SONICWALL

RESUMO EXECUTIVO: TRÊS COISAS QUE VOCÊ PRECISA SABER SOBRE PHISHING

Entenda o phisher, o phish e os fatos

RESUMO

O phishing ainda é uma ameaça real e tem evoluído de formas perigosas, como para spear phishing e whaling. Antigamente, ele era visto principalmente como um problema do consumidor, mas os ataques de hoje em dia apresentam impacto financeiro e reputacional direto nos negócios. Geralmente, os ataques direcionados são iniciados por meio de campanhas de phishing sofisticadas para obter acesso a credenciais ou para distribuir payloads, como o ransomware. Muitas vezes, as organizações ignoram ou subestimam o phishing ao acreditar que seus filtros de spam por si só podem detectá-lo ou que seus funcionários podem facilmente relatá-lo. Nada disso é verdade. Este documento analisa os desafios enfrentados por uma organização para estar à frente do phishing.

Parta combater o phishing de forma eficiente, há três coisas que devem ser entendidas: o phisher, o phish e os fatos.

O phisher: o alter ego maldoso e superior do spammer

Muitas organizações tratam os phishers como "apenas outro spammer" e, em determinados aspectos, os e-mails de phishing se parecem e funcionam como spam. Eles chegam de forma não solicitada e tendem a requisitar algo do destinatário, como uma compra, uma ação ou a inserção de informações. Mas a semelhança acaba aí.

Enquanto os spammers enviam lixos eletrônicos que normalmente são spams evidentes, os phishers se escondem por trás de um amigo ou parceiro de confiança. Enquanto o spammer busca atenção, o phisher a evita ao se mascarar como fonte confiável e usar seu sistema de e-mail corporativo e seus funcionários contra você.

Ao mesmo tempo que nem o spammer nem o phisher são bem-vindos no seu sistema de e-mail corporativo, o phisher é de longe muito mais ameaçador. Um pouco de spam é irritante, mas é aceitável. Por outro lado, o phishing é totalmente inaceitável. Um único caso bem-sucedido de e-mail phishing direcionado à sua organização pode expor sua rede corporativa, seus dados corporativos, funcionários e clientes à imaginação mal-intencionada e criminosa de todos os hackers e criminosos na Web.Mesmo que seja realizado o patch do problema quase que imediatamente, pode haver tempo suficiente para que o phisher ou (ainda mais provável) seus associados mal-intencionados ativem um ataque de ransomware ou coletem todo um banco de dados de números de cartões de crédito de clientes, o que acabará com a sua reputação.

O phish: phishing, atualizações falsas e fraude em cobranças

Os três tipos mais comuns de e-mails fraudulentos são phishing, atualizações falsas e fraude em cobranças.

Phishing

O phishing tenta fisgar vítimas indefesas aproveitando-se de sua confiança em marcas reconhecidas e fontes confiáveis. Como seus equivalentes em relação ao consumidor, os e-mails de phishing empresariais também aparentam vir de fontes confiáveis, como o gerenciamento da empresa, seu departamento de TI ou um parceiro de negócios. Eles informam ao destinatário que são necessárias informações atualizadas imediatamente para manter uma conta aberta ou um acesso à rede. Geralmente, eles incluem um link para um site falso ou "enganoso". Basta que o funcionário siga as instruções para fornecer involuntariamente dados financeiros confidenciais ou informações de acesso à rede ao phisher. Com sua rede corporativa comprometida, sua única opção

Uma pesquisa da SonicWall mostra que as campanhas de phishing são o vetor preferido para ataques de ransomware.

será revogar e reemitir todos os IDs de segurança, verificar todos os dispositivos quanto a softwares mal-intencionados e rastrear todas as atividades da conta à procura de indícios de atividades não autorizadas.

Atualizações falsas

Outra forma de ataque por e-mail são as atualizações falsas. Entre os tipos mais comuns de atualizações falsas está a atualização de software. Esse é um e-mail fraudulento que informa aos funcionários sobre a disponibilidade de novas versões do software e os direciona a sites falsos. Lá, eles são solicitados a verificar informações da conta a fim de receber a atualização e então fazer o download do código mal-intencionado involuntariamente. Uma vez feito o download do código mal-intencionado, ele poderá atacar de diversas formas. Ele pode desviar dos protocolos de segurança para obter informações empresariais, danificar discos rígidos e deixá-los irrecuperáveis, roubar endereços de e-mail para o envio de e-mails em massa com mensagens mal-intencionadas ou infectar outros usuários por meio de sessões de chat. Para que um funcionário detecte uma atualização falsa, é essencial que haja uma política claramente definida e divulgada sobre "como o sistema é atualizado", de forma que ele nem mesmo confie em e-mails de atualização falsa.

