Mai 2020

13 types d'attaques par e-mail à connaître immédiatement

Comment la protection des boîtes de réception permet de contrer des attaques toujours plus sophistiquées

Barracuda
Your journey, secured.

Table des matières

Barracuda

Introduction : Réduire radicalement le risque d'attaques par e-mail ciblées

Une cyberattaque peut avoir des conséquences très diverses sur votre entreprise, selon sa nature, sa portée et sa gravité. Selon l'Internet Crime Complaint Center (IC3) du FBI, le cybercrime a coûté 3,5 milliards de dollars rien qu'en 2019, les attaques Business Email Compromise (BEC) ayant été les plus dévastatrices. Et ce chiffre ne prend pas en compte les pertes non signalées, qui sont considérables. L'IC3 a reçu 467 361 plaintes l'an dernier (plus de 1 300 par jour), le phishing constituant 93 % des attaques par e-mail. Divers impacts indirects et intangibles peuvent également découler de ces attaques, comme des frais juridiques, des amendes, la perturbation des opérations, la détérioration de la réputation des marques et d'autres conséquences graves.

Dans l'environnement en évolution rapide d'aujourd'hui, les solutions de sécurité de la messagerie traditionnelles ne suffisent plus pour protéger les entreprises. Il convient également de contrer efficacement les menaces sophistiquées, qui sont souvent capables de contourner les défenses en utilisant des techniques de porte dérobée, notamment l'usurpation, l'ingénierie sociale et la fraude, pour pénétrer les réseaux et faire des ravages.

Bien que les défenses complètes de passerelle de messagerie fournissent une base solide, l'adoption d'une stratégie de protection multicouche réduit radicalement la vulnérabilité aux attaques par e-mail et aide à mieux défendre les entreprises, les données et les personnes.

Ce livre numérique offre un aperçu détaillé des principales attaques par e-mail et de leur impact sur les entreprises. Il explique également comment l'apprentissage machine et la protection des boîtes de réception par API peuvent combler les lacunes des passerelles de messagerie et contribuer à fournir une protection complète.

« Jusqu'en 2023, les attaques de type BEC vont continuer à doubler chaque année pour atteindre plus de 5 milliards de dollars, ce qui représentera des pertes financières énormes pour les entreprises. »

Source : Gartner (mars 2020)

Barracuda

Combattre des attaques par e-mail toujours plus complexes

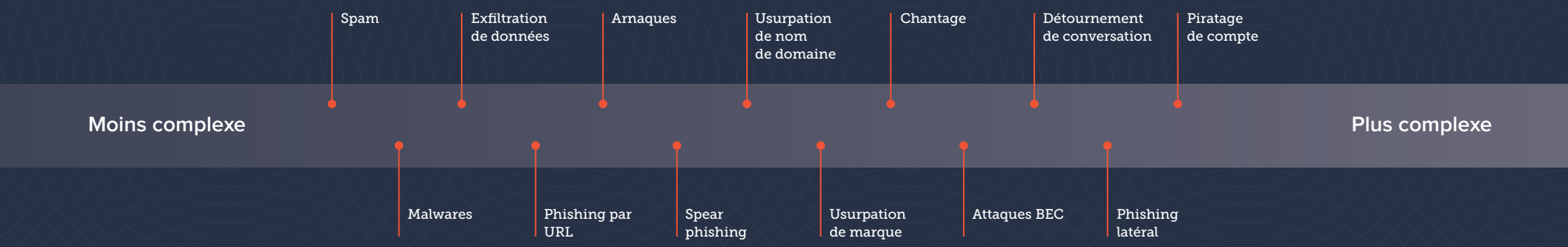
Les attaques par e-mail et de phishing auxquelles font face les organisations aujourd'hui varient grandement en complexité, en volume et en impact sur les entreprises et leurs employés. On compte ainsi plusieurs catégories de menaces par e-mail :

- **Le spam :** un grand nombre de messages non sollicités, généralement de nature commerciale, sont envoyés sans tenir compte de l'identité des destinataires.
- **Les malwares :** il s'agit de logiciels spécifiquement conçus pour causer des dommages aux infrastructures techniques, perturber les opérations, exfiltrer des données ou obtenir un accès à un système distant. Les malwares sont généralement distribués via des pièces jointes ou des URL contenues dans les e-mails, qui renvoient vers du contenu malveillant.
- **L'exfiltration de données :** ce type d'attaque correspond à la copie ou à l'extraction de données depuis un système distant sans le consentement du propriétaire. Il peut s'agir d'un acte malveillant ou accidentel.
- **Le phishing :** ce type d'e-mail vise à piéger un utilisateur final en lui faisant croire que le message vient d'une personne ou d'une organisation de confiance, afin de le pousser à réaliser certaines actions : divulguer des informations d'identification, virer de l'argent ou encore se connecter à un compte légitime pour le cyberattaquant.
- **L'usurpation :** cette catégorie comprend toutes les attaques lors desquelles l'acteur malveillant se fait passer pour une personne, une organisation ou un service. Il s'agit d'un large ensemble d'attaques qui vont en général de pair avec le phishing.

Barracuda

Au total, 13 types de menaces par e-mail entrent dans ces catégories, et certaines de ces attaques sont utilisées conjointement ; les hackers associent souvent différentes techniques. Par exemple, de nombreux spams incluent des URL de phishing, et il n'est pas rare qu'un compte piraté soit utilisé pour une fraude électronique interne ou latérale. Comprendre la nature et les caractéristiques de ces attaques vous aidera à façonner la meilleure protection possible pour votre entreprise, vos données et vos employés.

Voici un aperçu des 13 principaux types de menaces par e-mail et comment s'en protéger. Plus les attaques par e-mail sont complexes, plus elles sont difficiles à neutraliser.

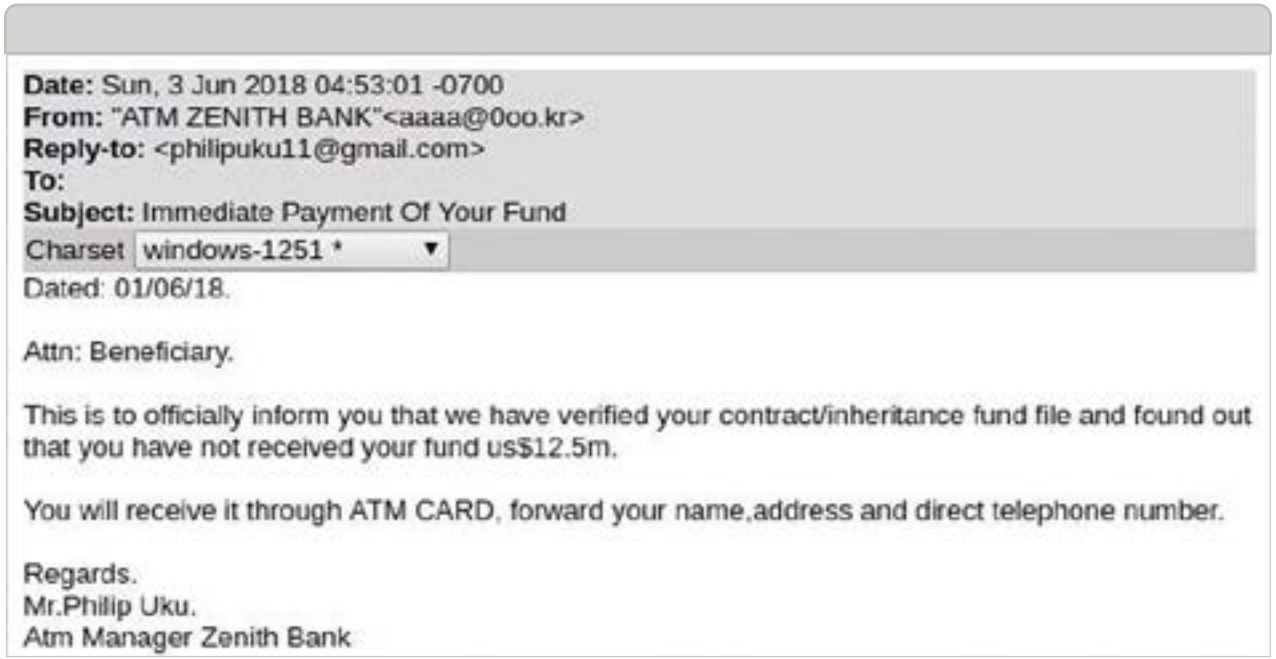


Le spam

Barracuda

Le spam est l'envoi d'e-mails non sollicités en masse. On parle également de « pourriel » ou de « courrier indésirable ». Les spammeurs envoient en général ce type d'e-mail à des millions d'adresses, en espérant une réponse d'un petit nombre d'entre elles. Les adresses e-mail sont récupérées depuis diverses sources, parfois à l'aide de logiciels spécialement conçus pour les extraire à partir d'annuaires. Elles sont en outre souvent vendues à d'autres spammeurs.

Le spam existe sous différentes formes : certains de ces messages véhiculent des arnaques, d'autres sont utilisés pour réaliser des fraudes. Le spam peut également se présenter sous forme d'e-mails de phishing usurpant une marque pour pousser les utilisateurs à révéler leurs informations personnelles, comme des informations de connexion ou un numéro de carte bancaire.



Date: Sun, 3 Jun 2018 04:53:01 -0700
From: "ATM ZENITH BANK"<aaaa@0oo.kr>
Reply-to: <philipuku11@gmail.com>
To:
Subject: Immediate Payment Of Your Fund
Charset windows-1251 *
Dated: 01/06/18.

Attn: Beneficiary.

This is to officially inform you that we have verified your contract/inheritance fund file and found out that you have not received your fund us$12.5m.

You will receive it through ATM CARD, forward your name,address and direct telephone number.

Regards.
Mr.Philip Uku.
Atm Manager Zenith Bank

Exemple d'attaque

Barracuda

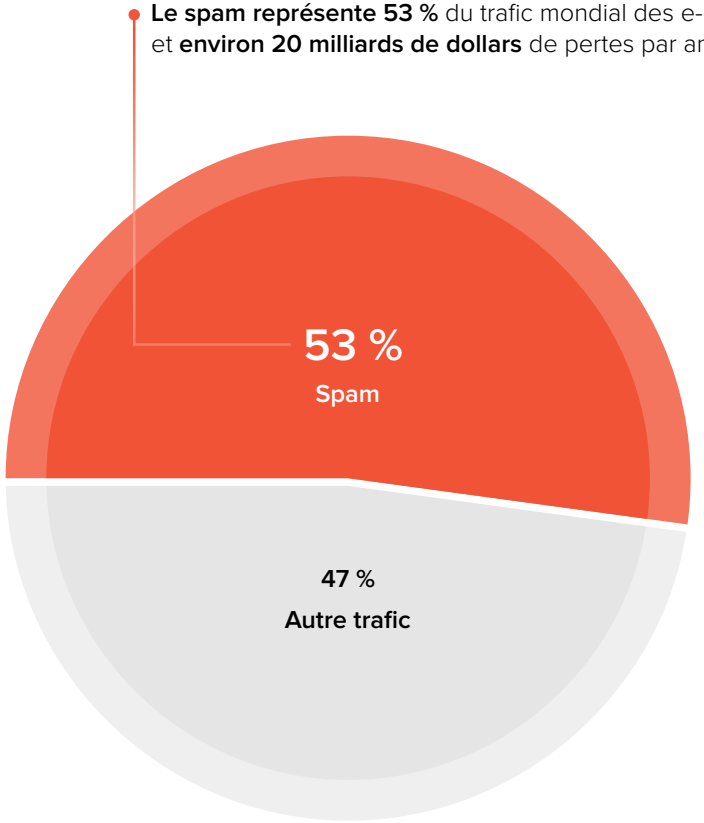
L'impact du spam

Le spam coûte aux entreprises environ 20 milliards de dollars par an. Il diminue la productivité en inondant les boîtes de réception de courriers indésirables et accapare le trafic du serveur qui traite les messages. Le spam peut être utilisé pour diffuser des malwares et dans le cadre d'attaques de phishing à grande échelle.

Se protéger contre le spam

Les passerelles modernes permettent de contrer efficacement le spam ; le déploiement en ligne de filtres anti-spam contribue à bloquer ces messages avant leur arrivée dans les boîtes de réception.

La protection des boîtes de réception par API n'est pas aussi efficace contre ces attaques à grande échelle. Les attaques volumineuses, comme le spam, peuvent submerger les serveurs de messagerie et nuire à la performance des boîtes de réception, en faisant peser une lourde charge sur celles-ci avant d'être récupérées par les API.



Les malwares

Barracuda

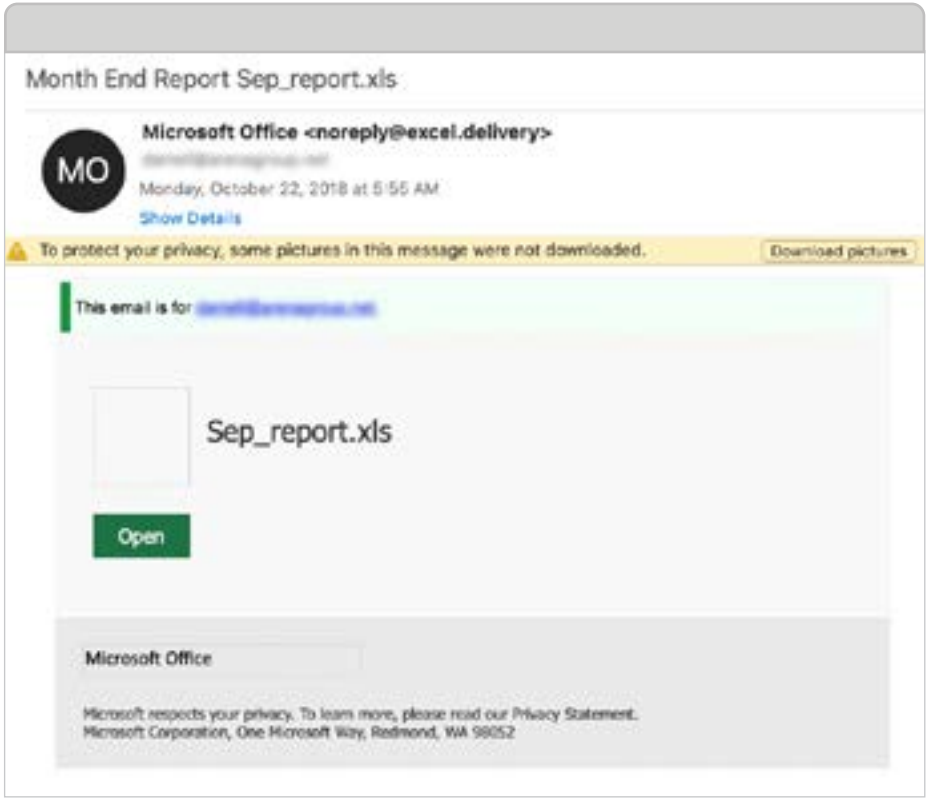
Les cybercriminels utilisent les e-mails pour envoyer des documents contenant des logiciels malveillants, ou malwares. En général, soit le logiciel malveillant est dissimulé directement dans le document lui-même, soit un script intégré le télécharge depuis un site Web externe. Les malwares les plus courants sont les virus, les chevaux de Troie, les logiciels espions, les vers et les ransomwares.

Les types de malwares les plus courants

Malwares volumétriques : les malwares de ce type sont conçus pour être diffusés en masse et cibler les systèmes plus anciens et non corrigés présentant des vulnérabilités courantes. Ils exploitent les failles connues et peuvent généralement être neutralisés grâce aux signatures et à une simple analyse heuristique. *Les malwares volumétriques sont également appelés « malwares de base » ou « virus ».*

Malwares de type « zero-day » : les attaques par malware avancées constituent des menaces de type « zero-day » : des attaques encore jamais rencontrées et qui ne correspondent à aucune signature de malware connue. Elles peuvent exploiter une vulnérabilité logicielle jusqu'alors inconnue ou utiliser une nouvelle variante de malware envoyée par des moyens classiques. Ces attaques de type « zero-day » sont impossibles à détecter via les solutions classiques basées sur les signatures. *Les malwares de ce type sont également appelés « 0Day ».*

Attaques par URL : les URL qui renvoient vers des sites Web ou des charges utiles malveillants sont généralement conçues pour piéger les utilisateurs en les incitant à cliquer pour télécharger un malware.



