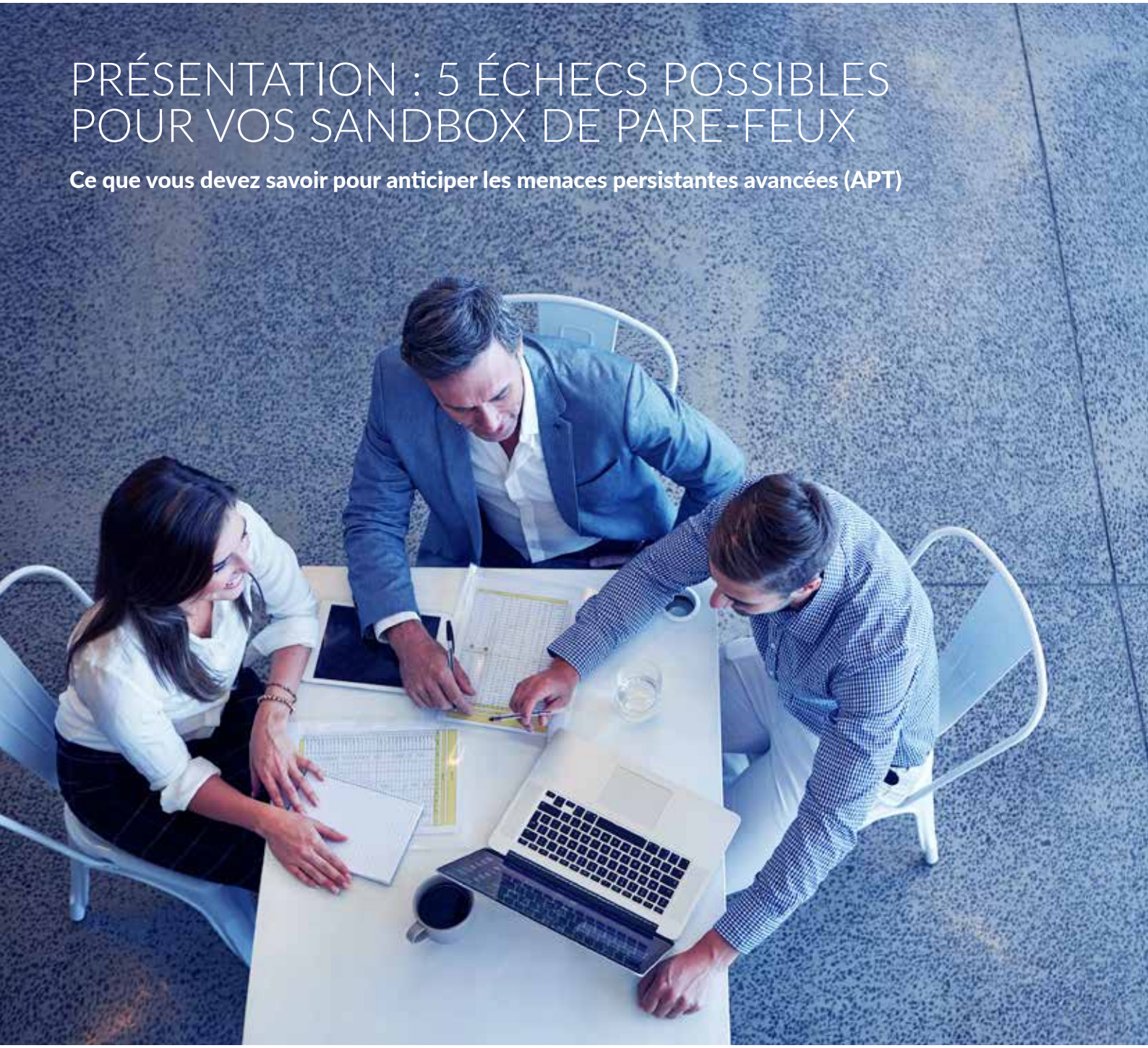
SONICWALL®

PRÉSENTATION : 5 ÉCHECS POSSIBLES POUR VOS SANDBOX DE PARE-FEUX

Ce que vous devez savoir pour anticiper les menaces persistantes avancées (APT)



