

9/9.8

Amstrad CPC et les virus ou comment manipuler les disquettes

NOTIONS SUR LES VIRUS

Il y a environ une dizaine d'années, parler d'un virus se trouvant dans votre ordinateur aurait fait rire votre interlocuteur qui vous aurait conseillé de consulter un psychiatre plutôt qu'un médecin généraliste. Par contre depuis quelques années, cette affirmation procure un grand frisson, et a en général pour effet de vous bloquer l'accès de tout ordinateur, de peur de la contagion, par vos disquettes, bien entendu.

Mais rassurez-vous, tout d'abord, les virus informatiques n'ont aucun rapport avec les virus biologiques que nous connaissons en médecine humaine ou animale : ce sont des entités programmées qui ont certains effets sur les programmes ou matériels informatiques. Donc pas de risque de les attraper en posant les mains sur un clavier !...

Ensuite, il n'existe à notre connaissance aucun virus sur CPC.

Définition du virus

Aucune définition officielle des virus n'a actuellement été donnée, mais sont considérés comme tels les programmes qui modifient plusieurs logiciels (programmes) en s'insérant à l'intérieur de ceux-ci, ne « contaminent » pas un logiciel qui est déjà atteint et/ou se multiplient pour se propager le plus possible.

Pourquoi pas sur CPC ?

Les virus ne sont pas apparus sur CPC, car la majorité des utilisateurs de CPC n'utilisent pas le système d'exploitation livré avec celui-ci : CP/M.

De plus il existe peu de virus écrits sous CP/M, et uniquement sur les gros systèmes, car la mise au point sous CP/M est plus fastidieuse que sous MS-DOS, de plus l'éventail des utilisateurs tend à diminuer rapidement.

Dernière et probablement la plus contraignante des particularités du CPC pour les virus extrêmement « virulents », le CPC ne possède pas de mémoire sauvegardée, dans laquelle il peut se loger pour infecter une disquette après extinction de celui-ci.

Les virus et la loi

Avant la généralisation des programmes virus, la loi française accusait un vide juridique concernant l'activité spécifique des programmeurs de virus. Ce n'est qu'en 1986 qu'apparut une proposition de loi, proposée par M. J. Godfrain, qui aboutit à un texte de loi en 1988.

Ce texte dans ses grandes lignes, permettait de sanctionner les délits commis par l'accès en fraude à un système informatique, les falsifications, destructions et dommages causés aux informations (programmes ou données) et matériels. Les peines prévues en cas d'infraction vont de l'amende relativement conséquente jusque l'emprisonnement quelquefois durable selon le préjudice commis.

LE VIRUS ANTIVOL

Un procédé tentant

Il est par contre tentant pour les concepteurs de logiciel d'utiliser le programme virus pour protéger leurs logiciels contre la copie illégale, par exemple en effaçant une copie du programme initial.

Hélas, ou heureusement (pour des raisons autres que la copie – car on ne maîtrise pas forcément les dérives qui peuvent être effectuées par un virus), cette méthode est répréhensible car elle peut modifier, ou au pire détruire des fichiers qui sont étrangers au programme initial.

Simulation d'un virus

Il n'est nullement l'intention ici de vous proposer un programme de virus, mais de simuler l'apparition de celui-ci dans un logiciel et ainsi de provoquer une frayeur chez l'utilisateur du programme de votre conception, de quoi réaliser une bonne blague... mais nous verrons plus loin en quoi consiste notre simulation de virus (ménageons votre curiosité).

Nous introduirons ce virus sous forme d'une instruction RSX, et nous profiterons de l'occasion pour ajouter quelques instructions de manipulation de lecteur de disquette.

Les nouvelles instructions et le virus

I DISKON

Cette instruction permet de mettre en route les lecteurs de disquette. Elle peut être utile lorsque vous effectuez régulièrement des accès à la disquette, car elle permet de limiter les temps d'attente de la vitesse optimale de travail. Elle sera donc à exécuter durant la préparation de données, un peu avant la sauvegarde, ou le chargement.

I DISKOFF

Cette instruction arrête les moteurs des lecteurs de disquette.

I DISKFIND

Cette instruction, dont la syntaxe exacte est :

I DISKFIND, lecteur, @variable%

permet de connaître, en ayant défini la variable `variable%` auparavant, si une disquette est présente dans un lecteur donné.

La valeur `lecteur` sera égale à 0 pour le lecteur **A**, et à 1 pour le lecteur **B**. L'instruction rendra la valeur 0 dans `variable%`, si aucune disquette n'y est présente, et 1 dans le cas contraire.

Ainsi le programme suivant :

```
10 variable% = 0
20 I DISKFIND, 0, @variable%
30 IF variable% = 1 THEN GOTO 70
40 PRINT « Introduisez une disquette...
      et appuyez sur une touche »
50 CALL &BB06
60 GOTO 20
70 suite du programme
```

permettra d'attendre l'insertion d'une disquette dans le lecteur **A** sans afficher l'affreux message de l'AMSDOS :

```
Drive A : Disc Missing
Retry, Ignore or Cancel ?
```

I DISKWR

Cette instruction de syntaxe proche de la précédente permet de déterminer si la disquette dans un lecteur précisé est protégée ou non contre l'écriture en entrant :

I DISKWR, lecteur, variable%

Le lecteur **A** sera aussi codé par 0 et le **B** par 1. L'instruction rendra, dans la variable `variable%`, la valeur 0 si la disquette n'est pas protégée en écriture, et 1 s'il est impossible d'y écrire des données.

