Rapport 2019 SonicWall sur les cybermenaces

RÉSUMÉ | ÉDITION EUROPE

SonicWall.com

SONICWALL®

CAPTURE LABS

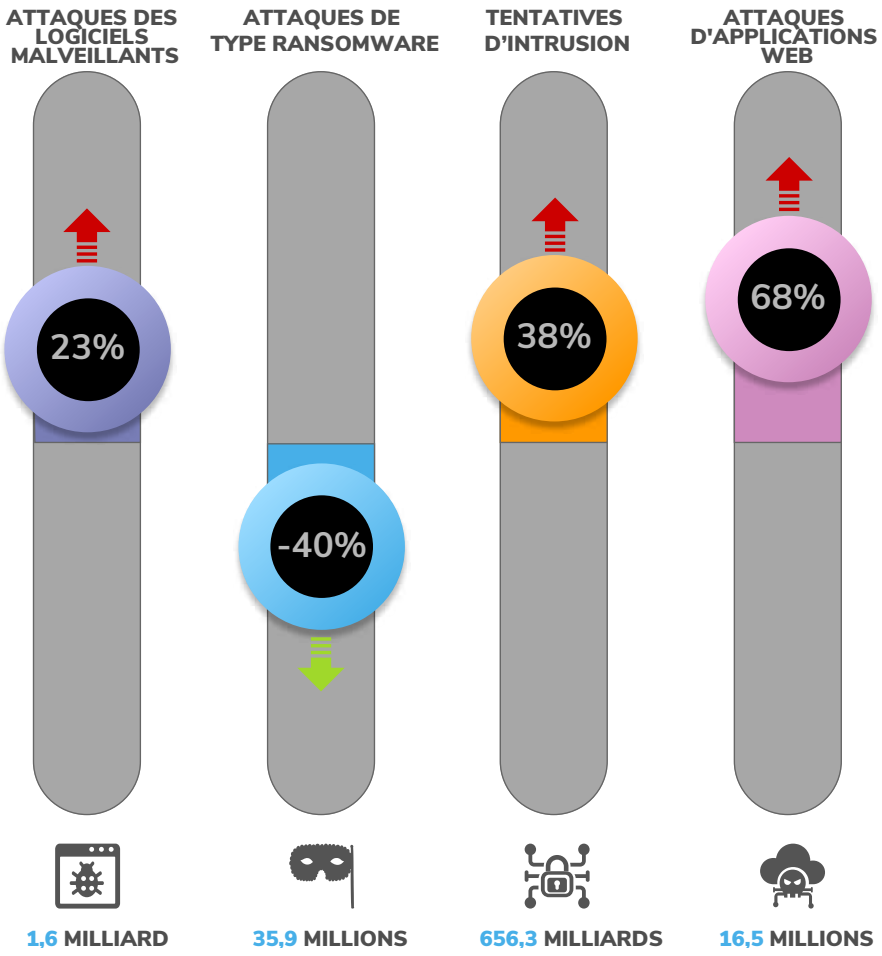
INTRODUCTION : ÉDITION POUR L'EUROPE

La course au cyber-armement ne fait aucune discrimination ou différence. Si un réseau, une identité, un appareil ou des données sont précieux, en particulier s'ils contiennent des informations liées à la propriété intellectuelle, aux données financières, aux fichiers sensibles, aux infrastructures critiques ou à une influence politique, les cybercriminels identifieront, cibleront et attaqueront sans pitié.

Afin d'augmenter le niveau de sensibilisation mondial et de faciliter les dialogues importants, SonicWall poursuit son engagement en faveur de la recherche, de l'analyse et du partage des renseignements sur les cybermenaces via son Rapport 2019. En complément du rapport approfondi, ce résumé apporte une perspective générale sur les renseignements concernant les menaces du point de vue des spécialistes du Capture Labs de SonicWall.

PRINCIPAUX ENSEIGNEMENTS DE 2018

TENDANCES EUROPÉENNES DES CYBERATTAQUES EN 2018



- Albanie
- Allemagne
- Andorre
- Autriche
- Belgique
- Biélorussie
- Bosnie-Herzégovine
- Bulgarie
- Chypre
- Croatie
- Danemark
- Espagne
- Estonie
- Finlande
- France
- Gibraltar
- Grèce
- Guernesey
- Hongrie
- Île de Man
- Irlande
- Islande
- Italie
- Jersey
- Lettonie
- Liechtenstein
- Lituanie
- Luxembourg
- Macédoine
- Malte
- Norvège
- Pays-Bas
- Pologne
- Portugal
- République tchèque
- Roumanie
- Royaume-Uni
- Russie
- Saint-Marin
- Serbie
- Slovaquie
- Slovénie
- Suède
- Suisse
- Ukraine

