Grupo de Trabalho Antiabuso de Mensagens, Malware e Móvel (M³AAWG)

M³AAWG, socorro! Caí em uma armadilha de spam!

Fevereiro de 2023

O URL de referência para este documento é: https://www.m3aawg.org/help-i-hit-a-spam-trap

Introdução

Este documento ajuda os Provedores de Serviços de E-mail (ESP) a mitigar as consequências de cair em armadilhas de spam. Ele também sugere maneiras de usar as informações fornecidas por essas armadilhas para melhorar as práticas de envio dos clientes, minimizando assim futuros eventos de spam. Neste documento, "cliente" se refere à organização que usa o ESP para enviar e-mails.

A maioria dos remetentes de e-mail enfrenta, em algum momento, as consequências de ter enviado e-mails para armadilhas de spam. A magnitude das consequências pode variar muito dependendo do número de mensagens enviados à armadilha, do tipo de armadilha, de quem opera a armadilha e de outras variáveis –todos fatores dos quais os clientes podem não estar cientes. Nestes casos, os ESP têm a responsabilidade de monitorar e informar seus clientes quando ocorrer uma armadilha. O ESP vai querer evitar o acesso a estas armadilhas no futuro e mitigar os efeitos destes eventos na entrega de correio. Não fazer isso poderia levar a consequências mais severas na infraestrutura de envio do ESP.

Uma alta taxa de mensagens enviadas para uma armadilha de spam a partir de um determinado fluxo de correio pode indicar um remetente abusivo ou, no mínimo, um que aplica as melhores práticas de envio de modo inconsistente (os padrões recomendados são descritos em M³AAWG Sender Best Common Practices). O domínio do destinatário pode decidir que o melhor para seus usuários é rejeitar mensagens desse fluxo ou atribuir uma prioridade menor para os e-mails apresentados para sua entrega. Em circunstâncias extremas, o ESP pode descobrir que foi bloqueado e que seus e-mails foram rejeitados por uma grande parte da Internet.

Embora ninguém queira cair em uma armadilha de spam, o ESP pode aproveitar as visitas a uma dessas armadilhas como uma oportunidade não apenas para detectar e remover clientes abusivos, mas também para ajudar seus clientes legítimos a identificar e corrigir práticas de envio inadequadas. Mais adiante vamos falar sobre a mitigação e apresentar alguns pontos de discussão para compartilhar com os clientes.

O que é uma armadilha de spam?

Uma armadilha de spam é um endereço de e-mail usado para coletar, registrar e monitorar o envio de spam e

outros e-mails não solicitados ou abusivos. Essas armadilhas são projetadas para serem indistinguíveis de outros endereços de e-mail e podem ser encontradas em todo tipo de redes, incluindo domínios corporativos e de e-mail gratuitos.

Embora existam diferentes tipos de armadilhas de spam, todas elas compartilham uma característica: não enviam mensagens nem assinam listas de e-mail ou newsletters. O operador de uma armadilha monitora as mensagens enviadas para esses endereços e usa os dados para analisar a reputação do endereço IP e do nome de domínio, bem como para avaliar o conteúdo do e-mail.

Muitas vezes, esses dados são usados e redistribuídos por meio de listas negras baseadas em DNS (DNSBL) e outros sistemas de reputação para ajudar a tomar decisões informadas sobre entrega ou bloqueio nos domínios de destinatários que os usam.

Uma taxonomia das armadilhas de spam

Alguns dos tipos mais comuns de armadilhas incluem:

Armadilha reciclada

> Um endereço ou domínio que já foi alguma vez válido, mas que depois de um período de inatividade se tornou uma armadilha de spam. O tempo de inatividade pode variar significativamente entre os operadores, mas o M^{3}AAWG sugere 12 meses como mínimo. Esse tipo de armadilha geralmente é um indicador de uma lista mal gerenciada (ou de uma lista antiga) e/ou da falta de um processamento de rejeição correto.

Armadilha prístina ou pura

> Um endereço que nunca esteve ativo para um usuário de e-mail antes de sua implementação como uma armadilha de spam. Em geral, a gente cai nessas armadilhas pela coleta de dados na web, sondagem do espaço de endereços ou ataques de dicionário. Cair nesse tipo de armadilhas pode ser um forte indicador de listas compradas.

Armadilha tipográfica

> Esta armadilha normalmente inclui um erro tipográfico intencional e talvez comum, principalmente na parte do endereço correspondente ao domínio, por exemplo, user@gmial.com, user@notmail.com e semelhantes. Esse tipo de ocorrência geralmente indica que o cliente não confirmou o endereço do destinatário, possivelmente como resultado de erros de transcrição ou digitalização no momento em que o remetente coletou o endereço de e-mail. Embora isso possa ser tecnicamente uma armadilha perfeita, muitos operadores as classificam de forma diferente, pois os remetentes podem obtê-las por meio de práticas de coleta legítimas.

