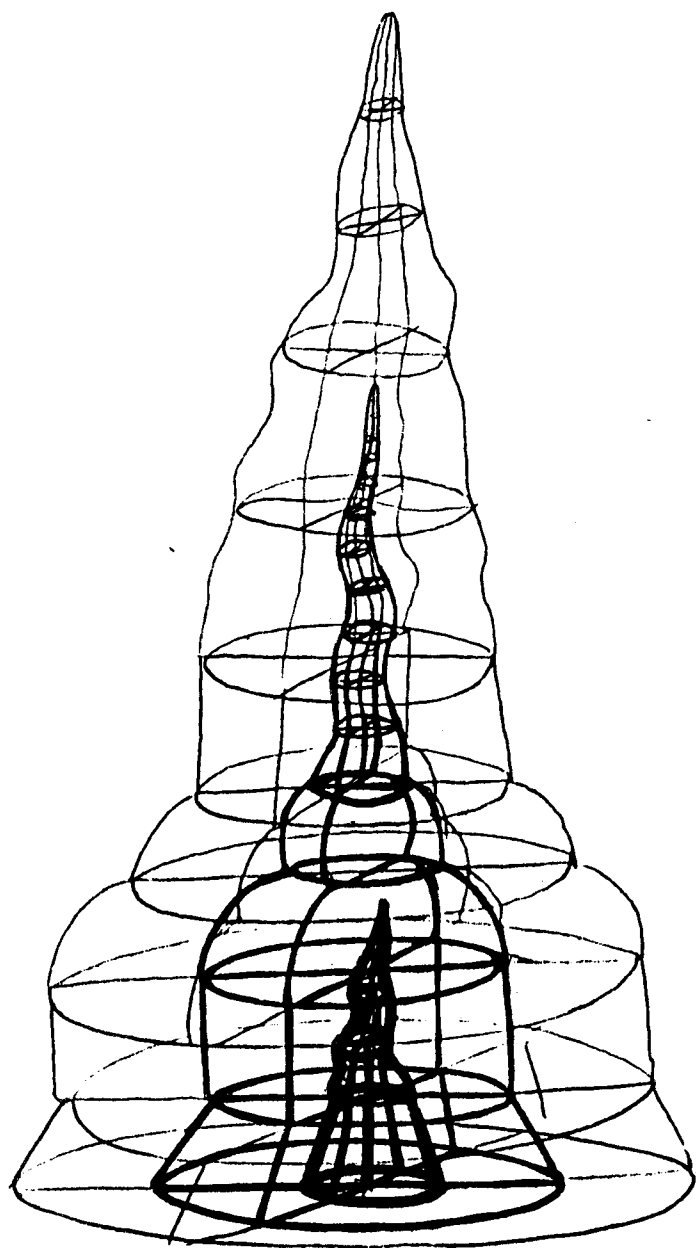


Chronique d'une épidémie

PAR JEAN-YVES SPARFEL



Evolution - ciels à l'intérieur
stari - du f

Dessin de Christian Todé extrait du Manifeste théorique,
aux éditions Les Immatériels.

