SONICWALL™

SYNTHÈSE TECHNIQUE : DES SANDBOX RÉSEAU POUR BLOQUER LES RANSOMWARES

Voici pourquoi vous devez associer sandboxing, signatures et analyse heuristique

Résumé

Les pare-feux nouvelle génération s'appuient à juste titre sur les signatures et l'analyse heuristique. Mais cela n'est plus suffisant face aux attaques actuelles de programmes malveillants. Avec les défis inhérents aux attaques ciblées et aux menaces de type zero-day, l'ajout de sandbox devient essentiel à l'efficacité des systèmes de sécurité.

Comprendre le véritable défi et les mesures requises

Les menaces externes se développent aujourd'hui de manière stupéfiante. Pour faire continuellement évoluer leurs menaces, les agresseurs combinent la nature opportuniste de l'automatisation et la façon de penser des éditeurs de logiciels, l'objectif étant de se propager le plus vastement possible, en évitant toute détection. Étant donné l'impact négatif subi par toute entreprise victime d'un piratage de ses données ou d'une attaque par ransomware, il est impératif qu'elles puissent détecter les programmes malveillants avant qu'ils n'atteignent leur réseau.

Le véritable défi ne réside pas dans le ransomware qui s'est déjà propagé sur Internet, mais plutôt dans les attaques ciblées et les menaces zero-day. Les attaques ciblées utilisent un code d'un type entièrement nouveau, conçu spécifiquement pour l'entreprise visée, tandis que les menaces zero-day exploitent les nouvelles vulnérabilités pour lesquelles les éditeurs n'ont pas encore créé de correctifs. Les entreprises doivent s'intéresser de très près à ces types d'attaques, car elles sont habituellement bien plus efficaces que leurs anciens équivalents. Quelle est donc la meilleure façon d'empêcher une menace d'apparaître au sein de votre réseau ?

Vous disposez de plusieurs options pour choisir à quel endroit vous souhaitez réagir à ces attaques et comment les détecter et les éliminer. L'objectif est de détecter et d'éliminer les programmes malveillants aussi près que possible de la source de l'attaque. Pour choisir l'endroit auquel elles vont réagir à une attaque, les entreprises suivent généralement deux écoles : celle de la sécurité des terminaux, selon laquelle le programme malveillant parvient jusqu'au terminal, puis est détecté et détruit, et celle des sandbox, selon laquelle le programme malveillant est identifié et détruit avant qu'il ne pénètre sur le réseau. Jusqu'à ce qu'il existe une solution efficace à 100 %, les deux

Aujourd'hui, les programmes malveillants sont si évolués que la détection nécessite une approche multifacette. Signatures et analyse heuristique présentent toutefois chacune leurs limites.

technologies resteront probablement des lignes de défense importantes. Les sandbox peuvent constituer un rempart préventif, à condition d'être déployées de la bonne façon.

Faire barrière aux programmes malveillants

Si vous comparez votre réseau à un château, le meilleur endroit pour contrer une attaque se trouve sur le pont-levis, un point d'étranglement qui permet d'inspecter tous les visiteurs et tous les éléments avant d'autoriser leur entrée. En plaçant une solution capable de détecter les programmes malveillants juste à l'intérieur de votre pare-feu nouvelle génération, c'est comme si vous placiez un garde sur le pont-levis du château. Rien ne peut entrer sans que le garde ne le sache. Lorsque des données arrivent, plusieurs méthodes permettent d'analyser le trafic afin de détecter les éléments malveillants :

- Signatures
  L'analyse du trafic s'effectue via une base de données de signatures numériques de programmes malveillants afin de détecter d'éventuels éléments similaires. Tout élément correspondant est identifié comme étant malveillant.
- Analyse heuristique
  Contrairement aux signatures, qui recherchent des correspondances spécifiques dans une base de données, l'analyse heuristique utilise des règles et des algorithmes pour détecter le code susceptible d'être malveillant.
- Sandbox
  Plutôt que d'essayer de filtrer le code pour trouver les signatures ou les intentions malveillantes, la sandbox permet de déclencher le code, de l'exécuter de la manière prévue, tout en surveillant son comportement et ses actions malveillantes. Ce processus est réalisé dans un environnement spécifiquement conçu, appelé sandbox, qui évite tout incident.