M^{3}AAWG Best Current Practices for Building and Operating a Spam Trap (Melhores práticas atuais para construir e operar uma armadilha de spam) fornece uma análise mais detalhada dos tipos de armadilhas de spam e seus modos de uso. Este documento faz referência principalmente às armadilhas que afetam diretamente a entrega, não às redes de armadilhas de sensores usadas para monitorar a reputação em vez de para bloquear o e-mail.

Você sabe que caiu em uma armadilha de spam quando...

Como as armadilhas de spam são geralmente projetadas para serem indistinguíveis de outros endereços de e-mail, muitas vezes é difícil saber quando uma determinada mensagem foi enviada para uma delas. No entanto, existem indicadores de que estamos enviando mensagens a uma armadilha de spam, entre eles, a inclusão de um domínio ou um IP em uma lista negra ou um aumento no número de e-mails rejeitados. As ferramentas que monitoram as listas negras e a reputação podem fornecer métricas sobre os envios a armadilhas de spam sem revelar (ou "queimar") as próprias armadilhas de spam.

Em raras ocasiões, um domínio destinatário anuncia a existência de uma armadilha de spam. Isso pode ser feito por meio do nome do host do seu servidor MX no DNS (por exemplo, spamtrap.domain.com) ou de um texto em uma resposta SMTP que indique que o endereço é uma armadilha de spam.

Também existem *feeds* de armadilhas de spam comerciais. Esses serviços, fornecidos por empresas de monitoramento da entregabilidade, têm suas próprias redes de armadilhas de spam. Estas redes não são usadas para bloqueio, mas sim para permitir que os clientes das empresas de monitoramento da entregabilidade vejam que parte de seus e-mails está sendo enviado para essas armadilhas.

Exposição não intencional de armadilhas

Em geral, quem operam as armadilhas não procuram expô-las. O investimento necessário para criar e manter armadilhas que possam produzir dados úteis é significativo. Os operadores devem assumir que, uma vez exposto, o conhecimento da existência de uma armadilha se espalhará rapidamente, minimizando assim a sua eficácia.

No decorrer da pesquisa e correção, os ESP ou seus representantes podem revelar inadvertidamente a identidade de um endereço IP, domínio ou rede de uma armadilha de spam. Para manter a operação discreta necessária, os ESP devem tomar todas as medidas apropriadas para manter a confidencialidade desses dados.

A comunicação com o cliente nunca deve revelar, explícita ou implicitamente, a identidade das armadilhas ou redes, e qualquer discussão sobre esses dados por parte de um ESP deve ser tratada estritamente de acordo com o princípio da "necessidade de saber".

Se forem revelados dados que permitam identificar a armadilha ou a rede, e a identidade do seu operador for conhecida, seria recomendável notificar o operador da armadilha. Informar o operador que a sua armadilha pode estar comprometida permitirá que ele tome as medidas necessárias para manter a eficácia da sua rede. Notificar o operador da armadilha também pode ajudar um ESP a estabelecer ou manter um relacionamento de trabalho positivo com o proprietário da rede.

Remediação

Notificação ao cliente

Um ESP deve notificar seu cliente quando houver evidências de que ele caiu em uma armadilha de spam. Abaixo estão algumas considerações que devem ser levadas em conta ao notificar um cliente sobre esses tipos de eventos.

Auditoria de aquisição

Em geral, os eventos com armadilhas de spam exigem uma auditoria dos procedimentos de aquisição que permitiram que o endereço da armadilha acabasse no banco de dados do remetente. Esta auditoria necessariamente será semelhante aos procedimentos de verificação de listas detalhados no documento M³AAAWG Vetting Best Common Practices. No entanto, alguns de seus aspectos exigirão uma abordagem mais granular e deverão incluir considerações adicionais, tais como:

- Como as listas de contatos foram criadas? Uma auditoria do processo de aquisição deveria se concentrar principalmente nos métodos usados para adquirir e verificar os destinatários dentro de cada lista de contatos.
- É possível saber quando o remetente enviou pela primeira vez uma mensagem para uma armadilha de spam e correlacionar esse evento com um envio específico ou segmento de uma lista a ser alvo de revisão?
- O IP ou domínio apareceu em uma lista de bloqueio como resultado do evento? É possível então inferir que tipos de armadilhas estão implicadas?
- Alguns domínios de destinatários aparecem com maior frequência no segmento implicado, indicando um envenenamento das listas ou a coleta de dados?
- O proprietário da lista está disposto e é capaz de reconstruí-la e obter novamente a permissão dos destinatários?
- Os envios anteriores resultaram em listas de bloqueio prévias? Se sim, como foi resolvida a situação?
- O proprietário da lista pode identificar a origem dos dados problemáticos e remover todos os dados adquiridos por meio dessa fonte?
- O ESP usado para enviar a mensagem pode obter dados adicionais do proprietário da rede de armadilhas de spam?

