Attaque par spoofing avec lien

Darktrace a détecté une attaque par spoofing avec lien visant un établissement financier à Atlanta, minutieusement élaborée pour tromper le destinataire afin qu'il clique sur un lien malveillant.

L'auteur de la menace avait enregistré un domaine similaire à celui de l'entreprise cible, mais sans être identique. Il suffit pour cela de modifier légèrement le nom de l'entreprise tout en ayant un domaine qui ressemble à l'original : par exemple, une seule lettre du nom ou l'ajout d'un trait d'union dans le domaine.

L'auteur de la menace a pu pénétrer dans le flux des échanges d'e-mails. Une fois les échanges en place, l'attaquant exploite la confiance établie pour envoyer un e-mail contenant un lien malveillant.

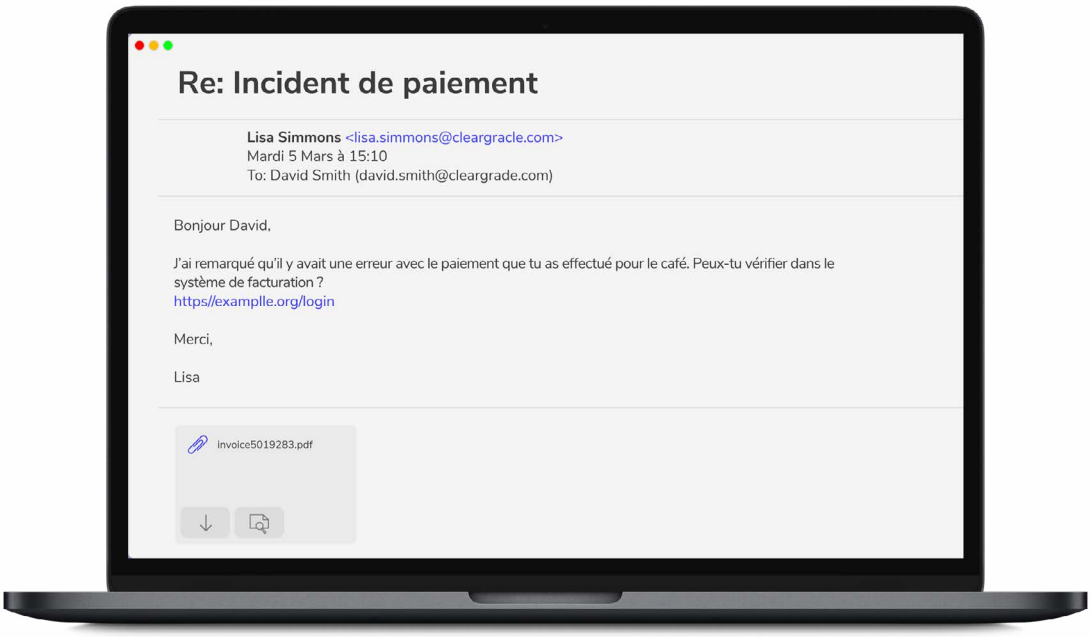

Figure 1: Un e-mail entrant contenant un lien vers un domaine usurpé.

Notez dans l'image d'un e-mail usurpé ci-dessus, l'orthographe incorrecte du mot « example ». Il s'agit d'un changement subtil qui n'est pas repéré par le destinataire qui clique sur le lien. L'utilisateur est alors dirigé vers un site web bien conçu qui réplique parfaitement la page de connexion de Example.org, amenant l'utilisateur à saisir ses informations d'identification. Elles sont ensuite récupérées par l'auteur de la menace qui peut utiliser les identifiants de la victime dans le système de paiement légitime.

Bloquer les attaques par spoofing avec lien

À la différence des autres solutions, Antigena Email et Immune System peuvent corréler des données issues du réseau, du Cloud et de la messagerie pour détecter si les domaines associées à un lien et à un expéditeur sont anormaux, si l'emplacement du lien contenu dans un e-mail est étrange ou si les modèles du chemin de l'URL sont suspects.

Grâce à cette approche fondamentalement unique, le processus décisionnel de Darktrace est considérablement plus précis que les autres outils, de sorte que notre solution est capable de prendre des mesures proportionnées et ciblées pour neutraliser les attaques d'hameçonnage à grande échelle.

Darktrace a non seulement reconnu la tentative d'usurpation d'identité en détectant le nom de domaine similaire, mais également en constatant que les e-mails violaient le modèle « No Association » : dans la compréhension globale de l'environnement réseau et e-mail de l'entreprise, la solution n'avait jamais constaté la preuve d'une relation préalable entre cet expéditeur et l'organisation.

Antigena Email a réagi de façon autonome pour neutraliser la menace en interdisant l'accès au lien. De plus, une bannière d'avertissement a été ajoutée pour informer l'utilisateur et l'équipe de sécurité de la menace potentielle. Immune System de Darktrace était prêt à prendre d'autres mesures si ce lien avait été envoyé à d'autres utilisateurs dans l'entreprise, empêchant la propagation de l'attaque.

En outre, le score d'exposition aux utilisateurs dont le compte avait été piraté était élevé, indiquant qu'il s'agissait de profils sensibles, ce qui viole le modèle « Whale Spoof ». En comprenant que des utilisateurs internes clés avaient été ciblés, l'IA de Darktrace a pu accorder la priorité à cette attaque en réagissant de façon proportionnée en temps réel.

