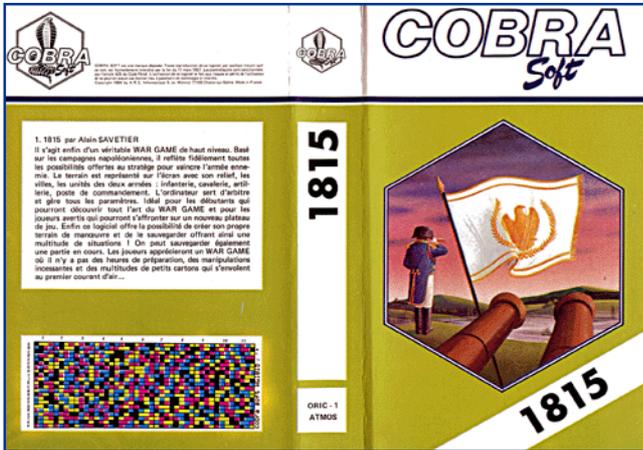


La Rom Déplombeuse 2

par André Chéramy et Claude Sittler

avec en démonstration la récupération de la cassette '1815' de Cobra Soft



Nous avons expérimenté les Roms 'Déplombeuse' (voir Ceo-Mag n°139 pages 6-8) et 'Suceuse' (voir Ceo-Mag n°140 pages 7-10) avec de nombreux programmes. Certains exemples ont déjà été publiés, par Thierry Bestel ou par nous-mêmes. Mais nous nous sommes cassé les dents sur '1815' de Cobra Soft.

Nous avons donc dû perfectionner notre stratégie. Car si la Rom 'Suceuse' permettait bien de récupérer tout ce qu'il y avait sur la cassette, il s'agissait d'un tel paquet de noeuds de protections qu'il était impossible de comprendre comment le programme était généré. Nous disons bien généré, car **le programme n'existe pas, tant que le 'paquet de noeuds' n'a pas été exécuté.** Nous vous ferons grâce de l'analyse de ce

paquet de noeuds, d'autant que nous n'en sommes pas venus à bout. Sachez seulement que les fichiers ne sont pas au format 'cassette Oric' et que le tout est bourré de pseudos fichiers destinés à égarer les déplombeurs. Mais nous sommes venus à bout de tout ça, grâce à la nouvelle Rom 'Déplombeuse 2', que nous allons vous décrire aujourd'hui. Cette Rom permet d'exécuter le programme '1815' sans perturber les protections et ensuite de sauver le programme généré.

ROMS 'DÉPLOMBEUSE' ET 'SUCEUSE'

La simplicité de la Rom 'Déplombeuse' (checksum #26E3) est désarmante ! La commande LET a été remplacée par une commande OLD, très utile avec les programmes incompatibles avec Sedoric comme '1815' (gestion de la page 4 par exemple). Le démarrage automatique des programmes chargés a été totalement neutralisé. La routine #FA14, qui 'teste' la mémoire, mais qui en fait l'écrase, a été supprimée et la place a été récupérée pour installer le code de la commande OLD. Utilisation de base : Suite à un CLOAD, on fait un SAVE"nom", pour un programme Basic ou un SAVE"nom", ADEEK(#2A9), EDEEK(#2AB), dans les autres cas. Avec encore quelques petits trucs, on arrive à résoudre la plupart des cas.

Le concept de la Rom 'Suceuse' (checksum #239F) est encore plus simple : lire la cassette octet par octet et stocker en mémoire sans chercher à comprendre. Il s'agit en fait d'une Rom 'Déplombeuse' dans laquelle la commande EDIT a été remplacée par une commande SUCE. Avec cette Rom, nous avons réussi à récupérer toutes les cassettes originales que nous avons testées. Toutes, sauf '1815' !

ELABORATION DE LA ROM 'DÉPLOMBEUSE 2'

Dans le cas précis de '1815', il fallait absolument exécuter le programme. Nous avons donc restauré l'exécution automatique des programmes au chargement et modifié le copyright (utile pour identifier la Rom en service) :

- 1) De #E8DB à #E8E7 et de #E8F6 à #E902 les octets d'origine ont été restaurés à la place des NOPs (#EA), qui avaient été installés dans la Rom 'Déplombeuse'.
- 2) En #EDAA le 'V1.1' a été modifié en 'V1.2' et en #F91A la couleur PAPER a été changée de #14 (bleu) à #12 (vert).

