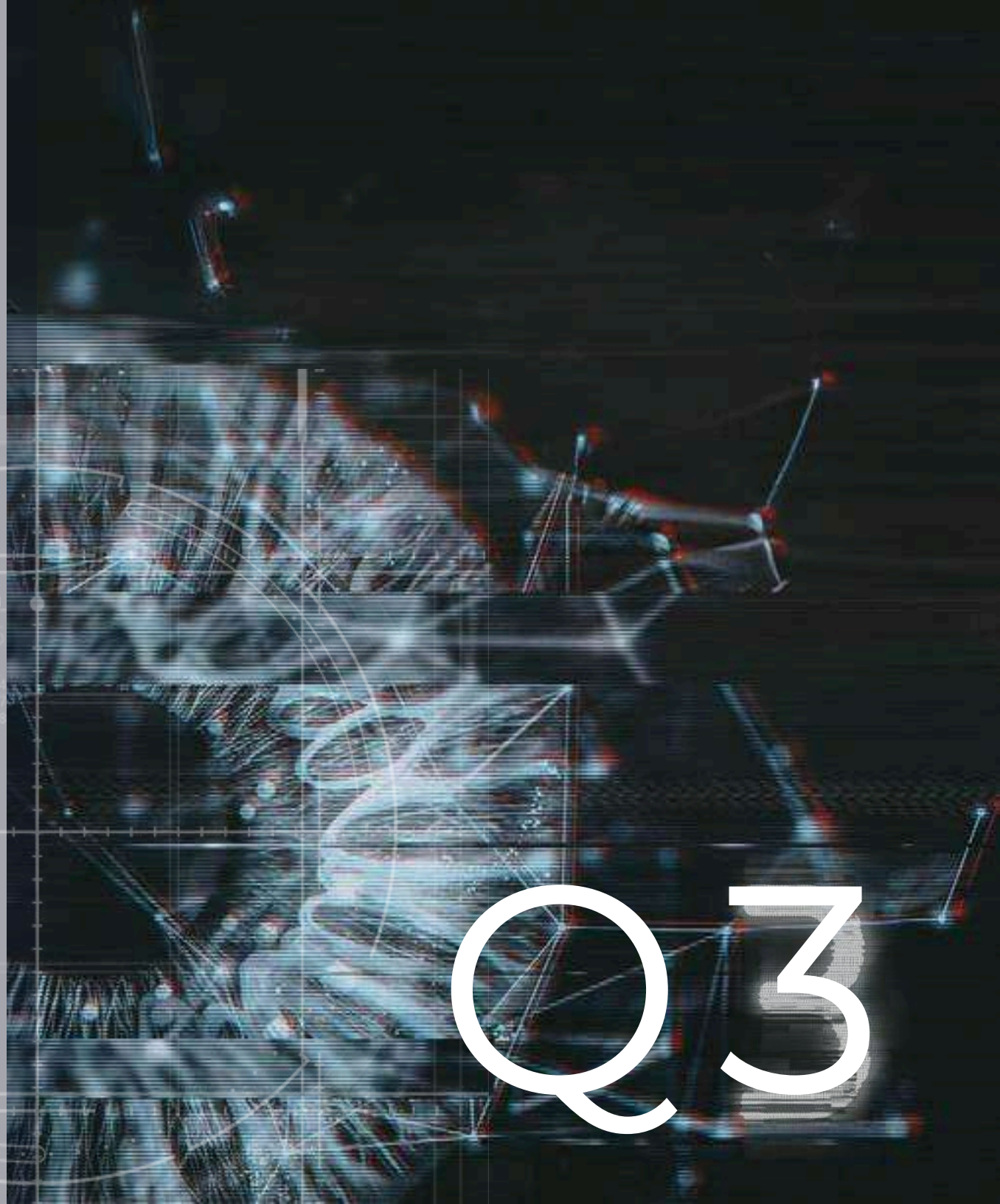
mimecast

# Relatório Global de Inteligência

Julho-Setembro 2023



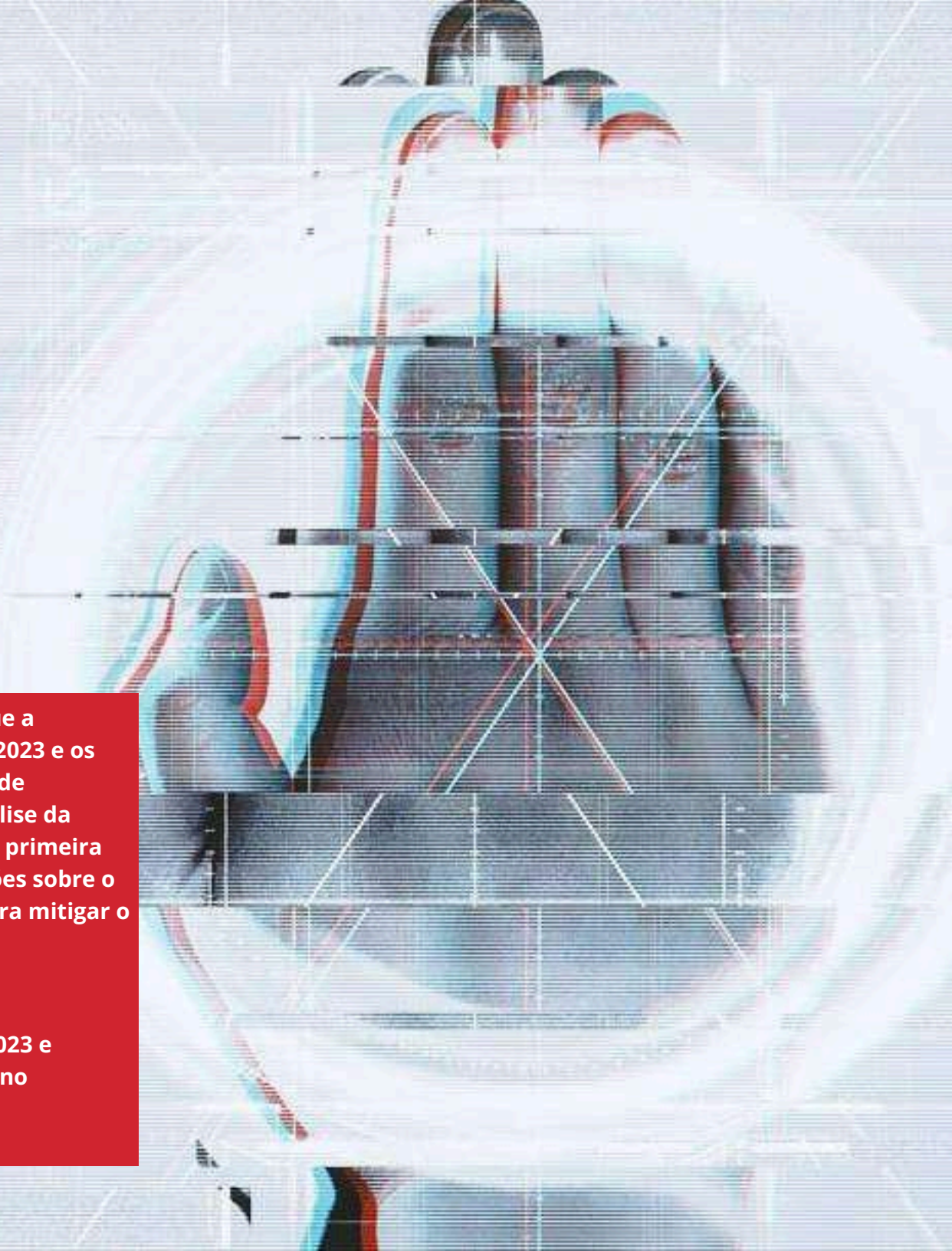
# INTRODUÇÃO

As grandes e pequenas organizações estão cada vez mais buscando alavancar uma boa inteligência de ameaças para atualizar suas infraestruturas de segurança cibernética em tempo real e maximizar a proteção das comunicações, pessoas e dados de seus negócios.

A Mimecast gera inteligência de ameaças por meio de sua análise de mais de um bilhão de e-mails por dia em nome de mais de 42.000 clientes. Como o e-mail é o canal pelo qual a maioria das ameaças cibernéticas são lançadas, o Mimecast vê muitas ameaças novas antes que elas se tornem amplamente conhecidas.

**Este relatório apresenta insights da inteligência que a Mimecast gerou ao longo do terceiro trimestre de 2023 e os combina com inteligência externa da comunidade de segurança cibernética em geral. Ele inclui uma análise da atividade de ameaças, uma série de estatísticas de primeira linha que moldaram essa atividade e recomendações sobre o que pequenas e grandes empresas podem fazer para mitigar o risco que essas ameaças representam.**

**Convidamos você a explorar nosso relatório de inteligência de ameaças do terceiro trimestre de 2023 e estamos ansiosos para compartilhar mais insights no futuro.**



# SUMÁRIO EXECUTIVO

Os invasores que tentaram se infiltrar em empresas se concentraram em um punhado de vulnerabilidades significativas de dia zero no terceiro trimestre de 2023, mesmo quando aumentaram os ataques de personificação. Nossa pesquisa mostra que dois terços das empresas sofreram um ataque de ransomware no ano passado, quase todas (97%) foram alvos de ataques de phishing baseados em e-mail e a grande maioria (76%) das equipes de segurança em organizações em todo o mundo espera ter um ataque com consequências sérias usando e-mail como vetor.

