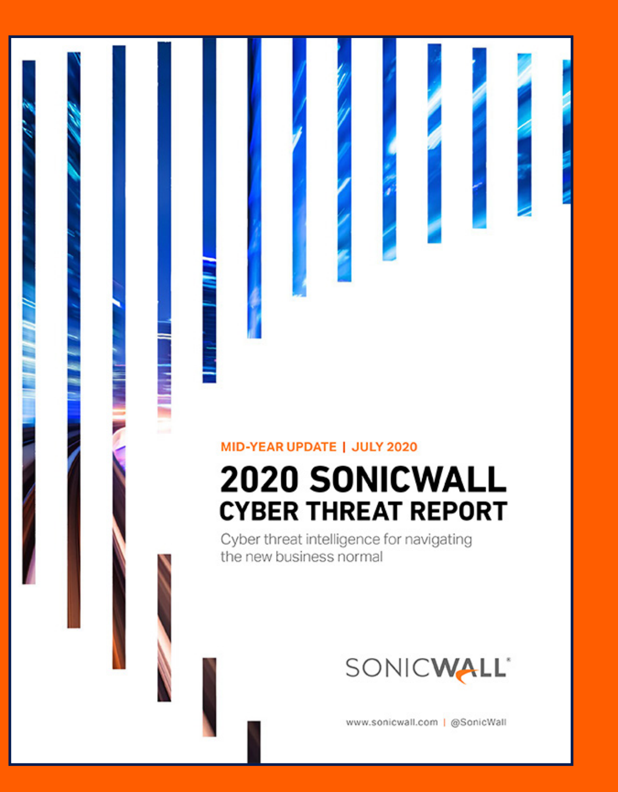
MISE À JOUR SEMESTRIELLE

RAPPORT SONICWALL 2020 SUR LES CYBERMENACES



#KnowTheThreats

OBTENEZ LA MISE À JOUR »

AU COURS DES SIX DERNIERS MOIS,

alors que la pandémie de COVID-19 a sévi dans le monde entier, nous avons vu des changements, qui, selon nous, auraient dû prendre des décennies, se produire quasiment du jour au lendemain.

Bien que cette perturbation historique ait été difficile pour les entreprises et les gouvernements, elle a été une véritable aubaine pour les cybercriminels.

121,4 millions de RANSOMWARES PLUS CHIRURGICAUX QUE JAMAIS.

Malgré une baisse globale des logiciels malveillants (-33 %), les ransomwares restent la charge utile de choix pour les cybercriminels. **Les attaques par ransomware ont augmenté de 20 % au premier semestre 2020 dans le monde**, et de 109 % aux États-Unis.

TIRER PROFIT DE LA PANDÉMIE.

SonicWall a commencé à voir des attaques, des escroqueries et des exploits spécifiquement basés sur le COVID-19 le 4 février ; depuis, **au moins 20 types différents d'attaques** ont été détaillés dans presque toutes les catégories, notamment :

- LOGICIEL MALVEILLANT
- RANSOMWARE
- CRYPTOMINEURS
- CHEVAUX DE TROIE
- CHEVAUX DE TROIE D'ACCÈS À DISTANCE (RAT)
- SPAM
- SCAREWARE ET AUTRES

« Ce n'était qu'une question de temps avant qu'un État-nation n'ait recours à la cybercriminalité pour influencer ou contrôler les soins de santé mondiaux en période de grand besoin. »