Exemple d'attaque

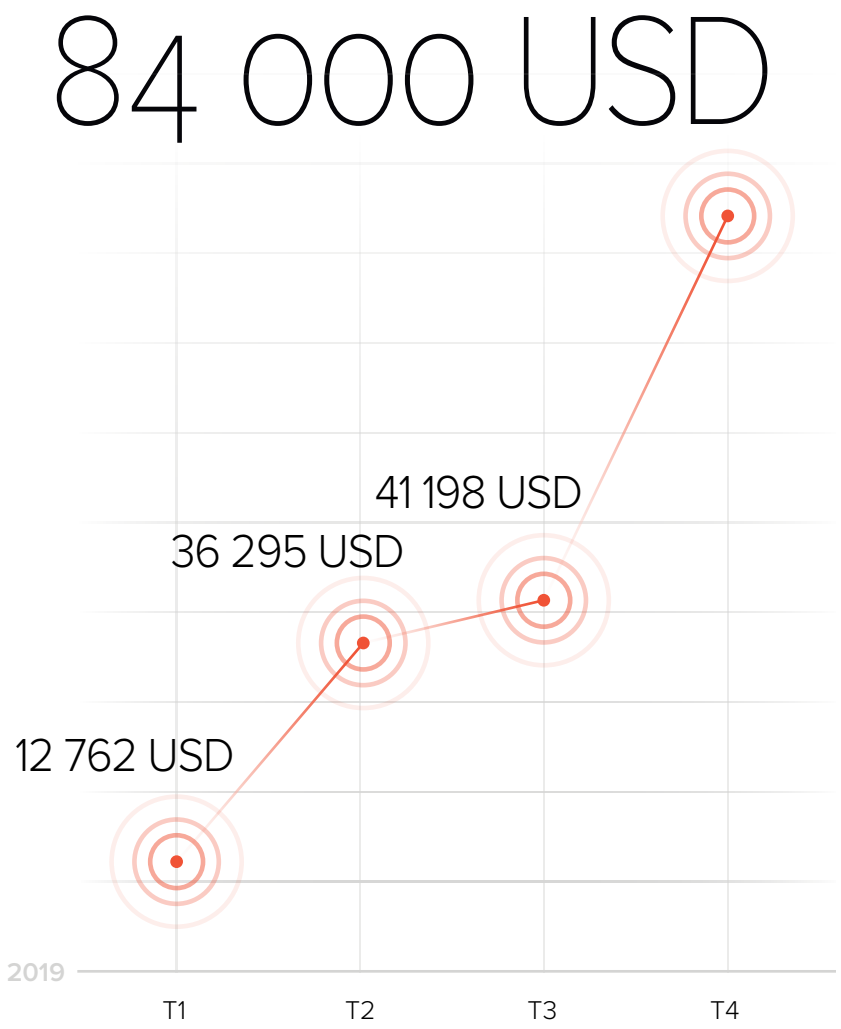
Barracuda

L'impact des malwares

94 % des malwares sont envoyés par e-mail. Avec les ransomwares, l'une des formes de malware les plus répandues, les cybercriminels infectent le réseau et bloquent les e-mails, les données et d'autres fichiers critiques jusqu'au paiement d'une rançon. Ces attaques sophistiquées et en constante évolution sont dévastatrices et coûteuses. Elles peuvent paralyser les opérations quotidiennes, semer le chaos et occasionner des pertes financières résultant des temps d'arrêt, du paiement de la rançon, des coûts de récupération et d'autres dépenses non prévues au budget ou anticipées.

En 2019, les ransomwares ont ainsi coûté quelque 170 milliards de dollars. Ce chiffre inclut non seulement les rançons payées, mais également la perte de productivité et de données, ainsi que d'autres dommages causés par ces attaques. Le montant moyen des rançons a par ailleurs plus que doublé, passant de 41 198 dollars au T3 2019 à 84 000 dollars au T4 2019.

En 2019, de nombreuses attaques par ransomware, très médiatisées, ont visé des entreprises et des organismes gouvernementaux. En ce qui concerne les attaques de ransomware contre l'administration publique, tous les niveaux de collectivité ont été ciblés, avec notamment des écoles, des établissements de santé, des bibliothèques, des tribunaux et d'autres entités.

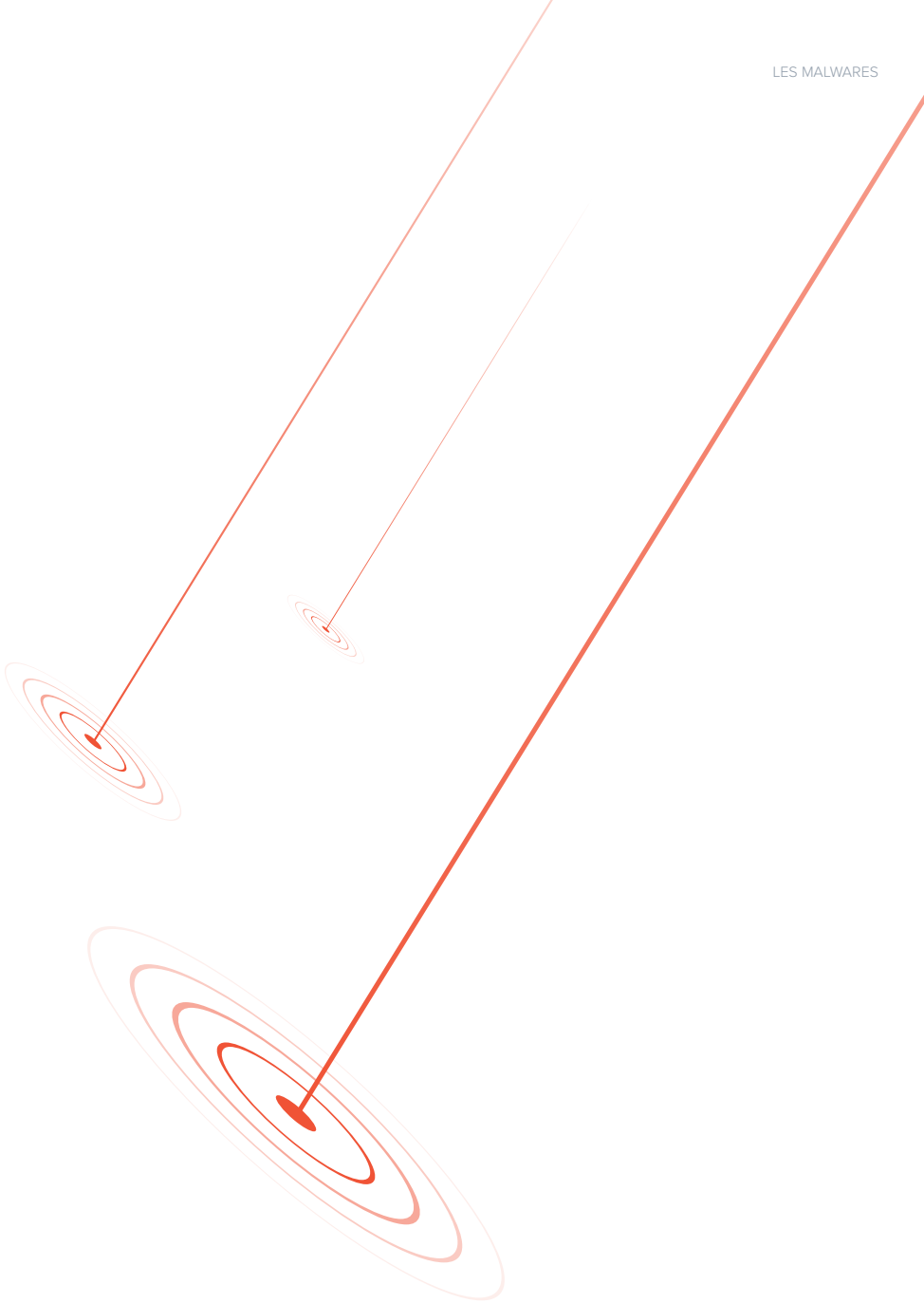


Une véritable explosion du montant moyen des rançons

Barracuda

Se protéger contre les malwares

Pour une efficacité optimale, la protection contre les malwares doit être installée au niveau de la passerelle, avant que les e-mails n'atteignent les boîtes de réception. La correspondance des signatures demeure un outil important pour détecter et bloquer la plupart des variantes des malwares. Toutefois, il existe d'autres techniques plus avancées permettant de déceler les menaces de type « zero-day ». Citons notamment le sandboxing : les fichiers et liens suspects sont analysés dans un environnement de test isolé afin de s'assurer qu'ils sont sans danger, avant d'être envoyés vers les boîtes de réception des utilisateurs. De nouvelles signatures de malwares peuvent être créées sur la base d'une analyse par sandbox, afin de se prémunir contre les attaques futures.



Barracuda

L'exfiltration de données

Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte

Moins complexe

Plus complexe

Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

Barracuda

L'exfiltration de données est le transfert non autorisé de données depuis un ordinateur ou un autre appareil. Cette opération peut être réalisée manuellement via un accès physique à un ordinateur ou par un processus automatisé, à l'aide d'une programmation malveillante sur Internet ou un réseau. Les attaques sont généralement ciblées, dans l'objectif d'obtenir un accès à un réseau ou une machine en vue de localiser et de copier des données spécifiques. Mais outre ces attaques malveillantes, il est fréquent que des données soient perdues accidentellement en raison d'erreurs humaines.

L'exfiltration de données compte de nombreuses appellations, telles que « extrusion de données », « exportation de données », « fuite de données », « perte de données » ou encore « vol de données ».

L'impact de l'exfiltration de données

Selon un rapport IBM annuel, le coût total moyen des violations de données était de 3,92 millions de dollars en 2019. Et ce chiffre double quasiment pour certains secteurs, comme la santé. C'est en outre aux États-Unis que ces attaques ont été les plus coûteuses, avec une moyenne de 8,19 millions de dollars. En moyenne, les violations de données ont touché 25 575 documents.

La perte de données peut occasionner des pertes financières et avoir des conséquences à long terme sur la réputation d'une organisation.

Coût moyen d'une violation de données en 2019

3,92 M USD

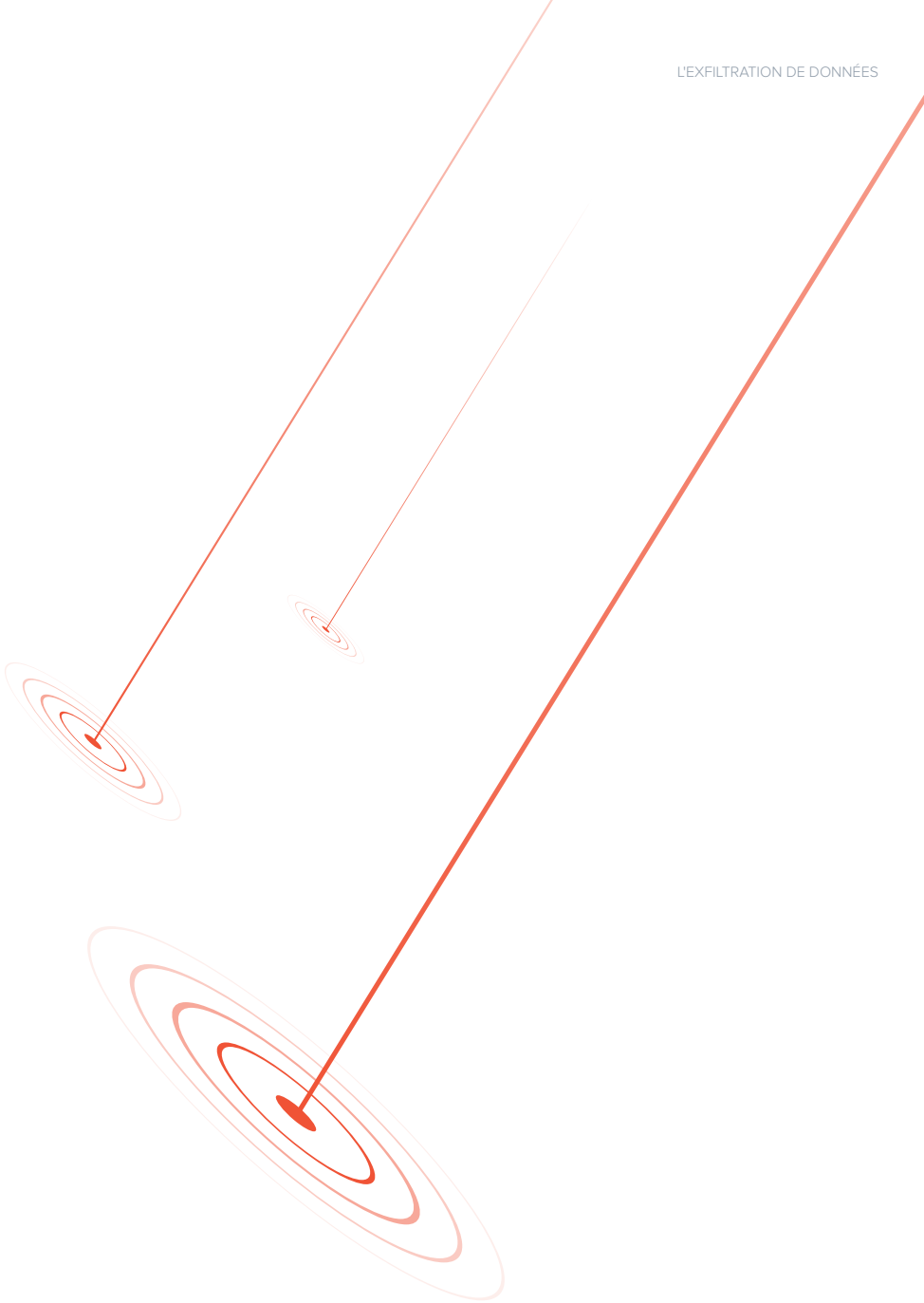
Ampleur moyenne d'une violation de données

25 575 documents

Barracuda

Se protéger contre l'exfiltration de données

Les passerelles de sécurité sont déployées en ligne avec le flux de messagerie ; elles filtrent à la fois les messages entrants et sortants. La prévention contre la perte de données se présente sous la forme d'un ensemble de technologies et de politiques d'entreprise permettant de s'assurer que les utilisateurs finaux n'envoient pas de données sensibles ou confidentielles en dehors de l'entreprise. Le système analyse tous les e-mails sortants pour y déceler des modèles prédéterminés qui pourraient indiquer des données sensibles, notamment des numéros de carte bancaire, de sécurité sociale et des renseignements médicaux. Les messages contenant ce type de données sensibles sont ainsi chiffrés automatiquement.



Barracuda

Phishing par URL

Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte

Moins complexe

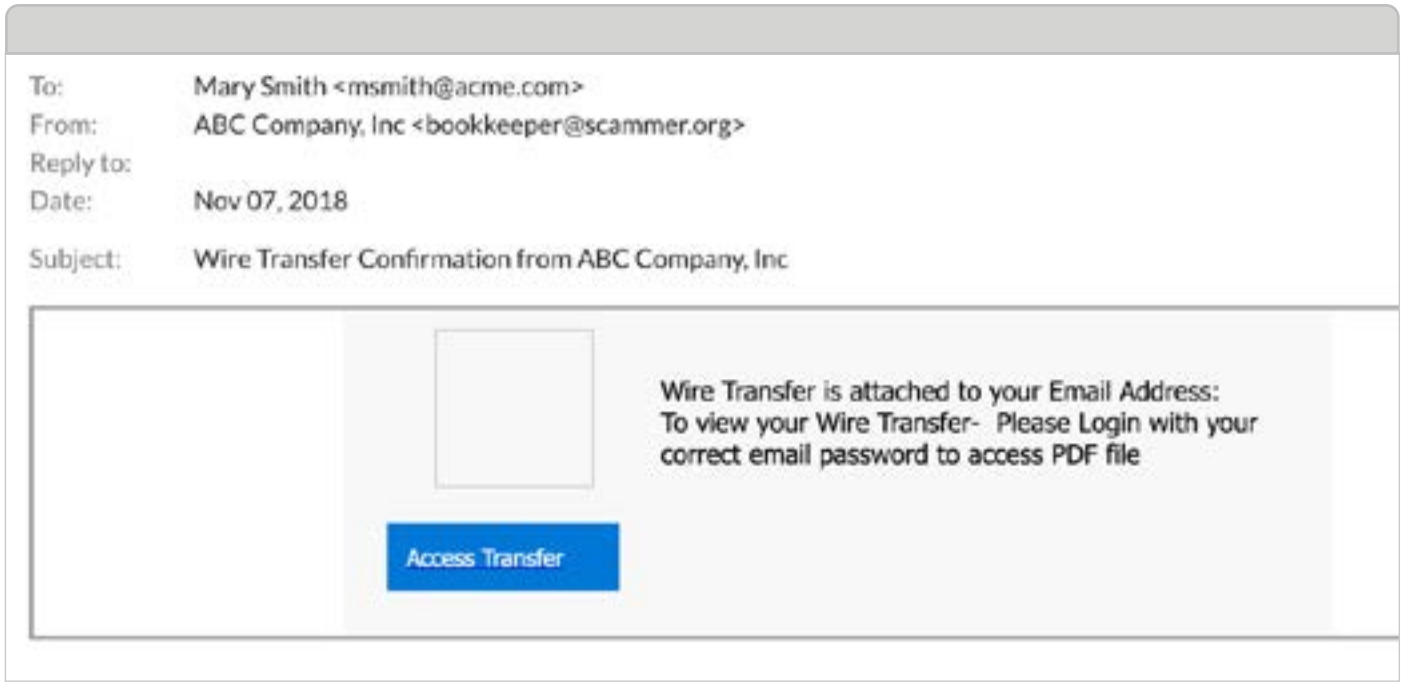
Plus complexe

Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

Barracuda

Lors des attaques de phishing, les cybercriminels tentent d'obtenir des informations sensibles pour une utilisation malveillante, comme des noms d'utilisateur, des mots de passe ou des informations bancaires. Le phishing par URL utilise les e-mails pour inciter les utilisateurs à saisir des informations sensibles sur un faux site Web qui ressemble à un site authentique.

Le phishing par URL correspond à ce que l'on appelle également les « faux sites Web » et les « sites Web de phishing ».



Exemple d'attaque

L'impact du phishing par URL

Environ 32 % des violations de données utilisent le phishing, et de nombreuses attaques de phishing incluent des liens malveillants vers de faux sites Web. L'utilisation d'URL dans les e-mails de phishing est une méthode répandue et efficace. Malheureusement, environ 4 % des destinataires d'une campagne de phishing cliquent sur le lien malveillant, et les hackers n'ont besoin que d'une personne pour les laisser entrer.

Étant donné le taux de réussite, il n'est pas surprenant que les pertes imputables au phishing rapportées en 2019 aient atteint presque 58 millions de dollars. Ce fait est assez inquiétant, dans la mesure où seules 57 % des organisations disposent d'une protection des URL, selon une étude récente.