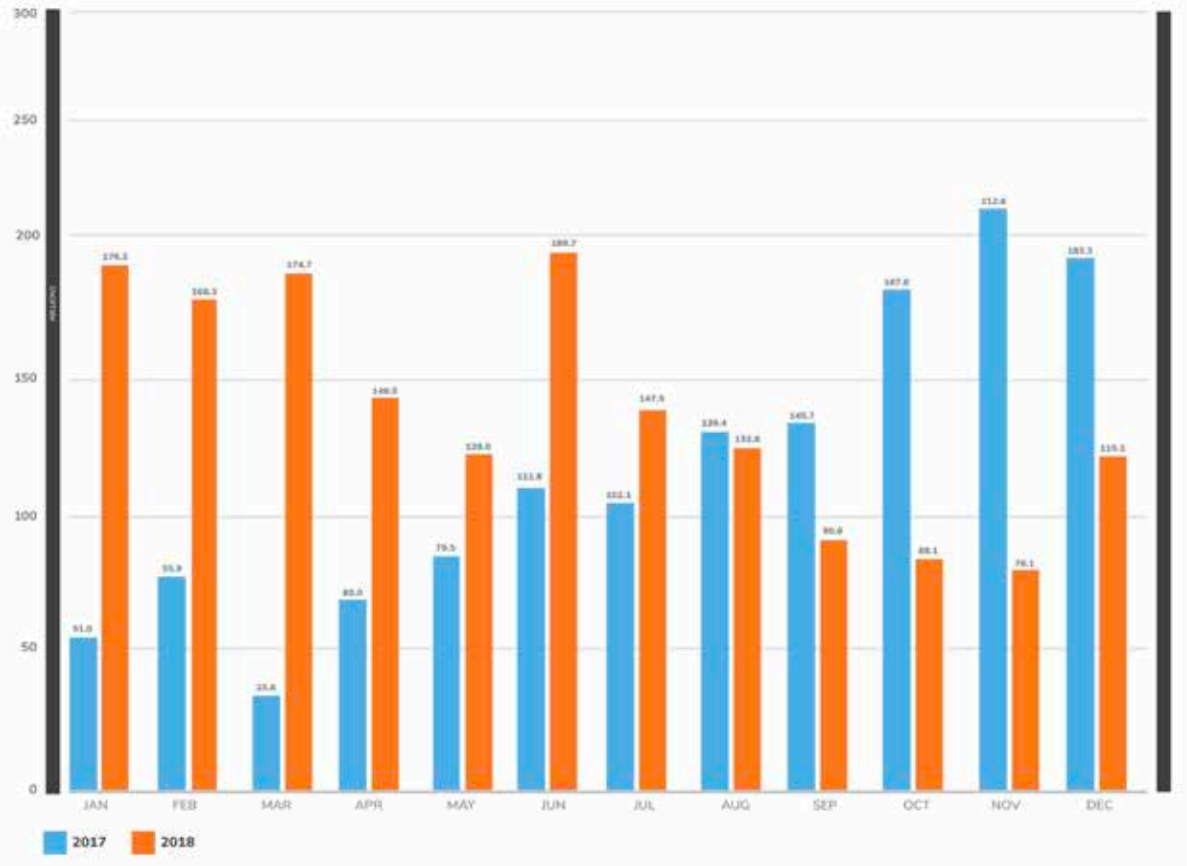
SONICWALL®

HAUSSE CONSTANTE DU VOLUME DES LOGICIELS MALVEILLANTS

En 2016, le secteur a connu une baisse du volume des logiciels malveillants, ce qui a conduit certains à spéculer sur le déclin global de la cybercriminalité. Depuis, **les attaques de logiciels malveillants ont augmenté de 33,4 %.**

Sur un plan international, SonicWall a enregistré 10,52 milliards* d'attaques de logiciels malveillants en 2018, un seuil encore jamais atteint. En Europe, SonicWall a identifié **1,64 milliard** d'attaques de logiciels malveillants, soit un pic de 23 % en 2017. Il est intéressant de noter que, malgré l'augmentation du volume en 2018, le volume d'attaques a commencé à baisser en juin 2018.