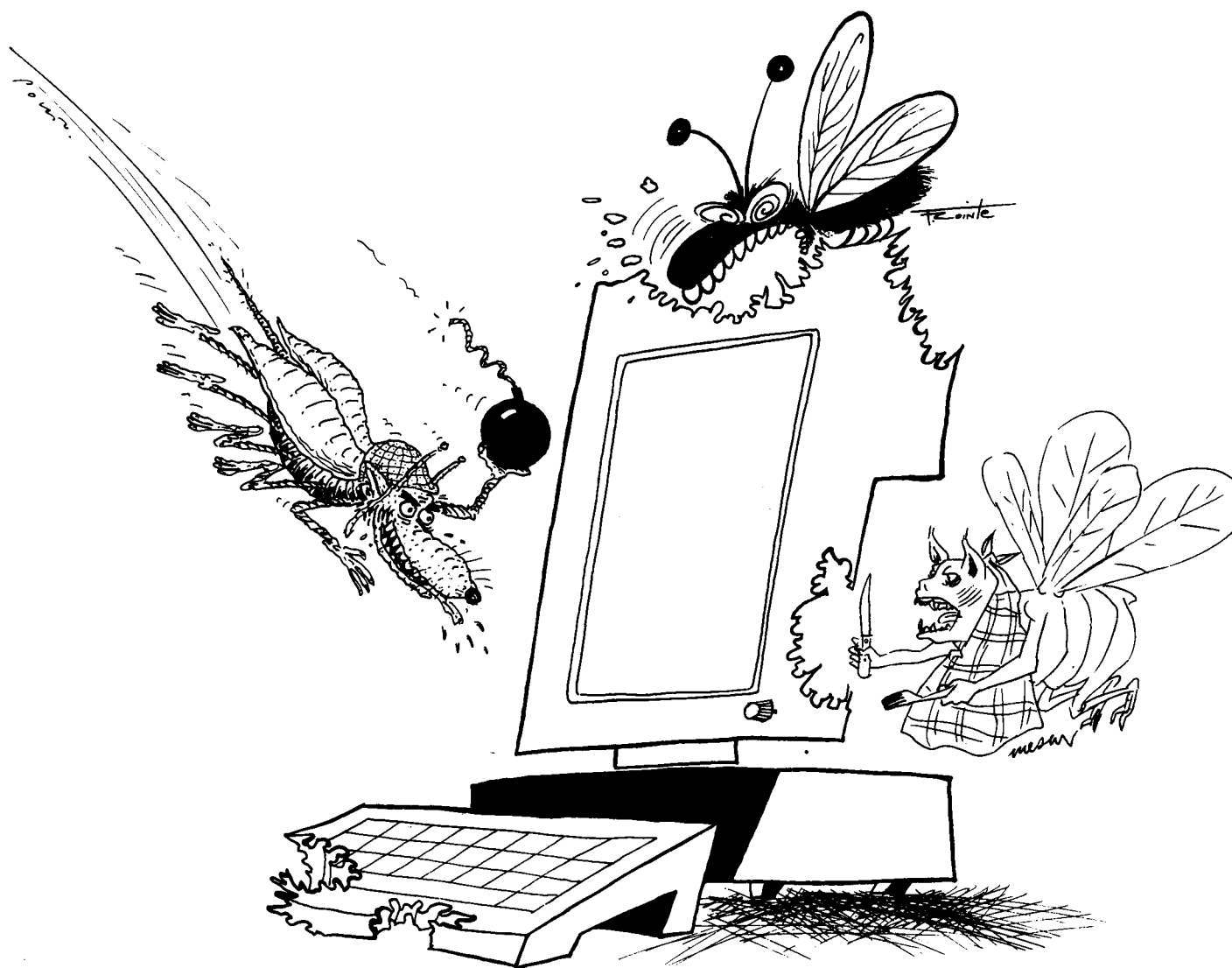
Aux discours sur la toute-puissance de l'ordinateur ont succédé ceux sur sa fragilité. Une campagne médiatique friande d'images, d'analogies et de métaphores biologiques et médicales a, l'année dernière, brandi la nouvelle menace pour l'informatique : les virus, avec comme corollaire l'obsession sécuritaire. Est-ce bien sérieux, docteur ? Nos ordinateurs auraient-ils la fièvre ?

De multiples définitions du virus informatique ont été données. Toutes plus ou moins bonnes, toutes plus ou moins parano. Relevons celle-ci figurant maintenant dans les manuels d'informatique : « séquence d'instructions introduite illicitement et subrepticement dans un programme afin d'altérer la finalité de son fonctionnement ». Les virus sont donc de courts programmes qui, cachés à l'intérieur d'applications, exercent une action double : l'auto-reproduction et le plus souvent la dégradation des logiciels atteints. L'histoire de ces virus remonte pratiquement à l'origine de l'ordinateur.

A cheval sur les ondes de choc

Un peu d'histoire donc ! Dès 1948, John von Neumann, le fondateur de l'informatique moderne, inventait déjà l'idée de codes auto-reproducteurs et l'exposait dans *Théorie et organisation des automates complexes*.

Plus tard, à la fin des années 70, le jeu *Core War*, créé par trois programmeurs des Bell's Laboratories, faisait fureur dans certaines universités américaines. Son principe reposait sur le fait que les programmes consommant des données, était proches des programmes eux-mêmes de par leur structure et leur support, il était possible de créer des programmes se dévorant entre eux. Les adeptes de ce jeu concevaient des pro-



grammes gloutons, baptisés “organismes” (et pas encore “virus”), se combattant les uns les autres. Le gagnant était celui qui conservait le maximum de programmes intacts à la fin du jeu. Cette passion de technicien, un peu confidentielle, fut révélée en mai 1984 par Dewdney, chroniqueur d'*American Scientific* avec mode d'emploi à la clé.

