Isolamento de links de e-mail

Isole os links de e-mail para reduzir a superfície de ataque e simplificar operações

Reduza os riscos de phishing com as proteções e os controles do isolamento do navegador

Desafio: phishing multicanal sofisticado

O phishing multicanal abrange a entrega de e-mail e da web de maneiras que podem escapar habilmente das regras de filtragem. Os tipos mais comuns são:

- **Phishing com atraso**: um link inicialmente inofensivo em um e-mail é posteriormente armado com um destino malicioso após a entrega.
- **Phishing de serviço em nuvem:** links HTTPS perigosos que se assemelham a serviços de nuvem comuns (por exemplo, Google Drive, Box)

A fim de parar essas ameaças, a proteção para e-mails moderna precisa que a Zero Trust aplique o controle "nunca confie, sempre verifique" a todos os links.

Solução: isolamento de links de e-mail

Integrar recursos de isolamento do navegador remoto (RBI) com a segurança para e-mail em nuvem (CES) aplica controles para reforçar a proteção contra phishing. Os clientes que usam o Cloudflare Area 1 podem ativar o isolamento do navegador da Cloudflare para neutralizar essas ameaças multicanal.

Os administradores podem controlar as interações do usuário em páginas web isoladas (como restringir entradas pelo teclado e carregar arquivos) para evitar os impactos do phishing, como a coleta de credenciais ou o roubo de dados confidenciais.

Além disso, abrir links de e-mail em um navegador isolado neutraliza o malware, pois todo o código é executado em nuvem, bem longe dos dispositivos locais.

O que os analistas dizem:

"URLs baseados em e-mails determinados externamente muitas vezes são usados para phishing de funcionários. Isolá-los pode reduzir a quantidade de ataques de phishing bem-sucedidos."

"A maioria dos ataques são realizados pela internet pública, por meio de links em e-mails ou na navegação da web que induzem o usuário a visitar sites maliciosos. A simples remoção (ou, mais amplamente, o isolamento) do navegador do desktop do usuário final melhora de forma significativa a postura de segurança da empresa, incluindo a proteção contra ataques de ransomware."

"Avalie e teste uma solução de isolamento do navegador para usuários de alto risco específicos (como equipes de finanças) ou casos de uso (como a renderização de URLs baseados em e-mail), principalmente se sua organização for avessa ao risco." [1]

Gartner

Leia mais

Benefícios da integração de CES e RBI para a empresa

Reforçar a proteção contra phishing

O isolamento de e-mail não apenas impede que códigos prejudiciais em um link de phishing sejam executados localmente, mas também aplica controles de proteção de dados para evitar que informações confidenciais caiam em mãos erradas.

Desbloquear a produtividade da TI e da segurança

Ative o isolamento de e-mail para qualquer site com alguns cliques.

As equipes de TI e segurança evitam o incômodo de configurar políticas de filtragem que correm o risco de "bloqueio excessivo" (e limitar a produtividade do usuário) e "bloqueio insuficiente" (e permitir a entrada de ameaças).

Exemplo de caso de uso: parar o phishing com atraso

Problema: o phishing com atraso escapa da detecção

Com as táticas e a motivação certas, campanhas de phishing com atraso podem escapar das proteções tradicionais.

Configuração da campanha: os invasores podem começar enviando um e-mail que parece autêntico de um domínio recém-criado, usando uma autenticação de e-mail real (SPF, DKIM, DMAR) e uma página da web benigna.

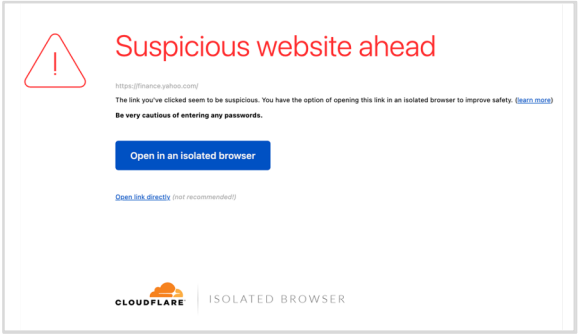
Entrega bem-sucedida nas caixas de entrada: esses e-mails podem escapar da detecção por gateways seguros de e-mail, filtros baseados em autenticação ou outros serviços que usam sinais baseados em reputação e outras técnicas determinísticas.

Direcionamento para um link malicioso: com a entrega bem-sucedida do e-mail, o invasor pode direcionar o link para um destino malicioso mudando a página web controlada por ele. Por exemplo, um redirecionamento comum é para uma página de login falsa usada para coletar credenciais.

Solução: isolamento de links suspeitos após a entrega

O isolamento de links de e-mail é uma parte fundamental da proteção após a entrega. A Cloudflare analisa todos os links em que o usuário clica em um e-mail. Se o link for considerado suspeito ou perigoso, a Cloudflare exibirá uma página de aviso *(veja abaixo)* e isolará a página web caso o usuário decidir navegar mesmo assim.

Os administradores impedem a execução de código malicioso em dispositivos locais e podem aplicar controles de proteção de dados, como a restrição para uploads e downloads de arquivos, a proibição de entradas do usuário pelo teclado ou a abertura da página no modo somente leitura.



Linha do tempo de uma campanha de phishing com atraso

A Cloudflare analisa cada link na hora do clique

Link seguro: os usuários serão redirecionados ao site de forma transparente.