Se protéger contre le phishing par URL

Les passerelles sont un moyen très efficace de prévenir les attaques de phishing par URL. Elles déploient des technologies de filtrage et de réécriture des URL pour bloquer l'accès aux liens de sites Web malveillants distribués par e-mail, notamment tous les logiciels malveillants et sites de phishing connus. Le sandboxing peut également aider à bloquer les liens malveillants.

La protection des boîtes de réception par API complète la sécurité assurée par les passerelles. L'API peut fournir une visibilité historique et interne des véritables URL utilisées par une organisation. Les URL anormales ou usurpées, qui indiquent des attaques de phishing, peuvent ainsi être bloquées. Même lorsqu'un site Web de phishing n'a jamais été utilisé dans des campagnes antérieures ou est hébergé sur un domaine de bonne réputation, la défense de la messagerie peut contribuer à neutraliser les attaques de spear phishing ciblées utilisant des URL malveillantes.

Arnaques

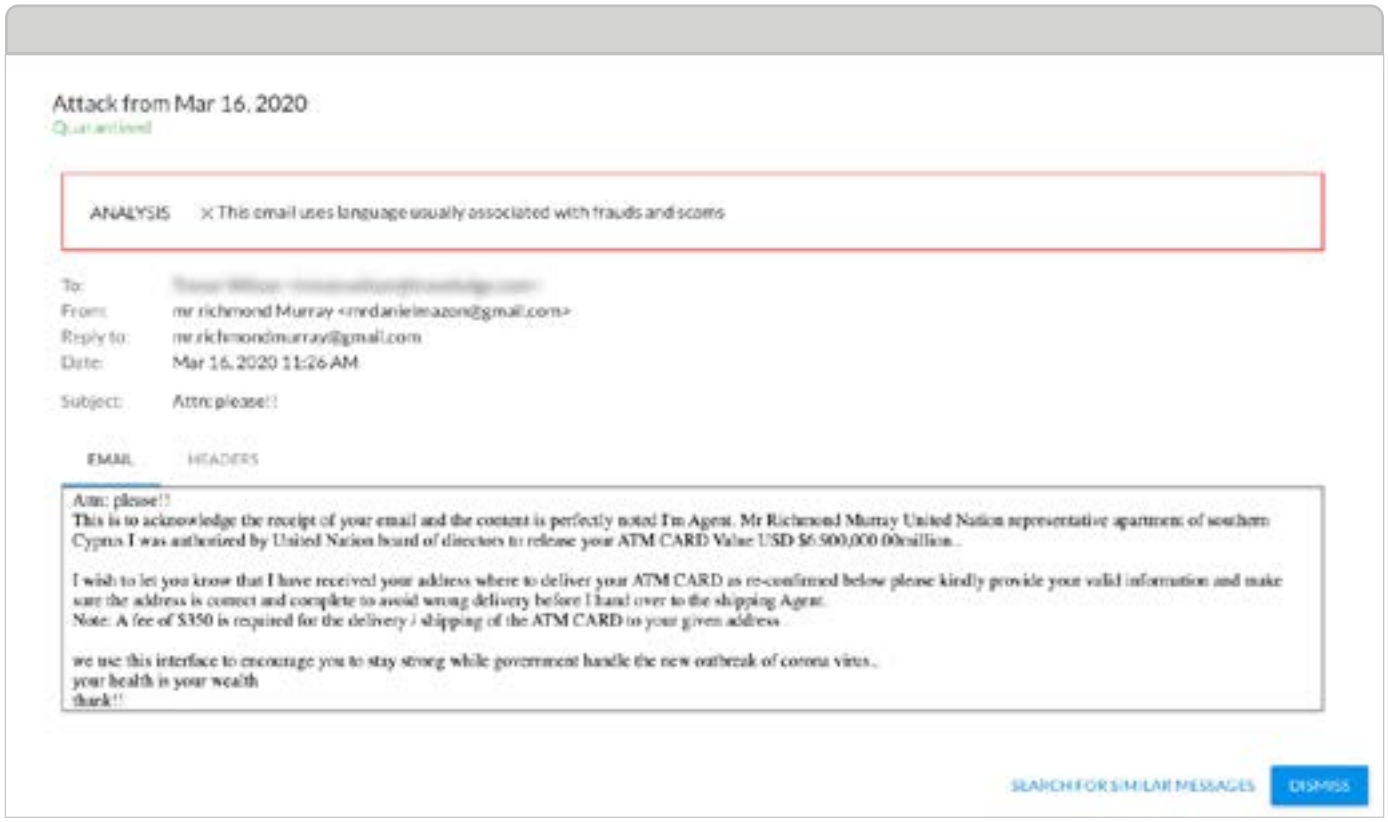
Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte

Moins complexe — **Plus complexe**

Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

Barracuda

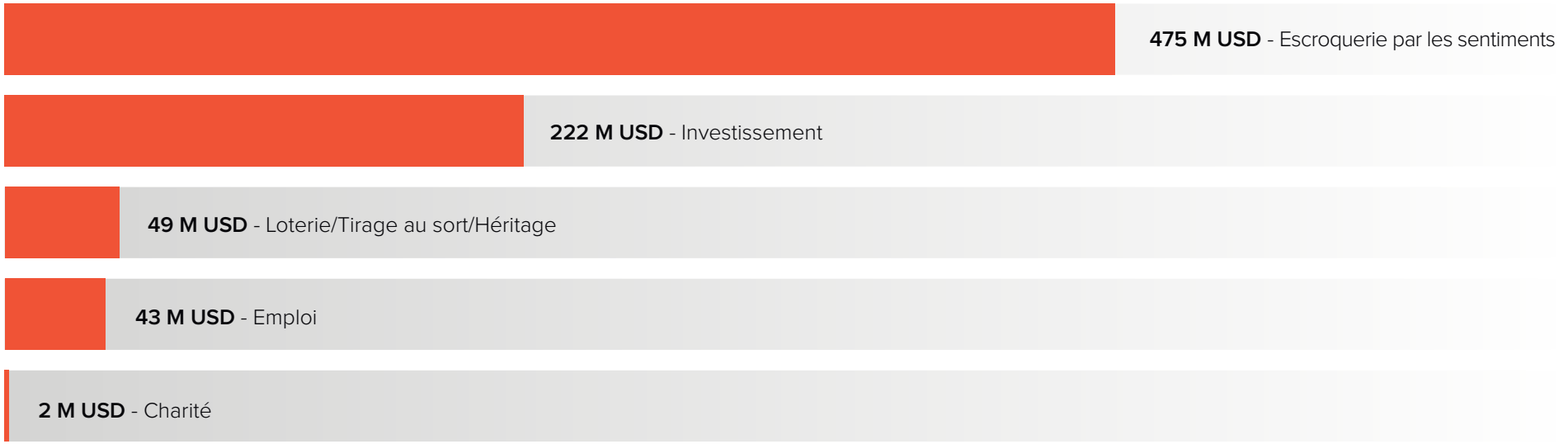
Pour les arnaques par e-mail, les cybercriminels utilisent des stratagèmes frauduleux pour escroquer leurs victimes ou voler leur identité en les poussant à divulguer des informations personnelles. Les arnaques peuvent prendre la forme de fausses offres d'emploi, d'opportunités d'investissement, de notifications d'héritage, de prix de loterie ou encore de transferts de fonds.



Exemple d'attaque

L'impact des arnaques

Les arnaques représentent 39 % de toutes les attaques de spear phishing. Les arnaqueurs utilisent une large gamme de techniques, des faux gains de loterie aux arnaques à l'investissement. Il n'est en outre pas rare qu'ils tentent de gagner de l'argent en exploitant des tragédies comme les ouragans, la pandémie de COVID-19 et d'autres catastrophes. Ils se nourrissent aussi bien de la compassion, que de la charité et de la peur des gens. Malheureusement, de nombreuses personnes tombent dans leurs pièges, et partagent involontairement des informations sensibles ou transfèrent de l'argent. Le FBI a ainsi comptabilisé des millions de dollars de pertes résultant de ces arnaques.



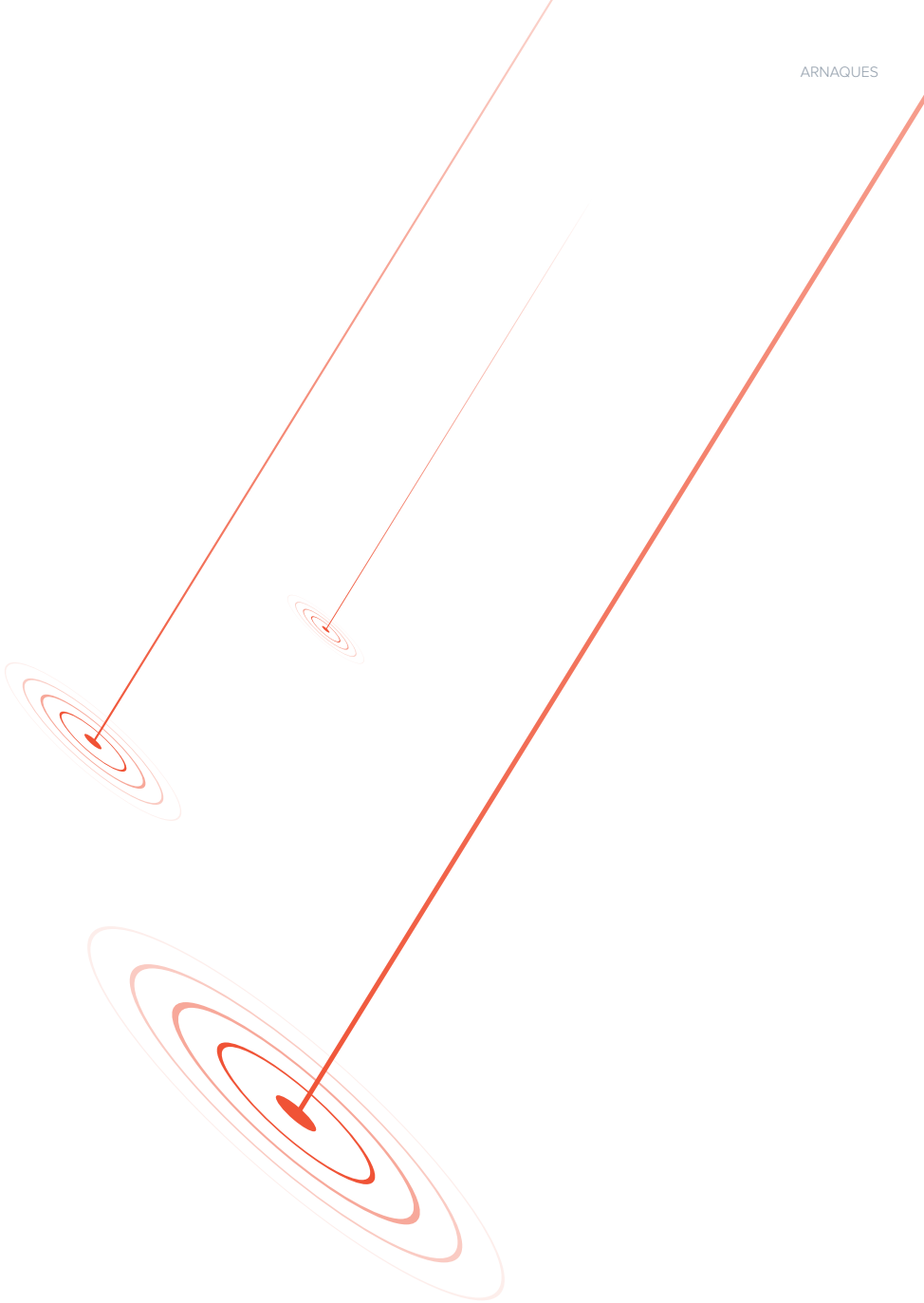
Arnaques : pertes signalées au FBI en 2019

Se protéger contre les arnaques

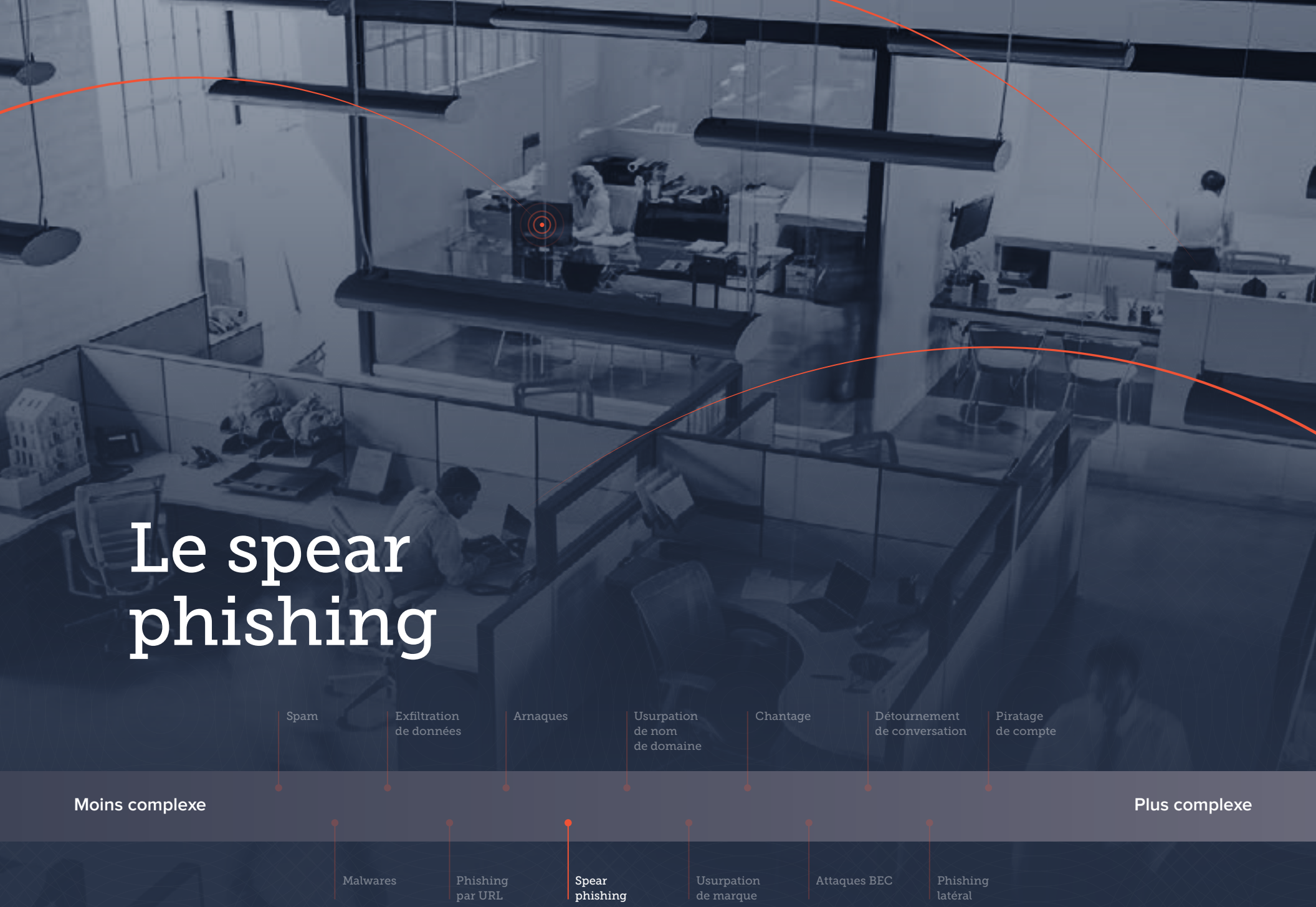
La protection des boîtes de réception par API contre les arnaques s'appuie sur l'historique des communications par e-mail afin d'établir à quoi ressemblent des échanges normaux pour chaque employé. Lorsque les cybercriminels envoient des arnaques par e-mail qui s'éloignent de ces communications habituelles attendues, les messages sont signalés et bloqués par la défense de la boîte de réception.

Les solutions de passerelle reposent sur des politiques granulaires, cherchant des mots-clés spécifiques susceptibles d'indiquer des arnaques. En combinaison avec des filtres de réputation et des listes noires, elles peuvent être efficaces, mais aboutissent souvent à des faux positifs, empêchant l'envoi de messages importants.

De nombreuses arnaques par e-mail peuvent également être classées comme du spam. Les organisations doivent donc déployer à la fois des filtres anti-spam au niveau de la passerelle de messagerie et une protection des boîtes de réception par API pour une défense efficace contre les arnaques.