A la même époque, des programmes nommés *worm*, ver en français, furent mis au point pour permettre une pénétration des systèmes d'exploitation. Ancêtres des virus, ils sont une sophistication des jeux multi-utilisateurs. L'idée du ver provient probablement de la nouvelle de science-fiction *A cheval sur les ondes de choc*, de John Brunner, publiée en 1979. On y voit en effet un héros : le cavalier des ondes de choc, créatif et rusé, découvrir un ver de logiciel exécutant des ordres ciblés annoncés à l'avance. Dans un monde où les humains sont réduits à des codes informatiques, à une identité électronique, ce héros tient en échec de méchants adversaires et change d'identité à volonté. Ce programme *worm* se déplace dans des programmes porteurs. Associés à d'autres, ils se propagent dans tous les types de mémoire et peuvent peu à peu détruire des données, subtiliser des ressources.

Mis au point par des programmeurs et *hackers* (pirates) surdoués dans une atmosphère ludique, ces jeux, puis ces vers intéressèrent les scientifiques.

Des vers aux virus

Ken Thomson, un des auteurs d'Unix et du langage C, lors d'une remise de distinction en 1983, exposa à l'assistance comment les concevoir. Dans le même temps, en novembre 1983, lors de son séminaire à l'université de Californie du sud, Fred Cohen présentait les données théoriques de ce qui a été considéré comme le premier virus informatique. Une semaine plus tard, dans le cadre d'une activité universitaire, un virus simple fut construit sur un VAX 11/750, sous système d'exploitation UNIX, et introduit dans le programme pour mettre en branle un processus d'infection. Cette expérimentation, dont la répétition fut ensuite interdite par les autorités universitaires jusqu'en juillet 1984 — où un autre essai eut lieu sur un ordinateur UNIVAC —, permit à Fred Cohen de donner la définition suivante de la structure d'un “virus”.

Il se compose de deux éléments principaux : infection et tâches.

Self-reproduction : reproduction ou infection. Cela signifie que le programme est capable de créer des copies de lui-même et d'implanter ces copies dans d'autres programmes.

Functionality : tâche ou fonction de manipulation. Le programme est capable d'exécuter une tâche clairement définie.

Virus Parano

La définition succincte donnée par Fred Cohen (cf. ci-dessus) a connu quelques applications et surtout des complexifications.

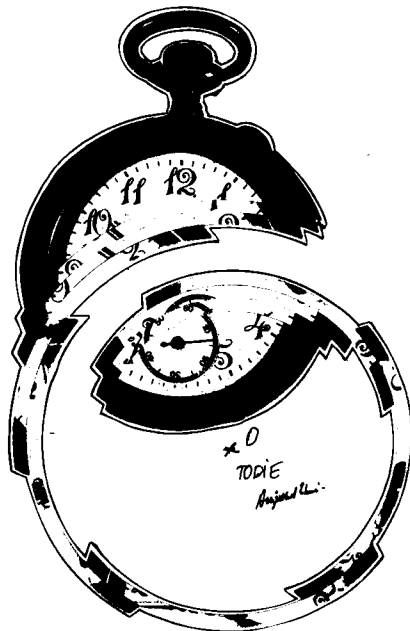
Technique

« Un virus est un programme autonome, self-réplicateur inséré dans les systèmes informatiques à l'insu de ses utilisateurs autorisés et destiné à en dégrader le fonctionnement. Par autonome, on souligne qu'une fois en place le virus accomplira son action (effacement et réécriture) de façon indépendante, remplissant sa mission sans aucun contact avec ses auteurs. La self-réplication du virus constitue son mode de production. » (*Micro-systèmes*, décembre 1988).

Technico-médicale

« Les virus sont des petits programmes qui, camouflés au sein d'applications, assument une double fonction. La première, véritable phase d'incubation, est un processus de multiplication par codes autoreproducteurs, destiné à leur permettre de migrer vers d'autres applications et d'y infecter tout porteur potentiel. La seconde, phase active celle-ci, consiste à produire des effets nocifs imaginés par le concepteur, le déclenchement s'opérant à un moment déterminé en fonction de l'horloge interne du microbe-horodateur ou compteur atteignant une date ou un incrément spécifique. Les virus ont ainsi pénétré au cœur de la cité informatique à la manière du cheval

de Troie.... Peu sectaires ils n'ont rien épargné, et dépourvus de systèmes immunitaires, minis, PL, et plus récemment Macintosh, sont tour à tour devenus la proie des microbes ». (*Data*, décembre 1988).



Analogie biologique

« L'OS est à l'ordinateur ce que l'ADN, ou code génétique, est à la cellule. Les deux, OS comme ADN, contiennent des milliers de recettes codées indispensables au fonctionnement et à la perpétuation du système. Dès lors, on flaire tout de suite un moyen d'aller trafiquer tout ça. Lorsque un petit bout d'ADN parasite se greffe sur l'ADN normal pour dicter une nouvelle conduite à la cellule infectée, on parle de virus biologique, genre grippe ou sida. On se sent obligé de baptiser le petit bout de programme informatique qui, greffé sur l'OS d'un ordinateur, va le rendre malade ». (*Nouvel Observateur*, novembre 1988).