A l'image du précédent programme, il sera possible d'utiliser cette instruction pour éviter le message **DISC WRITE PROTECTED** de l'AMSDOS et demander « poliment » une disquette accessible en écriture.

I CODE

Cette instruction permet d'entrer un code compris entre - 32768 et 32767 dans la mémoire du CPC, pour permettre l'identification de l'utilisateur et ainsi mettre en œuvre notre simulateur de virus.

Sa syntaxe est la suivante : **I CODE, nombre**, ou encore : **I CODE, variable%**. Si vous n'utilisez pas cette instruction, le nombre code initial en mémoire est le chiffre zéro.

I VERIFIE

Cette instruction permet de comparer le code donné par l'instruction code et le code d'utilisation du logiciel placé en mémoire. Si CPC constate une différence, il active automatiquement notre faux virus.

I SIMULEF

I SIMULEF ? Voilà une instruction bizarre ! Il s'agit en fait de l'instruction qui permettra d'activer sans condition notre virus, contrairement à la précédente.

Parlons-en de notre pseudo-virus : celui -ci consiste à rechercher une disquette sur l'un des deux lecteurs, de demander l'introduction d'une disquette, le cas échéant, de déterminer ensuite si cette disquette est protégée ou non contre l'écriture, et de faire croire à un formatage de celle-ci. Précisons que même si la disquette est protégée, notre pseudo-virus le signale et affirme qu'il passe outre cette protection.

De quoi faire bondir notre utilisateur sur son lecteur pour en retirer la précieuse disquette, avant la fin du formatage. Dans ce cas, seul un RESET permettra de quitter le « virus ».

Comment simuler un formatage nous direz-vous ? Notre programme effectue en fait un déplacement de sa tête de lecture sur toutes les pistes de la disquette, moyennant une temporisation intermédiaire équivalente à celle d'un vrai formatage. L'affichage des pistes en cours de formatage faisant le reste.

LE PROGRAMME

Pour permettre à tous de profiter de cette blague, nous vous proposons le programme sous sa forme Assembleur, tel que nous avons été obligé de l'écrire, mais aussi sous forme de chargeur de codes hexadécimaux sous Basic.

Le programme Assembleur

```

1          ;*****
2          ;**                **
3          ;** PROGRAMMES EXEMPLES **
4          ;** DE GESTION DISQUE **
5          ;**                **
6          ;*****
7          ;
8          ;
9          ;*** TABLE DES EQUIVALENCES ***
10         ;
11         ;ATTENTE TOUCHE FRAPPEE
12         ;           KM-WAIT-CHAR
13         KMWAIT:   EQU  0BB06H
14         ;
15         ;AFFICHAGE D'UN CARACTERE
16         ;           TXT-OUTPUT
17         TXTOUT:   EQU  0BB5AH
18         ;
19         ;RECHERCHE D'UNE RSX EN ROM
20         ;           KL-FIND-COMMAND
21         KLFCOM:   EQU  0BCD4H
22         ;
23         ;INSERTION DES RSXs
24         ;           KL-LOG-TEXT
25         KLOGTX:   EQU  0BCD1H
26         ;
27         ;ADRESSE MOTEUR LECTEUR
28         ADRMOT:   EQU  0FA7EH
29         ;
30         ;
31         ;*** ORIGINE D'ASSEMBLAGE ***
32         ;***   ET DE CHARGEMENT   ***
33         ;
34         ;           ORG  0A000H
35         ;
36         ;           LOAD 0A000H
37         ;
38         ;
39         ;*** INSERTION DES RSX ***
40         ;
41         DEBUT:    EQU  $
42         A000 210FA0      LD  HL,KERNEL          ;A RESERVER POUR RSXs
43         A003 0113A0      LD  BC,VECTEU          ;TABLE INSTRUCTIONS
44         ;
45         A006 3EC9        LD  A,0C9H            ;RET POUR EVITER
46         A008 3200A0      LD  (DEBUT),A          ;UN NOUVEL APPEL
47         ;
48         A00B CDD1BC      CALL KLOGTX            ;INITIALISE RSXs
49         ;
50         A00E C9          RET                    ;FIN
51         ;
52         ;
53         ;*** RESERVE POUR KERNEL ***
54         ;
55         KERNEL:        EQU  $
56         A00F 00000000    DEFB 00,00,00,00
57         ;
58         ;*** TABLE INSTRUCTIONS ***
59         ;
60         VECTEU:        EQU  $

