SOPHOS

# L'état des ransomwares 2024

**Résultats d'une étude indépendante et agnostique menée entre janvier et février 2024 auprès de 5 000 responsables informatiques/cybersécurité dans 14 pays.**

*Un livre blanc Sophos. Avril 2024*

# Introduction

La cinquième étude annuelle de Sophos sur les expériences réelles des entreprises du monde entier face aux ransomwares explore le parcours complet de la victime, de la cause première à la gravité de l'attaque, en passant par l'impact financier et le temps de rétablissement. De nouvelles informations, combinées aux enseignements tirés de nos études précédentes, dévoilent la réalité à laquelle sont confrontées les entreprises aujourd'hui, ainsi que l'évolution de l'impact des ransomwares au cours des cinq dernières années.

Le rapport de cette année intègre également de nouveaux champs d'études, parmi lesquels l'exploration du montant des demandes de rançon initiales par rapport au paiement final effectué, et étudie davantage dans quelle mesure l'issue d'une attaque de ransomware dépend du chiffre d'affaires de l'entreprise ciblée. De plus, pour la première fois, il met en lumière le rôle des forces de sécurité dans la lutte contre les ransomwares.

## Remarque sur les dates mentionnées

Pour faciliter la comparaison des données entre nos enquêtes annuelles, le nom du rapport correspond à l'année au cours de laquelle l'enquête a été menée : dans le cas présent, 2024. Nous sommes conscients que les entreprises interrogées ont fait part de leurs expériences au cours de l'année précédente, c'est la raison pour laquelle nombre des attaques mentionnées se sont produites en 2023.

## À propos de l'enquête

Le rapport est basé sur les résultats d'une enquête indépendante commandée par Sophos, réalisée auprès de 5 000 responsables informatiques/cybersécurité répartis dans 14 pays sur le continent américain, la région EMEA et la région Asie-Pacifique. Tous les répondants appartiennent à des organisations comptant entre 100 et 5 000 employés. L'enquête a été menée par le cabinet d'études Vanson Bourne, entre janvier et février 2024. Les participants ont été invités à répondre sur la base de leurs expériences au cours de l'année précédente. Pour le secteur de l'éducation, les participants ont été séparés en deux groupes : enseignement des premier et second degrés et enseignement supérieur.

# Taux d'attaques de ransomware

59 % des organisations ont été touchées par un ransomware l'année dernière, un chiffre en légère baisse par rapport aux 66 % rapportés les deux années précédentes. Même si toute évolution à la baisse est encourageante, gardons en tête que plus de la moitié des organisations ont subi une attaque ; ce n'est donc pas le moment de baisser la garde.

| 2020 | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|
| 51 % | 37 % | 66 % | 66 % | 59 % |

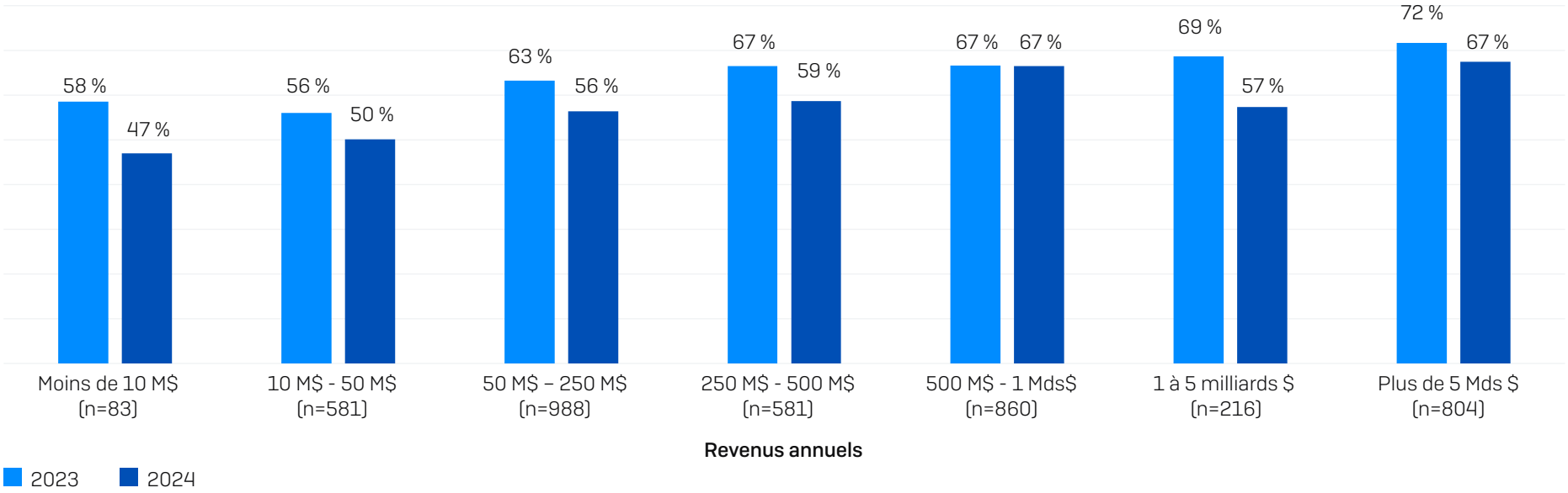
Au cours de l'année passée, votre organisation a-t-elle été touchée par un ransomware ?
Oui. n=5 000 (2024) n=3 000 (2023), 5 600 (2022), 5 400 (2021), 5 000 (2020)

## Attaques - selon le chiffre d'affaires

En 2023, tous les segments de chiffre d'affaires ont connu moins d'attaques de ransomware, ce qui est encourageant (bien que pour la tranche de 500 millions à 1 milliard de dollars, cette réduction soit inférieure à un point de pourcentage).

En général, la propension à être touché par un ransomware augmente avec le chiffre d'affaires ; les entreprises de plus de 5 milliards de dollars affichant le taux d'attaque le plus élevé (67 %). Cependant, même les plus petites entreprises (moins de 10 millions de dollars de chiffre d'affaires) sont encore régulièrement prises pour cible ; un peu moins de la moitié d'entre elles (47 %) ont été touchées par un ransomware en 2023. Si de nombreuses attaques de ransomware sont le fait de gangs sophistiqués et bien financés, le nombre de ransomwares rudimentaires et bon marché lancés par des acteurs moins qualifiés est en augmentation.

**Pourcentage des entreprises touchées par un ransomware au cours de l'année passée**




Au cours de l'année passée, votre organisation a-t-elle été touchée par un ransomware ? Oui. n=5 000 (2024) n=3 000 (2023). Chiffres de base du secteur en 2024 dans le graphique.

## Attaques - selon le secteur d'activité

À quelques exceptions près, les taux d'attaque par ransomware étaient globalement similaires dans les différents secteurs, avec entre 60 % et 68 % des organisations touchées dans 11 des 15 secteurs couverts. Cette année, ceux qui s'en sortent le mieux sont les *administrations publiques* et les entreprises du secteur du *retail*, où moins de la moitié des répondants ont déclaré avoir été touchées au cours de l'année écoulée (respectivement 34 % et 45 %).

Fait intéressant, l'*administration publique centrale* affiche le taux d'attaque le plus élevé, tout secteur d'activité confondu (68 %), soit le double du taux enregistré par l'*administration publique* (34 %). En même temps, reflet de la tendance générale à la baisse du nombre d'attaques, le taux de l'*administration publique centrale* est inférieur au chiffre de 70 % de l'année 2023 pour ce secteur.

Cette différence peut s'expliquer par plusieurs raisons. Il est possible qu'au cours d'une année marquée par des troubles généralisés, les administrations centrales aient été confrontées à une augmentation des attaques pour des motifs politiques. Ces résultats pourraient également être le reflet des efforts déployés au cours de l'année écoulée par les organisations gouvernementales au niveau territorial et local pour renforcer leur résistance aux attaques, ou indiquer un changement d'approche de la part des adversaires en réponse à la capacité limitée du secteur gouvernemental à payer les rançons, et ce tant au niveau territorial que local.

Parmi les autres changements notables survenus dans le secteur en 2023, on peut citer :

- La réduction du taux d'attaque individuel le plus élevé, qui passe de 80 % (*enseignement 1er et 2nd degrés*) à 69 % (*administration publique centrale*).
- Le secteur de l'éducation n'enregistre plus les deux taux d'attaque les plus élevés, avec 66 % (*enseignement supérieur*) et 63 % (*enseignement 1er et 2nd degrés*) cette année, contre 79 % et 80 % respectivement l'année dernière
- *La santé* est l'un des cinq secteurs à avoir connu une augmentation du taux d'attaque au cours de l'année écoulée, passant de 60 % à 67 %.
- *Le secteur de l'informatique, des télécommunications et de la technologie* ne présente plus le taux d'attaque le plus faible avec 55 % des entreprises touchées au cours de l'année écoulée, un chiffre en augmentation par rapport aux 50 % signalés dans le précédent rapport.

Consultez l'annexe pour le détail de la répartition du taux d'attaques de ransomware par secteur d'activité.

## Attaques - selon le pays

La France a enregistré le taux le plus élevé d'attaques de ransomware cette année, avec 74 % des répondants déclarant avoir été touchés en 2023, suivie de l'Afrique du Sud (69 %) et de l'Italie (68 %). Les taux d'attaque les plus faibles ont été rapportés au Brésil (44 %), au Japon (51 %) et en Australie (54 %).

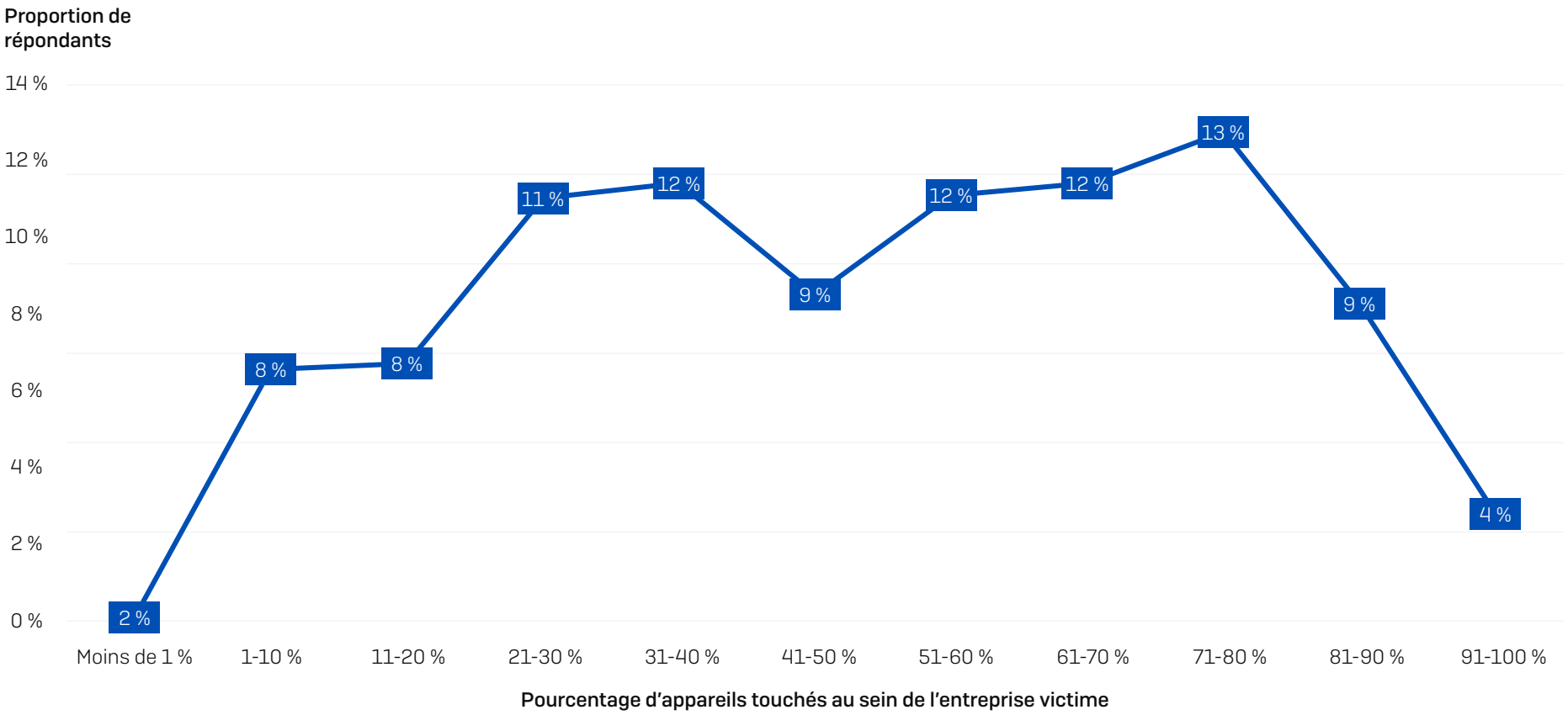
Dans l'ensemble, neuf pays ont fait état d'un taux d'attaque inférieur à celui du rapport précédent. Les cinq pays ayant déclaré une augmentation du nombre d'attaques par rapport à l'étude précédente se trouvent tous en Europe : l'Autriche, la France, l'Allemagne, l'Italie et le Royaume-Uni (l'augmentation pour l'Allemagne est inférieure à 1 %). Cela peut refléter le fait que les entreprises européennes sont davantage ciblées ou indiquer la difficulté des défenses européennes à suivre l'évolution des pratiques des attaquants que dans d'autres régions du monde.

Consultez l'annexe pour le détail de la répartition du taux d'attaques de ransomware selon le pays.

# Pourcentage d'ordinateurs affectés

En moyenne, un peu moins de la moitié (49 %) des ordinateurs d'une entreprise sont touchés lors d'une attaque de ransomware. Un chiffrement malveillant complet de l'environnement est extrêmement rare, puisque seulement 4 % des entreprises déclarent que 91 % ou plus de leurs appareils ont été affectés. Il arrive que certaines attaques n'affectent qu'une poignée d'appareils, mais cela reste également très rare, puisque seulement 2 % des organisations touchées déclarent que moins de 1 % de leurs appareils ont été affectés.

### Pourcentage d'appareils touchés au sein de l'entreprise victime



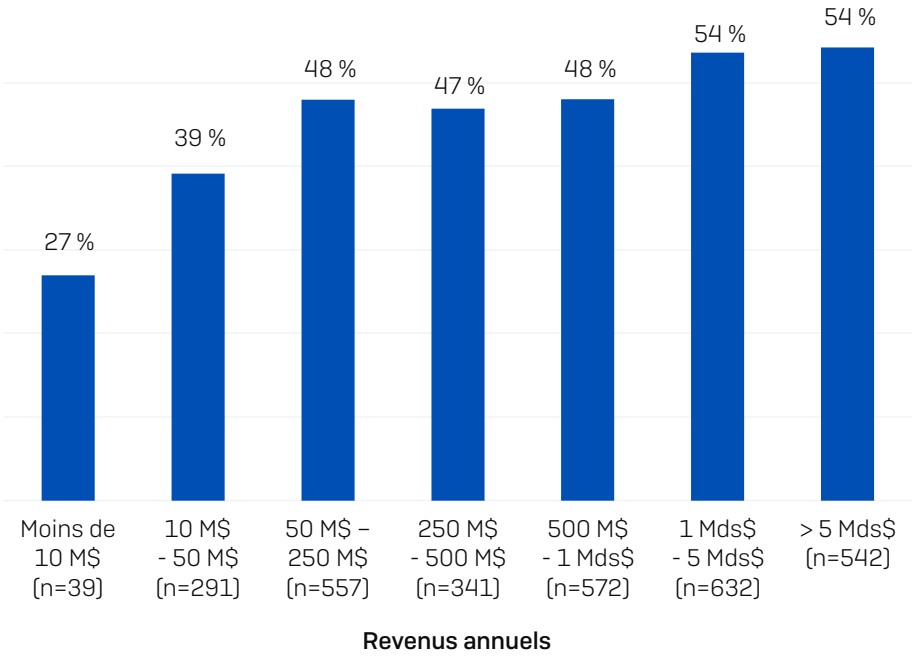

Quel pourcentage des ordinateurs de votre entreprise a été touché par une attaque de ransomware au cours de l'année écoulée ? n=2 974 entreprises touchées par une attaque de ransomware.

## Pourcentage d'ordinateurs affectés - selon le chiffre d'affaires

Si, dans l'ensemble, parmi tous les répondants, la distribution est large, nous constatons des écarts considérables dans les appareils affectés à la fois selon la taille de l'organisation et le secteur d'activité.

Plus le chiffre d'affaires augmente, plus la proportion du parc informatique touché par l'attaque de ransomware augmente. Les plus petites entreprises (moins de 10 millions de dollars) déclarent un pourcentage deux fois moins élevé d'appareils impactés que celles dont le chiffre d'affaires est supérieur ou égal à 1 milliard de dollars (27 % contre 54 %).

Plusieurs facteurs peuvent être à l'origine de cette situation. Les petites entreprises sont moins susceptibles de gérer l'ensemble de leur parc informatique de manière centralisée, ce qui réduit les possibilités de propagation des attaques à l'ensemble du parc. En outre, la plupart des petites entreprises et des startups utilisent massivement les plateformes SaaS, ce qui réduit le risque d'interruption de service dû à des menaces telles que les ransomwares.




