LE COIN DE LA SÉCURITÉ INFORMATIQUE

SÉCUR IT

Michel-Ange se balade dans on ordinateur et refuse d'en sortir *ou* Comment j'ai appris à cesser de m'inquiéter et à faire échec aux virus

Les virus informatiques font l'objet de beaucoup de publicité dès que les médias entrevoient la possibilité d'en tirer quelque nouvelle qui fera sensation. Songez par exemple à ce qui s'est produit il y a trois ou quatre ans, alors qu'ils annonçaient que le virus baptisé Michelangelo s'apprêtait à détruire tous les ordinateurs de la planète. Le but du présent article est de vous fournir quelques notions de base au sujet des virus (tels qu'ils fonctionnent dans un environnement d'OP de type IBM), et de vous donner des trucs pratiques pour vous éviter d'avoir à y faire face et pour percer le mystère qui les entoure, de manière à dissiper une bonne partie de vos CID (craintes, incertitudes, doutes).

Les virus informatiques font désormais partie intégrante du monde cybernétique. Vous allez certainement en être victime, comme d'ailleurs d'autres personnes de votre connaissance. Peut-être même perdrez-vous des données à cause d'eux, et sans doute en entendrez-vous de belles à leur sujet (comme cette histoire de virus « Good Times » sur l'Internet — qui n'est qu'une vaste plaisanterie)

Il existe principalement deux types de virus informatiques : les virus de type secteur de démarrage, et les virus de type dispositif d'infection de fichier. Ils se ressemblent beaucoup du point de vue des résultats qu'ils provoquent, mais leur façon de se propager est très différente. Il est important de bien comprendre ces différences pour pouvoir les combattre efficacement et éviter de les attraper. Ne laissez pas la terminologie médicale (virus, infection, vecteur, etc.) utilisée à leur égard vous convaincre qu'ils sont plus complexes qu'ils ne le sont en réalité.

Il importe d'abord de préciser qu'un virus informatique n'est rien d'autre qu'un petit programme informatique enregistré par un programmeur. Les virus se comportent comme des programmes et remplissent un objectif ou visent un résultat.

Les virus de type secteur de démarrage sont de loin les plus courants au MAECI. Voyons comment ils fonctionnent. Tout disque d'ordinateur, qu'il s'agisse d'un disque dur ou d'une disquette, est doté d'un programme d'amorçage situé au tout début du disque. On parle d'amorçage du fait qu'il s'agit d'une séquence d'instructions initiales qui enclenche le processus par lequel l'ordinateur va ensuite pouvoir se lancer (s'allumer) lui-même. Les ordinateurs contiennent habituellement tout juste l'essentiel, en fait de codes microprogrammés, pour leur permettre d'enclencher le processus de démarrage et de poser certains diagnostics simples. Ces codes commandent aussi à l'ordinateur de consulter le secteur d'amorçage du premier disque pour connaître la suite des opérations à effectuer.

Ce que nous venons de décrire correspond exactement à ce qui se produit lorsque vous mettez en marche votre ordinateur. Le microprogramme effectue certains diagnostics initiaux, puis transfère le contrôle du système au secteur d'amorçage du disque rigide (ou disque C) qui prend en charge la suite du processus de démarrage. S'il y a une disquette dans le lecteur de disque A au moment où vous lancez l'ordinateur, ce dernier tentera en premier lieu de lire le secteur d'amorçage de cette disquette. Si la disquette en question n'est pas un disque système (et n'est donc pas amorçable, puisque les codes appropriés n'ont pas été programmés dans son secteur de démarrage), le système affichera un message d'erreur vous indiquant qu'il ne s'agit pas d'un disque système ou que le disque comporte une erreur et vous demandant de remplacer le disque et d'appuyer sur une touche quelconque. Il ne vous restera plus alors qu'à vous demander où vous pouviez bien avoir la tête, à retirer la disquette du lecteur de disque A et à appuyer sur une touche quelconque, comme demandé. Le système relancera alors le processus d'amorçage à partir du disque dur. Les virus de type secteur de démarrage mettent à profit ce « comportement » des ordinateurs. Ils sont programmés pour s'infiltrer dans le secteur d'amorçage des disques. Lorsque l'ordinateur est mis en marche, le système va chercher les renseignements dont il a besoin dans le secteur d'amorçage, et charge du même coup le ou les virus qui s'y trouvent, lesquels peuvent alors entrer en action et commencer leurs ravages. Parmi les virus de ce type figurent les virus Stoned, Michelangelo, NYB, Monkey et Form — qui diffèrent tous du point de vue des dégâts qu'ils provoquent, mais qui ont en commun le fait qu'ils se dissimulent dans le secteur de démarrage.

