La protection des disquettes selon Daniel Duffau (1ère partie)

Par André C.

Etat de la question

Récemment, je me suis intéressé au jeu MLUCH de Daniel Duffau, édité par le CEO. Ce jeu a été très peu diffusé : Dans la disquette trimestrielle de juin 1998 et dans la disquette CEO-soft2.

Il en a été très peu question dans le Ceo-Mag, mis à part l'article "Des trucs pour tricher n°HS 18" de Dominique P. (mag n°220, page 51), l'article "Réalisez vos cartouches PB5 (3)" d'André C. et Claude S. (mag n°99, pages 14-15) et enfin "MLUCH pour Super-Oric (mags n° 251 à 253 et 258).

Bref, je souhaitais revenir sur ce jeu que j'apprécie beaucoup et qui devrait faire l'objet d'un article et d'une disquette, dans les mois à venir.

Au cours de cette approche, je me suis penché sur la disquette CEO-soft2 (proposée par la section VPC en 1988). Et là, je suis tombé sur un os auquel j'aurais dû m'attendre, vu que j'y avais déjà été confronté avec la disquette CEO-soft1 (Willy, également de Daniel Duffau).

Ces disquettes font l'objet d'une protection anti-piratage pas piquée des hannetons. A l'époque le CEO vendait les softs dont il était éditeur.

A propos de Willy justement, je me rappelle que Jean B. m'a appris (quelques années plus tard) que Daniel avait fourni au club une disquette-clef permettant de copier les disquettes protégées par la méthode "DD" (la section VPC devait pouvoir dupliquer les softs à vendre).

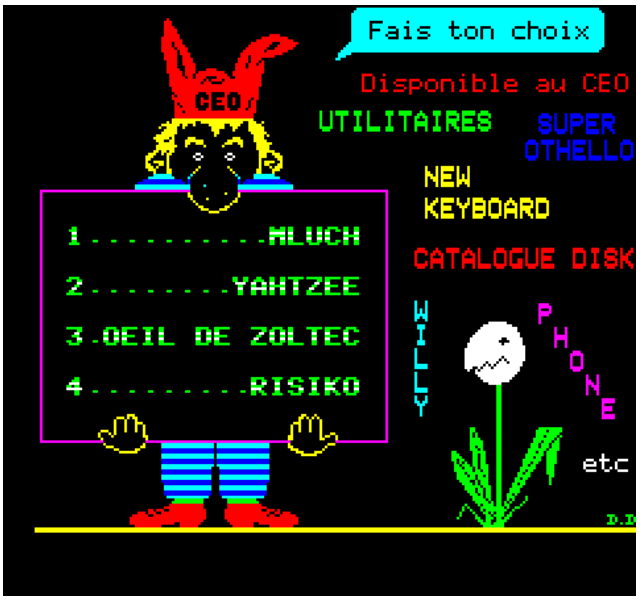
Entre temps, le CEO a ouvert gratuitement ses archives à tous ses membres et donc les disquettes "CEO-soft" sont disponibles... mais toujours pas copiables, car la disquette-clef a été perdue (enfin, très probablement pas, mais qui en a hérité?).

NB. Suite à ce problème, une méthode de copie de Willy a été publiée (Ceo-Mag n°138, page 27). Elle marche probablement pour les autres disquettes protégées "DD".

Notons qu'aucun des excellents programmes de Daniel Duffau (Willy, Mluch, Tetris, L'œil de Zoltec, 3D Graph, Bataille Navale, Pom'Oric, Robinson Crusoé, Mizar, etc.) n'est présent sur oric.org. Il faut le faire !

Une protection anti-piratage se traduit surtout par une diffusion confidentielle ! Dommage, car ce sont en général de très bons programmes.

Bref, je me suis penché sur cette protection "DD" (Daniel Duffau) en prenant comme exemple la



disquette CEO-soft2, sur laquelle figurent deux programmes dont je possède une version non-protégée (Mluch et Œil de Zoltec). Ça peut aider quand on sait ce qu'on doit obtenir à la fin...

