E-mail: cuidado ao clicar

Como se proteger contra phishing, fraude e outros scams

CISCO

Conteúdo

Introdução

No ano passado, o spam fez 40 anos. Sim, em 1978, Gary Thuerk, gerente de marketing da Digital Equipment Corporation, enviou a primeira mensagem de spam para 393 pessoas na ARPANET original para comercializar um novo produto. Não é surpresa que essa mensagem conseguiu ser disseminada da mesma forma que o spam atual. A Thuerk recebeu uma reprimenda rígida e foi orientado a não fazer isso novamente.

Se ao menos fosse tão simples hoje em dia. Quarenta anos depois, o spam cresceu exponencialmente em prevalência, inundando nossas caixas de entrada com ofertas indesejadas de produtos farmacêuticos, dietas e oportunidades de emprego. Não apenas ele, mas também seus primos muito mais perigosos, o phishing e o malware. O phishing surgiu pela primeira vez há mais de 30 anos, e o malware também tem um histórico de décadas de distribuição em e-mail.

Hoje, o fato triste é que muitos e-mails são compostos por spam indesejado ou pior. O volume é impressionante – 85% de todos os e-mails em abril de 2019 foram spam, de acordo com a Talos Intelligence. O volume de e-mails indesejados também está aumentando; o spam atingiu a marca de 15 meses em ascensão em abril.

Remetente vs. destinatário

Você pode argumentar que o e-mail está estruturado em um formato quase ideal para scammers. O e-mail obriga o usuário a ler e fazer avaliações sobre o que eles recebem e, em seguida, tomar decisões sobre o que eles abrem ou clicam como resultado. Apenas a quantidade certa de engenharia social, explorando a boa natureza do indivíduo, pode motivar o usuário a agir.

É essa engenharia social que não apenas a torna um vetor de entrega atraente mas também desafiadora a ser sistematicamente defendida. Raramente, se for o caso, um ataque por e-mail será ignorado pelo usuário. Enquanto as URLs que levam a sites comprometidos ou mal-intencionados com kits de exploração são comuns, elas ainda dependem do usuário clicar primeiro em um link de e-mail.

O que isso significa para a empresa

Não é surpresa que o e-mail seja um dos principais desafios que preocupam os CISOs. Em nosso mais recente Estudo comparativo de CISO, aprendemos que 56% dos CISOs entrevistados achavam que a defesa contra os comportamentos do usuário, como clicar em um link mal-intencionado em um e-mail, é muito ou extremamente desafiadora. Isso é mais preocupante do que qualquer outro problema de segurança pesquisada – mais do que os dados na nuvem pública e do que o uso de dispositivos móveis.

Além disso, a frequência de tais tentativas de ataque que chamam a atenção dos CISOs. Por exemplo, 42% dos CISOs entrevistados lidaram com um incidente de segurança que se manifestou porque um e-mail de spam mal-intencionado foi aberto na empresa. E 36% lidaram com um incidente semelhante como resultado de detalhes roubados em um ataque de phishing. De acordo com nossos dados comparativos de CISO, os CISOs consideram que as ameaças de e-mail sejam o principal risco de segurança para as empresas.

Em um estudo separado, encomendado pela Cisco e realizado pelo ESG em 2018, 70% dos entrevistados relataram que a proteção contra ameaças de e-mail está ficando cada vez mais difícil. Em termos das consequências dos ataques por e-mail, 75% dos entrevistados disseram que sofreram impactos operacionais significativos e 47% relataram grandes impactos financeiros.

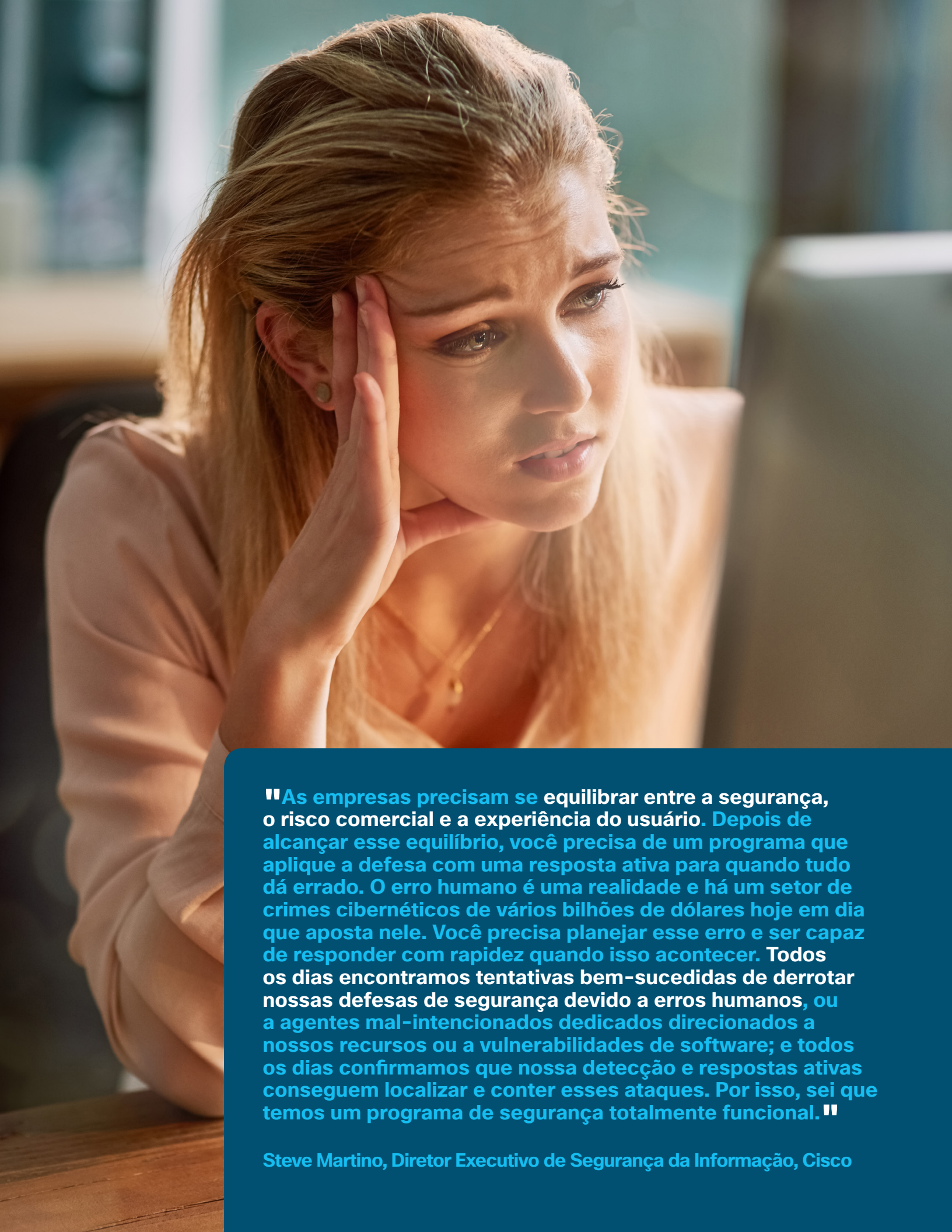
Resposta necessária

Como você protege algo que é uma necessidade e um risco ao mesmo tempo? Para muitas empresas, a mudança para a nuvem tem sido vista como uma solução. No entanto, a nuvem não é uma proteção definitiva contra os perigos do e-mail. Na maioria dos casos, é simplesmente adiar a solução do problema. Os problemas de segurança persistem, não desaparecem.

