Cinq mesures pour lutter contre le piratage de la messagerie en entreprise

Principaux avantages

- Détection et blocage des variantes BEC couvrant de nombreuses tactiques utilisées par les cybercriminels
- Visibilité sur les utilisateurs les plus attaqués et les tiers présentant le plus grand risque d'attaque
- Réception de notifications lorsque les fournisseurs avec qui vous interagissez disposent de comptes potentiellement compromis
- Formation des utilisateurs à l'identification et au signalement des fraudes par email
- Accélération de la réponse aux menaces et gain de temps grâce à l'automatisation de la correction
- Renforcement de la sécurité et de l'efficacité opérationnelle grâce à une solution intégrée de bout en bout

Le piratage de la messagerie en entreprise (BEC, Business Email Compromise) contribue grandement aux pertes financières. D'après le rapport Internet Crime Report du FBI, les pertes annuelles dues aux attaques BEC sont supérieures à 2,7 milliards de dollars, soit 80 fois plus que celles imputables aux ransomwares[1].

Les attaques BEC usurpent souvent l'identité des expéditeurs dans des emails qui tentent de faire croire aux destinataires qu'ils interagissent avec une source de confiance. Les cybercriminels exploitent ensuite cette confiance pour inciter les destinataires à effectuer un virement bancaire frauduleux, par exemple. Il est difficile de se défendre contre de telles attaques, car elles n'ont pas recours à des charges virales malveillantes. Certains cybercriminels vont encore plus loin et utilisent des comptes fournisseur légitimes mais compromis pour lancer leurs attaques BEC.

La protection de votre entreprise contre les attaques BEC requiert à la fois des technologies et des formations. Vous avez besoin d'une approche plus globale pour briser véritablement la chaîne d'attaque des compromissions par email. Proofpoint peut vous aider.

Proofpoint est le premier et le seul fournisseur proposant une plate-forme complète et intégrée de protection contre les menaces qui offre les avantages suivants :

- Détection et blocage des menaces BEC avant qu'elles n'atteignent les boîtes de réception
- Formation des utilisateurs à la détection et au signalement des attaques BEC
- Visibilité sur les risques associés aux fournisseurs et les comptes tiers compromis
- Automatisation de la détection et de la neutralisation des menaces
- Protection de votre marque face aux fraudes par email

Cette fiche solution décrit notre approche plus en détail.

1 *Internet Crime Report*, FBI, 2022.

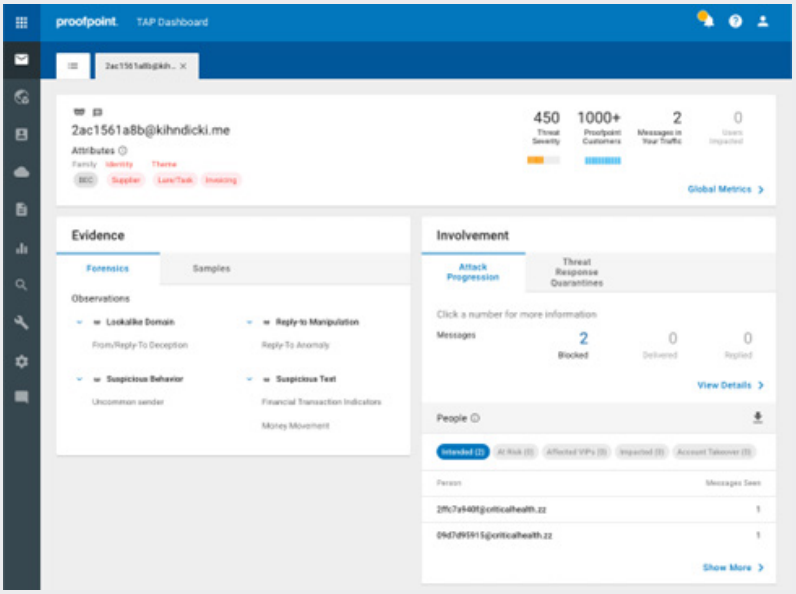

Figure 1. Proofpoint identifie les utilisateurs les plus ciblés par des attaques BEC et offre une visibilité granulaire sur les détails des menaces BEC, y compris les thèmes, les tactiques employées, etc.

