Les antivirus

Introduction: Les sources d'information sur les antivirus

- Internet: l'interrogation de l'annuaire de recherche Yahoo et du méta-moteur Copernic a permis de trouver l'adresse des sites web des éditeurs de logiciels antivirus. De là, de nombreux professionnels ont été contactés par messagerie électronique, mais aucune réponse n'a été reçue à ce jour. La documentation trouvée sur le Web, précise sur le plan technique (hormis la mention des prix), n'offre aucun jugement critique sur les produits présentés: une source spécialisée et critique devait donc être consultée
- les périodiques: la consultation de revues spécialisées en informatique a permis de trouver un important dossier sur le sujet ainsi qu'un test comparatif des produits les plus commercialisés. Ainsi, des documents critiques se sont ajoutés aux documents commerciaux
- les fiches techniques de certains logiciels ont pu être trouvées dans des magasins spécialisés (FNAC)

1)Présentation rapide du problème

Un virus est un programme informatique susceptible d'entraîner des perturbations dans le fonctionnement d'un ordinateur en dénaturant ses programmes exécutables ou ses fichiers systèmes. La plupart des virus informatiques ajoutent des commandes dans le fichier cible lorsqu'ils sont chargés en mémoire. Ces commandes ralentissent, empêchent l'exécution ou détruisent intégralement les fichiers visés.

Trois grandes familles de virus existent:
-les virus de *boot*: infectent le système par l'intermédiaire d'une disquette en se logeant dans le secteur de démarrage du disque dur
-les virus de fichier: corrompent les fichiers exécutables (exe, bat, ini, etc.), peuvent déjouer les protections antivirus, devenir résidents et accéder directement aux ressources systèmes de l'ordinateur
-les macro-virus: s'en prennent aux documents contenant des macros, emploient les langages scripts présents au sein des outils bureautiques pour se diffuser.
Ces derniers virus constituent les 80% des virus actuellement en circulation. Les dégâts sont considérables pour les entreprises, puisque le virus macro détruit notamment des documents Word, Excel ou Access. En même temps, les macro-virus sont les moins dangereux car les plus simples à combattre.
Auparavant, les virus informatiques s'échangeaient par le biais de disquettes. Aujourd'hui, les réseaux et Internet constituent le principal vecteur d'infection et voient apparaître de nouvelles formes de virus, les vers (se propageant à travers les réseaux) et les chevaux de Troie (programme de contrôle total de l'ordinateur à distance). La seule manière de détecter et d'éradiquer les virus est d'utiliser un logiciel antivirus, moteur de recherche de virus, afin de scanner toute nouvelle information insérée dans l'ordinateur.

Cependant, environ quinze nouveaux virus apparaissent quotidiennement. Le logiciel antivirus doit donc être le plus récent et le plus actualisé possible, sachant qu'il existe toujours un délai entre l'apparition d'un nouveau virus et l'élaboration de la parade. Acheter un antivirus ne suffit pas: il est nécessaire de mettre à jour (via Internet, CD-Rom,...) son antivirus régulièrement.
Ainsi, les éditeurs de programmes antivirus disposent souvent d'un laboratoire de recherche chargé d'identifier les nouvelles espèces de virus. Toutes les caractéristiques des virus sont répertoriées dans une base de données mise à jour quasi quotidiennement: c'est en effet dans la détection de nouveaux virus que l'on peut mesurer l'efficacité des logiciels antivirus.

