PROTÉGEZ-VOUS DES ANTIVIRUS

Les antivirus (AV) ne sont pas la bonne solution pour éviter les failles de sécurité sur les terminaux ; ils sont le problème. Aujourd'hui, les AV ne sont plus efficaces pour protéger contre les menaces informatiques. Même s'ils satisfont à de nombreuses exigences en termes de réglementation, de gouvernance et de conformité, ils font peser des frais indirects sur les organisations sans fournir de réelle valeur du point de vue de la sécurité. Parfait exemple, malgré le fait que des solutions AV traditionnelles « protègent » presque tous les terminaux et serveurs du monde, les failles de sécurité sont quand-même en augmentation. Les organisations qui décident de remplacer leurs antivirus traditionnels par des technologies plus avancées devraient choisir un produit qui apporte une plus grande valeur de ganranté, pas seulement en termes de coûts financiers mais également en termes d'efficacité du point de vue de la sécurité.

Ce document souligne trois raisons principales pour lesquelles les AV traditionnels ne fournissent plus aux organisations. Au-delà des coûts concrets d'effectifs, opérationnels, de licences et de soutien, le document souligne certains des frais cachés associés à l'exécution d'un système d'antivirus qui peuvent être intangibles, difficiles à quantifier ou incontestables en raison de l'antériorité.

Le document souligne cinq exigences de sécurité que chaque technologie ou produit AV de remplacement doit remplir afin d'éviter des failles de sécurité sur le terminal. Ce document se termine avec une discussion sur la façon dont la protection de terminal avancée de Palo Alto Networks ® Traps™ permet aux organisations de remplacer leur ancien antivirus par des méthodes de prévention des logiciels et programmes malveillants les plus efficaces et spécifiques pour protéger leurs terminaux de menaces connues et inconnues.

Table des matières

Les Antivirus ne fournissent plus de garanties de sécurité suffisantes

Beaucoup affirment que les AV traditionnels existent depuis 1987. [1] Depuis, le déchiffrage des fichiers basé sur la reconnaissance de la signature est la pierre angulaire pour détecter les contenus malveillants. Cependant, l'efficacité de cette technologie diminue avec le temps tandis que les systèmes d'exploitation, les réseaux et les applications deviennent de plus en plus complexes et sophistiqués. Aujourd'hui, les AV traditionnels ne fournissent plus de garanties de sécurité suffisantes aux organisations qui les utilisent encore. D'ailleurs, les professionnels de la sécurité ont maintenant accès à des technologies et des produits supérieurs qui non seulement éliminent le besoin d'AV traditionnels mais les dépassent grandement en termes de valeur de garantie réelle.

Le facteur le plus critique dans la définition de la valeur de garantie d'une technologie ou d'un produit est son *efficacité*. A son tour, l'efficacité de la sûreté est au minimum mesurée par l'aptitude de la technologie à fournir trois capacités clés :

1. **La performance de la fonction prévue :** Livre-t-elle la fonction de sécurité prévue et attendue ?
2. **La persistance intrinsèque :** Empêche-t-elle les assaillants et les utilisateurs de contourner ses fonctions sécurisées ?
3. **La flexibilité** : Évolue-t-elle pour accueillir et protéger de nouvelles applications**, de nouveaux systèmes et de nouvelles plate-formes ?**

Le cryptage renforcé est un exemple de technologie de sécurité qui offre toujours une valeur de garantie importante car cela reste un moyen efficace d'assurer la sécurité. Le cryptage sert à éviter la perte de confidentialité en « encodant les messages et informations de sorte que seules les parties autorisées peuvent les lire ».[2] C'est une fonction pour laquelle le cryptage est toujours performante. De par sa nature, le cryptage renforcé livre également une persistance intrinsèque : Il empêche les assaillants et les utilisateurs de contourner ses fonctions sécurisées. Enfin, le cryptage renforcé reste flexible : il continue à évoluer pour servir de nouvelles applications avec des ajustements tels que de nouveaux algorithmes, une plus grande puissance de calcul et des mises en œuvre basées sur le matériel.

