

RESUMO EXECUTIVO

Você tem scam: Por que e-mail é o seu vetor primário de ameaça

Hoje em dia, as maiores violações começam com um simples e-mail

Resumo

Phishing não significa somente você clicar em um link para um malware se iniciar. O mais insidioso é o roubo das credenciais de usuários experientes. Isso permite aos criminosos ganhar acesso, enviar e-mails, fazer pedidos financeiros e espalhar códigos maliciosos por todos os lugares onde a identidade do usuário está autorizada.

E-mail continua a ser um vetor primário de ameaça. As organizações têm que estar atentas quanto a proteger os funcionários contra ataques phishing e de malware avançados que se iniciam como, comprometimento do e-mail corporativo (BEC), falsificação de identidade em e-mail e fraude.

Introdução

As pessoas enviam quase que 320 bilhões de e-mails em um único dia. E-mail continua a ser um meio básico para as pessoas compartilharem informações – e ameaças. COVID-19 e o trabalho em casa contribuíram para o e-mail se tornar o canal mais abrangente para todas as formas de ataques de phishing e de ransomware.

Como aprendemos nas últimas grandes violações de dados, esses ataques avançados geralmente misturam múltiplos ataques, técnicas e procedimentos para comprometer o usuário. Normalmente, o e-mail é o ponto inicial para ataques de engenharia social, tais como BEC ou ataques para coletar credenciais.

Por exemplo, o relatório 2020 Verizon Data Breach Report afirma que 22% das violações envolveram engenharia social e 96% desses vêm por e-mail. No mesmo relatório, outros 22% de violações foram resultados de falha humana, quando dados sensíveis foram enviados acidentalmente ao destinatário errado.

Outro estudo do 451 Research mostra que, enquanto 87% das organizações já usam um produto de segurança em e-mail, 46% admitem que o e-mail ainda é o risco de dados mais significante. Assim, 46% citaram o e-mail como a maior vulnerabilidade, quase cinco vezes mais acima de suas próximas grandes preocupações.

Microsoft e Google dominam o mercado global de e-mail baseado na nuvem, como um elemento de suas maiores ofertas de office suite. A participação no mercado mundial de tecnologias de office suite está dividida entre Google e Microsoft. Mundialmente, Gmail é a plataforma de e-mail mais popular, com mais de 1,8 bilhões de usuários. No final de 2020, Microsoft Office 365 era usado por mais de um milhão de empresas em todo o mundo, com mais de 650.000 somente nos EUA.

Atraídos por essa imensa quantia de vítimas em potencial, os criminosos investem constantemente nos usuários novos destes serviços de e-mail baseados na nuvem. Isso faz com que o e-mail baseado na nuvem seja um dos vetores de ataque mais desejáveis e lucrativos para hackers oportunistas.



A eficiência persistente de phishing e fraude de e-mail

Os e-mails de phishing, elaborados para parecerem verdadeiros, são enviados de identidades roubadas, fakes ou identidades conhecidas roubadas e conseguem enganar até mesmo os usuários mais treinados e conscientes sobre a segurança. Apesar dos esforços de educação sobre segurança, os ataques de phishing ainda são muito citados como um elo fraco na segurança. Os líderes de segurança com quem conversamos ainda vêm usuários clicando em temas específicos e em e-mails de phishing baseados em eventos, personalizados de tal forma que parecem verdadeiros. Muitos são incapazes de diferenciar os e-mails

verdadeiros dos falsos, reconhecer links suspeitos ou tomar medidas cautelares, tais como autentificar a URL, a identidade do remetente e o site da empresa.

Além disso, a divulgação simplesmente faz parte da natureza humana. E-mails e anexos enviados entre funcionários, parceiros, clientes – sem mencionar família e amigos – prevalecem na força de trabalho colaborativa e remota de hoje em dia. Nós os aceitamos, porque são identidades confiáveis e porque precisamos ter acesso a contexto e informações para continuarmos com nosso trabalho coletivo.

Comprometimento de E-Mail Corporativo

BEC está no topo da lista para falsificação de identidade e fraude. Esse tipo de ataque envolve normalmente uma conta de e-mail comprometida em nível de CEO e de outros níveis executivos. Scammers usam a conta comprometida para enviar pedidos financeiros fraudulentos, tais como o pagamento de uma fatura falsa ou a transferência de dinheiro para fechar um negócio fictício.

