Cours de Cracking

(7ième Partie)

Mon objectif : récupérer le serial de startClean 1.2 avec softice

1/ Les logiciels utiles pour ce cours

-> Le programme à craquer : **Start Clean v1.2**
-> Le débugger : **Softice 4.05**

2/ Les protections

-> Registration par code
-> Un Nagscreen au lancement

3/ Récupérer le serial

-> Commencez par installer Start Clean (et ouais ca aide si on veut le cracker non ?).

Vous allez voir que choper un serial pour StartClean est très, mais très facile... Mais cela constitue, tout de même, une bonne introduction à l'utilisation de SoftIce. Commencons...

-> Lancez Start Clean
-> Lorsque le nag apparaît, cliquez sur Register...
-> Renseignez les champs : mettez votre nom (par exmple CrAzY SquirreL) et un serial bidon 12345.
-> Appuyez sur Ok

Une boite de dialogue apparait avec 'Incorrect code!'. Et oui, on ne chope pas un serial valable avec la chance, vous croyez quoi !

-> Appuyez sur Ok dans la boîte de dialogue "Incorrect code!".
-> Maintenant allez sous SoftIce en tapant CTRL D
-> En bas de la fenêtre de Softice tapez dans la zone de saisie bpx GetdlgitemtextA (Smeita: cette commande de SoftIce permet de poser un point d'arret sur les "objets" de la fenêtre où vous rentrez le nom et le numéro de série.. . Comme ca, dès que StarClean va regarder ce que vous avez rentré comme serial,

on va arriver dans SoftIce et on pourra suivre les opération pas-a-pas :)
-> Sortez de SoftIce par CTRL D
-> Appuyez sur OK.

Voilà vous êtes sous SoftIce (Smeita: grâce au bpx !).Si ce n'est pas le cas enlevez le ; devant EXP= \SystemRoot\System32\user32.dll dans le fichier de configuration de softice C:\WINDOWS\system32\drivers \winice.dat et redémarrez votre machine (cette action vous autorise à poser un point d'arrêt sur l'APi user32. dll qui contient la fonction Getdlgitemtexta).

-> Faites ensuite F12 pour sortir du call (la fonction appelée) et revenir à la fonction appelante.
-> Là, regardez dans la fenêtre des registres (tout en haut...), et plus spécialement là où il y a marqué "EAX".
(Smeita: dans la fenêtre des registres, vous pouvez voir les valeur de tout les registres memoire à un instant donné. Tous les registres sont intéressant à observer. En fait, il est très utile de les regarder à chaque pas que l'on effectue sous SoftIce.C'est indispensable pour trouver un serial...Et n'oubliez pas que les registres sont en hexadécimal !!).

La valeur de EAX est de 0000000E. Tiens, bizarre ca ne serait pas la longueur de notre nom ? Et oui 0E en décimal ca donne 14 (y'a 14 lettre dans CrAzY SquirreL !!). Si vous voulez convertir une valeur hexadécimale en décimale tapez ? valeur_hexa ou ? nom_du_registre.

[interlude de Smeita / Pifoman]
La fenêtre des données est la partie de SoftIce où il y a des trucs du style de ce qu'on peut voir dans un editeur hexadecimal et d nom_du_registre affiche les infos contenu a l'adresse du registre. C'est souvent grâce a cette commande qu'on peut trouver un serial.)

La zone de saisie que l'on trace pour l'instant semble être celui où l'on a rentré notre nom. En effet, chaque zone de saisie est traitée l'une apres l'autre. De façon générale, l'ordre dans lequel elles sont traitées coïncide souvent avec l'ordre qu'elles ont dans la fenêtre de haut en bas. Par exemple, dans StarClean, on a d'abord le nom et ensuite le code. Donc il est fort probable que l'on attérisse d'abord sur la première zone (le nom) puis sur la seconde (le serial). Je rappelle que bpx getdlgitemtexta permet d'arriver sur SoftIce dès que StartClean appelle une zone de saisie en particulier dès que le fonction GetDlgItemTextA est invoquée par le programme.
[Fin de l'interlude]

Tout le reste du cours du cours je l'ai complètement réécrit moi pifoman.Il y a avait plein de lignes de code qui ne correspondait pas à la réalité du code affiché dans softice.En plus certaines parties paraissaient assez flou voire enigmatiques au niveau des explications.