Há várias maneiras de minimizar o impacto geral das ameaças de e-mail. Neste documento, discutiremos o cenário de ameaças atual, fornecendo uma visão geral dos tipos de ataques de e-mail mais comuns de hoje. Vamos compartilhar como eles agem, os objetivos e a infraestrutura por trás deles. Vamos discutir o que você pode fazer para manter sua empresa segura, bem como identificar ameaças transmitidas por e-mail quando os usuários a encontrarem.

"Em um dia normal, recebemos cerca de 412.000 mensagens de e-mail, das quais 266.000 nem chegam aos nossos mecanismos de SMTP porque o Talos as bloqueia com base em sua inteligência global de ameaças."

Milind Samant, Diretor de Segurança, SUNY Old Westbury



"As empresas precisam se equilibrar entre a segurança, o risco comercial e a experiência do usuário. Depois de alcançar esse equilíbrio, você precisa de um programa que aplique a defesa com uma resposta ativa para quando tudo dá errado. O erro humano é uma realidade e há um setor de crimes cibernéticos de vários bilhões de dólares hoje em dia que aposta nele. Você precisa planejar esse erro e ser capaz de responder com rapidez quando isso acontecer. Todos os dias encontramos tentativas bem-sucedidas de derrotar nossas defesas de segurança devido a erros humanos, ou a agentes mal-intencionados dedicados direcionados a nossos recursos ou a vulnerabilidades de software; e todos os dias confirmamos que nossa detecção e respostas ativas conseguem localizar e conter esses ataques. Por isso, sei que temos um programa de segurança totalmente funcional."

Steve Martino, Diretor Executivo de Segurança da Informação, Cisco

O cenário de e-mail e phishing atual

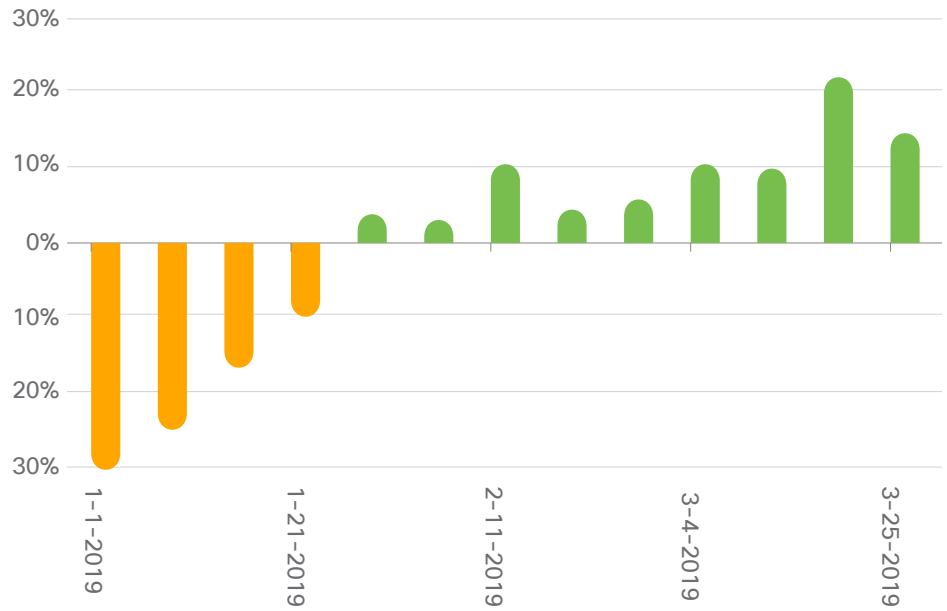
Os perigos apresentados através de e-mail são numerosos. De acordo com o Relatório sobre investigações de violações de dados da Verizon, de 2018, que conta com a colaboração da Cisco, o e-mail é o principal vetor para distribuição de malware (92,4%) e phishing (96%). Siga o que está no e-mail errado e você poderá servítima de cryptomining, ter suas credenciais roubadas ou, se você cair no golpe de engenharia social errado, perder grandes somas de dinheiro. Escale isso para o nível empresarial, e o e-mail errado pode causar estragos.

Com que frequência os usuários caem em scams de e-mail? Basta perguntar ao pessoal da Duo Security. A equipe criou a ferramenta Duo Insight gratuita há alguns anos, o que permite que os usuários criem as próprias campanhas falsas de phishing e as testem nas próprias empresas para ver quem é ou não enganado por elas.

Infelizmente, muitas pessoas caem nos golpes. De acordo com o Relatório de acesso confiável da Duo de 2018, 62% das campanhas de simulação de phishing executadas capturaram pelo menos um conjunto de credenciais de usuário. De todos os destinatários, quase um quarto deles clicouno link de phishing no e-mail. E metade dessas credenciais entraram no site falso.

Com esse nível de sucesso, não é de admirar que o e-mail seja uma escolha tão popular para lançar campanhas de phishing. Na verdade, parece que a atividade de phishing pode estar aumentando, se nos Fizemos uma média semanal para o primeiro trimestre de 2019 e, em seguida, comparamos cada semana com essa média. Os resultados na Figura 1 mostram que, embora o ano tenha começado lento, o número de novos domínios que estão sendo produzidos acelerou, com um aumento de 64% na primeira semana do trimestre até o último.

Figura 1 Novos domínios de phishing semanais em comparação com a média semanal do primeiro trimestre.



Fonte: Cisco Umbrella

Tipos de ataques de e-mail comuns

A seguir, há uma lista dos scams atuais baseados em e-mail. Pegue seu laptop, abra a caixa de entrada e imagine que as seguintes mensagens não lidas estejam esperando por você.

Phishing no Office 365

O e-mail parece vir da Microsoft. Ele diz que o endereço de e-mail do Office 365 será desativado devido a erros ou violações de políticas. A única forma de evitar que isso ocorra é verificando o endereço no link fornecido.

Esta é uma tentativa de phishing das suas credenciais do Office 365. Os e-mails e as URLs usados podem até se parecer com algo que você esperaria encontrar no Office 365, por exemplo: micros0ftsupport@hotmail.com. Se você clicar no link, ele o levará para uma página de logon de aparência oficial, solicitando o endereço de e-mail e senha.

No entanto, o site é falso. Assim que os fraudadores tiverem suas credenciais, eles poderão tentar fazer logon em outros serviços relacionados à Microsoft, além de coletar seus contatos. Uma técnica comum é entrar na sua conta de e-mail e enviar aos seus contatos um e-mail informal (por exemplo, assunto: FYI) que inclui outra URL de phishing.

Esse estilo de ataque está aumentando. De acordo com dados publicados por nossos parceiros da Agari em seu relatório do segundo de trimestre de 2019, Tendências de roubo e identidades e fraude de e-mail, 27% dos ataques de e-mail avançados se originam de contas de e-mail comprometidas. Isso aumentou sete pontos percentuais em relação ao último trimestre de 2018, quando 20% dos ataques de phishing vieram do e-mail comprometido.

Não é apenas o Office 365 que está sendo alvo. Ataques de phishing semelhantes foram observados em outros serviços de e-mail na nuvem, como o Gmail e o G Suite, a oferta de e-mail na nuvem do Google. Devido à prevalência de contas do Google e como eles são utilizado na Internet para entrar em vários sites, não é nenhuma surpresa que os invasores tenham criado sites de phishing nesses locais também.

Ataques de phishing semelhantes foram observadosem outros serviços de e-mail em nuvem , como o Gmail e o G Suite.

Figura 2 Site de phishing deliberadamente projetado para parecer com a página de logon da Microsoft.

