DARKTRACE

Ciber IA da Darktrace

Um Immune System para e-mail

> Mais do que nunca, a segurança moderna de e-mail exige inovação e uma mudança de mentalidade para combater o cenário de ameaças em evolução.
>
> **– Peter Firstbrook, Analista vice-presidente da Gartner**

Introdução

Conteúdo

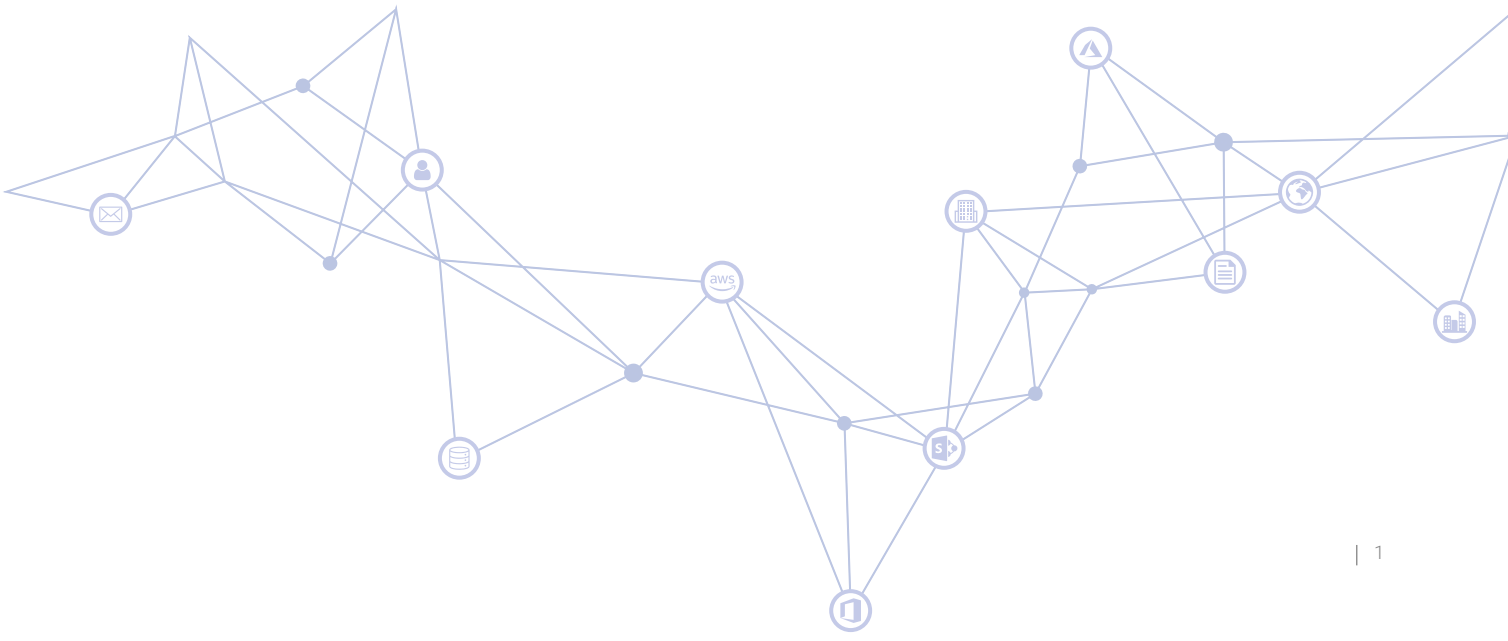
As plataformas de colaboração e e-mail representam o tecido conjuntivo de qualquer negócio digital. Informações são compartilhadas, projetos são elaborados e alianças são formadas no mundo digital da correspondência escrita. No entanto, como um meio conduzido por pessoas, o e-mail sempre será abastecido por uma suposição generalizada de confiança que permanece como o "elo mais fraco" da estratégia de segurança de uma organização.

Embora essa suposição de confiança seja fundamental para a colaboração e o crescimento, ela significa que o e-mail, mais do que qualquer outra área da empresa, permanecerá estruturalmente resistente ao espírito moderno de "confiança zero", e, portanto, não surpreende que 94% das ameaças cibernéticas ainda tenham origem nele.

Para minimizar a influência de falhas humanas nessa área, o setor em geral chegou à conclusão de que se deve contar com a tecnologia para identificar e-mails maliciosos que nem mesmo os funcionários mais exigentes e bem treinados são capazes de identificar. No entanto, até recentemente, as defesas tradicionais se esforçavam para acompanhar as inovações no cenário de ameaças cibernéticas.

Spear-phishing, ataques de clonagem e aquisição do controle de contas, em particular, ainda são vias de ataque frutíferas para criminosos cibernéticos que buscam se infiltrar em uma organização com facilidade. Ataques direcionados a e-mails desse tipo, juntamente com as limitações das defesas tradicionais, continuam sendo um grande desafio até mesmo para as organizações com estratégias de segurança mais avançadas e maduras.

Peter Firstbrook, Analista vice-presidente da Gartner, resume bem a dinâmica do mercado: "Controles comuns, como antispam padrão com base na reputação e antivírus baseado em assinaturas, são adequados para ataques generalizados e campanhas de fraude, mas não são bons o suficiente para proteger contra ataques mais direcionados, sofisticados e avançados. Mais do que nunca, a segurança moderna de e-mail exige inovação e uma mudança de mentalidade para combater o cenário de ameaças em evolução."



IA da Darktrace: Plataforma do Immune System

No entanto, graças ao recente surgimento da IA em escala corporativa, essa "mudança de mentalidade" finalmente se concretizou na forma de uma abordagem de "sistema imunológico" para a segurança de e-mail.

Como sugere Firstbrook, as defesas tradicionais de e-mail podem ser adequadas para ameaças simples e indiscriminadas, mas não são projetadas para combater ataques mais avançados que foram personalizados para destinatários e empresas específicos.

Gateways de e-mail legados e controles nativos dependem de regras codificadas e de um conhecimento de ataques históricos para detecção. Portanto, seu alcance é necessariamente limitado a ameaças conhecidas ou que são pelo menos básicas o suficiente para acionar uma regra estática e binária na fronteira. Porém, como muitos líderes empresariais podem dizer com base em sua experiência, esse não é o desafio que enfrentamos.

Felizmente, a mudança de paradigma que surgiu na segurança de e-mail ficou fora de uma distinção importante entre a "abordagem comum" de Firstbrook e uma nova aplicação da IA em escala corporativa. Essa distinção é comparada à diferença entre a "pele protetora" de uma organização e seu "sistema imunológico" de aprendizagem para ameaças que se infiltram.

Enquanto a "pele protetora" conhece os ataques históricos e pode interromper ameaças conhecidas, o "sistema imunológico" conhece os "padrões de vida" que caracterizam o fluxo de trabalho digital de cada funcionário. Essencialmente, esses "padrões de vida" se manifestam não apenas no tráfego de e-mail, mas também no tráfego da rede e da nuvem, e de uma maneira que pode ser unificada em uma imagem abrangente e em evolução de normalidade para cada usuário.

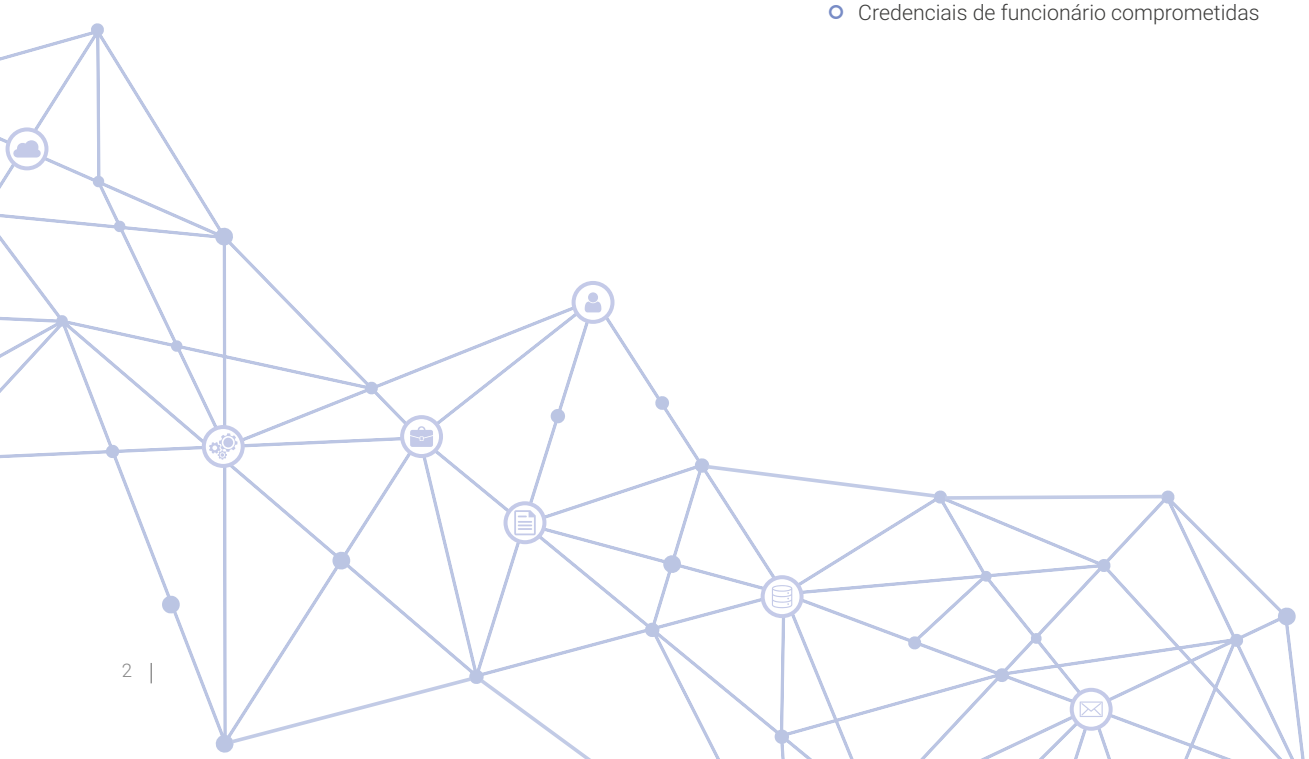
Esse entendimento único de toda a empresa tem permitido que as organizações neutralizem mais do que nunca ataques direcionados, pois continua sendo a única abordagem que pode fornecer evidências suficientes para determinar com precisão se desvios sutis em um e-mail direcionado são realmente mal-intencionados.