Quel pourcentage des ordinateurs de votre entreprise a été touché par une attaque de ransomware au cours de l'année écoulée ? n=2 974 entreprises touchées par une attaque de ransomware.

## Pourcentage d'ordinateurs affectés - selon le secteur d'activité

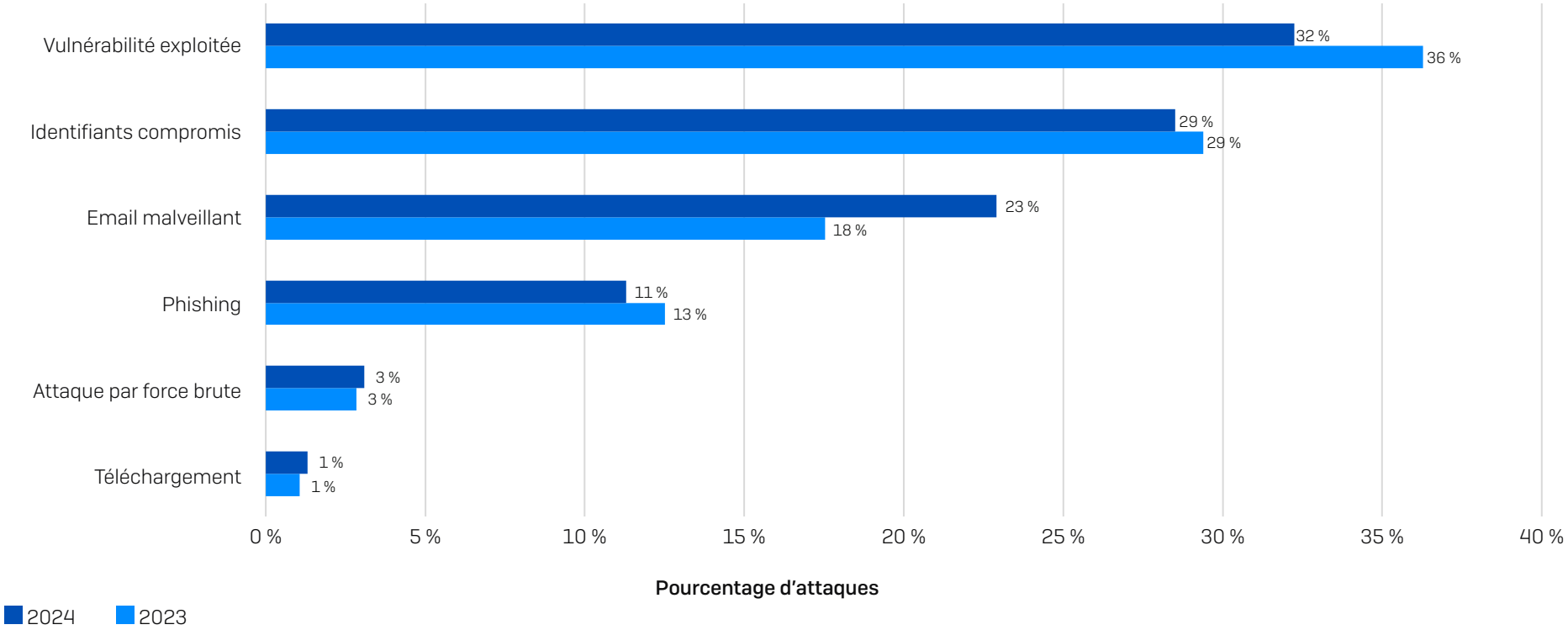
*Le secteur de l'informatique, des technologies et des télécommunications* a enregistré le plus faible pourcentage d'appareils touchés (33 %), ce qui illustre la posture robuste souvent observée de ce secteur en matière de cybersécurité. À l'inverse, le secteur de l'*énergie, du pétrole, du gaz et des services d'utilité publique* est celui où les effets des attaques se font le plus sentir, avec 62 % des appareils touchés en moyenne, suivi par le secteur de la *santé* (58 %). Les deux secteurs doivent composer avec des niveaux plus élevés de contrôle des technologies et des infrastructures que la plupart des autres secteurs, ce qui complexifie sans doute la sécurisation des appareils, la limitation des mouvements latéraux et la prévention de la propagation des attaques.

Consultez l'annexe pour le détail de la répartition du pourcentage d'ordinateurs touché par secteur d'activité.

# Causes premières des attaques de ransomware

99 % des entreprises victimes d'un ransomware ont pu identifier la cause première de l'attaque ; l'exploitation d'une vulnérabilité étant le point de départ le plus souvent identifié pour la deuxième année consécutive. Dans l'ensemble, l'ordre d'exécution reste similaire à celui de notre étude précédente.

34 % des personnes interrogées ont indiqué que les attaques par email étaient la cause première de l'attaque. Environ deux fois plus d'attaques commencent par un email malveillant (c'est-à-dire un message contenant un lien malveillant ou une pièce jointe permettant de télécharger des logiciels malveillants) que par un email de phishing (c'est-à-dire un message conçu pour inciter les lecteurs à révéler des informations). Il est à noter que la technique de phishing est généralement utilisée pour dérober des identifiants de connexion et peut donc être considérée comme la première étape d'une attaque par compromission d'identifiants.




Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? Oui. n= 2 974 organisations touchées par un ransomware

## Attaques par exploitation d'une vulnérabilité

Si toutes les attaques de ransomware ont des résultats négatifs sur les entreprises, certaines ont des conséquences plus désastreuses que d'autres. Les entreprises ayant subi une attaque basée sur l'exploitation d'une vulnérabilité non corrigée font état de conséquences beaucoup plus graves que celles dont l'attaque a commencé par la compromission d'identifiants, notamment d'une plus grande propension à :

- Avoir des sauvegardes compromises (taux de réussite de 75 % contre 54 % pour les identifiants compromis)
- Avoir des données chiffrées (taux de chiffrement de 67 % contre 43 % pour les identifiants compromis)
- Payer la rançon (taux de paiement de 71 % contre 45 % pour les identifiants compromis).
- Prendre en charge l'intégralité du coût de la rançon en interne (31 % ont financé l'intégralité de la rançon en interne, contre 2 % pour les identifiants compromis)

Elles ont également signalé :

- Des coûts globaux de rétablissement 4 fois plus élevés (3 M$ contre 750 000 $ pour les identifiants compromis)
- Temps de rétablissement plus lent (45 % ont mis plus d'un mois contre 37 % pour les identifiants compromis)

Pour en savoir plus, consultez le rapport « Vulnérabilités non corrigées : le vecteur d'attaque de ransomware le plus agressif ».

## Causes premières - selon le secteur d'activité

Certaines failles au niveau des cyberdéfenses sont plus répandues dans certains secteurs que d'autres, et les adversaires sont toujours prompts à les exploiter. Par conséquent, la cause première des attaques de ransomware varie considérablement d'un secteur à l'autre :

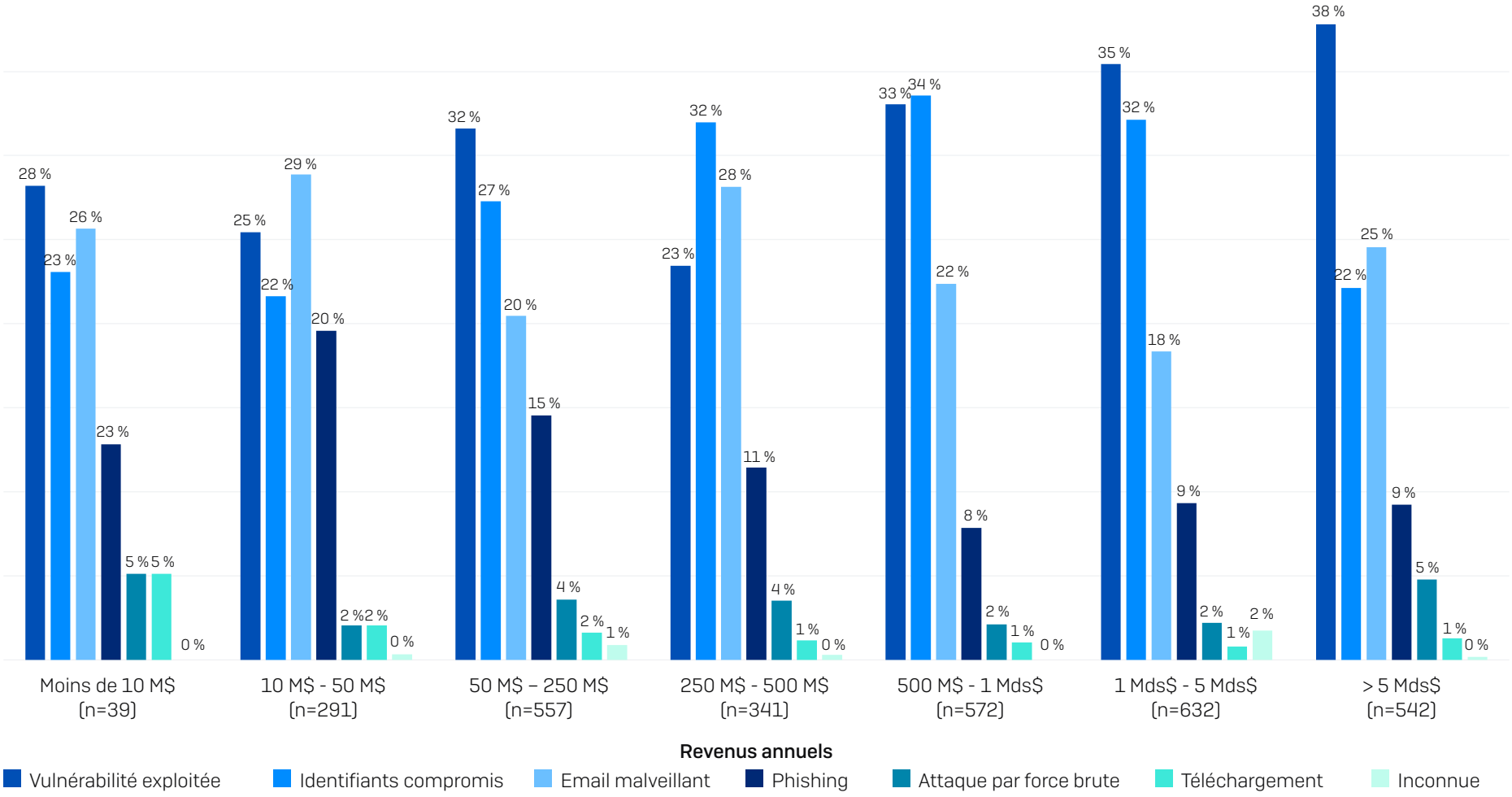
- *Le secteur de l'énergie, du pétrole/gaz et des services d'utilité publique* est le plus susceptible d'être victime d'une exploitation de vulnérabilités non corrigées - près de la moitié (49 %) des attaques commençant de cette manière. Ce secteur fait généralement appel à une plus grande proportion de technologies anciennes, plus sujettes aux failles de sécurité que de nombreux autres secteurs, et il n'existe pas toujours de correctifs pour les systèmes anciens ou en fin de vie.
- Les organisations gouvernementales sont particulièrement vulnérables aux attaques initiées à l'aide d'identifiants compromis : 49 % (*admin. publique*) et 47 % (*admin. publique centrale*) des attaques avaient pour point de départ des identifiants de connexion volés.
- *Les secteurs de l'informatique, des technologies et des télécoms* ainsi que du *retail* ont tous deux indiqué que 7 % des incidents de ransomware ont commencé par une attaque par force brute. Il est possible que leur exposition réduite aux vulnérabilités non corrigées et aux identifiants compromis contraigne les adversaires à privilégier, dans une certaine mesure, d'autres approches.

Consultez l'annexe pour le détail du taux de causes premières d'attaques par secteur d'activité.

## Cause première - selon le chiffre d'affaires

D'une manière générale, les grandes entreprises sont plus susceptibles de subir une attaque dont le point de départ est une vulnérabilité non corrigée ; le segment des entreprises de plus de 5 milliards de dollars affichant le pourcentage le plus élevé d'attaques ayant commencé de cette manière (38 %). Plus les organisations se développent, plus leurs infrastructures informatiques augmentent en taille et en complexité, et plus il est difficile pour les services informatiques de repérer toutes les vulnérabilités et de les corriger avant qu'elles ne soient exploitées.

La compromission des identifiants en tant que vecteur d'attaque de ransomware atteint son maximum dans la cohorte des entreprises générant un chiffre d'affaires moyen/élevé et constitue la principale cause d'attaque dans les segments de 250 millions à 500 millions de dollars et de 500 millions à 1 milliard de dollars. Tandis que les vulnérabilités et les identifiants compromis font à juste titre l'objet d'une grande attention, les emails malveillants sont la cause première signalée par les entreprises ayant un chiffre d'affaires compris entre 10 et 50 millions de dollars. Dans l'ensemble, les menaces véhiculées par des emails représentent un peu moins de la moitié (49 %) des attaques subies par les entreprises appartenant à cette catégorie.




Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? n=2 974 entreprises touchées par un ransomware.

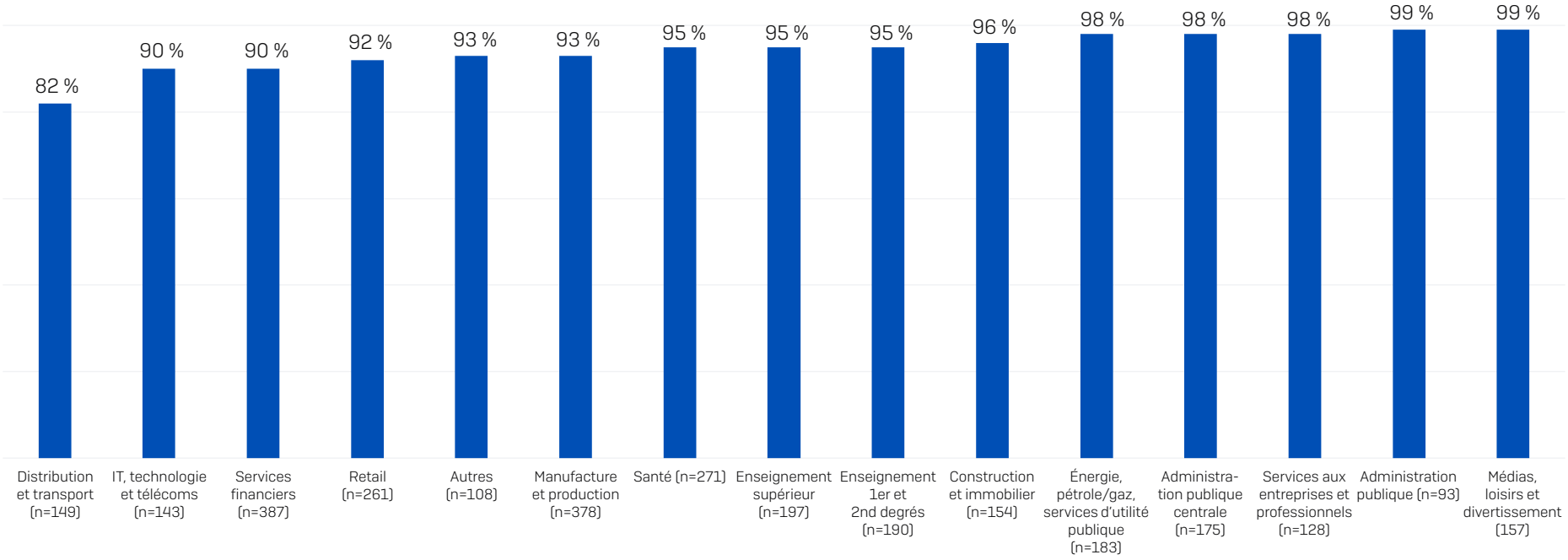
# Compromission des sauvegardes

Il existe deux principaux moyens de récupérer les données chiffrées lors d'une attaque de ransomware : restaurer à partir de sauvegardes ou payer la rançon. En compromettant les sauvegardes d'une organisation, les adversaires limitent la capacité de leur victime à récupérer ses données chiffrées et poussent ainsi la victime à payer la rançon.

## Tentative de compromission des sauvegardes

Parmi les entreprises ayant fait l'objet d'une attaque de ransomware au cours de l'année écoulée, 94 % ont déclaré que les cybercriminels avaient tenté de compromettre leurs sauvegardes au cours de cette attaque. Ce chiffre s'élève à 99 % dans les *administrations publiques*, ainsi que dans le secteur des *médias, des loisirs et du divertissement*. Le taux de tentatives de compromission le plus faible a été enregistré dans le secteur de la *distribution et du transport*, mais même dans ce cas, plus de huit sociétés sur dix (82 %) touchées par un ransomware ont rapporté une tentative d'accès à leurs sauvegardes par les malfaiteurs.

**Pourcentage d'attaques au cours desquelles les adversaires ont tenté de compromettre les sauvegardes**




Les cybercriminels ont-ils tenté de compromettre les sauvegardes de votre entreprise ? Oui. Chiffres de base dans le graphique.