D'autre part, l'antivirus est un exemple de technologie de sûreté qui fournit plus de garanties de sécurité suffisantes car il n'est plus efficace dans la garantie de la sécurité.

Performance de la fonction prévue

Généralement parlant, la fonction primaire prévue d'un AV traditionnel est d'empêcher des assaillants de mettre des terminaux et des serveurs en danger. À la fin des années 1980 et pendant les années 1990, les antivirus à détection de signature étaient capables d'assurer cette fonction correctement, étant donné la nature, la complexité et la fréquence des attaques dans ce domaine.
Cependant, dans le contexte informatique actuel, les AV ne peuvent plus accomplir cette fonction avec un succès garanti ; les vendeurs d'AV ont ouvertement admis ce fait.[3]

Les assaillants comptent principalement sur deux vecteurs d'attaque pour compromettre les terminaux : des exécutables malveillants (malware) et la vulnérabilité des programmes. Ces vecteurs d'attaque sont utilisés individuellement ou dans diverses combinaisons mais ils sont de nature fondamentalement différente :

- **Les programmes malveillants** sont un executable souvent indépendant visant à effectuer des activités malfaisantes sur un système.
- **Les exploits** sont des fichiers ou du contenu visant à exploiter les défauts des logiciels ou les bugs dans les applications légitimes ce qui permet à l'assaillant d'exécuter les codes à distance. Une exploitation réussie permet à l'assaillant d'opérer le programme malveillant sur le terminal visé à distance.

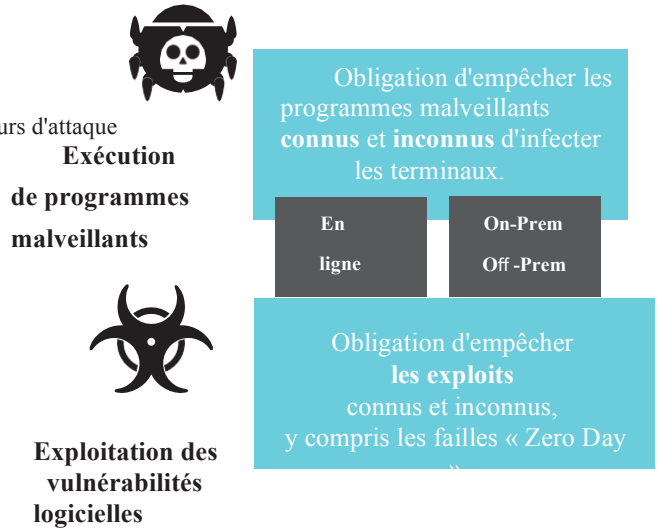

Figure 1 : Une sécurité des terminaux efficace doit empêcher à la fois les programmes et logiciels malveillants

Afin d'empêcher les assaillants de mettre les terminaux et les serveurs en danger, une technologie ou un produit de sécurité doit empêcher à la fois les programmes malveillants et les exploits (Figure 1). De plus, il faut empêcher à la fois les variations connues et inconnues de chaque programme malveillant et faille. Le déchiffrage de la signature et la technologie AV traditionnelle ne sont malheureusement pas aptes à détecter la vulnérabilité des programmes et ne peuvent pas détecter ou bloquer les logiciels malveillants ou les failles pour lesquels il n'y a pas de signature

La persistance intrinsèque :

Les AV traditionnels manquent de persistance intrinsèque depuis le début. Les utilisateurs ont toujours redouté l'interférence et les ralentissements de système causés par l'analyse des systèmes AV. Admettant l'impact que ces interruptions ont sur les utilisateurs et les systèmes d'entreprise, les vendeurs d'AV ont proposé aux utilisateurs la possibilité de passer les contrôles antivirus lorsqu'ils dérangent des priorités commerciales concurrentes. Par conséquent, les utilisateurs ont l'habitude de passer les contrôles programmés ou de désactiver des composants AV dès que possible.

