

Une protection proactive pour se défendre contre les menaces d'Internet

Présentation

Cette TechNote vous explique pourquoi une protection proactive constitue un composant vital des produits de sécurité d'aujourd'hui en décrivant comment l'utilisation intelligente des commandes de comportement d'un programme peut minimiser, sinon éliminer, l'impact des menaces de sécurité en ligne.

Le paysage de la menace

Les menaces de sécurité évoluent pratiquement chaque jour. De nouveaux virus, chevaux de Troie et autres programmes malveillants sont écrits dans le but de s'insinuer dans notre utilisation sûre et utile d'Internet. Les vulnérabilités non corrigées¹ laissent les ordinateurs ouverts à une infection par des exploitations de type « zéro jour » (zero-day) qui risquent d'infliger de sérieux dommages à peine quelques heures après leur apparition sur Internet.

Les chercheurs en matière de sécurité indiquent que le volume de menaces a considérablement augmenté au cours des cinq dernières années et reconnaissent qu'il devient de plus en plus dur pour la détection de signature de garder le rythme avec les créateurs de logiciels malveillants. Les boîtes à outils prêtes à l'emploi permettant la création de logiciels malveillants personnalisés à partir d'échantillons de code donnent même la possibilité aux programmeurs amateurs de créer leurs propres logiciels malveillants. Les équipes de recherche des entreprises de sécurité sont de petite taille quand on les compare au nombre de programmeurs « de l'ombre » qui œuvrent désormais dans les pays très peuplés comme la Chine ou l'Inde, et qui viennent grossir les rangs des pirates et des cybercriminels.

La réduction de la menace est encore plus freinée par le fait que les créateurs de virus adoptent les mêmes techniques de contrôle qualité que les développeurs de logiciels anti programmes malveillants, testant leurs dernières créations sur les dernières versions des logiciels anti programmes malveillants pour s'assurer de toujours avoir une longueur d'avance.

Pour être clair, il est pratiquement impossible de vouloir se protéger des nouveaux programmes malveillants modifiés ou obscurs uniquement avec une solution à base de signature ; les créateurs de programmes malveillants seront toujours capables de maintenir une marge par rapport à ce type de défense réactive².

Besoin de mesures supplémentaires

Bien qu'une protection réactive demeure un composant important de la protection contre les logiciels malveillants pour l'identification précise et la désinfection des programmes connus, le besoin d'une protection proactive pouvant empêcher en premier lieu toute activité non autorisée des programmes est nettement avéré.

En ajoutant une protection proactive qui surveille ce que font les programmes, avec quels programmes et composants un programme donné est autorisé à communiquer, ou toute tentative de modification du système d'exploitation, les ordinateurs sont mieux protégés contre les activités inappropriées et mieux positionnés pour éviter les infections à un stade précoce.

¹ La vulnérabilité du curseur animé de Windows en est l'exemple (<http://secunia.com/advisories/24659>). Ce défaut permet à un agresseur d'accéder aux données et d'exécuter un code non autorisé sur l'ordinateur de l'utilisateur. Microsoft a publié un correctif il y a quelques temps, mais les utilisateurs continuent à être infectés s'ils n'ont pas corrigé leurs systèmes.

² « L'antivirus est mort : vive l'anti logiciels malveillants » : ces recherches de Yankee Group sont abondamment abordées dans un [article](#) de PC World.

L'interactivité entre applications : une faiblesse clé

Windows offre plusieurs méthodes d'interaction entre les programmes sur un PC³ et la majorité de ces interactions sont légitimes. Les programmes peuvent librement partager des composants communs, appeler et lancer les fichiers exécutables d'un autre programme et utiliser un certain nombre d'accroches différentes pour simplifier l'interaction entre les programmes et rendre l'expérience informatique de l'utilisateur plus simple et plus pratique. Voici un exemple de ce que nous venons d'expliquer : pour lire un fichier PDF joint à un message électronique il vous suffit de cliquer sur l'icône du fichier pour que le PDF se charge automatiquement dans la visionneuse par défaut. Cela prendrait beaucoup plus de temps si vous deviez enregistrer le fichier sur le disque, ouvrir Acrobat Reader, puis charger le fichier dans l'application.

Toutefois, Windows autorise également les interactions moins bénignes, ce qui constitue un risque de sécurité majeur. Les applications elles-mêmes peuvent aussi être autorisées à effectuer une activité malveillante, du détournement de la mémoire jusqu'à l'utilisation des droits d'accès d'un autre programme dans le but néfaste d'apporter des modifications illégales à la configuration de Windows.

Bien entendu, ce type d'interaction est totalement inacceptable et doit être contrôlé. Le meilleur moyen d'y parvenir est d'utiliser des outils spécialisés conçus spécifiquement pour contrôler ce type d'activité et bloquer les opérations illégales avant qu'elles ne soient tentées.

