DARKTRACE

Darktrace Cyber AI

Eメールの免疫システム

「これまで以上に、現代の E メールセキュリティには変化する脅威環境に対抗するためのイノベーションとマインドセットの転換が必要とされています。」

– ピーター・ファーストブルック（ガートナー社 VP アナリスト）

はじめに

脅威一覧

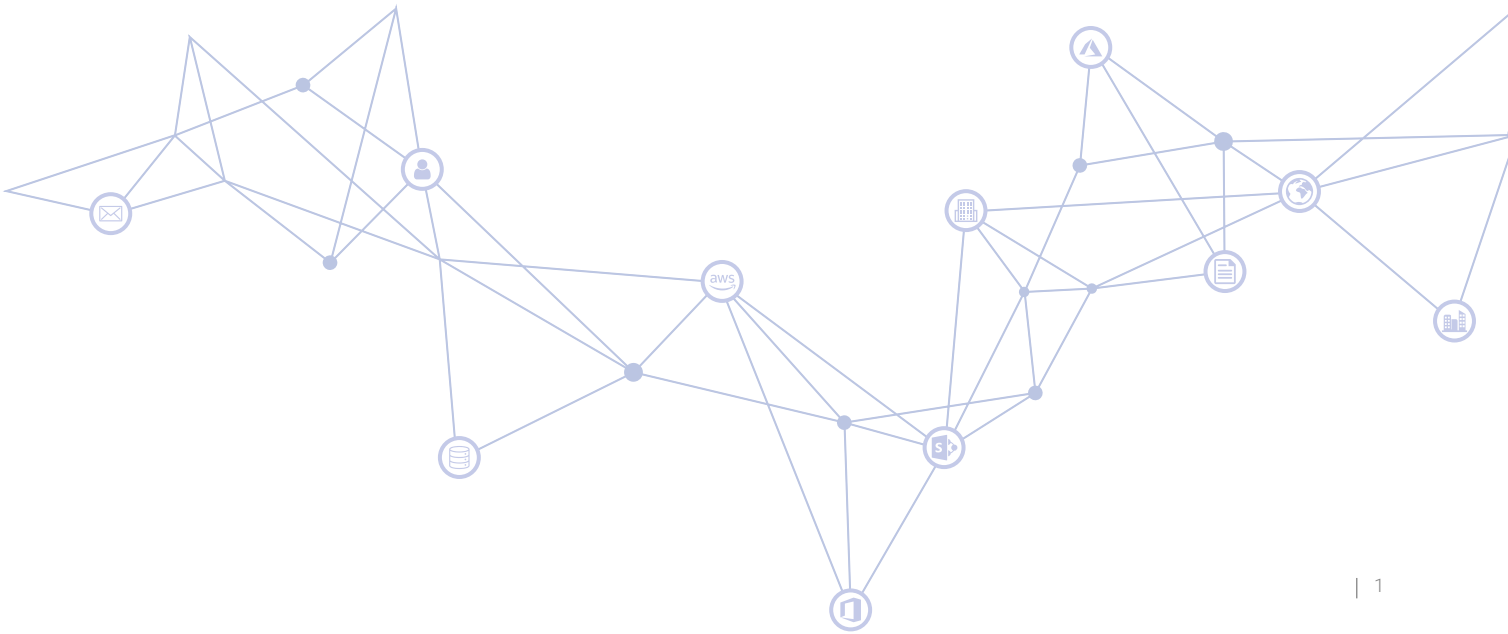
E メールや各種コラボレーションプラットフォームはあらゆるデジタルビジネスを結合しています。デジタル形式の往復書簡を使って情報が共有され、計画が生まれ、アライアンスが形成されています。しかし、人間が主体の媒体であるため、E メールは常に信頼を大前提としたものになり、これが組織のセキュリティ戦略においての最大の弱点となります。

この信頼の前提はコラボレーションと成長にきわめて重要な要素ですが、このことはビジネスの他のどの分野よりも現代の「ゼロトラスト」の精神に対して構造的耐性があるということを意味します。そのため、サイバー脅威の 94% が依然として E メールから発生していることは全く驚くに値しません。

この分野において人間の誤りやすさの影響を最小化するには、テクノロジーを利用して最も優れた判断力を持つ熟練した従業員でも特定が難しい悪意ある E メールを識別する他ないという考えに業界全体が至っています。しかし、最近まで、従来型の防御システムはサイバー脅威のイノベーションのペースに後れをとっていました。

スピアフィッシング、なりすまし攻撃、そして特にアカウント乗っ取りなどは、組織に簡単に侵入しようとするサイバー犯罪者にとって効果的な方法です。この種の標的型 E メール攻撃は、従来型防御システムの限界もあり、最も多層的で成熟したセキュリティ戦略を持つ組織においても喫緊の課題です。

ガートナー社 VP アナリストのピーター・ファーストブルック氏はこのような市場の動向をよく言い表しています。「一般に使われている制御手法、たとえば標準やレピュテーションベースの、アンチスパムおよびシグネチャベースのアンチウイルスなどは、広範囲な攻撃や詐欺キャンペーン対策には適していますが、より的を絞った、洗練された高度な攻撃からの保護には不十分です。これまで以上に、現代の E メールセキュリティには変化する脅威環境に対抗するためのイノベーションとマインドセットの転換が必要とされています。」



Darktrace AI:免疫システムプラットフォーム

しかし、近年のエンタープライズスケールの AI の登場により、この「マインドセットの転換」が E メールセキュリティに対する「免疫システム」アプローチの形で遂に結晶したのです。

ファーストブルック氏が言うように、従来型の E メール防御はシンプルな無差別型の脅威には十分かもしれませんが、特定の受信者やビジネスに合わせてカスタマイズされた、より高度な攻撃に対抗するように設計されてはいません。

従来型の E メールゲートウェイとネイティブコントロールによる検知は、ハードコードされたルールおよび過去にあった攻撃の知識に依存しています。そのため検知の範囲は既に見たことのある脅威、あるいは少なくとも静的なバイナリルールを境界でトリガすることのできる基本的な脅威に必然的に限定されてしまいます。ただ、多くのビジネスリーダーも彼らが受けた傷を指し示しているように、私達が現在直面している問題はこれだけではありません。

幸運なことに、E メールセキュリティに出現したパラダイムシフトは、ファーストブルック氏の指摘する「一般的なアプローチ」とエンタープライズスケール AI の新しい応用の間にある重要な違いから生まれました。この違いは、組織の「身体を保護する皮膚」と、侵入してしまった脅威に対する学習型の「免疫システム」の違いに例えることができます。

身体を保護する皮膚は過去の攻撃について知っており、よく知られた脅威については止めることができますが、「免疫システム」はすべての従業員のデジタルワークフローを特徴づける、バラバラな「生活パターン」について知っています。重要なことに、これらの「生活パターン」は E メールトラフィックだけではなく、ネットワークやクラウドトラフィックにも現れ、あらゆるユーザーにとって何が正常かについての変化し続ける包括的な全体像として統合することができます。

このエンタープライズ全体に対する独自の理解により、かつてないレベルで標的型攻撃を無害化することができます。これは、標的型攻撃の E メールに含まれるわずかな逸脱が実際に悪意あるものであるかどうかを、正確に判断するための十分な証拠を揃えることができる唯一のアプローチです。

初めて、E メール防御システムが、あるユーザーにとってその E メールを受け取ることが「おかしい」のではないかという意味のある問いを、その従業員、同僚、また E メールだけでなくクラウドやコーポレートネットワークも含めた幅広い組織全体の「生活パターン」についてシステムが知っていることに基づいて発することができるようになったのです。

また、これは E メールが配信された後からでも、新たな証拠（E メールに現れたもの、あるいはネットワーク上に現れた悪意ある動作など）に照らしてその判断やアクションを更新することができる唯一のアプローチです。

本ホワイトペーパーは、ネットワーク、クラウド、E メールトラフィックに対する統一された独自の理解が、なぜ E メールセキュリティ市場でのパラダイムシフトとなるのかを説明します。

Darktrace は Antigena Email および Enterprise Immune System Platform によってこのアプローチを切り開きました。以後紹介するケーススタディは、「保護膜」を日常的にすり抜けているが、Darktrace の AI であれば数秒でたやすく無害化できる、4 つの高度に洗練された攻撃カテゴリーのいずれかに当てはまるものです。

