SOPHOS
Cybersecurity evolved.

L'état des ransomwares 2021

L'enquête annuelle de Sophos offre de nouvelles perspectives sur l'impact des ransomwares sur les entreprises de taille moyenne dans le monde entier. Elle explore tout particulièrement la prévalence des attaques et leur impact sur les victimes, et compare les tendances d'une année sur l'autre. Cette année, pour la première fois, l'enquête révèle l'ampleur des sommes payées par les victimes, ainsi que la proportion de données que les victimes récupèrent après avoir payé.

Un livre blanc Sophos. Avril 2021

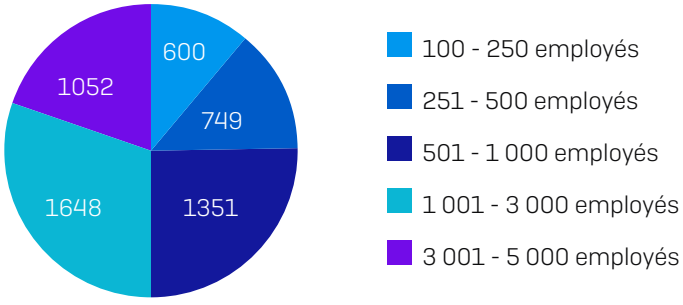
À propos de l'enquête

Sophos a chargé le cabinet d'étude indépendant Vanson Bourne d'interroger 5 400 décideurs informatiques dans 30 pays. Cette enquête s'est déroulée entre janvier et février 2021.

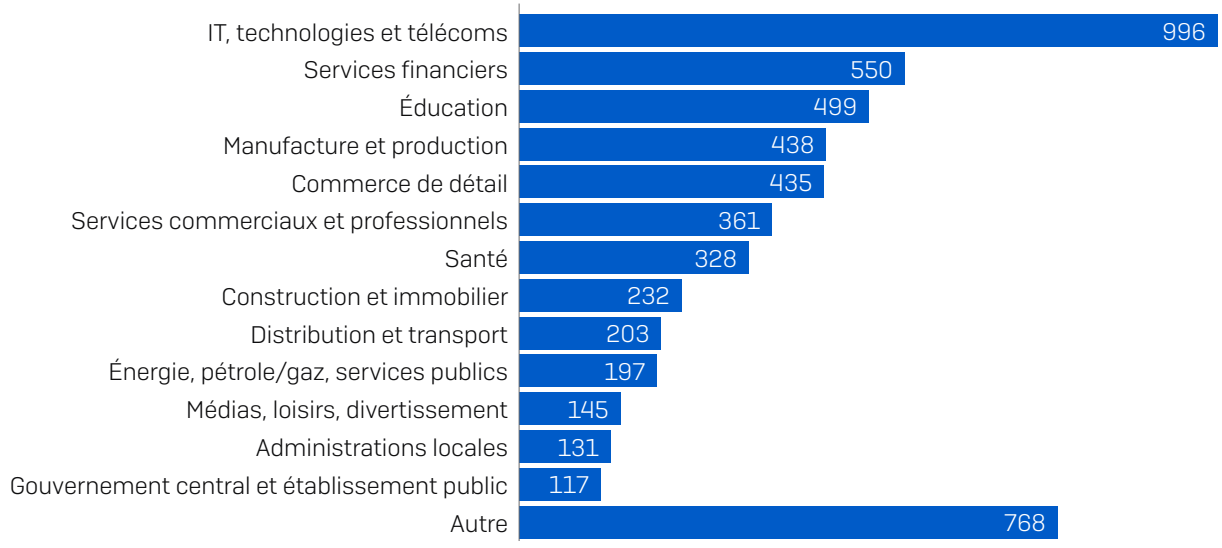
PAYS	NB DE RÉPONDANTS	PAYS	NB DE RÉPONDANTS	PAYS	NB DE RÉPONDANTS
Australie	250	Inde	300	Arabie Saoudite	100
Autriche	100	Israël	100	Singapour	150
Belgique	100	Italie	200	Afrique du Sud	200
Brésil	200	Japon	300	Espagne	150
Canada	200	Malaisie	150	Suède	100
Chili	200	Mexique	200	Suisse	100
Colombie	200	Pays-Bas	150	Turquie	100
République tchèque	100	Nigeria	100	EAU	100
France	200	Philippines	150	Royaume-Uni	300
Allemagne	300	Pologne	100	États-Unis	500

Comme chaque année, 50 % des personnes interrogées dans chaque pays proviennent d'entreprises de 100 à 1 000 employés et 50 % d'entreprises de 1 001 à 5 000 employés. Les répondants provenaient de secteurs industriels variés.

Combien d'employés votre entreprise compte-t-elle dans le monde entier ?



Quel est votre secteur d'activité ?



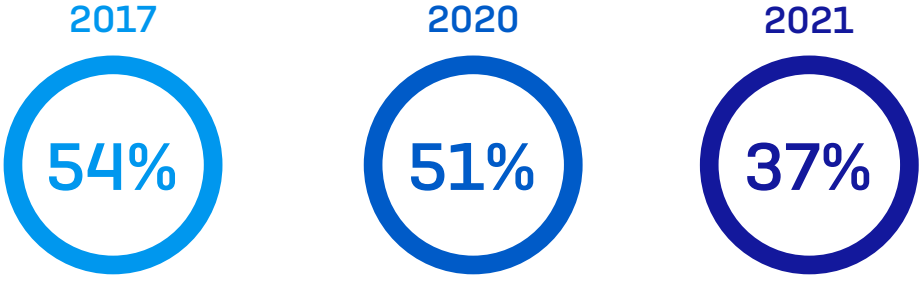
Principales découvertes

- **37 %** des entreprises déclarent avoir **été touchées par un ransomware au cours de l'année passée**.
- **54 %** des entreprises touchées ont déclaré que les **cybercriminels ont réussi à chiffrer leurs données** lors de l'attaque la plus significative.
- **96 %** des entreprises dont les données ont été chiffrées **ont réussi à récupérer des données** lors de l'attaque la plus importante.
- Le **montant moyen des rançons payées** par les entreprises de taille moyenne était de **170 404 dollars, soit environ 140 000 euros**.
- Cependant, en moyenne, seulement **65 % des données chiffrées ont été restaurées** après le paiement de la rançon.
- Le **coût moyen de remédiation d'une attaque de ransomware**, en tenant compte des temps d'arrêt, des ressources humaines nécessaires, du coût des équipements et du réseau, du manque à gagner, de la rançon payée, etc. s'élevait **à 1,85 million de dollars, soit environ 1,53 million d'euros.**
- **Les attaques d'extorsion** où les données n'ont pas été chiffrées mais dont la victime a tout de même dû payer une rançon **ont plus que doublé** depuis l'année dernière, passant de 3 % à 7 %.
- Le fait de disposer d'un **personnel informatique formé et capable d'arrêter les attaques** est la principale raison pour laquelle certaines entreprises sont convaincues qu'elles ne seront pas touchées par un ransomware à l'avenir.

La prévalence des ransomwares

Les ransomwares restent une véritable menace

37 % des entreprises, soit plus d'un tiers des 5 400 entreprises interrogées, ont été touchées par un ransomware l'année dernière, c'est-à-dire que **plusieurs ordinateurs ont été touchés, mais pas nécessairement chiffrés**. C'est un chiffre élevé, mais très en baisse par rapport à l'année dernière, où 51 % avaient déclaré avoir été touchés.

