

Novembro de 2004



McAfee Research
Relatório Técnico Nº 04-004

Anti-Phishing: Práticas Recomendadas para Instituições e Consumidores

Gregg Tally
Roshan Thomas
Tom Van Vleck

1 Introdução

Phishing é uma forma de golpe pela Internet, na qual os atacantes tentam convencer os consumidores a divulgar informações pessoais confidenciais. Normalmente, as técnicas envolvem e-mails e sites fraudulentos que se passam por e-mails e sites legítimos. Os e-mails fraudulentos podem ser considerados um tipo mal-intencionado de e-mail em massa não solicitado, geralmente conhecido como "spam." Os consumidores ficam vulneráveis ao furto de identidades e a prejuízos financeiros por meio de transações fraudulentas. As instituições financeiras estão em perigo devido ao grande número de transações fraudulentas realizadas com as informações roubadas. Os ataques de phishing são, muitas vezes, eventos de larga escala cujo alvo são milhares de consumidores, ou mais, esperando que uma parte deles caia na armadilha. Uma porcentagem relativamente grande de destinatários realmente responde a esses e-mails, pois eles parecem ser legítimos e sua autenticidade não pode ser facilmente verificada. As estimativas de resposta variam entre 1% e 20%, dependendo do ataque. Os atacantes podem copiar facilmente imagens, links e textos de sites legítimos para fazer o e-mail parecer autêntico.. Devido à escala dos ataques, a possibilidade de enormes prejuízos financeiros é grande. Alguns ataques envolvem um milhão ou mais de e-mails de phishing.

Como foi observado pelo APWG (Anti-Phishing Working Group), os clientes de muitos bancos e várias instituições financeiras têm sido alvos de ataques de phishing. Os objetivos são, geralmente, o furto de números de contas de cartões de crédito, débito e PINs. Clientes de outras empresas também têm sido alvos de operações de furto de identidade.

A ameaça do phishing está aumentando rapidamente. O APWG relatou 176 ataques únicos de phishing no mês de janeiro de 2004. Até abril, o número de ataques únicos por mês aumentou para 1.125, atingindo 1.422 em junho. Clientes de instituições financeiras, empresas de varejo e provedores de serviços de Internet foram alvos freqüentes.

Muitas organizações e empresas diferentes propuseram mudanças básicas na infra-estrutura de e-mail para ajudar a minimizar o spam, o que acabaria reduzindo os problemas com o phishing. O Anti-Spam Research Group, do Internet Research Task Force, é uma dessas organizações.. Até que essas mudanças sejam efetuadas, as instituições financeiras e seus clientes podem tomar medidas para ajudar a reduzir o risco dos ataques de phishing. Essas medidas abrangem uma autenticação mais forte para as transações eletrônicas, a distribuição mais ampla de produtos anti-spam, antivírus e firewall pessoal, além da distribuição de software de proteção de privacidade.

Nossas soluções propostas pressupõem que empresas e consumidores continuarão usando por muitos anos alguma forma de hardware e software existentes hoje. Não acreditamos que seja prático propor mudanças radicais nessa base instalada como parte de uma solução de curto prazo. Portanto, as soluções que propomos são compatíveis com produtos amplamente usados por consumidores e empresas, inclusive os atuais navegadores e servidores de Web, aplicativos e servidores de e-mail e sistemas operacionais padrão.

No curto prazo, há pouca chance de que as empresas mudem suas formas consagradas de verificação de identidade, tais como números de documentos pessoais e nome de solteira da mãe. Nossa proposta é tornar mais difícil que os atacantes tenham acesso a essas informações.

Este white paper apresenta um panorama dos estágios de um ataque típico de phishing. Também propomos uma série de práticas recomendadas para que as empresas e seus clientes reduzam o impacto dos futuros ataques de phishing.

2 Estágios dos Ataques de Phishing

Os ataques de phishing possuem diversos estágios:

- O atacante obtém os endereços de e-mail das vítimas. Esses endereços podem ser adivinhados ou obtidos de várias fontes.
- O atacante gera um e-mail que parece legítimo e solicita que o destinatário realize alguma ação.
- O atacante envia um e-mail às suas vítimas de forma que ele pareça legítimo e oculte a verdadeira fonte.
- Dependendo do conteúdo do e-mail, o destinatário abre um anexo mal-intencionado, preenche um formulário ou visita um site.
- O atacante coleta as informações confidenciais da vítima e pode explorá-las no futuro.

O atacante tem várias maneiras de executar esses passos. Também há contramedidas que as vítimas podem utilizar para impedir alguns deles. Os fluxogramas de ataque a seguir mostram os passos que o atacante (e a vítima) precisam realizar para obter um ataque de phishing bem-sucedido. Os fluxogramas também mostram maneiras pelas quais as atuais tecnologias podem ser usadas para reduzir a vulnerabilidade a ataques de phishing.

No diagrama, o estado "início" está no alto. As ações do atacante e da vítima são mostradas como bordas ou linhas entre os retângulos. Cada retângulo contém o recurso ou a condição que o atacante está tentando atingir. O ataque é impedido se ele passar para o estado de "Ataque frustrado". O ataque será bem-sucedido se atingir o estado final "Atacante obtém informações confidenciais do usuário".

Devido ao tamanho e à complexidade do fluxograma, nós a dividimos em quatro seções. A primeira seção mostra os estágios do ataque que são comuns a todos os métodos. Cada um dos métodos de ataque é detalhado no seu próprio diagrama. Esses métodos são os seguintes:

- Instalação de cabalos de Tróia (software mal-intencionado que não se comporta como o destinatário espera).
- Utilização de fraude para convencer o destinatário a seguir algumas instruções.
- Utilização de spyware para interceptar comunicações legítimas entre a vítima e a uma empresa legítima. O spyware é um programa que coleta secretamente informações sobre as atividades do usuário (digitação, sites visitados, etc.), transmitindo essas informações a terceiros.

Como mostra a Figura 1 a seguir, o ataque de phishing começa com o envio de um e-mail às vítimas. O atacante cria o e-mail com o objetivo inicial de fazer o destinatário crer que o e-mail *pode* ser legítimo e deve ser aberto. Os atacantes obtêm endereços de e-mail em diversas fontes, inclusive por geração semi-aleatória, procurando-os em fontes na Internet, e listas de endereços que o usuário acreditava serem confidenciais [CNET]?. A filtragem de spam pode bloquear muitos dos e-mails de phishing. Se as instituições cujos clientes recebam phishing regularmente utilizarem e-mails autenticados (com PGP ou S/MIME, por exemplo), o destinatário poderá perceber que o e-mail não possui uma assinatura válida, bloqueando, assim, o ataque. Assim que o e-mail for aberto pelo usuário, o conteúdo precisará ser suficientemente realista para levar o destinatário a seguir suas instruções.