- スピアフィッシングとペイロードデリバリー
- サプライチェーンアカウント乗っ取り
- ソーシャルエンジニアリングと勧誘
- 従業員の認証情報悪用

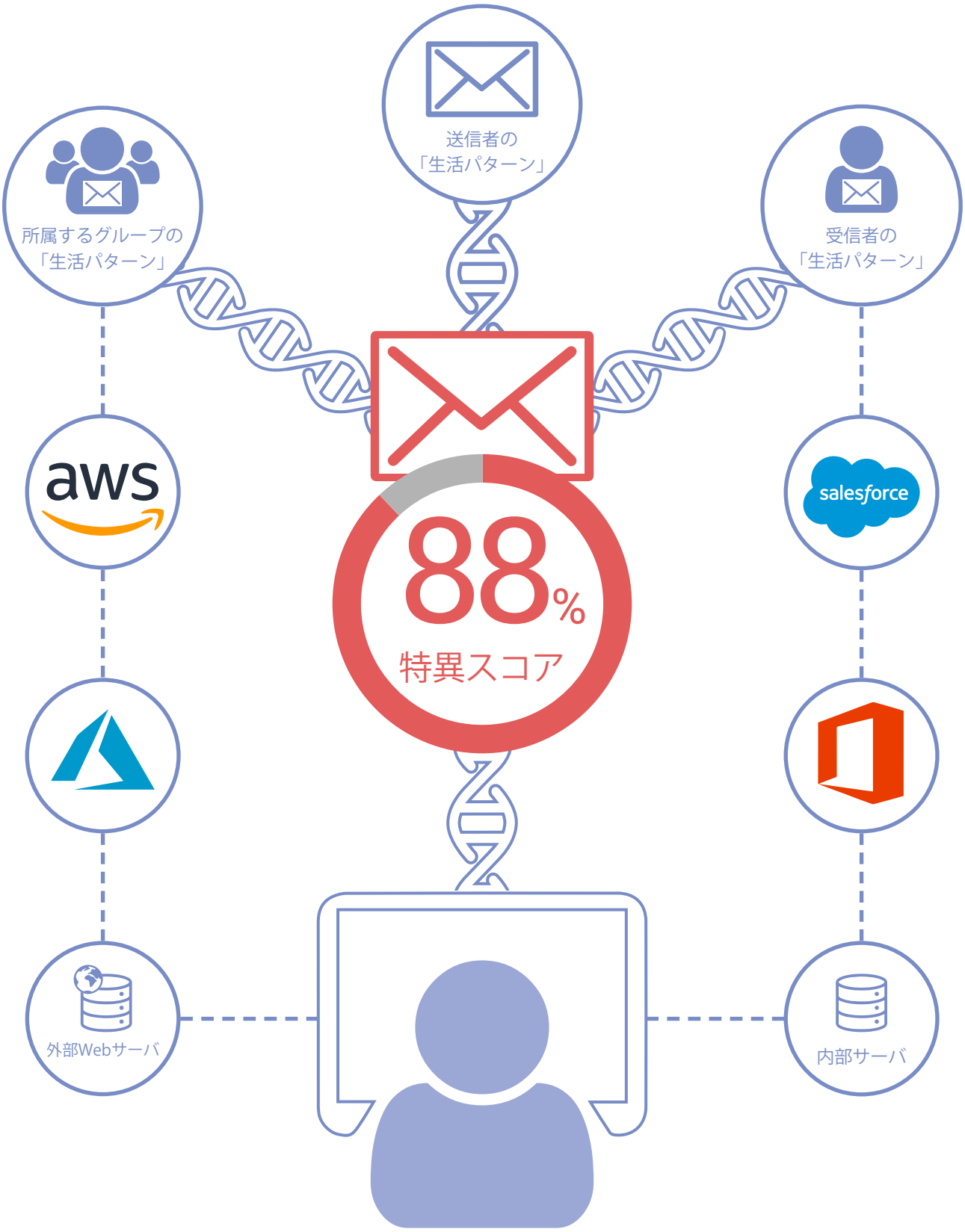


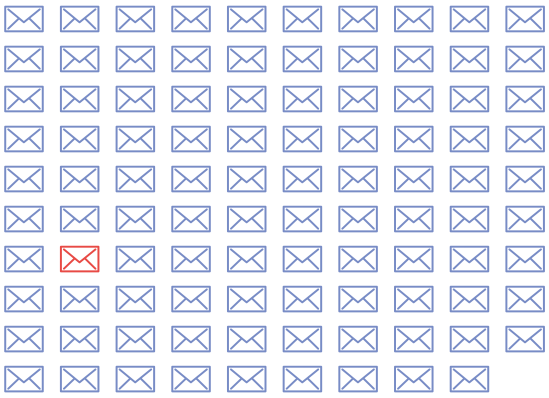
図 1: Antigena Email は E メールデータだけでなく、より広範な組織のコンテキストで E メールを分析する唯一のソリューションです。エンタープライズ全体を理解することで、境界上の従来型防御システムをすり抜ける悪意ある E メールを特定することができます。

スピアフィッシングとペイロードデリバリー

「Antigena Email は E メールとネットワークトラフィック両方にとっての「正常」についての理解によって脅威を捕捉でき、非常に貴重なツールです。」

– IT 部長、Entegrus 社

E メール 99 件のうち 1 件はフィッシング攻撃



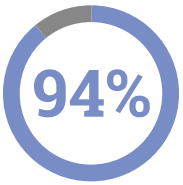
出典：Avanan

ほとんどのフィッシング攻撃は E メールに含まれる悪意あるリンクや添付ファイルをユーザーにクリックさせようとするものであり、最終的な目標は認証情報を取得すること、あるいは組織内に破壊的なマルウェアを展開することです。これらの攻撃は何千もの組織に対する標的を区別しない「無差別型」の攻撃として実施されることも、または特定の受信者またはビジネスに合わせてカスタマイズされた「スピアフィッシング」攻撃として実行されることもあります。

フィッシング攻撃を防御する際、従来の防御システムは E メールを過去の攻撃、ブラックリスト、およびシグネチャの理解に照らして分析するのが一般的です。しかしサイバー犯罪者達はこの受け身のアプローチを誰よりもよく理解しているため、当然ながら従来型防御を回避するよう設計された新手の戦術やテクニックを活用しています。

ところが、新種の攻撃は以前に見られていないために境界で従来型の防御をすり抜けるのですが、このことはいずれかの記述レベルにおいてこれらの E メールは標的とするユーザーまたはビジネスにとって特異性が高くなることを意味します。少なくともデジタル環境全体の「生活パターン」を考慮すればそうなります。この基本的真理こそが、外側の E メールレイヤーと Darktrace の Immune System Platform が持つようなネットワーク全体の知識の間にあった従来の知識のギャップを埋めることが非常に重要である理由です。

エンタープライズスケールの AI により、Antigena Email は E メールのリンク、添付ファイル、ドメイン、内容およびその他の要素をクラウドおよびネットワークの「生活パターン」に沿って分析し、豊富なデータポイントの集まりを相関づけることにより、一見無害な E メールも間違いなく悪意のあるものであることを明らかにすることができます。



今日のマルウェアの 94% は受信箱から見つかっています

他のどのソリューションとも異なり、Antigena Email と Immune System はネットワーク、クラウド、E メールデータを相関づけ、ペイロードと送信者に関連するドメインに異常があるか、E メールに含まれるリンクの場所におかしな点があるか、話のテーマや内容が通常と異なるか、そして URL パスウェイのパターンに疑わしい点があるか、などを識別することができます。

この根本的に独自のアプローチは Darktrace の意思決定が他のツールよりも格段に正確であることを意味します。そのためきわめて適切で的を絞ったアクションにより大規模なフィッシング攻撃を無害化できます。

Immune System もあらゆる環境で感染を検知し、自動的に原因分析を行ってこれが E メールから来たものかを確認できる能力がユニークです。E メールから発生している場合には、同じ攻撃の標的となった他のすべての従業員を即座に保護します。これは戦略的な自動対処と呼ばれるもので、「第一号患者」から学習することによって人手による介入なくビジネスの他の部分を戦略的に保護することが可能になります。セキュリティチームの視点から見れば、それでも誰かが最初の被害者のラップトップをクリーンアップする必要がありますが、200 台やそれ以上のクリーンアップを行うことに比べればずっとましです。

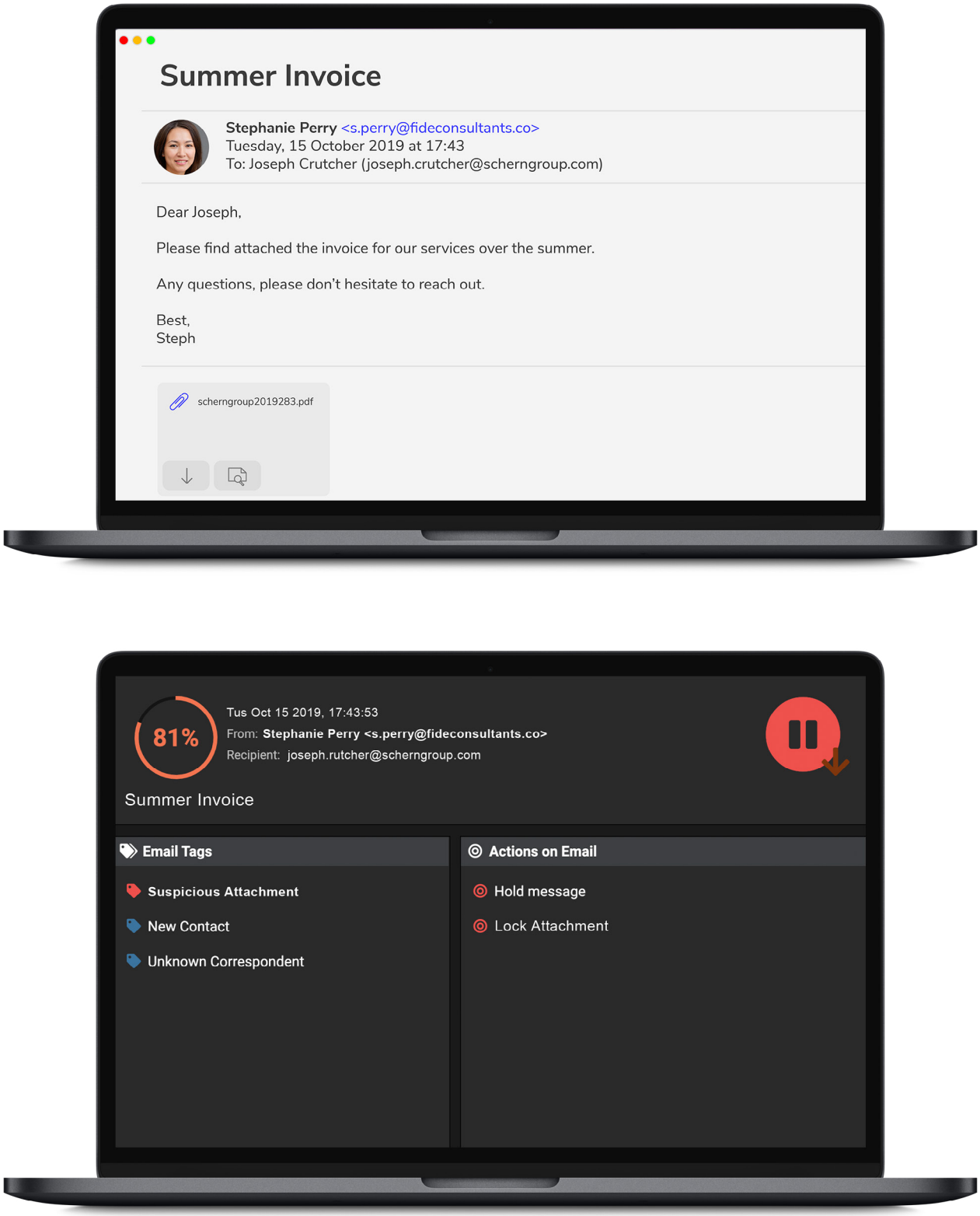


図 2: 悪意のあるペイロードを含む添付ファイルを従業員にクリックさせようとする E メール（上）と、特異性のタグおよび取られたアクションを示す Darktrace のユーザーインターフェイス（下）。

WeTransfer 攻撃

Darktraceはシンガポールの大学に属する5人の著名なユーザーを標的とした、悪意あるリンクをクリックさせるために巧妙に作られたフィッシング攻撃を検知しました。

