Antigena Email: Spear Phishing & Payload-Einschleusung

Phishing-Angriffe zielen in der Regel darauf ab, Mitarbeiter zu verleiten auf schädliche Links oder Anhänge in einer E-Mail zu klicken. Auf diese Weise sollen Zugangsdaten abgegriffen oder Malware in das Unternehmen eingeschleust werden. Diese E-Mails können entweder wahllose Kampagnen sein, die sich gleich gegen Tausende von Unternehmen richten, oder sorgfältig als Spear Phishing-Angriffe konzipiert sein, die auf den Empfänger zugeschnitten sind.

Die meisten E-Mail-Sicherheitstools ziehen Erkenntnisse aus bereits identifizierten Bedrohungen heran und gleichen eingehende E-Mails mit einer vordefinierten Blacklist ab, um zu bestimmen, ob sie schädlich sind. Diese Lösungen prüfen E-Mails am Gateway und analysieren E-Mails nur isoliert. Zudem werden Payloads, die neuartige Malware-Stämme enthalten, von solchen herkömmlichen Tools leicht übersehen, sodass das Unternehmen solchen hochkomplexen Angriffen schutzlos ausgeliefert ist.

Da E-Mail-Angriffe mittlerweile auch künstliche Intelligenz nutzen, können Phishing-E-Mails immer auf den Empfänger zugeschnitten werden, und schädliche Payloads verbergen sich oftmals hinter plausiblen Links und getarnten Schaltflächen.

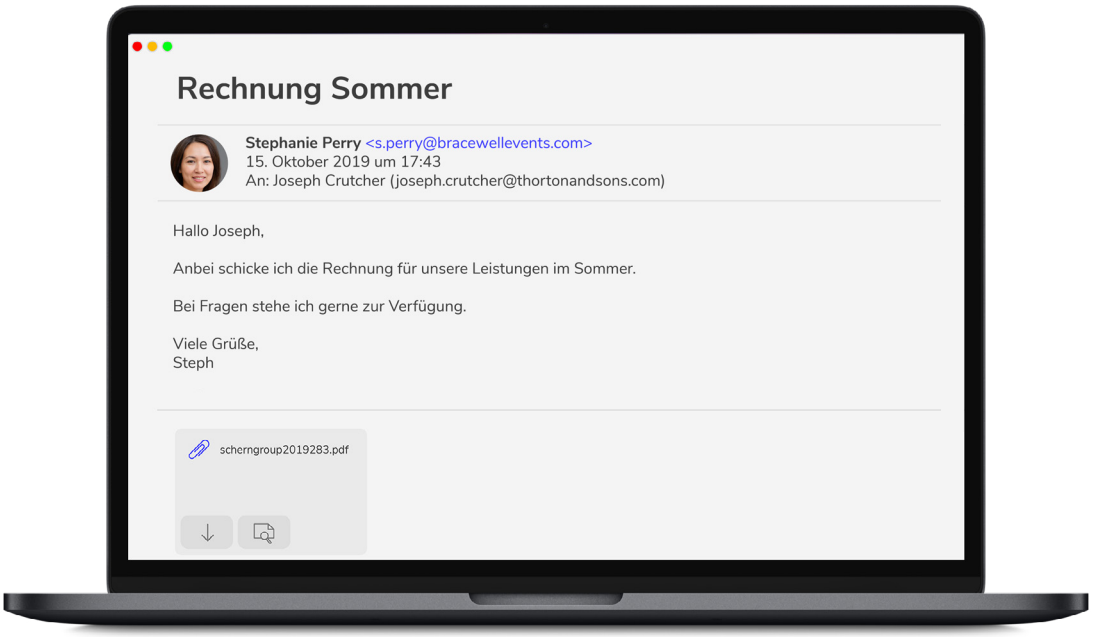

Abbildung 1: E-Mail, mit der ein Mitarbeiter verleitet wird auf einen Anhang zu klicken der eine schädliche Paypload enthält

Antigena Email lernt die normalen Verhaltensmuster („Patterns of Life“)

Antigena Email ist in der Lage, verborgene Links und Anhänge in Verbindung mit sämtlicher eingehender, ausgehender und lateraler Kommunikation zu analysieren, und nutzt dafür den reichhaltigen Kontext der normalen Verhaltensmuster der dynamischen Personen hinter jeder E-Mail. Bei Phishing-Angriffen erkennt Antigena, dass weder der Empfänger noch irgendjemand in seiner Peer-Group die verdächtige Domain jemals zuvor besucht hat. So kann die Technologie eine Warnmeldung über die zuverlässig erkannte Bedrohung herausgeben. Sie untersucht auch, an welcher Stelle in der E-Mail sich die potenziell schädliche Paypload befindet und erkennt zum Beispiel auch, wenn sie sich hinter Schaltflächen verbirgt, die denen auf vertrauenswürdigen Websites ähnlich sind.