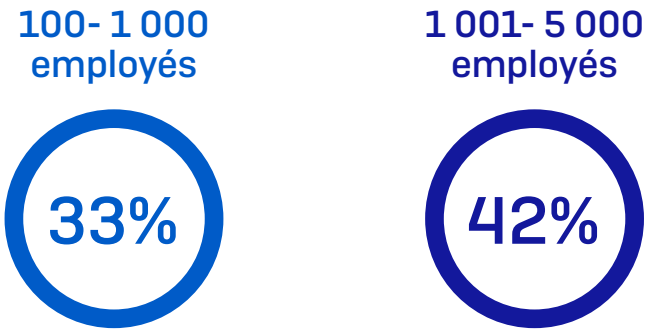


Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Oui [2021=5 400 ; 2020=5 000 ; 2017=2 700] en omettant certaines options de réponse, répartition par année

Selon les observations des SophosLabs et de nos équipes MTR, cette réduction pourrait être due en partie à l'évolution de l'approche utilisée par les cybercriminels. Par exemple, nombre d'entre eux préfèrent désormais lancer des attaques beaucoup plus ciblées utilisant des techniques de piratage manuel plutôt que de mener des attaques à grande échelle, génériques et automatisées. Bien que le nombre total d'attaques soit plus faible, notre expérience montre que les dommages infligés par ces attaques ciblées sont beaucoup plus importants.

Plus une entreprise est grande, plus elle est susceptible d'être touchée

En examinant le rapport entre le nombre d'incidents par un ransomware et la taille de l'entreprise, nous avons constaté que les grandes entreprises signalent une plus grande prévalence d'attaques. En effet, 42 % des entreprises de 1 001 à 5 000 employés déclarent avoir été touchées, contre 33 % de celles de plus petite taille.

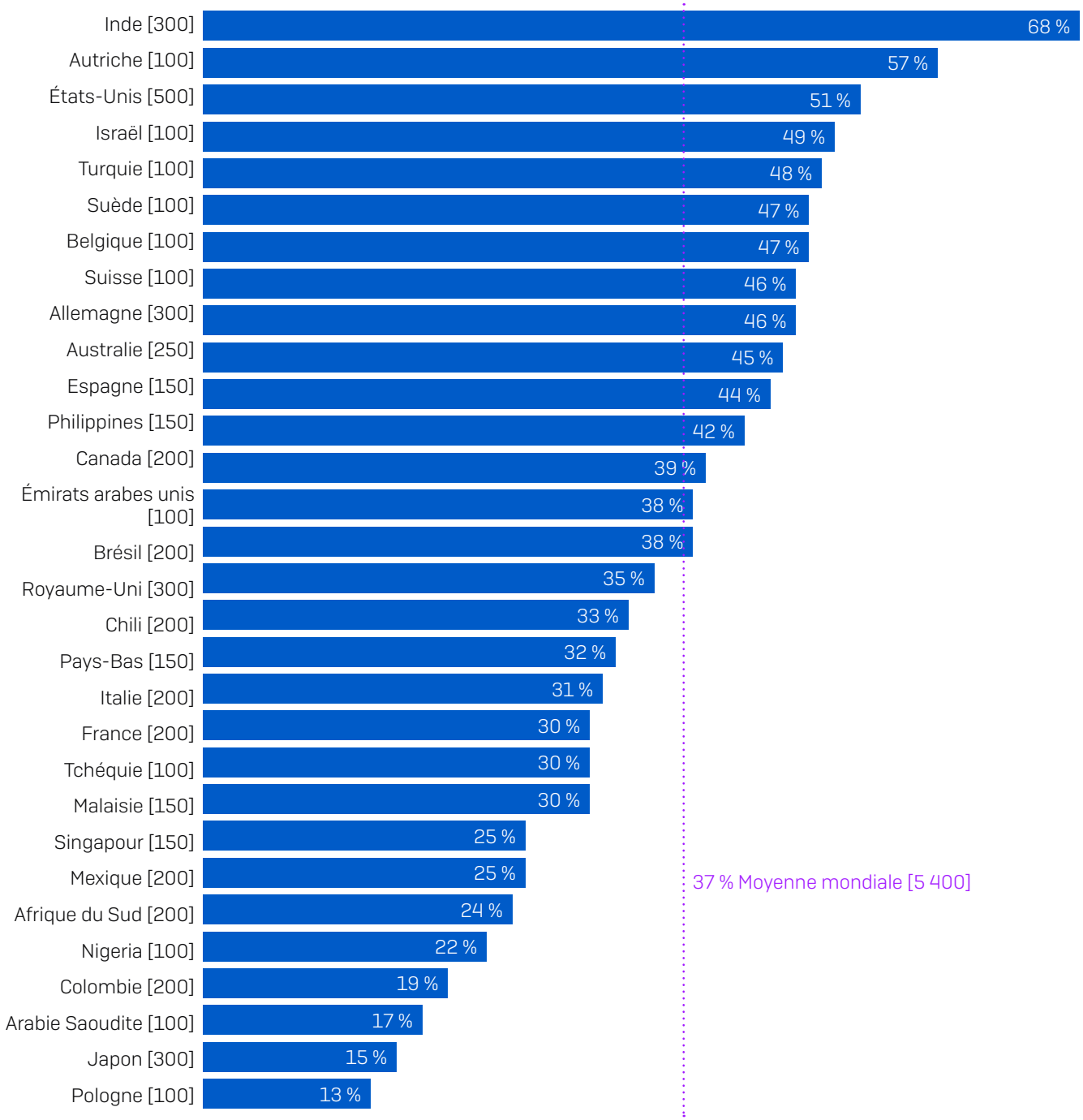


Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Oui [5 400] en omettant certaines options de réponse, répartition selon la taille de l'entreprise

En 2020, l'écart entre les petites et les grandes entreprises s'est également creusé, passant d'une différence de 7 % à 9 %. Il n'est peut-être pas surprenant que les attaques se concentrent davantage sur les grandes entreprises : elles sont susceptibles d'avoir plus de moyens financiers et sont donc une cible plus lucrative. Cela dit, un tiers des entreprises de petite taille ont été frappées par des ransomwares l'année dernière, confirmant qu'elles restent des proies de choix. Aucune entreprise n'est à l'abri d'une attaque.

Le nombre d'attaques varie selon les pays

L'analyse des données par pays révèle des résultats intéressants.



Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Oui [nombre total dans le tableau] en omettant certaines options de réponse, répartition par pays

L'Inde arrive malheureusement en tête de liste avec 68 % des répondants déclarant avoir été touchés par un ransomware l'année passée. Bien que les auteurs de ransomware les plus médiatisés viennent souvent de Chine, de Corée du Nord, de Russie et d'autres pays de l'ancien bloc de l'Est, les SophosLabs voient des niveaux élevés de ransomwares locaux en Inde, c'est-à-dire que des adversaires indiens attaquent des entreprises indiennes.

