Bitdefender®

Active Threat Control

Protection proactive contre les menaces nouvelles et émergentes

Sommaire

1. Pourquoi vous devriez lire ce livre blanc

La hausse sans précédent de nouvelles menaces a rendu les mécanismes de sécurité traditionnels à la fois inefficaces et peu fiables pour fournir une défense adéquate. De nos jours, les menaces prépondérantes ont gagné en complexité, rendant la prévention, la détection et la désinfection difficiles pour les logiciels de sécurité traditionnels.

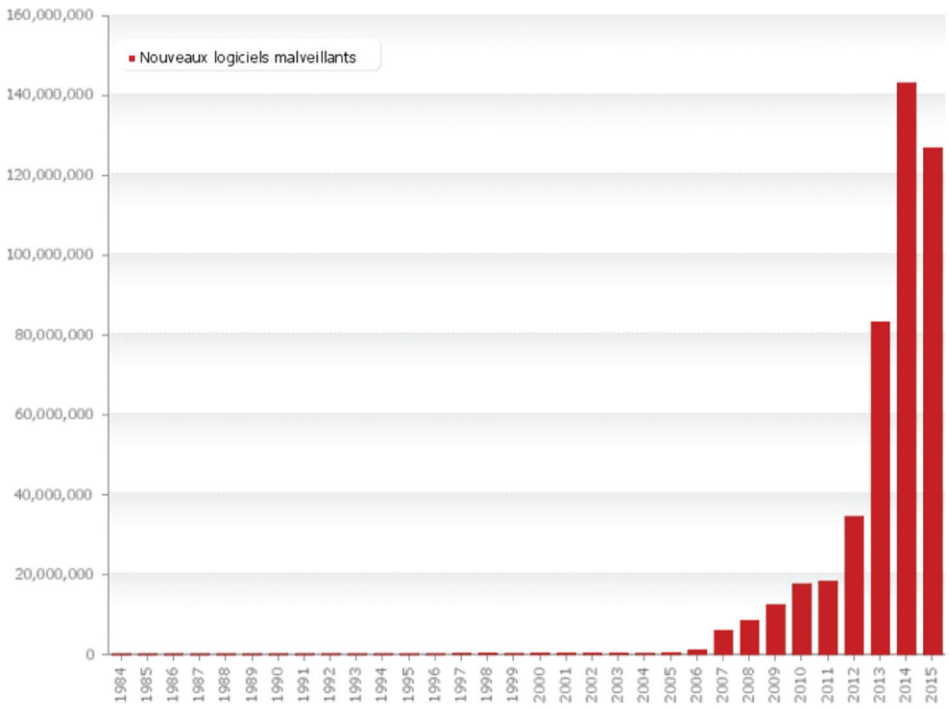
Bitdefender Active Threat Control est une technologie de détection proactive et dynamique, basée sur le contrôle des processus et des événements système et le marquage des activités suspectes. Elle a été conçue pour lutter contre les menaces encore inconnues, en analysant leur comportement.

Ce livre blanc explique pourquoi une telle protection est nécessaire et fournit un aperçu technologique et technique des méthodes de détection utilisées par les solutions Bitdefender.

2. Les malwares modernes impliquent la mise en place de contre-mesures pour lutter contre les menaces

Préserver la sécurité des endpoints contre les menaces n'a jamais été plus difficile qu'aujourd'hui. Avec plus d'un demi-million de nouvelles souches et variantes de malwares émergeant chaque mois, détecter et contenir chaque menace est devenu une tâche extrêmement difficile pour tous les éditeurs de sécurité.

La situation est aggravée par le fait que les malwares et les mécanismes utilisés pour les distribuer sont devenus de plus en plus sophistiqués. Les sites de confiance peuvent être compromis et utilisés pour lancer des attaques basées sur des scripts complexes, en utilisant de multiples exploits de manière cyclique. Des méthodes avancées de packaging sont déployées dans le but de dissimuler les charges malveillantes. Ces malwares ont également la capacité de désactiver des logiciels de sécurité connus au moment de l'installation et pendant leur fonctionnement en essayant en permanence de tuer les processus de l'antimalware ou du pare-feu.



Source : av-test.org : Plus de 14 millions de nouvelles variantes de codes malveillants sont découvertes chaque mois. Chiffres arrêtés au 09/11/2015.

