SONICWALL

VOS DONNÉES CONTRE UNE RANÇON

Pourquoi les ransomwares sont aujourd'hui l'exploit de prédilection des cybercriminels

CAPTURER DÉFINITIVEMENT LES RANSOMWARES

Les auteurs des menaces et les cybercriminels savent depuis longtemps comment infiltrer les réseaux et dérober des données. Il était en revanche souvent complexe et fastidieux de parvenir à transformer ces données en monnaie d'échange.

L'introduction des ransomwares leur a permis de ne plus devoir exfiltrer les données pour ensuite les revendre sur des marchés souterrains.

Aujourd'hui, il est plus facile de s'infiltrer sur votre réseau, de déchiffrer les données et de les garder en otage jusqu'à ce que vous payiez une rançon. Sans stratégie proactive de cybersécurité en temps réel, les entreprises n'ont que peu d'options à leur disposition.

Au fil de ce guide, vous comprendrez mieux ce que sont les ransomwares et comment le sandboxing Cloud peut permettre de limiter les attaques avant qu'elles ne pénètrent dans votre environnement et ne s'emparent de vos données, et par conséquent de votre entreprise, en échange d'une rançon.

Vue d'ensemble

SONICWALL®

Ransomwares : êtes-vous protégé contre une autre attaque ?

Serez-vous la prochaine victime des ransomwares ? Les agresseurs peuvent-ils déchiffrer vos données et les garder en otage jusqu'à ce que vous payiez une rançon ?

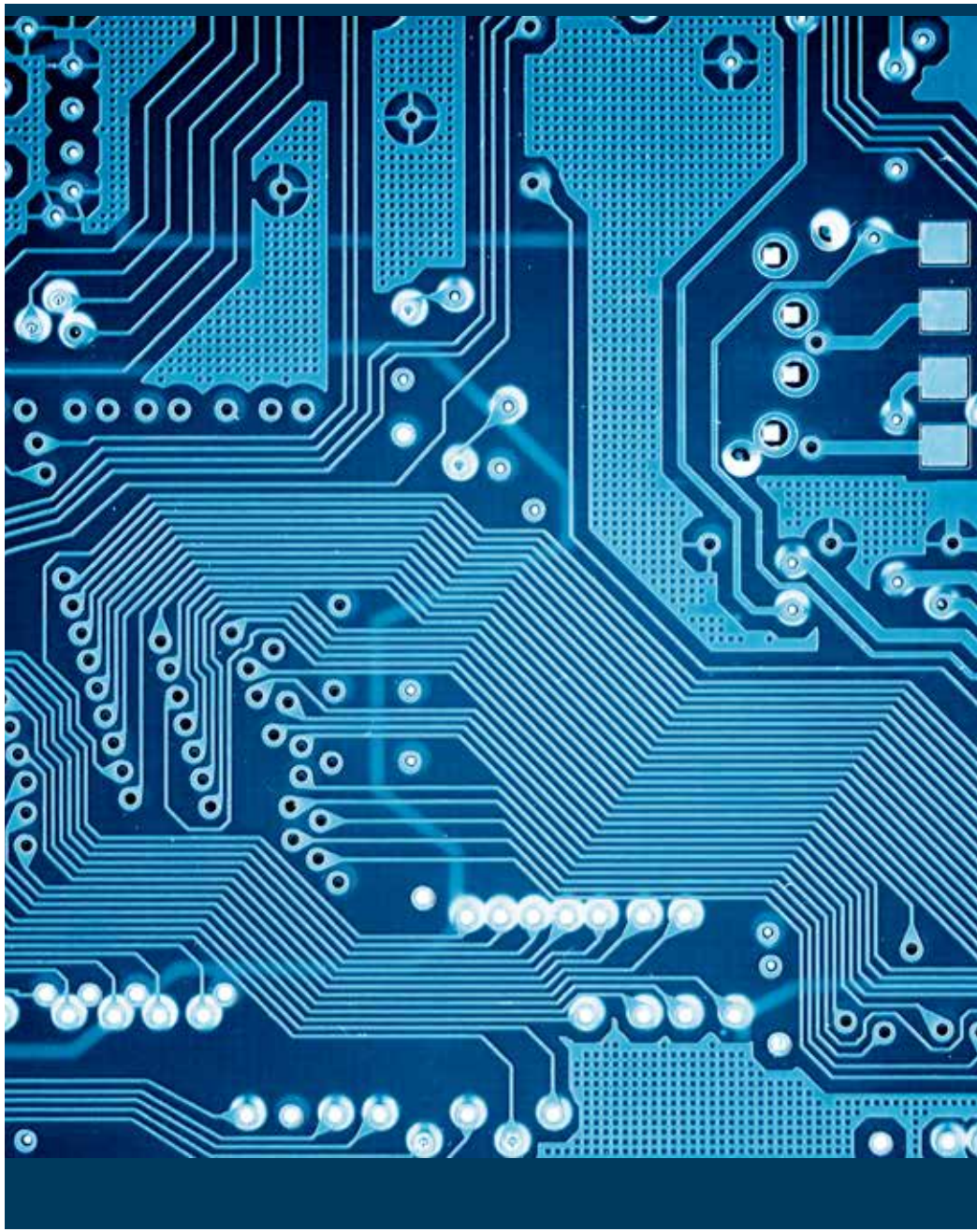
Toutes les entreprises, grandes ou petites, tous secteurs confondus, dans le monde entier, risquent une attaque par ransomware. La presse fait état d'attaques contre de grandes institutions, comme l'hôpital d'Hollywood qui, en 2016, est resté une semaine sans aucune connexion suite à une attaque par ransomware sur des fichiers chiffrés et à une demande de rançon pour déchiffrer ces données.