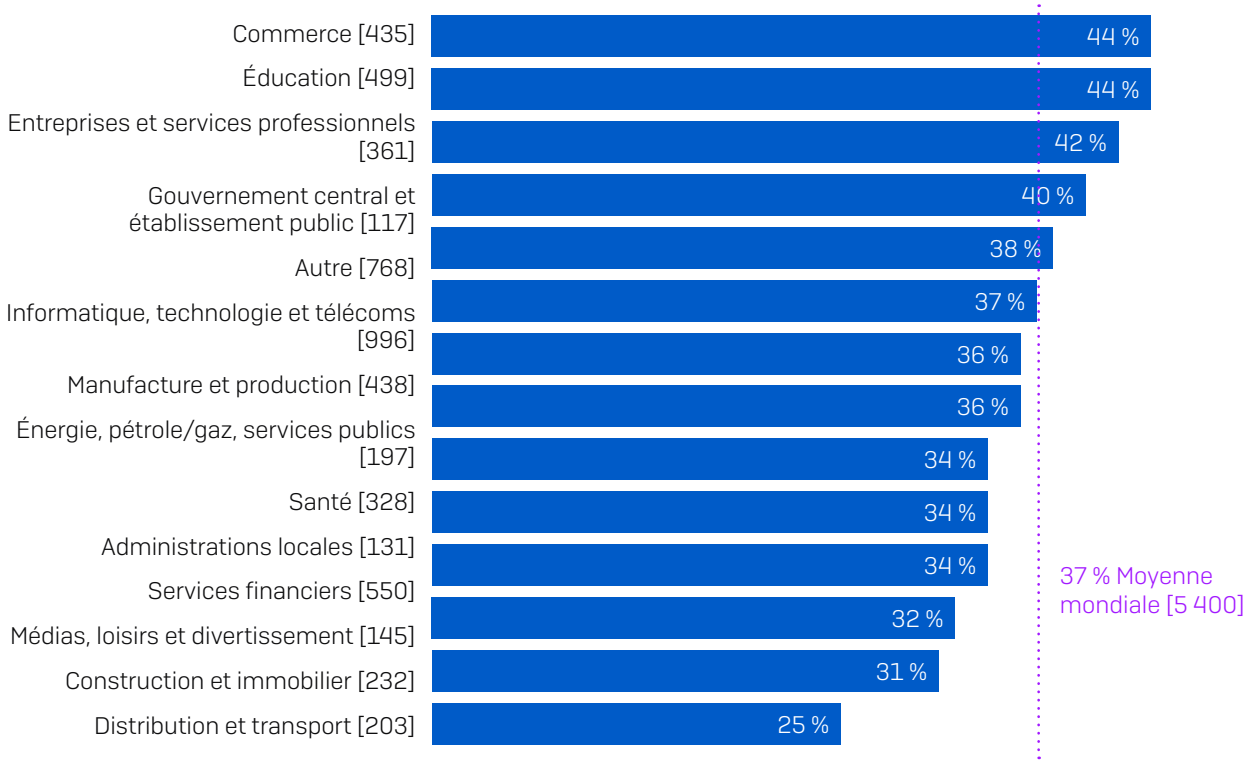
Les **États-Unis** sont une cible très populaire auprès des cybercriminels, attirés par des rançons potentiellement plus élevées. En effet, un peu plus de la moitié (51 %) des répondants américains déclarent avoir été touchées l'année dernière.

La **Pologne, la Colombie, le Nigeria, l'Afrique du Sud,** et **le Mexique** ont signalé le moins d'attaques, probablement en raison d'un PIB plus faible et donc d'un potentiel de rançon moindre pour les attaquants.

Le Japon se distingue comme étant une économie développée avec des niveaux de ransomware très faibles — seulement 15 % des répondants ont déclaré avoir été touchés l'année dernière. Dans toutes nos enquêtes annuelles, le Japon déclare généralement peu d'attaques par ransomware. Cela est peut-être dû au fait que les entreprises japonaises ont fortement investi dans des défenses anti-ransomware, ou que la nature unique de la langue japonaise en fasse une cible plus difficile pour les criminels.

Le commerce et l'éducation ont subi le plus d'attaques de ransomware

En étudiant les attaques par secteur industriel, nous voyons des variations considérables d'un secteur à l'autre.



Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Oui [nombre total dans le graphique] en omettant certaines options de réponse, répartition par secteur

Les secteurs du commerce *et de* l'éducation *ont le plus grand nombre d'attaques, avec 44 % des répondants déclarant avoir été touchés.*

Le secteur de la santé, dont les attaques de ransomwares sont souvent très médiatisées, a signalé un niveau d'attaques légèrement inférieur à la moyenne, soit 34 %. La sur-représentation de ce secteur dans les actualités est probablement due à des obligations réglementaires qui exigent que les organismes de santé révèlent avoir fait l'objet d'une attaque, contrairement aux entreprises privées, qui peuvent généralement garder l'information confidentielle.

L'impact des ransomwares

Le chiffrement est en baisse. L'extorsion est en hausse.

Nous avons demandé aux entreprises touchées par un ransomware si les cybercriminels ont réussi à chiffrer les données. 54 % ont répondu oui. 39 % ont pu interrompre l'attaque avant le chiffrement de leurs données, tandis que 7 % ont déclaré que leurs données n'avaient pas été chiffrées, mais qu'elles avaient tout de même reçu une demande de rançon.

Il est très intéressant de comparer ces chiffres avec les résultats de notre enquête de 2020.

2020	2021	
73 %	54 %	Les cybercriminels ont chiffré les données
24 %	39 %	Attaque interrompue avant que les données ne puissent être chiffrées
3 %	7 %	Données non chiffrées mais la victime a été rançonnée

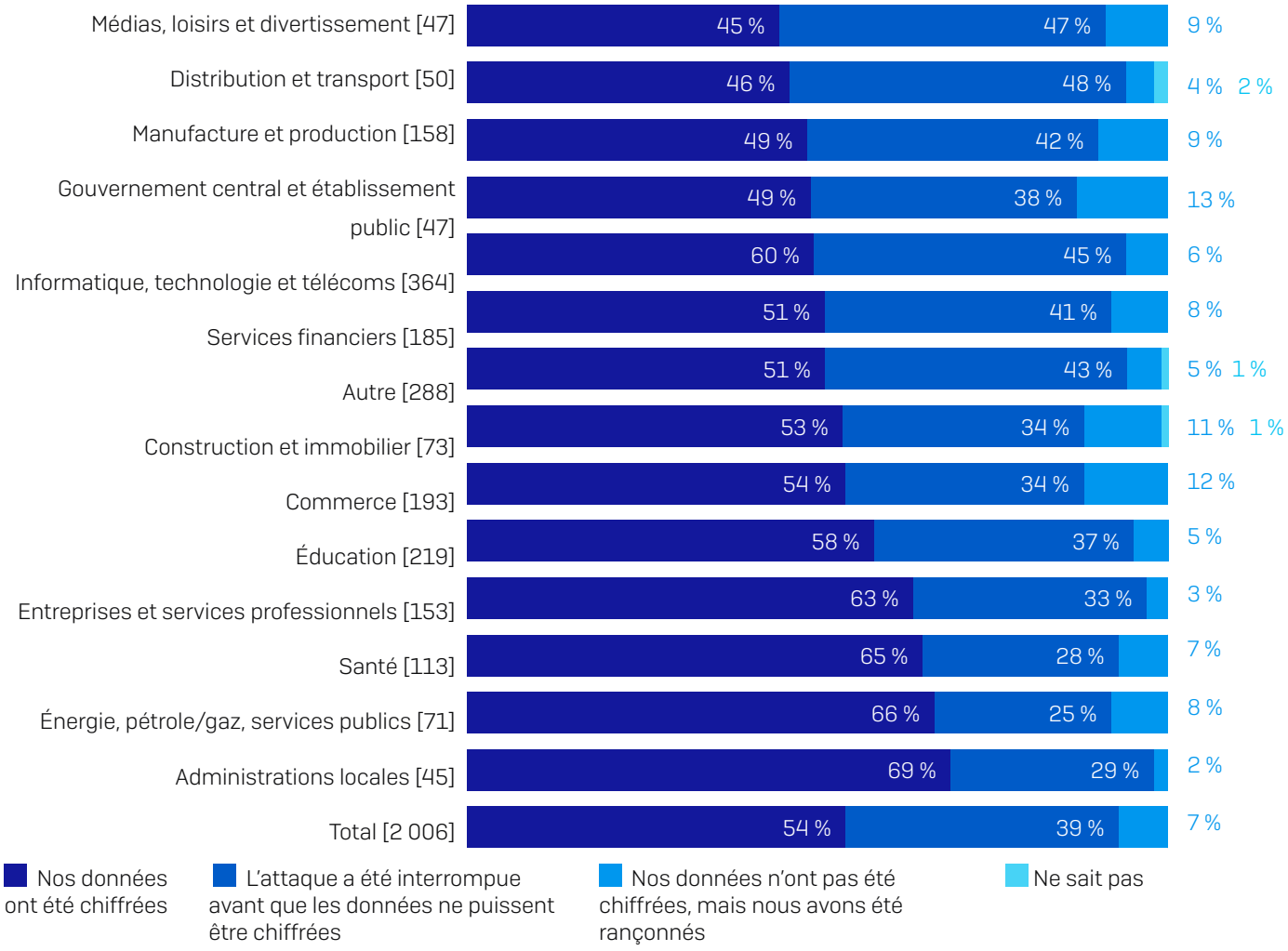
Lors de l'attaque de ransomware la plus importante, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? [2021=2 006, 2020=2 538] Question posée aux répondants ayant déclaré avoir été touchés par un ransomware au cours de l'année passée.

