ÉDITIONS PROFIL

B-HAVE – LA VOIE DE LA RÉUSSITE

ÉTUDE DE CAS SUR LE DÉPLOIEMENT RÉUSSI DE LA NOUVELLE TECHNOLOGIE DE DÉTECTION DE CODES MALVEILLANTS

bitdefender
secure your every bit

EN OCTOBRE 2004, AV-Test, un centre de test indépendant situé en Allemagne, présente les résultats d'un nouveau type de test conçu pour déterminer la vitesse d'émission des signatures de nouveaux virus ITW («dans la nature»). Le temps de réponse moyen est considéré comme une mesure pertinente pour évaluer le niveau de sécurité offert, sachant que plus la réponse est rapide, moins le risque d'être infecté par un nouveau virus est élevé (le contexte étant alors moins favorable aux virus).

Conduite sur les neuf derniers mois de l'année 2004, l'étude révèle les temps de réponse moyens de tous les développeurs d'antivirus. BitDefender en sort vainqueur avec un temps de réaction moyen de quatre heures contre une moyenne de dix heures pour les autres sociétés.

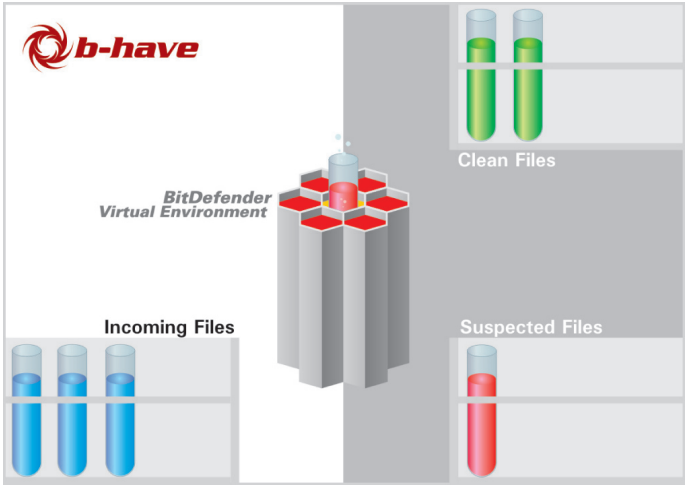
Mais avec les vers autopropulsés (codes malveillants ne nécessitant pas l'intervention de l'utilisateur pour se propager), comme le tristement célèbre ver Witty, quelques minutes seulement peuvent suffire pour infecter une partie non négligeable de la population vulnérable. Compte tenu du fait que les signatures peuvent arriver trop tard, les limites du modèle de signature apparaissent alors évidentes.

Les signatures de virus sont tout simplement des règles qui déterminent «l'aspect» d'un fichier, un peu à l'image des empreintes. Toutefois, de nombreux fichiers (notamment les virus) prennent un aspect différent lorsqu'ils se trouvent dans une mémoire (ou dans l'environnement virtuel) et lorsqu'ils sont sur un disque ou en transit car ils se modifient (ou sont modifiés) au moment de l'exécution, lorsqu'ils sont compressés ou cryptés, par exemple. Il n'est pas possible de relever efficacement les «empreintes» de ce type de fichiers car leur aspect lorsqu'ils sont sur un disque ou en transit n'est pas révélateur de leur mode de fonctionnement.

Les limites du modèle de signature sont finalement prises en compte dans une nouvelle technologie mise au point par le laboratoire BitDefender qui permet aux ordinateurs d'identifier bon nombre de nouveaux virus par eux-mêmes, sans qu'il soit au préalable nécessaire de recevoir de signature depuis un serveur central.

En avril 2005, à la foire CeBit de Hanovre en Allemagne, Bogdan Dumitru, directeur de la technologie BitDefender, présente une nouvelle technologie :

«*Concrètement, et pour employer des termes simples, cette technologie crée un ordinateur virtuel qui exécute des logiciels ayant un comportement suspect pour savoir s'ils essaient de faire ce que font habituellement les virus ou les vers. A partir de là, s'ils ressemblent à un code malveillant et qu'ils se comportent comme tel, nous les bloquons*».