2) Le marché de la sécurité antivirale

La protection contre les virus est devenue un véritable *business*. On peut s'interroger sur l'éventualité d'une communauté d'intérêt unissant les codeurs de virus et les marchands d'antivirus. Les premiers se satisfont de donner du fil à retordre aux seconds et font un commerce florissant avec les mises à jour mettant au défi la création de nouveaux virus.
Cependant, avec l'introduction d'Internet dans les foyers et dans les entreprises, la sécurité antivirale est plus que jamais indispensable: chacun se trouve confronté au choix d'un logiciel antiviral[1].
La multiplication des échanges (courriers électroniques, groupes de news, forums de discussions...) et des connexions soumet les ordinateurs à un danger quasi permanent. Le marché du logiciel antivirus, en pleine expansion, apparaît comme indispensable: la réactualisation des anciennes versions et l'apparition de nouveaux logiciels (Panda, Sophos) attestent de cette nécessité.
Pour preuve, de plus en plus d'entreprises s'abonnent au *Virus Bulletin*, organisme indépendant (lié à aucun éditeur d'antivirus) publiant des tests comparatifs de logiciels antivirus. Ce service vendu aux professionnels leur permet de déterminer la protection la plus fiable pour leur parc informatique.[2]

3) Les solutions ou technologies concurrentes, la complémentarité

Pour mieux choisir un logiciel antivirus et pour comprendre les caractéristiques vantées sur les fiches techniques, il faut savoir qu'il existe trois techniques majoritairement utilisées par les antivirus pour localiser les virus.

♦ **le scanner**
Cette méthode est la plus ancienne et la plus utilisée. L'antivirus dispose d'une base d'empreintes qui lui permet d'identifier les éventuels virus présents sur le système. Ainsi, il peut détecter les virus avant leur exécution en mémoire. Ce procédé, fiable pour les virus connus, n'est pas efficace face aux espèces inconnues.

[1] Le marché de l'antivirus a généré en France un chiffre d'affaires de plus de 60 millions de francs en 1998.
[2]Le poids des différents segments dans le marché en valeur des produits de sécurité en 1998 est de 54,6% pour les produits antivirus contre 54,4% pour les autres outils de sécurité (Source IDC). Avec 644,28 MF, les sociétés d'antivirus représentaient plus de la moitié des produits de sécurité en 1998. Elles devraient dégager 1 571,15 MF en 2002 (Source IDC).

♦ **le contrôle d'intégrité**

L'antivirus garde des informations sur les fichiers susceptibles d'être infectés et établit une somme de contrôles. Pour vérifier qu'aucun virus n'a atteint le système, il vérifie périodiquement si ces informations se révèlent toujours exactes. Dans le cas où une modification aurait été constatée, l'antivirus avertit l'utilisateur et propose de reconstituer les fichiers contaminés.

♦ **la méthode heuristique**

L'antivirus scrute le fonctionnement de l'exécutable ou de la macro et recherche tout code suspect susceptible de correspondre à des fonctions virales. Grâce à cette méthode, il lui est même parfois possible d'extraire le virus et de restituer le fichier original. L'heuristique est certainement la technique la plus fiable pour dépister les virus qui sont encore inconnus (ce que ne fait pas la méthode du *scanning*)et dont la signature ne figure pas dans la base de données.

4) Des slogans publicitaires aux critères de choix des logiciels

Les slogans publicitaires vantent des logiciels capables de détecter 100% des virus. En fait, les garanties des compagnies d'antivirus se limitent à la détection et à l'éradication des virus **connus**. Par contre, ce que certains éditeurs sont prêts à garantir, c'est le **temps de réactivité**: ils stipulent dans leur contrat qu'ils livreront avant un certain délai l'antidote du nouveau virus. Ainsi, certaines sociétés sont très rapides et peuvent élaborer une **mise à jour** de leur produit en seulement quelques heures.

En effet, les variantes se proliférant sans cesse, le nombre de signatures virales répertoriées ne constitue plus un critère valable. Le **service après-vente**, la **garantie**, la réactivité d'un éditeur sont aujourd'hui les véritables arguments pour s'orienter dans le marché des antivirus.

De plus, la **vitesse d'analyse**, l'**ergonomie** du logiciel, son aptitude à être mis en oeuvre et paramétré tant par un néophyte que par un administrateur de réseau, sont des éléments fondamentaux. A l'heure de la Toile, les fonctions de **filtre Internet** sont indispensables et relèvent du simple bon sens.

De toute évidence, le meilleur produit est celui qui présente le meilleur compromis entre les services, les fonctions antivirus, l'ergonomie, la protection sur Internet et le prix.

