# Cinco passos para combater o comprometimento de e-mail corporativo

## Principais vantagens

- Detectar e bloquear variantes de BEC lidando com múltiplas táticas dos atacantes
- Obter visibilidade sobre quais usuários são mais atacados e quais terceiros representam maior risco de ataque
- Receber notificações caso os fornecedores com os quais você interage tenham contas que possam estar comprometidas
- Educar os usuários para identificar e denunciar fraudes de e-mail
- Acelerar a resposta a ameaças e economizar tempo automatizando a remediação
- Melhorar a segurança e a eficácia operacional com uma solução integrada de ponta a ponta

O comprometimento de e-mail corporativo (BEC) é um fator preponderante na perda financeira. Segundo o relatório de crimes de Internet do FBI, as perdas anuais associadas a BEC excederam US$ 2,7 bilhões, 80 vezes mais do que as associadas a ransomware.[1]

Os ataques de BEC costumam se fazer passar por remetentes utilizando e-mails que tentam levar os destinatários a pensar que estão interagindo com uma fonte confiável. Em seguida, os atacantes utilizam essa confiança para, por exemplo, induzir os destinatários a efetuar uma transferência de dinheiro fraudulenta ou algum outro pagamento financeiro. A defesa contra tais ataques é desafiadora porque sua eficácia não depende de cargas virais maliciosas. Alguns atacantes vão ainda mais longe, utilizando contas de fornecedores comprometidas, mas legítimas, para lançar seus ataques de BEC.

Proteger a sua organização contra BEC exige tanto tecnologia quanto instrução. Você precisa de uma abordagem mais holística para realmente quebrar a cadeia de ataque do comprometimento de e-mail. A Proofpoint pode ajudar.

Somos o primeiro e único fornecedor a oferecer uma plataforma de proteção contra ameaças abrangente e integrada que:

- Detecta e bloqueia as ameaças de BEC antes que elas cheguem às caixas de entrada
- Permite que os usuários identifiquem e denunciem o BEC
- Oferece visibilidade sobre riscos de fornecedor e contas de terceiros comprometidas
- Automatiza a detecção e resposta a ameaças
- Protege a sua marca em ataques de fraude de e-mail

Este resumo de solução descreve nossa abordagem mais detalhadamente.

1 *Internet Crime Report* (Relatório de crimes de Internet), Federal Bureau of Investigation dos EUA, 2022.

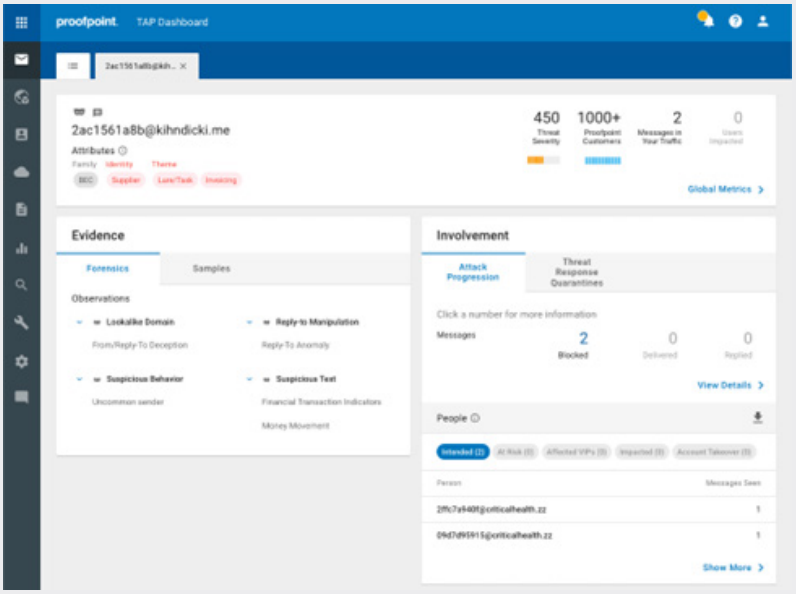


Figura 1. A Proofpoint identifica os usuários mais atacados por BEC e proporciona visibilidade granular sobre os detalhes das ameaças de BEC, inclusive temas, táticas utilizadas e mais.