Barracuda



Le spear phishing

Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte

Moins complexe

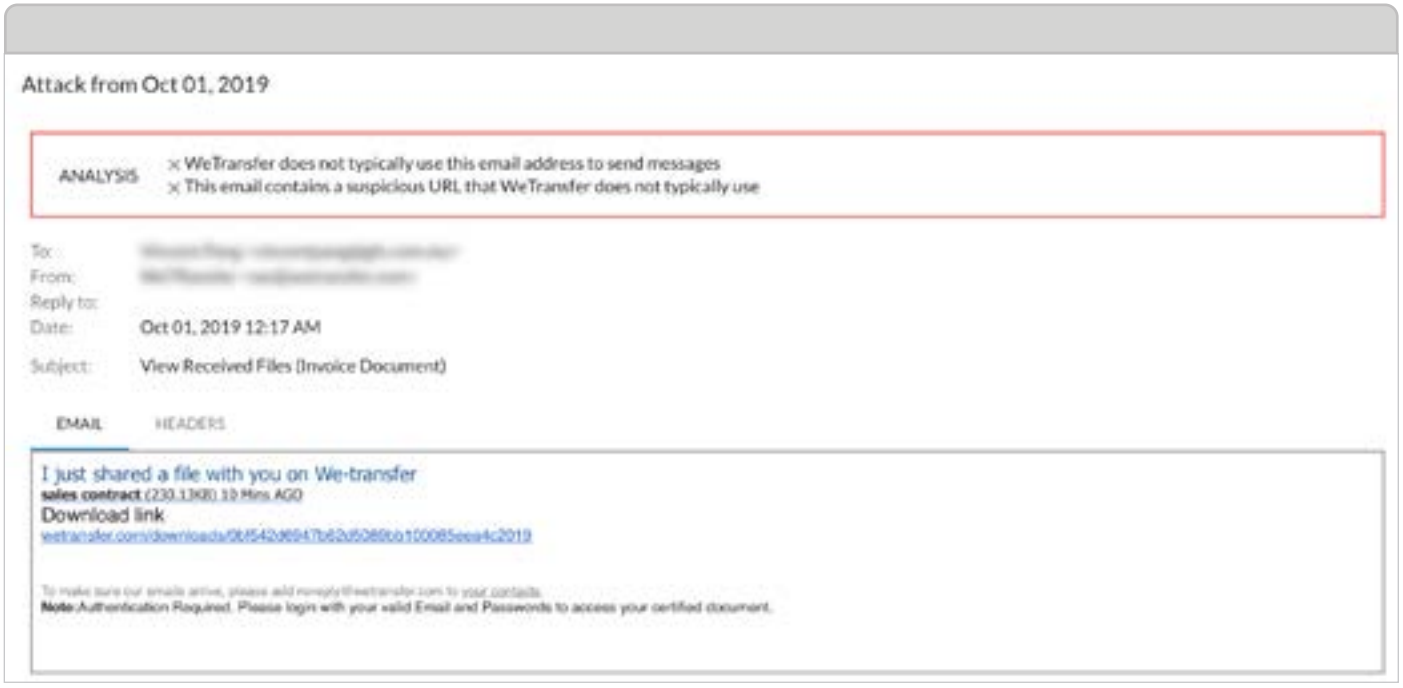
Plus complexe

Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

Barracuda

Le spear phishing est une forme hautement personnalisée d'attaque de phishing par e-mail. Les cybercriminels mènent des recherches sur leurs cibles et conçoivent des messages particulièrement convaincants, en usurpant souvent l'identité d'un collègue, d'un site Web ou d'une entreprise de confiance. Les e-mails de spear phishing visent généralement à voler des informations confidentielles, telles que des informations de connexion ou des données financières, qui sont ensuite utilisées pour commettre des fraudes, des usurpations d'identité et d'autres délits. Les cybercriminels utilisent également des tactiques d'ingénierie sociale pour leurs attaques de spear phishing, telles que l'urgence, l'échéance et la pression, pour accroître leurs chances de réussite.

Le spear phishing est aussi appelé « whaling » et « laser phishing ».



Exemple d'attaque

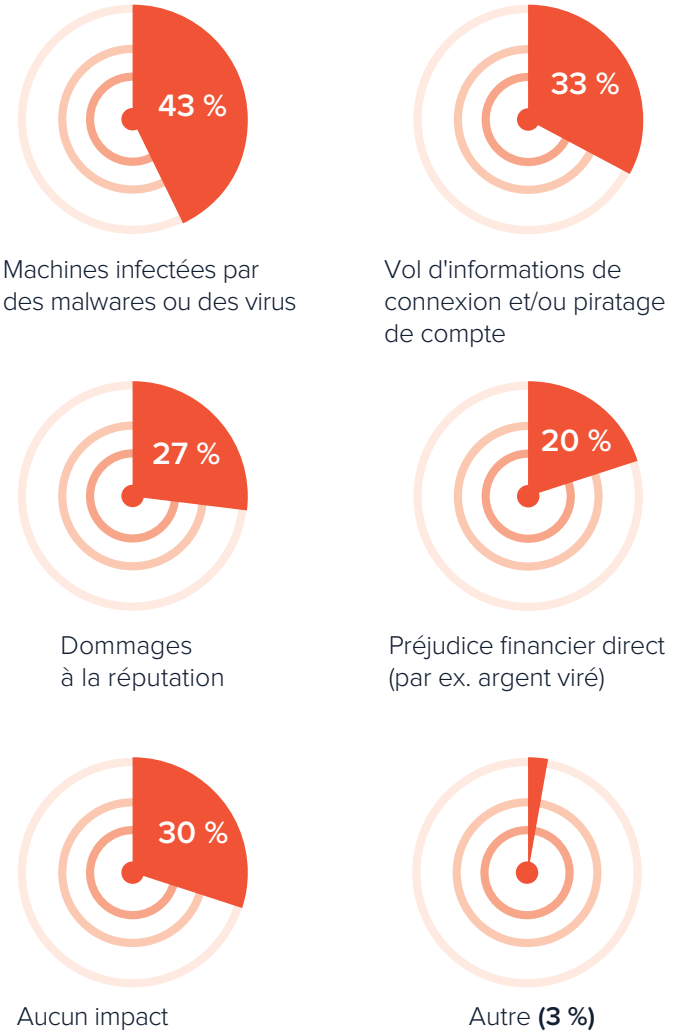
Barracuda

L'impact du spear phishing

Dans le cadre de la récente enquête Email Trends de Barracuda, 43 % des entreprises ont rapporté avoir été victimes d'une attaque de spear phishing au cours des 12 derniers mois. Toutefois, seules 23 % d'entre elles ont déclaré avoir mis en place une protection dédiée contre le spear phishing.

Les attaques de spear phishing peuvent entraîner une infection par logiciel malveillant des machines et du réseau des entreprises, mais également des préjudices financiers directs via des virements et des dommages à leur réputation. Dans de nombreux cas, le spear phishing aboutit au vol d'informations d'identification et au piratage de comptes de messagerie. Des comptes piratés bien souvent utilisés pour lancer de nouvelles attaques de spear phishing. Afin d'enrayer ce cercle vicieux, il est donc essentiel que les organisations déploient une protection dédiée.

Impact des attaques de spear phishing en 2019[1]

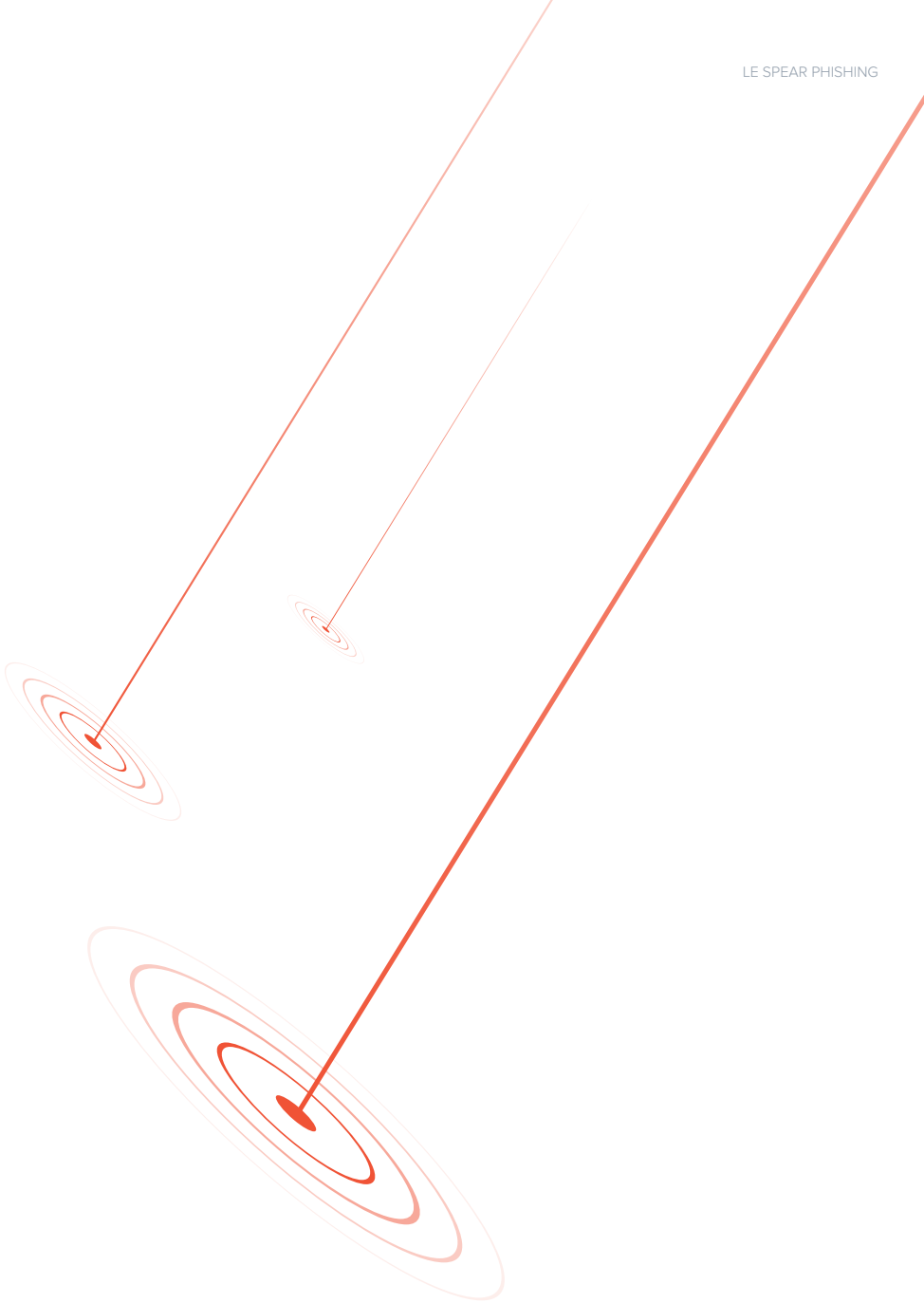


1 Les tendances 2019 en matière de sécurité de la messagerie

Se protéger contre le spear phishing

La protection des boîtes de réception par API accède à l'historique des données de communication par e-mail afin d'élaborer un modèle d'identité des communications, un modèle statistique spécifique à chaque utilisateur. Ce modèle d'identité est ensuite utilisé pour détecter les modèles de communication inhabituels, qui ne correspondent pas au modèle statistique, afin de prévoir et de bloquer les attaques de spear phishing qui parviendraient à contourner la passerelle.

Les passerelles de sécurité de la messagerie traditionnelles n'ont aucune visibilité sur l'historique de données. C'est pourquoi elles évaluent chaque e-mail selon un ensemble de politiques, de filtres et de signatures prédéterminés, plutôt que selon les antécédents de communication et le contexte. Les attaques de spear phishing sont conçues pour contourner ces filtres et politiques, et atteignent donc souvent la boîte de réception des utilisateurs.



Barracuda

L'usurpation de nom de domaine

Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte

Moins complexe

Plus complexe

Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

Barracuda

L'usurpation de nom de domaine est souvent utilisée par les hackers dans le cadre d'une attaque de détournement de conversation. Les attaquants tentent d'usurper un nom de domaine par le biais de diverses techniques, comme le typosquatting, en remplaçant une ou plusieurs lettres dans un nom de domaine de messagerie légitime par des lettres similaires, ou en y ajoutant une lettre difficile à distinguer. En préparation de l'attaque, les cybercriminels enregistrent ou achètent même le nom de domaine servant à l'usurpation.

L'usurpation de nom de domaine est également appelée « typosquatting ».

L'usurpation de nom de domaine est une attaque à très fort impact. On peut aisément passer à côté des différences subtiles entre le nom de domaine de messagerie légitime et celui qui est usurpé. Par exemple, un cyberattaquant tentant d'usurper le nom de domaine barracuda.com pourrait utiliser l'une de ces URL, très similaires :

barraeuda.com

barracada.com

barracúda.com

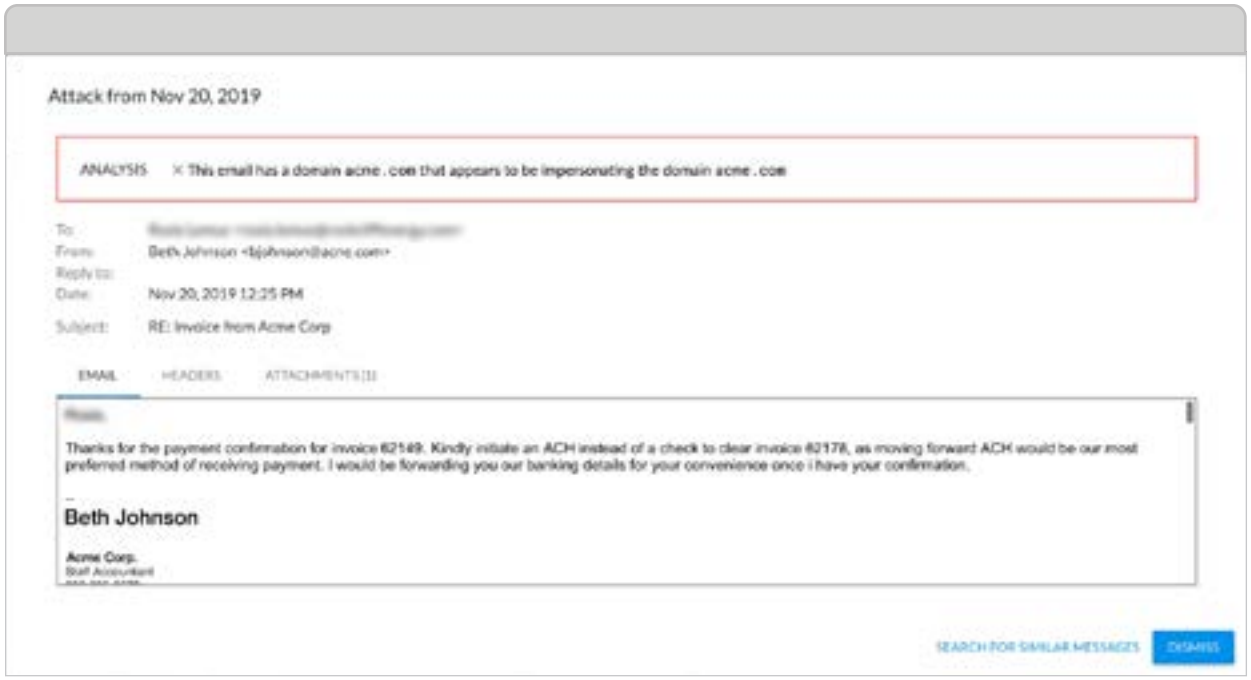
barrracud.com

Parfois, les cyberattaquants modifient le nom de domaine de premier niveau, en utilisant l'extension « .net » ou « .co » au lieu de « .com » afin de tromper leurs victimes :

barracuda.net

barracuda.co

Barracuda



Exemple d'attaque

L'impact de l'usurpation de nom de domaine

Ces derniers mois, les chercheurs de Barracuda ont constaté une nette augmentation des usurpations de nom de domaine utilisées à des fins de détournement de conversation. Une analyse d'environ 500 000 attaques par e-mail par mois montre en effet une augmentation de 400 % des usurpations de nom de domaine utilisées à cette fin.

+400 %

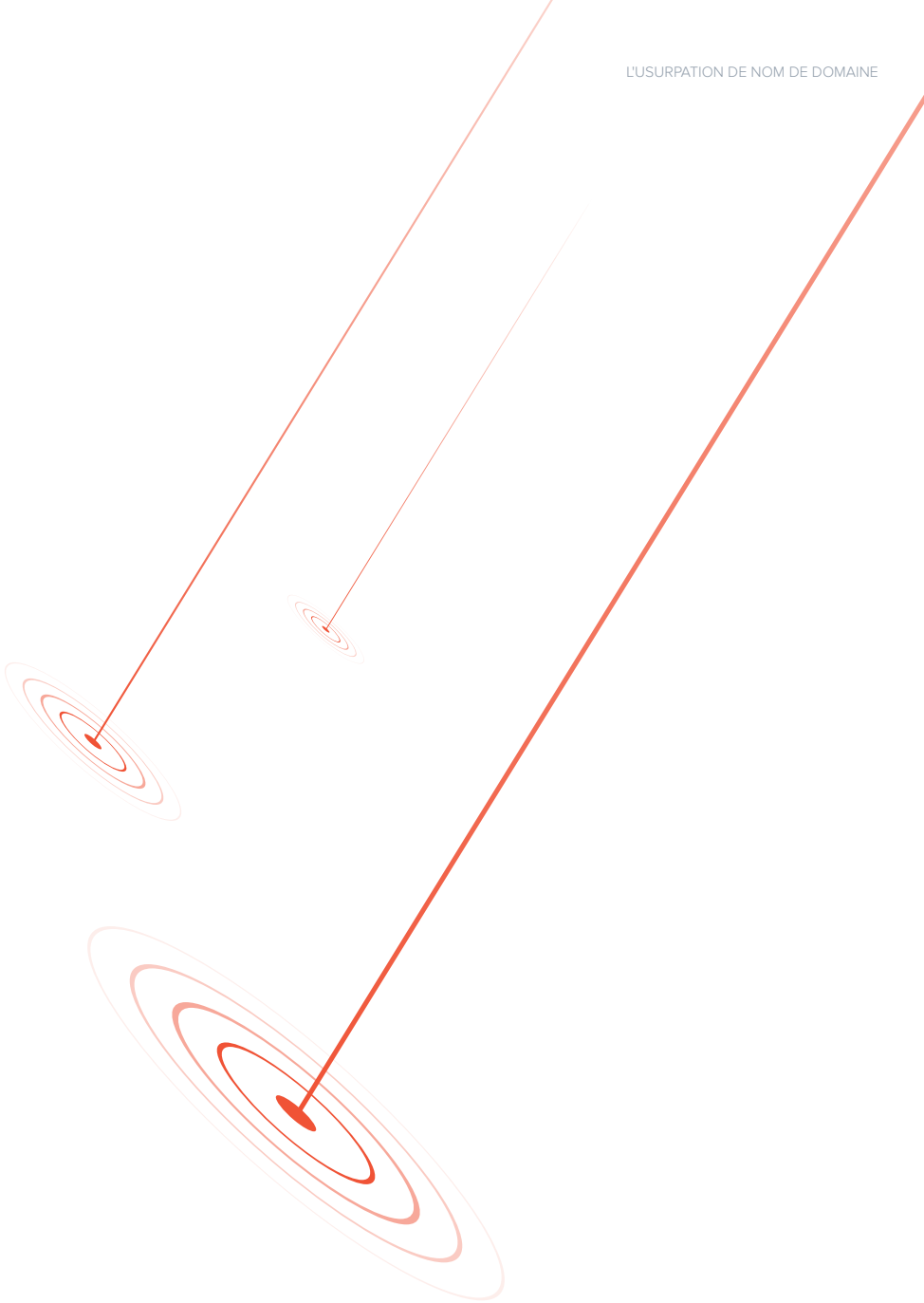
Augmentation des usurpations de nom de domaine au cours du 2e semestre 2019

Barracuda

Se protéger contre l'usurpation de nom de domaine

Le plus gros défi concernant l'usurpation de nom de domaine est de parvenir à détecter de manière précise les noms de domaine typosquattés, et de différencier les tentatives d'usurpation des sites Web authentiques. Les passerelles de messagerie doivent dresser la liste des noms de domaine utilisés par les entreprises et leurs partenaires au fil du temps, un long processus sujet à erreurs et nécessitant une gestion et des mises à jour continues. Étant donné le nombre colossal de noms de domaine et de variantes, le recours aux passerelles pour détecter l'usurpation de nom de domaine occasionne de grands nombres de faux positifs tout en laissant passer des attaques.