**2/3**
Das empresas sofreram um ataque de ransomware no ano passado

**97%**
foram alvos de ataques de phishing por e-mail

## Equipe de inteligência de ameaças Mimecast

A equipe de inteligência de ameaças da Mimecast é composta por um conjunto globalmente distribuído de engenheiros, cientistas, analistas e pesquisadores de ameaças que auxiliam o Mimecast Security Operations Center (MSOC). As ameaças são monitoradas continuamente em mais de um bilhão de e-mails por dia, e os especialistas em segurança cibernética da Mimecast analisam, investigam ataques e testam a eficácia para desenvolver inteligência de ameaças sofisticada e oportuna que aplica a proteção mais recente em todas as soluções de segurança da Mimecast.

# PRINCIPAIS CONCLUSÕES

**Aumento de impersonificação,** tornando-se mais sofisticado à medida que grupos cibercriminosos oportunistas o utilizavam para obter acesso inicial às organizações visadas.

**A exploração de vulnerabilidades de dia zero se tornou uma ameaça maior**, com invasores mirando falhas no MOVEit, diversas vulnerabilidades de dia zero em softwares da Microsoft e navegadores e aplicativos que usam as bibliotecas de imagens de código aberto libvpx e libwebp, entre outros problemas.

Empresas de recursos humanos, software e serviços de tecnologia da informação e serviços financeiros (especialmente bancários) **viu o maior número de ameaças por usuário.** Níveis consistentemente altos de atividade de ameaça também foram detectados contra os setores de manufatura, transporte, armazenamento e entrega, além de varejo e atacado.

**A Mimecast recomenda que os profissionais de segurança e gestores de risco** revisem seus acordos de nível de serviço para definir níveis mínimos de segurança de dados e segurança cibernética e encontrem maneiras de monitorar os fornecedores mais de perto. Os alvos de aquisição devem estar sujeitos a um escrutínio extra de segurança cibernética.

As organizações devem **configurar sua infraestrutura de e-mail** para bloquear o carregamento automático de imagens, pois esperamos que os invasores usem cada vez mais tipos de arquivos de imagem como portadores de malware e conteúdo malicioso, como códigos QR que levam a sites maliciosos.

# SURTO DE DIA ZERO, NUVENS ATACADAS

**Várias ameaças de dia zero surgiram durante o terceiro trimestre de 2023, e os agentes de ameaças aumentaram seu foco crescente em plataformas e aplicativos de nuvem. Também vimos vários grupos de criminosos cibernéticos fazerem mudanças estratégicas notáveis no trimestre.**

Profissionais de segurança continuaram enfrentando violações generalizadas causadas por uma vulnerabilidade crítica na plataforma de transferência de arquivos gerenciada MOVEit, que começou no segundo trimestre, no final de maio.

Então, o grupo de ransomware Cl0p usou a vulnerabilidade não revelada anteriormente para comprometer pelo menos 200 — e mais provavelmente, 400 ou mais — empresas. As divulgações de violações continuaram a surgir durante o terceiro trimestre. Muitas das vítimas ~~forneceram serviços para organizações clientes, o que~~ expandiu o impacto das violações de dados para mais de 2.300 organizações.

Outros relatórios de novas vulnerabilidades de dia zero no trimestre incluíram fraquezas críticas de segurança nas bibliotecas gráficas de código aberto libvpx1 e libwebp2, que provavelmente serão incorporadas em ferramentas de invasores daqui para frente. As vulnerabilidades nas duas bibliotecas gráficas de código aberto podem expor o Google Chrome, o Mozilla Firefox e centenas de aplicativos.

Embora o Cl0p seja um grupo criminoso oportunista, atores patrocinados e vinculados ao estado continuaram a participar do componente cibernético da invasão da Ucrânia pela Rússia. Grupos afiliados à Rússia, como Anonymous Sudan e Killnet, tiveram como alvo agências governamentais e empresas afiliadas aos aliados da Ucrânia, enquanto hackers chineses roubaram com sucesso uma chave de assinatura de consumidor da Microsoft em julho

Tanto grupos criminosos quanto grupos apoiados pelo país continuaram a tendência de visar serviços de nuvem, seguindo muitas empresas que mudaram operações de TI e outros serviços para a nuvem.

1. CVE-2023-5217 Detail, NIST National Vulnerability Database.
2. CVE-2023-4863 Detail, NIST National Vulnerability Database.

O phishing de credenciais se tornou um foco importante de ataques baseados em e-mail, e grupos de ameaças estão encontrando maneiras — como movimento lateral baseado em SQL e phishing de consentimento — de contornar a segurança básica da principal tríade de serviços de nuvem: Amazon Web Services, Google Cloud e Microsoft Azure. Além disso, plataformas de software de colaboração baseadas em nuvem, como Microsoft Teams e Slack, se tornaram canais para ataques de phishing e outras tentativas de roubo de credenciais, com ataques aumentando por meio dessas plataformas durante o terceiro trimestre de 2023.

Enquanto isso, grupos de ameaças enfrentando seus próprios desafios fizeram mudanças na estratégia. O grupo LockBit pareceu cessar a atividade por uma semana em agosto e pode ter sido comprometido. O grupo de ransomware Snatch Team mudou sua estratégia e começou a comentar sobre suas violações bem-sucedidas, apontando deficiências nas defesas cibernéticas das vítimas para pressionar as empresas a pagar resgates. As deficiências de segurança das organizações de denúncia fornecem munição que as seguradoras podem usar para evitar pagamentos, bem como combustível para possíveis processos judiciais. No final de agosto, uma operação multinacional de aplicação da lei e da indústria privada interrompeu o grupo de malware Qakbot e sua infraestrutura associada — usada por muitas gangues de ransomware para atingir vítimas — e cooptou a rede para distribuir código para remover o malware dos computadores afetados.

**76%**

esperam que um comprometimento sério baseado em e-mail tenha impacto em sua empresa este ano

**72%**

antecipam um ataque semelhante por meio de suas ferramentas de colaboração

Olhando para o futuro, a preocupação dos profissionais de segurança com ataques baseados em e-mail continua alta, com 76% esperando que um comprometimento sério baseado em e-mail impacte sua empresa este ano e 72% antecipando um ataque semelhante por meio de suas ferramentas de colaboração. Empresas de capital aberto podem se ver como alvos com mais frequência, à medida que grupos de ransomware consideram se as novas regras da Securities and Exchange Commission para divulgação de violações tornarão as empresas mais propensas a pagar resgates.

# TERCEIRO TRIMESTRE DE 2023 EM GRÁFICOS

## Aumento nas ameaças para empresas de médio porte

**01**

Pequenas e médias empresas enfrentam um número maior de ameaças do que suas concorrentes maiores.

## Aumento de impersonificação

**02**

Os ataques de impersonificação se tornaram mais sofisticados à medida que grupos de criminosos cibernéticos oportunistas os utilizavam para obter acesso inicial às organizações visadas.

## PPDFs ainda dominam, Excel se torna mais comum

**03**

O uso de formatos PDF e Microsoft Excel por invasores está crescendo. Nossos dados mostram que o uso de arquivos PDF maliciosos por invasores aumentou em 158% no terceiro trimestre de 2023 em relação ao trimestre anterior, enquanto o uso de vários formatos Excel aumentou em 86%.

## Principais indústrias visadas

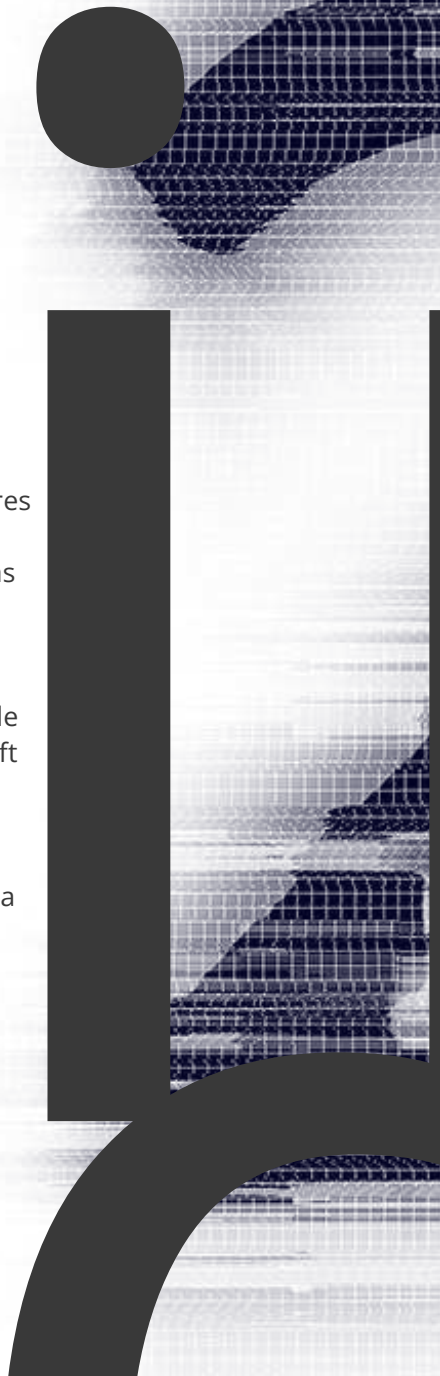
**04**

Empresas de recursos humanos, software e serviços de tecnologia da informação e serviços financeiros (especialmente bancários) viram as maiores ameaças por usuário. Níveis consistentemente altos de atividade de ameaça também foram detectados contra a fabricação,transporte, armazenamento e entrega, varejo e atacado.