Antigena Emailはこれらの Eメールに 100% の特異スコアをつけ、これらを保留し、配信しないというアクションを取りました。また、この大学が送信者と既知の関係を持っていたにも関わらず、サービススプーフィングのかすかなインジケータを識別しました。

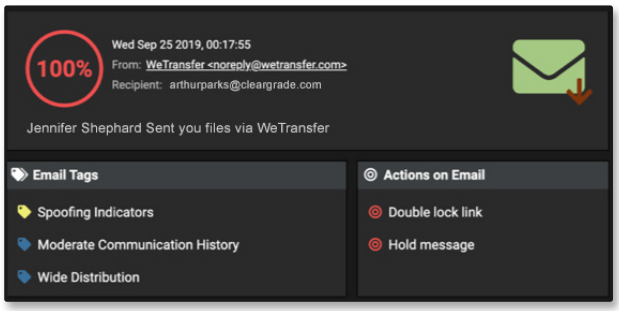


図 3: モデルに対する違反およびアクションを示すユーザーインターフェイス

1. ヘッダーデータからは、この Eメールが WeTransfer 以外のソースを持っているという明確な形跡はなく、受信者にとっては全く正常に見えたはずです。'Width' および 'Depth' はこの Eメールアドレスが組織内の多数の人と、複数日に渡って通信したことを示しています。

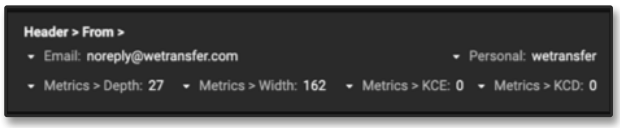


図 4: 各 Eメールの接続データ

2. しかし、Antigena Email はユーザーと組織に対する「正常」の理解と、ネットワークレイヤーから得られたその他のコンテキストを用いて、さまざまな微細な特異性を見つけることができます。

a. まず、'Address IP Anomaly Score' が高い値（63%）を示していました。このメトリックは、この Eメールアドレスがこの IP から送信することが過去の送信パターンからみてどの程度珍しいかということを示します。そしてこれは通常スプーフィングまたはアカウント乗っ取りを示すものです。

b. さらに、Darktrace はすべての外部送信者の「正常な」動作を絶えずモデル化しているため、Eメール本文に含まれていた主要な特異性を見つけることができました。それは Darktrace が WeTransfer からそれまで観測していたものとは大きく異なるリンクであり、Antigena Email はこれを Eメールに含まれる悪意あるペイロードと識別することができました。

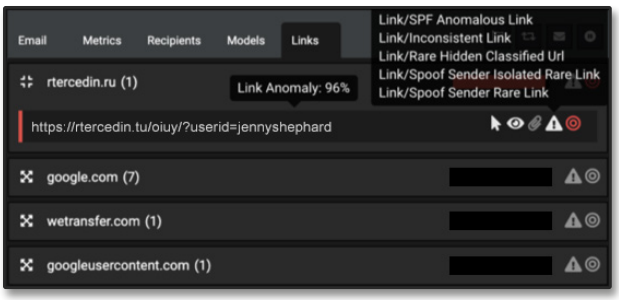


図 5: Eメールに含まれるリンクの内訳

c.Eメールに含まれていたリンクは 96% の特異スコアが付けられ、偽の 'https://wetransfer.com/…' リンク（以下の図を参照）および「お問い合わせシート .xls」や、「ファイルを取得」というテキストなど、Eメールのいくつかの部分に配置された「ここをクリック」スタイルのボタンの背後に隠されていました。

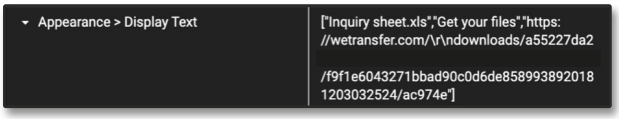


図 6: Antigena は Eメール内のどこにリンクが出現しているかを特定しました

この攻撃は全くの新種で、大学が設定していた他のあらゆるシグネチャベースのツールを通過しました。また、このリンクが全く無害なドメインを使用しており、悪意あるペイロードに即座に結びつくものではなかったため、ヒューリスティックな検知方法やサンドボックスでも検知は失敗したと思われます。

偽請求書に隠されたマルウェア

ある大手法律事務所が、認証情報を盗み出すマルウェアを偽の請求書に添付された ISO ファイルに見せかけた、高度なフィッシング攻撃の主要な標的の 1 つとなりました。従来の E メール防御は、一般に ISO ファイルをホワイトリストに入れており、オペレーティングシステムはイメージをシングルクリックで自動的にマウントするため、脅威アクター達には当然魅力的な標的です。

しかし、一連の攻撃メールがこの事務所の従来型 E メール防御を通過すると、Darktrace はさまざまな特異性のインジケータを認識して攻撃を特定しました。たとえば、これらの E メールによって発動した AI モデルの 1 つが “Attachment/Unsolicited Anomalous MIME” です。これは添付ファイルの MIME タイプがユーザーまたはその属するグループにとって特異性が高く、受信者はそのファイルを要求する通信を送信者としたことがない、ということを意味します。

疑わしいと思われるすべての E メールに対して一般的な警告（無視される可能性が高い）でマーキングするのではなく、これらの脅威の正確な出処をピンポイントで特定することにより、Darktrace は外科的アクションでこれを無害化しました。この有害な ISO ファイルに対処するため、Darktrace は添付ファイルを無害な PDF に変換し、E メールをゴミフォルダに移動しました。また、この攻撃で最初の E メールを検知した後、攻撃がビジネスに影響を及ぼす機会を得る前にさらに 20 通の E メールを自動的に無害化しました。

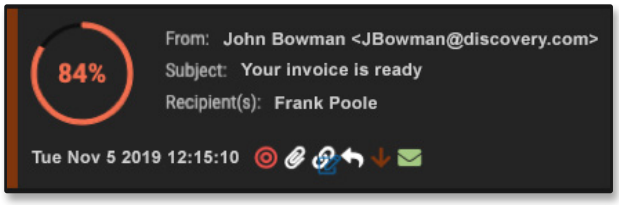


図 7: 悪意ある E メールのヘッダと、提案されたアクション

地方公共団体のアドレス帳流出

脅威アクターが米国の地方自治体のアドレスブックを取得することに成功し、A から Z へアルファベット順に受信者に攻撃を仕掛けました。それぞれのメールは丁寧に作られ、受信者に合わせた内容でしたが、それらすべてには悪意のあるペイロードが含まれ、それらは Netflix や Amazon など信頼されているサービスへのリンクに偽装されたボタンの背後に隠されていたのです。

最初のメールが来た時点で、Darktrace はすぐにこの受信者もその所属するグループの他の人も、そして他の市のスタッフも誰もこのドメインを以前に訪れたことがないということを認識しました。また、システムはリンクがそれぞれボタンの背後に隠されているやり方も非常に疑わしいと認識しました。システムは即座に確度の高い警告を発し、各リンクがネットワークに受信され次第自動的にロックすることを提案しました。

興味深いことに、Antigena が「パッシブモード」で運用されていたことにより、他のツールでは見逃されてしまう巧妙な攻撃を阻止するこのシステムの能力についての明確かつ具体的な証拠が提示されました。Antigena はアルファベットの ‘A’ の時点で攻撃を発見し無害化を求めましたが、セキュリティチームが使用していた従来のツールが攻撃に気づいたのは ‘R’ に到達してからでした。「アクティブモード」で運用されていたならば、Antigena は攻撃を 1 人のユーザーにも到達させることなく無害化していたはずです。

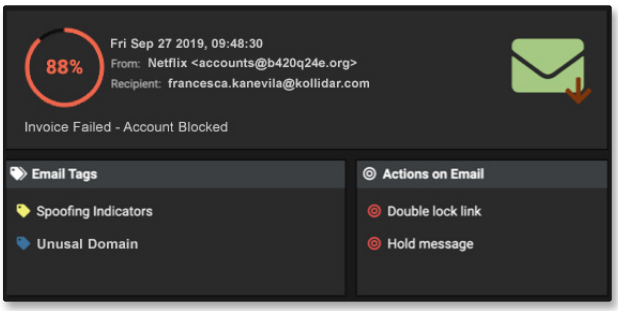
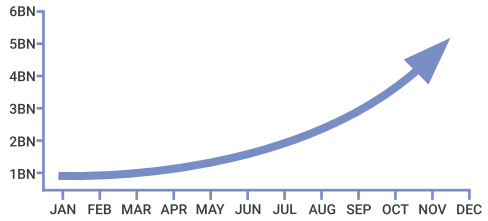


図 8: 88% の特異スコアを示す Antigena Email

サプライチェーンアカウント乗っ取り

昨年度のアカウント乗っ取りによる損害は、従来の 3 倍の 51 億ドルに拡大



出典: Javelin

信頼されているサプライチェーン内のベンダーなどのアカウント情報を乗っ取ることにより、脅威アクターはネットワーク内の受信者の信頼を容易に獲得し、悪意のあるリンクをクリックさせたり、会社から何百万ドルも送金させることができます。従来型の E メール防御システムは信頼を前提としています。このことは高度なアカウント乗っ取りが全く気付かれない場合が多いことを意味します。

アカウントの乗っ取りは、過去数年に発生した大企業に対するいくつかの重大な攻撃の原因となっています。サイバー犯罪者達は組織に侵入する、またはオフライン通信を確立するための攻撃において、ますますサプライチェーン（ベンダー、パートナーや請負業者）を活用するようになっています。今年の初めに発表された、いわゆる「アイランドホッピング」（攻撃者がサプライチェーンを通じて侵入を広げようとすること）についてのレポートでは、今日の攻撃の半分がこの方法で行われていることが明らかになっています。

サプライヤーの E メールアカウントに完全なアクセスを持つ攻撃者は、それまでの E メールのやり取りを調べ、最新のメッセージに的を絞って返信を作成することができます。彼らの使用する言葉は無害に見えることが多く、フィッシングを示すようなキーワードやフレーズを探す従来の E メールセキュリティツールはこのような攻撃を特定することができません。

Antigena Email はあらゆる社内ユーザーに対する正常性についての包括的な見解を形成することができるため、人間であれ機械であれほとんどの観測者にとってその言葉遣いがどれほどもっともらしく見えても、単語やフレーズの不規則な分布を識別することができるのです。すべての E メールおよびネットワークトラフィックの完全なコンテキストを用いてコミュニケーションのパターンを分析することにより、Antigena Email は多様なメトリックに基づいてアカウント乗っ取りのさまざまなケースを確信を持って特定することができます。これはデジタル環境全体の「正常」な動作についての詳細な理解なくしては検知不可能な問題です。