VOLUME EUROPÉEN DE LOGICIELS MALVEILLANTS EN 2018



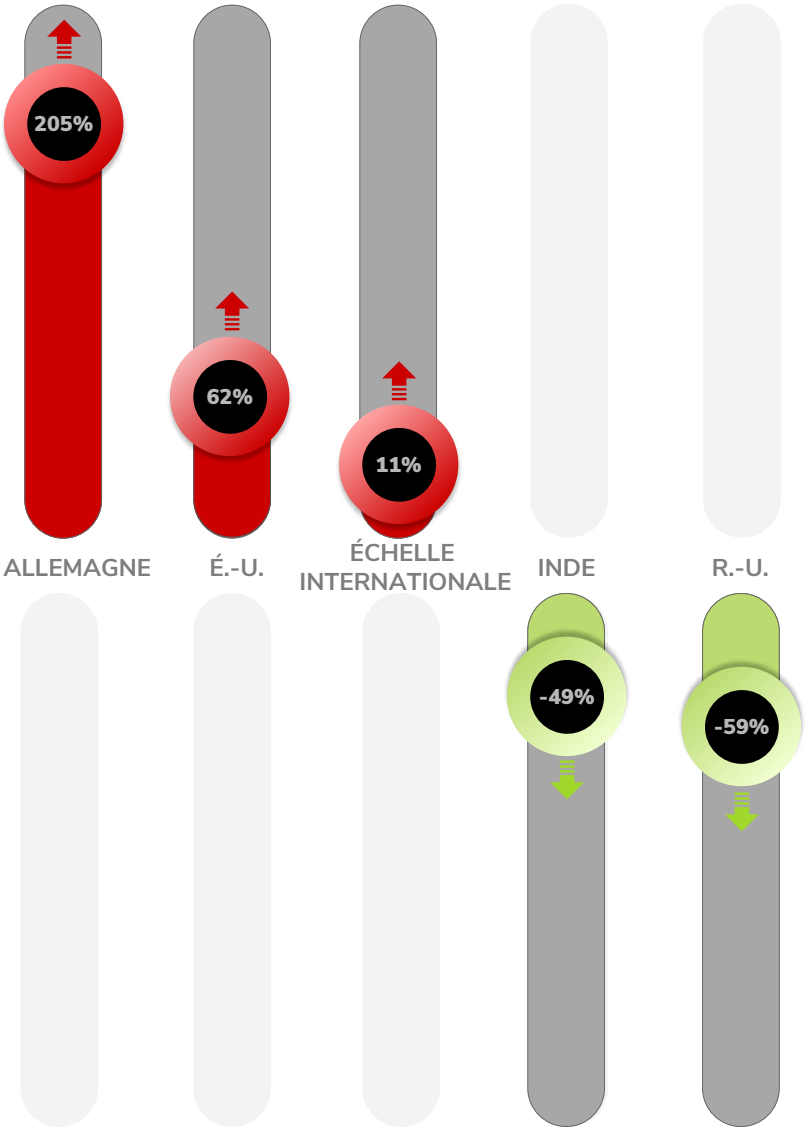
* Dans le cadre d'une bonne pratique, SonicWall optimise systématiquement ses méthodologies de collecte et d'analyse des données, ainsi que d'établissement de rapports. Cela consiste notamment à améliorer le nettoyage des données, modifier les sources de données et consolider les flux de menaces. Il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

LE ROYAUME-UNI ET L'INDE S'AGUERRISSENT FACE AUX ATTAQUES DE TYPE RANSOMWARE

L'analyse des données sur les menaces pour l'année 2018 par les spécialistes des menaces du Capture Labs de SonicWall s'est conclue par une révélation choquante : les attaques de type ransomware étaient en hausse dans presque toutes les régions géographiques, sauf deux : le Royaume-Uni et l'Inde.

Alors que les principaux pays d'Amérique du Nord, d'Europe et d'Asie observaient tous une augmentation des attaques de type ransomware, le **Royaume-Uni et l'Inde ont tranquillement fait face à des baisses respectives de 59 % et 49 %.**

À un niveau national, **l'Allemagne a été ciblée dans 27,6 % de toutes les attaques de type ransomware en Europe.** L'Italie (23 %), le Royaume-Uni (13,2 %), les Pays-Bas (10,7 %) et la France (9,9 %) complètent les principales cibles de cette zone géographique.



DES MENACES DANGEREUSES POUR LA MÉMOIRE ET DES ATTAQUES PAR CANAL AUXILIAIRE IDENTIFIÉES PRÉCOCEMENT

La solution RTDMI de SonicWall atténue les attaques dangereuses par canal auxiliaire en utilisant une technologie en attente de brevet. Ces canaux cachés constituent le vecteur fondamental utilisé pour exploiter et extraire les données sur les vulnérabilités des processeurs, comme Foreshadow, PortSmash, Meltdown, Spectre et Spoiler.

