SOPHOS

L'état des ransomwares 2023

Résultats d'une étude indépendante et agnostique menée entre janvier et mars 2023 auprès de 3 000 responsables informatiques et responsables cybersécurité dans 14 pays.

Un livre blanc Sophos. Mai 2023

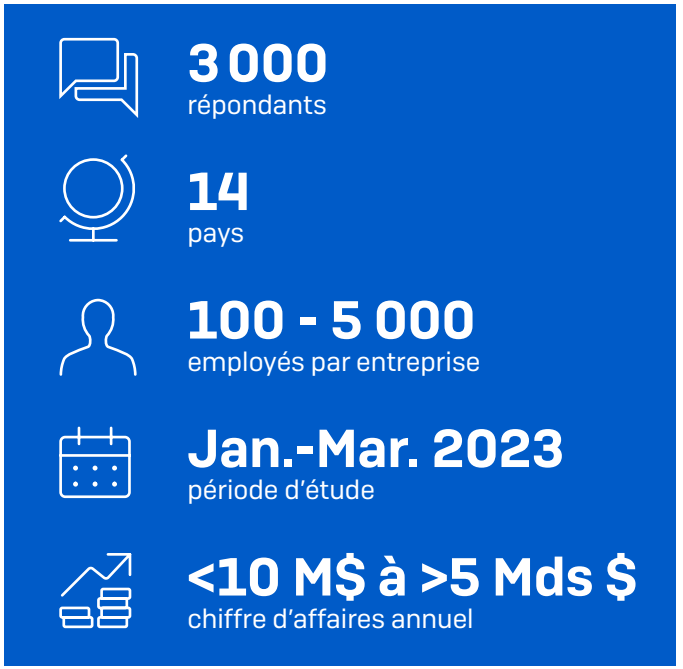
Introduction

L'étude annuelle de Sophos porte sur les expériences réelles des responsables informatiques et des responsables cybersécurité face aux ransomwares et illustre clairement la réalité à laquelle les entreprises seront confrontées en 2023. Le rapport dévoile les causes premières à l'origine des attaques et met en lumière la manière dont ces attaques diffèrent en fonction du chiffre d'affaires de l'entreprise. Il révèle également l'impact commercial et opérationnel du paiement d'une rançon dans le but de récupérer des données plutôt que d'utiliser des sauvegardes.

À propos de l'enquête

Sophos a commandé une enquête indépendante auprès de 3 000 responsables informatiques et responsables cybersécurité travaillant dans des entreprises comptant entre 100 et 5 000 employés dans 14 pays répartis sur le continent américain, dans la région EMEA et dans la région Asie-Pacifique. Cette enquête s'est déroulée entre janvier et mars 2023 ; les participants ayant été invités à répondre sur la base de leurs expériences vécues en 2022.

Pour le secteur de l'éducation, les participants ont été séparés en deux groupes : enseignement primaire/secondaire et enseignement supérieur.



Sommaire

Taux d'attaques de ransomware

L'étude a révélé que le taux d'attaques par ransomware est resté stable d'une année sur l'autre : 66 % des personnes interrogées ont déclaré que leur entreprise avait été touchée par un ransomware au cours de l'année passée, soit le même pourcentage que dans notre précédente étude réalisée en 2022. Les adversaires étant désormais capables d'exécuter des attaques à grande échelle, le ransomware est sans doute le plus grand cyber risque auquel les entreprises sont confrontées aujourd'hui.

Depuis plusieurs années, les cybercriminels développent et perfectionnent le modèle de « ransomware-as-a-service ». Ce modèle abaisse toutes sortes de barrières et facilite ainsi l'entrée de cybercriminels novices en matière de ransomware, tout en augmentant la sophistication des attaques en permettant aux adversaires de se spécialiser dans différentes étapes d'une attaque. Pour plus d'informations sur les ransomwares « en tant que service », consultez le Rapport Sophos 2023 sur les menaces.

2020	2021	2022	2023
51 %	37 %	66 %	66 %

Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ?
Oui. n=3 000 (2023), 5 600 (2022), 5 400 (2021), 5 000 (2020)

Attaques par pays

Si le taux global d'attaques de ransomware signalées reste stable par rapport à 2022, l'enquête a révélé des variations selon les pays. Singapour a subi le plus grand nombre d'attaques de ransomware cette année, avec 84 % des entreprises touchées en 2022. À l'inverse, c'est au Royaume-Uni que le nombre d'attaques signalées est le plus faible (44 %).

La plus forte baisse du nombre d'attaques a été enregistrée en Autriche, où le pourcentage d'entreprises touchées est passé de 84 % à 50 % en un an. À l'inverse, la plus forte augmentation du nombre d'attaques a été enregistrée en Afrique du Sud, où 78 % des entreprises signalent avoir été touchées dans notre rapport 2023, contre 51 % un an plus tôt.

Pour plus de détails, consultez la section Taux d'attaques de ransomware par pays : 2022 vs 2023 à la page 20.

Attaques par secteur

Le secteur de l'éducation est celui où la probabilité d'une attaque de ransomware a été la plus forte en 2022 : 80 % des établissements du primaire et du secondaire et 79 % du supérieur ont déclaré avoir été touchés. L'éducation est traditionnellement confrontée à des budgets moindres et des technologies inférieures à celles de nombreux autres secteurs, et les données montrent que les adversaires savent profiter de ces faiblesses.

Le secteur de l'informatique, des technologies et des télécoms est celui qui a subi le moins d'attaques (50 %), ce qui indique un niveau plus élevé de cyber préparation et de cyberdéfenses.

Pour plus de détails, consultez la section Taux d'attaques de ransomware par secteur en page 21.

66 % touchés par un ransomware

Singapour plus fort taux d'attaques (pays)

Royaume-Uni plus faible taux d'attaques (pays)

Éducation plus fort taux d'attaques (secteur)

IT, technologies et télécoms plus faible taux d'attaques (secteur)

Attaques par taille de l'entreprise : employés vs chiffre d'affaires

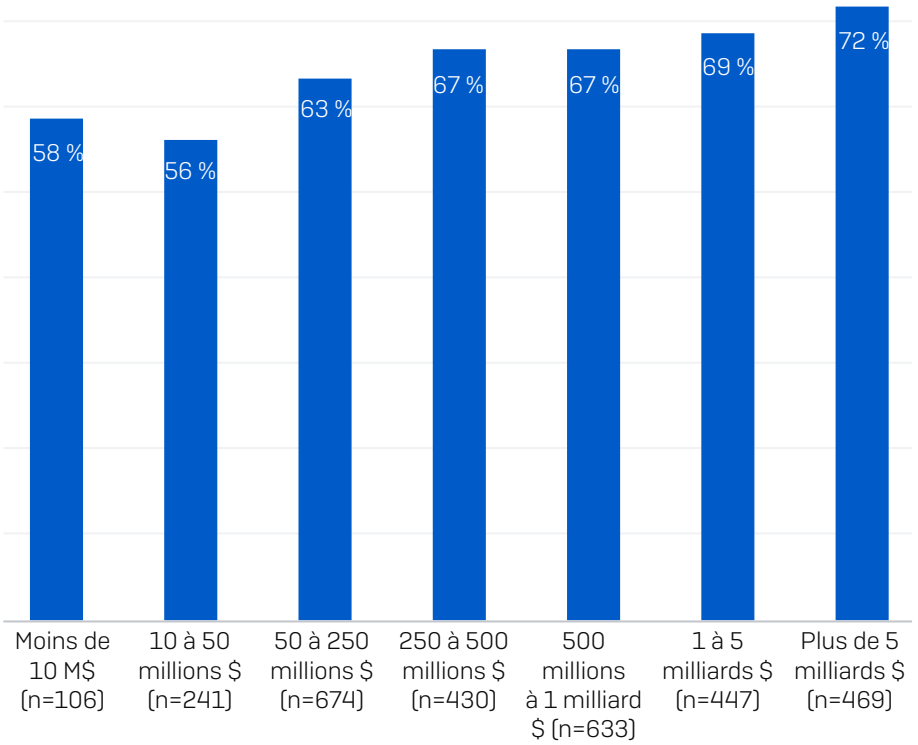
L'étude a révélé une corrélation nette entre le chiffre d'affaires annuel d'une entreprise et sa propension à subir une attaque de ransomware ; le pourcentage d'entreprises touchées par un ransomware augmentant progressivement avec le chiffre d'affaires. 56 % des entreprises dont le chiffre d'affaires se situe entre 10 et 50 millions de dollars ont subi une attaque de ransomware en 2022, allant jusqu'à 72 % pour celles dont le chiffre d'affaires est supérieur à 5 milliards de dollars.

À l'inverse, il n'y a pas de relation claire entre le fait d'être victime d'un ransomware et le nombre d'employés de l'entreprise. Hormis le segment '1 001 à 3 000 employés', le taux d'attaques de ransomware est très constant :

- 100-250 employés 62 %
- 251-500 employés 62 %
- 501-1 000 employés 62 %
- 1 001-3 000 employés 73 %
- 3 001-5 000 employés 63 %

Les données montrent que, du point de vue de la taille de l'entreprise, le chiffre d'affaires annuel est un indicateur beaucoup plus important quant à la probabilité d'être victime d'une attaque que le nombre d'employés.

