Cours de Cracking

(8ième Partie)

Mon objectif : récupérer le serial de winzip 7.0

1/ Les logiciels utiles pour ce cours

-> Le programme à craquer : **Start Clean v1.2**
-> Le débugger : **Winzip 7.0**

2/ Récupérer le serial

Dans ce cours nous allons expliquer comment cracker Winzip 7.0, programme de compression très utilisé et quasi indispensable surtout sur le net. Nous allons utiliser dans ce cours la méthode qui permet de trouver un serial qui corresponde à notre nom.

-> Lancez Winzip et tout de suite si vous avez une version shareware, un beau nag-screen s'affiche avec les boutons *"Quit", "I Agree", "Ordering Info", "View Evaluation Licence"* et *"Enter Registration Code"*... Il s'agit du dernier qui nous intéresse, quand vous cliquez dessus la boite de dialogue permettant de s'enregistrer s'affiche. Il y a deux champs , l'un pour le nom et l'autre pour le code.

-> Mettez votre nom, pour moi ThE CrAzY SquirreL et un serial bidon, 12345 et cliquez sur OK et une boite de dialogue s'affiche avec le message 'Incomplete or incorrect information'. Donc le programme a comparé notre code par rapport au bon code et nous informe que 12345 n'est pas le bon code pour notre nom.

Nous allons donc essayer de choper le bon serial en interrompant l'éxécution du programme lorsqu'il lit notre nom/serial. Pour cela il faut poser un breakpoint sous SoftIce, les deux fonctions les plus couramment utilisées dans la lecture d'un champs sont GetWindowTextA et GetDlgItemTextA.

-> Donc allez sous SoftIce (à l'aide de Ctrl-D) tapez bpx GetDlgItemTextA puis bpx GetWindowTextA.
-> Quittez SoftIce toujours avec Ctrl-D, et mettez un nom (ThE CrAzY SquirreL) et un serial bidon (12345).
-> Ensuite appuyez sur Ok.

Et là on se retrouve immédiatement sous SoftIce.

-> Faites F12 pour sortir de la fonction pour voir si Winzip lit notre nom et effectivement on voit EAX=12.

Mais qu'est que ca pourrais bien être ? Il faut savoir que les valeur des registres sont héxadécimales et non décimals, donc 12=18 en décimal... Et il se trouve que 18 est longueur de mon nom! Et la ligne sur laquelle nous emène SoftIce est PUSH EBX...
Faites donc "d EBX" et dans la fenêtre Data on apercoit notre nom !

-> Faites F12 pour que SoftIce continue son éxécution et lise notre serial *(car pour l'instant, on est dans la routine qui lit la zone de saisie contenant notre nom...)*.

Là, EAX=5 c'est à dire la longueur de notre code.Et la ligne sur laquelle on se trouve est PUSH ESI...Ainsi, comme précédemment, faites "d esi" et on voit notre serial bidon.

Et maintenant qu'est qu'on fait ?...On peut supposer que Winzip va générer le serial valide et le comparer au notre et s'il sont différents nous envoie la boite de dialogue *'Incomplete or ...'*On peut donc supposer qu'il va comparer à un moment ou à un autre notre serial (12345) au bon...

-> On va donc poser un bpm (arrêt sur une zone de la mémoire) sur 12345.Pour cela il nous faut l'adresse à laquelle se trouve le serial, donc quand Winzip lit notre serial et que vous faites d esi notez l'adresse à laquelle il se trouve. [Smeita: je rappelle que pour trouver l'adresse, il suffit de regarder sur la meme ligne que 12345, mais tout a gauche...(la ou il y a xxx:xxxxx sur mon beau dessin :))...].Dans mon cas, j'ai 47D958. La commande à taper est donc bpm 47D958 (notez que cette adresse n'est pas forcement la meme chez vous !!).

-> Ensuite faites F5 (pareil que Ctrl+D...) pour que Winzip continue son éxécution jusqu'à ce qu'il éxécute notre bpm. Winzip fais plusieurs fois référence à cette zone de la mémoire, en effet il est entrain de créer le bon serial par rapport à notre nom.

-> On fait plusieurs fois F5 (ou Ctrl+D...), cinq fois éxactement et là nous arrivons sur des lignes de code interressantes...:

```
MOV AL, [ESI] => met ESI dans AL
INC ESI
MOV AH, [EDI] => met EDI dans AH
INC EDI
CMP AH,AL     => compare AL et AH...(c'est pour ca que c'est intéressant...)
```

Faites d esi et vous on voit notre serial bidon dans la fenêtre des données.
On peut donc supposer que EDI contient le bon serial, faites d edi et vous voyez A24A388C :))

On peut constater que si on continue à faire F5 (ou Ctrl+D, c'est pareil...), on tombe de nouveau sur les mêmes lignes que précédemment mais que le serial est différent mais également valide. Peut être qu'il d'agit d'un sérial d'une version antérieur...(on obtient 21645132)

Donc pour ThE CrAzY SquirreL le serial est A24A388C ou 21645132 !!

-> Quittez SoftIce en enlevant d'abord les breakpoints (en faisant bc * puis F5) et rentrez les informations obtenues (c'est a dire le serial...) dans Winzip...

Maintenant Winzip est enregistré !

[interlude de Smeita...]
Bon, vous avez vu ?? C'est pas si dur !! En plus, ce qu'est cool avec SoftIce, c'est qu'y a pas de modif' en hexa ! ;). Maintenant, entrainez vous un peu avec des sharewares a deux balles, et puis vous deviendrez vite un virtuose de SoftIce :))...Quand aux prochains cours (les 'Flash Tuts'), il vont reprendre notre bon vieux WinDASM, histoire de compléter vos connaissances...Il sera peut être plus difficile de les mettre en pratique, car vous ne disposerez pas des logiciels sous la main...mais bon, lisez les quand même, il finiront peut-être de vous eclaircir sur l'utilisation de WinDASm :)
PS: Au fait, pour ceux qu'on toujours pas compris, Ctrl+D c'est pareil que F5 :)
[...Fin d'interlude...]