Plus récemment, des assaillants ont eu accès au codage mutualisé et à des outils de déchiffrage multiple qui automatisent et garantissent la capacité de l'attaque à contourner la majorité des produits antivirus traditionnels sur le marché. Nombre de ces outils proposent une intégration avec plusieurs kits d'exploitation qui déterminent automatiquement le moment où une attaque particulière ne peut plus contourner les antivirus traditionnels et choisit de façon automatique une autre attaque qui y parvient.

La flexibilité

Les antivirus à détection de signature ont du mal à s'adapter aux nouvelles applications, aux nouveaux systèmes et aux nouvelles plate-formes qui n'accueillent pas ou qui ne sont pas faits pour le déploiement d'une base de données de signatures ou pour la détection des signatures. Les ordinateurs de bureau et les serveurs utilisés dans une infrastructure de bureau virtuel (VDI) sont de parfaits exemples de ce genre d'environnement. Une fois qu'un système virtuel est instancié, il doit télécharger les dernières signatures antivirus avant que son AV ne puisse réaliser la fonction de sécurité prévue, ce qui rend le système vulnérable aux attaques pendant ce temps.

D'ailleurs, ce manque de flexibilité a porté préjudice à l'efficacité des AV traditionnels pendant de nombreuses années. Tandis que le but initial des AV traditionnels était d'empêcher les virus informatiques d'infecter un système, leur manque de flexibilité et leur incapacité à s'adapter à un paysage de menaces changeant ont pratiquement relégué les AV à détection de signature au role d'outil de sécurité réactif dont l'heure est venue il y a longtemps.

L'antivirus n'est pas seulement une technologie de garantie qui n'offre plus de garanties de sécurité suffisantes, il encombre également les organisations de frais indirects qui ne sont que rarement reconnus.

Les coûts cachés des antivirus

Les technologies et produits de garantie n'évoluent pas dans le vide. Ils font partie d'un écosystème d'outils visant à soutenir les objectifs d'une organisation. L'équilibre entre un plus grand besoin de sécurité tout en permettant aux utilisateurs de faire des affaires fait actuellement l'objet de débats. De même, les technologies de sûreté doivent trouver l'équilibre entre les bénéfices qu'elles offrent à une organisation et les coûts associés à leur fonctionnement. Les coûts associés au fonctionnement d'un système antivirus vont au-delà des coûts concrets d'effectifs, opérationnels, de licences et de soutien, dans des domaines qui sont parfois intangibles, difficiles à quantifier ou incontestables en raison de l'antériorité.

Souplesse opérationnelle

Comme expliqué plus tôt, les antivirus traditionnels dépendent fortement d'une technologie de détection des signatures plus ancienne qui n'est pas très flexible dans le soutien de nouvelles applications, de nouveaux systèmes ou de nouvelles plate-formes. Les organisations qui s'appuient toujours sur des antivirus se trouveront forcément face à des obstacles dans le déploiement et la sécurisation de nouvelles technologies qui peuvent offrir des avantages commerciaux importants (par ex. la VDI).

Les coûts des possibilités

Le soutien, le fonctionnement et l'entretien de systèmes antivirus demandent aux organisations de dédier du personnel, du temps et des ressources qui pourraient être utilisés pour soutenir d'autres projets avec de meilleurs retours sur investissement. Souvent, le personnel de sécurité informatique est censé à la fois assister des systèmes antivirus vieillissants et réparer la capacité sécuritaire de différentes solutions qui peuvent être plus longues à intégrer et sont moins efficaces en termes de sécurité.