Pourcentage d'entreprises touchées par un ransomware par chiffre d'affaires

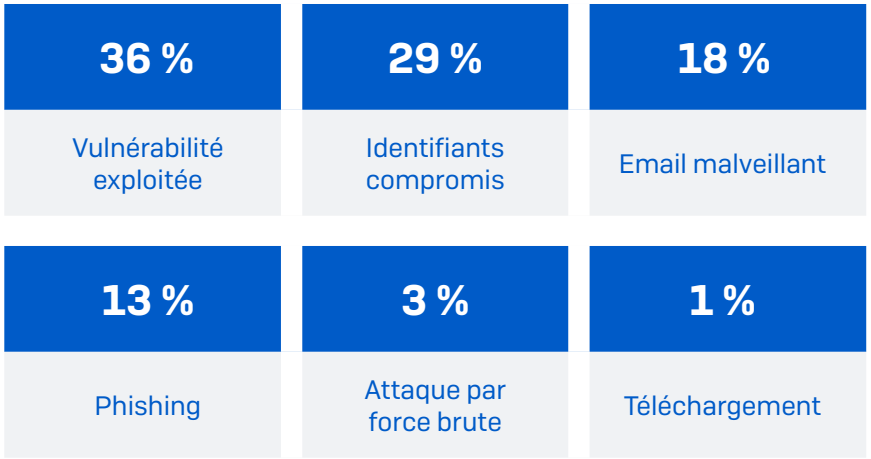


Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Oui. Chiffres de base dans le graphique.

Causes premières des attaques de ransomware

Selon les répondants, lors d'une attaque de ransomware, la cause première la plus fréquente était l'exploitation d'une vulnérabilité (36 %), suivie par la compromission d'identifiants (29 %). Ces résultats s'alignent presque exactement sur la dernière analyse rétrospective de Sophos. Portant sur 152 attaques prises en main par nos équipes de réponse aux incidents et MDR, elle révélait que 37 % d'entre elles avaient commencé par l'exploitation d'une vulnérabilité et 30 % par la compromission d'identifiants.

Les emails ont été à l'origine de 30 % (avec arrondi) des attaques : 18 % ont commencé par un email malveillant et 13 % par un email de phishing. 3 % ont commencé par une attaque par force brute et seulement 1 % par un téléchargement.



Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Si vous avez été touché plus d'une fois, pensez à l'attaque la plus importante. (n=1 974 entreprises touchées par un ransomware en 2022)

Causes premières par secteur

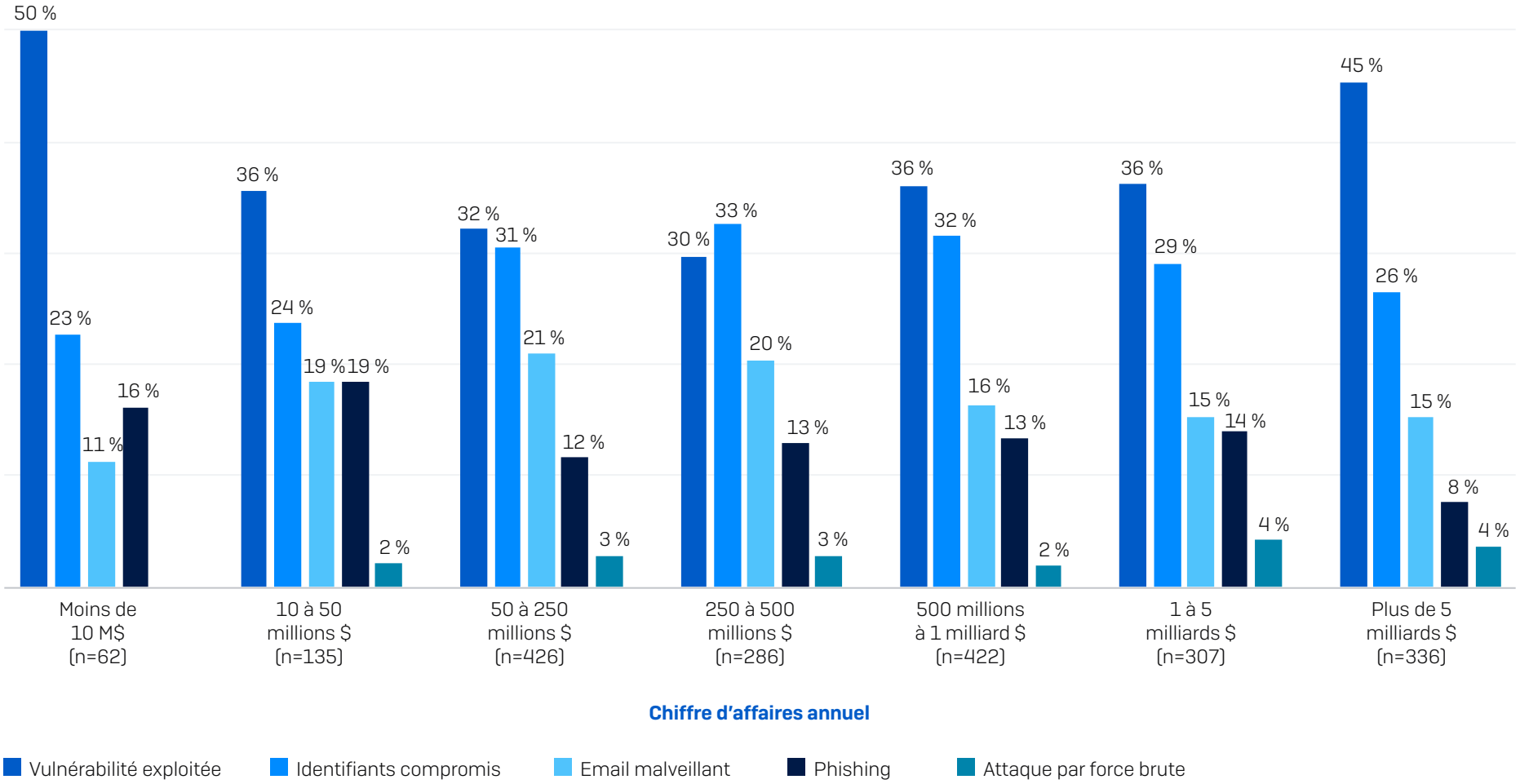
Le secteur des médias, des loisirs et du divertissement a signalé le pourcentage le plus élevé d'attaques dont la cause première était l'exploitation d'une vulnérabilité (55 %), ce qui indique des lacunes de sécurité généralisées dans ce domaine. L'administration centrale/fédérale a enregistré le pourcentage le plus élevé d'attaques ayant pour origine des identifiants compromis (41 %). Cela peut s'expliquer par un taux plus élevé de vols d'identifiants dans ce secteur, une capacité moindre à empêcher l'exploitation des identifiants volés, ou une combinaison des deux.

Le secteur de l'informatique, des technologies et des télécoms affiche les taux les plus faibles de vulnérabilités exploitées (22 %) et d'identifiants compromis (22 %), ce qui reflète probablement les niveaux élevés de cyberdéfense dans ce secteur. Cependant, ce secteur a signalé les taux les plus élevés d'attaques par email, dont plus de la moitié (51 %) sont parties des boîtes de réception d'utilisateurs.

Pour plus de détails, consultez la section Causes premières des attaques par secteur en page 22.

Causes premières par chiffre d'affaires

L'analyse des causes premières en fonction du chiffre d'affaires annuel révèle que l'exploitation de vulnérabilités et la compromission d'identifiants suivent des courbes de propension opposées. Les pourcentages les plus élevés d'attaques ayant commencé par l'exploitation d'une faille ont été rapportés par les entreprises dont le chiffre d'affaires est le plus faible (moins de 10 millions de dollars : 50 %) et le plus élevé (5 milliards de dollars et plus : 45 %), pour descendre à 30 % dans la cohorte intermédiaire (250 à 500 millions de dollars). Inversement, l'utilisation d'identifiants compromis atteint son paroxysme dans la cohorte du chiffre d'affaires moyen (33 %), tandis que l'utilisation la plus faible est signalée dans les cohortes du chiffre d'affaires le plus faible (23 %) et le plus élevé (26 %).

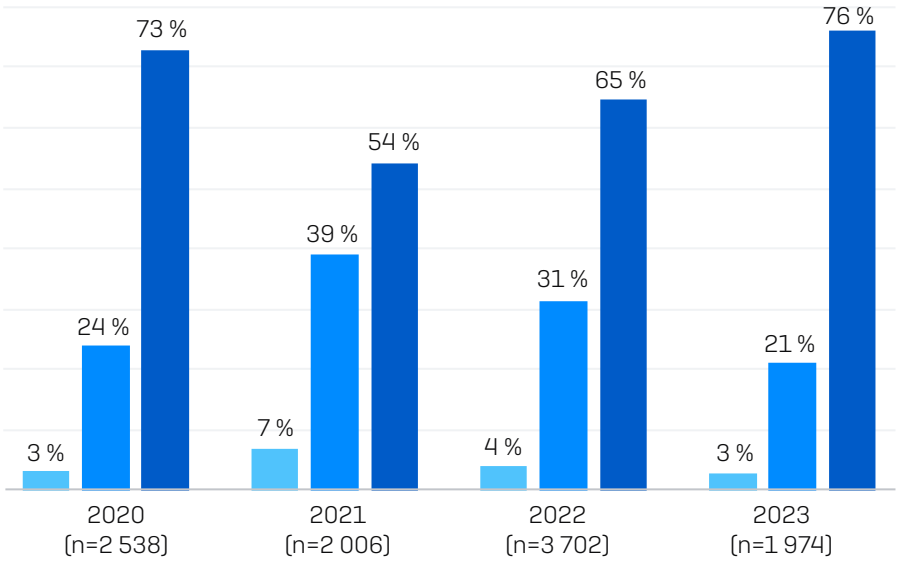


Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Sélection des options de réponse. Chiffres de base dans le graphique.