Cas pratiques

Un utilisateur habituel de Windows est exposé à plusieurs risques chaque jour. Les principaux vecteurs d'attaque sont les suivants :

1) *Téléchargement accessoire de logiciels malveillants après avoir visité un site Web altéré ou malveillant qui héberge un dispositif d'exploitation incorporé ou qui exécute un script hostile.*

Ceci peut se produire, par exemple, lorsqu'une personne surfe sur Internet à la recherche de contenus populaires comme des économiseurs d'écran, des téléchargements musicaux ou des jeux en Java et visite accidentellement un site Web empoisonné qui injecte discrètement un code malhonnête dans le navigateur. Ce dernier est alors altéré et risque de transmettre l'infection à l'ordinateur. Une victime innocente peut également être attirée vers des sites peu scrupuleux par le biais de pourriels ou d'un hameçonnage.

2) *Exécution de programmes obtenus par les réseaux d'échange P2P.*

Il est important de se souvenir que les fichiers obtenus à partir de sources non fiables ne sont pas toujours ce qu'ils semblent être. Le fichier « Britney.mpg » n'est pas nécessairement un clip vidéo de Britney Spears, mais peut facilement cacher un cheval de Troie. Si ce logiciel malveillant est relativement nouveau, les logiciels anti programmes malveillants traditionnels risquent de ne pas l'intercepter avant qu'il ne s'exécute.

3) *Ouverture de pièces jointes infectées ou téléchargement à partir de liens envoyés par messagerie instantanée.*

La propagation des virus par messagerie électronique reste l'un des vecteurs d'attaque les plus communs. Vous devez faire très attention lorsque vous ouvrez des pièces jointes à des courriels. Les fichiers portant l'extension .exe ou toute extension ne correspondant pas à un type de données doivent systématiquement être considérés comme suspects à moins que vous n'attendiez un fichier d'une connaissance dont vous pouvez vérifier la légitimité par téléphone ou autre moyen autre qu'informatique.

4) *Exécution ou installation d'un fichier ou programme apparemment inoffensif qui contiennent une charge malveillante.*

³ En supposant qu'un utilisateur se serve des droits d'Administrateur sous Windows XP. Pour les utilisateurs de Windows Vista, le contrôle de compte utilisateur (UAC) est mis en œuvre afin de limiter un ensemble d'actions autorisées sans intensifier les droits d'un programme.

N'importe quel composant d'une application téléchargée peut avoir un contenu viral. Les logiciels (freeware) sont bien connus pour contenir des logiciels-espions. Ne téléchargez **jamais** rien d'un site de logiciels illégaux (warez).

La différence proactive

Alors, comment une protection proactive aide-t-elle à empêcher l'infection ?

Étant donné que la majorité des opérations entre les applications ont lieu sous la surveillance d'outils qui contrôlent l'activité des programmes, vous pouvez choisir quel type d'activité doit être autorisé et lequel doit être bloqué. Vous pouvez alors empêcher toute activité non autorisée à l'avance en la contrôlant de façon proactive et en empêchant les logiciels malveillants de s'activer, de communiquer ou de se propager au-delà de l'ordinateur protégé. Les produits de détection de logiciels malveillants réactifs basés sur les signatures ne se valent pas tous pour accomplir cette tâche. Tout ce qu'ils peuvent faire, c'est désinfecter ou supprimer des objets déjà infectés.

La solution d'Outpost

Outpost Security Suite Pro contient un module appelé Protection de l'hôte qui vous permet de contrôler l'activité des programmes et de limiter la portée des actions qu'un programme peut réaliser. Grâce au module Protection de l'hôte, vous pouvez affecter des stratégies personnalisées aux programmes installés, notamment en désignant les programmes autorisés à interagir avec d'autres logiciels ainsi qu'à modifier les paramètres système. Ceci permet d'éviter toute activité non autorisée pour n'importe quel programme installé sur l'ordinateur. L'analyse anti logiciels malveillants devient alors un mécanisme de défense secondaire au lieu du mécanisme principal.

Vous pouvez choisir vous-mêmes les types d'activité que le module doit surveiller et contrôler, et compiler votre propre liste d'applications dignes de confiance.

Pour voir ce module en action et véritablement visualiser la façon dont il peut contrer les menaces de sécurité par la simple surveillance et l'alerte en cas de comportement suspect, regardez cette [vidéo](#) sur la protection proactive.

Conclusion

La protection proactive est un élément clé de la stratégie de défense de n'importe quel ordinateur de bureau. En surveillant les comportements non autorisés, elle peut réduire radicalement la sensibilité vis-à-vis des menaces sans dépendre entièrement du caractère actuel ou précis des bases de données de signatures.