PRÉVENTION DES MENACES

Protection complète de votre réseau contre les attaques, les logiciels malveillants et les vulnérabilités des commandes

Les entreprises font face à de fréquentes attaques perpétrées par des acteurs malveillants du monde entier dans le but de réaliser des profits. De nos jouers, les attaquants disposent de moyens et d'équipements. Ils utilisent des tactiques évasives afin de pénétrer votre réseau et lancer des attaques massives sophistiquées tout en restant invisibles pour les défenses réseau traditionnelles, par exemple par l'obscurcissement des paquets, les logiciels malveillants polymorphes, le chiffrement, les charges à phases multiples et le DNS à flux rapide.

Intégré à la plateforme de sécurité nouvelle génération de Palo Alto Networks®, le service Threat Prevention protège les réseaux lors des différentes phases de l'attaque :

- Analyse de la totalité du trafic dans l'ensemble du contexte des applications et des utilisateurs.
- Anticipe les menaces à tous les stades du cycle de vie des cyberattaques.
- L'architecture d'analyse à une seule passe permet de maintenir un débit élevé sans pour autant sacrifier la sécurité.
- Mises à jour automatiques et quotidiennes correspondant aux nouvelles menaces identifiées, disponibles 300 secondes après leur apparition pour les failles et logiciels malveillants de type « zero-day » via le service cloud d'analyse des menaces WildFire™.
- Des signatures de commande et contrôle automatisées générées à l'échelle et à la vitesse de la machine.

Pire encore, les produits de sécurité réseau appliquent encore les mêmes stratégies de défense que celles utilisées avant l'évolution du paysage des menaces. L'inspection du trafic ne s'opère que sur certains ports et, tandis que l'ajout de périphériques à fonction unique à la barrière défensive est censé réduire un problème particulier, cela donne lieu à une faible visibilité et à de piètres performances. La situation reste dangereuse, avec des trous béants dans les défenses réseau, car les solutions de sécurité sont fracturées et difficiles à gérer. Pendant ce temps, les pirates informatiques savent de mieux en mieux s'y infiltrer.

Activation de l'application, prévention des menaces

Les applications font partie intégrante de la manière dont les entreprises travaillent. Pour cette raison, elles sont rendues de plus en plus disponibles auprès des utilisateurs en pénétrant sur les réseaux à l'aide de canaux chiffrés, via des ports non standards, et en sautant d'un port ouvert à un autre pour garantir l'accès permanent des utilisateurs.

Malheureusement, les menaces avancées prennent le pas sur la manière dont les applications sont mises à la disposition des utilisateurs. Cela leur permet d'évoluer librement dans le réseau, sans être détectées. Elles forment des tunnels au sein des applications, se dissimulent dans le trafic chiffré SSL et profitent de cibles peu méfiantes pour pénétrer le réseau et exécuter leur activité malveillante.

Palo Alto Networks assure la protection de votre réseau en proposant plusieurs couches de prévention, en confrontant les menaces à chaque phase de l'attaque. En plus de ces fonctionnalités traditionnelles, Palo Alto Networks présente la capacité unique de détecter et de bloquer les menaces sur l'un ou la totalité des ports, au lieu d'invoquer des signatures basées sur un ensemble limité de ports prédéfinis. En tirant parti de la technologie d'identification User-ID™ et de la technologie d'identification des applications App-ID™ de notre pare-feu nouvelle génération, qui identifie l'ensemble du trafic sur tous les ports et lui affecte un contexte, le moteur de prévention des menaces ne perd jamais de vue la menace, quelle que soit la technique utilisée.

Notre abonnement à Threat Prevention comprend la prévention des intrusions, les systèmes anti-logiciels malveillants et les protections Commande et contrôle (CnC).

Éliminer les menaces à tous les stades

Dans pratiquement chaque violation récente, l'organisation ciblée disposait d'un outil de défense à fonction unique qui a été contourné.

- L'analyse heuristique détecte les motifs de trafic et les paquets anormaux, comme les analyses de ports, les balayages d'hôtes et les attaques d'envahissement DoS.
- D'autres fonctionnalités de protection contre les attaques, comme le blocage de paquets non valides ou mal formés, la défragmentation IP et le réassemblage TCP, assurent la protection contre les procédés d'évasion et d'obscurcissement utilisés par les pirates.
- Les signatures de vulnérabilité personnalisées faciles à configurer vous permettent d'adapter les fonctionnalités de prévention contre les intrusions aux besoins propres à votre réseau.

