**« Le coût lié à la reprise d’activité après une attaque par ransomware a plus que doublé par rapport à l’année dernière, atteignant désormais plus de 1,5 million d’euros »**

* *L’étude révèle que seules 8 % des entreprises ayant versé une rançon ont été en mesure de restaurer l’ensemble de leurs données*
* *54 % des répondants déclarent que les cyberattaques sont trop sophistiquées pour que leurs équipes IT puissent y faire face par elles-mêmes*

**Oosterhout, le 27 avril 2021** – [Sophos](https://www.sophos.com/fr-fr.aspx) annonce la publication des résultats de son étude internationale intitulée [*Etat des Ransomwares 2021*](http://www.sophos.com/ransomware2021). Celle-ci révèle que le coût moyen total de reprise d’activité après une attaque par ransomware a plus que doublé en un an, passant de 631 000 euros en 2020 à 1,54 million d’euros en 2021. Le montant moyen de rançon versé s’élève à 141 000 euros. Les résultats montrent également que seules 8 % des entreprises dans le monde sont parvenues à restaurer l’ensemble de leurs données après versement de la rançon et que 29 % d’entre elles en récupèrent au mieux la moitié.

Dans le cadre de cette étude, 5 400 décideurs IT ont été interrogés. Ils sont issus d’entreprises de taille moyenne réparties dans 30 pays situés dans les zones géographiques suivantes : Europe, Amérique, Asie-Pacifique et Asie centrale, Moyen-Orient et Afrique.

Le nombre d’entreprises victimes d’attaques par ransomware est passé de 51 % en 2020 à 37 % en 2021. De plus, elles sont de moins en moins nombreuses à souffrir d’un chiffrement de données qui découle d’une attaque de grande ampleur (54 % en 2021 par rapport à 73 % en 2020). Néanmoins, les résultats de l’enquête ont mis en lumière un certain nombre de tendances à la hausse qui peuvent paraître inquiétantes, en particulier celles qui concernent l’impact d’une attaque par ransomware.

« La diminution apparente du nombre d’entreprises ayant subi une attaque par ransomware est une bonne nouvelle, mais celle-ci est tempérée par le fait que cela indique probablement des changements dans le comportement des cybercriminels, du moins en partie, » déclare Chester Wisniewski, principal reasearch scientist chez Sophos. « Nous avons constaté que les attaquants sont passés d’attaques de grande ampleur, génériques et automatisées à des attaques plus ciblées, telles que des actes de piratages menés par des êtres humains qui mettent la “main au clavier‌”. Par conséquent, si le nombre total d’attaques est moins élevé, notre expérience nous montre que les dégâts potentiels causés par ces attaques ciblées, plus sophistiquées et plus complexes, sont beaucoup plus importants. Il est également plus difficile de se remettre de ces attaques et cela se reflète dans les résultats de l’étude, avec le doublement du coût total lié à la remédiation. »

Parmi les principales conclusions de l’étude *Etat des Ransomware 2021* figurent les éléments suivants :

* Le coût moyen de réduction de l’impact d’une attaque par ransomware a plus que doublé au cours des 12 derniers mois. Les coûts de remédiation moyens, qui incluent les temps d’arrêts, les commandes perdues, les coûts opérationnels et de nombreux autres paramètres, sont passés de 631 000 euros en 2020 à 1 540 000 euros en 2021. Ainsi, le coût moyen de reprise d’activité après une attaque par ransomware est désormais presque 10 fois plus important que le montant moyen des rançons versées.
* Le montant moyen des rançons versées est de 141 000 euros.
* Le nombre d’entreprises qui paient une rançon a augmenté, passant de 26 % en 2020 à 33 % en 2021, même si moins d’une sur dix (8 %) est parvenue à restaurer l’ensemble de ses données

« Ces résultats attestent d’une réalité crue : en matière de ransomware, verser une rançon n’est pas la solution gagnante. Même si de plus en plus d’entreprises acceptent de payer les sommes exigées, seule une minorité d’entre elles ont été en mesure de restaurer l’ensemble de leurs données, » ajoute Chester Wisniewski. « Cela pourrait être en partie dû à la complexité liée à l’utilisation de clés de déchiffrement pour récupérer les informations. De plus, il n’y aucune garantie de réussite. Par exemple, comme nous l’avons récemment constaté avec les ransomwares [DearCry](https://news.sophos.com/en-us/2021/03/15/dearcry-ransomware-attacks-exploit-exchange-server-vulnerabilities/) et [Black Kingdom](https://news.sophos.com/en-us/2021/03/23/black-kingdom/), les attaques lancées à l’aide de codes de mauvaise qualité ou compilés à la hâte peuvent rendre difficile, voire impossible, toute restauration des données. »

* Plus de la moitié (54 %) des répondants pensent que les cyberattaques sont désormais trop sophistiquées pour que leurs équipes IT puissent y faire face par elles-mêmes.
* L’extorsion sans chiffrement est en hausse. Une petite partie, quoique non négligeable (7 %), des décideurs IT interrogés déclare que les données de leur entreprise n’ont pas été chiffrées, mais qu’ils ont néanmoins reçu une demande de rançon, possiblement parce que les attaquants sont parvenus à dérober leurs informations. En 2020, ils n’étaient que 3 %.

« Il faut parfois des années pour se remettre d’une attaque par ransomware, car cela est loin de concerner seulement le déchiffrement et la restauration des données, » poursuit Chester Wisniewski. « Des systèmes entiers doivent être reconstruits à partir de rien et il faut aussi tenir compte des temps d’arrêt de l’activité, de l’impact pour les clients, ainsi que de bien d’autres paramètres. De plus, la définition de ce qui constitue une attaque par ransomware évolue. Pour une petite minorité non négligeable de personnes interrogées, les attaques ont été accompagnées d’une demande de rançon sans chiffrement de données. Cela pourrait être dû au fait qu’ils disposaient de technologies anti-ransomwares qui ont bloqué la phase de chiffrement des données ou bien que les attaquants ont simplement décidé de ne pas les chiffrer. Il est probable que les criminels aient exigé un paiement en échange de la promesse de ne pas publier les informations dérobées en ligne. Pour citer un [exemple](https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/) récent de ce type de méthode, le groupe d’opérateurs de ransomware Clop, en association avec un acteur connu du monde des menaces motivé par l’appât du gain, a fait près d’une douzaine de victimes présumées en se livrant à des attaques qui reposaient exclusivement sur l’extorsion.

En somme, il est plus essentiel que jamais de se protéger contre les criminels qui se tiennent à l’affût avant que ceux-ci ne puissent pénétrer les défenses et déployer leurs attaques de plus en plus multiformes. Heureusement, lorsque les entreprises sont victimes d’une attaque, elles ne sont pas forcées d’y faire face seules. Un service d’accompagnement est disponible 24h/24 et 7j/7, sous la forme de centres d’opérations et de sécurité (SOC) externes, d’une chasse aux menaces menée par des experts et de [services de réponse en cas d’incident](https://www.sophos.com/en-us/products/managed-threat-response/rapid-response.aspx). »

**À propos de Sophos**

En tant que leader mondial en solution 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, le phishing, et bien plus encore. Sophos Central, la 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 commercialise ses produits et services exclusivement par l’intermédiaire d’un réseau mondial regroupant plus de 53 000 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. Plus d'informations sont disponibles sur [www.sophos.com](http://www.sophos.com).

**Contacts presse :**

Sandra Van Hauwaert, Square Egg Communications, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497 251816.