KASPERSKY lab

Kaspersky Security for Microsoft Office 365

3.5 m

de e-mails são enviados a cada segundo.

Apenas um é suficiente
para derrubar o seu negócio.

Movendo para a nuvem? Faça com segurança.

Com mais de 100 milhões de usuários mensais, o Microsoft Office 365 é oficialmente mais popular entre os usuários empresariais do que o seu colega tradicional, instalado localmente [1].

No entanto, aliviar a carga na infraestrutura e de recursos não diminui as ciberameaças, especialmente, quando se trata do e-mail do Office 365.

Spam, anexos maliciosos, phishing (incluindo lançadores de phishing/acordo de e-mail corporativo - BEC), ransomware e roubo de dados são um problema tão grande para as correspondências do Office 365 quanto para a instalação local.

E os recursos que eles consomem? Da pressão na largura de banda até a perda de produtividade, o spam continua a entupir as artérias dos negócios ao redor do mundo: mais da metade de todo o tráfego global de e-mails é de spam.

Para pequenas e médias empresas, manter o fluxo de comunicação assim como as ciberameaças e os vampiros da produtividade distantes é um grande desafio.

+600% Aumento de malwares visando o Microsoft Office365 em 2016 [2].

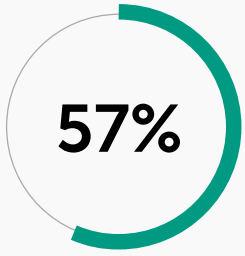
Clique, clique, BOOM!

Você já sabe: o e-mail é o vetor de malware número um ameaçando a segurança das empresas [3].

Então por que os usuários continuam clicando?

Apesar dos seus melhores esforços, um em cada dois, vai clicar em um e-mail não solicitado – ainda que 78% digam que conhecem os riscos [4].

Não é à toa que é a ferramenta escolhida pelos cibercriminosos; o caminho mais rápido para o coração do seu negócio é a caixa de entrada do usuário. E quando os cibercriminosos fabricam as mensagens para parecerem legítimas, é ainda mais difícil as deletar ou bloquear, então nem se esforce em tentar impedir que os usuários cliquem.



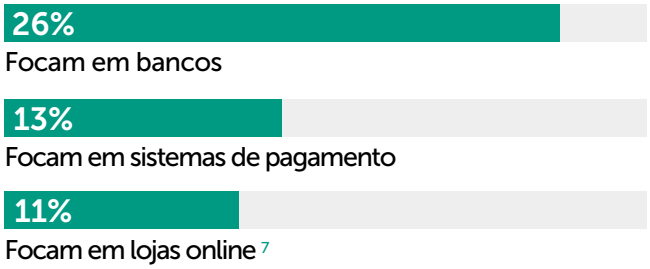
dos usuários do Microsoft Office 365 tiveram pelo menos uma cópia do Cerber (ataque de ransomware via spam) em suas caixas de entrada em 2016 [5].

1. *Satya Nadella, Microsoft Q3 2017 earnings call. Em 2017, a venda de licenças do Microsoft Office 365 superou a da versão instalada localmente pela primeira vez.*
2. *https://redmondmag.com/articles/2017/06/01/office-365-security.aspx*
3. *Relatório de Investigação de Violação de Dados da Verizon 2017*
4. *Friedrich-Alexander Universitat: https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/*
5. *https://www.scmagazine.com/microsoft-office-365-hit-with-massive-cerber-ransomware-attack-report/article/529295/*

Alguma coisa de phishing?

A maioria das empresas já dedicou tempo para educar usuários sobre ameças de e-mails maliciosos.