```



```

115 ;
116 DISFIN: EQU $
117 A069 3D DEC A
118 A06A 3D DEC A
119 A06B C0 RET NZ ;PAS 2 PARAMETRES
120 A06C DD6E00 LD L,(IX+00)
121 A06F DD6601 LD H,(IX+01H) ;ADRSSE VARIABLE
122 A072 E5 PUSH HL
123 A073 DD7E02 LD A,(IX+02H) ;NUMERO LECTEUR
124 A076 CDBAA1 CALL LPRESE ;VOIR PRESENCE?
125 A079 E1 POP HL ;ADRESSE
126 A07A 77 LD (HL),A ;ETAT LECTEUR
127 ;
128 A07B C9 RET ;FIN
129 ;
130 ;
131 ;** ENTREE D'UN CODE **
132 ;
133 CODE: EQU $
134 A07C 3D DEC A ;UN SEUL CARACTERE
135 A07D C0 RET NZ ;FOURNIT
136 A07E 218BA0 LD HL,NOCODE ;POUR RANGER
137 A081 DD7E00 LD A,(IX+00) ;OCTET BAS
138 A084 77 LD (HL),A ;A RANGER
139 A085 23 INC HL ;SUIVANT
140 A086 DD7E01 LD A,(IX+01) ;OCTET HAUT
141 A089 77 LD (HL),A ;A RANGER
142 A08A C9 RET ;FIN
143 ;
144 NOCODE: EQU $ ;CODE FOURNI
145 A08B 0000 DEFB 00,00
146 ;
147 ;*****
148 ;** **
149 ;** LA VALEUR SUIVANTE **
150 ;** SUR DEUX OCTETS EST **
151 ;** LE CODE A CONNAITRE **
152 ;** POUR L'UTILISATION **
153 ;** DU PROGRAMME **
154 ;** **
155 ;*****
156 ;
157 LECODE: EQU $
158 A08D 0100 DEFW 0001 ;VALEUR DECIMALE DU CODI
159 ;
160 ;*****
161 ;*****
162 ;
163 ;
164 ;*** VERIFICATION DU CODE ***
165 ;
166 VERIFE: EQU $
167 ;
168 ;
169 A08F 2A8BA0 LD HL,(NOCODE) ;CODE DONNE
170 A092 EB EX DE,HL ;DANS DE
171 A093 2A8DA0 LD HL,(LECODE) ;VRAI CODE
172 A096 AF XOR A ;FLAG A ZERO
173 A097 ED52 SBC HL,DE ;SOUSTRAIT POUR VOIR
174 A099 C49DA0 CALL NZ,SIMFOR ;SI PAS EGALITE

```

```

175 A09C C9          RET
176                  ;
177                  ;
178                  ;** SIMULATION DE FORMATAGE **
179                  ;
180 SIMFOR:          EQU $
181                  ;
182 SIMFOR3:         EQU $
183 A09D 3E00        LD  A,0          ;LECTEUR A
184 A09F CDBAA1     CALL LPRESE      ;VOIR PRESENCE LECTEUR
185 A0A2 B7         OR  A           ;TESTER
186 A0A3 204E       JR  NZ,SIMFO1   ;OK PRESENT
187 A0A5 3E01       LD  A,01H      ;LECTEUR B
188 A0A7 CDBAA1     CALL LPRESE      ;VOIR PRESENCE LECTEUR
189 A0AA B7         OR  A           ;TESTER
190 A0AB 204A       JR  NZ,SIMFO2   ;OK PRESENT
191                  ;
192 A0AD 21B8A0     LD  HL,ERLPRE    ;MESS. ERREUR DISK
193 A0B0 CDA2A2     CALL AFFMES     ;A AFFICHER
194 A0B3 CD06BB     CALL KMWAIT    ;ATTENTE TOUCHE
195 A0B6 18E5       JR  SIMFOR3     ;RECOMMENCER
196                  ;
197 ERLPRE:         EQU $
198 A0B8 0A0D       DEFB 0AH,0DH
199 A0BA 49E7365    DEFB "Inserer "
199 A0BE 72657220
200 A0C2 64697371  DEFB "disquette "
200 A0C6 75657474
200 A0CA 6520
201 A0CC 64616E73  DEFB "dans lecteur"
201 A0D0 206C6563
201 A0D4 74657572
202 A0D8 0D0A      DEFB 0DH,0AH
203 A0DA 41707075  DEFB "Appuyez sur"
203 A0DE 79657A20
203 A0E2 737572
204 A0E5 20756E65  DEFB " une touche"
204 A0E9 20746F75
204 A0ED 636865
205 A0F0 0D0A      DEFB 0DH,0AH
206 A0F2 00        DEFB 00H
207                  ;
208 SIMFO1:         EQU $
209 A0F3 3E00       LD  A,0          ;LECTEUR A
210 A0F5 1802       JR  SIMFO4     ;SUITE
211 SIMFO2:         EQU $
212 A0F7 3E01       LD  A,01H      ;LECTEUR B
213                  ;
214 SIMFO4:         EQU $
215 A0F9 F5         PUSH AF
216 A0FA 2113A1     LD  HL,MESLEC    ;MESS. "LECTEUR:..."
217 A0FD CDA2A2     CALL AFFMES     ;AFFICHER
218 A100 F1         POP  AF
219 A101 F5         PUSH AF
220 A102 C641       ADD  A,041H      ;CONVERSION ASCII A OU E
221 A104 CD5ABB     CALL TXTOUT     ;A AFFICHER
222 A107 3E0D       LD  A,0DH      ;RC
223 A109 CD5ABB     CALL TXTOUT
224 A10C 3E0A       LD  A,0AH      ;LF
225 A10E CD5ABB     CALL TXTOUT