Risques importants malgré la conformité

La plupart des professionnels de sécurité informatique s'accorde pour dire que conformité réglementaire n'est pas synonyme de sécurité. Malgré de nombreux cadres réglementaires et de conformité, par exemple les « Payment Card Industry Data Security Standards » (les normes de sécurité des données pour les industries de carte de paiement, PCI-DSS) ou le Health Insurance Portability and Accountability Act (HIPAA, une loi américaine concernant la santé et l'assurance maladie), exigeant que les organisations utilisent ces différentes fonctions des AV traditionnels, la conformité avec ces exigences ne garantit pas que les risques de sécurité soient suffisamment réduits. Comme expliqué plus tôt, les AV traditionnels ne fournissent plus de garanties de sécurité suffisantes dans le contexte actuel,
ce qui oblige les professionnels de la sécurité à utiliser d'autres technologies et produits pour réduire les risques de sécurité que les AV ne peuvent pas traiter, ce qui en retour impose des coûts tangibles et intangibles à l'entreprise.

Un sentiment de sécurité faussé

Du point de vue de l'utilisateur final, les départements responsables de l'informatique et de la sécurité sont chargés de la sécurisation des réseaux, des systèmes et de l'environnement informatique, et ceci malgré les programmes de formation aux connaissances de sécurité organisationnelle qui expliquent que la sécurité est de la « responsabilité de tous ». En général, les utilisateurs partent du principe que les professionnels dédiés à ces fonctions sont capables de définir quels outils et technologies doivent utilisés sur les systèmes des utilisateurs pour leur permettre d'effectuer leurs activités quotidiennes en toute sécurité. Lorsqu'une organisation décide de déployer un AV traditionnel, une technologie qui n'offre aucune réelle garantie comme expliqué plus haut, les utilisateurs peuvent faussement croire que leurs systèmes sont protégés des attaques. A cause de ce sentiment de sécurité faussé, les utilisateurs peuvent être moins vigilants et faire moins attention à éviter des menaces informatiques potentielles.

Les entreprises peuvent éviter les frais intangibles, difficilement quantifiables et incontestables d'un antivirus en remplaçant cette technologie vieillissante par des produits qui non seulement éliminent le besoin d'AV traditionnel mais le dépassent de loin en termes de valeur de garantie réelle.

Les 5 éxigences de sécurité de tout remplacement d'AV

Les organisations qui décident de remplacer leur antivirus traditionnel par des technologies plus avancées devraient choisir un produit qui apportent une plus grande valeur de sécurité, pas seulement en termes de coûts financiers mais également en termes d'efficacité du point de vue de la sécurité, comme expliqué plus haut. Précisément, un produit de protection avancée des terminaux devrait fournir les cinq capacités suivantes.

1. **La prévention d'abord**

   La fréquence, la variété et la complexité des violations de sécurité étant en augmentation, le secteur de la sécurité tout entier a du mal (et souvent échoue) à empêcher les failles de réussir. Le fait qu'en tant que collectif, le secteur se concentre sur l'amélioration de la détection et des temps de réponse est en partie responsable de cet échec. L'amélioration de la détection
   ne fait que réduire le laps de temps durant lequel une attaque peut être détectée et ne fait pas grand chose pour protéger des informations précieuses avant qu'elles ne soient mises en danger. L'augmentation récente des attaques rançongicielles (« ransomware ») réussies rend ce défaut douloureusement évident.

   La détection des failles et la réaction aux incidents offrent une garantie de sécurité mais doivent rester des priorités secondaires par rapport à la prévention. Se concentrer sur la prévention est le seul moyen efficace, évolutif et durable de réduire la fréquence et l'impact des failles de sécurité.

2. **Prévention des logiciels malveillants connus et inconnus**

   Une solution complète empêchant les failles de sécurité sur le terminal doit également empêcher l'exécution réussie de programmes malveillants connus et inconnus. Afin d'éviter les faiblesses associées aux antivirus à détection de signature, les capacités de prévention des logiciels malveillants du produit idéal ne devraient pas impliquer de signature ou nécessiter de connaissances préalables de cas de malveillance pour éviter son exécution. De plus, une prévention effective des logiciels malveillants à la fois ordinaires et avancés [4] nécessite le déploiement de nombreuses méthodes d'analyse et de prévention qui peuvent être réglées pour une efficacité maximale.