Epidémie et métaphore

« Similitude aussi dans le mode de transmission. Un virus informatique se transmet soit par l'intermédiaire de disquettes contaminées, soit par des réseaux télématiques qui mettent en relation des ordinateurs différents. La "proximité" informatique, comme dans le cas du sida, accroît évidemment les risques de contamination... Il existe cependant un moyen efficace de se protéger : c'est le "préservatif électronique" ... » (*L'Expansion*, janvier 89).

Cette structure simple fut exposée par Fred Cohen en août 1984 dans une étude : *Computer Viruses, Theory and Experiments*, où il s'appuyait sur d'autres ouvrages, notamment celui du mathématicien américain Bailey : *Mathematical Theory of Epidemics*, paru dans les années 50, ainsi que sur Gum : *Use of Virus Functions to provide a virtual APL interpreter under user controls* (1974) et sur Shock : *The "Worm" Programs. Early Experience with a distributed Computation* (1982). Ainsi donc, l'idée de virus, d'épidémie, datait de longtemps... Elle allait se répandre, parfois de façon plus ambitieuse, au point d'aboutir en 1988 à ces cris d'alarme des médias français. « Informatique : le virus est au programme » (*Le Point*, 25 janvier) – « IBM : les cartes de vœux étaient empoisonnées » (*Libération*, 4 mars) – « Les stratégies perverses d'une épidémie » et « Attaque virale sur l'informatique » (*Libération*, 9 mars) – « Le génie et le vice » (*Décision informatique*, octobre) – « Décontaminez votre

ordinateur » (*Micro-systèmes*, décembre) – « Votre ordinateur a la vérole » (*Nouvel Observateur*, novembre) – et enfin, fin du fin, « Le Sida informatique » (*L'Expansion*, janvier 1989), pour n'en citer que quelques uns... Comme le remarquait dans *Terminal* de juillet 88 Jean Chesnaux, « le mot "virus" "est devenu aussi important que la chose », objet de transfert, métaphore avec un « vocabulaire employé qui n'a rien d'innocent » puisqu'il vise à suggérer « qu'il s'agirait d'une sorte d'agent malfaisant attaquant de l'extérieur un organisme sain ».

De quelques typologies

Comme le but du programme-parasite nommé virus est de s'autoreproduire, de se copier lorsqu'il rencontre un programme non contaminé, et pas seulement de perturber le fonctionnement des applications, sa diffusion s'est développée à l'occasion d'échanges

De quelques virus célèbres...

Une cinquantaine de virus ont déjà été isolés et répertoriés. Citons-en quelques uns. Les virus, qui ne sont pas à confondre avec les bombes logiques, les vers ou les chevaux de Troie, techniques de sabotage de programmes ou de matériel, empruntent à ces techniques, mais ont la particularité de se reproduire. Se sont ainsi reproduits :

Le virus de Lahore. Deux frères commerçants pakistanais, vendant des copies de logiciels haut de gamme comme Lotus 1. 2. 3 ou Word, infectent des disquettes vendues surtout aux Américains à bas prix. Les victimes voient s'afficher sur leur écran : « Bienvenue dans le donjon, contactez-nous pour obtenir le vaccin ». Suivait le prix : 2 000 dollars mais aussi le numéro de téléphone qui permit à la police de les cueillir. Ce Pakistanais, Brain, "infesta" 10 000 IBM PC aux USA.

Le virus "israélien", dit aussi "palestinien". Une bombe logique devait se déclencher à retardement le 11 mai 1988, 40^e anniversaire de la création de l'Etat d'Israël, bloquant le fonctionnement des ordinateurs de l'Hebrew University et détruisant les informations en mémoire. Localisé, le virus fut bloqué dans son développement à cause d'une faute technique du saboteur.

Le virus Christmas ou la carte de vœux IBM. Sur le réseau Earn, un professeur allemand de Klaus Hall envoyait une carte de vœux en décembre 1987. Au moment où le destinataire la consulte, le programme Christmas devait être capable de répéter toutes les adresses électroniques

de ses correspondants habituels. Entre la récurrence de certains noms sur les répertoires et l'effet réseau, le point de saturation fut atteint le 9 décembre 87. Le 11 décembre, l'épidémie était contrôlée.



