

Quelle proactivité dans la lutte contre les virus ?

Kaspersky Lab, éditeur reconnu de solutions de sécurité informatique contre toutes les formes de cyber-menaces (cyber-escroquerie, botnet, spams, phishing...) publie un nouveau rapport dédié à la protection proactive et à son intégration dans les solutions anti-virus.

Désormais, les attaques par malware occupent la première place du palmarès des menaces sur la sécurité informatique. Ces codes malicieux entraînent non seulement des pertes financières directes, mais elles servent également de points de départ pour l'exécution de toute une série d'autres menaces, telles que le vol de données confidentielles et l'accès non autorisé aux données. Les éditeurs de logiciels anti-virus ont, quant à eux, adopté de nouvelles approches concernant la sécurité des structures informatiques : les technologies proactives, la diffusion forcée de vaccins critiques, l'augmentation notable de la fréquence d'actualisation des bases de données antivirales, etc. Ce rapport est le premier à livrer des pistes sur les nouvelles technologies proposées par les éditeurs de logiciels anti-virus. Ainsi, les utilisateurs pourront évaluer plus ou moins objectivement ces technologies.

Aujourd'hui, une des principales tendances n'est pas seulement l'augmentation du coût global des attaques virales mais également l'augmentation ininterrompue, au cours des 15 dernières années, du nombre de codes malicieux eux-mêmes. En 2005, leur croissance a tout simplement explosé. Selon les données de Kaspersky Lab, à la fin de l'année 2005, 6 368 codes malicieux ont été détectés chaque mois tandis que la croissance globale pour l'année 2005 atteignait 117% contre 93% pour l'année précédente.

La menace est évidente : le nombre de cyber-risques a considérablement augmenté et ils deviennent de plus en plus dangereux. Dans ce contexte, il était logique d'attendre une réaction de la part des éditeurs de logiciels anti-virus qui ont adopté de nouvelles stratégies contre les infections. Citons, parmi celles-ci, les technologies proactives, la rapidité de réaction face à l'émergence des menaces dangereuses capables de créer des épidémies ou la simple augmentation de la fréquence d'actualisation des bases de données antivirales.

Ce rapport analyse plus particulièrement sur la protection proactive, présentée souvent comme la solution miracle contre tous les virus présents et à venir.

Introduction aux technologies proactives : forces et faiblesses

Les logiciels anti-virus modernes adoptent deux démarches fondamentales pour l'identification des cyber-risques : les signatures et la méthode proactive/heuristique. Le principe de la première méthode est relativement simple : les objets analysés sur l'ordinateur sont comparés à des modèles (signatures) de codes malicieux connus. Cette technologie requiert le suivi permanent des nouveaux exemples de codes malicieux, leur description et leur inclusion dans la base de données antivirale. L'éditeur doit donc posséder un service d'identification et d'analyse (un laboratoire anti-virus). Les principaux critères qui définissent l'efficacité de cette méthode sont la rapidité de réaction face aux nouvelles menaces, la fréquence des actualisations et le nombre maximum de menaces identifiées.

Selon toute évidence, la méthode des signatures possède ses inconvénients. Le plus important d'entre eux, c'est le retard de la réaction face aux nouvelles menaces. Les signatures sont toujours ajoutées quelques temps après l'apparition du virus. Elles sont par définition réactives alors que les codes malicieux modernes sont capables d'infecter des millions d'ordinateurs dans un laps de temps très bref.

C'est pourquoi les méthodes proactives/heuristiques sont toujours plus populaires. Ces dernières ne requièrent pas la diffusion de signatures. Le logiciel anti-virus analyse le code de l'objet et/ou le comportement de l'application exécutée puis, sur la base de règles internes, il décide du caractère malveillant ou non de l'application.