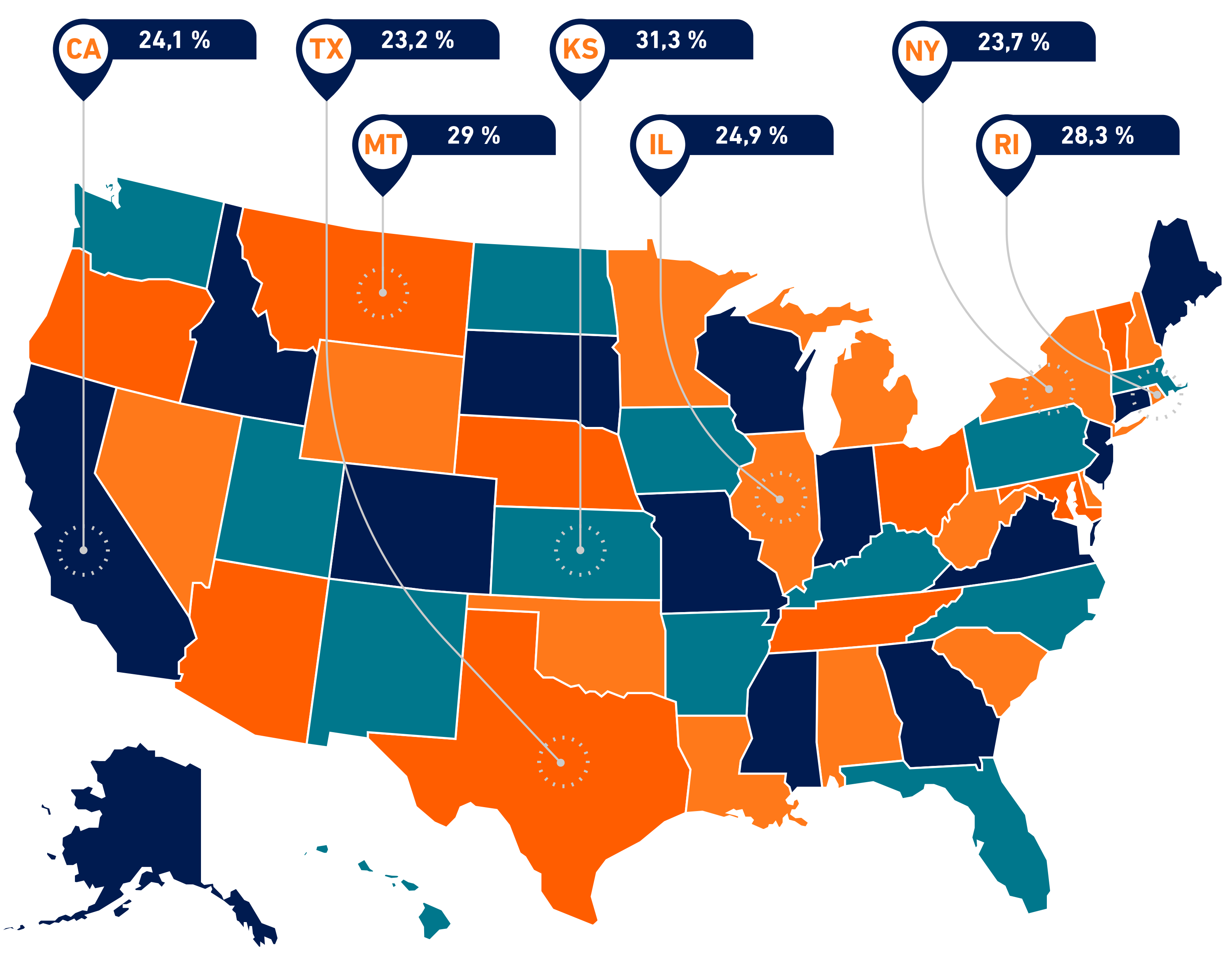
BILL CONNER | PRÉSIDENT et PDG | SONICWALL | NEWSWEEK INTERNATIONAL, 16 JUILLET 2020

CERTAINES RÉGIONS PEUVENT ETRE PLUS MENACÉES QUE D'AUTRES

Aux États-Unis, la Californie a de loin enregistré le plus grand nombre d'atteintes de logiciels malveillants (**304,1 millions** au total). Ce n'est toutefois pas l'État le plus à risque, loin de là.

En réalité, une entreprise est plus susceptible de rencontrer des logiciels malveillants au Kansas, où près d'un tiers (31,3 %) des capteurs SonicWall ont enregistré une atteinte.

% des capteurs SonicWall qui ont enregistré des atteintes de logiciels malveillants par État



IOWA 28,1 %
HAWAII 27,7 %
VIRGINIE OCCIDENTALE 27,4 %
VERMONT 27,2 %
IDAHO 27,2 %
LOUISIANE 27,2 %
FLORIDE 26,7 %
VIRGINIE 26,6 %
OREGON 26,5 %
NOUVEAU MEXIQUE 26,4 %
MICHIGAN 26,3 %
NEBRASKA 26,3 %
NEW JERSEY 26,3 %
PENNSYLVANIE 26,1 %
NEVADA 26 %
MARYLAND 26 %

79 %

LES RANSOMWARES SONT LA PRÉOCCUPATION NUMÉRO UN.

