DOSSIER DE SOLUTION

CLOUDFLARE AREA 1 SECURITY

Cloudflare Area 1 PhishGuard : un démultiplicateur de puissance pour les RSSI et les équipes de sécurité

Sécurité gérée des e-mails, traque des menaces internes et défense contre la fraude

Le défi :

La détection des auteurs de menaces sophistiquées, spécialisés dans la compromission des adresses e-mail professionnelles (BEC)/la compromission des comptes de messagerie (BEC/EAC), les rançongiciels/l'extorsion et la compromission des postes de travail/réseaux, est une tâche extraordinairement difficile. Le phishing, premier vecteur de cyberattaques, est également coûteux et difficile à arrêter. Selon le FBI, les pertes en dollars divulguées dues à des attaques par BEC/EAC ont atteint 43 milliards de dollars dans le monde entre juin 2016 et décembre 2021[1].

Les États-nations recrutent également du personnel hautement qualifié pour obtenir des informations sensibles et/ou propriétaires par des méthodes très nuancées, conçues pour échapper à la détection et ne pas éveiller les soupçons. L'équipe de spécialistes des menaces internes de Cloudflare Area 1 possède des années d'expérience dans l'identification de ces activités.

Les augmentations ponctuelles du nombre d'e-mails suspects signalés par les utilisateurs sollicitent encore davantage les ressources de cybersécurité. La transition vers le télétravail a contraint les équipes de cybersécurité à traiter un nombre d'incidents jusqu'à deux fois plus élevé[2], et beaucoup ne disposent pas de ressources internes suffisantes pour surveiller (et gérer) de manière proactive les tentatives de fraude.

La solution Cloudflare Area 1 PhishGuard :

PhishGuard démultiplie immédiatement la puissance de votre équipe de sécurité et de votre SOC, afin de leur permettre de neutraliser les campagnes de phishing avant qu'elles ne causent des dégâts. Libérez du temps pour des cycles d'investigation de sécurité, accédez à des données pertinentes pour votre équipe de direction et bénéficiez d'informations précieuses sur les menaces avec PhishGuard.

Cloudflare Area 1 PhishGuard s'exécute dans votre environnement et sur votre infrastructure VAR/MSSP pour fournir des services intégraux, offrant les avantages suivants :

La sécurité gérée des e-mails fournit des ressources dédiées pour la gestion et le traitement exhaustifs des attaques ciblées et par phishing.

Le programme de protection contre les menaces internes s'appuie sur des modèles personnalisés multilingues d'apprentissage automatique et la détection pour surveiller les vols de propriété intellectuelle commandités par des États-nations, ciblant des opérations et des infrastructures.

La défense anti-fraude fournit des notifications et des réponses personnalisées en cas de fraude par compromission d'adresses e-mail professionnelles et de menaces internes, et assure la traque personnalisée des menaces en fonction de votre environnement de messagerie.

[1] FBI Alert Number I-050422-PSA. « Business Email Compromise: The $43 Billion Scam ». FBI Internet Crime Complaint Center, https://www.ic3.gov/Media/Y2022/PSA220504. Consulté le 19 mai 2022.

[2] Rogers, Kate and Spring, Betsy. « "We are outnumbered" – cybersecurity pros face a huge staffing shortage as attacks surge during the pandemic. » CNBC, https://www.cnbc.com/2020/09/05/cyber-security-workers-in-demand.html. Consulté le 25 mai 2022.

RÉV. : JUIN 2022

La fraude moderne par e-mail et la compromission des adresses e-mail professionnelles (BEC) – Un problème coûteux

Les défis modernes en matière de sécurité des e-mails

La fraude par e-mail

Les e-mails constituent le premier vecteur de fraude; la compromission d'adresses e-mail professionnelles (BEC) a, à elle seule, coûté plus de 43 milliards de dollars aux organisations

Tentatives de phishing manquées

Les outils existants de sécurité des e-mails et les suites de messagerie cloud ne détectent pas le phishing

Volumes élevés d'e-mails suspects signalés par les utilisateurs

La formation de sensibilisation à la sécurité entraîne une augmentation du nombre de signalements de phishing envoyés par les utilisateurs

Équipes SOC surchargées

Tous les signalements de phishing doivent être examinés, ce qui demande du temps et des ressources

Méthode de communication fondamentalement peu sûre, les e-mails représentent le principal vecteur par lequel est perpétrée la cyberfraude. Avec la popularité croissante des solutions de messagerie cloud, qui fournissent aux acteurs malveillants[3] une infrastructure à la fois prête à l'emploi, peu coûteuse et évolutive, le problème demeure un défi pour les professionnels de la sécurité.