Pela primeira vez, nossas defesas de e-mail podem perguntar de maneira significativa se seria estranho um usuário receber um e-mail com base no que o sistema conhece sobre os "padrões de vida" desse funcionário, de seus colegas e de toda a organização, não apenas em relação a e-mails, mas também na nuvem e na rede corporativa.

Trata-se também da única abordagem que pode atualizar suas decisões e ações à luz de novas evidências, mesmo após a entrega de um e-mail – independentemente dessa evidência se manifestar no e-mail ou em comportamentos mal-intencionados que surjam na rede.

Este White Paper foi desenvolvido para ilustrar por que um entendimento unificado e personalizado do tráfego na rede, na nuvem e de e-mail representa uma mudança de paradigma no mercado de segurança de e-mail. A Darktrace foi pioneira nessa abordagem com a Antigena Email e sua Plataforma de Enterprise Immune System. Os case studies a seguir se enquadram em uma das quatro categorias de ataques altamente sofisticados que burlam rotineiramente a "pele protetora", mas que são neutralizados facilmente pela IA da Darktrace em segundos:

- Spear-phishing e entrega de carga
- Aquisição do controle de contas na cadeia de suprimentos
- Solicitação e engenharia social
- Credenciais de funcionário comprometidas



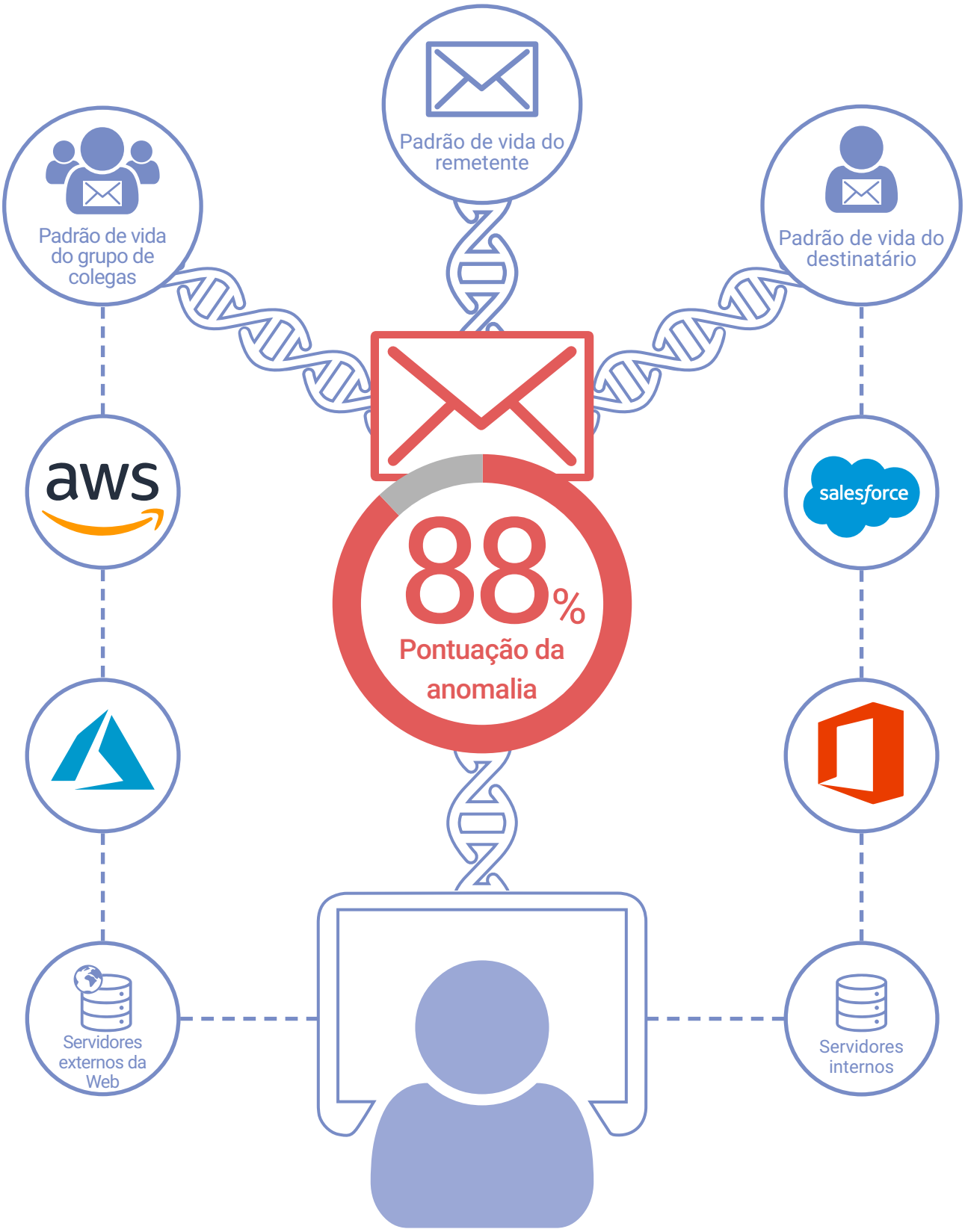
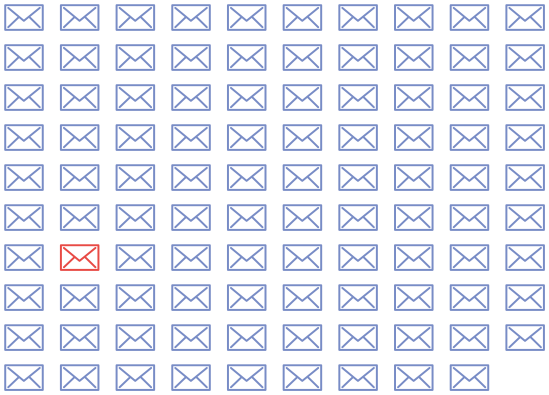


Figura 1: A Antigena Email é a única solução que analisa e-mails no contexto da organização como um todo, não apenas dados de e-mails. Esse entendimento de toda a empresa permite identificar e-mails mal-intencionados que se esquivam das defesas tradicionais na fronteira.

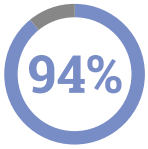
Spear-phishing e entrega de carga

> Com seu entendimento de "normal" em relação ao tráfego de e-mail e da rede, a Antigena Email tem sido incrivelmente valiosa na captura de ameaças.
>
> **– Chefe de TI, Entegrus**

1 em cada 99 e-mails é um ataque de phishing



Fonte: Avanan



de malware têm origem na caixa de entrada

A maioria das campanhas de phishing tenta enganar os usuários e fazê-los clicar em links ou anexos mal-intencionados em um e-mail com o objetivo principal de coletar credenciais ou implantar malware destrutivo em uma organização. Esses ataques podem ser lançados como campanhas "drive-by" indiscriminadas contra milhares de organizações, ou como ataques "spear-phishing" elaborados e personalizados para um destinatário ou uma empresa em particular.

Para se proteger de campanhas de phishing, as defesas tradicionais normalmente analisam os e-mails baseando-se no entendimento de ataques históricos, listas negras e assinaturas. Contudo, os criminosos cibernéticos entendem essa abordagem reativa melhor do que ninguém e têm todo incentivo para empregar novas táticas e técnicas que se esquivam das defesas legadas por padrão.

No entanto, como esses ataques nunca foram vistos antes, escaparão das defesas tradicionais na fronteira de entrada, eles serão altamente anômalos para o usuário ou a empresa visada – pelo menos se os "padrões de vida" de todo o ambiente digital for considerado. Essa realidade mostra por que é tão importante preencher a lacuna tradicional de conhecimento de segurança entre a camada de e-mail externa e a rede com um sistema como a Plataforma de Immune System da Darktrace.

Com a IA em escala corporativa, a Antigena Email pode analisar links, anexos, domínios, conteúdo e outros elementos de um e-mail juntamente com "padrões de vida" na nuvem e na rede, correlacionando um amplo conjunto de pontos de dados que revelam e-mails aparentemente benignos como inconfundivelmente mal-intencionados.

Diferentemente de qualquer outra solução, a Antigena Email e o Immune System podem correlacionar dados da rede, da nuvem e de e-mail para identificar se os domínios associados a uma carga e remetente são anormais, se a localização de um link em um e-mail é estranha, se os tópicos de discussão e o conteúdo são incomuns e até mesmo se os padrões no caminho da URL são suspeitos.

Essa abordagem fundamentalmente única significa que a tomada de decisão da Darktrace é muito mais precisa do que a de outras ferramentas, de modo que ela pode executar ações altamente proporcionais e direcionadas para neutralizar ataques de phishing em grande escala.

O Immune System também está na posição única de ser capaz de detectar um ataque em qualquer ambiente e executar automaticamente uma análise de causa raiz para verificar se ele se originou em e-mail. Nesse caso, ele protegerá instantaneamente todos os outros funcionários visados pelo mesmo ataque. Chamamos isso de resposta autônoma estratégica – quando a aprendizagem com o paciente zero possibilita a proteção estratégica do restante da empresa sem intervenção humana. Do ponto de vista de uma equipe de segurança, alguém ainda precisa limpar o laptop da primeira vítima, mas isso é muito melhor do que limpar 200 ou mais.