Cette combinaison de tactiques est plus efficace puisque les cibles faciles sont détectables par les technologies classiques, plus rapides et moins gourmandes en ressources. Cela permet à la sandbox de se concentrer sur le contenu restant pour lequel son niveau de contrôle est nécessaire.

Pourquoi signatures et analyse heuristique ne suffisent pas

La détection basée sur les signatures n'est pertinente que si la base de données qu'elle utilise pour identifier les programmes malveillants est performante. Si votre base de données n'est pas mise à jour chaque minute, vous risquez de passer à côté d'une attaque car les éditeurs de logiciels antivirus ont besoin de temps pour identifier les programmes malveillants, actualiser leurs bases de données et vous les distribuer. En outre, les créateurs de programmes malveillants connaissent la détection basée sur les signatures et utilisent un code permettant de l'éviter.

L'analyse heuristique peut aussi être imprécise. Une partie du code peut simplement être du trafic qui ne correspond pas au schéma prévu, ce qui génère des faux positifs. Parfois, les programmes malveillants ne semblent pas nuisibles a priori, jusqu'à ce qu'ils soient réassemblés en back-end, ce qui rend l'analyse heuristique inefficace.

Prenons l'exemple des ransomewares. Le code initialement téléchargé n'est pas nuisible. Il devient dangereux lorsqu'il se connecte à un serveur C2 (commande et contrôle) et télécharge du code supplémentaire. Autre exemple : une macro dans un document Microsoft Word. Si la macro malveillante n'utilise pas de méthode d'attaque suspecte ou connue, aucune signature ni analyse heuristique ne peut dire si la macro elle-même est bonne ou mauvaise.

L'utilisation de signatures ou d'outils heuristiques pour effectuer une analyse passive du trafic présente des limites. L'analyse ne laisse au code aucune chance de devenir actif et les agresseurs savent très bien obscurcir leur mauvais code (du point de vue de l'analyse) à l'intérieur du « bon » code. La façon la plus efficace de détecter un programme malveillant est

donc d'interagir avec une version devenue réellement dangereuse.

Jouer avec le feu

La seule façon de maîtriser des programmes malveillants évolués consiste à les « déclencher ».

Le processus de déclenchement est très différent d'une simple analyse de code. Il est plutôt comparable à la culture d'un microbe dangereux dans un laboratoire spécialisé dans les risques biologiques ou à l'explosion d'une bombe dans une chambre de confinement. La sandbox fournit un endroit sûr pour conserver ouvertes les données interceptées et les laisser exécuter leur parcours sous observation. Si la présence d'un programme suspect ou malveillant est confirmée, le fichier et la menace qu'il contient peuvent tous deux être éliminés.

Les sandbox tentent de déclencher tous les types de fichiers :

- Fichiers de contenu actif
  Ces fichiers incluent des exécutables, des scripts et des DLL. Les fichiers peuvent être exécutés et peuvent interagir avec la sandbox normalement, afin d'y déceler des actions malveillantes telles que la modification des paramètres de pare-feu du système d'exploitation ou l'établissement de connexions sortantes sur Internet.
- Fichiers de contenu passif
  Ces fichiers incluent tous types de documents, PDF, fichiers compressés (par ex. ZIP, JZIP, RAR) et même fichiers images. Ces fichiers sont analysés à l'aide de leur application par défaut pour surveiller l'activité malveillante, telle qu'une macro Word qui tente de télécharger du code supplémentaire via Internet. Si toutes les parties du logiciel ne sont pas disponibles dans la sandbox, il est impossible d'analyser chaque fichier passif. Au final, votre sandbox doit être configurée avec possibilité d'inspecter autant de types de fichiers que possible.

Des programmes malveillants dans des images

Vous vous demandez peut-être pourquoi les fichiers images doivent être minutieusement examinés, puisqu'il s'agit de l'un des types de données en apparence les plus inoffensifs. Ils peuvent en effet contenir des données de charge utile malveillante. Prenons l'exemple d'une attaque récemment menée au Brésil, dans laquelle une pièce jointe au format PDF contenait un lien vers un fichier ZIP. Ce fichier ZIP contenait un exécutable et un fichier PNG (Portable Network Graphics). Le fichier PNG était petit (moins de

Les mesures importantes prises pour obscurcir les programmes malveillants démontrent la nécessité d'une sandbox et des tentatives de déclenchement de tous les fichiers qui pénètrent sur votre réseau.