Deplombe.rom									
0000E8D0	B0CC	6020	51E6	ADAE	02F0	0E0A	EAEA	EAEA	...
0000E8E0	EAEA	EAEA	EAEA	EAEA	60AE	AB02	ADAC	0286	...
0000E8F0	9C85	9D20	5FC5	EAEA	EAEA	EAEA	EAEA	EAEA	...
0000E900	EAEA	EAEA	08C7	4CA8	C4A5	9AA4	98BD	A902	...
0000E910	8CAA	02A5	9CA4	9D8D	AB02	8CAC	0208	20B2	...

Deplombe2.ROM									
0000E8D0	B0CC	6020	51E6	ADAE	02F0	0EAD	AD02	F008	...
0000E8E0	ADB1	02EA	EA6C	A902	60AE	AB02	ADAC	0286	...
0000E8F0	9C85	9D20	5FC5	ADAD	02F0	08AD	B102	EAEA	...
0000E900	4C08	C720	08C7	4CA8	C4A5	9AA4	98BD	A902	...
0000E910	8CAA	02A5	9CA4	9D8D	AB02	8CAC	0208	20B2	...

Deplombe.rom									
0000ED90	5245	450A	0D00	4F52	4943	2044	4550	4C4F	REE...ORIC DEPLO
0000EDA0	4D42	4555	5345	2056	312E	3120	2020	0D0A	MBEUSE V1.1 ..
0000EDB0	6020	3139	3836	204D	4152	4741	5249	4E45	` 1986 MARGARINE

Deplombe2.ROM									
0000ED90	5245	450A	0D00	4F52	4943	2044	4550	4C4F	REE...ORIC DEPLO
0000EDA0	4D42	4555	5345	2056	312E	3220	2020	0D0A	MBEUSE V1.2 ..
0000EDB0	6020	3139	3836	204D	4152	4741	5249	4E45	` 1986 MARGARINE

Deplombe.rom									
0000F900	A950	8D7C	02A2	0C20	3802	68AA	6860	48A9	.P. ... 8.h.h'H.
0000F910	038D	6A02	A907	8D6C	02A9	148D	6B02	6860	..j...l..k.h'
0000F920	48AD	1F02	D005	A20B	20B2	F9A9	FE2D	6A02	H.....-j.

Deplombe2.ROM									
0000F900	A950	8D7C	02A2	0C20	3802	68AA	6860	48A9	.P. ... 8.h.h'H.
0000F910	038D	6A02	A907	8D6C	02A9	128D	6B02	6860	..j...l..k.h'
0000F920	48AD	1F02	D005	A20B	20B2	F9A9	FE2D	6A02	H.....-j.

La Rom résultante, sauvee sous le nom 'Deplombe2.rom' a une checksum de #1C60. Nous aurions pu tout aussi bien appliquer ces modifications sur la Rom 'Suceuse' et fabriquer un 'Suceuse 2'. Mais, selon le type de cassette à récupérer, il faudra disposer du CLOAD avec ou sans execution automatique, donc disposer de deux Roms et les inter changer (ce sera le cas pour '1815').

ESSAI DE LA ROM 'DÉPLOMBEUSE 2' AVEC LE PROGRAMME '1815'

La Casette '1815' comporte deux parties qui, après execution, se révéleront être des fichiers Basic :

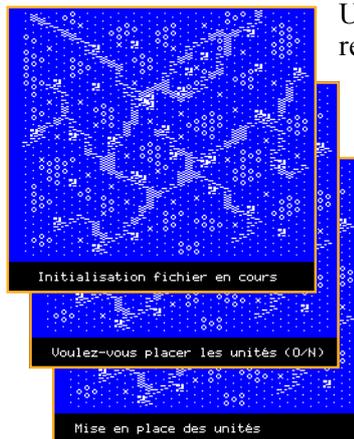
- 1) Une pseudo 'Présentation' (petite animation et musique) qui masque en fait la protection.
- 2) Le jeu proprement dit qui s'appuie sur ce qui a été installé par la première partie.

Dans le cas particulier de '1815', on ne peut pas travailler avec une configuration Microdisc, car la page 4 est utilisée. Il faut donc prévoir une cassette



vierge de bonne qualité pour sauvegarder le travail intermédiaire.

