DARKTRACE

Relatório de ameaças de email

4 principais tendências: do spear-phishing ao roubo de credenciais

Panorama das ameaças

Índice

As plataformas de colaboração e email representam o tecido conjuntivo de qualquer empresa, onde informações são compartilhadas, projetos são elaborados e alianças são formadas. No entanto, como um meio conduzido por pessoas, o email sempre será o "elo mais fraco" da estratégia de segurança de uma organização. 94% das ameaças cibernéticas têm origem no ambiente de email.

Embora as ferramentas tradicionais de gateway filtrem emails maliciosos na entrada, sua dependência de listas de IPs, domínios e hashes de arquivos "conhecidamente nocivos" para determinar o nível de ameaça de um email é extremamente limitante. Uma abordagem baseada em regras pode identificar spams e outros itens indesejados evidentes, mas não acompanha as inovações dos invasores.

Spear-phishing, ataques de clonagem e aquisição do controle de contas, em particular, ainda são vias de ataque que os criminosos cibernéticos podem usar para se infiltrar em uma organização. Esse tipo de ataque cada vez mais direcionados por email, que ultrapassam as limitações das defesas tradicionais, são um desafio significativo para as equipes de segurança atualmente.

Como afirma Peter Firstbrook, Analista vice-presidente da Gartner: "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 email exige inovação e uma mudança de mentalidade para combater o cenário de ameaças em evolução."

Antigena Email: caixa de entrada com autodefesa

A Antigena Email é a primeira solução de Ciber IA do mundo para a caixa de entrada. Ao aprender o "padrão de vida" normal de cada usuário e correspondente, a tecnologia desenvolve um entendimento crescente do que é "humano" nas comunicações de email.

Enquanto as defesas tradicionais questionam se os elementos em um email já foram observados em ataques históricos, a Antigena Email é a única solução que pode perguntar com segurança se seria incomum um destinatário interagir com um email específico, no contexto de seu "padrão de vida" normal, bem como, no contexto do "padrão de vida" de seus colegas e de toda a organização.

O conhecimento contextual permite à IA tomar decisões altamente precisas e neutralizar a gama completa de ataques por email, desde emails de falsificação "limpos" que buscam a transferência de um pagamento fraudulento, até tentativas sofisticadas de spear-phishing.

Inspirada no sistema imunológico humano, a Antigena Email usa a inteligência artificial da Darktrace para aprender um senso de "self" para cada usuário interno e externo, analisando as comunicações recebidas e enviadas juntamente com as comunicações internas. Ao tratar os destinatários como indivíduos e colegas dinâmicos, a Antigena Email identifica de maneira exclusiva os desvios sutis da "norma", que revelam que emails aparentemente benignos são claramente maliciosos.

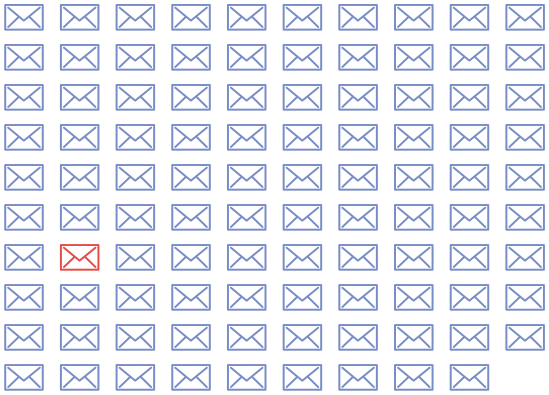
Nos estudos de caso a seguir, o senso de "self" em constante evolução sobre usuários de email e seus colegas permite à Darktrace detectar e interromper a ameaça de email que as ferramentas de segurança tradicionais normalmente não identificariam. Esses ataques por email são classificados em uma das quatro categorias de ataques altamente sofisticados que normalmente passam pela "pele protetora" da sua organização:

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

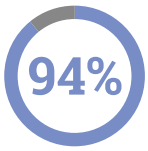
Spear-phishing e entrega de carga

> Com seu entendimento de “normal” em relação ao tráfego de email e da rede, a Antigena Email tem sido incrivelmente valiosa na captura de ameaças.
>
> **– Diretor de TI, Entegrus**

1 em cada 99 emails 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 maliciosos em um email 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 emails à luz do 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, eles escaparão das defesas tradicionais na fronteira e serão altamente anômalos para o usuário ou a empresa visada – pelo menos se os “padrões de vida” do indivíduo e de seu grupo de colegas for considerado. Essa realidade mostra a importância de uma análise dinâmica que considere centenas de métricas baseadas em comportamentos de usuários e grupos.

Acionada pela Ciber IA, a Antigena Email pode analisar links, anexos, domínios, conteúdo e outros elementos de um email juntamente com “padrões de vida” em toda a organização, correlacionando um amplo espectro de pontos de dados que revelam emails aparentemente benignos como inconfundivelmente maliciosos.

Diferente de todas as outras soluções, a Antigena Email entende o ser humano por trás das interações por email, identificando padrões anômalos de envio, se a localização de um link em um email é estranha, se os tópicos de discussão e o conteúdo são incomuns ou até mesmo se os padrões no caminho da URL são suspeitos.

Essa abordagem única significa a Darktrace é capaz de executar ações altamente proporcionais e direcionadas para neutralizar ataques de phishing em segundos.