3. **Prévention des failles « zero day » connues et inconnues**

   Les auteurs des menaces qui utilisent les moyens les plus efficaces pour contourner les mesures de sécurité existantes sur les terminaux se servent de failles dans les programmes, surtout ceux qui exploitent des vulnérabilités inconnues des logiciels (que l'on appelle les failles « zero day »). Incrustées dans des fichiers et contenus spécialement élaborés, comme les documents Adobe® PDF and Microsoft® Word, les failles « zero day » empêchent les applications légitimes de réaliser des activités
   malfaisantes. Leur capacité à se soustraire aux solutions AV traditionnelles et l'absence de correctifs de sécurité des vendeurs laissent souvent les entreprises avec peu de mesures préventives contre les failles « zero day », qui représentent généralement la première étape d'une attaque ciblée. Ainsi, une solution complète pour éviter les failles de sécurité sur le terminal doit empêcher les programmes connus et inconnus de saboter les applications légitimes.

4. **Intégration automatique de renseignements sur les menaces**

   Avec la prolifération d'outils gratuits ou à bas coût, les auteurs de menaces peuvent rapidement créer des attaques uniques et nouvelles qui échappent à la détection des signatures par les antivirus traditionnels. Selon le Rapport d'enquête 2016 sur la violation des données de Verizon, 81,9 % des attaques réussissent à mettre leurs cibles en danger en quelques minutes.
   Il est essentiel que les organisations fassent appel aux renseignements sur les menaces recueillis ailleurs lors de nouvelles attaques uniques pour empêcher les failles de sécurité dans leurs propres environnements. Un remplacement d'AV doit nativement intégrer et tirer profit des renseignements sur les menaces provenant de ressources globales pour détecter automatiquement les programmes malveillants et identifier rapidement les logiciels malveillants inconnus en empêchant les deux d'infecter les systèmes de l'organisation.

5. **Protection ubiquitaire**

   La main d'œuvre structurelle devient plus mobile. Elle est connectée aux ressources internes grâce à des points partout dans le monde qui sont en dehors du périmètre du réseau organisationnel. Elle utilise des logiciels à la demande (Saas) et des solutions de stockage pour traiter et partager des données, même lorsqu'elle n'est pas connectée au réseau structurel. Ces services et solutions peuvent synchroniser et diffuser des fichiers, y compris des logiciels et programmes malveillants, à tous les effectifs d'une organisation. Ainsi, une solution complète pour éviter les failles de sécurité sur le terminal doit empêcher à la fois les logiciels et programmes malveillants de mettre un système en danger, indépendamment de son statut en ligne ou hors ligne, de sa connectivité au réseau structurel ou de son emplacement physique (local ou non).

Considérations supplémentaires

Les fonctions de sécurité d'un produit représentent souvent la considération principale pour les organisations qui cherchent à remplacer leur AV traditionnel. Cependant, il existe d'autres considérations qui ne sont pas liées à la sécurité et qui peuvent avoir un impact considérable sur la capacité du produit à répondre aux besoins de remplacement d'AV d'une organisation.

Efficacité opérationnelle

Comme mentionné ci-dessus, la nature intrusive du déchiffrage des fichiers des AV et le ralentissement que cela cause sur les systèmes des utilisateurs sont une grande source d'agacement pour les utilisateurs et les administrateurs informatiques. Ainsi, un produit de remplacement AV optimal doit être le moins intrusif possible (idéalement invisible pour les utilisateurs) tout en imposant des exigences minimales sur la mémoire, le débit et les ressources des UC.