64 pixels carrés) mais sa taille était supérieure à 1 Mo. Lors de l'inspection de l'exécutable, il est apparu avec évidence que le code était conçu pour extraire et exécuter un binaire malveillant caché, depuis le fichier PNG.

Améliorer les signatures grâce à la sandbox

Comme indiqué précédemment, la meilleure approche pour détecter les programmes malveillants doit être multifacette. L'amélioration avec la méthode d'analyse passive peut accroître l'efficacité du processus de détection, car cela nécessite bien moins de cycles de traitement pour effectuer le contrôle à l'aide d'une base de données de signatures que pour générer et soutenir une sandbox capable de déclencher une seule instance de programme malveillant.

Outre les déclenchements, les sandbox peuvent également être utilisées pour créer des signatures lorsqu'il apparaît que le code est malveillant : elles sont en effet les mieux placées pour son exécution. Lorsqu'un programme malveillant est identifié, une signature est créée et la base de données correspondante peut être mise à jour, ce qui améliore la rapidité et la précision des futures détections de code malveillant.

Les méthodes d'analyse passives présentent toutefois leurs inconvénients en termes de détection. Il est donc pertinent de se demander si une sandbox sera ou non plus efficace.

Fonctionnement d'une sandbox

La sandbox constitue un environnement qui joue un rôle de « bouc émissaire » pour surveiller les programmes malveillants et leur interaction avec le système d'exploitation. Les sandbox recherchent les éléments suivants :

- Appels système : y compris appels système de surveillance et fonctions API.
- Modifications du système de fichiers : tout type d'action, notamment création, modification, suppression et chiffrement de fichiers.
- Modifications du réseau : tout type d'établissement anormal de connexions sortantes.
- Modifications du registre : toute modification destinée à établir une persistance ou apportée aux paramètres de sécurité ou de réseau.
- Mais aussi : surveillance des instructions qu'un programme exécute entre les appels système, afin de compléter le contexte d'autres observations.

Quel est le degré d'efficacité d'une sandbox ?

La détection basée sur les signatures est une méthode parfaite pour repérer les programmes malveillants plus anciens mais elle ne peut rien faire pour bloquer les attaques zero-day ni les attaques ayant simplement muté (par ex. des programmes malveillants spécifiques qui ne répondent pas à une signature en raison de leur mutation). Grâce à l'analyse heuristique, la détection progresse dans la bonne direction, afin de rechercher les schémas anormaux dans le code. Mais comme le montre l'utilisation d'un fichier image pour fournir une charge utile, les fichiers initiaux (par ex. un fichier PDF avec un lien vers un fichier ZIP externe) ne laissent sonner aucune alerte.

Voici pourquoi la sandbox constitue une méthode de détection si efficace. Même avec les attaques zero-day qui n'ont aucune signature et aucun code complètement inconnu, le sandboxing est la seule méthode qui détecte les comportements malveillants. Au final, les programmes malveillants nécessitent un nombre d'actions limité, notamment l'établissement d'une connexion externe, le téléchargement de charges utiles supplémentaires, la connexion à un serveur C2 et les tentatives de modification du système. Aucune de ces actions n'est normalement requise pour des fichiers utilisés à des fins professionnelles.

Conclusion

Il existe plusieurs façons de protéger votre entreprise des programmes malveillants. Il est certes important de protéger les terminaux, mais cela risque d'engendrer un risque encore plus grand en autorisant les programmes malveillants à pénétrer sur le réseau. Les sandbox permettent de bloquer les menaces avant qu'elles n'atteignent le réseau.

En savoir plus. Découvrez les principaux facteurs de différenciation à prendre en compte dans votre stratégie de sandboxing. Lisez nos infos solution *Putting a solid sandbox strategy in place.* (Mettre en place une solide stratégie de sandboxing).

À propos de nous

Depuis plus de 25 ans, SonicWall est un partenaire de confiance dans le secteur de la sécurité. Spécialisés dans la sécurité des réseaux, des accès et des messageries électroniques, nous développons sans cesse notre gamme de produits afin de permettre aux entreprises d'innover, d'accélérer leurs résultats et de se développer. Avec plus d'un million d'équipements de sécurité dans près de 200 pays et territoires de par le monde, les clients de SonicWall peuvent dire « oui » à l'avenir en toute confiance.

Pour toute question sur l'utilisation potentielle de ce produit, contactez :

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

ExecBrief-WhyNetworkingSandboxing-US-VG-24857