Une menace persistante avancée est un ensemble de processus de piratage informatique discrets et continus, souvent orchestrés par des agresseurs visant une entité spécifique. Ces menaces incluent souvent des logiciels malveillants inconnus et non documentés, notamment des menaces de type zero-day. Elles sont conçues pour être évolutives, polymorphes et dynamiques. Leur objectif est d'extraire ou de compromettre des données stratégiques, comme les informations d'identité, d'accès et de contrôle. Même si ces types d'attaques sont moins courants que les menaces automatisées ou standardisées dont la cible est plus vaste, les APT représentent une sérieuse menace.

Pour parvenir à mieux les détecter, les professionnels de la sécurité déploient des technologies de détection avancée des menaces, incluant souvent des sandbox virtuelles qui analysent le comportement des fichiers suspects et repèrent des logiciels malveillants dissimulés, jusque-là inconnus. Les menaces sont toutefois de plus en plus intelligentes et les techniques de sandboxing de nombreux éditeurs ne parviennent pas toujours à s'adapter. Cette présentation examine cinq aspects sur lesquels les techniques de sandboxing existantes sont en échec et explore ce dont votre entreprise a besoin pour pouvoir anticiper les APT.

Les technologies actuelles de détection avancée des menaces permettent souvent uniquement d'identifier la présence et le comportement des logiciels malveillants.

1. Infiltration avant analyse

Tout d'abord, certaines solutions de sandboxing ne fournissent aucun verdict d'analyse tant qu'un fichier potentiellement dangereux n'a pas pénétré le périmètre du réseau. Cela multiplie les vecteurs possibles dont un fichier malveillant dispose pour s'infiltrer sur le réseau, derrière son périmètre.

2. Analyses de fichiers limitées

Deuxièmement, certaines solutions de sandboxing au niveau de la passerelle sont limitées en termes de taille et de type de fichiers ou d'environnement d'exploitation analysable. Elles ne parviendront peut-être à traiter que les menaces visant un environnement informatique unique. Or les entreprises utilisent aujourd'hui des systèmes d'exploitation multiples, notamment Windows, Android et Mac OSX.

Parallèlement, l'adoption de plus en plus vaste d'appareils mobiles et connectés a étendu la surface d'attaque visée par les menaces. En 2015, SonicWall a observé de nombreuses nouvelles techniques offensives et défensives qui cherchaient à augmenter la puissance des attaques dirigées contre l'écosystème Android, lequel représente près de 85 % des smartphones dans le monde. Souvent, les technologies actuelles de détection analysent et détectent uniquement les menaces visant les systèmes d'exploitation et les applications utilisés à des fins de productivité. Les entreprises risquent ainsi de se trouver dans une position vulnérable face aux attaques dirigées contre les environnements mobiles et connectés modernes.

En outre, ces technologies ne parviendront peut-être pas à traiter le vaste éventail des types de fichiers standard pour l'entreprise : programmes exécutables (PE), DLL, PDF, documents MS Office, archives, fichiers JAR, APK, etc. En raison de ces limites, des menaces zero-day inconnues risquent de pénétrer sur le réseau sans analyse ni identification.

3. Moteurs de sandboxing en silos

Troisièmement, les solutions de sandboxing autonomes à un seul moteur ne sont plus appropriées.

Les logiciels malveillants sont désormais conçus pour détecter la présence d'une sandbox virtuelle et se soustraire à toute détection ; l'efficacité des technologies de sandboxing première génération est donc limitée. Les solutions de sandboxing à un seul moteur présentent une cible particulièrement facile pour les techniques d'évasion.

Elles créent par ailleurs des lacunes en termes d'analyse. Par exemple, l'analyse des appels entre applications et systèmes d'exploitation peut être moins granulaire que l'analyse des appels entre matériel et systèmes d'exploitation car nombre de ces appels sont dissimulés par les couches applicatives.

