. Dopo tutta questa esplicazione (forse in parte inutile o scontata) approdiamo qui:

```
00433146 5E                    pop esi              <--- noi arriviamo qua
00433147 5B                    pop ebx
00433148 C3                    ret                  <--- qui abbiamo un return cioé ci spostiamo
                                                         in un'altra parte di codice
```

Iniziamo a steppare ogni singola istruzione con F10 e e passiamo i vari return (ret). Quando ne abbiamo passati 6 arriviamo nel pezzo di codice che ci interessa:

```
00462627 8D4DF4                lea ecx, dword ptr [ebp-0C]    <-- arriviamo qua
0046262A BAA8274600            mov edx, 004627A8
0046262F 8B45FC                mov eax, dword ptr [ebp-04]
00462632 E865D0FFFF            call 0045F69C                  <-- calcola il seriale
00462637 8B45F4                mov eax, dword ptr [ebp-0C]    <-- metti un determinato valore in eax
0046263A 8B55F8                mov edx, dword ptr [ebp-08]    <-- metti un determinato valore in edx
0046263D E88A15FAFF            call 00403BCC                  <-- fai un chiamata a quell'indirizzo
00462642 7426                  je 0046266A
```

Esaminando i punti piú importanti di questo pezzo notiamo che all'indirizzo 00462637 viene messo un valore in eax; é sempre buona regola dumpare (cioé vedere quali valori ci sono nei registri) tutto il possibile. Quando abbiamo steppato fino a 0046263D vediamo cosa c'é nei registri: in eax c'é un valore assai sospetto, chissá forse il seriale. E controlliamo anche edx e vediamo nella data window di SI il seriale da noi immesso, ovvero 123456. Avanti vediamo che c'é un je (jump if equal), ma prima una call!! Posizioniamoci sulla call all'indirizzo 0046263D e premiamo F8 (esegui istruzione) e arriviamo alla seguente locazione:

```
00403BCC 53                    push ebx           <-- arriviamo qua
00403BCD 56                    push esi
00403BCE 57                    push edi
00403BCF 89C6                  mov esi, eax       <-- ricordate cosa c'era in eax? lo copia in esi
00403BD1 89D7                  mov edi, edx       <-- idem per edx che viene copiato in edi
00403BD3 39D0                  cmp eax, edx       <-- qui compara (controlla) che eax e edx siano uguali
00403BD5 0F848F000000          je 00403C6A        <-- se sono uguali vai alla locazione 00403C6A, altrimenti
                                                      continua col codice
```

Scriviamoci su un foglio il contenuto di eax e proviamo a utilizzarlo come numero seriale, sempre con il nome occasus. Funziona! Che bello! Il primo tutorial da solo che bello.

Ho provato a fare il tutto anche con un altro nome, peró il codice cambia. Suppongo che parta tutto dalla call all'indirizzo 00462632. Se Quequero, AndreaGeddon o qualsiasi altra persona in grado di aiutarmi sia disposta ad aiutarmi, (o che abbia VOGLIA), a capire il codice da quella call in poi ne sarei infinitamente grato. Grazie per la lettura a tutti e ciauz.

Ps.: Se disinstallate il programma e lo reinstallate per fare delle prove, dobbiamo andare in regedit e poi cancellare la seguente stringa: HKEYCurrentUser-->Software-->QTam.

Note finali

Vorrei salutare assolutamente per prima Quequero (credo sia il primo a leggere questo tute), AndreaGeddon, evilcry, active85k e qualsiasi persona che abbia scritto tutorials su SoftIce, Assembly, Cracking, Reversing. Grazie a tutti

Disclaimer

Vorrei ricordare che il software va comprato e non rubato, dovete registrare il vostro prodotto dopo il periodo di valutazione. Non mi ritengo responsabile per eventuali danni causati al vostro computer determinati dall'uso improprio di questo tutorial. Questo documento è stato scritto per invogliare il consumatore a registrare legalmente i propri programmi, e non a fargli fare uso dei tantissimi file crack presenti in rete, infatti tale documento aiuta a comprendere lo sforzo immane che ogni singolo programmatore ha dovuto portare avanti per fornire ai rispettivi consumatori i migliori prodotti possibili.

Noi reversiamo al solo scopo informativo e di miglioramento del linguaggio Assembly.