Comme l'avait annoncé Viorel Canja, directeur de recherche au laboratoire BitDefender, lors de cette manifestation, la technologie est introduite progressivement après avoir été testée en interne et sur le terrain. «*Cela fait deux ans que la technologie BitDefender est en gestation et elle ne sera complètement introduite sur le marché que fin 2005. Les taux de détection enregistrés lors des tests sont très satisfaisants. Les prochaines améliorations devraient nous rapprocher encore plus de l'objectif que nous nous sommes fixé : obtenir* ***60% de détection avec l'analyse heuristique comportementale***».

Cinq mois plus tard, les premiers résultats (PC Magazine, USA, août 2005)

Mais à peine cinq mois plus tard, alors qu'une partie de la technologie est en train d'être testée sur le terrain, un nouveau test indépendant démontre qu'elle fonctionne correctement et de façon très efficace.

Détection proactive des codes malveillants exploitant la vulnérabilité MS05- 039, source AV-Test

AV-Test (http://av-test.org/) est un projet de recherche antivirus mené par l'Institute of Technical and Business Information Systems de l'université Otto-von-Guericke de Magdeburg (Allemagne).

L'institut a mesuré les temps de détection de six des programmes malveillants émis la semaine précédente exploitant la vulnérabilité du Plug and Play MS05-039 avec trente-six produits antivirus différents. Onze de ces produits ont permis de détecter au moins une attaque de façon proactive sans mise à jour particulière pour l'identifier spécifiquement.

Voici les résultats obtenus par chacun de ces onze produits :

PRODUIT	RÉSULTAT
BitDefender	6 sur 6
Fortinet	6 sur 6
Nod32	5 sur 6
eSafe	3 sur 6
F-Prot	3 sur 6
Panda	3 sur 6
QuickHeal	3 sur 6
McAfee	2 sur 6
Norman	2 sur 6
AntiVir	1 sur 6
ClamAV	1 sur 6

«*BitDefender et Fortinet ont vraiment fait un travail formidable dans ce test et certains des autres produits ont également obtenu de bons résultats. AV-Test constate que eSafe, Fortinet et QuickHeal utilisent des règles de détection heuristique qui génèrent également un grand nombre de faux positifs lorsque les fichiers analysés sont simplement compressés au moment de l'exécution*».
Source : http://www.pcmag.com/article2/0,1895,1850851,00.asp (août 2005)

Finalement, BitDefender est le seul produit à avoir détecté de façon proactive les six variantes du ver Zotob sans avoir généré de «faux positifs».
B-HAVE se prépare à un bel avenir.

Cinq mois plus tard, la détection des codes malveillants Top-Notch (PC World, USA, janvier 2006)

Cinq mois plus tard, PC World USA publie un test qui démontre de façon irréfutable que B-HAVE est à la hauteur de toutes les espérances.

L'objectif de «60% de détection avec l'analyse B-HAVE» est quasiment atteint grâce à une technologie qui va en se perfectionnant. Des améliorations sont à prévoir dans les mois à venir. Le déploiement réussi de la technologie B-HAVE place BitDefender dans une position enviable.

PRODUIT	DÉTECTION PROACTIVE	
	Détection heuristique avec des signatures datant d'un mois	Détection heuristique avec des signatures datant de deux mois
BitDefender 9 Standard	56,00 %	38,00 %
McAfee VirusScan 2006	53,00 %	34,00 %
F-Secure Anti-Virus 2006	52,00 %	27,00 %
Kaspersky Anti-Virus Personal 5.0	51,00 %	26,00 %
Symantec Norton AntiVirus 2006	22,00 %	8,00 %
Panda Titanium 2006 Antivirus + Antispyware	21,00 %	16,00 %
AntiVir Personal Edition Classic 6.32	11,00 %	6,00 %
Alwil Software Avast Home Edition 4.6	9,00 %	5,00 %
Trend Micro PC-cillin Internet Security Security 2006	6,00 %	3,00 %
AVG Personal 7,1	8,00 %	4,00 %

«*Cet outil antivirus peu coûteux a obtenu les meilleurs résultats dans nos tests heuristiques et détecté le plus grand nombre de codes malveillants. BitDefender 9 Standard est un produit économique, simple d'utilisation et efficace pour détecter les menaces de codes malveillants ; cela explique qu'il ait remporté le prix du Meilleur Achat décerné par PC World dans The New Virus Fighters parmi dix produits antivirus*».