Palo Alto Networks emploie des technologies de défense intégrées en mode natif pour garantir que, lorsqu'une menace échappe à une technologie, une autre puisse la neutraliser. Pour une protection efficace, il est indispensable d'utiliser des fonctions de sécurité dédiées au partage des informations et à la fourniture de contexte quant au trafic qu'elles inspectent et aux menaces qu'elles identifient et bloquent.

Système de prévention des intrusions

Les protections agissant sur les menaces détectent et bloquent les tentatives d'attaque et les techniques de contournement, à la fois au niveau des couches réseau et application. Elles ciblent les analyses de port, les dépassements de capacité de la mémoire tampon, l'exécution de code à distance, la fragmentation de protocole et l'obscurcissement. Les protections sont basées sur la correspondance de signature et la détection d'anomalies. Elles décodent et analysent les protocoles et utilisent les informations obtenues pour lancer l'alerte et bloquer les modèles de trafic malveillants. La mise en correspondance de motifs d'états détecte les attaques visant plusieurs paquets, en tenant compte de l'ordre d'arrivée et de la séquence. Elle veille à ce que l'ensemble du trafic autorisé soit bien intentionné et qu'il n'utilise pas de techniques de contournement.

- L'analyse de protocole basée sur un décodeur décode les états du protocole, ainsi que les signatures, appliquées de façon intelligente, pour détecter les failles de sécurité au niveau du réseau et de l'application.
- Dans la mesure où il existe de nombreuses manières d'exploiter une seule vulnérabilité, nos signatures de prévention contre l'intrusion sont dédiées à la vulnérabilité, assurant une protection plus approfondie contre une grande variété d'attaques. Une seule signature peut bloquer plusieurs tentatives d'attaque sur une vulnérabilité de système ou d'application connue.
- La protection de protocole basée sur les anomalies détecte les utilisations du protocole non conformes à RFC, ainsi que la connexion FTP trop longue ou d'URI trop longues.
- Les signatures de vulnérabilité personnalisées faciles à configurer vous permettent d'adapter les fonctionnalités de prévention contre les intrusions aux besoins propres à votre réseau.

Protection contre les logiciels malveillants

La protection en ligne bloque les logiciels malveillants avant qu'ils n'atteignent l'hôte cible, par le biais de signatures basées sur la charge et non sur le hachage. Les protections contre les logiciels malveillants Palo Alto Networks bloquent les logiciels malveillants connus et leurs éventuelles variantes, y compris celles encore jamais observées. Le moteur d'analyse de flux protège le réseau sans ajouter de latence, ce qui est un sérieux inconvénient des antivirus réseau qui reposent sur des moteurs d'analyse de proxy. L'analyse des logiciels malveillants basée sur le flux inspecte le trafic dès réception des premiers paquets du fichier, ce qui permet d'éliminer les menaces ainsi que les problèmes de performances associés aux solutions autonomes traditionnelles. Les principales fonctionnalités de protection contre les logiciels malveillants comprennent :

- La détection de flux en ligne et la prévention des logiciels malveillants dissimulés dans les fichiers compressés et le contenu Web.
- La protection contre les charges dissimulées dans les types de fichiers communs, tels que les documents Microsoft® Office et PDF.
- Les mises à jour de WildFire, pour la protection contre les logiciels malveillants de type « zero-day ».

Les signatures de toutes sortes de logiciels malveillants sont générées directement à partir de millions d'échantillons collectés par Palo Alto Networks. Il s'agit notamment de logiciels malveillants jusqu'alors inconnus envoyés à WildFire, à notre équipe de recherche de l'unité 42, ainsi qu'à d'autres grandes organisations de recherche dans le monde entier.

Protection Commande et Contrôle (Spyware)

Nous savons qu'il n'existe pas de solution miracle lorsqu'il est question d'empêcher toutes les menaces d'entrer sur le réseau. À la suite d'une première infection, les pirates communiqueront avec la machine hôte via un canal Commande et Contrôle (CnC), qu'ils utiliseront pour introduire d'autres logiciels malveillants, publier d'autres instructions et voler des données. Nos protections CnC ont accès à ces canaux de communication non autorisés et les interrompent en bloquant les demandes sortantes vers des domaines malveillants et à partir de boites à outils CnC connues installées sur des périphériques infectés. Palo Alto Networks va bien au-delà de la simple automatisation des signatures CnC basées sur les URL et les domaines. Nous générons automatiquement des signatures CnC sur la base de modèles, proposant ainsi des signatures CnC destinées à la recherche à la vitesse et à l'échelle de la machine.

