

Sécurité Internet

Bunker tout confort

Si la protection des ordinateurs reste leur priorité, plusieurs éditeurs s'attachent désormais à améliorer le confort d'utilisation de leurs logiciels de sécurité Internet. Une nouvelle stratégie qui était nécessaire.

**Le nombre
de logiciels
toxiques
a explosé**

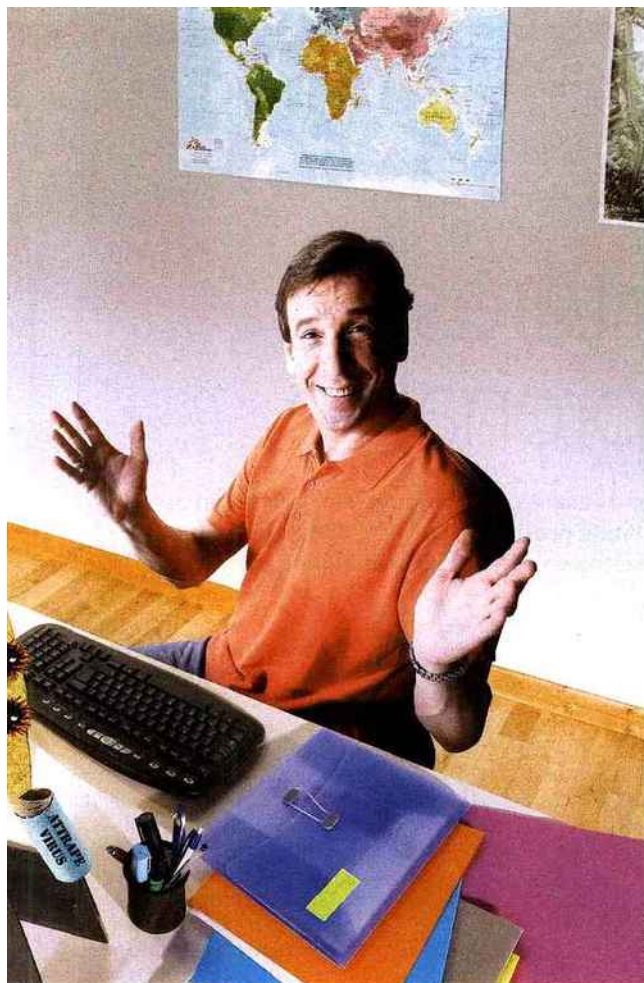
Les logiciels de sécurité Internet n'en finissent pas de s'étoffer. Ils détectent depuis longtemps la majorité des virus, spywares, chevaux de Troie et autres codes malveillants qui traînent sur la Toile (voir glossaire, p. 34). Depuis quelques années, la plupart sont aussi en mesure de repérer les codes nocifs non recensés par les éditeurs, de bloquer les courriels non sollicités (spams) et de protéger les internautes contre les mails frauduleux destinés à dérober des informations personnelles (phishing). Cette année, ils vont encore plus loin. Dans la version 2009 de sa suite Internet (un logiciel comprenant au moins un pare-feu et un antivirus), BitDefender intègre un coffre-fort qui sécurise les données les plus sensibles contenues dans l'ordinateur, ainsi qu'un système de cryptage des messageries instantanées. Panda a inséré dans sa suite un filtre protégeant contre le vol de données personnelles. Quant à Symantec, il met l'accent, dans la dernière version de sa suite Internet, sur une nouvelle fonction « antibot » qui empêche l'ordinateur d'être employé par des pirates pour lancer des campagnes de spams de grande ampleur. Pour les éditeurs, cette débauche sécuritaire est indispensable. « Nous devons nous adapter aux méthodes des pirates », déclarent-ils en chœur.



À en croire les études qu'ils ont menées, le nombre de logiciels toxiques circulant dans le monde aurait explosé. Les experts de GDATA disent en avoir recensé, en 2008, près de 900 000 supplémentaires, soit presque sept fois plus qu'en 2007. « Pour les utilisateurs de Windows, il n'y a jamais eu de période plus dangereuse pour surfer sur le Net avec un PC non protégé », avertit le directeur de la sécurité. Du côté de l'éditeur Panda Security, on assure que « 23 % des PC avec un antivirus à jour sont infectés ». On en a froid dans le dos ! Surtout que les pirates affûtent leurs armes. Ils amélioreraient sans cesse leurs logiciels et profiteraient ainsi des nouveaux outils de communication en vogue (messageries instantanées, réseaux sociaux...) pour récupérer un maximum d'informations personnelles ou pour se servir des PC infectés à des fins malhonnêtes.

Simplifier la vie de l'utilisateur

Si la sécurisation des données reste leur priorité absolue, plusieurs éditeurs affirment prendre en compte plus que jamais la simplicité d'emploi de leurs logiciels et l'utilisation raisonnée des ressources de l'ordinateur. Cette nouvelle stratégie n'est pas anodine. Un logiciel trop encombrant peut ralentir l'ordinateur et perturber son



Didier Crette

fonctionnement. Parfois, les désagréments sont tels que certaines personnes sont tentées de désactiver leur logiciel de protection. Longtemps décrié pour la lourdeur et la désinstallation malaisée de ses logiciels, Symantec a annoncé avoir fait du « confort d'utilisation » un élément central de sa nouvelle suite de sécurité Internet. Le numéro 1 mondial du secteur a notamment promis une installation en un clic et en moins d'une minute, une occupation mémoire minimale et l'intégration de diverses fonctionnalités visant à rendre la surveillance plus discrète. Norton Internet Security 2009 propose, par exemple, un mode silencieux qui met en veille les alertes pendant que l'on joue ou que l'on regarde une vidéo. Le logiciel est également capable d'interrompre ses contrôles dès que l'on se sert de l'ordinateur, afin que toute la puissance nécessaire soit disponible. Des progrès confirmés par nos tests. G Data a lui aussi mis au point, pour la version 2009 de sa suite Internet, une série de fonctionnalités censées simplifier la vie de l'utilisateur. Les résultats sont moins probants. Nos tests montrent que la suite de G Data est assez lourde et encombrante. Il reste des efforts à faire. ■

Cyril Brosset

Dossier technique Neil McPherson

ANTIVIRUS GRATUITS

Que valent-ils ?

C'est un débat qui agite le monde des internautes depuis longtemps. D'un côté, il y a ceux qui ne voient pas pourquoi ils devraient payer pour un logiciel qu'ils peuvent télécharger librement et légalement sur Internet. De l'autre, les sceptiques pour qui gratuité rime avec moindre efficacité. Quant aux éditeurs de logiciels de sécurité Internet qui ont fait le pari de la gratuité, ils se veulent rassurants. Selon eux, leurs antivirus gratuits ressembleraient comme deux gouttes d'eau (ou presque) à leur version payante. « La concurrence est si rude qu'il est difficile aujourd'hui de vendre un antivirus seul, explique un éditeur qui propose une version gratuite de son antivirus. *Étant donné que notre suite Internet se vend bien, nous pouvons nous permettre d'offrir notre antivirus.* » Seuls quelques détails manqueraient parfois. Ici, les utilisateurs de la version gratuite ne profiteraient pas de l'assistance téléphonique promise à ceux qui ont payé. Là, quelques fonctionnalités seraient absentes, les mises à jour un peu moins fréquentes ou les instructions disponibles uniquement en anglais... Rien de dramatique. Et force est de constater que la plupart des antivirus gratuits sont à la hauteur. Lors de notre test, Avast! a même rivalisé à plusieurs reprises avec les meilleures suites Internet payantes.

Des lacunes

Néanmoins, un antivirus gratuit ne remplace pas une suite Internet payante. D'une part, parce que, outre

un antivirus, cette dernière intègre un pare-feu, pour surveiller les échanges de données entre l'ordinateur et le réseau, et divers autres outils de protection (anti-phishing, antispywares, logiciel de contrôle parental, etc.). D'autre part, parce que les versions gratuites des antivirus ne bénéficient pas forcément des dernières innovations des éditeurs en matière de protection. Ainsi, certains antivirus gratuits ne détectent pas les menaces les plus récentes comme les spywares, les rootkits ou les bots. Ils ne portent pas non plus d'attention particulière aux fichiers téléchargés, ne surveillent pas les éventuelles attaques subies sur les messageries instantanées, ne contrôlent pas automatiquement les mails et leurs pièces jointes avant leur enregistrement sur le disque dur et ne cherchent pas toujours à repérer les sites infectés des pages Web sur lesquelles il suffit de surfer pour attraper un virus. Enfin, ils n'intègrent pas nécessairement les dernières innovations des éditeurs en matière de détection des virus inconnus. Loin d'être anodines, ces lacunes sont rarement connues du grand public. Sur leurs sites, les éditeurs donnent bien quelques détails. En revanche, sur les nombreuses plates-formes qui permettent de télécharger ces logiciels librement, ces informations ne transparissent jamais. Accompagné d'un bon pare-feu, un antivirus gratuit peut assurer une bonne protection. Mais il faut être conscient de ses limites.

Nulle forteresse n'est imprenable

LE CHOIX DU TESTEUR

La capacité des logiciels à protéger l'ordinateur prime. La facilité d'emploi et l'utilisation des ressources du PC sont aussi prises en compte.

LE PROTOCOLE

Les logiciels de protection ont été installés sur un PC de configuration moyenne fonctionnant sous Windows Vista, édition familiale Premium SP1. La compatibilité avec Windows XP SP3 a été vérifiée.

PROTECTION ANTIVIRUS/ANTISPYWARE

Environ 1 600 fichiers pirates (troyens, rootkits, virus...) ont été soumis aux antivirus. Des analyses ont d'abord été réalisées sur le disque dur (analyse sur demande). Ensuite, sans mettre à jour les bases de données des antivirus, 30 fichiers malveillants nouveaux (apparus depuis la date de la dernière mise à jour de l'antivirus) ont été soumis à l'analyse des antivirus, pour tester l'efficacité de leur technologie. Enfin, 56 sites Web hébergeant des fichiers toxiques ou contenant des codes suspects ont été visités, afin d'évaluer les systèmes de protection en temps réel.

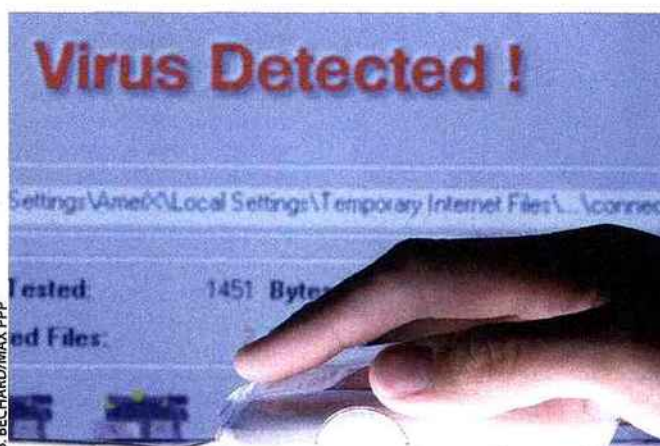
PROTECTION PARE-FEU

L'efficacité du pare-feu a été testée en simulant diverses attaques : analyse de ports, attaques DOS, contournement des protections, etc. Le pare-feu était configuré avec son niveau de sécurité par défaut.

FACILITÉ D'EMPLOI

On évalue la facilité d'installation (et l'efficacité de la désinstallation), de mise à jour et d'utilisation du logiciel. La clarté de la documentation et du système d'aide embarqué a aussi été jugée, tout comme les besoins des logiciels en termes de ressources (espace disque, charge du processeur et de la mémoire vive) et les possibilités de configuration offertes.

Face à une menace protéiforme et sans cesse renouvelée, pare-feu et antivirus sont indispensables et offrent une protection correcte dans l'ensemble. Malheureusement, aucun système de défense n'est infaillible.



Licence Vérifiez la durée

Lors de l'achat, outre le prix, vérifiez le nombre d'ordinateurs sur lesquels la suite Internet peut être installée, ainsi que la durée de validité de la licence. La plupart sont prévues pour 3 ordinateurs avec mises à jour pendant 1 an. Une fois ce délai écoulé, vous devrez payer pour que le logiciel reste efficace. Néanmoins, certains éditeurs proposent d'autres versions de leur suite. Celles de BitDefender, F-Secure et AVG existent avec 2 ans de mises à jour (elles sont un peu plus chères, respectivement 54, 80 et 120 €). Si vous n'avez qu'un ordinateur à protéger, Kaspersky, Avira, McAfee, AVG et Checkpoint commercialisent des versions 1 an/1 poste. Mais si les quatre premiers appliquent une ristourne (ces suites sont vendues respectivement 50, 40, 60 et 54 €), le dernier met sa version « 1 PC » au même prix que la « 3 postes ». Par ailleurs,

sachez que certains éditeurs imposent, en cas de téléchargement, une tacite reconduction de la licence au bout d'un an ou cochant d'office des options payantes au moment de la commande (garantie de téléchargement d'un an, copie de sauvegarde sur CD...).

Protection antivirus

Il y a toujours une faille

Virus connus. Aucun des logiciels que nous avons testés n'a été capable de repérer la totalité des quelque 1 600 malwares (vers, virus, rootkits, troyens, logiciels espions...) que nous avons installés sur un ordinateur. G Data a été plus efficace que ses concurrents. Seuls quelques troyens, vers et logiciels espions lui ont échappé. F-Secure, BitDefender, ZoneAlarm (Checkpoint), McAfee et Kaspersky s'en sont aussi sortis honorablement, alors qu'AVG, Panda et Agnitum ont détecté moins de 80% des logiciels espions. De manière surprenante,

l'efficacité de la suite Panda baisse lorsque la connexion Internet est coupée. Dommage, quand on sait que des logiciels malveillants peuvent aussi se cacher dans des fichiers provenant de supports externes (disques durs, clés USB, DVD...). Parmi les antivirus gratuits, seul Avast! (Alwil) tire son épingle du jeu. Ses performances en matière de détection des malwares connus n'ont rien à envier à celles des meilleures suites de sécurité payantes. À noter qu'Avira AntiVir Personal a laissé passer plus de logiciels espions que sa version payante AntiVir Premium Security. **Virus inconnus.** Les suites Internet sont aussi capables de reconnaître les malwares avant même que l'éditeur ne les ait recensés et que leur antidote ait été téléchargé sur l'ordinateur au cours d'une mise à jour. Ils utilisent pour cela des technologies dites « heuristiques »⁽¹⁾. Mais mieux vaut ne pas trop compter dessus. La suite la plus efficace (celle de l'éditeur Panda) n'a détecté « que » 16 logiciels pirates sur les 30 auxquels nous l'avions soumise. Celle de G Data n'en a repéré que 7. Et avec F-Secure, ZoneAlarm et Trend Micro, aucun virus inconnu n'a été intercepté. Parmi les antivirus gratuits, Avast! s'approche une fois de plus des performances des meilleures suites payantes, avec 15 fichiers repérés sur 30. **BON À SAVOIR** Même s'ils donnent une bonne idée des performances de détection des logiciels de sécurité, ces résultats doivent être pris

PARAMÉTRAGE

Réservé aux initiés

Tous les éditeurs permettent aux utilisateurs de modifier le paramétrage d'origine de leurs logiciels. Dans la plupart des cas, la protection du pare-feu, par exemple, peut être renforcée soit en optant pour un niveau de sécurité plus élevé, soit en configurant soi-même le logiciel. Les analyses heuristiques de certains antivirus

(censées détecter les virus encore inconnus des éditeurs) peuvent également être paramétrées manuellement. Cela dit, à moins de bien s'y connaître, mieux vaut s'en abstenir. Si le paramétrage est mal réalisé, le risque est grand de voir apparaître des failles dans la protection. Nos tests ont même montré que le renforcement

du niveau de protection de l'analyse heuristique augmentait à peine le taux de détection (voire ne l'améliorait pas du tout pour les logiciels Avira et Kaspersky). Au contraire, cela risquait de ralentir excessivement l'ordinateur et d'engendrer des « faux positifs », des alertes erronées concernant des programmes innocents.

SUITE PAYANTE

► G Data InternetSecurity 2009

La plus sûre

Avec ses deux moteurs antivirus, l'un provenant de BitDefender et l'autre d'Alwil, la suite de G Data détecte presque tous les virus connus. Si elle éprouve plus de difficultés à repérer les virus inconnus, c'est son utilisation intensive des ressources de l'ordinateur qui l'handicape le plus. Avant de l'acheter, il est préférable de télécharger sa version d'essai, afin de vérifier qu'elle ne ralentit pas trop le PC. Prix : 36 € (1 an/3 postes).



G. PODGORSKI POUR QPC

MEILLEUR CHOIX



SUITE PAYANTE

► BitDefender Internet Security 2009

La légèreté en plus

Cette suite assure, elle aussi, une bonne protection. Mais en plus, elle a l'avantage d'être moins gourmande en ressources que la suite de G Data. Elle devrait donc mieux convenir aux ordinateurs peu puissants. Prix : 42 € (1 an/3 postes) ou 54 € (2 ans/3 postes).

MEILLEUR CHOIX

ANTIVIRUS GRATUIT



► Alwil Avast! 4 Édition familiale

Il n'a pas à rougir

Sa capacité de détection des virus connus et inconnus n'a rien à envier à celle des suites payantes. Cet antivirus est, en outre, capable de repérer bon nombre de sites infectés. Associé à un bon pare-feu, il peut offrir une protection de base satisfaisante.

13 suites de sécurité Internet et 3 antivirus gratuits

Suites de sécurité Internet	Prix téléchargement**	Site Internet www.	Version d'essai (durée)	Disponible version boîte (magasins)	Judgement global		Protection antivirus			Facilité d'emploi				
					Note sur 20	Appréciation	Virus connus	Virus inconnus	Protection Internet	Protection pare-feu	Installation/désinstallation	Ressources	Utilisation	Aide
1 G Data InternetSecurity 2009	36	gdata.fr	30	●	14,3	★★	★★★	■	★	★★★	★★	■	★★	★★★
2 BitDefender Internet Security 2009	42	bitdefender.fr	30	●	13,9	★★	★★	■	■	★★★	★★	★★	★★	★★
3 Kaspersky Internet Security 2009	70	kaspersky.fr	30	●	13,4	★★	★★	■	■	★★	★★	★	★★	★★★
4 Avira AntiVir Premium Security Suite 2009	60	avira.com	30	-	12,6	★★	★	■	★	★★	★	★★	★★	★★★
5 F-Secure Internet Security 2009	60	f-secure.fr	30	●	12,2	★★	★★	■	■	★	★★	★	★★	★★
7 Panda Internet Security 2009	66	pandasecurity.com	30	●	11,8	★	■	★	★	★★	★★	★	★★	★★
8 McAfee Internet Security 2009	75	mcafee.fr	30	●	11,8	★	★★	■	■	★★	★★	★	★★	★
9 Symantec Norton Internet Security 2009	65	symantec.fr	15	●	11,8	★	★	■	■	★	★	★★	★★	★★
10 Checkpoint ZoneAlarm Internet Security Suite 2009	50	zonealarm.com	15	●	11,4	★	★★	■	■	★	★★	★	★★	★★
11 Trend Micro Internet Security 2009	60	trendmicro.com	31	●	9,8	★	★	■	■	★★	★★	★	★★	★★
12 Agnitum Outpost Security Suite Pro 2009	50	agnitum.fr	30	-	8,5	★	■	■	■	★★★	★★	★	★★	★
13 AVG Internet Security 8.0	80	avgfrance.com	30	-	8,2	★	■	■	■	★★	★★	★	★★	★★
Antivirus gratuits														
1 Alwil Avast! 4 Édition familiale	-	avast.com	n.a.	-	11,6	★	★★	★	★★	n.a.	★	★★	■	■
2 Avira AntiVir Personal	-	free-av.com	n.a.	-	10,9	★	★	■	★	n.a.	★★	★★	★★	★★★
3 AVG Anti-Virus Free Edition	-	gratuit.avg.fr	n.a.	-	8,2	★	■	■	■	n.a.	★★	★★	★	★★

* Sur le site de l'éditeur ; licence de mises à jour 1 an/3 postes. ★★ TRES BON ★ BON ★ MOYEN ■ MÉDIocre ■ MAUVAIS ● oui ; - non. n.a. : non applicable

avec précaution. D'abord, parce que nos tests ont été réalisés sur la base de codes malveillants prédéfinis. Ce n'est pas parce qu'un logiciel a arrêté ces virus qu'il bloquera forcément tous les autres codes pirates à venir. Ensuite, parce que nos tests ont été effectués à partir de fichiers infectés non exécutés. Or, certains antivirus analysent aussi le comportement des fichiers une fois qu'ils sont entrés en action. Certains codes toxiques pourraient donc être identifiés à ce moment.

Protection Internet

Le surf est un sport dangereux

Avoir son ordinateur infecté juste en surfant sur Internet, c'est possible. À en croire les éditeurs de logiciels de sécurité, ce type d'attaque est même à la mode chez les pirates. Il suffit de se rendre sur certaines pages Web pour qu'un logiciel malveillant s'installe insidieusement sur l'appareil. Pour lutter contre cette menace, les suites de protection analysent en temps réel les sites Internet visités. Malheureusement, ces fonctionnalités sont loin d'être infaillibles. Parmi les

logiciels payants, seuls trois (G Data, Avira et Panda) ont réussi à détecter plus de la moitié des 56 sites infectés de notre test. Pas très rassurant ! Le moins bon, l'Agnitum, n'en a trouvé que 13. Quant au meilleur antivirus sur ce critère, il est gratuit. Il s'agit d'Avast!, qui a décelé 47 sites sur 56.

Pare-feu

Un bouclier assez efficace

Lorsqu'une application inconnue tente d'établir une connexion Internet, le pare-feu doit lui bloquer l'accès, au moins le temps de solliciter l'accord de l'utilisateur. Pourtant F-Secure, ZoneAlarm et Norton (Symantec) ont autorisé l'accès à notre logiciel de test (et sans prévenir l'utilisateur de cette action). Kaspersky a bloqué automatiquement l'accès sans alerte. Les autres pare-feu ont demandé l'accord de l'utilisateur, parfois avec la recommandation de refuser la connexion. Il n'est pas toujours facile pour un débutant de deviner l'action à choisir. En cas de doute, il est préférable de refuser provisoirement la connexion.

Facilité d'emploi

Gardez des ressources

Installation/désinstallation.

