Mai 2023

ÉTUDE DE MARCHÉ

Tendances du spear phishing en 2023

Principales conclusions concernant d'une part l'impact des attaques et d'autre part les défis liés à la détection des menaces et aux mesures prises pour y faire face »

Barracuda®
Your journey, secured.

Sommaire

Résultats clés

50% des entreprises ont été victimes d'attaques par spear phishing au cours des 12 derniers mois

En moyenne, **10 e-mails suspects** sont signalés au service informatique d'une entreprise pour chaque journée de travail

Une entreprise typique reçoit **5 e-mails de spear phishing hautement personnalisés** par jour

Il faut en moyenne **deux jours** pour détecter un incident lié à la sécurité des e-mails

1 entreprise sur 4 a vu au moins un de ses comptes de messagerie compromis en 2022

Les pirates envoient en moyenne **370 e-mails malveillants** à partir de chaque compte compromis

Introduction

Le spear phishing reste un phénomène de faible ampleur mais à fort impact

Alors que les cybercriminels cherchent à tirer parti de nombreux vecteurs d'attaques différents, les e-mails restent parmi les plus populaires. Les 13 types de menaces par e-mail identifiés par les chercheurs de Barracuda, notamment le spear phishing ne cessent d'évoluer.

Face à la profusion d'attaques basées sur les e-mails, les entreprises s'exposent à des pertes financières, à une dégradation de la réputation et à d'autres impacts négatifs.

Le spear phishing est une forme d'attaque par e-mail hautement personnalisée. Les pirates font des recherches sur leurs cibles et rédigent des messages soigneusement conçus, se faisant souvent passer pour un collègue, un site Web ou une entreprise de confiance. Les e-mails de spear phishing visent généralement à voler des informations sensibles (identifiants, informations financières, etc.) qui sont ensuite utilisées pour effectuer des activités frauduleuses, usurper des identités et commettre d'autres crimes en tout genre.

Méthodologie

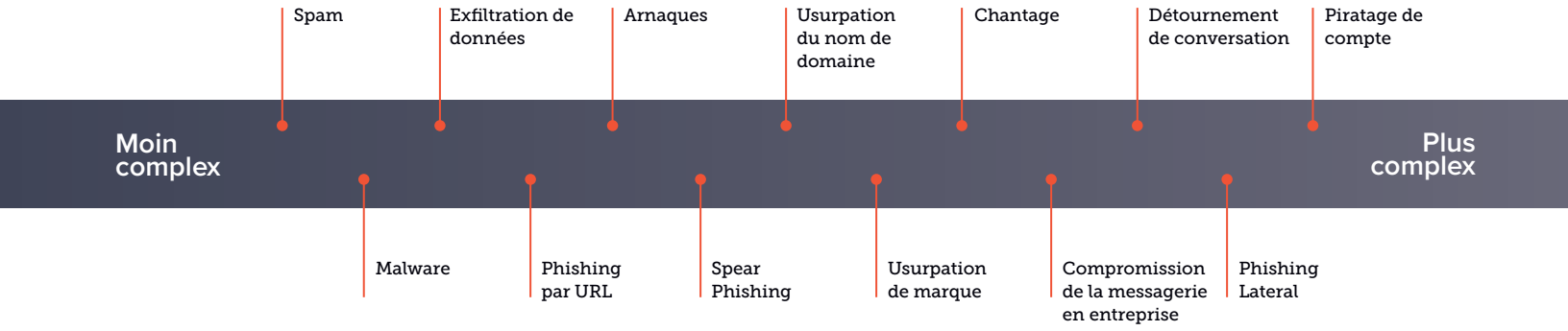
Ce rapport présente des données et des analyses exclusives sur le spear phishing collectées et produites par les chercheurs de Barracuda à partir d'un ensemble de données comprenant 50 milliards d'e-mails répartis dans 3,5 millions de boîtes de réception, dont près de 30 millions d'e-mails de spear phishing.

Le rapport présente également les résultats d'une étude commandée par Barracuda à Vanson Bourne. Le cabinet d'études de marché indépendant Vanson Bourne a mené une enquête mondiale auprès de 1 350 responsables informatiques, professionnels techniques de l'informatique, responsables de la sécurité informatique et décisionnaires principaux en informatique et en sécurité informatique, qui représentent des entreprises de toutes tailles dans un large éventail de secteurs d'activité. Les participants à l'enquête travaillent aux États-Unis, en Australie, en Inde et en Europe. En Europe, les pays représentés sont : le Royaume-Uni, la France, le DACH (Allemagne, Autriche, Suisse), le Benelux (Belgique, Pays-Bas, Luxembourg) et les pays nordiques (Danemark, Finlande, Norvège, Suède). L'enquête a été réalisée en décembre 2022.

Conçues pour échapper aux mesures traditionnelles de protection des e-mails, y compris les passerelles et les filtres anti-spam, les attaques par spear phishing proviennent souvent de domaines à la réputation élevée ou de comptes de messagerie déjà compromis. Les e-mails de spear phishing n'incluent pas toujours de pièces jointes ou de liens malveillants. Étant donné que la plupart des techniques traditionnelles de sécurité des e-mails reposent sur des listes de blocage et des analyses de réputation, ces attaques passent à travers les mailles du filet. D'autre part, elles utilisent généralement des techniques de spoofing et incluent des liens « zero-day », des URLs hébergées sur des domaines non utilisés lors d'attaques précédentes ou qui ont été insérées dans des sites Web légitimes piratés et il est donc peu probable que les technologies de protection des URLs les bloquent.

Les cybercriminels adoptent également des tactiques de social engineering (création d'un sentiment d'urgence, caractère laconique des instructions et mise sous pression des victimes) dans leurs attaques par spear phishing afin d'accroître les chances de réussite.

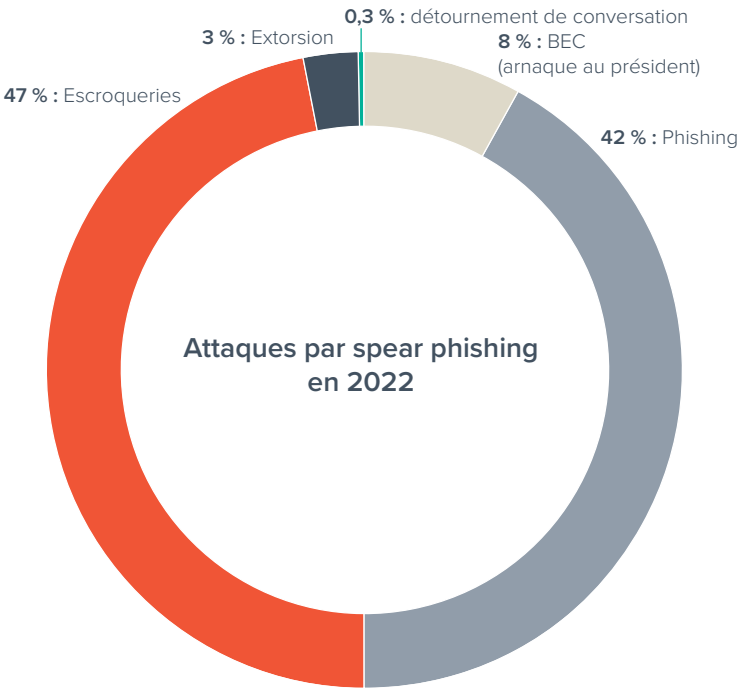
13 types de menaces par e-mail



Détection et analyse par Barracuda des attaques par spear-phishing en 2022

Lors d'une analyse de 50 milliards d'e-mails dans 3,5 millions de boîtes de messagerie, les chercheurs de Barracuda ont découvert près de 30 000 000 e-mails de spear-phishing. Bien que ces e-mails représentent moins de 0,1 % de tous les e-mails envoyés, ils ont un impact considérable sur les entreprises lorsque les attaques réussissent (à titre de comparaison, les attaques en masse telles que le spam et les malwares représentent environ 16 % des e-mails, mais leur impact n'est pas aussi fort). Le coût moyen d'une violation de données causée par la compromission d'un e-mail professionnel s'élevait à près de 5 millions de dollars en 2022, selon IBM. Et aucune entreprise n'est à l'abri.