```

```

226 A111 180D          JR    SIMFO9
227                   ;
228                   MESLEC: EQU  $
229 A113 0DOA          DEFB 0DH,0AH
230 A115 4C656374      DEFB "Lecteur : "
230 A119 65757220
230 A11D 3A20
231 A11F 00            DEFB 00
232                   ;
233                   SIMFO9: EQU  $
234 A120 F1            POP  AF
235 A121 F5            PUSH AF
236 A122 CDCBA1        CALL WPROTE          ;VOIR SI PROTEGE
237 A125 FE00          CP   00
238 A127 2836          JR   Z,SIMFO5        ;NON SAUTER
239 A129 2131A1        LD   HL,WRIPRO       ;"Disquette protegee"
240                   ;"Protection ignoree..."
241 A12C CDA2A2        CALL AFFMES          ;A AFFICHER
242 A12F 182E          JR   SIMFO5
243                   ;
244                   WRIPRO: EQU  $
245 A131 0DOA          DEFB 0DH,0AH
246 A133 44697371      DEFB "Disquette"
246 A137 75657474
246 A13B 65
247 A13C 2070726F      DEFB " protegee"
247 A140 74656765
247 A144 65
248 A145 0A0D          DEFB 0AH,0DH
249 A147 50726F74      DEFB "Protection"
249 A14B 65637469
249 A14F 6F6E
250 A151 2069676E      DEFB " ignoree..."
250 A155 6F726565
250 A159 2E2E2E
251 A15C 0A0D          DEFB 0AH,0DH
252 A15E 00            DEFB 00H
253                   ;
254                   SIMFO5: EQU  $
255 A15F 2169A1        LD   HL,FORSIM       ;"Formattage Piste:..."
256 A162 CDA2A2        CALL AFFMES
257 A165 0627          LD   B,027H          ;COMPTEUR 39 PISTES
258 A167 1814          JR   SIMFO7          ;SUITE
259                   ;
260                   FORSIM: EQU  $
261 A169 0A0D          DEFB 0AH,0DH
262 A16B 466F726D      DEFB "Formatage"
262 A16F 61746167
262 A173 65
263 A174 20506973      DEFB " Piste: "
263 A178 74653A20
264 A17C 00            DEFB 00H
265                   ;
266                   SIMFO7: EQU  $
267 A17D 3E28          LD   A,028H
268 A17F 90            SUB  B                ;ET CALCUL PISTE
269 A180 C5            PUSH BC
270                   ;
271 A181 47            LD   B,A              ;COMPTEUR POUR
272 A182 AF            XOR  A                ;CORRECTION BCD

```

```

273          SIMFO6:    EQU  $
274 A183 C601          ADD  A,1
275 A185 27            DAA                      ;CORRECTION BCD
276 A186 10FB          DJNZ SIMFO6                ;SUIVANT
277          ;
278 A188 C1            POP  BC
279 A189 F5            PUSH AF
280 A18A 1F            RRA
281 A18B 1F            RRA
282 A18C 1F            RRA
283 A18D 1F            RRA
284 A18E E60F          AND  0FH                      ;DIZAINNE
285 A190 F630          OR   030H                    ;CONVERSION ASCII
286 A192 CD5ABB        CALL TXTOUT                ;A AFFICHER
287 A195 F1            POP  AF                      ;RECUPERE
288 A196 E60F          AND  0FH                      ;UNITES
289 A198 F630          OR   030H                    ;CONVERSION ASCII
290 A19A CD5ABB        CALL TXTOUT                ;A AFFICHER
291 A19D 3E08          LD   A,08H                    ;RETOUR ARRIERE
292 A19F CD5ABB        CALL TXTOUT
293 A1A2 CD5ABB        CALL TXTOUT
294          ;
295 A1A5 50             LD   D,B                      ;NUMERO DE PISTE
296 A1A6 F1            POP  AF
297 A1A7 F5            PUSH AF
298 A1A8 5F            LD   E,A                      ;NUMERO DE LECTEUR
299 A1A9 C5            PUSH BC
300 A1AA CD5AA2        CALL CHPIST                ;POSITIONNE PISTE
301          ;
302 A1AD 21FFFF        LD   HL,0FFFFH                ;TEMPO
303          SIMFO8:    EQU  $
304 A1B0 2B            DEC  HL
305 A1B1 7C            LD   A,H
306 A1B2 B5            OR   L
307 A1B3 20FB          JR   NZ,SIMFO8
308          ;
309 A1B5 C1            POP  BC
310 A1B6 10C5          DJNZ SIMFO7                ;PISTE SUIVANTE
311          ;
312 A1B8 F1            POP  AF
313 A1B9 C9            RET
314          ;
315          ;
316          ;** TEST PRESENCE DISQUETTE **
317          ;
318          LPRESE:    EQU  $
319 A1BA C5            PUSH BC
320 A1BB 47            LD   B,A                      ;No LECTEUR
321 A1BC 3E02          LD   A,2                      ;2 POUR
322 A1BE 90            SUB  B                      ;CONVERSION
323 A1BF CDDCA1        CALL LITLEC                ;INTERROGE FDC
324 A1C2 C1            POP  BC                      ;RECUPERE BC
325 A1C3 E620          AND  020H                    ;BIT 5 LECTEUR PRET
326 A1C5 FE20          CP   020H
327 A1C7 C0            RET  NZ
328 A1C8 3E01          LD   A,01H                    ;OK PRET
329 A1CA C9            RET
330          ;
331          ;
332          ;** TEST WRITE PROTECTED **