Une technique plus efficace consisterait à intégrer des couches de plusieurs moteurs de sandboxing. Et pourtant, les solutions de sandboxing actuelles sont souvent des appliances en silos, à moteur unique, autonomes, ou des services Cloud. Le déploiement de multiples technologies de sandboxing, même si elles sont viables, augmenterait considérablement la complexité de la configuration, la charge administrative et les coûts.

4. Des menaces chiffrées

Pendant de nombreuses années, les institutions financières et autres sociétés manipulant des informations stratégiques ont opté pour le protocole HTTPS sécurisé qui chiffre les données

partagées. Aujourd'hui, d'autres sites tels que Google, Facebook et Twitter adoptent également cette pratique en réponse à une demande croissante de confidentialité et de sécurité des utilisateurs. Même si l'utilisation plus intensive du chiffrement sur Internet présente de nombreux avantages, une tendance moins positive apparaît : des pirates exploitent ce chiffrement afin de « masquer » les logiciels malveillants pour les pare-feux des entreprises.

En utilisant le chiffrement SSL (Secure Sockets Layer) et TLS (Transport Layer Security) (SSL/TLS) ou le trafic HTTPS, les agresseurs expérimentés peuvent chiffrer les communications C&C ainsi que du code malveillant pour échapper au contrôle des systèmes de prévention des intrusions (IPS) et de filtrage anti-malware. Ces attaques peuvent être extrêmement efficaces, tout simplement parce que les entreprises ne possèdent pas l'infrastructure adéquate pour les détecter. En général, soit les solutions de sécurité réseau en place ne sont pas capables d'inspecter le trafic chiffré SSL/TLS, soit leurs performances sont trop faibles pour pouvoir effectuer l'inspection.

5. Des corrections déjouées

Par ailleurs, les technologies actuelles de détection avancée des menaces permettent souvent uniquement d'identifier la présence et le comportement des logiciels malveillants. Même si la technique de sandboxing identifie de manière efficace une menace récemment créée sur un terminal spécifique, les entreprises ne disposent d'aucun moyen évident pour réagir face à cette menace. Elles ne possèdent pas de solution simple et efficace pour mettre à jour les signatures des pare-feux sur un réseau distribué global.

Une fois le logiciel malveillant découvert, généralement après l'infection du système, les mesures de correction incombent au service informatique de l'entreprise qui doit passer un temps considérable à repérer et éradiquer le logiciel en cause, puis réparer les dommages collatéraux subis par les systèmes infectés. Il doit également créer et déployer rapidement de nouvelles signatures de logiciels malveillants sur toute l'entreprise afin d'éviter des attaques supplémentaires.

Que faire ?

Les sandbox existantes ne sont pas parfaites mais elles reposent sur une base solide. Pour que le sandboxing soit efficace, il convient de trouver une réponse à ses défauts. Dans cette optique, votre solution de sandboxing doit :

- appliquer une analyse Cloud aux fichiers suspects afin de détecter et de bloquer des menaces inconnues en dehors de la passerelle, dans l'attente d'un verdict ;
- analyser un vaste éventail de types de fichiers et d'environnements d'exploitation, quels que soient la taille des fichiers ou le chiffrement ;
- mettre à jour rapidement et automatiquement les signatures correctives ;
- intégrer plusieurs moteurs afin d'accroître la résistance aux tactiques d'évasion, de gagner en visibilité sur le comportement des logiciels malveillants et de renforcer la détection des menaces.
- réduire les coûts et la complexité.

En savoir plus.

Découvrez comment le sandboxing multicouche détecte davantage de menaces zero-day. Regardez ce webcast à la demande.

> Une technique plus efficace consisterait à intégrer des couches de plusieurs moteurs de sandboxing.

À propos de SonicWall

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

Pour toute question concernant l'usage potentiel de ce document, contactez :

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

Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com