Taux de chiffrement des données

Le chiffrement des données a continué d'augmenter, les adversaires réussissant à chiffrer les données dans plus des trois quarts (76 %) des attaques de ransomware. Dans les faits, les niveaux de chiffrement n'ont jamais été aussi élevés que ces quatre dernières années. Cela reflète probablement le niveau de compétence toujours plus élevé des adversaires qui continuent d'innover et d'affiner leurs approches.

Lors de l'attaque de ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ?



Non – Les données n'ont pas été chiffrées, mais une rançon a tout de même été demandée (extorsion)
Non – L'attaque a été stoppée avant que les données ne soient chiffrées
Oui – Les données ont été chiffrées

Chiffrement des données par secteur

Presque tous les secteurs peinent à bloquer les attaques avant que les données ne puissent être chiffrées : à une exception près, tous secteurs confondus, plus des deux tiers des attaques ont abouti au chiffrement des données. La fréquence la plus élevée de chiffrement des données (92 %) a été signalée par le secteur des services aux entreprises et des services professionnels.

Le secteur de l'informatique, des technologies et des télécoms est celui qui va à l'encontre de la tendance, les adversaires parvenant à chiffrer les données dans moins de la moitié (47 %) des attaques. Il s'agit là d'un autre indicateur du niveau élevé des cyberdéfenses et de la préparation à la réponse aux incidents de ce secteur.

Pour plus de détails, consultez la section Chiffrement des données par secteur en page 23.

Vol de données

Dans 30 % des attaques où des données ont été chiffrées, des données ont également été volées. Cette approche dite du « double dip » devient de plus en plus courante, car les adversaires cherchent tous les moyens possibles de monétiser leurs attaques. Ils peuvent menacer de rendre publiques des données volées pour extorquer de l'argent ou même vendre ces données. Le nombre élevé des vols de données accroît l'importance de stopper les attaques le plus tôt possible, avant que les informations ne soient exfiltrées.

30 %
des attaques de ransomware où les données ont été chiffrées, des données ont également été volées.

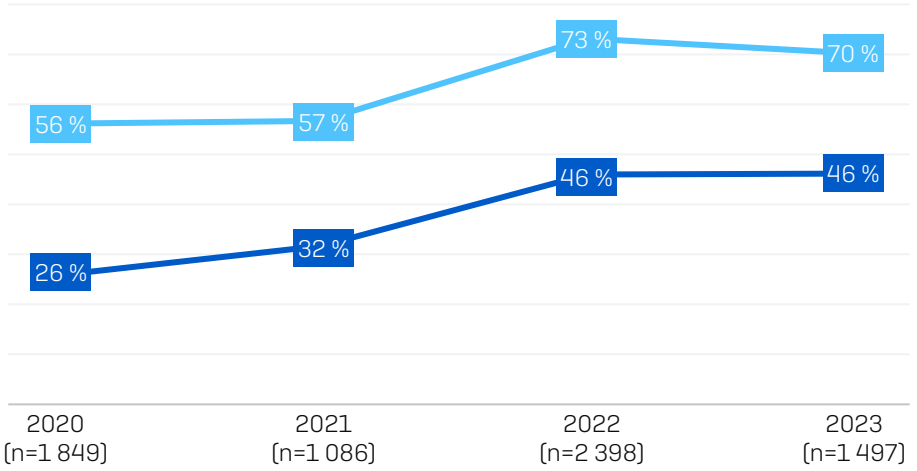
Lors de l'attaque de ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? Oui ; Oui, et les données ont également été volées. n=1 497

Récupération des données

97 % des entreprises dont les données ont été chiffrées ont réussi à en récupérer. Les sauvegardes étaient l'approche la plus courante, utilisées dans 70 % des incidents. 46 % ont payé la rançon et récupéré des données, tandis que 2 % ont utilisé d'autres moyens. Dans l'ensemble, une entreprise sur cinq (21 %) a eu recours à plusieurs méthodes pour restaurer ses données. 1 % des entreprises dont les données ont été chiffrées ont payé la rançon, mais n'ont pas récupéré leurs données.

Ont utilisé des sauvegardes pour restaurer leurs données	Ont payé la rançon et ont récupéré leurs données	Ont utilisé d'autres moyens pour récupérer leurs données
70 %	**46 %**	**2 %**

Il est inquiétant de constater que l'utilisation des sauvegardes pour récupérer des données a chuté par rapport à l'année précédente, où elles étaient utilisées dans 73 % des cas. Le taux de paiement de la rançon est resté stable par rapport à l'année précédente.



Votre entreprise a-t-elle récupéré des données ? Oui, nous avons payé la rançon et avons récupéré des données ; Oui, nous avons utilisé des sauvegardes pour restaurer les données. Chiffres de base dans le graphique.

Récupération des données par pays

Dans l'ensemble, les personnes interrogées dans la région EMEA (Europe, Moyen-Orient, Afrique) ont déclaré des niveaux plus élevés d'utilisation des sauvegardes (75 %) et des niveaux plus faibles de paiement de la rançon (40 %) que celles du continent américain (65 %/55 %) et de la région Asie-Pacifique (67 %/49 %). Au niveau national, c'est en France que le taux d'utilisation des sauvegardes est le plus élevé (87 %), suivi de près par la Suisse (84 %).

L'importance des sauvegardes est démontrée par le fait que les deux pays les moins à même d'utiliser des sauvegardes pour restaurer des données, l'Italie (55 %) et Singapour (57 %), sont également les deux pays qui ont enregistré les taux de récupération de données les plus faibles (93 % et 90 %, respectivement). C'est également en Italie que la propension à payer la rançon est la plus élevée (56 %), suivie de près par les États-Unis et le Brésil (55 % chacun).

Dans la plupart des cas, les entreprises ayant payé la rançon ont pu récupérer des données. Toutefois, en France et au Royaume-Uni, environ une entreprise sur dix ayant payé la rançon n'a pas récupéré ses données.

Pour plus de détails, consultez la section Récupération des données par pays en page 24.

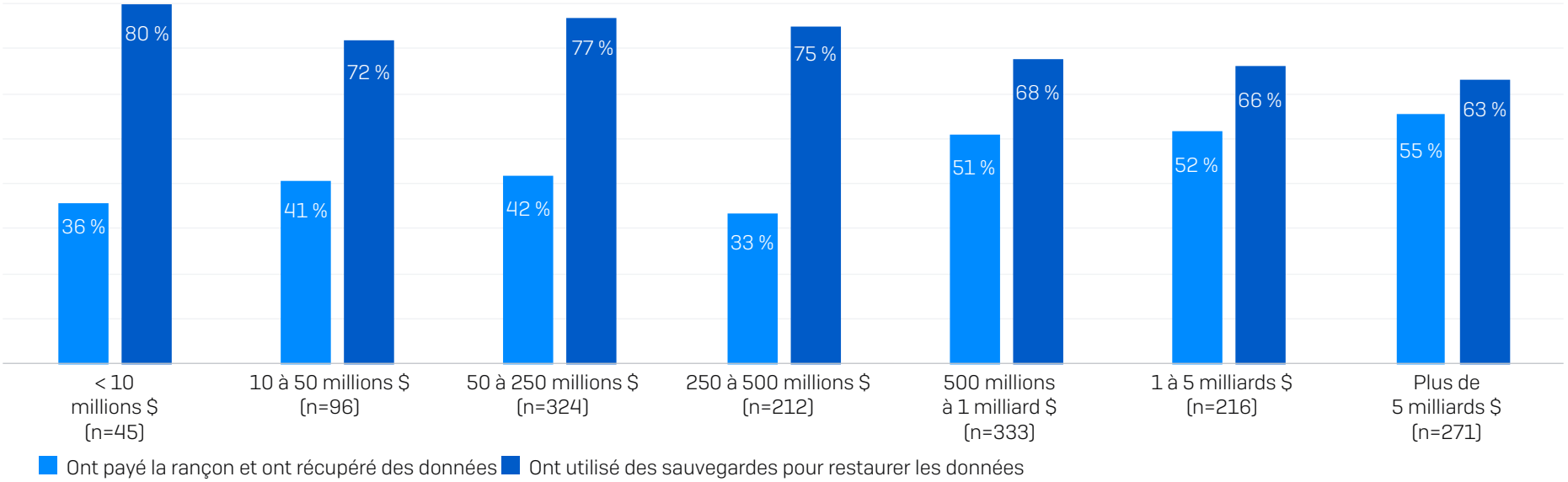
Paiement de la rançon et utilisation de sauvegardes par chiffre d'affaires

D'une manière générale, plus le chiffre d'affaires annuel augmente, plus la propension d'une entreprise à récupérer des données en payant une rançon augmente. Dans le même temps, la fréquence d'utilisation des sauvegardes diminue.

Parmi les entreprises dont le chiffre d'affaires est supérieur à 5 milliards de dollars, 55 % ont récupéré leurs données en payant la rançon et 63 % ont utilisé des sauvegardes. Dans le même temps, 36 % des entreprises dont le chiffre d'affaires est inférieur à 10 millions de dollars ont récupéré leurs données en payant la rançon, tandis que 80 % ont utilisé des sauvegardes — le taux d'utilisation des sauvegardes le plus élevé de toutes les catégories de chiffre d'affaires.

Les entreprises dont le chiffre d'affaires annuel est le plus faible disposent de moins d'argent pour financer le paiement des rançons, ce qui les oblige à se concentrer sur les sauvegardes pour récupérer les données. Par ailleurs, les entreprises ayant un chiffre d'affaires plus élevé disposent généralement d'infrastructures informatiques complexes, ce qui peut les empêcher d'utiliser les sauvegardes pour récupérer les données en temps voulu. Ce sont également les entreprises les plus à même de payer pour se sortir de telles situations.