En principe, cette technologie permet de découvrir les programmes malveillants inconnus. De nombreux éditeurs de logiciels anti-virus se sont empressés de présenter les méthodes proactives comme le remède miracle face aux vagues croissantes de nouveaux codes malicieux. Mais, il n'en est pas vraiment ainsi. Afin d'évaluer l'efficacité de la démarche proactive et la possibilité de l'utiliser séparément de la méthode des signatures, il convient d'étudier minutieusement le principe de fonctionnement des technologies proactives.

La protection proactive se décline en quelques modes. Nous nous intéresserons aux deux les plus répandus : les analyseurs heuristiques et les inhibiteurs de comportement.

Analyse heuristique : forces et faiblesses

La méthode heuristique permet d'étudier le code de l'objet à analyser et de définir, grâce à divers indices, si cet objet est malveillant ou non. A la différence des signatures, la méthode heuristique est capable d'identifier aussi bien les codes malicieux connus que les codes malicieux inconnus (c'est-à-dire les virus créés après le module d'analyse heuristique).

La tâche de l'analyseur consiste à rechercher dans le code les signes (commandes) suspects propres aux codes malveillants. Il s'agit d'une méthode d'analyse statistique. Par exemple, de nombreux programmes malveillants recherchent des fichiers exécutables, les ouvrent et les modifient. L'analyseur heuristique étudie le code d'une application et lorsqu'il découvre une commande suspecte, il augmente le «compteur suspicion» pour cette application. Si la valeur de ce compteur, après l'analyse, dépasse un seuil défini, l'objet est considéré comme suspect.

L'avantage de cette méthode se situe au niveau de sa simplicité et de sa rapidité. Toutefois, le taux de découverte de nouveaux codes malicieux reste assez faible et la probabilité de fausses alertes est élevée.

C'est la raison pour laquelle les logiciels anti-virus combinent analyse statistique et analyse dynamique. L'idée à l'origine de cette approche conjointe consiste à simuler l'exécution d'une application dans un environnement sécurisé virtuel avant que l'utilisateur n'exécute le fichier sur son ordinateur. C'est ce qu'on appelle «l'émulation en tampon» ou le «bac à sable». On trouve également chez les différents éditeurs le terme «émulation d'un ordinateur virtuel dans l'ordinateur».

L'analyseur heuristique dynamique lit une partie du code de l'application dans le tampon d'émulation de l'anti-virus et grâce à des procédés spéciaux, émule son exécution. Si des

actions suspectes sont dévoilées au cours de cette «pseudo-exécution», l'objet est considéré comme malveillant et il ne pourra pas être exécuté sur l'ordinateur de l'utilisateur.

A la différence de la méthode statistique, la méthode dynamique est plus gourmande en ressources puisque l'analyse a lieu dans un espace virtuel sécurisé. Par conséquent l'exécution de l'application sur l'ordinateur est reportée le temps de l'analyse. Toutefois, l'analyse dynamique se caractérise par un taux d'identification des objets malveillants bien supérieur à celui de l'analyse heuristique. Le risque de fausses alertes est alors considérablement réduit.

Pour conclure, signalons qu'à l'heure actuelle toutes les solutions anti-virus exploitent des analyseurs plus ou moins modernes.

Inhibiteur de comportement, un programme d'analyse des applications

L'inhibiteur de comportement est un programme qui analyse le comportement de l'application lancée et qui bloque toute action dangereuse. A la différence des analyseurs heuristiques qui analysent les actions suspectes dans un environnement virtuel (heuristique dynamique), les inhibiteurs de comportement travaillent dans des conditions réelles.

Le principe de fonctionnement des premiers inhibiteurs de comportement était simple. Dès qu'une action potentiellement dangereuse était identifiée, un message invitait l'utilisateur à la bloquer ou à l'autoriser. Dans la majorité des cas, cette approche fonctionnait mais il arrivait que même des programmes légitimes, voire le système d'exploitation, produisent des actions «suspectes». Donc, si les connaissances en informatique de l'utilisateur n'étaient pas très poussées, ces questions pouvaient semer le doute.

