RAPPORT 2019 SUR LES CYBERMENACES DE SONICWALL

Mieux connaître leurs intentions.
Mieux connaître leurs attaques.
Savoir les stopper.

Une cyberattaque est personnelle. Elle vise essentiellement à déposséder les organisations, leurs employés, leurs partenaires et leurs clients de toutes leurs ressources : propriété intellectuelle, identités, vie privée, réputation et actifs monétaires. Suivez les tendances des attaques pour comprendre comment et où les cybercriminels ciblent les entreprises, les agences gouvernementales et les PME.

LE VOLUME DES LOGICIELS MALVEILLANTS A ATTEINT UN NOUVEAU SEUIL RECORD

Sur un plan international, SonicWall a enregistré

10,52 milliards

d'attaques de logiciels malveillants en 2018, un seuil encore jamais atteint. Depuis 2016, les attaques des logiciels malveillants ont augmenté de 33,4 %.

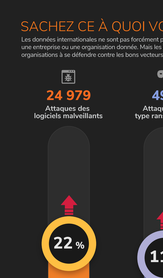
ATTAQUES INTERNATIONALES DES LOGICIELS MALVEILLANTS

LES ATTAQUES DE TYPE RANSOMWARE NE SONT NI PLUS NI MOINS QUE DU RACKET, AU NIVEAU INTERNATIONAL

SonicWall a enregistré plus de

206,4 millions

d'attaques de type ransomware dans le monde en 2018, soit une hausse de 11 % sur un an. Certaines régions connaissent un volume d'attaques équilibré. Dans d'autres, comme l'Amérique du Nord et l'Asie, les attaques visent des pays, des organisations ou des entités spécifiques.



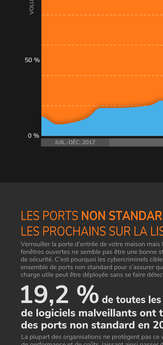
SACHEZ CE À QUOI VOUS ÊTES CONFRONTÉ

Les données internationales ne sont pas forcément parlantes tant qu'elles n'affectent pas une personne, une entreprise ou une organisation donnée. Mais les données exploitables sur les menaces aident les organisations à se défendre contre les bons vecteurs d'attaque.

24 979
Attaques des logiciels malveillants

490
Attaques de type ransomware

1 276
Menaces chiffrées

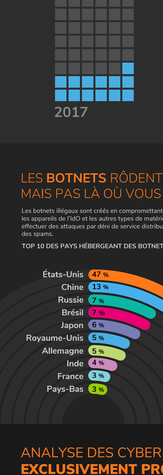


NOMBRE MOYEN DE CYBERATTAQUES SUBIES PAR CLIENT

NE FAITES PAS CONFIANCE À CE PDF

Les cybercriminels utilisent des PDF et des fichiers Microsoft Office pour masquer les logiciels malveillants et contourner les défenses du réseau. La plupart des contrôles de sécurité ne peuvent pas identifier ni atténuer les logiciels malveillants cachés dans ces types de fichiers. En 2018, SonicWall Capture ATP a découvert et bloqué des logiciels malveillants cachés dans

47 073 fichiers PDF et
50 817 fichiers Microsoft Office



LES PORTS NON STANDARD SONT LES PROCHAINS SUR LA LISTE

Verrouiller la porte d'entrée de votre maison mais laisser les fenêtres ouvertes ne semble pas être une bonne stratégie de sécurité. C'est pourquoi les cybercriminels ciblent un ensemble de ports non standard pour s'assurer que leur charge utile peut être déployée sans se faire détecter.

19,2 % de toutes les attaques de logiciels malveillants ont transité par des ports non standard en 2018.

La plupart des organisations ne protègent pas ce vecteur à cause de problèmes de performance et de coûts, laissant ainsi passer des millions d'attaques.

LES BOTNETS RÔDENT, MAIS PAS LÀ OÙ VOUS PENSEZ

Les botnets illégaux sont créés en compromettant les serveurs, les routeurs, les ordinateurs, les appareils de l'IdO et les autres types de matériel connectés à Internet. Ils sont utilisés pour effectuer des attaques par déni de service distribué (DDoS), voler des données et envoyer des spams.

TOP 10 DES PAYS HÉBERGEANT DES BOTNETS

ANALYSE DES CYBERMENACES EXCLUSIVEMENT PROPOSÉE PAR CAPTURE LABS DE SONICWALL

26 millions
d'attaques de phishing

3,9 milliards
d'événements d'intrusion

27 %
de menaces chiffrées

Rendez-vous sur SonicWall.com/ThreatReport pour télécharger le rapport 2019 sur les cybermenaces de SonicWall. Vous découvrirez de nouvelles perspectives en matière de stratégies d'attaques cybercriminelles et comprendrez comment bien défendre votre entreprise ou votre activité contre les cyberattaques les plus sophistiquées.

EN SAVOIR PLUS

SonicWall.com | #KnowTheThreats

* Dans le cadre d'une bonne pratique, SonicWall a systématiquement optimisé ses méthodologies de collecte et d'analyse des données, ainsi que d'établissement de rapports. Cela consiste notamment à améliorer le nettoyage des données modifiées, les sources de données et consolider les flux de menaces. Il se peut que les chiffres publiés dans les rapports précédents aient été ajustés selon les différentes périodes, régions ou secteurs.