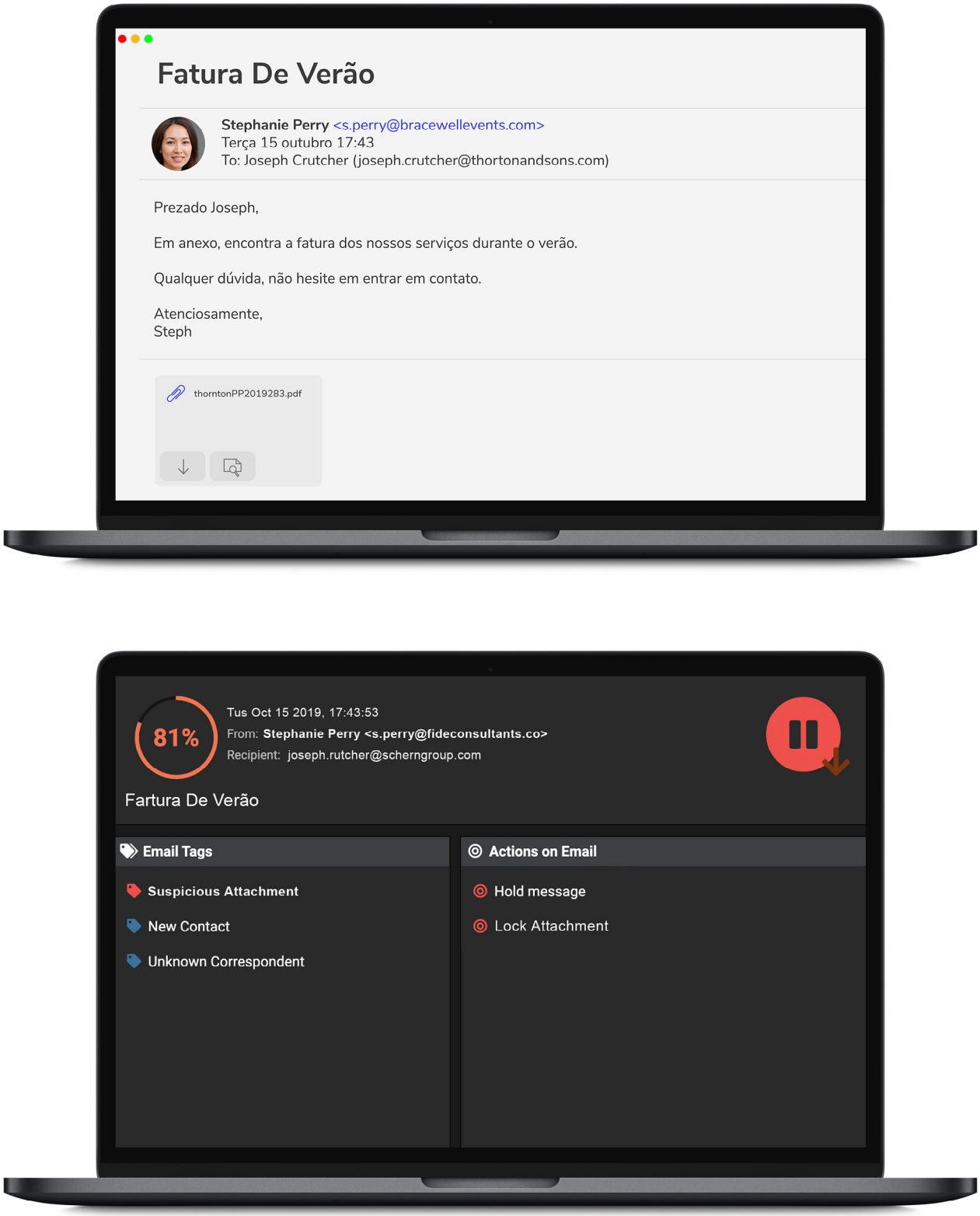


Figura 2: Um e-mail persuadindo um funcionário a clicar em um anexo contendo uma carga mal-intencionada e a visualização correspondente na interface do usuário da Darktrace, mostrando as tags de anomalia e as ações tomadas.

Ataque WeTransfer

A Darktrace detectou um ataque de phishing direcionado a cinco usuários de alto nível de uma organização acadêmica em Cingapura, cuidadosamente projetado para induzi-los a clicar em um link mal-intencionado.

A Antigena Email atribuiu a esses e-mails uma pontuação de 100% de anomalia e tomou medidas para "retê-los", impedindo sua entrega. Ele identificou também indicadores sutis de falsificação de serviço, apesar da organização ter um relacionamento conhecido com o remetente.

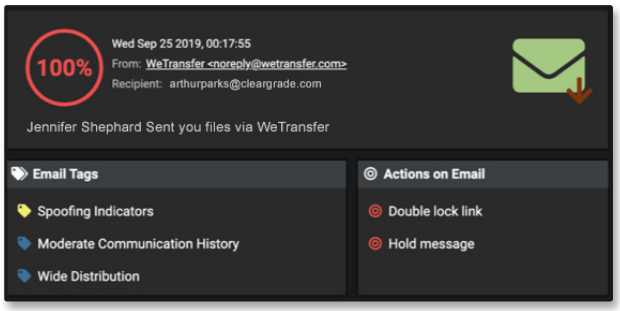


Figura 3: A interface do usuário mostrando as violações do modelo e ações

1. Nos dados do cabeçalho, não havia sinais claros de que o e-mail tivesse uma origem diferente do WeTransfer e teria parecido perfeitamente normal para o destinatário. A "Largura" e a "Profundidade" indicam que esse endereço de e-mail se comunicou com muitas pessoas na organização, em vários dias.

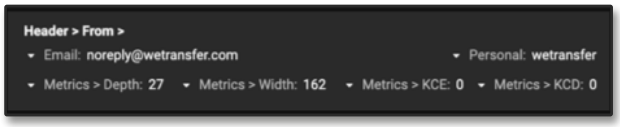


Figura 4: Os dados de conexão dos e-mails relevantes

2. No entanto, a Antigena Email pôde captar várias anomalias sutis, dado o entendimento de "normal" para o usuário e a organização, juntamente com o contexto adicional obtido da camada de rede.

a. Primeiro, a "Pontuação de anomalia do endereço IP" foi alta (63%). Com base nos padrões históricos de envio, essa métrica indica o quão incomum é para esse endereço de e-mail enviar mensagens usando esse IP, e isso é geralmente um indicativo de conta falsificada ou sequestrada.

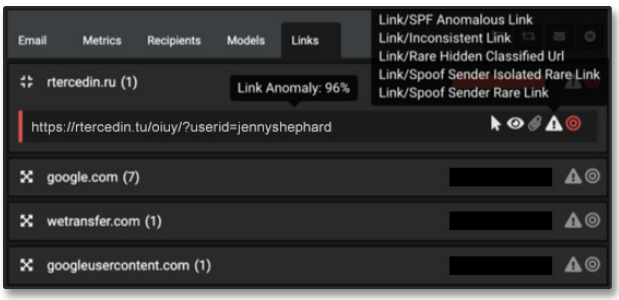


Figura 5: Um detalhamento dos links mostrados nos e-mails

b. Além disso, como a Darktrace constantemente modela o comportamento "normal" de cada remetente externo, ela pôde identificar uma anomalia importante no corpo do e-mail – um link que era altamente inconsistente com o que a Darktrace havia observado anteriormente do WeTransfer, permitindo à Antigena Email identificá-lo como carga maliciosa no e-mail.

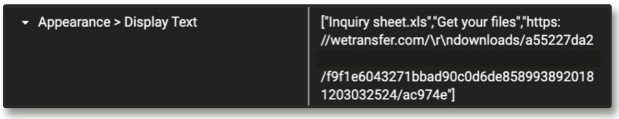


Figura 6: A Antigena pôde determinar onde o link apareceu no e-mail

c. O link em questão recebeu uma pontuação de 96% de anomalia e estava escondido atrás de links no estilo "clique aqui" em várias partes do e-mail, incluindo um link falso "https://wetransfer.com/..." (foto abaixo) e o texto "Inquiry Sheet.xls" e "Get Your Files".

Esse ataque contornou todas as ferramentas baseadas em assinaturas da universidade. De modo semelhante, como o link usava um domínio completamente benigno e não levava a uma carga obviamente maliciosos, provavelmente a detecção heurística e o sandboxing teriam falhado.

Malware oculto em faturas falsas

Um grande escritório de advocacia se tornou um dos principais alvos de uma campanha avançada de phishing, que procurava disfarçar um malware de roubo de credenciais em arquivos ISO anexados a faturas falsas. As defesas de e-mail tradicionais normalmente incluem arquivos ISO na lista de permissões, enquanto os sistemas operacionais montam automaticamente suas imagens com um único clique, tornando-os um atrativo óbvio para agentes de ameaças.

No entanto, quando uma pontuação de e-mails nocivos passou pelas defesas tradicionais de e-mail da empresa, a Darktrace capturou a campanha identificando um amplo alcance de indicadores anômalos. Por exemplo, um dos modelos de IA acionado pelos e-mails foi "Attachment/Unsolicited Anomalous MIME" (Anexo/MIME anômalo não solicitado), o que significa que o tipo MIME do anexo era altamente incomum para o usuário e seu grupo de colegas e que o destinatário nunca havia se comunicado com o remetente para solicitar o arquivo.

Ao identificar a proveniência exata da ameaça, a Darktrace tomou uma ação precisa para desarmá-la, em vez de simplesmente marcar todos os e-mails potencialmente suspeitos com avisos genéricos que provavelmente seriam ignorados. Para combater os arquivos ISO prejudiciais, a Darktrace converteu os anexos em PDFs inofensivos e moveu os e-mails para a pasta de lixo eletrônico. E, sobretudo, ao detectar o primeiro e-mail da campanha, a tecnologia neutralizou automaticamente outras 20 mensagens antes que causassem impacto nos negócios.

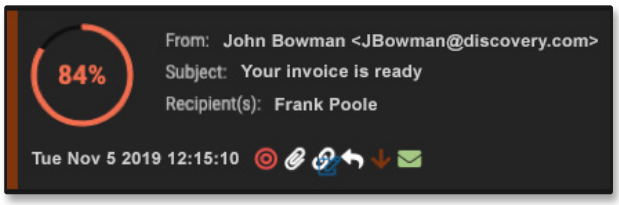


Figura 7: Cabeçalho dos e-mails maliciosos, mostrando a ação sugerida

Catálogo de endereços do município comprometido

Um agente de ameaças conseguiu obter acesso ao catálogo de endereços de um município dos EUA, proferindo um ataque aos destinatários em ordem alfabética, de A a Z. Cada e-mail foi criado e personalizado para o destinatário, e todas as mensagens continham uma carga mal-intencionada escondida atrás de um botão disfarçado de várias formas, como um link para a Netflix, Amazon e outros serviços de confiança.

Quando o primeiro e-mail foi recebido, a Darktrace reconheceu imediatamente que nem o destinatário, nem ninguém em seu grupo de colegas ou no restante da equipe da cidade, havia acessado esse domínio anteriormente. O sistema também reconheceu que a maneira como os links estavam ocultos atrás de cada botão era altamente suspeita. Um alerta de alta confiança foi levantado imediatamente com a sugestão de que cada link fosse bloqueado autonomamente quando entrasse na rede.

Curiosamente, o fato de a solução Antigena ter sido implantada no "Modo Passivo" forneceu evidências claras e concretas da capacidade do sistema de impedir ataques sutis que outras ferramentas não perceberiam. Enquanto a Antigena detectou e buscava neutralizar a campanha na letra "A", as ferramentas legadas da equipe de segurança detectaram a ameaça na letra "R". Em "Modo Ativo", a Antigena teria neutralizado o ataque antes que ele atingisse um único usuário.

