Spear Phishing : Menaces et tendances principales

Vol. 7 Mars 2022

Principales conclusions sur les dernières tactiques d'ingénierie sociale et la complexité croissante des attaques

Les cybercriminels affinent constamment leurs tactiques pour rendre leurs attaques plus compliquées et difficiles à détecter. Dans ce rapport détaillé, les chercheurs de Barracuda partagent leurs points de vue sur les dernières tendances en matière d'ingénierie sociale et sur les nouvelles méthodes utilisées par les cybercriminels pour piéger leurs victimes.»

Barracuda
Your journey, secured.

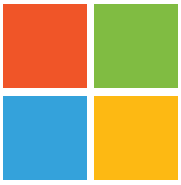
Table des matières

Résultats clés

Le phishing représente **51 %** des attaques d'ingénierie sociale.

Le détournement de conversations a augmenté de près de **270 %** en 2021.

Un employé d'une petite entreprise de moins de 100 employés recevra **350 %** plus d'attaques par ingénierie sociale qu'un employé d'une grande entreprise.



Microsoft est la marque la plus usurpée ; elle est utilisée dans **57 %** des attaques de phishing.

Des comptes ont été piratés dans **1 entreprise sur 5** en 2021.

Les cybercriminels ont piraté environ **500 000** comptes Microsoft 365 en 2021.

Le Nigeria est le pays d'origine de **1 connexion malveillante sur 3** aux comptes piratés.

Les cybercriminels ont envoyé **3 millions de messages à partir** de 12 000 comptes piratés.

Les 13 types de menaces e-mail sont de plus en plus complexes

Pendant des années, les fournisseurs de sécurité ont centré leurs efforts sur la protection contre les attaques par e-mail et les périmètres de défense qu'ils ont pu proposer à leurs clients se sont avérés efficaces contre la plupart des messages électroniques malveillants ou indésirables. Mais cette approche ne suffit plus à elle seule.

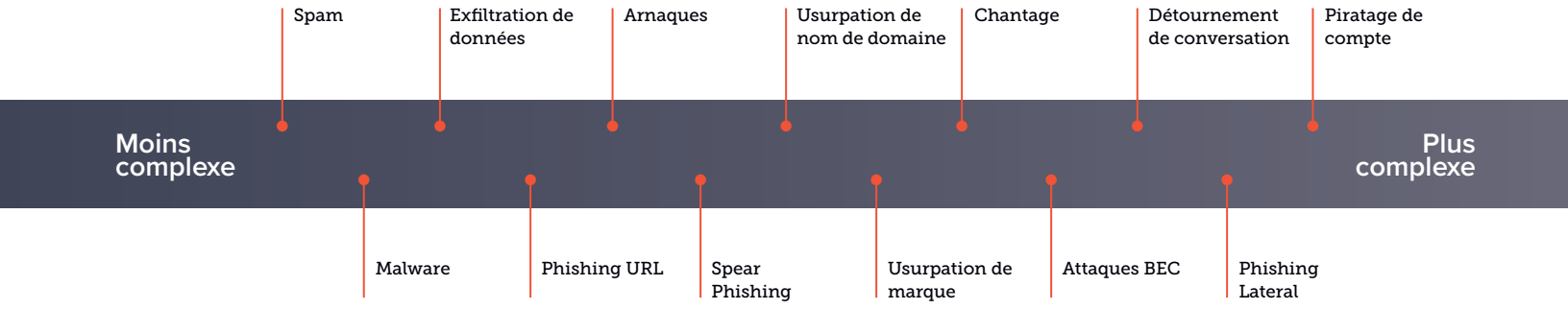
Même si les entreprises arrivent à arrêter des millions d'attaques, les menaces par e-mail continuent à faire des ravages, car elles deviennent de plus en plus complexes et sophistiquées. On assiste à un véritable changement de paradigme dans lequel les attaques volumétriques laissent place aux attaques ciblées, les logiciels malveillants sont délaissés au profit de l'ingénierie sociale et le pirate solitaire est remplacé par une cybercriminalité organisée dont les attaques commencent souvent par un simple e-mail de phishing.

Les méthodes de protection qui s'appuient sur un ensemble de règles, de politiques, de listes d'expéditeurs autorisés ou bloqués, de signatures et d'autres attributs de sécurité traditionnels s'avèrent inefficaces face à la menace en constante évolution des attaques par ingénierie sociale.

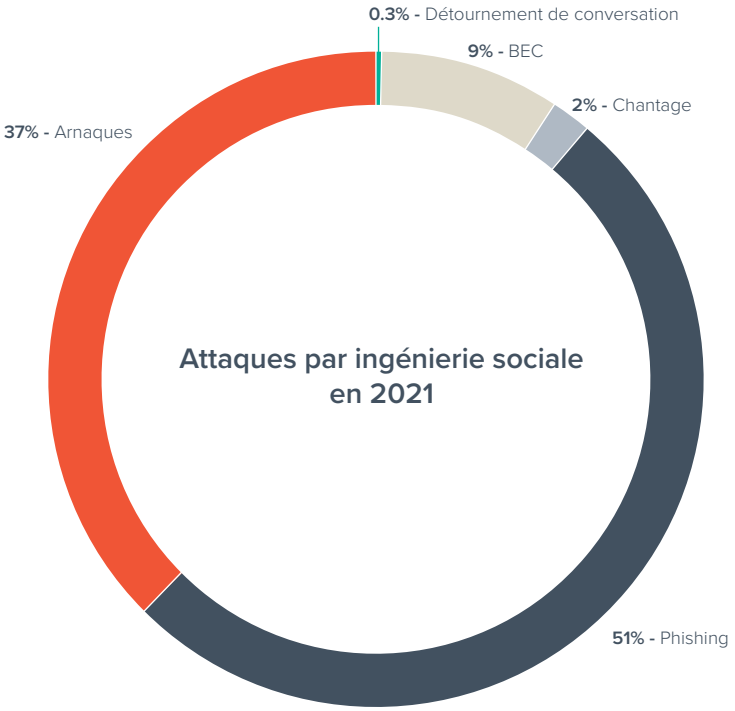
Les pirates combinent différentes tactiques pour amener les victimes à divulguer leurs identifiants afin d'accéder à l'environnement de l'entreprise, à partager des informations sensibles qu'ils pourront vendre ou utiliser lors d'une prochaine attaque, ou encore à effectuer un paiement, un virement ou l'achat de cartes cadeaux.