このテクノロジーはあらゆる E メールのトピックや内容に含まれる異常を識別し、これをログイン場所、リンクおよび添付ファイル、送信者に対する過去の主な受信者などとの整合性とあわせて分析します。Antigena Email はこの多元的な理解を用いて、信頼できるサプライヤーからの E メールが実際に本物である可能性を予測することができます。信頼を前提とはしないのです。その後脅威の深刻度に応じて適切な対応を取り、リンクや添付ファイルのロック、あるいは E メールを従業員の受信箱から完全に削除してしまう、などのアクションを実行します。

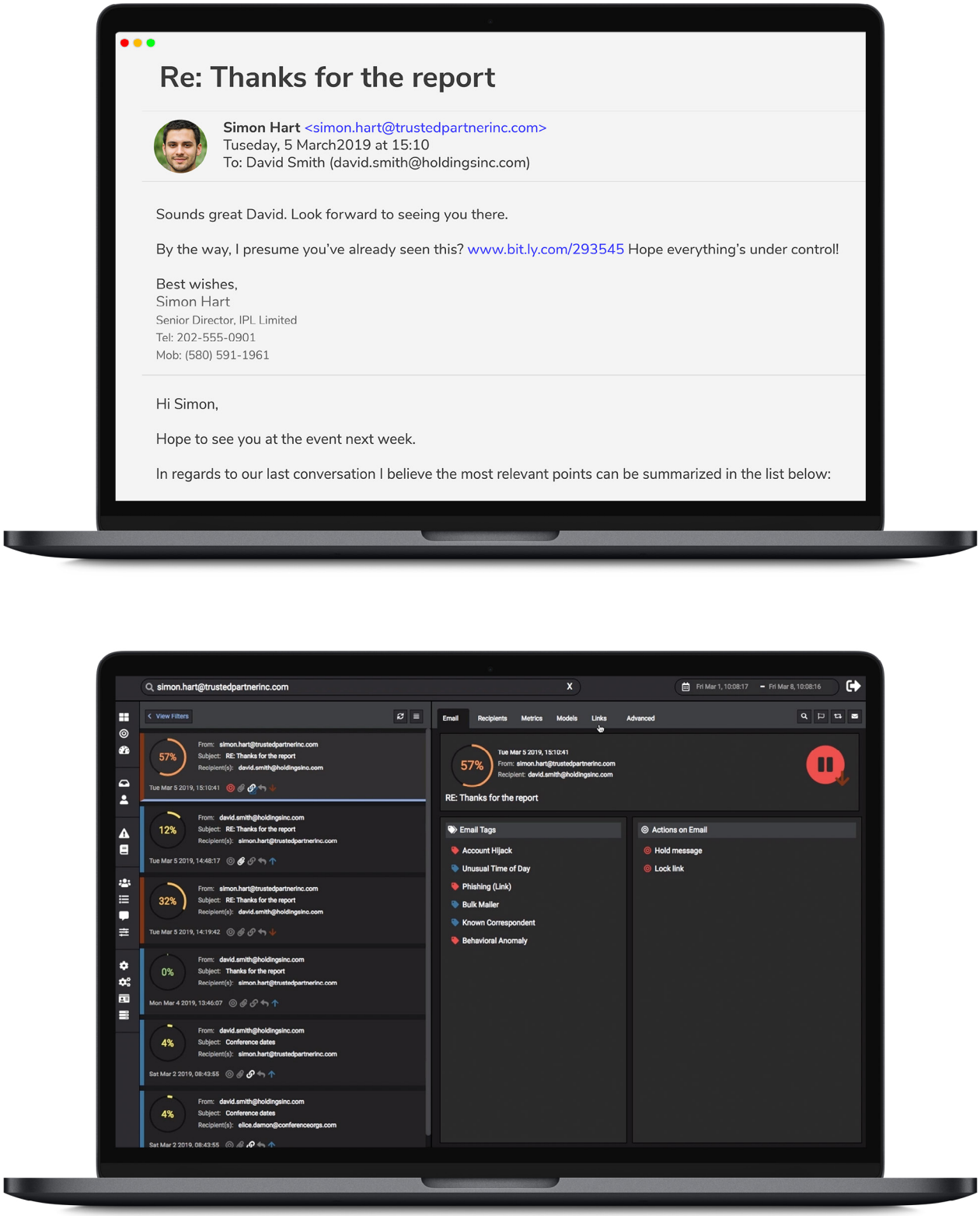


図 9: 一連のメールでのやり取りの後、信頼のおけるサプライヤーの乗っ取られたアカウントから送られてきたもっともらしい返信。リンクには悪意あるペイロードが含まれていました。

連続サプライチェーン攻撃

Antigena Email をトライアル運用中のある顧客は、2 日連続して深刻なインシデントに遭遇しました。信頼のおけるサプライヤーの E メールアカウントが、おそらくは侵入を受けた後、悪意ある攻撃の発信元となっていたのです。

Antigena Email は自動アクションを実行するように設定されていなかったため、ユーザーはこれらの E メールの内容に完全にさらされることになりました。しかし、Antigena Email が E メールを保留しリンクペイロードを二重ロックしたであろうと指摘したすべてのケースに対し、Microsoft 内蔵のセキュリティツールは何らの疑わしさも検知しておらず、アクションを取らずにすべてを通過させていました。

インシデント 1 – コンサルティング会社

最初のケースでは、Antigena Email は送信者がこの会社にとってよく知る相手であることを認識していました。社内の多数のユーザーがこの相手と以前に直接やり取りしていたからです。実際、インシデント発生前、同じ日にユーザーの 1 人が、その後ほどなくハイジャックされるアカウントと通常のやり取りを行っていたのです。問題のサプライヤーは英国にある環境関連のコンサルティング会社でした。

この普段通りのやりとりから 2 時間も経たないうちに、フィッシングリンクを含む E メールが 39 名のユーザーに次々と送信されたのです。E メールの件名とリンクにはバリエーションがあり、よく準備をした攻撃者からの高度に的を絞った E メールであることが推察されます。リンクの目的は支払いの要求や、パスワードの取得、マルウェアの展開であったかもしれません。

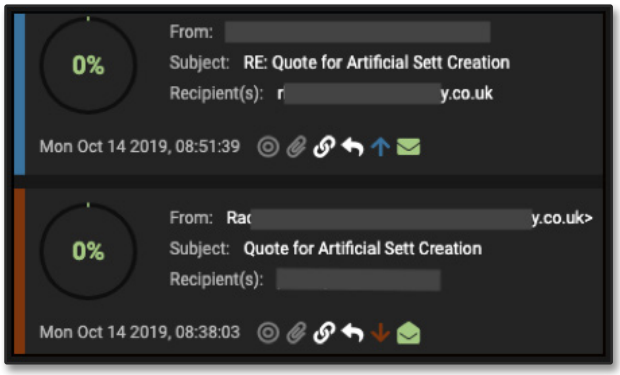


図 10: 送信者との以前の「正常な」通信 – 特異スコアは 0%

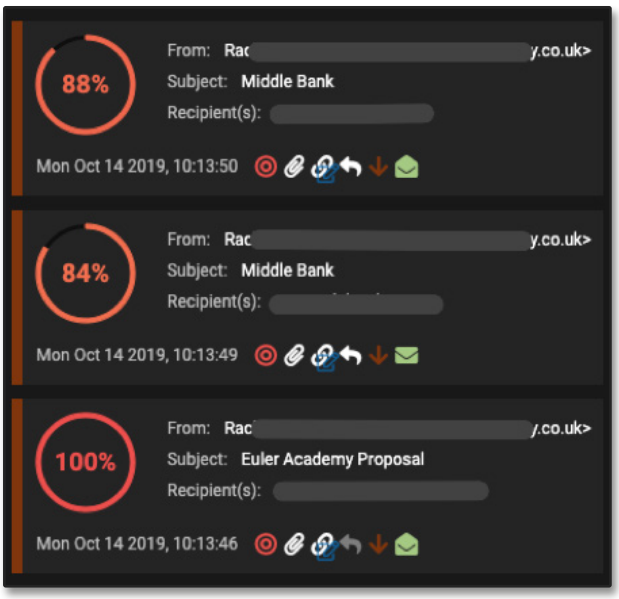


図 11: 同じ日にそれ以降送信された悪意ある添付ファイルを含む E メール

Antigena Email はサプライチェーンアカウント乗っ取りによくある多数の危険信号を特定しました：

1. 珍しいログイン場所： Antigena Email はこれらの E メールが正規の Outlook Web サーバから送信されたものであると判断しました。そのことはこのサプライヤーにとって異常ではありませんでしたが、この接続データの内部からジオロケーションを含む IP アドレスを抽出することにより、攻撃者が米国内の IP からログインを開始したことがわかりました。しかしサプライヤーの通常のログイン場所は英国だったのです。

2. リンクの不整合性： E メールに含まれていたフィッシングリンクはすべて Microsoft Azure 開発者プラットフォームでホスティングされていました。これはおそらくホストドメインのレピュテーションチェックを回避するためです。azurewebsites.net の正統性は Web 全体で幅広く受け入れられていますが、Antigena Email は過去の通信の履歴に基づいてこのドメインは送信者ときわめて不整合であることを検知できたのです。未知のサブドメインであったことも、このホスト名が組織のネットワークトラフィックのコンテキストでは最高の希少性スコアを持つことを意味します。他の E メールセキュリティ製品はこうしたコンテキストに基づくインテリジェンスを利用していないため、このような結論に至ることは不可能であったでしょう。

3. 異常な受信者： 受信者の 'association anomaly' スコアはこの特定の受信者グループが同じソースから E メールを受け取る可能性を見積もったものです。調査にコンテキスト情報が加わっていった結果、3 通目のメールまでに Antigena Email はこの受信者グループが 100% 特異であるという推論を得ました。

Usage > Darktrace Host Rarity	100
Usage > Domain External User Hostnames	0
Usage > Domain Inconsistency Score	88

図 12: リンクの珍しさと不整合性を示すメトリック

4. トピックの特異性： これらの E メールの件名は、なるべく目立たないよう、仕事関連のものと見えるようにしたことがうかがえます。そのため、フィッシングに関連するようなキーワードを探そうとするシグネチャベースの試みであればすべて失敗したと思われます。しかし、Antigena Email はこれらの受信者が通常このスタイルのフレーズを使ったビジネス提案についての E メールを受信していないということを理解していました。