## Taux de réussite des tentatives de compromission des sauvegardes

Tous secteurs confondus, 57 % des tentatives de compromission des sauvegardes ont abouti, ce qui signifie que les adversaires ont été en mesure de compromettre les opérations de récupération des ransomwares de plus de la moitié de leurs victimes. L'analyse a révélé une variation considérable du taux de réussite des attaques en fonction du secteur :

- C'est dans les secteurs de l'*énergie*, du *pétrole/gaz et des services d'utilité publique* (taux de réussite de 79 %) et de l'*éducation* (taux de réussite de 71 %) que les attaquants ont eu le plus de chances de compromettre les sauvegardes de leurs victimes.
- À l'inverse, les secteurs de l'*informatique, de la technologie et des télécoms* (30 % de taux de réussite) et du *retail* (47 % de taux de réussite) ont enregistré les taux les plus faibles de compromission des sauvegardes.

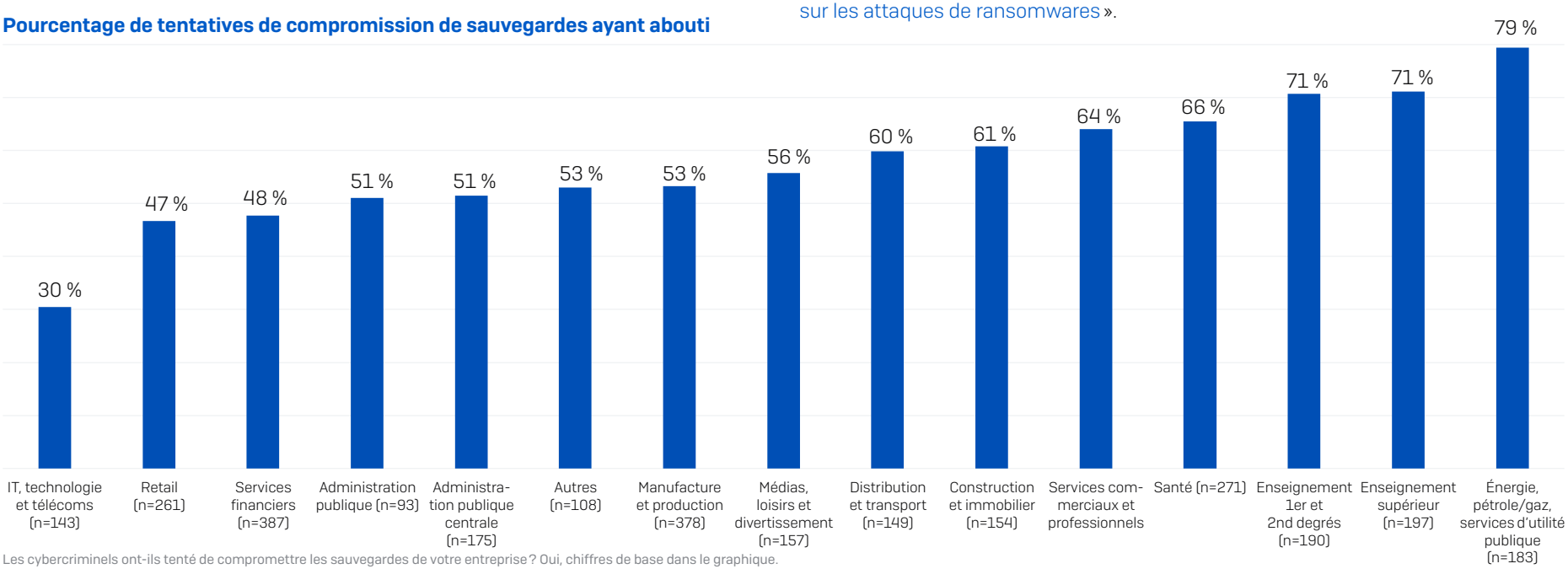
Plusieurs raisons peuvent expliquer les différents taux de réussite. D'une part, les secteurs de l'*informatique, des télécoms et de la technologie* disposent peut-être d'une protection des sauvegardes plus robuste, ce qui leur a permis de faire preuve d'une résilience accrue face à l'attaque. Par ailleurs, leur protection leur a sans doute permis de détecter et de bloquer plus efficacement les tentatives de compromission avant que les attaquants ne parviennent à leurs fins.

Quelle qu'en soit la cause, les organisations ayant fait l'objet d'une compromission de sauvegardes ont fait état d'une issue nettement moins favorable que celles dont les sauvegardes n'ont pas été violées :

- les demandes de rançon étaient en moyenne plus de deux fois supérieures à celles des entreprises dont les sauvegardes n'avaient pas été touchées (2,3 millions de dollars contre 1 million de dollars pour la demande de rançon initiale médiane).
- Les entreprises dont les sauvegardes ont été compromises sont presque deux fois plus susceptibles de payer une rançon pour récupérer leurs données chiffrées (67 % contre 36 %).
- Les coûts médians de rétablissement ont été huit fois plus élevés (3 millions de dollars contre 375 000 dollars) pour les sociétés dont les sauvegardes ont été compromises.

Pour en savoir plus, consultez le rapport « L'impact des sauvegardes compromises sur les attaques de ransomwares ».

**Pourcentage de tentatives de compromission de sauvegardes ayant abouti**




Les cybercriminels ont-ils tenté de compromettre les sauvegardes de votre entreprise ? Oui, chiffres de base dans le graphique.

# Taux de chiffrement des données

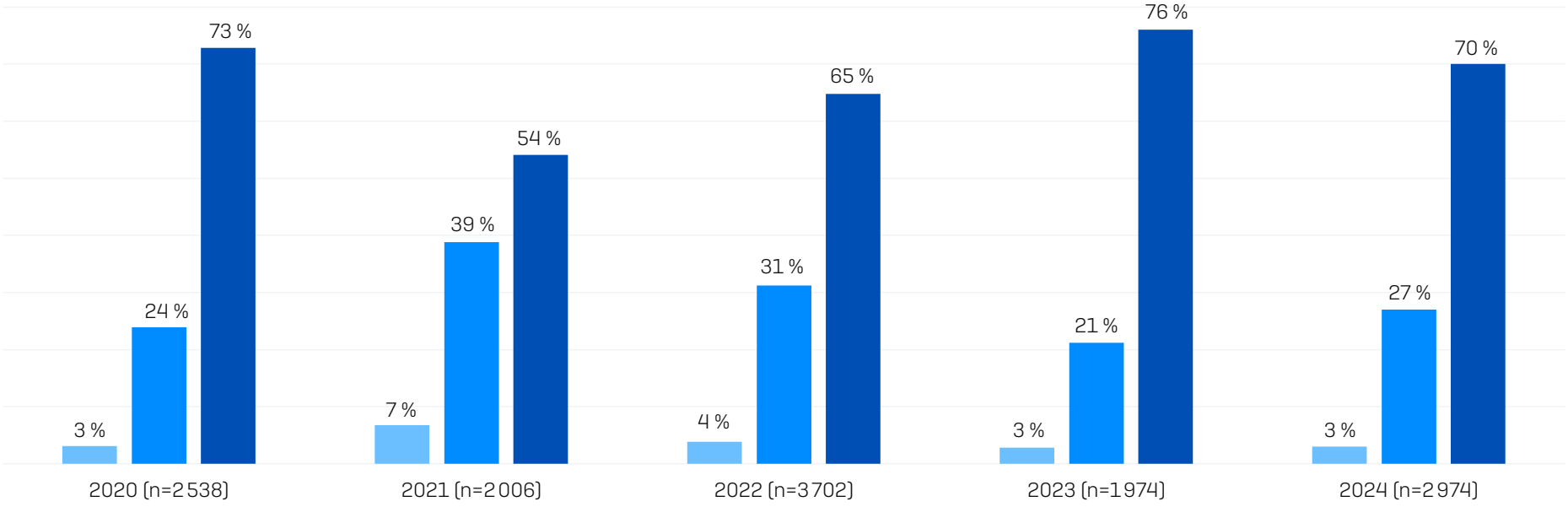
Sept attaques de ransomware sur dix (70 %) au cours de l'année écoulée ont abouti au chiffrement malveillant de données. Si ce taux est élevé, il est toutefois en légère baisse par rapport aux 76 % signalés dans le rapport précédent.

## Taux de chiffrement des données - selon le secteur d'activité

L'enquête de 2024 révèle des écarts considérables dans le taux de chiffrement malveillant d'un secteur à l'autre.

- Si les organisations du secteur de l'*administration publique* ont signalé le taux d'attaque le plus faible cette année (34 % touchés par un ransomware), elles ont également signalé le **taux le plus élevé de chiffrement des données**, 98 % des attaques ayant abouti au chiffrement des données.
- *Les services financiers* (49 %), suivis par le secteur du retail (56 %), affichent les **taux les plus bas de chiffrements des données**
- Le secteur de la *distribution et du transport* est le plus susceptible d'être victime d'une **attaque basée sur l'extorsion** avec 17 % des personnes interrogées déclarant que leurs données n'avaient pas été chiffrées, mais qu'une rançon leur avait tout de même été réclamée, un taux près de trois fois supérieur à celui des autres secteurs.

Consultez l'annexe pour le détail du taux de chiffrement de données par secteur d'activité.




Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? Chiffres de base dans le graphique.

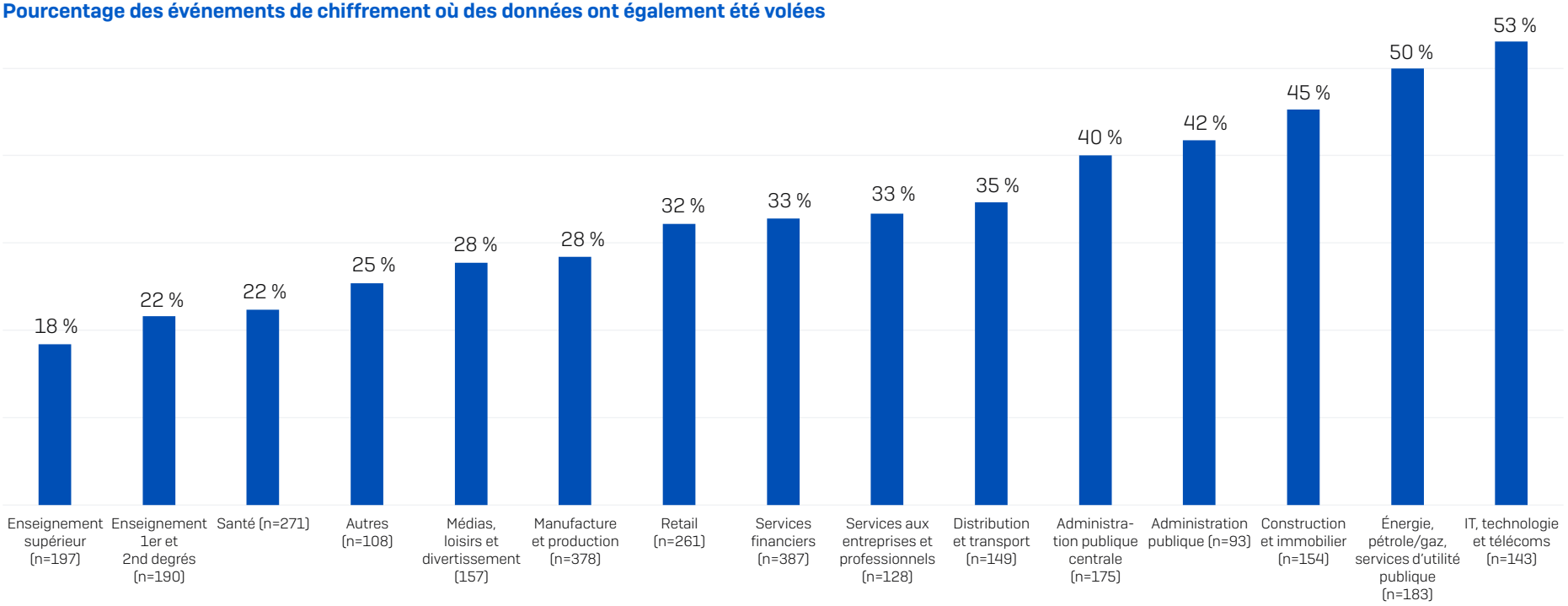
# Vol de données

Les adversaires ne se contentent pas de chiffrer les données, ils les volent également. Dans 32 % des incidents impliquant le chiffrement de données, des données ont également été dérobées, légèrement supérieur au taux de 30 % de l'année dernière. Avec le vol de données, les attaquants renforcent leur capacité à extorquer de l'argent à leurs victimes, tout en leur permettant de rentabiliser davantage l'attaque sur le dark web en revendant les données subtilisées.

Là encore, les disparités sont considérables d'un secteur à l'autre. En apparence, c'est le secteur de l'*informatique, des technologies et des télécoms* qui est le plus mal loti, puisque dans 53 % des attaques impliquant des données chiffrées, ces dernières ont également été volées. *Le secteur de l'énergie, du pétrole/gaz et des services d'utilité publique* arrive en deuxième position, avec des données volées dans 50 % des incidents de chiffrement. À l'inverse, les entreprises du secteur de l'éducation sont celles qui ont le moins tendance à signaler des vols de données lors d'une attaque ; l'*enseignement supérieur* ayant la plus faible propension globale à se faire chiffrer et dérober des données (18 %), suivi par le secteur de l'*enseignement des 1er et 2nd degrés*, qui partage la deuxième place avec le secteur de la santé (22 % dans les deux cas).

Les résultats peuvent refléter des niveaux différents de capacités d'investigation selon les secteurs, ainsi que des priorités différentes. Pour déterminer si des données ont été exfiltrées, il faut pouvoir disposer de niveaux de capacités d'analyses supérieures et s'appuyer souvent sur les journaux des outils EDR/XDR. Il se peut que le secteur de l'*informatique, des technologies et des télécoms* soit tout simplement mieux armé que d'autres pour repérer les vols de données. Il se peut également que les entreprises du secteur de l'*énergie, du pétrole/gaz et des services d'utilité publique* parviennent à repérer plus facilement les vols de données, en raison de la simplicité de leur environnement. A contrario, les établissements scolaires ne disposent souvent pas des compétences et des outils nécessaires pour détecter les vols de données. À cela s'ajoute le fait que certaines entreprises préfèrent ne pas savoir si des données ont été exfiltrées, toute violation de données les obligeant à procéder à des déclarations coûteuses.

**Pourcentage des événements de chiffrement où des données ont également été volées**




Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? Oui. Oui, et les données ont également été volées. Chiffres de base dans le graphique.

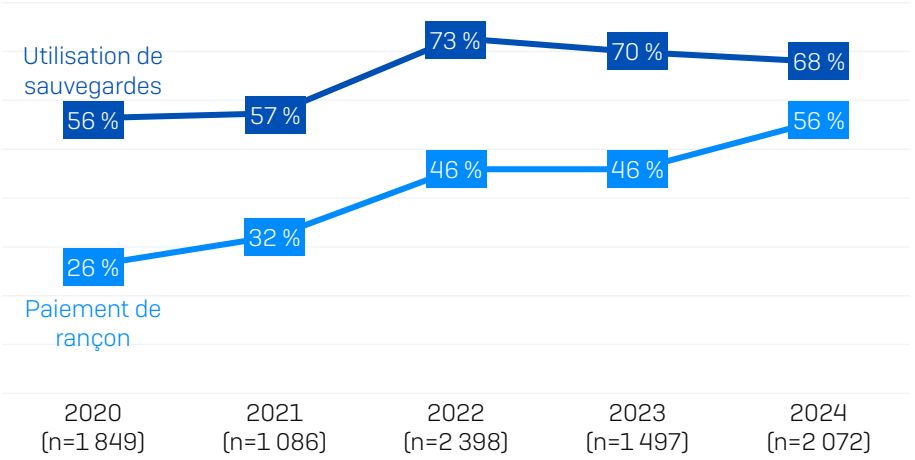
# Récupération des données

98 % des entreprises dont les données ont été chiffrées ont réussi à en récupérer. Pour récupérer leurs données, les entreprises ont eu recours à deux principaux moyens : la restauration à partir de sauvegardes (68 %) et le paiement d'une rançon pour obtenir une clé de déchiffrement (56 %). 26 % des sociétés ayant fait l'objet d'un chiffrement de données ont indiqué avoir utilisé « d'autres moyens » pour récupérer leurs données – bien que l'enquête n'ait pas approfondi ce point, il pourrait s'agir d'une collaboration avec les forces de l'ordre ou de l'utilisation de clés de déchiffrement qui avaient déjà été rendues publiques.

| 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 |
|---|---|---|
| **68 %** | **56 %** | **26 %** |

Fait notable, depuis un an, la tendance des victimes à recourir à plusieurs méthodes de récupération des données chiffrées (paiement de la rançon et utilisation de sauvegardes, par exemple) s'est considérablement renforcée. Près de la moitié des entreprises ayant été victimes d'un chiffrement de données ont déclaré avoir employé plus d'une méthode (47 %) cette fois-ci, un taux plus de deux fois supérieur à celui enregistré dans le précédent rapport (21 %).

L'analyse sur cinq ans révèle que l'écart entre l'utilisation des sauvegardes et le paiement de la rançon continue de se réduire. L'utilisation des sauvegardes a diminué, quoique légèrement, pour la deuxième année consécutive. Parallèlement, le nombre de rançons payées a augmenté de 10 points de pourcentage depuis l'étude réalisée en 2023. La propension à payer la rançon dépend de nombreux facteurs, notamment de la disponibilité des sauvegardes. Il s'agit toutefois d'une tendance alarmante et il est préoccupant de constater que plus de la moitié des victimes acceptent de payer pour obtenir la clé de déchiffrement.