Tout d'abord, en 2020, le pourcentage d'attaques où le criminel a réussi à chiffrer les données a baissé de 73 % à 54 %. De nombreuses entreprises sont désormais en mesure de bloquer l'attaque avant que les données ne puissent être chiffrées. Cela prouve l'utilité des solutions anti-ransomware.

Cependant, nous constatons également que le pourcentage d'attaques où les données n'ont pas été chiffrées mais dont la victime a tout de même été prise en otage contre rançon a plus que doublé. Certains attaquants ont changé de tactique : plutôt que de chiffrer les fichiers, ils menacent de publier les données volées à moins que la rançon ne soit payée. Cela leur demande moins d'efforts puisqu'aucun chiffrement ou déchiffrement n'est nécessaire. Comme les fuites de données peuvent coûter cher aux entreprises, c'est une technique de négociation efficace que les criminels utilisent souvent pour forcer leurs victimes à payer.

La capacité de bloquer le chiffrement varie considérablement d'un secteur à l'autre

Lorsqu'il s'agit de bloquer le chiffrement des fichiers, certains secteurs y parviennent mieux que d'autres.



Lors de l'attaque de ransomware la plus importante, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? [Nombre total dans le graphique] entreprises qui ont été touchées par un ransomware au cours de l'année passée, omettant certaines options de réponse, répartition par secteur

La distribution et le transport sont les secteurs les plus capables d'empêcher les attaquants de chiffrer les fichiers (48 %), suivis de près par **les médias, les loisirs et les divertissements** (47 %).

À l'inverse, **les administrations locales** sont le secteur dont les données sont les plus susceptibles d'être chiffrées au cours d'une attaque de ransomware (69 %). Cela est probablement dû à la fois :

- À des défenses plus faibles : en général, les administrations locales ont des budgets informatiques moins importants et des équipes informatiques limitées.
- À l'intérêt croissant des cybercriminels : en raison de leur taille et de leur accès aux fonds publics, les organismes gouvernementaux sont souvent considérés comme des cibles lucratives et, par conséquent, font l'objet d'attaques plus sophistiquées. De plus, comme nous le verrons plus tard, les administrations locales sont également le secteur avec la deuxième plus forte propension à payer la rançon.

Les gouvernements centraux et les établissements publics sont le secteur le plus susceptible d'être extorqué (13 %).

La santé, comme nous l'avons vu, connaît un nombre d'attaques inférieur à la moyenne. Cependant, les criminels parviennent à chiffrer les fichiers dans près des deux tiers (65 %) des incidents, ce qui est considérablement supérieur à la moyenne.

Davantage de victimes payent la rançon

Nous avons demandé aux entreprises dont les données avaient été chiffrées (1 086) si elles avaient récupéré leurs données et, le cas échéant, de quelle manière.

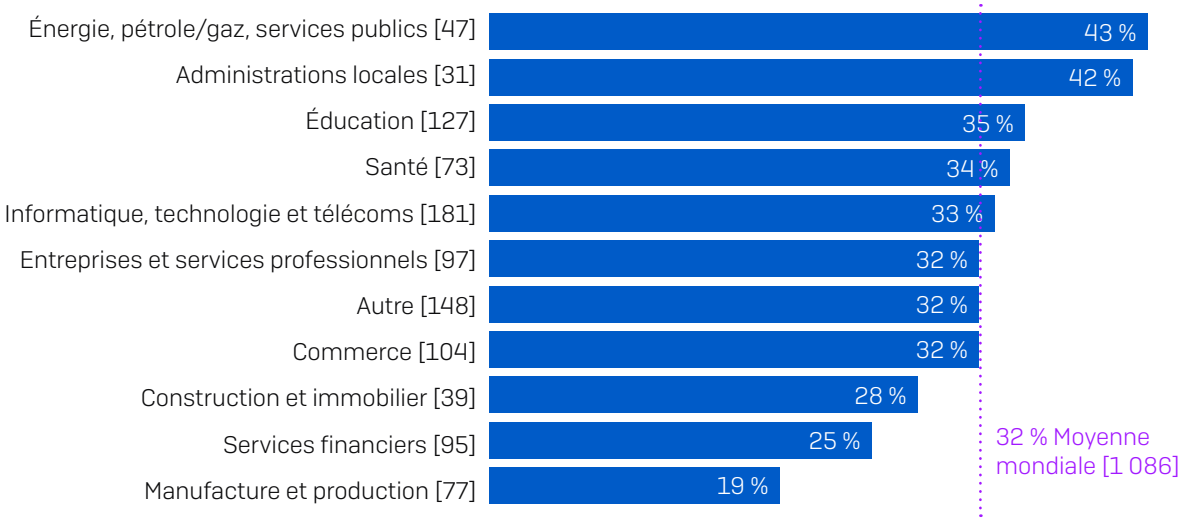
2020	2021	
26 %	32 %	Ont payé la rançon pour récupérer leurs données
56 %	57 %	Ont utilisé des sauvegardes pour récupérer leurs données
12 %	8 %	Ont utilisé d'autres moyens pour récupérer leurs données
94 %	96 %	Pourcentage total ayant récupéré des données

Remarque : en raison des arrondis, certains totaux ne correspondent pas à la somme des chiffres séparés.
Lors de l'attaque de ransomware la plus importante, votre entreprise a-t-elle récupéré ses données ?
[2021=1 086, 2020=1 849] entreprises dont les données ont été chiffrées.

Comme le montre le graphique ci-dessus, 32 % des répondants ont payé la rançon pour récupérer leurs données, chiffre en hausse par rapport à l'année dernière (26 %). 57 % ont pu utiliser des sauvegardes pour restaurer leurs données, ce qui est similaire aux résultats de l'année dernière. Dans l'ensemble, presque tout le monde (96 %) a récupéré une partie de ses données.

La propension à payer varie selon le secteur

Il existe des différences considérables dans le paiement des rançons entre les secteurs.



Lors de l'attaque de ransomware la plus importante, votre entreprise a-t-elle récupéré ses données ? Oui, nous avons payé la rançon [nombre total dans le graphique] pour les entreprises où les cybercriminels ont réussi à chiffrer leurs données lors de l'attaque de ransomware la plus importante, en omettant certaines options de réponse, répartition par secteur

L'énergie, le pétrole/gaz et les services publics sont le secteur le plus susceptible de payer la rançon, avec 43 % des répondants déclarant l'avoir payé. Ce secteur a généralement beaucoup d'infrastructures anciennes qui ne peuvent pas être aisément mises à jour ; les victimes peuvent ainsi se sentir obligées de payer la rançon pour assurer la continuité des activités.