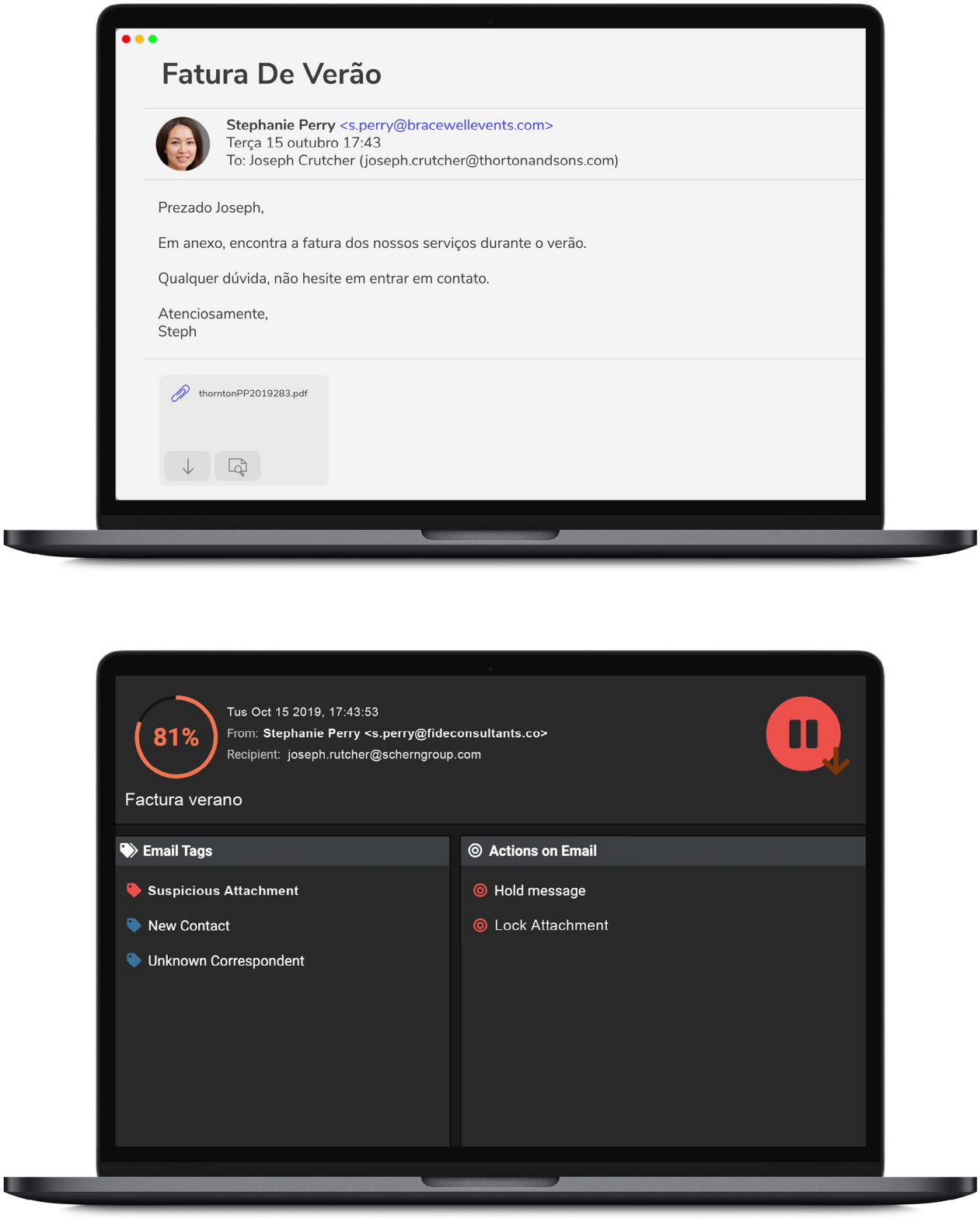


Figura 1: Um email persuadindo um funcionário a clicar em um anexo contendo uma carga maliciosa e a visualização correspondente na interface do usuário da Darktrace, mostrando as tags de anomalia e as ações tomadas

ESTUDO DE CASO REAL
Ataque WeTransfer

A Antigena Email neutralizou um ataque por email sofisticado direcionado a cinco usuários importantes em uma instituição acadêmica. Os emails eram bem redigidos e convincentes, tentando persuadir os destinatários a clicar em um link malicioso.

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

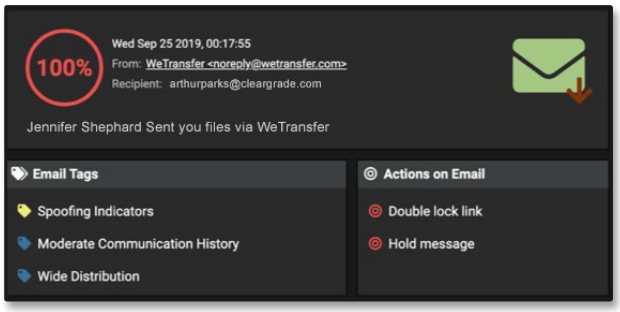


Figura 2: Interface do usuário mostrando as violações do modelo e ações

1. A partir dos dados de conexão, não havia sinais claros nos cabeçalhos de que esse email não fosse realmente originário do WeTransfer; portanto, a tentativa de clonagem teria provavelmente ludibriado o destinatário. A "Largura" e a "Profundidade" indicam que esse endereço de email se comunicou com muitas pessoas na organização, em vários dias.

Figura 3: Dados de conexão dos emails relevantes

2. No entanto, a Antigena Email pôde detectar uma série de anomalias sutis graças ao seu entendimento sobre o que é "normal" para o usuário e o ambiente mais amplo.

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 email enviar mensagens usando esse IP, e isso é geralmente um indicativo de conta falsificada ou sequestrada.

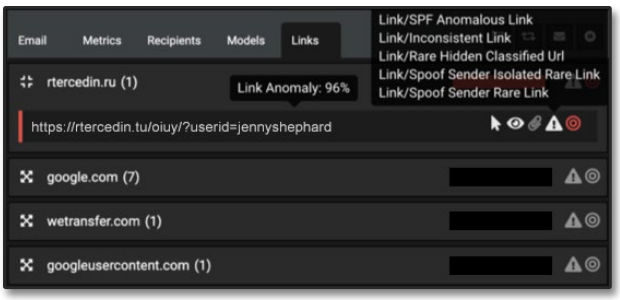


Figura 4: D Detalhamento dos links mostrados nos emails

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

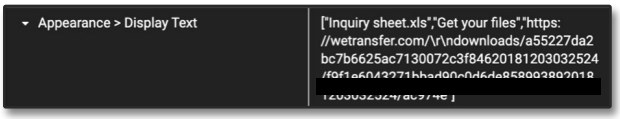


Figura 5: A Antigena pôde determinar onde o link apareceu no email

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

Esse incidente demonstra como a abordagem de autoaprendizagem permite à Antigena Email identificar ataques avançados de phishing que aproveitam a familiaridade de um site confiável para enviar um link nocivo e obter vários pontos de infiltração na organização.

ESTUDO DE CASO REAL

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 email 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 emails nocivos passou pelas defesas tradicionais de email da empresa, a Darktrace capturou a campanha identificando um amplo alcance de indicadores anômalos. Por exemplo, um dos modelos de IA acionado pelos emails 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 da ameaça, a Darktrace tomou uma ação precisa para desarmá-la, em vez de simplesmente marcar todos os emails 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 emails para a pasta de lixo eletrônico. E, sobretudo, ao detectar o primeiro email da campanha, a tecnologia neutralizou automaticamente outras 20 mensagens antes que causassem impacto nos negócios.

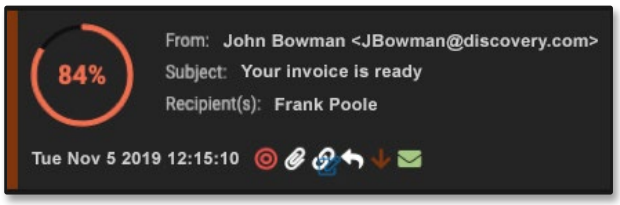


Figura 6: Cabeçalho dos emails maliciosos, mostrando a ação sugerida

ESTUDO DE CASO REAL

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 email foi criado e personalizado para o destinatário, e todas as mensagens continham uma carga maliciosa escondida atrás de um botão disfarçado de várias formas, como um link para a Netflix, Amazon e outros serviços confiáveis.

Quando o primeiro email chegou, a Antigena Email reconheceu imediatamente que o domínio era incomum para a organização. O sistema também reconheceu que a maneira como os links estavam ocultos atrás de cada botão era altamente suspeita. Isso acionou um alerta de alta confiança que foi respondido com o bloqueio de cada link. Enquanto as defesas legadas de email do município somente identificaram o ataque na letra "R", a Antigena Email o neutralizou na letra "A", assim que chegou o primeiro email.