La protection des boîtes de réception par API utilise l'historique des communications par e-mail pour obtenir des données sur les noms de domaine utilisés par les entreprises, leurs partenaires et leurs clients. Une telle protection associe les conversations spécifiques, les demandes et les individus avec des noms de domaine de messagerie spécifiques. Ainsi, lorsqu'un fournisseur envoie une demande inhabituelle depuis un nom de domaine suspect, celle-ci est automatiquement détectée et bloquée.



Barracuda

L'usurpation de marque

Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte

Moins complexe

Plus complexe

Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

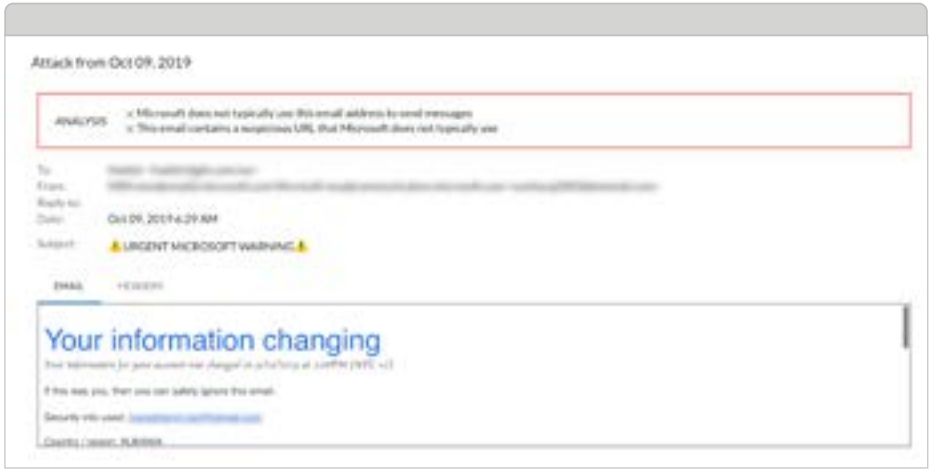
Barracuda

L'usurpation de marque consiste à usurper l'identité d'une entreprise ou d'une marque dans l'objectif d'inciter les victimes à répondre et à divulguer des informations personnelles ou d'autres renseignements sensibles.

Les types d'usurpation de marque les plus fréquents sont les suivants :

L'usurpation d'identité est un type d'attaque de phishing qui consiste à usurper l'identité d'une entreprise connue ou d'une application professionnelle courante. Ce type d'attaque est très répandu, car les e-mails constituent un point d'accès idéal pour collecter des informations d'identification et prendre le contrôle de comptes. Les attaques par usurpation d'identité permettent également de dérober des informations confidentielles, telles que des numéros de carte bancaire et de sécurité sociale.
L'usurpation d'identité est également connue sous le nom d'« attaque par e-mail d'entreprise ».

Le détournement de marque est une forme d'attaque de phishing courante. Dans ce cas de figure, l'attaquant semble utiliser le nom de domaine d'une entreprise pour en usurper l'identité ou celle de l'un de ses employés. Généralement, le procédé consiste à envoyer des e-mails avec des noms de domaine frauduleux mais qui paraissent légitimes.
Le détournement de marque est également connu sous l'appellation « mystification de marque » ou « usurpation d'identité d'entreprise ».

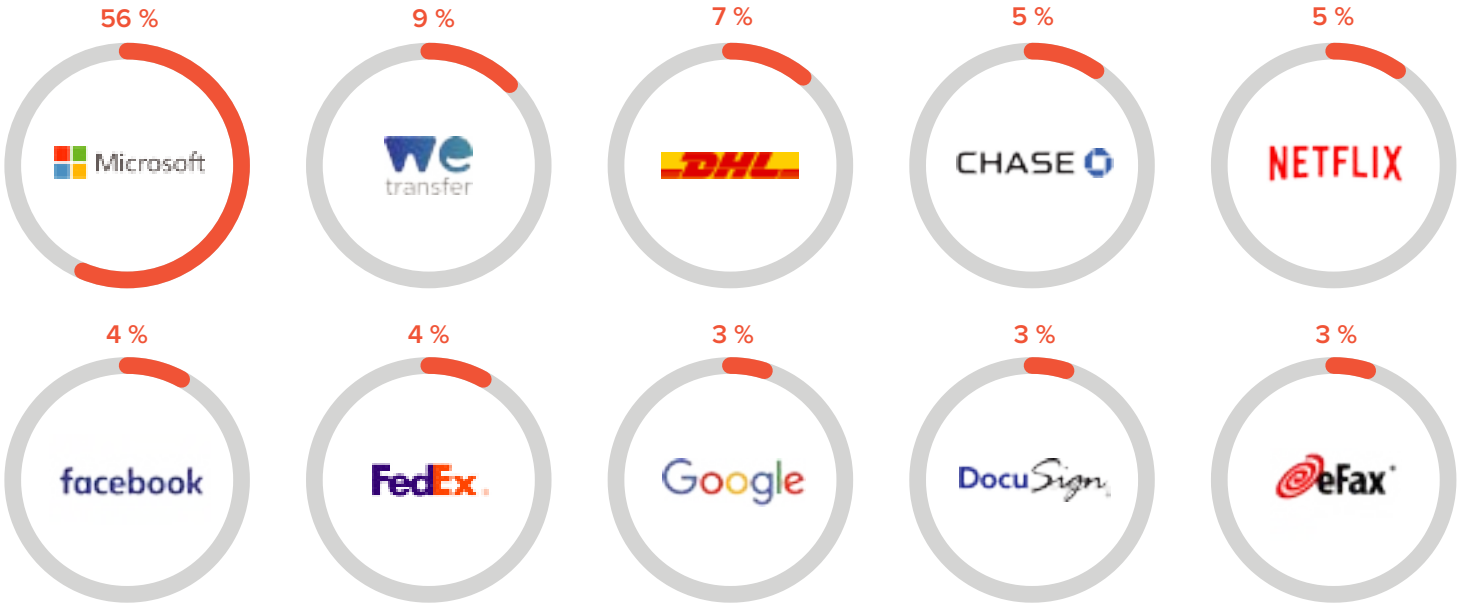


Exemple d'attaque

L'impact de l'usurpation de marque

L'usurpation d'identité est utilisée dans 47 % des attaques de spear phishing, et Microsoft est la marque la plus usurpée dans le cadre de ces attaques. Usurper l'identité de Microsoft est l'une des techniques les plus couramment utilisées par les cybercriminels pour prendre le contrôle d'un compte. Les informations d'identification Microsoft et Office 365 ont une grande valeur, car elles permettent aux hackers de pénétrer au sein des organisations afin de lancer de nouvelles attaques.

Le détournement de marque et les attaques par usurpation sont rendues possibles par une faille de la norme RFC concernant les e-mails, qui n'exige pas une authentification complète pour les domaines expéditeurs. Les normes comme DKIM, SPF et DMARC rendent le lancement de ces attaques bien plus complexe. Cependant, l'usurpation de nom de domaine est couramment utilisée par les hackers lors des attaques par usurpation. Une récente étude a révélé qu'il y a presque 30 000 attaques par usurpation chaque jour. Par ailleurs, 77 % des entreprises figurant dans le classement Fortune 500 n'ont pas de politique DMARC, ce qui facilite l'usurpation de leurs marques lors des attaques de phishing.



Marques les plus fréquemment usurpées

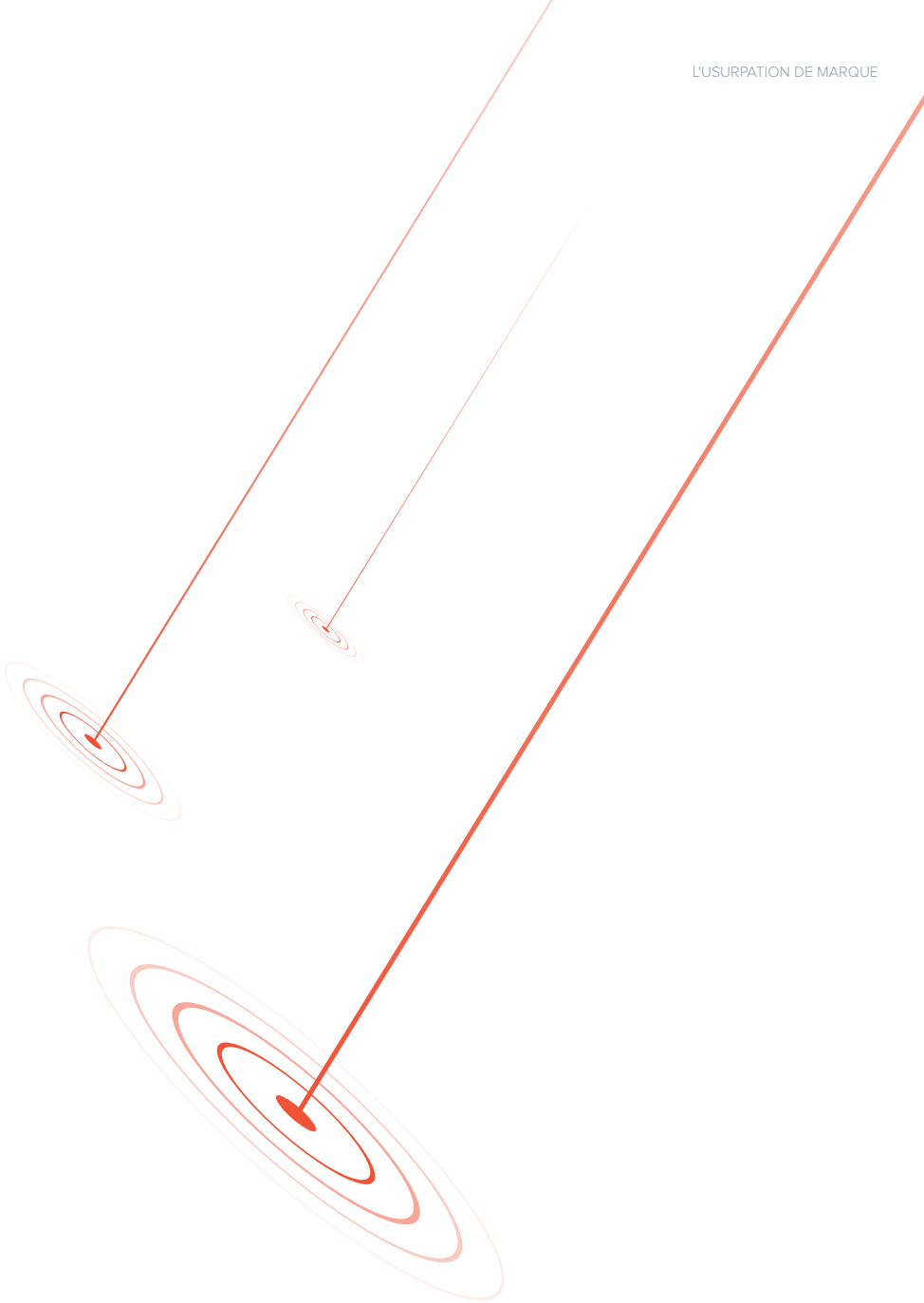
Barracuda

Se protéger contre l'usurpation de marque

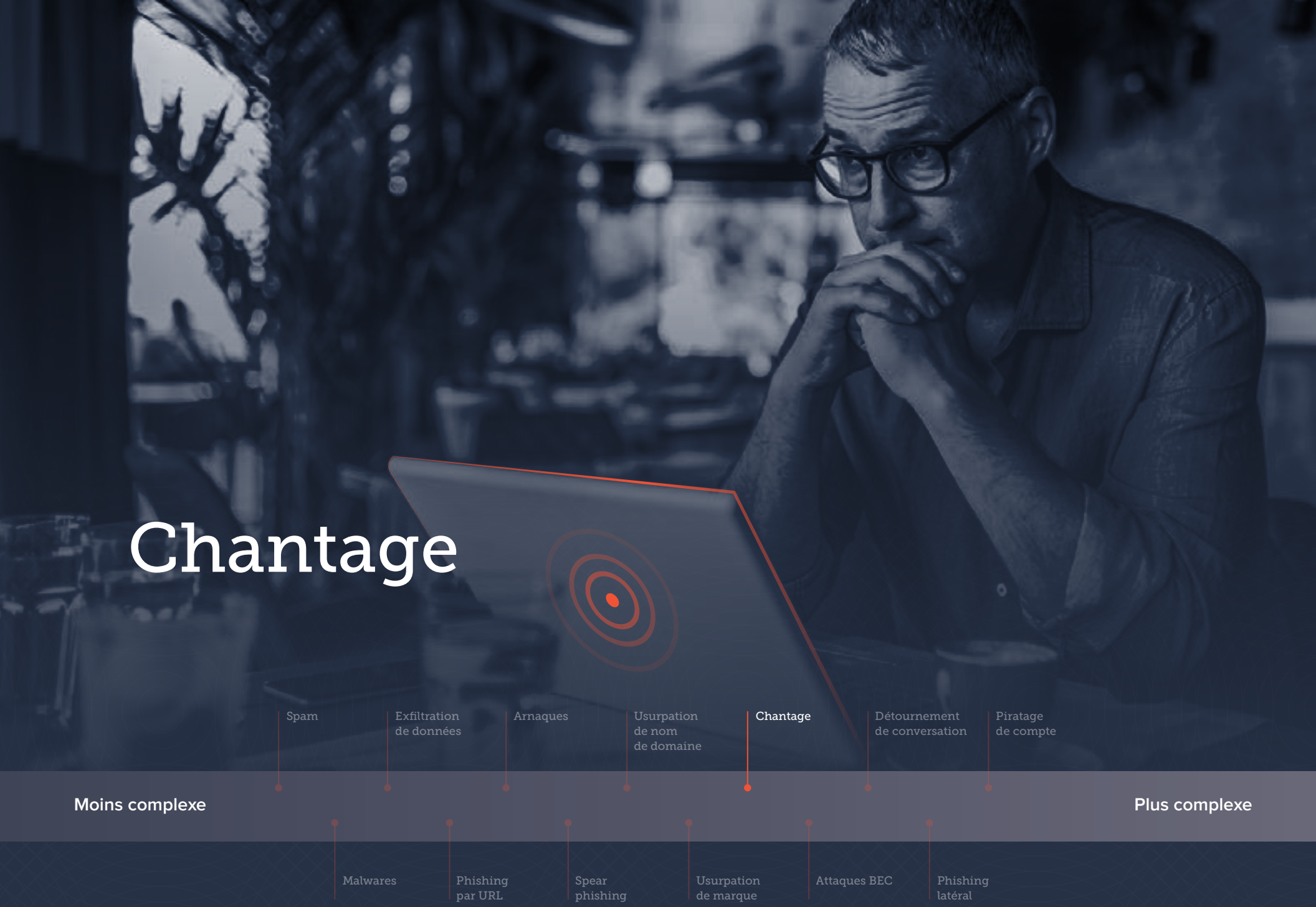
La protection des boîtes de réception par API utilise l'historique de messagerie et les e-mails internes pour obtenir de la visibilité sur les services utilisés par une entreprise. Les données sont exploitées dans un modèle de détection statistique pour comprendre la différence entre les e-mails frauduleux et légitimes, en incluant le branding et les photos oficielles utilisés par l'entreprise.

Les passerelles ne disposent pas d'une telle visibilité et ne peuvent donc pas reconnaître le branding et les photos officielles. Leur approche reposant sur des politiques prédéterminées n'est pas adaptée en raison de la grande variété d'attaques d'usurpation d'identité. La protection des boîtes de réception par API est davantage efficace contre les attaques d'usurpation d'identité.