Soutien pour les systèmes irréparables

Toutes les entreprises ne veulent pas (ou ne peuvent pas) mettre leurs systèmes de production à jour. Elles peuvent choisir de ne pas appliquer les mises à jour système ou les patchs de sécurité disponibles car cela pourrait diminuer, éliminer ou interférer avec des capacités opérationnelles critiques. Autrement, elles pourraient ne pas être capables d'appliquer ces mises à jour si un système ou un logiciel est arrivé en fin de garantie et si les vendeurs respectifs ne fournissent plus de mises à jour de sécurité ou système. Ainsi, un produit de remplacement d'AV complet doit soutenir et protéger ces systèmes et applications logicielles devenues fondamentalement « irréparables ».

Personnalisation pour répondre aux besoins commerciaux

Les besoins commerciaux des entreprises en termes de remplacement d'AV peuvent grandement varier. Dans ce cas, il n'existe pas de modèle uniforme. Une approche basée sur plusieurs méthodes, combinée et flexible de la prévention s'adapte à des besoins commerciaux qui varient probablement d'un bout à l'autre des entreprises et même à l'intérieur des groupes d'utilisateurs au sein d'une même organisation. Un produit de remplacement d'AV idéal doit permettre cette flexibilité pour adapter la sécurité aux exigences commerciales d'une entreprise.

Traps remplace l'antivirus

Même si les solutions AV traditionnelles « protègent » presque tous les terminaux et serveurs dans le monde, les failles de sécurité restent en augmentation. Afin d'éviter les failles de sécurité sur leurs terminaux, les organisations doivent se protéger à la fois contre les menaces informatiques connues et inconnues et contre les solutions antivirus inefficaces déployées dans leurs environnements.

La protection de terminal avancée Palo Alto Networks Traps remplace les anciens antivirus grâce à une prévention multi-méthode qui utilise un mélange unique des méthodes de prévention des failles et programmes malveillants les plus efficaces et spécifiques afin d'empêcher les menaces connues et inconnues avant qu'elle ne mettent un terminal en danger.

Prévention des programmes malveillants multi-méthode

Traps bloque les exécutables malveillants grâce à une approche unique qui maximise la couverture contre les programmes malveillants tout en réduisant la surface d'attaque et en augmentant la précision de leur détection. Cette approche allie plusieurs couches de protection qui empêchent instantanément les programmes malveillants connus et inconnus d'infecter un système (Figure 2) :

1. **Analyse statique grâce à l'apprentissage automatique** Cette méthode donne un verdict instantané pour chaque dossier exécutable inconnu avant d'autoriser l'exécution. En examinant les centaines de caractéristiques des fichiers en une fraction de seconde, cette méthode détermine s'ils risquent d'être malveillants ou bénins sans dépendance ou signature, déchiffrage ou analyse comportementale.
2. **Inspection et analyse WildFire :** Cette méthode tire profit de la puissance de l'analyse collaborative de l'environnement malveillant de Palo Alto Networks WildFire™ pour détecter rapidement les programmes malveillants et reprogrammer automatiquement Traps pour empêcher les logiciels malveillants connus. WildFire élimine la menace de l'inconnu en la transformant en connu en environ 300 secondes.

Figure 2 : Prévention des programmes malveillants multi-méthode Traps

3. **Limites d'exécution de l'éditeur fiable :** Cette méthode permet aux organisations d'identifier les fichiers exécutables compris dans les « bons inconnus » car ils sont publiés et signés numériquement par des éditeurs fiables, des entités que Palo Alto Networks reconnaît comme des éditeurs de logiciel responsables.
4. **Limites d'exécution à la politique :** Les organisations peuvent facilement définir des politiques pour limiter les scénarios d'exécution spécifique, ce qui réduit la surface d'attaque de chaque environnement. Par exemple, Traps peut empêcher l'exécution de fichiers provenant du répertoire « temporaire » d'Outlook ou d'un fichier spécial provenant directement d'une clé USB.
5. **Politiques de dérogation pour les administrateurs :** Cette méthode permet aux organisations de définir des politiques basées sur le hachage d'un fichier exécutable, pour contrôler ce qui est autorisé à fonctionner dans tous les environnements et ce qui ne l'est pas. Cette capacité de liste blanche (ou noire) détaillée contrôle l'exécution de chaque fichier en se basant sur des conditions définies par l'utilisateur.