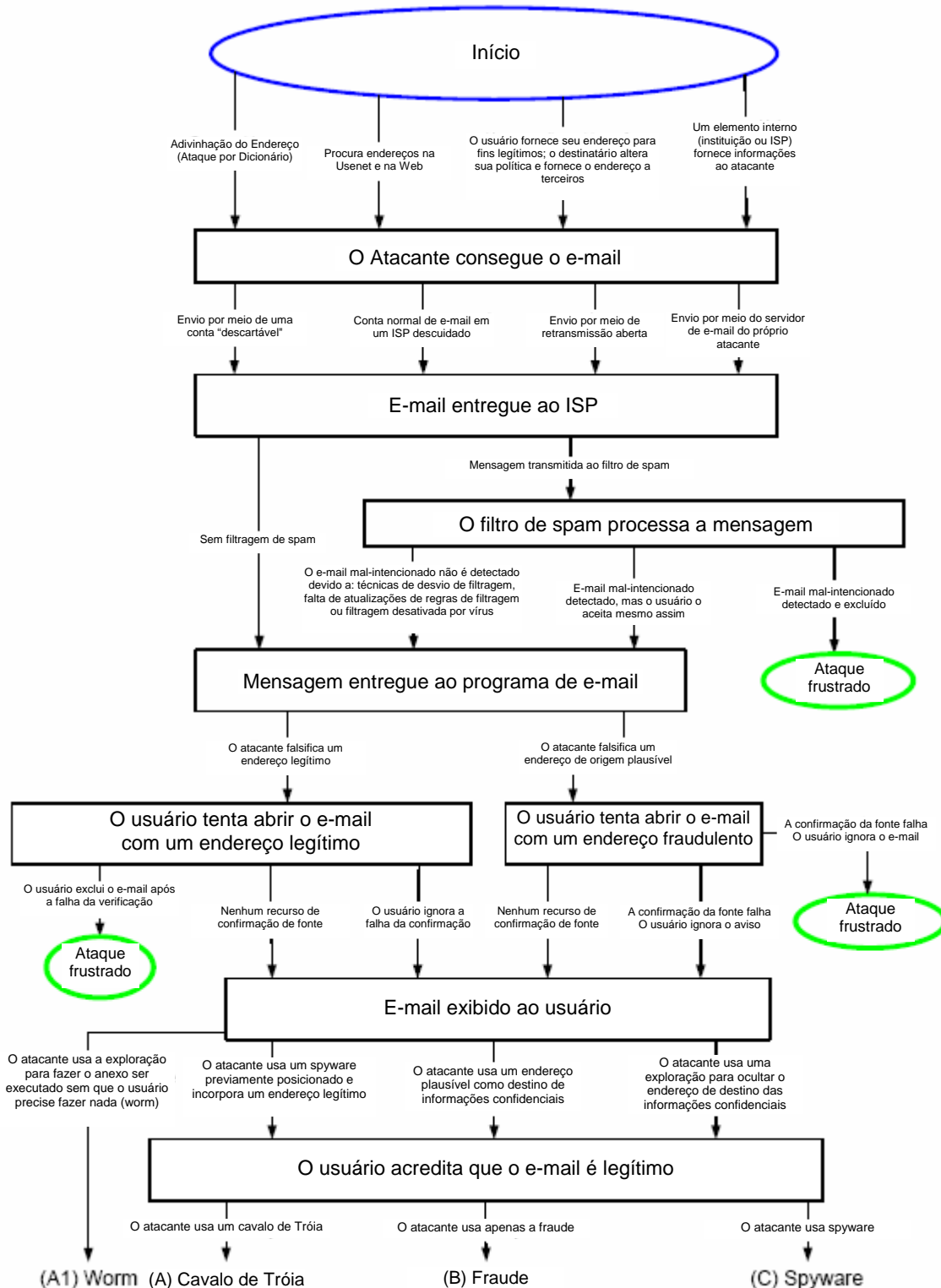


Figura 1 – Métodos Comuns do fluxograma de Ataques

Worms e cavalos de Tróia

Na Figura 2, o atacante continua o ataque, enviando um anexo de e-mail que finge ser bem-intencionado, por exemplo, um cartão virtual ou um protetor de tela. Na realidade, o anexo contém um programa executável que intercepta as comunicações posteriores entre o computador da vítima e uma instituição legítima. O spyware transmite as informações ao atacante pela rede. Softwares antivírus, detecção de invasões baseadas no host e softwares de firewall pessoal podem bloquear muitos ataques nessa situação.

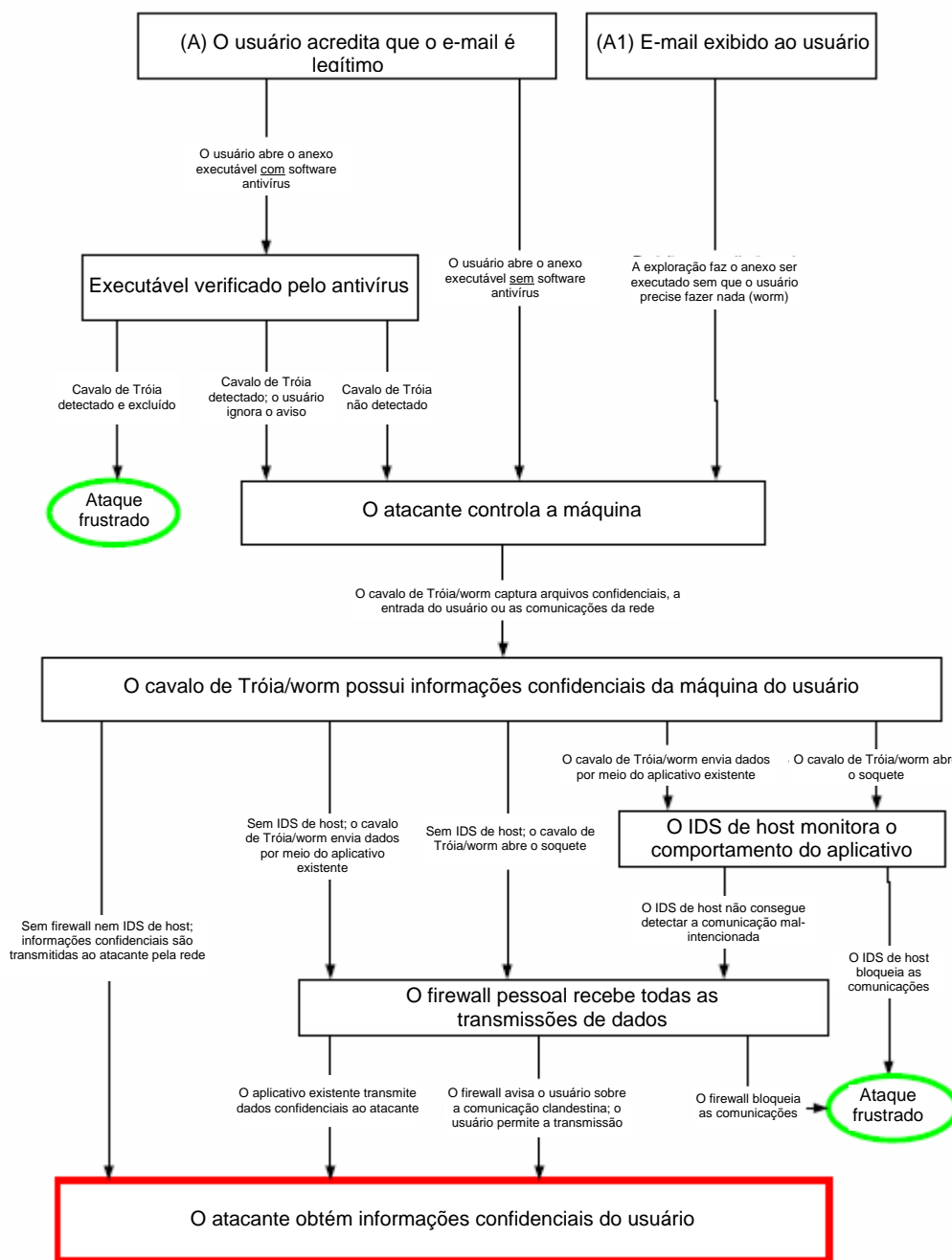


Figura 2 – Ataques com worms e cavalos de Tróia

Spyware

A Figura 4 mostra o atacante utilizando um programa espião previamente posicionado no computador da vítima para extrair informações confidenciais. Isso pode ser realizado por meio de um ataque anterior por worm ou cavalo de Tróia (vide Figura 2) ou de outras maneiras. Muitas vezes, o spyware pode ser detectado por programas especializados em detecção de spyware e por muitos antivírus disponíveis comercialmente. Além disso, os firewalls pessoais e sistemas de detecção de invasões baseadas no host podem, muitas vezes, impedir que o spyware transmita informações confidenciais a terceiros.