5) Description des logiciels antivirus représentatifs du marché actuel

Huit logiciels antivirus représentatifs du marché actuel ont été testés sous les plates-formes Windows 95/98/NT/2000.

♦ **Esafe Protect Desktop 2.2**

Pour poste individuel, ce logiciel est le seul à réunir un antivirus, un filtre Internet et un pare-feu. L'objectif est de sécuriser les applications de communication, notamment les logiciels de navigation et de courrier électronique. Il excelle dans la détection des vandales (codes mobiles malveillants de type Java, ActiveX, scripts,...) et utilise différentes techniques pour détecter les virus inconnus. Installable dans plusieurs langues, ce logiciel présente un mode d'apprentissage adaptable aux habitudes de l'utilisateur.

Comme pour beaucoup de logiciels antivirus, la garantie d'un an couvre toutes les évolutions du produit, mais les mises à jour ne sont malheureusement que mensuelles. De plus, le renouvellement de garantie coûte presque autant que le logiciel.

Editeur: Alladin (http://www.cti.fr)
Prix: env. 600 F TTC

♦ **V-Control 4**

Ce logiciel se destine au déploiement sur de grands réseaux, ce qui explique son prix élevé en monoposte. Son installation est automatique et son analyse rapide. Malheureusement, cet antivirus n'a pas encore pris le virage d'Internet et ne gère pas les applets Java hostiles. Par contre, il immunise Word contre les virus macros, même inconnus.
La gamme des services d'Amplitude offre un support technique à vie et un envoi trimestriel gratuit des nouvelles versions sur CD-Rom. En plus, les mises à jour de l'antivirus sont disponibles sur le site d'Amplitude (la dernière se nomme mise à jour 53). V-Control bénéficie d'un droit de copie, autorisant l'acheteur à installer sur son ordinateur personnel l'antivirus acquis par l'entreprise.

Editeur: Amplitude (http://www.ampitude.fr/)
Prix: env.1800 F TTC

♦ **VirusScan 4.5**

Malgré une interface peu explicite, ce logiciel permet une configuration immédiate des protections: analyse du système, des messages électroniques (via MAPI ou POP3), des fichiers téléchargés et du filtre Internet. Ce dernier bloque notamment les adresses IP et les URLs hostiles. De plus, un moteur heuristique très perfectionné (ViruLogic) permet la détection des virus inconnus.
Malheureusement, l'assistance technique se limite aux heures de bureau. La garantie d'un an couvre les mises à jour automatiques du produit. Passé un an, toute modification du moteur nécessite le rachat du logiciel. L'actualisation des signatures sur le site Web de l'éditeur est possible à vie, quelle que soit l'évolution du logiciel.

Editeur: Network Associates (http://www.nai.com/)
Prix: env. 240 F TTC

♦ **Norman Virus Control 4.7**

Récompensé le 23 mars 2000 par le Virus Bulletin, le logiciel intègre le moteur heuristique de ThunderByte, pionnier du genre, et bénéficie du savoir-faire d'AB Soft, ancien ré éditeur de Dr Solomon's. L'interface recèle des trésors de personnalisation. Pour la chasse aux virus, cet

antivirus intègre deux moteurs, l'un traquant les comportements suspects et l'autre les signatures virales.

Malheureusement, les mises à jour ne sont que bimensuelles (disponibles sur leur site) et le délai de réponse de son laboratoire est de deux jours. En revanche, les utilisateurs connectés à Internet sont prévenus par messagerie de la mise à disposition des nouvelles signatures sur son site Web.
Ce logiciel ne supporte pas encore Windows 2000.

Editeur: Norman (http://www.norman.com) Distributeur: AB Soft
Prix: env. 780 FTTC

♦ **Panda Platinum 6.04**

La version de l'éditeur espagnol se distingue par son interface agréable, colorée et sonorisée. Multilingue, cet antivirus est très facile à utiliser. Le logiciel peut se paramétrer lui-même en fonction du système lors de l'installation. Il est l'un des rares dont les fonctions de filtre Internet s'appliquent aux sites Web comme aux forums de discussion. Support technique 24H/24, mises à jour quotidiennes automatisées, garantie des signatures à vie: les services Panda sont des plus complets.
La version actuelle de ce logiciel ne supporte pas Windows 2000.

