SONICWALL®

RESUMO EXECUTIVO

Seus e-mails do Office 365 e do G Suite são realmente seguros?

Por que a segurança de nuvem nativa não é suficiente

RESUMO

A comunicação por e-mail baseada em nuvem do Office 365 e do G Suite está presente em todas as partes das organizações atuais. No entanto, ela também é um vetor importante para os ciberataques, que contornam a defesa nativa e os Security Email Gateways (SEGs). Este resumo examina as lacunas inerentes à segurança e os requisitos para realmente proteger o e-mail baseado em nuvem contra os ataques sofisticados atuais.

INTRODUÇÃO

Segundo um estudo do 451 Research[1], cerca de nove em cada dez organizações contam com um produto de segurança de e-mail já implantado. No entanto, quase metade dos participantes da pesquisa admite que o e-mail ainda representa a maior ameaça de dados. É uma margem muito maior em comparação com outras ameaças analisadas no estudo. E quase metade cita o e-mail como sua maior vulnerabilidade.

Os cibercriminosos que geram ameaças recebidas por e-mail são rápidos para responder a megatendências. O movimento do trabalho em casa e a COVID-19 são apenas exemplos mais recentes do que torna o tráfego de e-mail o canal ideal para ataques. Como o e-mail continua sendo nossa principal forma de comunicação e compartilhamento de dados pessoais e profissionais, bilhões de pessoas usam o e-mail diariamente. No entanto, a maioria não foi bem treinada para identificar a diferença entre e-mails legítimos e falsos, reconhecer links suspeitos ou tomar medidas cautelosas, por exemplo, autenticação da URL ou do site da empresa do remetente.

Além disso, os cibercriminosos de hoje são tão hábeis na elaboração de e-mails de phishing que pareçam ser verdadeiros, que até mesmo usuários experientes em segurança podem ser enganados. Por exemplo, ataques de phishing que imitam e-mails sobre Coronavirus, Aid, Relief e Economic Security (CARES) tiraram proveito de vítimas ansiosas e confusas durante a pandemia de COVID-19.

Com um conjunto maciço de vítimas novas e desavisadas, todas compartilhando a mesma monocultura de segurança, os hackers redirecionaram e multiplicaram seus ataques para serviços em nuvem como o Office 365 e o G Suite. Não há alvo melhor e prêmio maior, pois seus usuários combinados aumentam o crescimento em dois dígitos anualmente. Isso sem dúvida continua tornando as aplicações de e-mail em nuvem e do Office os vetores de ataque mais desejáveis e lucrativos para todos os tipos de hackers oportunistas.

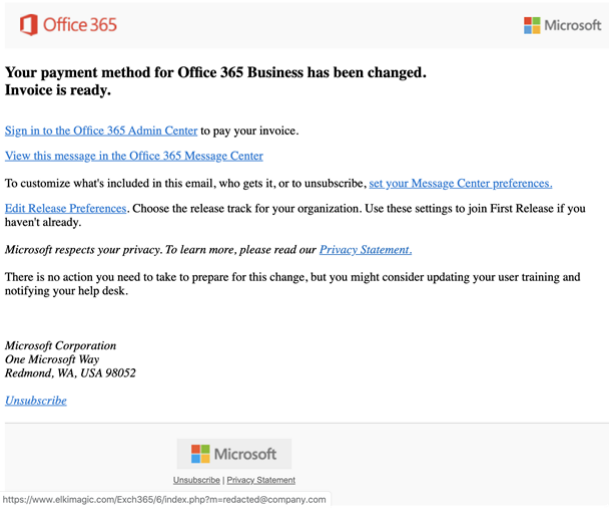
Segundo o Relatório de Investigações de Violações de Dados de 2019 da Verizon[2], 90% dos ataques foram iniciados com um e-mail de phishing. Aproximadamente 60% do tempo, o vetor da aplicação da Web comprometida era o front-end dos servidores de e-mail baseados em nuvem. Os serviços de e-mail baseados em nuvem criam vários desafios de segurança:

- A segurança de nuvem nativa não é suficiente
- Os SEGs não são desenvolvidos para a nuvem
- Os SEGs apenas protegem e-mails recebidos e enviados
- Os SEGs limitam-se a e-mails
- Os SEGs se autotransmitem aos hackers

A segurança de nuvem nativa não é suficiente

O Relatório do Microsoft ATP de 2020[3] revelou que, de mais de 500 mil mensagens analisadas, mais de um em cada dez e-mails de phishing direcionados pode chegar à caixa de entrada dos usuários. Cada ataque exclusivo utiliza vários métodos de ofuscação desenvolvidos especificamente para contornar o Microsoft ATP. Essas técnicas comprovadas incluem vários redirecionamentos, divisões de URL, manipulação de tags HTML, malware polimórfico e scripts dinâmicos ofuscados.

Embora o Microsoft ATP aplique quatro motores de políticas principais para combate ao phishing, inteligência contra falsificação, Links Seguros e Anexos Seguros, ele ainda é


Office 365

Microsoft

Your payment method for Office 365 Business has been changed.
Invoice is ready.

