Antigena Email : Ingénierie sociale et démarchage

À chaque fois, les attaques d'ingénierie sociale tentent d'exploiter le postulat omniprésent de confiance établi au sein de l'entreprise. En se faisant passer pour un collègue, un contact ou un dirigeant de confiance, les pirates peuvent personnaliser leurs communications en conséquence et pénétrer rapidement dans une entreprise dans le but d'effectuer un paiement frauduleux ou de persuader un employé de partager des documents et des informations sensibles sur l'entreprise. Ces attaques se présentent généralement sous la forme d'e-mails inoffensifs, sans liens ou contenus malveillants, ce qui les rend encore plus difficiles à détecter.

Alors que les pirates continuent de développer leurs tactiques et leurs techniques, les attaques d'ingénierie sociale et par démarchage sont de plus en plus efficaces. Un logiciel de Machine learning (apprentissage automatique) est aujourd'hui capable d'apprendre le style d'interactions entre deux utilisateurs et de répliquer ces modèles de communication. Cette fonctionnalité peut être exploitée par les pirates pour convaincre l'utilisateur et passer pour un contact de confiance, à tel point que la tâche de différenciation entre un e-mail légitime et une attaque d'ingénierie sociale générée par l'IA devient presque impossible.

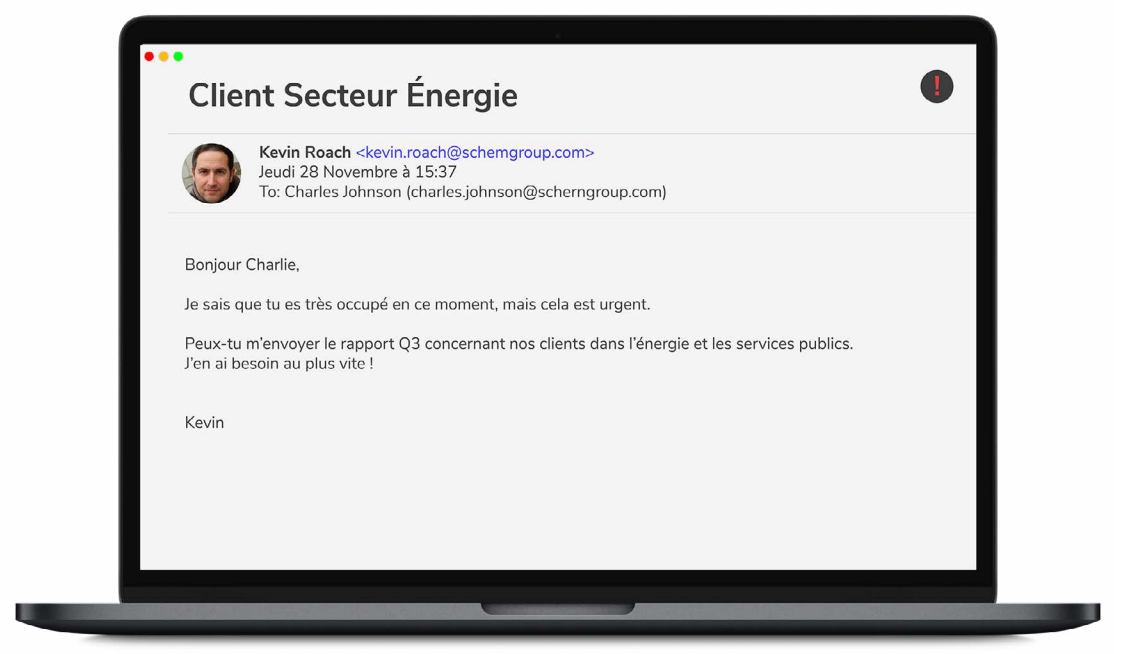

Figure 1: Attaquant se faisant passer pour un dirigeant afin d'obtenir des documents sensibles. Remarquez la fausse adresse e-mail.

Antigena Email : L'approche du système immunitaire (Immune System)

Adoptant une approche véritablement unique dans ce domaine, Antigena Email utilise une IA auto-apprenante pour aider les entreprises à reprendre finalement l'avantage. La technologie exploite la Cyber IA pour analyser l'ensemble du trafic e-mail entrant, sortant et latéral, ce qui lui permet de comprendre les humains et les relations dynamiques derrière les e-mails. Ces informations approfondies permettent à Antigena d'identifier immédiatement les menaces, ce qui est crucial dans le cas des attaques par démarchage, dans lesquelles l'objectif est souvent de déplacer la conversation hors ligne et de contourner les mesures de sécurité.