Les entreprises peuvent obtenir une visibilité sur les fraudes au nom de domaine grâce à l'authentification DMARC, qui les protège contre l'usurpation de nom de domaine et le détournement de marque. Le reporting DMARC offre une visibilité sur la manière dont un nom de domaine de messagerie est utilisé, ce qui permet à une entreprise de mettre en place des politiques qui empêcheront son usurpation.



Barracuda

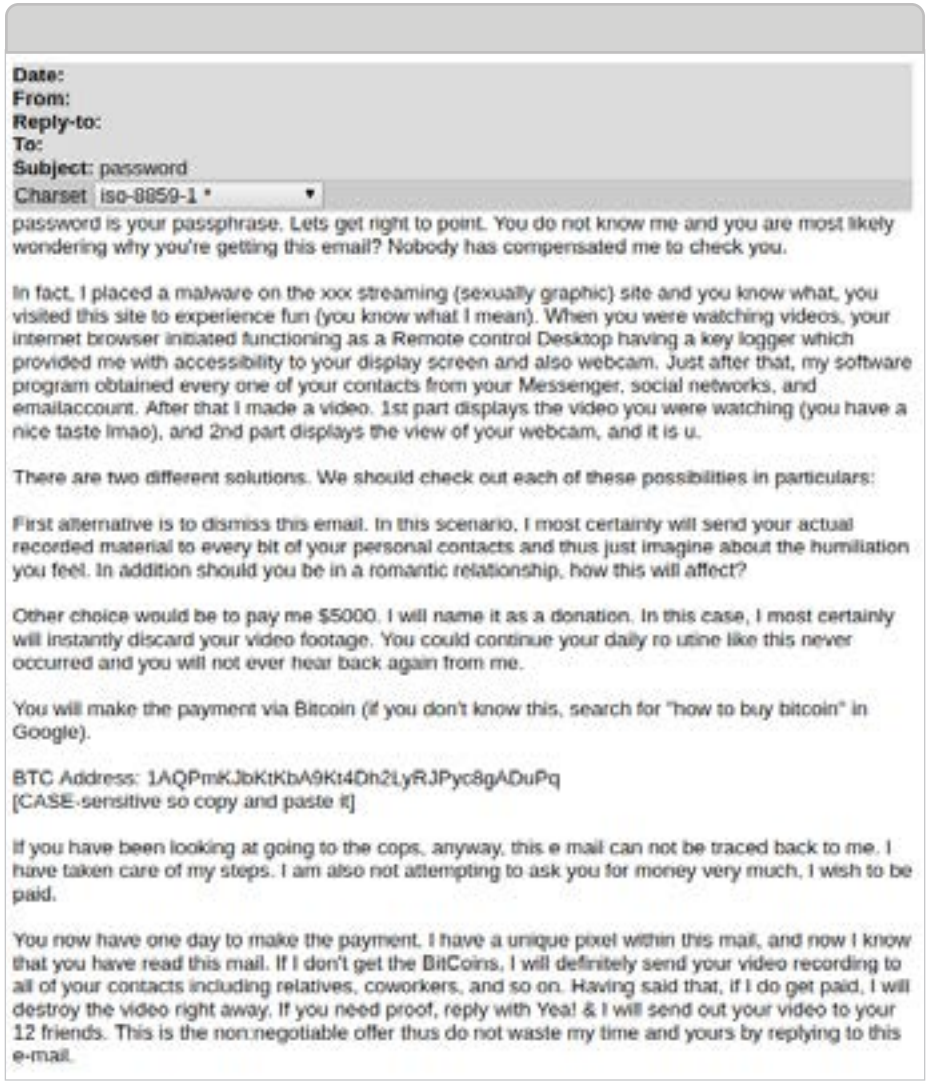

Chantage
Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte
Moins complexe
Plus complexe
Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

Barracuda

Les arnaques par chantage, y compris celles de type « sextorsion », sont de plus en plus fréquentes, plus sophistiquées et contournent désormais les passerelles de messagerie.

Lors de ces attaques, les cybercriminels utilisent des noms d'utilisateur et des mots de passe volés lors de violations de sécurité pour contacter les victimes et les inciter à leur donner de l'argent. Ils déclarent alors détenir une vidéo compromettante supposément enregistrée sur l'ordinateur de la victime, et menacent de divulguer ce contenu à tous ses contacts sauf si elle paye la somme demandée.

Le chantage est également appelé « extorsion » ou « sextorsion ».



Date:
From:
Reply-to:
To:
Subject: password
Charset iso-8859-1 *

password is your passphrase. Lets get right to point. You do not know me and you are most likely wondering why you're getting this email? Nobody has compensated me to check you.

In fact, I placed a malware on the xxx streaming (sexually graphic) site and you know what, you visited this site to experience fun (you know what I mean). When you were watching videos, your internet browser initiated functioning as a Remote control Desktop having a key logger which provided me with accessibility to your display screen and also webcam. Just after that, my software program obtained every one of your contacts from your Messenger, social networks, and emailaccount. After that I made a video. 1st part displays the video you were watching (you have a nice taste lmao), and 2nd part displays the view of your webcam, and it is u.

There are two different solutions. We should check out each of these possibilities in particulars:

First alternative is to dismiss this email. In this scenario, I most certainly will send your actual recorded material to every bit of your personal contacts and thus just imagine about the humiliation you feel. In addition should you be in a romantic relationship, how this will affect?

Other choice would be to pay me $5000. I will name it as a donation. In this case, I most certainly will instantly discard your video footage. You could continue your daily ro utine like this never occurred and you will not ever hear back again from me.

You will make the payment via Bitcoin (if you don't know this, search for "how to buy bitcoin" in Google).

BTC Address: 1AQPmKJbKtKbA9Kt4Dh2LyRJPyc8gADuPq
[CASE-sensitive so copy and paste it]

If you have been looking at going to the cops, anyway, this e mail can not be traced back to me. I have taken care of my steps. I am also not attempting to ask you for money very much, I wish to be paid.

You now have one day to make the payment. I have a unique pixel within this mail, and now I know that you have read this mail. If I don't get the BitCoins, I will definitely send your video recording to all of your contacts including relatives, coworkers, and so on. Having said that, if I do get paid, I will destroy the video right away. If you need proof, reply with Yea! & I will send out your video to your 12 friends. This is the non-negotiable offer thus do not waste my time and yours by replying to this e-mail.

Exemple d'attaque

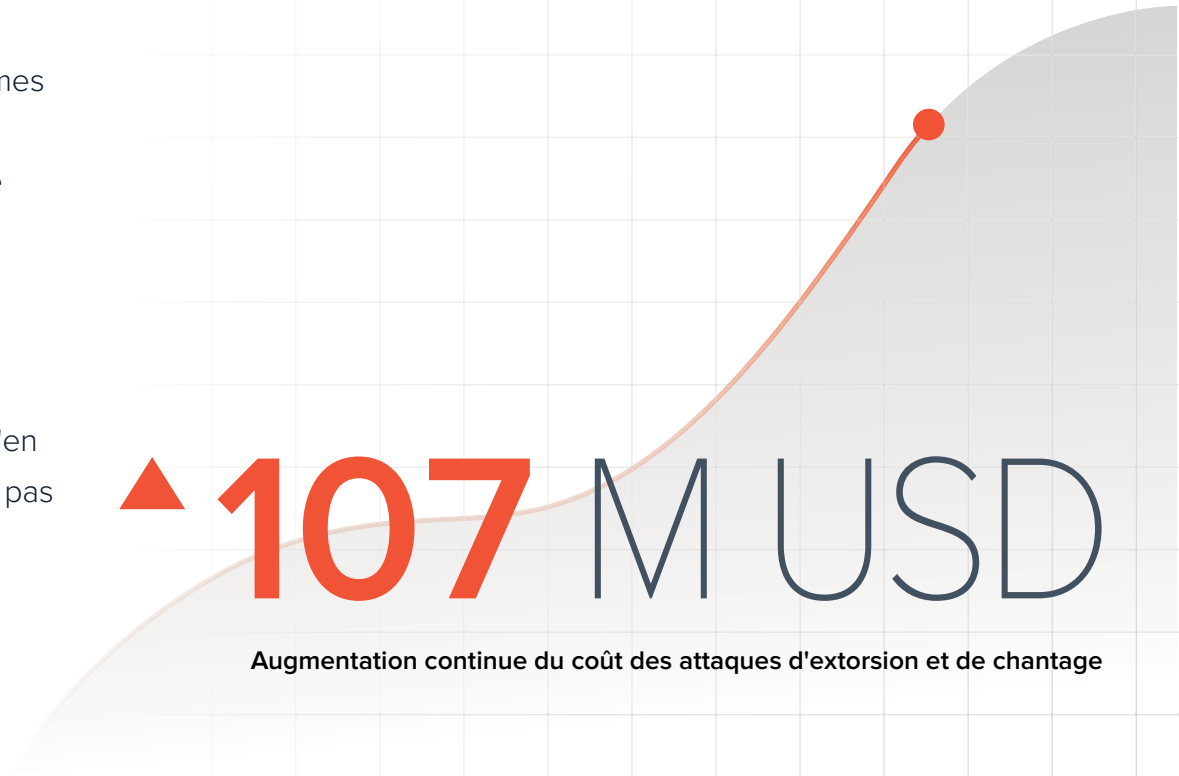
Barracuda

Impact du chantage

Comme les attaques BEC, le chantage constitue environ 7 % des attaques de spear phishing. Les employés sont ainsi tout aussi susceptibles d'être la cible d'une attaque par chantage que d'une attaque BEC.

Selon le FBI, les attaques d'extorsion, qui incluent le chantage, ont coûté plus de 107 millions de dollars en 2019. Les cybercriminels demandent généralement quelques centaines ou milliers de dollars, des montants que les victimes sont susceptibles de pouvoir payer. Les attaques étant très nombreuses, les petits paiements s'accumulent de manière substantielle pour les attaquants.

Les arnaques par chantage sont sous-déclarées en raison de la nature intentionnellement embarrassante et sensible des menaces. Le personnel informatique des entreprises n'en a souvent pas connaissance car les employés ne signalent pas ces e-mails, qu'ils payent la somme demandée ou non.



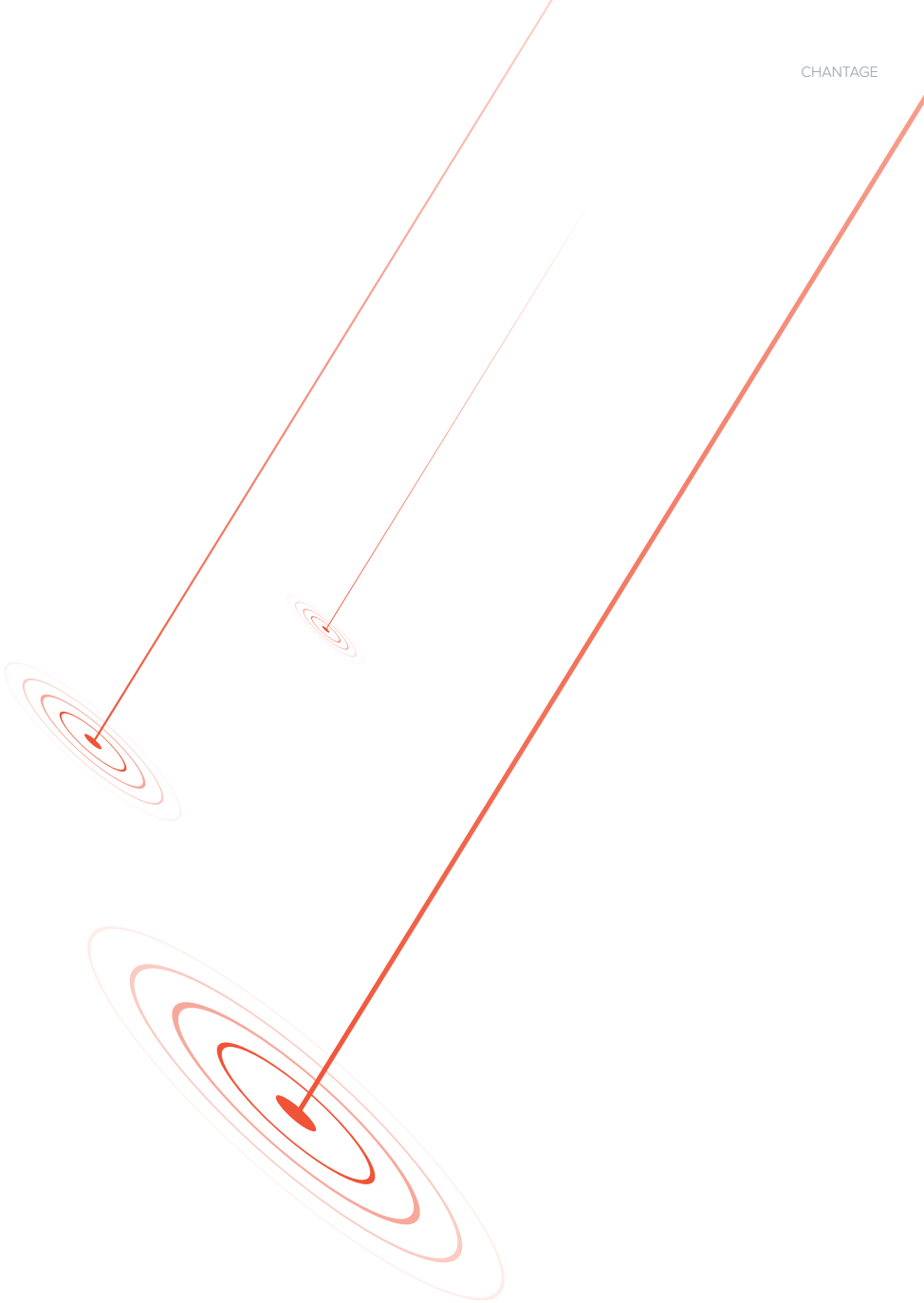
Augmentation continue du coût des attaques d'extorsion et de chantage

Barracuda

Se protéger contre le chantage

La protection des boîtes de réception accède à l'historique des e-mails via les API et élabore ainsi un modèle statistique de schémas de communication, incluant l'intonation utilisée par les individus. Le système reconnaît alors le ton inhabituel et menaçant des attaques par chantage et les associe à d'autres signaux pour les identifier comme des e-mails malveillants.

Les passerelles repèrent des signes de chantage comme l'utilisation de certains mots-clés, mais leur manque de visibilité sur l'historique des données de messagerie et leur incapacité à reconnaître une intonation anormale ne leur permettent pas de prévenir ces attaques.



Barracuda

Attaques BEC

Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte

Moins complexe

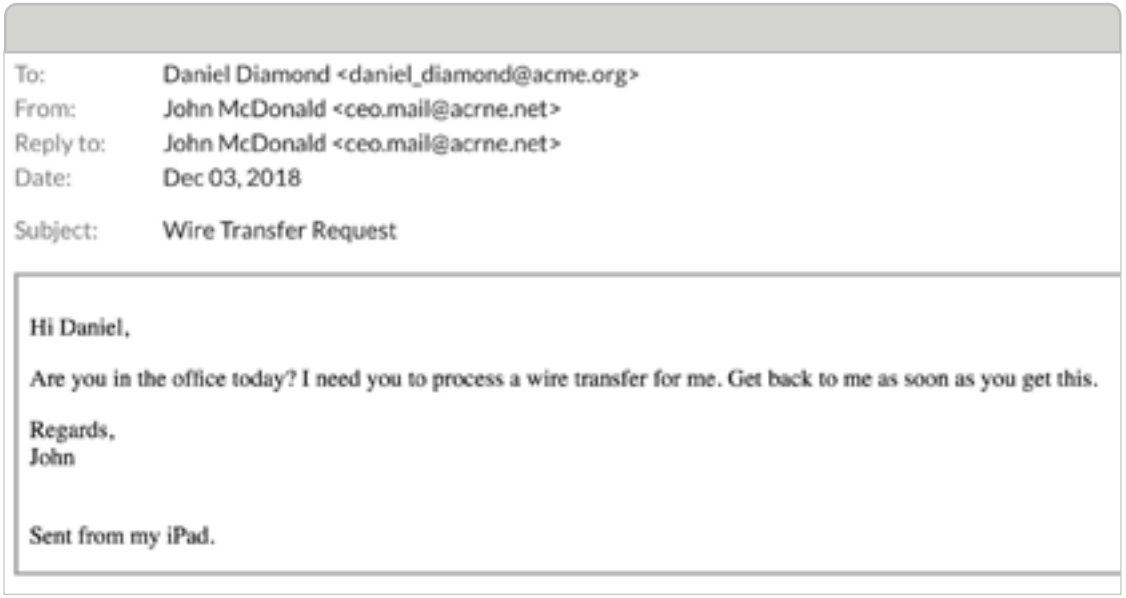
Plus complexe

Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

Barracuda

Dans le cadre des attaques BEC, les cybercriminels usurpent généralement l'identité d'un employé de l'entreprise afin d'escroquer l'entreprise, ses employés, ses clients ou ses partenaires. Dans la plupart des cas, les attaquants concentrent leurs efforts sur les employés ayant accès aux données financières ou aux informations personnelles de l'entreprise, les piégeant pour qu'ils réalisent des virements bancaires ou divulguent des informations sensibles. Ces attaques utilisent des tactiques d'ingénierie sociale et des comptes piratés, et n'incluent généralement pas de pièces jointes ni de liens.

Les attaques BEC sont aussi connues sous les appellations suivantes : « CEO ou CFO Fraud », « usurpation de l'identité d'un employé », « whaling », « ingénierie sociale » et « fraude au virement ».



To: Daniel Diamond <daniel_diamond@acme.org>
From: John McDonald <ceo.mail@acrne.net>
Reply to: John McDonald <ceo.mail@acrne.net>
Date: Dec 03, 2018
Subject: Wire Transfer Request

Hi Daniel,

Are you in the office today? I need you to process a wire transfer for me. Get back to me as soon as you get this.

Regards,
John

Sent from my iPad.

Exemple d'attaque

Barracuda

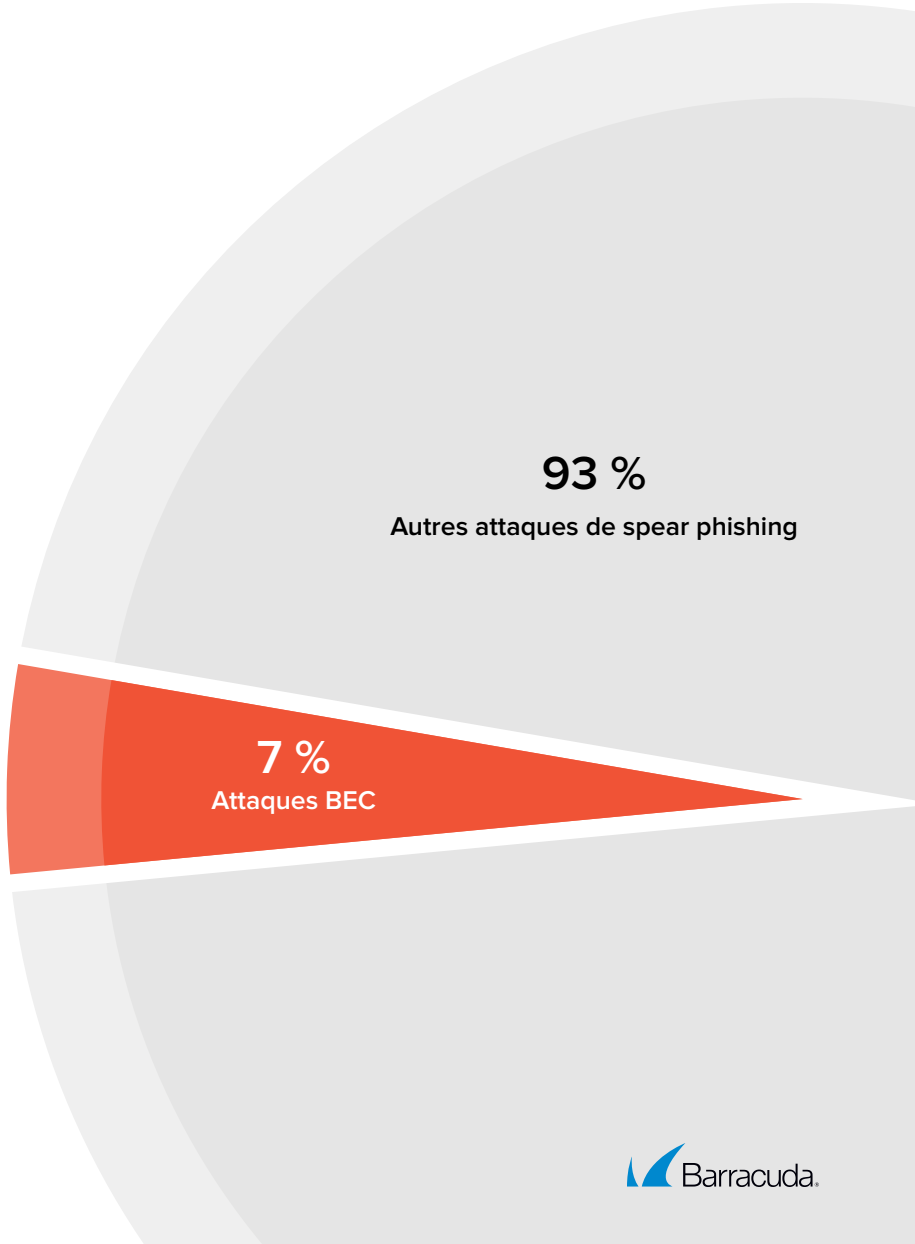
Impact des attaques BEC

Les attaques BEC ne comptent que pour 7 % des attaques de spear phishing, mais elles ont engendré plus de 1,7 milliard de pertes rien qu'en 2019, selon le FBI. Et il faut savoir que 47 % de ces attaques passent par des comptes Gmail.

Les arnaques sur les salaires constituent une forme répandue d'attaque BEC. Elles ciblent les ressources humaines et les départements en charge des salaires, avec pour objectif de faire transférer le salaire d'un employé sur un compte frauduleux. Les hackers usurpent l'identité des employés en fournissant des nouveaux numéros de compte pour le dépôt du salaire. Les arnaques sur les salaires représentent 8 % des attaques BEC, mais ces dernières sont en nette augmentation puisqu'elles ont récemment connu une hausse de plus de 800 %.

1,7 Mrd USD

de pertes en **2019**



Barracuda

Se protéger contre les attaques BEC

La protection des boîtes de réception par API utilise l'historique des données de messagerie pour élaborer un modèle statistique ou un modèle d'identité, afin d'identifier les interactions possibles entre les individus, ainsi que les noms et identités utilisés. Elle examine également les requêtes fréquentes entre les employés de l'entreprise à l'aide d'une analyse relationnelle. En cas de requête inhabituelle, la protection des boîtes de réception par API identifie une tentative d'usurpation en se basant sur l'historique des communications plutôt que sur un ensemble de règles et de politiques, comme le font les passerelles de messagerie traditionnelles.

Les passerelles de messagerie n'ont aucune visibilité sur les schémas relationnels et de communication entre les individus basés sur l'historique des données. Elles utilisent des politiques granulaires personnalisées et la technologie DMARC pour prévenir les usurpations. Ces techniques sont insuffisantes pour empêcher les attaques BEC, et leur dépendance excessive envers des politiques prédéterminées engendre un grand nombre de faux positifs comme négatifs. La protection des boîtes de réception par API constitue une défense plus efficace contre les attaques BEC.

« Les solutions les plus avancées se basent sur l'analyse des schémas de communication pour détecter les usurpations potentielles. »

Source : Gartner (mars 2020)

Barracuda

Détournement de conversation

Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte

Moins complexe

Plus complexe

Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

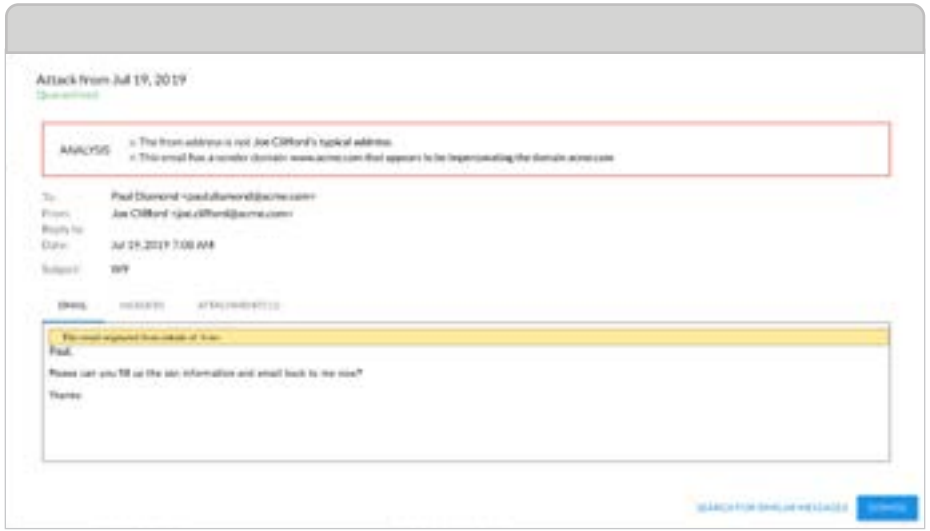
Barracuda

Les cybercriminels procédant à un détournement de conversation s'insèrent dans des échanges professionnels existants ou en lancent de nouveaux en se basant sur les informations qu'ils ont collectées via des comptes de messagerie piratés, afin de voler de l'argent ou de récupérer des informations personnelles.

Le détournement de conversation peut être utilisé à des fins de piratage de compte. Les attaquants passent du temps à lire les e-mails et à surveiller le compte compromis pour analyser l'activité de l'entreprise et en savoir plus sur les affaires en cours, les procédures de paiement, etc.

Cependant, les cybercriminels utilisent rarement les comptes piratés pour lancer une attaque de détournement de conversation. Ils ont davantage recours à l'usurpation de nom de domaine de messagerie.

L'exemple ci-dessous présente une tentative d'usurpation de nom de domaine de messagerie interne dans le cadre d'une attaque de détournement de conversation.



Exemple d'attaque

Impact du détournement de conversation

Ces derniers mois ont vu une hausse importante de plus de 400 % des attaques d'usurpation de nom de domaine ayant pour but de faciliter un détournement de conversation. La part des détournements de conversation dans les attaques d'usurpation de nom de domaine est extrêmement faible en comparaison avec d'autres types d'attaques de phishing, mais ces menaces sophistiquées sont extrêmement personnalisées, ce qui les rend efficaces, difficiles à détecter et coûteuses.

Barbara Corcoran, une femme d'affaires qui a notamment fait quelques apparitions dans l'émission Shark Tank, a ainsi perdu près de 400 000 dollars suite à une attaque de phishing. Les arnaqueurs ont piégé son comptable à l'aide d'une usurpation de nom de domaine de messagerie, via une facture prétendument envoyée par son assistante. Une fausse facture provenant en réalité d'une adresse e-mail fortement similaire. Malheureusement, lorsque l'équipe de Barbara Corcoran s'est rendu compte du subterfuge, l'argent avait déjà été transféré.

USD

400 000

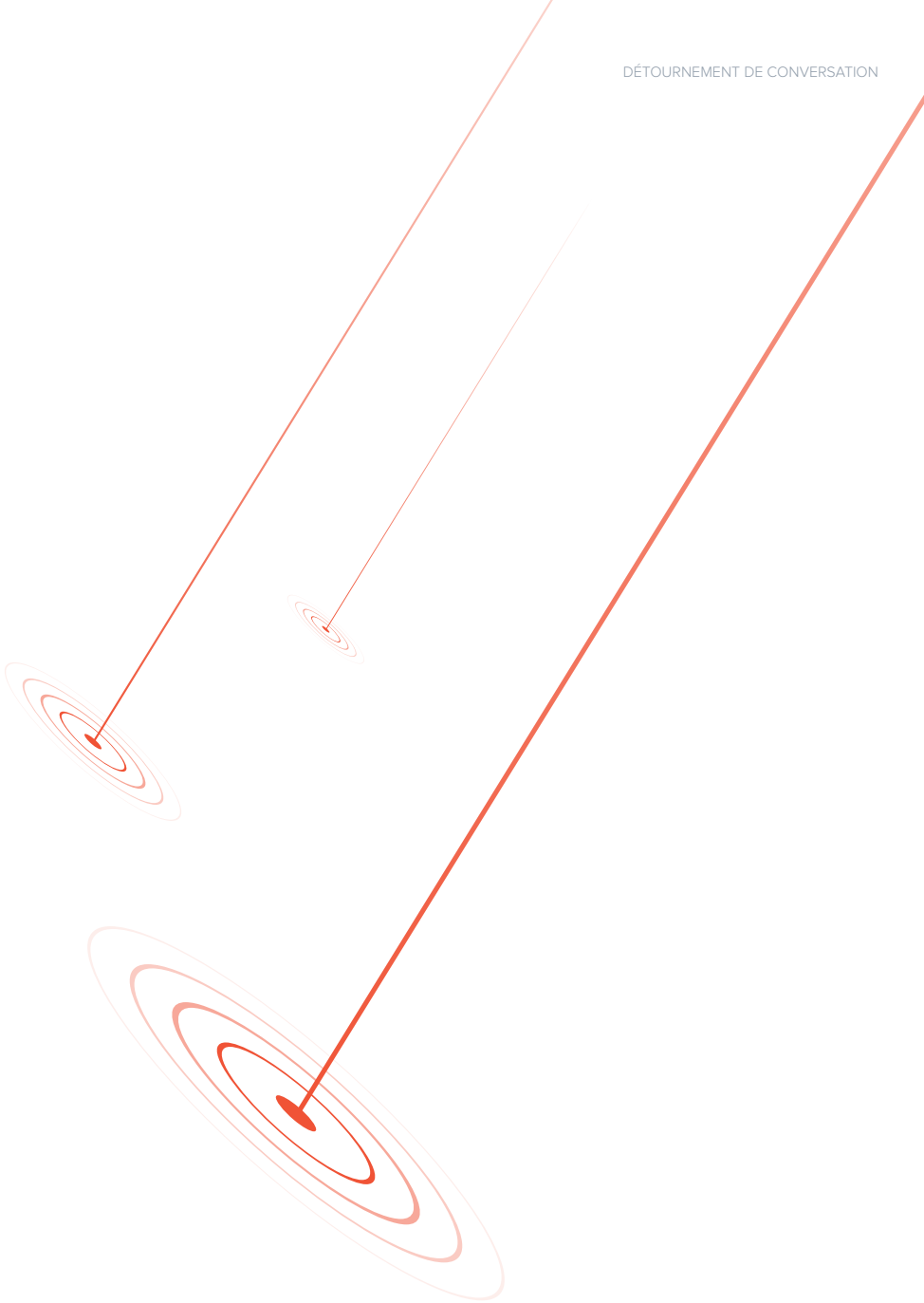
perdus par Barbara Corcoran de Shark Tank lors d'une attaque par détournement de conversation

Barracuda

Se protéger contre le détournement de conversation

La protection des boîtes de réception accède à l'historique des communications par e-mail via une intégration API ; les données sont utilisées dans l'apprentissage machine pour comprendre qui est susceptible de communiquer avec qui, en incluant les contacts externes et les interactions avec ces derniers. Lorsqu'une conversation par e-mail est détournée et que l'identité d'un partenaire de confiance est usurpée par des cybercriminels, la protection des boîtes de réception bloque l'attaque.

Les passerelles n'ont pas cette visibilité. Même si des politiques et des listes blanches peuvent être créées, cette approche est difficile à mettre en œuvre et peut engendrer des faux positifs. Les passerelles autorisent l'envoi d'e-mails même lorsqu'une conversation est détournée. Elles ne sont donc pas en mesure de fournir une protection contre ce type d'attaque.



Barracuda

Phishing latéral

Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte

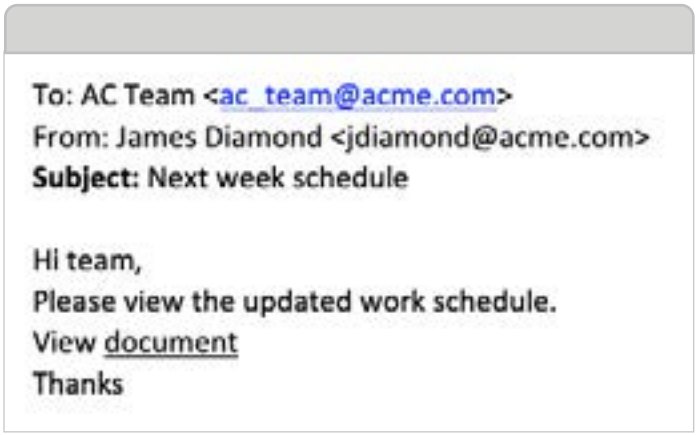
Moins complexe

Plus complexe

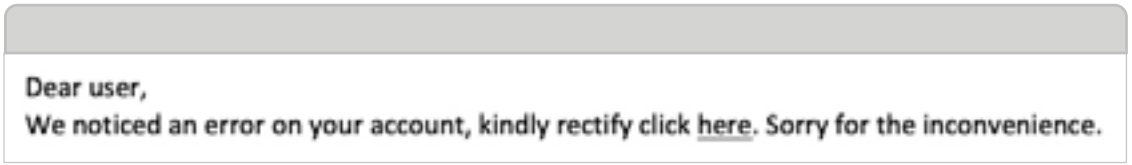
Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

Barracuda

Dans le cadre du phishing latéral, les attaquants utilisent des comptes récemment piratés pour envoyer des e-mails de phishing à des destinataires peu méfiants, comme des contacts proches au sein de la même entreprise ou des partenaires externes, en vue de propager l'attaque. Comme ces e-mails proviennent d'un compte de messagerie légitime et qu'ils semblent avoir été envoyés par un collègue ou un partenaire de confiance, ces attaques ont tendance à être très efficaces.


To: AC Team <ac_team@acme.com>
From: James Diamond <jdiamond@acme.com>
Subject: Next week schedule

Hi team,
Please view the updated work schedule.
View document
Thanks


Dear user,
We noticed an error on your account, kindly rectify click here. Sorry for the inconvenience.

Exemple d'attaque

Impact du phishing latéral

Une récente étude a permis d'établir que 1 organisation sur 7 a déjà subi une attaque de phishing latéral. Ces attaques, qui ciblent un large éventail de victimes et d'organisations, peuvent nuire lourdement à la réputation d'une entreprise, surtout si elles permettent de nouvelles attaques de grande envergure au sein d'autres sociétés.

Plus de 55 % de ces attaques ciblent des destinataires ayant un lien professionnel ou personnel avec le compte piraté. Il n'est donc pas surprenant de constater qu'environ 11 % de ces attaques permettent aux cybercriminels de pirater de nouveaux comptes et, par là-même, d'étendre encore leur emprise.