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 - selon le chiffre d'affaires

La propension à payer la rançon pour récupérer les données augmente généralement avec le chiffre d'affaires. Les plus petites entreprises (moins de 10 millions de dollars) affichent de loin le taux de paiement de rançon le plus bas (25 %), tandis que les plus grandes entreprises (plus de 5 milliards de dollars) affichent le taux de paiement de rançon le plus élevé (61 %). L'insuffisance des fonds disponibles pour régler la rançon est probablement l'un des principaux facteurs en jeu : de nombreuses petites entreprises sont tout simplement incapables de trouver l'argent nécessaire au paiement d'une rançon.

Toutefois, comme nous l'avons vu, la récupération des données n'est pas une simple question de sauvegardes ou de rançon. Les nuances derrière les méthodes de récupération des données deviennent évidentes lorsque l'on se penche plus avant sur les données et que l'on compare les chiffres de 2024 avec les résultats de l'année dernière.

En dehors du groupe des entreprises générant un chiffre d'affaires de moins de 10 millions de dollars, tous les segments de chiffre d'affaires ont fait état d'une augmentation du taux de paiement des rançons par rapport à l'année dernière, et trois d'entre eux ont également signalé une augmentation de l'utilisation des sauvegardes pour restaurer les données. Alors que le groupe au chiffre d'affaires le plus faible a déclaré le taux le plus élevé d'utilisation de sauvegardes (88 %), le groupe des 250 millions à 500 millions de dollars le suivait de près (85 %).

## Récupération des données - selon le secteur d'activité

Il n'est peut-être pas surprenant de constater que le secteur de l'*administration publique centrale* est le moins enclin à payer la rançon pour récupérer les données — sa capacité de paiement étant sans doute fortement limitée par des réglementations — et qu'il est également celui qui utilise le plus les sauvegardes pour restaurer les données (39 % et 81 % respectivement).

Dans l'ensemble, il n'y a pas de corrélation évidente entre l'utilisation des sauvegardes et le paiement des rançons :

- *Le secteur des médias, des loisirs et du divertissement* a fait état du taux le plus élevé de paiement de rançons pour récupérer des données (69 %) et de l'un des taux les plus élevés d'utilisation de sauvegardes (74 %).
- *Le secteur de l'énergie, du pétrole/gaz et des services d'utilité publique* est celui qui a le moins recours aux sauvegardes (51 %) et dont le taux de paiement des rançons est de 61 %, un chiffre inférieur à celui de quatre autres secteurs.

Consultez l'annexe pour le détail des méthodes de récupération des données selon le secteur d'activité.

| | CHIFFRE D'AFFAIRES ANNUEL | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Moins de 10 M$ (n=39) | | 10 M$ - 50 M$ (n=291) | | 50 M$ – 250 M$ (n=557) | | 250 M$ - 500 M$ (n=341) | | 500 M$ - 1 Md$ (n=572) | | 1 Md$ - 5 Mds$ (n=632) | | > 5 Mds$ (n=542) | |
| **Méthodes de récupération des données** | 2023 | 2024 | 2023 | 2024 | 2023 | 2024 | 2023 | 2024 | 2023 | 2024 | 2023 | 2024 | 2023 | 2024 |
| Ont utilisé des sauvegardes pour restaurer les données | 80 % | 88 % ▲ | 72 % | 68 % ▼ | 77 % | 60 % ▼ | 75 % | 85 % ▲ | 68 % | 70 % ▲ | 66 % | 65 % ▼ | 63 % | 66 % ▲ |
| Ont payé la rançon et ont récupéré leurs données | 36 % | 25 % ▼ | 41 % | 49 % ▲ | 42 % | 57 % ▲ | 33 % | 50 % ▲ | 51 % | 59 % ▲ | 52 % | 56 % ▲ | 55 % | 61 % ▲ |

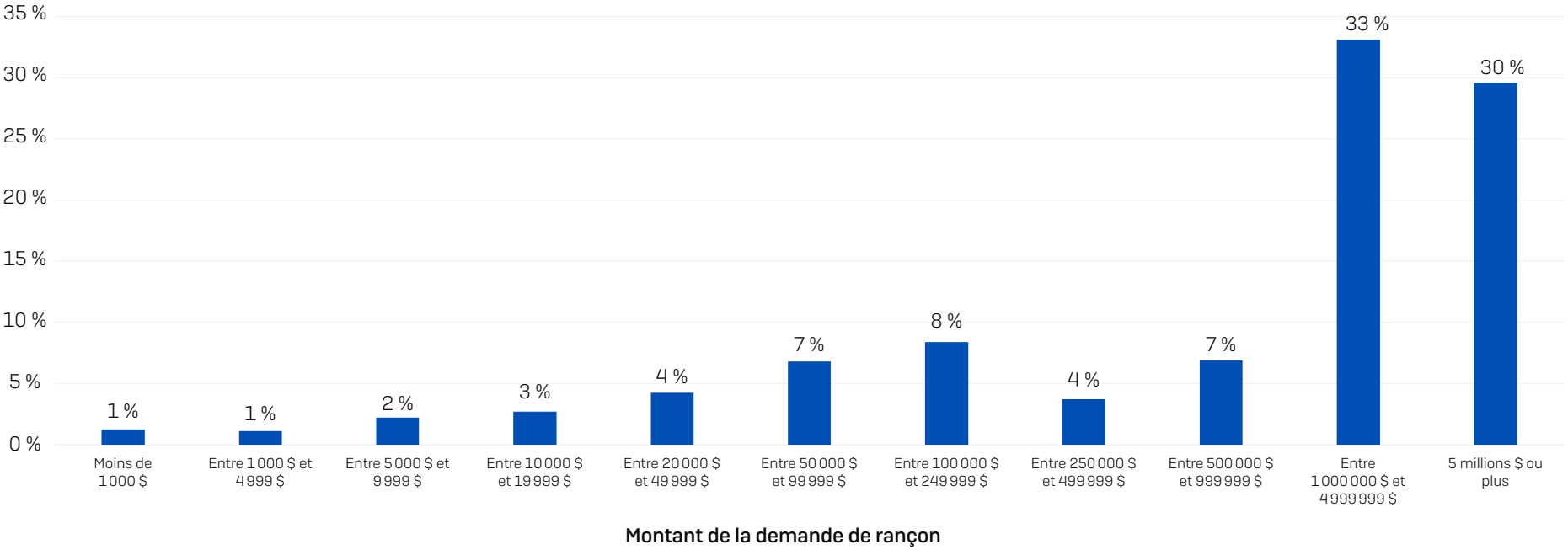
Votre entreprise a-t-elle récupéré des données ? Oui, nous avons payé la rançon et avons récupéré des données ; Oui, nous avons utilisé des sauvegardes pour restaurer les données. Chiffres de base pour 2024 dans le graphique. La flèche indique une hausse/baisse par rapport à 2023.

# Demandes de rançon

Cette année, pour la première fois, nous faisons figurer dans ce rapport le montant des demandes de rançon initiales et le montant des versements finaux. Sur les 1 701 organisations dont les données ont été chiffrées et qui ont pu nous communiquer le montant, la demande de rançon initiale s'élevait en moyenne à 4 321 880 dollars, avec une valeur médiane de 2 millions de dollars.

L'une des observations les plus remarquables de l'étude de cette année est que 63 % des demandes de rançon s'élèvent à 1 million de dollars ou plus, et 30 % se chiffrent à 5 millions de dollars ou plus. Quelques répondants ont fait état de demandes de rançon à quatre chiffres, mais il s'agit d'une minorité.

**Pourcentage de demandes de rançon par montant**




Quel était le montant de la rançon demandée par les attaquants ? n=1 701

## Montant des demandes de rançon - selon le chiffre d'affaires

Lorsqu'on examine les données moyennes et médianes, on constate que le montant de la demande de rançon augmente avec le chiffre d'affaires, ce qui indique que les adversaires ajustent leur demande en fonction — en partie, du moins — de la capacité probable de la victime à payer.

Les demandes de rançon astronomiques ne sont plus réservées aux entreprises les plus lucratives, les demandes d'un montant de 1 million de dollars ou plus étant désormais monnaie courante : 47 % des entreprises dont le chiffre d'affaires est compris entre 10 et 50 millions de dollars ont fait l'objet d'une demande de rançon à sept chiffres au cours de l'année écoulée.

## Montant des demandes de rançon - selon le secteur d'activité

Aucun secteur ne tire son épingle du jeu ici, puisque tous les secteurs cités (à l'exception de la catégorie « autres ») font état de demandes de rançon dont le montant médian était égal ou supérieur à un million de dollars.

- Le secteur du *retail* et celui de l'*informatique, des technologies et des télécoms* ont reçu les demandes les plus faibles (1 million de dollars, montant médian), suivis par le secteur de la *construction* (1,1 million de dollars).
- *L'administration publique centrale* est le secteur visé par les demandes les plus élevées, avec des montants médian (7,7 millions de dollars) et moyen (9,9 millions de dollars) records.

Consultez l'annexe pour le détail du montant des rançons demandées selon le secteur d'activité.

| | CHIFFRE D'AFFAIRES ANNUEL | | | | | |
|---|---|---|---|---|---|---|
| **Demande de rançon** | **10 M$ - 50 M$ (n=207)** | **50 M$ – 250 M$ (n=288)** | **250 M$ - 500 M$ (n=158)** | **500 M$ - 1 Md$ (n=268)** | **1 Md$ - 5 Mds$ (n=366)** | **> 5 Mds$ (n=398)** |
| Moyenne | 1 774 941 $ | 1 704 853 $ | 3 407 796 $ | 5 184 024 $ | 4 281 258 $ | 7 467 294 $ |
| Médiane | 330 000 $ | 220 000 $ | 840 000 $ | 2 000 000 $ | 3 000 000 $ | 6 600 000 $ |

Quel était le montant de la rançon demandée par les attaquants ? Chiffres de base dans le graphique. Note : la catégorie « Moins de 10 M$ » a été exclue de ce tableau en raison du faible nombre de répondants dans ce segment.

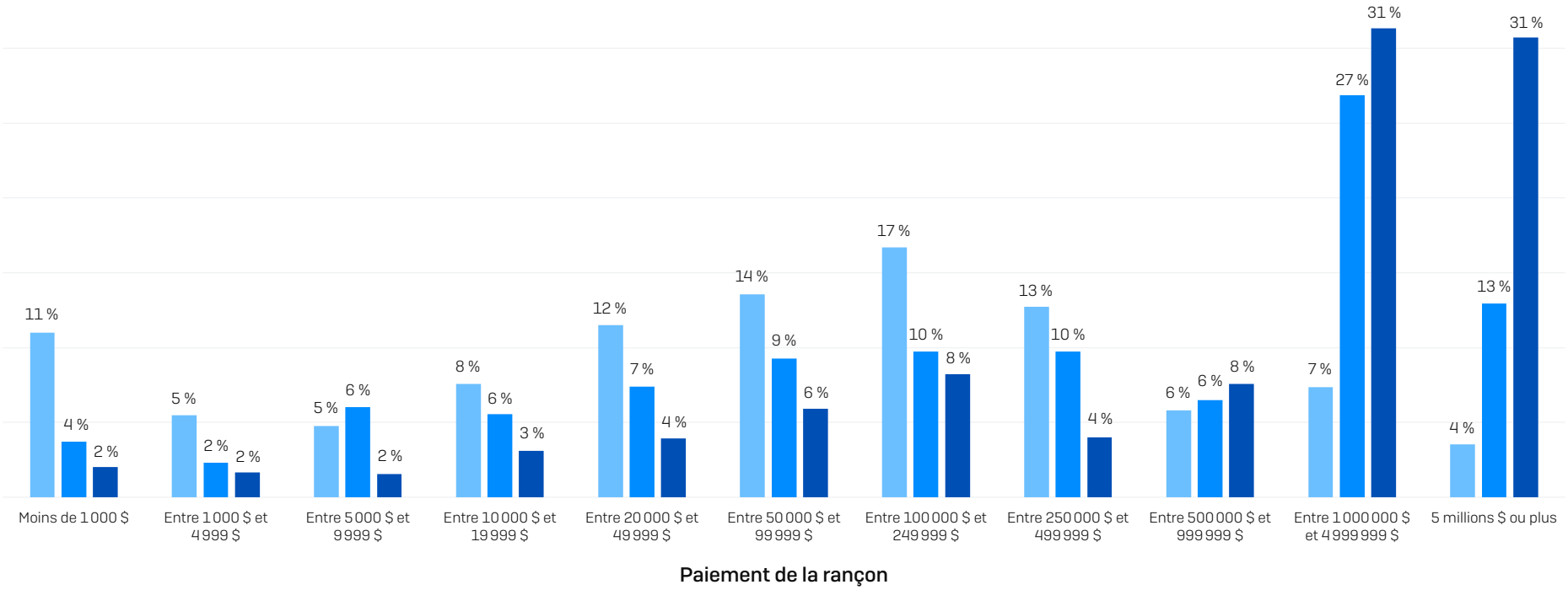
# Montant des rançons payées

1 097 répondants dont l'entreprise a payé la rançon nous ont révélé la somme effectivement payée. Si l'on considère les valeurs médianes et moyennes, il apparaît que les montants versés ont considérablement augmenté en 2023 :

- Montant médian du paiement : 2 000 000 $ (soit 5 fois plus que les 400 000 $ déclarés dans le rapport précédent)
- Montant moyen du paiement : 3 960 917 $ (soit 2,6 fois plus que les 1 542 330 $ déclarés dans le rapport précédent)

Le graphique ci-dessous illustre clairement la fait que la proportion de rançons aux montants faibles n'a cessé de diminuer au cours des trois dernières années, tandis que la proportion de rançons aux montants très élevés a explosé. Aujourd'hui, le paiement d'une rançon à sept chiffres ou plus est devenu la norme.

**Distribution du paiement des rançons 2022-24**




Quel était le montant de la rançon payée aux attaquants ? Chiffres de base dans le graphique.

## Montant des rançons payées - selon le secteur d'activité

Le montant moyen des rançons versées, tout comme celui des demandes initiales, varie considérablement d'un secteur d'activité à l'autre. C'est dans le secteur de l'*informatique, de la technologie et des télécoms* que le montant médian des rançons est le plus bas (300 000 dollars), suivi par le secteur de la *distribution et des transports* (440 000 dollars). À l'autre extrémité du classement, les secteurs de l'*enseignement des 1er et 2nd degrés* ainsi que l'*administration publique centrale* ont payé des rançons d'un montant médian de 6,6 millions de dollars.

Si l'on constate une forte corrélation entre montants demandés faibles et montants payés faibles (et inversement), il existe toutefois des exceptions, notamment dans le secteur de la *distribution et du transport*, où la demande médiane de rançon était supérieure à 2,8 millions de dollars, mais où le montant moyen des paiements s'élevait à 440 000 dollars.

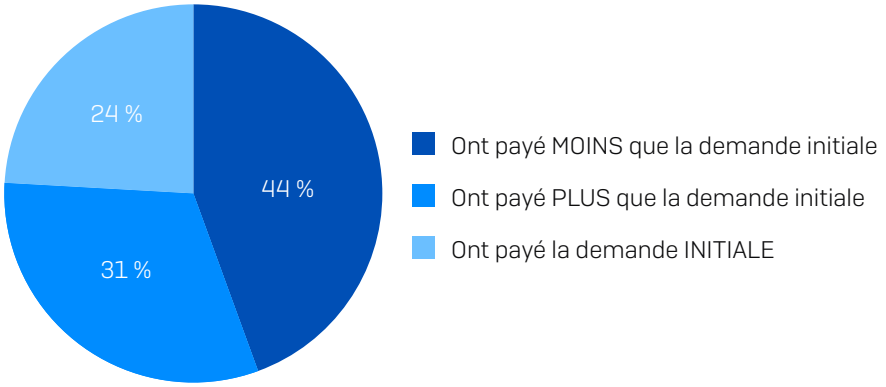
Consultez l'annexe pour le détail du montant moyen des rançons payées selon le secteur d'activité

# Montant de la rançon demandée VS montant de la rançon payée

Lorsque des données sont chiffrées, la pression est très forte pour toutes les parties concernées, chacune essayant de parvenir à l'issue la plus favorable possible. Si, de leur côté, les entreprises dont les données ont été chiffrées cherchent à minimiser l'impact financier, les adversaires, pour leur part, font tout pour obtenir le plus d'argent possible dans les plus brefs délais. Ils n'hésitent pas à brandir la menace d'une augmentation du montant de la rançon si le paiement n'est pas effectué dans un certain délai, mettant davantage de pression sur l'entreprise.

## Propension à négocier le montant de la rançon

L'étude a révélé que les victimes s'acquittent rarement de la somme initiale exigée par les attaquants : 24 % seulement des personnes interrogées déclarant que leur paiement correspondait à la demande de rançon initiale. 44 % ont payé moins que la demande initiale, tandis que 31 % ont payé plus.




Quel était le montant de la rançon demandée par les attaquants ? Quel était le montant de la rançon payée aux attaquants ? n=1 097.

Si l'on examine les données par secteur, on remarque que les deux secteurs de prestations de services (*les services professionnels* et les *services financiers*) sont les plus susceptibles de négocier le paiement de la rançon : 67 % d'entre eux déclarant avoir payé un montant inférieur à celui demandé à l'origine. Le secteur de la *fabrication et de la production* suit de près avec 65 % des entreprises ayant payé moins que la somme initialement demandée.