En mai 2006, le centre de test indépendant AV Comparatives.org démontre que le taux de détection proactive des moteurs BitDefender est supérieur à celui de tous ses principaux concurrents (à savoir F-Secure, Kaspersky, McAfee, Symantec et Panda), enregistrant une performance de 15 % supérieure au taux de son plus proche concurrent et pas moins de 29 % par rapport à Symantec. Les résultats détaillés sont consultables sur le site Web d'AV-Comparatives :

http://www.av-comparatives.org/seiten/ergebnisse_2006_05.php

Cinq mois plus tard, détection proactive d'un code malveillant inconnu lors du test Virus Bulletin (Octobre 2006)

Rappelons que la certification VB100 est décernée par Virus Bulletin lorsque le produit antivirus détecte 100% des virus en circulation, dits «In the Wild», et, de surcroît, ne détecte aucun «faux positif», un fichier «sain» déclaré comme «contaminé»- durant le test.

Alors que l'organisme indépendant Virus Bulletin réalise une nouvelle fois ses tests sur les différents éditeurs d'antivirus, un incident survient qui va démontrer la supériorité de la technologie d'analyse comportementale B-HAVE, incluse dans les moteurs d'analyse BitDefender.

En effet, BitDefender détecte, selon Virus Bulletin, un faux positif. Après une analyse plus approfondie par BitDefender et validée par Virus Bulletin, il s'avère que le faux positif n'en était finalement pas un. Le fichier «sain» est apparu être un exemple de Multiexploit qui contenait un «nuker» (un meta-ver, qui essaie régulièrement un certain nombre de failles à la suite contre un éventail de cibles préprogrammées).

Seul le moteur d'analyse BitDefender a détecté ce malware en utilisant sa technologie d'analyse comportementale B-HAVE. Virus Bulletin a publié très rapidement un erratum pour le dernier test VB100, certifiant ainsi la toute nouvelle version de BitDefender v10 pour station de travail.

Tous les produits BitDefender conçus pour les postes de travail et serveurs de fichiers bénéficient de la technologie B-HAVE, la nouvelle technologie de défense proactive le plus aboutie du marché.

Avantages de la technologie B-HAVE par rapport aux autres technologies existantes :

- Méthodes génériques de décompression procurant un support de décompression immédiat pour les nouveaux formats de compression ;
- Moteur d'exécution Visual Basic pour la détection proactive des virus Visual Basic ;
- Plus rapide car la plupart des fonctions utilisées dans le sous-système de fenêtrage ne sont pas émulées mais plutôt exécutées directement, ce qui augmente considérablement la vitesse d'analyse ;
- Activée par défaut sur demande et à l'accès ;
- Support COM permettant d'émuler totalement les virus VB ;
- Efficace contre les virus et les portes dérobées, mais aussi contre les chevaux de Troie ;
- Très bon support de décompression statique ;
- Indépendante des plateformes : fonctionne sous Windows ainsi que sur toutes les versions de Linux et FreeBSD ;
- Emulation BAT/CMD intégrée à l'ordinateur virtuel.

A propos de BitDefender®

Les technologies antivirus BitDefender protègent aujourd'hui plus de 120 millions d'utilisateurs dans plus de 180 pays, directement ou via leur intégration dans des applications tierces (GFI Mail, 602Software, Sharman Networks, Gdata, Bullguard…). Les moteurs de détection antivirus BitDefender sont certifiés par les organismes indépendants ICSA Labs, Checkmark, CheckVir, TUV et Virus Bulletin. BitDefender a par ailleurs reçu le prix de l'innovation technologique décerné par la Commission Européenne (www.ist-prize.org). Les solutions Linux sont certifiées «RedHat Ready» et «Mandriva Certified». Les solutions BitDefender sont éditées en exclusivité par Editions Profil sur les marchés francophones.

La gamme BitDefender®
est éditée dans les pays francophones
en exclusivité par Editions Profil.

ÉDITIONS PROFIL
49, rue de la Vanne - 92120 Montrouge
Tél. (+33) 1 47 35 72 73
Fax (+33) 1 47 35 07 09
www.editions-profil.eu

bitdefender
secure your every bit