```

```

333 ;
334 WPROTE: EQU $
335 A1CB C5 PUSH BC
336 A1CC 47 LD B,A ;No DE LECTEUR
337 A1CD 3E02 LD A,02H ;2 POUR
338 A1CF 90 SUB B ;CONVERSION
339 A1D0 CDDCA1 CALL LITLEC ;INTERROGE FDC
340 A1D3 C1 POP BC ;RECUPERE BC
341 A1D4 E640 AND 040H ;BIT6 WRITE PROTECTED
342 A1D6 FE40 CP 040H ;?
343 A1D8 C0 RET NZ ;NON
344 A1D9 3E01 LD A,01H ;OUI
345 A1DB C9 RET
346 ;
347 ;
348 ;** LIT LE REGISTRE D'ETAT **
349 ;** DU CONTOLEUR DISQUETTE **
350 ;
351 LITLEC: EQU $
352 A1DC E5 PUSH HL
353 A1DD C5 PUSH BC
354 A1DE 47 LD B,A ;SAUVE LECTEUR A TESTER
355 A1DF 2A7DBE LD HL,(0BE7DH) ;ADRESSE DE LA
356 ;ZONE DECALABLE DE L'AMSDOS
357 A1E2 7E LD A,(HL) ;LECTEUR ACTUEL
358 A1E3 F5 PUSH AF ;RANGE
359 A1E4 78 LD A,B ;LECTEUR A TESTER
360 A1E5 77 LD (HL),A ;DANS ZONE AMSDOS
361 A1E6 CDF3A1 CALL LITFDC ;EFFECTUE INSTRUCTION
362 ;DU FDC-765
363 A1E9 47 LD B,A ;RANGER ETAT
364 A1EA 2A7DBE LD HL,(0BE7DH) ;ZONE DECALABLE
365 A1ED F1 POP AF
366 A1EE 77 LD (HL),A ;ANCIEN ETAT LECTEUR
367 A1EF 78 LD A,B ;REPREND ETAT LECTEUR
368 A1F0 C1 POP BC
369 A1F1 E1 POP HL
370 A1F2 C9 RET
371 ;
372 ;
373 ;** ENVOI INSTRUCTION AU FDC **
374 ;** POUR CONNAITRE SON ETAT **
375 ;
376 LITFDC: EQU $
377 A1F3 E5 PUSH HL
378 A1F4 D5 PUSH DE
379 A1F5 C5 PUSH BC
380 A1F6 F5 PUSH AF
381 ;
382 A1F7 CD40A2 CALL LMOTON ;MOTEUR ON
383 A1FA 017FFB LD BC,0FB7FH ;ADRESSE COMANDE
384 A1FD 3E04 LD A,04H ;INSTRUCTION 4
385 A1FF ED79 OUT (C),A ;A EXECUTER
386 ;
387 LITFD1: EQU $
388 A201 017EFB LD BC,0FB7EH ;ADRESSE REGISTRE
389 ;D'ETAT PRINCIPAL
390 A204 ED78 IN A,(C) ;A LIRE
391 A206 E680 AND 080H
392 A208 FE80 CP 080H ;2 BITS HAUT = 10?

```

```

393 A20A 20F5          JR    NZ,LITFD1          ;PAS PRET
394 A20C 017FFB        LD    BC,0FB7FH
395 A20F F1            POP   AF
396 A210 ED79          OUT   (C),A              ;LECTEUR
397                    LITFD2: EQU $
398 A212 017EFB        LD    BC,0FB7EH
399 A215 ED78          IN    A,(C)
400 A217 E6C0          AND   0COH
401 A219 FEC0          CP    0COH              ;2 BIT HAUT = 11?
402 A21B 20F5          JR    NZ,LITFD2
403                    ;
404 A21D 017FFB        LD    BC,0FB7FH        ;ADRESSE RESULTAT
405 A220 ED78          IN    A,(C)            ;A LIRE
406 A222 CD4FA2        CALL  LMOTOF           ;ARRET LECTEUR
407                    ;
408 A225 C1            POP   BC
409 A226 D1            POP   DE
410 A227 E1            POP   HL
411 A228 C9            RET
412                    ;
413                    ;
414                    ;
415                    ;** TEMPORISATION SUITE **
416                    ;** A L'ACTIVATION DES **
417                    ;** LECTEURS DE DISQUETTE **
418                    ;
419                    LTEMPO: EQU $
420 A229 E5            PUSH  HL                ;SAUVEGARDE
421 A22A F5            PUSH  AF                ;DES REGISTRES
422                    ;
423 A22B 210300        LD    HL,0003           ;LONGUE TEMPO
424                    LTEMP2: EQU $
425 A22E E5            PUSH  HL
426                    ;
427 A22F 21FFFF        LD    HL,0FFFFH        ;COURTE TEMPO
428                    LTEMP1: EQU $
429 A232 2B            DEC   HL
430 A233 7D            LD    A,L
431 A234 B4            OR    H
432 A235 20FB        JR    NZ,LTEMP1
433                    ;
434 A237 E1            POP   HL
435 A238 2B            DEC   HL
436 A239 7D            LD    A,L
437 A23A B4            OR    H
438 A23B 20F1        JR    NZ,LTEMP2
439                    ;
440 A23D F1            POP   AF                ;RECUPERATION
441 A23E E1            POP   HL                ;DES REGISTRES
442                    ;
443 A23F C9            RET
444                    ;
445                    ;
446                    ;*** MISE EN MARCHE DES ***
447                    ;*** MOTEURS DES LECTEURS *
448                    ;*** DE DISQUETTES ***
449                    ;
450                    LMOTON: EQU $
451 A240 C5            PUSH  BC                ;SAUVEGARDE
452 A241 F5            PUSH  AF                ;DES REGISTRES

