Sécuriser l'inconnu

LIVRE BLANC

B-HAVE, LA TECHNOLOGIE PROACTIVE DE DÉFENSE CONTRE DES MENACES EN PERPÉTUELLE ÉVOLUTION

Les codes malveillants : le défi d'aujourd'hui

L'univers de la sécurité informatique a nettement changé ces dernières années et les risques auxquels les entreprises sont aujourd'hui exposées n'ont plus rien à voir avec ceux des années passées. Il n'y a pas si longtemps, la création de codes malveillants était encore l'apanage d'amateurs adolescents "frustrés" et cherchant à faire parler d'eux ; aujourd'hui ces codes sont créés par des criminels qui sont des développeurs qualifiés, dans le but de gagner de l'argent. L'exploitation commerciale de cette véritable industrie de malware est à l'origine du développement non seulement de la fréquence mais de la sophistication des attaques.

Les codes malveillants ont désormais atteint un stade épidémique

Avec plus de 3.000 souches identifiées chaque jour en 2007[1], il est devenu extrêmement difficile aux fournisseurs de solutions de sécurité uniquement basées sur les signatures de suivre le rythme. A l'heure actuelle on recense plus de 1 million de malwares connus en circulation.

Les attaques de codes malveillants deviennent de plus en plus sophistiquées

Les risques d'hier étaient relativement "basiques" et généralement assez faciles à évaluer. Les menaces actuelles sont beaucoup plus sophistiquées et spécifiquement conçues pour exploiter les faiblesses des architectures de sécurité classiques :

- Des menaces polymorphes éphémères peuvent échapper à la détection à la fois des solutions antivirus et des systèmes de prévention d'intrusion (IDSs et IPSs) qui reposent sur la réactivité des signatures.
- Les attaques à base de scripts parcourent les multiples zones de vulnérabilité jusqu'à la découverte d'une faille exploitable. Elles utilisent de plus en plus des modules empaquetés pour dissimuler leurs contenus malveillants.
- Les techniques de fragmentation, d'entrelacement et d'injection SQL peuvent être utilisées pour franchir les architectures statiques d'analyse des paquets utilisées par beaucoup de solutions de défense.
- Les ordinateurs portables, comme d'autres matériels mobiles, peuvent aussi servir de vecteurs d'infection ; ils peuvent être utilisés pour introduire des codes malveillants sur le réseau en échappant complètement aux solutions censées protéger le périmètre de sécurité.
- Les méthodes de propagation rapide sont utilisées pour toucher le plus grand nombre possible de systèmes dans un intervalle le plus court possible, avant que les fournisseurs de sécurité puissent diffuser une mise à jour avec la nouvelle signature.
- Entre la découverte d'une menace et la diffusion d'une mise à jour par le fournisseur, il peut s'écouler plusieurs heures, voire plusieurs jours. Cette période constitue une fenêtre de vulnérabilité pendant laquelle les systèmes sont vulnérables.
- Les ordinateurs infectés sont de plus en plus interconnectés dans ce qu'on appelle des réseaux de botnets[2]. Cette stratégie est un moyen extrêmement efficace de mettre à jour les codes malveillants présents sur les machines atteintes. Elle diminue en effet la durée de vie utile d'une signature de virus – certaines familles de bots sont mises à jour quotidiennement.
- Certains codes malveillants prennent désormais pour cible des individus ou des organismes particuliers. De telles attaques peuvent ne pas attirer l'attention des fournisseurs de solutions de sécurité aussi rapidement que celles visant Internet en général, ce qui retarde d'autant la diffusion de la nouvelle signature et contribue à accentuer encore la fenêtre de vulnérabilité.

En résumé, les codes malveillants actuels, très évolués techniquement, mettent en lumière les limites des solutions de sécurité qui ne reposent que sur la réactivité de mise à jour des signatures. Ces solutions ne sont pas devenues obsolètes pour autant ; au contraire, la détection basée sur les signatures reste la méthode la plus fiable et la plus efficace pour déceler les menaces. Néanmoins, pour toutes les raisons mentionnées plus haut, la détection par signatures n'est pas suffisante, et doit être renforcée par un autre type de détection qui :

1. Diminue le facteur de risque entre le moment de la découverte d'une menace et la diffusion de la mise à jour correspondante ;
2. Est immunisé contre les techniques de contournement comme le polymorphisme.