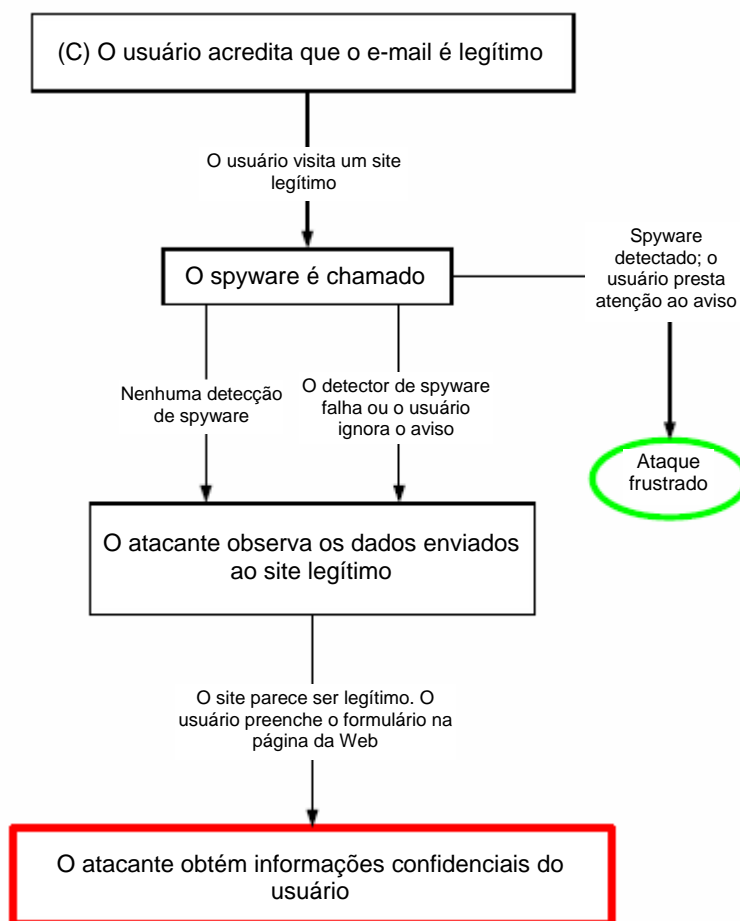


Figura 4 – O atacante usa o spyware para extrair informações

3 Práticas Recomendadas

As “práticas recomendadas” apresentadas a seguir para empresas e consumidores solucionam muitos problemas percebidos na discussão sobre os estágios dos ataques de phishing na Seção 2. Essas soluções se encaixam em duas categorias gerais:

Práticas Recomendadas para Empresas

- Estabeleça políticas corporativas e divulgue-as aos consumidores: Crie políticas corporativas de conteúdo de e-mail para que as mensagens legítimas não possam ser confundidas com phishing. Divulgue essas políticas aos clientes e siga-as.
- Crie uma maneira para que o consumidor confirme se o e-mail é legítimo: O consumidor deve ser capaz de identificar se o e-mail é da instituição, não um phisher. Para isso, a instituição remetente precisa estabelecer uma política para incluir informações de autenticação em *todos* os e-mails enviados por ela aos consumidores.
- Autenticação mais rígida nos sites: Se as instituições não pedem informações confidenciais dos clientes para a entrada em um site (por exemplo, números de CPF ou senhas), fica mais difícil para que os phishers extraiam essas informações do consumidor.
- Monitore a Internet em busca de sites que podem ser de phishing: Geralmente, o site de phishing aparece em algum lugar da Internet antes do envio dos e-mails de phishing. Muitas vezes, esses sites se apropriam indevidamente de marcas comerciais de empresas para parecerem legítimos.
- Implemente soluções antivírus, de filtragem de conteúdo e anti-spam de boa qualidade no gateway de Internet: A varredura antivírus no gateway estabelece uma camada de defesa a mais além da varredura antivírus na própria máquina. Filtre e bloqueie sites de phishing conhecidos no gateway. A filtragem de spam no gateway ajuda os usuários finais a evitar mensagens indesejadas e e-mails de phishing.

Práticas Recomendadas para o Consumidor

- Bloqueie automaticamente e-mails mal-intencionados/fraudulentos: Os detectores de spam podem ajudar a evitar que o consumidor precise abrir e-mails suspeitos, mas eles não são infalíveis.
- Detecte e exclua automaticamente softwares mal-intencionados: Muitas vezes, os spywares fazem parte de um ataque de phishing, mas eles podem ser eliminados por muitos programas disponíveis no mercado.
- Bloqueie automaticamente a saída de informações confidenciais a terceiros mal-intencionados: Mesmo que o consumidor não consiga identificar visualmente o verdadeiro site que receberá as informações confidenciais, existem produtos de software que conseguem.
- Sempre desconfie: Se você não sabe ao certo se um e-mail é legítimo, ligue para a instituição que aparentemente enviou o e-mail de modo a verificar sua autenticidade.

Nenhuma dessas soluções constitui, individualmente, uma resposta completa ao problema.

Recomendamos uma combinação de contramedidas que:

- Reduzirá o número de ataques de phishing enviados aos consumidores;
- Aumentará a probabilidade de que o consumidor reconheça um ataque de phishing e
- Reduzirá as oportunidades de que o consumidor forneça inadvertidamente informações confidenciais.

A conscientização continua sendo crítica para que os consumidores conheçam tanto as técnicas de phishing quanto a maneira pela qual as empresas legítimas se comunicam com eles por e-mail e pela Web.

Algumas das soluções propostas exigem software no computador do consumidor. Se essa solução for adotada, ela será a base para mais soluções com pouco esforço de manutenção extra.

As recomendações abaixo acrescentam detalhes às práticas recomendadas para empresas e consumidores relacionadas acima. Há outras estratégias de longo prazo que exigem a cooperação dos Provedores de Serviços de E-Mail e dos ISPs (Provedores de Serviços de Internet), que também deverão entrar em vigor daqui a algum tempo. Uma dessas estratégias é a abordagem de Chaves de Domínio, recentemente defendida pela Yahoo!™ e a varredura de e-mail no gateway.

3.1 Práticas Recomendadas para as Empresas

3.1.1 Estabeleça Políticas Corporativas Uniformes

3.1.1.1 Evite Hiperlinks Incorporados

Problema

Muitas vezes, os e-mails comerciais legítimos possuem hiperlinks para o site da empresa, os quais solicitam ao consumidor que envie informações confidenciais, como o nome de usuário e a senha. Os phishers aproveitam esses links incorporados para levar os consumidores a revelar essas informações para sites fraudulentos.

Abordagem

Embora a incorporação de hiperlinks em e-mails possa facilitar a navegação do consumidor, ela também cria mais oportunidades de fraude. As vulnerabilidades em algumas versões do Microsoft Internet Explorer podem dar ao phisher a oportunidade de disfarçar o verdadeiro destino de uma URL. Uma alternativa mais segura é incluir no e-mail um link que não possa ser clicado. O consumidor precisará digitar ou cortar e colá-lo no navegador. Muito provavelmente, os clientes regulares terão o link da instituição nos seus favoritos, facilitando ainda mais esse processo.

Essa abordagem funcionará melhor se a política institucional for freqüentemente divulgada aos clientes e se todas as comunicações com os clientes seguirem essa política. A uniformidade é essencial.

Vantagens

- O número de ataques de phishing por meio de URLs enganosas pode ser reduzido.
- Nem a empresa nem o consumidor precisam instalar novos softwares.