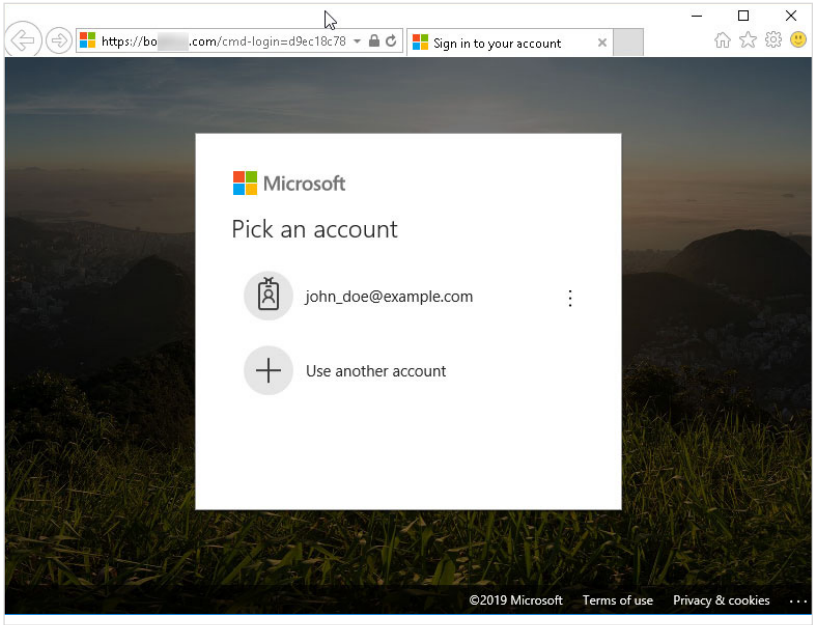
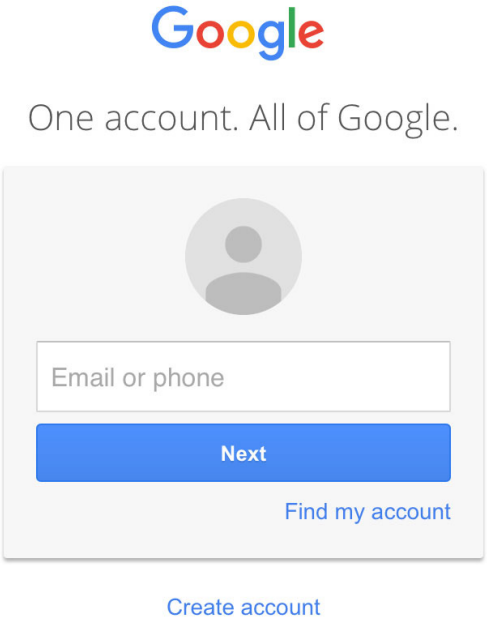


Figura 3 Exemplo de logon na conta do Google. Você pode diferenciar entre o real e o falso?



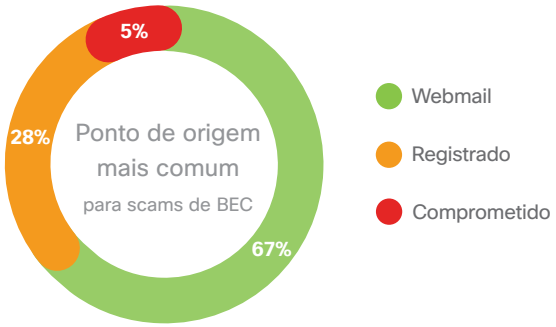
Comprometimento do e-mail empresarial

É a semana do grande encontro da empresa e todos estão fora do escritório, exceto por um pequeno número de pessoas que têm funções essenciais. Você é membro da equipe de finanças e parte da equipe estrutural ainda está no local. De repente, um e-mail chega à caixa de entrada que parece vir do CFO com o assunto " falta de pagamento". O e-mail explica que um pagamento que deveria sair na semana passada foi ignorado e pode resultar em uma quebra na cadeia de suprimentos da empresa. As instruções de transferência bancária estão em anexo. O remetente termina dizendo que ligarão em uma hora para falar sobre isso.

Este é o puro comprometimento do e-mail empresarial (BEC). Os scams de BEC são uma forma de fraude de e-mail em que o invasor se mascara como um executivo de nível C ou superior e tenta induzir o destinatário a executar sua função comercial, para uma finalidade ilegítima, como transferência de dinheiro. Às vezes, ele chega até a ligar para o indivíduo e se passar pelo executivo. E parece que funciona. De acordo com o Internet Crime Complaint Center (IC3), houve US$ 1,03 bilhão em perdas em 2018 devido a scams de BEC.

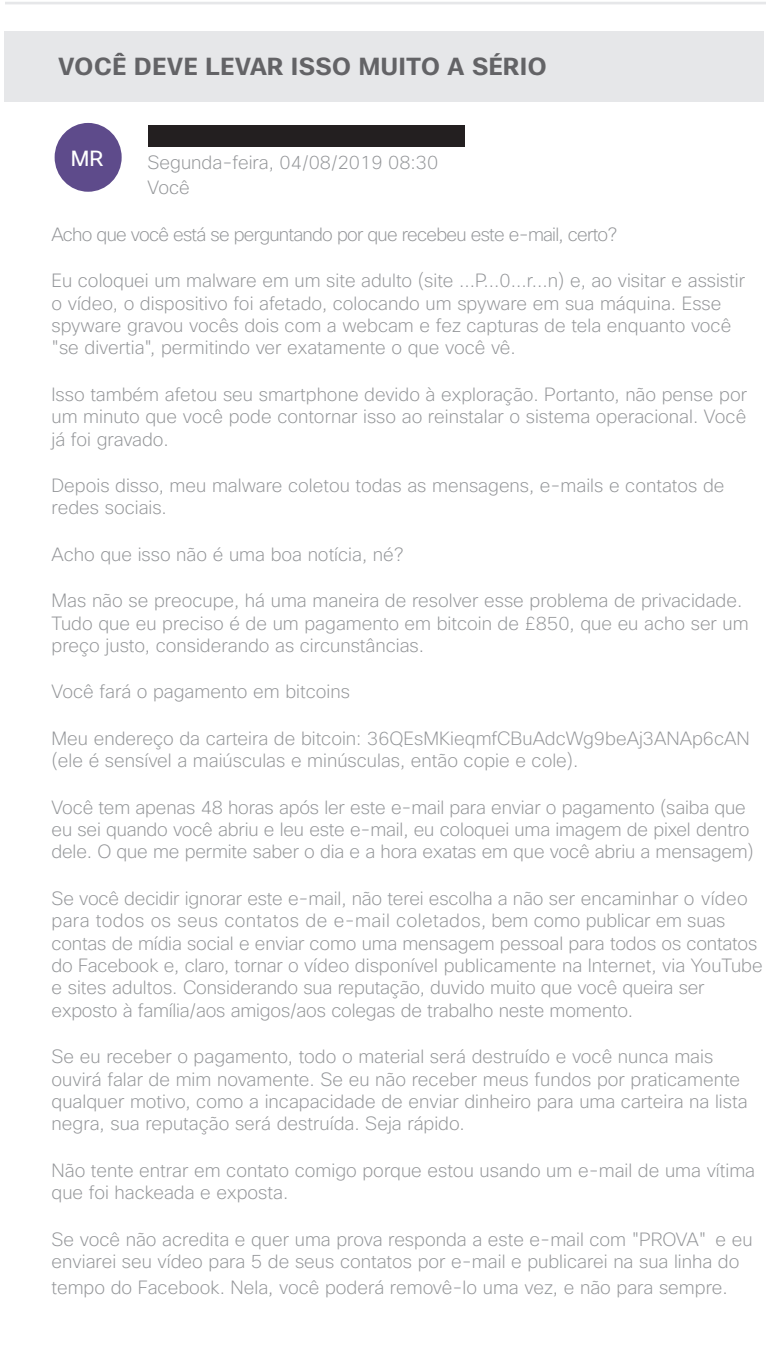
Você acha que os invasores usariam contas comprometidas em scams de BEC, como fazem com scams de phishing do Office 365. Surpreendentemente, de acordo com o relatório de Tendências de engano e fraude de identidade no segundo trimestre de 2019 da Agari, apenas cerca de cinco por cento desses scams fazem isso. Dois terços de tais ataques ainda usam contas de webmail gratuitas para lançar os ataques, enquanto os 28 por cento restantes criam ataques personalizados usando domínios registrados. O último nível de personalização se estende ao corpo do e-mail, onde de acordo com a Agari, um em cada cinco e-mails de BEC inclui o nome do destinatário-alvo.