Les administrations locales arrivent en deuxième place avec 42 % des répondants ayant payé une rançon. Il est intéressant de noter le lien entre ce chiffre et le fait que les administrations locales sont le secteur le plus susceptible d'avoir ses données chiffrées. Il se peut que cette forte propension des organismes gouvernementaux à payer pousse les criminels à lancer des attaques toujours plus complexes et plus efficaces.

Il semble y avoir un lien entre la capacité d'une entreprise à restaurer des données à partir de sauvegardes et la probabilité qu'elle ne paye pas la rançon. **Le secteur de la manufacture et de la production** est le moins susceptible de payer la rançon et le plus à même de restaurer ses données à partir de sauvegardes (68 %). De même, **la construction et l'immobilier**, ainsi que **les services financiers**, se distinguent comme les secteurs ayant payé moins de rançons et ayant restauré le plus de données à partir de sauvegardes que la moyenne des répondants.

Les gouvernements centraux et les établissements publics ont été exclus de ce graphique car le nombre est trop faible pour être intéressant du point de vue statistique. Fait intéressant, sur les 23 entreprises de ce secteur dont les données ont été chiffrées, 61 % ont déclaré les avoir restaurées à partir de sauvegardes et seulement 26 % ont payé la rançon. Cette constatation peut aider à expliquer pourquoi ce secteur est principalement ciblé par les attaques basées sur l'extorsion.

Payer la rançon ne permet de récupérer qu'une partie des données

65%

des données ont été restaurées après paiement de la rançon

Quantité moyenne de données récupérées par les entreprises après l'attaque de ransomware la plus importante [344] entreprises qui ont payé la rançon pour récupérer leurs données

Ce que les attaquants omettent de vous dire lorsqu'ils vous rançonnent est que même si vous payez, vos chances de récupérer l'intégralité de vos données sont faibles. En moyenne, les entreprises ayant payé une rançon n'ont récupéré que 65 % des fichiers chiffrés — perdant ainsi plus d'un tiers de leurs données. 29 % des répondants ont indiqué avoir restauré moins de 50 % de leurs fichiers et seulement 8 % ont récupéré l'intégralité de leurs données.

Le coût des ransomwares

Le montant des rançons varie considérablement

Parmi les 357 répondants ayant déclaré que leur entreprise avait payé la rançon, 282 ont pu nous indiquer le montant exact. Le **paiement moyen était de 170 404 $, soit environ 140 000 €**. Cependant, les montants demandés varient considérablement. Le montant le plus courant était de 10 000 $ (env. 8 200 €) payé par 20 répondants et le montant le plus élevé était de 3,2 millions $ (env. 2,63 millions €) payé par 2 répondants.

Ces chiffres sont très différents des montants à huit chiffres que l'on voit fréquemment faire les gros titres des journaux.

1. **Taille de l'entreprise.** Les répondants de cette enquête proviennent d'entreprises comptant 100 à 5 000 utilisateurs, qui, en général, ont moins de ressources financières que les grandes entreprises. Les auteurs des ransomwares fixent le montant de la rançon en fonction des moyens de la victime et demandent généralement des montants plus modestes aux petites entreprises. Les données le confirment : le montant moyen payé par les entreprises de 100 à 1 000 employés était de 107 694 $ (env. 88 700 €), contre 225 588 $ (env. 185 700 €) pour les entreprises de 1 000 à 5 000 employés.
2. **Nature de l'attaque.** Il existe autant d'auteurs de ransomware que de types de ransomware différents. On rencontre aussi bien des criminels experts qui ciblent des organismes précis à l'aide de tactiques, de techniques et de procédures sophistiquées (TTP), que des amateurs qui utilisent des ransomwares « prêts à l'emploi » et une approche de diffusion en masse qui ne génère pas toujours de retours. Les criminels qui investissent des efforts considérables dans des campagnes ciblées exigent des rançons élevées, tandis que les diffuseurs d'attaques génériques se satisfont généralement d'un retour sur investissement plus faible.
3. **Géographie.** Les entreprises situées dans les pays occidentaux sont confrontées à des montants plus élevés, car elles sont perçues comme ayant des ressources plus importantes. Les deux rançons les plus chères ont toutes deux été déclarées en Italie. En outre, le paiement moyen aux États-Unis, au Canada, au Royaume-Uni, en Allemagne et en Australie s'élevait à 214 096 $ (env. 176 000 €), soit 26 % de plus que la moyenne mondiale (base : 101 répondants). À l'inverse, en Inde, le montant moyen de la rançon était de 76 619 $ (env. 63 000 €), soit moitié moins que le chiffre mondial (base : 86 répondants).

Le coût de remédiation d'une attaque de ransomware a plus que doublé au cours de l'année dernière

Le paiement de la rançon ne représente qu'une petite partie du coût total de remédiation d'une attaque. Bien que le nombre d'attaques de ransomware et le pourcentage de cas dans lesquels les criminels ont réussi à chiffrer des données ont diminué depuis l'année dernière, le coût total de remédiation a augmenté.

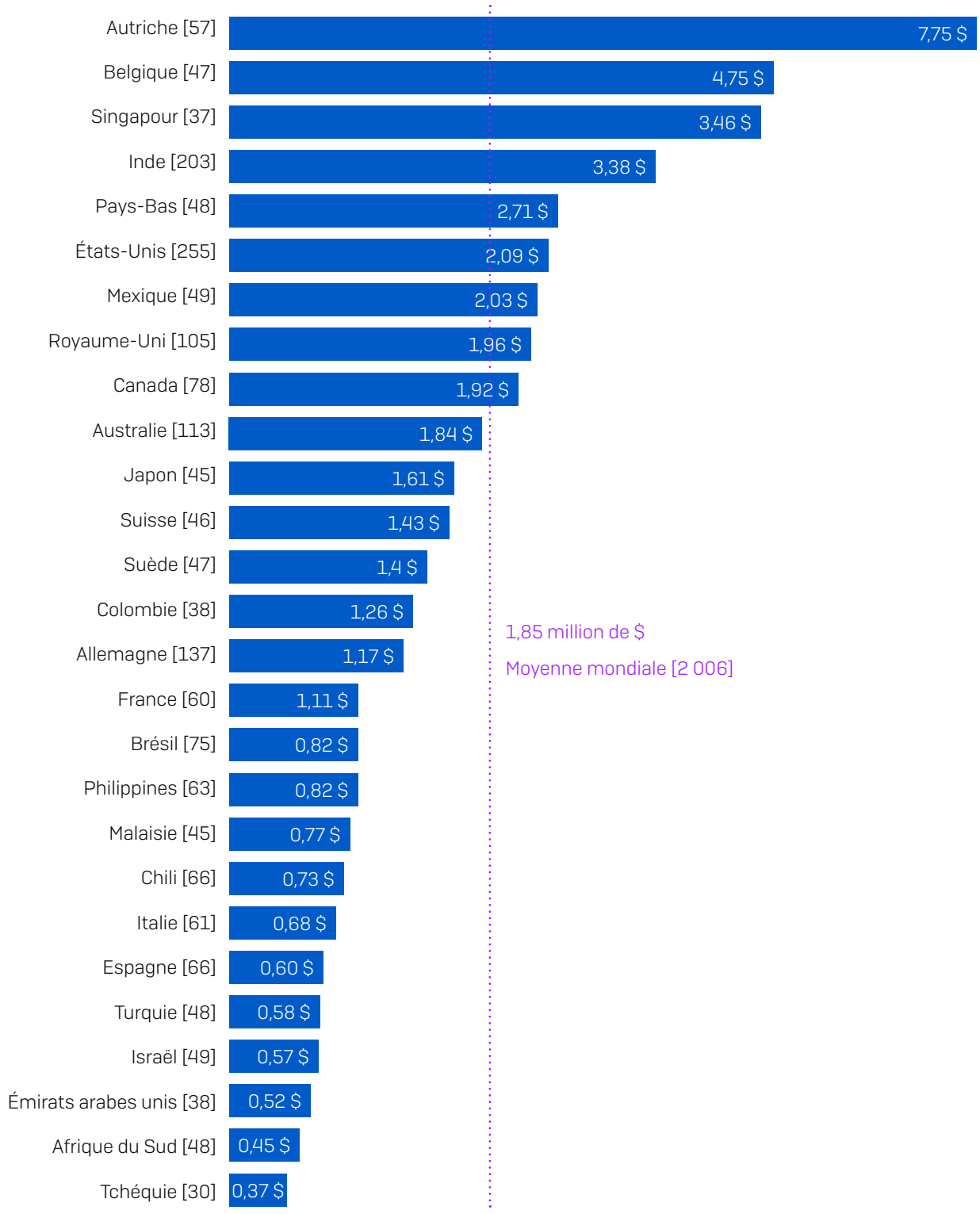
Selon les répondants, le coût moyen de remédiation de l'attaque la plus récente (en tenant compte des temps d'arrêt, des ressources humaines nécessaires, du coût des équipements et du réseau, du manque à gagner, de la rançon payée, etc.) s'élevait à 1,85 million de dollars (env. 1,52 million d'euros), soit plus du double du montant déclaré l'an dernier (761 106 000 $/ env. 627 000 000 €).