-> On fait F5 pour continuer l'exécution du programme. Aussitôt Softice resurgit. StartClean traite cette fois-ci le serial que l'on a entré tout à l'heure dans la 2ième zone de texte de la boîte d'enregistrement.On relève en effet dans softice la valeur du registre **EAX** qui vaut cette fois-ci 00000005.Le code 05 doit vous faire penser à la longueur du serial entré qui est je le rappelle est 12345. Voici le code assembleur que vous voyez à ce moment là dans softice :

```
001B:004011C5       FFD6              call    esi
001B:004011C7       6830604000        push    00406030
001B:004011CC       6830614000        push    00406130
```

Si on fait d 00406030 dans la fenêtre de saisie de Softice on voit apparaître le bon serial dans la zone de données de softice(en haut en dessous de la 1ière ligne verte). Il vaut 2730-26346-1673-333. Si vous faites d 00406130 vous voyez apparaître dans cette même zone de données le nom entré initialement à savoir CrAzY SquirreL.Plus précisément l'adresse 00406130 contient le C de CrAzY SquirreL, 00406131 contient le r de CrAzY SquirreL et ainsi de suite jusqu'à la fin du nom.Voici le contenu de la zone de données une fois tapé la commande d 00406030 (suivi de entrée)

```
0023:0040630       32 37 33 30 2D 32 36 33 - 34 36 2D 31 36 37 33 2D      2730-26346-1673-
0023:0040640       33 33 33 30 00 00  00 00 - 00 00 00 00 00 00 00 00      333 . . . . . .
```

[interlude de Pifoman]
Il y en a qui doivent se dire "Comment on sait qu'il faut faire d 00406030 ou autre chose ?". Bon, dans ce genre de cas, après avoir appuyé sur F12, on arrive sur une instruction du style push adresse. Il suffit alors de faire d adresse avec adresse qui vaut dans notre exemple 00406030 ou bien 00406130.

Certains doivent aussi se demander ce que signifie les couleurs employées.
-> Le bleu ciel désigne une adresse.
-> Le rouge du code hexadécimal.
-> Le jaune désigne du texte
-> Le orange désigne du code assembleur
[Fin d'interlude]

Bon a trouvé le serial.C'est ce q'uon voulait.On peut aller plus loin et analyser l'endroit où craquer le programme.

On va poser un bpm (breakpoint on memory access <=> un point d'arrêt sur une zone de la mémoire) sur l'adresse 00406030 (qui contient le vrai serial).Comme ça dès que le programme va comparer notre serial au bon on pourra essayer de voir comment il fait pour savoir s'il doit s'enregistrer ou non.Mais pour poser un bpm il faut une adresse (l'instruction bpm prend pour paramètre une adresse <=> bpm adresse. Onn prend donc l'adresse qui contient 2730-26346-1673-333 à savoir 00406030.

Attention : l'adresse n'est pas la même tout le temps, ne vous étonnez pas si c'est different chez vous.

-> On tape donc bpm 406030 (c'est pareil que bpm 00406030)
-> On fait F5 ou CTRL D (pour laisser le programme continuer son éxécution).
-> Sitôt sorti de SoftIce on y retourne, et on voit alors qu'on est dans user32!wvsprintfA (pas intéressant).
-> On refait 5 fois F5 ou CTRL D.A chaque fois on tombe dans Kernel32!lstrcatA (pas intéressant).
-> Si on refait une fois F5 on tombe dans Kernel32!CompareStringA (regardez la 2 ième ligne verte en partant du bas dans Softice).
-> Comme la fonction compareStringA est généralement impliquée dans la comparaison de chaînes on fait

F12 4 fois pour arriver dans Start Clean.

A ce moment là vous avez le code suivant dans softice.Le cuseur d'exécution est alors positionné sur la prochaine instruction à exécuter qui se trouve à l'adresse 004011E9.

```
:004011DD        50                  push eax                    => met le contenut de EAX = 12345 sur la pile
:004011DE        6830604000          push 00406030               => met l'adresse de 2730-26346-1673-333 sur la pile
:004011E3        FF1520924000        Call KERNEL32!lstrcmp       => appelle la fonction de comparaison lstrcmp
:004011E9        85C0                test eax, eax               => eax = 00000001 (12345 != 2730-26346-1673-333)
:004011EB        0F8580000000        jne 00401271                => comme les 2 serials sont différents saut 00401271
```

Sur la ligne d'adresse 004011E9 si vous faites F10 pour exécuter cette ligne vous arrivez sur l'adresse 004011EB.

-> Tapez r fl z (reverse flag zero) suivi de entrée pour inverser (ici annuler) le saut en 004011EB et faire croire à StartClean que les 2 chaînes 12345 et 2730-26346-1673-333 sont identiques.
-> Tapez bc* (breakpoint clear) pour effacer tous les breakpoints posés.
-> F5 pour repasser sous windows.

Bravo ! StartClean est une nouvelle fois cracké !

[interlude de Smeita...]
Bon, maintenant, je crois qu'on a suffisament cracké StartClean :)) Les prochains cours ne s'attaqueront plus à ce logiciel en particulier :) Par exemple, dans le cours qui suit, vous allez apprendre a choper un serial pour Winzip 7.0 ! Comme ca, au moins, vous pourrez flamber devant les copains ;)
[Fin d'interlude]