

MISE À JOUR SEMESTRIELLE

2023

**RAPPORT SONICWALL
SUR LES
CYBERMENACES**

SUIVEZ LES
CYBERCRIMINELS
DANS L'OMBRE

SYNTHÈSE

CETTE SYNTHÈSE OFFRE UN EXCELLENT APERÇU DES PRINCIPALES CONCLUSIONS TIRÉES DE L'ANNÉE PASSÉE. POUR OBTENIR UNE ANALYSE PLUS APPROFONDIE DES DONNÉES EXCLUSIVES DE SONICWALL SUR LES MENACES, TÉLÉCHARGEZ LA MISE À JOUR COMPLÈTE

Au premier semestre 2023, les cybercriminels ont affiché une préférence pour des attaques plus calmes, se mettant à délaissier les ransomwares ou à les doubler de cryptojacking, de malwares IoT et de menaces chiffrées. Suite à l'intensification des mesures de répression, aux arrestations spectaculaires et au renforcement de la sécurité aux États-Unis, les auteurs des menaces se mettent également à cibler de nouveaux horizons et portent désormais leur attention sur des cibles de choix, très médiatisées, susceptibles de rapporter gros, ainsi que sur des cibles plus faciles à atteindre, comme les établissements d'enseignement. Alors que le paysage des menaces est en pleine évolution, SonicWall maintient sa surveillance tout au long de la seconde moitié de l'année 2023 et au-delà.

OBTENEZ LA MISE À JOUR COMPLÈTE

— sonicwall.com/threatreport



LA HAUSSE RECORD DU CRYPTOJACKING CONTINUE

En 2022, le volume de cryptojacking a pour la première fois excédé les 100 millions. Au cours des six premiers mois de 2023, les volumes d'attaques ont surpassé ce chiffre historique, voire presque *triplé*, ce qui représente 399 % d'augmentation pour un total de 332 millions. Si ce chiffre représente un record aujourd'hui inégalé, ce n'est pas encore terminé. Avec un tel rythme d'évolution – *ou même si cela ralentit considérablement* – les volumes de cryptojacking en 2023 sont sur le point de surpasser toutes les autres analyses des années précédentes portant sur ce type de menace *combinée*.

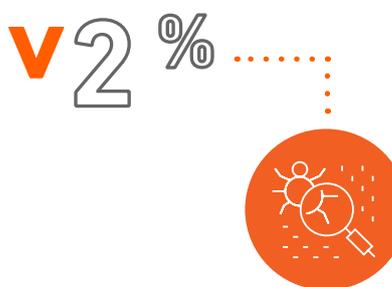
Les clients d'Amérique du Nord, les clients européens et les clients qui travaillent dans la fonction publique et dans l'enseignement ont enregistré d'énormes pics du volume de cryptojacking au cours du premier semestre.



LES RANSOMWARES EN REPLI, MAIS SUSCEPTIBLES D'UN REBOND

Les auteurs des menaces s'étant tournés vers des formes d'attaque plus furtives, les ransomwares ont continué de chuter au premier semestre 2023, avec une perte de 41 % à 140 millions. Pourtant, même avec cette diminution marquée, les ransomwares ne sont pas encore revenus à leurs niveaux pré-pandémie – et avec une augmentation de 74 % du volume d'attaques entre le premier et le deuxième trimestre, il semble probable qu'un rebond apparaisse au deuxième semestre.

Mais tandis que les volumes d'attaques sont globalement bas, les ransomwares poursuivent leur envolée chez certains clients, notamment en Allemagne et en Inde et dans la fonction publique.



LES LOGICIELS MALVEILLANTS CONTINUENT LEUR MIGRATION

Tandis que les *volumes* de logiciels malveillants restent globalement inchangés par rapport à la même période en 2022, le vrai changement réside dans le choix des cibles. Avec 1,3 milliards de cas (sur un total mondial de 2,7 milliards), les États-Unis restent l'épicentre mondial des logiciels malveillants. Cette région a toutefois été la seule à afficher une diminution, soit 12 % en moins en glissement annuel. À l'inverse, l'Europe et l'Amérique latine ont enregistré une croissance à deux chiffres, ce qui laisse supposer que les pirates continuent de porter leur attention vers de nouveaux horizons.