Figura 4 Ponto de origem do e-mail do BEC.



Fonte: Agari Data, Inc.

Figura 5 Um exemplo recente de extorsão digital.



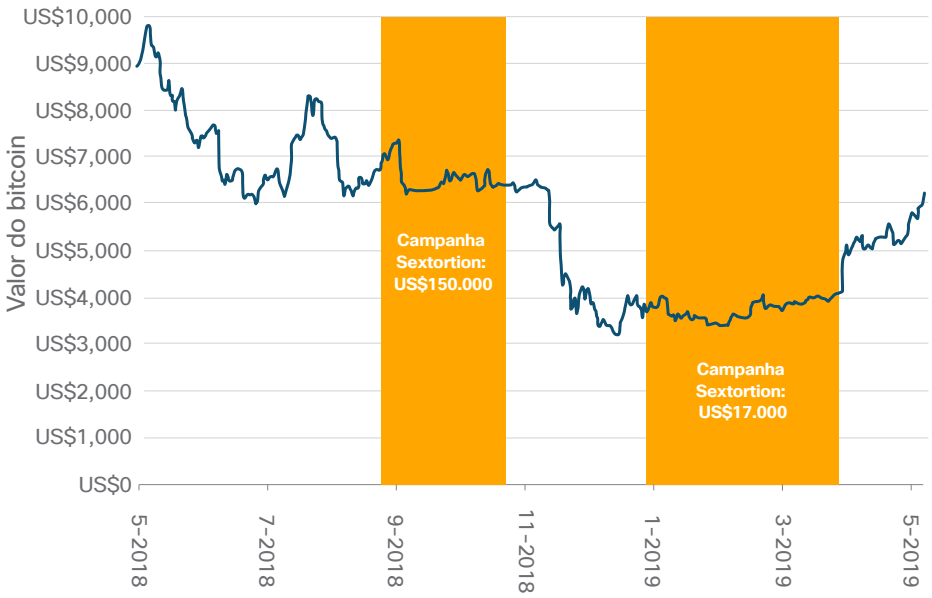
Extorsão digital.

Um e-mail chega à sua caixa de entrada com o assunto **"VOCÊ DEVE LEVAR ISSO À SÉRIO."** O remetente do e-mail alega ter invadido um site de vídeo de conteúdo para adultos acessado por você. Ele também afirma ter gravado você em sua webcam, juntamente com os vídeos supostamente assistidos por você. Além disso, o remetente alega ter obtido acesso aos seus contatos para os quais as filmagens serão enviadas, a menos que você pague a ele centenas, ou milhares, de dólares em bitcoins.

Isso é extorsão digital. A única coisa que separa isso de cenários de extorsão mais tradicionais é que as reivindicações são totalmente inventadas. Os golpistas não invadiram um site, eles não o gravaram e não têm sua lista de contatos. Eles estão simplesmente esperando induzi-lo a acreditar que farão tudo isso.

Abordamos muitas formas deste tipo de scam de e-mail em nossa publicação de blog Ameaça do mês, Seu dinheiro ou sua vida: scams de extorsão digital.

Figura 6 Comparação do valor de bitcoin (USD) para as campanhas de sextortion.



Fonte: Cisco Talos

É um truque interessante e lucrativo para os invasores, onde os lucros obtidos em uma campanha de extorsão digital atingiram a faixa de seis dígitos no final de 2018. No entanto, de acordo com a análise mais recente realizada pelo Cisco Talos, abrangendo janeiro a março de 2019, os lucros diminuíram. Ainda assim, a ascensão e a queda desses lucros correspondem vagamente ao valor do bitcoin, embora com declínios maiores. Como o valor de bitcoin parece estar aumentando no momento atual, será interessante ver se o mesmo acontece com os pagamentos de extorsão digital.

Spam de pacote e fatura

"Não me lembro de ter comprado uma assinatura para esse aplicativo móvel", você diz para si mesmo. Pelo menos é isso que o e-mail indica: uma assinatura vitalícia para, digamos, um clube de cinema. Calma aí, o local listado na fatura diz que foi comprado no Sri Lanka. E você nem mora no Sri Lanka. "Deve haver algum erro", você pensa à medida que abre rapidamente o PDF anexado para investigar.

Infelizmente, o PDF continha uma exploração que, então, baixou o Emotet para seu dispositivo. O esquema varia, mas geralmente se concentra em um pacote que você não solicitou, uma fatura de algo que você não comprou ou um pagamento mensal de uma assinatura ou serviço no qual você não se inscreveu. Isso pode resultar em vários resultados mal-intencionados, de credenciais bancárias roubadas a cryptomining.

Figura 7 E-mail de scam Emotet, fingindo ser da UPS.

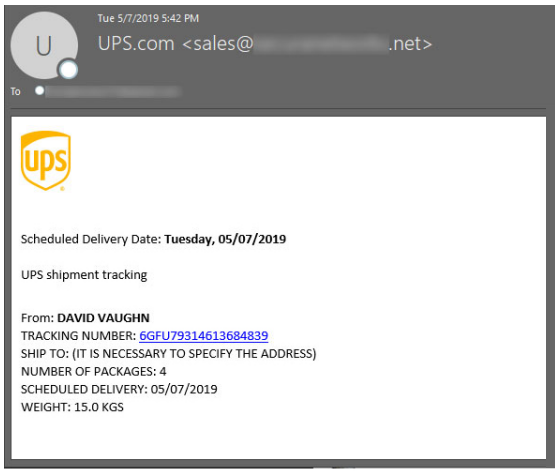


Figura 8 Exemplo recente de fraude de taxa antecipada.

Sr. Christoper A. Wray

CW

Diretor do Federal Bureau of Investigation (FBI)
Para: [redacted]
Responder para: [redacted]

A/C: Beneficiário.

De acordo com a ética de um escritório, a apresentação é sempre muito importante em um primeiro contato como este. Sou o Sr. Christopher A. Wray, Diretor do Federal Bureau of Investigation (FBI). Este memorando oficial é para informá-lo sobre a descoberta de que algumas autoridades que trabalham sob o governo dos Estados Unidos tentaram desviar seus fundos através de um canal de backdoor. Na verdade, descobrimos isso hoje, através de nossos agentes secretos sob a Unidade Disciplinar do FBI (Federal Bureau of Investigation) depois de prendermos um suspeito.

O suspeito mencionado foi preso no Aeroporto Internacional de Dulles esta manhã, enquanto tentava levar a enorme quantia de dinheiro para fora dos EUA. Em relação ao decreto de lavagem de dinheiro dos Estados Unidos, tal quantia de dinheiro não pode ser movimentada em espécie fora dos Estados Unidos porque a tentativa é uma ofensa criminal e punível sob a lei de lavagem de dinheiro de 1982 dos Estados Unidos da América. Este decreto é uma lei globalizada aplicável na maioria dos países desenvolvidos para combater o terrorismo e a lavagem de dinheiro.

Conforme nossas informações coletadas aqui nesta Unidade, descobrimos que os referidos Fundos realmente pertencem a você, mas foram propositalmente retidos porque os funcionários encarregados do seu Pagamento estão em algum tipo de irregularidade, o que é totalmente contra a ética de qualquer instituição de pagamento. Atualmente, esses fundos estão sob a custódia do banco pagador e posso garantir que serão liberados sem problemas, desde que haja com sinceridade conosco. Além disso, exigimos a sua cooperação em todos os níveis, porque estamos monitorando de perto essa transação para evitar pessoas desonestas presentes na nossa sociedade atual.

Hoje, com data de 9 de maio de 2019, instruímos à Administração Executiva do Banco Pagador a Liberar os referidos Fundos para você como o Beneficiário certificado em questão, porque temos informações valiosas/registros de autenticidade de que esses Fundos realmente pertencem a você. Seja como for, você é obrigado a nos fornecer informações abaixo listadas (para verificação oficial).

1. Nome e sobrenome.
2. Idade.
3. Profissão.
4. Estado civil.
5. Número de telefone/fax direto.
6. Endereço residencial.

Aguardamos a conformidade imediata com essa obrigação oficial, para que você possa ser pago pelo banco de pagamento autorizado.

Oficialmente lacrado.

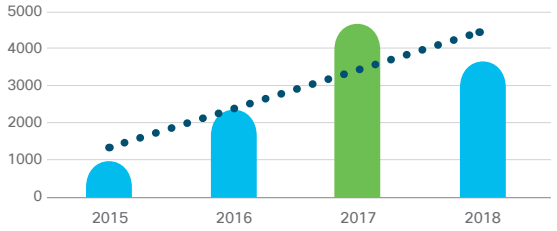
Sr. Christopher A. Wray
Diretor do Federal Bureau of Investigation (FBI)

Fraude de taxa antecipada

Não é todos os dias que você recebe um e-mail do FBI. É ainda menos comum receber um informando sobre uma transferência pendente de US$ 10,5 milhões! Tudo o que você precisa fazer é responder ao e-mail e eles vão instruí-lo sobre o como receber o pagamento.

Esse é um golpe clássico de fraude de taxa antecipada. Como o nome indica, os golpistas vão pedir uma taxa antes de enviarem o dinheiro prometido, que nunca aparecerá. É também um dos golpes de e-mail mais antigos, tendo evoluído para formas diferentes ao longo dos anos, de um príncipe estrangeiro que deseja compartilhar sua riqueza com a aprovação de empréstimos para pessoas com crédito ruim. Ainda assim, as fraudes persistem, com milhares desses scams de e-mail notificados ao EUA Better Business Bureau (BBB) a cada ano.

Figura 9 Scams de fraude de taxa antecipada conforme relatado ao BBB por ano.
(Total de categorias de tipo de scam: taxa de antecipação de empréstimo, troca de dinheiro nigeriano/estrangeiro, romance, reparação de crédito/alívio da dívida, investimento e viagens/férias.)



Fonte: Better Business Bureau

Malware no e-mail

Uma boa parte do malware ainda é enviado por e-mail. Ele costumava ser mais evidente, com arquivos .exe anexados diretamente aos e-mails. Mas, como os usuários perceberam que a abertura de um arquivo executável não era uma decisão segura, os agentes mal-intencionados mudaram de tática.

Hoje em dia, é muito mais provável que o malware seja entregue indiretamente, através de anexos menos suspeitos, como documentos comerciais comumente usados ou por URLs contidas no corpo da mensagem, todos esses itens enviados regularmente em uma comunicação de e-mail válida e regular. A ideia é passar pelas varreduras de e-mail tradicionais que travariam e colocariam em quarentena um arquivo binário ou outros anexos distribuídos com pouca frequência.

Isso é mais evidente ao analisar anexos de e-mail sinalizados observados até o momento neste ano (de janeiro a abril de 2019). Os arquivos binários compõem menos de 2% de todos os anexos mal-intencionados – que não incluem apenas arquivos. exe, mas sim todos os binários. Essa é uma grande mudança em relação aos anos passados, quando arquivos executáveis, Java e flash eram encontrados regularmente. Na verdade, o Java e o Flash caíram tanto na preferência que, se você adicioná-los a binários, ainda representarão somente 1,99% dos anexos.

Arquivos, como arquivos. zip, compõem quase um terço dos anexos mal-intencionados e quatro dos dez principais tipos de arquivos usados pelos invasores.

Tabela 1 Tipos de anexos mal-intencionados.

Tipo	Porcentagem
Escritório	42,8%
Arquivo	31,2%
Script	14,1%
PDF	9,9%
Binário	1,77%
Java	0,22%
Flash	0,0003%

Fonte: Talos Intelligence

Os tipos de anexos mais comuns são simplesmente os tipos enviados ao escritório em um dia comum. Dois em cada cinco arquivos mal-intencionados são documentos do Microsoft Office.

Quais são os tipos de anexos que os invasores mais usaram? Arquivos, como arquivos .zip, compõem quase um terço dos anexos e quatro dos dez principais tipos de arquivos. Os scripts, como arquivos .js, compõem 14,1%. Esses scripts aumentaram bastante desde a última vez que analisamos os tipos de anexos no 2018 Annual Cybersecurity Report (ACR), quando os arquivos .js, combinados com XML e HTML, representavam apenas um percentual de extensões de arquivo mal-intencionado.

Sua frequência como anexos mal-intencionadoscontinuou a crescer, subindo quase cinco pontos percentuais desde o ACR 2018. Insira os documentos PDF nesse meio e verá que mais da metade de todos os anexos mal-intencionados são tipos de documentos usados normalmente, onipresentes no local de trabalho moderno.

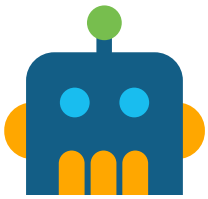
Tabela 2 As 10 principais extensões mal-intencionadas no e-mail.

Extensão	Porcentagem
.doc	41,8%
.zip	26,3%
.js	14,0%
.pdf	9,9%
.rar	3,9%
.exe	1,7%
.docx	0,8%
.ace	0,5%
.gz	0,5%
.xlsx	0,2%

Fonte: Talos Intelligence

Infraestrutura de entrega de e-mail

Vamos analisar os bastidores agora, longe dos tipos de e-mails ou das cargas úteis e dar uma olhada na forma como os e-mails mal-intencionados são distribuídos. Há dois métodos principais usados pelos golpistas para lançar campanhas de spam: botnets e kits de ferramentas de e-mail em massa.



Botnets

Os botnets de spam são, de longe, usados como os principais culpados pela maioria dos spams enviados hoje. A seguir, há alguns dos principais atuantes no cenário de botnet de spam.

Necurs

O botnet Necurs surgiu pela primeira vez em 2012 e espalhou uma variedade de ameaças, desde Zeus até o ransomware. Embora a atividade dele tenha recebido muito mais atenção no passado, o Necurs parece ter ficado em segundo plano, pelo menos em termos de cobertura de imprensa. No entanto, esse botnet ainda está muito ativo. Na verdade, o botnet Necurs é o principal veículo de distribuição para uma variedade de scams, incluindo extorsão digital.

Para obter mais informações sobre Necurs, confira a análise, Os muitos tentáculos do botnet Necurs, realizada pelo Cisco Talos.

Emotet

Grande parte do spam enviado pelo Emotet está na categoria de pacotes e fatura. O Emotet é um malware modular e inclui um plugin de spam. Devido ao modo como os agentes por trás do Emotet ganham dinheiro usando-o como um canal de distribuição para outras ameaças, o objetivo da maioria dos spams enviados pelo módulo spambot é infectar mais sistemas com o Emotet, ampliando ainda mais o alcance do canal de distribuição mal-intencionado.