A contrario, les secteurs les plus susceptibles de payer un montant supérieur à celui de la demande initiale sont ceux qui comptent une forte proportion d'organisations du secteur public :

- *L'enseignement supérieur* est le secteur le plus susceptible de payer davantage que la demande initiale (67 % des entreprises de ce secteur ont payé plus) et le moins susceptible de payer moins que la demande initiale (20 % ont payé moins).
- *Le secteur de la santé* est le deuxième secteur le plus susceptible de payer plus que la demande initiale (57 % des répondants de ce secteur ont payé plus), suivi par celui de l'*enseignement des 1er et 2nd degrés* (55 % ont payé plus).

Il est possible que ces secteurs n'aient pas forcément accès à des négociateurs professionnels qui pourront les aider à réduire la somme demandée. Il se pourrait aussi qu'ils aient davantage besoin de récupérer les données « à tout prix » en raison du caractère public de leur mission. Quoi qu'il en soit, il est clair qu'il y a une marge de manœuvre entre la demande initiale et le paiement final.

Consultez l'annexe pour le détail de la différence entre les montants demandés et les montants payés selon le secteur d'activité

## Proportion des demandes de rançon payées

Bien les victimes négocient la rançon dans la majorité des cas, cela a peu d'incidence sur le fait de payer la rançon initiale : 94 % ont indiqué de la demande initiale a été payée, en moyenne, sur l'ensemble de la cohorte.

En regardant de plus près, nous constatons que tous les segments de chiffre d'affaires, à l'exception des plus grandes entreprises, sont parvenus à réduire le montant de la rançon. C'est dans le segment des entreprises au chiffre d'affaires de 50 à 250 millions de dollars que le paiement de demande initiale est le plus faible (84 %). Le seul groupe ayant payé plus que la demande initiale est le segment des entreprises au chiffre d'affaires de plus de 5 milliards de dollars : elles ont payé, en moyenne, 115 % de la rançon demandée.

| | CHIFFRE D'AFFAIRES ANNUEL | | | | | |
|---|---|---|---|---|---|---|
| **Cohorte** | **10 M$ - 50 M$ (n=100)** | **50 M$ – 250 M$ (n=206)** | **250 M$ - 500 M$ (n=104)** | **500 M$ - 1 Md$ (n=175)** | **1 Md$ - 5 Mds$ (n=233)** | **> 5 Mds$ (n=275)** |
| Proportion des demandes de rançon payées | 93 % | 84 % | 90 % | 88 % | 85 % | 115 % |

Quel était le montant de la rançon demandée par les attaquants ? Quel était le montant de la rançon payée aux attaquants ? n=1 097. Remarque : la cohorte « moins de 10 M$ » est exclue de cette analyse des chiffres d'affaires annuels en raison d'un taux de réponse très faible.

## Proportion des demandes de rançon payées - selon le secteur d'activité

Les secteurs les plus susceptibles de négocier à la baisse le montant de la rançon sont aussi ceux qui paient le pourcentage le plus bas de la demande initiale, et inversement.

| MOINS DE 100 % | PLUS DE 100 % |
|---|---|
| Manufacture et production (70 %) | Enseignement supérieur (122 %) |
| Services aux entreprises et professionnels (74 %) | Enseignement 1er et 2nd degrés (115 %) |
| Services financiers (75 %) | Santé (111 %) |
| Autre (79 %) | Administration publique (104 %) |
| IT, télécoms et technologie (82 %) | Administration publique centrale (103 %) |
| Retail 84 % | Énergie, pétrole/gaz, services d'utilité publique (101 %) |
| Construction et immobilier (95 %) | |
| Distribution et transport (95 %) | |
| Médias, loisirs et divertissement (95 %) | |

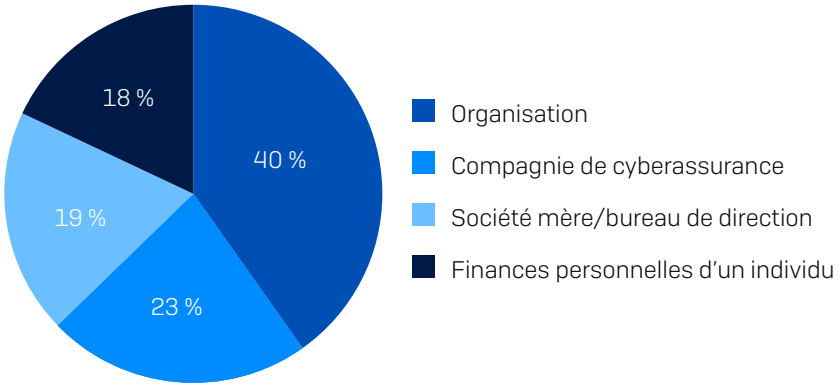
Quel était le montant de la rançon demandée par les attaquants ? Quel était le montant de la rançon payée aux attaquants ? n=1 097.

## Source de financement de la rançon

La question de savoir qui finance la rançon est un sujet d'un intérêt considérable, et l'étude a révélé un certain nombre d'informations éclairantes à ce sujet :

- Le financement de la rançon est le résultat d'un effort collectif, les répondants déclarant des sources financières multiples dans plus de quatre cas sur cinq (82 %).
- La principale source de financement des rançons est l'entreprise elle-même, qui couvre 40 % du montant payé en moyenne ; la société mère de l'entreprise ou l'organe directeur de l'entreprise fournissant généralement 19 % du montant.
- Les compagnies d'assurance jouent un rôle important dans le paiement des rançons.
  - 23 % du financement des rançons provient des compagnies d'assurance
  - Les compagnies d'assurance contribuent au paiement de la rançon dans 83 % des attaques
  - Cependant, les assureurs ne couvrent que très rarement (1 %) le montant total : dans 79 % des cas, l'assureur a financé moins de la moitié du paiement total.

### Source de financement du paiement de la rançon




quelle(s) source(s) suivante(s) provient l'argent qui a servi à financer le paiement de la rançon ? n=1168.

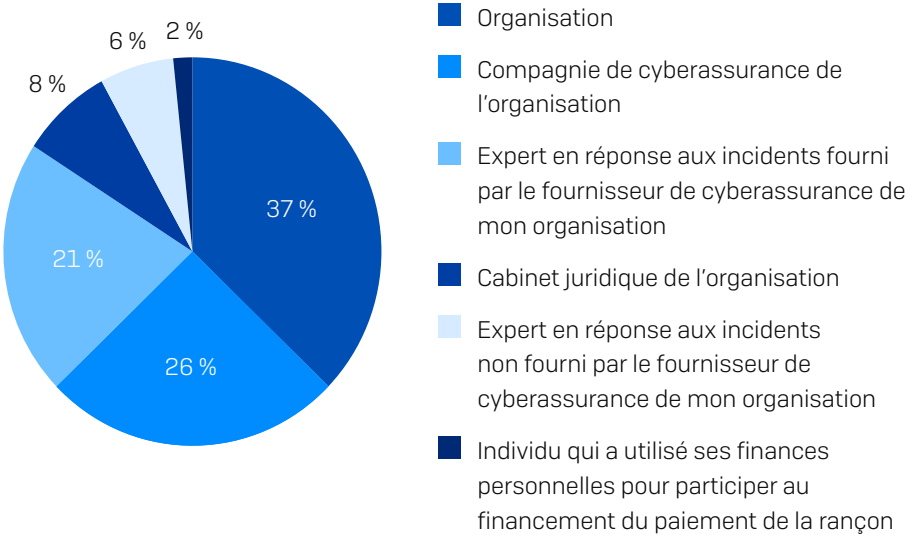
## Exécution du transfert de la rançon

Bien que plusieurs entités puissent contribuer au paiement de la rançon, les fonds sont généralement transférés sous forme d'un paiement unique par une seule partie.

Globalement, ce sont les compagnies d'assurance qui ont transféré les fonds dans près de la moitié des cas, soit directement (26 %), soit par l'intermédiaire d'un spécialiste de la réponse aux incidents (21 %). L'entreprise victime a effectué le virement de 37 % des paiements, tandis que 8 % ont été exécutés par le cabinet juridique de la victime.

Dans l'ensemble, 28 % (chiffre arrondi) des transferts ont été effectués par des spécialistes de la réponse aux incidents, qu'ils soient désignés par la compagnie d'assurance (21 %) ou par une autre partie, généralement la victime (6 %).

### Auteur du transfert du paiement de la rançon




Qui a effectué la transaction pour le paiement de la rançon, c'est-à-dire qui a transféré l'argent sur le compte de l'attaquant ? n=1168.

# Coûts de rétablissement

Le montant de la rançon ne représente qu'une partie du coût de rétablissement encouru par l'entreprise après une attaque par ransomware. En excluant les rançons payées, dans le rapport 2024, les organisations ont déclaré un coût moyen de rétablissement après une attaque de ransomware de 2,73 millions de dollars, soit une hausse de près de 1 million de dollars par rapport au chiffre de 1,82 million de dollars déclaré en 2023.

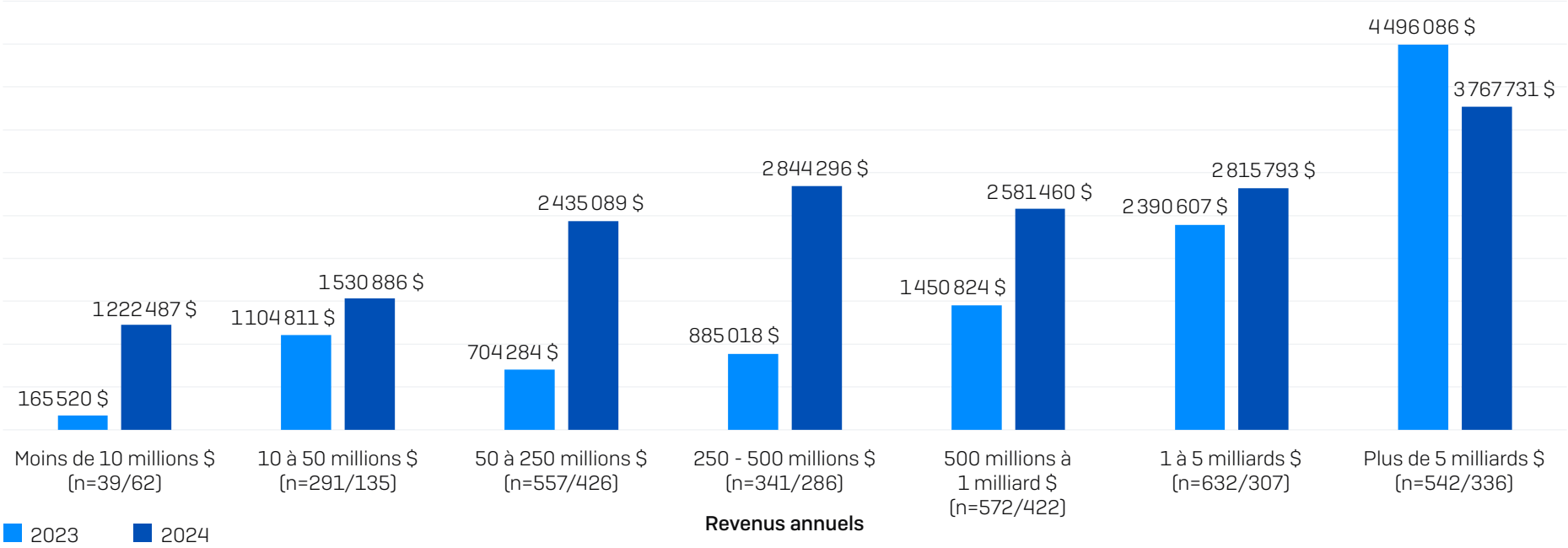
| 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|
| 1,85 M$ | 1,4 M$ | 1,82 M$ | 2,73 M$ |

Quel était le coût approximatif payé par votre organisation 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=2 974 (2024)/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 ».

L'augmentation la plus importante des coûts de rétablissement globaux a été observée dans les segments de chiffre d'affaires inférieur et moyen, la cohorte des 250 millions à 500 millions de dollars ayant enregistré la plus forte augmentation individuelle avec 2 millions de dollars (passant de 885 018 dollars à 2 885 296 dollars).

Les entreprises dont le chiffre d'affaires se situe entre 1 et 5 milliards de dollars ont fait état d'une augmentation (relativement) faible d'un peu plus de 400 000 dollars, tandis que les plus grandes entreprises dont le chiffre d'affaires annuel est supérieur à 5 milliards de dollars ont été les seules à constater une réduction des coûts de rétablissement, qui sont passés de 4 496 096 dollars à 3 767 731 dollars.

L'examen des données relatives aux coûts médians de rétablissement confirme ces tendances. Globalement, les coûts médians de rétablissement ont doublé, passant de 375 000 à 750 000 dollars au cours de l'année écoulée. Les augmentations sont surtout observées dans les cinq cohortes d'entreprises présentant un chiffre d'affaires inférieur, qui ont toutes fait état d'une hausse considérable de leurs coûts, alors qu'elles sont restées relativement stables dans les deux cohortes d'entreprises présentant un chiffre d'affaires supérieur.



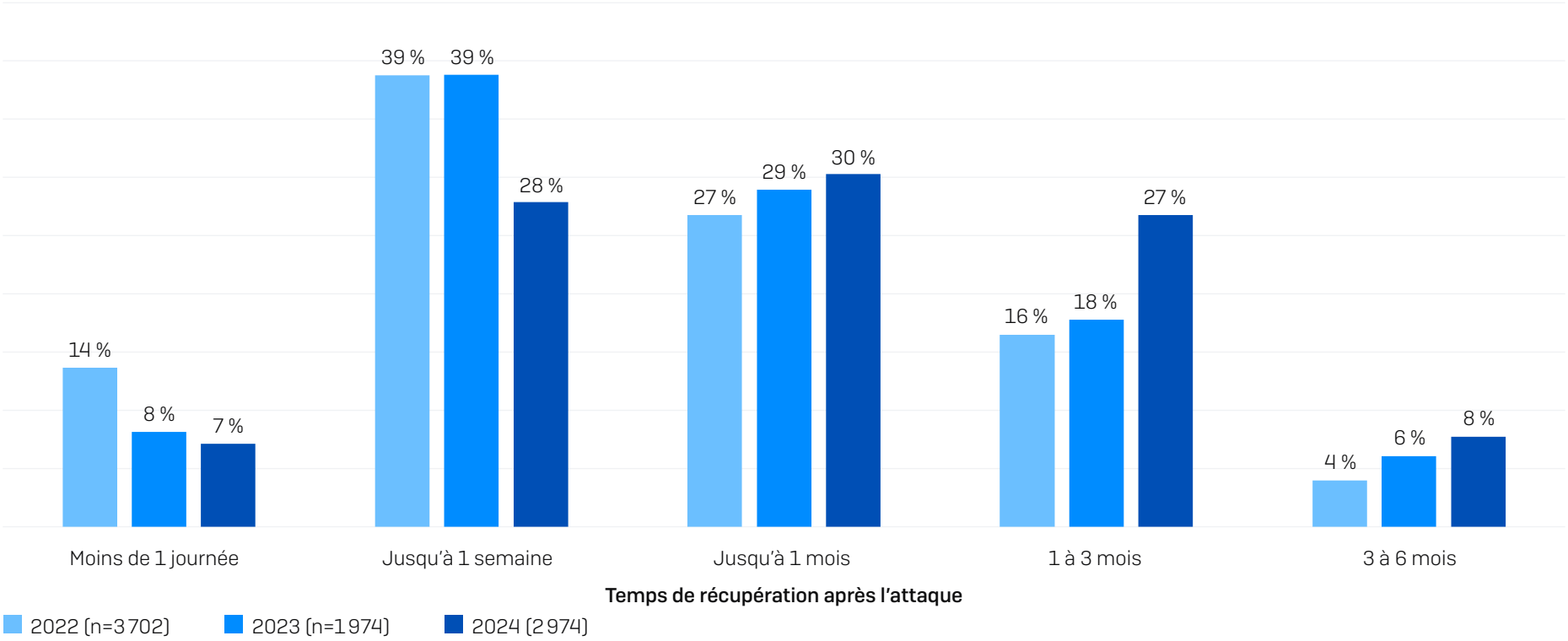

Quel était le coût approximatif payé par votre entreprise pour remédier aux conséquences de l'attaque de ransomware la plus significative (en prenant en compte les interruptions de services, le temps passé à résoudre l'incident, les coûts matériels, les pertes d'exploitation, etc.) ? n=2 974 (2024), 1 974 (2023). Chiffres de base selon le chiffre d'affaires en 2023/2024 dans le graphique

# Temps de rétablissement

Le temps nécessaire pour se remettre d'une attaque de ransomware tend à s'allonger. Notre étude 2024 a révélé que :

- 35 % des victimes de ransomware sont totalement rétablies en une semaine ou moins, contre 47 % dans l'édition 2023 et 52 % en 2022.
- Un tiers des victimes (34 %) met désormais plus d'un mois à se rétablir, contre 24 % en 2023 et 20 % en 2022.