1 entreprise sur 7 victime d'une attaque de phishing latéral

Se protéger contre le phishing latéral

Dans la plupart des cas, le phishing latéral est une attaque interne. Les passerelles de messagerie n'ont aucune visibilité sur ces communications et ne sont pas en mesure d'arrêter les attaques internes car elles ne les détectent pas. Les passerelles ne peuvent pas non plus neutraliser les attaques post-réception. Une fois qu'un e-mail a atteint une boîte de réception, il y reste. Les API dédiées à la protection des boîtes de réception offrent une visibilité sur les communications internes. Elles permettent donc de détecter les menaces internes comme le phishing latéral et de les neutraliser post-réception.

Barracuda

Piratage de compte

Spam
Exfiltration de données
Arnaques
Usurpation de nom de domaine
Chantage
Détournement de conversation
Piratage de compte

Moins complexe

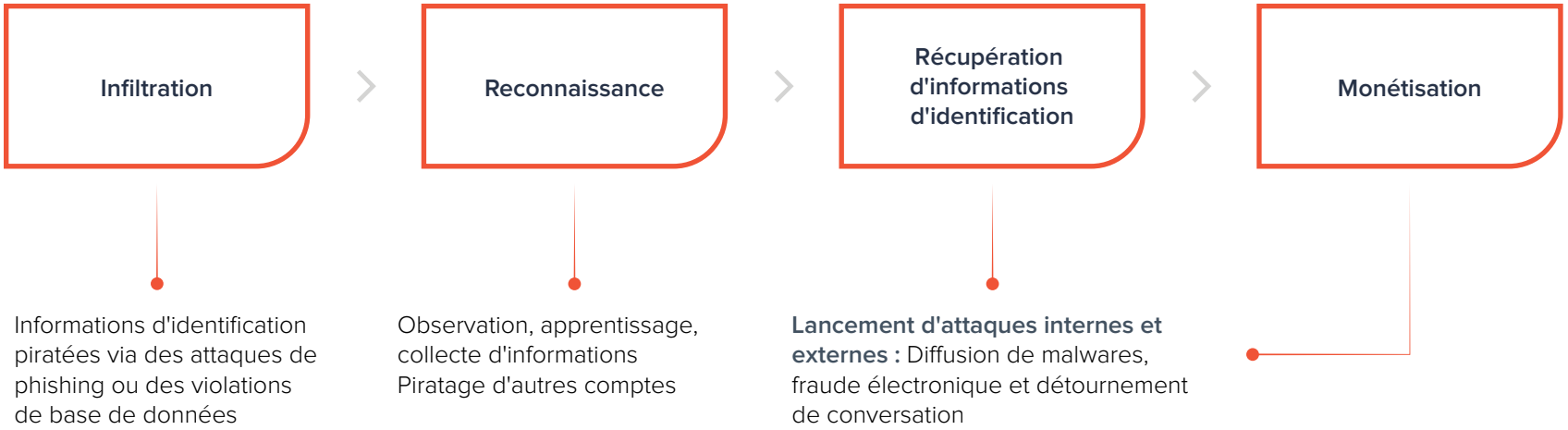
Plus complexe

Malwares
Phishing par URL
Spear phishing
Usurpation de marque
Attaques BEC
Phishing latéral

Barracuda

Le piratage de compte est une forme d'usurpation d'identité et de fraude, au cours de laquelle un tiers malveillant parvient à obtenir les informations d'identification d'un utilisateur. Les cybercriminels utilisent l'usurpation de marque, l'ingénierie sociale et le phishing pour dérober des informations de connexion et accéder à des comptes de messagerie. Une fois qu'un compte est compromis, les hackers surveillent l'activité pour comprendre comment l'entreprise gère ses affaires, quelles signatures elle utilise et de quelle manière les transactions financières sont réalisées. Ces informations leur permettent ensuite de lancer des attaques efficaces afin, notamment, de collecter des informations de connexion à d'autres comptes.

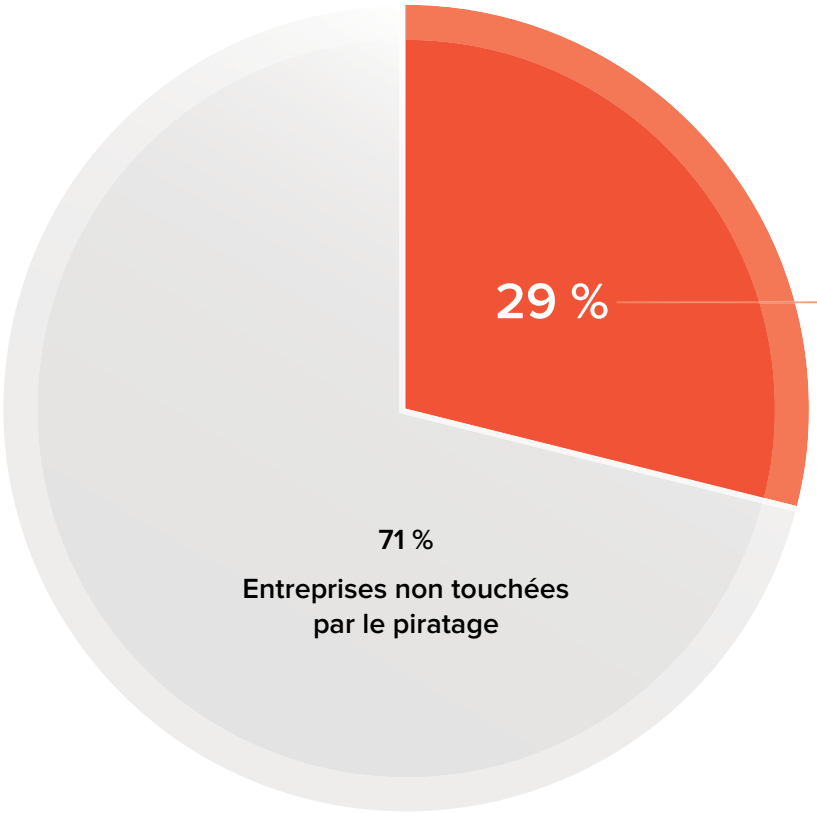
Le piratage de compte est également connu sous le nom de « prise de contrôle de compte » ou « compromission de compte ».



Procédé d'un piratage de compte

Impact du piratage de compte

Une récente étude sur le piratage de compte a révélé qu'en un mois, 29 % des organisations avaient subi ce type d'attaque sur leurs comptes Office 365. Plus de 1,5 million d'e-mails frauduleux et de spams ont ainsi été envoyés depuis des comptes Office 365 piratés sur cette période de 30 jours.

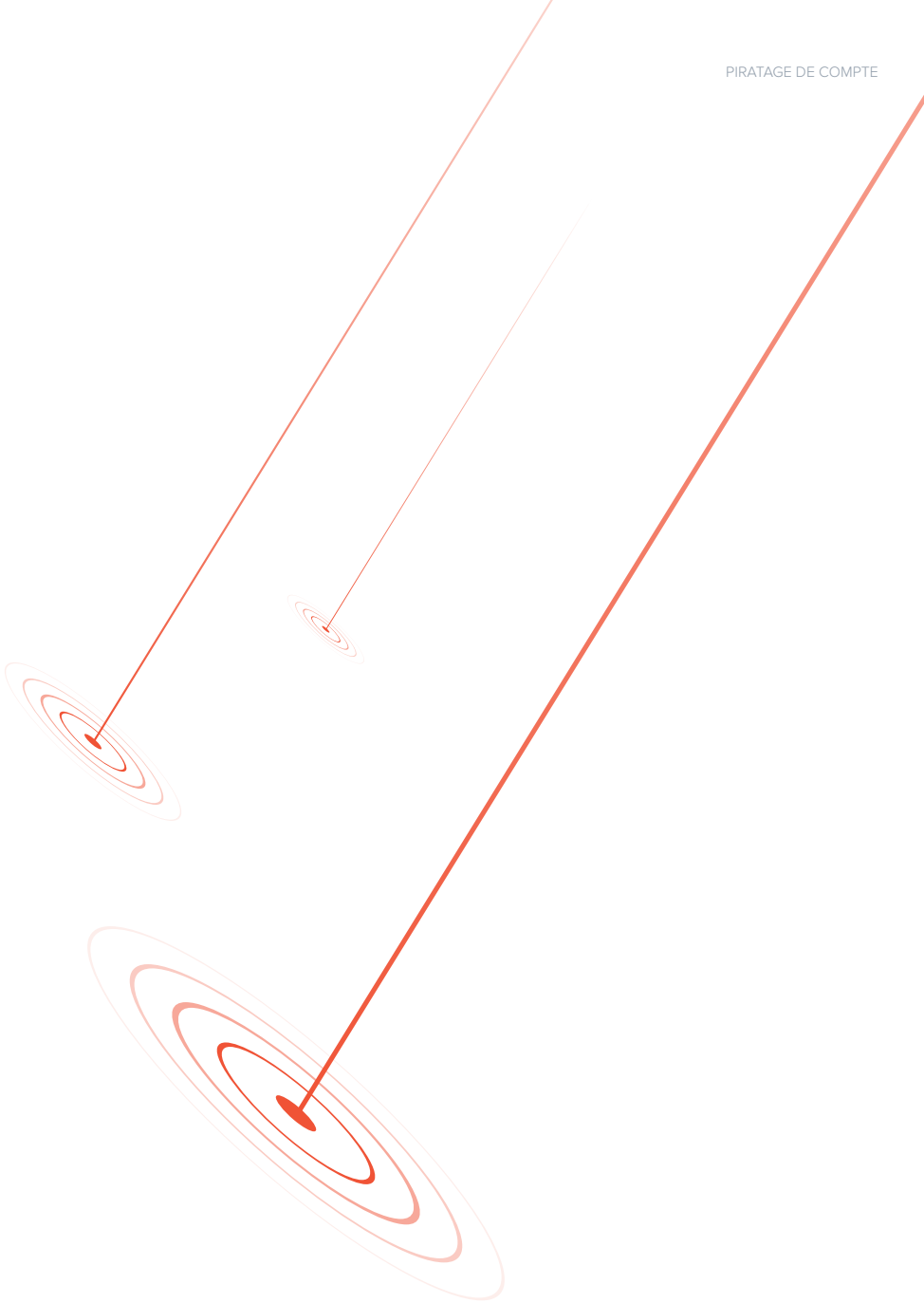


des entreprises **ayant vu leurs comptes Microsoft Office 365 piratés en un mois**

Barracuda

Se protéger contre le piratage de compte

Les passerelles sont installées en périphérie, en dehors des organisations ; elles sont donc déconnectées des boîtes de réception et des utilisateurs. Elles ne sont pas en mesure de surveiller les comportements suspects, comme des connexions effectuées depuis des points d'accès inhabituels ou des messages transférés en interne. La protection des boîtes de réception par API se connecte directement aux boîtes de réception des utilisateurs et surveille les changements suspects dans les règles, les activités de connexion inhabituelles et les messages malveillants envoyés depuis des comptes déjà compromis. Cela permet de détecter le piratage de compte avant qu'il ne soit utilisé à des fins frauduleuses et de prévenir les attaques en empêchant l'accès au compte piraté par des utilisateurs malveillants.



Barracuda

Renforcer la sécurité de la messagerie grâce à la protection des boîtes de réception par API

Passerelles de sécurité de la messagerie traditionnelles

Les passerelles de messagerie constituent un périmètre de sécurité qui veille sur le serveur de messagerie ; elles filtrent les messages entrants et sortants, et bloquent les contenus malveillants. Elles utilisent diverses technologies, telles que des filtres de réputation qui repèrent les adresses IP suspectes. Elles évaluent le contenu des e-mails à la recherche de signes d'intention malveillante, de virus et de malwares. Elles authentifient également l'expéditeur et analysent les URL afin de bloquer celles pointant vers des sites de phishing ou des sites conçus pour diffuser des malwares. Les passerelles de messagerie permettent de détecter et de bloquer efficacement les attaques « zero-day » et les ransomwares. Cette couche de protection inclut des technologies avancées de protection contre les menaces comme le sandboxing, qui évaluent des variantes de malware inédites et inconnues au sein d'un environnement contrôlé.

Les passerelles constituent les fondements essentiels de la sécurité de la messagerie. Elles bloquent la plupart des messages malveillants, notamment les spams, les attaques de phishing de grande envergure, les malwares, les virus et les attaques « zero-day ».

Cependant, en raison de leur dépendance excessive envers les filtres, les règles et les politiques, les passerelles ne permettent pas de prévenir les attaques de messagerie hautement ciblées utilisant des tactiques d'ingénierie sociale, telles que le spear phishing et les attaques BEC. Les passerelles recherchent des signes de contenus ou d'expéditeurs malveillants, mais elles ne bloquent pas les attaques qui n'activent pas leurs politiques, filtres ou règles d'authentification prédéterminés.

Protection des boîtes de réception par API

Les passerelles de messagerie restent nécessaires, mais ne suffisent plus pour assurer une protection efficace contre les menaces de cybersécurité en constante évolution. Pour protéger votre organisation contre les attaques d'ingénierie sociale, vous avez besoin d'une couche de protection supplémentaire au-delà de la passerelle, au niveau des boîtes de réception.

La protection des boîtes de réception repose sur des API, qui s'intègrent directement à l'environnement de messagerie, y compris les boîtes de réception individuelles. L'intégration des API fournit une visibilité sur les communications internes et l'historique de messagerie de chaque individu au sein de

« Améliorez vos solutions de passerelle de sécurité de messagerie pour y inclure une protection avancée contre le phishing, la détection des imposteurs et une protection de messagerie interne. »

Gartner : Comment élaborer une architecture de sécurité de messagerie efficace (mars 2020)

Barracuda

l'organisation. Elle utilise ensuite ces données de communication et l'intelligence artificielle pour créer un modèle d'identité propre à chaque utilisateur qui reflète ses schémas de communication.

Ce modèle d'identité est élaboré à l'aide de nombreux classificateurs qui déterminent ce à quoi ressemblent les communications par e-mail normales pour chaque employé. Par exemple, il détermine (d'après l'historique de données) dans quels lieux chaque employé est susceptible de se connecter, les adresses e-mail qu'il utilise régulièrement, les individus avec lesquels il communique, le type de demandes qu'il effectue ainsi que des centaines d'autres signaux. Lorsqu'un événement suspect ne correspondant pas au modèle d'identité d'un individu est détecté, l'IA de la protection des boîtes de réception le signale comme étant potentiellement malveillant et le supprime de la boîte de réception de l'utilisateur avant que ce dernier ne puisse interagir avec le message.

Certaines passerelles de messagerie peuvent se comporter d'une manière similaire, mais avec une efficacité moindre. Nombre des passerelles de messagerie actuelles permettent de bloquer les attaques ciblées grâce à la personnalisation granulaire et au paramétrage des politiques. Chaque classificateur peut potentiellement être transformé en règle ou en politique, mais cette solution n'est pas adaptée car il faudrait mettre en place des centaines de politiques pour des milliers d'employés. Cette méthode n'est pas évolutive et elle est susceptible d'engendrer un grand nombre de faux positifs comme négatifs. Les organisations qui s'appuient sur des passerelles personnalisées pour protéger leurs utilisateurs contre les attaques de spear phishing ne sont en réalité en mesure de protéger qu'un certain nombre d'employés, identifiés comme à haut risque. Inévitablement, les attaques de spear phishing contourneront leurs passerelles pour atteindre les boîtes de réception de leurs utilisateurs.

Taxonomie des attaques par e-mail - 13 types d'attaques

TYPE D'ATTAQUE	PASSERELLE DE MESSAGERIE	PROTECTION DES BOÎTES DE RÉCEPTION PAR API
Spam	●	○
Malwares	●	○
Exfiltration de données	●	○
Phishing par URL	◑	●
Arnaques	◑	●
Spear phishing	○	●
Usurpation de nom de domaine	○	●
Usurpation de service	○	●
Chantage	◑	◑
Attaques BEC	○	●
Détournement de conversation	○	●
Phishing latéral	○	●
Piratage de compte	○	●

○ N'offre pas une protection suffisante ◑ Offre une protection suffisante ● Offre une protection optimale

Barracuda

Conclusion : Se protéger efficacement contre des attaques par e-mail en constante évolution

Les attaques par e-mail ont évolué et sont désormais capables de contourner les défenses traditionnelles ; il est donc essentiel de mettre en place une protection au niveau de la passerelle, mais également au-delà. Toutes les entreprises doivent déployer la bonne combinaison de technologies et d'individus pour protéger efficacement leur messagerie.

Bloquer le maximum d'attaques au niveau de la passerelle

Les passerelles constituent les fondements essentiels de la sécurité de la messagerie. Elles bloquent la plupart des messages malveillants, notamment les spams, les attaques de phishing de grande envergure, les malwares, les virus et les attaques « zero-day ». Mais lorsqu'elles ne sont pas contrôlées, ces attaques font de véritables ravages, en impactant la productivité et en infectant les machines.

Protéger les utilisateurs au niveau des boîtes de réception

Les passerelles sont importantes, mais elles ne sont plus suffisantes. Déployer une protection des boîtes de réception par API permet d'accéder aux historiques de messagerie et aux e-mails internes, ce qui est nécessaire pour protéger les utilisateurs contre des attaques extrêmement ciblées capables de contourner les passerelles.

Informer les utilisateurs sur les menaces actuelles

Certaines attaques de phishing sophistiquées, et notamment celles qui utilisent des tactiques d'ingénierie sociale, sont capables de contourner les passerelles de sécurité de la messagerie. Protégez-vous de ces types de menaces en sensibilisant vos employés. Grâce à une simulation et à une formation continue, ils seront à même de reconnaître et de signaler les contenus malveillants, et constitueront ainsi une véritable couche de défense.

Barracuda
Your journey, secured.

Analysez votre environnement Office 365. C'est rapide, gratuit et sûr avec **Barracuda Email Threat Scanner**.