## Detecte e bloqueie ameaças de impostura antes que elas entrem

Nossa plataforma integrada utiliza o Advanced BEC Defense, respaldado pelo Supernova, nosso mais recente mecanismo de detecção de BEC orientado por inteligência artificial. Essa tecnologia de ponta resultou em um aumento de 17 vezes na quantidade de ameaças identificadas, expandindo nossa detecção para uma ampla variedade de ataques de fraude de e-mail.

O Advanced BEC Defense realiza análise detalhada de vários atributos das mensagens, inclusive:

- Dados dos cabeçalhos das mensagens
- Endereço IP do remetente
- Relacionamento do remetente ou destinatário
- Reputação do remetente

O Advanced BEC Defense utiliza análise semântica baseada em um grande modelo de linguagem (LLM) para verificar o corpo das mensagens quanto ao tom e o idioma. Isso ajuda a determinar se a mensagem é uma ameaça de BEC. O mecanismo de autoaprendizagem comportamental rastreia as atividades para extrair indícios comportamentais, ou assinaturas de ameaças, para compreender padrões que são subsequentemente utilizados para detectar anomalias em tempo real.

Alguns dos elementos rastreados incluem:

- Se um remetente está enviando uma quantidade incomum de e-mails
- Se os e-mails estão vindo de um endereço IP incomum
- Se o remetente já teve contato com os usuários da empresa

Esses sinais reforçam a solução de detecção e viabilizam novos casos de uso. Como resultado, o mecanismo de detecção agora captura outras ameaças avançadas de e-mail, como ransomware, phishing de credenciais e contas comprometidas de terceiros.

O Advanced BEC Defense detecta falsificações do nome de exibição e domínios parecidos. Ele até bloqueia os ataques mais sofisticados de fraude de fornecedor analisando dinamicamente as mensagens quanto a táticas associadas a fraudes de faturamento de fornecedores. Ele utiliza autoaprendizagem para se ajustar e aprender em tempo real, objetivando baixas taxas de falsos positivos.

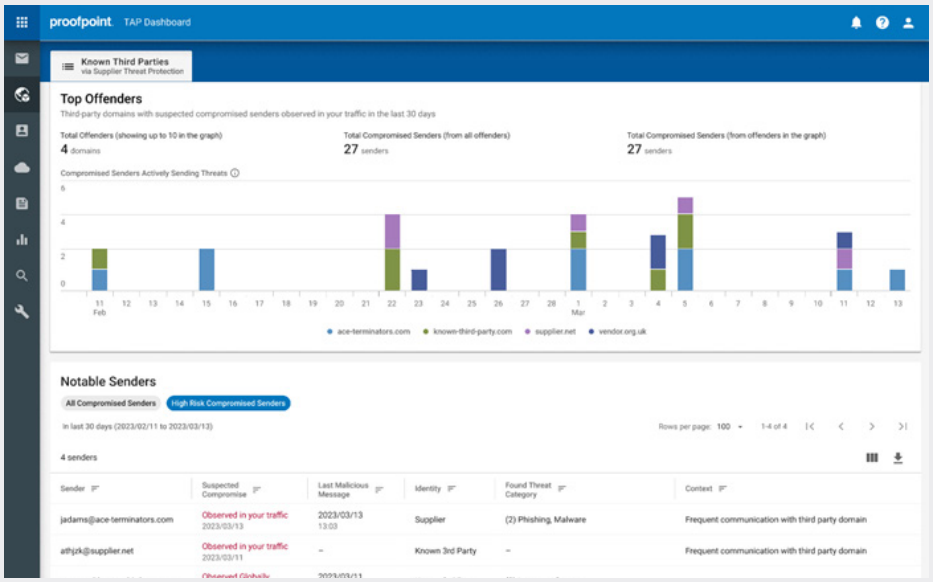


Figura 2. O add-on Supplier Threat Protection detecta contas comprometidas de terceiros com os quais a sua organização interage.