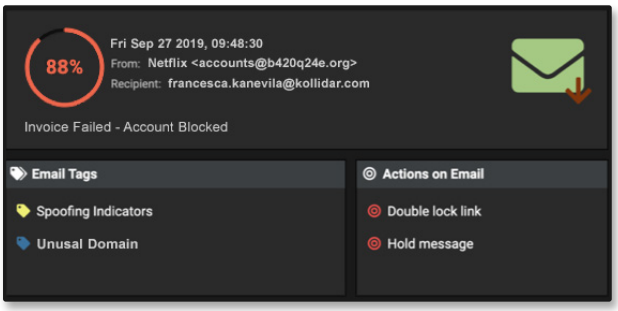
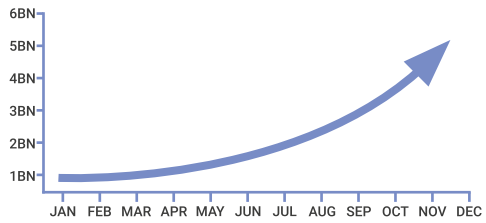


Figura 8: Antigena Email mostrando uma pontuação de 88% de anomalia

Aquisição do controle de contas na cadeia de suprimentos

As perdas por aquisição de controle de contas mais que triplicaram no ano passado, chegando a US$ 5,1 bilhões



Fonte: Javelin

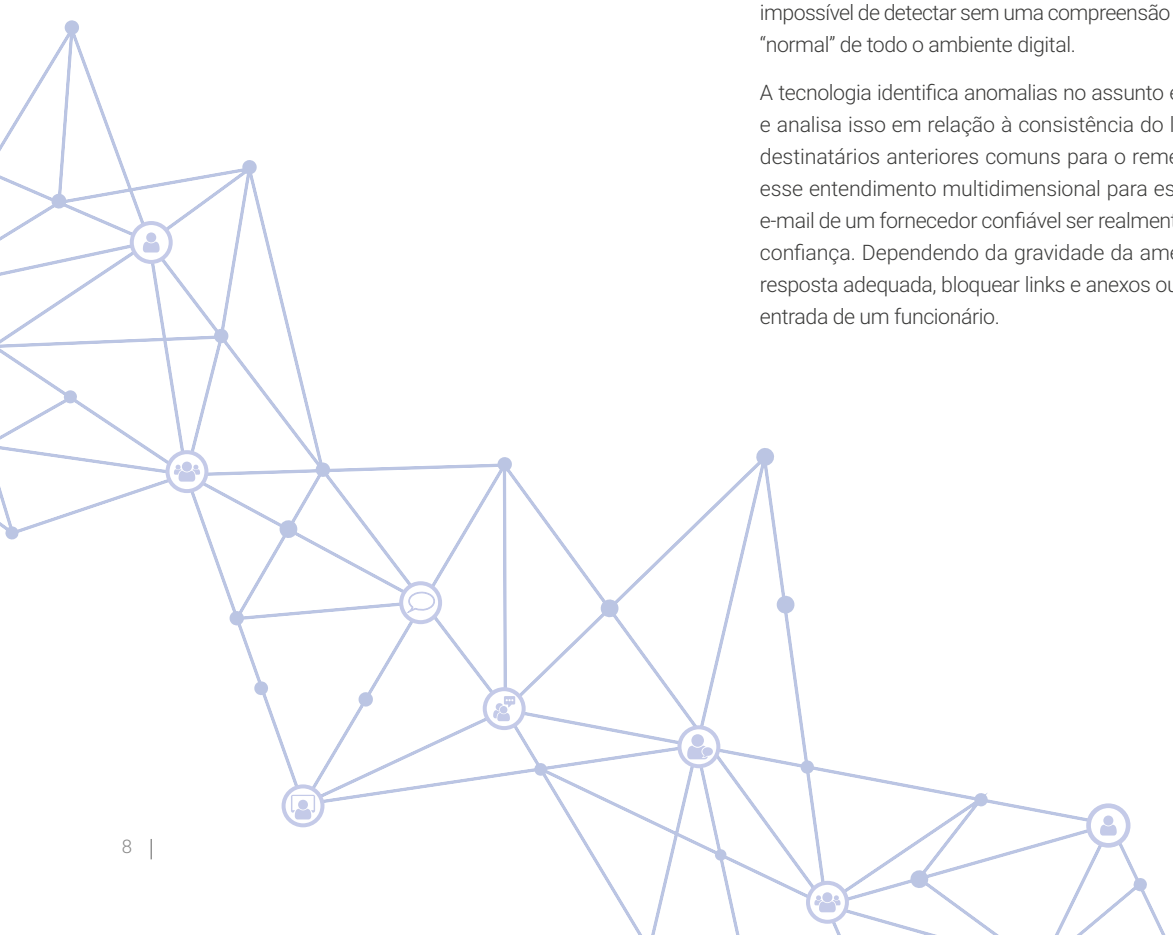
Com o sequestro de credenciais de acesso da conta de um contato de confiança em sua cadeia de suprimentos, os invasores podem obter facilmente a confiança de um funcionário na rede e convencê-lo a clicar em um link mal-intencionado ou a transferir milhões da empresa. As defesas de e-mail legadas assumem confiança, o que significa que aquisições de controle sofisticadas de contas passam completamente despercebidas com frequência.

Contas comprometidas foram responsáveis por vários ataques importantes a grandes organizações nos últimos anos. Os criminosos cibernéticos estão cada vez mais utilizando as cadeias de suprimentos – compostas por fornecedores, parceiros e prestadores de serviços – em seus ataques para se infiltrar em uma organização ou estabelecer comunicação off-line. No início do ano, um relatório sobre o chamado "island hopping" — em que invasores tentam expandir uma brecha nas cadeias de suprimentos – descobriu que esse método é responsável por metade dos ataques atuais.

Os invasores com acesso total à conta de e-mail de um fornecedor podem estudar as interações anteriores e produzir uma resposta direcionada à mensagem mais recente. A linguagem usada geralmente parece benigna; portanto, as ferramentas de segurança de e-mail legadas que pesquisam palavras-chave ou frases indicativas de phishing não identificam esses ataques.

A Antigena Email é capaz de formular uma noção abrangente de normalidade das palavras usadas por cada usuário interno; portanto, independentemente de quão plausível a frase possa ser para a maioria dos observadores, humanos ou máquinas, ela é capaz de identificar distribuições irregulares de palavras e frases. Analisando padrões de comunicação com o contexto completo de todo o tráfego de e-mail e na rede, a Antigena Email usa várias métricas para identificar com confiança casos de aquisição de controle de conta, algo que é impossível de detectar sem uma compreensão detalhada do comportamento "normal" de todo o ambiente digital.

A tecnologia identifica anomalias no assunto e no conteúdo de cada e-mail e analisa isso em relação à consistência do local de login, links, anexos e destinatários anteriores comuns para o remetente. A Antigena Email usa esse entendimento multidimensional para estimar a probabilidade de um e-mail de um fornecedor confiável ser realmente legítimo. Ele não pressupõe confiança. Dependendo da gravidade da ameaça, ele pode executar uma resposta adequada, bloquear links e anexos ou retirar um e-mail da caixa de entrada de um funcionário.



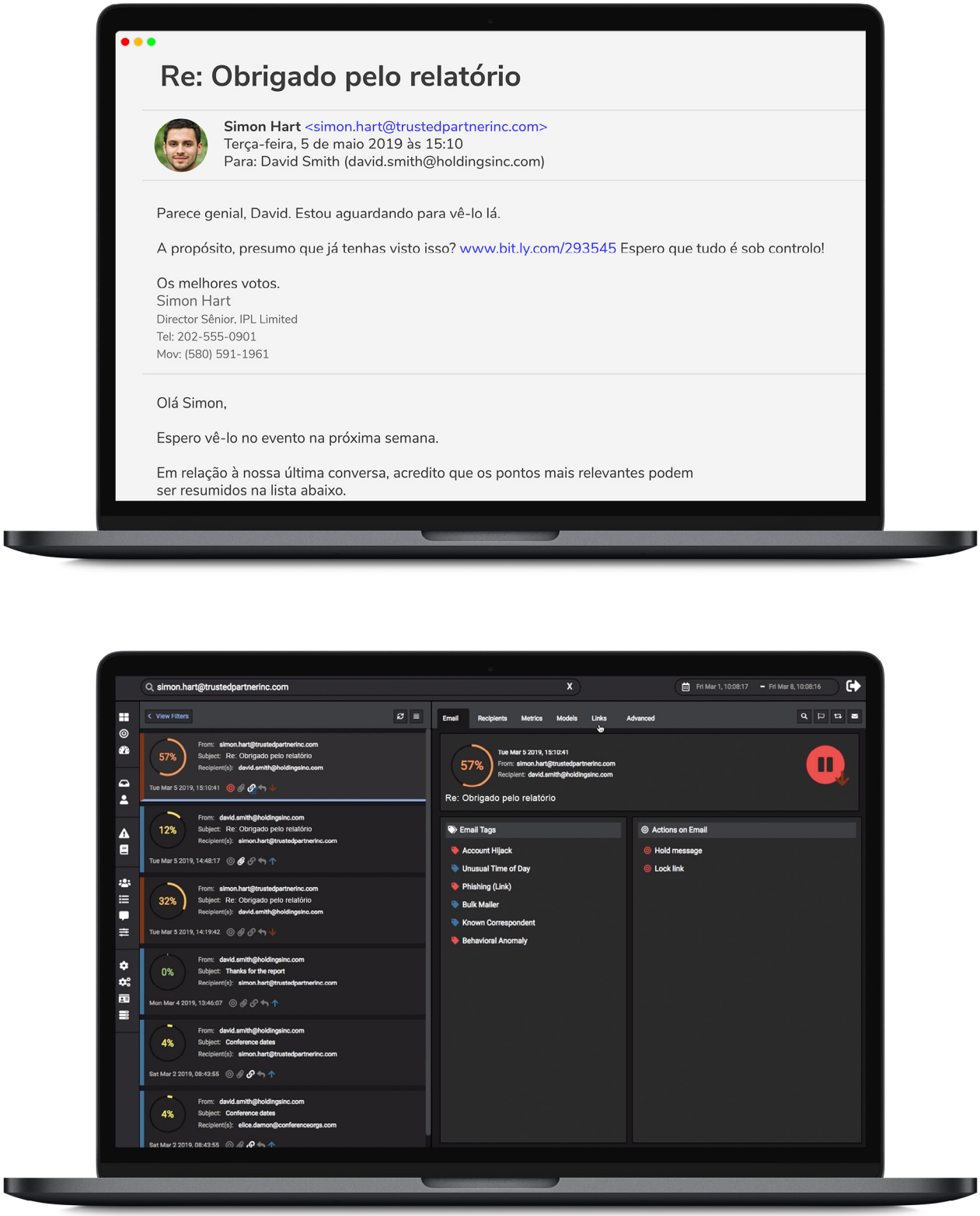


Figura 9: Uma resposta plausível enviada da conta comprometida de um fornecedor confiável após uma conversa de correspondência por e-mail. O link continha uma carga mal-intencionada.