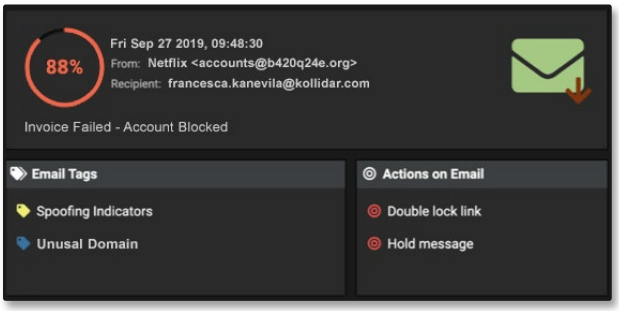
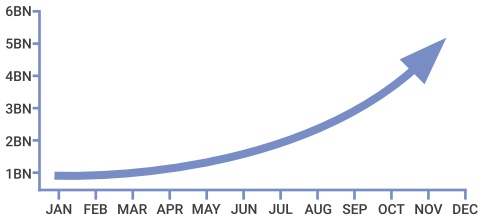


Figura 7: Antigena Email mostrando uma pontuação de 88% de anomalia

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



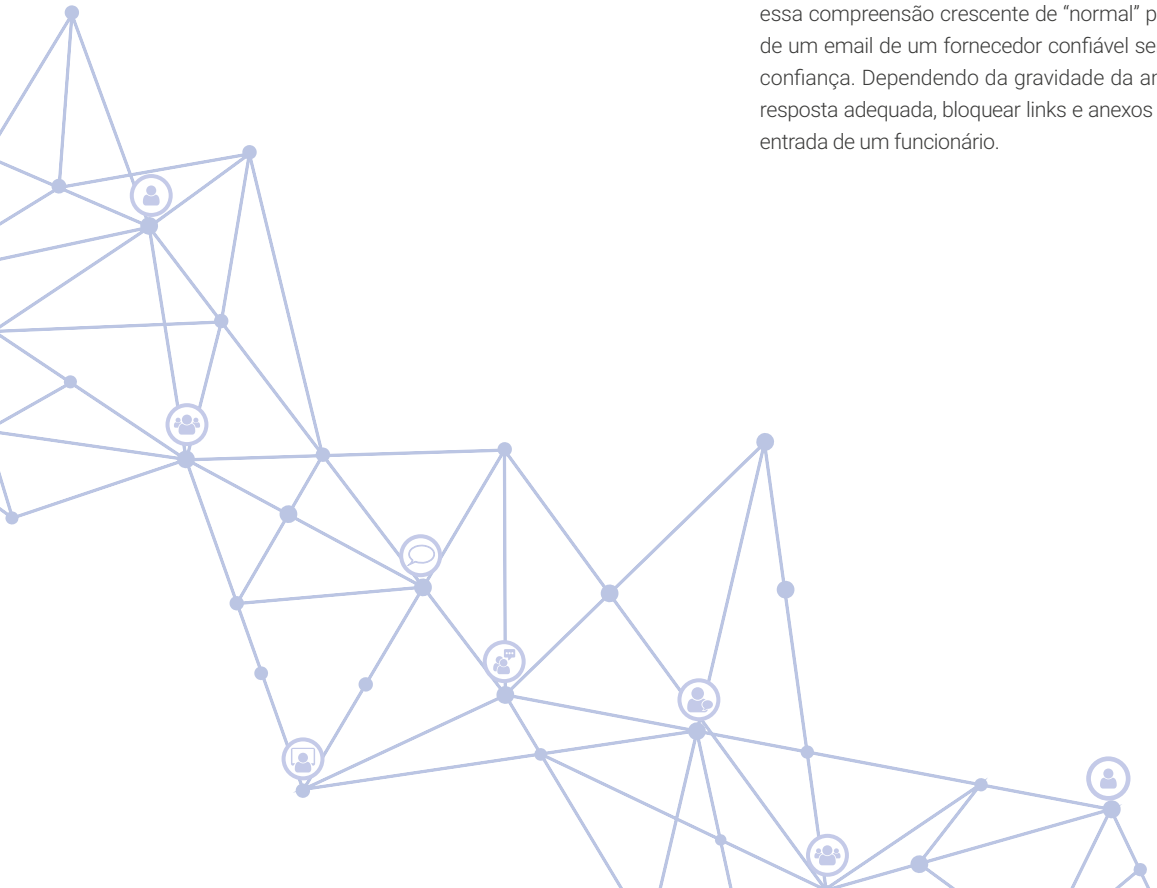
Com o sequestro da conta de um contato confiável na sua cadeia de suprimentos, os agentes de ameaças podem obter facilmente a confiança de um usuário e levá-lo a clicar em um link malicioso ou a transferir milhões da empresa. As defesas de email legadas pressupõem confiança, o que significa que ataques sofisticados de aquisição do controle de contas passam frequentemente despercebidos.

Contas comprometidas foram responsáveis por vários ataques importantes a grandes organizações nos últimos anos. Os criminosos cibernéticos estão cada vez mais aproveitando as cadeias de suprimentos — fornecedores, parceiros, prestadores de serviços — para se infiltrar em seu destino final 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 à conta de email 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 email legadas que pesquisam palavras-chave ou frases indicativas de phishing não identificam esses ataques.

Ao analisar os padrões de comunicação com o contexto completo de todo o fluxo de emails internos, de entrada e de saída, a Antigena Email usa várias métricas para identificar casos de aquisição do controle de contas, algo impossível de detectar sem uma compreensão detalhada do comportamento "normal" de toda a organização.

A tecnologia identifica anomalias no assunto e no conteúdo de cada email e analisa isso em relação à consistência do local de login, links, anexos e destinatários anteriores comuns para o remetente. A Antigena Email usa essa compreensão crescente de "normal" para determinar a probabilidade de um email de um fornecedor confiável ser legítimo — ela não pressupõe confiança. Dependendo da gravidade da ameaça, ele pode executar uma resposta adequada, bloquear links e anexos ou retirar um email da caixa de entrada de um funcionário.