La disquette CEO-soft2

La disquette se lance automatiquement. Après une page aux scrollings un peu pénible (voir animation initiale ci-dessus), on arrive enfin au menu qui nous propose :

1. Mluch (de Daniel Duffau)
2. Yahtzee (de Thomas Gempp)
3. Œil de Zoltec (de Daniel Duffau)
4. Risiko (de S. Regnault et V. Talvas)

Le lancement d'un de ces jeux est très très lent. On comprendra pourquoi plus loin. Si l'on fait un "soft reset" (bouton sous l'Oric ou touche F7 d'Euphoric) juste avant l'affichage du menu, on prend la main (la protection n'est pas encore en place !).

La commande : !DIR révèle la présence d'un seul fichier "CEO.COM" de 16 secteurs (trop petit pour être honnête) tandis que la disquette aurait une géométrie de 0 piste, 0 secteur, 0 secteur libre, 0 fichier ! Bigre, comme avec celle de Willy !

Un examen de la disquette CEO-soft 2 avec un éditeur hexadécimal montre qu'il s'agit d'une disquette formatée en 42 pistes de 17 secteurs, double face et que 360 secteurs sont occupés (c'est nettement plus que les 16 secteurs de "CEO.COM" !). La première face est donc quasiment pleine.

Pour terminer l'exploration sous Euphoric, je tente la commande : !CEO,V et j'obtiens :
8900 97DC 40 0000

En clair, fichier en langage machine (bloc de données), non auto, allant de #8900 à #97DC.

Bon, si malgré ce mode non auto, ça se lance au démarrage, il doit y avoir une commande dans INIST. Je tente cette commande, mais ça plante.

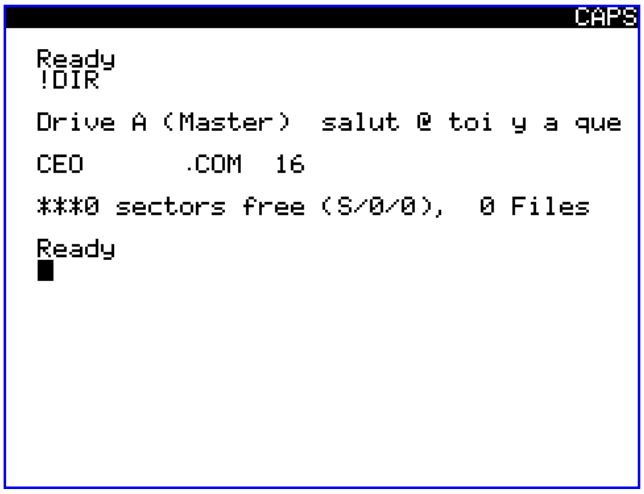
Comme j'ai un peu (et même beaucoup) de sang breton, je suis tenace, voire coriace, donc je passe à la commande : !CEO,N suivie de
CSAVE"CEO",A#8900,E#97DC

Je repars avec une disquette vierge, y copie l'excellent programme MONAC1.COM (le petit moniteur d'André Chénière). Je récupère ce fichier grâce à la commande : CLOAD"CEO" suivie d'un SAVE"CEOCOM",A#8900,E#97DC

Enfin, avec Monac1, j'analyse le contenu de ce bloc de données et je trouve :

- De 8900 à 8A62, langage machine se terminant par un JMP#977A.
- De 8A63 à 8FBF, données.
- De 8FC0 à 8FEF, copyright CEO.
- De 8FF0 à 9411, données.
- De 9412 à 975B, suite incohérente d'octets, surtout des #40 (une partie codée ?).
- De 975C à 9779, message "CEOSOFT 2 chargement en cours".
- De 977A à 97DC, langage machine qui se termine par un JMP#3F95

On remarquera, qu'en théorie, il n'y a rien en #3F95. En fait, outre les animations initiales, le programme CEO.COM met en place la suite, à savoir l'écran-menu proposant les 4 jeux et le programme qui permettra d'analyser la réponse de l'utilisateur, de charger le jeu choisi et de le lancer. Sous Sedoric, un appui sur la touche F9 après l'exécution de CEO.COM ou plus précisément pendant la boucle d'attende de l'écran-menu four-



nit le contenu de la mémoire. L'analyse de ce contenu par un éditeur hexadécimal révèle que la mémoire contient beaucoup plus de choses que le seul programme CEO.COM (#8900-#97DC) :