La nouvelle génération d'inhibiteurs de comportement analyse non plus des actions individuelles mais bien des suites d'actions. En d'autres termes, la décision sur la dangerosité d'une application particulière est prise sur la base d'une analyse plus poussée. Le nombre de messages de confirmation adressés à l'utilisateur est réduit et la fiabilité de la détection augmente.

Les inhibiteurs de comportement modernes sont capables de contrôler un large éventail d'événements dans le système. Il s'agit avant tout du contrôle de l'activité dangereuse (analyse de l'activité de tous les processus exécutés dans le système, les enregistrements sans modification dans le système de fichiers ou la base de registres). Lorsqu'une application particulière exécute une série d'actions suspectes, l'utilisateur est prévenu de la dangerosité. De plus, l'inhibiteur de comportement est capable de déceler les rootkits. Ce sont des programmes qui dissimulent l'action d'un code malicieux sur des fichiers, des répertoires ou des clés du registre et qui cachent également les programmes exécutés, les services du système, les pilotes et les connexions de réseau.

Notons, la fonction des inhibiteurs de comportement qui contrôle l'intégrité des applications et de la base de registres système de Microsoft Windows. Dans ce dernier cas, l'inhibiteur contrôle les modifications des clés de la base de registres et permet d'établir des règles d'accès à celles-ci pour diverses applications. Il est donc possible de rétablir un système à l'état antérieur à l'infection du fait de l'action des programmes inconnus.

A la différence des analyseurs heuristiques présents dans la majorité des logiciels anti-virus de dernières générations, les inhibiteurs de comportement sont moins fréquents. En guise d'exemple, citons le module de protection proactive (Proactive Defence Module) intégré aux logiciels de Kaspersky Lab.

Ce module propose toutes les fonctions décrites ci-dessus ainsi qu'un système efficace d'information de l'utilisateur sur la menace que représentent réellement ces actions dangereuses. Tout inhibiteur de comportement requiert à un moment ou à un autre l'intervention de l'utilisateur, ce qui suppose que celui-ci possède un certain niveau de connaissances en informatique. Dans les faits, les utilisateurs possèdent rarement l'expérience requise et c'est pour cela que le soutien en informations, en réalité une aide à la prise de décision, est une fonction indispensable de toute solution anti-virus moderne.

En guise de synthèse, nous pouvons dire que l'inhibiteur de comportement peut prévenir la propagation de menaces connues ou inconnues (créés après l'inhibiteur), ce qui est un avantage indéniable de ce type d'approche. Le principal inconvénient se situe au niveau de la réaction vis-à-vis de toute une série de programmes parfaitement légitimes. De plus, la prise de décision finale sur la dangerosité d'une application appartient à l'utilisateur, ce qui suppose une certaine qualification.

Protection proactive et vulnérabilités des applications

La « littérature » commerciale des éditeurs de logiciels anti-virus laisse souvent penser que la protection proactive et l'analyse heuristique constituent la solution universelle contre les cyber-risques, qu'aucune actualisation n'est nécessaire et que par conséquent, le système est toujours prêt à repousser les attaques, même celles qui n'existent pas encore. De plus, les brochures évoquent non seulement les nouvelles menaces, les vulnérabilités connues, mais également les menaces de la catégorie «zéro jour». En d'autres termes, les éditeurs prétendent que leurs technologies proactives sont capables de bloquer même les codes malveillants capables d'exploiter les vulnérabilités inconnues, c'est-à-dire les vulnérabilités pour lesquelles aucun correctif n'a encore été publié.

Malheureusement, ces documents présentent une certaine dose d'incompréhension et de ruse. En particulier, lorsqu'ils présentent la lutte contre les codes malicieux comme une lutte qui oppose les cyber-criminels aux méthodes automatiques (heuristique). En réalité, la lutte oppose des êtres humains des deux côtés : cyber-criminels et experts en virologie.