Assim como na verificação inicial do cliente, as principais áreas a serem examinadas no decorrer de uma auditoria incluirão a coleta, validação e higiene de endereços.

Higiene de listas

Conforme descrito no documento Sender Best Common Practices de M³AAWG (Melhores práticas comuns para remetentes), os ESP deveriam revisar todo o processamento de ciclos de feedback, rejeição e cancelamento de assinatura para garantir que os endereços dos destinatários estejam sendo processados corretamente e removidos quando necessário.

Os ESP também deveriam revisar as práticas de higiene das listas dos clientes para mitigar o risco de enviar e-mails para armadilhas de spam. A adesão rigorosa às políticas detalhadas no documento de *melhores práticas comuns para remetentes* resultará na redução orgânica de ocorrências de armadilhas de spam. As considerações deveriam, portanto, incluir:

- Se a atividade ou participação dos destinatários em um domínio específico for menor à media, poderia estar indicando uma rede de armadilhas de spam. Se a aquisição de endereços nesse domínio puder ser correlacionada com um segmento de lista ou método de aquisição específico, esses segmentos de lista deveriam ser candidatos à correção, e o método de aquisição deveria ser descontinuado.
- Os remetentes deveriam considerar a implementação de uma política para eliminar os destinatários que

nunca participam ou que não podem receber e-mails. Isso minimiza a possibilidade de cair na armadilha se esses endereços se tornarem armadilhas de spam recicladas. Se a incidência de envios a armadilhas continuar no nível atual, o remetente poderia considerar ajustar sua política existente para torná-la um pouco mais agressiva.

- As mudanças recentes nos critérios de segmentação de listas ou no gerenciamento de arquivos de supressão podem estar correlacionadas a um aumento na taxa de acessos a armadilhas de spam e devem sempre ser monitoradas de perto. Cuidado especial deve ser tomado quando o resultado da segmentação é que alguns destinatários que não lhes foi enviado há muito tempo recebem e-mail, já que durante esse período um endereço pode ter sido removido e reutilizado como uma armadilha de spam.

Em qualquer caso, um cliente ou lista que produza muitos acessos a armadilhas de spam deveria ser candidato a uma revisão completa. Se o cliente ou a lista já tiver sido submetido a um rigoroso processo de revisão, então é possível que uma mudança mais recente seja cúmplice de uma maior atividade de armadilhas de spam:

- Houve alguma mudança de pessoal na organização do cliente?
- Houve uma nova implementação de API ou mudanças recentes em uma API existente que possam ter criado oportunidades para seu abuso?
- Houve mudanças nos pontos de coleta de endereços do cliente que possam indicar um formulário web abusivo ou oportunidades de envenenamento da lista?
- Houve mudanças organizacionais mais amplas, por exemplo, fusões e aquisições ou mudanças no modelo de negócios, que pudessem indicar a necessidade de uma nova pesquisa detalhada do cliente?

Eventualmente, um ESP poderia encontrar um cliente que se recusa a participar de qualquer processo de remediação. É fortemente recomendado que os ESP terminem as suas relações com clientes que recusem a remediação, e que considerem limitar o acesso a dados que, de outra forma, poderiam ser fornecidos a esses clientes.

Minimizando incidentes futuros

Práticas de coleta de endereços

Os ESP deveriam revisar os meios usados pelos clientes para coletar endereços para identificar quaisquer áreas potencialmente problemáticas.
Às vezes, as práticas de coleta incentivam os consumidores a compartilhar um endereço de e-mail sem qualquer tipo de verificação dos dados para garantir que o endereço pertence a esse consumidor. Essas práticas geralmente levam a armadilhas de spam nas listas. As práticas de coleta de risco mais alto incluem:

- Inscrições incentivadas
- Inscrições em mídias sociais
- Formulários de recomendação de amigos
- Sorteios

Os endereços coletados usando essas estratégias priorizam *qualquer* endereço de e-mail em vez do endereço de e-mail *correto*, pelo que as listas geradas são de baixa qualidade.

Existem também outras maneiras pelas quais as armadilhas de spam podem acabar em uma lista, entre elas:

- Erros de digitação de endereços inseridos em um ponto de venda
- Endereços extraídos de sites (automática ou manualmente)
- Listas compradas, alugadas ou *e-pended*.
- Listas de participantes em feiras comerciais.
- Formulários de registro de adesão *(opt-in)*.