Après Chargement de la première partie avec CLOAD"", il faut laisser l'exécution courir, fournir le code de couleur à l'aide du tableau figurant sur la jaquette, admirer la 'présentation' (longuette), répondre 'N' à la question "Voulez-vous dessiner un nouveau terrain?". Enfin, le programme demande de remettre le magnétophone en marche pour charger la suite. C'est alors qu'il faut appuyer sur le bouton reset sous l'Oric. Faire OLD puis LIST, le programme est bien là ! Il suffit de le sauver par exemple avec un CSAVE"W1", après avoir mis la cassette vierge en place.



Un RUN relance le programme, il faut tout se retaper (notamment la 'présentation') et lorsque le programme demande de remettre le magnétophone en marche pour charger la suite, remettre en place la cassette originale et appuyer sur PLAY. Après encore beaucoup de patience, pendant que le programme dessine le champ de bataille, vous avez largement le temps d'appuyer sur le bouton reset sous l'Oric. Faire OLD puis LIST, le nouveau programme est bien là ! Il suffit de le sauver par exemple avec un CSAVE"W2", après avoir mis la cassette vierge en place.

Il faut ensuite remplacer la Rom 'Deplombe2' par la Rom 'Suceuse' (ou utiliser un Atmos Octocéphale), ajouter un Microdisc à la configuration et rebooter avec Sedoric 3.0 (rappel: les versions antérieures sont

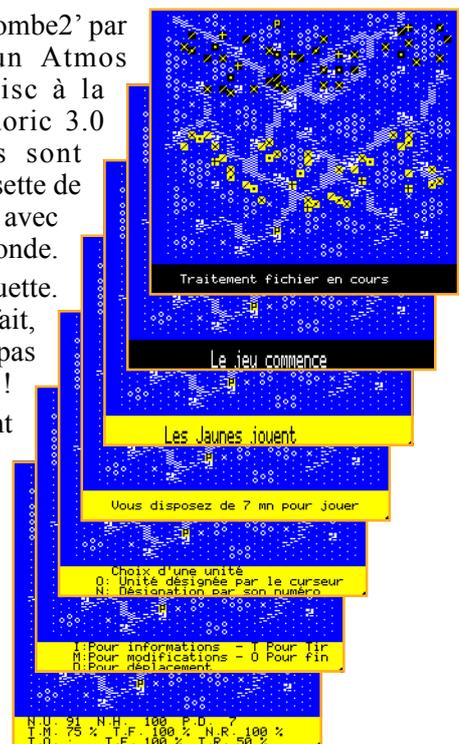
incompatibles avec les commandes 'cassette'). Il suffit de relire la cassette de sauvegarde avec des CLOAD"" (dont l'exécution est inhibée). On sauve avec SAVE"W1" pour la première partie, puis avec SAVE"W2" pour la seconde.

Nous disposons donc maintenant des deux parties de '1815' sur disquette. Le plus difficile est fait et avouez que ce n'était pas grand chose. En fait, nous avons beaucoup galéré avant d'en arriver là et nous ne rapportons pas toutes les péripéties de nos essais, mais seulement la recette qui marche !

Du calme, ce n'est pas encore fini : Ces deux parties de '1815' ne sont pas utilisables telles quelles, car le programme demande toujours un code de couleurs et utilise une table qui n'a pas été sauvee avec le Basic de la première partie. De plus la version actuelle est une version cassette qui n'est pas encore adaptée au fonctionnement sur disquette.

INHIBITION DE LA DEMANDE DU CODE DE COULEURS.

A propos de version, vous avez dit quelle version ? Il nous a fallu du temps pour réaliser un aspect insoupçonné du problème. Et un coup de chance : Grâce à Grégory, qui lors de la dernière visu nous a prêté sa cassette originale de 1815 (avec manuel) et en comparant avec les résultats obtenus avec la cassette originale que Luc nous avait envoyée, il y a déjà bien longtemps, nous avons pu comprendre et résoudre l'ensemble de nos problèmes d'adaptation.



Nous avons de notre coté une version disquette, qui ne marchait pas et qui était très différente de la version de Luc. Nous ne comprenions pas pourquoi ces différences avaient été introduites pour l'adaptation disquette.

Nous avons découvert que deux versions de '1815' ont été commercialisées. En comparant ces deux versions, nous avons vu que la plus ancienne était très boguée, (nous sommes désolés, Grégory). Pas de chance, c'est cette version boguée qui a servi de base à l'adaptation disquette (avec par ailleurs une grosse bogue supplémentaire pour faire bon poids). La seconde (tu as eu du pot, Luc) a été corrigée par Cobra Soft, (quoique nous nous posons encore des questions sur certains points, voir plus loin le problème des CSAVE sans CLOAD).