Antigena Email : Ingénierie sociale et démarchage

Les attaques d'ingénierie sociale et par démarchage impliquent souvent une tentative sophistiquée d'usurpation d'identité, dans laquelle les attaquants déguisés incitent de toute urgence le destinataire à répondre, à accepter des communications hors ligne ou à réaliser des transactions hors ligne. L'objectif de ces attaques va de la fraude au transfert de fonds à l'espionnage d'entreprise, en passant par le vol de propriété intellectuelle. Même s'il est essentiel pour les entreprises d'investir dans la formation à la sécurité et de sensibiliser leurs employés aux signaux d'alerte, le conseil ne suffit pas à garantir une immunité complète face à ces attaques de plus en plus sophistiquées.

Alors que les campagnes d'hameçonnage traditionnelles prennent généralement la forme d'un contenu malveillant dissimulé dans un lien ou une pièce jointe, les attaques d'ingénierie sociale passent souvent par l'envoi d'e-mails inoffensifs qui contiennent uniquement du texte. Ces attaques contournent facilement les outils traditionnels de sécurité qui cherchent à corréler des liens et des pièces jointes avec des listes noires et des signatures. Qui plus est, ce vecteur d'attaque implique en général d'enregistrer de nouveaux domaines « similaires » qui trompent le destinataire et contournent les dispositifs de défense traditionnels.

Antigena Email dispose d'une compréhension unifiée de ce qui constitue un comportement « normal » pour l'ensemble du trafic e-mail et réseau, ce qui lui permet de détecter les scénarios de sollicitation subtils. Les e-mails inoffensifs qui échappent aux outils traditionnels peuvent être identifiés en quelques secondes en analysant de nombreux indicateurs, y compris la similarité suspecte avec des utilisateurs connus, les associations anormales entre les différents destinataires internes, et même les anomalies au niveau du contenu de l'e-mail et de son objet.

La plupart du temps, les attaques d'ingénierie sociale cherchent à déplacer la conversation hors ligne, ce qui signifie que les mesures de sécurité lentes et réactives interviennent bien souvent une fois que le mal est fait. Grâce à sa connaissance détaillée de chaque utilisateur, de chaque appareil et de chaque relation au sein de l'entreprise, Antigena Email est capable de répondre de façon proactive et avec un niveau de confiance élevé dès la première occurrence, en intervenant le plus tôt possible, à un moment crucial.

Antigena Email peut réagir de différentes manières, notamment en informant l'équipe de sécurité, en alertant les destinataires de l'e-mail en ajoutant une bannière d'avertissement au contenu de l'e-mail, en réécrivant et en verrouillant les liens et en suspendant complètement les e-mails. Antigena possède également la capacité unique d'adapter sur mesure et de façon autonome sa réponse au type de menace spécifique constaté.

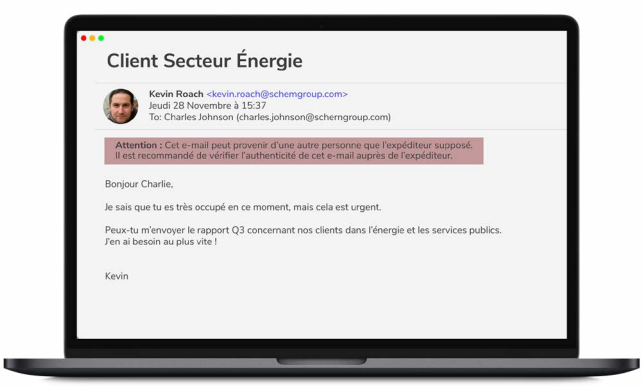

Figure 2: Une bannière d'avertissement ajoutée à un e-mail entrant usurpé demandant des documents d'entreprise sensibles.

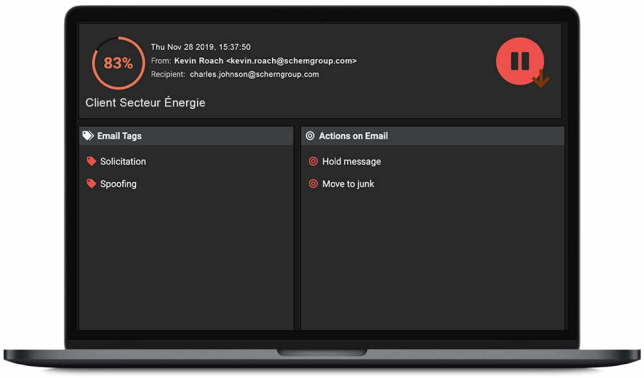

Figure 3: Antigena Email a identifié l'e-mail ci-dessus comme anormal à 83 % en raison des indications de démarchage et d'usurpation.

Performance à l'échelle de l'entreprise

Darktrace Antigena Email est capable d'analyser les pièces jointes et liens cachés en rapport avec l'ensemble du trafic de messagerie, ainsi que le « modèle comportemental normal » traditionnel de l'environnement digital. Dans le cas des attaques par hameçonnage, Darktrace détectera que ni le destinataire ni aucun membre du groupe de pairs n'a visité le domaine suspect auparavant, émettant une alerte de confiance élevée et mettant en place de façon autonome une réponse ciblée.

Il analyse également l'emplacement du contenu potentiellement malveillant dans un e-mail, en notant par exemple s'il est caché derrière différents boutons conçus pour imiter des sites de confiance. De plus, il examine les modèles dans l'adresse URL, en la comparant aux attaques déjouées précédemment afin de détecter des liens suspects. En appliquant ce contexte riche à chaque e-mail entrant et sortant dans votre entreprise, Antigena Email peut prendre des décisions intelligentes de façon autonome, en mettant en place une réponse ciblée en temps réel.

Selon la nature de la menace, les actions suivantes sont possibles : abréger les pièces jointes, verrouiller les liens malveillants et même supprimer rétrospectivement les e-mails des boîtes de réception à la lumière des informations qui émergent.