Contrairement aux outils de défense périmétriques traditionnels qui s'appuient sur des informations rétrospectives, la compréhension personnalisée et évolutive de Darktrace de la situation « normale » permet à Antigena Email de répondre de façon autonome aux attaques subtiles par usurpation d'identité qui échappent délibérément aux passerelles de messagerie électronique. Le processus de prise de décision d'Antigena Email est actif pendant toute la durée de vie d'un e-mail, permettant au système de mettre à jour son analyse à la lumière de nouvelles informations même après la distribution de l'e-mail. En plus de poursuivre la surveillance après la distribution, Antigena est capable de récupérer rétroactivement les e-mails envoyés, s'ils s'avèrent plus tard être malveillants.

Étude de cas : Antigena Email identifie de façon préventive l'usurpation d'identité des cadres supérieurs

Darktrace a récemment détecté une attaque d'ingénierie sociale extrêmement ciblée dont le but était d'usurper l'identité de cadres supérieurs dans une entreprise de technologie américaine. L'auteur de la menace a apparemment envoyé un certain nombre d'e-mails « inoffensifs » dans le but de gagner la confiance et d'établir des communications hors ligne, avant de demander un paiement.

Il est évident que l'attaquant a réalisé des recherches approfondies, car, pour chaque utilisateur ciblé, l'attaquant connaissait le cadre supérieur responsable et l'a donc utilisé dans sa tentative d'usurpation d'identité. Antigena Email a identifié les tentatives d'attaque d'ingénierie sociale et a, en conséquence, suspendu chaque e-mail l'empêchant d'atteindre les destinataires visés, en suivant ce processus :

1. Reconnaître un objet et un expéditeur anormaux. L'objet de chaque e-mail incluait le prénom de l'employé cible, et provenait d'une adresse Gmail sans lien apparent. Malgré l'absence de contenu malveillant (comme un lien ou une pièce jointe), Antigena Email a su identifier que ces e-mails étaient nuisibles.

2. Constater le « No Association ». Antigena 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 ». Cela indique que, dans le cadre de la compréhension globale de l'environnement e-mail de l'entreprise, Antigena n'avait jamais constaté la preuve d'une relation préalable entre cet expéditeur et l'entreprise.

3. Empêcher la communication hors ligne. En corrélant ces multiples indicateurs faibles, Antigena a identifié que ces e-mails étaient les éléments d'une attaque méthodique. La solution a alors suspendu ces messages pour permettre à l'équipe de sécurité de l'entreprise de les examiner. Antigena a déterminé que c'était l'action la plus adaptée dans ce cas, empêchant les destinataires visés de lire le contenu de l'e-mail et d'établir des communications hors ligne.

4. Identifier l'usurpation. Antigena Email a non seulement identifié les trois cadres supérieurs de l'entreprise dont l'identité avait été usurpée, mais elle a également reconnu que l'attaquant utilisait une contrefaçon de l'adresse personnelle externe et légitime de leur PDG.

5. Exposer le « Whale Spoof ». En outre, le score d'exposition aux utilisateurs dont le compte avait été piraté était élevé, ce qui indique qu'il s'agissait de profils clés et sensibles qui étaient visés par une attaque « Whale Spoof ». Tandis que les outils traditionnels de défense de la messagerie ont été incapables de détecter l'attaque en raison de leur analyse statique et de leur portée limitée, Antigena Email a utilisé ses connaissances approfondies des utilisateurs digitaux de l'entreprise et de leur « modèle comportemental » dans la boîte de réception pour neutraliser la menace.

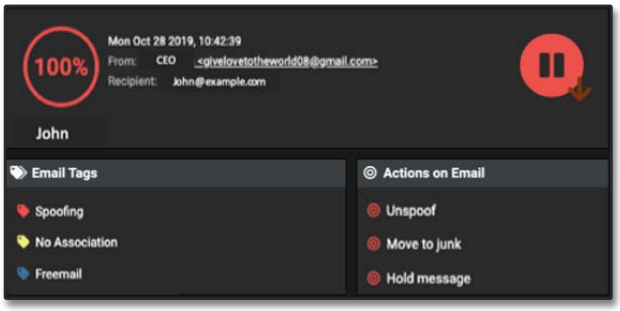

Figure 2: Un des 30 e-mails envoyés, présentant un score d'anomalie de 100 %

Figure 3: Les modèles qui ont permis à Antigena Email de réagir

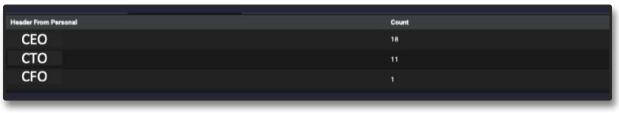

Figure 4: Identification de trois cadres supérieurs de l'entreprise

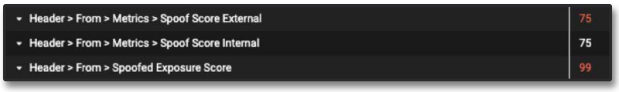

Figure 5: Antigena Email identifiant la tentative d'usurpation d'identité