Mas o que pode ser feito quando cibercriminosos desviam disso, focando em departamentos e usuários específicos com mensagens fabricadas para parecerem que vieram do chefe, do fornecedor ou de um candidato a uma vaga? Vinte e um por cento dos incidentes relatados envolvem alguma forma de phishing[6] e mais da metade de todos os ataques focam no setor financeiro:



Ataques de phishing normalmente envolvem tentativas em larga escala de roubar senhas, detalhes bancários, números de cartões de crédito ou espalhar códigos maliciosos como ransomware no computador da vítima. Eles geralmente parecem 'normais' – à primeira vista – e são enviados em grande quantidade, para aumentar a chance de que pelo menos uma pessoa seja enganada. Antes que você pense que é muito esperto para ser pego, pense:

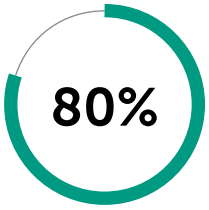
Alguém do departamento de contabilidade recebe um e-mail 'ÚLTIMA NOTIFICAÇÃO DE FATURA URGENTE' perto do final do mês. Eles estão ocupados, parece legítimo e tem um anexo em PDF, algo que estão acostumados a ver em e-mails. Então clicam... e o malware foi lançado.

"Como aconteceu?"

Como estavam em um ritmo acelerado, o usuário não viu que o arquivo acabava em '.exe' – após o mais conhecido '.pdf'. Ou então ele viu – mas o cibercriminoso escondeu a extensão da vista casual (chamado de 'spoofing de extensão'). Às vezes, é tão fácil quanto esquecer de mudar uma configuração do Windows que esconde extensões de arquivo como padrão.

Independente da maneira que você analisar, bloquear esses e-mails de chegarem na caixa de entrada de seus usuários poderia salvar a sua empresa de muitos problemas. Reconhecimento do real tipo de arquivo e filtro de anexos por extensão são apenas duas das tecnologias de segurança que podem ajudar a deletar e bloquear arquivos mascarados de anexos inofensivos ou legítimos.

No Windows, desativar a opção "Ocultar extensões para tipos de arquivos conhecidos" na seção "Opções de pasta" na guia de controle. Isso faz com que os usuários identifiquem mais facilmente um arquivo que não é o que parece.



das violações de dados envolvem senhas roubadas ou fracas, sendo em sua maioria adquiridas através de e-mails de phishing[8]

Especialmente para você: lançadores de phishing

Mas o que acontece quando cibercriminosos partem para outro nível e focam em destinatários específicos da sua empresa com mensagens e anexos que parecem quase que exatamente com as comunicações legítimas?

Lançadores de phishing podem enganar até o funcionário mais cauteloso: um 'currículo' enviado especificamente para o nome do gerente contratante – com um e-mail que se refere a um anúncio de emprego legítimo. Ou uma fatura enviada para a pessoa certa da contabilidade, referindo-se a uma empresa que realmente faz negócios com você. Às vezes, até o endereço de e-mail do remetente é mascarado para parecer legítimo, pelo menos à primeira vista ou para um usuário não técnico. Esses e-mails normalmente carregam anexos maliciosos ou links para sites maliciosos, de onde um ataque pode ser lançado ou credenciais roubadas.

6. *Relatório de Investigação de Violação de Dados da Verizon 2017*
7. *Kaspersky Lab: https://www.kaspersky.com/about/press-releases/2017_5000-fold-decrease-in-spam-botnet-mailings)*
8. *Relatório de Investigação de Violação de Dados da Verizon 2017*

Uma inclusão mais recente da família do phishing é o 'e-mail do presidente da empresa', autorizando uma transferência urgente de dinheiro. Conhecido como 'Acordo de E-mail Coporativo' (Business Email Compromise - BEC), essas mensagens possuem um pedido convincente e um endereço de remetente mascarado para parecer que realmente vieram do chefe. Uma vez que são perfeitamente fabricados, esses ataques frequentemente ultrapassam as armadilhas para spam – não são enviados em grande quantidade e normalmente são encaminhados apenas para alguns funcionários bem escolhidos.

Especificamente com o BEC, é fácil entender por que as pessoas erram e clicam. Mais uma vez, a melhor defesa é detectar e filtrar esses e-mails antes que cheguem aos seus usuários. As soluções de segurança que permitem a detecção de arquivos do Microsoft Office com macros, por exemplo, podem aumentar a proteção contra anexos maliciosos. A habilidade de analisar anexos vistos previamente para conteúdo de phishing adicionam uma camada extra de proteção. Enquanto isso, o suporte de e-mails autorizados pode reduzir significativamente as chances de um e-mail mascarado chegar ao usuário final.