- De #0500 à #1FFF, la zone est vierge.
- De #2000 à #3F3F, une zone riche en #40. Tiens, sa longueur de #1F40 octets est la même que celle d'un écran Hires (#A000 à #BF3F). Je copie cette zone dans l'écran Hires et admire l'écran-menu ! Conclusion, ces données ont été copiées à partir de la disquette et stockées là en attente d'être utilisées.
- De #3F40 à # 3FCF, une zone de langage machine, que je baptise "LM1". Cette zone est pour le moins obscure et perturbée. Ce n'est que plus tard que j'en ai percé la protection. Nous verrons ça en temps et en heure. Notez que le JMP#3F95 signalé précédemment atterrit dans cette zone (d'ailleurs en plein "pataquès" obscur).
- De #3FD0 à #4044, encore une zone de langage machine, que je baptise "LM2". Cette zone est également pour le moins obscure. En fait, à cause de ce camouflage, je me suis laissé abuser car LM1 et LM2 ne font sans doute qu'un seul bloc en langage machine.
- De #4045 à #4083, une zone de données utilisées par le langage machine ci-dessus.
- De #4084 à #88FF, une zone de mémoire vierge.
- De #8900 à #97DC, une zone occupée par l'ancien programme CEO.COM, qui est toujours en place. Etonnant, on peut voir qu'une partie au moins de ce programme a été écrasée (ou décodée). Ainsi, de #92C4 à #97DC, on trouve maintenant un programme qui copie les données de #2000 à #3F3F (voir plus haut) dans l'écran Hires et déclenche l'affichage du menu. Il me semble que ce "MOVE" est bien inutilement compliqué, vu la place qu'il occupe, mais bon, c'est pas grave puisque ça marche. J'ai rebaptisé ce morceau LM4 par erreur, car je l'ai découvert en dernier (il était caché dans la zone CEO.COM). Mais en fait, ce n'est pas grave, car il est exécuté après LM3 !
- De #97DD à #97FF, des #FF sans intérêt.
- De #9800 à #9854, un programme (que j'ai baptisé LM3), qui lit des secteurs de la disquette et les copie en Ram. Il se termine par un JMP#92CB. C'est cette adresse qui a attiré mon attention sur LM4. Mais les octets de LM4 sont introuvables sur la disquette. Je suppose donc qu'entre le JMP#92CB et l'appel à LM4 (qui débute clairement en #92C4), il y a eu décodage, déplacement et écrasement.
- De #9855 à #98FF, une zone de mémoire vierge.
- De #9900 à #9BFF, le jeu de caractères normaux.
- De #9C00 à #9CFF, une zone de mémoire vierge.
- De #9D00 à #9EFF, le jeu de caractères alternés.
- De #9F00 à # 9FFF, une zone de mémoire vierge.
- De #A000 à # BF3F, écran Hires (le menu).
- De #BF40 à #BF67, des espaces (#20)
- De #BF68 à #BFDF, les 120 caractères des 3 dernières lignes de l'écran Text. On y voit le message "CEOSOFT 2 Chargement en cours". Et enfin ...
- De #BFE0 à #BFFF, une zone normalement vide, mais qui contient ici un bout de code machine que je ne suis pas arrivé à comprendre. Il faudra voir si je rencontre des JMP ou JSR appelant cette zone.

On voit donc que l'exécution du code de CEO.COM installe de nouvelles zones de code et se poursuit dans ces zones. Il est à noter que si l'on examine la disquette avec un éditeur hexadécimal, on n'y trouve aucun texte en clair. Or les 4 jeux proposés en comporte bel et bien (et même des quantités). Donc ce "lanceur" a pour objet réel de transcoder des octets présents sur la disquette (inévitablement présents dans des fichiers non répertoriés au directory) et à mettre à la bonne place en Ram le vrai programme résultant de ce transcodage.

Ceci implique, selon l'option choisie (de "1" à "4" au menu), de trouver les secteurs correspondants, d'en transcoder les octets, de charger le résultat en mémoire et de lancer l'exécution. Après avoir attaqué l'analyse de ce code en langage machine, je me suis rendu compte que c'était un travail de titan. J'ai peut-être du sang breton, mais je ne suis quand même pas Dominique P. !

De toute évidence, comme je suis un partisan du moindre effort, une autre solution m'a sauté aux yeux : La fonction Dump (touche F9) d'Euphoric devrait me livrer les programmes tout décodés ! Pas si simple sans doute, mais cela semble quand même plus facile et plus concret. Nous verrons ce que ça donne dans les prochains articles.

à suivre…