
SONICWALL®
Types de stratégies de cyberattaques et moyens de prévention
E-BOOK

Introduction

Les cybercriminels modernes ont perfectionné leurs techniques déjà complexes pour éviter d'être détectés. Ils se faufilent discrètement dans les réseaux pour diverses raisons, souvent motivés par le gain financier. Entre autres activités criminelles, ces auteurs de menaces cherchent à voler la propriété intellectuelle, à espionner, à perturber les processus ou à demander une rançon en échange de fichiers. Ils utilisent les techniques les plus récentes pour échapper à la détection, dans le but de conserver leur accès et de mener leurs activités malveillantes sans se faire remarquer.

Une fois la cible exploitée, les attaquants tentent généralement de télécharger et d'installer des programmes malveillants sur le système compromis. Bien souvent, ces programmes sont des variantes récemment créées et donc inconnues des solutions antivirus conventionnelles.

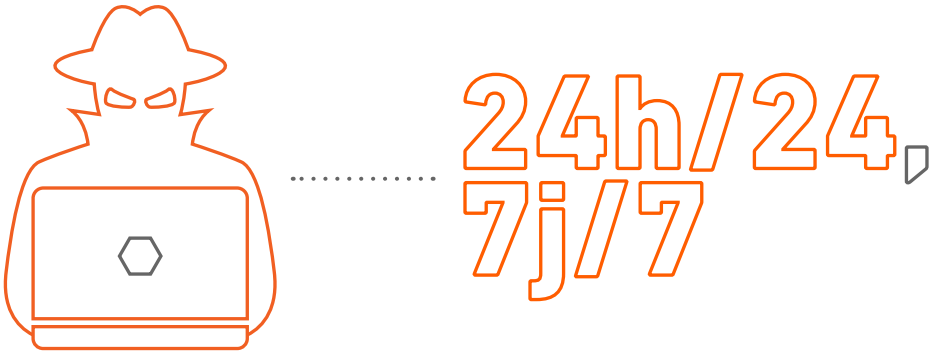
Cet e-book détaille les stratégies de cyberattaques et les outils qu'utilisent les cybercriminels pour infiltrer votre réseau et vous explique comment contrer ces stratégies pour stopper les cybercriminels dans leur élan.

Les cybercriminels travaillent 24h/24, 7j/7 pour exploiter vos faiblesses.

Stratégie de cyberattaque nº 1 Bombarder les réseaux de programmes malveillants 24h/24

Le volume total de malwares est en hausse, certains pays enregistrant des tentatives record de plusieurs millions. Les attaques peuvent provenir de tous les vecteurs pour cibler et compromettre votre réseau. E-mails, équipements mobiles, trafic Web notamment sont autant de cibles pour les pirates qui peuvent même vous compromettre via des exploits automatisés. Qui plus est, la taille de votre entreprise n'a pas d'importance. Pour un pirate informatique, vous êtes une adresse IP, une adresse e-mail ou un prospect pour une attaque de point d'eau. Les attaquants utilisent des outils automatisés pour exécuter des exploits ou pour lancer des e-mails de phishing de jour comme de nuit.

Le problème que rencontrent de nombreuses entreprises est qu'elles ne disposent pas des outils adéquats. La plupart n'ont pas d'outils automatisés permettant d'analyser le trafic, de protéger les terminaux et de filtrer les mauvais e-mails. D'autres utilisent des pare-feux qui ne peuvent pas voir le trafic chiffré pour détecter des menaces cachées ou s'appuient sur la mémoire limitée du système embarqué pour stocker les signatures des malwares.



Contre-attaque n° 1
Protéger votre réseau, 24h/24, 7j/7

Avec des centaines de variantes de malwares inédites développées toutes les heures, les entreprises ont besoin d'une protection actualisée en temps réel contre ces nouvelles menaces. Une solution de sécurité efficace doit disposer des technologies les plus récentes pour détecter les dangers en temps réel et protéger votre entreprise 24h/24h, 7j/7j. Avec l'afflux important de types et de variantes de malwares, la mémoire disponible des pare-feux est saturée. Une solution de services de sécurité qui inclut une technologie Real-Time Deep Memory Inspection (RTDMI™) détecte et bloque de manière proactive les menaces zero-day grand public et les variantes de malwares inconnues.

Les pare-feux doivent utiliser un sandbox cloud pour fournir la vision la plus large possible des malwares et découvrir et identifier les nouvelles variantes. Il est également essentiel de s'assurer que votre solution de sécurité prend en charge une protection mise à jour de manière dynamique non seulement au niveau de la passerelle du pare-feu, mais également au niveau des terminaux distants et mobiles, car les appareils IoT peuvent servir de points d'entrée pour les attaquants.