Les recherches de Barracuda montrent que l'entreprise lambda reçoit environ 5 e-mails de spear-phishing par jour, soit plus de 1 700 par an. La plus mauvaise nouvelle est sans doute que l'analyse de Barracuda révèle que les e-mails de spear-phishing ont un taux de clics moyen de 11 %. Sachant qu'une seule attaque réussie peut être dévastatrice, il est essentiel de disposer d'une protection à plusieurs niveaux contre ces menaces basées sur les e-mails.



Les chercheurs de Barracuda ont identifié cinq principaux types d'attaques par spear phishing :

Arnaques

Les escroqueries représentent 47 % des e-mails de spear phishing analysés, ce qui en fait l'attaque la plus fréquente. Les escroqueries peuvent prendre de nombreuses formes, mais elles sont toutes conçues pour voler des informations privées, sensibles et personnellement identifiables, telles que des numéros de comptes bancaires, de cartes de crédit et de sécurité sociale. Les pirates incitent les victimes à divulguer ces informations, puis les utilisent pour les escroquer, usurper leur identité, ou les deux. Les attaques sont exécutées en recourant à divers procédés, tels que les gains de loterie, les colis non réclamés, les fausses offres d'emploi, les sollicitations de dons et d'autres tactiques.

Usurpation de marque

Ce type de spear phishing, conçu pour usurper l'identité d'entreprises connues et d'applications professionnelles fréquemment utilisées, représente 42 % de l'ensemble des attaques. C'est l'un des types d'attaques les plus populaires, car il permet de collecter des identifiants et de pirater des comptes. Les attaques par usurpation de marque sont généralement utilisées pour voler des identifiants de compte, mais elles sont parfois utilisées pour voler des informations personnelles identifiables, telles que les numéros de carte de crédit et de sécurité sociale. Les pirates se font passer pour de grandes entreprises et des applications populaires, telles que Microsoft, DHL, DocuSign, WeTransfer et bien d'autres.

Compromission d'une boîte de messagerie professionnelle

Également connue sous le nom de fraude au Président, whaling et fraude au virement bancaire, la compromission des e-mails professionnels ne représente qu'un petit 8 % des attaques par spear phishing, mais elle a généré des milliards de dollars de pertes. Les escrocs se font passer pour un employé, un partenaire, un fournisseur ou une autre personne de confiance dans un e-mail et demandent un virement bancaire ou des informations personnelles identifiables à des employés du service financier ou à d'autres personnes ayant accès à des informations sensibles. Ces attaques très ciblées sont particulièrement difficiles à détecter, car elles comportent rarement une URL ou une pièce jointe malveillante.

Chantage

Les attaques par extorsion représentent 3 % du nombre total d'attaques par phishing ciblées. La plupart des attaques sont des menaces de sextorsion par e-mail. Les cybercriminels prétendent détenir des vidéos, des images ou d'autres contenus sensibles ou embarrassants qui auraient été enregistrés sur l'ordinateur de la victime. Ils menacent de les partager avec tous les contacts e-mail de la victime, à moins qu'une rançon ne soit payée. Les demandes varient généralement de quelques centaines à quelques milliers de dollars et doivent être payées en bitcoins, dont la traçabilité est difficile.

Détournement de conversations

Le détournement de conversation, également connu sous le nom d'usurpation d'identité d'un fournisseur, peut être dévastateur. Dans ces attaques complexes, qui ne représentent que 0,3 % de tous les e-mails de spear-phishing, les cybercriminels se glissent dans des conversations professionnelles existantes ou en lancent de nouvelles sur la base d'informations qu'ils ont recueillies à partir de comptes e-mail compromis ou d'autres sources.

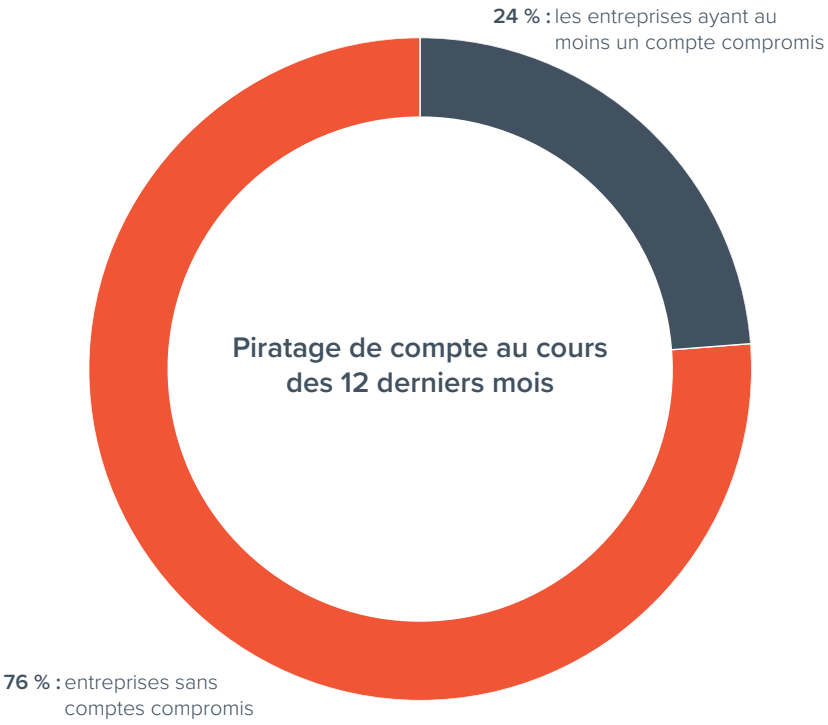
La plupart du temps, le détournement de conversations s'inscrit dans une attaque de piratage de comptes. Les pirates utilisent des attaques par phishing pour voler les identifiants de connexion et compromettre les comptes professionnels. Ils lisent ensuite les e-mails et surveillent le compte compromis afin de cerner les opérations de l'entreprise et de se renseigner sur

les transactions en cours, les procédures de paiement et d'autres détails. Les pirates vont alors exploiter ces informations, y compris les conversations internes et externes entre les employés, les partenaires et les clients, pour élaborer des messages convaincants, les envoyer à partir de domaines usurpés, et inciter leurs victimes à transférer de l'argent ou à mettre à jour leurs informations de paiement.

La compromission ou le piratage d'un compte est souvent le fruit d'une attaque par phishing. Les pirates utilisent des tactiques de social engineering pour inciter les utilisateurs à divulguer leurs identifiants de connexion, qui sont ensuite utilisés pour infiltrer le réseau d'une entreprise. Une fois à l'intérieur, les pirates peuvent se déployer latéralement au sein de l'entreprise et compromettre des comptes stratégiques ou utiliser des comptes compromis comme base pour lancer d'autres attaques.