En comparant la version issue de la cassette de Luc et notre version disquette, nous avons compris comment contourner la demande du code de couleurs. Il suffisait de supprimer l'appel à un sous-programme.

Cette demande ne nous posait pas vraiment de problème. En effet, nous avions le code (tableau de couleurs sur les diverses jaquettes en notre possession). Mais la lenteur du lancement du programme (assommante présentation + demande du code + compilation des deux morceaux de programme Basic) était bien pénible et il nous a semblé que la suppression de cette demande de code apporterait un soulagement substantiel.

Nous avons donc facilement élaboré un fichier '1815.tap' qui marche parfaitement. Dans la première partie "W1", la ligne :

```
20006 GOSUB61000:HIRES:DOKE#306,#FFFF:INK0 a été remplacée par
20006 ::::::HIRES:DOKE#306,#FFFF:INK0 qui a la même longueur en octets (un octet pour le
token de GOSUB + 5 octets pour 61000, remplacés par 6 ':' supplémentaires. Remarquez que nous aurions pu
tout simplement supprimer la partie "GOSUB61000:", mais par principe, nous essayons de conserver la longueur
d'origine des programmes, car certains ne fonctionnent plus quand on modifie cette longueur.
```

Un petit SAVE"WG1" pour sauver cette mise à jour. Un CSAVE pour chacune des deux parties. Et il ne restait plus qu'à mettre bout à bout les deux fichiers 'tap' obtenus pour obtenir enfin le fichier '1815.tap' que vous trouverez sur la prochaine disquette trimestrielle.

ADAPTATION DE LA VERSION CASSETTE POUR UTILISATION SUR DISQUETTE.

En comparant la version de la cassette de Grégory et notre version disquette, nous avons vu ce qui avait été fait pour l'adaptation disquette. Outre le remplacement d'un CLOAD pour charger la deuxième partie, il y avait la ré-installation en #9600 d'une routine située à l'origine en page 4 (incompatibilité avec Sedoric).

Nous avons reporté ces modifications dans la version de Luc et obtenu une version disquette Sedoric qui marche. Voici le détail des modifications :

Pour la première partie "WG1" du programme, les lignes suivantes ont été modifiées :

```
9400 CLS:PRINT:PRINT"Remettez le magnétophone en marche.";
9440 CLOAD""
20004 CLS:PRINT:PRINT" ";CHR$(4);CHR$(27);"N Arrêtez le magnetophone SVP";
60020 CS=1024:DOKE757,CS
```

par :

```
9400 CLS:PRINT:PRINT"Préparez vous pour charger la suite.";
9440 WG2
20004 CLS:PRINT:PRINT" ";CHR$(4);CHR$(27);"N Chargement enfin terminé !!";
60020 CS=#9600:DOKE757,CS
```

Ici encore nous avons essayé de conserver la longueur du programme : Aux 3 octets du CLOAD"" correspondent les 3 octets de "WG2" pour le chargement de la deuxième partie. On sauve avec un SAVE"WG1",AUTO.

Pour la deuxième partie "W2", une ligne 0 a été ajoutée pour fixer le drapeau de fin du Basic :

```
0 DOKE#9C,#7961
```

On sauve avec un SAVE"WG2",AUTO. Le programme WG1 pourra donc charger WG2.

BILAN ET PERSPECTIVES

Nous avons aussi recherché s'il existait d'autres CLOAD, CSAVE, STORE ou RECALL et s'ils avaient été correctement adaptés. Nous avons été bien surpris : S'il existe encore un CSAVE"TERAIN" (avec une faute) et un CSAVE"PARTIE", il n'existe ni autre CLOAD, ni chargement direct de "TERAIN" et "PARTIE". Par ailleurs, nous n'avons trouvé ni STORE, ni RECALL. L'adaptation disquette est donc très limitée et pourrait encore être améliorée. Mais pour l'instant il est déjà possible de passer quelques heures à jouer avec le programme tel qu'il est...

Comme bon nombre d'Oriciens, nous avons toujours éprouvé une certaine frustration à ne pouvoir utiliser avec Euphoric certaines de nos cassettes originales. Avec ces deux Roms, ce ne devrait plus être un ennui pour personne et nous devrions pouvoir nous livrer avec nostalgie à tous les jeux qui ont fait jadis notre ravissement.