```

```

453                                     ;
454 A242 017EFA                         LD   BC,ADRMOT           ;ADRESSE MOTEUR
455 A245 3E01                           LD   A,01H            ;CODE ACTIVATION
456 A247 ED79                           OUT  (C),A           ;MOTEUR TOURNE
457 A249 CD29A2                         CALL LTEMPO          ;TEMPO POUR VITESSE
458                                     ;
459 A24C F1                             POP  AF              ;RECUPERATION
460 A24D C1                             POP  BC              ;DES REGISTRES
461                                     ;
462 A24E C9                             RET
463                                     ;
464                                     ;*** ARRET DES MOTEURS DES ***
465                                     ;*** LECTEURS DE DISQUETTE ***
466                                     ;
467 LMOTOF: EQU $
468 A24F C5                             PUSH BC              ;SAUVEGARDE
469 A250 F5                             PUSH AF              ;DES REGISTRES
470                                     ;
471 A251 017EFA                         LD   BC,ADRMOT           ;ADRESSE MOTEUR
472 A254 AF                             XOR  A               ;0 = CODE ARRET MOTEUR
473 A255 ED79                           OUT  (C),A           ;ARRET MOTEUR
474                                     ;
475 A257 F1                             POP  AF              ;RECUPERATION
476 A258 C1                             POP  BC              ;DES REGISTRES
477                                     ;
478 A259 C9                             RET
479                                     ;
480                                     ;
481                                     ;*** POSITIONNEMENT SUR ***
482                                     ;*** UNE PISTE DETERMINE **
483                                     ;
484 CHPIST: EQU $
485 A25A F5                             PUSH AF
486 A25B C5                             PUSH BC
487 A25C E5                             PUSH HL
488 A25D D5                             PUSH DE
489                                     ;
490 A25E 2184A2                         LD   HL,CCHPIS        ;ADRESSE INSTRUCTION
491 A261 CDD4BC                         CALL KLFCOM          ;VECTEUR RECHERCHE RSX
492 A264 380B                           JR   C,CHPIS2        ;TROUVEE
493 A266 2188A2                         LD   HL,ERRROM       ;MESSAGE ERREUR ROM
494 A269 CDA2A2                         CALL AFFMES          ;A AFFICHER
495 A26C D1                             POP  DE
496 A26D E1                             POP  HL
497 A26E C1                             POP  BC
498 A26F F1                             POP  AF
499 A270 C9                             RET                  ;FIN
500                                     ;
501 CHPIS2: EQU $
502 A271 2285A2                         LD   (CHPADR),HL     ;ADRESSE ROUTINE ROM
503 A274 79                             LD   A,C             ;RECUPERE No DE ROM
504 A275 3287A2                         LD   (CHPROM),A     ;A RANGER
505 A278 D1                             POP  DE              ;CARACTERISTIQUES PISTE
506 A279 D5                             PUSH DE
507 A27A DF                             RST 018H            ;POSITIONNE PISTE
508 A27B 85A2                         DEFW CHPADR          ;VECTEUR SUR ADRESSE
509 A27D 30F2                         JR   NC,CHPIS2      ;PAS POSITIONNEE
510 A27F D1                             POP  DE
511 A280 E1                             POP  HL
512 A281 C1                             POP  BC

```

```

513 A282 F1          POP  AF
514 A283 C9          RET                ;FIN
515                  ;
516                  CCHPIS:  EQU  $
517 A284 87          DEFB  087H                ;NOM INSTRUCTION
518                  ;
519                  CHPADR:  EQU  $
520 A285 0000        DEFB  00,00                ;RESERVE ADRESSE ROM
521                  ;
522                  CHPROM:  EQU  $
523 A287 00          DEFB  00                ;RESERVE No DE ROM
524                  ;
525                  ERRROM:  EQU  $
526 A288 0A0D        DEFB  0AH,0DH
527 A28A 45525245    DEFB  "ERREUR SUR"
527 A28E 55522053
527 A292 5552
528 A294 20524F4D    DEFB  " ROM AMSDOS"
528 A298 20414D53
528 A29C 444F53
529 A29F 0A0D        DEFB  0AH,0DH
530 A2A1 00          DEFB  00
531                  ;
532                  ;
533                  ;*** AFFICHAGE D'UN MESSAGE ***
534                  ;
535                  AFFMES:  EQU  $
536 A2A2 7E          LD    A, (HL)
537 A2A3 B7          OR    A
538 A2A4 C8          RET    Z
539 A2A5 CD5ABB      CALL  TXTOUT
540 A2A8 23          INC   HL
541 A2A9 18F7        JR    AFFMES
542                  ;
543                  ;
544                  ;
545                  END

```

Le programme dans ses grandes lignes est un programme classique d'introduction d'instruction sous formes de RSX, avec gestion de celles-ci, aussi nous ne nous attarderons pas sur son explication, mais aussi pour ne pas tenter ceux qui sont désireux de modifier celui-ci et qui prendraient le risque de créer un virus non voulu risquant de détériorer un ou plusieurs secteurs sur leur disquette voire des fichiers importants à leurs yeux, ce qui nous navrerait.

Quand aux spécialistes de l'Assembleur, qui comprendront sans peine notre programme, eux, ne nous ont certainement pas attendu pour gérer directement en Assembleur le formatage et l'écriture de secteur sur les disquettes.

Le chargeur Basic

```
10 REM *****
20 REM **          PROGRAMME DE          **
30 REM **  CHARGEMENT DES CODES  **
40 REM **  MACHINE DES NOUVELLES **
50 REM **  INSTRUCTION GERANT   **
60 REM **  LE LECTEUR DISQUETTES **
70 REM *****
80 REM
90 REM ** initialisation memoire **
100 REM
110 CALL &BB4E
120 MEMORY &9FFF
130 OPENOUT "bidon."
140 MEMORY HIMEM-1
150 CLOSEOUT
160 REM
170 REM ** presentation **
180 REM
190 MODE 2
200 PRINT:PRINT
210 PRINT "Chargement des codes en cours
"
220 REM
230 REM ** initialisation **
240 REM
250 ADRESSE = &A000
260 ADRESSEBASE = &A000
270 LIGNE = 1000
280 RESTORE 1000
290 SOMME = 0
300 REM
310 REM ** boucle de chargement **
320 REM
330 FOR I = 1 TO 8
340     LOCATE 10,10
350     PRINT I
360     READ A$
370     IF UPPER$(A$) = "XX" THEN GOTO 60
0
380     A = VAL("&"+A$)
390     POKE ADRESSE,A
400     ADRESSE = ADRESSE + 1
410     SOMME = SOMME + A
420 NEXT I
430 REM
440 REM ** verification **
450 REM
460 READ CONTROLES$
```

```
470 CONTROLE = VAL("&"+CONTROLE$)
480 IF CONTROLE <> SOMME THEN GOTO 540
490 LIGNE = LIGNE + 10
500 GOTO 290
510 REM
520 REM ** ERREUR **
530 REM
540 PRINT "Vous avez fait une erreur en
ligne : ";
550 PRINT LIGNE
560 STOP
570 REM
580 REM ** ok sauvegarde **
590 REM
600 MODE 2
610 REM
620 PRINT "Programme charge en memoire"
630 PRINT:PRINT:PRINT
640 REM
650 REM ** sauvegarde des codes **
660 REM
670 PRINT "Sauvegarde du programme:"
680 PRINT "SAVE ";CHR$(34);"VIRUS.BIN";C
HR$(34);", B, &";HEX$(ADRESSEBASE);", &";HE
X$(ADRESSE-ADRESSEBASE)
690 SAVE "VIRUS.BIN", B, ADRESSEBASE, ADRES
SE-ADRESSEBASE
700 REM
710 REM ** presentation utilisation **
720 REM
730 PRINT:PRINT:PRINT
740 PRINT "Pour utiliser le programme:"
750 PRINT "MEMORY &9FFF"
760 PRINT "LOAD ";CHR$(34);"VIRUS.BIN";C
HR$(34);", &A000"
770 PRINT "CALL &A000"
780 PRINT:PRINT
790 PRINT "pour installer les RSXs disqu
ette"
800 PRINT:PRINT
810 PRINT "|DISKON |DISKOFF |SIMULEF
CODE,code |VERIFE
|DISKFIND,lecteur,@variable%
|DISKWR,lecteur,@variable%"
820 REM
830 PRINT:PRINT:PRINT
840 END
850 REM *****
860 REM
950 REM
```

```
960 REM *****
970 REM **  DONNEES DU PROGRAMME  **
980 REM *****
990 REM
1000 DATA 21,0F,A0,01,13,A0,3E,C9,28B
1010 DATA 32,00,A0,CD,D1,BC,C9,00,3F5
1020 DATA 00,00,00,2A,A0,C3,40,A2,26F
1030 DATA C3,4F,A2,C3,9D,A0,C3,7C,4F3
1040 DATA A0,C3,8F,A0,C3,69,A0,C3,521
1050 DATA 56,A0,44,49,53,4B,4F,CE,33E
1060 DATA 44,49,53,4B,4F,46,C6,53,2D9
1070 DATA 49,4D,55,4C,45,C6,43,4F,2D4
1080 DATA 44,C5,56,45,52,49,46,C5,34A
1090 DATA 44,49,53,4B,46,49,4E,C4,2CC
1100 DATA 44,49,53,4B,57,D2,3D,3D,2CE
1110 DATA C0,DD,6E,00,DD,66,01,E5,434
1120 DATA DD,7E,02,CD,CB,A1,E1,77,4EE
1130 DATA C9,3D,3D,C0,DD,6E,00,DD,42B
1140 DATA 66,01,E5,DD,7E,02,CD,BA,430
1150 DATA A1,E1,77,C9,3D,C0,21,8B,46B
1160 DATA A0,DD,7E,00,77,23,DD,7E,3F0
1170 DATA 01,77,C9,00,00,01,00,2A,16C
1180 DATA 8B,A0,EB,2A,8D,A0,AF,ED,509
1190 DATA 52,C4,9D,A0,C9,3E,00,CD,427
1200 DATA BA,A1,B7,20,4E,3E,01,CD,38C
1210 DATA BA,A1,B7,20,4A,21,B8,A0,3F5
1220 DATA CD,A2,A2,CD,06,BB,18,E5,49C
1230 DATA 0A,0D,49,6E,73,65,72,65,27D
1240 DATA 72,20,64,69,73,71,75,65,31D
1250 DATA 74,74,65,20,64,61,6E,73,313
1260 DATA 20,6C,65,63,74,65,75,72,314
1270 DATA 0D,0A,41,70,70,75,79,65,28B
1280 DATA 7A,20,73,75,72,20,75,6E,2F7
1290 DATA 65,20,74,6F,75,63,68,65,30D
1300 DATA 0D,0A,00,3E,00,18,02,3E,0AD
1310 DATA 01,F5,21,13,A1,CD,A2,A2,3DC
1320 DATA F1,F5,C6,41,CD,5A,BB,3E,50D
1330 DATA 0D,CD,5A,BB,3E,0A,CD,5A,35E
1340 DATA BB,18,0D,0D,0A,4C,65,63,20B
1350 DATA 74,65,75,72,20,3A,20,00,23A
1360 DATA F1,F5,CD,CB,A1,FE,00,28,545
1370 DATA 36,21,31,A1,CD,A2,A2,18,352
1380 DATA 2E,0D,0A,44,69,73,71,75,24B
1390 DATA 65,74,74,65,20,70,72,6F,323
1400 DATA 74,65,67,65,65,0A,0D,50,271
1410 DATA 72,6F,74,65,63,74,69,6F,369
1420 DATA 6E,20,69,67,6E,6F,72,65,312
1430 DATA 65,2E,2E,2E,0A,0D,00,21,127
1440 DATA 69,A1,CD,A2,A2,06,27,18,360
```

```
1450 DATA 14,0A,0D,46,6F,72,6D,61,220
1460 DATA 74,61,67,65,20,50,69,73,2ED
1470 DATA 74,65,3A,20,00,3E,28,90,229
1480 DATA C5,47,AF,C6,01,27,10,FB,3B4
1490 DATA C1,F5,1F,1F,1F,1F,E6,0F,327
1500 DATA F6,30,CD,5A,BB,F1,E6,0F,4EE
1510 DATA F6,30,CD,5A,BB,3E,08,CD,41B
1520 DATA 5A,BB,CD,5A,BB,50,F1,F5,52D
1530 DATA 5F,C5,CD,5A,A2,21,FF,FF,50C
1540 DATA 2B,7C,B5,20,FB,C1,10,C5,40D
1550 DATA F1,C9,C5,47,3E,02,90,CD,463
1560 DATA DC,A1,C1,E6,20,FE,20,C0,522
1570 DATA 3E,01,C9,C5,47,3E,02,90,2E4
1580 DATA CD,DC,A1,C1,E6,40,FE,40,56F
1590 DATA C0,3E,01,C9,E5,C5,47,2A,3E3
1600 DATA 7D,BE,7E,F5,78,77,CD,F3,55D
1610 DATA A1,47,2A,7D,BE,F1,77,78,42D
1620 DATA C1,E1,C9,E5,D5,C5,F5,CD,6AC
1630 DATA 40,A2,01,7F,FB,3E,04,ED,38C
1640 DATA 79,01,7E,FB,ED,78,E6,80,4BE
1650 DATA FE,80,20,F5,01,7F,FB,F1,4FF
1660 DATA ED,79,01,7E,FB,ED,78,E6,52B
1670 DATA C0,FE,C0,20,F5,01,7F,FB,50E
1680 DATA ED,78,CD,4F,A2,C1,D1,E1,596
1690 DATA C9,E5,F5,21,03,00,E5,21,3CD
1700 DATA FF,FF,2B,7D,B4,20,FB,E1,556
1710 DATA 2B,7D,B4,20,F1,F1,E1,C9,508
1720 DATA C5,F5,01,7E,FA,3E,01,ED,45F
1730 DATA 79,CD,29,A2,F1,C1,C9,C5,551
1740 DATA F5,01,7E,FA,AF,ED,79,F1,574
1750 DATA C1,C9,F5,C5,E5,D5,21,84,5A3
1760 DATA A2,CD,D4,BC,38,0B,21,88,3EB
1770 DATA A2,CD,A2,A2,D1,E1,C1,F1,617
1780 DATA C9,22,85,A2,79,32,87,A2,3E6
1790 DATA D1,D5,DF,85,A2,30,F2,D1,59F
1800 DATA E1,C1,F1,C9,87,00,00,00,3E3
1810 DATA 0A,0D,45,52,52,45,55,52,1EC
1820 DATA 20,53,55,52,20,52,4F,4D,228
1830 DATA 20,41,4D,53,44,4F,53,0A,1F1
1840 DATA 0D,00,7E,B7,C8,CD,5A,BB,3EC
1850 DATA 23,18,F7,00,00,00,00,00,132
1860 DATA XX
```