## Vulnerabilidades de anexos

**05**

A maioria dos invasores confiou na exploração de duas vulnerabilidades usando anexos maliciosos: uma falha no editor de equações do Microsoft Office (CVE-2018-0802) e um desvio dos recursos de segurança do Microsoft Office (CVE-016-76).



# 01 Taxas de ocorrência: aumento nas ameaças para empresas de médio porte

Usuários em pequenas e médias empresas enfrentam um número maior de ameaças do que as maiores, porque invasores oportunistas tendem a ver empresas menores como alvos mais fáceis para campanhas de phishing e ransomware. Além disso, devido ao seu tamanho menor, ameaças de e-mail direcionadas a grupos internos específicos — como contadores ou desenvolvedores — terão um impacto descomunal em empresas menores.

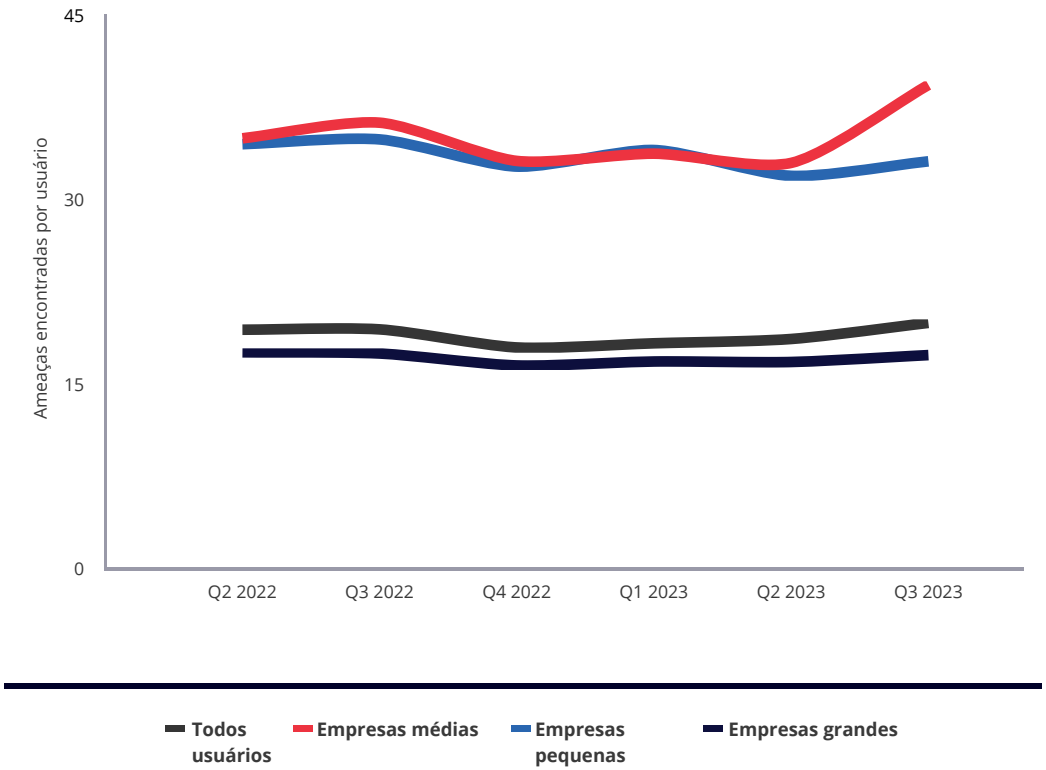
Empresas de médio porte, especificamente, observaram mais ameaças por usuário no terceiro trimestre (veja a Figura 1), com o Mimecast bloqueando quase 40 e-mails maliciosos para cada usuário por trimestre, acima dos 33 do trimestre passado.

Para CISOs e gerentes de segurança, esse número aparentemente modesto de ameaças pode rapidamente sobrecarregar seus recursos quando multiplicado por toda a base de funcionários — especialmente porque os invasores precisam apenas de um único sucesso.

Esse aumento nas ameaças por usuário (TPU) provavelmente se deve a uma combinação de fatores: os invasores veem as empresas de médio porte como uma combinação lucrativa de vulnerabilidade e potencial valor em dinheiro, e elas geralmente são bons pontos de partida de terceiros para comprometer empresas parceiras maiores.

**FIGURA 1 - Usuários em empresas de médio porte viram mais ameaças**

Empresas pequenas (linha azul) e médias (linha vermelha) veem mais ameaças em média a cada trimestre, mas no terceiro trimestre, usuários em empresas de médio porte viram um aumento significativo nas ameaças.




3. As Attacks Rise, SMBs Need a Cybersecurity Playbook, Mimecast Cyber Resilience Insights Blog

## 02 Taxas de ocorrência: impersonificação em ascensão

Em média, os usuários viram mais ameaças não spam e não malware no terceiro trimestre de 2023 em comparação ao segundo trimestre de 2023. Enquanto o número de mensagens de spam encontradas pelo usuário médio aumentou 7% no terceiro trimestre em relação ao trimestre anterior, tanto o número de tentativas de representação quanto os links maliciosos enviados a cada usuário aumentaram em dois dígitos — 12% e 22%, respectivamente. No geral, as URLs continuam sendo uma ameaça menos frequente do que a representação, que rivaliza com o spam como o tipo de ataque de e-mail mais encontrado.

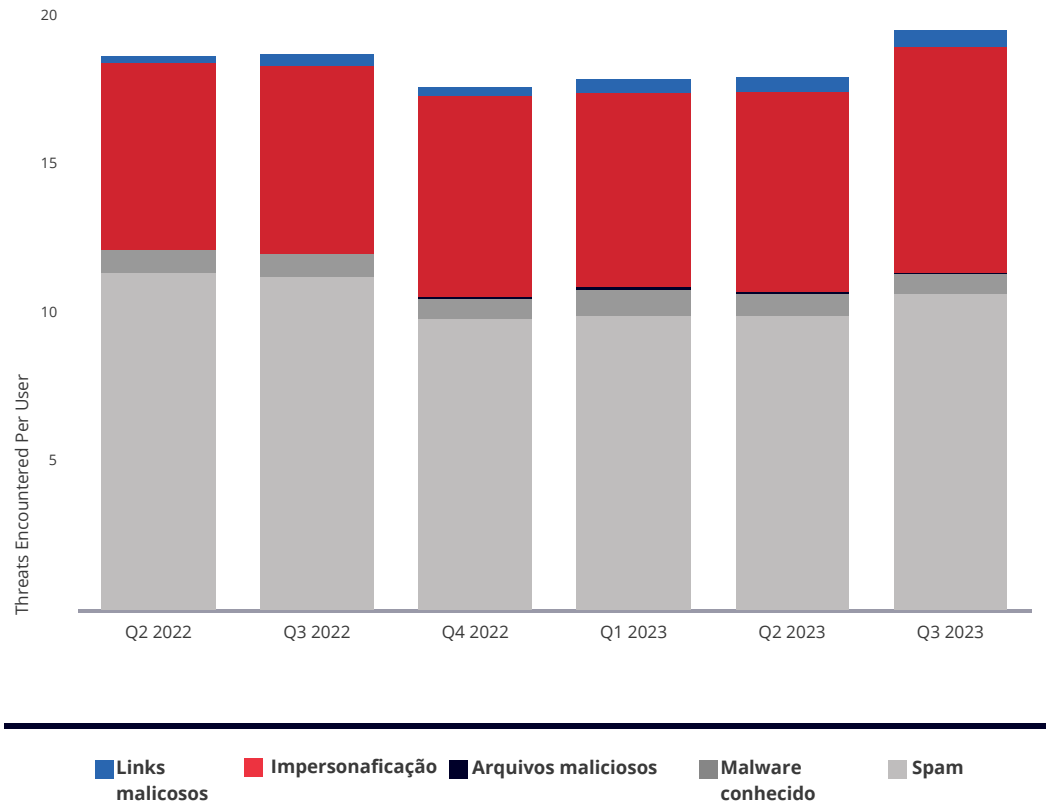
Ataques de personificação são uma tática-chave de grupos ligados ao estado que buscam estabelecer acesso inicial em redes-alvo, e o componente cibernético da invasão da Ucrânia pela Rússia provavelmente contribuiu para o aumento dos ataques de personificação. Tradicionalmente, as táticas russas têm como alvo um adversário ou região específica; mas como outros países estão ajudando na defesa da Ucrânia, os ataques agora parecem estar abrangendo alvos mais amplos. Na verdade, os ataques direcionados a organizações fora da Ucrânia superam em número aqueles contra alvos ucranianos. O resultado é um transbordamento de ataques de e-mail maliciosos para outras regiões — 116 ataques relacionados a conflitos cibernéticos tiveram como alvo a Ucrânia no segundo trimestre, em comparação com 489 ataques direcionados a organizações em outros países, como Polônia, Alemanha e França. Isso se assemelha ao impacto generalizado do NotPetya em 2017.