Paiement de la rançon et utilisation de sauvegardes par chiffre d'affaires



Votre entreprise a-t-elle récupéré des données ? Oui, nous avons payé la rançon et avons récupéré des données ; Oui, nous avons utilisé des sauvegardes pour restaurer les données. Chiffres de base dans le graphique.

L'impact de la cyberassurance sur la récupération des données

Les entreprises disposant d'une cyberassurance étaient nettement plus susceptibles de récupérer des données chiffrées que celles qui n'avaient pas souscrit à une telle police d'assurance. Toutefois, le type de cyberassurance ne fait guère de différence : 98 % des entreprises ayant souscrit une police d'assurance spécifique cyber et 97 % de celles ayant souscrit une police d'assurance 'classique' avec une clause cyber ont récupéré leurs données. En comparaison, 84 % de ceux qui n'ont pas de police d'assurance ont pu récupérer leurs données chiffrées.

Pourcentage de victimes de ransomware ayant récupéré des données chiffrées

Votre entreprise a-t-elle récupéré des données ? n= 1497 entreprises touchées par un ransomware l'année passée ayant eu des données chiffrées.

Plusieurs facteurs expliquent probablement cet écart. Tout d'abord, les cyberassurances exigent généralement des entreprises qu'elles disposent de sauvegardes et de plans de rétablissement comme conditions de couverture. Les assureurs sont également en mesure de guider les victimes de ransomware tout au long du processus de récupération afin d'optimiser les résultats. En outre, les entreprises ayant souscrit une cyberassurance sont plus susceptibles de payer la rançon pour récupérer leurs données que celles n'ayant pas souscrit à une telle police d'assurance.

Impact de l'assurance sur la propension à payer la rançon

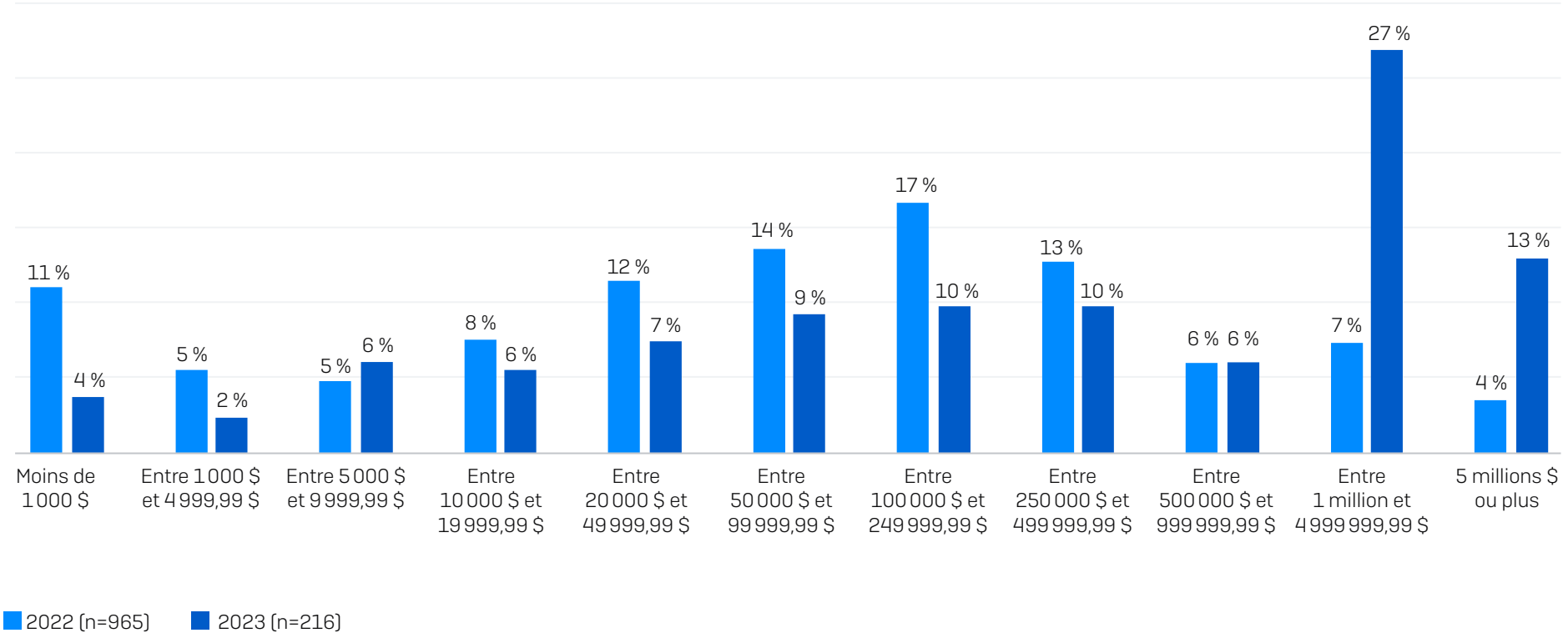
Votre entreprise a-t-elle récupéré des données ? Oui, nous avons payé la rançon et avons récupéré des données. n= 1497 entreprises touchées par un ransomware en 2022 ayant eu des données chiffrées (771 police spécifique cyber, 658 police classique avec clause cyber, 67 pas de police cyber)

Montant des rançons payées

Si la propension globale à payer la rançon reste au même niveau que celle constatée dans notre précédente étude, le montant des paiements a considérablement augmenté au cours de l'année écoulée. Le montant moyen des rançons payées a presque doublé, passant de 812 380 dollars dans notre rapport 2022 à 1 542 333 dollars dans le présent rapport 2023. L'enquête de cette année a révélé que le montant médian des rançons payées était de 400 000 dollars.

L'étude montre une large diversité de montants, mais plus d'entreprises ont payé une rançon plus élevée par rapport à notre étude de 2022 : 40 % d'entre elles ont déclaré un paiement de 1 million de dollars ou plus, contre 11 % dans notre précédente étude. À l'inverse, 34 % seulement ont payé moins de 100 000 dollars, contre 54 % dans notre précédente étude.

Paiement de la rançon : 2023 vs 2022



Quel était le montant de la rançon payée aux attaquants ? À l'exclusion des réponses « Ne sait pas ».

Montant des rançons payées par chiffre d'affaires

Il n'est peut-être pas surprenant de constater que les entreprises ayant le chiffre d'affaires le plus élevé sont les plus susceptibles de payer les rançons les plus chères. Cela montre que les adversaires ajustent les montants en fonction de la capacité à payer de l'entreprise ciblée. L'étude ne distingue pas les paiements pris en charge par les entreprises de ceux couverts par les assureurs.

Il est intéressant de noter qu'il y a très peu de différence entre la moyenne et la médiane du montant des rançons payées par les entreprises dont le chiffre d'affaires est compris entre 250 et 500 millions de dollars et entre 500 et 1 milliard de dollars.

	50 À 250 MILLIONS $ (N=37)	250 À 500 MILLIONS $ (N=33)	500 MILLIONS À 1 MILLIARD $ (N=72)	1 À 5 MILLIARDS $ (N=45)	PLUS DE 5 MILLIARDS $ (N=21)
Montant moyen de la rançon	690 996 $	1 523 652 $	1 466 240 $	2 049 817 $	2 464 339 $
Montant médian de la rançon	145 000 $	428 000 $	425 000 $	1 000 000 $	3 000 000 $

Quel était le montant de la rançon payée aux attaquants ? À l'exclusion des réponses « Ne sait pas ». Excluant les entreprises dont le chiffre d'affaires annuel est inférieur à 50 millions de dollars en raison de chiffres de base très faibles. Chiffres de base dans le graphique. Les données relatives aux segments ayant reçu moins de 30 réponses ne doivent être considérées que comme indicatives.

Coûts de rétablissement

Le montant de la rançon n'est qu'un élément du coût de rétablissement encouru par l'entreprise après une attaque de ransomware. En excluant le montant de la rançon payée, les entreprises ont déclaré un coût moyen de rétablissement après une attaque de ransomware estimé à 1,82 million de dollars, soit une augmentation par rapport au chiffre de 1,4 million de dollars du rapport 2022 et un alignement sur les 1,85 million de dollars du rapport 2021.

Remarque : la formulation de la question dans les rapports 2021 et 2022 incluait le montant de la rançon payée dans les coûts estimés, mais ce montant a été supprimé de la formulation dans l'enquête 2023. Par conséquent, la comparaison d'une année sur l'autre ne doit être considérée qu'à titre indicatif.