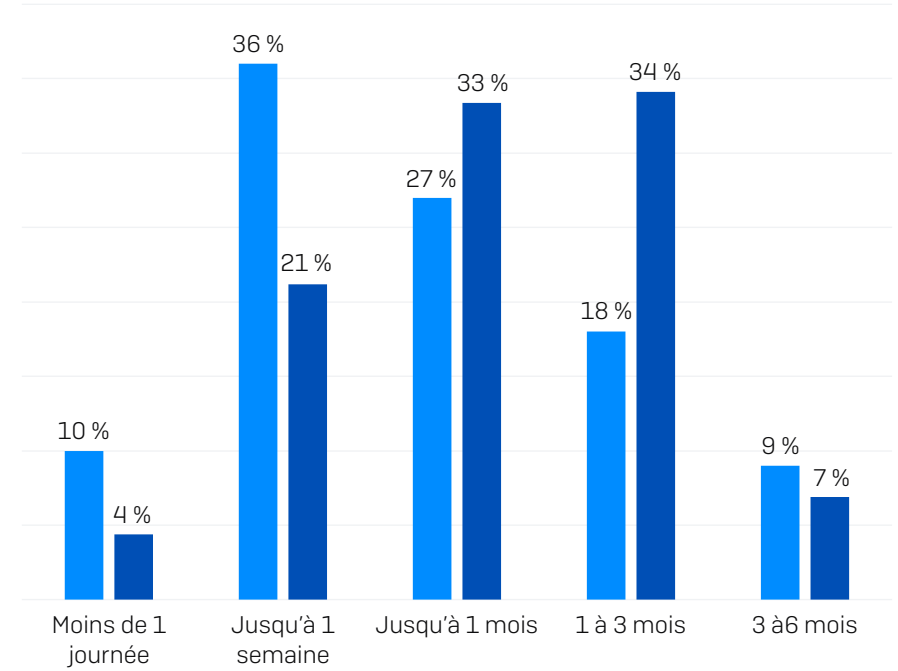
Ce phénomène peut s'expliquer par la complexité et la gravité accrues des attaques, qui nécessitent un travail de rétablissement plus important. Il pourrait également être le signe d'un manque croissant de préparation à la reprise après une attaque.




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

## Temps de rétablissement : l'incidence de la compromission des sauvegardes

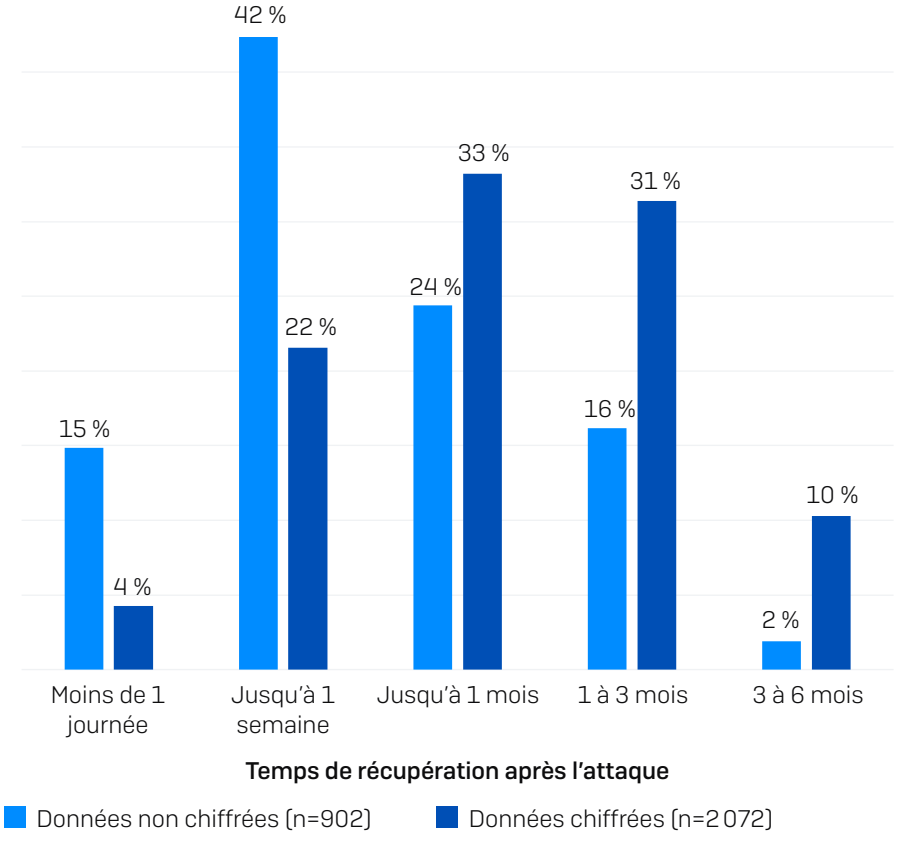
Toute compromission des sauvegardes a un impact majeur sur le temps de rétablissement global. Près de la moitié des organisations dont les sauvegardes n'ont pas été compromises se rétablissent en une semaine ou moins (46 %), contre un quart seulement (25 %) de celles dont les sauvegardes ont été affectées. La compromission de vos sauvegardes accroît la complexité des opérations de récupération des données chiffrées tout en augmentant les frais généraux liés à la création et à la sécurisation de nouvelles sauvegardes non contaminées.




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

## Temps de rétablissement : l'incidence du chiffrement des données

Sans surprise, un chiffrement de données lors d'une attaque augmente considérablement le temps de rétablissement. 57 % des entreprises dont les données n'avaient pas été chiffrées se sont rétablies en une semaine, contre 25 % de celles dont les données avaient été chiffrées.

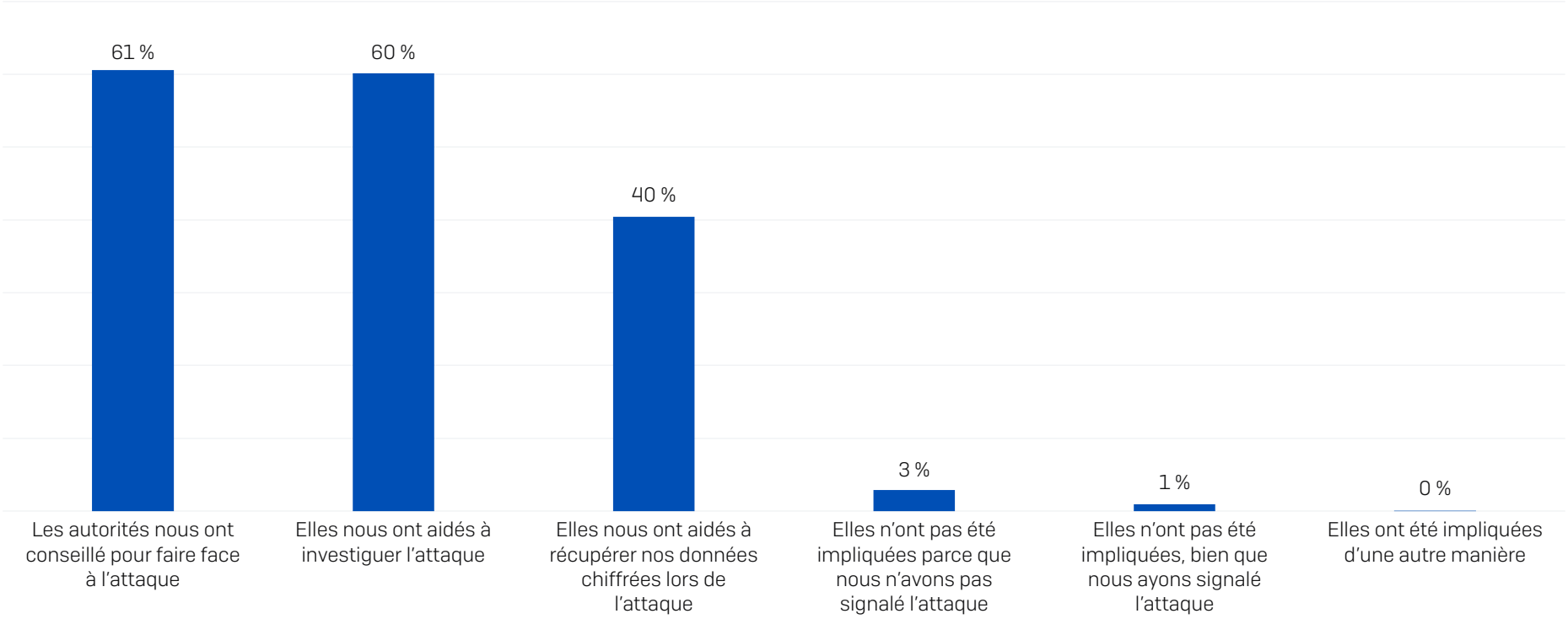



Combien de temps a-t-il fallu à votre organisation pour se rétablir complètement après l'attaque de ransomware ? Chiffres de base dans le graphique.

# Implication des forces de l'ordre

La nature et la mise à disposition d'une aide officielle en cas d'attaque par un ransomware varient d'un pays à l'autre, tout comme les outils permettant de signaler une cyberattaque. Les entreprises américaines peuvent s'adresser à la Cybersecurity and Infrastructure Security Agency (CISA), les entreprises britanniques au National Cyber Security Centre (NCSC) et les entreprises australiennes à l'Australian Cyber Security Center (ACSC), pour n'en citer que quelques-unes.

Signe de la normalisation des attaques de ransomware, 97 % des entreprises du monde entier qui ont été touchées par un ransomware ont pris contact avec les forces de l'ordre ou des instances gouvernementales officielles à la suite de l'attaque. 61 % ont déclaré avoir reçu des conseils pour faire face à l'attaque, 60 % ont reçu de l'aide pour investiguer l'attaque et 40 % ont déclaré avoir reçu de l'aide pour se rétablir après l'attaque.

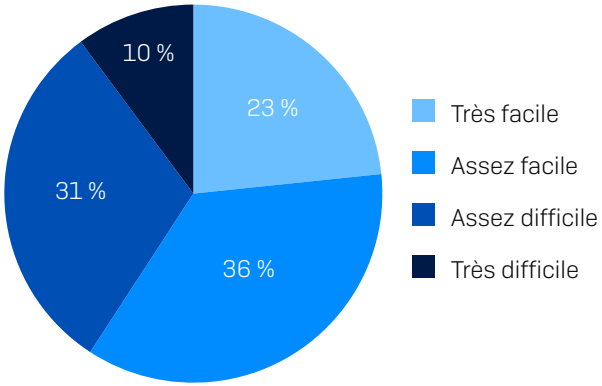



**Comment les forces de l'ordre ou les instances gouvernementales ont-elles été impliquées ?**

Si votre entreprise a signalé l'attaque aux forces de l'ordre ou à une instance gouvernementale officielle, comment ont-elles été impliquées ? n=2 974.

## Simplicité du processus de signalement

Il est encourageant de constater que plus de la moitié (59 %) des répondants ayant pris contact avec les forces de l'ordre ou les instances officielles au sujet de la cyberattaque ont déclaré que le processus de signalement avait été facile (23 % très facile, 36 % assez facile). Seuls 10 % ont déclaré que la procédure était très difficile, tandis que 31 % l'ont qualifiée de relativement difficile.




Dans quelle mesure a-t-il été facile ou difficile pour votre entreprise de dialoguer avec les forces de l'ordre ou les organismes officiels au sujet de cette attaque ? n=2 874 (à l'exclusion des réponses « ne sait pas »).

## Non-implication des instances officielles

Les raisons pour lesquelles 3 % des entreprises (86 répondants) n'ont pas signalé l'attaque sont diverses. Les deux raisons les plus fréquentes étant la crainte d'un impact négatif sur leur activité, telles que des amendes, des frais ou un surcroît de travail (27 %), et le fait qu'elles ne pensaient pas que cela leur servirait à quelque chose (27 % également). Plusieurs répondants ont indiqué dans des commentaires que leur entreprise n'avait pas fait appel à des organismes officiels parce qu'elle était parvenue à résoudre le problème en interne.

| | |
|---|---|
| Nous étions préoccupés par l'impact négatif que cela pourrait avoir sur notre entreprise (amendes, frais, travail supplémentaire, etc.). | **27 %** |
| Nous avons estimé que notre entreprise n'avait aucun intérêt à signaler l'attaque. | **27 %** |
| Nous avons pensé que les autorités ne seraient pas intéressées par l'attaque. | **22 %** |
| Nous n'avons pas songé à faire un signalement, car nous étions trop occupés à gérer l'attaque. | **21 %** |
| Les attaquants nous ont avertis de ne pas prévenir les autorités. | **19 %** |
| Nous ne savions pas à quels organismes ou services chargés de l'application de la loi faire appel. | **10 %** |
| Nous n'étions pas légalement tenus de signaler l'attaque. | **9 %** |
| Autre (veuillez préciser) | **3 %** |
| Ne sait pas | **1 %** |

Pourquoi n'avez-vous pas signalé cette attaque aux forces de l'ordre ou aux organismes officiels ? (n=86).

# Conclusion

Les ransomwares restent une menace majeure pour les entreprises de toutes tailles dans le monde entier. Si le taux d'attaque global a baissé au cours des deux dernières années, les répercussions des attaques sur les victimes sont plus fortes. Tandis que les adversaires continuent de multiplier et de faire évoluer leurs attaques, il est essentiel que les défenseurs ne soient pas pris de vitesse et que leurs cyberdéfenses évoluent en conséquence.

**Prévention**. Une bonne attaque de ransomware est une attaque qui n'a pas eu lieu, parce que les adversaires n'ont pas réussi à pénétrer votre entreprise. Sachant qu'un tiers des attaques commencent par l'exploitation de vulnérabilités non corrigées, il est important de prendre le contrôle de votre surface d'attaque et de déployer un processus de priorisation des correctifs basée sur les risques. L'utilisation de l'authentification multifacteur (MFA) pour limiter l'utilisation abusive des identifiants de connexion devrait également figurer parmi les priorités de chaque entreprise. La formation continue des utilisateurs à la détection des emails malveillants et du phishing reste indispensable.

**Protection**. Il est impératif de disposer d'outils de sécurité de base performants, notamment en matière de protection Enpoint, de messagerie et de pare-feu. Les systèmes endpoint (dont les serveurs) sont la cible principale des auteurs de ransomwares, c'est pourquoi il faut vous assurer que ceux-ci sont bien protégés, y compris par une protection anti-ransomware dédiée pour bloquer et annuler tout processus de chiffrement malveillant. Les outils de sécurité doivent être correctement configurés et déployés pour garantir une protection optimale. Il convient donc de rechercher des solutions prêtes à l'emploi qui prévoient des contrôles de posture simples en matière de sécurité. Toute protection trop complexe et difficile à mettre en œuvre peut facilement aggraver les risques au lieu de les réduire.

**Détection et intervention**. Il est essentiel de stopper une attaque le plus tôt possible. Pour améliorer considérablement vos résultats, il est essentiel d'être en mesure de détecter et de neutraliser un adversaire dans votre environnement avant qu'il ne puisse compromettre vos sauvegardes ou chiffrer vos données.

**Planification et préparation**. En disposant d'un plan de réponse aux incidents que vous savez parfaitement mettre en œuvre, vous améliorerez considérablement vos résultats si le pire se produit et que vous êtes victime d'une attaque de grande ampleur. Entraînez-vous régulièrement à restaurer des données à partir de sauvegardes : vous gagnerez en rapidité et en fluidité si vous deviez intervenir au lendemain d'une attaque.

Pour découvrir comment Sophos peut vous aider à optimiser vos défenses contre les ransomwares, contactez un conseiller ou visitez le site www.sophos.fr

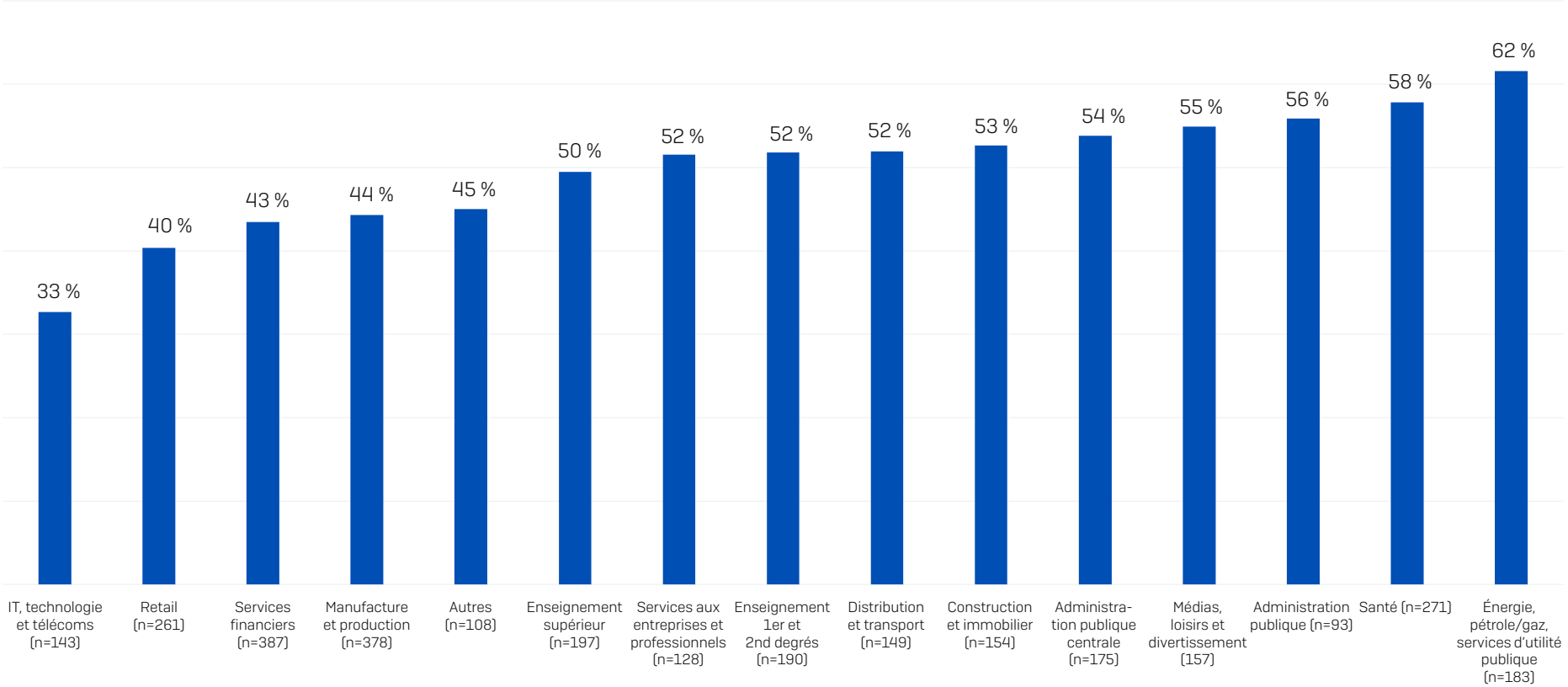
## À propos de Vanson Bourne

Vanson Bourne est un cabinet d'études de marché indépendant spécialisé dans le secteur des technologies. Sa réputation d'analyste solide et crédible repose sur des principes de recherche rigoureux et sur sa capacité à solliciter l'avis des décideurs de haut niveau dans les domaines techniques et commerciaux, dans tous les secteurs d'activité et sur l'ensemble des marchés dominants. Pour en savoir plus, consultez le site www.vansonbourne.com.