Les programmes de sensibilisation à la sécurité, obligatoires dans certains secteurs de l'industrie, ont également formé les utilisateurs à signaler tous les e-mails suspects, ce qui a pour effet d'inonder les équipes SOC de signalements de tentatives de phishing et de messages de phishing réels. Tous les messages suspects signalés par les utilisateurs (ainsi que les tentatives de phishing légitimement malveillantes) doivent être examinés, entraînant un allongement des temps de réponse globaux et une saturation des files d'attente des SOC.

L'augmentation des tentatives de fraude par compromission des adresses e-mail professionnelles (par le biais de la compromission lente et méthodique de comptes (attaques BEC de type 3) et des attaques par phishing de la chaîne logistique (attaques BEC de type 4) ne fait qu'accroître le défi. Ces tentatives ne sont que rarement détectées par les passerelles de messagerie sécurisées existantes et les défenses des plateformes de messagerie cloud. Celles-ci doivent être détectées au début du cycle de vie de l'attaque, afin que des mesures puissent être prises avant que l'attaque ne cause des dommages.

La fraude par phishing diffusée par e-mail est une menace très répandue, qui n'épargne aucun secteur de l'industrie et dont la gestion nécessite l'intervention de tous. Cependant, les organisations de toute taille ne disposent souvent pas des ressources de sécurité nécessaires pour surveiller et arrêter les tentatives de fraude.

[3] Tung, Liam. « Microsoft disrupted this large cloud-based business email scam operation ». ZDNet. https://www.zdnet.com/article/microsoft-disrupted-this-large-cloud-based-business-email-scam-operation/. Consulté le 10 juin 2022.

L'approche de Cloudflare Area 1 PhishGuard

PhishGuard s'appuie sur l'approche préventive unique de Area 1 en matière de sécurité des e-mails, avec des services activement surveillés comprenant des notifications en cas de fraude, des notifications en cas de menaces internes et la traque proactive des menaces par e-mail.

PhishGuard met ses ressources et son expertise en matière de sécurité à la disposition de l'équipe de sécurité de votre entreprise, ainsi que des VAR et MSSP spécialistes de la cybersécurité.

Les services essentiels incluent notamment :

- Réponse gérée aux fraudes, signatures personnalisées pour votre environnement de messagerie, réponse aux menaces internes et traque proactive des menaces véhiculées par e-mail
- Notifications proactives en cas de fraude/ compromission d'adresses e-mail professionnelles, afin que votre organisation puisse réagir dès le début du cycle de vie de l'attaque
- Signalement, réponse et quarantaine gérés en cas de tentative de phishing pour la plateforme de sécurité des e-mails Area 1

Cloudflare Area 1 PhishGuard – Fonctionnalités et avantages

- **Signalements et réponse gérés en cas de tentative de phishing**
  Gérez les processus de signalement de tentatives de phishing, analysez les messages suspects et réagissez aux incidents directement dans l'environnement de messagerie du client
- **Notifications et réponse en cas de fraude active**
  Informez les clients en cas de communications frauduleuses potentielles, bloquez automatiquement les messages malveillants visant à compromettre les adresses e-mail professionnelles et rétractez les messages malveillants confirmés
- **Notifications et réponses en cas de menace interne**
  Diffusez des notifications en cas de menace interne et fournissez un rapport en cas d'activités nécessitant un examen approfondi
- **Surveillance active des services**
  Surveillance en temps réel de l'environnement de messagerie des clients
- **Signatures personnalisées**
  Créez des signatures de blocage personnalisées (par ex., signatures ML, YARA) reposant sur une analyse des menaces pour l'environnement des clients et accompagnez-les lors du déploiement
- **Traque des menaces véhiculées par e-mail**
  Examinez les environnements de messagerie des clients ; fournissez des indicateurs de compromission et des indicateurs spécifiques aux campagnes et identifier les attaques nouvelles ou inédites
- **Affectation d'un analyste de la sécurité**
  Affectation d'un analyste de la sécurité pour l'organisation du client, afin d'assurer un examen périodique des résultats
- **Affectation d'un responsable de compte technique**
  Affectation d'un responsable de compte technique pour les remontées clients et l'examen périodique des comptes clients

Dirigé par une équipe de chercheurs et d'analystes avec une expérience de la sécurité acquise auprès de la National Security Agency (NSA), du ministère de la Défense des États-Unis et d'éminentes sociétés de conseil en sécurité, PhishGuard ajoute des services de sécurité proactifs à notre technologie préventive de sécurité des e-mails.

Renforcez votre équipe de sécurité et protégez votre organisation contre la fraude avec le service PhishGuard de Cloudflare Area 1. Pour en savoir plus, contactez l'équipe responsable de votre compte ou écrivez à area1sales@cloudflare.com.