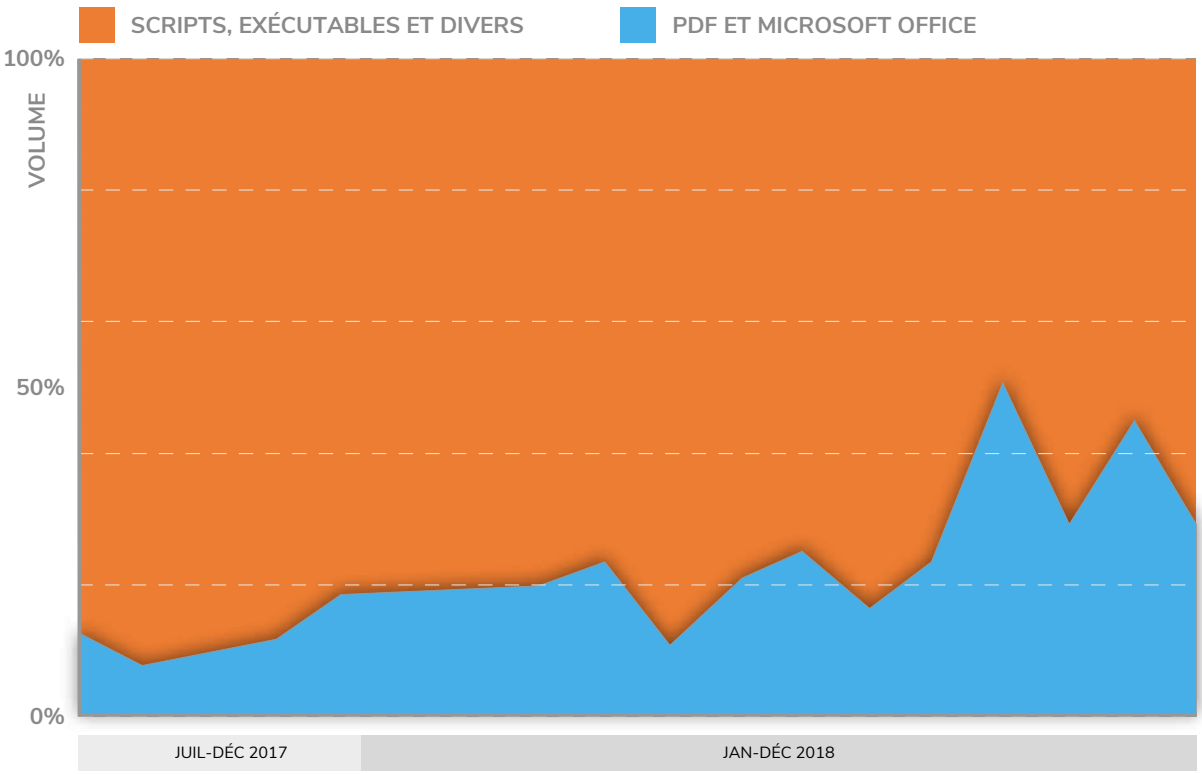
Malheureusement, les recherches actuelles montrent que **« Spectre n'est pas près de partir »** et reconnaissent que certaines vulnérabilités dans les processeurs ne peuvent pas être corrigées, que ce soit dans les logiciels ou le matériel, et qu'elles constituent un problème de sécurité beaucoup plus grave. À ce titre, les attaques par canal auxiliaire représenteront toujours un risque pour le paysage informatique, d'où la nécessité d'avoir recours à des technologies capables de les atténuer.

SONICWALL®

LES FICHIERS PDF ET MICROSOFT OFFICE MALVEILLANTS ONT LE DESSUS SUR LES CONTRÔLES DE SÉCURITÉ EXISTANTS

Les cybercriminels se servent de fichiers PDF et Microsoft Office fiables pour aider les logiciels malveillants à contourner les pare-feu traditionnels et même les technologies sandboxes à moteur unique.