Coût moyen approximatif de remédiation de la dernière attaque de ransomware (en tenant compte des temps d'arrêt, des ressources humaines nécessaires, du coût des équipements et du réseau, du manque à gagner, de la rançon payée, etc.) [2021=2 006, 2020=2 538] répondants dont l'entreprise a été touchée par un ransomware au cours l'année passée, répartition par année

Pendant l'année écoulée, nos experts en ransomware ont constaté une forte hausse des attaques avancées combinant automatisation et piratage manuel. Ces attaques complexes nécessitent des processus de remédiation plus complexes, ce qui peut expliquer l'augmentation générale des coûts d'une attaque.

Les coûts de remédiation varient selon les pays

L'analyse par pays du coût de remédiation des attaques de ransomware révèle des variations importantes.



Coût moyen approximatif de remédiation de la dernière attaque de ransomware (en tenant compte des temps d'arrêt, des ressources humaines nécessaires, du coût des équipements et du réseau, du manque à gagner, de la rançon payée, etc.) [chiffres de base dans le graphique] répondants dont l'entreprise a été touchée par un ransomware au cours de l'année passée, répartition par pays, millions de dollars américains

Un livre blanc Sophos. Avril 2021

L'Autriche se distingue comme le pays avec le coût total le plus élevé. L'année dernière, l'Autriche a fait l'objet d'une multitude d'attaques de grande envergure : le ministère des Affaires étrangères a été visé par un acteur étatique et le groupe de cybercriminels Netwalker a revendiqué sur Twitter le vol des données de la ville de Weiz. Notons cependant que même en excluant l'Autriche des données, le coût moyen diminue très peu : 1,68 million de dollars (env. 1,38 million €), ce qui représente plus du double du montant moyen déclaré l'année dernière.

De manière générale, les pays où les salaires sont les plus élevés (Belgique, États-Unis, Pays-Bas, Singapour) affichent des coûts totaux parmi les plus élevés, tandis que les pays où les salaires sont les plus bas (Afrique du Sud, République tchèque) affichent les coûts totaux les plus bas. Cela reflète l'effort manuel considérable nécessaire pour remédier à une attaque. En effet, les coûts de remédiation représentent environ 10 fois le montant de la rançon.

Israël fait partie des pays où le coût total de remédiation est le plus faible, malgré le fait qu'il s'agisse d'une économie développée. Pour des raisons géopolitiques, Israël est une cible majeure de cyberattaques (pas seulement de ransomware), ce qui se traduit par des niveaux très élevés de cyberdéfense, de préparation et d'expertise en matière de remédiation. Ces facteurs contribuent à réduire l'impact financier des attaques.

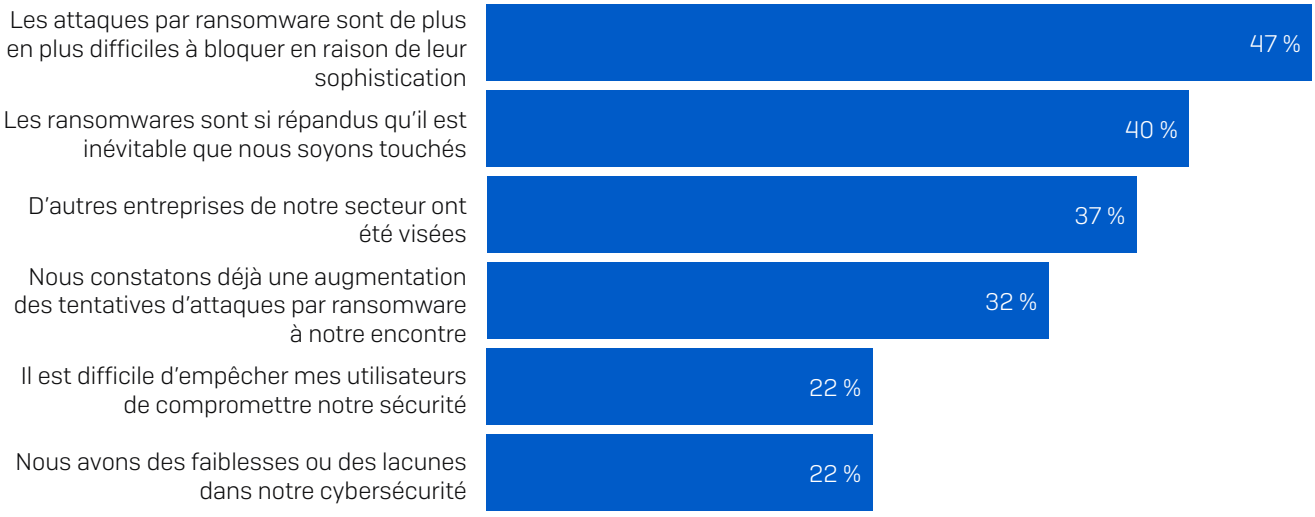
À quoi s'attendre pour l'avenir ?

Les perspectives en matière d'attaque de ransomware varient

62 % des répondants (3 353) ont déclaré que leur entreprise n'avait pas été touchée par un ransomware au cours de l'année passée. Au sein de ce groupe, nous voyons une variation considérable dans leur attitude et leur confiance dans le traitement des ransomwares. 65 % s'attendent à être touchés par un ransomware à l'avenir, tandis que 35 % n'anticipent pas une attaque.

Pourquoi les entreprises s'attendent-elles à être touchées par un ransomware ?

Parmi les 2 187 répondants qui n'ont pas été touchés par un ransomware l'année dernière mais qui s'attendent à l'être à l'avenir, 47 % s'y attendent car « les attaques de ransomware deviennent de plus en plus difficiles à bloquer en raison de leur sophistication ».



