Alerte au virus !

par Dominique Pessan et André Chéramy

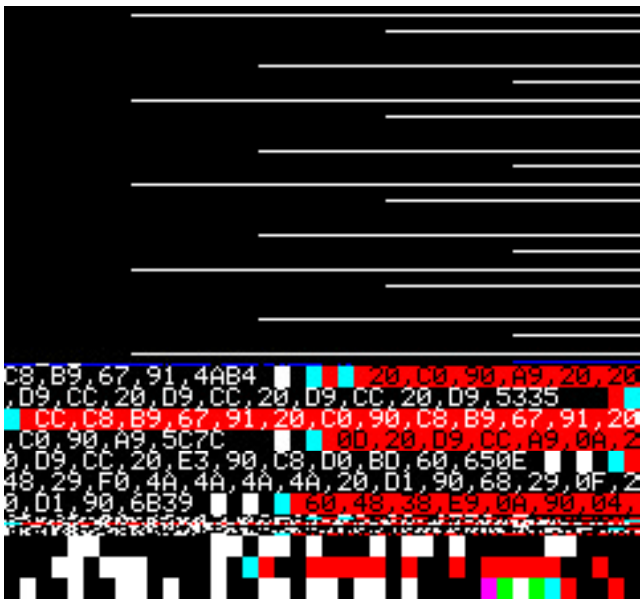
Comme vous le savez, Dominique, André et Claude ont plusieurs casseroles sur le feu commun de l'amitié Oricienne. Dominique, qui est un Oricien très actif a chopé un virus sur le oueb. Il l'a ensuite refilé en toute innocence à André et André l'a refilé à deux autres personnes. Et cela aurait pu durer, si par hasard, nous n'avions pas compris que pour la première fois un virus circulait dans le monde Oric ! Nous sommes tellement habitués aux plantages à répétition et aux comportements erratiques, que l'idée d'un virus ne nous serait jamais venu à l'esprit, sans sa mise en évidence fortuite.

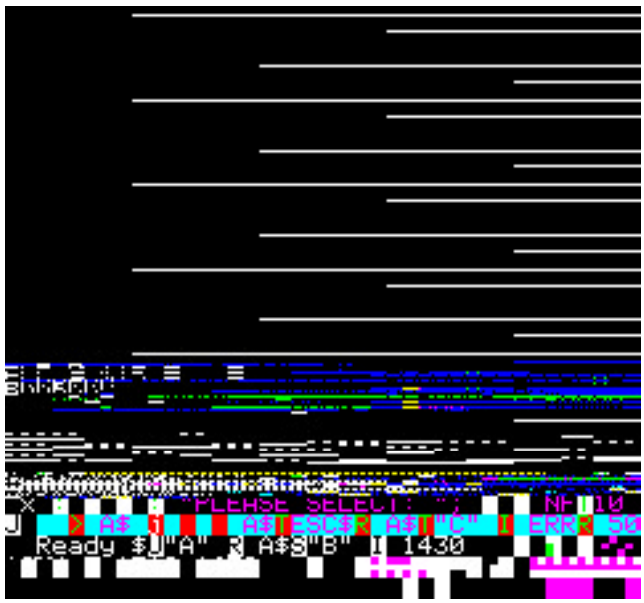
Soyez rassurés, d'une part la disquette trimestrielle de mars a échappé à la contamination, d'autre part le virus a été caractérisé et peut facilement être neutralisé. Si vous êtes contaminés, ce ne devrait donc pas être de notre fait. Les deux autres personnes touchées ont été prévenues à temps et ont pu détruire l'image DSK en cause. Reste que comme Dominique, vous avez pu être contaminé soit en surfant sur le oueb, soit en recevant une disquette ou un fichier DSK de quelqu'un qui a été lui-même contaminé.

De Quoi s'Agit-il ?

A notre connaissance, ce virus touche toutes les versions de Sedoric et seulement de Sedoric. Mais rien n'exclu que le s..... (le malfaisant) qui a agit si méchamment n'ait mis en circulation des virus spécifiques pour le FT-DOS ou pour d'autres DOS. Donc prudence !