AUGMENTATION DES FICHIERS PDF ET MICROSOFT OFFICE MALVEILLANTS



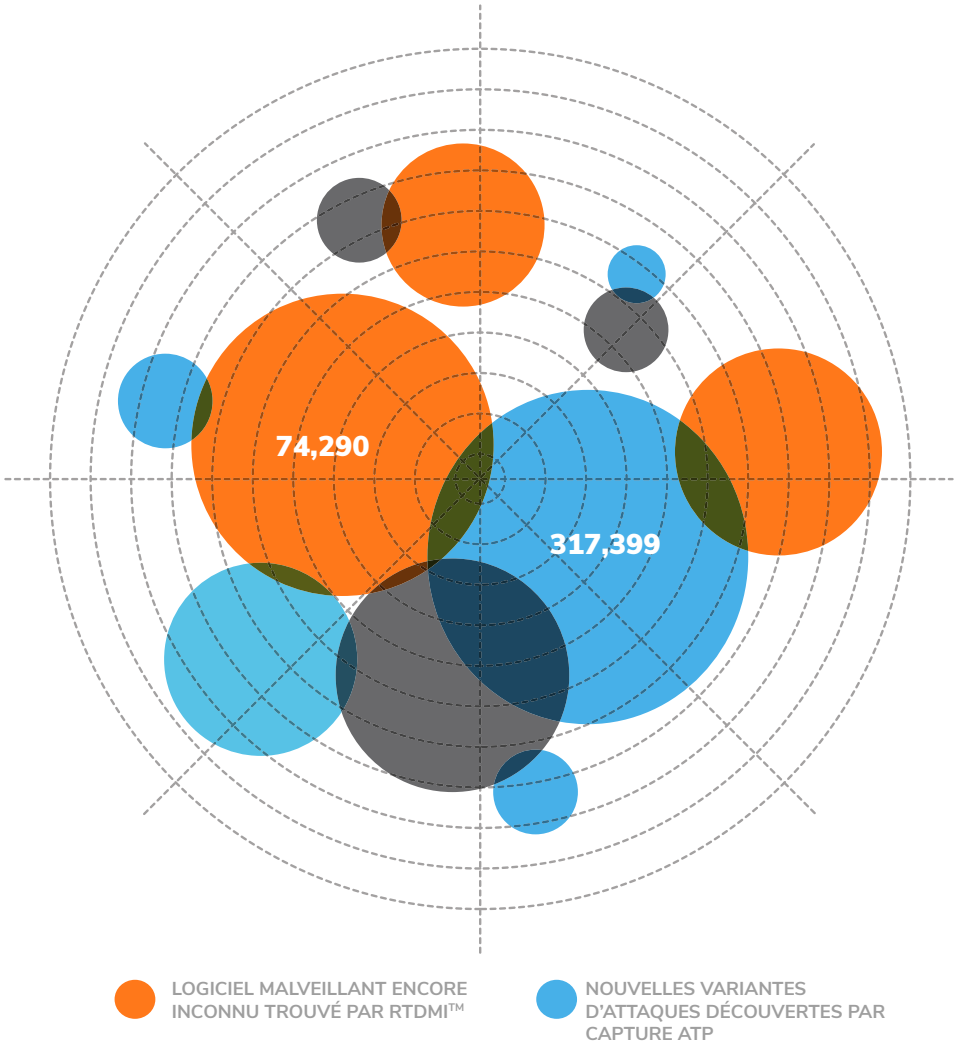
Le service sandbox multimoteur de Capture ATP de SonicWall a trouvé des **logiciels malveillants cachés dans 47 073 PDF et 50 817 fichiers Microsoft Office** en 2018. Bien que le volume semble faible à première vue, la plupart des contrôles de sécurité ne peuvent identifier et atténuer les logiciels malveillants cachés dans ces fichiers, augmentant considérablement le succès de la charge utile.

LA MATURATION DE L'APPRENTISSAGE AUTOMATIQUE POUR BLOQUER LES VARIANTES INÉDITES DE LOGICIELS MALVEILLANTS

SonicWall Capture Advanced Threat Protection (ATP) a identifié 391 689 nouvelles variantes d'attaques en 2018. C'est-à-dire en moyenne plus de **1 072 nouvelles attaques découvertes et bloquées chaque jour.**

Capture ATP exploite une technologie sandbox multimoteur basé sur le cloud parallèlement à la technologie RTDMI (Real-Time Deep Memory InpsectionTM) de SonicWall en attente de brevet. Ces deux fonctionnalités ont appris et se sont améliorées dynamiquement et automatiquement tout au long de 2018.

En effet, **RTDMI™ a identifié 74 290 attaques inédites en 2018**. Il s'agit de variantes de logiciels malveillants tellement nouvelles, uniques ou complexes qu'aucun autre fournisseur au monde n'a pu suivre ou créer des signatures pour elles au moment où SonicWall les a découvertes.