Link malicioso: a navegação será bloqueada para os usuários.

Link suspeito: os usuários são fortemente desencorajados de navegar e veem uma aviso em uma página de erro incentivando a visualizar o link em um navegador isolado.

Como integrar a segurança para e-mails em nuvem com a Zero Trust da Cloudflare

Segurança moderna com Zero Trust

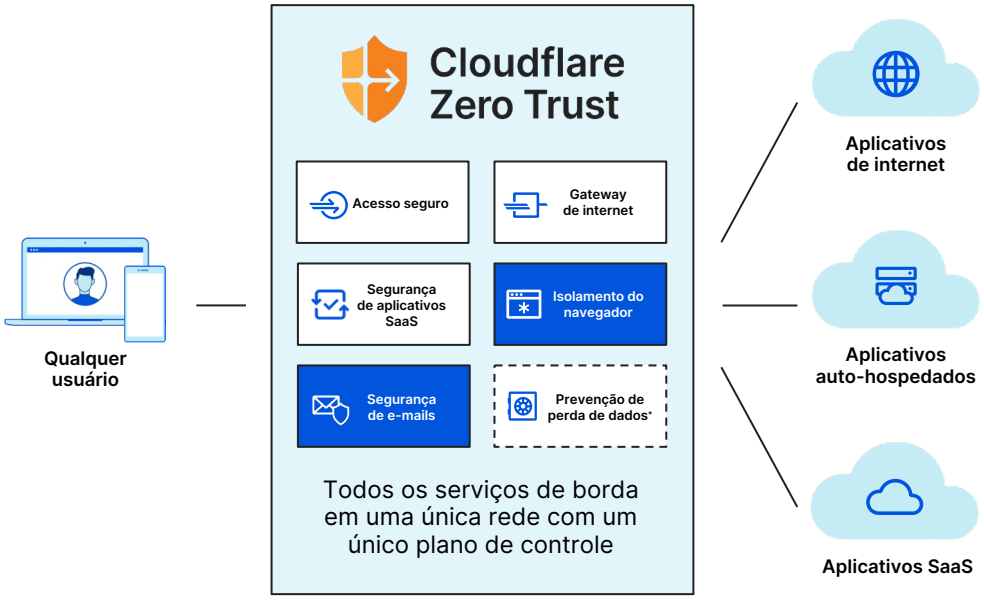
A Zero Trust da Cloudflare aumenta a visibilidade, elimina a complexidade e reduz os riscos à medida que usuários remotos e no escritório se conectam a aplicativos e à internet pública.

Em 1º de abril de 2022, a Cloudflare concluiu a aquisição do Area 1 Security com o objetivo de ampliar a forma como nossa plataforma Zero Trust protege usuários contra ataques de phishing em ambientes de e-mail, web e rede. Leia mais aqui.

Segurança para e-mails: do básico à Zero Trust

A segurança para e-mails do Area 1 da Cloudflare aprimora a Zero Trust ao remover a confiança implícita do e-mail para parar preventivamente ataques de phishing e comprometimento de e-mail corporativo (BEC).

Nunca confie em nenhum remetente, mesmo os internos. Em vez disso, garanta que todo o tráfego de usuários, incluindo o e-mail, seja verificado, filtrado, inspecionado e isolado das ameaças da internet. A segurança de e-mail será integrada aos serviços Zero Trust da Cloudflare, em uma poderosa combinação com RBI, CASB e muito mais.



Substituição de VPN
simplifica e protege a conexão de qualquer usuário a qualquer recurso

Proteção da internet
mantém seus dados a salvo de ameaças com qualquer porta e protocolo

Simplifique a segurança de SaaS
visibilidade e controle de aplicativos, incluindo e-mail

Modernização da segurança
mais produtividade, operações mais simples, superfície de ataque reduzida

* Cadastre-se na nossa lista de espera de DLP

Segurança de e-mail em nuvem (CES)

- Reduza o tempo de resposta a incidentes de phishing em 90%.
- Identifique a infraestrutura do invasor e os mecanismos de entrega com antecedência para interromper o phishing nos estágios iniciais do ciclo de ataque.
- Remova a confiança implícita do e-mail ao analisar o conteúdo, o contexto e os gráficos sociais das comunicações.
- Use integrações com a Microsoft, o Google e outros ambientes para aprimorar a segurança interna.

Isolamento de Navegadores Remotos (RBI)

- Evite o comprometimento de credenciais com a abertura de sites arriscados no modo "somente leitura" controlando as interações dos usuários (por exemplo, entradas pelo teclado, copiar e colar, upload e download).
- Execute todo o código do navegador na Rede da Cloudflare, isolando dispositivos locais do código malicioso.
- Proporcione uma experiência do usuário rápida e sem atritos. Em vez do streaming normal de pixels, criamos uma réplica idêntica da página em um navegador remoto a menos de 50 ms de 95% dos usuários conectados à internet mundialmente.

Solicite uma avaliação de risco de phishing agora — Fale conosco

+55 (11) 3230 4523 | enterprise@cloudflare.com | www.cloudflare.com/pt-br/

REV: PMM-2022JUN

[1] *Gartner Hype Cycle for Network Security, 2021* / GARTNER e HYPE CYCLE são marcas registradas e marcas de serviços da Gartner, Inc. e/ou de suas afiliadas nos EUA e internacionalmente, sendo usadas no presente documento mediante permissão. Todos os direitos reservados.