Détection et blocage des menaces d'imposteurs avant qu'elles n'infiltrent votre environnement

Notre plate-forme intégrée s'appuie sur Proofpoint Advanced BEC Defense, qui est alimenté par Supernova, notre dernier moteur de détection des attaques BEC basé sur l'intelligence artificielle (IA). Cette technologie de pointe a permis de multiplier par 17 le nombre de menaces identifiées et d'étendre notre capacité de détection à un large éventail de fraudes par email.

Proofpoint Advanced BEC Defense procède à une analyse approfondie de plusieurs attributs des messages, dont les suivants :

- Données d'en-tête du message
- Adresse IP de l'expéditeur
- Relation entre l'expéditeur et le destinataire
- Réputation de l'expéditeur

Proofpoint Advanced BEC Defense a recours à une analyse sémantique basée sur de grands modèles de langage pour analyser le corps du message (ressenti et langage), ce qui permet de déterminer si le message constitue une menace BEC. Le moteur d'apprentissage automatique comportemental suit les activités pour extraire des indicateurs comportementaux, ou signatures de menaces, afin de comprendre les modèles qui seront ensuite utilisés pour détecter les anomalies en temps réel.

Voici certains des éléments suivis :

- Si un expéditeur envoie un nombre inhabituel d'emails
- Si des emails proviennent d'une adresse IP inhabituelle
- Si un expéditeur a déjà été rencontré par les utilisateurs de l'entreprise

Ces signaux renforcent la pile de détection et permettent de prendre en charge de nouveaux cas de figure. Par conséquent, le moteur de détection intercepte désormais d'autres menaces avancées véhiculées par email, comme les ransomwares, le phishing d'identifiants de connexion et les comptes tiers compromis.

Proofpoint Advanced BEC Defense détecte l'usurpation du nom d'affichage et les domaines similaires. Il bloque même les fraudes aux fournisseurs les plus sophistiquées grâce à une analyse dynamique des messages capable de déceler les tactiques associées à la fraude à la facturation fournisseurs. Il s'appuie sur l'apprentissage automatique pour s'adapter et apprendre en temps réel, et vise de faibles taux de faux positifs.

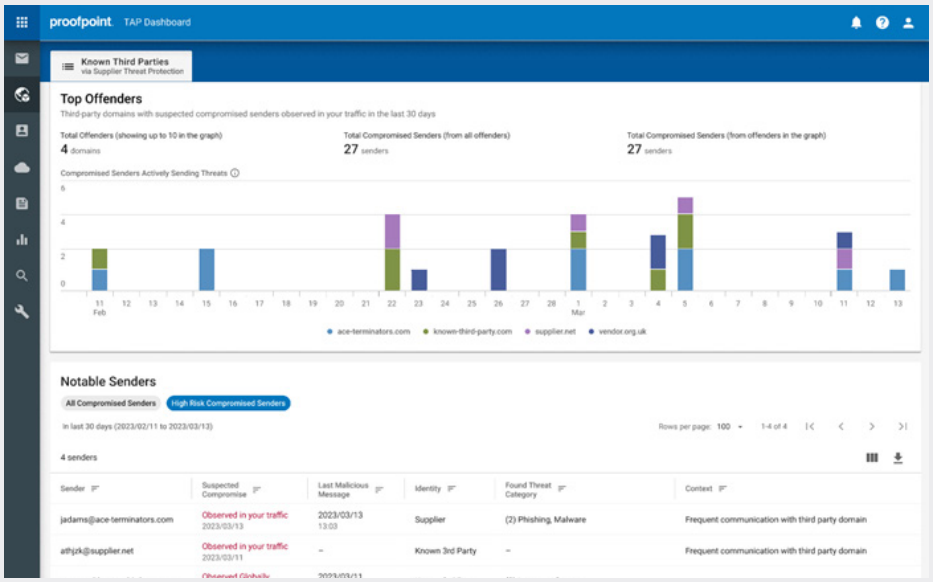

Figure 2. Le module complémentaire Proofpoint Supplier Threat Protection détecte les comptes tiers compromis avec lesquels votre entreprise interagit.