En 2022, d'après les données et les analyses de Barracuda, près d'une entreprise sur quatre (24 %) a vu au moins un de ses comptes de messagerie compromis à la suite du piratage d'un compte. Les pirates envoient en moyenne 370 e-mails malveillants à partir de chaque compte compromis.

Le reste du rapport traite du phénomène de spear-phishing dans le monde, de l'impact des attaques, des défis en matière de détection et de réponse et aborde finalement une série de questions connexes.



L'impact et les coûts des attaques par spear phishing

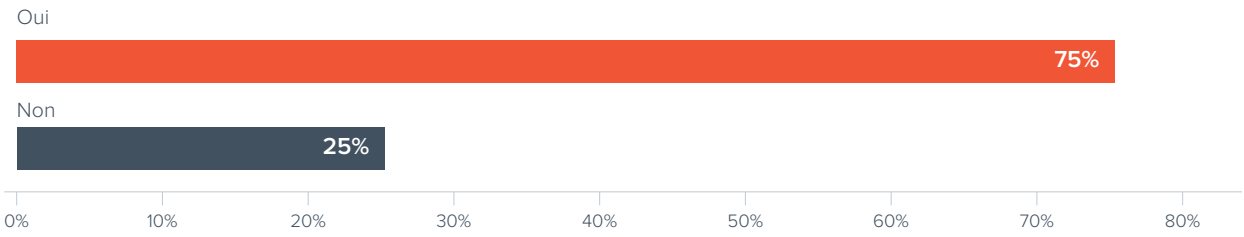
Alors que les attaques par spear phishing sont de faible ampleur, elles sont répandues et très efficaces par rapport aux autres types d'attaques par e-mail.

Le succès des attaques par spear-phishing

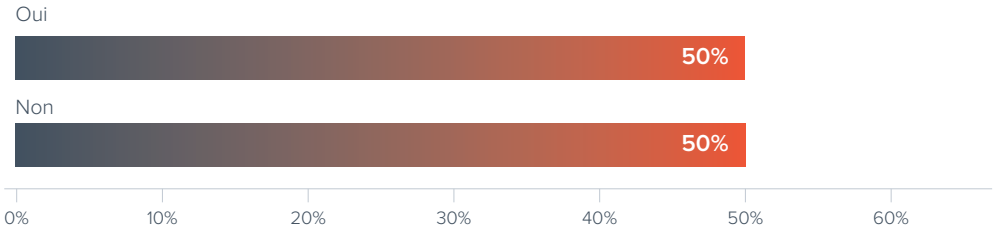
Les trois quarts des personnes interrogées ont déclaré avoir été victimes d'une attaque par e-mail au cours des 12 derniers mois. La moitié ont déclaré avoir été victimes de spear phishing. Cela signifie que 2 attaques par e-mail réussies sur 3 sont des attaques par spear phishing, qui utilisent des messages personnalisés, le social engineering et d'autres tactiques.

Ce chiffre est important car, selon les données de Barracuda, ces attaques ne représentent que 0,1 % de toutes les attaques par e-mail, mais sont à l'origine de 66 % de toutes les violations. D'autre part, les attaques en masse telles que le spam et les malwares représentent 16 % des e-mails, mais ne sont responsables que d'un tiers des violations. La protection contre le spear-phishing est essentielle, car une seule attaque réussie peut avoir des conséquences dévastatrices.

Votre entreprise a-t-elle été victime d'une attaque par spear phishing au cours des 12 derniers mois ? (n=1.350)

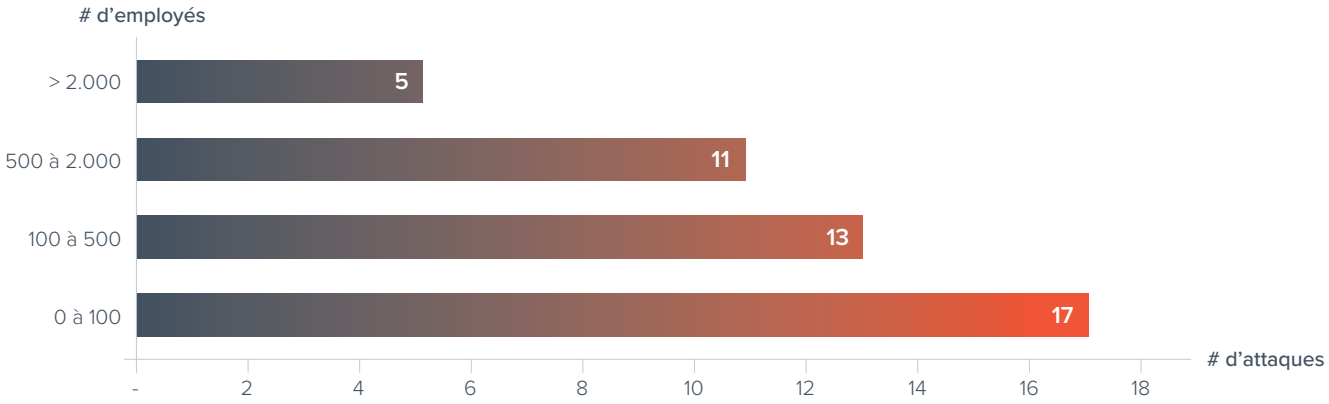


Votre entreprise a-t-elle été victime d'une attaque par spear phishing au cours des 12 derniers mois? (n=1.350)



Alors que les petites entreprises signalent moins d'attaques par e-mail dues au spear phishing (42 %), le rapport 2022 de Barracuda, Spear Phishing : les principales menaces et tendances (volume 7), a révélé que les petites entreprises étaient attaquées de manière disproportionnée, avec un nombre moyen d'attaques par social engineering plus élevé pour chaque boîte de réception. Souvent, les petites entreprises ne disposent pas des outils nécessaires pour identifier et bloquer les attaques complexes, ni même pour identifier les attaques en cours et y remédier. Nombre d'entre elles ne sont peut-être pas conscientes du nombre de menaces déjà présentes dans les boîtes de réception de leurs utilisateurs.

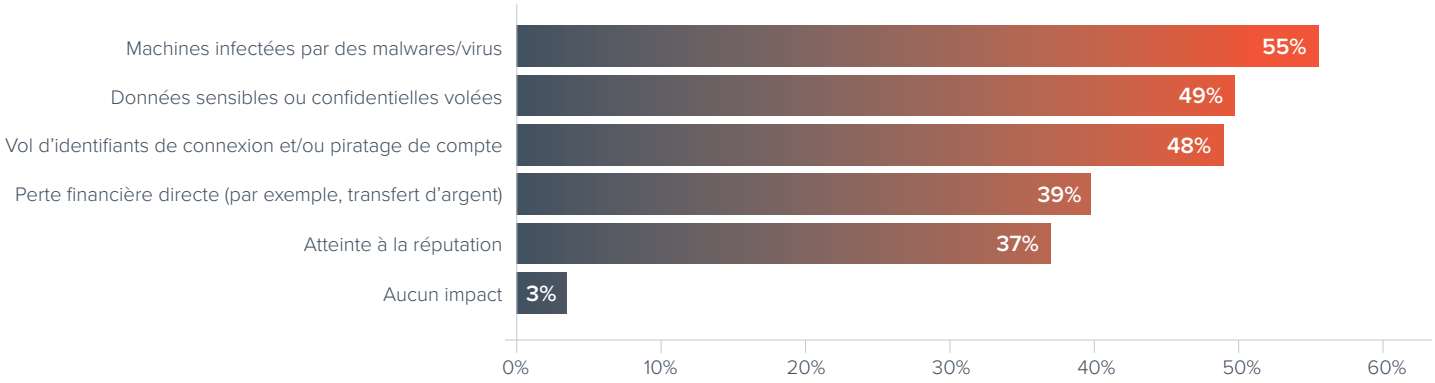
Nombre moyen d'attaques par ingénierie sociale par boîte mail