Les réseaux sociaux tels que Facebook et Twitter fournissent aussi aux cybercriminels de nouvelles opportunités de développement, grâce aux techniques d'ingénierie sociale. De plus, de par leur caractère viral, ces sites peuvent permettre aux malwares de se diffuser plus rapidement que jamais. Alors qu'auparavant un malware avait besoin de plusieurs jours, voire semaines pour se diffuser, il peut aujourd'hui atteindre des millions d'ordinateurs à travers le monde en seulement quelques heures.

Combinés, ces facteurs font qu'il est extrêmement difficile de détecter et de bloquer les malwares actuels en utilisant des méthodes et des technologies classiques.

3. Une question d'argent

Le principal vecteur d'augmentation à la fois du volume et de la complexité de ces menaces est l'argent. Historiquement, les virus étaient créés par des adolescents dans le but de se faire connaître et ainsi obtenir la reconnaissance de leurs compétences en codage. Les malwares d'aujourd'hui sont développés par des cybercriminels pour gagner leur vie et dans l'optique de générer des profits substantiels. Le spam, le phishing, les techniques de pump-and-dump ou encore les chevaux de Troie qui dérobent les données et enregistrent les frappes du clavier peuvent rapporter à leurs créateurs des revenus très importants. Le marché des malwares a évolué jusqu'à devenir une industrie internationale générant des millions de dollars, tout aussi qualifiée et familière des questions de sécurité que les experts travaillant dans l'univers de la sécurité informatique.

Ces questions d'argent ont également mené à un changement significatif de la nature des malwares d'aujourd'hui : ils sont invisibles pour l'utilisateur. Par exemple, si votre ordinateur est infecté par une de ces menaces, vous ne vous en rendrez pas compte tant que vous ne remarquerez pas sur votre relevé bancaire que des transactions inexpliquées ont été réalisées ou que votre appareil ne semble consommer plus de ressources qu'habituellement.

Etant donné que les criminels sont désormais en mesure d'utiliser leurs énormes profits pour refinancer le développement de nouveaux malwares, un cercle vicieux s'est créé : plus ils gagnent d'argent, meilleurs deviennent leurs logiciels malveillants. Meilleurs sont leurs logiciels, plus ils gagnent d'argent. La cybercriminalité coûte à l'économie mondiale environ 415 milliards d'euros chaque année, les dommages liés au vol de propriété intellectuelle seuls dépassent les 149 milliards d'euros, selon une analyse du Centre d'études stratégiques et internationales (CSIS) publiée le 9 juin 2014. Avec de telles sommes en jeu, il est évident que ces criminels ont à la fois la motivation et les moyens financiers de continuer à développer des menaces de plus en plus sophistiquées.

4. L'heuristique : détecter aujourd'hui les menaces de demain

Comme on l'a vu précédemment, assurer une réponse rapide à chaque nouvelle menace peut s'avérer particulièrement difficile. Cependant, il est essentiel que la réponse soit la plus rapide possible, les nouvelles variantes de malwares étant capables de se propager rapidement. Une réponse lente ou différée peut conduire à la compromission d'un grand nombre d'ordinateurs et entraîner la perte de données personnelles et professionnelles ou avoir un impact considérable sur les infrastructures réseau.

Le défi est que, indépendamment de la rapidité avec laquelle les fournisseurs de sécurité réagissent, il y a toujours un écart entre le moment où une nouvelle menace est mise en circulation et celui où les ordinateurs sont "immunisés" contre cette menace par l'intermédiaire d'une mise à jour de signature, fournie par la solution de sécurité installée. L'écart entre les premiers moments où une menace peut infecter un système jusqu'à ce que le correctif soit diffusé par l'éditeur crée une fenêtre d'opportunité pour les cybercriminels. Avec plus d'un demi-million de nouveaux échantillons de malwares qui apparaissent tous les mois, il y a de grande chance que cette fenêtre soit en faveur des attaquants.

La détection classique repose sur les signatures. Les signatures antimalwares sont des extraits de code des échantillons de malwares et sont utilisés par les logiciels de sécurité pour réaliser du pattern-matching. Le problème avec cette méthode est qu'il faut un certain temps pour "produire" la signature : en effet les fournisseurs d'antimalwares ont d'abord besoin d'obtenir un échantillon du malware en question, de développer une signature et enfin de "pousser" cette signature aux utilisateurs - ce qui conduit à la création de la fenêtre dont nous parlions précédemment.