Como o Emotet rouba conteúdo das caixas de correio das vítimas, muitas vezes é capaz de criar mensagens sequenciais mal-intencionadas, mas com aparência realista, que parecem fazer parte de conversas estabelecidas. O Emotet também é conhecido por roubar credenciais de SMTP, comandando os próprios servidores de e-mail de saída das vítimas, como um veículo para spam de saída.

Para obter mais informações sobre o Emotet, leia nosso relatório de ameaça anterior na Série de relatórios da segurança digital, Defesa contra as maiores ameaças dos dias de hoje.

"O Cisco Email Security diminuiu o tempo gasto na detecção e reduziu o spam em cerca de 80%."

Jacquelyn Hemmerich, Diretora de Segurança, Cidade de Sarasota, FL

Gama

O botnet Gamut está enviando spam de namoro e relações íntimas, principalmente alegando conhecer pessoas na sua área. Em outras campanhas, os agentes por trás do botnet enviam mensagens atraentes de produtos farmacêuticos ou oportunidades de emprego (consulte a Figura 10).

Eles registraram uma variedade de domínios, embora a própria infraestrutura pareça bastante simples, com vários subdomínios em um domínio e muitas vezes apontando para um endereço IP. Mesmo a Cisco não confirmando se os serviços oferecidos são legítimos, o processo de registro parece tentar fazer o phishing de informações pessoais.

Figura 10 E-mail de spam enviado pelo botnet Gamut.

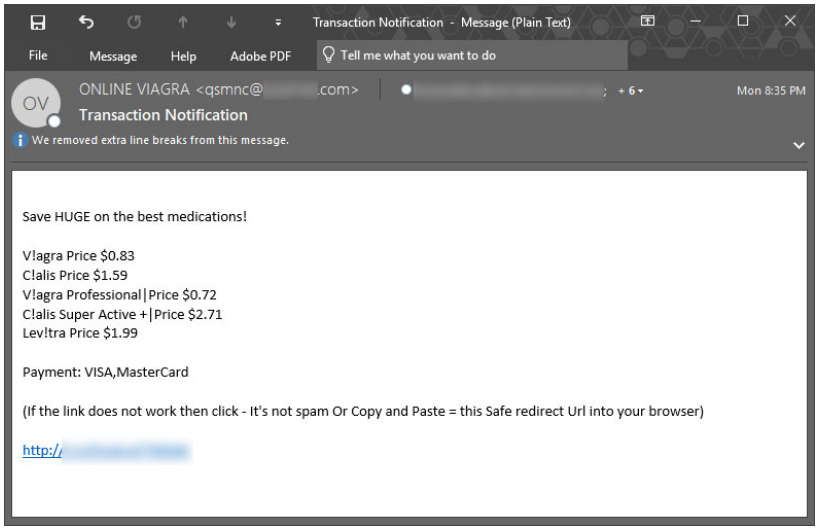
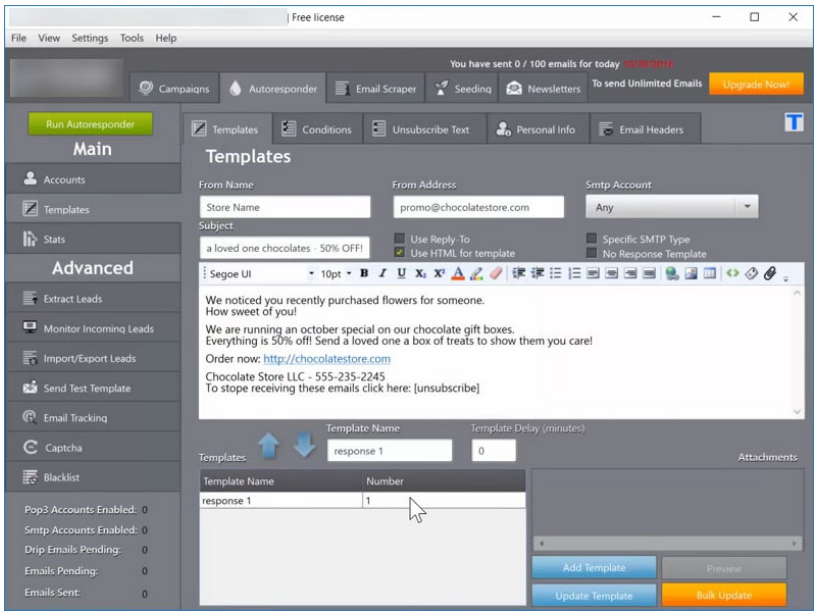


Figura 11 Exemplo de um kit de ferramentas de spam.



Kits de ferramentas de e-mail em massa

Uma abordagem alternativa que muitos spammers adotam é comprar kits de ferramentas para enviar a um grande número de e-mails. Muitas dessas ferramentas são semilegítimas, o que significa que, se você vendesse suas próprias cortinas de chuveiro personalizadas, poderia tecnicamente usar um desses kits de ferramentas para aumentar a notoriedade da marca via e-mail em massa para sua própria lista de inclusão de e-mail. No entanto, alguns dos recursos incluídos nesses kits de ferramentas, como os que permitem a rotação do envio do endereço IP e a reconstrução personalizada de anexos para gerar valores de hash exclusivos, são muito menos prováveis de serem usados nesses cenários.

Recentemente, os engenheiros do Cisco Talos descobriram grupos no Facebook em que agentes mal-intencionados estavam vendendo ferramentas de e-mail em massa, juntamente com listas de endereços de e-mail extensivas, provavelmente obtidas de violações de dados. Nesses casos, os compradores dessas ferramentas estavam claramente usando-as para fins ilícitos.

Fraude como o método

Se o e-mail é o vetor mais comum, a fraude é o método mais comum, especialmente para o crime organizado.

Se o e-mail é o vetor mais comum, a fraude é o método mais comum, especialmente para o crime organizado. Agentes mal-intencionados por trás de scams de BEC estão tentando fraudar as empresas em milhares de dólares. Os chantagistas digitais estão enganando de forma fraudulenta os usuários para pagá-los em bitcoins. E quando se trata de fraude de taxa antecipada, bem, o próprio nome diz tudo.

Nada disso é novo. O e-mail é apenas uma das ferramentas mais recentes que os criminosos usaram para cometer fraude. Historicamente, os criminosos se esforçam para aproveitar as oportunidades e maximizar a prática de atos ilícitos apresentados por cada geração de tecnologia.

Analisando as perdas registradas pela polícia federal alemã (Bundeskriminalamt BKA) e pelo FBI, mais de 80% de todas as perdas registradas por crimes digitais podem ser atribuídas à busca por fraude. A ênfase aqui está em "registrado", pois pode haver perdas intangíveis que são difíceis de quantificar e registrar com precisão. Isso significa que as estatísticas registradas são razoavelmente confiáveis.

Portanto, afirmar que a fraude é a força impulsionadora por trás das perdas de cibercrime é correto. De fato, ao examinar dois métodos de fraude divulgados pelas estatísticas do FBI, Comprometimento de conta empresarial (BEC) e Comprometimento de conta de e-mail (EAC), vemos que as perdas em 2018 foram de US$ 1,3 bilhão. Como comparação, as perdas equivalentes registradas para ransomware, uma forma mencionada e analisada de crime cibernético, foram de US$ 3,6 milhões. E o fato permanece: cada indicação é que as perdas associadas à fraude não detectada continuarão a crescer, enquanto as perdas associadas ao BEC/EAC aumentaram apenas 78% entre 2016 e 2017.