Desvantagens

- A navegação do consumidor será negativamente afetada, mas muito pouco.
- Pode ser que alguns grupos e indivíduos da instituição nem sempre sigam a política, levando à falta de uniformidade e à confusão entre os consumidores.
- Pode ser que nem sempre os consumidores se comportem da maneira que melhor atenda aos seus interesses. Eles podem continuar sendo enganados por e-mails fraudulentos com hiperlinks incorporados.
- Os consumidores que recebem e-mails fraudulentos, mas não são clientes da instituição, podem não estar a par da política.

Recomendação

As instituições devem avaliar com cuidado o impacto sobre a praticidade para o consumidor em relação ao aumento da segurança proporcionado pela implementação dessa política. Isso pode ser adequado a muitas instituições.

3.1.1.2 Evite Formulários de E-mail

Problema

Os phishers utilizam formulários de e-mail para coletar informações pessoais dos consumidores. Se a instituição legítima também usar esses formulários, será difícil para o consumidor distinguir entre e-mails legítimos e fraudulentos.

Abordagem

Como ocorre com os hiperlinks incorporados, os formulários de e-mail podem simplificar a navegação do consumidor quando a instituição solicita informações. Entretanto, o mecanismo é facilmente usado pelos phishers a fim de coletar as mesmas informações, dando pouca oportunidade para que o consumidor confirme a fonte do e-mail.

A instituição deve informar os consumidores de que e-mails legítimos nunca conterão formulários solicitando informações pessoais.

Vantagens

- Os ataques de phishing por meio de formulários de e-mail podem ser reduzidos.
- Nem a empresa nem o consumidor precisam instalar novos softwares.

Desvantagens

- A praticidade para o consumidor será ligeiramente afetada.
- Pode ser que alguns grupos e indivíduos da instituição nem sempre sigam a política, levando à falta de uniformidade e à confusão entre os consumidores.
- Pode ser que nem sempre os consumidores se comportem da maneira que melhor atenda aos seus interesses. Eles podem continuar sendo enganados por e-mails fraudulentos com formulários incorporados.
- Os consumidores que recebem e-mails fraudulentos, mas não são clientes da instituição, podem não estar a par da política.

Recomendação

A instituições devem avaliar com cuidado o impacto sobre a praticidade para o consumidor em relação ao aumento da segurança proporcionado pela implementação dessa política. Isso pode ser adequado à maioria das instituições.

3.1.2 Mecanismos de Verificação de E-mail

3.1.2.1 E-mails Assinados Digitalmente

Problema

Os clientes não contam com um meio infalível para verificar a autenticidade de mensagens potencialmente importantes de instituições legítimas.

Abordagem

As instituições devem estabelecer uma política pela qual todas as comunicações de alto valor por e-mail com os clientes sejam assinadas digitalmente com uma chave privada autorizada. Ao receber o e-mail, o destinatário verifica a autenticidade por meio da chave pública da instituição. Há uma probabilidade muito pequena de que um phisher consiga criar uma assinatura válida para um e-mail fraudulento.

PGP e S/MIME são exemplos de tecnologias de assinatura digital, mas muitos usuários acreditam que elas são muito difíceis de usar. Até hoje, essas tecnologias ainda não foram amplamente adotadas.

Vantagens

- As assinaturas digitais são extremamente difíceis de falsificar.
- As mensagens podem ser verificadas automaticamente por leitores de e-mail.
- Elas podem ser usadas como mecanismo de recuperação em um sistema de autenticação múltipla quando os tokens forem perdidos.

Desvantagens

- É pouco provável que o consumidor médio instale e mantenha uma tecnologia de assinatura digital.
- Quem não for cliente da instituição não conhecerá a política da instituição de assinatura em todos os e-mails.

Recomendação

Para um pequeno número de contas de clientes com transações de alto valor, vale a pena considerar essa abordagem.

3.1.2.2 SPF (Estrutura de Política de Remetentes)

Problema

Muitas vezes, os e-mails de phishing falsificam o domínio de envio da instituição visada.

Abordagem

As especificações de SPF que estão sendo desenvolvidas no IETF [SPF] estão tentando definir um mecanismo pelo qual os destinatários possam verificar se um servidor remetente tem autorização para enviar mensagens em nome do domínio de origem. Por si, a SPF não evita todas as formas de spam, pois os remetentes de spam podem registrar domínios descartáveis com registros de SPF para passar nos testes de SPF. Com os e-mails de phishing, isso é mais difícil porque o domínio de envio no e-mail precisa ser plausível para o destinatário humano como um domínio de envio legítimo da instituição visada.

A SPF precisa que os proprietários de domínios legítimos publiquem registros de SPF no DNS (Serviço de Nomes de Domínio). A aplicação do SPF pode ser realizada no MTA (Agente de Transferência de E-mail) de destino, no MDA (Agente de Distribuição de E-mail), ou no MUA (Agente de Usuário de E-mail).

Há problemas com o encaminhamento de mensagens que podem precisar de modificações para legitimar o encaminhamento de e-mails, tais como mudança de encaminhamento para reenvio.

Os usuários finais precisam conhecer o domínio de envio ao inspecionar o e-mail. Se o assunto e o corpo de um e-mail afirmarem ser do banco do destinatário, mas o endereço "De" for absurdo, a SPF não ajudará. Ficará por conta do usuário perceber que há uma discrepância no endereço "De" e no conteúdo da mensagem.

Vantagens

- Obriga os phishers a usar domínios de envio que não são idênticos ao nome do domínio de envio legítimo.
- Não é necessário nenhum software ou hardware a mais para o cliente final se o ISP efetuar a verificação de SPF no MTA.

Desvantagens

- As especificações ainda estão em evolução, mas já começou uma certa adoção.
- Não é totalmente à prova de fraudes, mas eleva o nível de segurança. Os phishers ainda podem criar domínios que parecem ser reais e efetuar registros de SPF desses domínios.
- Se os phishers não imitarem o domínio de envio, a SPF não será eficiente. Os usuários finais precisam verificar se o remetente corresponde ao conteúdo do e-mail.

Recomendação

As instituições devem publicar os registros de SPF dos seus domínios de envio de e-mail. À medida que cada vez mais ISPs e servidores de e-mail começarem a verificar os registros de SPF, a solução passará a ser mais eficiente.

3.1.2.3 Personalização Visual ou Sonora de E-mails

Problema

O cliente médio não conta com um meio simples de verificar a autenticidade das mensagens de instituições legítimas.

Abordagem

Essa abordagem oferece um mecanismo visual ou sonoro para verificar a autenticidade dos e-mails. Assim como ocorre com a atual prática de anexar a fotografia do titular aos cartões de crédito emitidos por bancos, as instituições poderiam incluir uma fotografia do cliente em todas as comunicações eletrônicas. Esse é um método simples e confiável para que o cliente de um banco reconheça mensagens legítimas sem precisar instalar mais nenhum software na sua máquina. Os clientes com deficiência visual utilizariam um objeto de identificação alternativo (talvez uma "imagem sonora" ou uma palavra de acesso) anexado adequadamente.

Observe que a única maneira de esse mecanismo ser bem-sucedido é ele ser acompanhado por uma campanha informativa da instituição para anunciar o novo "Mecanismo Seguro de Comunicação."

Vantagens

- O cliente final não precisa de mais nenhum software ou hardware.
- As mensagens podem ser facilmente verificadas por usuários sem conhecimentos sofisticados.
- O valor dos cartões de crédito "personalizados" já estabelecidos no mercado; pode se associar facilmente com essa mensagem de marketing.

