****

**Sophos:  
“Payer la rançon double le coût de la récupération après une attaque de ransomware”**

* *Une enquête mondiale montre que le coût moyen de la récupération est de €1,3 million si les entreprises paient la rançon, €675 000 si elles ne le font pas.*
* *En Belgique, 59% des personnes interrogées ont été attaquées par des ransomwares au cours de l'année écoulée; jusqu'à un tiers (32%) ont payé une rançon lorsque leurs données ont été chiffrées; Les coûts de réparation belges s'élèvent en moyenne à 340 000 €*
* *Le secteur public est le moins touché par les ransomwares*

OXFORD, Royaume-Uni - 12 mai 2020 – **Sophos a annoncé aujourd'hui les résultats de son enquête mondiale,** [**The State of Ransomware 2020**](https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/?url=%2fen-us%2fmedialibrary%2fGated-Assets%2fwhite-papers%2fsophos-the-state-of-ransomware-2020-wp.pdf)**, qui révèle que payer des cybercriminels pour restaurer des données chiffrées lors d'une attaque de ransomware n'est pas un choix facile et peu coûteux. En fait, le coût total de la récupération double presque lorsque les entreprises paient une rançon. L'enquête a interrogé 5 000 décideurs informatiques dans des organisations de 26 pays sur six continents, dont l'Europe, les Amériques, l'Asie-Pacifique et l'Asie centrale, le Moyen-Orient et l'Afrique.**

Plus de la moitié (51%) des entreprises ont subi une attaque de ransomware importante au cours des 12 derniers mois, contre 54% en 2017. Les données ont été chiffrées dans près des trois quarts (73%) des attaques qui ont réussi à atteindre l’entreprise. Le coût moyen de la gestion de l'impact d'une telle attaque, y compris les temps d'arrêt des affaires, les pertes de commandes, les coûts d'exploitation, etc., mais sans compter la rançon, était de plus de 675 000 euros. Ce coût moyen a atteint 1,3 million d’euros, soit près du double, lorsque les entreprises ont payé la rançon. Plus du quart (27%) des organisations touchées par des ransomwares ont admis avoir payé la rançon.

Cependant, contrairement à la croyance populaire, le secteur public a été le moins touché par les ransomwares, avec seulement 45% des organisations interrogées dans cette catégorie déclarant avoir été frappées par une attaque importante l'année précédente. Au niveau mondial, les entreprises de médias, de loisirs et de divertissement du secteur privé ont été les plus touchées par les ransomwares, 60% des répondants ayant signalé des attaques.

« Les entreprises peuvent ressentir une pression intense pour payer la rançon afin d'éviter des temps d'arrêt dommageables. À première vue, le paiement de la rançon semble être un moyen efficace de restaurer les données, mais c'est illusoire. Les résultats de Sophos montrent que le paiement de la rançon fait peu de différence avec la charge de récupération en termes de temps et de coût. Cela peut être dû au fait qu'il est peu probable qu'une seule clé de déchiffrement magique soit tout ce qui est nécessaire pour récupérer. Souvent, les attaquants peuvent partager plusieurs clés et les utiliser pour restaurer des données peut être une affaire complexe et longue », a déclaré Chester Wisniewski, chercheur principal, Sophos.

Plus de la moitié (56%) des responsables informatiques interrogés ont pu récupérer leurs données à partir de sauvegardes sans payer la rançon. Dans une très petite minorité de cas (1%), le paiement de la rançon n'a pas conduit à la récupération des données. Ce chiffre est passé à 5% pour les entreprises du secteur public. En fait, 13% des organisations du secteur public interrogées n'ont jamais réussi à restaurer leurs données chiffrées, contre 6% dans l'ensemble.

**Ransomware: la situation en Belgique**100 entreprises belges ont participé à l'étude The State of Ransomware 2020: 59% des répondants ont indiqué qu'ils avaient été victimes d'une attaque de ransomware au cours de l'année écoulée. De ce groupe, 23% ont pu réagir avant que les données puissent être cryptées. Environ un tiers des entreprises (32%) dont les données ont été cryptées ont payé la rançon. En Belgique, le coût moyen d’une réparation était d'environ 340 000 €. Enfin, il a été demandé aux entreprises belges si elles étaient assurées contre la cybersécurité: 81% ont indiqué l’être. 69% de ce groupe ont également une assurance spécifique contre les ransomwares.

