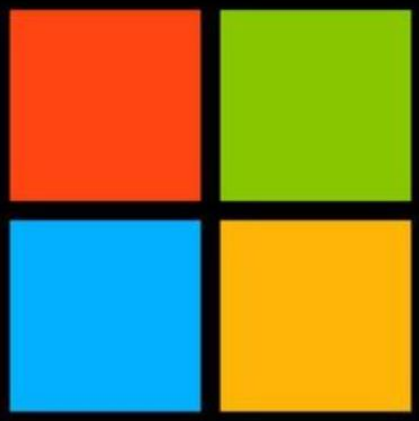
TLP: CLEAR



Microsoft

BOLETIM DE SEGURANÇA

Microsoft alerta para aumento no uso de serviços de hospedagem de arquivos em ataques de e-mail comercial

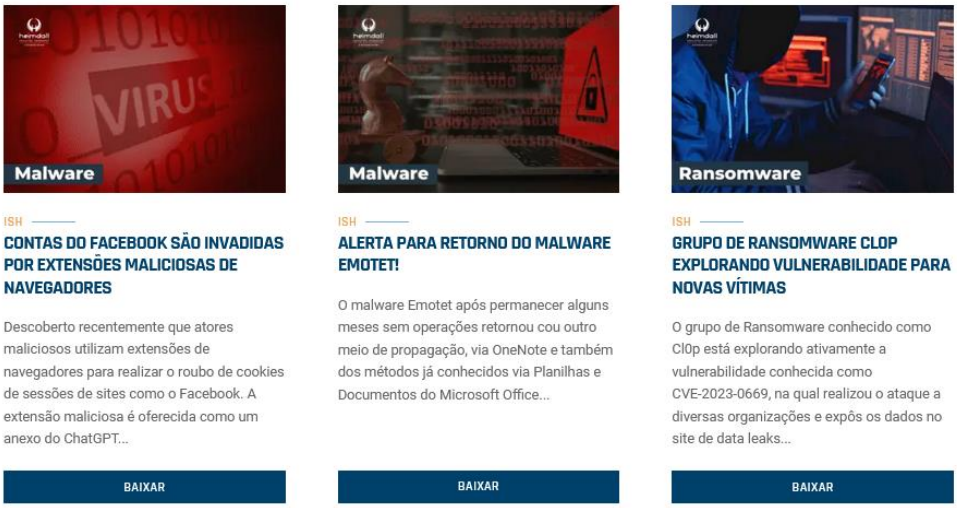
heimdall
security research
A DIVISION OF ISH

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A Microsoft está emitindo um alerta sobre campanhas cibernéticas que **exploram serviços legítimos de hospedagem de arquivos, como SharePoint**, OneDrive e Dropbox, usados amplamente em ambientes corporativos. Esses serviços são utilizados como uma tática para evitar defesas de segurança.

2 INFORMAÇÕES SOBRE A AMEAÇA

A Microsoft identificou um aumento no uso indevido de serviços legítimos de hospedagem de arquivos em campanhas cibernéticas. Essas campanhas utilizam táticas avançadas de evasão de defesa, como arquivos com acesso restrito e permissões somente para visualização. Embora sejam genéricas e oportunistas, essas campanhas empregam técnicas sofisticadas de engenharia social para evitar detecção e expandir o alcance dos agentes de ameaça para outras contas e locatários.

O objetivo principal é comprometer identidades e dispositivos, frequentemente resultando em ataques de comprometimento de e-mail comercial (BEC), além de fraudes financeiras, exfiltração de dados e movimentação lateral para outros endpoints. Serviços como **SharePoint**, **OneDrive** e **Dropbox** são amplamente utilizados por organizações para armazenar, compartilhar e colaborar em arquivos. No entanto, essa popularidade também os torna alvos atraentes para agentes de ameaça, que exploram a confiança e familiaridade desses serviços para distribuir arquivos e links maliciosos, muitas vezes escapando das medidas de segurança tradicionais.

A Microsoft está tomando medidas contra usuários mal-intencionados que violam o Contrato de Serviços da Microsoft ao usar aplicativos como SharePoint e OneDrive. Para proteger contas corporativas, o Microsoft 365 e o Office 365 oferecem suporte à autenticação multifator (MFA) e login sem senha. Consumidores também podem usar suas contas da Microsoft sem senha. A segurança é um esforço colaborativo, e a Microsoft trabalha com terceiros, como o Dropbox, para compartilhar inteligência de ameaças e proteger clientes e a comunidade em geral.