Les chercheurs de Barracuda ont identifié 13 types de menaces par e-mail qui pèsent actuellement sur les entreprises, des attaques à grande échelle comme le spam ou les malwares aux attaques par ingénierie sociale, plus ciblées, telles que la compromission d'e-mails professionnels et l'usurpation d'identité.

13 types de menaces par e-mail



Nous avons étudié l'évolution de cinq catégories distinctes d'attaques d'ingénierie sociale :



La **compromission d'e-mails professionnels**, ou BEC (Business email compromise), consiste généralement à se faire passer pour quelqu'un appartenant ou non à l'entreprise. En 2021, cette technique représentait 9 % des attaques par ingénierie sociale que nous avons observées, soit à peu près la même proportion que l'année précédente, mais elle prend de plus en plus d'ampleur. Quel que soit leur secteur d'activité, de l'enseignement au voyage en passant par la santé et le commerce, les entreprises ont succombé à ces attaques, leur perte se chiffrant souvent en millions de dollars. Lors d'une attaque BEC classique, le pirate se fait passer pour un collaborateur, généralement un cadre, afin de demander l'exécution d'un virement, l'achat de cartes cadeaux ou encore l'envoi d'un don au profit d'une association caritative fictive.

Ces attaques ne visent pas seulement les utilisateurs de haut rang. Notre précédent rapport a montré que, par exemple, le directeur financier d'une entreprise a autant de chances d'être la cible d'attaques que n'importe quel autre membre de son service.

La technique de **phishing par usurpation d'identité** consiste à envoyer des e-mails au nom d'une marque ou d'un fournisseur de services connus afin d'amener la victime à cliquer sur un lien de phishing. Ces attaques représentent 51 % des attaques par ingénierie sociale que nous avons observées au cours de l'année dernière. La plupart des e-mails de ce type contiennent une URL malveillante. La technique est connue de longue date, mais les pirates ont récemment utilisé de nouvelles astuces pour éviter d'être détectés par les technologies de protection des liens et déposer leurs contenus malveillants dans la boîte de réception de leurs victimes. Par exemple, afin de passer à travers les systèmes d'analyse des e-mails, ils raccourcissent les URL, multiplient les redirections et placent des liens malveillants sur les sites de partage de fichiers.

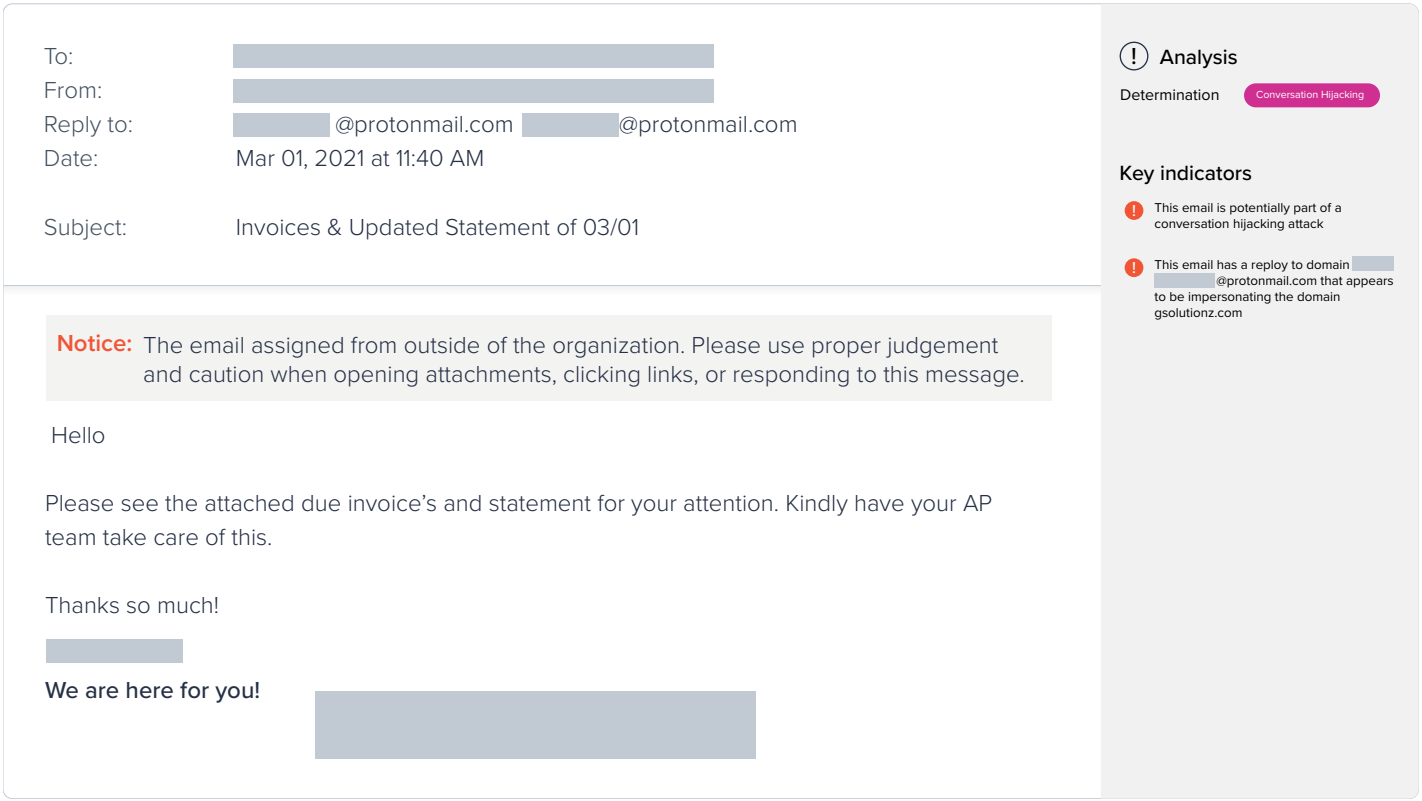
Les pirates ont de plus en plus recours au phishing dans le cadre de leurs attaques par ransomware. Ils usurpent l'identité de marques connues pour amener les victimes à accéder à des sites de phishing et voler leurs identifiants de connexion. Une fois qu'ils ont accès aux comptes d'une entreprise, ils sont en mesure de diffuser des ransomwares depuis l'intérieur, ce qui réduit les risques qu'ils soient détectés.

Les tentatives **de chantage** ne représentent que 2 % du nombre total d'attaques par phishing ciblé que nous avons observées l'année dernière. Il s'agissait pour la plupart d'e-mails de sextortion menaçant les victimes d'envoyer des contenus sensibles ou compromettants à des membres de leur entourage en cas de non-paiement d'une rançon. Le montant de cette dernière s'élève généralement à quelques centaines ou milliers de dollars payables en bitcoins, ce qui rend la transaction difficile à retracer. Au Royaume-Uni, le nombre de cas de sextortion signalés à la National Crime Agency a augmenté de 88 % entre 2018 et 2020, et le nombre devrait continuer à augmenter.

Les tentatives d'**escroquerie** sont très diverses : arnaques à la loterie, fonds ou colis non réclamés, propositions commerciales, fausses embauches et dons fictifs, pour n'en citer que quelques-unes. Contrairement aux autres types décrits ci-dessus, les tentatives d'escroquerie attaques semblent moins ciblées, mais elles représentent tout de même 37 % des attaques par ingénierie sociale que nous avons détectées l'année dernière et n'en sont pas moins efficaces. Étant donné que les pirates ratissent large, les différents types d'arnaques qu'ils mettent au point coûtent aux victimes des centaines de millions de dollars.

Par exemple, au cours des deux dernières années, les pirates ont utilisé le COVID-19 dans leurs escroqueries. Au début de l'année 2021, nous avons constaté une augmentation des escroqueries liées aux vaccins avec de fausses propositions d'accès anticipé au vaccin, alors que vers la fin de l'année 2021, les cybercriminels ont changé de tactique et se sont tournés vers la vente de tests de COVID-19 à leurs victimes.

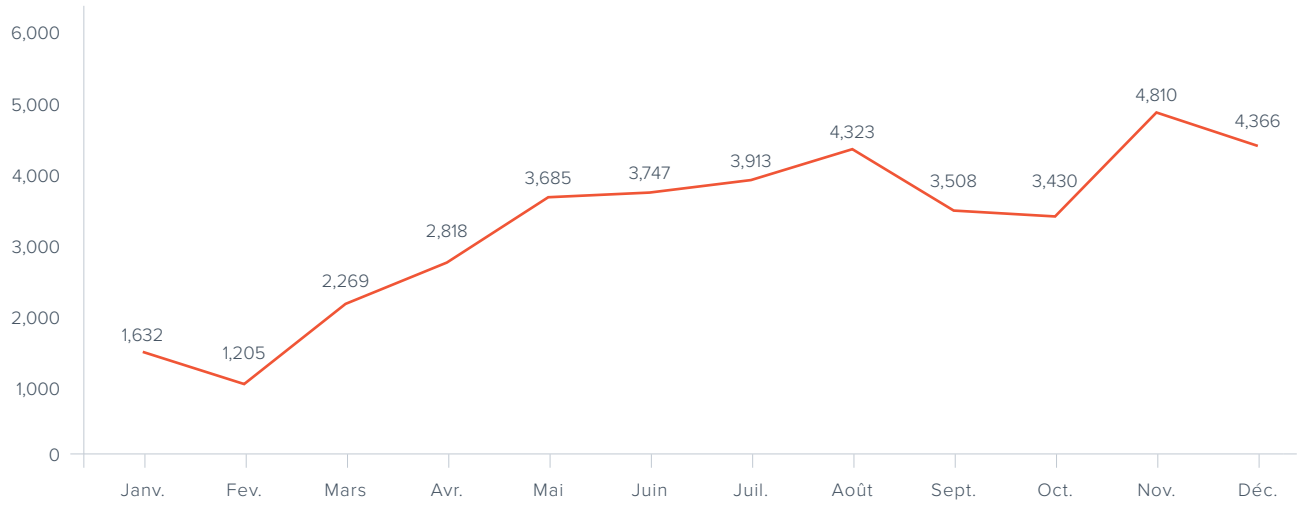
Le **détournement de conversations**, également appelé fraude au fournisseur, est un type d'attaque par e-mail ciblée dans laquelle les cybercriminels s'immiscent dans des conversations d'entreprise existantes ou en entament de nouvelles, en se basant sur les informations qu'ils ont recueillies à partir de comptes de messagerie 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 passent ensuite du temps à lire les e-mails et à surveiller 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, partenaires et clients, pour élaborer des messages paraissant authentiques et 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.

Le détournement de conversations ne représente que 0,3 % des attaques par ingénierie sociale que nous avons observées l'année dernière. Cependant, même si elles sont peu nombreuses, elles peuvent être dévastatrices pour les entreprises. Le volume global de détournements de conversations a augmenté au fil des ans et la popularité de ce type d'attaque chez les pirates a doublé en 2021. Cela n'est pas surprenant, car même si la mise en place de ces attaques demande beaucoup de travail de la part des pirates, elles peuvent être très lucratives.

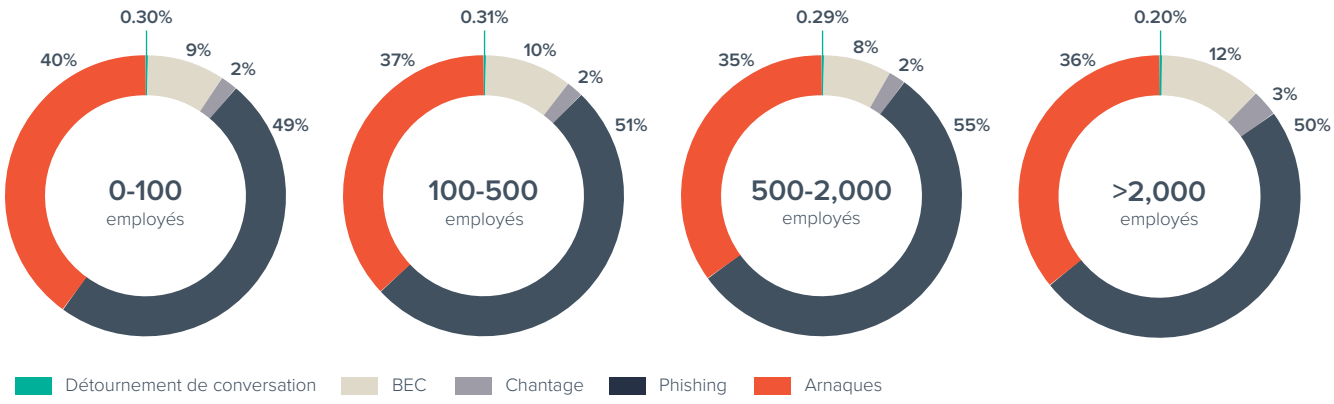
Attaques par détournement de conversation en 2021



Les cibles des attaques par ingénierie sociale

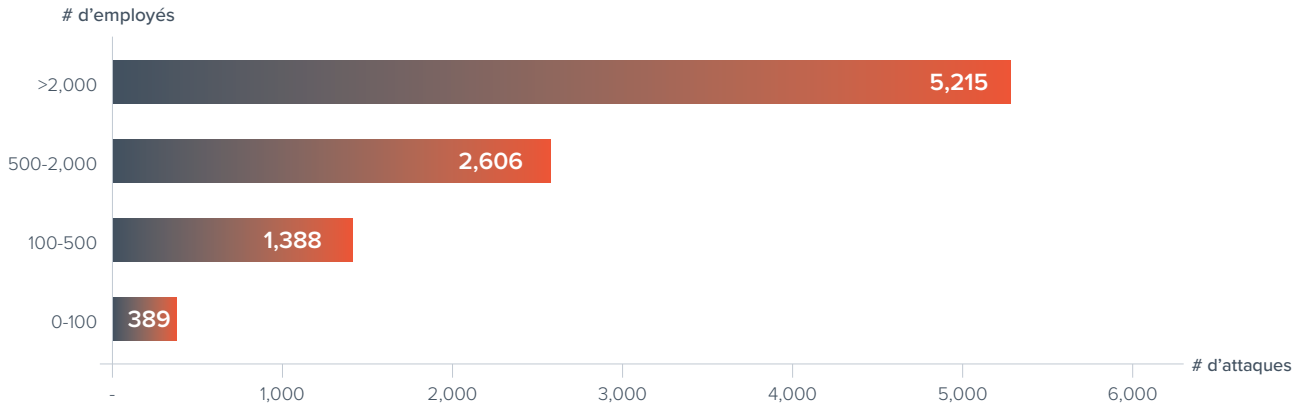
Les attaques par e-mail ciblent indifféremment des entreprises de toutes tailles. Les grandes entreprises de plus de 2000 employés ne reçoivent que légèrement plus d'attaques ciblées par compromission d'e-mails professionnels qu'une petite entreprise de moins de 100 employés. Il est important que les entreprises restent vigilantes face à tous les types d'attaques, quelle que soit leur taille.

Types d'attaques par taille d'entreprise



Il n'est pas non plus surprenant que les grandes entreprises soient confrontées à un plus grand nombre d'attaques du seul fait de leur taille. Par exemple, une entreprise de plus de 2000 employés recevra plus de 5000 attaques d'ingénierie sociale par e-mail chaque année. Ce chiffre est beaucoup plus petit dans les entreprises ayant moins d'employés.

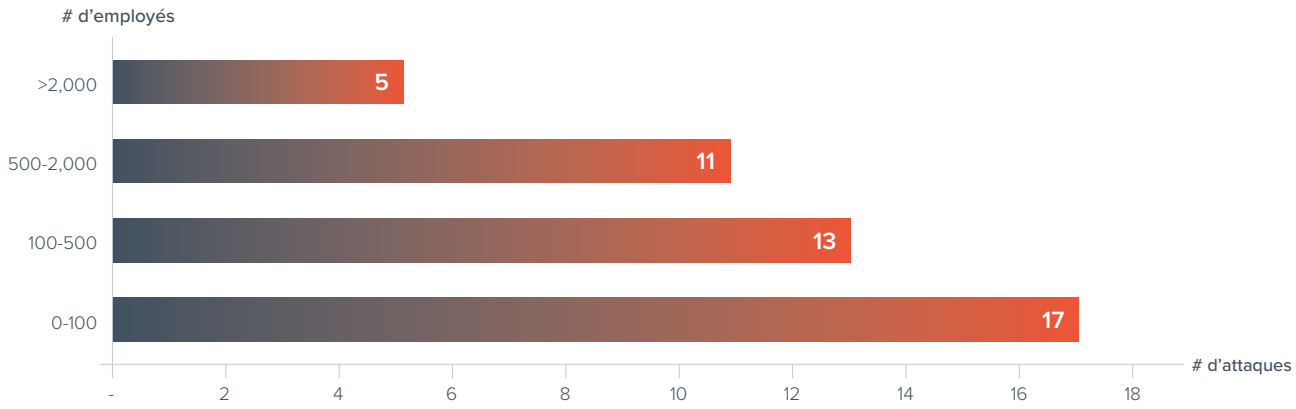
Nombre moyen d'attaques par ingénierie sociale par entreprise



Toutefois, le tableau est inversé lorsqu'on regarde le volume d'attaques par boîte de réception. Plus l'entreprise est petite, plus ses employés sont susceptibles d'être la cible d'une attaque. En fait, un employé d'une petite entreprise de moins de 100 employés recevra 350 % plus d'attaques par ingénierie sociale qu'un employé d'une grande entreprise. Les PME sont des cibles intéressantes pour les cybercriminels, car elles ont collectivement une valeur économique importante et manquent souvent de ressources ou d'expertise en matière de sécurité.

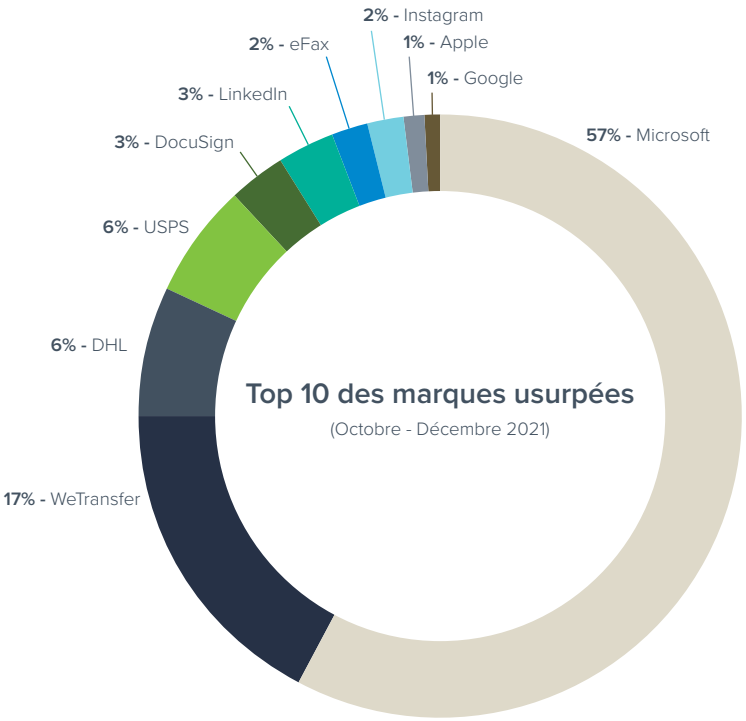
Les petites entreprises ne doivent pas négliger l'investissement dans la sécurité, tant sur le plan technologique que sur celui de la formation des utilisateurs. Les conséquences d'une attaque peuvent être beaucoup plus dévastatrices pour les petites entreprises. Selon une étude menée par Cybersecurity Ventures, 60 % des petites entreprises ferment leurs portes six mois après une violation de leur sécurité. Sachant que 43 % des attaques en ligne visent des petites entreprises, l'inaction peut coûter très cher.

Nombre moyen d'attaques par ingénierie sociale par boîte mail



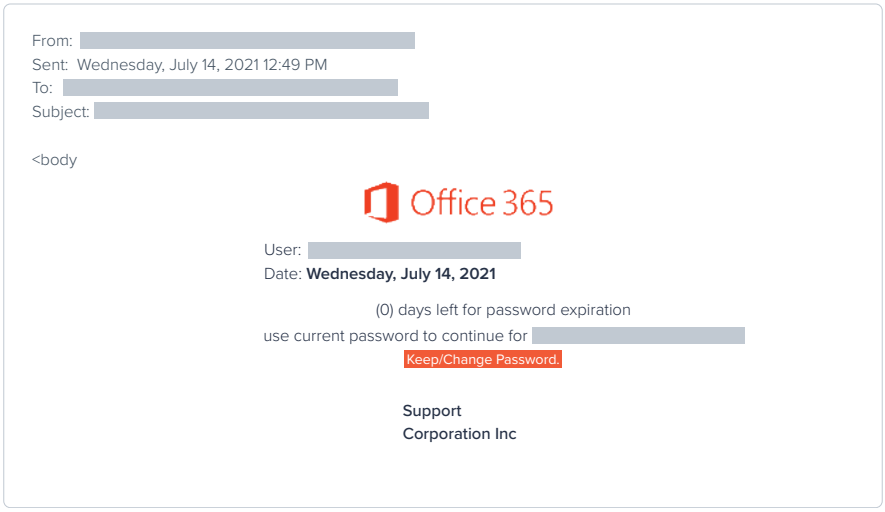
Les marques les plus usurpées

Usurper l'identité d'une marque dont la réputation n'est plus à faire est une technique courante utilisée par de nombreux pirates. Nous sommes habitués à recevoir des communications provenant de nos marques préférées et nous leur faisons confiance. Parmi les 10 marques les plus usurpées dans le cadre d'attaques par phishing ayant recours à l'usurpation d'identité, les trois premières marques (Microsoft, WeTransfer, DHL) sont les mêmes depuis 2019.



Sachant que 79 % des entreprises sont passées à Microsoft 365 et que de nombreuses entreprises comptent le faire prochainement, Microsoft demeure sans surprise une cible privilégiée des cybercriminels

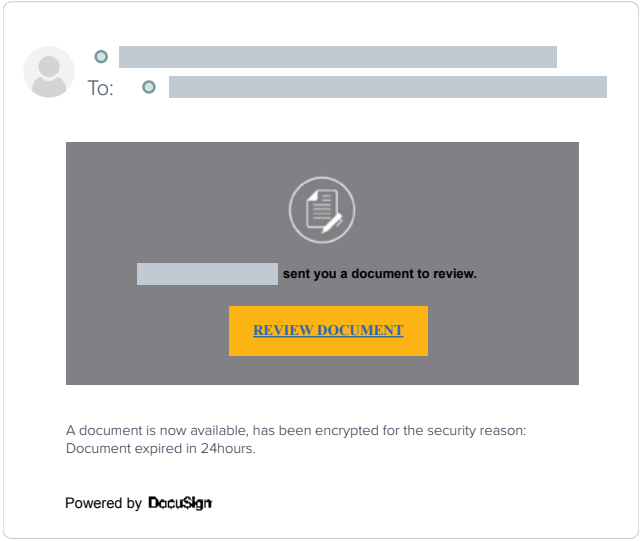
En examinant les 10 marques les plus usurpées, on constate que Microsoft a été utilisée dans 57 % des attaques par phishing, soit une augmentation significative par rapport aux 43 % de juillet 2021. Les pirates informatiques profitent du succès croissant des services cloud de Microsoft et de la généralisation du télétravail observée ces deux dernières années. Les cybercriminels envoient de fausses alertes de sécurité ou des demandes de mise à jour des comptes pour amener les victimes à cliquer sur un lien de phishing. L'objectif de ces attaques est simple : voler des identifiants de connexion afin d'accéder aux réseaux d'entreprise. À partir de là, les pirates peuvent lancer d'autres attaques par phishing, comme des tentatives d'infection par ransomware.



WeTransfer propose des services de transfert de fichiers en ligne permettant aux utilisateurs de partager des fichiers volumineux ne pouvant être envoyés directement par e-mail. Cette marque a été utilisée dans 17 % des attaques par phishing. Consciente que sa marque est utilisée dans ce type d'attaques, l'entreprise demande à ses utilisateurs d'être vigilants. Les scams utilisant la marque WeTransfer doivent être abordés dans les formations de sensibilisation organisées par les entreprises.

Les usurpations utilisant la marque DocuSign ne représentaient que 3 % des attaques par phishing, mais ces attaques peuvent s'avérer dévastatrices pour les entreprises. Les entreprises réalisant désormais de nombreuses activités en ligne et dans le cloud, il n'est pas rare de recevoir un e-mail de DocuSign invitant à signer un document et de nombreux employés n'hésiteront pas à cliquer. Les cybercriminels créent de faux comptes DocuSign ou détournent des comptes déjà existants, puis créent et envoient des fichiers à leurs victimes.

Les marques Google, DHL, USPS et LinkedIn ont elles aussi rejoint le top 10. La compromission des comptes ouverts sur ces plateformes permet aux cybercriminels de s'emparer d'une multitude de données personnelles, qu'ils pourront ensuite exploiter dans d'autres attaques.



Recrudescence des piratages de compte

Ces dernières années, l'adoption d'Microsoft 365 s'est accélérée, la pandémie ayant entrainé une généralisation du télétravail et une migration vers le cloud. Aujourd'hui, Microsoft compte plus de 200 millions d'utilisateurs actifs par mois. Cette popularité n'est pas surprenante, car Microsoft 365 améliore la productivité et la communication au sein des entreprises. Les employés peuvent désormais se connecter à leurs comptes de messagerie et accéder à leurs données où qu'ils se trouvent. Mais les pirates informatiques eux aussi profitent de la situation. L'accès aux comptes Microsoft 365 est particulièrement intéressant, car ces comptes leur servent de porte d'entrée pour accéder aux entreprises et à leurs données.

Le **piratage de compte** est un type d'usurpation d'identité et de fraude qui consiste, pour un tiers malveillant, à obtenir l'accès aux identifiants de connexion d'un compte utilisateur. En se faisant passer pour l'utilisateur légitime du compte, les cybercriminels parviennent à changer les informations du compte, à envoyer des e-mails de phishing, à voler des informations financières ou des données sensibles ou encore à utiliser des données volées pour accéder à encore plus de comptes au sein de l'entreprise.

Le piratage de compte est l'une des menaces que se développent le plus rapidement. En 2021, environ 1 entreprise sur 5 (20 %) a vu au moins un de ses comptes Microsoft 365 compromis. Cela signifie qu'en 2021, les pirates ont réussi à pirater environ 500 000 comptes Microsoft 365 dans le monde. Sans une protection appropriée, le piratage de compte peut passer inaperçu et causer de réels dommages à l'entreprise, à ses partenaires commerciaux et à ses clients.

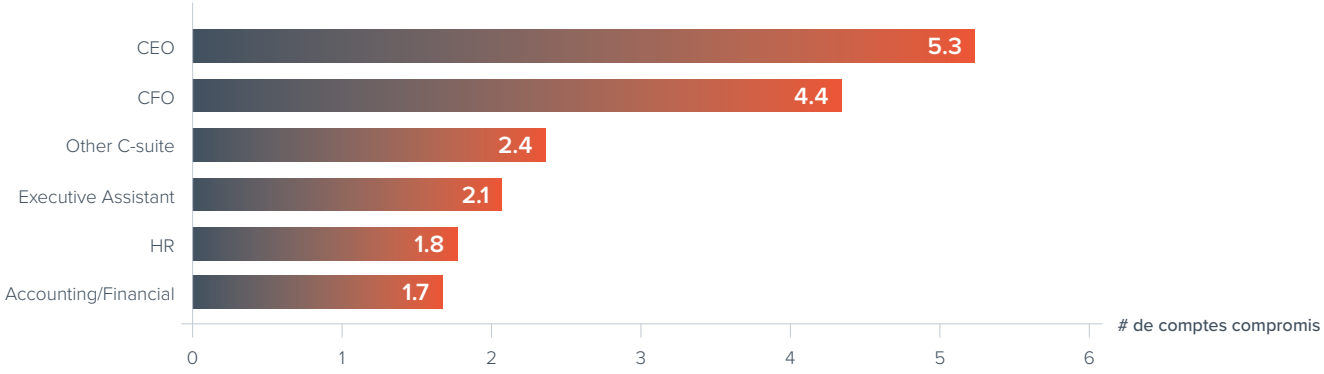
1 entreprise sur 5 a eu des comptes Microsoft 365 compromis.

Les cadres dirigeants sont les plus visés par les piratages de compte

Les pirates cherchent à pirater des comptes de grande valeur. Les comptes des PDG et des directeurs financiers sont presque deux fois plus susceptibles d'être piratés que ceux des employés moyens. Une fois qu'ils ont accès à ces comptes de grande valeur, les cybercriminels les utilisent pour recueillir des informations ou lancer des attaques au sein de l'entreprise.

Les assistants de direction sont également une cible fréquente, car ils ont souvent accès aux comptes et aux calendriers de la direction et peuvent généralement envoyer des messages au nom des équipes de direction.

Piratage de comptes selon les fonctions dans l'entreprise (par 1000 boîtes aux lettres)



Quatre étapes dans le piratage de compte

Infiltration

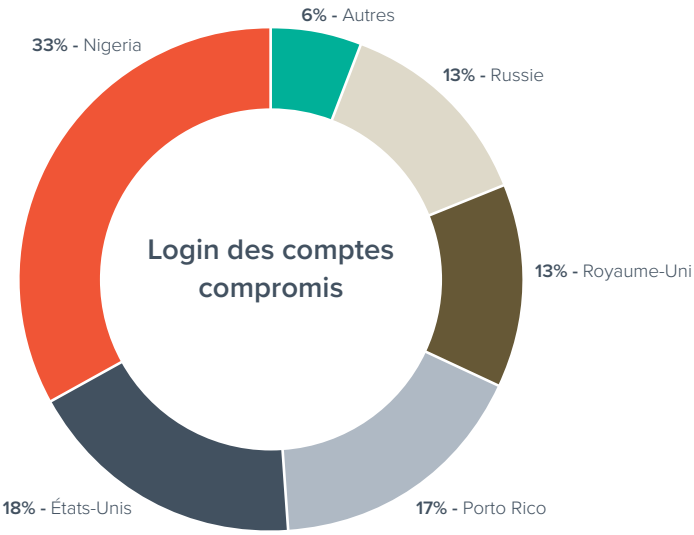
Microsoft est l'une des marques les plus usurpées. Environ 57 % des attaques par phishing usurpent l'une des marques de Microsoft, comme Microsoft 365, OneDrive, SharePoint, etc. Les pirates utilisent des tactiques d'ingénierie sociale pour inciter les utilisateurs à se rendre sur un site web de phishing et à entrer leurs identifiants de connexion, ce qui permet aux pirates d'infiltrer le système.

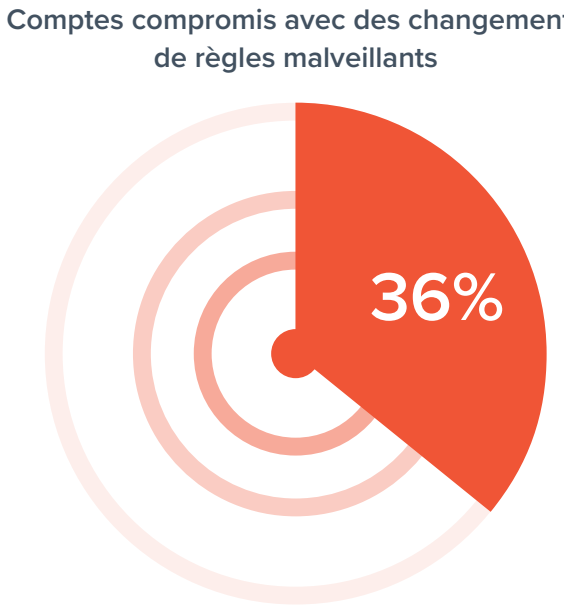
Reconnaissance

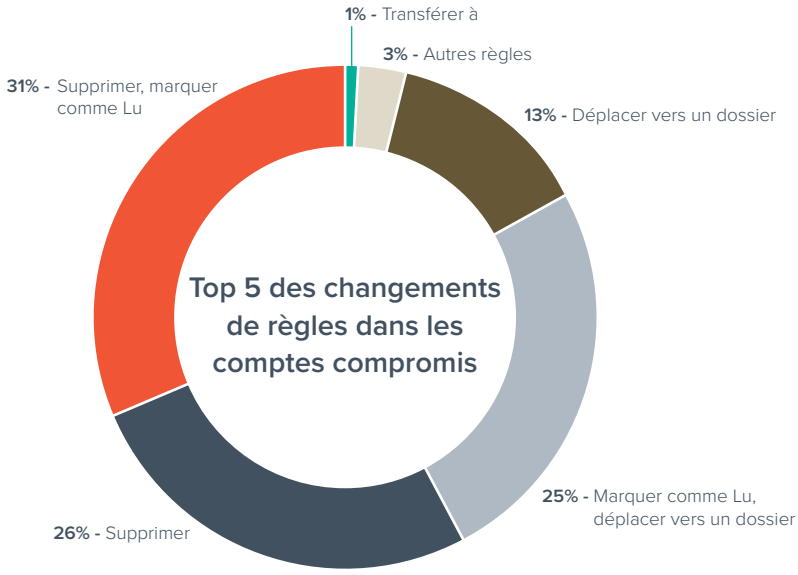
Une fois qu'ils ont accès au réseau d'une entreprise, les pirates lancent rarement leurs attaques sur-le-champ. Ils utilisent le compte piraté pour observer les activités de votre entreprise. Puis ils utilisent ces informations à leur avantage. La plupart des pirates qui ont participé aux attaques que nous avons analysées se connectent à partir d'un petit nombre de pays, le Nigeria étant en tête de la liste. Une connexion frauduleuse sur trois aux comptes piratés provient du Nigeria.

