Antigena Email : Piratage de compte dans la chaîne d'approvisionnement

En piratant les informations de connexion d'un contact de confiance de votre chaîne logistique, les créateurs de menaces sophistiquées peuvent gagner la confiance d'un destinataire et l'inciter à cliquer sur un lien malveillant ou à transférer des millions vers l'extérieur de l'entreprise. Les outils traditionnels de défense de la messagerie s'appuient sur un postulat de confiance, ce qui signifie que les prises de contrôle sophistiquées passent souvent inaperçues.

Les cybercriminels utilisent de plus en plus souvent la chaîne d'approvisionnement (qui inclut les fournisseurs, les partenaires et les sous-traitants) dans le but d'infiltrer une entreprise. Cette année, un rapport sur ce que l'on nomme communément « attaque par rebonds » (ou « island hopping »), dans laquelle les assaillants cherchent à exploiter une faille en passant par les chaînes d'approvisionnement, indiquait que cette méthode représente aujourd'hui la moitié des attaques.

Les attaquants qui disposent d'un contrôle total sur le compte de messagerie d'un fournisseur peuvent étudier les interactions par e-mail antérieures et produire une réponse ciblée au dernier message reçu. Le vocabulaire utilisé est souvent bienveillant, de sorte que les outils traditionnels de sécurité de la messagerie qui recherchent des mots-clés ou des expressions signalant une tentative d'hameçonnage ne relèvent pas ces attaques.

Figure 1: Une réponse plausible envoyée depuis le compte compromis d'un fournisseur de confiance. Le lien renfermait un contenu malveillant.

Antigena Email : Déterminer s'il s'agit d'un ami ou d'un ennemi

Pour analyser les modèles de communication dans le contexte du trafic e-mail entrant, sortant et latéral, Antigena Email utilise de nombreux indicateurs chiffrés pour identifier les piratages de compte, qui sont impossibles à détecter sans disposer d'une compréhension détaillée de ce qui constitue un comportement « normal » pour les humains et les relations uniques derrière les adresses e-mail.

Antigena est capable d'analyser plus de 1000 indicateurs chiffrés pour chaque e-mail, y compris le thème et le contenu, la cohérence de la localisation de la connexion et les destinataires associés, conjointement avec le « modèle comportemental » pour l'expéditeur. Antigena Email utilise ces connaissances approfondies de ce qui est normal pour votre entreprise pour estimer la probabilité que ce contact de la chaîne logistique est réellement légitime.

Lorsqu'il identifie une anomalie, Antigena met en œuvre une réponse autonome, selon la gravité de la menace, en verrouillant les liens et les pièces jointes ou en supprimant totalement un e-mail de la boîte de réception de l'employé. Antigena Email se met à jour en permanence à la lumière de nouvelles informations, en apprenant au fil de l'eau pour s'assurer que votre plateforme de messagerie est toujours protégée.

Étude de cas : Antigena Email identifie le piratage de compte de fournisseurs

Un client qui utilisait la version d'essai d'Antigena Email a subi un incident grave : le compte e-mail d'un fournisseur de confiance était devenu source d'une campagne malveillante. La technologie a reconnu que l'expéditeur était bien connu de l'entreprise, car plusieurs utilisateurs internes avaient déjà correspondu directement avec lui au préalable. En fait, l'un de ces utilisateurs avait correspondu le jour même avec le compte de fournisseur qui allait être piraté.

Moins de deux heures après cet échange légitime, routinier, des e-mails ont été rapidement envoyés à 39 utilisateurs, chacun contenant un lien malveillant. Le sujet des messages et les liens présentaient des variations, ce qui laisse penser qu'il s'agissait d'e-mails extrêmement ciblés rédigés par un attaquant bien préparé. L'objectif des liens était peut-être d'exiger un paiement, de récupérer des mots de passe ou de déployer un logiciel malveillant. Antigena Email a identifié la totalité des signaux d'alarme généralement associés à une prise de contrôle de compte dans la chaîne d'approvisionnement et a recommandé de suspendre les 39 e-mails en s'appuyant sur :

1. Lieu de connexion inhabituel : Antigena Email a détecté que les e-mails avaient été envoyés depuis un serveur Web Outlook authentique. En soi, cela n'était pas inhabituel pour le fournisseur, mais dans ces données de connexions, il était également possible d'extraire une adresse IP géolocalisable. Cette dernière qui a révélé que l'attaquant s'était connecté à partir d'une adresse IP située aux États-Unis, au lieu du Royaume-Uni.