Le virus de Robert Morris Junior. Sur le réseau Arpanet, reliant quelques centaines de laboratoires universitaires ou industriels, y compris certains de la Nasa, cet étudiant de Cornell University de New York injecta un virus fabriqué sur son ordinateur personnel. Le 4 novembre 1988, 6000 ordinateurs tombèrent en panne. En principe, ce virus devait être inoffensif. Par suite d'une erreur de programmation, il se multiplia à toute vitesse, accaparant toute la puissance de calcul des ordinateurs contaminés. Robert Morris est le fils de Robert Morris senior, patron de la sécurité informatique au National Computer Security Center de

Bethesda. Il risque la prison. Où mène l'Œdipe...

Le Boot Sector Virus. Il sévit sur Atari. Une fois chargé en mémoire centrale, il s'attache aux commandes d'appel du système liées aux fonctions disques. Il élabore des stratégies de destruction et de réplication.

Le Ram's RAM. Toujours sur Atari, il simule un mal fonctionnement de la mémoire centrale, incitant un recours à la maintenance pour défaillance de composants, en pure perte (de temps).

Les virus du DOS. Ils se servent de ce dernier de l'intérieur, utilisant des secteurs en bon état, qui seront ensuite désignés comme étant défectueux. Ils les occupent alors pour se camoufler.

Le virus nVIR. Agit dans les Macintosh. Nommé ainsi d'après le nom de la ressource supplémentaire qu'il crée dans le système, il émet un bip sonore lors du déclenchement des programmes. Sur l'émulateur vocal de certains "mac", certains ont ainsi entendu "don't panic". Il se pourrait qu'il soit l'œuvre d'un Allemand de l'ouest, Mathias Urliches, qui voulait avertir la communauté Macintosh des risques viraux.

Les virus Scores. Toujours sur Macintosh. Alors qu'un nVIR se contente de se reproduire, Scores s'attaque au Mac en le faisant se planter aléatoirement, en détruisant des fichiers, en réalisant d'autres méfaits. Facile à détecter. Le service antiviral d'Apple a mis au point des vaccins adaptés.

J.-Y. S.

de disquettes et de communications sur le réseau. On peut donc parler de contagion, car l'effet est d'autant plus répercuté si le virus est implanté sur un logiciel d'exploitation fréquemment appelé comme le Command-Com des P.C. Ces connexions facilitent la propagation, "l'épidémie" mais au sens premier de ce terme et non comme monstrueuses interventions pathologiques.

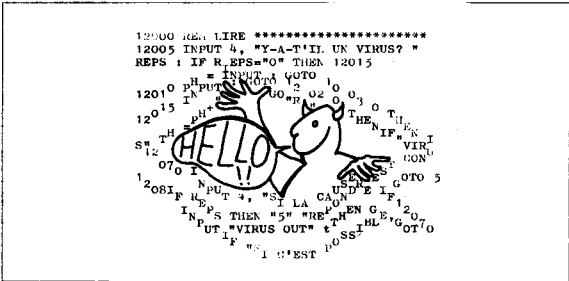
Il apparaît à de nombreux spécialistes qu'un programmeur moyen, avec de bonnes informations sur le système d'exploitation, peut fabriquer un virus. Seule l'ampleur du programme limite l'imagination, car il doit rester inaperçu. L'imagination peut produire de gentils virus : par exemple celui qui, au moment de la sauvegarde, "rétrécirait" tous les fichiers, les condensant afin de tenir moins de place en mémoire ou celui permettant de joyeux messages sur les écrans. Le cas s'est produit.

Mais les virus qui ont fait couler le plus d'encre

— et qui ont aussi coulé des ordinateurs — sont plutôt méchants. Dans leur livre : *Danger, pirates informatiques*, paru récemment ¹, les auteurs du *Chaos computer club* (association des hackers allemands) les recensent ainsi :

« Il y a les virus écraseurs, qui normalement détruisent la victime à l'intérieur de laquelle ils se copient. Même le programmeur du virus ne peut évaluer quelles fonctions du programme seront attaquées. Avantage du virus écraseur : comparé avec le programme original, le programme porteur n'indique pas de modification notable de la mémoire nécessaire. Il y a les virus non-écraseurs qui laissent le programme en état de fonctionner, mais qui occupent en mémoire une place attirant l'attention sur leur existence. Il y a les virus résidant en mémoire qui se répandent dans la mémoire vive. Leur vitesse de propagation est particulièrement grande. De plus tous ces virus peuvent cacher leur présence. Ils peuvent changer constamment de

¹ Cf. la note de lecture dans ce même numéro, p. 17.



forme, chaque génération comportant certaines variantes. Ceci empêche en particulier la recherche et l'effacement systématiques, puisqu'il n'est jamais certain que toutes les variantes aient été décelées. Des virus peuvent s'effacer eux-mêmes d'un programme, brouillant ainsi les pistes. Il devient alors impossible de remonter à la source d'une infection. »