Solutions actuelles aux limites de la sécurité

Les réponses actuelles aux contraintes pesant sur la sécurité reposent essentiellement sur la méthode de détection heuristique.

La détection heuristique

La détection heuristique part du principe que si un programme présente des caractéristiques et/ou un comportement analogues à celles/celui des codes malveillants, il est vraisemblable qu'il s'agisse en effet de codes malveillants. Les virus et les codes malveillants ont tendance à réaliser des actions spécifiques – que les logiciels légitimes n'effectuent pas en général – qui les rendent détectables. Raisonnement a priori élémentaire mais dont la mise en place fait en réalité appel à une technologie extrêmement complexe.

[1] Les malwares atteignent un stade épidémique http://www.darkreading.com/document.asp?doc_id=143424

[2] Botnet est un condensé de robot network. Un botnet peut être décrit comme un ensemble de logiciels malveillants robots (bots en abrégé) dont le rôle est de lancer différentes applications que contrôle leur propriétaire ou le disséminateur de la source du logiciel, sur des ordinateurs vulnérables, couramment connectés à Internet.

Les techniques d'analyses classiques basées sur les signatures utilisent une base de données des signatures de logiciels malveillants (séquences d'octets extraites d'échantillons de codes malveillants) à laquelle les fichiers sont comparés. Si un fichier contient une séquence correspondant à celle d'une signature enregistrée dans la base de données, il est présumé infecté.

Les analyses heuristiques utilisent également une base de données de signatures mais, contrairement aux analyses classiques, chaque signature correspond à une caractéristique ou un comportement typique d'un code malveillant.

Voici un exemple de la façon dont une détection heuristique peut opérer pour détecter une attaque de phishing en utilisant PayPal™. Pour pouvoir ouvrir le site de PayPal, un ordinateur doit d'abord trouver l'adresse IP de PayPal. Il peut consulter son fichier Host pour voir si l'adresse IP figure dans la liste (le fichier Host contient la liste des Host et leur IP correspondant). Si l'adresse existe, elle permet d'ouvrir le site Web. Dans le cas contraire, l'ordinateur essaie de la trouver en contactant le serveur de noms de domaines –Domain Name Server (DNS)-. Une attaque de type phishing modifie le fichier Host de telle sorte que le code malveillant peut diriger les utilisateurs vers un site imprévu – quelqu'un entrant www[point]paypal[point]com dans le champ de l'adresse peut être dirigé vers un site Web créé pour s'approprier les informations sur son compte PayPal. Il existe très peu de programmes légitimes qui modifient le fichier Hôtes. Il est donc relativement sûr de penser que n'importe quel programme essayant de le faire est en fait un logiciel malveillant.

Types de détection heuristique

Il existe deux types de technologie d'analyse heuristique : statique et dynamique. Elles reposent toutes les deux sur «des signatures de comportement» pour identifier les codes malveillants, mais leur ressemblance s'arrête là.

Les analyses statiques examinent la structure d'un logiciel et sa logique de programmation pour déterminer quelles activités il peut avoir, et si l'une d'entre elles correspond éventuellement à un comportement malveillant.

Les analyses dynamiques, exécutent le programme dans un environnement virtuel pour comprendre exactement les actions qu'il effectue afin d'évaluer si l'une de ces opérations correspond à un comportement de logiciel malveillant.

Chaque méthode a ses avantages et ses inconvénients. Dans la mesure où les créateurs de codes malveillants utilisent souvent le cryptage et d'autres techniques de brouillage pour masquer leurs codes, il peut être extrêmement difficile pour une analyse statique de comprendre quels peuvent être les agissements réels d'un programme. Pour surmonter ce handicap, les analyses statiques tentent d'identifier d'autres caractéristiques, par exemple l'existence de routines de cryptage qui peuvent indiquer si un programme est malveillant ou non. Ceci est une aide incontestable pour améliorer la précision de la détection, mais cela signifie aussi que les moteurs d'analyse statique n'ont qu'une visibilité restreinte de ce qu'un programme peut effectivement faire.

Les analyses dynamiques de leur côté n'ont pas de contraintes de visibilité, mais ont un problème différent. L'environnement virtuel mentionné plus haut est, de fait, un ordinateur dans un ordinateur, et nécessite donc des ressources complémentaires. En outre, l'exécution d'un programme et l'analyse de son comportement est souvent un processus long qui peut altèrer la performance du système au point d'avoir des conséquences sur son utilisation.