En plus des méthodes de prévention des programmes malveillants ci-dessus, Traps place en quarantaine les exécutables malveillants pour empêcher la transmission des fichiers infectés à d'autres utilisateurs. Même si elle est essentielle dans la plupart des environnements, cette capacité est particulièrement utile dans la prévention de la diffusion par mégarde de programmes malveillants dans les organisations où le réseau ou les applications de stockage partagé synchronisent automatiquement les fichiers de plusieurs utilisateurs et systèmes.

Le mélange des capacités et des méthodes susmentionnées permet non seulement à Traps d'empêcher les logiciels malveillants connus et inconnus de mettre un système en danger mais permet également aux organisations de personnaliser totalement cette prévention afin de répondre à leurs différents besoins commerciaux.

Prévention de failles basée sur plusieurs méthodes

De nombreuses attaques ciblées débutent avec une faille sous forme de fichier de données, sur un site internet, par courrier électronique ou via le réseau. Lorsqu'un utilisateur ouvre le fichier, le code malveillant présent à l'intérieur utilise une vulnérabilité dans l'application utilisée pour visionner le fichier pour saboter l'application et mettre en œuvre les instructions de l'assaillant. Ce type d'attaque étant difficile à distinguer du comportement normal de l'application, il contourne les antivirus traditionnels et les solutions de sécurité des terminaux. De plus, si l'application en cours d'exploitation est autorisée par la politique de sécurité informatique, l'attaque contournera également les contrôles de listes blanches.

Traps utilise une approche totalement nouvelle et unique pour éviter les failles. Au lieu de se concentrer sur les millions d'attaques individuelles ou leurs vulnérabilités logicielles sous-jacentes, Traps se concentre sur les techniques d'exploitation de fond utilisées par toutes les attaques à base de failles. Même s'il existe plusieurs milliers de programmes, ils sont tous basés sur une petite collection de techniques d'exploitation clés qui changent régulièrement. De plus, chaque exploitation doit utiliser toute une série de ces techniques d'exploitation pour réussir à saboter une application. Traps neutralise ces techniques en les identifiant et en les bloquant de façon préventive au moment où elles sont tentées. Les organisations qui utilisent Traps peuvent utiliser n'importe quelle application, y compris celles développées en interne et celles qui ne bénéficient plus de soutien de sécurité, sans menace imminente à leur environnement.

Traps met en œuvre une approche basée sur plusieurs méthodes pour la prévention des exploitations, en mélangeant plusieurs couches de protection pour bloquer les techniques d'exploitation (Figure 3) :

1. **Corruption de la mémoire / prévention de la manipulation :** La corruption de mémoire est une catégorie de techniques d'exploitation ; le programme manipule les mécanismes de gestion de mémoire normaux du système d'exploitation pour l'application qui ouvre le fichier contaminé contenant l'exploitation. La méthode de prévention de la corruption de mémoire reconnaît et arrête ces techniques d'exploitation avant qu'elles ne réussissent à saboter l'application.
2. **Prévention des défauts logiques :** Les défauts logiques sont une catégorie de techniques d'exploitation permettant au programme de manipuler les processus normaux du système d'exploitation utilisés pour soutenir et exécuter l'application ciblée qui ouvre le fichier infecté. Par exemple, le programme peut modifier l'emplacement à partir duquel les bibliothèques de liens dynamiques (DLL) sont chargées sur l'environnement d'exécution d'une application pour que les DLL malveillantes du programme puissent remplacer celles qui sont légitimes. La méthode de prévention des défauts logique reconnaît ces techniques d'exploitation et les arrête avant qu'elles ne réussissent.