Sign in to the Office 365 Admin Center to pay your invoice.

View this message in the Office 365 Message Center

To customize what's included in this email, who gets it, or to unsubscribe, set your Message Center preferences.

Edit Release Preferences. Choose the release track for your organization. Use these settings to join First Release if you haven't already.

Microsoft respects your privacy. To learn more, please read our Privacy Statement.

There is no action you need to take to prepare for this change, but you might consider updating your user training and notifying your help desk.

Microsoft Corporation
One Microsoft Way
Redmond, WA, USA 98052

Unsubscribe

Microsoft

Unsubscribe | Privacy Statement

https://www.elkimagic.com/Exch365/6/index.php?m=redacted@company.com

Esses ataques são sofisticados tanto em sua técnica para chegar à caixa de entrada quanto na experiência do usuário no back-end. Cada link incluiu o endereço de e-mail do usuário para que a página de log-in que ele acessasse se parecesse com a segunda página de um desafio de conta da Microsoft, que é exatamente o que ocorre quando você tenta ir para uma página de administrador quando já está conectado. O ataque demonstrou que ele já conhecia a identidade da vítima.

A Figura 2 abaixo examina a mesma amostra de campanha de ataque em várias organizações durante o período de teste. Em quase todos os casos, se uma organização via 5 ou 50, a maioria dos e-mails mal-intencionados contornava o EOP e o ATP. Nos dois casos mostrados com a barra azul, o EOP foi capaz de bloquear o ataque, mas só depois de deixar passar mais de 30 instâncias do ataque.

A ampla adoção do Office 365 e do G Suite torna-o um alvo fácil para todos os hackers. Nunca tantas caixas de entrada tiveram segurança idêntica. Os hackers também aproveitam o fato de que essas contas na nuvem são fontes de autenticação para outras aplicações SaaS corporativas. Esse é o perigo da monocultura de segurança na nuvem. O que contorna um bloqueio contorna todos.

Os hackers têm demonstrado consistentemente sua engenhosidade para driblar a detecção por meio de ataques de phishing direcionados e escapar dos filtros de segurança dos provedores de nuvem. As organizações claramente

uma tecnologia de segurança baseada em regras, como os SEGs tradicionais. A verificação de segurança depende exclusivamente de filtragem estática baseada em reputação, da qual os hackers podem realizar engenharia reversa até encontrarem maneiras de contornar esses filtros. Com isso, as empresas são colocadas em estado de risco constante, ameaçadas pela probabilidade de alguém na organização abrir o arquivo errado, clicar na URL errada e/ou inserir uma senha no lugar errado.

Alguns ataques parecem legitimamente enviados pela Microsoft, como mostra a Figura 1 abaixo. Eles são muito bem elaborados, são personalizados profissionalmente e enviados para um conjunto específico de usuários, e não para a empresa inteira.

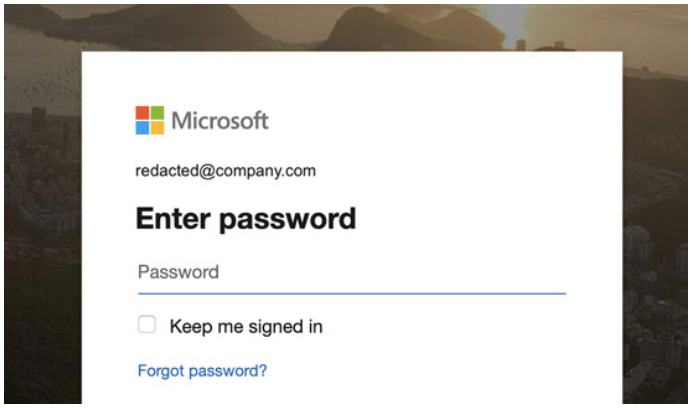


Figura 1

precisam de níveis adicionais de proteção além do Microsoft ATP e de outros SEGs.

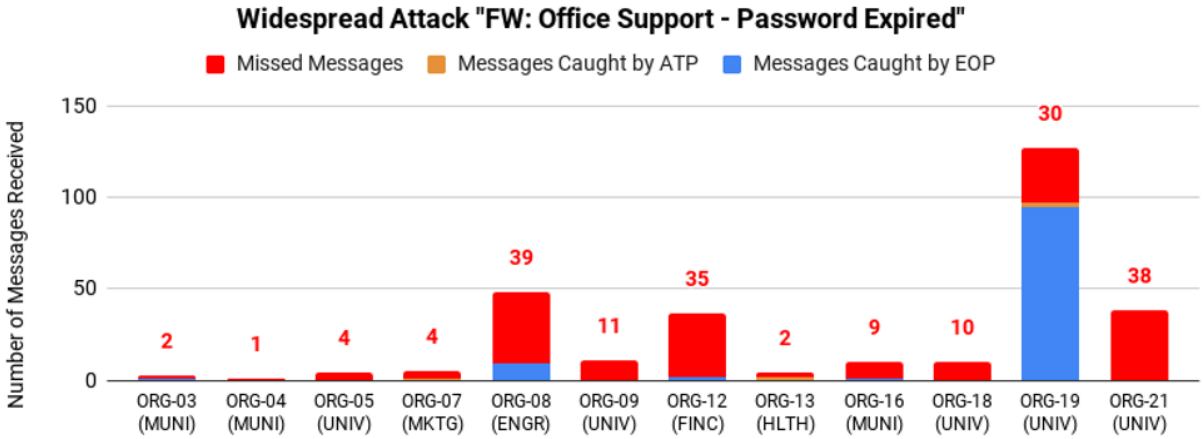
Os SEGs não são desenvolvidos para a nuvem