Ataques consecutivos à cadeia de suprimentos

Um cliente que testava a Antigena Email enfrentou dois incidentes graves em dias sucessivos, quando as contas de e-mail de fornecedores confiáveis se tornaram a fonte de uma campanha mal-intencionada – muito provavelmente após o comprometimento dessas contas.

A Antigena Email ainda não havia sido configurada para executar ações autônomas e, portanto, os usuários foram totalmente expostos ao conteúdo dos e-mails. No entanto, em todos os casos, a Antigena Email recomendou a retenção dos e-mails e o bloqueio das cargas dos links, enquanto as ferramentas de segurança integradas da Microsoft não detectaram nada suspeito, deixando tudo passar sem tomar uma ação.

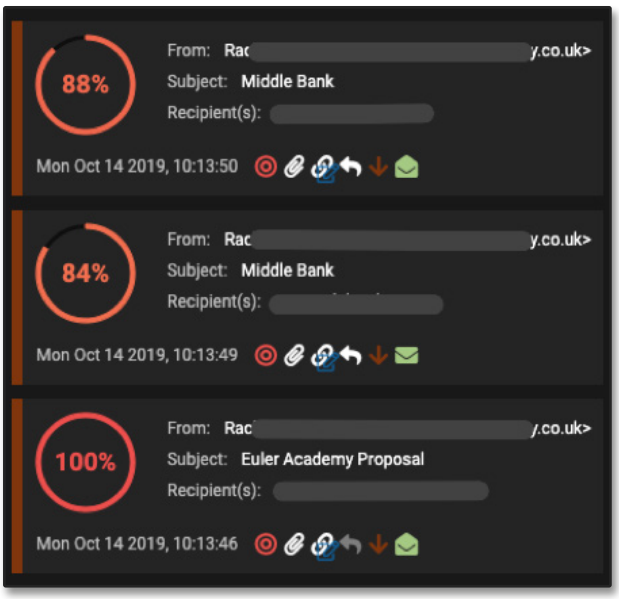


Figura 11: E-mails enviados mais tarde no mesmo dia contendo anexos mal-intencionados

Incidente 1 - Empresa de consultoria

No primeiro caso, a Antigena Email reconheceu que o remetente era bem conhecido pela empresa, com vários usuários internos se correspondendo diretamente com ele anteriormente. De fato, no início daquele dia, um desses usuários estava envolvido em uma correspondência normal com a conta que seria sequestrada em breve. O fornecedor em questão era uma empresa de consultoria ambiental sediada no Reino Unido.

Menos de duas horas após essa troca rotineira, e-mails foram rapidamente enviados para 39 usuários, cada um contendo um link de phishing. Houve variação nas linhas de assunto e nos links contidos nos e-mails, sugerindo e-mails altamente direcionados de um invasor bem preparado. O objetivo dos links poderia ser a solicitação de pagamentos, a coleta de senhas ou a implantação de malware.

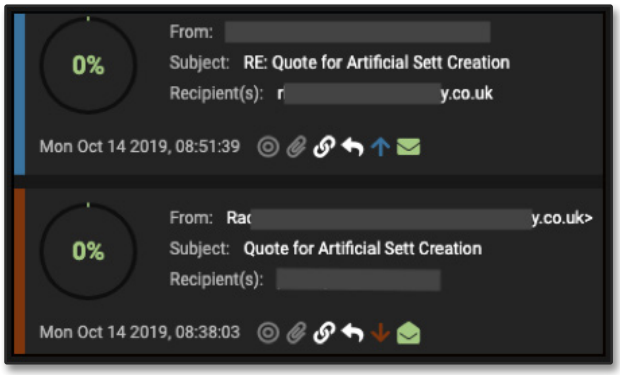


Figura 10: Correspondência anterior "normal" com o remetente – com pontuação de anomalia de 0%

A Antigena Email identificou todo o alcance de sinais de alerta que normalmente estão associados a aquisições de controle de contas da cadeia de suprimentos:

1. Localização incomum de login: A Antigena Email determinou que os e-mails foram enviados de um servidor Web autêntico do Outlook. Isso, por si só, não era incomum para o fornecedor. Porém, nesses dados de conexão também era possível extrair o endereço IP localizável geograficamente, revelando que o invasor fez login a partir de um IP nos EUA, em vez do local de login habitual no Reino Unido.

2. Inconsistência de links: Os links de phishing nos e-mails foram todos hospedados na plataforma de desenvolvedor do Microsoft Azure – provavelmente para contornar as verificações de reputação no domínio do host. Apesar da legitimidade amplamente pressuposta dos sites do Azure na Internet, a Antigena Email conseguiu detectar que esse domínio era altamente inconsistente para o remetente com base no histórico de correspondência anterior. O subdomínio incomum também significava que o nome do host tinha uma pontuação máxima de raridade no contexto do tráfego na rede da organização. Como outros produtos de segurança de e-mail não aproveitam essa inteligência contextual, seria impossível para eles chegarem a essa conclusão.

3. Destinatários incomuns: Uma pontuação de "association anomaly" (anomalia de associação) do destinatário é atribuída para estimar a probabilidade de esse grupo específico de destinatários receber um e-mail da mesma origem. Adicionando contexto à sua investigação ao longo do tempo, a Antigena Email deduziu que esse grupo de destinatários era 100% anômalo já no terceiro e-mail.

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

Figura 12: Métricas acionadas pela raridade e inconsistência do link

4. Anomalia de assunto: As linhas de assunto desses e-mails sugerem uma tentativa de parecerem discretos e profissionais e, consequentemente, qualquer tentativa baseada em assinaturas de buscar palavras-chave associadas a phishing teria falhado. No entanto, a Antigena Email reconheceu que esses destinatários normalmente não recebem e-mails sobre propostas de negócios usando esse estilo de frase.

Property	Value
Recipient > Metrics > Association Anomaly	100

Figura 13: a Antigena Email detectou rapidamente que esse grupo de destinatários não estava intimamente relacionado

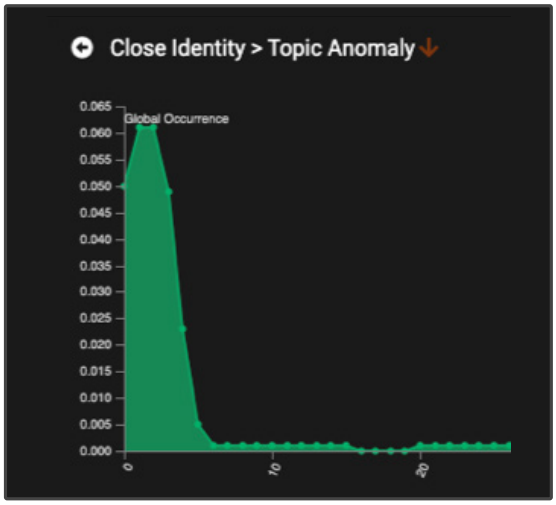


Figura 14: A visualização de resumo da métrica de anomalia de assunto

Incidente 2 – Provedor SaaS comprometido

Um segundo ataque no dia seguinte envolveu o envio de e-mails para 55 usuários internos de um provedor SaaS conhecido pela empresa. Na ausência de qualquer ação da Microsoft, mais de 50% desses e-mails foram lidos pelos destinatários. A Antigena Email recomendou que esses e-mails fossem retidos, impedindo-os de chegar à caixa de entrada.

1. Como antes, os e-mails enviados da conta comprometida continham um link maliciosos de phishing. Nesse caso, contudo, o link permaneceu ativo por um longo período, permitindo uma reconstrução precisa do que os usuários finais teriam encontrado.

2. Felizmente, aqueles que interagiram com os e-mails foram facilmente encontrados e as contas recuperadas, graças à inteligência compartilhada da Antigena Email e da Plataforma de Immune System da Darktrace na rede. O Immune System também detectou que os dispositivos na rede física estavam se conectando ao host de phishing. Funcionando em sincronia com a Antigena Email, o Immune System sinalizou essas interações com domínios suspeitos de phishing na rede.

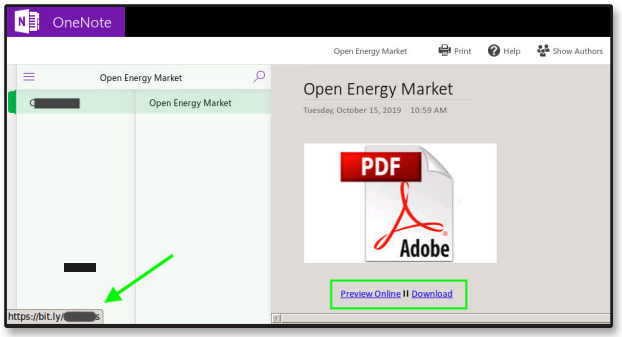


Figura 15: Captura de tela expondo um link oculto

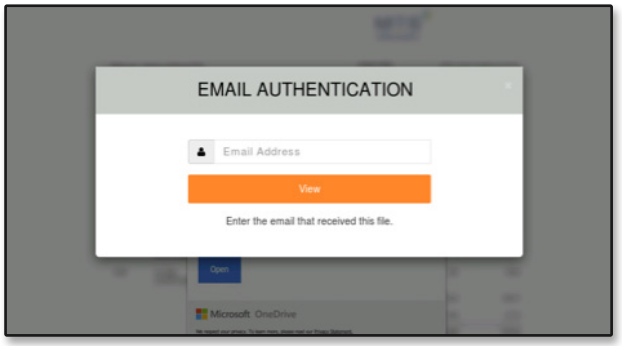


Figura 16: Isso levou a um formulário que coletaria as credenciais do usuário

3. Embora os links tenham sido incorporados em "links seguros" do ATP da Microsoft (o que significa que a Microsoft executaria uma verificação em tempo real nos links quando clicados pelo usuário), as conexões com os endpoints reais no tráfego da rede confirmaram que a inteligência disponível à Microsoft no momento a levou a concluir que os links eram seguros, expondo os usuários ao endpoint maliciosos.