Editeur: Panda Software (http://www.pandasoftware.com)
Prix: env. 400 F TTC

♦ **Sophos Anti-virus 3.32**

Le prix de Sophos le rend peu abordable pour le grand public. Sa force réside dans la variété des plates-formes supportées. Le logiciel est rapide, tant à l'installation qu'à l'utilisation. Malheureusement, il n'intègre nulle autre fonction que celle d'antivirus.
Le support technique est assuré de façon permanente, ainsi qu'une mise à jour quotidienne des signatures. La mise à jour du logiciel est mensuelle et peut s'effectuer à partir du site Web. L'absence de renouvellement de garantie constitue un gros point noir: au bout d'un an, il faut tout bonnement racheter le produit.

Editeur: Sophos (http://www.sophos.com) Distributeur: ID
Prix: env. 2350 F TTC

♦ **Norton Antivirus 2000**

Dans sa nouvelle version, ce logiciel présente une interface très simple. L'alliance avec IBM et sa technologie d'analyse permet des mises à jour quotidiennes des définitions des virus. Désormais, l'antivirus surveille automatiquement les pièces jointes aux courriers électroniques entrants et ouvre une fenêtre Windows, et non plus DOS, lors des alertes virales. Toutes les messageries électroniques POP3 sont prises en compte.
Tous les fichiers téléchargés d'Internet sont automatiquement analysés.

Le moteur de recherche est par ailleurs capable de vérifier les fichiers compressés plusieurs fois dans les formats les plus courants.

Tout fichier suspect peut être envoyé au centre de recherche (analyse et réponse en 48h).

Constructeur: Symantec (http://www.symantec.fr)
Prix: 300 F TTC

♦ **PC-Cillin 98 V.4**

Ce logiciel a hérité d'un moteur d'analyse par comportements des fichiers exécutés dans un ordinateur virtuel. Cette technologie donne au logiciel une efficacité et une capacité d'apprentissage remarquable, malgré sa lenteur. Les mises à jour, disponibles chaque semaine sur le Web et chaque mois sur CD-Rom, sont envoyées gratuitement.
L'aide en ligne est très bien conçue. En cas de nouveau virus, le laboratoire français s'engage à fournir le correctif en deux heures. Ce logiciel ne supporte pas encore Windows 2000.

Constructeur: Trend Micro (http://www.trendmicro.fr) Distributeur: Ide Pro
Prix: env. 380 F TTC

6) Bibliographie

Nous avons retenu six références:

1) **Cucchi M., Lichentin D, et Lecoutre F.** Dossier du mois. *INFO PC*, juin 1999, n.160, p.70-86.
Ce dossier, très complet, a constitué la trame de cette étude de marché. Expliquant la genèse des virus, il décrit en parallèle l'évolution de la recherche antivirale. Dans une deuxième partie figure un test comparatif extrêmement détaillé des logiciels antivirus. Bien que certaines versions testées ne soient pas les plus récentes, il constitue un excellent canevas.
2) **http://www.avpve.com**
Ce site constitue une véritable encyclopédie sur les virus.
3) **http://www.geocities.com/SiliconValley/Hills/4227/antivir.html**
A cette adresse figure une présentation générale des antivirus ainsi qu'un descriptif de leurs aspects techniques.
4) **http://www.lemonde.fr/aietek/**
Le site du Monde Interactif propose des liens vers des articles d'actualité sur le problème des virus informatiques (recherche par mot-clé *antivirus*).
5) **http://www.respublica.fr/site/**
Cette adresse est celle d'un important centre d'information contre les virus.
6) **http://www.virusbtn.com/**
Le *Virus Bulletin* est incontournable. Cet organisme teste depuis des années l'efficacité des antivirus et recense les virus existants. Son site propose notamment des liens vers les constructeurs.