- Reduz a probabilidade de ataques em larga escala, pois os phishers precisam coletar mensagens anteriores da instituição para cada cliente a fim de obter as informações de personalização.
- A abordagem pode ser usada como mecanismo de recuperação em um sistema de autenticação múltipla quando os tokens forem perdidos.

Desvantagens

- Despesas consideráveis de marketing para divulgar a mensagem "Não aceite mensagens que não contenham a sua foto".
- Aumento considerável do custo de geração das mensagens.
- Os clientes precisam comparecer à instituição para que sua foto seja tirada. Talvez isso não seja adequado a empresas virtuais que não contam com instalações físicas. Outros meios, tais como distribuição de senhas ou fotos por correio convencional, podem ser necessários para essas empresas. Entretanto, seria preferível que cada instituição utilizasse fotos exclusivas para que falhas de segurança em uma delas não se multiplicassem em cascata, tornando-se vulnerabilidades para todas.
- As instituições devem proteger rigidamente o banco de dados que contém os dados de autenticação (fotos, clipes de som ou senhas).
- O método não é completamente à prova de fraude, mas eleva o nível de segurança.

Recomendação

Para determinadas instituições, especialmente as que emitem cartões de crédito, essa pode ser uma solução viável se elas já estiverem reunindo imagens digitais para cartões de crédito ou outras finalidades.

3.1.2.4 Numeração Seqüencial de E-mails

Problema

O cliente médio não conta com um meio simples e de custo fixo baixo para verificar a autenticidade das mensagens de instituições legítimas.

Abordagem

Outra variação desse mecanismo é incorporar o equivalente a uma numeração seqüencial a cada e-mail enviado pela instituição. Os números seqüenciais seriam uma forma previsível de autenticação que poderia ser facilmente verificada pelo consumidor. Eis um exemplo de cabeçalho de autenticação:

Data: 16 de janeiro de 2004

Número de série: JJH0017

O último e-mail que enviamos a você foi o JJH0016 em 10 de dezembro de 2003.

O próximo e-mail que enviaremos a você terá o número de série JJH0018.

Observe que a única maneira de esse mecanismo ser bem-sucedido é ele ser acompanhado por uma campanha informativa da instituição para anunciar o novo "Mecanismo Seguro de Comunicação."

Vantagens

- O cliente final não precisa de mais nenhum software ou hardware.
- O valor dos cartões de crédito "personalizados" já estabelecidos no mercado; pode se associar facilmente com essa mensagem de marketing.
- Reduz a probabilidade de ataques em larga escala, pois os golpistas precisam coletar mensagens anteriores da instituição para cada cliente a fim de obter as informações de personalização.
- A abordagem pode ser usada como mecanismo de recuperação em um sistema de autenticação

múltipla quando os tokens forem perdidos.

Desvantagens

- Um pouco mais de dificuldade de confirmação pelo destinatário devido à necessidade de manter o e-mail mais recente.
- Os consumidores podem não validar os números seqüenciais.
- Aumento considerável no custo de geração das mensagens.
- A instituição precisa proteger de maneira rígida o banco de dados que contém os números seqüenciais.
- Não é completamente à prova de fraudes, mas aumenta o nível de segurança.

Recomendação

Se não for possível obter imagens digitais ou informações semelhantes de personalização, essa é a segunda solução mais confiável. Entretanto, também é a mais propensa a falhas para um grande número de consumidores.

3.1.2.5 Incorporação do Nome do Consumidor ao E-mail

Problema

O cliente médio não conta com um meio simples e de custo fixo baixo para verificar a autenticidade das mensagens de instituições legítimas.

Abordagem

A forma mais simples desse mecanismo é simplesmente incorporar o nome do cliente ao e-mail, por exemplo, "Prezado Sr. Jones". Algumas empresas já usam essa técnica. Entretanto, se o endereço de e-mail do consumidor contiver o nome deste, os phishers podem conseguir deduzir uma porcentagem considerável dos nomes. Os phishers não têm nada a perder se suas adivinhações não forem corretas.

Vantagem

- O cliente final não precisa de nenhum outro software ou hardware.
- As mensagens podem ser facilmente verificadas por usuários sem conhecimento sofisticado.
- Reduz a probabilidade de um ataque bem-sucedido em larga escala, pois os phishers precisam coletar ou adivinhar as informações de personalização de muitos consumidores.

Desvantagens

- Nem sempre os consumidores perceberão que o seu nome está faltando no e-mail.
- Gastos consideráveis de marketing para divulgar a mensagem "Não aceite mensagens que não contenham o seu nome".
- As instituições devem proteger de maneira rígida o banco de dados que contém os dados de autenticação (nome do consumidor).
- Não é completamente à prova de fraudes, mas aumenta o nível de segurança.

Recomendação

Essa abordagem deve ser usada por todas as instituições. Se essa for a política predominante em todas as instituições, os consumidores poderão se acostumar a esperar pela presença do seu nome nos e-mails.

3.1.3 Mecanismos de Autenticação Segura

3.1.3.1 Autenticação por Tokens Seguros

Problema

Golpes de engenharia social, tais como o phishing, sempre serão possíveis desde que a vítima saiba todas as informações necessárias para realizar uma transação.

Abordagem

O objetivo final dos ataques de phishing é levar a vítima a divulgar informações confidenciais. Muitas vezes, essas informações são o nome de usuário e a senha usados para acessar um site legítimo. Se os usuários não conhecerem as informações de autenticação, esse tipo de ataque será impossível.

Uma forma de fazer isso é fornecer tokens seguros (físicos) aos usuários e exigir uma seqüência de estímulo-resposta em todas as transações eletrônicas com a instituição. Nesse tipo de sistema de autenticação, o token físico é uma senha descartável válida apenas para a pessoa que possui o token. O token gera uma nova senha descartável a cada login, de forma que não importa se o atacante obtiver o valor. Além disso, o usuário não pode gerar os valores antecipadamente, de forma que ele não tem como divulgar acidentalmente as informações a um atacante.

Esses tokens já têm uso limitado. Algumas empresas exigem que seus funcionários usem esses tokens para acessar computadores remotamente.

Alguns bancos e algumas empresas de cartões de crédito também possuem um recurso semelhante para realizar transações com um smart card [GEMP] [MAST]. Uma alternativa à emissão de novos tokens físicos é integrar a função aos novos cartões de crédito. Entretanto, as soluções de smart card geralmente exigem a conexão de um leitor ao computador. Além disso, foram encontradas vulnerabilidades de segurança em alguns smart cards.

Vantagens

- O usuário não tem como divulgar acidentalmente as informações necessárias para realizar uma transação eletrônica.
- Todas as fraudes precisam de acesso físico ao token.
- O usuário não pode optar por se autenticar de forma a burlar a política de segurança.
- Já existem normas para a implementação desses sistemas. Veja em <http://www.emvco.com>.
- A duplicação do cartão físico exige muito mais sofisticação, mesmo que a vítima forneça o seu PIN.

Desvantagens

- Por si só, os tokens seguros não impedem que o usuário forneça informações que possam ser usadas como intermediárias para que as informações realizem uma transação. Especificamente, as informações usadas para identificar uma pessoa, por exemplo, o nome de solteira da mãe, ainda podem ser obtidas e levar a atividades fraudulentas.
- A emissão de tokens tem um custo, embora esse custo possa variar de acordo com o tipo de equipamento escolhido.
- O usuário pode precisar levar consigo vários tokens, um para cada serviço que assina.
- São necessárias atualizações de software no fabricante para que seja realizada a autenticação estímulo-resposta.
- Há custos consideráveis para a implementação e manutenção da solução, inclusive a atribuição inicial dos tokens e a revogação.

- Inicialmente, os usuários podem rejeitar a inconveniência adicional e os custos repassados a eles.
- Para serem seguras, as soluções de token seguro e smart card exigem ampla engenharia de segurança e atenção aos muitos detalhes correlacionados.