De plus, la détection heuristique est une science aléatoire, et il peut être extrêmement difficile pour les éditeurs de trouver le juste équilibre entre la détection d'une grande quantité de menaces et la maîtrise des erreurs de classification. Le succès des solutions heuristiques a longtemps été limité par les faux positifs – programmes légitimes classés par erreur dans la catégorie des menaces. Avec pour conséquence des interruptions de travail, un accroissement de l'assistance aux clients, et aussi un coût total de possession extrêmement élevé.

La solution heuristique idéale doit associer la rapidité d'une analyse heuristique statique aux capacités de détection d'une analyse dynamique, tout en assurant un haut degré de précision. C'est exactement ce que BitDefender® s'est attaché à réaliser avec la technologie B-HAVE.

B-HAVE de BitDefender - la nouvelle protection de haute technologie

B-HAVE de BitDefender est une technologie d'analyse heuristique dynamique spécialement développée et conçue pour compléter la technologie de sécurité disponible actuellement en apportant une protection proactive de niveau supérieur, tout en dépassant les limites architecturales propres à beaucoup d'autres solutions dynamiques.

Une approche globale

B-HAVE crée un ordinateur virtuel indépendant. Un émulateur système construit un environnement virtuel, qui comporte un ensemble de matériels virtuels imitant la configuration d'un ordinateur classique. L'environnement virtuel est complètement isolé du véritable ordinateur, de son système d'exploitation et de ses applications. N'importe quel programme peut être lancé dans l'environnement virtuel et son comportement et ses caractéristiques catalogués sans aucun risque pour l'hôte. Pour évaluer le potentiel malveillant d'un programme, B-HAVE recherche les caractéristiques connues pour être associées à un comportement malveillant. Par exemple, un programme peut être estimé malveillant s'il tente de modifier certains fichiers, de lire ou d'écrire dans une zone sensible de la mémoire, ou encore de créer un fichier issu d'un virus connu.

Quand vous essayez d'utiliser un programme suspect, B-HAVE en retarde le lancement jusqu'à ce que son comportement et ses caractéristiques aient été analysés et catalogués dans l'environnement virtuel. Si aucun agissement malveillant n'a été détecté, B-HAVE fait démarrer le programme normalement. En revanche, si une activité suspecte est détectée, B-HAVE met automatiquement l'application en quarantaine, ou la supprime (en fonction des options que vous avez sélectionnées).

De plus, B-HAVE vous offre ainsi qu'à votre ordinateur les avantages suivants :