Nos últimos anos, campanhas de phishing que utilizam serviços legítimos de hospedagem de arquivos têm se tornado cada vez mais comuns, devido à facilidade dessa técnica. Os arquivos são distribuídos por meio de várias abordagens, como e-mails e anexos em formatos como **PDF**, **OneNote** e **Word**, com o objetivo de comprometer identidades ou dispositivos. Essas campanhas se destacam dos ataques de phishing tradicionais pelas técnicas sofisticadas de evasão de defesa empregadas.

Desde abril de 2024, observou-se um aumento no uso dessas táticas por agentes de ameaças para driblar os mecanismos de defesa:

- **Arquivos com acesso restrito**: Os arquivos enviados por e-mails de phishing são configurados para serem acessíveis apenas ao destinatário designado. Isso exige que o destinatário esteja conectado ao serviço de compartilhamento de arquivos, como **Dropbox**, **OneDrive** ou **SharePoint**, ou que se autentique novamente inserindo seu endereço de e-mail e uma senha de uso único (OTP) recebida por meio de um serviço de notificação.

- **Arquivos com restrições de somente visualização**: Para evitar a análise por sistemas de detonação de e-mail, os arquivos compartilhados nesses ataques de phishing são definidos no modo “somente visualização”, desativando a capacidade de download e, consequentemente, a detecção de URLs incorporadas no arquivo.

Abaixo, um exemplo de cadeia de ataque ilustra as técnicas de evasão de defesa atualizadas usadas nos estágios 4, 5 e 6.

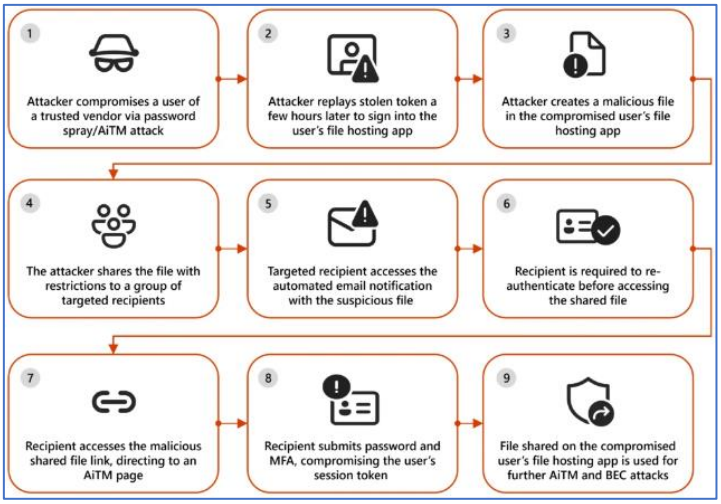


Figura 1 – Exemplo de cadeia de ataque.

O ataque geralmente começa com a invasão de um usuário de um fornecedor confiável. Após comprometer esse fornecedor, o agente malicioso hospeda um arquivo no serviço de hospedagem do fornecedor, que é então compartilhado com a organização alvo. Esse uso indevido de serviços legítimos de hospedagem é eficaz porque os destinatários tendem a confiar em e-mails de fornecedores conhecidos, permitindo que os agentes bypassem medidas de segurança e comprometam identidades. Frequentemente, usuários de fornecedores confiáveis são adicionados a listas de permissão por políticas da organização em produtos do Exchange Online, permitindo a entrega bem-sucedida de e-mails de phishing.

Os nomes dos arquivos observados nessas campanhas geralmente seguem padrões como:

1. **Tópicos familiares baseados em conversas anteriores**: Por exemplo, se as organizações já discutiram uma auditoria, os arquivos podem ser chamados de “***Audit Report 2024***”.
2. **Tópicos familiares com base no contexto atual**: Se o ataque não vier de um fornecedor confiável, o agente pode se passar por administradores ou

equipe de suporte de TI, usando nomes como "***IT Filing Support 2024***", "***Forms related to Tax submission***" ou "***Troubleshooting guidelines***".

3. **Tópicos baseados em urgência**: Outra técnica comum é criar uma sensação de urgência com nomes como "***Urgent:Attention Required***" e "***Compromised Password Reset***".

Após compartilhar os arquivos no serviço de hospedagem, o serviço envia uma notificação automática ao usuário alvo com um link para acessar o arquivo. Este e-mail não é de phishing, mas uma notificação sobre a ação de compartilhamento. Em cenários envolvendo SharePoint ou OneDrive, o arquivo é compartilhado do contexto do usuário comprometido. No Dropbox, o arquivo é compartilhado de **no-reply@dropbox[.]com**. Os e-mails de notificação têm o assunto: "***<User> shared <document>* with you**". Para evitar detecção, o agente implementa técnicas adicionais como:

- Apenas o destinatário pretendido pode acessar o arquivo
- O destinatário precisa se autenticar novamente antes de acessar
- O arquivo fica acessível por tempo limitado
- O PDF não pode ser baixado