Ce programme possède sa propre routine de contrôle des DATA, aussi nous vous conseillons de respecter scrupuleusement les numéros de lignes du listing, car il s'y réfère.

Après sauvegarde et lancement, le programme sauvegarde automatiquement le fichier binaire créé sous le nom **VIRUS.BIN**, que vous pourrez modifier à votre gré, à l'aide de la commande **I REN**, pour le rendre plus discret.

Pour le charger, il suffira des instructions suivantes :

```
10 MEMORY &9FFF
20 OPENOUT « MACHIN. »
30 MEMORY HIMEM - 1
40 CLOSEOUT
50 LOAD « VIRUS. BIN », &A000
60 CALL &A000
```

Les différentes RSX présentées seront alors utilisables.

Modification du code

Le code originel placé par le programme est le chiffre 1, mais nous vous proposons ici de le modifier à votre gré pour toute valeur comprise entre - 32767 et 32768.

Une fois le programme en mémoire, réfléchissez à votre code (supposons 7843) et frappez en mode direct :

```
PRINT HEX$ (7843,4)
Réponse du CPC : 1EA3
```

Il vous suffira ensuite d'effectuer les deux instructions suivantes :

```
POKE &A08E, &1E
POKE &A08D, &A3
SAVE « VIRUS.BIN », &A000, &2AA
```

Ce qui aura pour effet de sauvegarder sur la disquette le programme avec votre nouveau code sur la disquette.

Exemple d'utilisation du pseudo-virus

Nous vous proposons un court exemple utilisant l'accès régulier à la vérification du code entré, ce code étant demandé discrètement :

```
10 REM PLACER AVANT LE CHARGEMENT
20 REM ET L'INSTALLATION DES RSX
30 .....
100 INPUT « Quel est votre nom » ; nom$
110 nom = val (nom$)
120 I CODE, nom`
```

```
130 EVERY 200, 1 GOSUB 20 000
140. . . SUITE DU PROGRAMME . . .
150. . . AVEC EVENTUELLEMENT . . .
160. . . DE NOUVELLES DEMANDES DE CODE . . .
20000 I VERIFE
20010 RETURN
```

En fait, lorsque le programme demande le nom (ce pourrait être n'importe quoi), il vous suffira d'entrer le code que vous aurez choisi, au lieu d'un nom. La vérification s'effectuera régulièrement dans le programme.

Un dernier conseil

Lors de vos premiers essais, de bon fonctionnement du virus, veillez à utiliser une disquette dont le contenu vous importe peu, une erreur de DATA est si vite arrivée.

Bien que quasiment improbable, un incident est si vite arrivé, et l'on est jamais trop sage avec la manipulation des disquettes.