Na maioria dos casos, os ataques de engenharia social ou de coleta de credenciais estão atrás de sequestrar contas de executivos de alto nível para realizar tais ataques. O O centro de queixas contra crimes na internet do FBI (IC3) relata que, em 2020, os crimes cibernéticos superaram $4,1 bilhões, com BEC de 1,8 bilhões e causaram o maior dano financeiro como um único vetor de ameaça.

Já é tarde demais quando você percebe que as credenciais de um executivo foram comprometidas. Uma única conta comprometida já cria uma reação viral no esquema usuário para usuário, dispositivo para dispositivo e aplicativo para aplicativo, que é praticamente impossível de ser contida antes de acontecerem danos.

Segurança nativa na nuvem não é o suficiente

Os desenvolvedores de segurança em e-mail criaram meios para proteger usuários de links maliciosos que contornam filtros de pré-envio e chegam à caixa de entrada, tais como proteção click-time, retração pós-entrega e filtros web-browser. No entanto, os atacantes também se dedicam a criar meios de alcançar a caixa de entrada.

O relatório recente 2020 Microsoft ATP mostrou que mais de um em dez e-mails de phishing direcionados consegue chegar à caixa de entrada do usuário. Cada ataque único se beneficia de várias combinações de métodos de ofuscação criados especificamente para contornar o Microsoft's Exchange Online Protection (EOP) e a Advanced Threat Protection (ATP).

Alguns dos ataques mais comuns transmitidos por e-mail contornam os filtros de segurança em e-mail com alto grau de sucesso. Um exemplo desses ataques é um e-mail de phishing direcionado de alta qualidade que parece vir do Office 365 ou Gmail. Ele transmite bem, personaliza e costuma ser mais enviado a um grupo especifico de usuários do que por uma campanha tradicional de grande volume. Esses ataques são sofisticados tanto em sua técnica de chegar à caixa de entrada quanto à experiência de usuário no backend. Normalmente, cada link inclui o endereço de e-mail do usuário, de modo que a página de login se parece com a segunda página do desafio da conta, quando se tenta ir a uma página de administrador quando faz o login. Ele sabe quem você é e fornece análise pelo lado posterior.

A curva de inovação de phishing acontece então na pós-entrega. Isso signfica que, em vez de colocar URL maliciosa no e-mail, phishers se conectam a um servidor de redirecionamento que age como um gateway e envia consultas de uma empresa de segurança a um site begnigno. Por outro lado, as consultas das vítimas são direcionadas ao server de phishing.

Apesar da Microsoft ATP aplicar quatro motores para políticas principais contra antiphishing, spoof intelligence, Safe Links e Safe Attachments, ainda assim é uma tecnologia de segurança baseada em regras. A varredura de segurança confia somente na filtragem estática baseada na reputação, e os hackers podem fazer engenharia reversa até encontrar meios de contornar esses filtros. A fraqueza na camada de segurança deixa as empresas em constante estado de risco, ameaçadas pela probabilidade de alguém em sua organização abrir o arquivo errado, clicar em uma URL maliciosa ou colocar a senha no lugar errado.

A visibilidade e o acesso à grande população de usuários de e-mails na nuvem os tornam alvos fáceis para os hackers. Eles nunca tiveram tanto acesso a tantas contas de usuários e caixas e-mail com segurança idêntica. Hackers também sabem que essas contas na nuvem são fontes de autenticação para outros aplicativos SaaS da empresa e podem espalhar malware ou roubar dados. Esse é o perigo real e presente da monocultura da segurança em nuvem. Aquilo que contorna um, contorna todos.

SiteCloak é um bom exemplo de tal técnica, usada atualmente para contornar Microsoft 365 ATP Safe Links, a também conhecida como proteção click-time. Ela leva a ofuscação de phishing ao próximo nível, usando várias táticas e técnicas para esconder a verdadeira intenção da página visada, que normalmente é uma página de coletar credenciais.