Os SEGs foram originalmente desenvolvidos em torno de um perímetro físico para proteger ambientes de e-mail locais. Quando o e-mail foi movido para a nuvem por meio de serviços como Office 365 Email e Gmail, os SEGs foram reajustados e adaptados para esse novo ambiente. No entanto, a abordagem sofre muitas deficiências em decorrência de seu projeto não nativo.

A maior deficiência do SEG é o impedimento à segurança atual. As alterações necessárias nos registros MX prejudicam ou apagam completamente os filtros incorporados. Isso significa que, em vez de aumentar as verificações de segurança, elas substituem completamente o padrão e, por sua vez, desativam defesas importantes dessas camadas inerentes. Além disso, como essas soluções são implantadas no perímetro, elas têm visibilidade limitada. Elas geralmente não identificam ameaças internas, como contas comprometidas e mensagens de funcionário para funcionário.

Os SEGs apenas protegem e-mails recebidos e enviados

Como os SEGs se conectam ao fluxo de e-mails fora da nuvem do provedor de e-mail, os e-mails internos não são verificados em relação a ameaças. Em um ambiente em nuvem, o comprometimento de contas é muito mais comum em



decorrência do acesso com credenciais. Os e-mails internos podem conter ameaças tanto quanto e-mails recebidos e enviados.

Alguns gateways de e-mail usam regras de histórico para verificar e-mails internos. No entanto, esse método só verifica e-mails após a entrega e não impede que os e-mails cheguem à caixa de entrada. Isso não protege os usuários adequadamente contra e-mails internos mal-intencionados, pois o destinatário pode clicar no e-mail no tempo entre a entrega e a verificação.

Os SEGs limitam-se a e-mails

O e-mail não é o único vetor de ataque em um ambiente em nuvem. O compartilhamento de arquivos, as aplicações de mensagens e outras aplicações baseadas em SaaS estão todos interconectados e oferecem canais adicionais para que ameaças alcancem os usuários em uma organização. A proteção no nível da caixa de entrada oferecida pelos SEGs simplesmente não é suficiente nesse panorama interconectado. A menos que o cliente adquira módulos de segurança complementares, os SEGs não têm visibilidade dessas aplicações conectadas. Consequentemente, não é possível identificar ameaças nessa parte do ambiente.

Os SEGs se autotransmitem aos hackers

Para redirecionar e-mails por meio de um SEG, uma organização precisa alterar seus registros MX para o gateway. Ou seja, informações públicas por meio de sites como o MXToolbox, no qual os hackers podem desenvolver ataques direcionados personalizados para contornar a verificação de um SEG específico.

Conclusão

Os ciberataques enviados por e-mail estão em alta e mais sofisticados do que nunca. Uma abordagem em camadas é vital para o fechamento das lacunas de segurança. O SonicWall Cloud App Security (CAS) oferece proteção de conjunto completo para aplicações de e-mail na nuvem e SaaS. Ele identifica os ataques enviados por e-mail e de zero-day que as soluções da Microsoft e SEG deixam passar, por meio de um sistema de prevenção de ameaças internas em várias camadas que é facilmente implementado em poucos minutos com uma API. O CAS impede Comprometimento de E-mail Comercial, phishing direcionado, malware, ataques zero-day, invasão de contas e ameaças internas em toda a sua empresa.

Saiba mais. *Visite www.sonicwall.com/cas.*

[1]Relatório do 451 Research "Voice of the Enterprise: Information Security, Workloads & Key Projects" (Voice of the Enterprise: Segurança da Informação, Cargas de Trabalho e Projetos Importantes), primeiro trimestre de 2019

[2]https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

[3]https://track.eng.sonicwall.com/browse/WWW2-3226

Sobre a SonicWall

A SonicWall oferece Boundless Cybersecurity ou Cibersegurança sem Limites para a era da hiperdistribuição, em uma realidade de trabalho em que todos estão remotos têm mobilidade e estão menos seguros. Com o conhecimento do desconhecido, a disponibilização de visibilidade em tempo real e a viabilização de uma economia revolucionária, a SonicWall fecha a lacuna no ramo de cibersegurança para corporações, governos e pequenas e médias empresas no mundo inteiro. Visite www.sonicwall.com para obter mais informações

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte nosso website para obter informações adicionais.
www.sonicwall.com/pt-br/