# Annexe

## Pourcentage d'ordinateurs affectés - selon le secteur d'activité

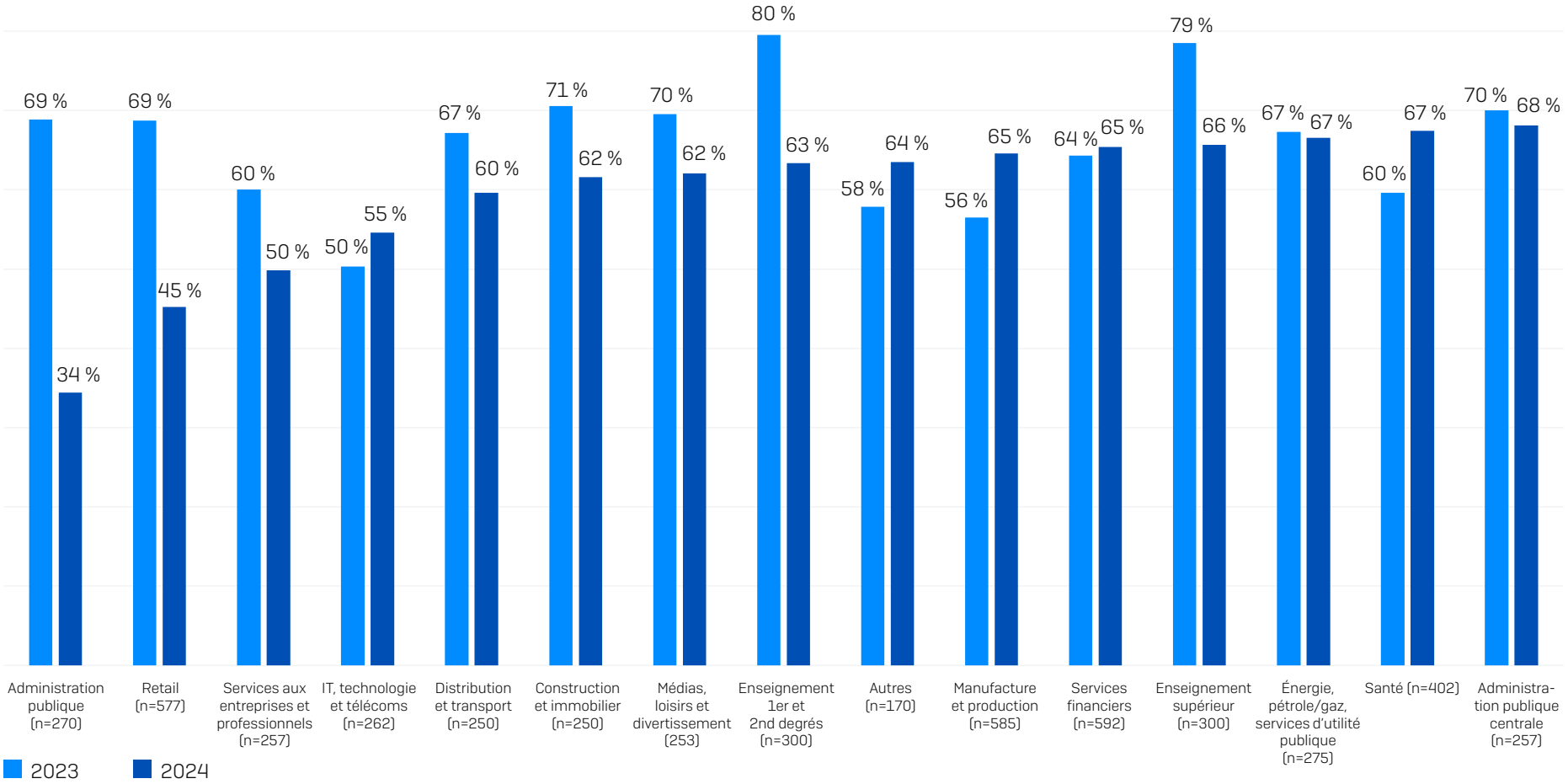
**Pourcentage d'appareils affectés**




Quel pourcentage des ordinateurs de votre entreprise a été touché par une attaque de ransomware au cours de l'année écoulée ? n=2 974 entreprises touchées par une attaque de ransomware. Chiffres de base du secteur dans le graphique.

## Taux d'attaques de ransomware - selon le secteur d'activité

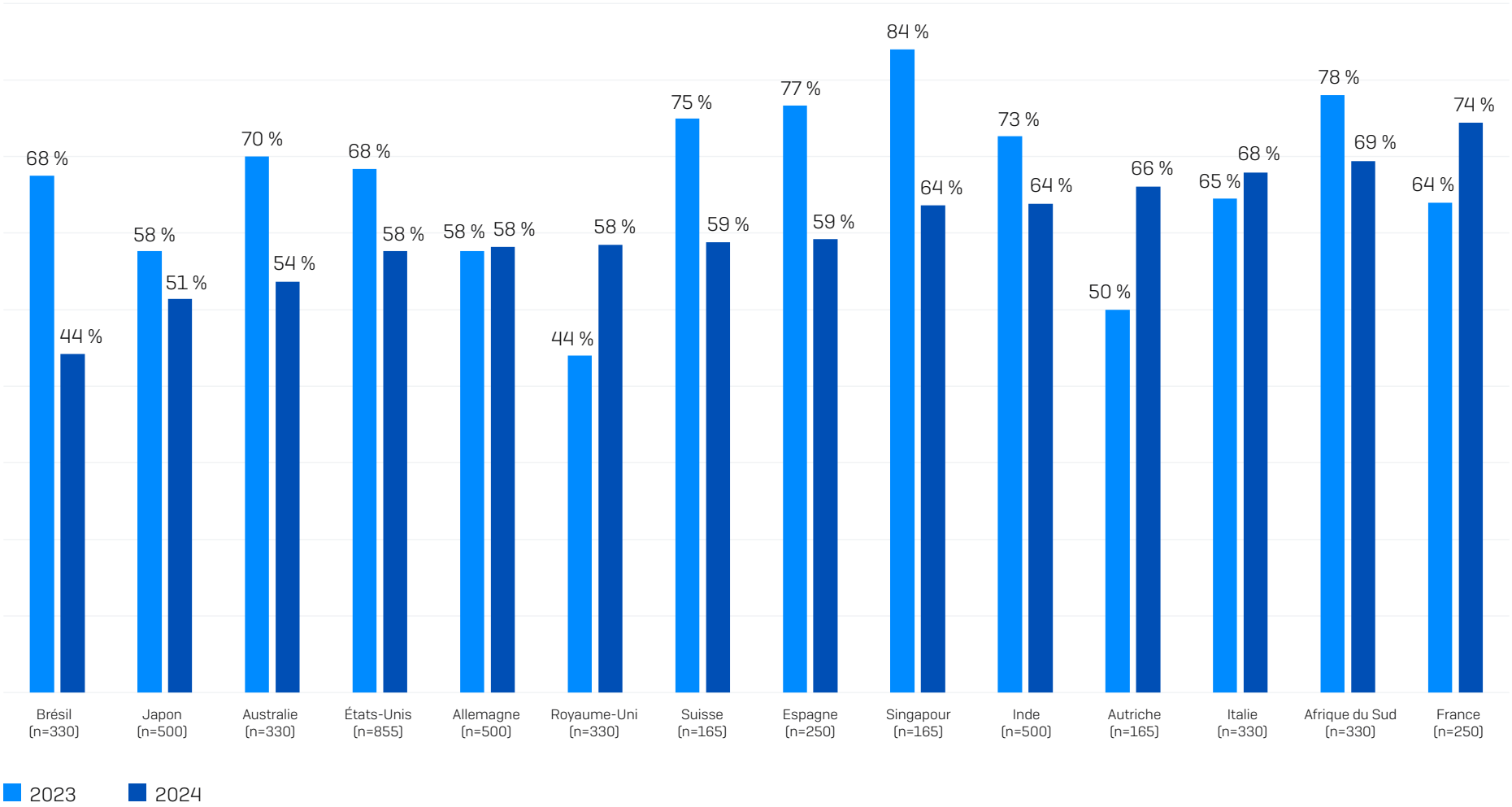
**Pourcentage des entreprises touchées par un ransomware au cours de l'année passée**




Au cours de l'année passée, votre organisation a-t-elle été touchée par un ransomware ? Oui. n=5 000 (2004), 3 000 (2023), 5 600 (2022) Chiffres de base du secteur en 2024 dans le graphique.

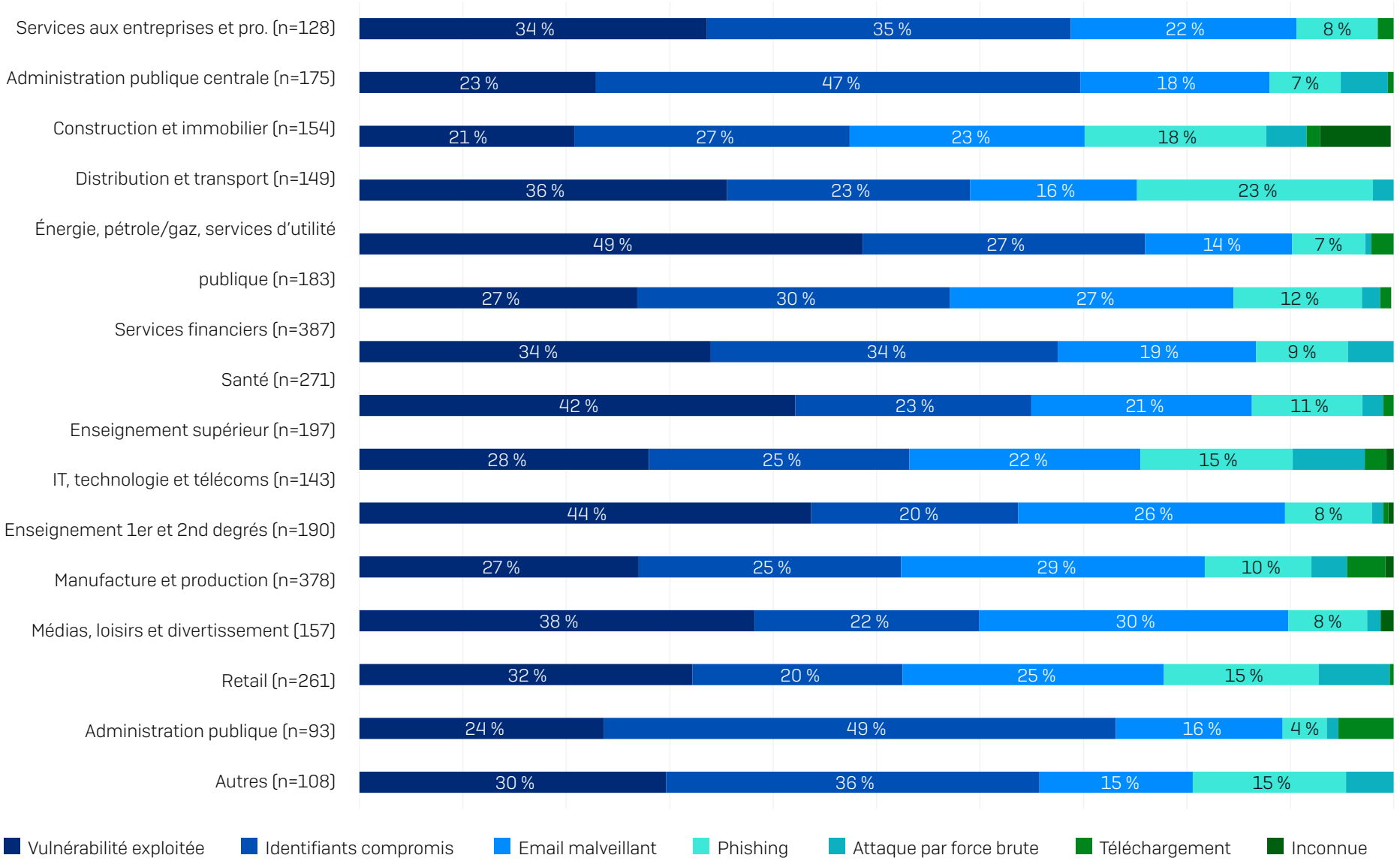
## Taux d'attaques de ransomware - selon le pays

**Pourcentage des entreprises touchées par un ransomware au cours de l'année passée**




Au cours de l'année passée, votre organisation a-t-elle été touchée par un ransomware ? Oui. n=5 000 (2024) n=3 000 (2023). Chiffres de base du pays en 2024 dans le graphique.

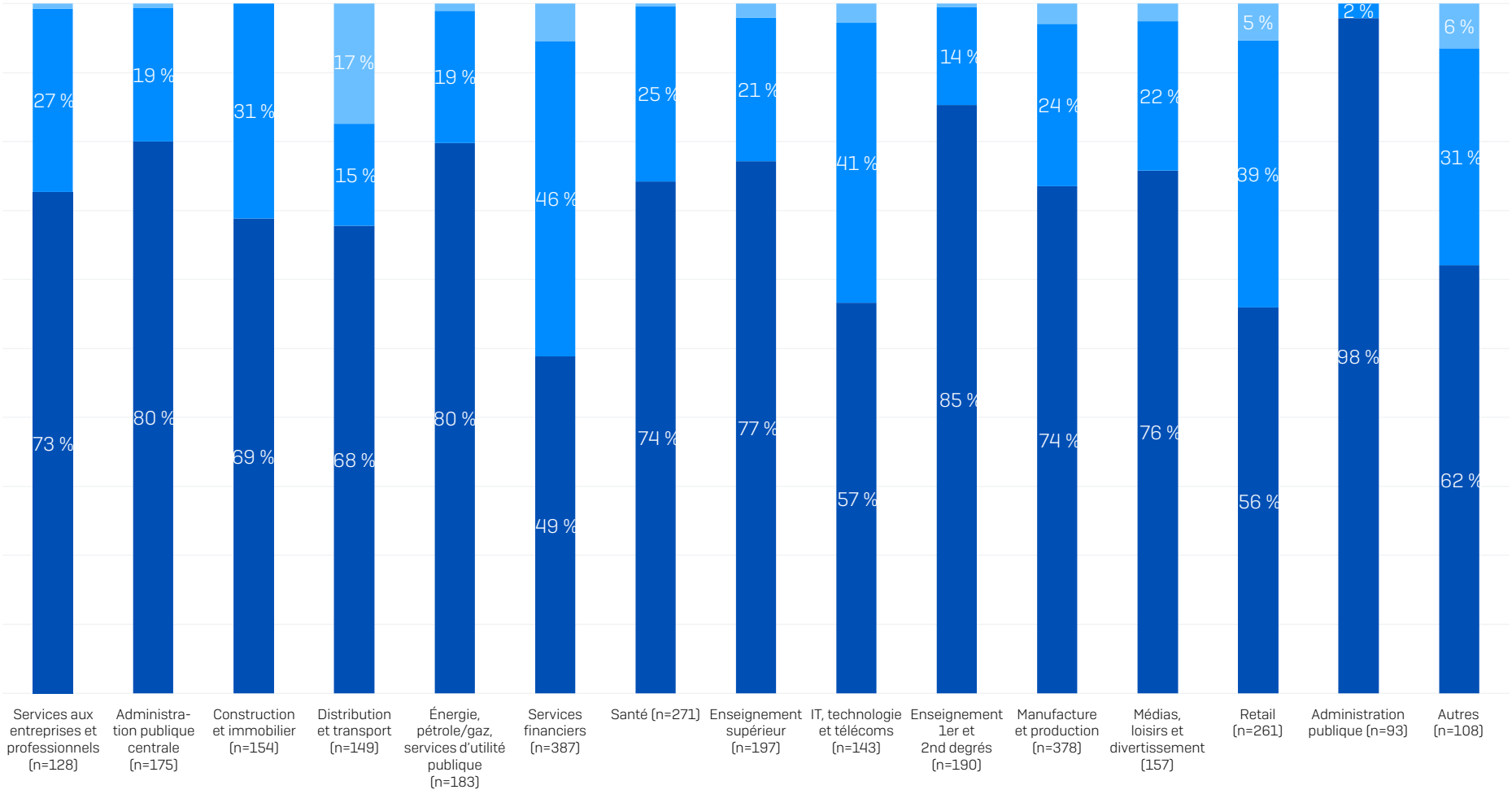
## Causes premières de l'attaque - selon le secteur d'activité




Connaissez-vous la cause première de l'attaque de ransomware dont votre entreprise a été victime au cours de l'année écoulée ? n=2 974 entreprises touchées par un ransomware.