Essas técnicas dificultam a análise do link malicioso, tornando a detonação quase impossível. Ao acessar o arquivo compartilhado, o usuário alvo é instruído a confirmar sua identidade inserindo seu endereço de e-mail:

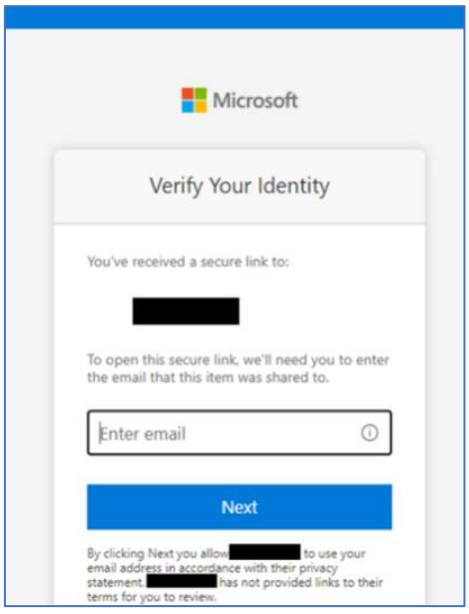


Figura 2 – Captura de tela da verificação de identidade do SharePoint.

Logo após, um OTP é enviado a partir do endereço **no-reply@notify.microsoft[.]com**. Assim que o OTP é recebido, o usuário é autenticado com sucesso e pode acessar um documento, frequentemente apresentado como uma prévia. Este documento contém um link malicioso, que serve como uma armadilha para induzir o usuário a clicar no link "**View my message**".

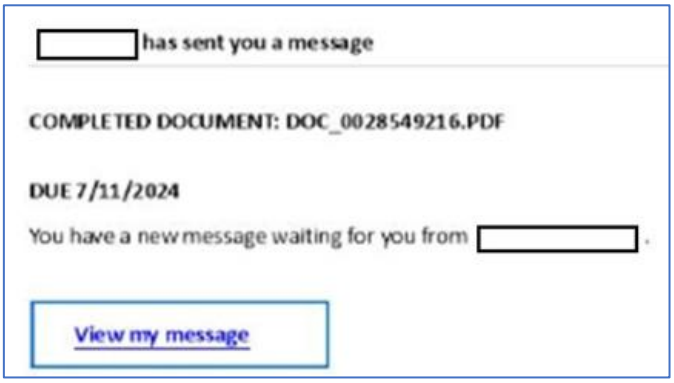


Figura 3 – Autorização final da postagem da landing page.

O link leva o usuário a uma página de phishing do tipo ***adversary-in-the-middle (AiTM)***. Nessa página, o usuário é induzido a inserir sua senha e completar a autenticação multifator (MFA). Com o token comprometido em mãos, o agente malicioso pode então realizar um ataque BEC de segundo estágio e dar continuidade à campanha.

3 RECOMENDAÇÕES

A Microsoft recomenda várias ações para mitigar essa ameaça:

- Habilite políticas de acesso condicional no Microsoft Entra, especialmente aquelas baseadas em risco. Essas políticas avaliam solicitações de entrada usando sinais adicionais, como associação de usuário ou grupo, localização de endereço IP e status do dispositivo, aplicando-se a entradas suspeitas.
- Proteja-se contra ataques que utilizam credenciais roubadas ativando políticas como dispositivos compatíveis, requisitos de endereço IP confiável do Azure ou políticas baseadas em risco com controle de acesso adequado. Se ainda estiver avaliando o acesso condicional, utilize padrões de segurança como um conjunto inicial de políticas para melhorar a postura de segurança de identidade.
- Implemente avaliação contínua de acesso.
- Adote o login sem senha do Microsoft Entra com chaves de segurança FIDO2.
- Ative a proteção de rede no Microsoft Defender for Endpoint para bloquear conexões com domínios e endereços IP maliciosos.
- Implemente o Microsoft Defender for Endpoint – Mobile Threat Defense em dispositivos móveis usados para acessar ativos corporativos.
- Utilize o Microsoft Edge para identificar e bloquear automaticamente sites maliciosos, incluindo aqueles usados em campanhas de phishing, e o Microsoft Defender para Office 365 para detectar e bloquear e-mails, links e arquivos maliciosos.
- Monitore atividades suspeitas ou anômalas no Microsoft Entra ID Protection. Investigue tentativas de login com características suspeitas, como localização, ISP, agente do usuário e uso de serviços anonimizadores.
- Eduque os usuários sobre os riscos do compartilhamento seguro de arquivos e e-mails de fornecedores confiáveis.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Microsoft**
- **Thehackernews**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH