La technologie BitDefender

Active Virus Control

Introduction

BitDefender® Active Virus Control est une nouvelle technologie de détection heuristique qui est disponible pour les produits Windows à partir de **BitDefender 2010**. Active Virus Control est le résultat des efforts réalisés par BitDefender pour rester à la pointe du développement des technologies proactives. Active Virus Control agit comme une couche supplémentaire de protection contre les nouvelles menaces, complétant les techniques heuristiques statiques existantes et B-Have (analyse heuristique dans un environnement virtuel).

Description

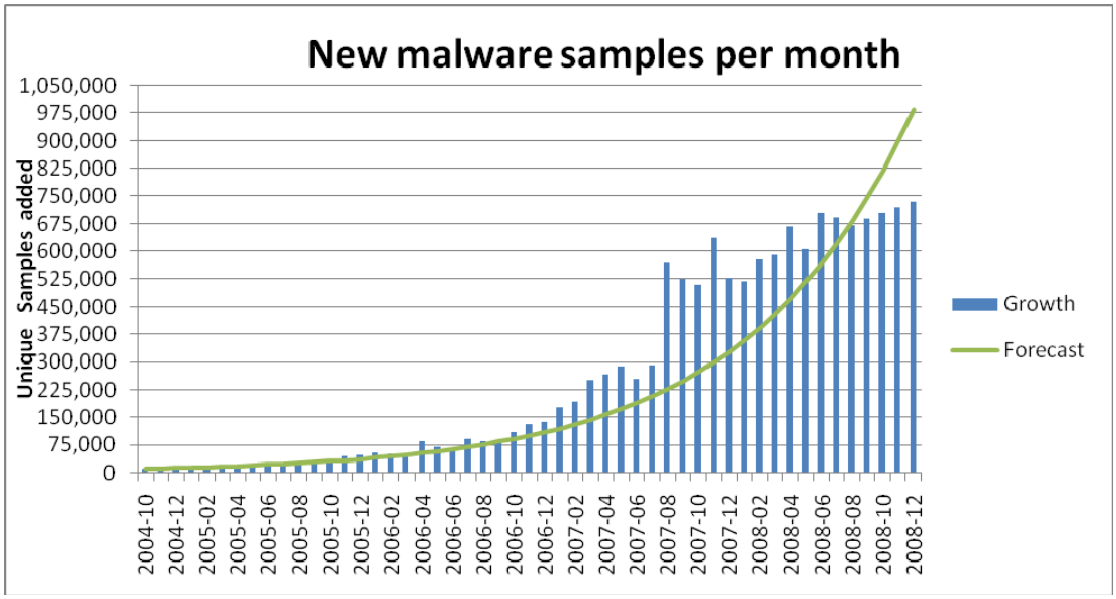
BitDefender ® Active Virus Control est une technologie proactive innovante qui utilise des méthodes heuristiques avancées pour détecter de nouvelles menaces potentielles en temps réel. Elle surveille les programmes en cours d'exécution sur votre PC à la recherche de comportements ressemblant à ceux des malwares. À partir d'un certain nombre d'actions détectées, le programme les ayant réalisées est considéré comme nuisible.

Fonctionnalités clés :

- Taux de détection des virus nouveaux et inconnus extrêmement élevé
- Surveillance des applications pendant toute la durée de leur exécution, pas seulement lorsque l'utilisateur y accède ou les lance pour la première fois
- Détection de virus conçus spécialement pour échapper à la détection des produits antivirus
- Bonne intégration au système permettant la surveillance des processus avec une faible consommation de ressources

Pourquoi Active Virus Control?

De nouveaux virus sont créés tous les jours. Jusque là rien de nouveau. Mais que se passerait-il si 500 000 nouveaux virus étaient créés tous les mois ? Et si certains d'entre eux intégraient des éléments conçus pour échapper à la détection basée sur les signatures, à l'analyse heuristique statique ou même, à des techniques de détection plus avancées ? Une nouvelle technologie serait alors nécessaire, une technologie créant une barrière supplémentaire entre le système et les menaces potentielles.