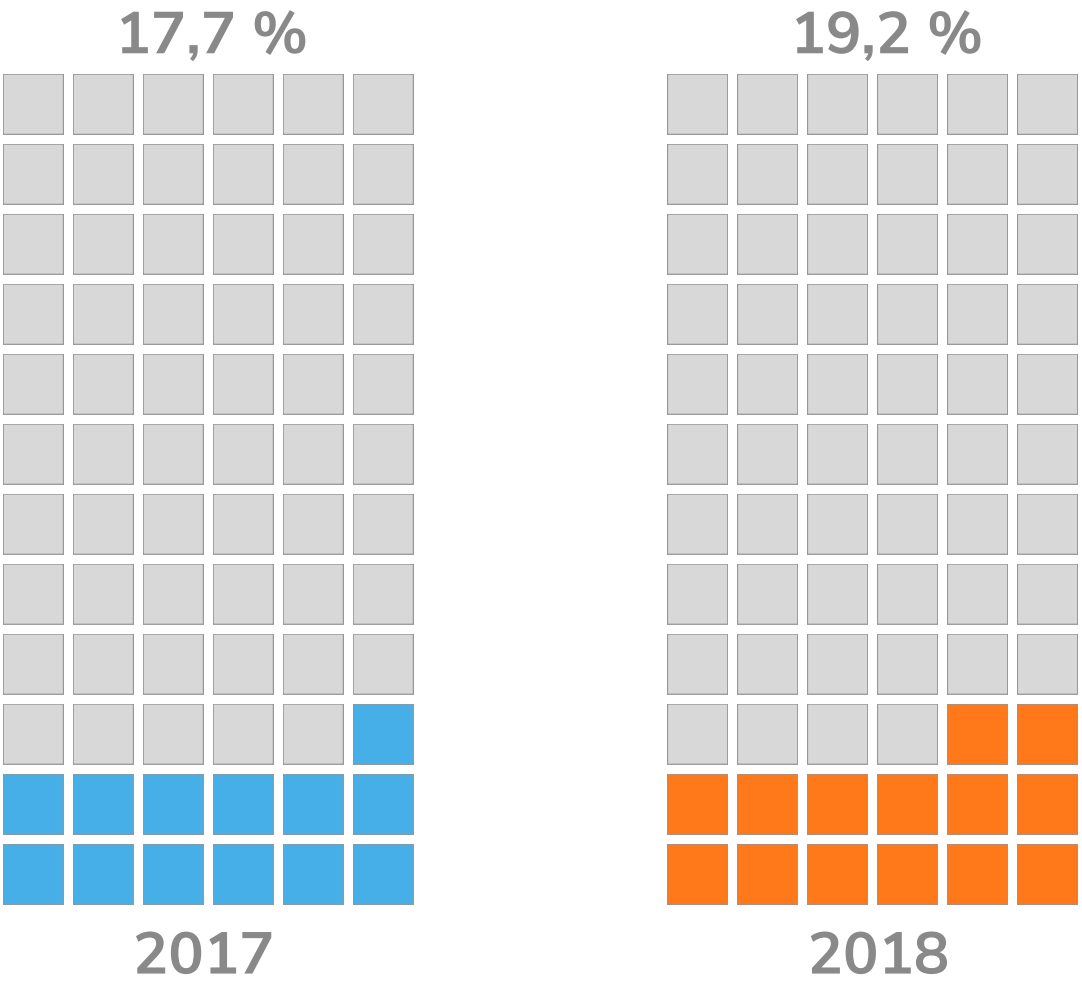


SONICWALL®

LES PORTS NON STANDARD SONT LES PROCHAINS SUR LA LISTE

Les ports 80 et 443 sont des ports standard pour le trafic web, c'est pourquoi la plupart des pare-feu y concentrent leur protection. En réponse, les cybercriminels ciblent les ports non standard pour s'assurer que leur charge utile peut être déployée sans être détectée dans un environnement cible.

ATTAQUES DE LOGICIELS MALVEILLANTS EN 2018
VISANT DES PORTS NON STANDARD



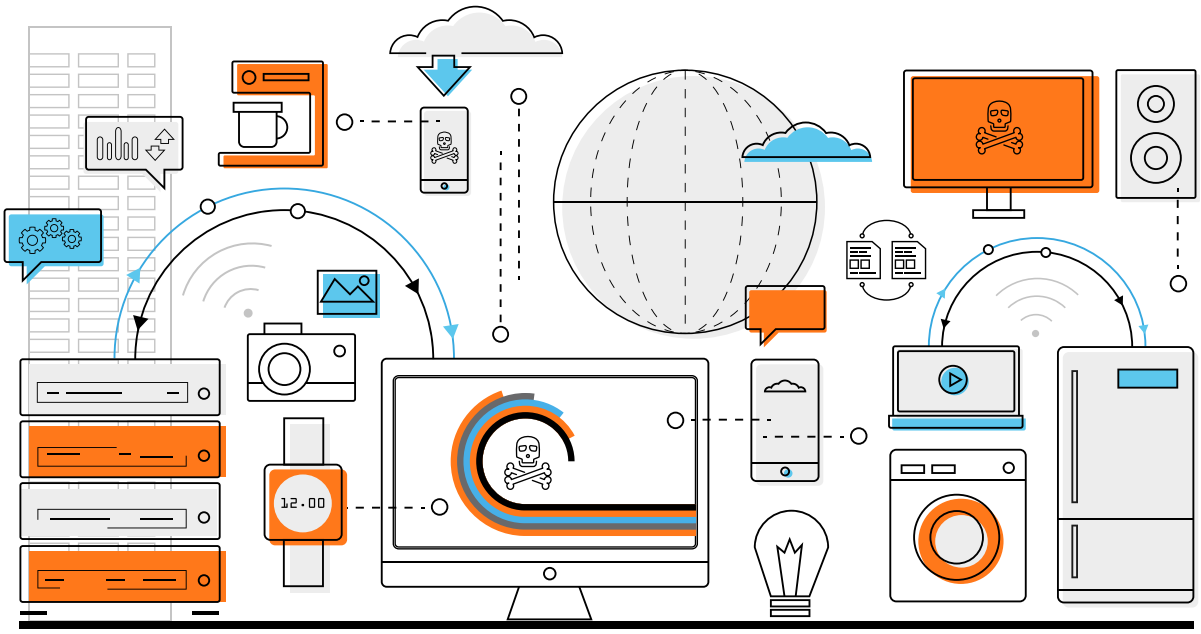
Sur la base d'un échantillon de plus de 700 millions d'attaques de logiciels malveillants, SonicWall a découvert que **19,2 % de toutes les attaques de logiciels malveillants transitaient par des ports non standard** en 2018. Les pare-feu traditionnels basés sur des proxys ne peuvent pas atténuer les attaques sur des ports non standard (pour le trafic chiffré et non chiffré) parce qu'ils sont trop nombreux pour pouvoir tous les surveiller.