Insistez sur une plateforme de sécurité qui tire parti de la puissance du cloud pour offrir une détection et une prévention automatisées et en temps réel des failles afin de contrer les toutes dernières menaces des logiciels malveillants.

Les cybercriminels utilisent différents types de programmes malveillants pour vous prendre de court.

Stratégie de cyberattaque nº 2 Infecter les réseaux avec différentes formes de programmes malveillants

Les cybercriminels utilisent une multiplicité de vecteurs d'attaque et de variantes de malwares pour compromettre les réseaux. Les cinq types les plus fréquents sont les virus, les vers, les chevaux de Troie, les logiciels espions et les logiciels ransomwares.

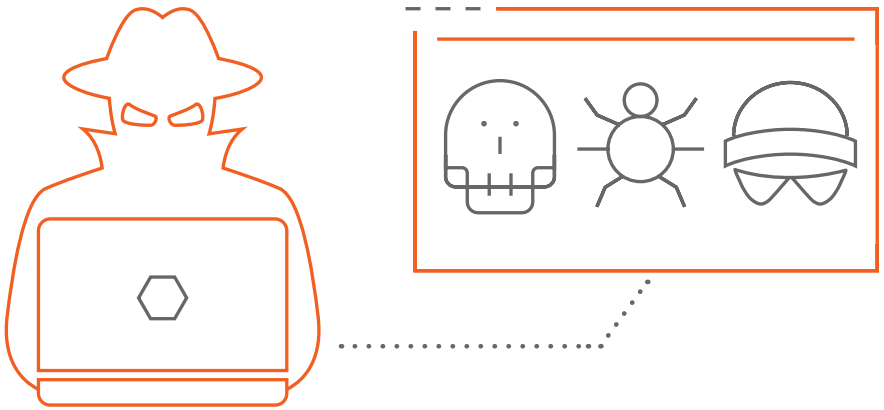
Les virus informatiques se répandaient à l'origine par le partage de supports infectés. La méthode de propagation a suivi l'évolution technologique. Aujourd'hui, les virus se transmettent généralement par les programmes légitimes, le partage de fichiers, les téléchargements sur le Web et les pièces jointes aux e-mails. Lorsqu'ils sont ouverts ou exécutés, ils peuvent provoquer toute une série d'actions malveillantes, allant de la corruption de données aux pannes système.

Les vers informatiques existent depuis la fin des années 1980, mais étaient peu répandus jusqu'à ce que les infrastructures réseau deviennent monnaie courante au sein des entreprises. Contrairement aux virus informatiques, les vers peuvent s'autorépliquer et se propager à travers les réseaux sans aucune interaction humaine. Ils peuvent provoquer des infections rapides et surcharger les réseaux.

Les chevaux de Troie sont des programmes malveillants qui se font passer pour des logiciels ou des fichiers légitimes et qui sont conçus dans le seul but d'extraire des données sensibles du réseau. De nombreux types de chevaux de Troie prennent le contrôle du système infecté et ouvrent une porte dérobée à laquelle l'attaquant peut accéder ultérieurement. Ils servent habituellement à la création de botnets.

Les logiciels espions ne sont en général pas malveillants par nature, mais ils constituent une nuisance importante, car ils infectent souvent les navigateurs Web et les rendent inopérants. Les logiciels espions prennent parfois l'apparence d'applications légitimes, offrant à l'utilisateur certains avantages tout en enregistrant secrètement la frappe et l'historique de navigation, en volant des données personnelles ou en suivant le comportement de l'utilisateur et ses habitudes d'utilisation. Les données volées sont ensuite envoyées à l'attaquant, ce qui compromet la confidentialité et la sécurité des utilisateurs.

Le ransomware est une attaque qui le plus souvent chiffre les fichiers sur un terminal ou un serveur entier, les rendant inaccessibles. Les cybercriminels demandent ensuite une rançon à l'entreprise, généralement en bitcoins, en échange de la clé de chiffrement. Lorsqu'il se propage aux systèmes critiques de l'entreprise, le coût du ransomware peut gonfler jusqu'à atteindre des centaines de milliers de dollars, voire plus.



Pour garder une longueur d'avance sur les menaces, envisagez plusieurs couches de protection contre les malwares.