## Obtenha visibilidade sobre seus riscos de BEC

Para ajudar você a compreender, comunicar e mitigar melhor os seus riscos de BEC, nós o ajudamos a dar à sua equipe de gerenciamento respostas para as seguintes perguntas:

- Quais são os seus riscos de BEC?
- Quais são os usuários mais visados?
- Quais dos seus terceiros confiáveis têm contas potencialmente comprometidas?
- Como podemos quantificar e mitigar os riscos?

A Proofpoint pode dizer a você quais dos seus usuários são atacados com mais frequência e quem tem mais possibilidades de se deixar enganar por ameaças de impostura. Nós oferecemos a você uma visibilidade granular sobre os detalhes das ameaças de BEC, revelando os temas quanto aos quais é preciso estar alerta, como fraudes de cartões de presente, de faturamento de fornecedores e de desvio de pagamentos (veja a Figura 1). Em seguida, você pode aplicar controles de segurança adaptáveis aos usuários visados e comunicar melhor o risco à sua liderança.

A Proofpoint estende a sua proteção oferecendo visibilidade e insights sobre fornecedores arriscados. Nós ajudamos você a gerenciar ameaças e riscos de fornecedores:

- Identificando proativamente contas de fornecedores potencialmente comprometidas ou impostoras.
- Proporcionando uma visão das ameaças de BEC priorizadas e centradas nos fornecedores.
- Identificando e evitando ameaças de domínios de fornecedor, bem como domínios maliciosos parecidos com os legítimos.

Nós avaliamos e priorizamos o nível de risco desses domínios de fornecedor e notificamos você sobre contas potencialmente comprometidas. Isso permite que as suas equipes de segurança concentrem-se nos fornecedores que constituem um risco maior para a sua organização.

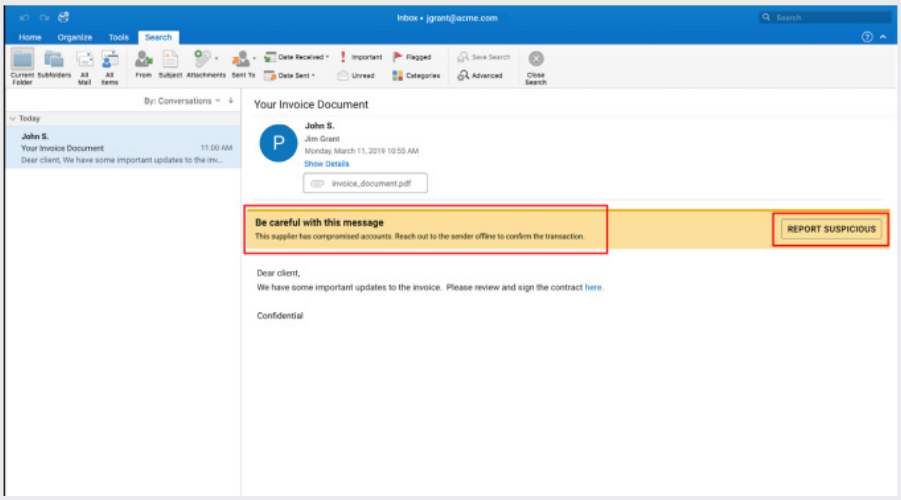


Figura 3. As tags de advertência de e-mail alertam os seus usuários e permitem que eles tomem decisões mais informadas quanto a e-mails duvidosos.

## Torne os usuários resilientes contra BEC

Os ataques de BEC visam pessoas, contando com elas para executar ações maliciosas inadvertidamente. Como esses ataques impostores dependem de engenharia social e falseamento de identidade, frequentemente os seus usuários são a última linha de defesa. É por isso que mitigar riscos de BEC exige tanto tecnologia quanto treinamento.

Com o botão de denúncia do Proofpoint PhishAlarm, você pode empoderar os seus usuários com as ferramentas e o conhecimento certos para identificar e denunciar e-mails suspeitos de impostura. Nossas tags de advertência de e-mail também alertam os usuários quanto a e-mails duvidosos, para que eles possam tomar decisões mais informadas. Você pode treinar os usuários nas táticas de ataque mais recentes utilizadas nas táticas de ataque de BEC mais comuns no momento e designar uma educação direcionada para os seus usuários mais atacados. Isso pode assegurar que eles sejam mais resilientes contra o BEC.