SONICWALL®

ESCALADE DES ATTAQUES SUR l'IdO

Les consommateurs sont friands d'appareils connectés. Mais cet appétit a entraîné un déluge d'appareils compatibles avec l'Internet des Objets (IdO) hâtivement commercialisés, sans contrôles de sécurité appropriés. Dans de nombreux cas, les appareils IdO sont configurés avec des paramètres de sécurité par défaut, ce qui les rend vulnérables à la compromission par des identifiants connus ou des botnets puissants.

Au total, SonicWall a enregistré **32,7 millions d'attaques d'IdO en 2018**, soit une hausse de 217,5 % par rapport aux 10,3 millions d'attaques d'IdO enregistrées en 2017.



PROGRESSION CONSTANTE DES ATTAQUES CHIFFRÉES

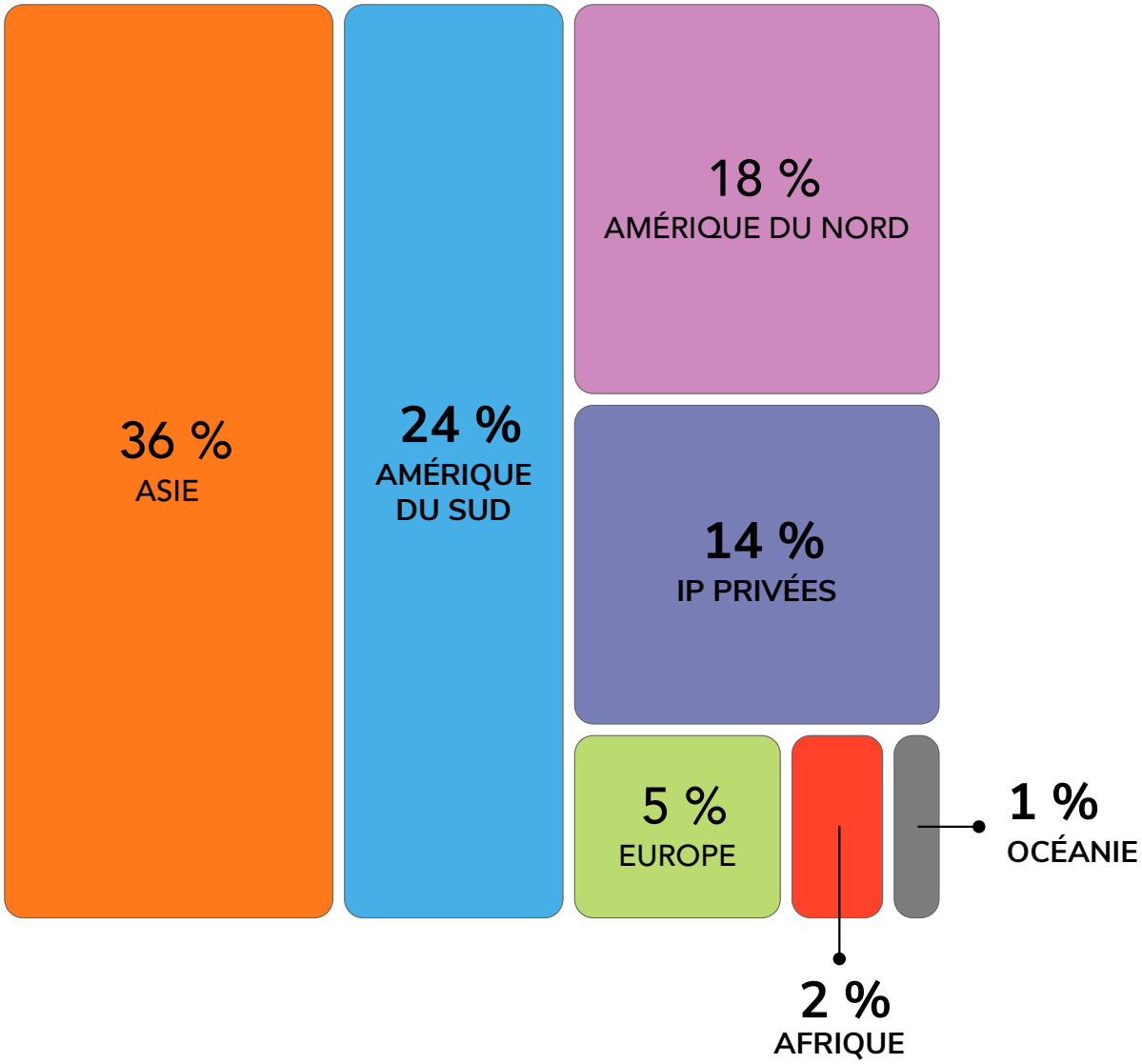
La croissance du trafic chiffré coïncide avec la multiplication des attaques dissimulées par un chiffrement TLS/SSL. Plus de **2,8 millions d'attaques ont été chiffrées** en 2018, soit une hausse de 27 % par rapport à 2017.