Contre-attaque n° 2
Assurer la protection de votre réseau contre tous les types de programmes malveillants

Tous les pare-feux doivent protéger les entreprises contre tous les types de cybermenaces. La meilleure façon d'y parvenir est d'intégrer ces protections dans une approche « single-pass » à faible latence qui bloque les vecteurs d'attaque non seulement au niveau de la passerelle, mais aussi au niveau des terminaux situés au-delà du périmètre traditionnel. Recherchez les caractéristiques suivantes :

- protection anti-malware au niveau du réseau pour empêcher les attaquants de télécharger ou de transmettre des programmes malveillants vers un système compromis ;
- mises à jour continues et opportunes pour protéger les réseaux 24h/24 contre les millions de nouvelles variantes de malwares dès qu'elles sont détectées ;
- service de prévention des intrusions (IPS) pour empêcher les attaquants d'exploiter les vulnérabilités ;
- service de sandboxing pour envoyer le code suspect dans un environnement cloud isolé afin de le faire exploser et de l'analyser à la recherche de malwares inédits ;
- sécurité des accès pour appliquer des contre-mesures de contrôle des accès utilisateurs aux terminaux mobiles et distants, à l'intérieur comme à l'extérieur du périmètre du réseau ;
- sécurisation de la messagerie pour bloquer le phishing, le spam, les chevaux de Troie et les attaques d'ingénierie sociale véhiculés par le courrier électronique.

En veillant à ce que chaque appareil qui accède à votre réseau soit équipé d'un logiciel de protection antivirus à jour, vous obtiendrez une couche supplémentaire de protection contre les logiciels malveillants sur le réseau. Lorsque les entreprises couplent un ordinateur équipé d'un antivirus complet à un pare-feu réseau, elles peuvent bloquer un grand nombre des outils dont disposent les cybercriminels pour compromettre le réseau.

Stratégie de cyberattaque nº 3 Trouver les réseaux les plus faibles et les compromettre

> Les cybercriminels choisissent souvent leurs victimes en fonction des faiblesses du réseau qu'ils découvrent.

Bien que de nombreux fournisseurs de pare-feux prétendent assurer une protection haut de gamme, peu parviennent à prouver l'efficacité de leurs solutions. Les entreprises qui utilisent d'anciens pare-feux peuvent penser que leurs réseaux sont protégés, mais des cybercriminels habiles peuvent se faufiler à travers les pare-feux qui ne disposent pas des bonnes mesures de sécurité en utilisant des algorithmes complexes afin de passer inaperçus et compromettre le réseau.

Certains pare-feux offrent la sécurité au détriment des performances, ce qui peut inciter les entreprises qui les utilisent à désactiver ou à limiter leurs mesures de sécurité pour maintenir les performances du réseau au niveau exigé. Cette pratique est extrêmement risquée, et formellement déconseillée.

Une autre vulnérabilité de la sécurité réseau provient du facteur humain. Les criminels comptent sur le potentiel des actions ou des comportements humains pour compromettre par inadvertance l'intégrité, la confidentialité et la disponibilité d'un réseau. Le phishing, l'ingénierie sociale, les systèmes mal configurés, les logiciels non corrigés, les règles de sécurité ignorées, etc. sont autant d'actions susceptibles d'introduire des risques et d'affaiblir les mesures de sécurité. Les auteurs de menaces exploitent ces tactiques pour obtenir des informations de connexion et autres autorisations qui peuvent leur permettre de contourner les protections des pare-feux en lançant des attaques de l'intérieur. À cela s'ajoute le fait que les collaborateurs connectent parfois des dispositifs personnels au réseau de l'entreprise sans prendre les mesures de sécurité adéquates. Cela peut conduire à un accès non autorisé si un dispositif personnel est perdu ou laissé sans surveillance, exposant l'entreprise à une faille lorsqu'il se trouve en dehors du périmètre de sécurité du réseau.

> Tous les pare-feux ont besoin d'un moteur qui protège les réseaux contre les attaques internes et externes, sans compromettre les performances.

Contre-attaque n° 3
Choisir une plateforme de sécurité complète qui offre une protection supérieure contre les menaces, des performances élevées et une gestion centralisée

Recherchez des solutions de sécurité qui ont été testées et certifiées de manière indépendante pour la protection contre les malwares au niveau réseau.

Envisagez la conception d'une plateforme multicœur capable d'analyser des fichiers de toute taille et de tout type pour répondre à l'évolution des flux de trafic. Tous les pare-feux ont besoin d'un moteur qui protège les réseaux contre les attaques internes et externes, sans compromettre les performances.