Recomendação

Como ocorre com as assinaturas digitais, esse método pode ser adequado a um pequeno número de clientes com transações de alto valor. Os consumidores e as empresas dos EUA já relutaram em usar tokens anteriormente.

3.1.3.2 Emulação de Tokens Seguros por Software para Autenticação

Problema

Golpes de engenharia social, tais como o phishing, sempre serão possíveis desde que a vítima saiba todas as informações necessárias para realizar uma transação. Os tokens de segurança física podem ajudar, mas a sua implementação pode ser dispendiosa.

Abordagem

A abordagem é muito semelhante à abordagem de Token Seguro, mas sem a necessidade de outros equipamentos. Em vez disso, um aplicativo de software atribuído a um determinado usuário fornece os valores de resposta para a autenticação eletrônica. Executado em um PC, pode ser possível evitar que o usuário precise digitar novamente os valores de estímulo e resposta. Se isso for feito, o site precisará autenticar-se no simulador de Token Seguro para impedir que os usuários sejam levados a se conectar a sites mal-intencionados.

Para usar essa abordagem, as instituições precisam distribuir o software aos consumidores através de CD ou outros meios físicos para evitar novas oportunidades de phishing. O software também precisa ser designado com uma chave específica para cada consumidor.

Uma variante dessa abordagem é desenvolver um software compatível com telefones celulares e PDAs para que os usuários possam levar sua autenticação com eles e usá-la em outros computadores. O usuário precisaria digitar seu PIN e o valor de estímulo no celular ou no PDA, e isso, por sua vez, geraria a resposta. Em seguida, o usuário digitaria o valor de resposta no aplicativo de web para concluir a autenticação.

Vantagens

- O usuário não tem como divulgar as informações necessárias para efetuar uma transação eletrônica.
- Todas as fraudes exigem o conhecimento do valor original no simulador de Token Seguro.
- O usuário não pode optar por se autenticar de forma a burlar a política de segurança.
- Os custos de distribuição de software devem ser muito menores que os custos da distribuição de tokens físicos.

Desvantagens

- Por si só, o método não impede que o usuário forneça informações que possam ser usadas como intermediárias para que as informações realizem uma transação. Especificamente, as informações usadas para identificar uma pessoa, por exemplo, o nome de solteira da mãe, ainda podem ser obtidas e levar a atividades fraudulentas.
- Há o custo de produção dos CDs.
- Há custos consideráveis para a implementação e manutenção da solução, inclusive a distribuição inicial dos CDs e a revogação.

- Às vezes, os usuários podem não possuir o software necessário quando não estiverem no computador de casa. Se o software for executado em um celular ou PDA, o problema pode ser minimizado.
- O simulador de Token Seguro pode ser vulnerável à corrupção, pois utiliza a segurança de um sistema operacional padrão. Se o software for executado em um celular ou PDA, o problema também pode ser aliviado.

Recomendação

Se o custo dos tokens físicos for muito alto, essa solução deverá ser levada em conta. Ela deve ser usada junto com outras tecnologias que impeçam a divulgação não intencional de outras informações confidenciais.

3.1.4 Monitore a Internet em Busca de Sites que Podem Ser de Phishing

3.1.4.1 Monitoramento Ativo da Web

Problema

A Figura 1 mostra que o conteúdo de Web presente em e-mails de phishing é obtido de fontes legítimas, com URLs direcionadas para fontes ilegítimas.

Abordagem

Essa abordagem envolve o desenvolvimento do equivalente aos testes de admissibilidade de "white list" de marcas comerciais e conteúdos-chave. As empresas de serviços de monitoramento implementam soluções que utilizam agentes para monitorar continuamente o conteúdo da Web, procurando ativamente todas as instâncias do logotipo de um cliente, da sua marca comercial ou de seu conteúdo-chave da Web. A instituição cliente fornece à empresa prestadora do serviço de monitoramento uma "white list" de usuários autorizados do logotipo, da marca comercial e do conteúdo-chave. Quando os agentes detectam usuários não-autorizados de logotipos, marcas comerciais ou outros conteúdos da Web, a instituição cliente pode tomar medidas de resolução.

Algumas empresas, tais como a NetCraft [NETC] e a NameProtect, já oferecem serviços de busca de sites potencialmente fraudulentos para clientes. Não está claro se o nível desejado de resposta automatizada está disponível.

Vantagens

- Os proprietários de conteúdo são alertados a respeito de possíveis usuários clandestinos de conteúdo reservado.
- Ordens de "cesse e desista" são geradas como resultado do monitoramento ativo de conteúdo e da identificação de uso inadequado.
- As regras de filtragem de spam podem ser rapidamente atualizadas pelos fornecedores para bloquear e-mails que contenham referências a sites mal-intencionados.

Desvantagens

- Exigência do monitoramento ativo.
- A defasagem entre a identificação e a ação de eliminação de uso pode, ainda assim, resultar em vários roubos de informações particulares.

Recomendação

Essa técnica deve ser levada em conta como parte de um pacote de iniciativas de redução do impacto econômico das ameaças de phishing.

3.1.5 Filtragem no Gateway

3.1.5.1 Varredura Antivírus no Gateway

Problema

Muitas vezes, os ataques de phishing envolvem programas mal-intencionados, entre eles cavalos de Tróia e programas de backdoor que roubam informações confidenciais. O antivírus de desktop é eficiente apenas se o banco de dados de regras for atualizado regularmente.

Abordagem

Com a varredura do tráfego da Web e do e-mail na fronteira da rede (gateway) em busca de programas potencialmente mal-intencionados, as instituições podem evitar que um grande número de códigos mal-intencionados consiga entrar na rede. É muito mais fácil e rápido para uma instituição de grande porte atualizar um número relativamente pequeno de scanners de gateway do que verificar se todos os scanners de desktop estão atualizados. As atualizações automatizadas de varredura de vírus em desktops ajudam, mas elas ainda são um pouco mais lentas do que as atualizações para o gateway. Dada a velocidade com que alguns programas mal-intencionados se propagam, uma hora ou alguns minutos podem fazer toda a diferença.

A varredura antivírus no gateway deve ser combinada com a varredura nos computadores. Uma parte do tráfego criptografado não pode ser submetida à varredura no gateway, devendo ser submetida no computador. Da mesma forma, os usuários móveis nem sempre estão protegidos pelo scanner de gateway quando não estão no escritório.

Vantagens

- Os códigos mal-intencionados podem ser impedidos de entrar na rede.
- A varredura no gateway permite atualizações rápidas de um número relativamente pequeno de nós de varredura.
- Já existem produtos eficientes de vários fabricantes.

Desvantagens

- Uma parte do tráfego de rede não pode passar pela varredura.
- Os usuários móveis não são protegidos pela varredura no gateway.

Recomendação

A varredura antivírus no gateway deve ser combinada com a varredura antivírus no computador como parte de uma estratégia de defesa em camadas contra códigos mal-intencionados.

3.1.5.2 Filtragem de Conteúdo no Gateway

Problema

Normalmente, os ataques de phishing envolvem um site mal-intencionado que, na maioria das vezes, está ativo antes da transmissão do primeiro e-mail de phishing.

Abordagem

Se a instituição tomar conhecimento de um site de phishing, ela deverá bloquear o acesso a esse site pela rede. Isso pode ser feito de várias maneiras, mas principalmente com a implementação de regras de bloqueio das URLs mal-intencionadas no gateway. Trabalhando com um prestador de serviços de monitoramento de rede, as instituições (especialmente os ISPs) podem ser avisadas antecipadamente sobre os sites de phishing e proteger os usuários da sua rede contra o acesso a eles.

