

# RESUMO EXECUTIVO: POR QUE AMEAÇAS AVANÇADAS REQUEREM UMA SEGURANÇA DE E-MAIL AVANÇADA

**Ameaças desconhecidas e de ransomware fazem da segurança de e-mail uma questão cada vez mais crucial**



## Resumo

No mundo hiperconectado de hoje, as comunicações baseadas em e-mail não são apenas comuns, elas se tornaram uma peça fundamental para efetivamente conduzir negócios, com o volume total de e-mails enviados por dia projetados para aumentar em pelo menos 5% a cada ano. Dada a natureza universal das comunicações por e-mail, eles são e continuarão a ser um vetor popular para uma variedade de ameaças.

## O uso do e-mail continua a crescer

Independentemente da proliferação de texto e mídia social, a comunicação por e-mail ainda cresce com força. De acordo com um estudo recente conduzido pelo Radicati Group, o volume total de e-mails enviados e recebidos no mundo atingiu 205 bilhões por dia, com este volume projetado para aumentar em pelo menos 5% a cada ano.<sup>1</sup> E esse fato não é desconhecido para os hackers que estão constantemente buscando oportunidades para explorar as organizações.

<sup>1</sup> The Radicati Group, Inc., [Email Statistics Report 2015-2019 \(em inglês\)](#)

A anatomia de um ataque por e-mail:

- Um CFO recebe um e-mail de um Diretor Executivo autorizando uma transferência emergencial de fundos. Mas, na verdade, o e-mail foi enviado por um cibercriminoso
- Um funcionário com direitos administrativos aos principais sistemas recebe um e-mail urgente da equipe de TI para atualizar sua senha de rede. E acaba por divulgar a sua senha para cibercriminosos.
- Um funcionário recebe um e-mail para ler um anexo importante sobre seu fornecedor de benefícios. Ao abrir o anexo, o malware de Trojan escondido é inadvertidamente ativado.

## Ameaças por email que as organizações enfrentam hoje em dia

Os e-mails oferecem aos hackers um veículo para distribuir uma série de vulnerabilidades para uma organização. Algumas das ameaças mais comuns, oriundas dos e-mails, são:

- **Malware** – e-mails são um dos principais mecanismos de fornecimento para distribuir malwares conhecidos e desconhecidos, que normalmente são incorporados em anexos de e-mail na esperança de que o anexo seja aberto ou baixado em um computador ou rede, permitindo que os hackers obtenham acesso aos recursos, roubem dados ou invadam sistemas.
- **Ransomware** – uma variante especialmente prejudicial de malware é o ransomware. Assim que um anexo de um e-mail é ativado, o código se integra na rede e o ransomware geralmente criptografa ou bloqueia arquivos e sistemas críticos. Os hackers então coagem a organização a pagar uma taxa de extorsão para que os arquivos ou sistemas não sejam descriptografados ou desbloqueados.
- **Phishing** – esta tática comum entre os hackers utiliza e-mails com links integrados para invadir sites. Quando os usuários inocentes visitam esses sites, eles recebem a solicitação para inserir PII (Personally Identifiable Information, ou Informações Pessoais Identificáveis) que, por sua vez, são usadas para roubar identidades, comprometer dados corporativos ou acessar outros sistemas críticos.
- **Spear Phishing/Whaling** – nesta modalidade de phishing, os principais profissionais de TI/rede ou os executivos da empresa são afetados ao utilizarem e-mails maliciosos que parecem vir de uma fonte confiável, em esforços para obter acesso aos sistemas e dados internos.
- **Comprometimento de e-mail corporativo/Fraude de CEO/E-mail impostor** – nos últimos dois anos, os esquemas de Comprometimento de e-mail empresarial (BEC) causaram pelo menos US\$ 3,1 bilhões em perdas totais a aproximadamente

22.000 empresas em todo o mundo, de acordo com os dados mais recentes do FBI<sup>1</sup>. O FBI define o Comprometimento de e-mail corporativo como um esquema de e-mail sofisticado que visa as empresas que trabalham com parceiros estrangeiros que realizam regularmente pagamentos de transferência bancária.