4. O link em si foi hospedado na conhecida plataforma de compartilhamento de arquivos SharePoint. Ao acessar o link, o usuário foi levado a um documento que se apresentava como um relatório sobre o mercado de energia. No entanto, um botão solicitava que o usuário baixasse o arquivo, redirecionando-o para outra página da Web, configurada para solicitar o e-mail e a senha do usuário com o objetivo de enviá-los diretamente ao invasor.

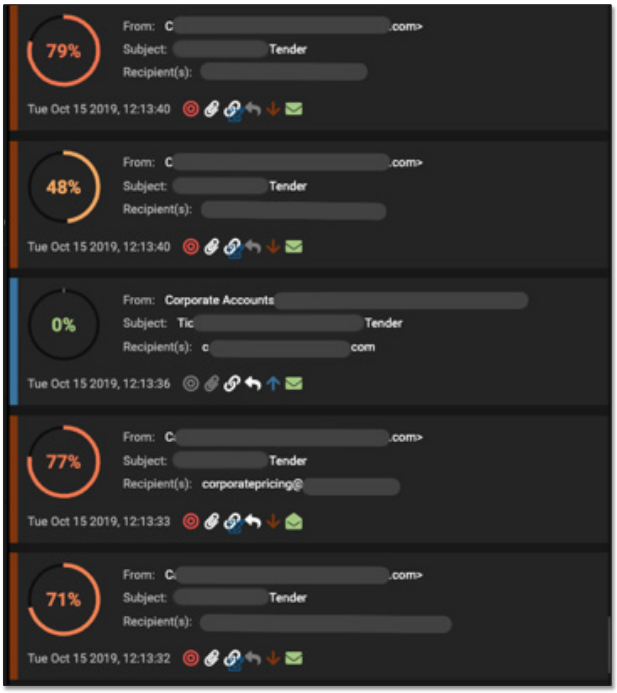


Figura 17: E-mails do Incidente 2 conforme exibidos no console da Antigena Email, incluindo aqueles que foram enviados em resposta. Isso revela que o usuário das "contas corporativas' reconheceu o e-mail ao abrir um ticket.

Arquivo oculto malicioso na página do OneDrive

Um agente de ameaças avançado sequestrou a conta de e-mail de um fornecedor de um grande grupo de hotéis, usando a conta confiável para enviar uma carga mal-intencionada à organização. Enquanto o ataque conseguiu burlar as defesas legadas da empresa, a Antigena Email neutralizou a ameaça em segundos.

1. A análise de um e-mail anterior revela o entendimento da Antigena Email de que havia uma relação entre os dois remetentes.

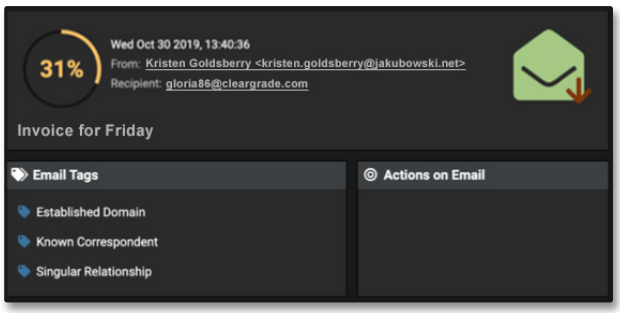


Figura 18: Um exemplo de uma comunicação anterior

2. Um e-mail subsequente foi sinalizado como altamente anômalo em comparação com os padrões de comunicação anteriores do remetente.

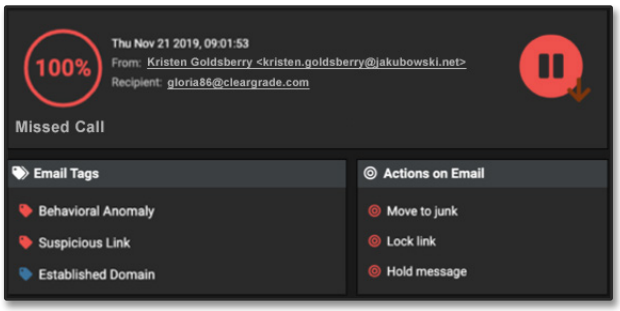


Figura 19: Um e-mail posterior marcado e três violações de modelo associadas

3. Como podemos observar, esses e-mails foram todos marcados com o modelo "Behavioral Anomaly" (anomalia comportamental), e a Antigena Email decidiu que a melhor ação a ser tomada era reter essas mensagens dos destinatários pretendidos.

4. A Antigena Email identificou vários desvios do "padrão de vida" normal do remetente externo, incluindo "Anomalous Source Country" (país de origem anômalo) e "Anomalous Source IP address" (endereço IP de origem anômalo).

5. Como o link mal-intencionado no e-mail também era altamente inconsistente com os "padrões de vida" da empresa para tráfego de e-mail e na rede, ele foi bloqueado pela Antigena Email.

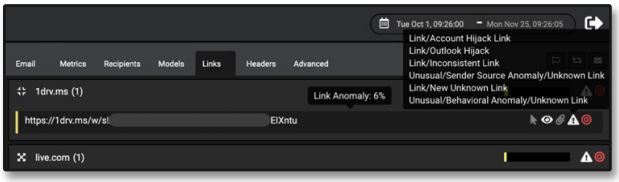


Figura 20: El enlace malicioso identificado

6. O link estava oculto no texto de exibição "Retrieve Message" (recuperar mensagem) e foi enviado para uma página do OneDrive. É difícil capturar o uso de domínios de armazenamento de arquivos para hospedagem de conteúdo mal-intencionado usando uma abordagem tradicional, pois é impossível incluir serviços como o SharePoint em lista negra. Além disso, decidir se um link como esse malicioso ou benigno requer uma compreensão do e-mail no contexto da organização como um todo.

Solicitação e engenharia social

> Temos a Antigena Email implantada, bem como ferramentas de segurança legadas. Ficamos impressionados com as coisas que as ferramentas tradicionais não identificaram e que foram capturadas pela Antigena Email.
>
> **– CTO, Bunim Murray Productions**

dos ataques nas caixas de entrada do usuário não continham malware

Os ataques de solicitação e engenharia social geralmente envolvem uma tentativa sofisticada de clonagem, nos quais os invasores disfarçados solicitam urgentemente que um destinatário responda ou faça comunicações ou transações off-line. Seus objetivos variam de fraude eletrônica a espionagem corporativa e até roubo de IP. Embora as organizações devam, obviamente, investir em treinamento sobre segurança e educar seus funcionários a procurar sinais de alerta, nenhuma orientação pode garantir imunidade completa a esses ataques cada vez mais sofisticados.

Enquanto as campanhas de phishing tradicionais incluem normalmente uma carga oculta mal-intencionada atrás de um link ou anexo, as tentativas de engenharia social envolvem geralmente o envio de "e-mails limpos" que contêm apenas texto. Esses ataques burlam facilmente as ferramentas de segurança legadas que dependem da correlação de links e anexos com listas negras e assinaturas. Além disso, esse vetor de ataque envolve geralmente o registro de novos domínios "semelhantes", que não apenas enganam o destinatário, mas também burlam as defesas tradicionais.

A Antigena Email tem um entendimento unificado de "normal" em todo o tráfego de e-mail e na rede que evolui com a empresa, permitindo detectar casos sutis de solicitação. E-mails limpos que burlam as defesas tradicionais podem ser identificados em segundos graças a um amplo alcance de métricas, incluindo semelhanças suspeitas com usuários conhecidos, associações anormais entre destinatários internos e até anomalias no conteúdo e no assunto dos e-mails.

Frequentemente, os ataques de engenharia social procuram levar imediatamente a conversa off-line, o que significa que medidas de segurança lentas e reativas tendem a intervir apenas depois que o dano foi feito. Seu poderoso entendimento de cada usuário, dispositivo e relacionamento na organização permite que a Antigena Email responda proativamente e com alta confiança na primeira vez, intervindo nesse importante estágio inicial.

A Antigena também é única em sua capacidade de adaptar respostas de maneira inteligente a tipos de ameaças específicos. Ele entende que o elemento "perigoso" em um ataque de solicitação será frequentemente o próprio conteúdo do e-mail, e o sistema impedirá a entrega antes que o destinatário pretendido possa atender à solicitação urgente do invasor.