Nous avons déjà abordé les différentes méthodes de protection proactive : l'analyse heuristique et les inhibiteurs de comportement. Elles reposent sur la « connaissance » que les solutions anti-virus possèdent des codes malicieux. En réalité, les programmes tirent « leurs connaissances » (les ensembles de règles sur les comportements) des experts en virologie. Ces derniers les ont obtenues par le biais de l'analyse de codes malicieux déjà connus. Ainsi, les technologies proactives sont totalement inefficaces contre les codes malveillants qui exploitent de nouvelles méthodes d'infection développées après la création de la règle. Il s'agit principalement des menaces de la catégorie «zéro jour». De plus, les auteurs de virus s'efforcent de trouver de nouvelles manières pour contourner les règles de comportement des anti-virus, ce qui réduit également l'efficacité des méthodes proactives.

En résumé, les éditeurs de logiciels anti-virus sont tout simplement obligés d'actualiser les règles de comportement et d'affiner leur heuristique afin de réagir aux nouvelles menaces.

Evidemment, ces actualisations sont moins fréquentes que l'actualisation des signatures (modèles de code), mais elles se produisent néanmoins régulièrement et au vu de l'augmentation accélérée du nombre de nouveaux codes malicieux et seront de plus en plus fréquentes. Finalement, le secteur va revenir à la méthode des signatures, mais ces signatures seront des signatures du comportement et non plus du code.

En dissimulant ces faits aux utilisateurs (nécessité de mettre à jour la mise à jour proactive), certains éditeurs trompent leurs clients, qu'ils soient entreprises, particuliers ou bien la presse. Cela contribue à donner une représentation inexacte des possibilités de la protection proactive

Signatures et méthodes proactives

Malgré leurs défauts, les méthodes proactives permettent en effet de découvrir certaines nouvelles menaces avant la publication des signatures correspondantes. Examinons la réaction des logiciels anti-virus au ver Email-Worm.Win32.Nyxem.e (ci-après, Nyxem). Le ver Nyxem (plus connu sous le nom de Blackmal, BlackWorm, MyWife, Kama Sutra, Grew et CME-24) infecte l'ordinateur dès l'ouverture d'une pièce jointe contenant des liens vers des sites pornographiques ou via des fichiers en accès libre sur le réseau. En quelques secondes, le virus nettoie le disque dur et infecte 11 formats différents, y compris Microsoft Word, Excel, PowerPoint, Access et Adobe Acrobat. Le texte est remplacé par une succession aléatoire de caractères. Le ver Nyxem se caractérise également par son activation le 3 de chaque mois.

Un groupe d'étude indépendant de l'université de Magdebourg (AV-Test.org) a étudié la vitesse de réaction des éditeurs de logiciels anti-virus face à l'émergence de Nyxem. Cette étude démontra que certains programmes avaient pu détecter le ver grâce aux technologies proactives, soit avant la publication de la signature :

1. Détection proactive de Nyxem à l'aide d'inhibiteurs de comportement :

Kaspersky Internet Security 2006 (Beta 2)	POSITIF
Internet Security Systems: Proventia-VPS	POSITIF
Panda Software: TruPrevent Personal	POSITIF

2. Détection proactive de Nyxem à l'aide d'analyseurs heuristiques :

eSafe	Trojan/Worm [101] (suspicious)
Fortinet	suspicious
McAfee	W32/Generic.worm!p2p
Nod32	NewHeur_PE (probably unknown virus)
Panda	Suspicious file

3. Date de publication de la signature de Nyxem :

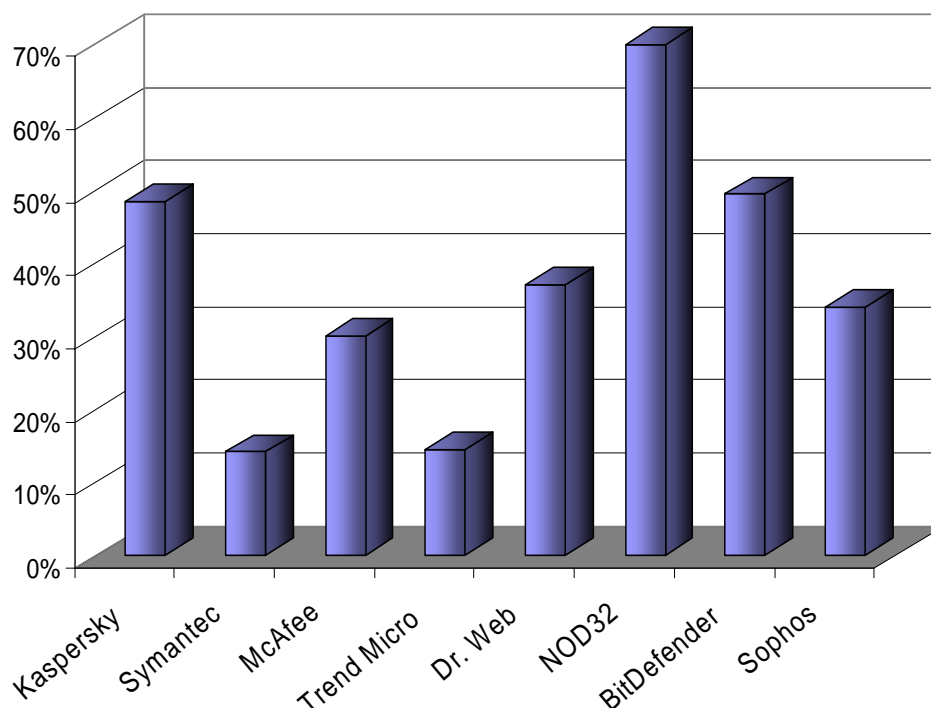
BitDefender	2006-01-16	11:13	Win32.Worm.P2P.ABM
Kaspersky	2006-01-16	11:44	Email-Worm.Win32.VB.bi
AntiVir	2006-01-16	13:52	TR/KillAV.GR
Dr Web	2006-01-16	14:56	Win32.HLLM.Generic.391
F-Secure	2006-01-16	15:03	Email-Worm.Win32.VB.bi
VirusBuster	2006-01-16	15:25	Worm.P2P.VB.CIL
F-Prot	2006-01-16	15:31	W32/Kapser.A@mm (exact)
Command	2006-01-16	16:04	W32/Kapser.A@mm (exact)
AVG	2006-01-16	16:05	Worm/Generic.FX
Sophos	2006-01-16	16:25	W32/Nyxem-D
Trend Micro	2006-01-17	03:16	WORM_GREW.A
eTrust-VET	2006-01-17	06:39	Win32/Blackmal.F
Norman	2006-01-17	07:49	W32/Small.KI
ClamAV	2006-01-17	08:47	Worm.VB-8
Avast!	2006-01-17	15:31	Win32:VB-CD [Wrm]
eTrust-INO	2006-01-17	16:52	Win32/Cabinet!Worm
Symantec	2006-01-17	17:03	W32.Blackmal.E@mm

Ainsi, huit logiciels anti-virus ont pu identifier Nyxem à l'aide de méthodes proactives. Cela veut-il dire que les technologies proactives sont capables de remplacer la méthode «classique» des signatures ? Bien sûr que non. Afin d'analyser l'efficacité des méthodes proactives, il faut tester les logiciels anti-virus sur un ensemble de codes malicieux et non pas sur un seul exemplaire (même s'il s'agit un exemplaire célèbre).

Andreas Clementi (www.av-comparatives.org) est un des rares chercheurs indépendants qui étudient l'application des technologies proactives à un large éventail de cyber-risques. Afin de vérifier si un logiciel anti-virus est capable de déceler les menaces qui n'existent pas encore dans les signatures, il est possible d'utiliser les menaces apparues récemment notamment celles parues sur les six derniers mois. Il va de soi dans ce cas, que le logiciel anti-virus est équipé des bases antivirales les plus récentes. Ainsi, le programme doit assurer la protection contre des menaces dont il ne connaît pas l'existence. C'est précisément les résultats de ce genre de tests qu'Andreas Clementi diffuse.