Grupos de criminosos cibernéticos oportunistas também estão adotando a impersonificação como técnica principal para obter acesso inicial às redes visadas.

A tecnologia Mimecast filtra e-mails perigosos conforme são detectados. Por exemplo, ataques de impersonificação neutralizados pela camada de spam nunca são vistos pela camada de detecção de personificação e, portanto, não são incluídos na parte vermelha de cada barra na Figura 2.

**FIGURA 2 - Aumentam os ataques com uso de impersonificação e links maliciosos**

Os usuários observaram mais ameaças usando spam, representação falsa e links maliciosos no terceiro trimestre de 2023.



# 03 Anexos: PDFs ainda dominam, formatos Excel se tornam mais comuns

Os usuários veem relativamente poucos anexos maliciosos devido ao sucesso das defesas atuais. No entanto, o uso de formatos PDF e Microsoft Excel pelos invasores está crescendo. Parte do motivo para as baixas taxas de encontro de anexos é que os invasores geralmente os usam contra alvos específicos em ataques de spear phishing ou comprometimento de e-mail comercial (BEC), com foco em executivos e departamentos de contabilidade.

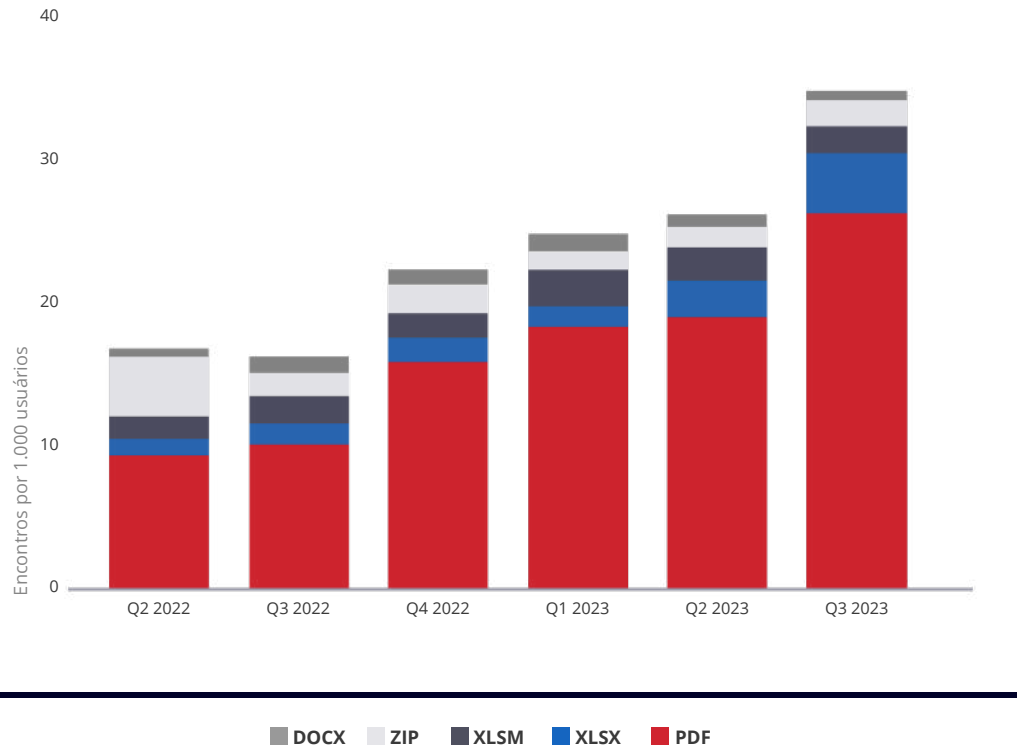
Nossos dados mostram que o uso de arquivos PDF maliciosos por invasores aumentou em 158% no terceiro trimestre de 2023 em relação ao trimestre anterior,
enquanto o uso de vários formatos do Excel aumentou em 86%. Os documentos do Microsoft Word usados em ataques mal-intencionados diminuíram 46%.

No geral, a Mimecast vê os invasores reduzindo sua dependência de malware enviado como arquivos anexados em favor de links que podem ser modificados dinamicamente. Os links dão ao invasor a capacidade de alterar a carga útil em tempo real e implantar recursos secretos adicionais.

Os dados sobre ataques baseados em anexos vêm do terceiro nível de proteção do Mimecast, Attachment Protect, que interrompe as tentativas de ataque mais sofisticadas que escapam das detecções de primeiro e segundo níveis. Como resultado, o número de ameaças por usuário é menor do que você pode esperar.

**FIGURA 3 - Anexos maliciosos em PDF e Excel aumentam**

Os usuários estão vendo mais arquivos PDF (vermelho) e formatos Excel (tons de azul) como anexos maliciosos (por 1.000 usuários)



# 04 Visão geral do setor: segmentação de operações comerciais

Os invasores retornaram aos alvos pré-pandêmicos no terceiro trimestre de 2023, concentrando-se nos grupos internos e serviços externos que são essenciais para as operações comerciais. Seus principais alvos eram empresas de recursos humanos, software e serviços de tecnologia da informação e serviços financeiros, especialmente bancários.

Usuários comuns nesses setores encontraram ameaças em uma taxa muito acima da média de todos os setores da indústria. Houve 9,3 ameaças por usuário (TPUs) em
recursos humanos e recrutamento, 5,5 (TPUs) para software e serviços de TI e 4,1 (TPUs) em serviços bancários.

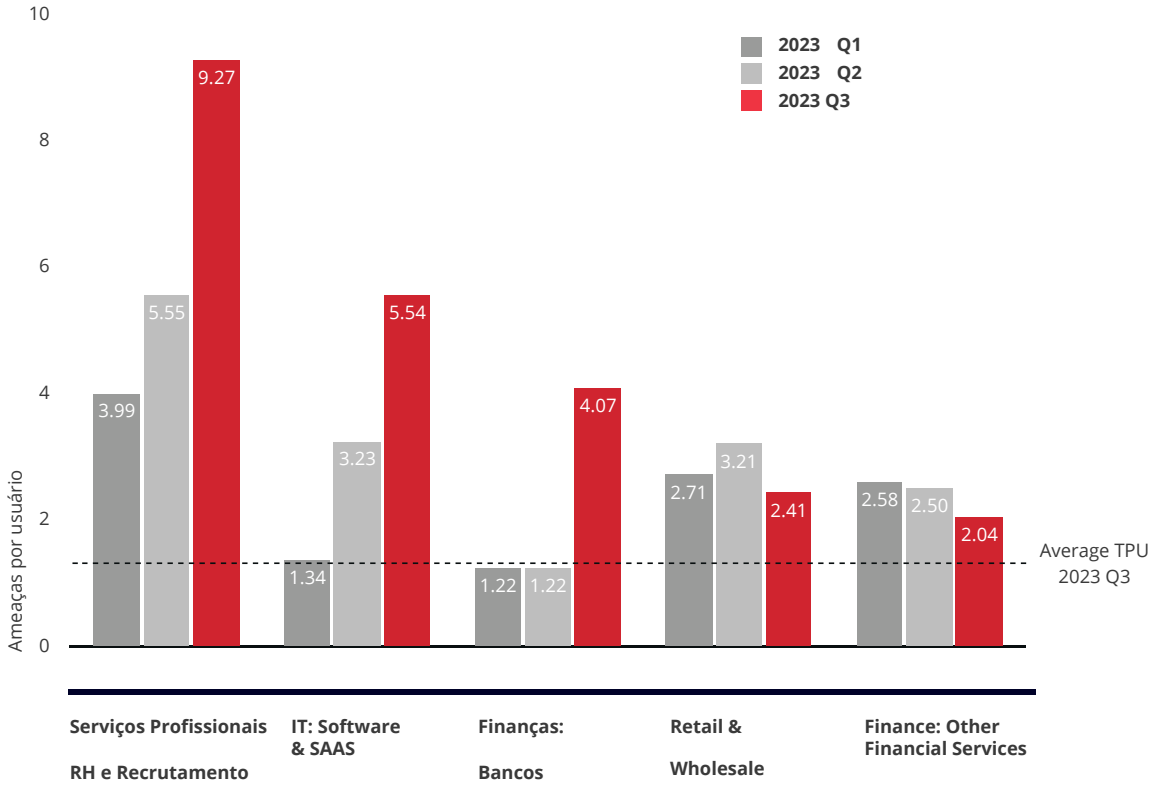
Serviços de TI e serviços bancários ficaram em segundo e terceiro lugar neste trimestre e tiveram muito menos atividade nos trimestres anteriores.

A Mimecast tem visto níveis consistentemente altos de atividade de malware sustentada em volume desde o início da pandemia. Isso agora está se normalizando de volta para os alvos criminosos e financeiros oportunistas como RH, bancos, serviços de TI e jurídicos.

Essa tendência tem sido aparente, mas gradual desde o início de 2023. O setor de varejo e atacado ficou em quarto lugar em ataques contra seus usuários no terceiro trimestre de 2023.