L'heuristique est une forme de détection proactive qui empêche la création de cette fenêtre de vulnérabilité. Plutôt que de compter sur ces signatures, ces empreintes ou données binaires, la détection heuristique repose sur des algorithmes complexes qui révèlent des profils et des comportements réels, pouvant indiquer qu'une application est malveillante. Ce modèle fonctionne car les programmes malveillants tentent inévitablement d'effectuer des actions dans un contexte où des applications légitimes ne le feraient pas. Voici quelques exemples de comportements suspects : copier des fichiers ou déguiser des processus, injecter ou l'exécuter du code dans l'espace mémoire d'un autre processus. Parce que la détection heuristique recherche des caractéristiques comportementales plutôt que de compter sur le simple pattern-matching, elle est capable de détecter et de bloquer les nouvelles menaces pour lesquelles une signature ou une empreinte digitale n'a pas encore été publiée.

Pour protéger les ordinateurs, la majorité des détections heuristiques, y compris le moteur heuristique Bitdefender B-HAVE, retarde temporairement l'exécution des applications, le temps que le code soit exécuté dans un environnement virtuel, complètement isolé - une sandbox - sur l'ordinateur réel. Si aucun comportement suspect n'est observé, l'ordinateur lance l'application normalement. Par contre, si un comportement suspect est détecté, le programme est bloqué et ne peut être exécuté. L'ensemble de ce processus se déroule en une fraction de seconde et n'a donc pratiquement aucune incidence sur l'expérience de l'utilisateur, ni sur les performances de l'ordinateur. Afin d'être encore plus efficace, Bitdefender utilise la réputation des applications, une forme de liste blanche, pour que les moteurs heuristiques nécessitent moins de ressources pour l'exécution des applications déjà connues comme étant sûres. La liste de réputation des applications est mise à jour en temps réel via le Cloud Bitdefender afin d'éviter tout faux positif.

Même si cette approche améliore grandement la sécurité, elle présente néanmoins quelques lacunes. Tout d'abord, les programmes ne peuvent être exécutés dans l'environnement virtuel que pendant une courte période. En effet, il ne serait pas acceptable de retarder leur lancement pendant trop longtemps. Cela signifie que les malwares peuvent éviter d'être détectés en étant programmés pour retarder l'exécution de leurs actions malveillantes. Deuxièmement, un programme qui a déjà été vérifié (et qui est par conséquent estimé comme étant de confiance) pourrait être exploité ou modifié en mémoire, pendant son exécution, ou utilisé pour lancer un processus malveillant de manière autonome.

Pour remédier à ces lacunes, Bitdefender a développé Active Virus Control en 2010 - qui a été renommé Active Threat Control en 2015.

5. Bitdefender Active Threat Control (ATC) : la détection heuristique de nouvelle génération

Disposant d'une centaine de paramètres heuristiques lors de son lancement en 2010, Active Threat Control a évolué et en possède plus de 300 à ce jour. Ils sont constamment affinés, mis à jour et améliorés par une équipe dédiée de chercheurs et ingénieurs au sein des Laboratoires antimalwares Bitdefender. Afin de fournir un maximum de sécurité, tous les produits Bitdefender intègrent Active Threat Control, qui comporte 4 étapes d'analyse :

Étape 1 : Chaque fois qu'un fichier est ouvert, copié, téléchargé via Internet, transféré par e-mail ou messagerie instantanée, celui-ci est intercepté soit par le pilote Bitdefender File System, soit par le proxy approprié et envoyé pour analyse.