Selon notre récente étude de marché, les entreprises utilisant Gmail sont plus susceptibles d'être victimes d'attaques par spear-phishing que celles utilisant Microsoft 365. 57 % des entreprises utilisant Gmail ont signalé avoir été victimes d'une attaque par spear-phishing, contre 41 % pour celles utilisant Microsoft. Dans l'environnement Microsoft, de nombreuses options de sécurité sont disponibles, ce qui offre une meilleure protection.

L'impact des attaques par spear phishing

Quel a été l'impact des attaques par spear phishing menées contre votre organisation au cours des 12 derniers mois ? (n=678)



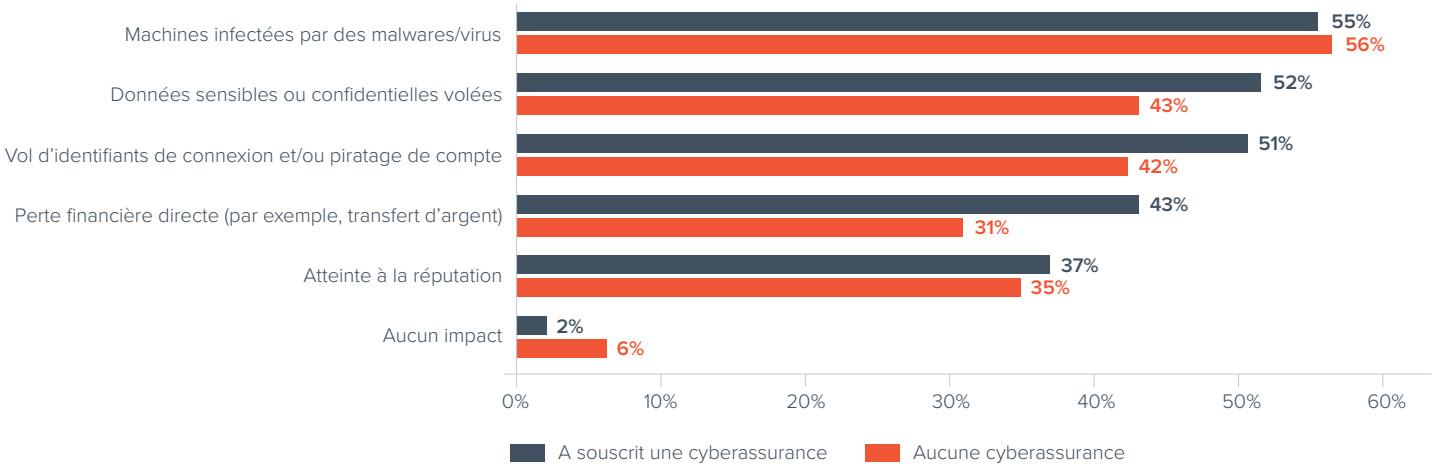
Presque toutes les victimes d'une attaque par spear-phishing au cours des 12 derniers mois ont constaté des répercussions sur leur entreprise, notamment des introductions de malwares, le vol de données et des atteintes à la réputation. Bien qu'une perte financière directe soit l'un des effets, tous les autres impacts peuvent également entraîner des conséquences financières pour une entreprise à la suite d'une attaque.

Les pirates qui cherchent à lancer des attaques par malwares, comme celles impliquant des ransomwares, ont souvent recours au phishing pour infiltrer une entreprise. Le vol d'identifiants constitue également un objectif commun de ces attaques, car les escrocs s'appuient de plus en plus sur des tactiques de spear-phishing pour avoir accès à un compte et le pirater par la suite.

Parmi ceux qui ont déclaré avoir été victimes d'une attaque par spear-phishing au cours des 12 derniers mois, près de la moitié ont dit avoir été victimes d'un vol d'identifiants de connexion et/ou d'un piratage de compte.

Pour les entreprises qui n'ont pas souscrit une cyberassurance, c'est l'infection des machines qui a été le plus souvent citée comme conséquence des attaques par spear-phishing. Si celles qui ont souscrit une cyberassurance ont également été victimes de ce phénomène, elles étaient plus susceptibles de subir d'autres préjudices, notamment le vol d'informations et d'identifiants, ainsi que des pertes financières directes. La différence pourrait être que seules les entreprises ayant des informations sensibles à voler citeraient cette conséquence. Il est également possible que les entreprises ne soient pas conscientes de ces problèmes et n'en recherchent pas toujours les conséquences (comme la perte d'informations sensibles ou le vol d'identifiants).

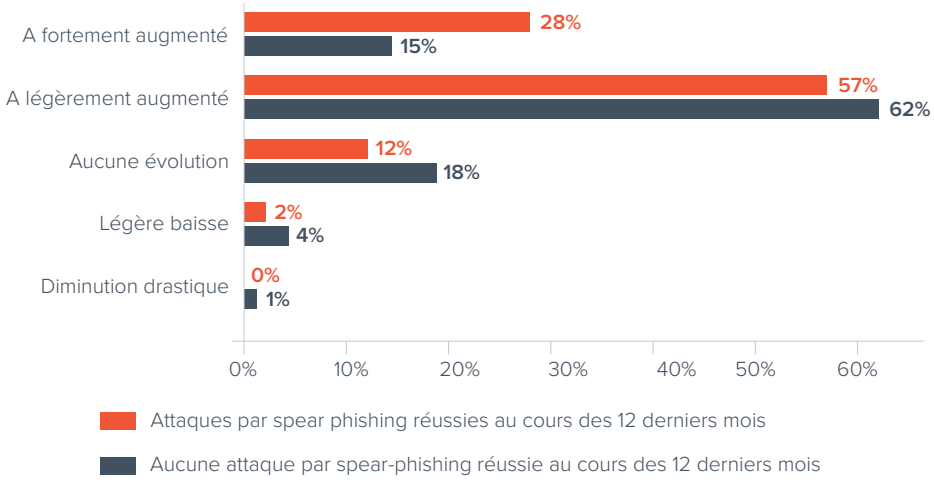
Quel a été l'impact des attaques par spear phishing menées contre votre organisation au cours des 12 derniers mois? (n=678)