D'autres typologies ont été tentées pour cerner les effets des virus : selon leur lieu d'apparition (californien ou israélien), selon leur fonction (observation, espionnage ou action destruction), selon leurs lieux d'application enfin. En tout cas, les effets peuvent être redoutables et aller, dans le cas des systèmes centraux, jusqu'au blocage du site et à la destruction logique de toutes les sauvegardes successivement installées. Les instructions complémentaires ajoutées à l'écran apparaissent dès lors comme d'aimables plaisanteries... surtout au regard d'une autre technique de virus : "le cheval de Troie". Ce dernier n'agit en effet que de façon ciblée : il ne se fixe dans un autre programme que lorsque cela répond à un objectif fixé ; il avance pas à pas dans un réseau ou un ordinateur jusqu'à ce qu'il atteigne l'endroit de sa mission. Les étapes intermédiaires peuvent être effacées et le cheval de Troie attend alors une instruction pour agir : un mot-clé, un élément de communication, une heure. Plus tard, il peut être rattrapé et effacé. Alors que les virus simples finissent par être remarqués un jour ou l'autre car ils saturent l'ordinateur jusqu'à la panne, le cheval de Troie peut conserver l'incognito. Il est surtout dangereux pour les grands ordinateurs.

Si ces typologies ont commencé à être établies, c'est que les virus ont été repérés, notamment parce que les victimes ont été nombreuses avec quelques cas spectaculaires (cf. encadré : les virus célèbres).

L'analogie a ses raisons...

Les Etats-Unis ont été plus touchés que l'Europe et la France. On estime maintenant à quelques centaines de milliers les IBM.PC qui auraient été, aux USA, endommagés notamment par la destruction de FAT (File Allocation Table) ou de master boot, interdisant l'utilisation de disquettes et de disques durs. Les effets de cette contagion ont été d'autant plus connus que les virus ont quitté le monde des gros ordinateurs pour apparaître sur les micros. Si une certaine infrastructure, des ingénieurs-système peuvent dans une entreprise éviter de gros dégâts, il n'en va pas de même chez les particuliers : ceux-ci ne connaissent généralement rien au fonctionnement interne de leur micro-ordinateur, ni aux règles de sécurité informatique. La surprise fut donc très grande de voir apparaître des virus dans le monde des Macintosh, que l'usage personnel, l'absence de télécommunication semblaient garantir contre l'épidémie. Pratiques conviviales,

l'échange et la copie de disquettes favorisent là aussi la transmission des virus. Dès lors, plus personne ne semble à l'abri. C'est ainsi que l'idée de contamination généralisée a pu prendre corps avec son cortège de scénarios catastrophistes, renforçant les discours sécuritaires face à cette nouvelle "maladie".

A qui profite le virus ? Tout d'abord à celui ou celle qui le programme. Leur plaisir est difficile à analyser : revanche, mégalomanie, autre rapport à la machine, malveillance... y entrent certainement.

D'autres bénéficiaires se trouvent parmi la hiérarchie de certaines entreprises d'informatique, de progiciels, qui voient là des arguments pour la reprise en main de la micro dont des utilisateurs devenaient trop indépendants à leur goût. Ainsi des notes de service sont apparues dans diverses entreprises, empêchant les utilisateurs de se servir d'autres programmes que ceux vérifiés et autorisés par la Direction Informatique. La peur de l'épidémie intervient là comme limitation du convivial.

...que le marché de la sécurité informatique n'a pas ignorée

Enfin, la crainte du virus, en même temps que la nécessité de le définir et le localiser, a élargi la prise de conscience sur la sécurité informatique en même temps que son marché ². En effet, la société informatique est liée, d'une manière bien plus importante qu'elle ne l'imaginait, à la fiabilité de ses systèmes dont les virus et les chevaux de Troie ont montré la vulnérabilité. Les virus ont donc agi comme systèmes-experts démontrant que la sécurité entraînait assez peu en ligne de compte dans la mise au point des systèmes.

Dès lors, les spécialistes se sont mis à parler de "dépistage", de "prophylaxie", de "destruction des foyers d'infection", d'"immunité" et un peu de motivation du personnel. La métaphore a poussé sa logique jusqu'au bout avec les "vaccins" anti-virus, les "préservatifs" de disquettes, les "mises en quarantaine" de logiciels douteux, les clients "à risque"... Les excès métaphoriques, outre l'idéologie d'exclusion à laquelle ils se réfèrent ³, ne doivent pas être l'arbre cachant la forêt : le marché de la lutte contre les virus a devant lui de belles potentialités, qu'il s'agisse de prévention, de diagnostic ou de soins.