**FIGURA 4 - Visão geral do setor: segmentação de operações comerciais**

Empresas do setor de RH e recrutamento enfrentaram sete vezes mais ameaças por usuário do que uma empresa média.



# 05 Visão geral das vulnerabilidades: o ataque de e-mail mais comum usa falha de 5 anos

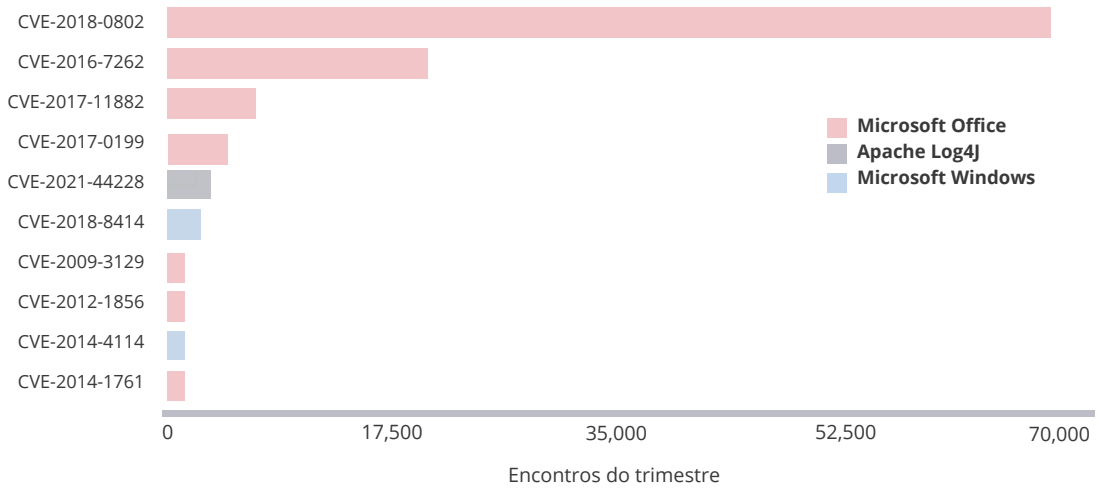
A maioria dos invasores confiou na exploração de duas vulnerabilidades — ambas com pelo menos cinco anos — usando anexos maliciosos: uma falha no editor de equações do Microsoft Office (CVE-2018-0802) e um desvio dos recursos de segurança do Microsoft Office (CVE-2016-7262). Como os anexos são escaneados somente após passar por outras verificações, como proteções contra spam, os dados de ameaças incluídos aqui representam os ataques mais sofisticados.

Dados da Agência de Segurança Cibernética e de Infraestrutura dos EUA (CISA) mostram que muitas vulnerabilidades encontradas por empresas não chegam em e-mails, mas têm como alvo dispositivos e servidores.

Por exemplo, entre os problemas de segurança mais explorados em 2022 estavam uma exposição de credencial SSL em dispositivos de rede privada virtual (VPN) da Fortinet, três problemas no Microsoft Exchange Server e um desvio de autenticação no Zoho ManageEngine.

**FIGURA 5 - Principais vulnerabilidades encontradas em ataques baseados em e-mail**

Duas vulnerabilidades foram responsáveis pela maioria dos anexos maliciosos, ambas com pelo menos cinco anos.



# SEGURANÇA NATIVA NÃO É SUFICIENTE

Além dessas vulnerabilidades, a Microsoft representa a maior parte dos serviços de e-mail de terceiros. Algumas empresas passaram a confiar na segurança nativa fornecida pelo Google Workspace e Microsoft 365; mas como os dois serviços respondem por 95% de toda a adoção de e-mail na nuvem, os invasores estão constantemente e ativamente buscando maneiras de contornar sua segurança e atingir seus usuários.

Por esse motivo, sua segurança nativa não é suficiente. Os invasores já encontraram maneiras de contornar muitas de suas defesas. Uma pesquisa conduzida por uma empresa de seguros cibernéticos descobriu que empresas que usam serviços de e-mail em nuvem — como Microsoft 365 ou Google Workspace — veem menos ataques do que aquelas que usam servidores de e-mail locais, mas que empresas que usam soluções de segurança de e-mail de terceiros melhoraram ainda mais o desempenho.

**As empresas reconhecem a necessidade de fechar lacunas em serviços de segurança nativos, com 94% dos líderes de segurança buscando melhores proteções de segurança do que aquelas que vêm com seus serviços de e-mail em nuvem. O Mimecast foi a solução de segurança de e-mail com melhor desempenho, com seus usuários enviando 22% menos reivindicações à seguradora do que a organização média.**

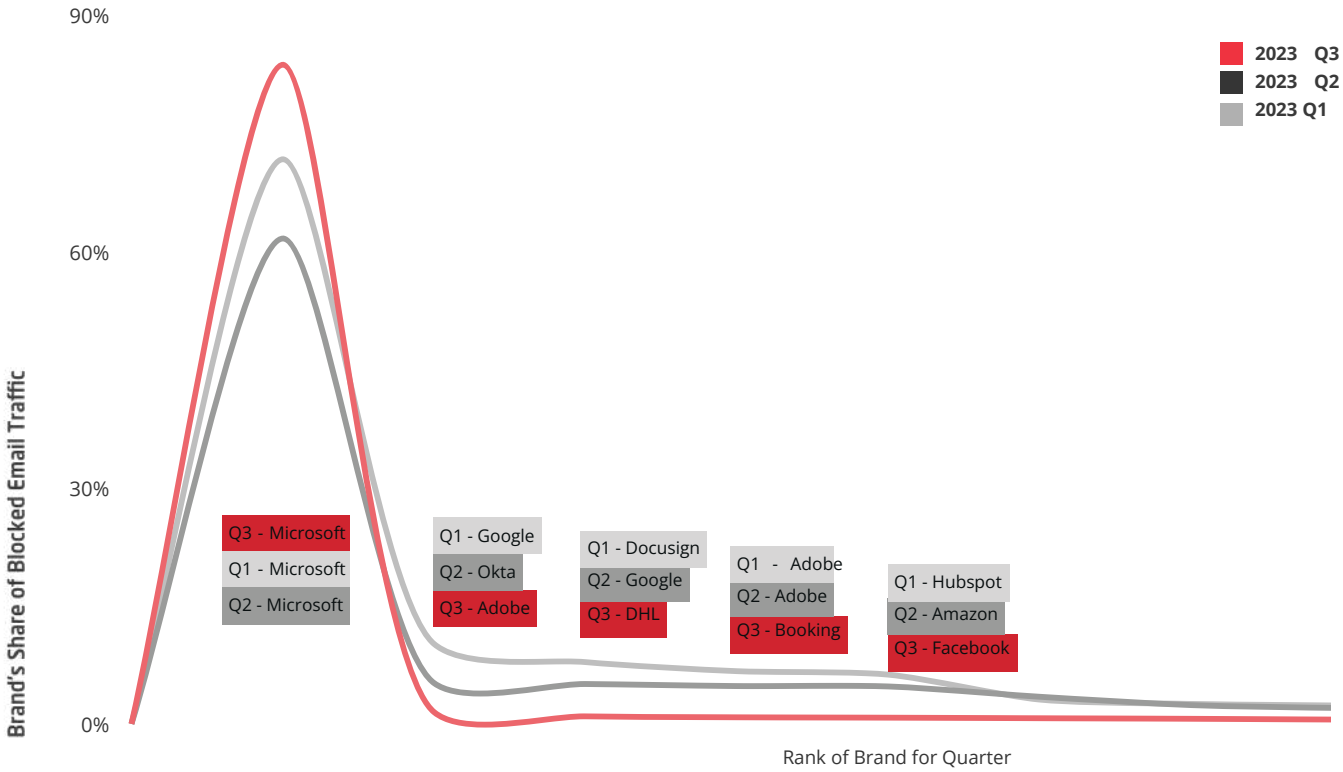
## Os atacantes movem-se mais rápido que as plataformas

Os cibercriminosos estão explorando vulnerabilidades conhecidas para lançar ataques muito mais rápido do que a maioria das organizações consegue corrigir seus sistemas. O Known Exploited Vulnerabilities (KEV) Catalog, por exemplo, documenta quais vulnerabilidades os invasores já exploraram, com 188 vulnerabilidades de 2021, 120 de 2022 e 78 de 2023 exploradas pelos invasores até o momento. Apenas um punhado de vulnerabilidades, no entanto, é responsável pela maioria dos ataques por e-mail, tornando a inteligência de ameaças uma chave para saber quais explorações são mais comuns e para ajudar a fortalecer a rede e os usuários contra elas.

Acompanhar quais vulnerabilidades foram exploradas, como se defender contra os ataques e quais exploits estão sendo usados atualmente para infectar usuários não é apenas uma tarefa difícil e cada vez mais complexa, mas também é uma tarefa que as equipes de segurança muitas vezes não têm tempo para fazer corretamente.

**FIGURE 6 - Microsoft dominates brand impersonation, even more so in Q3**

Email attacks impersonating the Microsoft brand dominated phishing and BEC lures.




Os provedores de serviços de e-mail normalmente não têm foco intenso em segurança para processar a inteligência necessária e fornecer proteção para seus clientes. Para minimizar os riscos baseados em e-mail, as empresas devem seguir as melhores práticas de segurança em camadas para o principal vetor de ataque — e-mail.