Les virus de type dispositif d'infection de fichiers diffèrent des précédents en ce qu'ils se logent dans les fichiers exécutables. Examinons leur mode de fonctionnement. Une connaissance vous prête une disquette contenant les meilleurs jeux informatiques récemment mis sur le marché. Vous insérez la disquette dans le lecteur de l'ordinateur, en prenant soin de ne pas amorcer le système alors qu'elle s'y trouve déjà, et vous lancez le jeu à partir de cette disquette, en tapant JEU.EXE. Le virus qui se cache à l'intérieur du programme est exécuté en premier et le programme par la suite seulement, de sorte que pendant la durée du jeu, vous ne constatez rien de particulier. Toutefois, pendant ce temps, le virus s'affaire, infectant votre système et causant les dégâts pour lesquels il a été programmé. Le virus baptisé Jerusalem, par exemple, provoque l'affichage à l'écran d'un rectangle noir mouvant et changeant de dimensions. Un autre virus, appelé Cascade, entraîne la chute des lettres, une à une, au bas de l'écran, où elles s'amoncellent en désordre. Imaginez que pendant que vous êtes innocemment en train de vous amuser à détruire les vilains extraterrestres qui tentent d'envahir la Terre, le virus s'amuse, lui, à détruire l'important rapport budgétaire qui allait, pensiez-vous, vous permettre d'obtenir une promotion. D'autres exemples de virus de ce type comprennent les virus Dark Avenger et Friday the 13th.

Pour rendre les choses encore plus intéressantes, de nouveaux virus combinent les caractéristiques des deux types - les virus Natas et One-Half, par exemple, se rangent dans cette catégorie. Cela signifie, en d'autres termes, qu'ils se propagent des deux façons.

Alors, comment faire échec aux virus? Il convient de prendre certaines précautions fondamentales. **D'abord, dotez-vous d'un programme efficace de détection des virus.** Le MAECI utilise le programme ViruScan de McAfee. **Vérifiez au moyen de ce programme de détection chaque nouveau programme ou chaque nouvelle disquette que vous avez l'intention de charger dans votre système; cela s'applique aussi bien aux logiciels commerciaux ou prêts à l'emploi qu'aux disquettes préformatées.** Signalons que le SIGNET-D offre, à partir du menu Utilitaires du Gestionnaire de programmes de Windows, un programme de détection des virus permettant de vérifier les disquettes. N'oubliez pas non plus de vérifier les fichiers que vous obtenez à partir de babillards électroniques, et les disquettes et programmes que vous prêtent des collègues. Pour vérifier votre disque dur, ou l'ordinateur que vous possédez à la maison, vous devrez vous munir d'une disquette protégée en écriture contenant certains fichiers DOS essentiels et le programme de vérification. Si vous ne savez pas comment procéder ou que vous ayez besoin d'aide, communiquez avec votre Administrateur des systèmes SIGNET, qui peut vous indiquer la marche à suivre.

Assurez-vous de ne pas laisser de disquettes dans votre ordinateur plus longtemps qu'il ne le faut. Par ailleurs, vérifiez toujours que votre lecteur de disque A ne contient pas de disquette avant de fermer votre ordinateur, ce qui réduira les chances que vous lanciez par mégarde votre système alors qu'une disquette demeure dans votre lecteur et que vous récoltiez ainsi un virus de type secteur de démarrage. Si vous devez réamorcer votre ordinateur pour une raison ou une autre, parce qu'il y a eu une panne ou que votre système a figé, par exemple, n'oubliez pas de retirer du lecteur la disquette qui s'y trouve, le cas échéant, afin de ne pas réamorcer accidentellement votre système à partir d'une disquette.

Surtout, si vous découvrez qu'un virus a infecté votre système, NE PANIQUEZ PAS. Vraisemblablement, la petite bête a déjà eu le temps de causer les dégâts qu'elle a été programmée pour causer, de sorte qu'il ne sert à rien de s'inquiéter. Si vous savez ou vous soupçonnez que votre ordinateur est contaminé par un virus, appelez votre Administrateur des systèmes SIGNET, qui peut vous aider à mener à bien le nettoyage de votre système.

Pour conclure, si vous prenez les précautions qui s'imposent et que vous les intégriez à vos habitudes, vous réduirez grandement vos chances de perdre des données en raison d'une infection causée par un virus.

Nouvelles du SIGNET est publié une fois par mois par la Direction des services à la clientèle du SIGNET (STC) et diffusé au Canada et dans les missions à l'étranger à tous les fonctionnaires du ministère des Affaires étrangères et du Commerce international.

Les unités qui veulent faire paraître un avis dans *Nouvelles du SIGNET* sont priées de faire parvenir le texte à STC accompagné d'une note de service signée par leur directeur. Tous les lecteurs sont invités par ailleurs à envoyer, par ICONDESK, (Suggestions) les ébauches d'articles qu'ils désirent faire publier.