2. Incohérence des liens : Les liens malveillants contenus dans les e-mails étaient tous hébergés sur la plateforme de développement Microsoft Azure, susceptible de contourner les contrôles de réputation sur le domaine hôte. Malgré la légitimité largement reconnue de azurewebsites.net sur le Web, Antigena Email a détecté que ce domaine était hautement incohérent pour cet expéditeur en se basant sur l'historique des correspondances.

3. Destinataires inhabituels : Le score « association anomaly » d'un destinataire estime la probabilité qu'un groupe de destinataires spécifique reçoive un e-mail provenant de la même source. En ajoutant du contexte à son analyse au fil du temps, Antigena Email a conclu que ce groupe était 100 % anormal à partir du troisième e-mail seulement.

4. Topic Anomaly : L'objet de ces e-mails suggère une volonté de rester discret et professionnel. Ainsi, toute tentative de rechercher des mots-clés associés à une attaque par hameçonnage aurait échoué. Pourtant, Antigena Email a détecté que ces destinataires ne recevaient généralement pas de propositions commerciales par e-mail utilisant ce style rédactionnel.

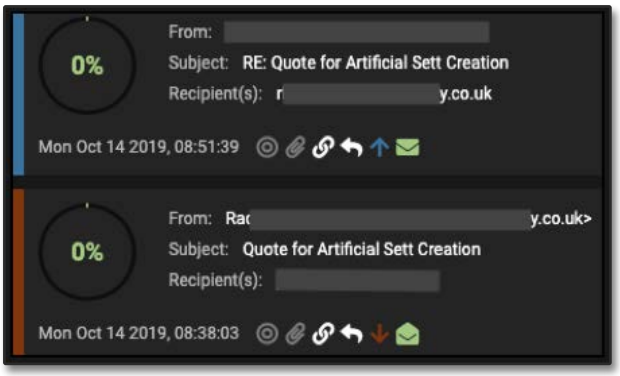

Figure 2: Correspondance « normale » antérieure avec l'expéditeur – avec un score d'anomalie de 0 %

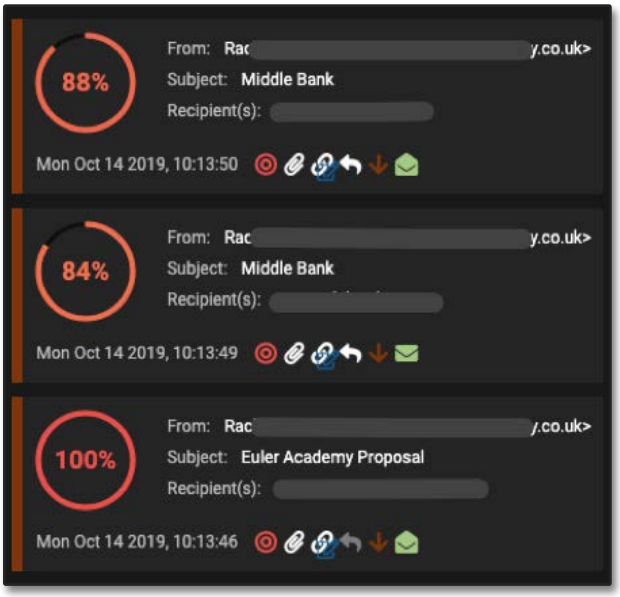

Figure 3: E-mails envoyés plus tard le même jour et renfermant des contenus malveillants

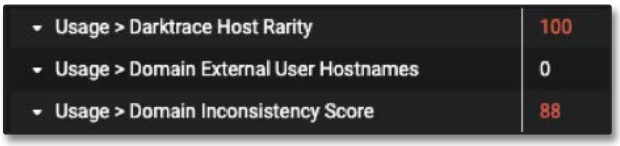

Figure 4: Modèles déclenchés par la rareté et l'incohérence du lien

Figure 5: Antigena Email a rapidement détecté que les destinataires de ce groupe n'entretenaient pas de lien étroit