Les coûts des attaques par spear phishing

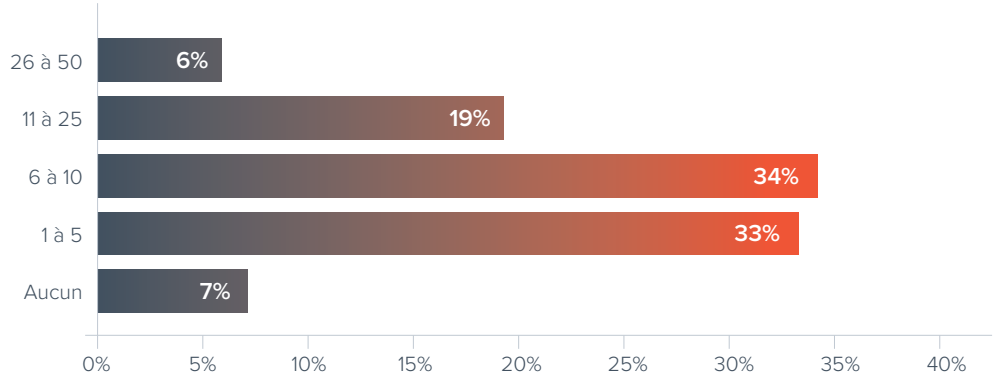
Les entreprises victimes d'une attaque par spear-phishing étaient plus susceptibles de déclarer que les coûts associés à une violation de la sécurité des e-mails avaient considérablement augmenté au cours de l'année écoulée (28 % contre 15 % pour les entreprises qui n'avaient pas été victimes d'une attaque par spear-phishing). Ces entreprises sont également plus susceptibles de supporter des coûts globaux de récupération et d'impact plus élevés suite à l'attaque la plus coûteuse qu'elles ont subie une moyenne de 1,1 million de dollars contre 760 882 $ pour celles qui ont été victimes d'autres types d'attaques par e-mail.

Quelle a été l'évolution du coût total des atteintes à la sécurité des e-mails au cours des 12 derniers mois? (n=1.003)



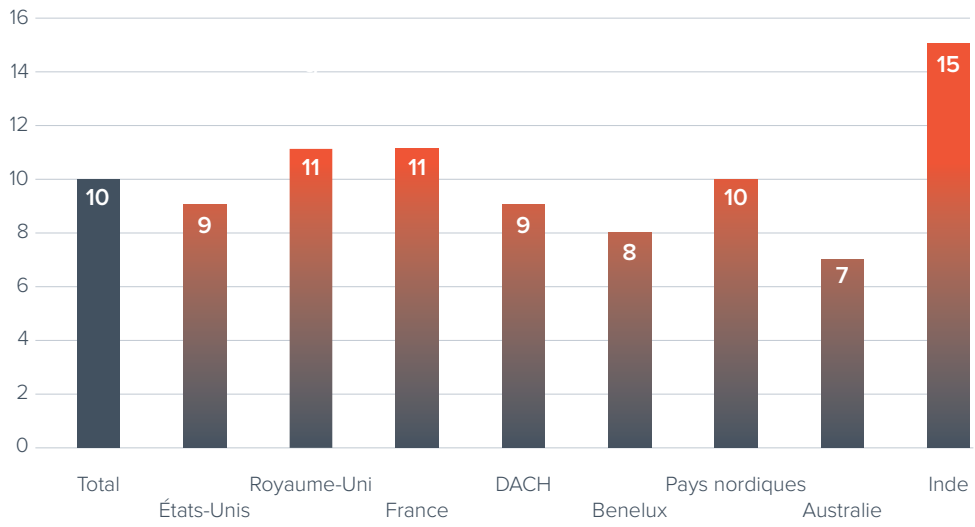
93 % des entreprises ont demandé à leurs utilisateurs de signaler les messages suspects après réception

Environ combien d'e-mails suspects sont signalés au service informatique de votre entreprise en une journée de travail? (n=1.350)



En moyenne, 10 e-mails suspects sont signalés au service informatique chaque journée de travail

Environ combien d'e-mails suspects sont signalés au service informatique de votre entreprise en une journée de travail? (n=1.350)



Par région, les utilisateurs indiens signalent le nombre moyen le plus élevé d'e-mails suspects par jour, soit 50 % de plus que la moyenne mondiale. Cela pourrait indiquer que les entreprises ont du mal à prévenir les attaques par e-mail ou que les entreprises indiennes accordent une plus grande attention aux e-mails suspects et qu'elles repèrent et signalent en conséquence une moyenne plus élevée. Toutefois, un grand nombre de messages signalés n'est pas toujours une bonne chose ; cela peut également signifier que les utilisateurs signalent beaucoup d'e-mails indésirables ou de messages indésirables et non des e-mails malveillants.

7 % des entreprises dans le monde affirment qu'aucun e-mail n'est signalé par leurs utilisateurs. Dans la région DACH et en Australie, les chiffres sont particulièrement élevés, avec 14 % d'entre elles déclarant qu'aucun e-mail n'est signalé. Ces régions présentent également des niveaux d'adoption des formations de sensibilisation à la sécurité informatique inférieurs à la moyenne. Alors que la moyenne mondiale est de 42 %, elle est de 28 % en Australie et de 37 % dans la région DACH.

Un investissement moindre dans la sensibilisation à la sécurité peut avoir conduit les utilisateurs à être moins vigilants ou moins aptes à reconnaître une menace potentielle par e-mail.

Compte tenu de la nature hautement personnalisée des e-mails de spear-phishing et des conséquences potentiellement graves d'une attaque réussie, chaque entreprise, quelle que soit sa taille et sa situation géographique, a tout intérêt à prendre les précautions nécessaires pour prévenir ces attaques.

En proportion, les utilisateurs des grandes entreprises signalent moins d'e-mails suspects.

Le nombre d'attaques signalées par les utilisateurs n'est pas proportionnel à la taille de leur entreprise. Les entreprises de 100 à 249 employés signalent en moyenne 7 e-mails suspects par jour, tandis que les entreprises de 1 000 à 2 500 employés en signalent en moyenne 12 par jour. Comme nous l'avons vu précédemment, les petites entreprises subissent un plus grand nombre d'attaques par spear-phishing par rapport à leur taille.

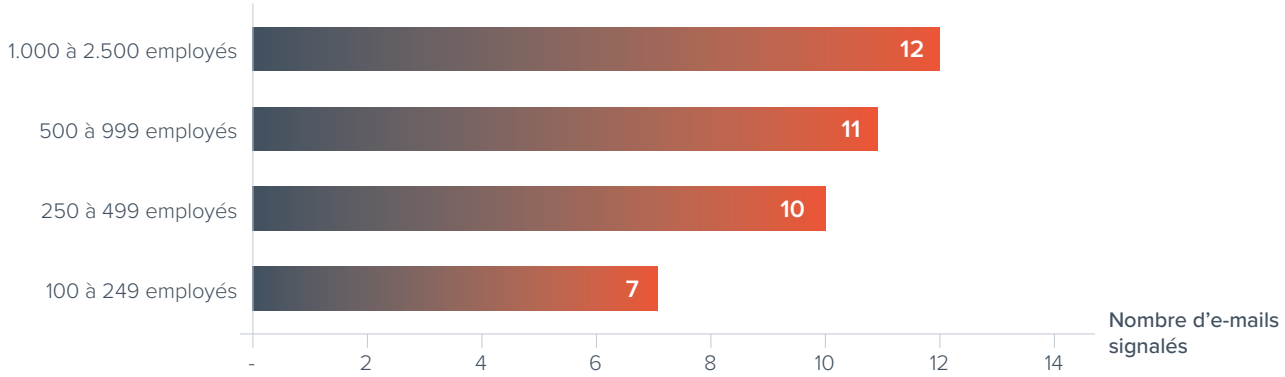
Ce volume plus important d'attaques et certains rapporteurs potentiellement trop zélés pourraient signifier que les équipes informatiques doivent traiter un plus grand nombre de messages. Malheureusement, les petites entreprises ont des équipes informatiques plus réduites et ne disposent donc pas toujours des outils et des ressources nécessaires pour traiter tous les incidents.