Property	Value
Recipient > Metrics > Association Anomaly	100

図 13: Antigena Email はこの受信者のグループの関連性が弱いことをすばやく検知しました

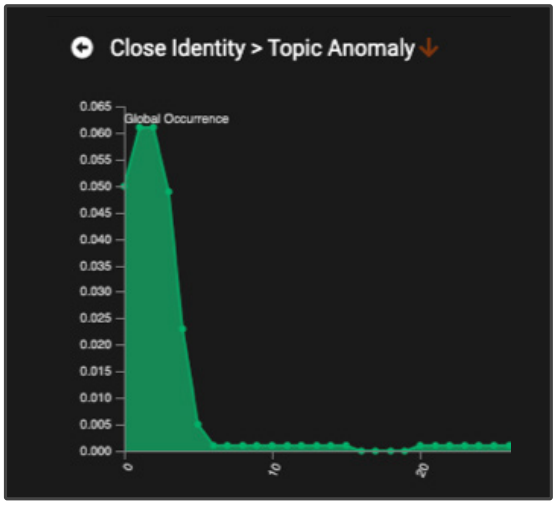


図 14: Topic Anomaly メトリックのサマリビュー

インシデント 2 – 侵入されたSaaSプロバイダ

次の日に起こった 2 番目の攻撃は、会社にとって既知の SaaS プロバイダから社内の 55 名のユーザーに対して E メールが送られたことでした。Microsoft ツールからは何のアクションもなく、これらの E メールの 50% 以上は受信者が開封しました。Antigena Email はこれらの E メールを保留して受信箱に入れない方が良いと提案しました。

1. 前回のインシデント同様、侵入を受けたアカウントから送られてきた E メールには、悪意あるフィッシングリンクが含まれていました。ただしこのケースでは、リンクがより長い期間アクティブな状態であったため、エンドユーザーに何が起こりえたかを正確に再構築することができました。

2. 幸いなことに、Antigena Email と Darktrace の Immune System Platform が共有するインテリジェンスにより、この E メールに接したユーザーを簡単に見つけ、アカウントを正常な状態に戻すことができました。また、Immune System は物理ネットワーク上のデバイスがフィッシングホストに接続していることを確認しました。Antigena Email との連携により、Immune System はネットワーク内でのこれらのフィッシングが疑われるドメインとの通信にフラグを立てることができました。

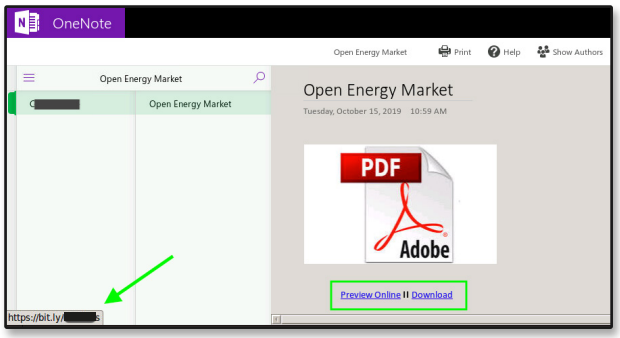


図 15: 隠れたリンクが表示されているスクリーンショット

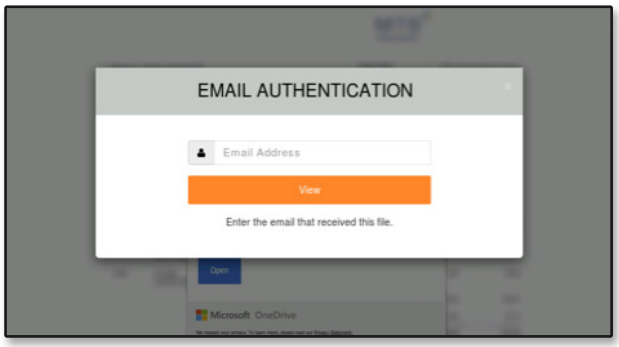


図 16: リンクにより、ユーザーの認証情報を盗み出すフォームが開きました

3. これらのリンクは Microsoft ATP 'safe- links' に組み込まれていましたが（ユーザーがクリックしたときに Microsoft がリアルタイムチェックを実行する）、ネットワークトラフィックに含まれていた実際のエンドポイントへの接続から、その時 Microsoft が利用できたインテリジェンスではこれらのリンクが安全であるとの結論に至ったものであり、ユーザーを悪意あるエンドポイントに露出させていたことが確認できました。

4. リンク自体はよく知られたファイル共有プラットフォームである SharePoint でホストされていました。リンクを踏むことによりユーザーにはエネルギー市場についてのレポートに見せかけたドキュメントが提示されます。ところが、ファイルをダウンロードするためのボタンを押すと、ユーザーの E メールとパスワードの入力を促す別のもっともらしい Web ページが表示され、これらの情報が直接攻撃者に送信されていたのです。

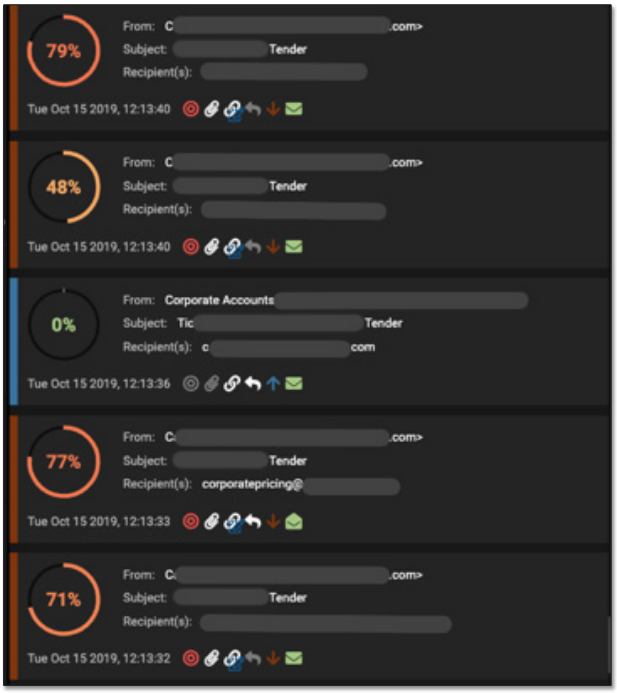


図 17: インシデント 2 の E メールを Antigena Email コンソールで見たところ。返信として送出されたものも含まれる 'Corporate Accounts' ユーザーがチケットを開くことにより E メールを承認していることがわかります

OneDrive ページに隠された悪意あるファイル

高度な脅威アクターが、信頼されるアカウントを使用して悪意あるペイロードを組織内に送信することにより、大手ホテルグループのサプライヤーの E メールアカウントを乗っ取りました。この攻撃はこの会社が持っていた従来型の防御システムをすり抜けることができましたが、Antigena Email は脅威を数秒で無害化しました。

1. 以前の E メールの分析により、Antigena Email は 2 つの送信者の間に関係があることを理解していました。

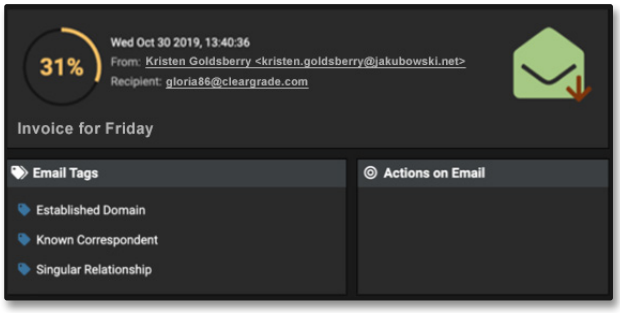


図 18: 以前の通信の例

2. 送信者の以前の通信パターンと比較して、それ以降の E メールは特異性が高いとフラグが立てられました。

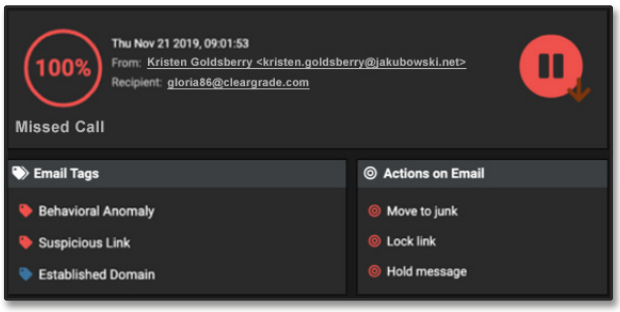


図 19: 後の E メールには 3 つのモデルに対する違反がタグ付けされました

3. 図に示す通り、これらの E メールはすべて 'Behavioral Anomaly' モデルでタグ付けされています。Antigena Email は、とるべき最良のアクションは宛先となっている受信者への配信を差し止めることだと判断しました。

4. Antigena Email は外部送信者の通常の「生活パターン」からの複数の逸脱点を特定しています。これには 'Anomalous Source Country' と 'Anomalous Source IP address' も含まれます。

5. E メールに含まれていた悪意のあるリンクも、この会社の E メールおよびネットワークトラフィック全体の「生活パターン」との不整合性が高く、その結果 Antigena Email によりロックされました。

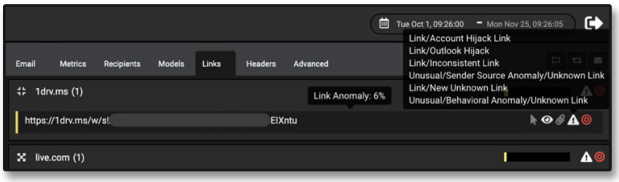


図 20: 悪意あるリンクが特定されました

6. リンク自体は、'Retrieve Message' という表示テキストの裏に隠されており、OneDrive のページに飛びます。ファイルストレージドメインを使って悪意のあるコンテンツをホストすることは従来のアプローチでは特定が困難です。それは SharePoint などのサービスをブラックリスト化することは不可能なことと、この例のようなリンクが悪性か良性かを判断するには、E メールを組織全体のコンテキストから理解する必要があるためです。

ソーシャルエンジニアリングと勧誘

「当社では Antigena Email を導入しましたが、従来のセキュリティツールも運用しています。従来のツールでは見つからなかった、Antigena Email で見つかったものを見て衝撃を受けています。」