Prévention de la corruption de la mémoire

Défauts logiques Prévention

Prévention de l'exécution de programmes malveillants

Figure 3 : Prévention d'exploitation multi-méthode

3. **Prévention de l'exécution de programmes malveillants :** Dans la plupart des cas, l'objectif final d'un programme est d'exécuter un code arbitraire (les commandes incluses dans le fichier d'exploitation). La méthode de prévention de l'exécution de programmes malveillants reconnaît les techniques d'exploitation qui permettent l'exécution du code malveillant et les bloque avant qu'elles ne réussissent.

Les méthodes susmentionnées permettent à Traps d'empêcher de façon efficace, continue et transparente à la fois les failles connues et « zero-day » de mettre un système en danger. Cette prévention protège les applications et les systèmes, qu'ils reçoivent des patches de sécurité ou non et quels que soient la connectivité du réseau ou l'emplacement physique.

Plate-forme de sécurité dernière génération

Traps est le seul produit de protection des terminaux à automatiquement convertir les renseignements sur les menaces recueillis dans la communauté globale d'environ 10 000 abonnés WildFire et de multiples sources de renseignements sur les menaces en prévention des logiciels malveillants. Lorsque WildFire identifie un fichier exécutable comme malveillant, d'où que les renseignements proviennent, Traps se reprogramme automatiquement pour empêcher l'exécution de ce fichier à partir de ce moment. La reprogrammation et la conversion automatique des renseignements sur les menaces en prévention élimine presque totalement la possibilité pour les assaillants d'utiliser un logiciel malveillant inconnu et avancé pour infecter un système. Un assaillant peut utiliser chaque logiciel malveillant une fois, partout dans le monde, et n'a que quelques secondes pour mener une attaque avant que WildFire ne le rende totalement inefficace.

L'intégration de Traps à la plate-forme de sécurité dernière génération permet aux organisations de continuer à appliquer les renseignements sur les menaces recueillis auprès de milliers de clients en entreprise, qui sont toujours plus nombreux, à la fois sur le réseau et les terminaux, dans leur propre environnement.

Conclusion

Les AV traditionnels ne fournissent plus de garanties de sécurité suffisantes ; ils ne représentent plus un moyen efficace pour empêcher les failles de sécurité. Les organisations ont maintenant accès à une technologie supérieure qui ne se contente pas d'éliminer le besoin d'AV traditionnels mais les surpasse en termes de valeur de garantie réelle, tout en évitant les coûts impondérables, difficilement quantifiables et incontestables d'un antivirus. La protection de terminal avancée Palo Alto Networks Traps remplace les antivirus traditionnels par une prévention basée sur plusieurs méthodes qui déploie un mélange unique des méthodes de prévention les plus efficaces et spécifiques afin d'empêcher les menaces connues et inconnues avant qu'elle ne mettent un terminal en danger.

Pour en savoir plus sur Traps, vous pouvez télécharger **la fiche technique de Traps** ou la **Présentation technique de Traps**. Sinon, vous pouvez voir Traps en action en participant à un **grand test** ou en contactant vos agents commerciaux pour programmer une évaluation en interne pour votre organisation.

[1] https://fr.wikipedia.org/wiki/Logiciel_antivirus

[2] https://fr.wikipedia.org/wiki/Chiffrement

[3] http://www.wsj.com/articles/SB10001424052702303417104579542140235850578

[4] Les logiciels malveillants avancés comprennent ceux qui déploient des mécanismes d'infection multiples ou ciblés, des déclencheurs et des charges et utilisent des stratégies furtives telles que le chiffrage automatique et le polymorphisme.

4401 Great America Parkway
Santa Clara, CA 95054

Tél : +1.408.753.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com