Antigena Email: Kaperung eines Supply-Chain-Kontos

Indem sie die Kontodaten eines vertrauenswürdigen Kontakts in der Lieferkette eines Unternehmens kapern, können raffinierte Bedrohungsakteure leicht das Vertrauen eines Empfängers gewinnen und dazu bringen, auf einen schädlichen Link zu klicken oder Gelder in Millionenhöhe aus dem Unternehmen zu transferieren. Herkömmliche Systeme für E-Mail-Schutz basieren auf einer Vertrauensvermutung, mit der Konsequenz, dass ausgeklügelte Kontokaperungen oft nicht bemerkt werden.

Cyberkriminelle machen sich zunehmend Lieferketten – Lieferanten, Partner und Vertragsnehmer – zunutze, um ein Unternehmen zu infiltrieren. Anfang des Jahres wurde ein Bericht zum sogenannten „Island Hopping" veröffentlicht, bei dem Angreifer ganze Lieferketten in ihre Gewalt bringen. Dieser Methode ist mittlerweile die Hälfte der heutigen Angriffe zuzurechnen.

Angreifer, die vollen Zugriff auf das E-Mail-Konto eines Lieferanten haben, können den bisherigen E-Mail-Verkehr einsehen und eine gezielte Antwort auf die letzte Kommunikation schicken. Die verwendete Sprache ist meist unauffällig, sodass traditionelle Tools für E-Mail-Sicherheit, die nach Schlüsselbegriffen oder -phrasen suchen, welche auf Phishing hindeuten, diese Angriffe nicht erkennen.

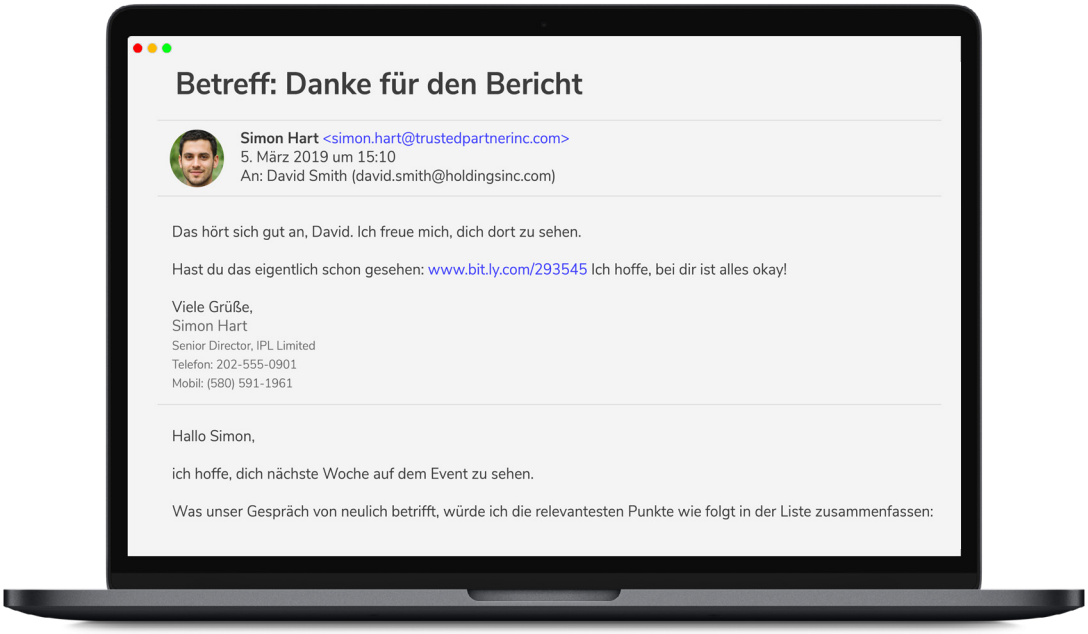

Abbildung 1: Eine plausible Antwort, gesendet von einem kompromittierten Konto eines vertrauenswürdigen Lieferanten. Der Link enthielt eine schädliche Payload.

