LIVRE BLANC

CLOUDFLARE
AREA 1 SECURITY

Arrêter les menaces BEC

Techniques avancées de lutte contre la fraude et le phishing

Présentation

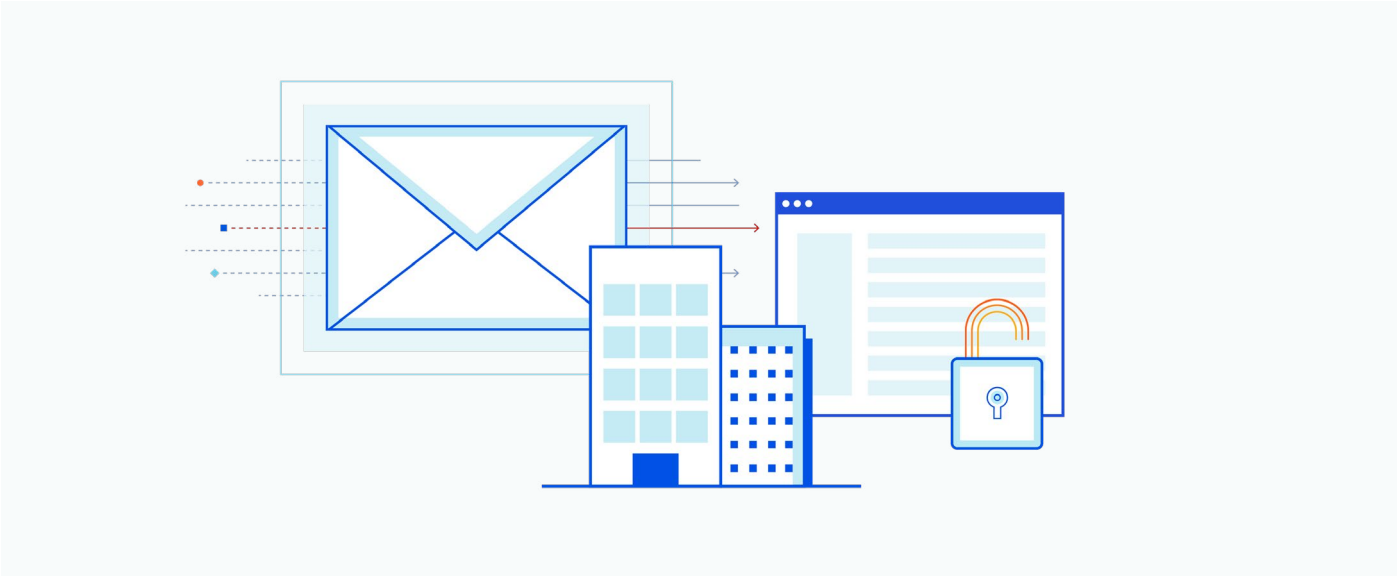
Les attaques BEC (Business Email Compromise, compromission du courrier électronique professionnel) désignent une forme spécifique d'attaques par phishing motivées par l'appât du gain. Elles reposent sur l'exploitation d'une relation existante entre une victime et une entreprise. Dans notre troisième mise à jour annuelle relative à la situation et à l'évolution des attaques BEC, nous constatons que ces dernières demeurent le type de cyberattaque le plus coûteux, avec des dégâts chiffrés en millions. Les conséquences financières surpassent même les coûts signalés pour les attaques par rançongiciel.

Le terme BEC bénéficie d'une reconnaissance suffisamment large dans de nombreux secteurs à l'heure actuelle. Nous pouvons donc nous passer d'effectuer une description détaillée des différents types d'attaques BEC dans ce rapport. (Pour les intéressés, nous avons déjà décrit les différents types d'attaques BEC dans notre e-book précédent, « BEC in 2021: Supply Chain-Based Phishing Attacks on the Rise » [Les attaques BEC en 2021 : l'essor des attaques par phishing basées sur la chaîne d'approvisionnement].) Les autorités ont également fait des progrès en matière de traduction des auteurs d'attaques BEC en justice. Plusieurs criminels liés à des cercles internationaux spécialisés dans les attaques BEC ont été appréhendés récemment, notamment des participants à une opération de blanchiment de 10 millions de dollars et SilverTerrier, un vaste gang de cybercriminels qui a amassé plus de 800 000 mots de passe volés auprès de 50 000 victimes.