Selon les résultats d'un test réalisé en 2005, les analyseurs heuristiques les plus efficaces étaient ceux d'Eset, de Kaspersky Anti-Virus et de Bitdefender.

Niveau de détection (heuristique) proactive :

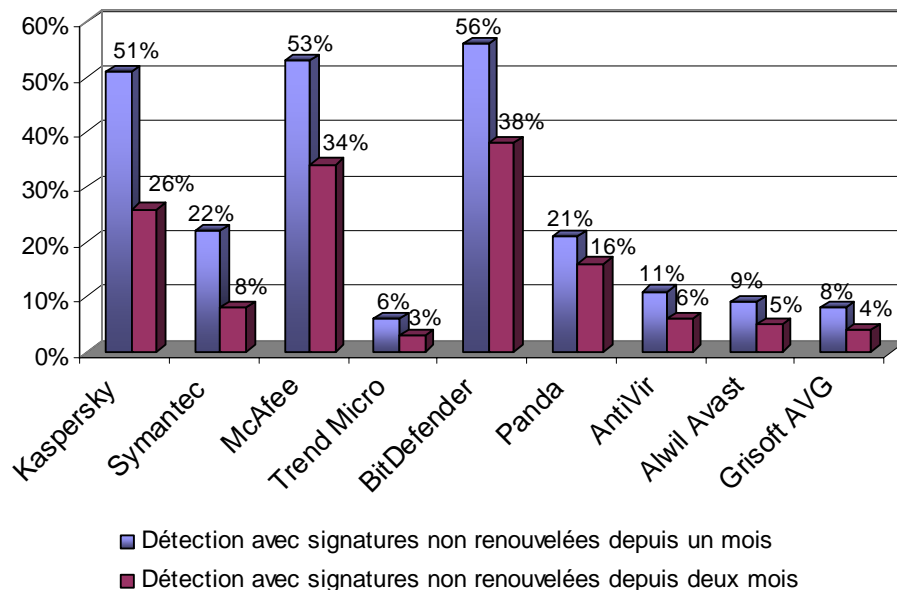


Source : AV-Comparatives.org

Ce test fut réalisé sur un ensemble de 8 259 codes malicieux. Comme le montre clairement le graphique, le taux d'efficacité de découverte proactive le plus haut fut de 70%. Cela signifie que 2 475 codes malicieux sont passés au travers.

Le même test mené par les experts de l'université de Magdebourg - AV-test.org - en mars 2006 à la demande de PC World, montre que les leaders du test atteignent un niveau de détection heuristique de 60%. Cette étude a été effectuée sur des logiciels anti-virus dont les signatures n'avaient pas été renouvelées depuis un ou deux mois.

Niveau de détection (heuristique) proactive



Source : AV-Test.org, PCWORLD

De plus, il ne faut pas oublier le nombre élevé de fausses alertes. Pour cette raison, il est nécessaire de trouver un équilibre entre le niveau de détection et le nombre de fausses alertes pour assurer un bon fonctionnement du logiciel anti-virus. Il en va de même pour les inhibiteurs de comportement.

Les résultats du test de AV-Comparatives.org et AV-Test.org illustrent clairement que les méthodes proactives ne peuvent, à elles seules, garantir le niveau de détection requis. Les éditeurs de logiciels anti-virus l'ont d'ailleurs très bien compris : malgré les déclarations sur les méthodes proactives, ils continuent à exploiter en parallèle la méthode de détection via les signatures (dite « méthode classique »). Signalons aussi que les développeurs de solutions qui reposent uniquement sur des technologies proactives (Finjan, StaForce Safe'n'Sec) doivent néanmoins acheter auprès de tiers des licences d'utilisation des technologies «classiques».