Antigena Email: Freund von Feind unterscheiden

Bei der Analyse von Kommunikationsmustern in eingehenden, ausgehenden und lateralen E-Mails greift Antigena Email auf eine breite Auswahl an Indikatoren zurück, um Kontokaperungen zuverlässig zu erkennen. Ohne detailliertes Verständnis des „normalen" Verhaltens der Menschen und der Beziehungen hinter den E-Mail-Adressen ist dies nicht möglich.

Antigena war in der Lage, mehr als 1.000 Indikatoren für jede E-Mail zu analysieren, einschließlich Thema und Inhalt, Konsistenz des Anmeldeorts und der jeweiligen Empfänger, in Verbindung mit dem erlernten „Pattern of Life" für den Absender. Antigena Email nutzt dieses tiefgreifende Wissen über die normalen Verhaltensmuster in Ihrem Unternehmen, um einzuschätzen, wie wahrscheinlich es ist, dass ein Kontakt aus einer Lieferkette tatsächlich legitim ist.

Wenn Antigena eine Anomalie erkennt, ergreift die Technologie eigenständige Maßnahmen, die je nach Schwere der Bedrohung von der Blockierung von Links und Anhängen bis zur kompletten Entfernung aus dem Posteingang eines Mitarbeiters reichen können. Antigena Email lernt „bei der Arbeit" und aktualisiert fortlaufend sein Wissen, um sicherzustellen, dass Ihre E-Mail-Plattform immer geschützt ist.

Fallstudie: Antigena Email erkennt Kaperung eines Lieferantenkontos

Bei einem Kunden, der Antigena Email testweise installiert hatte, ereignete sich ein schwerer Sicherheitsvorfall, bei dem das Konto eines vertrauenswürdigen Lieferanten für eine schädliche E-Mail-Kampagne missbraucht wurde. Die Technologie erkannte, dass der Absender dem Unternehmen bekannt war, weil einige interne Benutzer bereits direkt mit ihm kommuniziert hatten. Es war sogar so, dass diese Benutzer an dem betreffenden Tag ganz normal über das Lieferantenkonto kommuniziert hatten, das später gekapert werden sollte.

Nicht einmal zwei Stunden nach diesem legitimen regulären E-Mail-Austausch wurden zeitgleich E-Mails von dem Lieferanten an 39 Benutzer gesendet, die jeweils einen schädlichen Link enthielten. Der Betreff und die in der E-Mail enthaltenen Links waren individuell angepasst, was darauf hindeutete, dass der Angreifer gut vorbereitet war und die E-Mails ganz gezielt personalisiert hatte. Die Links hätten dazu dienen können, Zahlungen anzufordern, Kennwörter abzugreifen oder Malware zu installieren. Antigena Email erkannte alle Warnzeichen, die typischerweise auf eine Kaperung von Supply-Chain-Konten hindeuten, und empfahl aus folgenden Gründen, alle 39 E-Mails zurückzuhalten:

1. Ungewöhnlicher Ort der Anmeldung: Antigena Email stellte fest, dass die E-Mails von einem echten Outlook Webserver aus gesendet wurden. Das war an sich nichts Ungewöhnliches bei dem Lieferanten, aber aus den Verbindungsdaten ließ sich die geolokalisierbare IP-Adresse herauslesen – dabei stellte sich heraus, dass der Angreifer sich über eine IP in den USA angemeldet hatte und nicht wie sonst in Großbritannien.

2. nk-Inkonsistenz: Die in den E-Mails enthaltenen schädlichen Links wurden alle auf der Microsoft Azure Entwicklerplattform gehostet – vermutlich, um die Reputationsprüfungen auf der Host-Domain zu umgehen. Trotz der allgemein angenommenen Legitimität von azurewebsites.net im Web erkannte Antigena Email, dass diese Domain basierend auf dem bisherigen Kommunikationsverlauf sehr unüblich für den Absender war.