Le principe de phishing est connu de l'opinion publique depuis de nombreuses années. Pourtant, les attaques BEC (qui vont de l'attaque ridiculement simpliste aux « escroqueries à durée étendue », étayées par un travail de recherche conséquent) continuent d'échapper aux systèmes de sécurité et d'atteindre leurs victimes.

Pourquoi ? Ce constat résulte en grande partie de la nature des attaques BEC et des techniques employées par les acteurs malveillants, qui restent en évolution constante même à ce jour. Nous avons déjà signalé le cas de pirates cherchant à piéger leurs victimes en exploitant de manière abusive la disponibilité du vaccin contre la COVID-19 et d'autres événements fortement liés au facteur temps. La relative facilité, le faible coût d'exécution et la rentabilité constituent également des facteurs attractifs pour les gangs de cybercriminels, notamment les groupes de pirates relevant de certains pays qui cherchent à « élargir leurs horizons ».

Poursuivez la lecture pour en savoir plus sur la situation actuelle des attaques BEC et la manière de les arrêter efficacement.



Les attaques BEC sont tout aussi nuisibles que les rançongiciels (si ce n'est plus)

Si les ahurissantes demandes émises dans le cadre d'attaques par rançongiciel tendent à accaparer les gros titres, les attaques BEC constituent l'une des formes de cybercriminalité les plus dévastatrices sur le plan financier d'après le FBI, avec plus de deux milliards de dollars de pertes déclarées.

Or, les entreprises ont tendance à sous-estimer la gravité de ces dernières, notamment du fait que la plupart d'entre elles omettent de signaler les incidents liés aux attaques BEC. De plus, contrairement aux attaques par rançongiciel, dans lesquelles l'attaque en elle-même s'avère particulièrement évidente, certaines entreprises pourraient tout à fait ne pas avoir conscience d'être victimes d'une fraude BEC avant de faire l'objet d'un audit ou d'en avoir été notifiées par un tiers. Après tout, les transferts financiers effectués dans le cadre d'une manœuvre BEC sont généralement approuvés par un collaborateur légitime de l'entreprise !

Malgré ce manque de signalements, les attaques BEC sont la deuxième forme la plus courante d'attaques par ingénierie sociale d'après le 2021 Verizon Data Breach Investigations Report2 (rapport de l'enquête Verizon 2021 sur les violations de données), avec 95 % des pertes financières comprises entre 250 et 984 000 USD par incident.

Nos propres données, compilées dans le rapport 2021 sur les menaces véhiculées par e-mail, montrent que la demande moyenne effectuée dans le cadre d'une attaque BEC s'élève à 1,5 million de dollars, avec une médiane estimée à 260 000 USD.

Si les BEC ne représentent que 1,3 % des attaques, le fait que de nombreux outils de sécurité traditionnels échouent aussi facilement à les détecter peut impliquer de sérieuses conséquences financières. En 2021, Area 1 Security (une entreprise acquise par Cloudflare) a identifié et arrêté près de cinq millions d'attaques BEC (4 987 526), dont bon nombre avaient été négligées par les outils traditionnels que sont les passerelles de messagerie sécurisées et les suites de sécurité des e-mails basées sur le cloud.