Fraude de cobrança

Os e-mails de cobrança fraudulenta aproveitam o fato de que nenhum processo ou pessoa é perfeita. Todos os dias nos departamentos de contabilidade de todo o mundo, as equipes de contabilidade processam bilhões de dólares em pagamentos de negócios legítimos. Quando uma conta torna-se inadimplente, às vezes um fornecedor envia um aviso por e-mail, que solicita que algum funcionário da contabilidade processe determinado pagamento conforme orientado. Às vezes, para acelerar o pagamento, a equipe de contabilidade pode usar um cartão de crédito corporativo para pagar a fatura on-line. Ao imitar perfeitamente a aparência de um parceiro ou fornecedor de confiança, os phishers usam e-mails de cobrança fraudulentos para obter informações de cartões de crédito, pagamentos ilegais ou ambos. Em casos extremos, os phishers alteram seus processos para o faturamento eletrônico ao redirecionar todos os pagamentos ao phisher, e não a um determinado fornecedor.

Os fatos: as soluções antispam e antivírus sozinhas não interromperão o phishing

As empresas estão plenamente cientes de que as ameaças por e-mail, como spam e vírus, podem diminuir a produtividade, aumentar o risco e fazer disparar os custos com TI.Assim, elas investiram milhões de dólares em proteções antispam e antivírus.

1. **Mito: a melhor maneira de evitar o phishing é interromper os e-mails de phishing, da mesma forma como você interrompe os spams, com seu filtro de spam.**

   Fato: os e-mails de phishing são criados especificamente para imitar e-mails legítimos. Eles são e-mails bem escritos e direcionados aos negócios, enviados de uma fonte aparentemente confiável, exatamente o que os filtros antispam devem permitir na sua organização. Alguns e-mails de phishing enganam tão bem que constantemente passam pelos filtros de spam. Mesmo que seja tentador equiparar os dois, phishing não é spam. O phishing requer análise, identificação e abordagem específicas para que não apresente um impacto negativo à sua organização.

2. **Mito: usar um serviço de bloqueio de URL bloqueará os e-mails de phishing.**

   Fato: um serviço de bloqueio de URL é uma lista de sites de phishing conhecidos. Os links em um e-mail são testados em relação a essa lista e, se houver uma correspondência, o e-mail será considerado um e-mail de phishing. Esse método é bom, mas é lento. Os phishers podem iniciar ataques e coletar as informações desejadas em apenas algumas horas, geralmente antes que a URL seja relatada, verificada e listada na lista de bloqueio de URL. É necessária uma análise do conteúdo para ajudar na identificação de um e-mail de phishing em potencial. Os filtros de spam são treinados para encontrar spam, ou seja, e-mails que pareçam inadequados. É necessário um filtro de phishing que procure por e-mails que aparentem ser adequados, mas que possuam algumas armadilhas sutis, como encobrimento de URL ou remetente falso.

3. **Mito: se a tecnologia de detecção de phishing falhar, os funcionários poderão reconhecer os e-mails de phishing.**

   Fato: não é possível contar com as habilidades dos seus funcionários em distinguir conteúdo legítimo de imitações perfeitas de phishing. De acordo com um relatório, 30% dos e-mails de phishing são abertos e 12% dos anexos são clicados [1].

Conclusão

O phishing não é uma novidade e as empresas lutam contra ele desde o início do e-commerce.Mas assim como as práticas dos negócios evoluem para acompanhar a tecnologia emergente, os phishers também se adaptam às novas oportunidades oferecidas pela tecnologia, como ataques de ransomware. Entretanto, ao entender o phishing como um tipo mais sofisticado e distinto de ameaça por e-mail e ao buscar soluções projetadas especificamente para interromper o e-mail de phishing, você poderá se proteger e proteger a sua organização.

Saiba mais sobre as melhores práticas para interromper ataques de phishing. Leia o nosso resumo de solução, Quatro etapas para uma solução antiphishing eficaz.

[1] *Relatório de investigação de violação de dados da Verizon 2016*

Sobre nós

A SonicWall tem combatido a indústria do crime cibernético por mais de 25 anos, defendendo desde pequenas e médias empresas até grandes corporações mundialmente.A nossa combinação de produtos e parceiros propiciou uma solução de defesa cibernética em tempo real, associada às necessidades específicas de mais de 500.000 empresas globalmente, em mais de 150 países, permitindo que você faça mais em seus negócios com menos preocupações.

Se você tiver dúvidas sobre o possível uso deste material, entre em contato com:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Acesse o nosso site para obter mais informações.
www.sonicwall.com