Installer une suite de sécurité Internet sur son ordinateur ne pose pas de problème particulier. Il est juste regrettable que le logiciel de Symantec ne se mette pas à jour immédiatement après sa mise en place. Dommage aussi que la suite Internet d'Agnitum ne désactive pas le pare-feu de Vista au moment de son installation. Une manipulation pourtant indispensable pour que l'ordinateur continue à fonctionner correctement. Enfin, il est surprenant de voir que les suites de BitDefender, McAfee, Symantec et Trend Micro désactivent d'office Windows Defender. L'antispyware intégré de Vista n'est pas un logiciel de protection comme les autres et n'entre pas en conflit avec un antivirus classique. Au contraire, il pourrait même bloquer certains logiciels malveillants que les antivirus laissent passer. Mieux vaut donc le conserver actif, à moins que les performances de l'ordinateur ne s'en ressentent. La désinstallation aussi se

déroule bien, même si certains proposent une fonction spécifique dans le menu Démarrer de Windows, alors que d'autres obligent à passer par le panneau de configuration (Démarrer -> Panneau de configuration -> Désinstaller un programme). Seuls Agnitum et Avira AntiVir Personal n'ont laissé aucune trace sur l'ordinateur. À l'opposé, F-Secure a abandonné un mégaoctet (Mo) de données sans raison valable. McAfee, lui, ne réactive pas Windows Defender, qu'il a pourtant désactivé lui-même lors de son installation. **Ressources.** C'est un critère important à prendre en compte, surtout si votre ordinateur montre des signes de fatigue. Avec plus de 350 Mo d'espace utilisés sur le disque dur, les suites de Trend Micro et de G Data sont celles qui encombrant le plus l'ordinateur. À l'opposé, celle de Symantec, longtemps critiquée pour sa lourdeur, ne requiert plus « que » 107 Mo (contre plus de 500 Mo pour sa version précédente). Par ailleurs, l'analyse en temps réel allonge les délais de transfert. Ainsi, avec G Data Internet Security, copier des fichiers sur le disque dur prend 76% de temps en plus, contre 15 à 40% avec la plupart de ses concurrents et 10% en moyenne avec les antivirus gratuits. Norton est le logiciel qui emploie le moins de mémoire vive pendant le transfert, alors que celui de Trend Micro est le plus gourmand (environ 100 Mo de RAM sollicités). Pour éviter les mauvaises surprises, téléchargez les versions d'évaluation proposées sur les sites Internet des éditeurs. Vous pourrez ainsi essayer le produit et évaluer son effet sur votre ordinateur avant de l'acquiescer. En laissant votre adresse mail sur le site Internet de l'éditeur, vous êtes même susceptible de recevoir des remises sur le prix du logiciel. ■

(1) Méthode d'analyse qui tente de repérer des morceaux de codes suspects.

GLOSSAIRE

Les principales menaces

VIRUS : morceau de code malveillant caché dans un fichier exécutable et conçu pour se reproduire en infectant d'autres fichiers exécutables. Il peut perturber le fonctionnement de l'ordinateur, voire détruire des données ou détériorer le matériel.

DRIVE-BY DOWNLOAD : technique qui consiste à télécharger insidieusement un logiciel toxique sur l'ordinateur d'un internaute lorsqu'il surfe sur un site infecté. Généralement, la victime ne s'aperçoit de rien.

TROYEN (ou cheval de Troie) : programme qui recèle une fonction cachée permettant au pirate d'accéder au contenu d'un ordinateur, voire d'en prendre le contrôle.

ROOTKIT : logiciel chargé de camoufler les accès frauduleux à un ordinateur ouverts par les pirates afin qu'ils puissent, par la suite, s'introduire dans le PC quand ils le souhaitent.

SPYWARE (ou logiciel espion) : logiciel qui, une fois installé sur l'ordinateur, récolte des

informations personnelles et les transmet au pirate. Il en existe plusieurs variantes (adware, keylogger, hijacker...).

PHISHING (ou « hameçonnage ») : technique frauduleuse qui se présente sous la forme d'un courriel non sollicité.

Censé provenir d'un tiers de confiance (banque, cybercommerçant, site d'enchères en ligne...), celui-ci invite le destinataire à transmettre des données personnelles (identifiant, mot de passe, numéro de carte de crédit...).