Demande moyenne effectuée dans le cadre d'une attaque BEC = 1,5 million

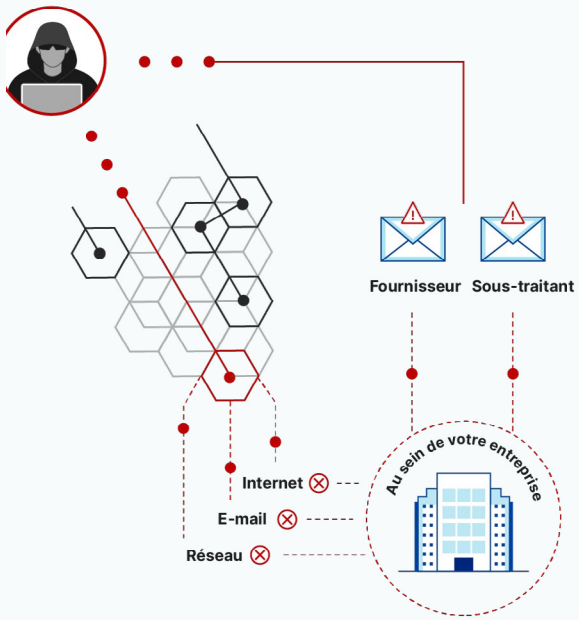
En 2021, Area 1 Security a identifié et arrêté près de 5 millions d'attaques BEC

[1] https://www.ic3.gov/Media/Y2020/PSA200406
[2] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/

Les attaques BEC « les plus sévères »

Vous trouverez ci-dessous quelques-unes des plus (tristement) célèbres attaques BEC conduites contre des marques de premier plan et ayant entraîné des pertes chiffrées en millions.

Victime	Pertes	Année	Que s'est-il passé ?
Facebook et Google	123 millions de dollars	2019	Un escroc lituanien s'est fait passer pour Quanta Computer, un fournisseur de matériel électronique pour Facebook et Google. Facebook et Google ont versé 123 millions de dollars à l'escroc sous forme de règlements de fausses factures.
Banque Crelan	75,8 millions de dollars	2016	La banque belge Crelan a perdu plus de 70 millions d'euros (environ 75,8 millions de dollars) du fait de fraudeurs qui avaient compromis le compte e-mail de son PDG. L'attaque n'a été découverte que plus tard, au cours d'un audit interne.
Filiale de Toyota	37 millions de dollars	2019	Une filiale européenne de la Toyota Boshoku Corporation (filiale de Toyota Group) a été amenée à transférer 4 milliards de yens (approximativement 37 millions de dollars) dans le cadre d'une fraude BEC.
Scoular	17,2 millions de dollars	2014	Scoular, une entreprise américaine de négociation de matières premières, a viré 17,2 millions de dollars vers un compte offshore frauduleux après la réception d'un faux e-mail de la part du PDG de l'entreprise.
Mattel	3 millions de dollars (récupérés)	2016	Un cadre financier de Mattel a transféré 3 millions de dollars vers un compte frauduleux après avoir reçu un e-mail usurpé semblant provenir du PDG.



Pourquoi les attaques BEC connaissent-elles toujours autant de succès ?

Les attaques BEC peuvent se révéler notoirement difficiles à détecter et donc à arrêter. Ces attaques s'appuient sur l'authenticité et sur une profonde compréhension des comportements et des procédures commerciales de la cible. Ces connaissances s'étendent également à la compromission des partenaires et de la chaîne d'approvisionnement de cette dernière. Les autres solutions de sécurité des e-mails, dont les fournisseurs de courrier électronique dans le cloud et les passerelles de messagerie sécurisées, sont incapables d'identifier avec précision ces e-mails comme des messages malveillants. Vous trouverez plus d'informations sur la manière dont les pirates « pêchent à l'aide du cloud » (rapport « Phishing with the Cloud ») ici.

Les quatre raisons principales pour lesquelles les victimes se font piéger par les attaques BEC

01

Les attaques BEC s'appuient sur l'ingénierie sociale plutôt que sur des logiciels malveillants.

Plutôt que d'inclure des liens malveillants ou des pièces jointes « militarisées », les BEC se présentent généralement sous la forme de messages courts et uniquement textuels. Ce type d'attaque se repose sur notre tendance à respecter l'étiquette sociale (en aidant un collègue par exemple) ou les logiques de pouvoir (comme le fait de répondre à une demande urgente provenant d'un dirigeant) pour duper les victimes et les amener à envoyer de l'argent vers des comptes frauduleux.