Antigena Email macht sich ein Bild von der digitalen DNA der E-Mail-Plattform Ihres Unternehmens und kann eigenständig intelligente Entscheidungen treffen und in Echtzeit gezielte Maßnahmen ergreifen. Je nach wahrgenommener Art der Bedrohung gehören dazu das Verkleinern von Anhängen, das Sperren schädlicher Links, sobald sie in das Netzwerk gelangen, und auch ein rückwirkendes Entfernen von E-Mails aus Posteingängen, wenn neue Erkenntnisse gewonnen werden.

Fallstudie: Antigena Email stoppt WeTransfer Phishing-Angriff

Antigena Email war erst eine Woche bei einer wissenschaftlichen Einrichtung installiert, als die Technologie einen raffinierten E-Mail-Angriff auf fünf hochrangige Benutzer feststellte. Die E-Mails waren gut formuliert und sehr plausibel und sollten die Empfänger dazu bringen, auf einen schädlichen Link zu klicken. Dieser Angriff wäre fast geglückt, hätte Antigena nicht jede eingehende E-Mail mit dem „Pattern of Life" des Unternehmens abgeglichen.

Den E-Mails, die von WeTransfer zu kommen schienen, wurde ein Anomaliewert von 100 % zugewiesen und Antigena Email empfahl, die Nachrichten zurückzuhalten und nicht dem Endnutzer zuzustellen. Darktrace erkannte einen getarnten schädlichen Link und Hinweise auf Spoofing, obwohl das Unternehmen bekanntermaßen eine Beziehung zu diesem Absender unterhielt.

Es gab keine klaren Hinweise in den Headern, dass diese E-Mail nicht von WeTransfer stammte. Es gab jedoch einige subtile Abweichungen, die Antigena Email erkannte. Zunächst einmal war der Anomaliewert für die IP-Adresse hoch (63 %). Dieser Indikator gibt an, wie ungewöhnlich es im Vergleich zu den bisherigen Mustern ist, dass die betreffende E-Mail-Adresse von dieser IP aus E-Mails sendet, und ist auch ein Hinweis auf Spoofing oder ein Account Hijack.

Da Antigena Email laufend das „normale" Verhalten für jeden vertrauenswürdigen externen Absender modelliert, konnte die Technologie eine entscheidende Anomalie im Textteil der E-Mail feststellen: Einen Link, der unter Berücksichtigung dessen, was Darktrace bei WeTransfer bisher beobachtet hatte, ungewöhnlich war. Vor diesem Hintergrund konnte Antigena Email den Link als schädliche Payload in der E-Mail identifizieren.

Der betreffende Link war hinter Schaltflächen in mehreren Stellen in der E-Mail verborgen, unter anderem ein gefälschter „https://wetransfer. com/..."-Link und der Text „Inquiry Sheet.xls". Antigena wies dem Link einen Anomaliewert von 96 % zu.

Dieser Vorfall zeigt, wie Antigena Email dank der Anomalieerkennung in der Lage ist, hochkomplexe Angriffe zu erkennen, die das Vertrauen zu einer Website ausnutzen, um einen schädlichen Link bereitzustellen und an mehreren Stellen einen Fuß in die Einrichtung zu bekommen.

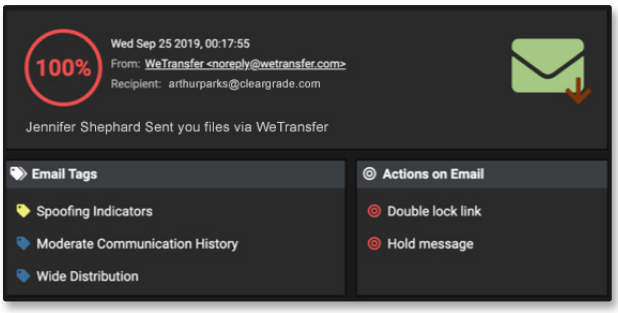

Abbildung 2: Benutzeroberfläche mit Übersicht der Abweichungen von den Modellen und der ergriffenen Maßnahmen

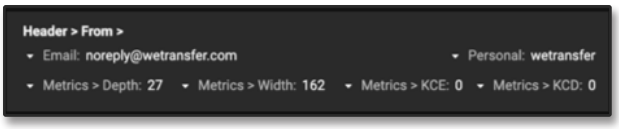

Abbildung 3: Verbindungsdaten der betreffenden E-Mails

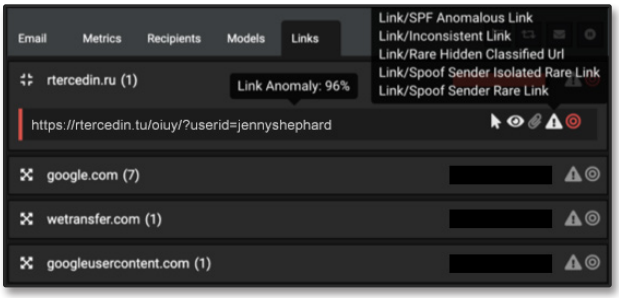

Abbildung 4: Aufschlüsselung der in den E-Mails enthaltenen Links