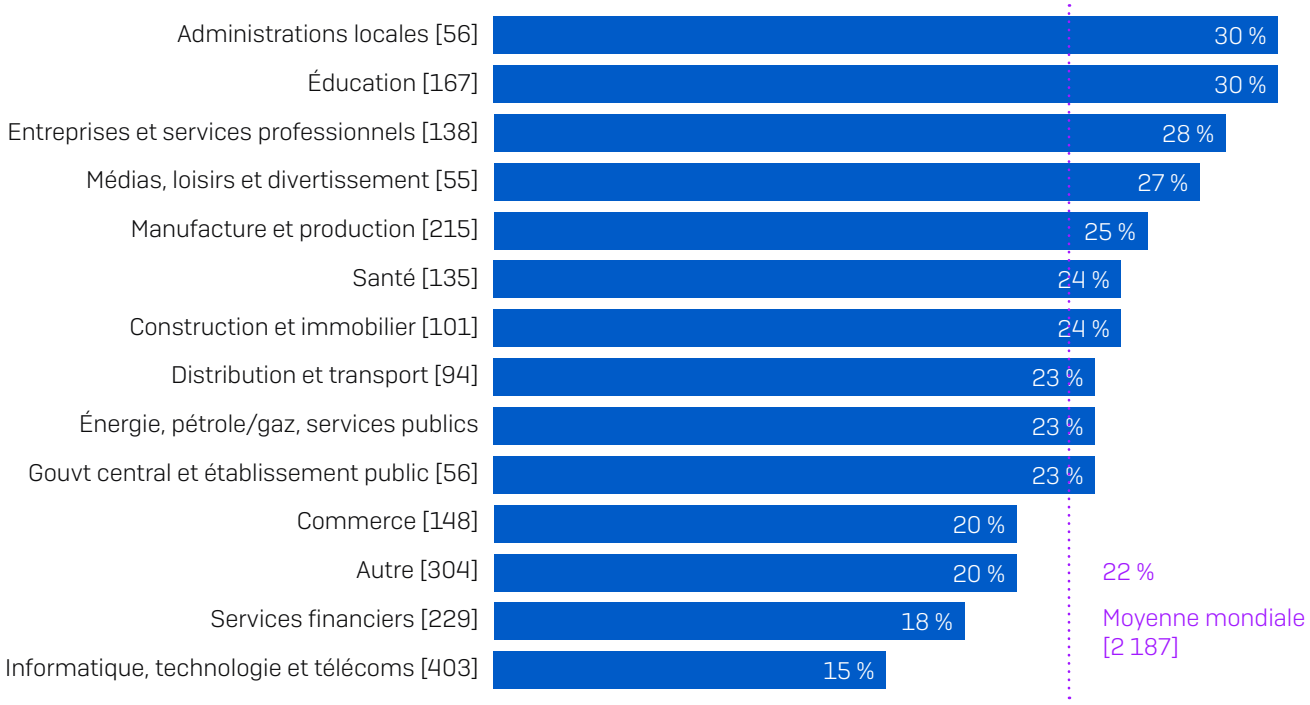
Pourquoi vous attendez-vous à ce que votre entreprise soit touchée par un ransomware à l'avenir ? [2 187] entreprises qui n'ont pas été touchées par un ransomware l'année dernière et qui ne s'attendent pas à l'être à l'avenir, omettant certaines options de réponse

Bien que ce chiffre soit élevé, le fait que ces entreprises soient vigilantes face à la multiplication des ransomwares est une bonne chose, et explique peut-être pourquoi ils n'ont pas subi d'attaque l'année dernière.

22 % des répondants considèrent que la négligence des utilisateurs pourrait être un facteur majeur dans une future attaque par ransomware. Il est encourageant de constater que, face à des attaques de plus en plus sophistiquées, la plupart des équipes informatiques ne tombent pas dans le piège de blâmer leurs utilisateurs.

Par ailleurs, 22 % des personnes interrogées admettent avoir des faiblesses ou des lacunes dans leurs défenses de cybersécurité. Bien qu'évidemment, ce ne soit pas une bonne idée d'avoir des vulnérabilités, reconnaître ce problème est une première étape importante pour améliorer votre sécurité.

Les administrations locales et le secteur de l'éducation sont les plus susceptibles d'admettre des failles de sécurité (30 % chacun).



Pourquoi vous attendez-vous à ce que votre entreprise soit touchée par un ransomware à l'avenir ? Nous avons des faiblesses ou des lacunes dans notre stratégie de cybersécurité [nombre total dans le graphique] entreprises qui n'ont pas été touchées par un ransomware mais qui s'attendent à l'être à l'avenir, en omettant certaines options de réponse, répartition par secteur

Bien que ceux ayant répondu à cette question n'aient pas été touchés par un ransomware l'an dernier, il est probable qu'ils aient été influencés par les expériences d'autres entreprises dans leur secteur :

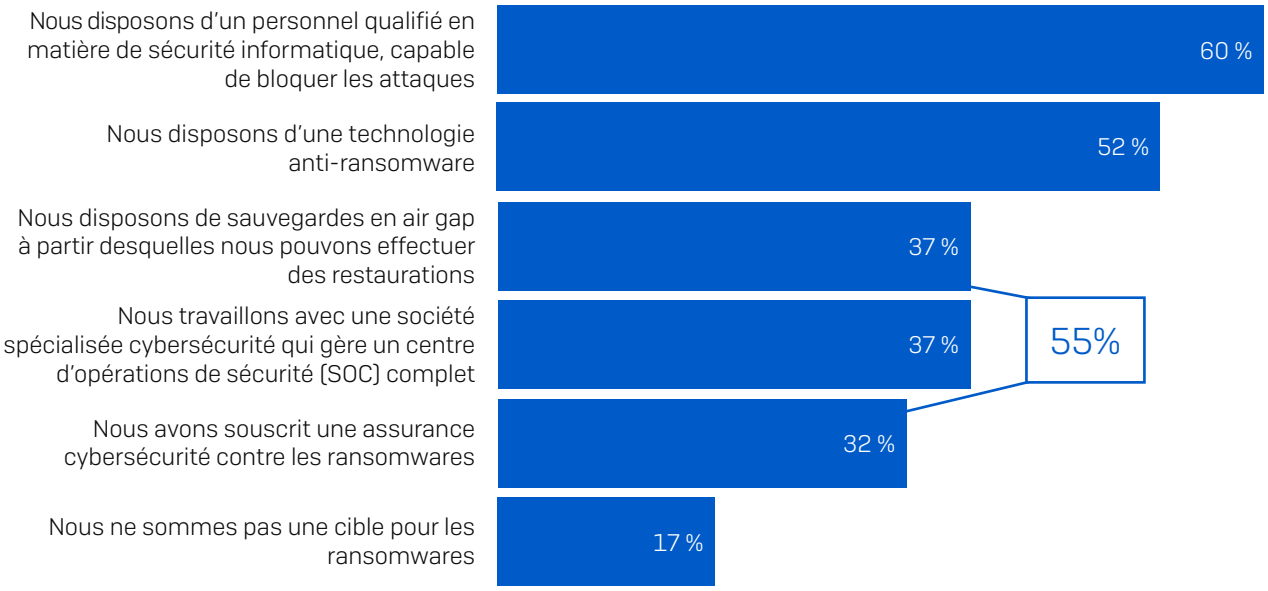
- **Les gouvernements locaux** sont le secteur où les attaquants sont les plus susceptibles de réussir à chiffrer les données de la victime.
- **L'éducation et le commerce** sont les secteurs ayant le plus grand nombre d'entreprises touchées par un ransomware l'année dernière.

En outre, ces deux secteurs ont souvent des budgets restreints et ne peuvent pas investir dans des ressources technologiques et informatiques, ce qui entraîne également des failles de sécurité.

À l'inverse, les **secteurs de l'informatique, des télécommunications et des technologies** (15 %) ainsi que **les services financiers** (18 %) sont ceux qui déclarent le moins avoir des lacunes en matière de sécurité. Ces secteurs adoptent en général rapidement les nouvelles technologies et ont des budgets plus conséquents ; ils sont donc plus susceptibles de corriger leurs failles de sécurité.