Le malaise provoqué par l'apparition du virus est loin de se dissiper. L'article de Jean-Pierre Cahier, ci-après, explique pourquoi. Pour l'instant, les programmes spéciaux de détection de virus sont souvent diffusés à prix coûtant ou gratuitement par certains producteurs de micros ou de logiciels (c'est le cas d'Apple ou d'Atlas Informatique). Aucun de ces vaccins (Virus RX, Kill scores, Viraid, Virusafe, Vaccinate, Data physician, Anti-virus, Vaccine, T Cell, pour en nommer quelques uns) n'a la prétention d'être infaillible, surtout que les programmeurs de virus ont pris un malin plaisir à les prendre en défaut : ainsi International Computer diffuse depuis peu un anti-antivirus car le vaccin lui-même était devenu inopérant. Si les virus n'ont constitué en 1987 que 9% des délits informatiques observés en Europe, les logiciels de protection de réseaux vont se

2 Cf. l'article sur le congrès de Securicom, p. 22.

3 Fort bien analysée par Isabelle Riéusset dans son article, L'Imagination rurale, paru dans la revue Traverse, juillet 1988.

développer et la "virustique" pourrait bien devenir une nouvelle spécialité des programmeurs, avec comme tâche essentielle la surveillance de la taille des fichiers d'exécution.

Aux yeux d'autres commentateurs comme Roland Moreno, directeur d'Innovation (carte à puces), la prévention et l'éducation des utilisateurs constituent "la seule parade sérieuse". Ainsi l'usage de copies illécitales de logiciels est montrée du doigt et les éditeurs de logiciels "sains" se frottent les mains au point qu'on les suspecte d'avoir entretenu cette brusque fièvre des ordinateurs. On le voit, cette méfiance n'épargne personne...

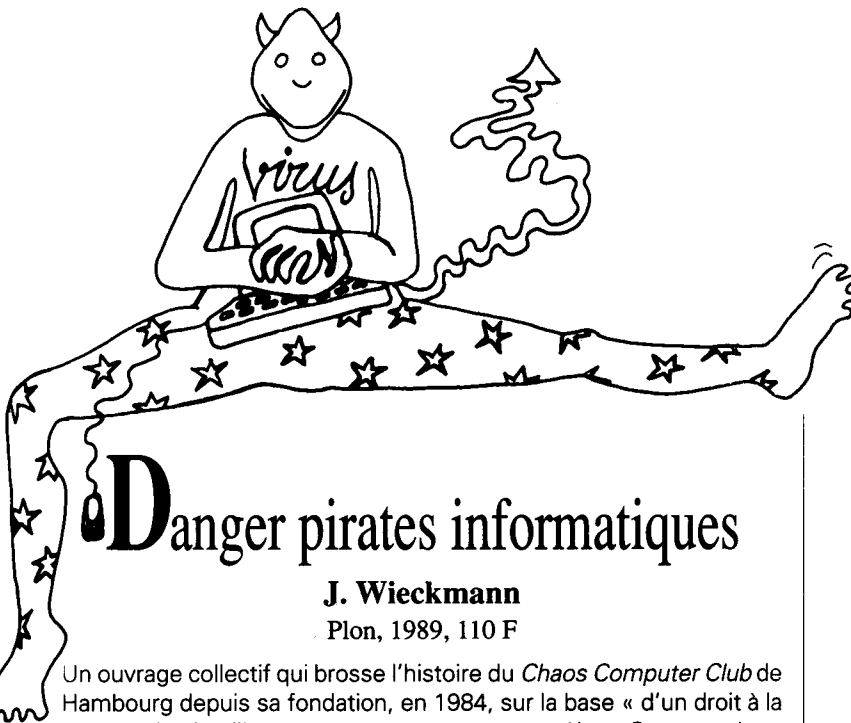
Ainsi, Apple rappelait à ses clients quelques précautions essentielles : *backup* multiples et réguliers, utilisation de logiciels provenant de sources sérieuses et éprouvées, tests intensifs préalables en environnement stérile pour toute disquette suspecte, verrouillage systématique des disquettes originales. Enfin, certains qui ne croient pas trop à la psychose du virus rappellent que le comportement anormal d'un ordinateur ne lui est pas toujours imputable et que le cafouillage d'un programme peut aussi provenir d'un simple bug.

Qui est malade ?

Si la vieille formule : "rien ne sort de la machine que ce que nous en attendons" a été mise à mal par des programmeurs non identifiés, l'affirmation selon laquelle les ordinateurs seraient malades prête à rire. Cela signifierait son autonomie, son humanité. Les ordinateurs n'ont pas de point de vue sur les programmes qu'on leur ingurgite : ils les appliquent ou pas, à moins qu'on ne leur ait été donné l'ordre de n'obéir qu'à leur propriétaire.