Dans le cas du virus qui attaque Sedoric, il s'agit d'un patch qui modifie la commande DIR. Le virus n'est donc exécuté que lorsqu'on exécute la commande DIR patchée. En effet, le virus se présente sous la forme d'un fichier «mergé», c'est à dire collé à un autre fichier, qui peut être lui-même quelconque. Rappelons que lorsque plusieurs fichiers sont «mergés», un seul nom (celui du premier fichier) est affiché par la commande DIR. Mais le chargement du fichier qui apparaît au directory entraîne celui de tous ceux qui lui sont mergé, à leur adresse respective.





Donc, lorsque le fichier «porteur» est chargé, le virus est lui-même envoyé dans la zone #E349 à #E3C1. Son adresse de chargement se trouve en effet en mémoire haute, dans la RAM overlay, là où il y a la commande DIR de Sedoric. Le «virus-patch», écrase une partie du code de la commande DIR et en modifie la fonctionnalité. Lorsqu'on tape la commande DIR, tout se passe normalement, sauf que les adresses caractéristiques du dernier fichier affiché par DIR sont modifiées de manière à ce que le fichier soit envoyé dans l'écran texte (de #BB80 à BFDF).

Rien n'apparaît donc, tant que le dit fichier n'est pas lui-même chargé... dans l'écran texte ! Les figures jointes montrent des exemples du gâchis résultant, qui ressemble à s'y méprendre à un plantage. Et nous nous sommes mépris, pendant un bon bout de temps ! Notez qu'un seul type de fichier n'est pas affecté par le virus : les écrans texte, qui continuent à s'afficher au bon endroit !

Il est scandaleux qu'un ordinateur avec si peu de «fan» et sans aucun but lucratif puisse être l'objet d'une telle attaque... Quel est l'affreux qui via l' Internet, se cache derrière cela ? Pour essayer d'en rire, nous avons évoqué quelques possibilités. Ça ne peut tout de même pas être Microsoft qui craindrait pour son monopole ? Ou un ex-dirigent d'Oric, qui suffisamment aigri et ivre de rage de voir l'Oric toujours vivre et ne plus rien lui rapporter, serait passé à l'acte ? Non, vraiment, on a du mal à imaginer qui serait assez c.. pour faire ça !

Comment se Débarrasser du Virus ?

D'abord, toutes vos anciennes disquettes, tant que vous n'avez pas copié dessus un fichier récent, sont indemnes (attention toutefois au DIR effectué sur les disquettes non protégées contre l'écriture). Mais prudence pour les fichiers DSK que vous avez téléchargés depuis le 1er février 2001, ou pour les disquettes que vous avez reçues depuis cette date. Surtout ne faites pas un DIR «pour voir !»

La parade ne vient d'aucun antivirus pour PC ou Mac, mais tout simplement de la commande CHKSUM de Sedoric v3.0 qui affiche non seulement les checksums, mais aussi le détail de tous les fichiers mergés. Surtout, ne bootez pas avec la disquette suspecte, un DIR se trouve peut-être dans INIST, la chaîne des commandes initiales.

Bootez plutôt avec une disquette master Sedoric v3.0 protégée contre l'écriture, puis examinez toute disquette suspecte avec un CHKSUM«*.*», AUTO. Si le même nom de fichier s'affiche plusieurs fois, il s'agit d'un fichier mergé. Regardez s'il y a un constituant dont les adresses sont #E349 à #E3C1 et dont la CHKSUM (le dernier chiffre de la ligne) est #22AC.

Si oui, vous avez été contaminé. Effacez immédiatement ce fichier (un simple DEL suffit). Si c'est un fichier important, dont il n'existe pas d'autre copie, il faut simplement supprimer le fichier-virus de la chaîne des fichiers mergés. Pour cela, il faut quelques connaissances de Sedoric et un éditeur de disquette (genre NIBBLE ou BD-DISK). Si vous êtes dans l'embarras, envoyez votre disquette ou votre fichier DSK à André.

Conclusion / Consolation

Le virus attaque la commande DIR en mémoire. Ce n'est pas en soit un programme exécutable. Il n'est pas activé par le mode AUTO. Mais il patche le code d'une des commandes les plus utilisées et en modifie le comportement. Lorsque l'écran texte est «brouillé», il suffit donc de couper le courant pour arrêter les frais. C'est une situation dont hélas nous avons déjà l'habitude en temps normal. Le dommage est donc très limité. Reste que des fichiers importants peuvent être endommagés, voire perdus, à la suite de cette contamination et là, c'est impardonnable...