Toutefois, les méthodes qui reposent sur les signatures ont également leur défaut. Mais à l'heure actuelle, le secteur anti-virus n'a toujours pas développé une méthode qui pourrait remplacer complètement ces signatures. Par conséquent, en plus de la protection proactive, la rapidité de référencement des nouvelles menaces dans la base de données antivirales demeure un gage de qualité de l'efficacité d'un logiciel anti-virus.

Le tableau ci-dessous retrace la vitesse de réaction en moyenne des éditeurs de logiciels anti-virus face aux principales menaces apparues au cours de l'année 2005. Le groupe de l'université de Magdebourg (AV-Test.org) a analysé le temps nécessaire qu'il fallait aux éditeurs pour diffuser les mises à jour contenant les signatures. L'analyse a impliqué les 16 vers les plus diffusés en 2005 dont Bagle, Bobax, Brodia, Fatso, Kelvir, Mydoom, Mytob, Sober et Wurmark.

Vitesse moyenne de réaction	2005
Entre 0 et 2 heures	Kaspersky
Entre 2 et 4 heures	BitDefender, Dr. Web, F-Secure, Norman, Sophos
Entre 4 et 6 heures	AntiVir, Command, Ikarus, Trend Micro
Entre 6 et 8 heures	F-Prot, Panda Software
Entre 8 et 10 heures	AVG, Avast, CA eTrust-InocuLAN, McAfee, VirusBuster
Entre 10 et 12 heures	Symantec
Entre 12 et 14 heures	-
Entre 14 et 16 heures	-
Entre 16 et 18 heures	-
Entre 18 et 20 heures	CA eTrust-VET

Source : Classement du temps de réaction des logiciels anti-virus (Andreas Marx, Av-Test.org) http://blogs.washingtonpost.com/securityfix/2005/12/anti-virus_resea.html.

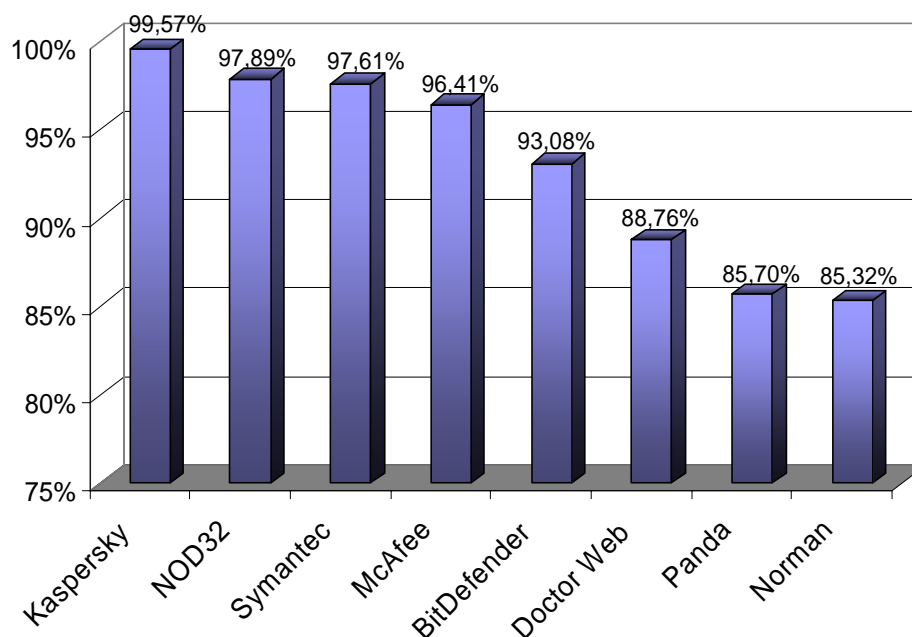
Conclusions

Ce qui précède nous permet de tirer quelques conclusions importantes.