Sont-ils malades ceux qui, transgressant cette propriété individuelle, dérangent les ordres de leurs voisins, piratent des systèmes qui leur ont été livrés clés en main avec la recommandation : "tais-toi et applique", veulent en savoir plus et même détruire les hiérarchies des concepteurs ? Farce ou sabotage, mise en cause des centralités, les virus ont ouvert un autre débat : celui de la diffusion des savoirs technologiques. Ainsi le *Chaos computer club* pose la question : « Différents programmeurs modifient constamment les systèmes d'exploitation, qui se retrouvent chamboulés selon les besoins internes... et les marottes des programmeurs. Il est rare que ceux-ci gardent des traces de ces petites modifications. Au bout de quelque temps, une personne extérieure aux services aura du mal à saisir le déroulement des programmes. Ces schémas sont aujourd'hui à des années-lumières d'une structure modulaire contrôlable ».

La question : informatiser quoi, où, comment ? rebondit. « Certes, un ordinateur n'est-il pas conçu pour être un média au service d'une fin ? Mais à une époque où les enjeux de pouvoir s'avouent plus que jamais pour ce qu'ils sont : des conflits d'intérêt pour la maîtrise d'interfaces, il semble difficile de ne voir dans le contrôle des réseaux informatiques que des moyens et non des fins dans la mesure où ils sont non seulement outils, mais buts de nombreuses stratégies, qu'elles soient politiques, économiques ou guerrières », conclut Isabelle Rieusset³. En effet, c'est là que les virus portent le débat. L'épidémie en cache une autre. ■

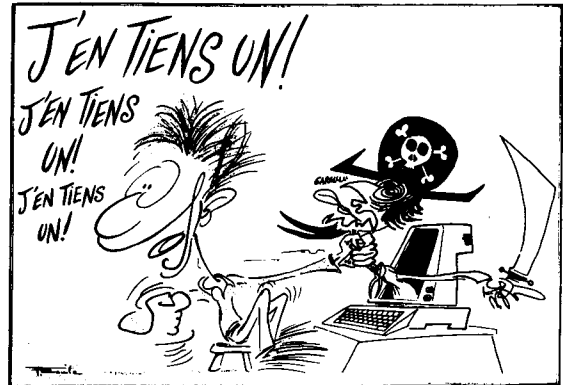


Danger pirates informatiques

J. Wieckmann

Plon, 1989, 110 F

Un ouvrage collectif qui brosse l'histoire du *Chaos Computer Club* de Hambourg depuis sa fondation, en 1984, sur la base « d'un droit à la communication libre sans entrave et sans contrôle ». On aperçoit un monde d'initiés qui s'échange des informations, s'affiche publiquement, qui perturbe le minitel allemand, visite le réseau SPAN de la NASA, édite ses revues spéciales, se faufile chez Philips et au CERN.



Puis viennent les virus, les bogues, et en 1986 la loi allemande sur les délits informatiques, les actions de la police du BKA à la recherche de pièces à conviction. On voit la crainte de la part des membres du CCC que l'action de la police ne conduise à l'apparition d'un underground informatique incontrôlable, sans éthique. L'ouvrage se termine sur la critique de la diffusion de jeux informatiques explicitement nazis, anti-Turcs, avec des SS...

Ces *hackers*, "accros" de l'informatique posent publiquement le problème de la diffusion, de la conception de l'informatique. Pour faire partie du CCC, inutile d'avoir une carte de membre. Il suffit de se passionner pour les possibilités de l'ordinateur, de rejeter cette foi aveugle en la technique, de stimuler l'esprit de contradiction et de ne pas se laisser éblouir par les prouesses des producteurs. Le piratage, c'est le refus d'être attaché pieds et poings liés à une machine, de devenir émetteur. Leurs aventures leur ont valu des démêlés avec la justice, la police, les médias. "Fous d'informatique", ils ont été accusés de terrorisme, d'accointances avec la Bande à Baader, rejetés par les alternatifs allemands, puis tout simplement considérés comme des saboteurs. Ce ne sont pas des adversaires de l'ordinateur, bien au contraire. Ils explorent les possibilités, les rigidités, les secrets, les fragilités. Ils ne sont pas pour rien dans la naissance de quelques virus, dans la non-installation du BTX, le projet de minitel allemand.

Leur livre jette les bases d'une autre culture informatique avec un humour sur leurs propres ambiguïtés, une lucidité sur l'informatisation de la société, très agréables à constater. Il est habité par cette question : « Qui dirige réellement le développement de la société informatique : les hommes politiques, les chefs d'entreprise ou les programmeurs de systèmes ? » Elle est essentielle.

JYS-JM