## Serviços de segurança de terceiros trazem foco e expertise

Os invasores estão usando cada vez mais os serviços de nuvem dos principais provedores para lançar ataques, com uma quantidade crescente de spam e phishing vindo de domínios públicos, como gmail.com e outlook.com.

Mimecast bloqueia milhares de mensagens de e-mail maliciosas direcionadas a contas do Microsoft 365 todos os dias, utilizando seus próprios serviços, como o Microsoft Dynamics 365 Customer Voice (veja Figura 7 e 8). Esses ataques — junto com aqueles de outros serviços públicos, como gmail.com e yahoo.com — podem ser difíceis para o trabalhador médio diferenciar em um ataque de phishing sofisticado.

Em julho, a Mimecast viu um grande pico de e-mails originados de contas comprometidas do O365 que continham anexos .eml. Embora essa não seja uma técnica nova, os agentes de ameaças continuam a usar esses métodos para contornar soluções de segurança. Para aumentar suas chances de sucesso, os invasores geralmente usam várias camadas dentro dessas campanhas, como ofuscação dentro do JavaScript.

Várias variações dessa ameaça com um anexo .eml incorporado foram vistas no último trimestre, usando empresas respeitáveis e outras iscas para atingir o mesmo resultado.

**FIGURA 7 - Ataques personificando domínios da Microsoft**
Mimecast registra milhares de ataques usando contas do Microsoft 365 diariamente.

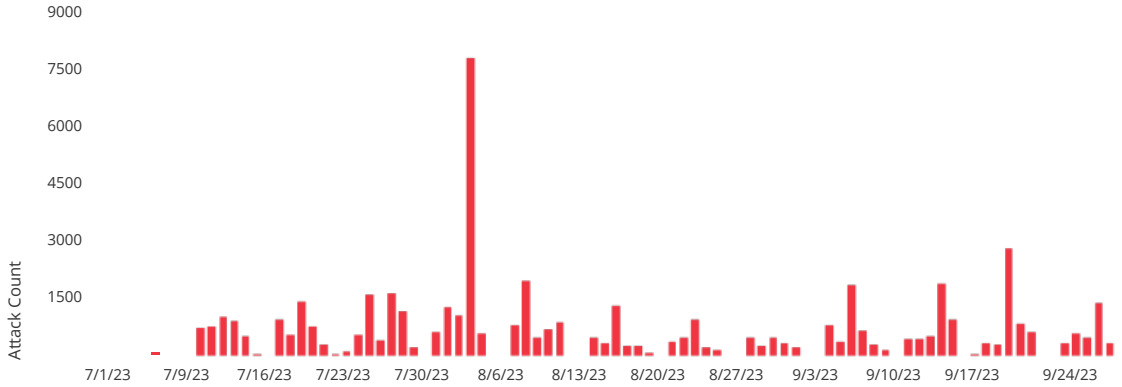



**FIGURA 8 - Página de phishing de voz do cliente do Microsoft 365 Dynamics**

Embora usuários individuais possam — e devam — ser educados sobre como usar o e-mail com mais segurança, a tecnologia apoiada por inteligência de ameaças de terceiros pode proteger os usuários e suas empresas de ataques baseados em e-mail de forma mais consistente.

As empresas, por exemplo, devem garantir que estão protegendo seus e-mails e canais de colaboração usando o protocolo de autenticação de e-mail DMARC para evitar que suas marcas sejam cooptadas para uso em ataques de spear phishing.

Além disso, abrir links em ambientes isolados pode impedir um ataque de phishing de credenciais bem-sucedido.

No final, provedores de serviços de e-mail, como Microsoft 365 e Google Workspace, fazem um ótimo trabalho entregando e-mails e até mesmo reduzindo spam. No entanto, gerenciar a segurança dos seus usuários requer mais:

## Um provedor de segurança focado em proteger empresas e trabalhadores contra ameaças em constante evolução.

# AVALIAÇÃO DE AMEAÇAS

Os agentes de ameaças continuam a se concentrar em expandir as maneiras pelas quais podem obter acesso inicial às empresas, incluindo a adoção de software de colaboração — como o Microsoft Teams — e a expansão de suas técnicas Living off the Land (LotL) para incluir uma variedade maior de programas. O mercado paralelo continua a produzir ferramentas mais avançadas — o terceiro trimestre viu a popularidade crescente de uma plataforma de phishing personalizada usada por pelo menos 500 agentes de ameaças.

Alguns sucessos notáveis em frustrar agentes de ameaças incluem a derrubada do botnet Qakbot por um grupo multinacional de autoridades policiais e empresas do setor privado, e o fato de que a pressão sobre agentes cibercriminosos para diminuir os resgates se tornou tão forte que pelo menos um grupo (LockBit) está considerando impor limites às suas afiliadas para negociar os valores dos resgates.

Além disso, o grupo Emotet pausou mais uma vez suas operações, mas se isso pode ser considerado um sucesso para os defensores não está claro, já que o grupo já havia encerrado as operações apenas para aparecer novamente.

# PRINCIPAIS EVENTOS 2023 T3

**1 JUL**

**Campanha publicitária BlackCat**

Análise descobre que gangue de ransomware BlackCat está usando "malvertising" para obter acesso inicial a redes de negócios.

**3 JUL**

**Emotet Hiberna?**

A operação Emotet parece entrar em um período de dormência novamente, de acordo com várias fontes. No entanto, o Mimecast detectou operações em andamento pelo grupo.

**13 JUL**

**TeamTNT Phishes for Credentials**

TeamTNT mira credenciais de nuvem, inicia campanha de mineração de criptomoedas.

**2 AUG**

Phishing através do Microsoft Teams

O grupo Midnight Blizzard usa inquilinos comprometidos do M365 para enviar mensagens maliciosas do Teams e credenciais de destino.

**3 AUG**

Viver da Terra Cresce Mais Popular

Os hackers estão encontrando mais maneiras de usar os arquivos executáveis presentes nos sistemas alvos — incluindo programas do Microsoft Office — para baixar códigos maliciosos..

**17 AUG**

Códigos QR em Campanhas de Phishing

Os invasores usam códigos QR para contornar soluções de segurança de e-mail e redirecionar as vítimas para sites de phishing, com foco em empresas dos setores de energia, manufatura e seguros.

**25 AUG**

Qakbot Takedown

Um esforço multinacional entre a polícia e provedores de tecnologia resultou na interrupção do malware e botnet Qakbot e na disseminação de um arquivo de desinstalação para sistemas afetados.

**Read article**

**5 SEP**

Segmentação de Grupo de Ameaças Okta SuperAdmins

Os invasores tiveram como alvo pelo menos quatro clientes Okta com campanhas de engenharia social que visavam contornar a segurança de autenticação de dois fatores protegendo as contas. O Mimecast começou a detectar os ataques em maio.

**Read article**

**6 SEP**

Kit de phishing BEC Descoberto

Pesquisadores descobrem o agente de ameaça W3LL, que estava vendendo um kit de phishing personalizado para ataques BEC e ignorando o MFA para mais de 500 outros agentes de ameaça.

**Read article**

**12 SEP**

Mais Phishing Através do Microsoft Teams

A Storm-0324 (também conhecida como TA543 e Sagrid), uma distribuidora de ferramentas de cibercriminosos, adotou amplamente iscas de phishing enviadas através do Microsoft Teams.

**Read article**

**12 SEP**

Vulnerabilidades WebP

Ameaça ataques em massa

Duas vulnerabilidades na biblioteca de imagens de código aberto WebP usada por navegadores, clientes de e-mail e outros aplicativos já foram exploradas por atores de estados-nação, ataques que prenunciam comprometimentos potenciais por meses, se não anos, conforme os consumidores corrigem.

**Read article**

**18 SEP**

Afiliados cibercriminosos Resgates com preços baixos?

Preocupado que muitos "afiliados" estejam descontando resgates, o grupo de ransomware LockBit discute a imposição de um resgate mínimo definido em 3% da receita anual da empresa vítima.

**Read article**

**26 SEP**

A técnica ZeroFont

Vê ressurgimento

TA tática de phishing de texto de tamanho de fonte zero incorporado passou por alguns refinamentos e agora tenta fazer com que os e-mails pareçam mais confiáveis usando texto de fonte zero no início da mensagem — texto que geralmente aparece na lista de mensagens de clientes de e-mail populares..

**Read article**

# Principais Avisos

Fontes do governo emitiram muitos avisos focados na segurança de e-mail durante o trimestre, incluindo avisos de um aumento nos ataques ao Outlook Online e descrições de extorsão de retorno rápido e golpes de criptomoeda.

Além disso, pesquisadores do governo observaram que muitos ataques de ransomware continuam a depender de técnicas bem compreendidas para monetizar qualquer comprometimento inicial da rede de uma organização.

**6 DE JULHO [NCSC] Active Cyber Defense (ACD) – O sexto relatório anual**

O número de sites maliciosos derrubados pelo governo do Reino Unido caiu em 2022 para 1,8 milhão de campanhas e 2,4 milhões de URLs, de 2,7 milhões de campanhas e 3,1 milhões de URLs em 2021. Embora a frequência de ataques tenha permanecido estável, os servidores por trás de e-mails de extorsão e golpes de investimento em criptomoedas têm tempos de atividade curtos (1 hora a 1 dia, em média), resultando no fim dos ataques antes que pudessem ser derrubados.