## Taux de chiffrement des données - selon le secteur d'activité

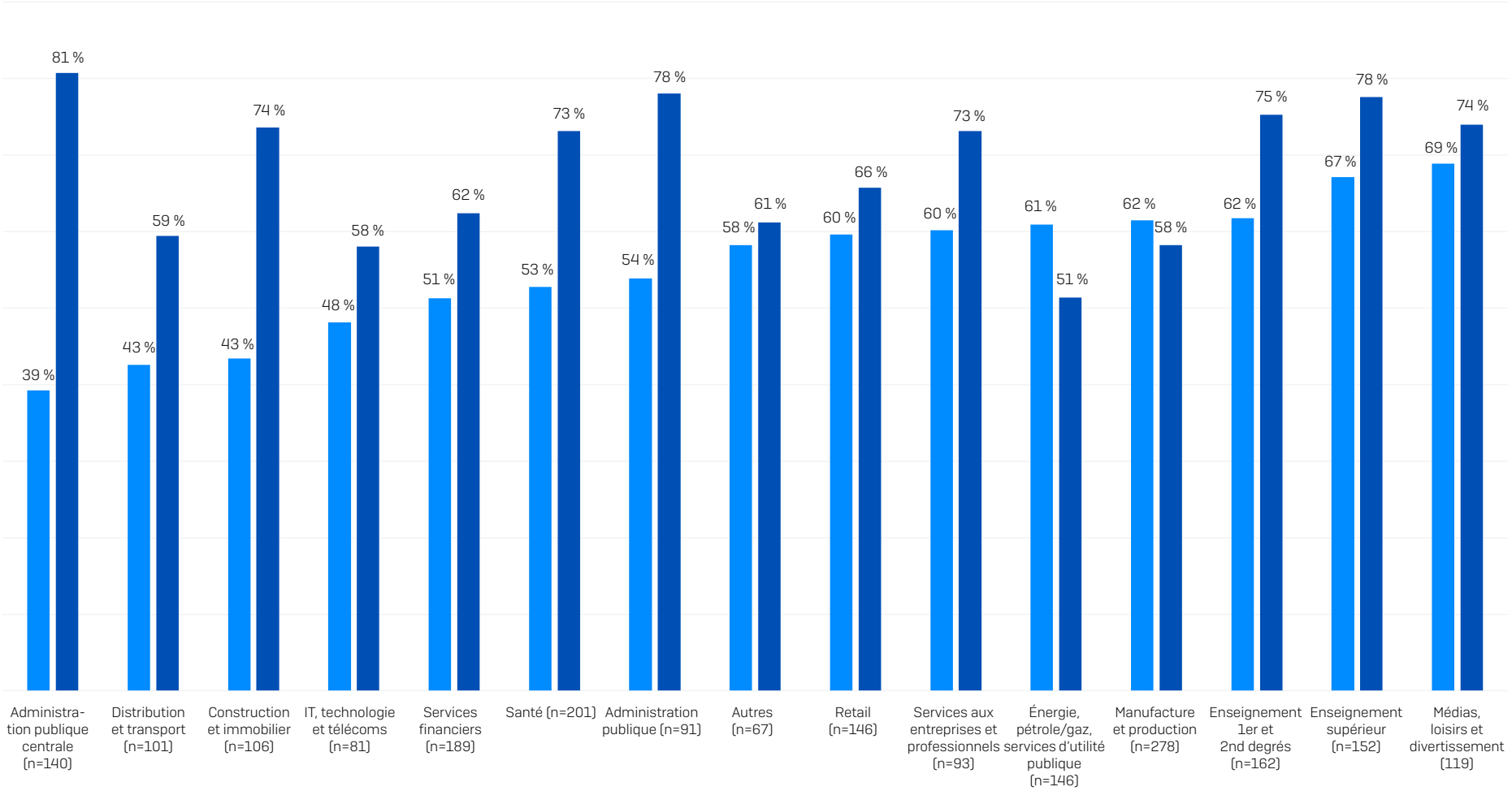
### Propension à subir un chiffrement des données lors d'une attaque




Lors de l'attaque par ransomware, les cybercriminels ont-ils réussi à chiffrer les données de votre entreprise ? Chiffres de base dans le graphique.

## Méthodes de récupération des données - selon le secteur d'activité

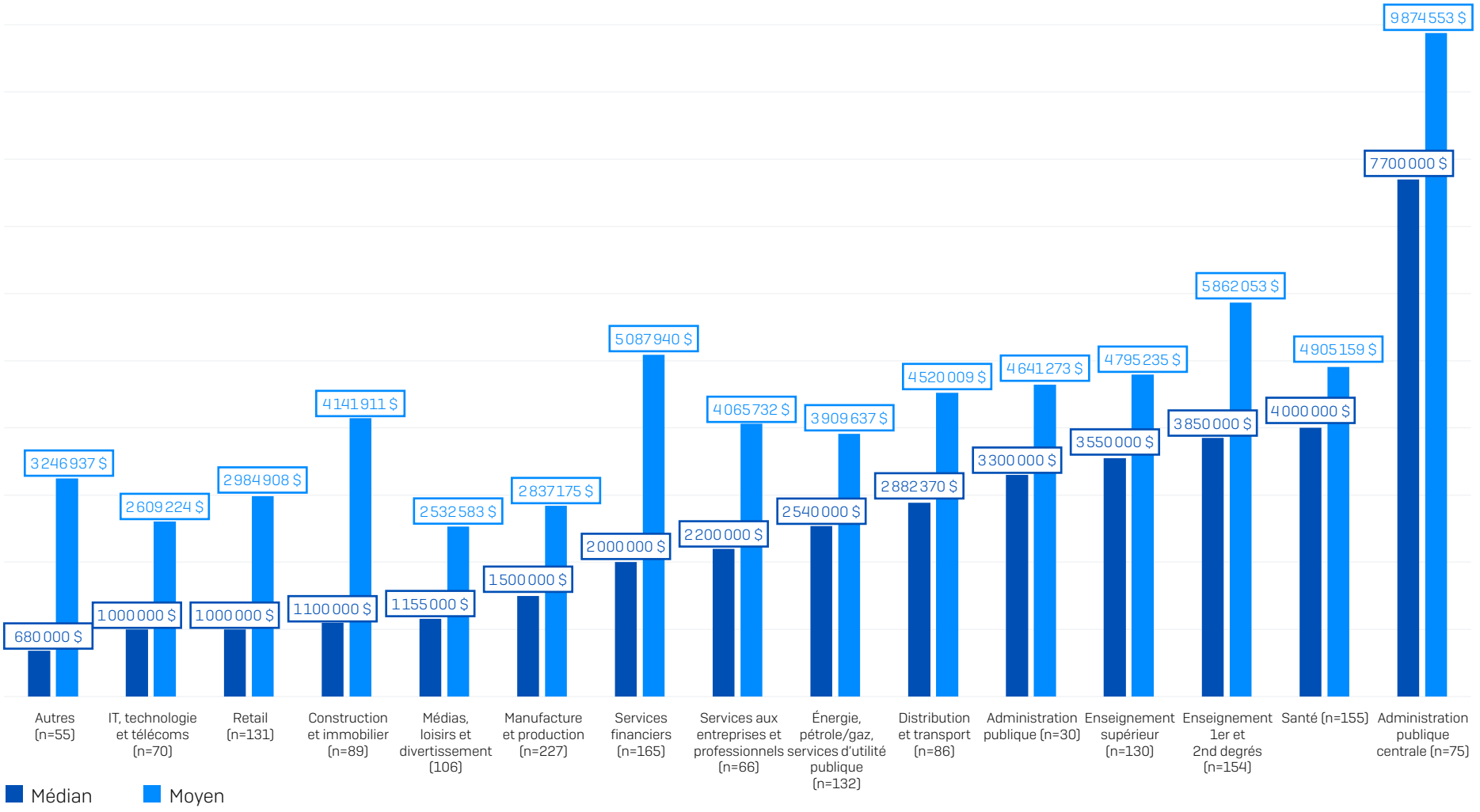
**À quelle fréquence les données sont-elles récupérées en utilisant des sauvegardes et en payant la rançon ?**




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. Classement effectué selon la propension à payer la rançon.

## Montant des demandes de rançon - selon le secteur d'activité

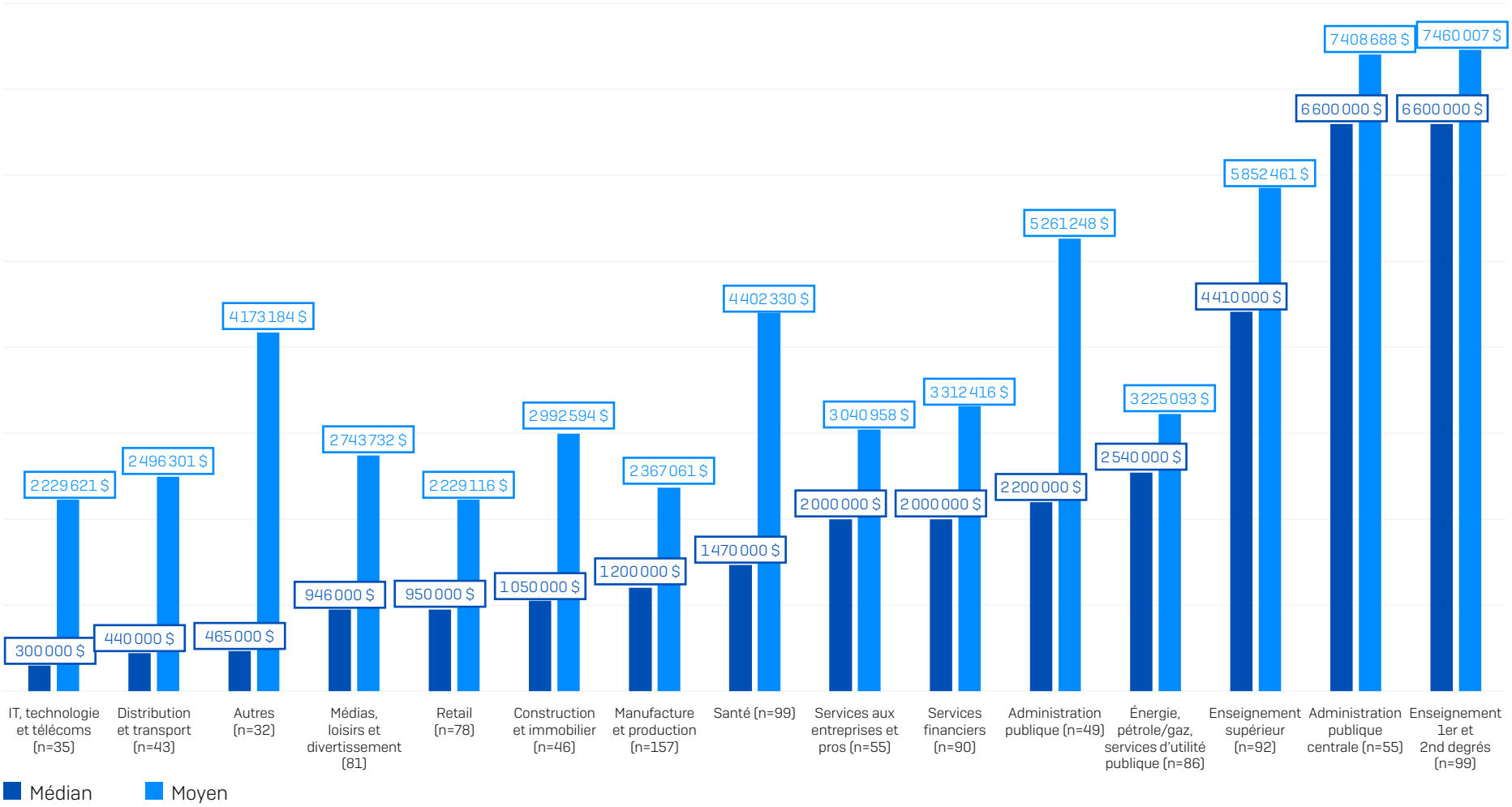
### Demande de rançon




Quel était le montant de la rançon demandée par les attaquants ? Chiffres de base dans le graphique. Classement effectué par demande médiane.

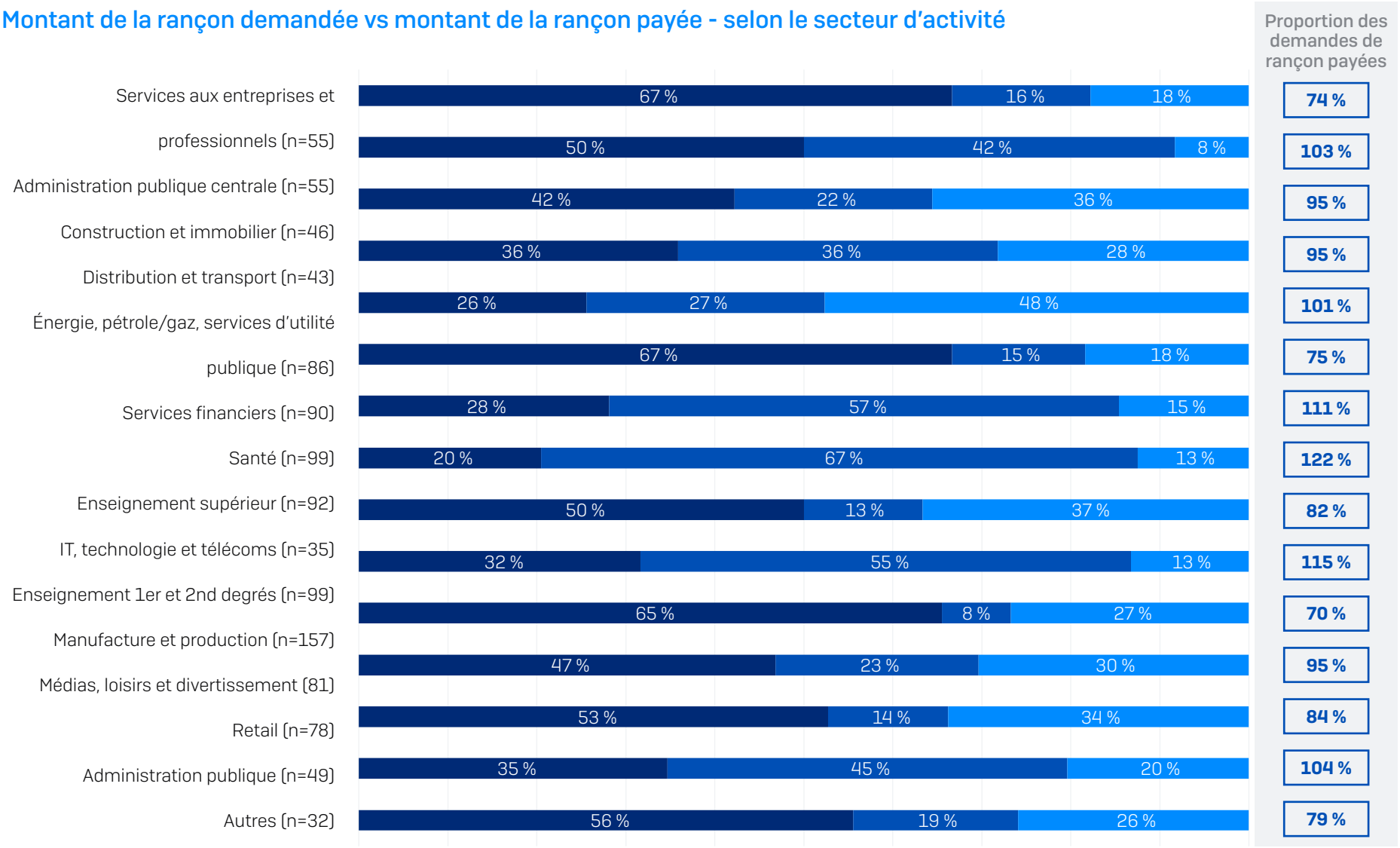
## Montant des rançons payées - selon le secteur d'activité

### Paiement de la rançon




Quel était le montant de la rançon payée aux attaquants ? Chiffres de base dans le graphique. Données classées par montant médian du paiement

## Montant de la rançon demandée vs montant de la rançon payée - selon le secteur d'activité




Quel était le montant de la rançon demandée par les attaquants ? Quel était le montant de la rançon payée aux attaquants ? Chiffres de base dans le graphique.

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.



2024-04-16 (WP-PC)

SOPHOS