Antigena Email : Hameçonnage ciblé et transmission de contenus malveillants

Les attaques de phishing (hameçonnage) tentent généralement de tromper les utilisateurs pour les forcer à cliquer sur des pièces jointes ou des liens malveillants placés dans un e-mail, dans le but final de subtiliser des informations d'identification ou de déployer un logiciel malveillant dans une entreprise. Ces e-mails peuvent être lancés soit lors de campagnes opportunistes ciblant des milliers d'entreprises, ou sous forme d'attaques par « hameçonnage ciblé » personnalisées pour viser un destinataire en particulier.

La plupart des outils de sécurité de la messagerie s'appuient sur des connaissances de menaces identifiées précédemment, en mesurant les e-mails entrants par rapport à une liste noire prédéfinie pour déterminer s'ils sont malveillants. Ces solutions sont limitées au périmètre du réseau et analysent les e-mails de façon isolée. De plus, les contenus renfermant de nouvelles souches de malware contournent facilement cette approche traditionnelle, exposant l'entreprise à ces attaques avancées.

Alors que les attaques par messagerie commencent à utiliser l'intelligence artificielle, les e-mails d'hameçonnage sont de plus en plus perfectionnés et personnalisés par rapport au destinataire, avec des contenus malveillants souvent dissimulés derrière des liens plausibles et des boutons masqués.

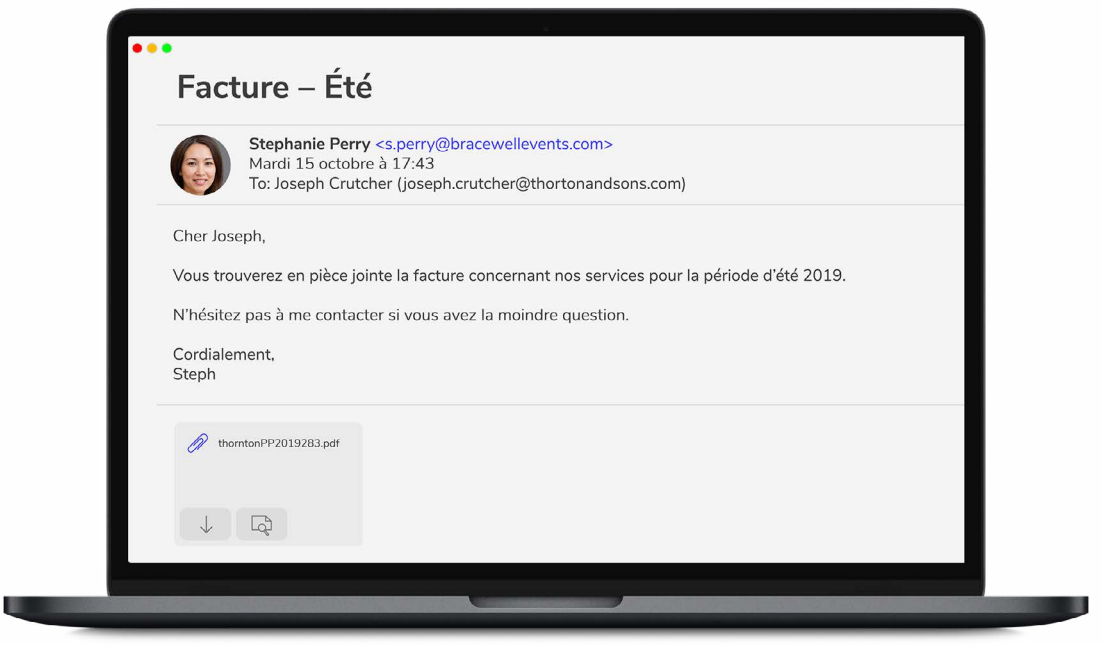

Figure 1: Un e-mail incitant un employé à cliquer sur une pièce jointe renfermant un contenu malveillant

Antigena Email : Apprendre les modèles comportementaux normaux

Antigena Email est capable d'analyser les pièces jointes et les liens cachés en rapport avec l'ensemble de la communication entrante, sortante et latérale et à l'aide du contexte riche du « modèle comportemental normal » des humains dynamiques derrière chaque e-mail. Dans le cas des attaques par hameçonnage, Antigena 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. 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.