– CTO、Bunim Murray Productions 社

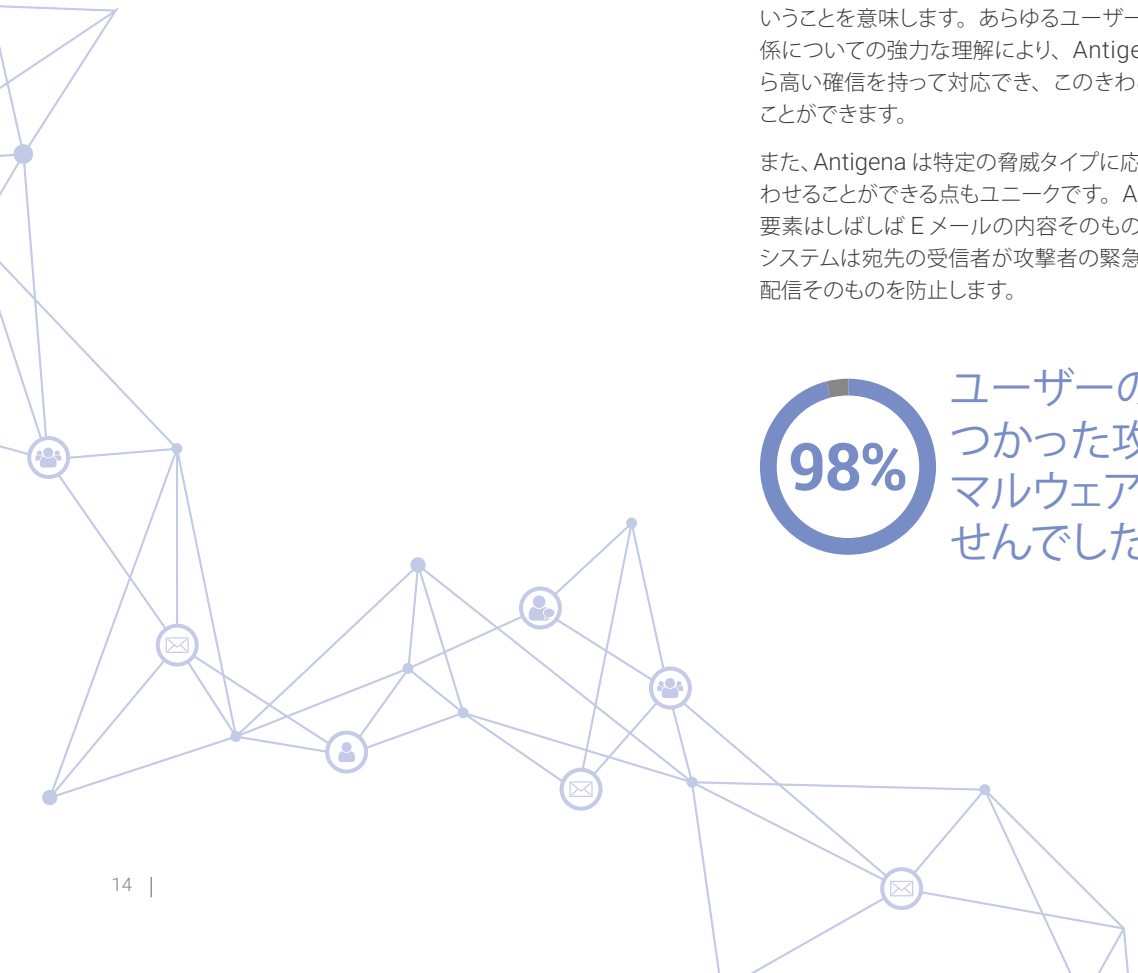
ソーシャルエンジニアリングおよび勧誘攻撃には、多くの場合洗練されたなりすまし行為が含まれます。偽装した攻撃者が受信者に対して緊急の返信を要請し、通信をオフラインに持ち込むまたはオフラインの取引を実行するなどします。彼らの目的は送金詐欺から産業スパイ、IP 盗用までさまざまです。セキュリティトレーニングに投資し、怪しい兆候に気を付けるよう従業員を教育するべきなのはもちろんですが、どれほどの指導を行っても、これらのますます洗練されていく攻撃に対してまったく無傷でいられる保証はありません。

従来のフィッシング攻撃は、一般に悪意あるペイロードをリンクまたは添付ファイルに隠したものですが、ソーシャルエンジニアリング攻撃では多くの場合、テキストのみが含まれる「クリーンな E メール」が送信されます。これらの攻撃は、リンクや添付ファイルをブラックリストやシグネチャに相関づける方法に依存した従来のセキュリティツールを容易に通過することができます。さらにこの攻撃ベクトルは通常、新しい「そっくりな」ドメインを登録することにより、受信者を欺くばかりでなく従来型防御も回避します。

Antigena Email は、ビジネスと共に変化する、E メールとネットワーク全体に渡る「正常」の統一された理解を持っているため、ごく目立たない勧誘のメールも検知することができます。従来型防御をすり抜けるクリーンな E メールも、既知のユーザーとの不審な類似性や、内部受信者間の関連性の異常、または E メールの内容と件名の異常までを含む幅広いメトリックの存在により数秒で検知できます。

多くの場合、ソーシャルエンジニアリング攻撃は直ちにコミュニケーションをオフラインに持ち込もうとします。このことは、動きの遅い受動的なセキュリティ手法では、たいてい被害が発生した後にしか対応できないということを意味します。あらゆるユーザー、デバイス、そして組織内の関係についての強力な理解により、Antigena Email は積極的かつ最初から高い確信を持って対応でき、このきわめて重要な初期段階で介入することができます。

また、Antigena は特定の脅威タイプに応じてインテリジェントに対処を合わせることができる点もユニークです。Antigena は勧誘攻撃の「危険な」要素はしばしば E メールの内容そのものであることを理解しているため、システムは宛先の受信者が攻撃者の緊急の要請に応える機会を得る前に配信そのものを防止します。



ユーザーの受信箱から見つかった攻撃の 98% にはマルウェアが含まれていませんでした

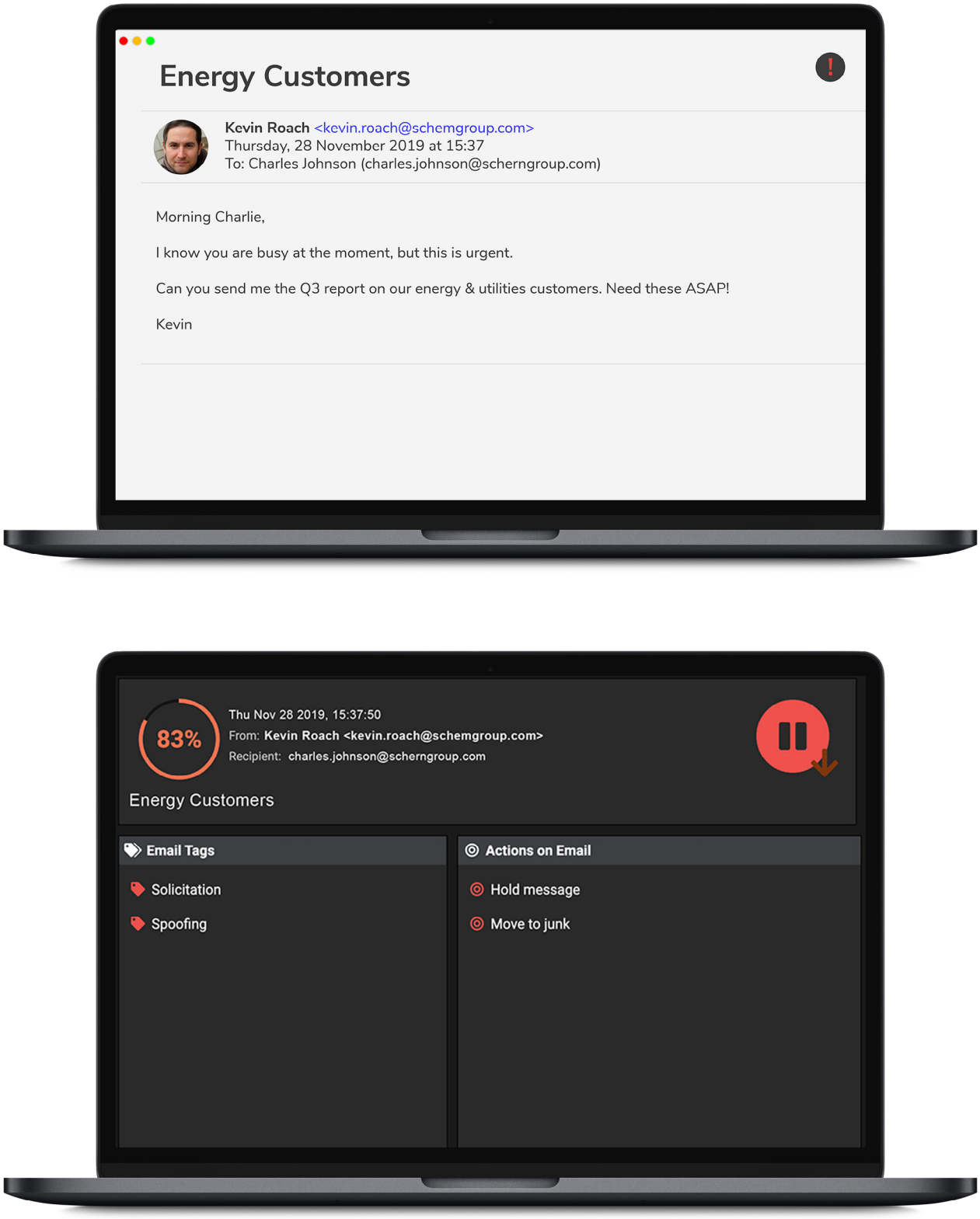


図 21: 攻撃者がエグゼクティブを装って機密情報を取得しようとしています。E メールアドレスが偽装されています。

なりすまし攻撃

Antigena Email は多国籍テクノロジー企業の 30 名の従業員を標的とした攻撃を検知しました。詳細なリサーチが行われたことは明らかでした。攻撃者は各ユーザーに対して、彼らがやりとりするであろう最高責任者レベルのエグゼクティブに注意深くなりすましたのです。Antigena Email はこれがソーシャルエンジニアリング攻撃であることを特定し、その結果各 E メールが宛先に送信されないよう保留しました。

1. 各メールの件名には標的となった従業員のファーストネームが含まれ、送信元は一見無関係な Gmail アドレスでした。悪意あるペイロード（リンクや添付ファイルなど）が含まれていなかったにも関わらず、Antigena Email はこれらの E メールを悪意あるものと識別することができました。