Lorsqu'on leur demande quel type de cyberattaques a influencé leur décision d'acheter un pare-feu SonicWall TZ, 79 % des entreprises sondées ont cité les ransomwares.

SOURCE : ENQUÊTE TECHVALIDATE AUPRÈS DE 250 CLIENTS DE LA SÉCURITÉ DU RÉSEAU SONICWALL

+176 %

QU'EST-CE QUI SE CACHE DANS VOS FICHIERS DE BUREAU ?

De plus en plus de logiciels malveillants sont dissimulés dans des fichiers Office de confiance. Au premier semestre 2020, SonicWall a enregistré une augmentation de 176 % des tout nouveaux fichiers Office malveillants. Voir le rapport complet pour plus de détails >

#WFH PIC D'ATTAQUES SUR L'IdO.

Depuis janvier, SonicWall a enregistré 20,2 millions d'attaques sur l'IdO ou Internet des objets/appareils connectés, soit un pic de 50 % depuis le début de l'année. Si le schéma actuel se maintient, le total des attaques sur l'IdO dépassera les niveaux de 2018 et 2019. Les appareils IdO non contrôlés peuvent offrir aux cybercriminels une porte ouverte sur ce qui serait autrement une entreprise bien sécurisée.

+50 % D'ATTAQUES sur L'IdO

DEPUIS LE DÉBUT DE L'ANNÉE

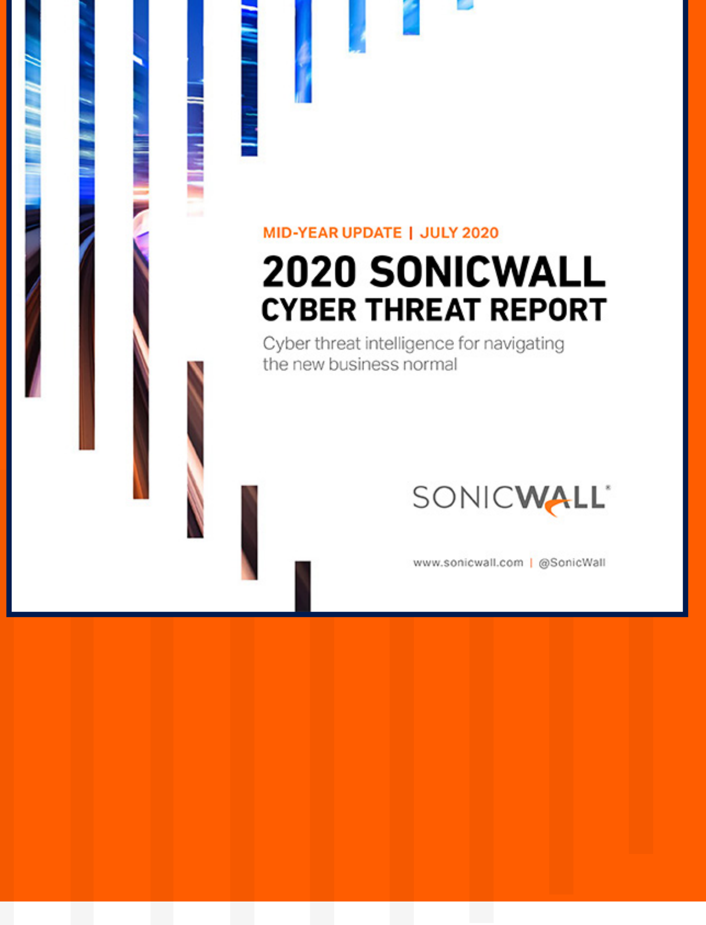
TENDANCES MONDIALES DES CYBERATTAQUES

41,4 millions d'attaques de cryptojacking

+19 % d'intrusions

1 client sur 12 a connu une attaque cryptée

PROSPÉREZ DANS LA NOUVELLE REALITÉ DES AFFAIRES.



Visitez **SonicWall.com/ThreatReport** pour télécharger la mise à jour semestrielle gratuite du rapport SonicWall 2020 sur les cybermenaces. Obtenez les dernières informations sur les cybermenaces pour mieux naviguer la nouvelle réalité des affaires.

OBTENEZ LA MISE À JOUR »

#KnowTheThreats

SONICWALL
CAPTURE LABS

SonicWall.com

*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 ajuster 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.

Infographic-2020ThreatReportMidYear-COG-2452