CRACK blob v1.0

Un tuto avec une approche un peu différente de celui du site flashtro
Merci de se reporter au crack de bad dudes pour éviter les explications redondantes

Quand on fait une copie du disque original (ipf file : CAPS 1202), on retrouve une erreur sur le premier track, vraisemblablement une protection de type RNC

Lorsqu'on boot sur le disque copié, le chargement s'arrête après quelques temps sur la fenêtre amigados, après un test du track 1 (le lecteur fait un bruit bizarre) alors qu'avec le disque original, le logo core design apparait et le jeu continue à charger.

```
Search from: 000000 to: C80000
014C1C  014C2C  C0986E  C0987E
Ready.
d 14c1c
~014C1C PEA     14C28(PC)
~014C20 MOVE.L  (A7)+,00000010
~014C26 ILLEGAL
~014C28 MOVEM.L D0-D7/A0-A7,-(A7)
~014C2C PEA     14C48(PC)
~014C30 MOVE.L  (A7)+,00000010
~014C36 MOVEA.L A7,A0
~014C38 LINEF
~014C3A ORI.B   #40,D2

d c0986e
~C0986E PEA     C0987A(PC)
~C09872 MOVE.L  (A7)+,00000010
~C09878 ILLEGAL
~C0987A MOVEM.L D0-D7/A0-A7,-(A7)
~C0987E PEA     C0989A(PC)
~C09882 MOVE.L  (A7)+,00000010
~C09888 MOVEA.L A7,A0
~C0988A LINEF
_
```

Si on rentre dans l'AR après un certain temps de chargement mais avant le test du track et qu'on cherche du code copylock grâce à F 48 7A, on tombe sur 2 fois 2 adresses espacées de $10 bytes, ce qui est typique d'un copylock.

Le code aux 2 adresses est identique
→ Le premier code semble commencer en $141C8
→ Le deuxième en $C0986A
(on retrouve le début de ces codes en désassemblant vers le haut ou en utilisant les commandes M et N de l'AR)

Lorsqu'on fait un FA 141C8 et un FA C0986A, on voit que la première adresse n'est utilisée nulle part alors que la 2ème est utilisée en $C0A150 donc le code de copylock exécuté par le programme est celui en $C0986A

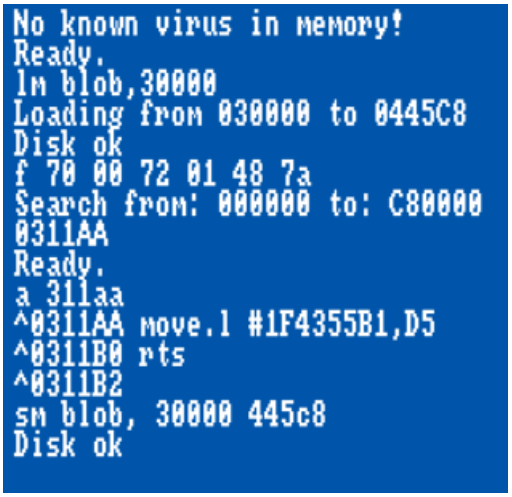
```
~C0A11E AND.L   #3F48EEC0,D5
~C0A124 AND.L   #5440EEC0,D4
~C0A12A AND.L   A1,D3
~C0A12C MOVE.W  #2230,-(A3)
~C0A130 ASR.?   #7,D0
~C0A132 ABCD.B  -(A6),-(A7)
~C0A134 SUBQ.B  #5,-111C(A0)
~C0A138 NOP
~C0A13A LEA     00C1A004,A1
~C0A140 CMP.L   (A1),D5
~C0A142 BNE     00C0A146
~C0A144 RTS
```

Examinons le code de ce copylock en désassemblant :
La plupart de ce code est du code crypté typique de copylock, mais on retrouve à la fin du code compréhensible en $C0A13A :
→ Le contenu de l'adresse $C1A004 est comparé au registre D5
→ S'ils ne sont pas égaux, on branche vers une routine cul de sac
→ Donc la clé renvoyée par le copylock se situe en D5

Il suffit de remettre le disk original, puis après un certain temps de chargement (mais avant le test du track) de modifier le code, par exemple en $C0A142 en insérant une boucle infinie (A C0A142 ..... BRA C0A142)
Puis on attend que le programme soit rentré dans la boucle infinie. A ce moment on examine le registre D5 qui nous renvoi le nombre magique : **1F 43 55 B1**

En faisant une recherche de ce nombre dans la mémoire (F 1F 43 55 B1), on ne le retrouve qu'en C1A004, y compris si on boot sur la copie de disquette, donc la seule chose a faire est de bypasser tout le copylock après avoir mis par sécurité le nombre magique dans D5.

Pour cela, comme on est sur une disquette amigaDOS standard (puisque la fenêtre amigados apparait lors du chargement), on recherche le fichier lancé au démarrage (en éditant la startup-sequence située dans le dossier S/), ce fichier s'appelle tout simplement blob.
On charge ce fichier dans la mémoire : LM blob, 30000
et on cherche les opcodes du début du copylock (F 70 00 72 01 48 7A), que l'on remplace par notre code (cf. ci-dessous)



Et voilà !

JEL 08/2018