La présence d'un personnel informatique qualifié donne confiance en l'avenir

1 166 répondants ont déclaré n'avoir pas été touchés par un ransomware au cours de l'année passée et ne pas s'attendre à l'être à l'avenir. Cette confiance face aux ransomwares repose essentiellement sur le fait qu'ils disposent d'un service informatique capable de bloquer les attaques.



Pourquoi ne vous attendez-vous pas à ce que votre entreprise soit touchée par ransomware à l'avenir ? [1 166] entreprises qui n'ont pas été touchées par un ransomware l'année dernière et qui ne s'attendent pas à l'être à l'avenir, omettant certaines options de réponse

Bien que l'utilisation de technologies avancées et automatisées soit essentielle à la lutte contre les ransomwares, le blocage des attaques nécessite également une surveillance humaine et l'intervention de professionnels qualifiés. Que la surveillance soit effectuée en interne ou par un prestataire externe, certains signes révélateurs d'attaques ne peuvent être repérés que par des opérateurs humains.

37 % des répondants qui ne s'attendent pas à être touchés à l'avenir travaillent avec une société spécialisée dans la cybersécurité dotée d'un centre d'opérations de sécurité (SOC) complet. Il y a quelques années encore, seules les grandes entreprises utilisaient les SOC. Cela représente donc un changement majeur dans la gestion de la sécurité des entreprises de taille moyenne.

Mais il n'y a pas que des bonnes nouvelles. Certains résultats sont préoccupants :

- 55 % des répondants qui ne s'attendent pas à être touchés font confiance à des approches qui n'offrent aucune protection contre les ransomwares :
  - 37 % ont affirmé ne pas être inquiets car ils utilisent des sauvegardes en « air-gap ». Les sauvegardes, comme nous l'avons vu, sont indispensables pour restaurer vos données après une attaque, mais ne vous empêchent pas d'être touché.
  - 32 % ont affirmé que leur assurance cybersécurité les protégeait contre les ransomwares. Encore une fois, les assurances peuvent vous aider à gérer les étapes de remédiation après l'attaque, mais ne l'empêchent pas de se produire.

Notez que certains répondants ont choisi les deux options, et 55 % ont choisi au moins l'une d'entre elles.

- En outre, 17 % des répondants ne pensent pas être concernés par les ransomwares. Mais la réalité prouve le contraire. Aucune entreprise n'est à l'abri.

Plans de rétablissement après incident de malwares

Il peut être extrêmement stressant de répondre à une cyberattaque ou un incident critique. Bien que rien ne puisse complètement atténuer le stress lié à une attaque, la mise en place d'un plan de réponse aux incidents efficace est un moyen sûr de minimiser son impact.

Il est donc encourageant de découvrir que 90 % des répondants déclarent que leur entreprise dispose d'un plan de rétablissement dédié aux malwares, et que parmi ces derniers, un peu plus de la moitié (51 %) disposent d'un plan complet et détaillé et 39 % d'un plan partiellement développé.

Il existe de nombreux parallèles entre la reprise des activités après une attaque de malware et la reprise des activités après une catastrophe naturelle ; dans les deux cas, vous devez être capable de recommencer de zéro. C'est aux Philippines, un pays qui subit des inondations et des tremblements de terre fréquents, que les entreprises sont les mieux préparées à subir l'attaque d'un malware : 83 % des répondants ayant un plan complet et détaillé.

Les organismes gouvernementaux sont les moins préparés pour répondre aux attaques de malware

La plupart des secteurs sont bien préparés pour se rétablir après une attaque de malware. Ce sont les organismes gouvernementaux qui sont les moins bien préparés : seuls 73 % des **administrations locales** et 81 % des **gouvernements centraux et des établissements publics** ont un plan de rétablissement en place.

Cela est inquiétant car ces secteurs sont parmi les plus touchés par les ransomwares. Les administrations locales sont le secteur le plus susceptible d'avoir ses données chiffrées dans une attaque, tandis que les gouvernements centraux et les établissements publics sont les plus susceptibles d'être extorqués.

L'absence de plan de rétablissement post-attaque est peut-être l'un des facteurs principaux contribuant à faire des administrations locales le deuxième secteur le plus susceptible de payer les demandes de rançon.

Recommandations

L'analyse des résultats de notre enquête a mené les experts Sophos à élaborer les recommandations suivantes :

1. **Partez du principe que vous serez touché.** Les ransomwares restent très répandus. Aucun secteur, pays ou entreprise n'est à l'abri. Il vaut mieux être préparé et ne pas être touché, que l'inverse.

2. **Faites des sauvegardes.** Les sauvegardes sont la méthode la plus utilisée par les entreprises pour récupérer leurs données après une attaque. Et comme nous l'avons vu, même si vous payez la rançon, vous n'êtes pas sûrs de récupérer toutes vos données, donc vous devrez dans tous les cas utiliser des sauvegardes.

3. **Déployez une protection multicouche.** Face à la forte augmentation des attaques d'extorsion, il est plus important que jamais de faire en sorte que vos adversaires ne puissent pas pénétrer dans votre environnement. Utilisez une protection multicouche pour bloquer les attaquants en tous points de votre environnement.

4. **Combinez expertise humaine et technologie anti-ransomware.** La meilleure façon de bloquer un ransomware est d'établir une défense en profondeur combinant une solution technologique dédiée et une surveillance humaine experte. La technologie vous offre la puissance et l'automatisation dont vous avez besoin, tandis que les opérateurs humains sont plus à même de détecter les tactiques, techniques et procédures indiquant qu'un attaquant de haut niveau tente de pénétrer dans votre environnement. Si vous ne disposez pas des compétences en interne, demandez l'aide d'une société spécialisée en cybersécurité. Les SOC sont désormais accessibles aux entreprises de toutes tailles.

5. **Ne payez pas la rançon.** Nous savons que c'est facile à dire, mais beaucoup moins facile à faire lorsque vos activités sont interrompues à cause d'une attaque ransomware. Indépendamment de toute considération éthique, payer la rançon est un moyen inefficace de récupérer vos données. Si vous décidez de payer, assurez-vous d'inclure dans votre analyse coûts/avantages le fait que vous ne récupèrerez, en moyenne, que les deux tiers de vos fichiers.

6. **Élaborez un plan de rétablissement des attaques.** La meilleure façon d'éviter qu'une cyberattaque ne se transforme en une véritable violation de sécurité est de se préparer à l'avance. Souvent, les victimes ne réalisent qu'après l'attaque qu'elles auraient pu s'éviter beaucoup de tracas, de dépenses et de temps perdu si elles avaient eu en place un plan de réponse aux incidents.

Ressources supplémentaires

Le Guide de Réponse aux incidents de Sophos aide les entreprises à définir le cadre du plan de réponse aux incidents de cybersécurité et décrit les 10 principales étapes que le plan devrait inclure.

Consulter également le livre blanc Quatre conseils clés des experts en réponse aux incidents, qui met en évidence les principales leçons que chacun devrait tirer lorsqu'il s'agit de répondre à des incidents de cybersécurité.

Ces deux documents sont basés sur l'expérience réelle des équipes Sophos Managed Threat Response et Sophos Rapid Response, qui ont collectivement répondu à des milliers d'incidents de cybersécurité.

En savoir plus sur les ransomwares et sur la façon dont Sophos peut vous aider à protéger votre entreprise.

Sophos fournit des solutions de cybersécurité de pointe aux entreprises de toutes tailles, les protégeant en temps réel contre les menaces avancées telles que les malwares, les ransomwares et le phishing. Grâce à des fonctionnalités Next-Gen éprouvées, les données de votre entreprise sont sécurisées efficacement par des produits alimentés par l'intelligence artificielle et le Machine Learning.

2021-04-19 (SB-NP)

SOPHOS