1. L'approche proactive de la lutte contre les programmes malveillants est la réponse adoptée par le secteur anti-virus pour faire face à l'augmentation du nombre de programmes malveillants et à leur vitesse de diffusion. Les technologies proactives d'aujourd'hui permettent en effet de lutter contre de nombreux nouveaux virus mais cela ne signifie pas pour autant que les mises à jour régulières de la protection anti-virus ne sont plus nécessaires. Au contraire, à l'instar des signatures, les méthodes proactives doivent également être actualisées.

L'utilisation de récentes techniques proactives ne peut garantir à elle seule un niveau élevé de détection de codes malicieux. De plus, l'augmentation du nombre de détections entraîne, dans ce cas, une augmentation du nombre de fausses alertes. Bien entendu, les signatures présentent également des inconvénients mais à l'heure actuelle, les éditeurs de logiciels anti-virus ne possèdent aucune alternative qui permettrait de remplacer complètement la méthode « classique ». Dans ces conditions, la vitesse de réaction face à l'émergence de nouvelles menaces demeure un important critère d'efficacité.

Niveau global de détection :



Source : AV-Comparatives.org

2. La protection anti-virus qui se veut optimale doit associer la démarche proactive et la démarche « classique ». C'est la seule manière d'atteindre un niveau maximum d'identification des menaces. Le schéma ci-dessus illustre les résultats des tests réalisés par Andreas Clementi (www.av-comparatives.org) sur le niveau global (signatures+heuristiques) de détection de codes malicieux. Il ne faut pas oublier que le test a été réalisé à l'aide d'une collection de plus de 240 000 virus et qu'un écart 1% représente environ 2 400 virus qui sont passés au travers des mailles.

3. Les utilisateurs de solutions anti-virus ne doivent pas par conséquent faire totalement confiance aux déclarations de certains éditeurs. Les études indépendantes permettent de comparer les caractéristiques complexes des produits et elles sont les mieux adaptées pour évaluer en toute objectivité l'efficacité des solutions proposées actuellement sur le marché.

A propos de Kaspersky Lab

Kaspersky Lab est un éditeur russe de solutions logicielles indispensables pour contrer toutes les formes de cyber-menaces en perpétuelle évolution. Depuis de nombreuses années, les meilleurs experts mondiaux travaillent dans les laboratoires de Kaspersky Lab afin d'offrir des services de hauts niveaux appréciés par les éditeurs et les utilisateurs. 24 h sur 24 h, 7 jours sur 7, les chercheurs analysent et traitent les codes malicieux. Des antidotes sont rapidement développés et validés puis proposés aux utilisateurs via les dizaines de mises à jour quotidiennes.

Kaspersky Lab dispose de bureaux à Moscou, en Allemagne, en Grande Bretagne, au Benelux, en Chine, en Corée du Sud, aux Etats-Unis, en France, au Japon, aux Pays-Bas, en Pologne et au Royaume-Uni.

Fondée en 1997, Kaspersky Lab concentre ses efforts sur le développement de solutions de pointe permettant de protéger les informations et les utilisateurs. Kaspersky Lab développe des logiciels de sécurité destinés à un large spectre d'applications et de clients, de l'utilisateur familial aux grands comptes. Kaspersky Lab distribue, supporte et assure la promotion de ses produits dans plus de 50 pays dans le monde.

Pour plus d'informations concernant Kaspersky Lab : <http://www.kaspersky.fr>
Pour plus d'informations sur l'actualité virale : <http://www.viruslist.com/fr>

***Toute l'actualité de Kaspersky Lab est accessible aux journalistes sur :
<http://presse.kaspersky.fr>***

Contacts presse :

MEDIASOFT COMMUNICATIONS
Emmanuelle Bureau du Colombier
Ebdc@mediasoft-rp.com
Peggy Lainé
Peggy.laine@mediasoft-rp.com
Tél : 01 55 34 30 00

KASPERSKY LAB France
Stéphane Le Hir / Directeur
Jean-Philippe Bichard / Directeur Marketing
Jean.philippe.bichard@fr.kaspersky.com
Tél : 01 41 39 04 89