Vantagens

- Muito eficiente para bloquear o acesso a sites de phishing conhecidos, sem esperar que o ISP os tire do ar.
- Já existem produtos eficientes de vários fabricantes.

Desvantagens

- Pode exigir a configuração manual de firewalls e outros dispositivos de gateway para implementar as regras de bloqueio.

Recomendação

Se a instituição possuir um firewall ou um gateway adequado, ela deve pensar em bloquear os sites de phishing conhecidos.

3.1.5.3 Filtragem de Spam no Gateway

Problema

Nem sempre os usuários da rede conseguem detectar e-mails fraudulentos que parecem ser provenientes de uma instituição legítima.

Abordagem

Como mostra a Figura 1, a filtragem anti-spam pode bloquear alguns e-mails fraudulentos antes que eles consigam chegar ao usuário. Os e-mails de phishing são uma forma específica de spam. Nessa versão da filtragem de spam, a instituição instala a filtragem no gateway de e-mail. O spam pode ser tratado de várias maneiras, entre elas a marcação (modificação do assunto), a exclusão e a quarentena.

Vantagens

- Os e-mails fraudulentos podem ser bloqueados antes que o usuário tenha a chance de responder a eles, parando o ataque em um estágio inicial.
- Os usuários finais não precisam instalar nenhum software nos seus PCs.
- Já existem produtos eficientes de vários fabricantes.

Desvantagens

- A detecção de spam está melhorando, mas, como os spammers mudam constantemente suas técnicas, nenhuma solução pode ser 100% precisa. Devido a essas imperfeições, os usuários podem optar por ler todos os e-mails suspeitos antes de excluí-los. O usuário precisa aprender a reconhecer os falsos positivos.

Recomendação

A filtragem anti-spam no gateway deve ser implementada em redes de grande porte e em ISPs.

3.2 Práticas Recomendadas para o Consumidor

3.2.1 *Bloqueie Automaticamente E-Mails Mal-Intencionados/Fraudulentos*

3.2.1.1 Filtragem Anti-Spam no Computador

Problema

Nem sempre os consumidores conseguem detectar os e-mails fraudulentos que aparentemente provêm de uma instituição legítima.

Abordagem

Como mostra a Figura 1, a filtragem anti-spam pode bloquear alguns e-mails fraudulentos antes que eles consigam chegar ao consumidor. Os e-mails de phishing são uma forma específica de spam. Nessa versão da filtragem de spam, o consumidor deve instalar um software no computador e configurá-lo.

Vantagens

- Os e-mails fraudulentos podem ser bloqueados antes que o consumidor tenha a chance de responder a eles, parando o ataque em um estágio inicial.
- Já existem produtos eficientes de vários fabricantes.

Desvantagens

- A detecção de spam está melhorando, mas, como os spammers mudam constantemente suas técnicas, nenhuma solução pode ser 100% precisa. Devido a essas imperfeições, os consumidores podem optar por ler todos os e-mails suspeitos antes de excluí-los. O consumidor precisa aprender a reconhecer os falsos positivos.
- As soluções anti-spam para PCs exigem que o consumidor compre, instale e mantenha o software. Devido às grandes variações de capacidade técnica, alguns consumidores podem não implementar a tecnologia de maneira eficaz.

Recomendação

Os consumidores devem pensar em comprar e usar produtos de filtragem de spam. Eles devem aprender a reconhecer os falsos positivos e negativos para não ignorarem as decisões corretas tomadas pelo filtro.

3.2.1.2 Filtragem Anti-Spam no Gateway

Problema

Nem sempre os consumidores conseguem detectar e-mails fraudulentos que parecem ser provenientes de uma instituição legítima e podem não instalar a filtragem anti-spam nos seus PCs.

Abordagem

Como mostra a Figura 1, a filtragem anti-spam pode bloquear alguns e-mails fraudulentos antes que eles consigam chegar ao consumidor. Os e-mails de phishing são uma forma específica de spam. Nessa versão da filtragem de spam, o provedor de serviços de e-mail instala a filtragem anti-spam no gateway de e-mail.

Existem várias maneiras de inserir a filtragem anti-spam no ciclo de processamento de e-mails. Uma abordagem em três camadas pode conter:

- Camada 1: Filtragem no provedor de serviços (ISP ou serviço de e-mail) para todos os clientes

- de e-mail;
- Camada 2: Filtragem em um appliance de rede para todos os usuários na LAN; e
- Camada 3: Filtragem em cada computador por meio de aplicativos de proteção de desktop.

Vantagens

- Os e-mails fraudulentos podem ser bloqueados antes que o usuário tenha a chance de responder a eles, parando o ataque em um estágio inicial.
- Com a filtragem em um provedor de serviços ou em um appliance de rede, o consumidor não precisa instalar nenhum software.
- Se o provedor de serviços excluir mensagens suspeitas de serem spam, o consumidor nunca abrirá nada que tenha sido detectado.
- Já existem produtos eficientes de vários fabricantes.

Desvantagens

- As instituições atacadas não podem controlar se os ISPs dos seus clientes fornecem filtragem de spam no gateway.
- A detecção de spam está melhorando, mas, como os spammers mudam constantemente suas técnicas, nenhuma solução pode ser 100% precisa. Devido a essas imperfeições, os consumidores podem optar por ler todos os e-mails suspeitos antes de excluí-los. O consumidor precisa aprender a reconhecer os falsos positivos.

Recomendação

Muitos ISPs e instituições já fornecem filtragem de spam nos seus gateways de e-mail. Se a sua instituição ainda não oferece, solicite-a.

3.2.2 Detecção e Exclusão de Softwares Mal-Intencionados

3.2.2.1 Software Antivírus e Anti-Spyware

Problema

Os spywares interceptam invisivelmente as comunicações entre o consumidor e as instituições legítimas.

Abordagem

Como mostram as Figuras 2 e 4, o spyware pode ser distribuído aos consumidores por e-mail e, posteriormente, interceptar comunicações legítimas entre os usuários e sites legítimos. Muitos consumidores já instalaram softwares antivírus, que ajudam a reduzir o risco desse tipo de ataque. Os softwares antivírus detectam muitas formas de malwares, inclusive o spyware, podendo excluí-lo quando ele for encontrado. A maioria dos programas antivírus funciona de maneira quase invisível para o consumidor, afetando pouco suas operações normais. Os programas anti-spyware podem efetuar a varredura no computador em busca de possíveis programas espiões, sendo, em geral, capazes de eliminá-los.

Vantagens

- Detecta e exclui o spyware antes que ele consiga interceptar informações confidenciais.
- Há poucos falsos positivos.

Desvantagens

- A detecção é imperfeita, mas está melhorando.
- Os arquivos de “assinaturas” precisam ser atualizados regularmente, caso contrário o software perde a sua eficiência contra os ataques mais recentes.
- Às vezes, o software anti-spyware pode eliminar alguns “programas espiões” necessários ao funcionamento correto de programas legítimos. Normalmente, o consumidor é avisado quando a remoção do spyware tiver essa consequência.
- O consumidor deve comprar e instalar o software, a menos que o fornecedor do computador instale uma versão antes da compra.

Recomendação

Os consumidores devem instalar programas antivírus, com opções ativadas para detectar programas potencialmente indesejáveis. Os consumidores também devem manter seus programas antivírus atualizados. Além disso, devem pensar em instalar um dos aplicativos gratuitos de detecção de spyware. Entretanto, é preciso tomar cuidado para instalar um aplicativo confiável de detecção de spyware, pois alguns têm sido acusados de eles mesmos serem spywares.

3.2.3 Bloqueio Automático do Envio de Informações Confidenciais a Terceiros Mal-Intencionados

3.2.3.1 Serviço de Privacidade de Desktops

Problema

Como mostra a Figura 3, os usuários podem ser levados a enviar dados confidenciais a sites sem segurança e mal-intencionados.