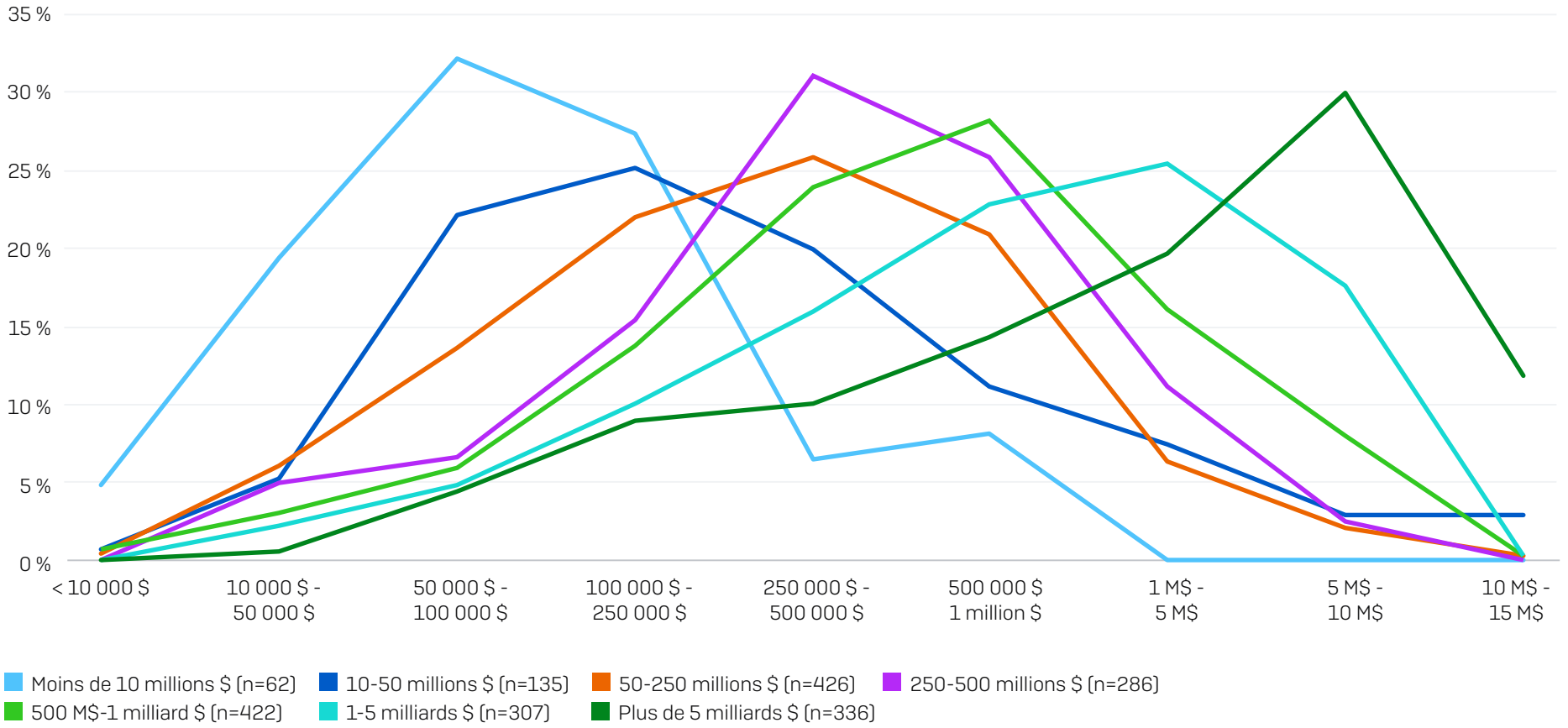
Coût moyen de rétablissement

2021	2022	2023
1,85 M$	1,4 M$	1,82 M$

Quel était le coût approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque de ransomware la plus significative (en prenant en compte les interruptions de services, le temps passé à résoudre l'incident, les coûts matériels, les pertes d'exploitation, etc.)? n=1 974 (2023)/ 3 702 (2022)/ 2 006 (2021). Note : la formulation des questions des rapports 2022 et 2021 incluait également le terme « montant de la rançon ».

Les coûts moyens de rétablissement déclarés commençaient à 165 520 dollars pour les entreprises dont le chiffre d'affaires annuel était inférieur à 10 millions de dollars, pour atteindre 4 496 086 dollars dans la cohorte des 5 milliards de dollars et plus. Bien que ces chiffres masquent tout un éventail de coûts de rétablissement, il existe une tendance claire à l'augmentation des coûts en fonction du chiffre d'affaires, comme l'indique le tableau de la page suivante.

Coût de rétablissement par chiffre d'affaires



Quel était le coût approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque de ransomware la plus significative (en prenant en compte les interruptions de services, le temps passé à la résolution de l'incident, les coûts matériels, les pertes d'exploitation, etc.)? Chiffres de base dans le graphique.

Coût de rétablissement par méthode de récupération des données

Quel que soit l'angle sous lequel on examine les données, pour se rétablir d'une attaque de ransomware, il est nettement moins coûteux d'utiliser des sauvegardes que de payer la rançon. Pour ceux qui ont utilisé des sauvegardes, le coût médian de rétablissement (375 000 dollars) est deux fois moins élevé que pour ceux qui ont payé la rançon (750 000 dollars). De même, le coût moyen de rétablissement est inférieur de près d'un million de dollars pour ceux ayant utilisé des sauvegardes. S'il fallait une preuve supplémentaire de l'intérêt financier d'investir dans une solide stratégie de sauvegarde, la voici.

Ont payé la rançon et ont récupéré leurs données	Ont utilisé des sauvegardes pour restaurer leurs données
750 000 $	**375 000 $**
médiane	médiane
2,6 millions $	**1,62 million $**
moyenne	moyenne

Quel était le coût approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque de ransomware la plus significative (en prenant en compte les interruptions de services, le temps passé à la résolution de l'incident, les coûts matériels, les pertes d'exploitation, etc.) ? n=694 ont payé la rançon et ont récupéré des données et n=1 053 ont utilisé des sauvegardes pour restaurer les données.

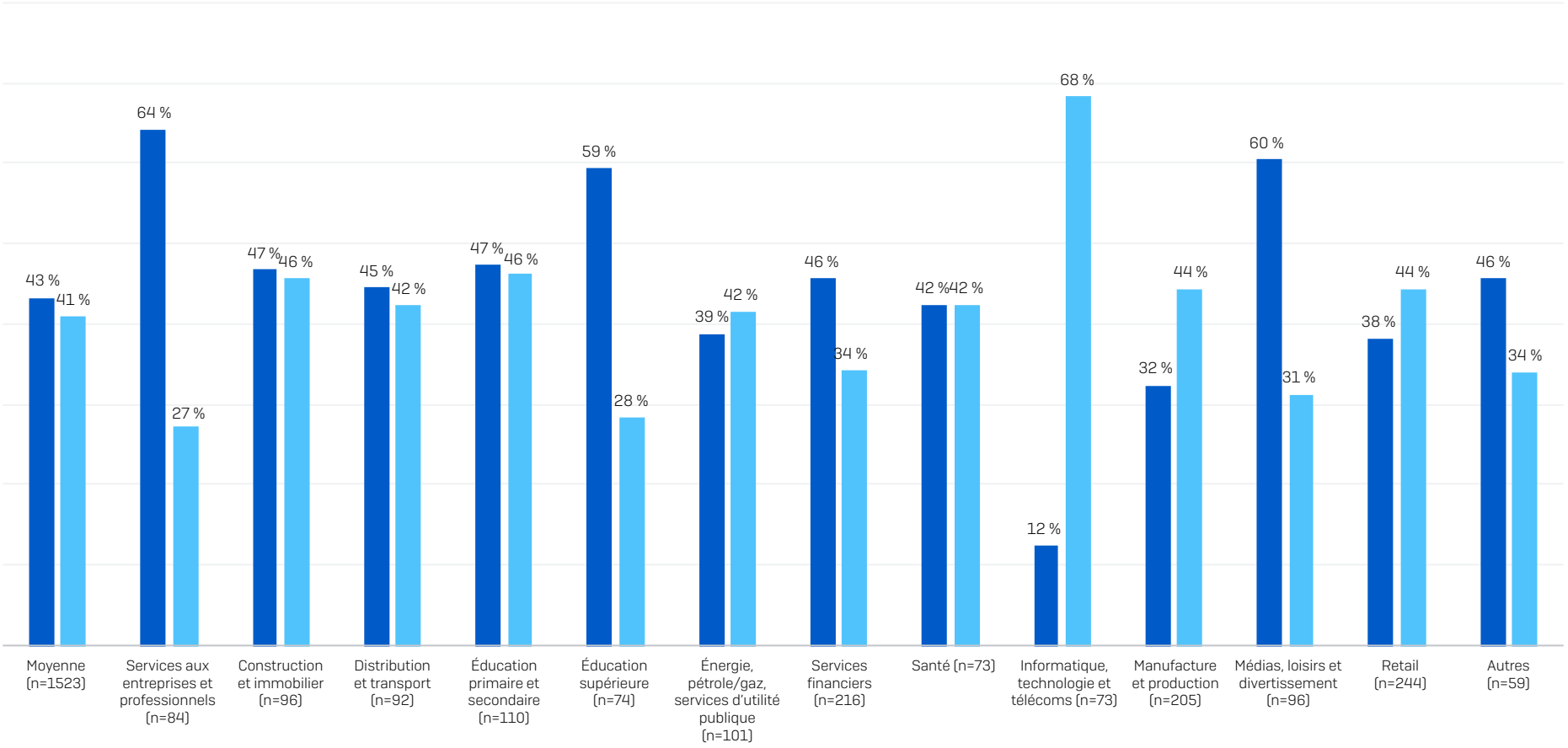
Impact commercial

84 % des entreprises du secteur privé victimes d'un ransomware ont déclaré que l'attaque leur avait fait perdre des activités ou des revenus. Le chiffre d'affaires annuel a un impact relativement faible sur la perte d'activité, le taux le plus bas (79 %) étant enregistré par la cohorte des entreprises au CA de 250 à 500 millions de dollars et le taux le plus élevé (88 %) par celles dont le CA est inférieur à 10 millions de dollars, ainsi que celles à plus de 5 milliards de dollars.

Le type d'industrie a joué un rôle beaucoup plus important dans la propension à subir une perte d'activité ou de revenus. Dans l'ensemble, les secteurs de l'enseignement primaire/secondaire (94 %) et de la construction et de l'immobilier (93 %) étaient les plus susceptibles de signaler une perte d'activités/de revenus due aux attaques, tandis que le secteur manufacturier et de production était le moins susceptible de subir une perte d'activités/de revenus (77 %).

En approfondissant, nous constatons des variations considérables dans les secteurs qui ont déclaré avoir subi « beaucoup » de pertes d'activités/de revenus. Le secteur des services aux entreprises et des services professionnels (64 %) est plus de cinq fois plus susceptible d'avoir subi ce niveau d'impact que le secteur de l'informatique, des technologies et des télécoms (12 %).