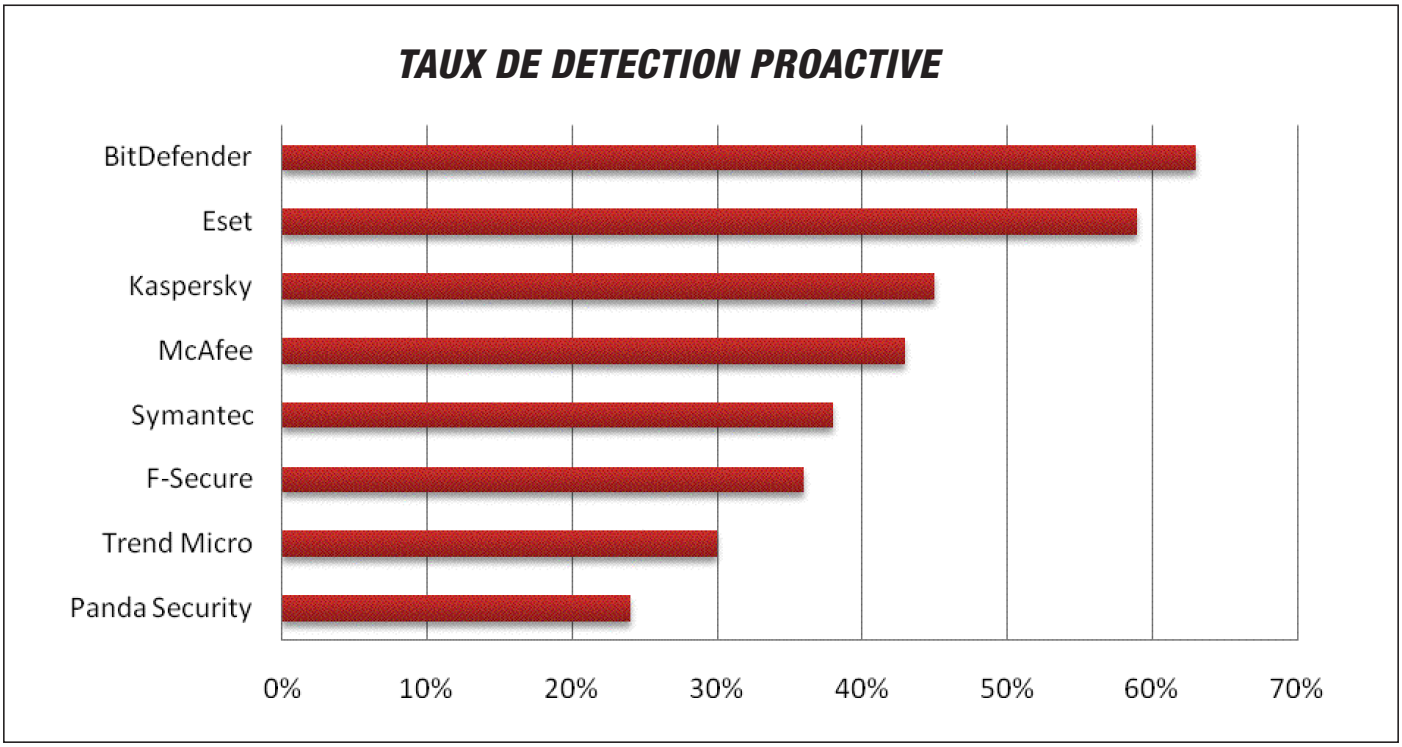
- méthodes génériques de désempaquetage pour une protection contre les menaces de type «Zero-day» utilisant de nouveaux empaqueteurs
- Visual Basic Runtime Engine pour la détection proactive des virus en Visual Basic
- compatibilité COM pour une émulation complète des virus VB
- très bon désempaqueteur statique
- Multiplateforme : fonctionne aussi bien sous Windows que sous les différentes versions de Linux et FreeBSD
- émulation BAT/CMD intégrée dans la machine virtuelle.

Fiabilité et précision

B-HAVE de BitDefender dispose d'un juste équilibre entre fiabilité et précision, en fournissant une solution qui détecte un pourcentage élevé de menaces sans engendrer un nombre important de faux positifs et sans altérer les performances. Les faux positifs sont évités en combinant des technologies (liste blanche) classiques et modernes, notamment :

- une base de données de fichiers connus pour ne représenter aucun danger, comme des exemples de logiciels installés ou de fichiers (multi)media ;
- un mécanisme de prise de décision, qui vous aide à maintenir votre système et vos fichiers en bon état. Pour vous protéger, B-HAVE vous signale par défaut tout comportement potentiellement dangereux. Vous pouvez décider d'approfondir la vérification en envoyant le fichier suspect au laboratoire antivirus de BitDefender, tout en le conservant en quarantaine, ou bien le sortir de la quarantaine s'il est connu pour être inoffensif.

B-HAVE fournit ainsi une protection immédiate et proactive contre les menaces émergentes et nouvelles. Une étude indépendante, entreprise en janvier 2008 par l'organisme Anti-Malware Test Lab[3], a montré que l'heuristique de B-HAVE détectait 63 % des menaces, sans avoir besoin d'une mise à jour de signature.