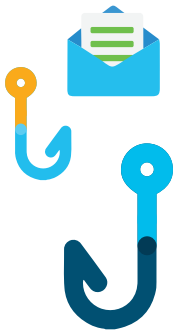
"O Cisco Email Security literalmente tirou a segurança de e-mail da nossa base de gerenciamento e nos permitiu nos concentrar em outras áreas. Ele detecta tudo! É uma paz de espírito saber que tomamos a decisão perfeita para a segurança de e-mail!"

Steven Wujek, Arquiteto Sênior de TI, Technology Concepts & Design, Inc.

Para obter mais informações sobre fraudes e perdas de crimes digitais, confira nossa série de blog sobre crimes digitais e fraude.

"Adotar uma abordagem holística da segurança não é apenas um problema de produtos de segurança ou uma obrigatoriedade nos negócios. **Trata-se de analisar as pessoas, os processos e a tecnologia em toda a empresa.** Na Cisco, começamos com uma abordagem centrada nas pessoas, nos concentrando no indivíduo, no trabalho que realizam e ajudando-os a fazê-lo de forma segura.Uma das maneiras de conquistar isso é oferecer aos funcionários dicas práticas para reconhecer e notificar e-mails suspeitos antes de clicar neles."

Steve Martino, Diretor Executivo de Segurança da Informação, Cisco



Como se proteger contra ataques de e-mail

Sinais indicadores de um e-mail de phishing

O lado positivo quando se trata de ameaças entregues por e-mail é que geralmente há discrepâncias que as identificam, se você apenas souber o que procurar. Veja a seguir alguns exemplos. Consulte a página a seguir para obter detalhes sobre cada um deles.

Para: voce@seuemail.com

1 De: Amazon Shipping <amz@123fnord.com>

Assunto: Seu pedida recente

Prezado(a),

2 Agradecemos o seu pedido. Os detalhes são os seguintes:

Compra: assinatura mensal de entrega para Puppy Food™
marca de alimento de filhote de cachorro
Custo mensal: US$ 121
Data e hora: 03 de meio de 2019 10:21
Endereço IP: 254.189.234.159.01
País de compra: Guatemala

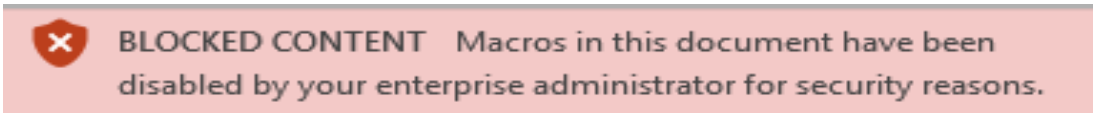
3 Se você não deseja mais se inscrever, cancele imediatamente seguindo as instruções anexadas ou inserindo os detalhes do seu cartão de crédito aqui:

4 5 http://badphishingsite.com/dontgothere.html

Atenciosamente,
Frete da Amazon

6 **dontopenthisis.bad**

Figura 12 Aviso do Microsoft Office sobre as macros no documento aberto.



1. **O endereço De:.** O nome no endereço De: não corresponde ao endereço de e-mail?
2. **Vários erros ortográficos e gramaticais ou logotipos desfocados.** Se o e-mail parece ter sido elaborado de forma descuidada, pode não ser legítimo.
3. **Senso de urgência.** Se um e-mail pedir que você tome medidas imediatas, se ele tiver um senso de urgência ou despertar sua curiosidade, isso é muito suspeito.
4. **Solicitação de informações pessoais ou confidenciais.** Nunca responda a um e-mail não solicitado que pede informações pessoais, financeiras ou confidenciais.
5. **URL que parece ilegítima.** Muitas URLs de e-mail de phishing parecem incomuns, se analisadas, e não devem ser clicadas. Se a URL estiver oculta em um link de texto, passe o mouse sobre ela e examine a parte inferior do navegador para analisá-la. Na dúvida, não clique nela.
6. **Arquivo não reconhecido.** Na maioria das competências profissionais, apenas alguns tipos de arquivo devem ser enviados por e-mail. Se o tipo de arquivo parecer estranho, não o abra.

Além disso:

- **Tenha calma.** A pessoa gasta em média de 8 a 10 segundos analisando um e-mail antes de agir. Tenha calma e procure as pistas que podem indicar uma tentativa de phishing.
- **Se parece bom demais para ser verdade, provavelmente é.** O e-mail oferece milhões de dólares? Ameaça constrangê-lo ou machucá-lo? É provável que ele seja totalmente falso.
- **Preste muita atenção aos avisos.** Se você reconhecer o remetente e abrir um anexo, preste muita atenção aos avisos do banner sobre extensões ou macros que precisam ser ativadas (Figura 12). Se for o caso, raramente são necessárias.

Estratégias de prevenção de ataque

Há várias abordagens que podem ser adotadas para reduzir o risco incluído nessas ameaças de e-mail.

Faça exercícios regulares de phishing. Seus funcionários são a maior defesa contra phishing, especialmente as tentativas de phishing mais personalizadas. Funcionários que podem aprender a reconheceruma tentativa de phishing podem interromper a principal fonte de comprometimento de endpoint.

Para aumentar a conscientização, faça exercícios regulares de phishing corporativo para testar e educar os usuários. Mimetize as técnicas mais recentes do mundo real para manter as pessoas cientes do que podem encontrar. A Cisco sugere fazer esses exercícios mensalmente, começando com campanhas de teste de phishing fáceis de detectar e aumentando gradualmente a complexidade. Para os usuários que são enganados pela mimetização de ataques de phishing, ofereça orientações imediatamente (por exemplo, envie um teste de URL "mal-intencionada" que leva a mais informações sobre phishing). Para usuários de alto risco em sua empresa, onde danos significativos podem ocorrer se eles caírem em um golpe, pratique exercícios personalizados de campanha de phishing.

Use a autenticação multifatorial. Caso as credenciais de uma conta de e-mail corporativa sejam roubadas com sucesso, a autenticação de vários fatores pode impedir que um invasor obtenha acesso à conta e provoque o caos.

A beleza da autenticação de vários fatores reside na simplicidade. Digamos que alguém consiga obter as suas credenciais de login, ou de alguém na sua rede, e tente efetuar logon. Com a autenticação de vários fatores, uma mensagem é enviada automaticamente para a pessoa que realmente é detentora da credencial para verificar se tentou fazer o logon. O usuário, nesse cenário, percebendo que não tentou efetuar login, nega a solicitação imediatamente. Isso frustra o ataque com sucesso.

Mantenha o software atualizado. Em alguns casos, os e-mails que incluem URLs mal-intencionadas podem levar os usuários para páginas com explorações. Manter os navegadores e software atualizados, bem como quaisquer plugins, ajuda a aliviar os riscos incluídos nesses ataques.

Nunca transfira dinheiro para um estranho. Isso se aplica a fraudes de taxa antecipada e scams de BEC. Se você suspeitar de uma solicitação, não responda. Para o BEC, em particular, configure políticas rígidas que exijam a autorização de transferência bancária de um indivíduo de alto escalão na empresa e implemente um signatário secundário designado.

Tenha cuidado com as solicitações para fazer logon. Agentes mal-intencionados, com a intenção de roubar credenciais de login, não medem esforços para fazer com que as páginas pareçam as páginas de logon que você reconheceria. Se encontrar um prompt de logon, certifique-se de verificar a URL para garantir que ela seja proveniente do site legítimo do proprietário. Se encontrar uma janela de estilo pop-up, expanda a janela para certificar-se de que a URL completa, ou pelo menos o domínio completo, seja visível.