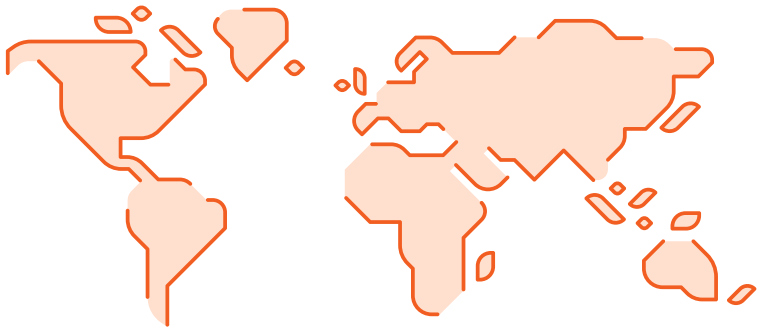
Recherchez un pare-feu qui propose un service de sandbox dans le cloud pour aider à découvrir de tout nouveaux malwares susceptibles de cibler votre environnement. Ces choix peuvent faire toute la différence entre une journée de travail normale et une où les cybercriminels prennent en otage vos ressources numériques.

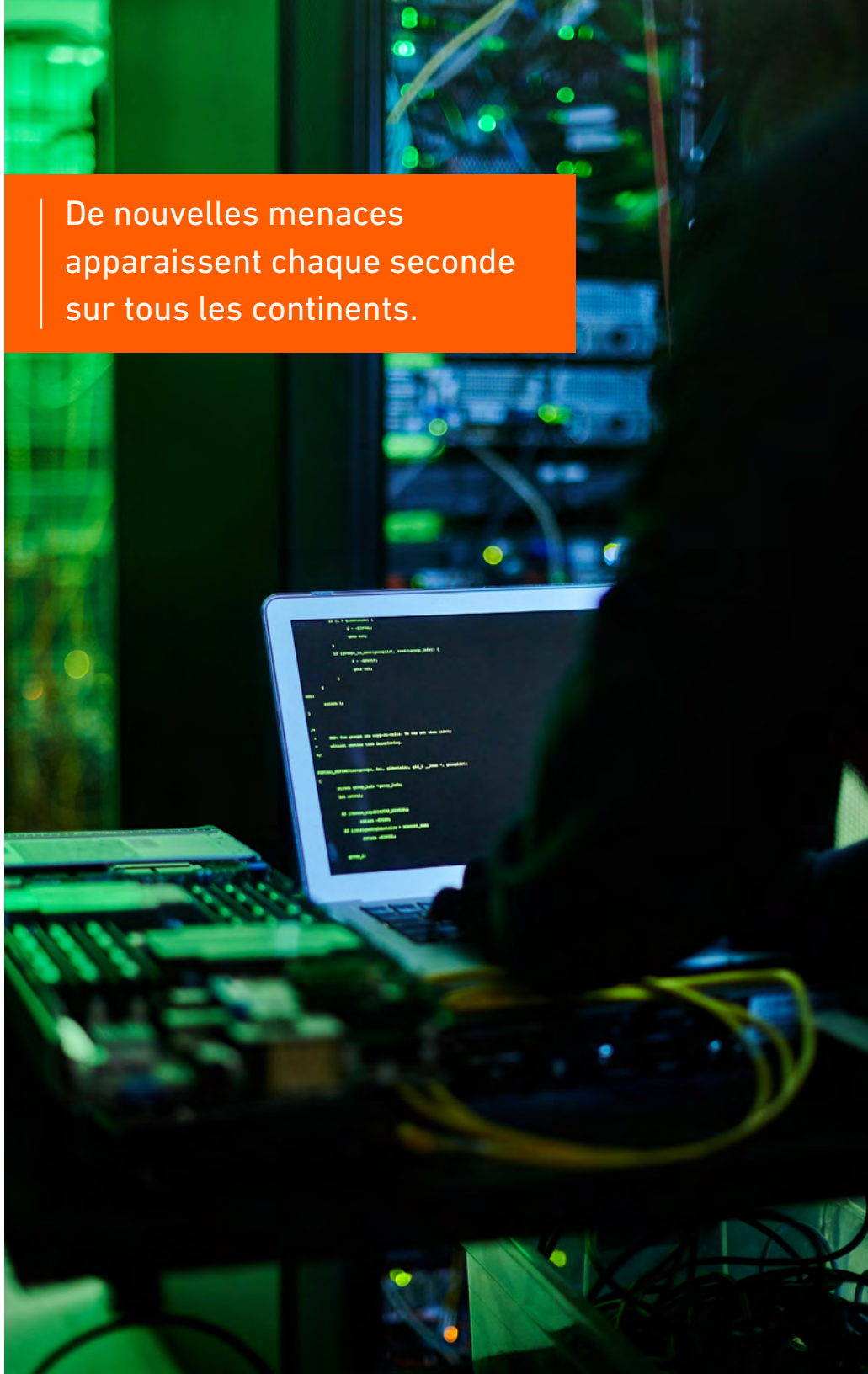
Votre stratégie de sécurité doit inclure la protection des terminaux mobiles et distants à l'intérieur et à l'extérieur du périmètre pour un accès mobile sécurisé.

En outre, vous avez besoin de sécuriser la messagerie pour vous protéger contre le phishing, le spam, les virus, l'ingénierie sociale et autres menaces véhiculées par e-mail. Utilisez des outils comme le quiz gratuit sur le phishing de SonicWall pour sensibiliser votre entreprise.

Stratégie de cyberattaque nº 4 Muter fréquemment et attaquer tous azimuts

De nombreux cybercriminels parviennent à leurs fins en inventant continuellement de nouveaux programmes malveillants et en les partageant avec leurs homologues du monde entier. En d'autres termes, de nouvelles menaces apparaissent chaque seconde sur tous les continents. De nombreux cybercriminels adoptent une approche « smash and grab » pour leurs attaques : ils entrent, prennent ce qu'ils peuvent et sortent avant même que quiconque puisse donner l'alerte. Ils peuvent entrer et sortir avant même que vous ne vous rendiez compte de ce qui vous arrive. D'autres y vont doucement et lentement pour tenter d'accéder à davantage de données sur une plus longue période. Certaines attaques passent par le Web, d'autres par la messagerie ou directement dans le réseau sur des appareils infectés qui étaient précédemment en itinérance hors du périmètre de sécurité du réseau.





> De nouvelles menaces apparaissent chaque seconde sur tous les continents.

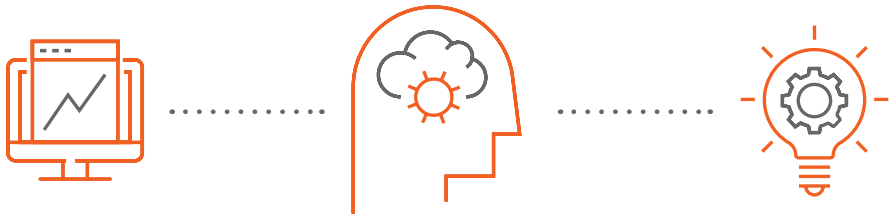
> Pour bloquer les dernières menaces mondiales, investissez dans une solution de sécurité dotée de renseignements sur les menaces mondiales.

Contre-attaque n° 4
Choisir un pare-feu qui protège contre les menaces mondiales

Réagir rapidement aux menaces est essentiel pour maximiser la protection. Pour pouvoir déployer rapidement des contre-mesures contre les menaces émergentes, vous avez besoin d'un fournisseur de solutions de sécurité qui dispose de sa propre équipe de renseignements sur les menaces, de recherche et de contre-mesures. En outre, cette équipe devrait élargir son champ d'action en collaborant avec la communauté de la sécurité au sens large, à l'instar du Rapport SonicWall sur les cybermenaces.

Une solution à large spectre utilise un catalogue de malwares cloud mondial complet pour compléter l'analyse des pare-feux locaux.

Enfin, si un simple pare-feu peut identifier et bloquer par zone géographique, un pare-feu de nouvelle génération plus sophistiqué ajoutera des capacités de filtrage des botnets afin de réduire l'exposition aux menaces mondiales connues en bloquant le trafic provenant de domaines dangereux ou en bloquant les connexions à destination et en provenance de sites malveillants.



Conclusion

Lors de l'élaboration de stratégies de défense efficaces contre les cyberattaques réseau, vous devez mettre en œuvre une approche holistique intégrant des pratiques de sécurité solides et l'utilisation d'outils de sécurité efficaces qui détectent les comportements anormaux du réseau et y répondent sans compromettre les performances. Protégez-vous ainsi que votre entreprise de l'inconnu en restant proactif et en vous adaptant à l'évolution des menaces.

Lorsque vous serez prêt à évaluer des solutions de contre-attaque adaptées aux besoins uniques de votre entreprise, contactez votre représentant SonicWall ou rendez-vous sur notre site Web pour en savoir plus sur les pare-feux de nouvelle génération SonicWall (NGFW).

Pour en savoir plus

Contactez-nous pour consulter un expert en sécurité SonicWall.

Regardez nos démos live de notre gamme de produits SonicWall.

Rendez-vous sur notre page Web, Pare-feux de nouvelle génération

Découvrez où se déroulent les attaques récentes dans notre Capture Labs Security Center.

À propos de SonicWall

SonicWall offre une solution de cybersécurité sans limites pour l'ère de l'hyper-distribution, dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé financier en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour plus d'informations, rendez-vous sur www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com

Ebook-TypesofCyberattacks-JK-8854