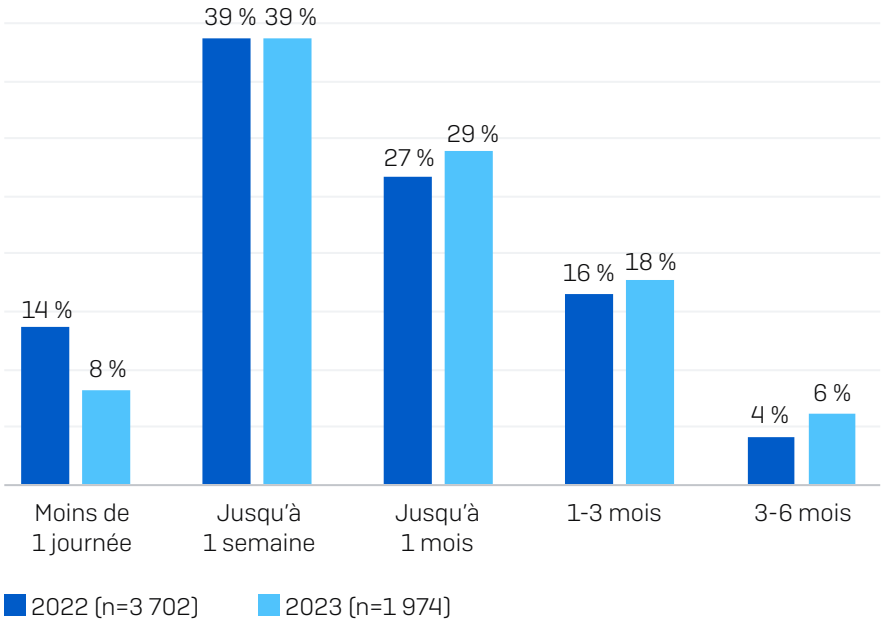
Perte d'activité/de revenus par secteur



L'attaque de ransomware a-t-elle entraîné une perte d'activité ou de revenus ? Oui, nous avons subi une perte importante d'activités/de revenus ; Oui, nous avons subi une légère perte d'activités/de revenus. Entreprises du secteur privé victimes d'un ransomware, chiffres de base dans le tableau

Temps de rétablissement

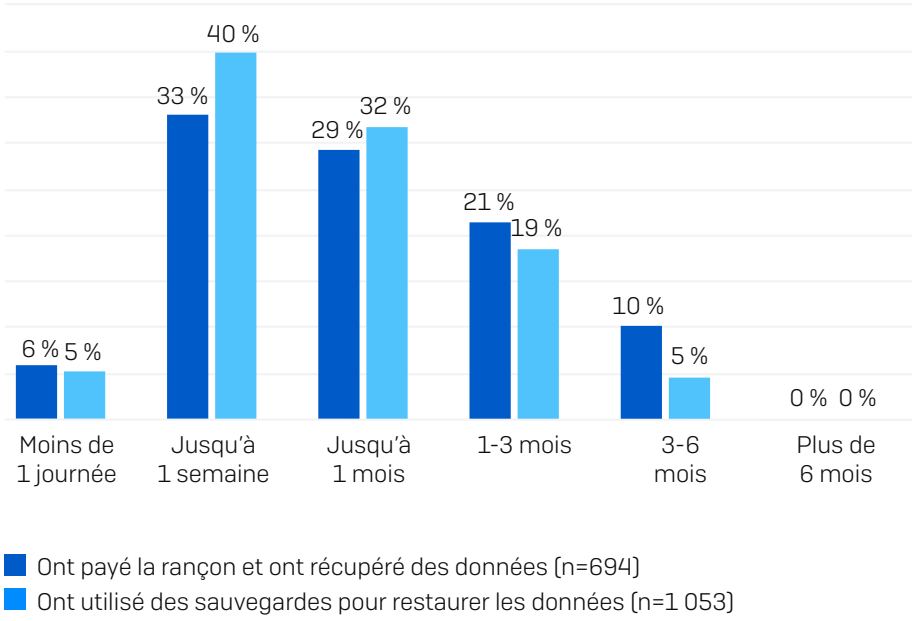
Si le temps de rétablissement après une attaque de ransomware est globalement conforme au rapport 2022, le pourcentage de personnes ayant pu se rétablir en moins d'un jour est passé de 14 % à 8 %.



Combien de temps a-t-il fallu à votre entreprise pour se rétablir complètement après l'attaque de ransomware ? Chiffres de base dans le graphique.

Temps de rétablissement par méthode de récupération des données

L'étude a révélé que les entreprises utilisant des sauvegardes pour récupérer leurs données se rétablissent plus rapidement que celles ayant payé une rançon. 45 % des entreprises ayant utilisé des sauvegardes ont récupéré leurs données en moins d'une semaine, contre 39 % de celles ayant payé une rançon. Près d'un tiers (32 %) de ceux ayant payé une rançon ont mis plus d'un mois à se rétablir, alors que le chiffre pour ceux ayant utilisé des sauvegardes est de 23 % (avec les arrondis). Bien que ces deux options de réponse ne s'excluent pas mutuellement et que certaines personnes interrogées aient à la fois payé la rançon et utilisé des sauvegardes, l'avantage des sauvegardes dans le processus de rétablissement est évident.



Combien de temps a-t-il fallu à votre organisation pour se remettre complètement de l'attaque de ransomware ? Entreprises ayant payé la rançon ou utilisé des sauvegardes pour récupérer leurs données. Chiffres de base dans le graphique.

Conclusion

Indépendamment du chiffre d'affaires, de la localisation ou de l'industrie, les ransomwares restent une menace majeure pour les entreprises. Alors que les adversaires continuent d'affiner leurs tactiques, techniques et procédures d'attaque (TTP), les défenseurs peinent à suivre le rythme, ce qui se traduit par une augmentation du taux de chiffrement.

La baisse de l'utilisation des sauvegardes pour récupérer les données chiffrées est une réelle source d'inquiétude. S'il fallait une preuve supplémentaire des avantages financiers et opérationnels d'un investissement dans une stratégie de sauvegarde solide, ce rapport la fournit.

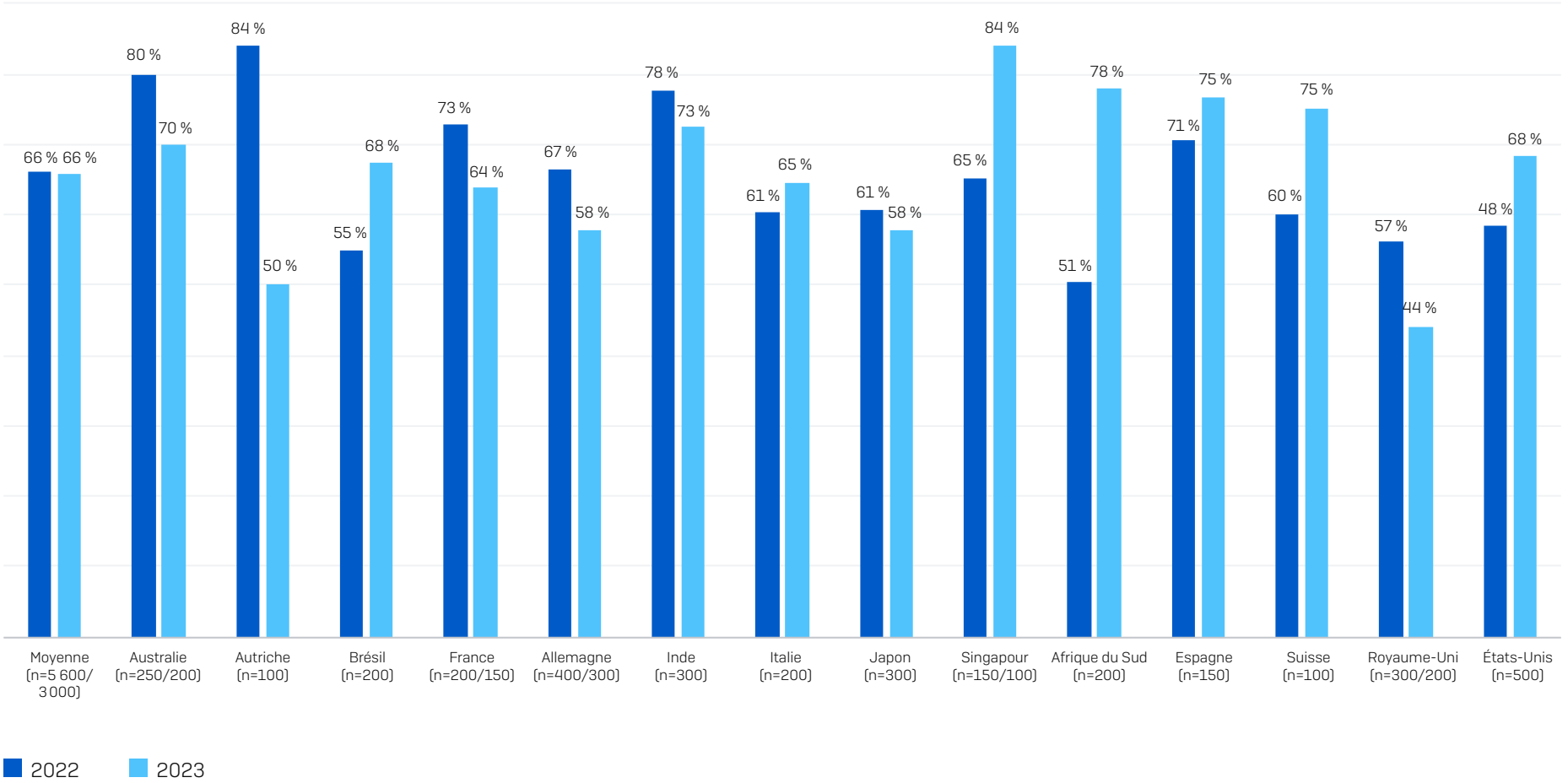
Compte tenu de la croissance du modèle économique « ransomware-as-a-service », nous ne prévoyons pas de baisse des attaques au cours de l'année à venir. Les entreprises devraient concentrer leurs efforts sur :