Visibilité sur les risques d'attaques BEC

Pour mieux comprendre, communiquer et réduire les risques d'attaques BEC auxquels vous êtes exposé, nous vous aidons à répondre aux questions suivantes pouvant émaner de votre direction :

- Quels sont les risques d'attaques BEC auxquels nous sommes exposés ?
- Quels sont les utilisateurs les plus ciblés ?
- Quels tiers de confiance disposent de comptes potentiellement compromis ?
- Comment pouvons-nous quantifier et réduire les risques ?

Proofpoint peut identifier vos utilisateurs les plus attaqués et ceux qui sont les plus susceptibles de tomber dans le piège de menaces d'imposteurs. Nous vous offrons une visibilité granulaire sur les détails des menaces BEC, en vous indiquant les thèmes dont vous devez vous méfier : escroqueries aux cartes cadeaux, fraude à la facturation fournisseurs, détournement de salaires, etc. (voir la figure 1). Vous pouvez ensuite appliquer des contrôles de sécurité adaptatifs aux utilisateurs ciblés et mieux communiquer les risques à votre direction.

Proofpoint étend votre protection en vous offrant une visibilité et des informations exploitables sur les fournisseurs à risque. Nous vous aidons à gérer les risques et menaces associés aux fournisseurs grâce aux avantages suivants :

- Identification proactive des comptes fournisseur potentiellement usurpés et compromis
- Vue des menaces BEC hiérarchisée et centrée sur les fournisseurs
- Identification et prévention des menaces émanant de domaines de fournisseurs ainsi que de domaines similaires malveillants

Nous évaluons et hiérarchisons le niveau de risque de ces domaines de fournisseurs et vous avertissons des comptes potentiellement compromis. Vos équipes de sécurité peuvent ainsi se concentrer sur les fournisseurs qui présentent le risque le plus élevé pour votre entreprise.

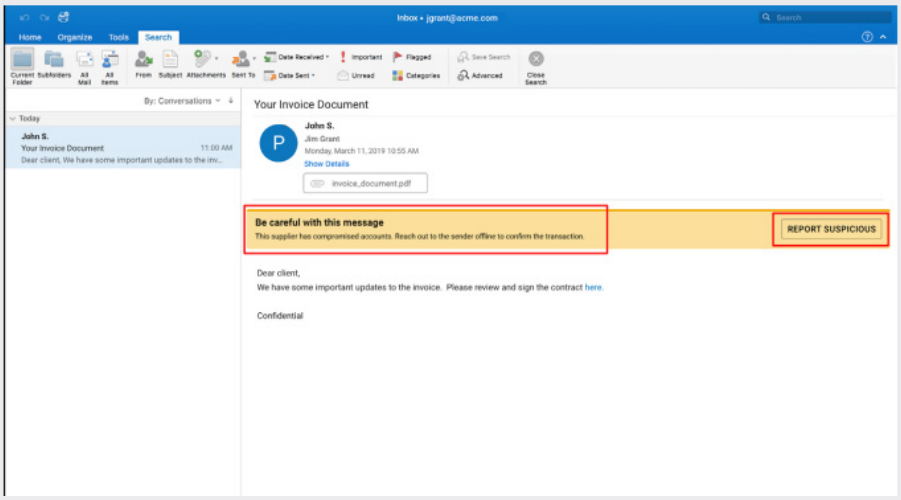

Figure 3. L'affichage d'avertissements en cas d'emails suspects met en garde vos utilisateurs et leur permet de prendre des décisions plus éclairées concernant les emails dont ils ne sont pas sûrs de la légitimité.