Abordagem

Pacotes de software disponíveis no mercado podem monitorar o tráfego de Web de saída em relação a um conjunto de dados que o usuário pode definir. Normalmente, os dados definidos são informações que identificam o usuário, tais como nome, CPF e números de cartões de crédito. Se qualquer um desses conjuntos de dados for encontrado em um dos pacotes enviados, o pacote é retido até que o usuário confirme se os dados devem ser enviados ao destino verdadeiro, ou se a transmissão dos dados deve ser interrompida. Se o usuário indicar que os dados não devem ser enviados, os dados confidenciais são retirados do pacote.

Uma das dificuldades para os consumidores com esse tipo de produto é identificar as informações confidenciais que devem ser protegidas, além dos sites específicos que devem ser colocados em listas de liberação/bloqueio. Quando as informações são corretamente mantidas, esses produtos podem fazer um trabalho muito eficiente de prevenção contra uma ampla variedade de ataques de phishing.

Vantagens

- Já há produtos disponíveis hoje no mercado.
- Embora a URL de destino possa não ser aparente para o consumidor, o software consegue ver o verdadeiro destino e bloqueia a divulgação indesejada das informações.

Desvantagens

- Exige a instalação de software no computador do consumidor.

Recomendação

Essa abordagem é essencial para bloquear alguns ataques de engenharia social que serão bem-sucedidos apesar da autenticação segura, do antivírus, do anti-spyware e dos softwares anti-spam. Os consumidores já podem instalar esses produtos.

3.2.4 Desconfie Sempre

3.2.4.1 Digite os Endereços da Web e Verifique sua Autenticidade

Problema

Várias explorações podem ocultar o verdadeiro endereço da Web de um link aparente e redirecionar o navegador para um site de phishing.

Abordagem

Há várias maneiras pelas quais um phisher pode fazer um e-mail parecer legítimo. Além disso, pode ser difícil determinar o verdadeiro endereço da Web por trás de links incorporados em e-mails. Geralmente, é mais seguro digitar no navegador o endereço da Web desejado do que clicar em links incorporados. Se você não tem certeza sobre a autenticidade de um e-mail, entre em contato diretamente com a instituição remetente.

Vantagens

- Não é necessário nenhum outro software

Desvantagens

- Endereços de Web longos são chatos de digitar e propensos a erros.
- Pode ser difícil verificar alguns e-mails.

Recomendação

Conheça a política da sua instituição em relação à solicitação de informações pessoais confidenciais. Em caso de dúvida, consulte a instituição por telefone ou por meio de um e-mail para um contato que você já conheça.

4 Conclusão

O phishing difere dos golpes tradicionais na escala da fraude que pode ser cometida. Os golpistas existem há séculos, mas o e-mail e a Rede Mundial deram a eles as ferramentas para chegar a milhares ou milhões de vítimas potenciais em questão de minutos, a um custo praticamente inexistente. Com os ataques de phishing, os golpistas ainda precisam conquistar a confiança do consumidor para terem êxito. Como não há contato pessoal entre o atacante e o consumidor, este conta com muito pouca informação para decidir se um e-mail ou site é legítimo.

A solução técnica definitiva para o phishing envolve mudanças consideráveis na infra-estrutura da Internet cuja implementação está além da capacidade de qualquer instituição. Entretanto, existem medidas que podem ser tomadas imediatamente para reduzir a vulnerabilidade do consumidor a ataques de phishing. Eis algumas delas:

Para Empresas:

- Estabelecer políticas corporativas e divulgá-las aos consumidores.
- Oferecer ao consumidor uma maneira de verificar a legitimidade dos e-mails.
- Autenticação mais segura nos sites.
- Monitorar a Internet em busca de possíveis sites de phishing.
- Implementar soluções antivírus, de filtragem de conteúdo e anti-spam de boa qualidade no gateway de Internet.

Para Consumidores:

- Bloquear automaticamente e-mails fraudulentos/mal-intencionados.
- Detectar e excluir automaticamente softwares mal-intencionados.
- Bloquear automaticamente o envio de informações confidenciais a terceiros mal-intencionados.
- Desconfiar sempre.

Todas essas tecnologias já estão à disposição e podem ser implementadas por consumidores e instituições interessadas em proteger seus clientes.

5 Agradecimentos

Além dos autores mencionados na capa, contribuíram com este white paper os seguintes cientistas e engenheiros da McAfee Research:

Brian Appel
David Carman
Mark Feldman
Michael Heyman
Jim Horning
Roger Knobbe
Patrick LeBlanc
Erik Mettala
Steve Schwab
Deborah Shands

6 Referências Bibliográficas

[APWG] *The Anti-Phishing Working Group*, "Proposed Solutions to Address the Threat of E-mail Spoofing Scams" (Propostas de Soluções para a Ameaça de Golpes de Falsificação de E-mails), dezembro de 2003.

[APJA] *The Anti-phishing Working Group*, "Phishing Attacks Trend Report" (Relatório de Tendências de Ataques de Phishing), janeiro de 2004.

[APAP] *The Anti-Phishing Working Group*, "Phishing Attacks Trend Report" (Relatório de Tendências de Ataques de Phishing), abril de 2004.

[APJU] *The Anti-Phishing Working Group*, "Phishing Attacks Trend Report" (Relatório de Tendências de Ataques de Phishing), junho de 2004.

[ASRG] The Anti-Spam Research Group, <http://asrg.sp.am/index.shtml>.

[CNET] McCullagh, Declan, "Treasury breaks word on e-mail anonymity" (O Tesouro quebra a promessa de manter o anonimato dos e-mails), <http://news.com.com/2100-1028-5137488.html>, CNet News.com, 8 de janeiro de 2004.

[GEMP] *GEMPLUS S.A.*, "Folheto GemAuthenticate", 2003.

[KOPR] *Koprowski, Gene J.*, "Beware of 'Spoofing' Scams" (Cuidado com os Golpes de Falsificação), UPI Technology News, janeiro de 2004.

[MAST] *MasterCard International, Inc.*, "OneSmart Growth Opportunity: Three Business-building Packages for Issuers" (Oportunidades de Crescimento OneSmart: Três Pacotes de Criação de Negócios para Emissores), 2003.

[NETC] *NetCraft Ltd*,

http://news.netcraft.com/archives/2004/01/02/phishing_identity_theft_and_banking_fraud_detection.html, 2004.

[SPF] M. W. Wong, M. Lentzner, "The SPF Record Format and Test Protocol" (O Formato de Registros de SPF e Protocolo de Testes), IETF MADRID Minuta para a Internet, 11 de julho de 2004.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

Os produtos da McAfee® denotam anos de experiência e compromisso com a satisfação do cliente. A equipe McAfee PrimeSupport® de técnicos de suporte colaboradores e altamente qualificados oferece soluções sob medida, oferecendo assistência técnica detalhada para administrar o sucesso de projetos essenciais — tudo isso com níveis de serviço que atendem às necessidades de todas as empresas clientes. A McAfee Research, líder mundial em sistemas de informação e pesquisas de segurança, continua na vanguarda da inovação no desenvolvimento e no refinamento de todas as nossas tecnologias.

McAfee, IntruShield, Protection-in-Depth, Entercept, Intrusion Intelligence, e PrimeSupport são marcas comerciais, registradas ou não, da McAfee, Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. A cor vermelha usada em relação à segurança é marca distintiva dos produtos que levam a marca McAfee®. Todas as outras marcas comerciais, registradas ou não, mencionadas neste documento pertencem exclusivamente aos seus respectivos titulares. © 2004 Networks Associates Technology, Inc. Todos os direitos reservados.