Cracking Elite Software

SOFTCRACK.4

Softcrack n0: 4.

Ecrit par The Softman.
Paris, 16 octobre 1984.

Ce petit cours de déplombage est destiné uniquement aux personnes qui sont intéressés par le déplombage. Ceux qui ne sont pas concernés n'ont qu'a utiliser et/ou faire ce qu'ils veulent.

Avant toute chose,permettez-nous de mettre les points sur les i.
Les logiciels déprotégés par notre groupe "Cracking Elite Software" ne sont nullement destinés à des buts lucratifs :ceci est une de nos règles d'or. Si vous etes contre ceci, allez donc voir Ccb qui Vous vendra ce qui ne leur appartient pas de droit; et en plus,ils vous prendront pour des "pigeons".Voilà, maintenant à vous de décider... C.E.S précise que les programmes déprotégés ayant notre label ne sont destinés qu'à des usages personnels et non pas (point très important) à des usages professionnels ou commercials.
Que les sociétés qui ont besoin d'un programme s'adressent directement aux détaillants de logiciels.

Maintenant,abordons si vous le voulez bien, le problème de déplombage de Papyrus comme un "hobby" et surtout comme un sport intellectuel tel que les mots croisés ou les échecs.

Après un quart d'heure de recherche à l'aide d'un disk-editor tel que celui de Nibbles Away, nous avons trouvé la routine qui vérifie que la disquette Papyrus que vous utilisez est un original ou pas. Elle est situé sur la piste $10.Attendons un peu; ne brulons pas les étapes. Pour trouver cette routine, nous avons utiliser une technique très simple.Il s'agit de rechercher une chaine d'octets qui met le drive en position de lecture.
Cette séquence est : 8C C0.
Ceux qui ne savent pas ce que c'est n'ont qu'à se reporter à Ben.Ap.Dos.
Ayant lister la routine, nous savons ce que la protection vérifie.

Mais après modification et rebootage du programme, on s'est aperçu qu'une routine vérifie que rien n'a été changé dans celle de protection.Cette vérification se fait à l'aide de l'instruction EOR:c'est à dire "faire la somme de tous les octets de la routine de protection.Pour résoudre ce problème,il y a 2 méthodes:1)recherche sur le disque, la routine de checsum.2)interchanger de telle façon que la somme des octets de

la routine de protection soit tjs la
même. Pour gagner du temps, nous avons
utiliser la seconde méthode.

Donc,en bref,voici ce qu'il faut faire:

1) Mettre un write-protect sur l'original pour éviter les erreurs de manipulations qui pourraient endommager la disquette.(Ceci est une des règres de stricte rigueur,si vous voulez déprotéger une disquette.)
2) Papyrus est copyable avec un pro-
gramme de copie standard tel que Copya
ou Disk muncher...Mais il ne marchera
pas encore à cause de la protection.
3) Ensuite,bootez la disquette Micmac
and The Softman avec le Speedy Boot et choisir Nibbles Away
4)Sous Nibbles,entrez en mode "sector
editor",lire piste $10,sector $09.
5)changer la $46-ième octet de:
-C9 (valeur originale)
en
-A9.(nouvelle valeur)
Ré-écrire le secteur sur la disquette que vous venez de copier.Ne jamais écrire sur l'original.
6) Puis,lire piste $10 secteur $0A.
7) Changer la $2D-ième octet de:
-00 (valeur originale)
en
-20 (valeur entrée)
Ré-écrire le secteur.
Comme vous avez constaté,nous avons
modifié ces 2 secteurs en préservant
la somme totale des octets d'origine.
Plus exactement, $C9+$00=$C9 (somme d'origine) et $A9+$20=$C9 (tjs même somme).
Cette méthode signifie:
-quelque soit le résultat final que donnera la routine de protection,le bon branchement se fera tjs comme si c'est une disquette originale (cela veut dire que la disquette déprotégée est compatible à 100% avec l'original.
Voilà.Maintenant, vous avez un Papyrus déprotégé et bootable.
Testez en le bootant comme si c'est l'original.
Si la disquette se scratche,c'est que
vous avez fait une erreur dans les modifications ci-dessus.
Si elle marche, bravo !!!
Ah!! Encore une chose:rangez votre original dans un coffre-fort ou dans un endroit sec et sans poussière;et n'utilisez que la version déprotégée. (Un original coûte très cher et son dépannage vous ferait perdre du temps: le temps, c'est de l'argent.)

Softcrack #04 écrit par

The Softman.

Cracking Elite Software.
Paris, 16 novembre 1984.

FIN de cet épisode.

Merci de nous lire. A suivre...