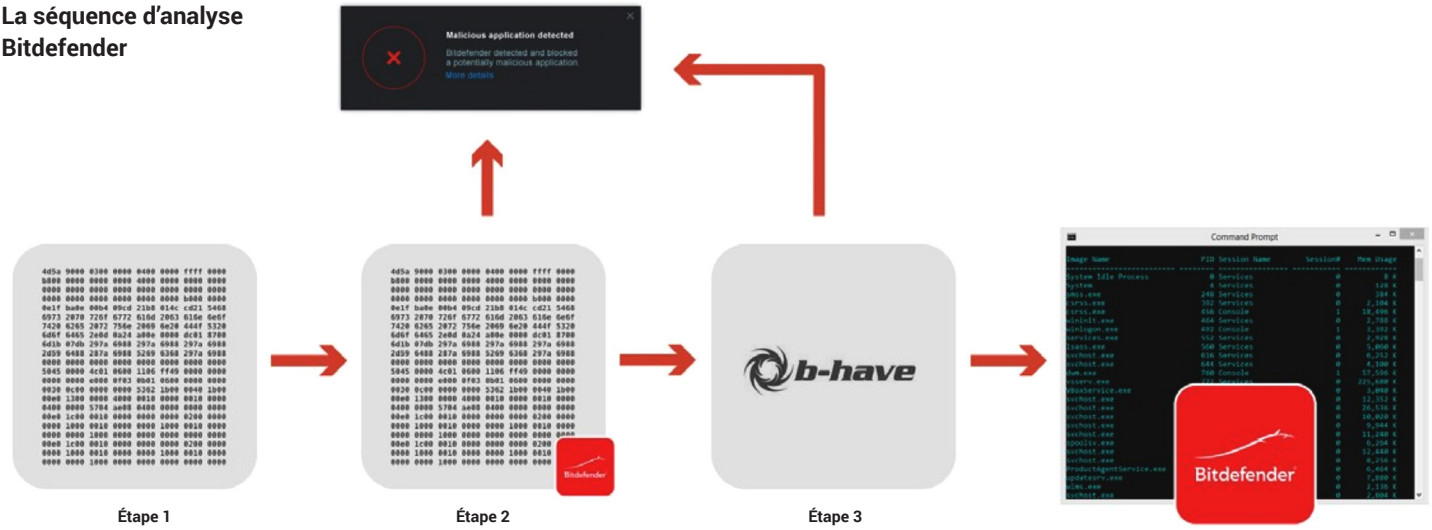
Étape 2 : Le fichier est comparé à la base de données de signatures Bitdefender (une base de données des "empreintes" des malwares) qui est mise à jour toutes les heures. Si le contenu du fichier correspond à l'une des signatures de la base de données, la solution tente automatiquement de désinfecter la menace en question et si cette action échoue, le fichier est placé en quarantaine. Par contre, si aucune signature ne correspond dans la base de données, le fichier est envoyé au moteur Bitdefender B-HAVE pour être analysé.

Étape 3 : B-Have vérifie le fichier en l'exécutant dans un environnement virtuel à l'intérieur même du moteur Bitdefender, conçu pour émuler le comportement d'un fichier ou d'un ordinateur. Si le fichier présente une activité suspecte, qui ressemble à celles que peuvent avoir des malwares, B-Have le signale comme fichier malveillant. Si son comportement n'est pas suspect, le fichier est déclaré sain et le processus est autorisé à s'exécuter.

Étape 4 : Active Threat Control surveille les actions spécifiques des processus en cours d'exécution au sein de l'OS. Le moteur recherche des comportements spécifiques aux malwares et attribue un score pour chaque processus en cours d'exécution, basé sur ses actions et le contexte dans lequel celles-ci ont été réalisées. Lorsque le score global d'un processus atteint un seuil donné, le processus est signalé comme dangereux. Selon le profil de l'utilisateur, il est soit stoppé afin d'isoler et mettre un terme à la menace, soit l'utilisateur est invité à indiquer l'action qui doit être prise (selon les paramètres du profil du produit Bitdefender). Les profils utilisateur sont propres à la solution installée.

La technologie exclusive Bitdefender pour la détection des menaces :

La séquence d'analyse Bitdefender



Étape 1
Accès ou copie d'un fichier ou application

Étape 2
Le fichier est comparé une liste de signatures

Étape 3
Le fichier est analysé par B-Have

Étape 4
Le processus est surveillé par ATC

Contrairement à B-HAVE et à d'autres types de détections heuristiques, Active Threat Control surveille en permanence les processus. De cette façon, l'exécution différée d'un malware peut tout de même être détectée et bloquée. Une surveillance constante empêche ainsi les malwares d'exploiter ou de détourner des applications reconnues comme étant fiables.

6. Fonctionnement d'Active Threat Control : aperçu de cette technologie exclusive

Active Threat Control surveille en permanence toutes les applications et les processus en cours d'exécution sur l'ordinateur. Pour permettre une certaine flexibilité et ne pas impacter les ressources il y a quelques exceptions :

• Les processus mis sur liste blanche par l'utilisateur ;

• Les processus système marqués comme étant fiables par le système de réputation d'applications Bitdefender.