Les clients du secteur de l'enseignement et de la finance en particulier ont constaté de vastes augmentations des malwares, même si aucun de ces secteurs analysés n'a affiché de ralentissement.

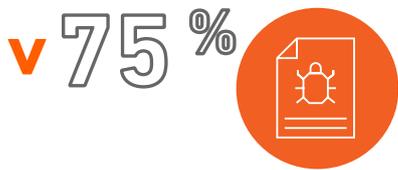
▲ 37 %



LES MALWARES IoT EXPLOSENT DE PLUS D'UN TIERS

Les malwares IoT ont continué de se répandre au premier semestre 2023, avec une hausse de 37 % pour atteindre 77,9 millions. Ce total représente un nouveau record ; l'année 2023 devrait facilement venir éclipser le record de l'année passée (112,3 millions). La tendance étant observée pour l'ensemble des logiciels malveillants, les malwares IoT ont affiché leur unique baisse en Amérique du Nord, où les volumes ont diminué de 3 % – elle a été facilement compensée par des pics à trois chiffres en Amérique latine et en Asie. L'Inde en particulier a été fortement touchée par ces attaques : le volume des malwares IoT y a atteint le chiffre astronomique de 311 %.

▼ 10 %



LES FICHIERS PDF ET OFFICE MALVEILLANTS AFFICHENT UNE BAISSÉ DE DEUX CHIFFRES

Les attaques impliquant des PDF malveillants ont diminué de 10 % au cours du premier semestre 2023, mais les fichiers Office malveillants ont connu une baisse bien plus importante : par rapport à la même période en 2022, ces attaques ont chuté de 75 %. Cette baisse peut s'expliquer en partie par les récents efforts de Microsoft pour renforcer la sécurité : l'avenir nous dira s'il s'agit d'une baisse durable ou si les cybercriminels parviennent à contourner les nouvelles restrictions.

▲ 21 %



HAUSSE GLOBALE DES TENTATIVES D'INTRUSION

Au premier semestre 2023, SonicWall a enregistré 3,7 billions de tentatives d'intrusion, soit plus 21% en glissement annuel. Mais si le volume total a augmenté, les tentatives de gravité moyenne à élevée ont globalement baissé de 7 %. Les clients du secteur de l'enseignement ont été visés à des rythmes largement supérieurs à ceux observés dans d'autres secteurs : environ 39 % d'entre eux ont subi une tentative chaque mois, soit davantage que la même période l'année précédente.

OBTENEZ LA MISE À JOUR
COMPLÈTE

sonicwall.com/threatreport

En tant que bonne pratique, SonicWall optimise régulièrement ses méthodes de collecte de données, d'analyse et de reporting. Cela implique notamment des améliorations dans le nettoyage des données, des changements de sources de données et la consolidation de flux de renseignements sur les menaces. Les chiffres publiés dans les rapports précédents peuvent avoir été ajustés sur différentes périodes, régions ou secteurs.

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, consultez notre site à l'adresse :

www.sonicwall.com ou suivez-nous sur [Twitter](#), [LinkedIn](#), [Facebook](#) et [Instagram](#).



SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035

SONICWALL®

© 2023 SonicWall Inc. TOUS DROITS RÉSERVÉS.

SonicWall est une marque commerciale ou déposée de SonicWall Inc. et/ou de ses filiales aux États Unis et et/ou dans d'autres pays. Toutes les autres marques commerciales et déposées sont la propriété de leurs sociétés respectives. Les informations contenues dans ce document sont fournies en relation avec les produits de SonicWall et/ou ses filiales. Aucune licence, expresse ou implicite, par estoppel ou un autre moyen, quant à un quelconque droit de propriété intellectuelle n'est accordée par le présent document ou en lien avec la vente de produits SonicWall.

2023-MidYearThreatReport-ExecSum-A4-JK-8743