Do ponto de vista da internet, bases de dados de URLs maliciosas e de phishing continuamente atualizadas significam que, mesmo que um usuário clique, o site será bloqueado.

Antes de clicar em qualquer link, sempre confira se a URL está correta: por exemplo, kaspesky.com versus Kaspersky.com. E nunca digite sua senha ou login por meio de um botão em um e-mail que o peça para fazer – no mínimo visite o site legítimo primeiro, digitando o endereço no navegador.

O FBI diz que mais de $2.3bilhões de dólares foram perdidos em golpes de e-mails do presidente da empresa[9] .Dentre as vítimas mais famosas estão as firmas globais Mattel, SnapChateFACC.

9. *https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/*

Spam: o vampiro da produtividade

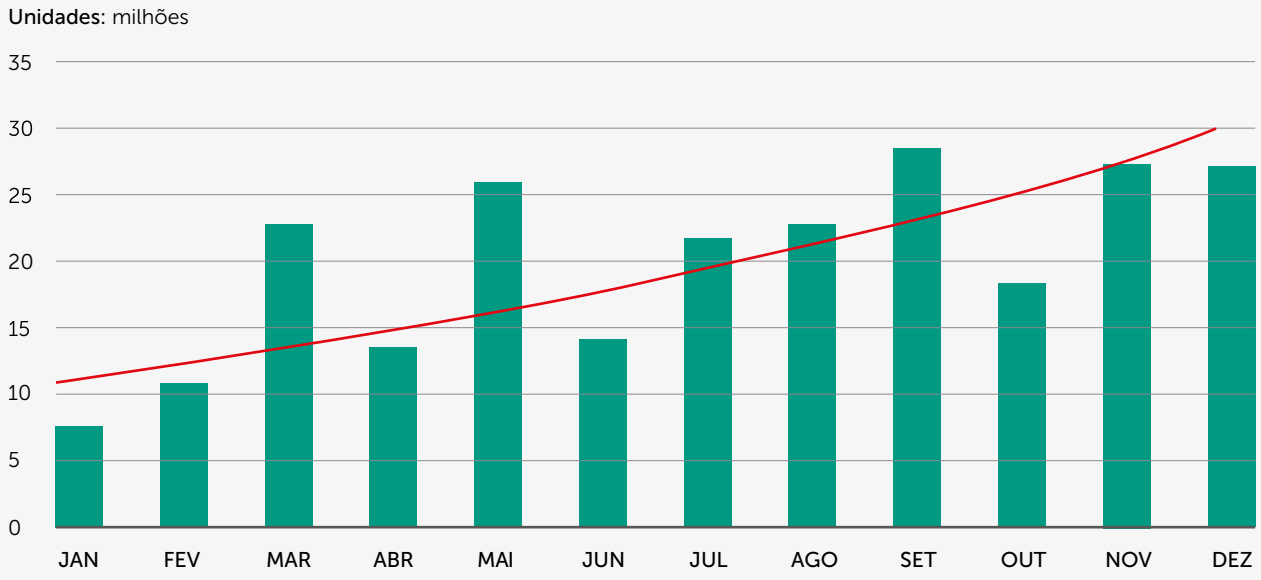
Mais de 58% de todo o tráfego de e-mails é spam [10]. E ao mesmo tempo em que muitos carregam malware, também são os principais ladrões de recursos e produtividade: o funcionário comum gasta 13 horas todo ano examinando e deletando spam, em um custo estimado de $1250 dólares por ano [11]. E também não se trata apenas do gasto de tempo de funcionários – mais da metade dos custos de energia relacionados ao spam são associados à sua exclusão e procura de e-mails legítimos [12].

Quando o tempo, recursos e dinheiro que você economizou migrando para a nuvem são consumidos por lixo eletrônico que ninguém quer, você sabe que tem um problema.