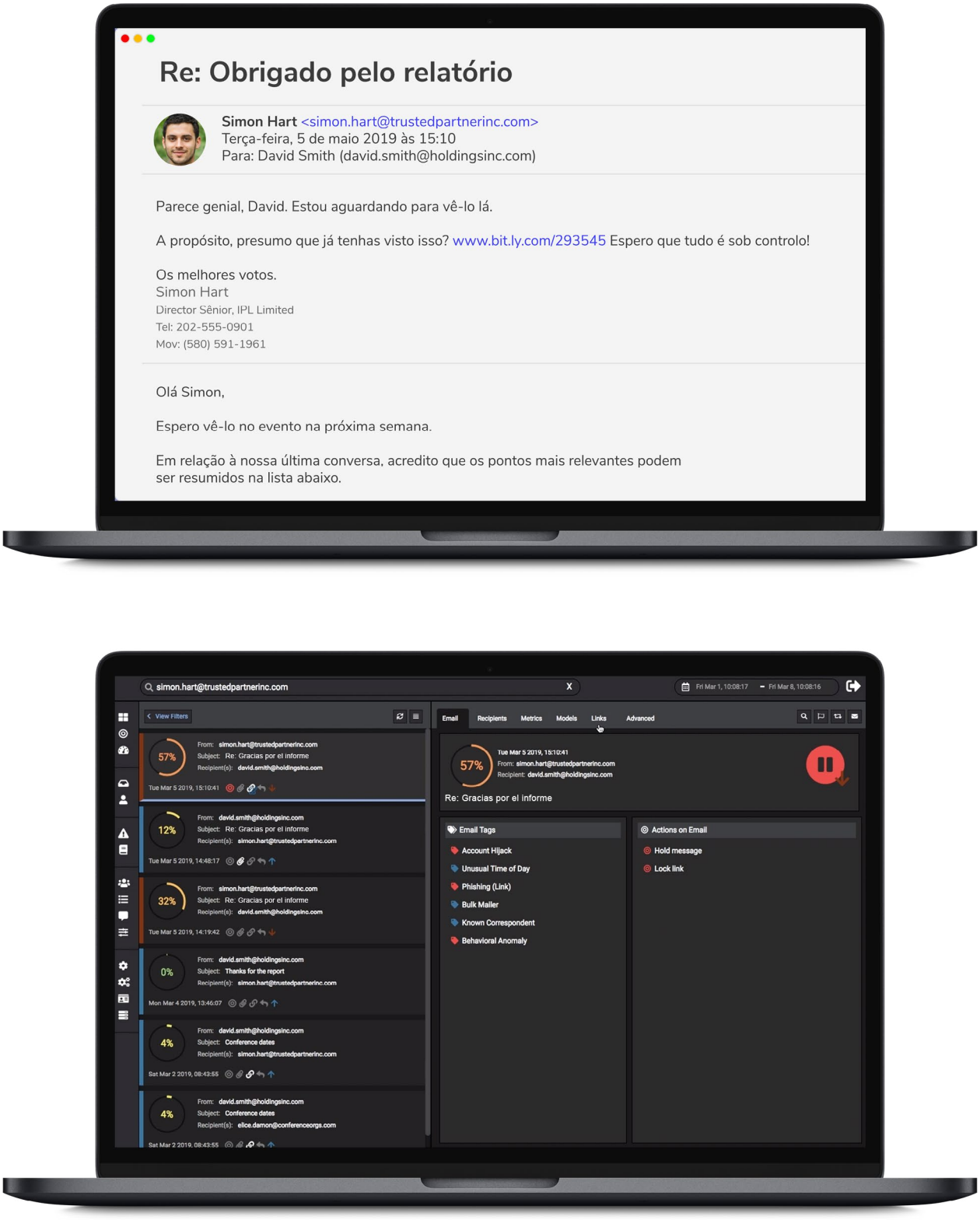


Figura 8: Uma resposta plausível enviada da conta comprometida de um fornecedor confiável após uma conversa de correspondência por email. O link continha uma carga maliciosa

CASE STUDY REAL

Ataques consecutivos à cadeia de suprimentos

Um cliente da Darktrace enfrentou dois incidentes sérios em dias sucessivos, quando as contas de email de fornecedores confiáveis tornaram-se a origem de uma campanha maliciosa — provavelmente após o comprometimento dessas contas.

Em todos os casos, a Antigena Email recomendou a retenção dos emails 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.

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 era uma empresa de consultoria ambiental sediada no Reino Unido.

Menos de duas horas após essa troca rotineira, emails foram rapidamente enviados para 39 usuários, cada um contendo um link de phishing. Houve variação nas linhas de assunto e nos links contidos nos emails, sugerindo emails 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.

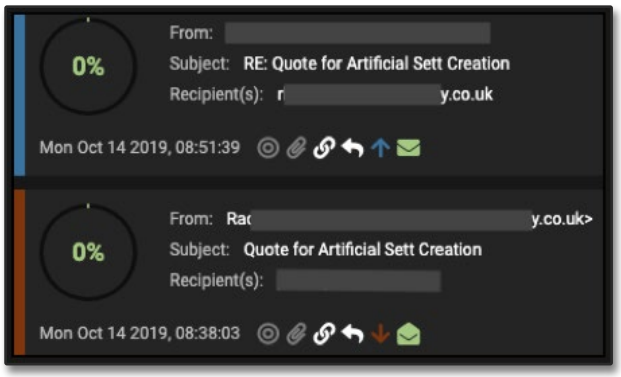


Figura 9: Correspondência anterior "normal" com o remetente – com pontuação de anomalia de 0%

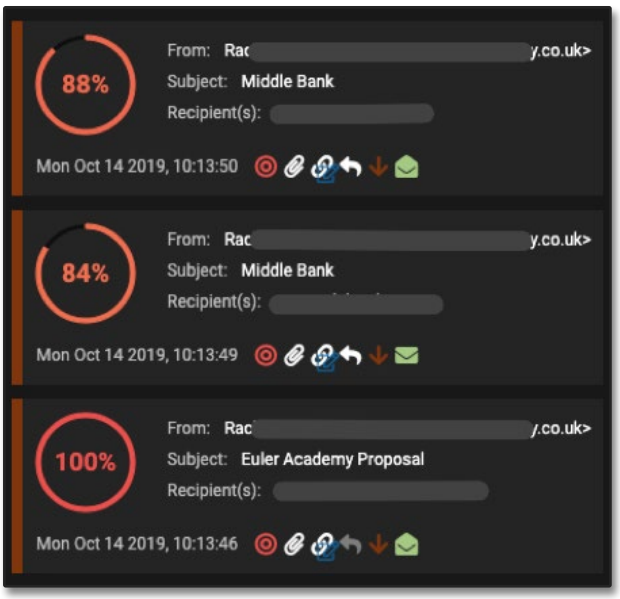


Figura 10: Emails enviados mais tarde no mesmo dia contendo anexos maliciosos

A Antigena Email identificou toda a gama 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 emails 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 emails 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.

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 email 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 email.

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

Figura 11: Métricas acionadas pela raridade e inconsistência do link

4. Anomalia de assunto: As linhas de assunto desses emails 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 emails sobre propostas de negócios usando esse estilo de frase.

Property	Value
Recipient > Metrics > Association Anomaly	100

Figura 12: a Antigena Email detectou rapidamente que esse grupo de destinatários não estava intimamente relacionado

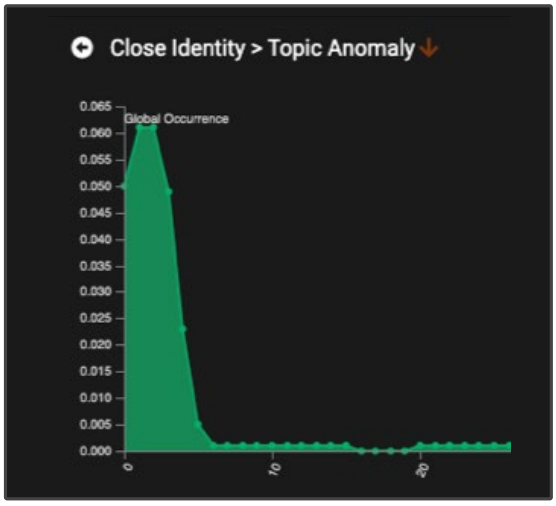


Figura 13: A visualização de resumo da métrica de anomalia de assunto

Incidente 2 – Provedor SaaS comprometido

Um segundo ataque no dia seguinte envolveu o envio de emails para 55 usuários internos de um provedor SaaS conhecido pela empresa. Na ausência de qualquer ação da Microsoft, mais de 50% desses emails foram lidos pelos destinatários. A Antigena Email moveu esses emails para a Lixeira e bloqueou os links.

1. Como antes, os emails enviados da conta comprometida continham um link malicioso 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 emails 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.

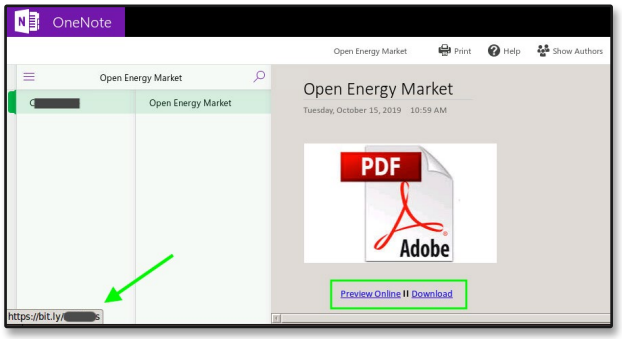


Figura 14: Captura de tela expondo um link oculto

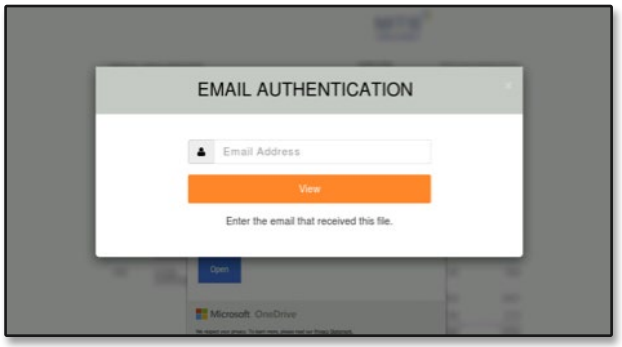


Figura 15: Isso levou a um formulário que coletaria as credenciais do usuário

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 malicioso.

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 email e a senha do usuário com o objetivo de enviá-los diretamente ao invasor.

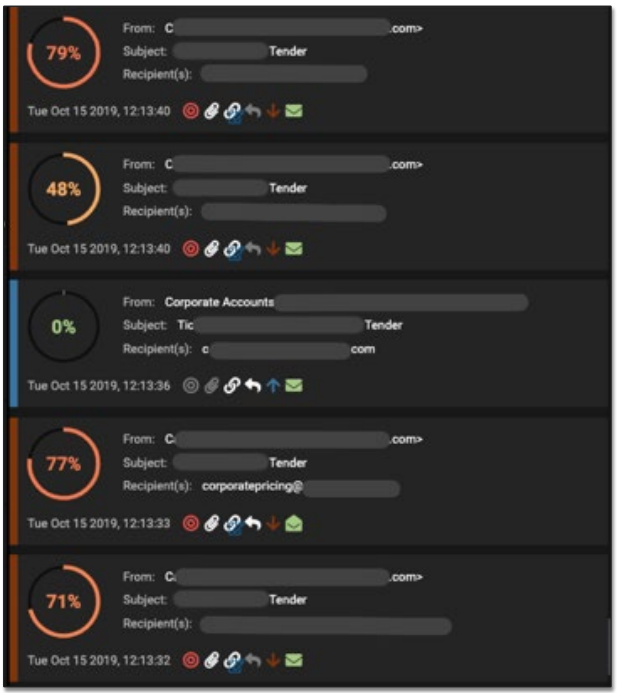


Figura 16: Emails do Incidente 2 conforme exibidos no console da Antigena Email, incluindo aqueles que foram enviados em resposta. Isso revela que o usuário de "contas corporativas" confirmou o email ao abrir um ticket

ESTUDO DE CASO REAL

Arquivo oculto malicioso na página do OneDrive

Um agente de ameaças avançado sequestrou a conta de email de um fornecedor de um grande grupo de hotéis, usando a conta confiável para enviar uma carga maliciosa 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 email anterior revela o entendimento da Antigena Email de que havia uma relação entre os dois remetentes.

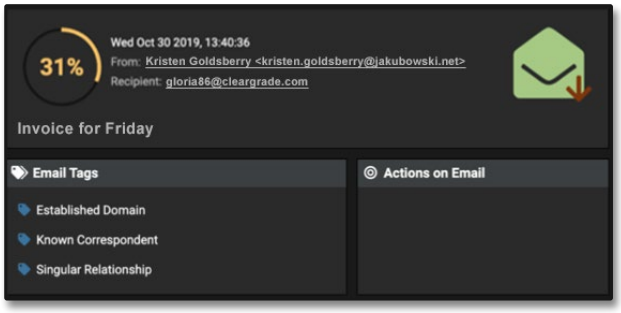


Figura 17: Um exemplo de uma comunicação anterior

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

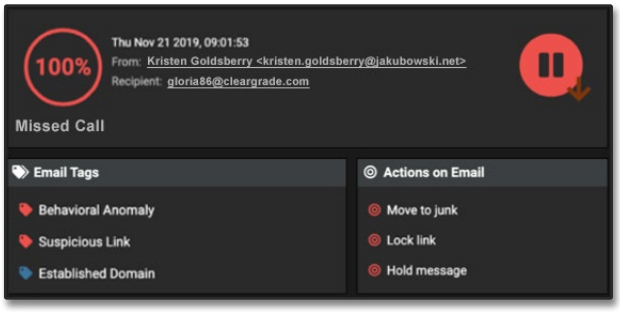


Figura 18: Um email posterior marcado e três violações de modelo associadas

3. Como podemos observar, esses emails 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 malicioso no email também era altamente inconsistente com os "padrões de vida" da empresa para tráfego de email, ele foi bloqueado pela Antigena Email.

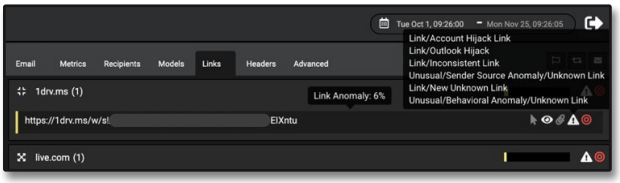


Figura 19: O link malicioso identificado

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 malicioso usando uma abordagem tradicional, pois é impossível incluir serviços como o SharePoint em lista negra. Além disso, decidir se um link como esse é malicioso ou benigno requer uma compreensão do email 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 sejam aconselhadas a investir no treinamento de segurança dos funcionários, nenhuma orientação pode garantir imunidade a esses ataques cada vez mais sofisticados.

Enquanto as campanhas de phishing tradicionais incluem normalmente uma carga oculta maliciosa atrás de um link ou anexo, as tentativas de engenharia social envolvem geralmente o envio de "emails limpos" que contêm apenas texto. 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 exclusivo do ser humano por trás do endereço de email que evolui ao longo do tempo, permitindo detectar casos sutis de solicitação. Emails limpos que burlam as defesas tradicionais podem ser identificados em segundos graças a uma ampla gama de métricas, incluindo semelhanças suspeitas com usuários conhecidos, associações anormais entre destinatários internos e até anomalias no conteúdo e no assunto dos emails.

Com frequência, os ataques de engenharia social procuram levar imediatamente a conversa off-line, e medidas de segurança lentas e reativas intervêm apenas depois que o dano está feito. Seu poderoso entendimento de cada usuário, dispositivo e suas relações na organização permite à Antigena Email responder proativamente e com alta confiança na primeira vez, intervindo no estágio inicial.

A Antigena Email também tem capacidade de adaptar as respostas a tipos de ameaças específicos. Ela entende que o elemento perigoso em um ataque de solicitação é frequentemente o próprio conteúdo do email e que o sistema pode impedir a entrega, protegendo preventivamente o destinatário pretendido.