3. Ungewöhnliche Empfänger: Es gibt einen Anomaliewert für „Verbindung", der Auskunft darüber gibt, wie wahrscheinlich es ist, dass diese Empfängergruppe eine E-Mail von derselben Quelle erhält. Da Antigena Email seine Analysen sukzessive mit Kontext anreichert, konnte die Technologie bereits bei der dritten E-Mail erkennen, dass diese Empfängergruppe 100 % anormal war.

4. Themen-Anomalie: Die Betreffzeilen dieser E-Mails sind unauffällig und professionell formuliert, sodass signaturbasierte Tools keine Schlüsselbegriffe finden würden, die auf einen Phishing-Angriff hindeuten. Antigena Email hingegen erkannte, dass diese Empfänger in der Regel keine E-Mails mit geschäftlichen Angeboten in diesem Schreibstil erhalten.

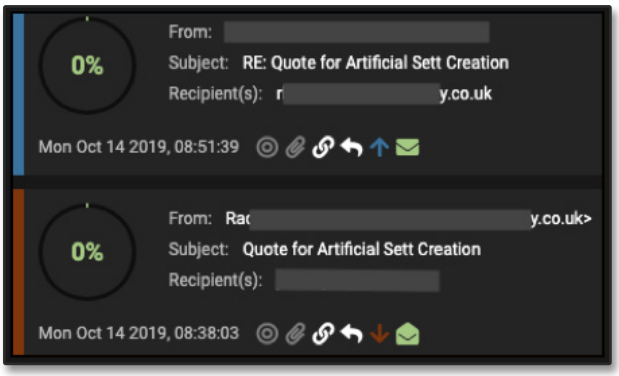

Abbildung 2: Frühere „normale" Korrespondenz mit dem Absender – mit einem Anomaliewert von 0 %

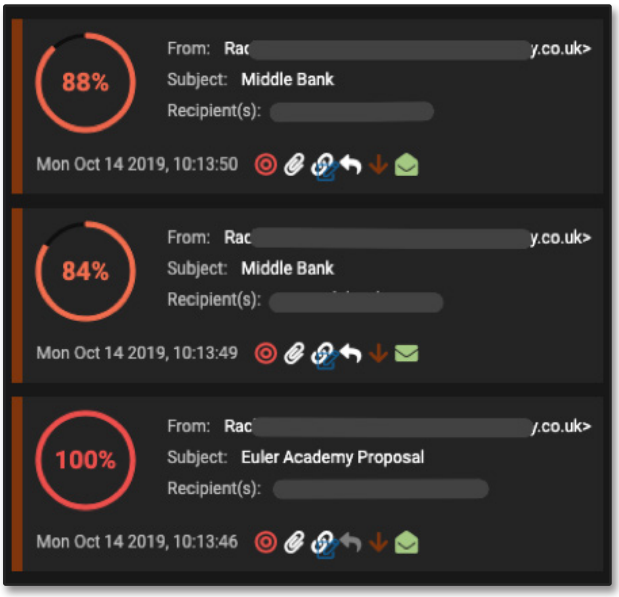

Abbildung 3: E-Mails, die am selben Tag zu einem späteren Zeitpunkt gesendet wurden und schädliche Anhänge enthielten

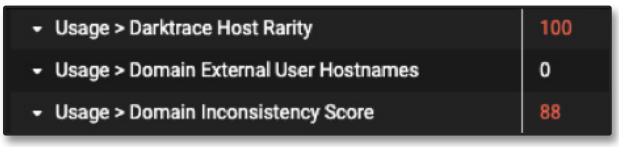

Abbildung 4: Modelle wurden durch den ungewöhnlichen Charakter und die Inkonsistenz des Links ausgelöst

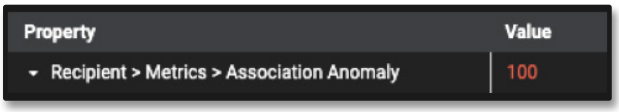

Abbildung 5: Antigena Email erkannte schnell, dass es keine enge Verbindung zwischen den Empfängern dieser Gruppe gab