Vítimas do SiteCloak não precisam entrar seus endereços de e-mail. Eles são capturados diretamente na página de entrada de senha, onde a página de coletar credenciais usa a técnica "Zero Font" para contornar os scanners de e-mail da Microsoft. Ela coloca caracteres aleatórios com fonte de tamanho zero entre caracteres na página, de modo que os filtros de linguagem natural da Microsoft vejam o texto aleatório, enquanto os leitores humanos vêm o que os atacantes querem que vejam. Em outras palavras, Safe Links pensa que é uma página benigna, mas para a vítima é uma página de coletar credenciais de aparência realista. Atacantes acionam o conteúdo malicioso somente depois que a mensagem chegou à caixa de entrada.

Conclusão

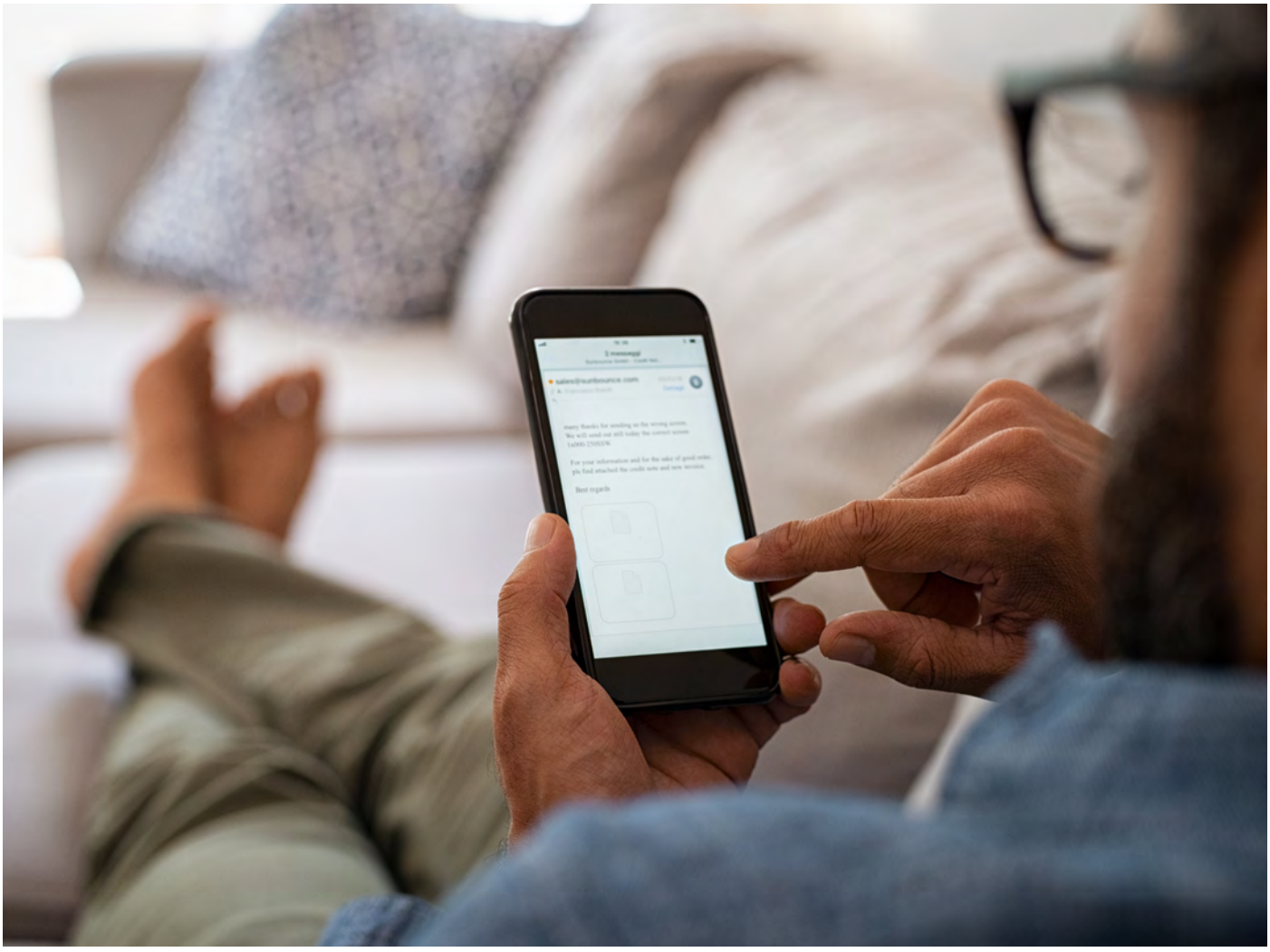
SiteCloak e outras formas de fraude de e-mails são o exemplo de que os hackers podem escapar da detecção ao usar ataques de phishing personalizados altamente preparados e bem desenvolvidos. Esses não serão os últimos que escapam pelos filtros de segurança em nuvem dos fornecedores. Empresas precisam de níveis adicionais de proteção além daqueles que a segurança integrada no sistema de escritório na nuvem oferece.