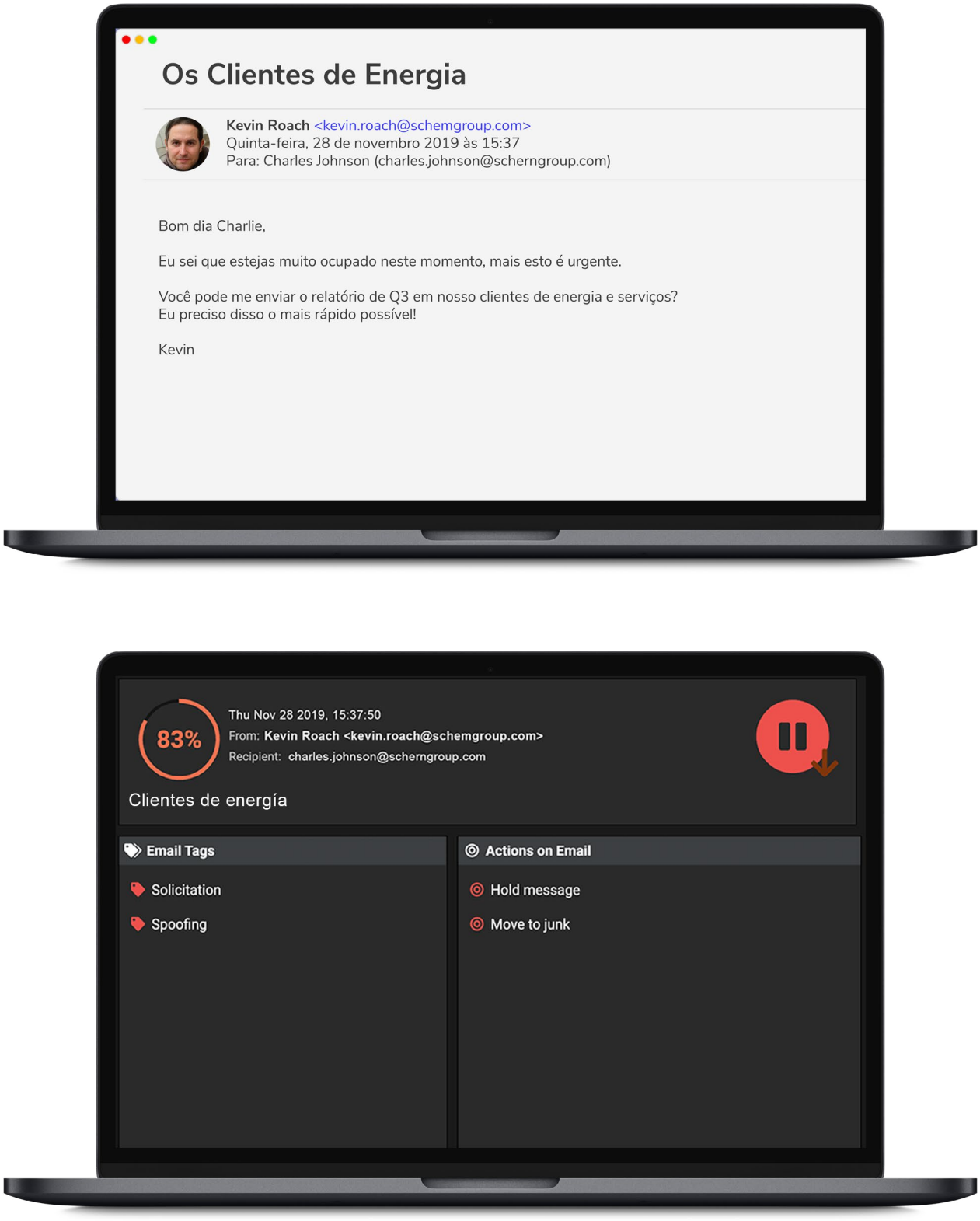


Figura 20: Um invasor que se apresenta como executivo, buscando documentos confidenciais. Observe o endereço de email falsificado

ESTUDO DE CASO REAL

Ataque de clonagem

A Antigena Email detectou um ataque direcionado contra 30 funcionários de uma empresa multinacional de tecnologia. É evidente que foi realizada uma pesquisa abrangente, pois, para cada usuário-alvo, o invasor clonou a identidade do executivo de nível C com quem o usuário tinha maior probabilidade de se comunicar. A Antigena Email identificou o ataque de engenharia social e impediu que os emails chegassem aos destinatários pretendidos.

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

2. A Darktrace não apenas identificou as tentativas de clonagem ao reconhecer o nome de domínio semelhante, mas também constatou que os emails violavam o modelo de "No Association" (Sem associação), não havia evidências de uma relação entre esse remetente e a organização.

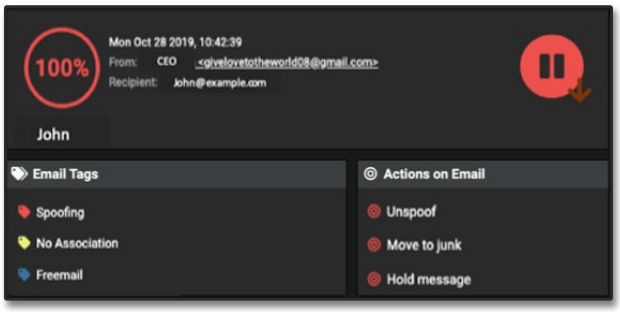


Figura 21: Um dos 30 emails com 100% de pontuação de anomalia

3. Correlacionando vários indicadores fracos, a Antigena reconheceu esses emails como componentes de um ataque coordenado, fazendo com que ela os mantivesse em 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.

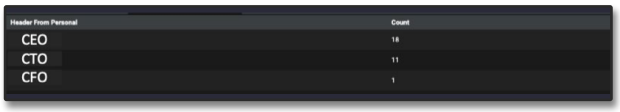


Figura 22: Três executivos de nível C identificados

5. Além disso, a pontuação de exposição dos usuários clonados era alta, indicando que eles eram alvos importantes e, portanto, violava 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.

Esses emails convidavam os destinatários a continuar a conversa fora do email, solicitando o envio de informações altamente confidenciais para fora da organização pelo aplicativo SaaS. Portanto, ferramentas de email com foco somente na detecção de incidentes de perda inesperada de dados não teriam identificado esse ataque.

CASE STUDY REAL

Solicitação de folha de pagamento do CEO

Em uma distribuidora de energia elétrica, a Antigena Email detectou uma tentativa de falsificação convincente em uma conta de email do Microsoft 365. Um email, 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.

O invasor havia imitado com precisão o estilo de escrita do CEO e o email teria provavelmente cumprido seus objetivos caso a IA da Darktrace não tivesse identificado suas características sutilmente anômalas.

1. Ao aprender o "padrão de vida" normal do funcionário, do CEO e de seus grupos de colegas, a Darktrace conseguiu sinalizar imediatamente uma série de anomalias sutis no email, inclusive o endereço do remetente falso.

Figura 23: Captura de tela do email clonando a identidade do CEO

2. Entre outros indicadores fracos, a antigena Email calculou automaticamente a proximidade anômala do domínio com a dos funcionários internos e contatos confiáveis.

3. A Antigena Email respondeu imediatamente, bloqueando os links do email e marcando a mensagem claramente como uma falsificação antes que ela chegasse ao departamento de folha de pagamento. A ampla compreensão da Darktrace sobre a usuária pretendida e seu grupo de colegas permitiu neutralizar uma ameaça de alta gravidade que as ferramentas baseadas em assinatura não teriam identificado.

ESTUDO DE CASO REAL

"Vice-presidente financeiro" visando a iniciar relação interna de confiança

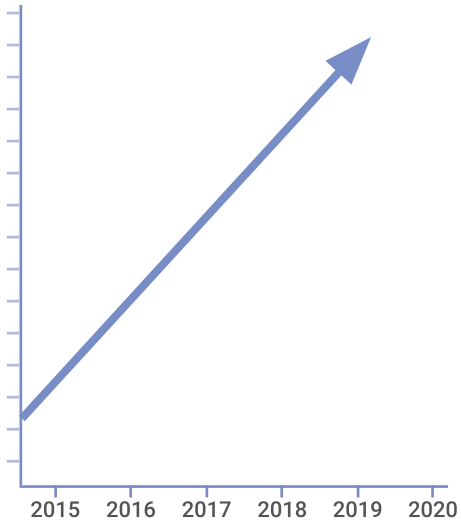
Esse incidente envolveu a clonagem da identidade de um vice-presidente de uma instituição financeira conhecida. Os agentes da ameaça enviaram 11 emails semelhantes à organização, mas a Antigena Email tomou medidas para reter todos eles graças ao seu entendimento multidimensional de "normal" sobre o tráfego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

Figura 24: Captura de tela do link suspeito de compartilhamento de email

Figura 25: Quatro dos 11 emails, mostrando a alta pontuação de anomalia e a ação associada da Antigena Email

Credenciais de funcionário comprometidas

O comprometimento de credenciais aumentou 280% entre 2016 e 2019



Os invasores roubam credenciais de email usando vários métodos, desde a utilização de software que registra toques no teclado em um computador comprometido até o roubo de bancos de dados. 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 email 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 email 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 são geralmente monitoradas por defesas simples e estáticas, incluindo regras de "impossible travel" (viagem impossível) que raramente capturam invasores que sabem se esconder.