Les outils traditionnels de sécurité des e-mails fondés sur l'analyse des liens malveillants ou des pièces jointes à la recherche de signatures connues manqueront immanquablement les BEC.

02

Les acteurs malveillants font appel à des domaines légitimes.

Grâce aux fournisseurs de courrier électronique dans le cloud, tout le monde peut bénéficier d'un domaine e-mail légitime, facilement et de manière peu onéreuse. Les pirates tirent régulièrement avantage d'un domaine Gmail gratuit ou à faible coût pour envoyer des e-mails de phishing, par exemple. L'achat d'un domaine légitime « sosie », c'est-à-dire ressemblant fortement au domaine de la cible, constitue également une tâche triviale pour un acteur malveillant.

En utilisant des domaines légitimes et/ou nouvellement créés, les e-mails de phishing peuvent passer les vérifications d'authenticité Les solutions qui se fondent uniquement sur la réputation du domaine pour déterminer le caractère malveillant d'un message peuvent également manquer ces attaques BEC.

03

Les attaques BEC affichent un faible volume, mais sont hautement ciblées.

Notre rapport 2021 sur les menaces véhiculées par e-mail montre que les BEC ne représentent que 1,3 % des attaques et un pourcentage encore plus faible du volume d'e-mails total. Ces attaques se révèlent toutefois extrêmement ciblées. Les pirates effectuent des recherches sur leurs cibles et les destinataires prévus afin de concevoir des messages d'apparence personnelle et légitime.

Les outils de sécurité qui s'appuient sur la comparaison des messages avec une base de référence détaillant l'aspect des messages « normaux » (c'est-à-dire bénins), ou qui nécessitent un plus haut volume de menaces pour créer une signature, ne parviendront pas à détecter les BEC avec précision.

04

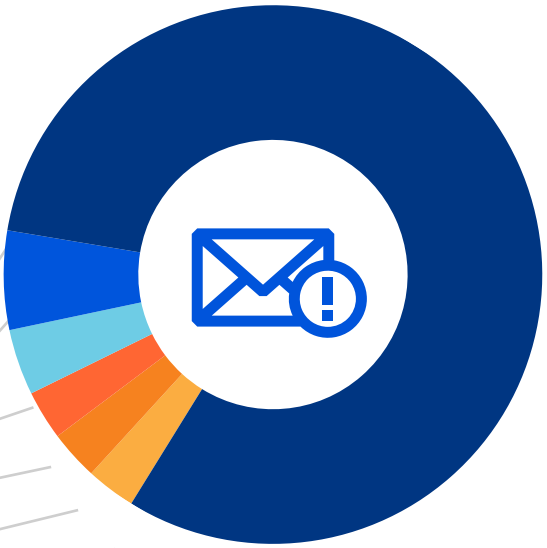
Les victimes n'ont généralement pas conscience de l'usurpation de leur compte ou de la compromission de leurs identifiants.

Les attaques BEC de type 4, telles que définies dans le rapport « Protecting Against Business Email Compromise Phishing » (Se protéger contre les attaques par phishing visant à compromettre le courrier électronique professionnel) de Gartner, constituent le type de BEC le plus sophistiqué. Elles tirent souvent avantage des situations d'usurpation de compte, dans lesquelles un acteur malveillant a détourné le compte d'un utilisateur légitime. Le pirate épie alors silencieusement le flux des fils d'e-mails (parfois pendant plusieurs mois) avant de s'insérer au sein de la conversation à un moment critique, dans l'optique de détourner un paiement.