SonicWall Email Security pode ser implementada como uma appliance virtual forte, aplicação de software, serviço hospedeiro ou appliance física reforçada — ideal para organizações que precisam de uma solução local eficiente. A solução multicamadas da SonicWall oferece proteção de entrada e de saída abrangente. Ela defende contra ameaças avançadas transmitidas por e-mail, tais como ransomware, ameaças zero-day, spear phishing e comprometimento de e-mail corporativo (BEC).

Aprenda mais em www.sonicwall.com/email-security.

Sobre SonicWall

A SonicWall fornece o modelo Boundless Cybersecurity na era da computação hiper distribuída e uma realidade de trabalho onde todos estão remotos, móveis e inseguros. Ao revelar ameaças ainda desconhecidas, fornecendo visibilidade em tempo real a SonicWall possibilita a contínua inovação da economia. SonicWall resolve as falhas na segurança cibernética para empresas, governos e SMBs em nível mundial. Para obter mais informações, visite www.sonicwall.com.



SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Faça referência ao nosso website para informação adicional.
www.sonicwall.com

© 2021 SonicWall Inc. TODOS OS DIREITOS RESERVADOS.

SonicWall é uma marca ou marca registrada da SonicWALL Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. Todas as marcas e marcas registradas são propriedade de seus respectivos proprietários. As informações neste documento são fornecidas em conexão com SonicWall Inc e/ou produtos de suas afiliadas. Nenhuma licença, explícita ou implícita, por preclusão ou de outra forma, a nenhum direito da propriedade intelectual é garantido por este documento ou em conexão com as vendas de produtos SonicWall. EXCETO O ESTABELECIDO NOS TERMOS E CONDIÇÕES ESPECIFICADOS NO CONTRATO DE LICENÇA PARA ESTE PRODUTO, SONICWALL E/OU SUAS AFILIADAS NÃO ASSUMEM QUALQUER RESPONSABILIDADE E EXIMEM-SE DE TODA GARANTIA, EXPRESSA, IMPLÍCITA OU JURÍDICA RELACIONADA A SEUS PRODUTOS, INCLUINDO, MAS NÃO LIMITANDO A GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UMA DETERMINADA FINALIDADE OU NÃO VIOLAÇÃO. EM NENHUMA CIRCUNSTÂNCIA A SONICWALL E/OU SUAS AFILIADAS SERÃO RESPONSÁVEIS POR PERDAS E DANOS, MULTA COMPENSATÓRIA, DANOS EMERGENTES OU IMPREVISTOS (ENTRE ELES, DANOS POR LUCROS CESSANTES, INTERRUPÇÃO DE NEGÓCIOS OU PERDA DE INFORMAÇÕES) DECORRENTES DO USO OU DA IMPOSSIBILIDADE DE USO DESTE DOCUMENTO, MESMO QUE A SONICWALL E/OU SUAS AFILIADAS TENHAM SIDO INFORMADAS SOBRE A POSSIBILIDADE DE TAIS DANOS. A SonicWall e/ou suas afiliadas não fazem declarações ou garantias quanto à exatidão ou à integridade do conteúdo deste documento e reservam-se o direito de fazer alterações às especificações e descrições de produtos a qualquer momento sem notificação prévia. A SonicWall Inc. e/ou suas afiliadas não assumem nenhum compromisso de atualizar as informações contidas neste documento.

ExecBrief-EmailThreatVector-A4-COG-5264