2.Darktrace はそっくりに作られたドメイン名を識別しただけでなく、これらの E メールが 'No Association' モデルの違反であることを識別しました。これは、この会社の E メールとネットワーク環境全体の理解に照らして、送信者と組織の間に関係があるという証拠が見つからないということを意味します。

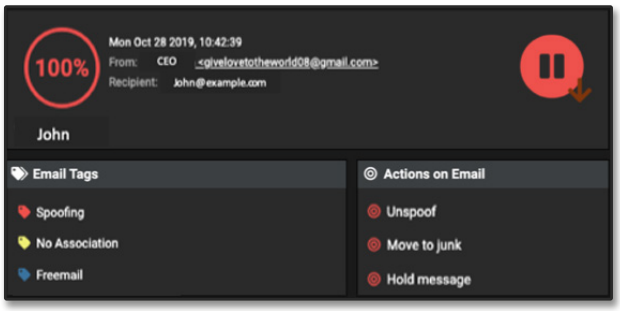


図 22: 30 件の E メールのうち 1 つは、特異スコアが 100% を示していました

3. 複数の弱いインジケータを相関づけることにより、Antigena はこれらの E メールを 1 つの連携した攻撃の要素であると認識し、セキュリティチームによるレビュー対象としてバッファに保留しました。

4. Antigena Email はなりすましされた 3 人の最高責任者レベルのエグゼクティブを特定しただけでなく、CEO が実際に外部で使っていた個人用アドレスを偽装したものが使われていたことも特定しました。

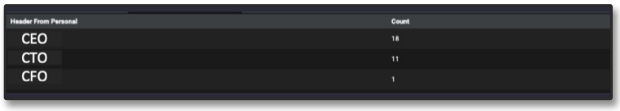


図 23: 特定された 3 人の最高責任者レベルのエグゼクティブ

5. さらに、なりすましされたユーザーの露出スコアが高い値を示していました。つまり彼らは重要標的であることを意味し、そのため 'Whale Spoof' モデルの違反となったのです。重要な社内ユーザーが標的にされたことを理解した結果、Darktrace の AI はこの攻撃の優先度を高め、リアルタイムに適切な対処を開始しました。

CEO の支払い要求

ある電気事業者において、DarktraceのAIはOffice 365のEメールアカウントの 1 つに明らかなスプーフィングの試みがされていることを検知しました。会社の CEO からとされるこの E メールは、支払い課のメンバーに送信されており、CEO の振込先情報を更新することを求めていました。

この E メールは CEO の通常のメールのスタイルをまねることに成功していたため、もし Darktrace の AI がこの会社の E メールの流れをビジネスの他の部分との関連性に基づいて分析していなければ、この攻撃は容易に成功していたかもしれません。

1. 従業員、CEO そしてクラウド上に広がる組織全体とネットワークトラフィックの通常の「生活パターン」を学習することにより、Darktrace は E メール内のいくつものわずかな異常性を即座に特定することができたのです。これには偽造された送信者アドレスも含まれていました。

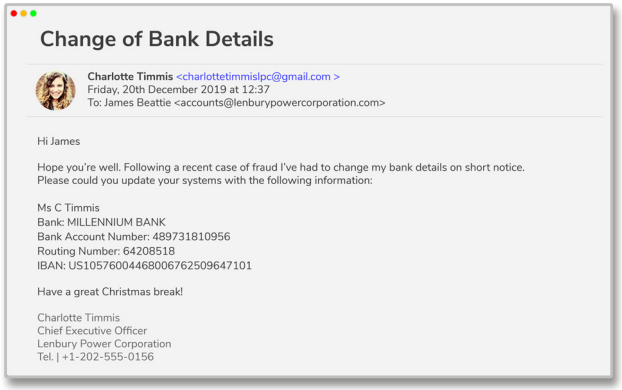


図 24: CEO になりすました E メールのスクリーンショット

2. その他の弱い兆候の中から、Darktrace の AI はこのドメインと社内の従業員や信頼される連絡先との近接性の異常も自動的に計算していました。

3.AI は即座に対応し、E メールのリンクをロックするとともにこのメールが支払い課に届く前にスプーフィングである旨を明確にマークしました。Darktrace のクラウドおよびネットワークトラフィックに対する詳細な理解により、シグネチャベースのツールであれば見逃されていたであろう深刻度の高い脅威を無害化することができました。

財務担当副社長スプーフィング攻撃

このインシデントには有名な金融機関の財務担当副社長のなりすましが関係していました。脅威アクターは 11 件の同様な E メールをこの組織に送信しましたが、Antigena Email はネットワーク、クラウド、E メールトラフィック全体に渡る「正常」の多元的理解によりこれらをすべて保留にするアクションを実行しました。関係のない、明らかに異常な E メールアドレスを E メールの内容に照らして分析した結果、Darktrace はなりすましの試みを識別しましたが、この会社の従来型ゲートウェイは 11 件すべてのメールを通過させていました。

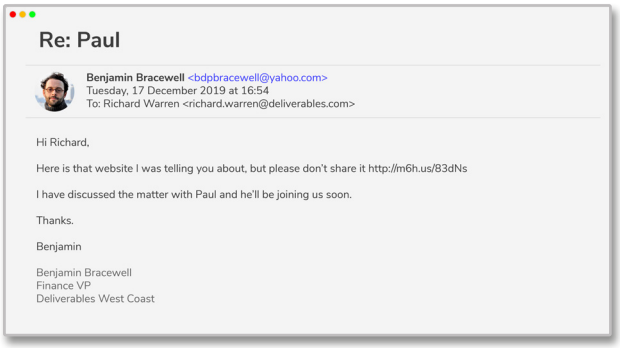


図 25: 疑わしいリンクを含む E メールのスクリーンショット

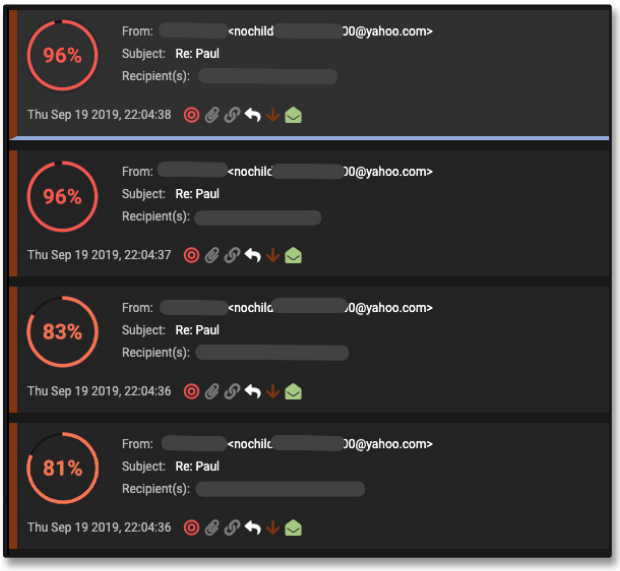
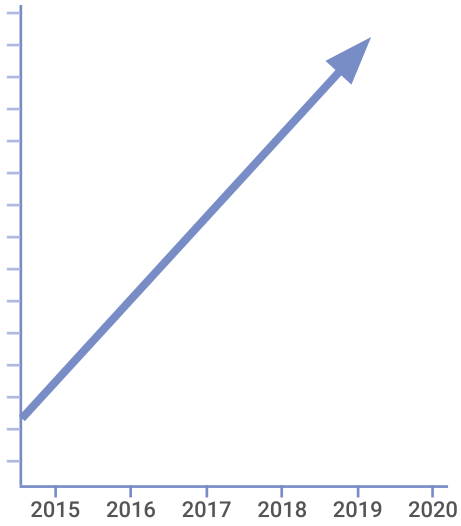


図 26: 11 件の E メールのうち高い特異スコアを示す 4 件と、関連する Antigena Email アクション

従業員の認証情報流出

認証情報の流出は 2016 年から 2019 年にかけて 280%増加しました



ビジネスリーダーは会社のメールボックスがどれほど貴重なものであるか、それが悪人の手に渡るまでは滅多に考えることはないでしょう。しかし一旦侵入してしまえば、脅威アクターは幅広い攻撃オプションや踏み台を選択することができます。フィッシング攻撃、総当たり攻撃、あるいはダークウェブ上での取引など、攻撃者が容易にアクセス権を獲得できることは大いに警戒すべきです。

多くのケースで、攻撃者はあなたの受信箱から貴重なデータを強奪しようとします。私的なチャットに含まれる個人情報や請求書の内容などは詐欺や恐喝に使われる可能性がありますし、古いメールスレッドには機密性の高い企業情報が含まれているかもしれません。顧客リスト、価格情報、ロードマップや IP の情報までも、わずかな単語を検索することで見つかってしまいます。

また、犯罪者がアカウントを次の攻撃ステージの開始点として使用するケースもあります。彼らは目立たないよう背後に潜んで重要なエグゼクティブやパートナーに関するインテリジェンスを収集し、ドキュメントをレビューし、会話を読み、最終的な攻撃実行時にどのように紛れ込むかを学習するのです。サプライチェーンのアカウント乗っ取り同様、継続中の E メールのスレッドを読み、もっともらしい返信を続けることは、多くの場合疑いを持たれることなく攻撃ミッションを達成する最も効果的な方法です。

攻撃者にとっての可能性はほぼ無限にありますが、防御側の選択肢は限られています。社内アカウントの乗っ取りは多くの場合、'impossible travel'（あり得ない移動）ルールなど、シンプルで静的な防御システムによって監視されていますが、隠れる方法を知っている攻撃者をこれで捕まえられることはめったにありません。しかし、Darktrace の Immune System Platform はエンタープライズ全体の視野をもつことにより、これらのルールベースのアプローチを補完し、これらの防御を通過する脅威を捕捉します。

あらゆるユーザーの通常の「生活パターン」を学習することにより、Immune System は疑わしいログイン動作、受信箱ルールの作成、あるいはユーザー権限の編集などに現れるわずかな逸脱も特定して、最も注意深い犯罪者をも明らかにします。サイバー脅威が進化しより高度になるにつれ、デジタルビジネス全体に自己学習型の AI を活用することは、企業の受信箱に犯罪者を寄せ付けないための唯一の有効な方法となるでしょう。