**Reference**

**112 DE JULHO [CISA] Monitoramento aprimorado para detectar atividade APT visando o Outlook Online**

A Agência de Segurança Cibernética e de Infraestrutura dos EUA (CISA) e o Federal Bureau of Investigation (FBI) alertaram as agências de infraestrutura crítica que grupos de ameaças persistentes avançadas (APT) começaram a visar o Outlook Online com ataques usando uma chave de consumidor de conta da Microsoft (MSA) para falsificar tokens.

**Reference**

**30 AUG [CISA, FBI] Identificação e interrupção da infraestrutura do QakBot**

A CISA e o FBI divulgaram um comunicado conjunto após a derrubada do botnet Qakbot em 25 de agosto. O comunicado incluiu uma descrição da derrubada, que cortou as conexões entre os servidores de comando e controle e as máquinas das vítimas, bem como indicadores de comprometimento. O FBI trabalhou com parceiros da indústria para compartilhar informações,incluindo indicadores de comprometimento, para ajudar os defensores a detectar infecções do Qakbot e remediar comprometimentos.

**Reference**

**11 SEP [NCSC, NCA] Ransomware, extorsão e o ecossistema do crime cibernético**

Ransomware e malware wiper causaram grandes interrupções nas operações comerciais nos últimos cinco anos. Mostrando sua adaptabilidade, no entanto, os criminosos cibernéticos de hoje estão mais focados em monetizar violações de dados oportunistas usando técnicas de ataque bem compreendidas.

**Reference**

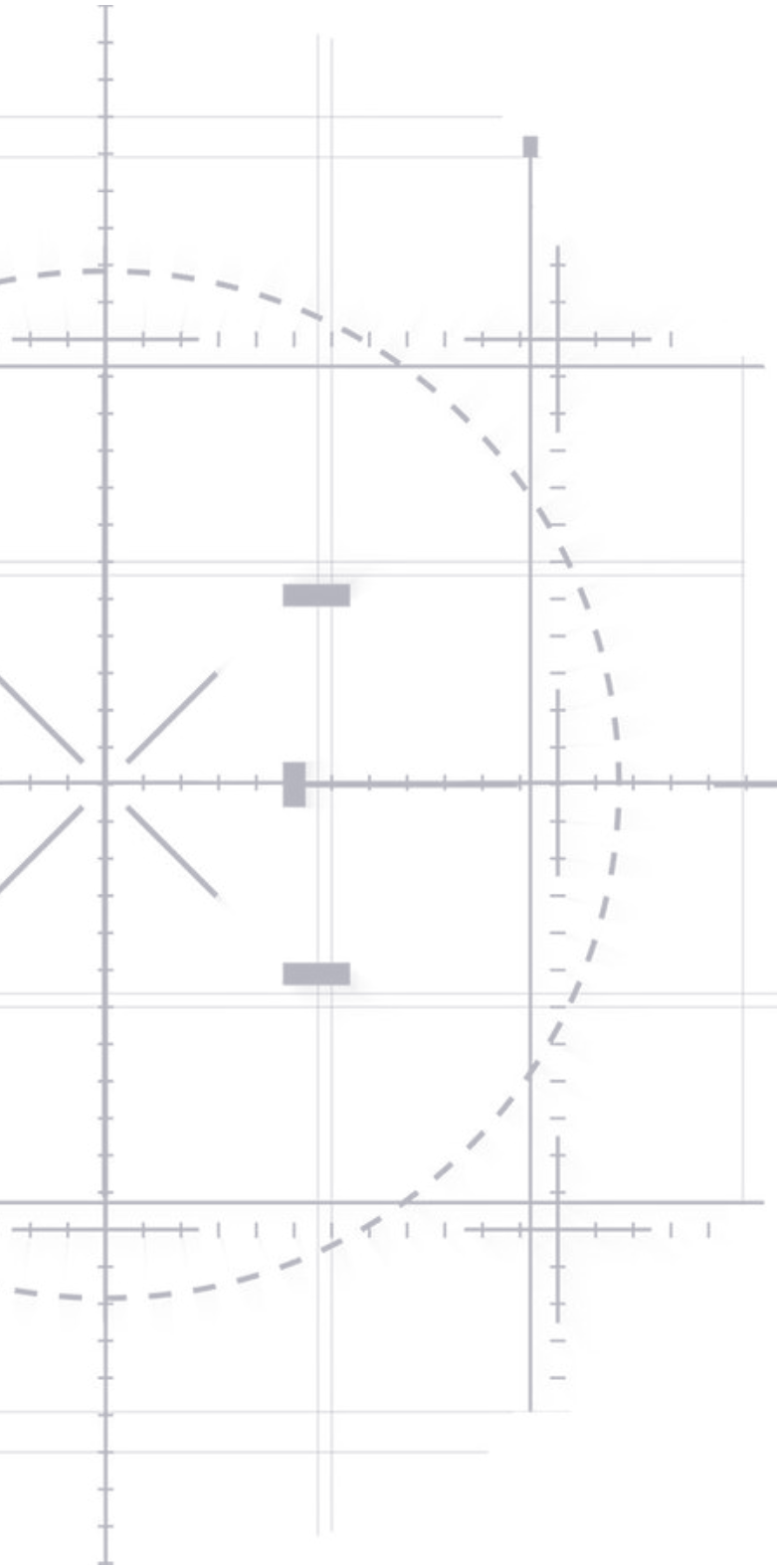
**12 SEP [NIST] Vulnerabilidades WebP (Chrome: CVE-2023-5217 e CVE-2023-4863; Apple: CVE-2023-41064)**

Tanto o Google quanto a Apple corrigiram vulnerabilidades de dia zero na biblioteca libwebp que estavam sendo exploradas por agentes estatais-nação. A biblioteca não é usada apenas por navegadores; ela também é usada por outros aplicativos, incluindo aqueles em dispositivos móveis, que podem não ser atualizados tão rapidamente quanto outros softwares de consumo.

**Reference**

COMO AGIR

# 5a



# Contramedidas específicas para ameaças

### Exija mais segurança de terceiros

Ataques contra organizações nos setores de fabricação, transporte, armazenamento e entrega, varejo e atacado representam risco significativo de terceiros de comprometimento da cadeia de suprimentos. As organizações devem revisar seus acordos de nível de serviço para definir níveis mínimos de segurança de dados e segurança cibernética e encontrar maneiras de monitorar seus fornecedores mais de perto, como serviços de classificação externa, bem como sujeitar as aquisições a um escrutínio extra.

### Escanear a rede externa em busca de portas abertas

As organizações devem escanear regularmente sua rede externa para garantir que todas as portas de servidor acessíveis ao público estejam fechadas ou adequadamente protegidas e protegidas. A Mimecast observou aumentos contínuos em ataques contra portas de protocolo de desktop remoto (RDP) que foram responsáveis por 80% dos comprometimentos efetivos de ransomware. Os invasores continuarão a procurar portas RDP abertas como uma forma de comprometer as organizações..

### Bloquear imagens em mensagens de e-mail

Os invasores estão aumentando o uso de tipos de arquivo baseados em imagem como uma forma de infiltrar iscas de phishing e código malicioso enquanto evitam a detecção. A análise da Mimecast identificou agentes de ameaças também usando criptografia e texto em idioma estrangeiro, acompanhado de criptografia, dentro de imagens para escapar da atenção. As empresas devem configurar clientes de e-mail para impedir o carregamento de imagens em mensagens e isolar quaisquer imagens que os usuários solicitem explicitamente.

Observação: os usuários do Cybergraph devem aproveitar sites confiáveis para garantir que os banners sejam carregados corretamente.

### Segmente a rede e registre o tráfego interno

Os invasores, especialmente durante um ataque de ransomware, podem se mover lateralmente rapidamente por uma rede. Segmentar a rede interna e colocar ativos críticos em seus próprios enclaves pode reduzir os danos causados por ransomware e outros ataques. Monitorar o tráfego interno, especialmente as comunicações em segmentos específicos, pode resultar na detecção mais precoce de ameaças.

## Recomendações gerais para combater ameaças

**Manter backups de sistemas e dados críticos** As organizações hesitam em pagar resgates, duvidando das promessas de recuperação de dados dos grupos de ransomware. Para minimizar o tempo de inatividade e os custos após um ataque, backups robustos, especialmente de dados críticos, e testes de rotina do processo de recuperação são vitais. Em um evento de ransomware, os backups podem ser a única opção de recuperação. Os backups em nuvem geralmente produzem melhores resultados, mas as organizações devem optar pelo método de backup mais adequado.

**Aumentar a conscientização e o treinamento do usuário** Educar os usuários em técnicas atuais de phishing ajudará significativamente as empresas a frustrar ataques de phishing e roubo de credenciais. Os usuários devem ser treinados regularmente usando exemplos de ataques atuais e receber estratégias específicas para ajudar a determinar se um e-mail é suspeito. Além disso, os usuários vulneráveis devem ter treinamento focado em conjunto com políticas de segurança restritivas. Os usuários também devem ser instruídos a relatar mensagens de e-mail suspeitas à segurança de TI para ajudar a determinar quando os invasores estão mirando em indivíduos específicos.