Une fois le compte piraté, le pirate crée des règles de transfert ou des scripts pour masquer et supprimer tout courrier électronique envoyé depuis la boîte de réception piratée. L'existence de règles suspectes dans une boîte de réception est souvent un signe indiquant que le compte a été piraté. Dans 36 % des entreprises ayant subi un piratage de compte, les pirates ont créé des règles malveillantes dans la boîte de réception pour dissimuler leur activité. En fait, les pirates ont créé en moyenne deux règles pour chaque compte piraté.

Dans plus de la moitié des cas impliquant la création de règles malveillantes, les pirates ont créé des règles pour supprimer les messages des comptes afin que les propriétaires de ces comptes ne remarquent aucune activité suspecte dans leurs e-mails. Une autre pratique courante consiste à déplacer les messages vers un dossier spécifique et à les marquer comme lus. Les pirates reviendront plus tard pour lire les messages placés dans ce dossier.







Collecte et monétisation des identifiants

Les pirates utilisent les comptes piratés comme rampe de lancement de leurs attaques. Ils ciblent les comptes de grande valeur et essaient de voler leurs identifiants, puis se déplacent latéralement au sein de l'entreprise. Les comptes piratés sont utilisés dans un large éventail d'attaques, du spam à la compromission d'e-mails professionnels. D'après notre étude portant sur près de 12 000 comptes piratés, ces comptes ont été utilisés pour envoyer plus de 3 millions de messages malveillants et de spams en 2021.

Bonnes pratiques pour se protéger contre le spear phishing

Aujourd'hui, les entreprises sont de plus en plus exposées aux attaques de phishing ciblées. Pour protéger votre entreprise et vos utilisateurs, vous devez investir dans une technologie permettant de contrer les attaques et former votre personnel en conséquence pour qu'il constitue la dernière ligne de défense.

Technologie

- **Tirez profit de l'intelligence artificielle.** Les cybercriminels adaptent leurs e-mails pour contourner les passerelles et les filtres anti-spam. Il est donc crucial de disposer d'une solution de détection et de protection contre les attaques par spear phishing, notamment la compromission d'e-mails professionnels, l'usurpation d'identité et les attaques par chantage. Déployez une technologie spécialisée qui ne se contente pas de détecter les pièces jointes ou les liens malveillants. Utilisez l'apprentissage automatique pour analyser les modèles de communication classiques au sein de votre entreprise et repérer toute anomalie susceptible d'indiquer une attaque.

- **Déployez une solution de protection contre le piratage de compte.** De nombreuses attaques de spear phishing latéral proviennent de comptes compromis ; assurez-vous qu'aucun pirate informatique n'utilise votre entreprise comme camp de base pour perpétrer ses attaques. Déployez une technologie qui utilise l'intelligence artificielle pour identifier les comptes compromis et corriger les problèmes en temps réel, en alertant les utilisateurs et en supprimant les e-mails malveillants envoyés par ces comptes.

- **Surveillez les règles des boîtes de réception et les connexions suspectes.** Utilisez la technologie pour identifier les activités suspectes, y compris les connexions provenant d'emplacements et d'adresses IP inhabituels, signe potentiel d'un compte piraté. Veillez également à surveiller les comptes de messagerie pour vous assurer de l'absence de règles de boîte de réception malveillantes, souvent utilisées pour pirater des comptes. Les pirates se connectent au compte, créent des règles de transfert et masquent ou suppriment les e-mails envoyés depuis ce compte afin d'effacer leurs traces.

- **Utilisez l'authentification multifacteur.** L'authentification multifacteur, également appelée MFA, authentification à deux facteurs et vérification à deux étapes, fournit une couche de sécurité supplémentaire en plus du nom d'utilisateur et du mot de passe, par exemple un code d'authentification, une empreinte de pouce ou un scan rétinien.

- **Mettez en œuvre l'authentification et le reporting DMARC.** L'usurpation de domaine est l'une des techniques d'usurpation d'identité les plus courantes. L'authentification DMARC permet de lutter contre l'usurpation des marques et des domaines, pendant que l'analyse et le reporting DMARC garantissent une mise en œuvre correcte.

- **Automatisez la réponse aux incidents.** Une solution de réponse automatisée aux incidents vous aidera à éliminer rapidement les menaces trouvées dans les boîtes de réception des utilisateurs, ce qui permettra de neutraliser plus efficacement les menaces contenues dans l'ensemble des messages par la suite.

Collaborateurs

- **Formez votre personnel à détecter et à signaler les attaques.** Sensibilisez vos utilisateurs aux attaques par spear phishing dans le cadre d'une formation à la sécurité. Apprenez-leur à identifier leur caractère frauduleux et à les signaler. Simulez des attaques par phishing vocal, par e-mail et par SMS pour former vos utilisateurs à les reconnaître, testez l'efficacité de votre formation et identifiez les utilisateurs les plus vulnérables aux cybermenaces.

- **Révisez les politiques internes.** Aidez vos employés à ne pas commettre d'erreurs coûteuses en élaborant des procédures pour confirmer toute demande reçue par e-mail, y compris les demandes de virements bancaires ou l'achat de cartes cadeaux.

- **Mettez en place une prévention optimale contre la perte de données.** Utilisez la combinaison de technologies et de stratégies professionnelles adaptée pour garantir la confidentialité des e-mails contenant des informations confidentielles, personnelles ou sensibles devant être protégées et ne jamais sortir de l'entreprise.

À propos de Barracuda

Notre objectif : faire du monde un endroit plus sûr.

Chez Barracuda, nous pensons que chaque entreprise mérite un accès à des solutions de sécurité cloud de niveau professionnel, à la fois abordables, intuitives et facilement déployables. Nous protégeons vos e-mails, réseaux, données et 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 aux quatre coins du monde font confiance à Barracuda pour les protéger, même lorsque le danger ne leur semble pas imminent : nous nous voulons invisibles afin de permettre aux entreprises de se concentrer sur leurs activités et leur développement.

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

Barracuda®
Your journey, secured.