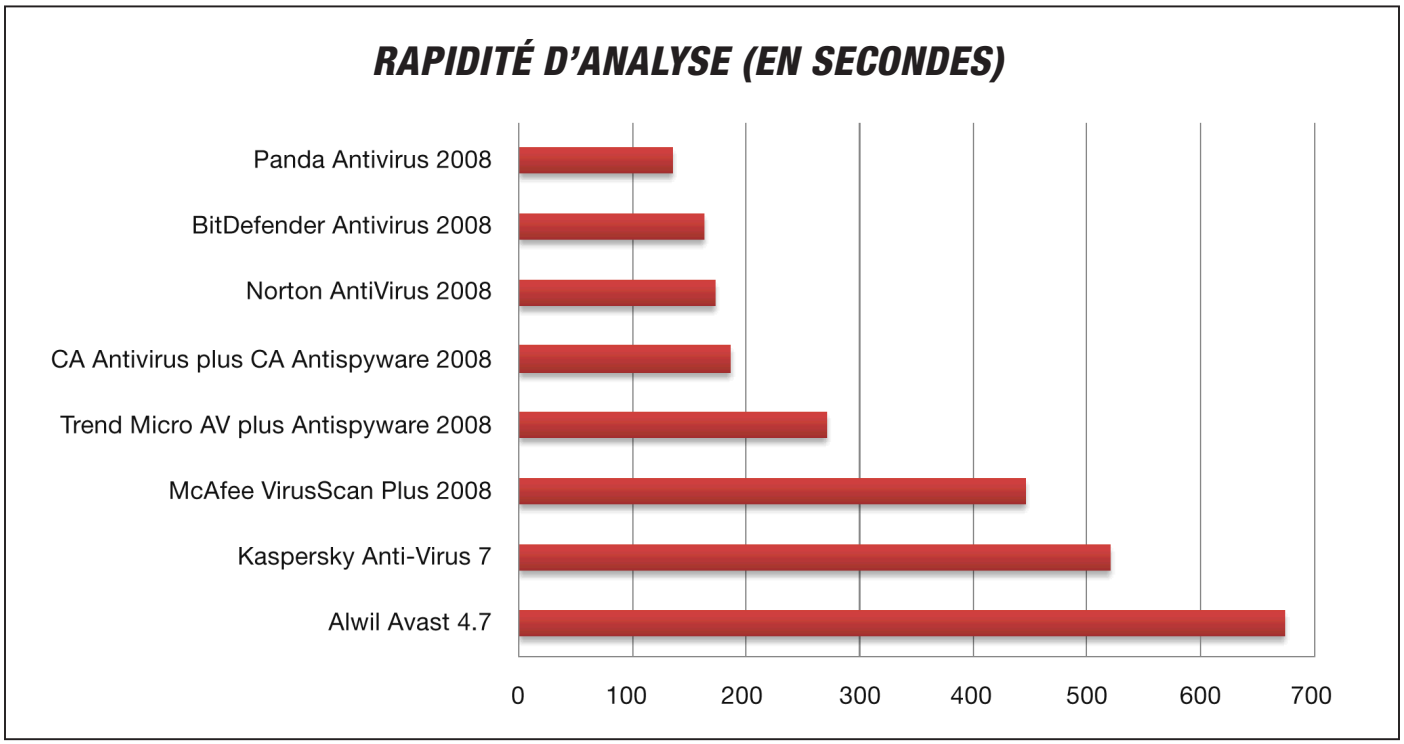
[3] Test de protection antivirus proactive http://www.anti-malware-test.com/?q=node/39

Sécurité dynamique contre menaces dynamiques

Pour éviter une baisse de la performance, B-HAVE entretient une liste de séquences de codes connues, des méthodes d'empaquetage et d'appels système qui sont émulés fonctionnellement par une routine d'accélération qui réduit de manière spectaculaire le temps nécessaire à l'exécution de séquences de code connues dans l'environnement virtuel.

Pour réduire encore l'impact de B-HAVE sur les ressources système, vous avez également la possibilité de choisir de faire confiance à des programmes en les excluant du processus d'analyse.

Bien que le processus puisse paraître long et compliqué, B-HAVE l'accomplit en une fraction de secondes, affichant les actions en cours et les mesures que vous pouvez appliquer. La même étude de AntiMalware Test Lab montre également que les méthodes heuristiques sophistiquées de BitDefender figure parmi les trois meilleures du classement en termes de rapidité d'analyse, comme le confirme dans le graphique ci-dessous.



A propos de BitDefender

BitDefender est le créateur de l'une des lignes de **logiciels de sécurité** les plus rapides et les plus efficaces reconnues au plan international. Depuis ses débuts, en 2001, BitDefender n'a pas cessé de mettre la barre plus haut et de créer de nouvelles normes de protection proactive contre les menaces. Chaque jour, BitDefender protège des dizaines de millions d'utilisateurs privés ou professionnels à travers le monde – leur apportant la tranquillité d'esprit de savoir que leur univers informatique est sécurisé. Les solutions BitDefender sont distribuées par réseau à haute valeur ajoutée et des partenaires revendeurs dans plus de 100 pays à travers le monde. D'autres informations sont disponibles **sur notre site de solutions de sécurité.**