- **Spam** – os e-mails são usados para distribuir spam ou mensagens não solicitadas, que podem obstruir caixas de entrada e recursos de rede, diminuir a produtividade das empresas e aumentar os custos operacionais.
- **Sequestro de e-mails enviados** – as corporações também estão sujeitas a políticas corporativas e regulamentações governamentais, que mantêm as empresas responsáveis por seus e-mails de saída e assegurando que protejam a PII de seus clientes. Os ataques de zumbis e sequestro de IP podem disseminar a PII de clientes, arruinando a reputação de um negócio.

## Conclusão

As comunicações por e-mail são essenciais para as organizações de hoje, algo de que os hackers estão conscientes. Dadas as ameaças complexas e maduras de hoje, é plausível que as organizações implantem uma solução de segurança multicamadas que inclua a proteção de e-mail dedicada e de ponta. Para combater com eficácia as ameaças emergentes de hoje, as organizações são devidamente aconselhadas a implementar uma solução de gerenciamento de segurança de e-mail de próxima geração que forneça uma proteção de e-mail fundamental.

Para saber mais sobre as formas de proteger os e-mails de sua organização, leia sobre as nossas soluções [O que a sua segurança de e-mail de próxima geração precisa para deter ameaças avançadas.](#)

<sup>1</sup> [www.ic3.gov/media/2016/160614.aspx](http://www.ic3.gov/media/2016/160614.aspx)

© 2017 SonicWall Inc. TODOS OS DIREITOS RESERVADOS.

SonicWall é uma marca comercial ou marca registrada da SonicWall Inc. e/ou de suas afiliadas nos Estados Unidos e/ou em outros países. Todas as outras marcas comerciais e registradas são de propriedade de seus respectivos proprietários.

As informações deste documento são fornecidas em relação aos produtos da SonicWall Inc. e/ou de suas afiliadas. Este documento, de forma isolada ou em conjunto com a venda de produtos SonicWall, não concede nenhuma licença, expressa ou implícita, por preclusão ou de outra forma, a qualquer direito de propriedade intelectual. SALVO CONFORME DEFINIDO NOS TERMOS E CONDIÇÕES ESPECIFICADOS NOS CONTRATOS DE LICENÇA PARA ESTE PRODUTO, A SONICWALL E/OU SUAS AFILIADAS NÃO ASSUMEM QUALQUER RESPONSABILIDADE E RENUNCIAM A QUALQUER GARANTIA, EXPRESSA, IMPLÍCITA OU ESTATUTÁRIA, RELACIONADA AOS SEUS

PRODUTOS, INCLUINDO, ENTRE OUTROS, A GARANTIA IMPLÍCITA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A DETERMINADO PROPÓSITO OU NÃO VIOLAÇÃO. EM HIPÓTESE ALGUMA A SONICWALL E/OU SUAS AFILIADAS SERÃO RESPONSÁVEIS POR QUAISQUER DANOS DIRETOS, INDIRETOS, CONSEQUENCIAIS, PUNITIVOS, ESPECIAIS OU INCIDENTAIS (INCLUINDO, SEM LIMITAÇÃO, DANOS POR PERDA DE LUCROS, INTERRUPTÃO DE NEGÓCIOS OU PERDA DE INFORMAÇÕES), DECORRENTES DO USO OU IMPOSSIBILIDADE DE UTILIZAR ESTE DOCUMENTO, MESMO QUE A SONICWALL E/OU SUAS AFILIADAS TENHAM SIDO AVISADAS DA POSSIBILIDADE DE TAIS DANOS. A SonicWall e/ou suas afiliadas não se responsabilizam por qualquer garantia ou declaração referente à exatidão ou à integridade deste documento e reservam-se o direito de fazer alterações em especificações e descrições de produtos a qualquer momento, sem aviso prévio. A SonicWall Inc. e/ou suas afiliadas não se comprometem em atualizar as informações contidas neste documento.

### Sobre nós

Em uma história de mais de 25 anos, a SonicWall tem sido a parceira de segurança confiável do setor. Desde a segurança de rede até a segurança de acesso e de e-mail, a SonicWall tem evoluído continuamente seu portfólio de produtos, o que permite que as organizações inovem, acelerem e cresçam. Com mais de um milhão de dispositivos de segurança em quase 200 países e territórios no mundo todo, a SonicWall permite que seus clientes digam sim com confiança para o futuro.

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](http://www.sonicwall.com)