Mas e toda a correspondência legítima que pode sumir por ser confundida com spam? 35% dos usuários empresariais dizem que o bloqueio de mensagens legítimas atrasou suas respostas a assuntos importantes 2-3 vezes por ano; 19% dizem que aconteceu de 4-6 vezes [13]. Uma boa tecnologia anti-spam permite uma marcação facilmente personalizável de possíveis mensagens de lixo eletrônico, melhorando a produtividade ao filtrar mensagens potencialmente úteis, sem as deletar.

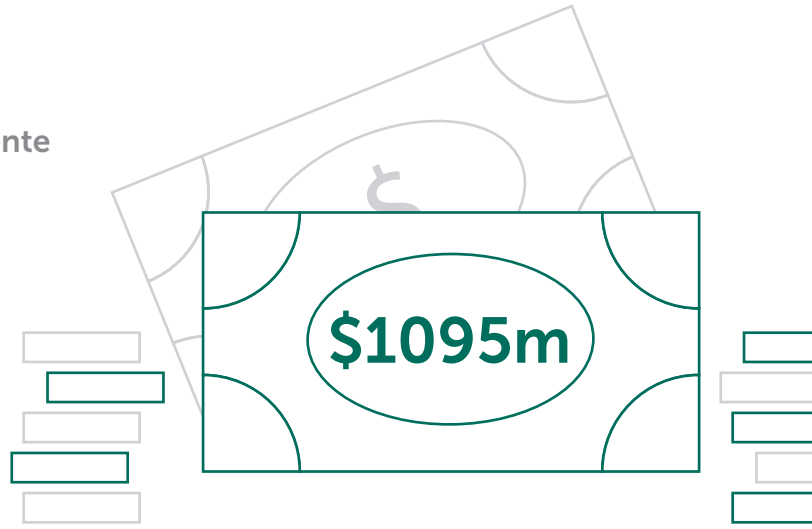
O bloqueio de correspondências corporativas desperdiça tempo, mas é ainda pior quando mensagens legítimas são deletadas automaticamente, antes que o administrador ou usuário possa dizer alguma coisa, gastando tempo e recursos na busca – ou duplicação – de trabalho.

Pesquisa da Kaspersky mostra um aumento massivo no volume de spams maliciosos em 2016



10. *Boletim da Kaspersky Security: Spam e Phishing em 2016.*
11. *Fonte: Atlassian, Perda de Tempo no Trabalho*
12. *http://www.brighthub.com/environment/green-computing/articles/33434.aspx*
13. *https://techtalk.gfi.com/survey-spam-email-disrupts-two-thirds-of-businesses-each-year-infographic/*

Seja mais esperto que o cibercriminoso: não tem certeza sobre um site que parece legítimo, mas está solicitando inesperadamente que digite sua senha? Invente uma – o site verdadeiro vai rejeitá-la. Melhor ainda, procure pelo prefixo 'https' na URL do site, indicando que é seguro. Um site sem https deve aumentar a suspeita, especialmente se é uma página financeira ou de comércio eletrônico.



O mercado de spam tem um valor estimado de $1095 milhões anuais[14].

Malware: a ameaça no coração de tudo

Enquanto muitos cibercriminosos estão focados em roubar credenciais ou enganar usuários para que efetuem pagamentos, é válido lembrar que 66% dos malwares são instalados por meio de anexos de e-mail maliciosos [15]. Noventa e cinco por cento dos ataques de phishing que levam a uma violação acontecem seguidos de alguma forma de instalação de software [16].

Mas você educou seus usuários e ativou a segurança enviada com a instalação do seu Office 365. Como isso aconteceu?