Ao aprender o "padrão de vida" normal de cada usuário, o IA de autoaprendizagem 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.

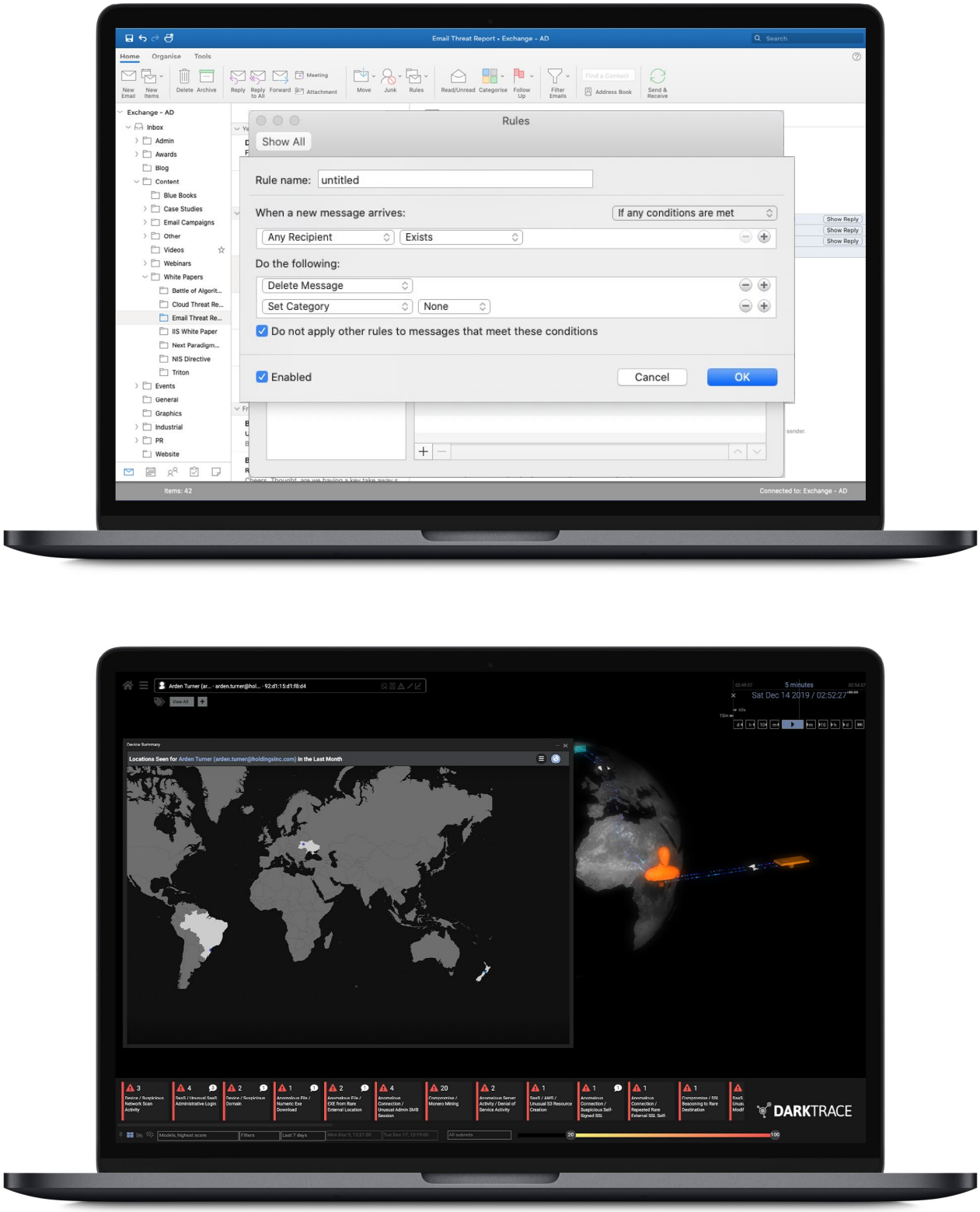


Figura 26: Uma regra de processamento de emails sendo configurada em uma conta comprometida e o Threat Visualizer exibindo os locais geográficos de login

ESTUDO DE CASO REAL

Comprometimento do Microsoft 365 e Teams

Uma conta do Microsoft 365 foi comprometida recentemente em uma empresa de contabilidade pública localizada nos Estados Unidos. A Darktrace detectou inicialmente várias anomalias, incluindo um aumento repentino no tráfego de saída de emails, bem como a localização incomum de login – embora a empresa e praticamente todos os seus usuários estejam localizados em Wisconsin, um endereço IP no Kansas foi usado para fazer login na conta do Microsoft 365. Juntamente com o login incomum, foi detectado um login no Microsoft Teams partindo do mesmo endereço IP do Kansas.

Figura 27: Logo após a criação da nova regra de email, ocorreu um login de um endereço IP 100% incomum no Microsoft Teams

As regras de "impossible travel" (viagem impossível) sozinhas não teriam identificado essas anomalias, mas um entendimento da atividade e do comportamento em diferentes aplicativos SaaS permitiu à IA da Darktrace reconhecer esses eventos como um caso sistemático de roubo de credenciais. Quando o agente da ameaça criou subsequentemente uma nova regra de email, a Darktrace foi capaz de associar esse evento a outro comportamento anormal e entender sua natureza potencialmente maliciosa.

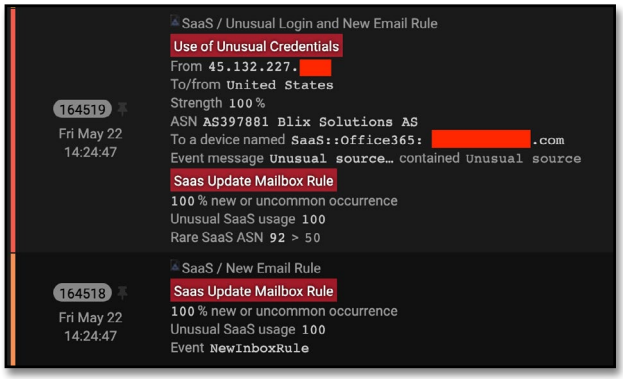


Figura 28: O Módulo de SaaS da Darktrace observou o login de um IP 100% incomum na conta do Microsoft 365 do usuário e a criação de novas regras de caixa de entrada. Todos os fatores indicavam 100% uma atividade totalmente incomum no SaaS

Cinco minutos depois, a Antigena Email alertou sobre o envio de um grande número de emails contendo uma linha de assunto genérica e um PDF anexado. A tecnologia detectou também um aumento claro no envio de emails por esse usuário e sinalizou tais emails com a tag "Out of Character" ("Em desacordo"), que nesse caso denotava uma alteração no comportamento normal com o aumento de destinatários e provável comprometimento interno.