**Les attaquants augmentent la pression pour payer**

Les chercheurs des SophosLabs ont publié un nouveau rapport, [Maze Ransomware: Extorting Victims for 1 Year and Counting](https://news.sophos.com/en-us/2020/05/12/maze-ransomware-1-year-counting/), qui examine les outils, techniques et procédures utilisés par cette menace avancée qui combine le chiffrement des données avec le vol d'informations et la menace d'exposition. Cette approche, que les chercheurs de Sophos ont également observée être adoptée par d'autres familles de ransomwares, comme LockBit, est conçue pour augmenter la pression sur la victime pour qu'elle paie la rançon. Le nouveau rapport Sophos aidera les professionnels de la sécurité à mieux comprendre et anticiper les comportements évolutifs des attaquants ransomwares et à protéger leurs organisations.

«Un système de sauvegarde efficace qui permet aux entreprises de restaurer des données chiffrées sans payer les attaquants est essentiel pour l'entreprise, mais il y a d'autres éléments importants à considérer si une entreprise veut être vraiment résister aux ransomwares», a ajouté Wisniewski. "Les adversaires avancés comme les opérateurs derrière le rançongiciel Maze ne se contentent pas de crypter les fichiers, ils volent des données à des fins d'exposition ou d'extorsion. Nous avons récemment signalé que LockBit utilisait cette tactique. Certains attaquants tentent également de supprimer ou de saboter les sauvegardes pour rendre plus difficile pour les victimes de récupérer des données et augmenter la pression sur elles pour payer. La façon de faire face à ces manœuvres malveillantes consiste à garder les sauvegardes hors ligne et à utiliser des solutions de sécurité efficaces et multicouches qui détectent et bloquent les attaques à différentes étapes. »

**Selon l’enquête**

De plus amples informations sur le rançongiciel Maze sont disponibles dans le rapport sur les SophosLabs Uncut.

L'enquête State of Ransomware 2020 a été réalisée par Vanson Bourne, spécialiste indépendant des études de marché, en janvier et février 2020. L'enquête a interrogé 5 000 décideurs informatiques dans 26 pays, aux États-Unis, au Canada, au Brésil, en Colombie, au Mexique, en France, Allemagne, Royaume-Uni, Italie, Pays-Bas, Belgique, Espagne, Suède, Pologne, République tchèque, Turquie, Inde, Nigéria, Afrique du Sud, Australie, Chine, Japon, Singapour, Malaisie, Philippines et EAU. Tous les répondants provenaient d'entreprises comptant entre 100 et 5 000 employés.

**À propos de Sophos**En tant que leader mondial en solutions de cybersécurité Next-Gen, Sophos protège plus de 400 000 entreprises, de toutes tailles et dans plus de 150 pays, contre les cybermenaces actuelles les plus avancées. Développées par les SophosLabs, une équipe présente dans le monde entier et spécialisée dans le renseignement sur les menaces et la science des données, les solutions Cloud-Native et basées sur l'IA de Sophos protègent les systèmes endpoint (les ordinateurs portables, les serveurs et les périphériques mobiles) ainsi que les réseaux contre les techniques de cyberattaque évolutives, notamment les ransomwares, les malwares, les exploits, l'exfiltration de données, les violations par adversaire-actif, le phishing, et bien plus encore.

Sophos Central, une plateforme de management Cloud-Native, intègre l'ensemble des produits Next-Gen de Sophos, y compris la solution Intercept X endpoint et le pare-feu XG Next-Gen, via un système unique de «sécurité synchronisée» accessible via un ensemble d'API. Sophos a favorisé la transition vers une cybersécurité moderne en exploitant des fonctionnalités avancées au niveau du Cloud, de l'apprentissage automatique, des API, de l'automatisation, du service MTR (Managed Threat Response), entre autres, afin d’offrir une protection de niveau professionnel à toutes les entreprises. Sophos commercialise ses produits et services exclusivement par l’intermédiaire d’un réseau mondial regroupant plus de 47 000 partenaires et fournisseurs de services gérés (MSP : Managed Service Provider). Sophos met également ses technologies commerciales innovantes à la disposition des particuliers via Sophos Home. Le siège de l’entreprise est basé à Oxford, au Royaume-Uni, et Sophos est cotée à la Bourse de Londres sous le symbole «SOPH». Plus d'informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contact presse :**  
Square Egg Communications, Sandra Van Hauwaert, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497251816.