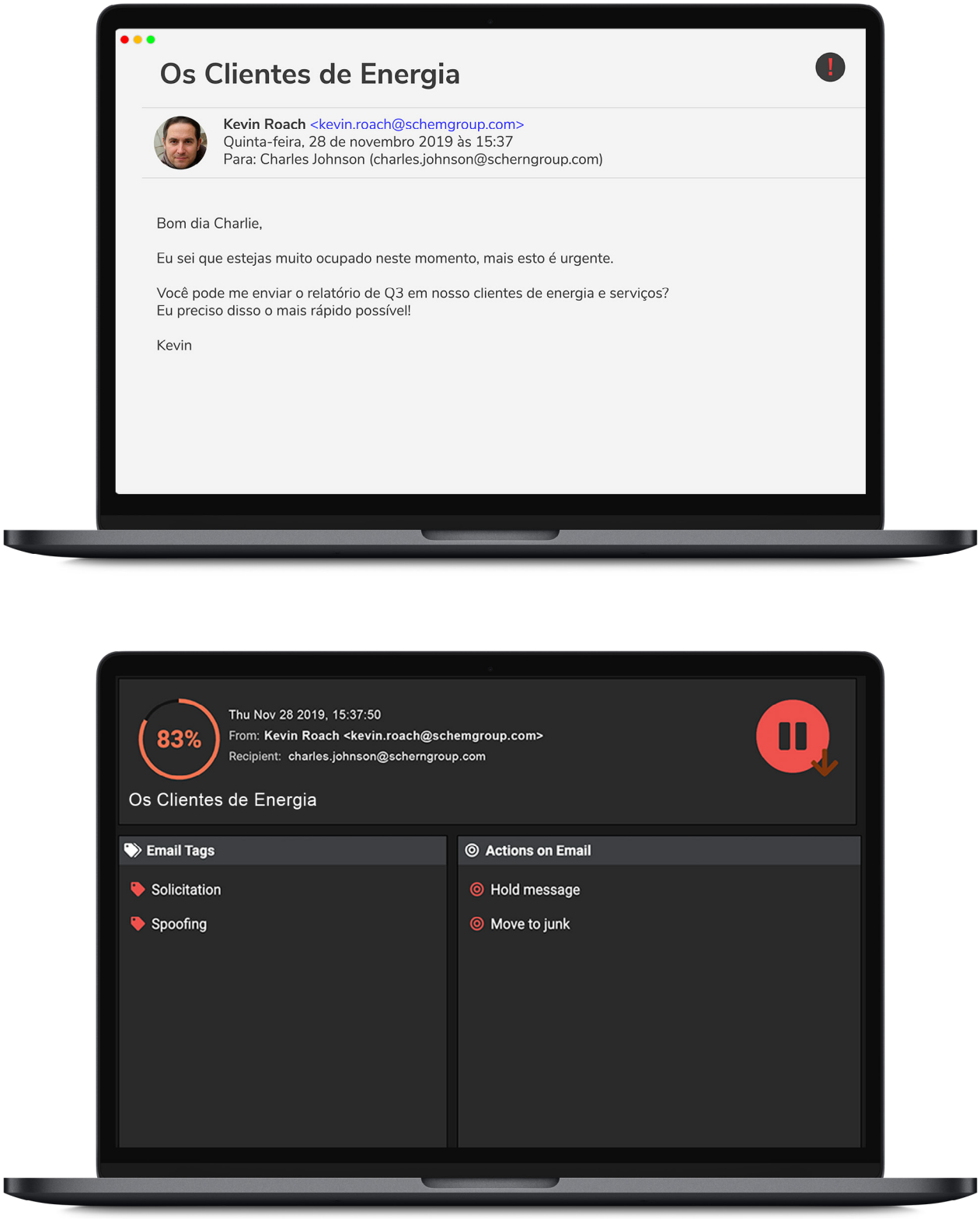


Figura 21: Um invasor que se apresenta como executivo, buscando documentos confidenciais. Observe o endereço de e-mail falsificado.

Ataque de clonagem

A Antigena Email detectou um ataque direcionado contra 30 funcionários de uma empresa multinacional de tecnologia. Uma pesquisa abrangente foi realizada, pois para cada usuário-alvo, o invasor clonou cuidadosamente a identidade do executivo de nível C com quem era mais provável que o usuário se comunicasse. A Antigena Email identificou o ataque de engenharia social e, como resultado, reteve cada e-mail dos destinatários pretendidos.

1. A linha de assunto de cada e-mail incluía o primeiro nome do funcionário-alvo e se originava de um endereço do Gmail aparentemente não relacionado. Apesar da ausência de carga mal-intencionada (como links ou anexos), a Antigena Email conseguiu identificar os e-mails como maliciosos.

2. A Darktrace não apenas identificou as tentativas de clonagem ao reconhecer o nome de domínio semelhante, mas também constatou que os e-mails violavam o modelo de "No Association" (Sem associação), indicando que em sua compreensão do ambiente de e-mail e da rede da empresa, não havia evidências de uma relação entre esse remetente e a organização.

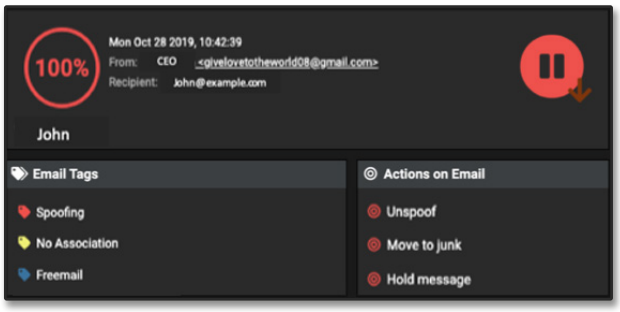


Figura 22: Um dos 30 e-mails com 100% de pontuação de anomalia

3. Correlacionando vários indicadores fracos, a Antigena reconheceu esses e-mails como componentes de um ataque coordenado, fazendo com que ela os mantivesse em um buffer para que fossem analisados pela equipe de segurança da organização.

4. A Antigena Email não apenas identificou os três executivos de nível C cujas identidades estavam sendo clonadas, mas também reconheceu que o invasor estava usando uma falsificação do endereço pessoal externo legítimo do CEO.

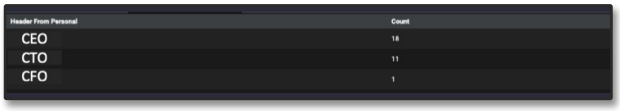


Figura 23: Três executivos de nível C identificados

5. Além disso, a pontuação de exposição dos usuários clonados era alta, indicando que eles eram alvos importantes e, portanto, violavam o modelo "Whale Spoof". A compreensão de que usuários internos importantes haviam sido alvo permitiu que a IA da Darktrace priorizasse esse ataque, iniciando uma resposta proporcional em tempo real.

Solicitação de folha de pagamento do CEO

Em uma distribuidora de energia elétrica, a IA da Darktrace detectou uma tentativa de falsificação convincente em uma conta de e-mail do Office 365. Um e-mail, supostamente do CEO da empresa, foi enviado a um membro do departamento de folha de pagamento solicitando que o funcionário atualizasse as informações de depósito direto do CEO.

Como o e-mail imitava com êxito o estilo típico de escrita do CEO, a fraude poderia ter sido bem-sucedida se a IA da Darktrace não estivesse analisando o fluxo de mensagens da empresa relacionado ao restante dos negócios.

1. Ao aprender o "padrão de vida" normal do funcionário, do CEO e de toda a organização no tráfego na nuvem e na rede, a Darktrace conseguiu sinalizar imediatamente uma série de anomalias sutis no e-mail, incluindo o endereço do remetente falso.

Figura 24: Captura de tela do e-mail clonando a identidade do CEO

2. Entre outros indicadores fracos, a IA da Darktrace calculou a proximidade anômala do domínio com a dos funcionários internos e contatos confiáveis.

3. A IA respondeu imediatamente, bloqueando os links do e-mail e marcando a mensagem claramente como uma falsificação antes que ela chegasse ao departamento de folha de pagamento. A ampla compreensão da Darktrace sobre o tráfego na nuvem e na rede permitiu neutralizar uma ameaça de alta gravidade que as ferramentas baseadas em assinatura não teriam identificado.

Ataque de suplantación de identidad de un 'Vicepresidente Financiero'

Esse incidente envolveu a clonagem da identidade de um vice-presidente de Finança em uma instituição financeira conhecida. Os agentes da ameaça enviaram 11 e-mails semelhantes à organização, mas a Antigena Email tomou medidas para reter todos eles graças ao seu entendimento multidimensional de "normal" sobre o tráfego na rede, na nuvem e de e-mails. Analisando o endereço de e-mail claramente anômalo e não relacionado em relação ao conteúdo dos e-mails, a Darktrace reconheceu essa tentativa de falsificação, enquanto o gateway herdado da empresa deixou passar todos os 11 e-mails.

Figura 25: Captura de tela do link suspeito de compartilhamento de e-mail

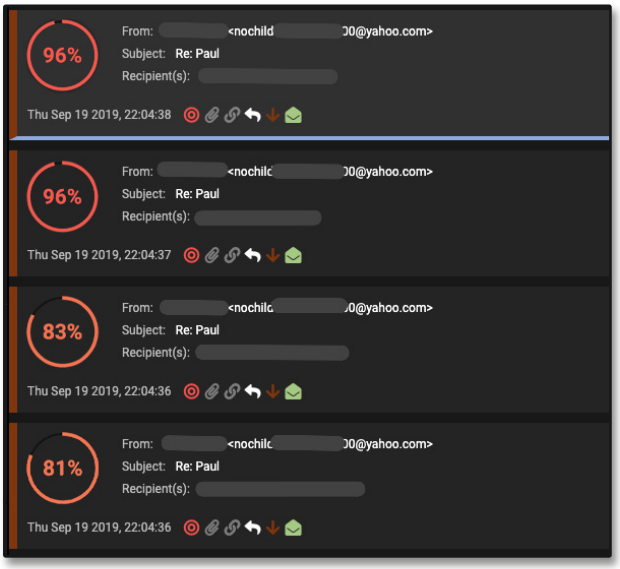
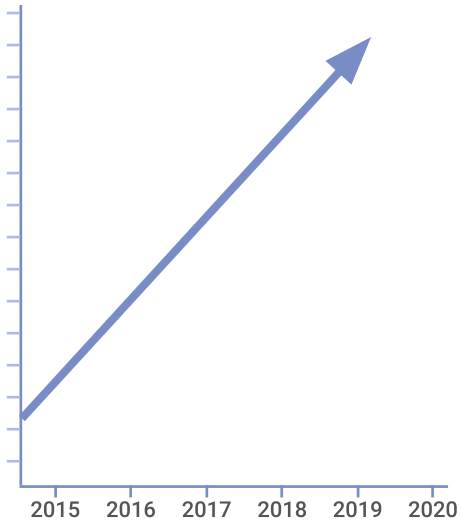


Figura 26: Quatro dos 11 e-mails, mostrando a alta pontuação de anomalia e a ação associada da Antigena Email

Credenciais de funcionário comprometidas

O comprometimento de credenciais aumentou em 280% entre 2016 e 2019



Os líderes empresariais raramente consideram o quanto vale uma caixa de entrada de e-mail corporativo até que ela caia em mãos erradas. Porém, depois de entrar, os agentes de ameaças desfrutam de uma ampla variedade de opções de ataque e pontos de articulação para escolher. A facilidade com que os invasores podem obter acesso, seja por meio de campanhas de phishing, tentativas de força bruta ou trocas na Dark Web, deve ser motivo de preocupação.

Em muitos casos, os invasores vasculham sua caixa de entrada em busca de dados valiosos. Informações pessoais, desde conversas particulares até detalhes de cobrança, podem ser aproveitadas para fraude ou chantagem, enquanto as conversas de e-mail antigas podem conter informações altamente confidenciais da empresa. Listas de clientes, documentos de preços e até mesmo detalhes de roteiro e IP geralmente estão a poucos termos de pesquisa para serem descobertos.

Em outros casos, os criminosos usarão a conta como ponto de partida para as próximas etapas de um ataque. Eles podem permanecer silenciosos em segundo plano para coletar informações sobre executivos ou parceiros importantes, analisando documentos, lendo conversas e aprendendo como podem se camuflar para inevitavelmente atacar. Assim como acontece nas aquisições de controle de contas da cadeia de suprimentos, a capacidade de ler uma conversa de e-mail em andamento e acompanhar uma resposta plausível costuma ser a maneira mais eficaz de realizar uma missão de invasão sem levantar suspeitas.