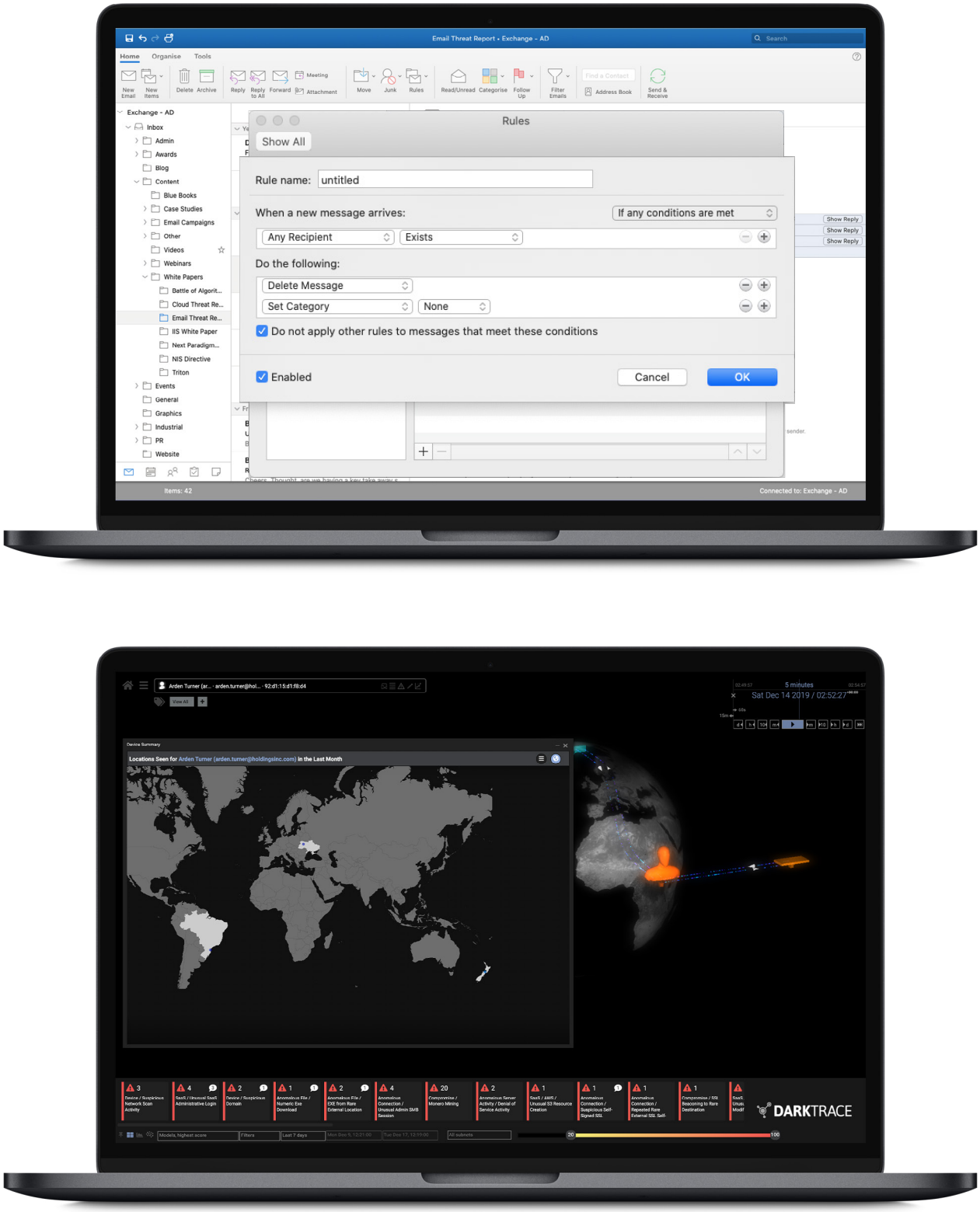


図 27: 侵入されたアカウントに設定された E メール処理ルールと Threat Visualizer に表示されたログインの地理的位置

パナマの銀行での異常なログイン

ある Office 365 アカウントがパナマの大手銀行に対する総当たり攻撃に使用され、ログインはこの会社の業務の通常の「生活パターン」とは離れた国から発生していました。

Darktrace は 7 日間に渡り 885 回のログインを特定しました。認証のほとんどはパナマの IP アドレスからのものでしたが、そのうち 15% は 100% 未知のインドにある IP アドレスからのものでした。さらに分析を行うと、この外部エンドポイントは複数のスパムブラックリストに含まれていることがわかり、最近オンラインでの、おそらくは不正なインターネットスキャニングやハッキングとみられる攻撃的な行為に関連するものでした。

図 28: ログイン場所を示すユーザーインターフェイス

Darktrace はその後パスワードリセット機能の不正使用と思われる動作を観測しました。インドにいるユーザーが非常に不審なやり方でアカウント権限の変更を行っていたのです。この動作が特に疑わしいものとしてマークされた理由は、パスワードリセット後、普段この組織と関連のある IP からログイン試行の失敗が見られ、正しいユーザーがロックアウトされている疑いがあったからです。

03/12 20:45:39	Saas::Admin	Regular	UpdateUser
03/12 20:45:39	Saas::Admin	Regular	ChangeUserLicense
03/12 20:26:43	Saas::Login	Regular	UserLoggedIn
03/12 20:26:43	Saas::FailedLogin	Regular	UserLoginFailed
03/12 20:26:36	Saas::FailedLogin	Regular	UserLoginFailed
03/12 18:31:31	Saas::Login	Regular	UserLoggedIn
03/12 17:57:46	Saas::Admin	Regular	ChangeUserLicense
03/12 17:57:46	Saas::Admin	Regular	UpdateUser
03/12 17:06:57	Saas::Admin	Regular	UpdateUser

図 29: この SaaS アカウントに関連した動作。認証情報の変更がハイライトされています

日本の田園地方からのアクセス試行

ヨーロッパにある金融サービス企業において、Office 365 の認証情報を使って日本の田園地方のとある場所に関連付けられた未知の IP アドレスからのログインが観測されました。

ユーザーが旅行する、またはプロキシサービスを使って遠隔地からアクセスすることはあり得ますが、認証情報の流出および不正なユーザーからの悪意あるアクセスの可能性を強く示すものとも考えられます。アクセスポイントが通常アクセスのある IP とは著しく異なることから、Darktrace は異常であるとフラグを立て、即座に詳細の調査を行うよう提案しました。

セキュリティチームはリモートからこの Office 365 アカウントをロックし、認証情報をリセットして悪意のあるアクターがこれ以上活動できないようにしました。このアクティビティに気づくことがなければ、脅威アクターはアクセス権限を使って組織にマルウェアを展開する、または支払いを要請する詐欺などを行ったかもしれません。

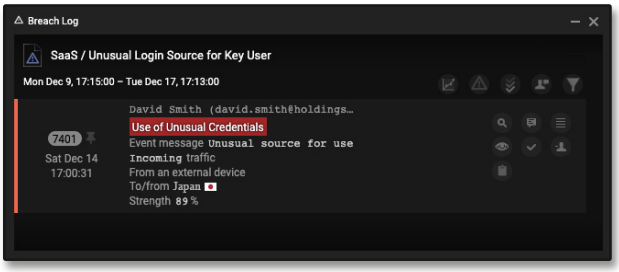


図 30: 日本からのログインは複数のモデルに対し違反となりました

Office 365 アカウントの乗っ取りと妨害

国際的な非営利団体で、Darktrace は Office 365 のアカウント乗っ取りを検知しました。これは Azure AD の静的な 'impossible travel' ルールをすり抜けたものです。この組織は世界各地に事務所を展開していましたが、Darktrace の自己学習型 AI は 1 つの IP アドレスからのログインがそのユーザーおよび所属するグループの履歴から見て異常であることを特定し、即座にセキュリティチームに警告しました。

その後 Darktrace はそのアカウントに対して受信および送信メールを削除するような新しい E メール処理ルールが設定されているという事実に注意を喚起しました。これは明らかに侵害を示すものでありセキュリティチームは攻撃者が損害を与える前にこのアカウントをロックすることができました。

この新しい E メール処理ルールの設定により、攻撃者は本当のユーザーがまったく知らない間にこの組織の他の従業員と数々のやり取りを開始することができたはずです。これはサイバー犯罪者が永続的なアクセスを獲得し組織内で複数の足掛かりをつかもうとする際によく使用される戦略で、より大規模な攻撃の準備の可能性があります。

未知の IP アドレスと見かけ上のユーザーの特性にそぐわない行動と併せて分析することにより、Darktrace はこれをアカウント乗っ取りであることを確信を持って特定し、業務への深刻な被害を防ぎました。

自動化された総当たり攻撃

Darktrace は Office 365 アカウントで複数回の失敗したログインイベントを検知しました。これは同じ認証情報を使って、1 週間に渡り毎日発生していました。6 日間、まとまったログイン試行が 6.04pm ぴったりに実行されていました。時刻とログイン試行回数が一致していたことは、ロックアウトを避けるために一定の回数失敗した後停止するようプログラムされた、自動的な総当たり攻撃を示すものでした。

Darktrace はこのログイン試行の失敗のパターンは異常性が高いとしてセキュリティチームに警告しました。複数の弱いインジケータを相関づけ、出現しつつある脅威のわずかな兆候を具体的に説明する Darktrace の存在がなければ、この自動化された攻撃は何週間、あるいは何ヶ月も継続し、収集された他の情報に基づいてユーザーのパスワードを推測した可能性もあります。

図 31: 繰り返しログインの試行がされたことを示すグラフ

ダークトレースについて

ダークトレースは、サイバーセキュリティ分野で世界をリードする AI 企業で、内部ネットワークの脅威を自動遮断する技術を世界で初めて開発しました。人間の免疫システムに着想を得たダークトレースの自己学習型 AI は世界各国で 3,000 社以上の組織に導入されています。クラウド、E メール、IoT、企業ネットワーク、産業用制御システムなどあらゆる種類のネットワークインフラを、内部脅威、産業スパイ、IoT デバイスのハッキング、ゼロデイのマルウェア、データの損失、サプライチェーンリスク、長期にわたる重要インフラの脆弱性などを含む未知の脅威からリアルタイムに保護します。

従業員数は 1,000 名を超え、本社は米国サンフランシスコと英国ケンブリッジにあり、世界に 44 の拠点を置いています。ダークトレースの AI は平均 3 秒毎に新たなサイバー脅威に自動対処しており、損害がもたらされる前に顧客を保護しています。

お問い合わせ

東京: +81 (03) 5456 5537
大阪: +81 (06) 6133 4570
シンガポール: +65 6804 5010
米国: +1 (415) 229 9100
japan@darktrace.com | darktrace.jp
@darktraceJP