Certifique-se de que o e-mail seja plausível. No caso de fraudes como a extorsão digital ea taxa antecipada, os remetentes geralmente elaboram histórias para tentar convencê-lo de que o e-mail é legítimo. O cenário que foi proposto faz sentido? Há alguma lacuna em suas histórias, do ponto de vista técnico, alguma perspectiva de processo financeiro ou outro problema? Em caso afirmativo, desconfie.

Esteja preparado

Há muitas maneiras diferentes de as ameaças de e-mailtentarem enganá-lo ou induzi-lo a responder, como clicando em URLs ou abrindo anexos. Isso justifica o uso de software de segurança de e-mail que pode capturar e colocar em quarentena e-mails mal-intencionados, além de filtrar spam.

Infelizmente, descobrimos uma tendência preocupante: o percentual de empresas que usa a segurança de e-mail está em declínio. De acordo com nosso mais recente Estudo comparativo de CISO, somente 41% dos entrevistados usam atualmente a segurança de e-mail como parte da defesa contra ameaças, mesmo quando relatam que o e-mail é o principal vetor de ameaças que coloca as empresas em risco. Isso está abaixo de 2014, quando 56% das empresas usavam a segurança de e-mail.

Há várias razões possíveis para esse declínio. Uma causa pode ser a mudança para a nuvem. Em um estudo recente conduzido pelo ESG em nome da Cisco, mais de 80% dos entrevistados relataram que sua empresa está usando serviços de e-mail na nuvem. À medida que mais empresas optam por ter seus serviços de e-mail hospedados na nuvem, os dispositivos de e-mail dedicados no local parecem menos necessários, conforme a opinião da equipe de TI.

No entanto, enquanto muitos serviços de e-mail na nuvemfornecem recursos básicos de segurança, a necessidade de proteção em camadas é fundamental. Na verdade, na mesma pesquisa realizada pelo ESG, 43% dos entrevistados descobriram que precisavam de segurança complementar para proteção de e-mail após a mudança. No final das contas, a equipe de TI ainda precisa definir políticas, obter visibilidade e controle, usar sandboxes e aproveitar os recursos de bloqueios externos.

Outro problema que as equipes de segurança enfrentam no momento é uma maior superfície de ataque, o que resulta naturalmente em mais áreas para proteção. Se os orçamentos de segurança não acompanharem esse aumento, as equipes podem ter que reduzir recursos para cobrir a superfície de ataque maior.

Como o e-mail é o vetor de ameaças mais comum, a importância de protegê-lo não pode ser subestimada. Ao realizar qualquer avaliação de risco digital, é importante priorizar os pontos de entrada mais importantes com sistemas completos de defesa e gerenciamento de riscos, bem como trabalhar com a classificação de probabilidade de ataque e risco à empresa, se ocorrer uma violação. Em seguida, aloque recursos compatíveis com a importância de possíveis perdas.

Além disso, o Gartner sugere que a segurançae os gerentes de risco (SRMs) adotem umaabordagem para melhorar asdefesas contra ataques de phishing:

1. Atualize o gateway de e-mail seguro e outros controles para melhorar a proteção contra phishing.
2. Integre os funcionários à solução e crie recursos para detectar e responder a ataques suspeitos.
3. Trabalhe com os gerentes de negócios para desenvolver procedimentos operacionais padrão e lidar com dados confidenciais e transações financeiras.

Como proteger seu e-mail

Analisamos os sinais indicadores de um e-mail de phishing e as estratégias de prevenção contra ataques. Agora, vamos analisar as expectativas para a tecnologia de segurança de e-mail em 2019.

Como no passado, uma abordagem em camadas para a segurança é fundamental para defender sua empresa contra ataques por e-mail. Há vários recursos de segurança de e-mail testados que ainda são importantes hoje.

Por exemplo:

- A defesa contra spam ainda deve ser implantada para manter o e-mail indesejado e o spam mal-intencionado fora das caixas de entrada.
- A defesa contra ameaças de e-mail, como malware e recursos de bloqueio de URL, é vital para bloquear malware, spear phishing, ransomware e cryptoming em anexos, juntamente com inteligência de URLpara combater links mal-intencionados em e-mails.
- O sandbox integrado deve acontecer automaticamente em segundo plano para novos arquivos que chegam ao e-mail, com o objetivo de verificar rapidamente se são mal-intencionados.

No entanto, é importante ressaltar que o cenário de ameaças está em constante evolução e os agentes mal-intencionados sempre buscam novos caminhos para lançar ataques.

Além das testadas, as seguintes tecnologias de segurança podem ajudar a combater esse cenário em constante mudança:

- As proteções de phishing mais modernas surgiram com aprendizagem de máquina para entender e autenticar identidades de e-mail e relações comportamentais visando bloquear ataques de phishing avançados.
- As proteções de domínio DMARC agora podem ser ativadas para proteger a marca de uma empresa ao impedir que os invasores usem um domínio corporativo legítimo em campanhas de phishing.
- A funcionalidade de quarentena de mensagens é útil para reter uma mensagem enquanto um anexo de arquivo é analisado antes de liberá-la para o destinatário, removendo o anexo mal-intencionado ou removendo completamente a mensagem.
- A remediação de e-mail será útil se um arquivo for detectado como mal-intencionado após a entrega ao destinatário, permitindo que você o retorne e coloque a mensagem em quarentena com o anexo mal-intencionado dentro de uma caixa de correio.
- Os feeds de ameaças de e-mail externos em STIX agora são comumente detidos por produtos de segurança de e-mail, sendo útil se uma empresa desejar deter um feed de ameaça com foco em verticais além da inteligência de ameaças nativa no produto.
- A integração de segurança de e-mail com portfólios de segurança mais amplos também está se tornando comum para entender se um malware ou mensagens avançadas em um ambiente podem ter sido entregues a usuários específicos ou a caixas de entrada.

"A Cisco é líder em segurança de e-mail corporativo da Forrester Wave em 2019, recebendo as classificações mais altas por opções de implantação, proteção contra ataques e autenticação de e-mail, desempenho e operações (incluindo escalabilidade e confiabilidade) e liderança em tecnologia."

The Forrester Wave™: Segurança de e-mail corporativo, segundo trimestre de 2019

O Cisco Cybersecurity Series

Ao longo da última década, a Cisco publicou uma série de informações sobre inteligência de ameaças para profissionais de segurança interessados no status global da segurança digital. Estes relatórios abrangentes têm fornecido detalhes dos cenários de ameaças e as implicações para as empresas, bem como as melhores práticas para se defenderem contra os impactos das violações de dados.

Na nova abordagem da nossa liderança de pensamento, a Cisco Security está publicando vários artigos baseados em pesquisas e orientados por dados sob o banner Cisco Cybersecurity Series. Ampliamos o número de títulos para incluir relatórios diferentes para profissionais de segurança com interesses diferentes. Apelando para a profundidade e amplitude da experiência de pesquisadores de ameaças e inovadores no setor de segurança, a coleção anterior de relatórios da série 2019 inclui o Relatório de Privacidade de Dados, o Relatório de Ameaças e o Relatório de Referência do CISO, e outros ainda virão ao longo do ano.

Para obter mais informações e todos os relatórios e cópias arquivadas, acesse www.cisco.com/br/securityreports.

Sede - Américas
Cisco Systems, Inc.
San Jose, CA

Sede - região da Ásia Pacífico
Cisco Systems (USA), Pte. Ltd.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdã,
Holanda

A Cisco possui mais de 200 escritórios em todo o mundo. Os endereços, números de telefone e de fax estão disponíveis no site da Cisco www.cisco.com/go/offices.

Publicado em junho de 2019 THRT_02_0519_r1