Source : av-test.org – Augmentation du nombre de malwares

BitDefender ® Active Virus Control est une technologie proactive innovante qui utilise des méthodes heuristiques avancées pour détecter de nouvelles menaces potentielles en temps réel. Elle surveille les programmes en cours d'exécution sur votre PC à la recherche de comportements ressemblant à ceux des malwares. À partir d'un certain nombre d'actions détectées, le programme les ayant réalisées est considéré comme nuisible.

Contrairement à d'autres technologies heuristiques qui contrôlent uniquement les fichiers exécutables lorsque l'utilisateur y accède ou les lance pour la première fois, Active Virus Control surveille toutes les actions des applications tant qu'elles sont actives.

Active Virus Control est l'une des technologies de protection proactive de BitDefender, avec l'analyse heuristique statique et B-Have (analyse heuristique dans un environnement virtuel). En raison de son implantation unique (Active Virus Control commence à agir lorsque tous les autres types de scanners ont autorisé l'exécution d'un fichier), Active Virus Control peut être considéré comme la dernière ligne de défense d'un PC.

FAQ

Q : Active Virus Control ressemble beaucoup à B-Have. Quelle différence y a-t-il entre ces deux technologies ?

R : En fait, il s'agit de deux technologies heuristiques – c'est-à-dire qu'elles détectent de nouveaux virus en fonction de leur comportement plutôt qu'à l'aide des signatures de virus. Mais B-Have exécute et analyse des fichiers dans un environnement virtuel, pendant une durée limitée, alors qu'Active Virus Control travaille en temps réel, sur le véritable PC, en surveillant les applications pendant toute la durée de leur exécution.

Q : Pourquoi a-t-on besoin d'Active Virus Control si l'on a B-HAVE ?

R : B-HAVE présente certaines limites :

- L'émulation ne peut pas se poursuivre indéfiniment – un morceau de code peut devenir nuisible après une minute ou une heure de fonctionnement et personne ne souhaite attendre aussi longtemps avant que sa solution de sécurité ne garantisse que l'application ne présente aucun danger.

- une application déjà vérifiée (et donc de confiance) peut être exploitée et même modifiée en mémoire, pendant son exécution, ou utilisée pour lancer un processus malveillant avec ses propres données d'authentification

Active Virus Control est une nouvelle technologie capable de détecter et de bloquer les processus masquant leurs activités, en temps réel, sur un système actif. C'est une couche de sécurité supplémentaire entre les systèmes et les codes inconnus / potentiellement malveillants.

Q : Active Virus Control est-il efficace ?

R : D'après des tests internes, Active Virus Control a détecté 63.5% des malwares qui n'avaient pas été détectés par BitDefender en utilisant B-Have ou les autres moteurs antivirus.

Q : Active Virus Control affectera-t-il les performances de l'ordinateur ?

R : BD-AVC n'ajoute que très peu de temps système aux entrées/sorties et au temps UC, c'est pourquoi nous pensons que son impact ne sera pas significatif.

Q : Quelles sont les actions considérées comme suspectes ?

R : Actions suspectes possibles :

- Se présenter comme un type de processus différent
- Exécuter du code dans l'espace d'un autre processus (dans la mémoire d'un processus)
- Se répliquer
- Déposer des fichiers et d'autres éléments.

Q : Donc, si un processus réalise l'une de ces actions, il est bloqué ?

R : Non, car toutes ces actions ne sont pas aussi suspectes les unes que les autres. Un calcul est effectué, et chaque action suspecte ajoute des points au score total. Une fois un certain score atteint, le processus est considéré comme malveillant.

Q : Active Virus Control est-il présent dans tous les produits BitDefender ?

R : Actuellement, Active Virus Control est présent uniquement dans les produits Windows s'adressant aux particuliers et au marché SOHO : BitDefender Antivirus 2010, BitDefender Internet Security 2010, et BitDefender Total Security 2010.