Durante uma pesquisa de práticas de coleta de endereços, os ESP devem solicitar os dados de adesão específicos do cliente. Uma técnica de pesquisa comum consiste em fornecer vários endereços ao cliente, incluindo alguns endereços que não estão na lista. Depois, o cliente tem que fornecer os dados de adesão que incluem:

- A hora e a data do registro
- O URL do formulário usado e o IP de conexão (se a inscrição foi feita on-line)
- O local da transação, se o endereço foi coletado pessoalmente.

Os clientes deveriam poder fornecer dados específicos da adesão, incluindo, mas não se limitando, o URL de quaisquer formulários web. Como armadilhas de spam às vezes são adicionadas às listas por meio de envios de formulários automatizados, os clientes e os ESP deveriam revisar as análises de tráfego do site. Um tráfego não tradicional ou picos incomuns de volume poderiam indicar que um formulário se tornou o alvo de *bots*, o que leva a um aumento de armadilhas de spam em uma lista.

Os ESP também podem verificar se os processos de adesão estão funcionando conforme o esperado. O resultado de um registro no URL fornecido pelo proprietário da lista no momento da auditoria resulta em uma assinatura verificável? Caso contrário, considere a possibilidade de que os URL fornecidos não pertençam ao proprietário da lista ou que os registros desde a página sejam compartilhados entre muitos. Verifique se algum mecanismo de confirmação existe e se funciona conforme o esperado.

Validação no ponto de coleta

Os clientes podem complementar as boas práticas de coleta com estratégias de validação de endereços de e-mail. Essa validação pode ser realizada por meio de uma revisão interna no ESP ou por um dos vários serviços que fornecem validação sob demanda ou no momento da coleta de endereços. A melhor prática é validar o endereço conforme ele é inserido e solicitar que o assinante insira novamente o endereço se a validação falhar.

Se a validação for feita internamente, há uma série de pistas que os ESP podem procurar em uma lista, e que poderiam indicar estratégias de validação deficientes ou inexistentes. M³AAWG Vetting Best Common Practices oferece uma descrição completa destas estratégias.

Outras estratégias de prevenção

Também existem outras ações que podem ser consideradas para reduzir problemas futuros. Estas incluem limitar a capacidade do cliente de importar listas, por exemplo, ao permitir que os endereços sejam adicionados exclusivamente por meio de um *script* de formulário fornecido pelo ESP ou por meio de algum outro processo.

Restrições de envio, como enviar apenas para segmentos engajados ou exigir ao remetente que, como passo adicional, exclua ou suprima os segmentos que mostrem pouca ou nenhuma interação histórica. Acima de tudo, o cliente deve ser obrigado a descartar os segmentos sem permissões confirmadas, embora poderia ser

aceitável permitir que o cliente tente primeiro reconfirmar suas permissões.

Se um cliente for parte de um ambiente compartilhado, poderia ser necessário isolar esse cliente em uma infraestrutura dedicada para minimizar o potencial de danos à reputação de outros remetentes que usam a mesma infraestrutura compartilhada.

Conclusões

Quando nosso sistema cai em uma armadilha de spam, há muitas coisas a serem consideradas. Os ESP devem proteger a sua infraestrutura, mas também devem avaliar os clientes que caem nestas armadilhas. No final das contas, a armadilha de spam não é o problema, mas sim um sinal de um problema subjacente que tem a ver com a forma como o cliente adquire e valida os endereços. As armadilhas de spam são uma maneira de identificar técnicas inadequadas de coleta de endereços. As armadilhas em si são um indicador de que há endereços na lista sem permissão. Em muitos casos, esses endereços pertencem a pessoas reais que estão recebendo spam. Ao corrigir os processos de coleta que levam às armadilhas de spam também se está abordando o spam que está afetando pessoas reais. A principal preocupação deve ser sempre com os destinatários que possam estar recebendo spam. Existem muitas estratégias eficazes; este documento fornece um ponto de partida para corrigir o problema.

Referência

- No site de M[3]AAWG, acesse "Documents for Senders and ESPs"
  https://www.m3aawg.org/documents-for-senders-and-esps
  e em particular
- M[3]AAWG Sender Best Common Practices, versão 3.0, atualizado em fevereiro de 2015
  https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf
- M[3]AAWG Best Current Practices for Building and Operating a Spam Trap, versão 1.2.0, atualizado em agosto de 2016
  https://www.m3aawg.org/documents/en/m3aawg-best-current-practices-for-building-and-operatin g-a-spamtrap-ver-120
- Vetting Best Common Practices (BCP), novembro de 2011
  https://www.m3aawg.org/sites/default/files/document/MAAWG_Vetting_BCP_2011-11.pdf

Tal como acontece com todos os documentos que publicamos, confira o site do M[3]AAWG (www.m3aawg.org) para ver as atualizações mais recentes.