Les grandes entreprises sont plus susceptibles d'utiliser des outils et des ressources qui permettent de déterminer quels incidents doivent être traités en priorité et de faire rapidement la différence entre les e-mails anodins et les e-mails malveillants.

Les utilisateurs des entreprises dont plus de 50 % du personnel travaille à distance signalent des niveaux plus élevés d'e-mails suspects (12 par jour en moyenne, contre 9 par jour pour les entreprises dont moins de 50 % du personnel travaille à distance). En raison de la dispersion de leurs employés, les entreprises qui emploient un grand nombre de travailleurs à distance sont plus sensibles aux menaces potentielles. Étant donné qu'elles sont plus susceptibles d'être victimes d'une attaque par spear-phishing, il se peut qu'elles accueillent favorablement certains signalements erronés de la part de leurs utilisateurs.

Dans les entreprises victimes de plusieurs attaques par ransomware, les employés signalent également des niveaux plus élevés d'e-mails suspects (avec une moyenne quotidienne de 17 e-mails suspects pour les entreprises victimes d'au moins trois attaques par ransomware). La sensibilisation des utilisateurs à la sécurité dans les entreprises est susceptible d'augmenter après une attaque par ransomware, ce qui pourrait conduire les utilisateurs à faire plus de signalements que d'habitude.

Environ combien d'e-mails suspects sont signalés au service informatique de votre entreprise en une journée de travail? (en moyenne) (n=1.350)



Défis liés à la détection des menaces et à la réponse

Aucune sécurité n'est efficace à 100 %. Lorsqu'une menace est détectée, les équipes de sécurité doivent agir rapidement pour l'identifier et y remédier avant qu'elle ne se propage et ne cause des dommages importants. Des temps de détection et de réponse plus rapides réduisent le risque de faille de sécurité.

En moyenne, les entreprises mettent près de 100 heures à identifier une menace par e-mail après réception, à y répondre et à y remédier

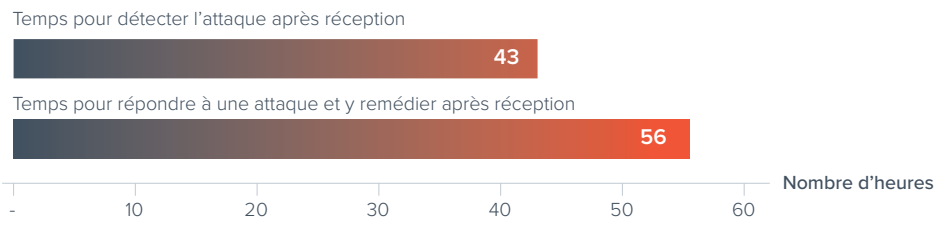
Avec un temps de détection moyen de 43 heures et un temps de réponse et de remédiation moyen de 56 heures pour les menaces par e-mail après réception, les entreprises ont besoin de près de 100 heures pour traiter un incident de sécurité par e-mail.

Pour une entreprise sur cinq (22 %), il faut plus de 24 heures pour identifier une attaque par e-mail. Cette longue période donne aux utilisateurs le temps et l'occasion de cliquer sur un lien malveillant ou de répondre à un e-mail. Dans ce cas, les pirates peuvent utiliser le compte piraté pour infiltrer le réseau et compromettre éventuellement d'autres comptes.

Comme si les longs délais de détection n'étaient pas assez préoccupants, 38 % des personnes interrogées ont déclaré qu'il leur fallait plus de 24 heures pour répondre aux attaques et y remédier une fois qu'elles ont eu connaissance de leur existence.

Les délais de détection, de réponse et de remédiation sont en moyenne plus courts pour les grandes entreprises, qui disposent généralement de plus de ressources et peuvent réagir plus rapidement. Bien qu'une grande entreprise soit potentiellement plus vulnérable aux menaces, une équipe dédiée à la sécurité plus nombreuse devrait être en mesure de détecter les attaques, d'y répondre et d'y remédier plus rapidement.

En ce qui concerne vos temps de détection et de réponse pour les incidents par e-mail (après réception ou signalés), combien de temps environ faut-il à votre entreprise pour prendre les mesures suivantes? (heures) (n=1.350)

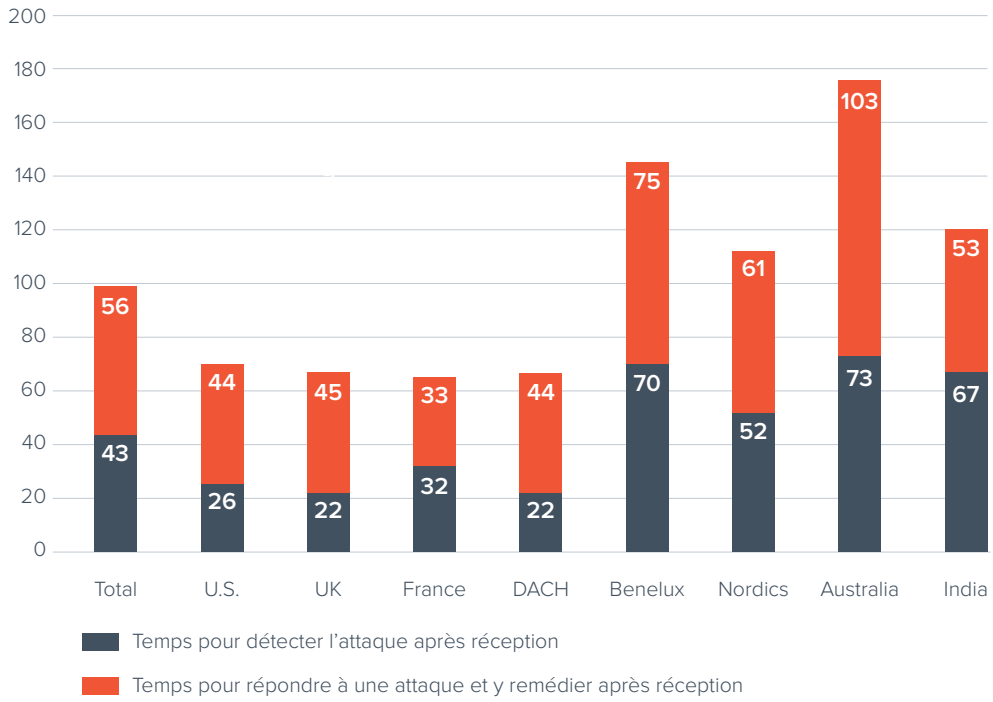


Les investissements dans l'automatisation et la formation à la sécurité réduisent les délais de réponse

Le faible taux d'adoption de la réponse automatisée en cas d'incident en Australie (24 %) peut très bien être un facteur expliquant les longs délais de réponse. L'Australie affiche également les taux d'adoption des formations de sensibilisation à la sécurité informatique les plus faibles. La responsabilité de détecter les menaces après réception et d'y répondre incombe principalement aux services informatiques, ce qui prend trop de temps s'ils ne disposent pas des bons outils (175 heures en moyenne en Australie).