Signatures basées sur le contenu et basées sur le hachage

Les signatures basées sur le contenu détectent les éléments récurrents dans le corps du fichier afin d'identifier toute variation future du fichier, même si le contenu a été légèrement modifié. Ceci permet d'identifier immédiatement le code malveillant polymorphe qui pourrait autrement être identifié comme un nouveau fichier totalement inconnu.

Les signatures basées sur le hachage examinent la correspondance du codage fixe de chaque fichier. Étant donné que le hachage d'un fichier est très facile à modifier, les signatures basées sur le hachage ne sont pas efficaces pour la détection des logiciels malveillants polymorphes ou des variantes d'un même fichier.

Analyse de toutes les menaces en un seul passage

Le moteur de Threat Prevention de Palo Alto Networks figure au premier rang du secteur pour l'inspection et la classification du trafic, ainsi que pour la détection et le blocage des logiciels malveillants et la propagation des failles de vulnérabilité en un seul passage. Les technologies traditionnelles de prévention des menaces requièrent deux, voire plus, moteurs d'analyse. Cela ajoute une latence importante et ralentit sensiblement le débit. Palo Alto Networks utilise un format de signature uniforme pour toutes les menaces afin de garantir un traitement rapide en effectuant l'analyse en un seul passage intégré. Fini les processus redondants qu'offrent les solutions qui utilisent plusieurs moteurs d'analyse.

Notre technologie Threat Prevention passe en revue chaque paquet lorsqu'il traverse la plateforme. Chaque séquence d'octets est examinée dans l'en-tête de paquet et dans la charge. À partir de cette analyse, nous serons en mesure d'identifier d'importants détails concernant le paquet, notamment l'application utilisée, sa source et sa destination, si le protocole est conforme à RFC et si la charge contient une attaque ou un logiciel malveillant. Au-delà de chaque paquet, nous analysons également le contexte fourni par l'ordre d'arrivée et la séquence de plusieurs paquets afin de neutraliser les techniques de contournement. Cette analyse et cette correspondance de signature interviennent en un seul passage et, par conséquent, le trafic de votre réseau ne perd pas en rapidité.

Abonnement à Threat Prevention et intégration à WildFire

Les organisations peuvent étendre la protection contre les logiciels malveillants de type « zero-day » et autres failles avec le service Wildfire. WildFire est le moteur d'analyse et de prévention des menaces le plus avancé du secteur. Il cible les logiciels malveillants de type « zero-day » et autres failles similaires. Ce service cloud applique une approche unique, basée sur des techniques multiples combinant une analyse statique et dynamique, des techniques d'apprentissage automatique innovantes et un environnement révolutionnaire d'analyse sur « ordinateur nu » afin de détecter et prévenir les menaces, même les plus difficiles à détecter.

Réduction de la surface d'attaque

Déchiffrement SSL

Près de 40 % du trafic réseau des entreprises est chiffré avec SSL, ce qui laisse un trou béant dans les défenses réseau s'il n'est pas déchiffré et analysé en vue de détecter des menaces. Notre plateforme est dotée du déchiffrement SSL intégré, qui peut être utilisé de manière sélective pour déchiffrer le trafic SSL entrant et sortant. Une fois que le trafic est déchiffré et confirmé comme étant sûr, il est de nouveau chiffré et autorisé à aller vers sa destination.

Blocage des fichiers

Près de 90 % des fichiers malveillants utilisés dans les attaques de harponnage sont des exécutables. Cela, associé au fait que près de 60 % des incidents de sécurité sont le résultat de la négligence des employés, signifie que vos employés risquent de ne pas faire la distinction entre ce qui est sûr et ce qui ne l'est pas. Réduisez le risque d'infection par un logiciel malveillant en empêchant les types de fichiers dangereux, connus pour dissimuler les logiciels malveillants, comme les exécutables, de pénétrer votre réseau. La fonctionnalité de blocage de fichiers peut être combinée à User-ID afin de bloquer les fichiers superflus en fonction du rôle des utilisateurs. Elle veille à ce que tous les utilisateurs aient accès aux fichiers dont ils ont besoin et vous donne un moyen granulaire de réduire votre exposition au risque inhérent aux diverses exigences de votre organisation. Vous pouvez aussi faire baisser le nombre des opportunités d'attaque en envoyant tous les fichiers autorisés à WildFire à des fins d'analyse pour déterminer s'ils contiennent des logiciels malveillants de type « zero-day ».