- Renforcer davantage leurs boucliers défensifs avec :
  - Des outils de sécurité qui protègent contre les vecteurs d'attaque les plus courants, y compris une protection Endpoint dotée de fortes capacités anti-exploit pour empêcher l'exploitation des vulnérabilités et un accès réseau Zero Trust (ZTNA) pour contrecarrer l'utilisation abusive d'identifiants compromis.
  - Des technologies adaptatives qui répondent automatiquement aux attaques, interrompant les adversaires et donnant aux défenseurs le temps de répondre.
  - Une solution de détection des menaces, d'investigation et de réponse 24/7, assurée en interne ou en partenariat avec un fournisseur de services MDR spécialisé.
- Se préparer aux attaques, notamment en effectuant des sauvegardes régulières, en s'entraînant à récupérer les données à partir des sauvegardes et en maintenant à jour un plan de réponse aux incidents.
- Maintenir une bonne hygiène de sécurité, notamment par l'application des correctifs le plus tôt possible et l'examen régulier de la configuration des outils de sécurité.

Autres graphiques

Taux d'attaques de ransomware par pays : 2022 vs 2023

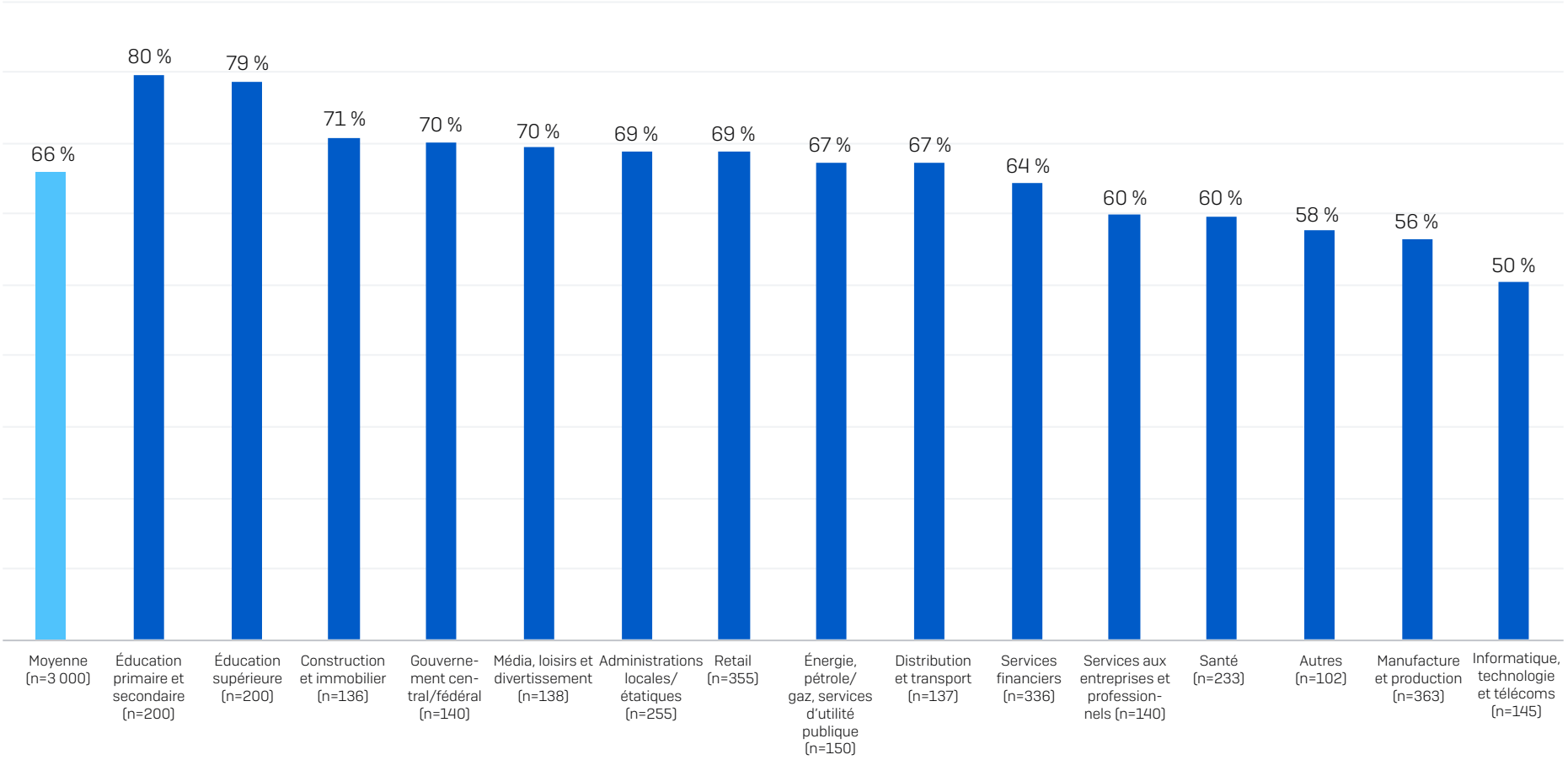
Pourcentage d'entreprises touchées par un ransomware



Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Chiffres de base dans le graphique.

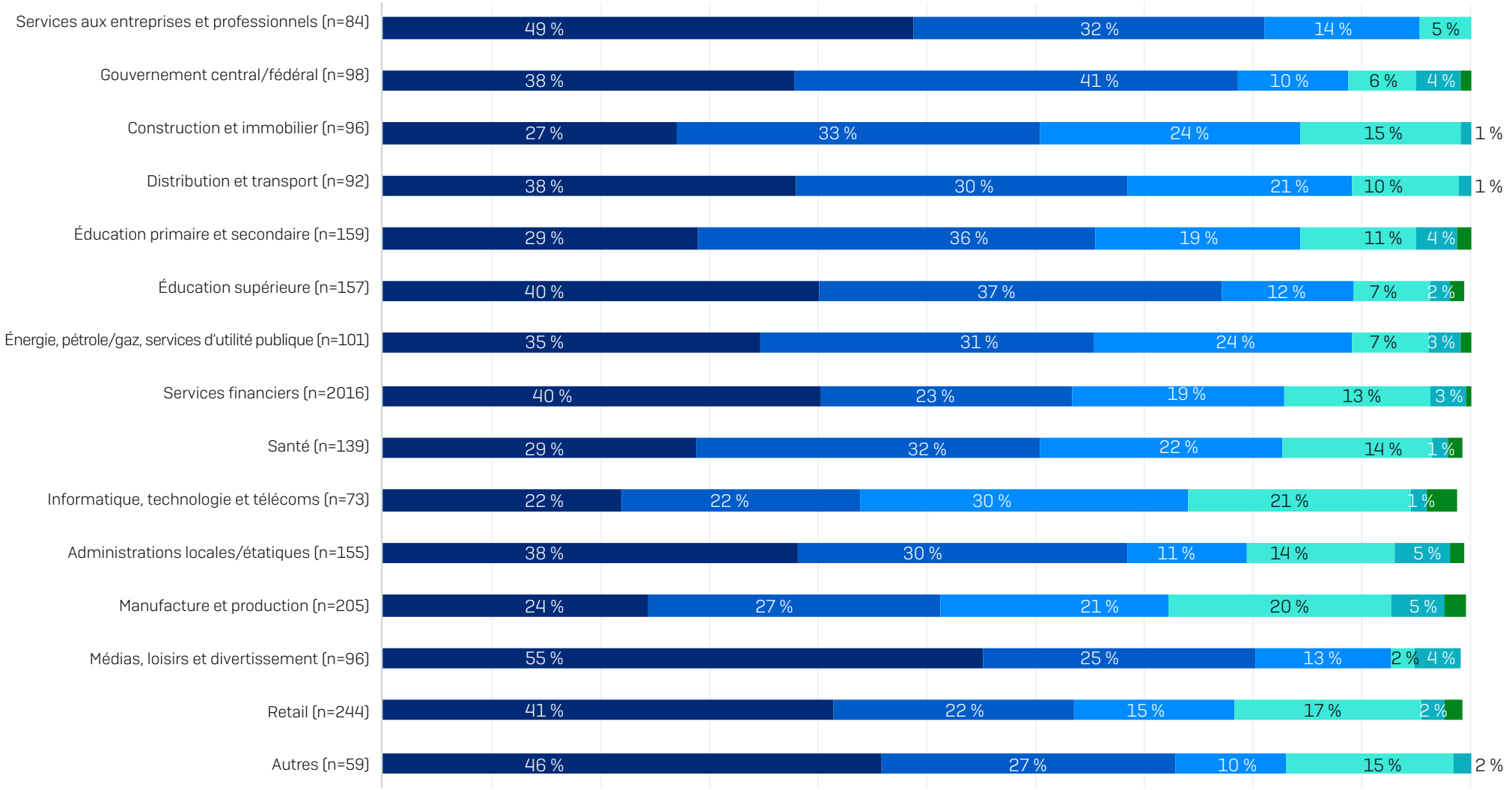
Taux d'attaques de ransomware par secteur

Pourcentage d'entreprises touchées par un ransomware



Au cours de l'année passée, votre entreprise a-t-elle été touchée par un ransomware ? Chiffres de base dans le graphique.