À l'inverse, 36 % des entreprises américaines ont recours à la réponse automatisée aux incidents et 45 % à la formation de sensibilisation à la sécurité informatique. Elles présentent également des temps de réponse plus rapides en moyenne, ce qui signifie qu'elles utilisent moins de ressources informatiques et que celles-ci peuvent se consacrer à d'autres tâches.

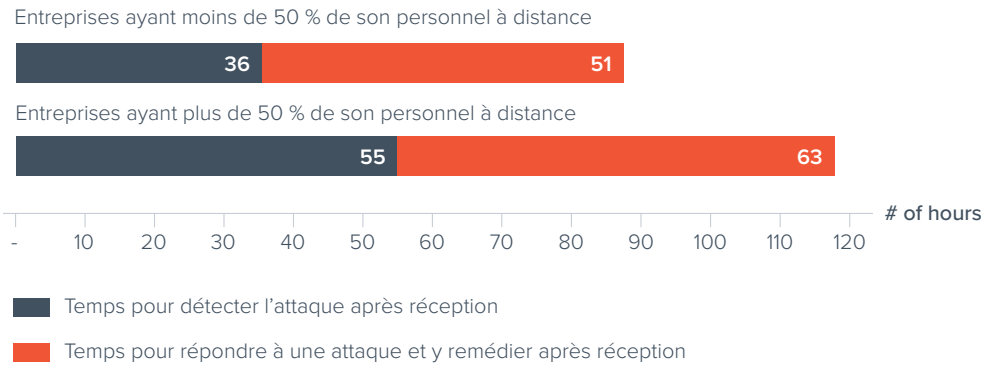
En ce qui concerne vos temps de détection et de réponse pour les incidents par e-mail (après réception ou signalés), combien de temps environ faut-il à votre entreprise pour prendre les mesures suivantes? (heures) (n=1.350)



L'augmentation du nombre de travailleurs à distance entrave la détection et le temps de réponse

Les entreprises qui emploient davantage de travailleurs à distance mettent plus de temps à détecter les incidents liés à la sécurité des e-mails et à y répondre. Les entreprises dont moins de 50 % des employés travaillent à distance ont eu un temps de détection moyen de 36 heures, tandis que celles dont plus de 50 % des employés travaillent à distance ont eu besoin de 55 heures en moyenne pour détecter un incident lié à la sécurité des e-mails. Il en va de même pour les mesures correctives : les entreprises ayant moins de 50 % de personnel à distance ont eu un temps de réponse et de correction moyen de 51 heures, tandis que celles ayant plus de 50 % de personnel à distance ont eu besoin de 63 heures en moyenne pour répondre à un incident de sécurité des e-mails et y remédier.

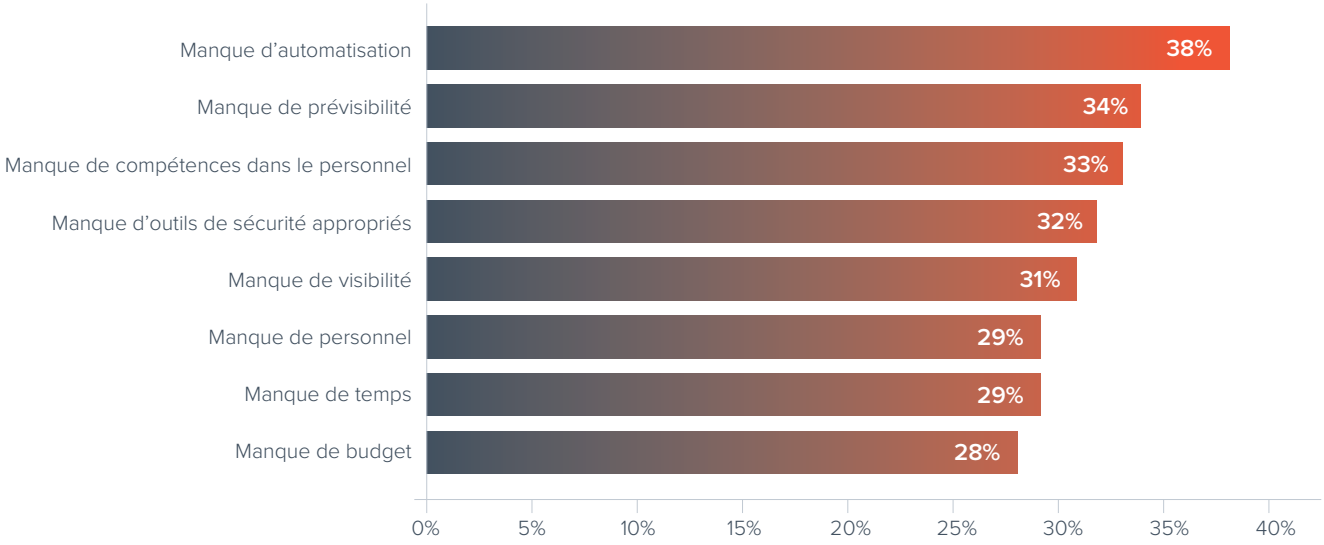
En ce qui concerne vos temps de détection et de réponse pour les incidents par e-mail (après réception ou signalés), combien de temps environ faut-il à votre entreprise pour prendre les mesures suivantes? (heures) (n=1.350)



Le manque d'automatisation est un problème majeur

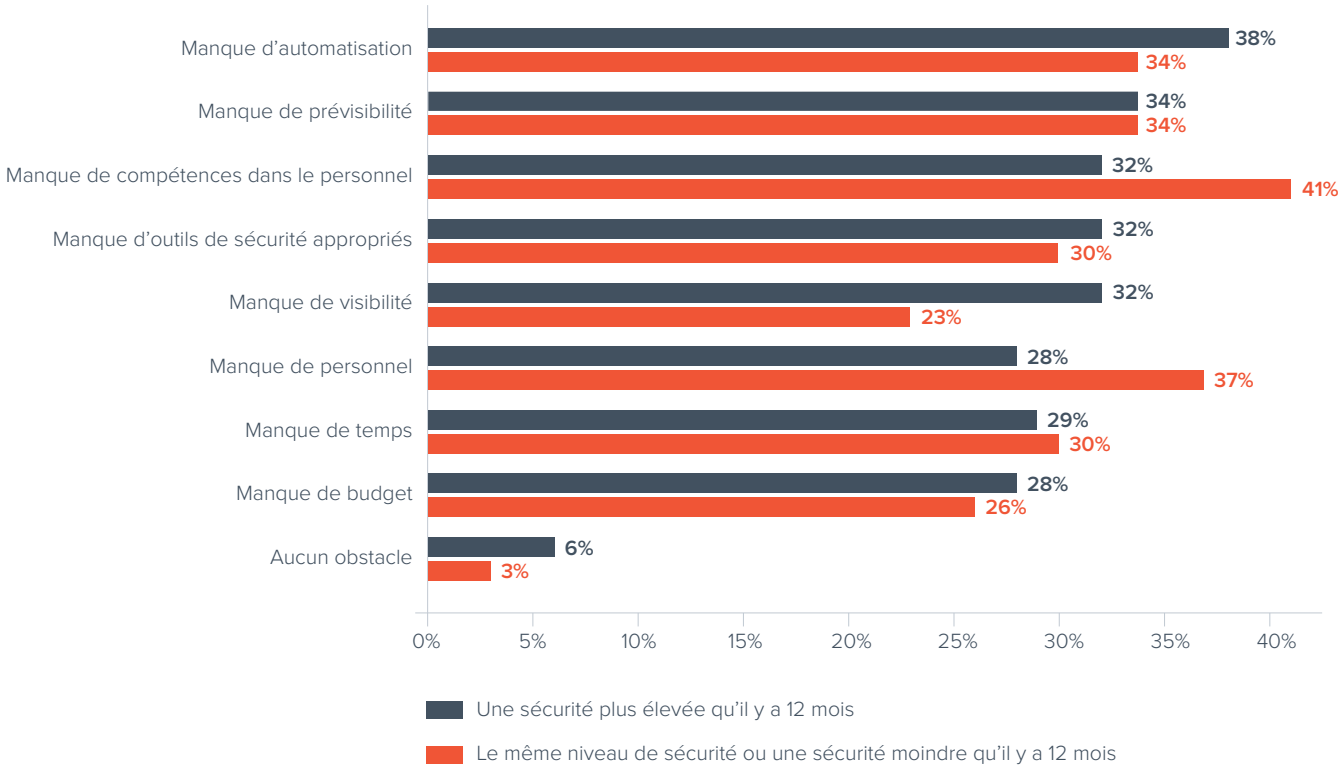
Les grandes entreprises citent le manque d'automatisation comme le principal obstacle à une réponse rapide à un incident : 41 % pour les entreprises de plus de 250 employés contre 28 % pour les entreprises de 100 à 249 employés. Ces petites entreprises citent presque à égalité d'autres raisons, notamment le manque de prévisibilité (29 %), les compétences du personnel (32 %) et les outils de sécurité appropriés (32 %). Les petites entreprises semblent être toujours en phase d'adoption d'outils appropriés et semblent avoir des difficultés à recruter et à conserver un personnel compétent. Une fois que les entreprises ont mis en place le personnel, les processus et la technologie appropriés, elles peuvent tirer parti des outils disponibles pour optimiser le traitement des problèmes, notamment l'automatisation.