Renforcement de la résilience des utilisateurs face aux attaques BEC

Les attaques BEC ciblent des personnes et les incitent à exécuter des actions malveillantes contre leur gré. Étant donné que ces attaques d'imposteurs ont recours à l'ingénierie sociale et à l'usurpation d'identité, vos utilisateurs constituent souvent votre dernière ligne de défense. C'est la raison pour laquelle la réduction des risques d'attaques BEC requiert à la fois des technologies et des formations.

Grâce à notre bouton de signalement PhishAlarm, vous pouvez doter vos utilisateurs des connaissances et outils nécessaires pour identifier et signaler les emails suspects. L'affichage d'avertissements en cas d'emails suspects aide également les utilisateurs à prendre des décisions plus éclairées. Vous pouvez former les utilisateurs aux dernières tactiques d'attaque BEC et attribuer des formations ciblées à vos collaborateurs les plus attaqués. Vous pourrez ainsi renforcer leur résilience face aux attaques BEC.

Automatisation de la réponse aux menaces

De nombreuses entreprises sont confrontées à des pénuries de personnel au sein des équipes de sécurité informatique. Il est dès lors difficile d'identifier, d'analyser et de neutraliser des menaces BEC à l'échelle d'une entreprise. Nous plaçons l'automatisation au cœur des processus de détection et de neutralisation des menaces. Grâce à Proofpoint Threat Response Auto-Pull (TRAP), vous pouvez mettre en quarantaine ou supprimer rapidement tout email suspect ou indésirable en un seul clic. L'automatisation s'étend aux messages transférés ou reçus par d'autres utilisateurs, ainsi qu'aux emails reçus par d'autres clients de Proofpoint. Tout le monde profite ainsi des informations supplémentaires recueillies.

Nous simplifions également la gestion des boîtes email de signalement d'abus. Les emails signalés par les utilisateurs sont automatiquement analysés, et ceux identifiés comme malveillants peuvent être mis en quarantaine ou supprimés. Cela vous permet d'accélérer la réponse aux menaces et de réduire les tâches manuelles.

Protection de votre marque face aux fraudes par email

Dans le cas de l'usurpation de marque, les cybercriminels utilisent le nom et la marque de votre entreprise pour piéger vos clients et vos partenaires commerciaux et leur voler de l'argent. Proofpoint protège votre marque contre l'usurpation lors d'attaques BEC en empêchant l'envoi d'emails frauduleux via vos domaines de confiance. Nous authentifions également tous les messages envoyés par ou à votre entreprise. En rationalisant l'implémentation de l'authentification DMARC grâce à un workflow guidé et à des services managés, nous vous aidons à sécuriser vos domaines contre l'usurpation et nous bloquons toutes les tentatives d'envoi d'emails non autorisés à partir de vos domaines de confiance.

En outre, nous vous offrons une visibilité sur tous les emails envoyés via votre domaine, y compris les expéditeurs tiers de confiance. Nous identifions les domaines similaires aux vôtres. Nous détectons de façon dynamique les domaines récemment enregistrés usurpant l'identité de votre marque dans des attaques par email. Grâce à notre service Virtual Takedown, vous pouvez agir rapidement pour faire fermer ces sites.

Résumé

La fraude par email est à l'origine des plus grosses pertes financières. Dans un contexte de sophistication croissante des fraudeurs, les attaques BEC ont également évolué, jusqu'à inclure des fraudes aux fournisseurs complexes. Proofpoint est le premier et le seul fournisseur proposant une solution intégrée de bout en bout qui assure une protection efficace contre ces menaces émergentes.

Notre solution de protection contre les attaques BEC présente les avantages suivants :

- Détection et blocage de différents types d'attaques BEC
- Visibilité sur la surface d'attaque humaine et informations granulaires sur les menaces BEC
- Identification des fournisseurs qui présentent un risque et dont les comptes peuvent avoir été compromis
- Renforcement de la résilience des utilisateurs face aux attaques BEC
- Automatisation de l'investigation et de la réponse aux incidents
- Protection de votre marque face aux fraudes par email

Proofpoint vous permet de lutter plus rapidement, plus facilement et plus efficacement contre les attaques BEC.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 75 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0201-012-03-02 11/23