**Fortaleça as credenciais do usuário** As ameaças Emotet e ransomware exploram senhas comuns para se infiltrar em redes. Ataques recentes destacam como senhas fracas contribuem para violações. Fortaleça qualquer rede aplicando senhas robustas, especialmente para usuários privilegiados. A segurança de TI deve eliminar senhas de administrador padrão.

**Implementar autenticação multifator resistente a phishing** Adotar um fator adicional de autenticação, especialmente uma tecnologia resistente a phishing, pode resultar em uma redução significativa em ataques baseados em credenciais, como parte de uma abordagem de confiança zero para segurança. As empresas que adicionam autenticação multifator generalizada à sua infraestrutura interna e de nuvem reduzirão seus riscos em uma ordem de magnitude.

**Priorize vulnerabilidades e aplique patches rapidamente** Embora milhares de vulnerabilidades sejam relatadas anualmente, apenas algumas são exploradas. Para aumentar a segurança, concentre-se em atualizações regulares para software crítico. A inteligência de ameaças ajuda a identificar e priorizar vulnerabilidades exploradas ativamente para aplicação de patches mais rápida. O Mimecast prevê um aumento em explorações de dia zero devido a criminosos cibernéticos adotando ferramentas avançadas como IA e aprendizado de máquina. Priorize a proteção de sistemas e softwares essenciais expostos à Internet, como VPNs e ferramentas de desktop remoto, pois eles apresentam riscos maiores.

## Recursos

**Aqui está uma lista de recursos (webinars, artigos, avisos) que os grupos de segurança podem visitar para entender melhor as ameaças e defesas.**

**CISA**
Known exploited vulnerabilities catalog
Updated Weekly

**NCSC**
Spotlight on shadow IT
27 July 2023

**CISA**
Review of the attacks associated with Lapsus$ and s related threat group report
10 August 2023

**CISA**
Open source software urity roadmap
12 September 2023

**CISA**
Phishing guidance: stopping the attack cycle at phase one
18 October 2023

# Metodologia

Os dados neste relatório são derivados da análise de mais de um bilhão de e-mails por dia monitorados pela Mimecast em nome de suas mais de 42.000 organizações de clientes globais e compilados pelo Mimecast Threat Intelligence Center.

O mecanismo de detecção de ameaças da Mimecast procede de filtros simples a cada vez mais sofisticados e elimina ameaças em cada camada conforme são detectadas. Isso significa que ameaças identificadas pela camada de spam serão interrompidas ali e não serão escaneadas por camadas subsequentes. Então, ameaças de impersonificação simples e óbvias, por exemplo, podem ser neutralizadas pela camada de spam e, portanto, não incluídas em nossos dados para impersonificações detectadas.

# Etapas específicas para clientes Mimecast

**Etapas acionáveis para proteger seus usuários das ameaças no relatório, com detalhes técnicos de nível médio.**

**Login único**

É recomendável utilizar o login único do seu provedor de identidade ou aproveitar a autenticação multifator integrada do Mimecast para reduzir a capacidade de um invasor de aproveitar o e-mail como seu vetor deataque.
**Read more**

**Proteção contra impersonificação**
Otimize a Proteção contra Representação conforme as diretrizes de melhores práticas de dois hits definidos para marcar Assunto/ Corpo e inclua uma política separada de Nível C/VIP com base na correspondência de nome com uma retenção para revisão do administrador. Além disso, crie outra política para quaisquer detecções de três hits ou mais com a ação de retenção do administrador. **Read more**

**Arquivo Seguro**

Considere o arquivo seguro para departamentos em risco que não precisam de acesso a anexos editáveis em Proteção de anexos. **Read more**

**Políticas de autenticação DNS**
Garantir que as políticas de autenticação DNS honrem os registros DMARC. Uma segunda política com escopo para um grupo de políticas com a ação DMARC Fail definida como Ignorar/ Remetentes Gerenciados e Permitidos fornecerá uma

**Caso não tenha certeza do efeito de qualquer uma das configurações propostas, entre em contato com seu gerente de conta do Mimecast, gerente de sucesso do cliente ou registre uma chamada com o suporte do Mimecast.**

bypass efetiva para qualquer e-mail legítimo que esteja sendo rejeitado/colocado em quarentena por falhas de DMARC.**Read more**

**Reescrita de URLs**

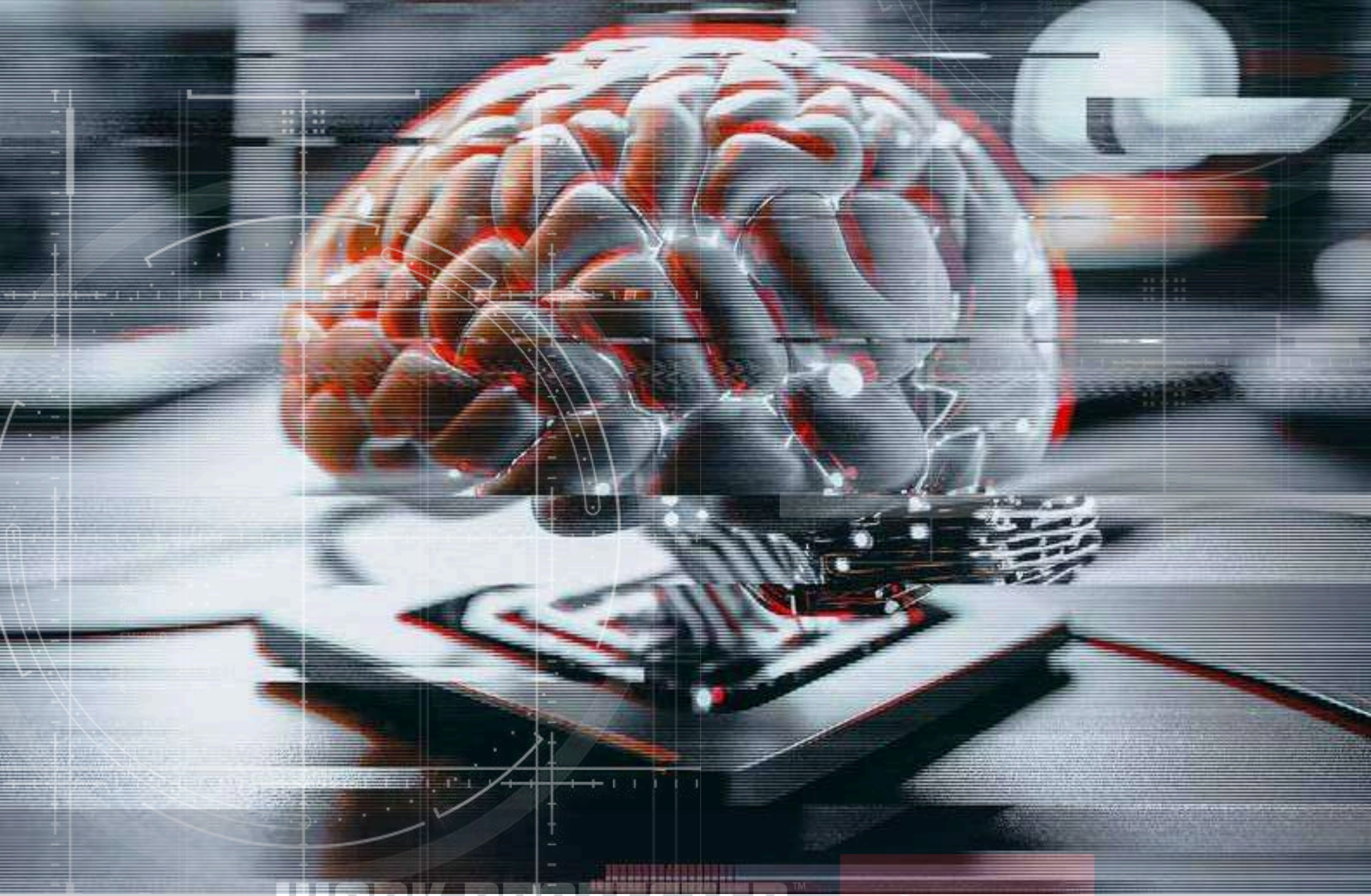
Definir uma reescrita agressiva de URLs irá garantir que todas as URLs sejam escaneadas no clique, mas esteja ciente de que qualquer coisa que pareça uma URL será reescrita, por exemplo, endereços IP e links internos.
**Read more**

**Bloqueio anti-spoofing**

Utilize o bloqueio anti-spoofing, se possível, para adicionar uma camada extra de proteção, no entanto, certifique-se de estar ciente de qualquer entidade que esteja falsificando seu domínio, pois esta política rejeitará e não reterá e-mails.
**Read more**

**Capture e revise logs** Capture e revise regularmente logs em sua conta Mimecast para aplicar políticas de segurança

**Feeds de ameaças de terceiros** Feeds de ameaças de terceiros Aproveite a inteligência de ameaças "traga sua própria" para aproveitar qualquer feed de ameaças de terceiros para rejeição automática de indicadores correspondentes.
**Read more**


WORK PROTECTED.™
Advanced Email & Collaboration Security
mimecast