Quels sont les principaux obstacles qui empêchent une détection des menaces et une réponse rapides après réception dans votre entreprise (n=1.350)



Les entreprises qui se sentent plus en sécurité déclarent également que le manque d'automatisation est l'obstacle le plus probable à la réponse rapide aux incidents. En revanche, les entreprises qui se sentent moins en sécurité font état d'un manque de personnel compétent. Disposer d'un personnel compétent est une condition préalable à la mise en place d'un solide programme de réponse aux incidents et l'automatisation peut contribuer à accélérer considérablement cette réponse.

Quels sont les principaux obstacles qui empêchent une détection des menaces et une réponse rapides après réception dans votre entreprise? (n=1.350)



Bonnes pratiques pour contrer les attaques par spear phishing

Alors que les attaques par e-mail évoluent et deviennent de plus en plus sophistiquées, les entreprises sont confrontées à de sérieuses menaces d'attaques ciblées par spear-phishing. L'impact d'une seule attaque réussie peut avoir des conséquences dévastatrices. Pour protéger votre entreprise et vos utilisateurs, vous devez investir dans une technologie permettant de contrer les attaques et former votre personnel pour qu'il constitue la dernière ligne de défense.

Technologie

- **Tirez parti de l'intelligence artificielle.** Les escrocs adaptent leurs stratégies d'attaque par e-mail pour contourner les passerelles et les filtres anti-spam. Il est donc essentiel de disposer d'une solution qui protège des attaques par spear-phishing, notamment la compromission des boîtes de messagerie professionnelle, l'usurpation d'identité et les attaques d'extorsion. Déployez une technologie conçue à cet effet qui ne repose pas uniquement sur la recherche de pièces jointes ou de liens malveillants. Utilisez l'apprentissage automatique pour analyser les schémas de communication habituels de votre entreprise et pour repérer les anomalies qui témoignent potentiellement d'une attaque.

- **Déployez une protection contre le piratage de compte.** Veillez à ce que les escrocs n'utilisent pas les comptes compromis de votre entreprise pour lancer des attaques par spear-phishing. Utilisez une technologie fondée sur l'intelligence artificielle qui reconnaît les comptes compromis et qui prend des mesures correctives en temps réel en alertant les utilisateurs et en supprimant les e-mails malveillants envoyés à partir des comptes compromis.

- **Gardez un œil sur les règles de la boîte de réception et sur les connexions suspectes.** Utilisez la technologie pour identifier les activités suspectes, notamment les connexions à partir d'adresses IP et de lieux inhabituels, signe potentiel que votre compte est compromis. Veillez également à surveiller les comptes de messagerie pour détecter d'éventuelles règles malveillantes dans la boîte de réception, car elles sont souvent utilisées pour masquer ou supprimer des e-mails envoyés dans le cadre d'un piratage de compte.

- **Utilisez l'authentification multifacteur.** Prévoyez un niveau de sécurité supplémentaire au-delà du nom d'utilisateur et du mot de passe, tel qu'un code d'authentification, une empreinte de pouce ou une authentification biométrique.

- **Mettez en œuvre l'authentification DMARC et la création de rapports.** Cela permet de prévenir l'usurpation de domaine, l'une des techniques les plus couramment utilisées dans les attaques d'usurpation d'identité. Prévenez l'usurpation de domaine et le détournement de marque grâce à l'authentification et à l'application de DMARC. Définissez avec précision les règles d'application pour votre entreprise à l'aide des rapports et des analyses DMARC.

- **Automatisez la réponse aux incidents.** Avec une solution automatisée de réponse, vous pouvez rapidement éliminer les menaces détectées dans les boîtes de réception et assurer un traitement plus efficace de tous les messages à venir.

- **Apprenez aux membres du personnel à reconnaître et à signaler les attaques.** Sensibilisez les utilisateurs aux attaques par spear-phishing en les faisant suivre une formation de sensibilisation à la sécurité. Assurez-vous que les membres du personnel savent reconnaître ces attaques, comprennent leur caractère frauduleux et sont en mesure de les signaler.

- **Maximisez la prévention de la perte des données.** Utilisez la bonne combinaison de technologies et de stratégies professionnelles pour garantir que les e-mails contenant des informations confidentielles, personnelles ou sensibles ne puissent jamais sortir de l'entreprise.

Barracuda en quelques mots

Notre objectif : faire du monde un endroit plus sûr.

Chez Barracuda, nous pensons que chaque entreprise mérite un accès à des solutions de sécurité de niveau professionnel cloud-first, abordables, intuitives et facilement déployables. Nous protégeons vos e-mails, vos réseaux, vos données et vos applications à l'aide de solutions innovantes capables de s'adapter au parcours de nos clients et de se développer en conséquence.

Plus de 200 000 entreprises partout dans le monde ont choisi Barracuda pour veiller à leur sécurité pendant qu'elles prospèrent

Pour en savoir plus, rendez-vous sur barracuda.com.

À propos de Vanson Bourne

Vanson Bourne est un cabinet indépendant spécialiste des études de marché pour le secteur des technologies. Sa réputation de produire des analyses solides, fiables et basées sur des études est elle-même fondée sur des principes rigoureux ainsi que sur sa capacité à interroger des décisionnaires majeurs qui occupent des fonctions techniques et métier dans tous les secteurs et sur les marchés principaux.

Pour plus d'informations, accédez à vansonbourne.com.

Barracuda
Your journey, secured.