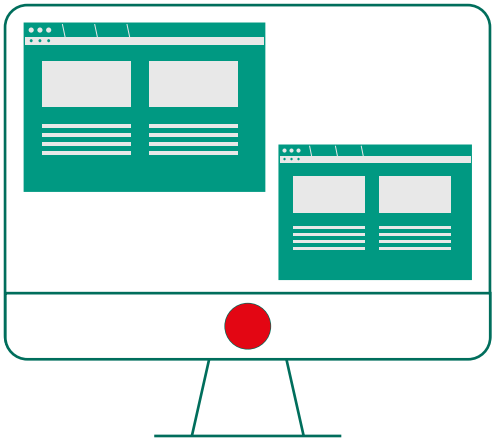
Alguns criminosos são tão persistentes quanto os cibernéticos. Eles estão sempre procurando novas maneiras de evitar a detecção e novas vulnerabilidades em softwares populares que possam ser exploradas antes de serem corrigidas.

Essas vulnerabilidades são chamadas de 'dia-zero'– consistindo em lacunas perigosas no software que acabaram de ser descobertas, mas para as quais ainda não há proteção.

Essas ameaças em evolução, frequentemente desconhecidas e avançadas são enfrentadas da melhor maneira com tecnologias de segurança que utilizam aprendizado de máquina e inteligência de ameaças constantemente atualizadas. Juntas, elas garantem que a sua segurança esteja sempre aprendendo a partir dos modelos de ameaças que analisa – e do que está acontecendo no mundo real dos ataques.

Enfim, significa que uma tecnologia de detecção e suavização anti-malware poderosa é um componente essencial para a segurança de e-mails, bem como para as ameaças que acabamos de ver como spam e phishing.

14. *Kaspersky Lab, Securelist.*
15. *Relatório de Investigação de Violação de Dados 2017*
16. *Relatório de Investigação de Violação de Dados 2017*



Quando o Office 365 encontra ciberameaças 24 horas por dia

Quando se trata de proteger a correspondência do seu Microsoft Office 365, a melhor estratégia é garantir que as ameaças sejam detectadas e bloqueadas antes de se tornarem um problema.

Instale o Kaspersky Security for Microsoft Office 365. Ele combina anti-malware de última geração com anti-spam e anti-phishing, líder da indústria para proteger seu e-mail e seus usuários de ameaças conhecidas, desconhecidas e avançadas.

Para ser realmente eficaz, você precisa ser capaz de fazer isso sem desacelerar ou acidentalmente deletar o tráfego de correspondências legítimas. É preciso manter o fluxo de comunicação – e as ciberameaças de fora. E se você for realmente proativo, pode usar toda a informação obtida das ameaças bloqueadas para entender quais delas o seu negócio está encarando.

O **Kaspersky Security for Microsoft Office 365** foi feito especificamente para fazer isso para a sua empresa.Como o seu Microsoft Office 365, ele também é baseado na nuvem. E como todas as soluções da Kaspersky Lab, foi construído a partir da segurança mais testada e premiada do mundo [17].

O **Kaspersky Security for Microsoft Office 365** utiliza heurística avançada, SandBox, aprendizado de máquina e outras tecnologias de última geração para proteger os e-mails de ransomware, anexos maliciosos, spam, phishing e ameaças desconhecidas.

Também gerencia falsos positivos mais efetivamente: administradores têm controle completo sobre o que acontece com correspondências suspeitas. Mensagens deletadas são colocadas em backups que podem ser facilmente procurados e restaurados. Nossa taxa de detecção de spam superior a 99% significa que nossos usuários vão gastar menos tempo, gerenciando lixo eletrônico inútil e potencialmente perigoso.

E como sabemos que você está na nuvem por causa da conveniência, eficiência de recursos e eficácia de custos, o Kaspersky Security for Microsoft Office é fácil de usar: um console único de gerenciamento cuida de tudo, incluindo uma visão única de ameaças detectadas e estatísticas. Não é preciso hardware adicional ou treinamento para instalação.

Descubra como nossas tecnologias de segurança de última geração pode tornar mais fácil de gerenciar e manter segura a correspondência do seu Microsoft Office 365.

17. *Em 2016, os produtos da Kaspersky Lab participaram de 78 testes e revisões independentes. Nossos produtos foram 55 vezes campeões e estiveram 70 vezes entre os três finalistas. https://www.kaspersky.co.uk/top3*