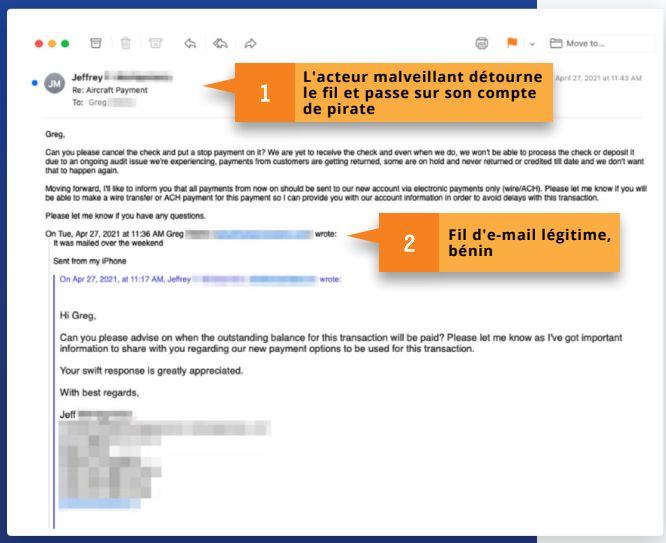
Seules les techniques de détection avancées reposant sur l'analyse contextuelle peuvent repérer ces attaques sophistiquées construites autour de la compromission du fournisseur.

Principales cibles des attaques BEC

Voici les principaux secteurs observés par Area 1 comme ayant été la cible d'attaques BEC en 2021.



- Services de réparation et de maintenance | 87,65 %
- Services non gouvernementaux | 3,8 %
- Fabrication de savon et de composés nettoyants | 2,09 %
- Autres entreprises du secteur manufacturier | 1,74 %
- Commerce de détail | 1,31 %
- Tous les autres secteurs



À quoi ressemble une attaque BEC sophistiquée de type 4 ?

Une tentative de fraude BEC de plus de 4 millions de dollars

Cette attaque s'appuie sur l'usurpation du compte d'un partenaire pour détourner un fil de conversation légitime et bénin avant de faire pivoter cette dernière vers le compte du pirate.

Ce dernier compromet le compte d'un partenaire (« Jeffrey »), avant de détourner le fil. En envoyant son message depuis un domaine malveillant « ressemblant » au domaine de l'expéditeur, l'auteur de l'attaque bascule le fil vers son compte de pirate. Le domaine ressemblant est identique au domaine de l'expéditeur, si ce n'est qu'il se termine en .co plutôt qu'en .com.

Cette attaque fait appel à l'ensemble des quatre « facteurs de réussite d'une attaque BEC » détaillés ci-dessus.

Quatre techniques permettant d'arrêter les attaques BEC

Si certaines attaques BEC peuvent être repérées par des destinataires attentifs, la plupart des BEC sophistiquées (celles qui peuvent entraîner de considérables pertes financières) nécessitent généralement l'œil de professionnels formés et des solutions avancées de détection du phishing. Les moindres variations des détails ont leur importance, en particulier pour les BEC qui impliquent l'usurpation de comptes de partenaires, car l'acteur malveillant disposent déjà des identifiants et des privilèges adéquats.

01

Analyse des sentiments

L'examen du contenu du message ne suffit pas. La détection efficace des BEC nécessite d'examiner l'intention elle-même derrière ce dernier. Plusieurs éléments doivent être pris en compte, comme le ton du message, la ou les relations entre l'expéditeur et le ou les destinataires, ainsi que les liens hiérarchiques.

02

Remontées des verdicts de fraude active

Dans les attaques BEC sophistiquées de type 4, la plupart des messages d'une conversation sont de nature bénigne. La seule menace provient de l'acteur malveillant qui se glisse au sein du fil afin de détourner un paiement. Une solution efficace de détection des BEC doit inclure un moyen de faire remonter l'information et de prévenir de la présence de potentielles communications frauduleuses en temps réel. Le blocage/la mise en quarantaine/ la suppression automatique des messages malveillants, de même que le lancement d'une procédure d'examen, peut empêcher un éventuel transfert de fonds.