Protection contre les téléchargements automatiques

Les utilisateurs non méfiants peuvent télécharger par inadvertance des logiciels malveillants, simplement en consultant leur page Web favorite. Souvent, l'utilisateur, voire le propriétaire du site Web, peut ne pas savoir que le site a été compromis. La technologie Palo Alto Networks identifie les téléchargements potentiellement dangereux et envoie un avertissement à l'utilisateur pour veiller à ce que le téléchargement soit intentionnel et approuvé. Empêchez les attaques provenant de domaines nouveaux et à évolution rapide en associant cette fonctionnalité à des stratégies de filtrage des URL et de blocage de fichiers.

Atténuation rapide et précise des risques

DNS Sinkhole

Notre protection CnC va plus loin en fournissant des fonctionnalités entonnoir pour les requêtes sortantes vers des entrées DNS suspectes, ce qui empêche l'exfiltration et permet d'identifier précisément la victime. Configurez l'entonnoir de sorte que toute requête sortante vers un domaine ou une adresse IP suspecte soit plutôt redirigée vers une des adresses IP internes de votre réseau. Cela bloque la communication CnC de manière efficace, en empêchant ces requêtes de quitter le réseau, quelle que soit la fréquence ou l'heure à laquelle elles sont effectuées. Un rapport des hôtes de votre réseau qui émettent ces requêtes est compilé, même si ces hôtes se trouvent derrière le serveur DNS. Les équipes en charge de la réponse aux incidents disposent d'une liste mise à jour quotidiennement des machines suspectes sur lesquelles intervenir. Elles ne sont pas pressées par le temps pour y remédier dans la mesure où les communications avec le pirate ont déjà été coupées.

Objets de corrélation automatisés

Notre technologie de prévention des menaces peut identifier la présence de menaces avancées grâce à la surveillance et à la corrélation du trafic réseau et des journaux des menaces. Vous pouvez ainsi identifier rapidement les utilisateurs infectés et analyser les modèles de comportement étranges. Les objets de corrélation exploitent les résultats des recherches sur les menaces menées par l'unité 42 et l'analyse des menaces inconnues de WildFire et User-ID afin de mettre en lien les anomalies de trafic et les indicateurs de danger afin que les appareils de votre réseau qui ont été infectés puissent être identifiés de façon rapide et précise.

Tirez parti des renseignements mondiaux sur les menaces pour empêcher les attaques

Les journaux détaillés de toutes les menaces ne sont pas simplement hébergés au sein de la même interface de gestion, mais partagés entre tous les mécanismes de prévention pour fournir du contexte. Nous tirons profit des renseignements mondiaux sur les menaces via WildFire afin de découvrir automatiquement les logiciels malveillants inconnus et assurer la protection de tous nos clients, en maintenant la vigilance à l'égard des dernières menaces avancées.

Réseau DNS passif

Modèle	Débit des menaces
PA-200	50 Mbit/s
PA-500	100 Mbit/s
PA-2020	200 Mbit/s
PA-2050	500 Mbit/s
PA-3020	1 Gbit/s
PA-3050	2 Gbit/s
PA-3060	2 Gbit/s
PA-5020	2 Gbit/s
PA-5050	5 Gbit/s
PA-5060	10 Gbit/s
PA-7050	100 Gbit/s*
PA-7080	160 Gbit/s*

*DSRI activé

Protégez votre organisation contre les réseaux de logiciels malveillants à évolution rapide et les sites Web mal intentionnés en profitant de l'analyse DNS de Palo Alto Networks. Bénéficiez d'un vaste réseau de renseignements en activant la surveillance DNS passive, qui enrichit notre base de données de domaines malveillants. Elle est ensuite utilisée dans la génération de protections destinées à notre clientèle mondiale.

Recherche sur les menaces d'après l'unité 42

L'unité 42, l'équipe de recherche sur les menaces Palo Alto Networks, met en œuvre l'intelligence humaine pour identifier les failles de sécurité de type « zero-day » dans les logiciels Microsoft®, Adobe®, Apple®, Android™ et autres écosystèmes. En identifiant ces failles de façon proactive, en développant des protections destinées à nos clients et en partageant ces informations avec l'ensemble des acteurs du secteur de la sécurité, nous éliminons les armes qu'utilisent les attaquants pour menacer les utilisateurs et pénétrer dans les réseaux des entreprises, ceux des administrations et ceux des fournisseurs de services.

unit 42

4401 Great America Parkway
Santa Clara, CA 95054, États-Unis

Accueil téléphonique : +1 408 753 4000
Service commercial : +1 866 320 4788
Assistance : +1 866 898 9087

www.paloaltonetworks.com

threat-prevention-ds-020617