GRANDEUR ET DÉCADENCE DU CRYPTOJACKING

En 2018, le cryptojacking a disparu presque aussi vite qu'il n'était apparu. SonicWall a enregistré **57,5 millions d'attaques de cryptojacking** dans le monde entre avril et décembre. Le volume a atteint un pic en septembre avec 13,1 millions d'attaques enregistrées, mais est en baisse constante depuis.

Selon les données de SonicWall, l'Europe n'a été confrontée qu'à 5 % de toutes les attaques de cryptojacking internationales en 2018. Malgré la baisse des prix, les cryptomonnaies restent une précieuse marchandise pour les cybercriminels en raison de leur anonymat.

LE CRYPTOJACKING PAR RÉGION EN 2018



VOLUME GLOBAL DU PHISHING EN BAISSE, DES ATTAQUES PLUS CIBLÉES

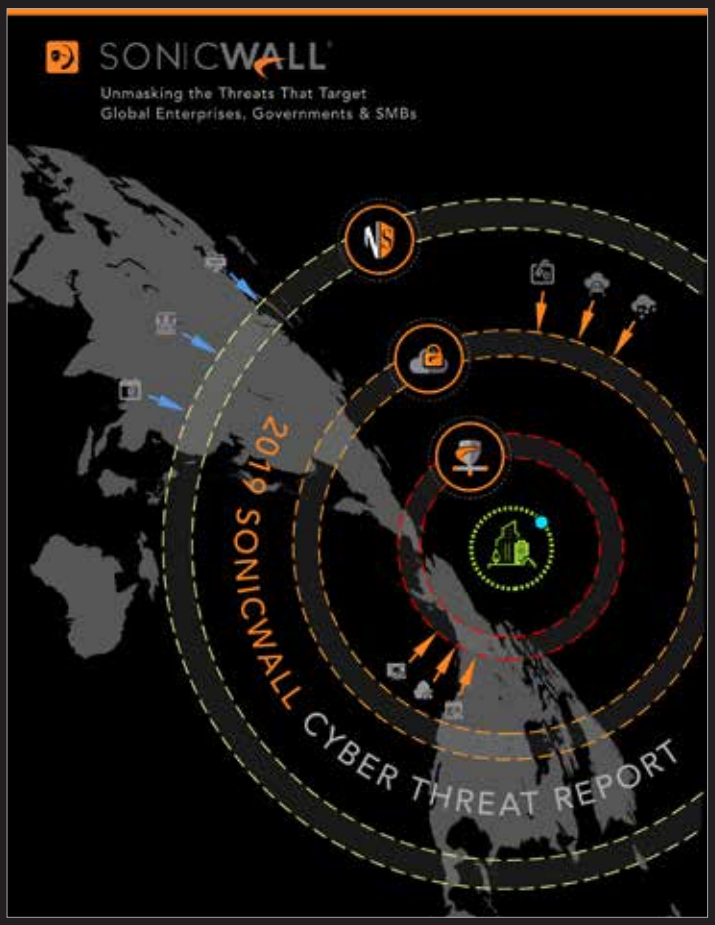
ATTAQUES DE PHISHING
À L'INTERNATIONAL **26 MILLIONS**

Alors que les entreprises s'efforcent de bloquer les attaques par e-mail et de s'assurer que les employés peuvent repérer et supprimer les e-mails suspects, les pirates informatiques changent de tactique. Ils réduisent le volume global des attaques et lancent des attaques de phishing plus ciblées (par ex., compromission d'e-mails professionnels, prises de contrôle de comptes, whaling ou pêche à la baleine pour cibler des cadres dirigeants par exemple, etc.).

En 2018, SonicWall a enregistré **26 millions d'attaques de phishing dans le monde**, soit une baisse de 4,1 % par rapport à 2017. Le client moyen de SonicWall a été confronté à 5 488 attaques de ce type en 2018.

Informations et analyses exclusives sur les cybermenaces. Exclusivement proposées par Capture Labs de SonicWall.

EN SAVOIR PLUS



Rendez-vous sur SonicWall.com/ThreatReport pour télécharger l'intégralité du Rapport 2019 SonicWall sur les cybermenaces. Vous découvrirez de nouveaux points de vue sur les stratégies d'attaque des cybercriminels et vous apprendrez comment défendre au mieux votre organisation ou entreprise contre les cyberattaques les plus sophistiquées.

* Dans le cadre d'une bonne pratique, SonicWall optimise systématiquement ses méthodologies de collecte et d'analyse des données, ainsi que d'établissement de rapports. Cela consiste notamment à améliorer le nettoyage des données, modifier 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 différent(e)s périodes, régions ou secteurs.

SONICWALL