A ascensão do phishing nativo: aplicativos do Microsoft 365 abusados em

Data: 2025-08-11 17:50:05

Autor: Inteligência Against Invaders

Os invasores não precisam de exploits; eles precisamCONFIANÇA.

Mudanças nos métodos de ataque refletem mudanças nas gerações. A Geração Z, uma geração conhecida por priorizar a facilidade e a eficiência, agora está entrando no cenário da segurança cibernética em ambos os lados. Alguns estão protegendo dados e outros estão roubando.

Com o surgimento de plataformas de IA e no-code nos kits de ferramentas de phishing dos invasores, construir confiança e enganar os usuários nunca foi tão fácil. Os agentes de ameaças estão combinando ferramentas confiáveis padrão com serviços gratuitos e legítimos para contornar as defesas de segurança tradicionais e as suspeitas humanas.

Os invasores ainda estão enviando anexos de e-mail maliciosos. No entanto, eles expandiram sua série de truques, compartilhando arquivos ou links maliciosos em toda a organização usando recursos de colaboração integrados e confiáveis de uma conta comprometida – uma tática que chamamos de “phishing nativo”.

O phishing nativo fornece conteúdo malicioso de uma forma que parece completamente legítima para a vítima. Nesse caso, por exemplo, ele foi enviado pelo sistema de compartilhamento de arquivos do M365, o arquivo não é verificado como anexos, parece nativo e é uma maneira menos comum de phishing para os usuários.

Basta um usuário interno comprometido e, de repente, toda a organização está em risco. Neste blog, detalharemos incidentes recentes do mundo real mostrando como um invasor comprometeu um usuário e usou ferramentas de IA/sem código com o M365 para phishing nativo.

OneNOT: Como os invasores aproveitam o OneNote

O Microsoft OneNote, parte do pacote Microsoft 365, é um aplicativo de anotações que os defensores geralmente ignoram.

Ao contrário do Word ou do Excel, o OneNote não oferece suporte ao VBAMacros. No entanto, o Varonis Threat Labshas observou seu uso crescente em ataques de phishing devido a váriosFatores-chave:

- Não está sujeito à Exibição Protegida
- Sua formatação flexível permite que os invasores criem layouts enganosos
- Ele suporta a incorporação de arquivos ou links maliciosos

Como o OneNote também é um aplicativo padrão e confiável na maioria das organizações,os adversários estão cada vez mais usandocomo um mecanismo de entrega, mudando de código

macro para técnicas de engenharia social, para que possam contornarBarreiras de segurança.

Um usuário, OneNote, OneDrive e muitas vítimas

[IMAGEM REMOVIDA]

Em incidentes recentes, vimos invasores usarem um método direto, mas altamente eficaz. Depois que o agente da ameaça obteve credenciais M365 de um usuário em uma organização por meio de um ataque de phishing, ele criou um arquivo do OneNote na pasta Documentos pessoais do usuário comprometido no OneDrive, incorporando a URL de atração para o próximo estágio de phishing.

[IMAGEM REMOVIDA]

[IMAGEM REMOVIDA]Varonis, observamos um aumento nos eventos de ‘Link compartilhado de pasta criado’ de um usuário comprometido e os comparamos com seus últimos 90 dias de atividade.

[IMAGEM REMOVIDA][IMAGEM REMOVIDA]

Ao contrário de muitas campanhas de phishing que vimos na natureza, esta teve uma taxa de sucesso excepcionalmente alta. Muitos usuários clicaram no link e inseriram voluntariamente suas credenciais. Depois de clicar, as vítimas foram redirecionadas para uma página de login falsa que parecia quase idêntica ao portal de autenticação real da empresa.

O site de phishing foi construído usando uma plataforma chamada**Flazio**, e sim, você acertou, é um construtor de sites gratuito com inteligência artificial. Isso tornou incrivelmente fácil para o invasor criar uma réplica convincente da página de login rapidamente.

Abaixo, você pode ver uma comparação lado a lado da página de login legítima e da versão de phishing. A semelhança é perturbadoramente próxima.

[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]**Funis de clique**e**JotForm**.

Em vários casos, eles hospedavam páginas falsas no estilo Adobe “Clique para visualizar o documento” que redirecionavam os usuários para telas de login de phishing projetadas para roubar credenciais. Essas plataformas oferecem uma maneira fácil, rápida e gratuita para os invasores criarem e hospedarem páginas de phishing com o mínimo de esforço.

[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]vibe-scamming.

O que você pode fazer hoje?

Siga estas etapas para minimizar o phishing no OneNote:

- **Impor MFA e acesso condicional**para todos os usuários para reduzir o risco de conta Tomada de controle se as credenciais forem roubadas
- **Execute simulações regulares de phishing e vishing**, incluindo executivos, para conscientizar e testar respostas do mundo real
- **Facilite a denúncia de atividades suspeitas**garantindo que os canais de denúncia interna sejam claros e acessíveis
- **Revise e aperte**Configurações de compartilhamento do Microsoft 365para limitar a exposição desnecessária de arquivos internos
- **Definir alertas para comportamento incomum de compartilhamento de arquivos**e monitorar o tráfego para construtores de sites sem código conhecidos

À medida que as táticas de phishing evoluem, nossas defesas também devem evoluir. Ao entender como os invasores exploram a confiança e aproveitam as ferramentas modernas, as organizações podem se preparar, detectar e responder melhor. No final, não se trata apenas de proteger sistemas, trata-se de proteger as pessoas.

Como a Varonis pode ajudar

A Varonis monitora as atividades de e-mail e navegação em tempo real e as atividades de usuários e dados, fornecendo uma ferramenta abrangente para investigações forenses cibernéticas. Isso permite que você determine rapidamente o impacto e os riscos potenciais de uma campanha de phishing direcionada à sua organização.

OVaronis MDDRA equipe oferece experiência em segurança de dados 24 horas por dia, 7 dias por semana, 365 dias por ano e resposta a incidentes, garantindo suporte contínuo para praticamente qualquer preocupação de segurança.

Quer ver a Varonis em ação? Agende umdemoHoje.

*Este artigo foi publicado originalmente no*Varonis blog.

Patrocinado e escrito por Varonis.