03

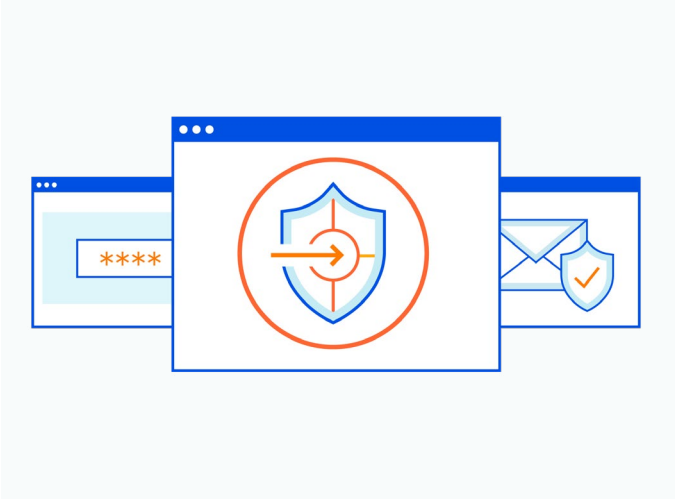
Analyse des fils et des conversations

À l'instar de l'analyse des sentiments, l'analyse des fils et des conversations examine l'intention et les relations exprimées sur des fils entiers. Les nuances, comme la variation de ton et de longueur des messages au sein d'un fil, peut indiquer que l'expéditeur n'est pas celui qu'il prétend être. Il peut s'agir là d'un signe d'usurpation de compte ou de détournement d'une conversation par un acteur malveillant.

04

Graphiques de confiance de l'expéditeur

Les graphiques sociaux sont importants pour détecter les BEC, particulièrement les attaques basées sur la chaîne d'approvisionnement, car ils peuvent servir à dresser une carte des expositions aux risques et des liens de confiance. Cet aspect s'avère essentiel pour découvrir les cas d'usurpation de comptes et d'usurpation d'identité de partenaires dans lesquels l'expéditeur est un individu « de confiance » travaillant en dehors de votre entreprise. Les techniques avancées de détection des BEC analysent également les graphiques sociaux et l'historique d'expédition des partenaires.



Étendre les principes Zero Trust aux e-mails

Tandis que les entreprises cherchent à adopter les derniers principes de sécurité et les nouvelles architectures réseau, comme le Zero Trust, la sécurité des e-mails constitue une faille considérable. Dans cet e-book, nous avons vu comment les acteurs malveillants dérobent de l'argent et des données simplement « en le demandant » à un moment opportun. Les attaques BEC n'ont pas besoin de faire appel à des logiciels malveillants ou à des modèles d'intrusion sophistiqués pour réussir. Il leur suffit d'exploiter la confiance implicite résidant dans les communications par e-mail.

Maintenant qu'Area 1 fait partie de l'offre Cloudflare, les clients bénéficieront d'une solution Zero Trust complète couvrant également l'application SaaS la plus utilisée et la plus attaquée de nos jours : le service de courrier électronique.

Découvrez comment Area 1 contribue à étendre les principes Zero Trust au courrier électronique :

Toujours supposer la possibilité d'une violation

Area 1 présume à raison que de nouvelles campagnes de phishing sont mises sur pied en permanence. En s'appuyant sur son système d'indexation du phishing à grande échelle, Area 1 sonde le réseau Internet à la recherche d'infrastructures employées par les acteurs malveillants et bloque de manière proactive les attaques par phishing plusieurs jours avant qu'elles n'atteignent la boîte de réception de la cible.

Ne jamais accorder sa confiance

Le courrier électronique constitue une porte ouverte capable de compromettre même les architectures réseau Zero Trust les plus blindées. La solution Area 1 n'accorde pas de confiance aux e-mails uniquement du fait qu'ils disposent d'une authentification, sont issus de domaines réputés ou s'appuient sur un historique de communication préalable avec la cible potentielle. En réalité, les attaques BEC ont bien plus de chances de provenir d'infrastructures et d'expéditeurs évalués comme « de confiance » par des mesures de sécurité déterministes.

Toujours vérifier

L'un des principes fondamentaux du Zero Trust consiste à continuellement vérifier chaque requête et chaque utilisateur, même au sein du réseau de l'entreprise. Area 1 permet de déployer plusieurs couches de protection avant, pendant et après l'arrivée d'un e-mail dans la boîte de réception. Tous les types de communications (externes, internes, issues de partenaires de confiance) sont analysés avec la même assiduité. Grâce à l'intégration d'Area 1 à la solution d'isolation de navigateur à distance Cloudflare, les utilisateurs sont protégés contre les campagnes d'attaques différées (c'est-à-dire, des attaques au cours desquelles des liens bénins pivotent vers une infrastructure contrôlée par un acteur malveillant après la réception de l'e-mail infecté).