Étape 1
ATC surveille les processus en cours d'exécution
- Pour chaque processus, ATC définit un score global
- Un score spécifique est donné à chaque action importante prise par le processus

Étape 2
ATC détecte malwareapp.exe comme étant une application potentiellement malveillante
- Le score global de malwareapp.exe atteint un certain seuil

Étape 3
ATC notifie l'utilisateur qu'une application malveillante a été détectée et qu'elle a été automatiquement bloquée

Les applications et processus actifs sont surveillés en permanence à la recherche de comportements suspects, comme :

- La copie ou le déplacement de fichiers dans des dossiers Système ou Windows, ou encore vers un emplacement du disque caractérisé par un accès limité ;
- L'exécution ou l'injection de code dans l'espace mémoire d'un autre processus afin d'être exécuté avec des privilèges plus élevés ;
- L'exécution de fichiers qui ont été créés avec des informations stockées dans le fichier binaire ;
- L'auto-réplication ;
- La création d'une entrée de démarrage automatique dans le registre, l'accès ou l'exécution d'opérations illégales dans des emplacements du registre qui nécessitent des privilèges élevés ;
- La copie ou l'enregistrement de pilotes.

Étant donné que même des applications légitimes vont parfois effectuer une ou plusieurs de ces actions (comme la création d'une entrée de démarrage automatique), Active Threat Control ne détermine pas qu'un processus est malveillant en se basant sur une seule et unique action ; à la place, il contrôle un score global et ne catégorise une application comme étant malveillante que lorsqu'un certain seuil est atteint. Cela minimise le risque d'erreurs d'identification (faux positifs) et évite des interventions inutiles de la part de l'utilisateur.

7. Active Threat Control améliore le taux de détection des malwares

Une grande quantité d'échantillons de malwares est détectée par Active Threat Control. Étant donné que B-HAVE est déjà l'un des moteurs les plus avancés et efficaces en matière d'analyse heuristique sur le marché, il est clair qu'Active Threat Control a la capacité de fournir une protection encore meilleure que d'autres solutions sur le marché. Il réduit considérablement le risque de compromission d'un système par une menace nouvelle ou émergente.

8. Conclusion

Les cybercriminels qui développent des malwares ont des méthodes de plus en plus sophistiquées pour minimiser le risque que leurs menaces soient repérées par des détections heuristiques. Certains malwares sont même capables de détecter quand ils sont exécutés dans une machine virtuelle et de retarder le plus longtemps possible le lancement de leurs actions malveillantes, jusqu'à ce qu'ils soient certains d'être exécutés dans l'environnement informatique réel. Pour compliquer le tout, déterminer si oui ou non une application est malveillante en se basant sur les actions qu'elle effectue est loin d'être un processus simple à mettre en place. Par exemple, une application qui va effacer le disque dur peut être un outil système parfaitement légitime ; toutefois, si cette application tente de tromper l'utilisateur et de lui faire restaurer son disque en se faisant passer pour une image disque ou un autre type de fichier inoffensif - alors il peut tout à fait s'agir d'un malware.

Active Threat Control est la réponse de Bitdefender à ces défis. Cette technologie représente une couche de sécurité supplémentaire entre l'ordinateur et les codes potentiellement malveillants, offrant aux utilisateurs un degré de protection sans précédent.

Bitdefender propose des technologies de sécurité dans plus de 100 pays via un réseau de partenaires de premier plan, de distributeurs et de revendeurs à valeur ajoutée. Depuis 2001, Bitdefender produit régulièrement des technologies leaders du marché pour les entreprises et les particuliers et est l'un des plus grands fournisseurs de solutions de sécurité pour les technologies de virtualisation et cloud. Bitdefender associe ses technologies primées à des alliances et des partenariats commerciaux et renforce sa position sur le marché mondial via des alliances stratégiques avec des fournisseurs de technologies cloud et de virtualisation leaders dans le monde.

PROFIL TECHNOLOGY

Plus de **500 millions d'utilisateurs**
sont protégés par les technologies Bitdefender

Bitdefender

Bitdefender est édité en France et dans les pays francophones par PROFIL TECHNOLOGY S.A., éditeur et distributeur de logiciels pour les particuliers et les entreprises.