Mais les petites entreprises sont également touchées. En fait, les équipes de recherche Kaspersky ont indiqué que les petites et les moyennes entreprises étaient les plus touchées, 42 pour cent d'entre elles étant victimes d'une attaque par ransomware sur une période de 12 mois.

Parmi ces victimes, une sur trois a payé la rançon, tandis qu'une sur cinq n'a jamais récupéré ses fichiers malgré le paiement. Que votre entreprise soit grande ou petite, elle est exposée à un risque.

SUITE ET FIN >

Les sept habitudes des attaques par ransomware ultra efficaces



En 2016, SonicWall a observé une croissance de 600 pour cent dans les familles de ransomwares. Notre rapport annuel 2017 sur les menaces fait état d'une vaste palette de formes de ransomwares et de vecteurs d'attaques, dont certains ont réussi à atteindre leur cible et d'autres seulement partiellement.

Quel est donc l'élément central d'une attaque réussie ? Si vous connaissez les sept composants de la stratégie des campagnes de ransomware, vous saurez mieux vous protéger contre l'une des formes les plus pernicieuses des logiciels malveillants de l'histoire.

1. Recherche intelligente de la cible

Tout bon escroc sait comment identifier, au sein d'une entreprise, les bonnes personnes à cibler pour délivrer le message voulu. Les pirates savent qu'il est judicieux de choisir des cibles dans les milieux municipaux et médicaux.

Les entreprises proposent pourtant des programmes de sensibilisation, mais les utilisateurs continuent de cliquer sur des e-mails et des contenus de médias sociaux habilement créés. En outre, les pirates peuvent aller dans toute base de données publique de génération de leads et trouver le groupe de victimes approprié pour leur campagne de phishing.

2. Transmission efficace

Étant donné que 65 pour cent des attaques par ransomware se produisent via e-mail, il est facile pour les pirates d'envoyer une pièce jointe infectée à quelqu'un en lui présentant comme une facture impayée. Après une attaque de ce type, le fournisseur d'énergie BWL de Lansing (Michigan, USA) a été privé de système pendant deux semaines, ce qui lui a coûté environ 2,4 millions de dollars US.

LISTE COMPLÈTE >

SONICWALL®

RaaS, les ransomwares en tant que service sont la nouvelle norme

Dans l'entreprise, les modèles doivent toujours prendre en compte la méthode de distribution : va-t-elle vendre directement ou via un canal de distributeurs ou une combinaison des deux ? Il en va de même pour les développeurs de ransomwares.

Ils sont nombreux à choisir de vendre leur code sous forme de kit, ce qui permet d'éviter de nombreux risques et le travail fastidieux de distribution, tout en récoltant leur part de butin.

L'année passée, et même jusqu'aux attaques WannaCry de grande envergure, des petites attaques ciblées sont apparues ça et là entre deux pics d'événements tristement célèbres, en masse à partir de kits d'exploits usurpant une identité de marque. SonicWall a découvert un mélange de logiciels malveillants porteurs de chaos, créés par des développeurs amateurs, des ransomwares utilisant le rebranding et des ransomwares RaaS repackagés.

- Trumplocker
- AlmaLocker
- Jigsaw
- Lambda
- Derialock
- Shade
- Popcorn
- Jaff

Récemment, un auteur a montré combien il était facile de lancer une attaque par ransomware en l'espace d'une heure… **sans aucune compétence en piratage**.

Qu'est-ce que cela signifie pour une entreprise comme la vôtre ? Devez-vous vous en inquiéter ? En résumé, plus les sources d'attaques sont nombreuses, plus les attaques se multiplient. Mais SonicWall est là pour vous aider.

SUITE >

SONICWALL®

Pourquoi le sandboxing réseau est nécessaire pour bloquer les ransomwares

Les pare-feux de 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.

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 ?