Causes premières de l'attaque par secteur



Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Sélection des options de réponse. Chiffres de base dans le graphique.

Chiffrement des données par secteur

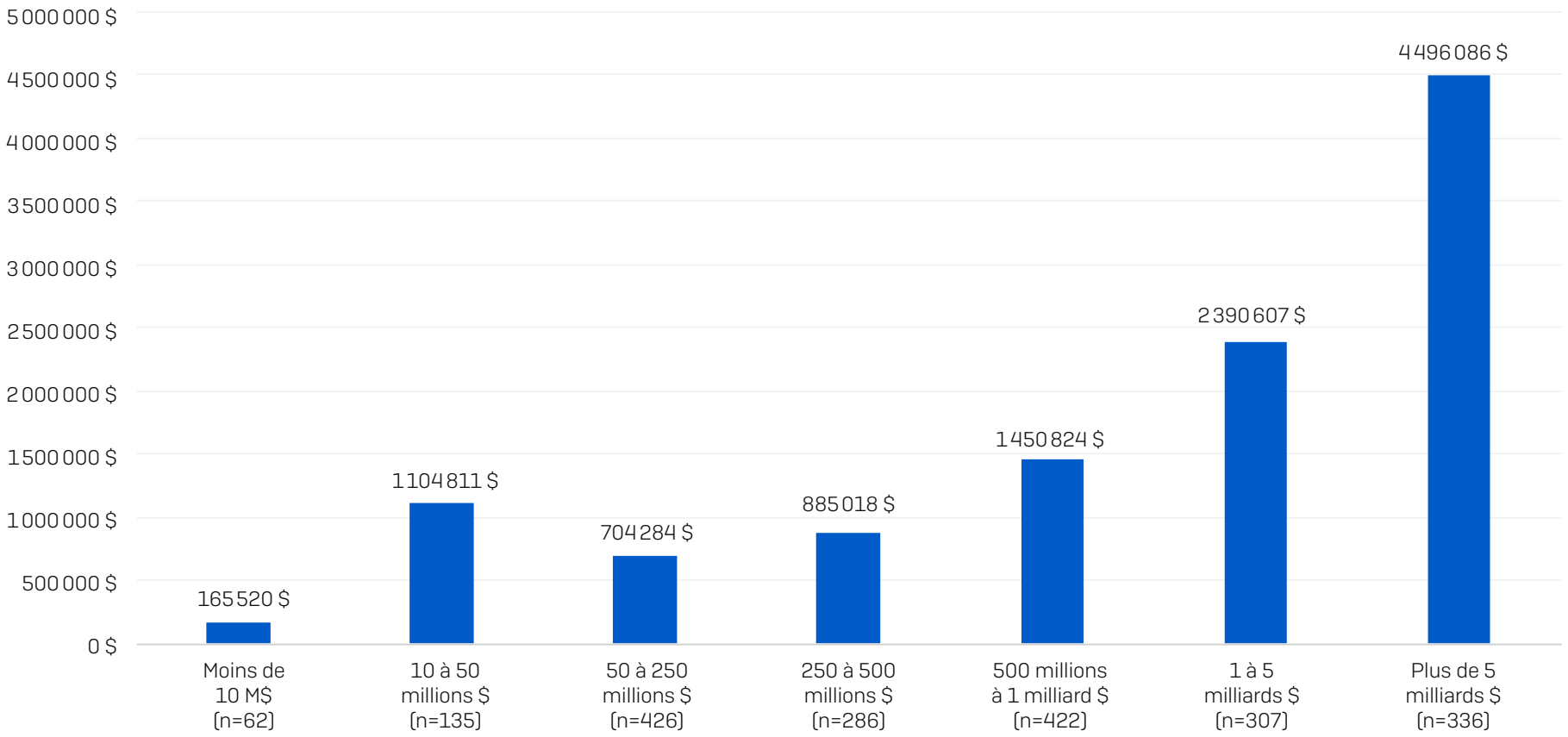
Lors de l'attaque de ransomware, les cybercriminels sont-ils parvenus à chiffrer les données de votre entreprise ? Consolidation des options de réponse. Chiffres de base dans le graphique.

Récupération des données par pays

Votre entreprise a-t-elle récupéré des données ?

	ÉTATS-UNIS (N=274)	BRÉSIL (N=98)	ALLEMA-GNE (N=122)	AUTRICHE (N=48)	SUISSE (N=68)	ROYAUME-UNI (N=66)	ITALIE (N=82)	ESPAGNE (N=93)	FRANCE (N=68)	AFRIQUE DU SUD (N=139)	INDE (N=167)	AUSTRALIE (N=96)	JAPON (N=125)	SINGAPOUR (N=51)
Oui, nous avons payé la rançon et avons récupéré des données	54 %	55 %	44 %	42 %	38 %	44 %	54 %	29 %	22 %	45 %	43 %	53 %	52 %	53 %
Oui, nous avons utilisé des sauvegardes pour restaurer les données	66 %	61 %	78 %	73 %	84 %	68 %	55 %	81 %	87 %	76 %	73 %	73 %	60 %	57 %
Oui, nous avons utilisé d'autres moyens pour récupérer nos données	1 %	4 %	1 %	0 %	3 %	0 %	0 %	0 %	3 %	3 %	3 %	3 %	6 %	0 %
Non, bien que nous ayons payé la rançon	1 %	0 %	0 %	0 %	0 %	5 %	2 %	0 %	3 %	0 %	1 %	0 %	0 %	0 %
Non, nous n'avons pas payé la rançon	0 %	1 %	2 %	2 %	1 %	2 %	5 %	2 %	0 %	0 %	1 %	1 %	5 %	10 %
Ne sait pas	0 %	0 %	2 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %	0 %
Ont récupéré des données par n'importe quelle méthode	99 %	99 %	95 %	98 %	99 %	94 %	93 %	98 %	97 %	100 %	98 %	99 %	95 %	90 %
Ont utilisé plusieurs méthodes pour récupérer les données	22 %	21 %	27 %	17 %	26 %	18 %	16 %	12 %	12 %	24 %	20 %	29 %	22 %	20 %
Paiement de rançon	55 %	55 %	44 %	42 %	38 %	48 %	56 %	29 %	25 %	45 %	44 %	53 %	52 %	53 %
Pourcentage de ceux ayant payé la rançon et n'ayant pas récupéré leurs données	1 %	0 %	0 %	0 %	0 %	9 %	4 %	0 %	12 %	0 %	3 %	0 %	0 %	0 %

Coûts moyens de rétablissement par chiffre d'affaires



Quel était le coût approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque de ransomware la plus significative (en prenant en compte les interruptions de services, le temps passé à la résolution de l'incident, les coûts matériels, les pertes d'exploitation, etc.)? Chiffres de base dans le graphique.

Méthodologie

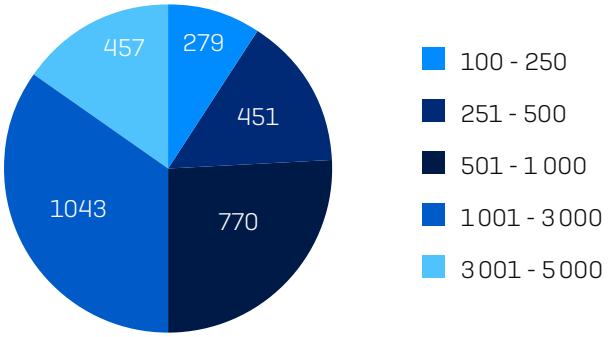
Sophos a commandé une enquête indépendante et agnostique auprès de 3 000 responsables informatiques (RSI) et responsables cybersécurité (RSSI), qui a été réalisée entre janvier et mars 2023. Les personnes interrogées étaient basées dans 14 pays du continent américain, de la région EMEA (Europe, Moyen-Orient, Afrique) et de la région Asie-Pacifique.

Tous les participants appartenaient à des organisations comptant entre 100 et 5 000 employés (50 % 100-1 000 employés, 50 % 1 001-5 000 employés). Au sein de la cohorte d'étude, le chiffre d'affaires annuel allait de moins de 10 millions de dollars à plus de 5 milliards de dollars.

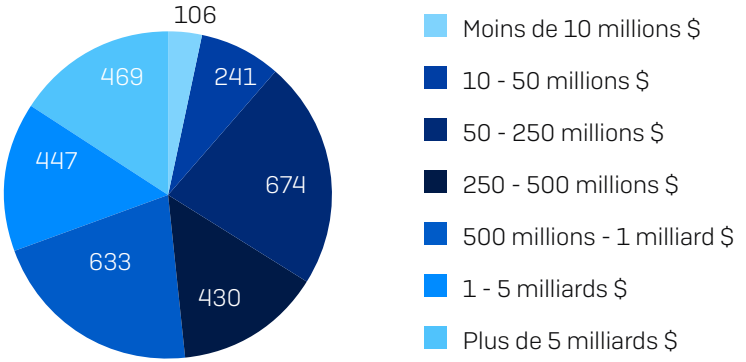
Répondants par pays

PAYS	NOMBRE DE RÉPONDANTS	PAYS	NOMBRE DE RÉPONDANTS
États-Unis	500	Royaume-Uni	200
Allemagne	300	Afrique du Sud	200
Inde	300	France	150
Japon	300	Espagne	150
Australie	200	Autriche	100
Brésil	200	Singapour	100
Italie	200	Suisse	100

Répondants selon la taille de l'entreprise (nombre d'employés)



Répondants selon la taille de l'entreprise (CA annuel)



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.

2023-05-05 (WP-DD)

SOPHOS