Enquanto as possibilidades para os invasores sejam praticamente infinitas, as opções de proteção são limitadas. As aquisições de controle de contas corporativas geralmente são monitoradas por defesas simples e estáticas, incluindo regras de "impossible travel" (viagem impossível) que raramente capturam invasores que sabem se esconder. No entanto, graças à sua visão de toda a empresa, a plataforma de Immune System da Darktrace complementa essas abordagens baseadas em regras, capturando as ameaças.

Ao aprender o "padrão de vida" normal de cada usuário, o Immune System detecta desvios sutis que revelam até os criminosos mais cuidadosos – independentemente desses desvios se manifestarem em comportamentos suspeitos de login, criações de regras de caixa de entrada ou edições de permissões do usuário. À medida que as ameaças cibernéticas se desenvolvem e se tornam mais avançadas, a utilização da IA de autoaprendizagem em toda a empresa digital será a única maneira viável de manter os criminosos longe da sua caixa de entrada.

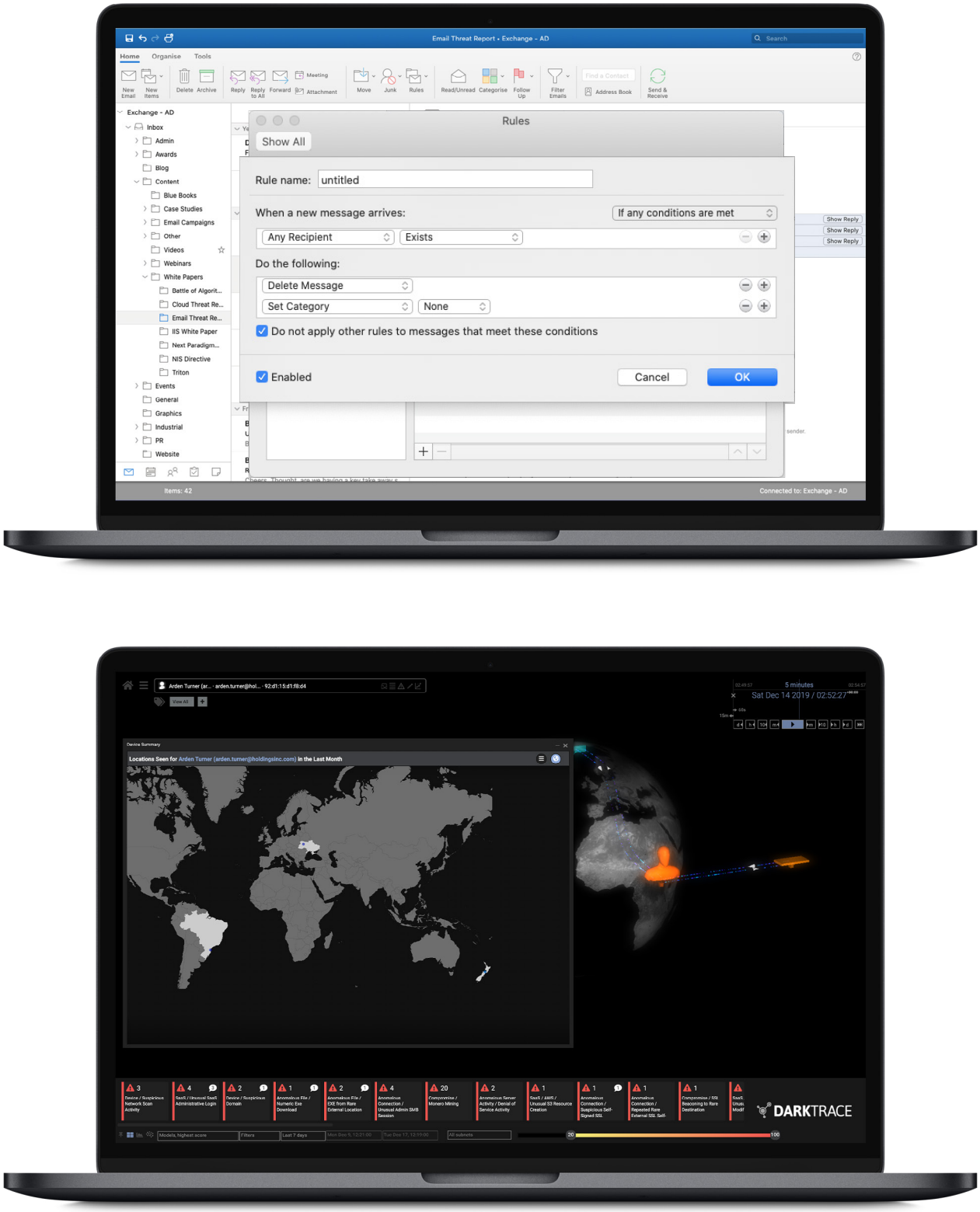


Figura 27: Uma regra de processamento de e-mails sendo configurada em uma conta comprometida e o Threat Visualizer exibindo os locais geográficos de login.

Login incomum no Banco do Panamá

Uma conta do Office 365 foi usada em um ataque de força bruta contra um banco conhecido no Panamá, com logins originários de um país que se desviava dos "padrões de vida" normais das operações da empresa.

A Darktrace identificou 885 logins durante um período de 7 dias. Embora a maioria das autenticações se originasse de endereços IP no Panamá, 15% das autenticações tinham origem em um endereço IP 100% raro e localizado na Índia. Uma análise adicional revelou que esse endpoint externo foi incluído em várias listas negras de spam e que havia sido associado recentemente a comportamentos abusivos on-line – possivelmente varreduras não autorizadas na Internet ou atividades de hackers.

Figura 28: A interface do usuário mostrando os locais de login

A Darktrace então testemunhou o que parecia ser um abuso da função de redefinição de senha, pois foi observado que o usuário na Índia alterava os privilégios da conta de uma maneira altamente incomum. O que marcou a atividade como particularmente suspeita foi que, após a redefinição da senha, foram observadas tentativas malsucedidas de login de um IP normalmente associado à organização, sugerindo que o usuário legítimo foi bloqueado.

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

Figura 29: A atividade associada à conta SaaS, destacando as credenciais alteradas

Tentativa de acesso com origem no interior do Japão

Em uma empresa de serviços financeiros sediada na Europa, foi observada uma credencial do Office 365 efetuando login a partir de um endereço IP incomum vinculado a um local no interior do Japão.

Embora o acesso a partir de locais remotos seja possível quando um usuário viaja ou usa um serviço de proxy, isso também pode ser um forte indicador de credenciais comprometidas e acesso mal-intencionado por um usuário não autorizado. Como o ponto de acesso era substancialmente diferente dos IPs de acesso usuais, a Darktrace sinalizou isso como anômalo e sugeriu imediatamente uma investigação adicional.

A equipe de segurança conseguiu bloquear remotamente a conta do Office 365 e redefinir as credenciais, impedindo que o agente mal-intencionado executasse mais atividades. Se essa atividade não fosse identificada, o agente da ameaça poderia ter usado seus privilégios de acesso para implantar malware na organização ou solicitar um pagamento fraudulento.

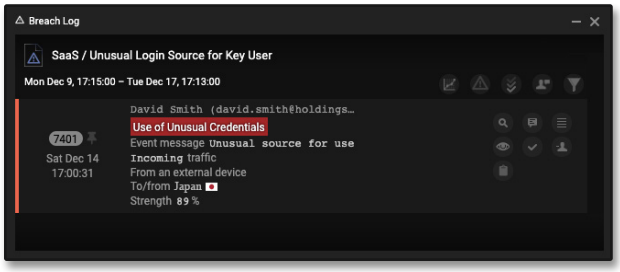


Figura 30: O login do Japão gerou várias alertas

Conta do Office 365 comprometida e sabotada

Em uma organização internacional sem fins lucrativos, a Darktrace detectou uma aquisição de controle de conta no Office 365 que burlou a regra estática de "impossible travel" (viagem impossível) do AD do Azure. Como a organização tinha escritórios em todos os cantos do mundo, a IA de autoaprendizagem da Darktrace identificou um login de um endereço IP historicamente incomum para esse usuário e seu grupo de colegas e alertou imediatamente a equipe de segurança.

A Darktrace alertou para o fato de que uma nova regra de processamento de e-mails, que apaga e-mails recebidos e enviados, foi configurada na conta. Isso era um indicador claro de comprometimento e a equipe de segurança conseguiu bloquear a conta antes que o invasor causasse danos.

Com essa nova regra de processamento de e-mails, o invasor poderia ter iniciado várias interações com outros funcionários da empresa, sem que o usuário legítimo soubesse. Essa é uma estratégia comum usada por criminosos cibernéticos que buscam obter acesso persistente e utilizar vários pontos de apoio dentro de uma organização, possivelmente como preparação para um ataque em larga escala.

Analisando o endereço IP raro em conjunto com o comportamento incomum do usuário aparente, a Darktrace identificou com confiança a atividade como um caso de aquisição de controle de conta, evitando danos sérios à empresa.

Ataque automatizado de força bruta

A Darktrace detectou vários eventos de login malsucedido em uma conta do Office 365 usando a mesma credencial, diariamente ao longo de uma semana. Cada lote de tentativas de login foi realizado exatamente às 18h40 em seis dias. A consistência na hora do dia e no número de tentativas de login era indicativa de um ataque automatizado de força bruta, programado para ser interrompido após um certo número de tentativas malsucedidas para evitar bloqueios.

A Darktrace considerou esse padrão de tentativas malsucedidas altamente anômalo e, portanto, alertou a equipe de segurança. Se a Darktrace não correlacionasse vários indicadores fracos e acionasse sinais sutis de ameaça emergente, esse ataque automatizado poderia ter continuado por semanas ou meses, possibilitando suposições fundamentadas sobre a senha dos usuários com base em outras informações já coletadas.

Figura 31: Um gráfico que ilustra as tentativas repetidas de login

Sobre a Darktrace

A Darktrace é a empresa líder mundial em IA para segurança cibernética e a criadora da tecnologia de resposta autônoma. A IA de autoaprendizagem é baseada no sistema imunológico humano e é utilizada por mais de 3.000 empresas em todo o mundo para proteger contra ameaças cibernéticas em ambientes Cloud, email, IoT, redes e sistemas industriais.

A Darktrace tem mais de 1.000 funcionários e está sediada em San Francisco e Cambridge, no Reino Unido. A IA Darktrace responde contra uma ameaça cibernética a cada 3 segundos, evitando que danos sejam causados.

Contate-nos

São Paulo: +55 (11) 4949 7696

Londres: +44 (0) 1223 394 100

EUA: +1 415 229 9100

APAC: +65 6804 5010

info@darktrace.com | darktrace.com

@darktrace