Comprendre (et partager) le contexte des menaces véhiculées par e-mail

Une plateforme de courrier électronique diffère de toutes les autres applications SaaS du fait du vaste ensemble de signaux « incertains » qu'elle génère, comme le contenu, le ton et l'intention d'un e-mail, les variations inattendues au sein des fils d'e-mails, de même que la relation entre l'expéditeur et le destinataire. Area 1 s'appuie sur un outil d'analyse contextuelle sophistiqué pour évaluer et peser l'ensemble de ces signaux afin d'identifier les attaques extrêmement ciblées en cours et de protéger les utilisateurs sur l'application SaaS la plus utilisée (et la plus différente).

En outre, l'échange croisé des informations sur les menaces générées par Area 1 à partir des milliards de requêtes DNS observées quotidiennement sur le réseau Cloudflare permettra de mieux protéger les clients contre les menaces circulant sur Internet.

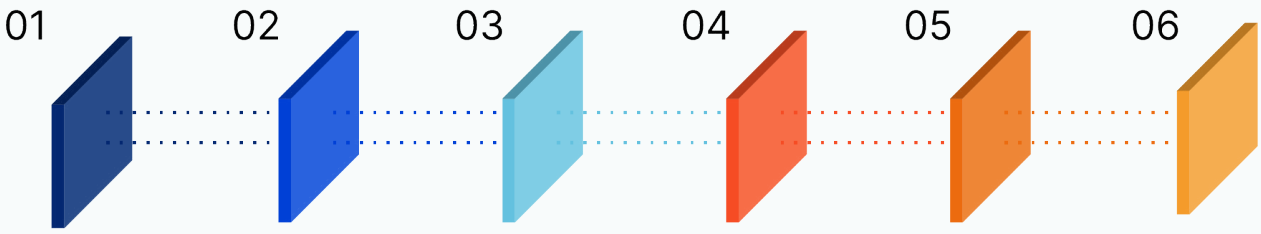
Et ensuite ?

La compromission du courrier électronique professionnel d'une seule entreprise peut lui coûter des millions en pertes directes. Difficiles à identifier par les outils de sécurité traditionnels, les attaques BEC peuvent être arrêtées de manière efficace par les solutions de sécurité des e-mails reposant sur l'utilisation de techniques de détection avancées.

La solution Area 1 s'est toujours concentrée sur le blocage des attaques par phishing (le plus vaste vecteur unique de cybermenaces à l'heure actuelle), notamment les attaques BEC. Notre plateforme de sécurité des e-mails native du cloud s'appuie sur un algorithme d'analyse contextuelle sophistiqué pour détecter tous les types de BEC avant qu'elles ne puissent causer des dégâts.

Techniques avancées de détection et de blocage des BEC

Nous faisons appel à diverses technologies propriétaires pour détecter une gamme complète d'attaques avancées, dont les attaques BEC. Notre solution à l'échelle du cloud s'intègre aux entreprises de toutes tailles et prend en charge leurs spécificités.



Analyse structurelle
En-têtes
Corps, images
Interprétation de données visuelles
Liens, contenu

Modélisation NLU
(Natural Language Understanding)
Schémas d'écriture
Catégories
Expressions

Analyse des sentiments
Intention, ton, relation, hiérarchie

Analyse des fils
Conversations
Variations
Durée

Modélisation du secteur
Verticales
Lingua franca
Processus commerciaux

Graphiques de confiance
Graphiques de confiance des partenaires
Historique d'expédition
Recherche des usurpations de compte
Usurpation d'identité des partenaires

Pour découvrir comment nous détectons et arrêtons les attaques BEC sophistiquées, n'hésitez pas à demander une démo.