## Automatize a resposta a ameaças

Muitas organizações têm dificuldades com escassez de funcionários em seus departamentos de segurança de TI. É difícil localizar, investigar e mitigar ameaças de BEC em toda uma organização. Nós trazemos automação para a linha de frente dos processos de detecção e remediação de ameaças. Com nosso Threat Response Auto-Pull (TRAP), você pode colocar em quarentena ou remover rapidamente qualquer e-mail suspeito ou indesejado com apenas um clique. A automação estende-se a mensagens encaminhadas para ou recebidas por outros usuários, bem como a mensagens recebidas por outros clientes da Proofpoint. Isso significa que todos são beneficiados pela inteligência adicional.

Nós também simplificamos o gerenciamento da caixa de correio para denúncia de abuso. Os e-mails denunciados pelos usuários são automaticamente analisados e aqueles considerados maliciosos podem ser colocados em quarentena ou remediados. Isso permite a você acelerar a resposta a ameaças e reduzir o trabalho manual.

## Proteja a sua marca em ataques de fraude de e-mail

No caso de falsificação da marca, os atacantes podem colocar você contra os seus clientes e parceiros comerciais utilizando o nome e a marca da sua empresa para roubá-los. A Proofpoint evita que a sua marca seja vítima de abuso em ataques de BEC impedindo que e-mails fraudulentos sejam enviados pelos seus domínios confiáveis. Nós autenticamos todos os e-mails entregues à sua organização ou enviados por ela. Simplificando a implementação DMARC com um fluxo de trabalho orientado e serviços gerenciados, nós ajudamos você a proteger os seus domínios contra falsificação e bloqueamos todas as tentativas de envio de e-mails não autorizados pelos seus domínios confiáveis.

Nós também proporcionamos visibilidade sobre todos os e-mails enviados com o seu domínio, inclusive de remetentes terceiros confiáveis. Nós identificamos domínios semelhantes aos seus. Nós detectamos dinamicamente domínios recém-registrados que estejam imitando a sua marca em ataques de e-mail. E com nosso serviço Virtual Takedown, você pode tomar providências rápidas para derrubar esses sites.

# Resumo

A fraude de e-mail está por trás das maiores perdas financeiras. Conforme os fraudadores se tornaram mais sofisticados, os esquemas de BEC também evoluíram para incluir ataques complexos de fraude de fornecedor. A Proofpoint é o primeiro e único fornecedor a entregar uma solução integrada de ponta a ponta para defesa efetiva contra essas ameaças emergentes.

Nossa solução para BEC:

- Detecta e bloqueia vários tipos de ataques de BEC
- Proporciona visibilidade sobre a superfície de ataque humana e detalhes granulares das ameaças de BEC
- Identifica os fornecedores que representam risco e que podem ter contas comprometidas
- Treina os usuários para que estes sejam mais resilientes ao BEC
- Automatiza a investigação e resposta a incidentes
- Protege a sua marca em ataques de fraude de e-mail

Com a Proofpoint, você pode se defender do BEC com mais rapidez, facilidade e efetividade.

## SAIBA MAIS

Para obter mais informações, visite **proofpoint.com/br**.

**SOBRE A PROOFPOINT**

A Proofpoint, Inc. é uma empresa líder em cibersegurança que protege as organizações em seus maiores riscos e seus ativos mais valiosos: sua equipe. Com um pacote integrado de soluções baseadas em nuvem, a Proofpoint ajuda empresas do mundo todo a deter ameaças direcionadas, proteger seus dados e tornar seus usuários mais resilientes contra ataques cibernéticos. Organizações líderes de todos os portes, incluindo 75% das empresas da Fortune 100, contam com a Proofpoint para obter soluções de segurança e conformidade centradas nas pessoas e que minimizem seus riscos mais críticos em e-mail, nuvem, redes sociais e Web. Mais informações estão disponíveis em **www.proofpoint.com/br**.



proofpoint.

0201-012-07-02 11/23