Téléchargez le rapport IDC gratuit pour comprendre comment le sandboxing permet de limiter l'impact des menaces évoluées.


IDC

IDC ANALYST CONNECTION

Addressing Advanced Threats Through Multiple Sandbox Options

Rapport IDC gratuit

Répondre aux menaces évoluées grâce aux diverses options de sandboxing.

TÉLÉCHARGER LE RAPPORT >

SONICWALL®

Bloquer les ransomwares avec Capture ATP

Le service SonicWall Capture Advanced Threat Protection (ATP) est une sandbox multi-moteur basée sur le Cloud, conçue pour identifier et bloquer les attaques inconnues et zero-day (par ex. les ransomwares) au niveau de la passerelle, et pour déclencher des corrections automatiques.

Ce service est la seule détection des menaces évoluées à combiner un mécanisme de sandboxing multicouche, comprenant des techniques de virtualisation et d'émulation complètes du système, pour analyser le code suspect.

Un puissant cocktail qui intercepte davantage de menaces que les solutions de sandbox à un seul moteur, spécifiques à un environnement et plus faciles à contourner.

- **Bloque les ransomwares en temps réel**
- **Analyse de nombreux types de fichiers**
- **Analyse multi-moteur des menaces évoluées**
- **Déploiement rapide des signatures correctives**
- **Analyses et rapports**
- **Blocage jusqu'au verdict**

Pour en savoir plus sur le service SonicWall Capture Advanced Threat Protection, téléchargez la fiche technique ou rendez-vous sur **sonicwall.com/capture**.

Comment fonctionne Capture ATP ?

TÉLÉCHARGER LA FICHE TECHNIQUE >

SONICWALL®

Démo : SonicWall Capture ATP vs. logiciels malveillants les plus récents

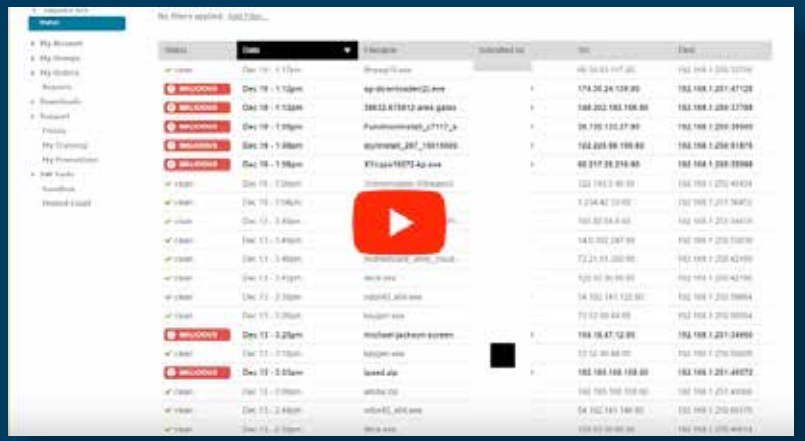
Afin de protéger les clients face aux dangers croissants des menaces zero-day (par ex. les ransomwares), SonicWall Capture Advanced Threat Protection, un service Cloud proposé avec les pare-feux SonicWall, détecte et bloque toute menace évoluée au niveau de la passerelle jusqu'à ce que l'analyse ait rendu son verdict.

Quel est le niveau de performance de Capture ATP ? Nous avons pris le logiciel malveillant le plus dangereux et le plus récent d'Internet et nous l'avons soumis à la technologie SonicWall pour montrer comment nous stoppons les menaces évoluées en temps réel, responsables d'attaques incessantes au sein des entreprises.

Avec seulement Gateway Anti-Virus (GAV) et Capture ATP, nous montrons comment le logiciel malveillant a été identifié et maîtrisé en temps réel. Capture ATP décèle ce que veut faire le logiciel malveillant depuis l'application, auprès du système d'exploitation et des logiciels situés sur le matériel.

À partir de là, l'infrastructure globale de renseignement sur les menaces fournit rapidement les signatures correctives pour les nouvelles menaces identifiées à toutes les appliances de sécurité réseau SonicWall, empêchant ainsi toute propagation.

Les clients bénéficient d'une sécurité haute efficacité, de délais de réponse brefs et d'un coût total de possession réduit.



DÉMO INTÉGRALE >

SONICWALL®

À propos de nous

En 25 ans d'histoire, SonicWall a toujours été un partenaire industriel de confiance dans le domaine de la sécurité. De la sécurité réseau à celle des accès, en passant par la sécurisation de messagerie, SonicWall n'a cessé de développer son portefeuille de produits, permettant aux entreprises d'innover, d'aller plus vite et de croître. Avec plus d'un million d'appareils de sécurité en place dans près de 200 pays et territoires de par le monde, SonicWall permet à ses clients de dire en toute confiance oui à l'avenir.

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 plus d'informations.
www.sonicwall.com