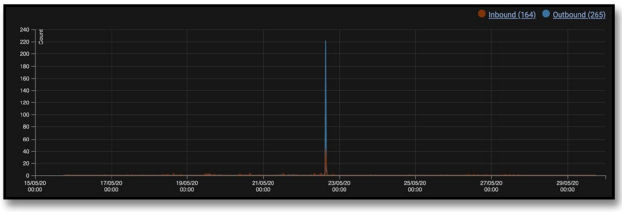


Figura 29: A Antigena Email detectou um aumento nos destinatários que indicava uma violação séria no comportamento normal desse usuário

O comportamento incomum de login detectado pelo Módulo de SaaS da Darktrace pôde ser associado ao comportamento anormal no envio de emails sinalizado pela Antigena Email, permitindo à equipe de segurança verificar a extensão do ataque e neutralizá-lo no momento de seu surgimento. Era evidente que a conta estava sendo usada para participar de atividades maliciosas, pois cada um dos 220 emails enviados usava uma linha de assunto genérica e continha um anexo suspeito. Portanto, a equipe de segurança desativou imediatamente a conta comprometida.

Figura 30: Reprodução do email enviado pelo invasor, contendo o anexo mal-intencionado

ESTUDO DE CASO REAL

“Alteração de detalhes bancários” enviado do departamento de contas

Quando uma conta do Microsoft 365 do Departamento de contas foi comprometida e usada para enviar emails de phishing direcionados, a Darktrace conseguiu rastrear a movimentação do invasor na caixa de entrada, juntando as informações do módulo de SaaS da Darktrace com os alertas da Antigena Email para entender o cenário completo da ameaça e interromper o ataque.

A conta de SaaS parece ter sido comprometida por um ataque de spear-phishing de entrada ou por outra forma de ataque ocorrido antes da Darktrace começar a monitorar a organização. Embora a Ciber IA da Darktrace não tivesse supervisão do comprometimento inicial, ela ainda pôde identificar o comportamento posterior do invasor como malicioso, com base em seu entendimento em constante evolução sobre a organização e seus colaboradores.

Quando o usuário da conta fez login usando um endereço IP francês 100% raro, o Módulo de SaaS da Darktrace detectou imediatamente a anomalia e identificou ainda uma série de atividades realizadas após o login incomum. Ao mesmo tempo, a Antigena Email detectou o envio de um email.

Figura 31: O login de um IP francês foi considerado 100% raro para esse usuário e conta de SaaS

A Darktrace identificou mais atividades ocorrendo em um segundo local de login incomum: um endereço IP suíço. Houve muito pouca atividade de email quando a conta estava conectada usando esse IP. Em vez disso, a Ciber IA observou que o agente da ameaça usava seu acesso ilegítimo ao SaaS para visualizar informações sobre o usuário legítimo da conta e arquivos relacionados a transações bancárias, faturas e pagamentos.

Em seguida, a Antigena Email identificou uma série de comunicações por email que, quando observadas no contexto do comprometimento da conta de SaaS, apontavam para uma clara ameaça. Não havia anexos ou links maliciosos óbvios nos emails. No entanto, o assunto “Alteração de detalhes bancários” da resposta final do destino era um forte indício de que o agente malicioso havia enviado emails instruindo o destino a alterar os detalhes de pagamento para transferir dinheiro para o invasor, e não para a empresa.

Aparentemente, os invasores examinaram os arquivos de transações bancárias e faturamento para encontrar um cliente com uma conta a pagar volumosa e depois usaram a conta de email comprometida para iniciar um ataque de phishing de saída, alterando os detalhes da cobrança. Com a IA da Darktrace correlacionando informações na plataforma de SaaS e conhecimentos profundos da Antigena Email, foi possível conter esse ataque de phishing direcionado antes que houvesse outros comprometimentos ou danos.

A captura de tela a seguir indica também uma série de regras de processamento de caixa de entrada realizadas na conta comprometida, mostrando ações típicas de uma aquisição de controle de conta.

Figura 32: Registros da Darktrace de novas regras de caixa de entrada sendo definidas na conta de SaaS comprometida

ESTUDO DE CASO REAL

Aquisição do controle de contas num banco do Panamá

Uma conta do Microsoft 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 no 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 mais detalhada 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 33: A atividade associada à conta de SaaS, destacando as credenciais alteradas

A Darktrace testemunhou então 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 34: A atividade associada à conta de SaaS, destacando as credenciais alteradas

ESTUDO DE CASO REAL

Origem externa incomum

Em uma empresa de serviços financeiros sediada na Europa, foi observado um usuário do Microsoft 365 fazendo 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 malicioso 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 mais detalhada.

A equipe de segurança conseguiu bloquear remotamente a conta do Microsoft 365 e redefinir as credenciais, impedindo que o agente malicioso 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.

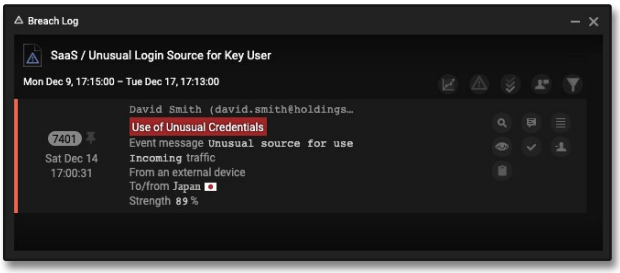


Figura 35: O login do Japão violou vários modelos

ESTUDO DE CASO REAL

Conta do Microsoft 365 comprometida e sabotada

Em uma organização internacional sem fins lucrativos, a Darktrace detectou uma aquisição de controle de conta no Microsoft 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 emails, que apaga emails recebidos e enviados, havia sido configurada na conta. Esse era um indicativo 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 emails, 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 usar 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.

A Plataforma de Ciber IA

Antigena Email pode ser aprimorada com fontes de dados adicionais quando implantada como parte da Plataforma de Ciber IA mais ampla da Darktrace. Isso permite à Antigena Email incorporar a inteligência de outras partes dos negócios e aumentar ainda mais sua capacidade, estendendo a compreensão da IA sobre os "padrões de vida" normais dos usuários no ambiente de email ao comportamento e à atividade deles em plataformas na nuvem e SaaS, bem como em uma rede tradicional e muito mais.

Isso não apenas melhora a tomada de decisão da Antigena Email na camada de email, mas também oferece proteção de autoaprendizagem em toda a infraestrutura digital, deixando os invasores sem ter onde se esconder. A análise contínua da IA, em particular, é aprimorada, pois novas evidências de uma ameaça que se torna evidente em uma rede mais ampla podem ser utilizadas para retornar retroativamente um email entregue.

Nenhuma outra solução de segurança de email tem a capacidade de integrar informações em tempo real a partir de várias fontes no restante da empresa. Quando implantada com o restante da Cyber AI Platform, a Antigena Email complementa uma estratégia de segurança verdadeiramente corporativa, fornecendo visibilidade incomparável dos sistemas e proteção inigualável até contra as ameaças cibernéticas mais sofisticadas.

Descubra a Antigena Email em seu próprio ambiente.

Clique aqui para solicitar uma avaliação gratuita

Sobre a Darktrace

A Darktrace é a principal empresa de Ciber IA do mundo e a criadora da tecnologia Autonomous Response. Sua IA de autoaprendizagem é modelada com base no sistema imunológico humano e usada por mais de 3.500 organizações para proteção contra ameaças à nuvem, a emails, ao IoT, a redes e sistemas industriais.

A empresa tem mais de 1.200 profissionais e está sediada em São Francisco, EUA, e em Cambridge, Reino Unido. A cada três segundos, a IA da Darktrace combate uma ameaça cibernética, impedindo-a de causar danos.

Contate-nos

América Latina: +55 11 4949 7696
América do Norte: +1 (415) 229 9100
Europa: +44 (0) 1223 394 100
Região Ásia-Pacífico: +65 6804 5010
info@darktrace.com | darktrace.com
@darktrace