En apprenant l'ADN digitale de la plateforme de messagerie de votre entreprise, Antigena Email peut prendre des décisions intelligentes de façon autonome, en mettant en œuvre une réponse ciblée en temps réel. Selon la nature perçue de la menace, les actions suivantes sont possibles : abréger les pièces jointes, verrouiller les liens malveillants lorsqu'ils pénètrent dans le réseau et même supprimer rétrospectivement les e-mails des boîtes de réception à la lumière des informations qui émergent.

Étude de cas : Antigena Email bloquant les attaques par hameçonnage « WeTransfer »

Antigena Email était déployé depuis une semaine seulement dans un établissement universitaire lorsqu'il a détecté une attaque sophistiquée par e-mail ciblant cinq profils sensibles. Ces e-mails étaient bien rédigés et tout à fait plausibles. Ils cherchaient à tromper les destinataires pour les faire cliquer sur un lien malveillant. Cette attaque aurait pu facilement réussir si Antigena n'avait pas analysé chaque e-mail entrant en le comparant au « modèle comportemental normal » de l'entreprise.

Les e-mails, censés venir de WeTransfer, ont obtenu un score d'anomalie de 100 % et Antigena Email a suggéré de les suspendre avant de les transmettre à l'utilisateur final. Darktrace a également identifié un lien malveillant déguisé, ainsi que les signes d'une usurpation, bien que l'organisation ait une relation déjà établie et connue avec l'expéditeur.

D'après les données de connexion, les en-têtes ne contenaient aucun signe évident indiquant que cet e-mail ne provenait pas réellement de WeTransfer. Toutefois, Antigena Email a réussi à détecter certaines anomalies subtiles. Tout d'abord, le score « Address IP Anomaly Score » était élevé (63 %). Cette mesure indique à quel point il est inhabituel pour cette adresse e-mail d'envoyer des messages depuis cette adresse IP au vu des modèles d'expédition historiques, et signale une usurpation d'identité ou une prise de contrôle de compte.

De plus, comme Antigena Email modélise en permanence le comportement « normal » de chaque expéditeur externe de confiance, elle a pu détecter une anomalie critique dans le corps du message : un lien incohérent, qui était extrêmement inhabituel par rapport à ce que Darktrace avait pu observer au préalable de la part de WeTransfer. Ce contexte a permis à Antigena Email d'identifier le lien comme étant le contenu malveillant dans l'e-mail.

Le lien en question était dissimulé derrière des boutons à plusieurs endroits dans l'e-mail, y compris dans un faux lien « https://wetransfer.com/… » et dans le texte « Inquiry Sheet.xls ». Antigena a affecté à ce lien un score d'anomalie de 96 %.

Cet incident montre comment la détection d'anomalie permet à Antigena Email d'identifier les attaques par hameçonnage sophistiquées, qui exploitent notre confiance envers un site Web connu afin de distribuer un lien malveillant et de s'installer de façon persistante au sein de l'entreprise.

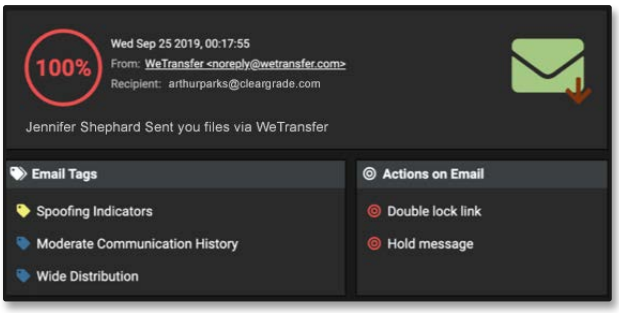

Figure 2: L'interface utilisateur montrant les violations du modèle et les actions entreprises

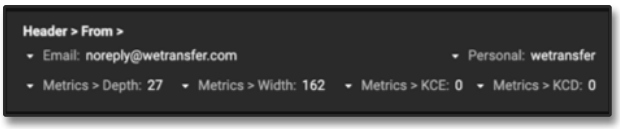

Figure 3: Données de connexion des e-mails concernés

Figure 4: Analyse détaillée des liens contenus dans les e-mails