BOLETIM DE SEGURANÇA

Ator de ameaça Storm-0324 com nova campanha de phishing no Microsoft Teams

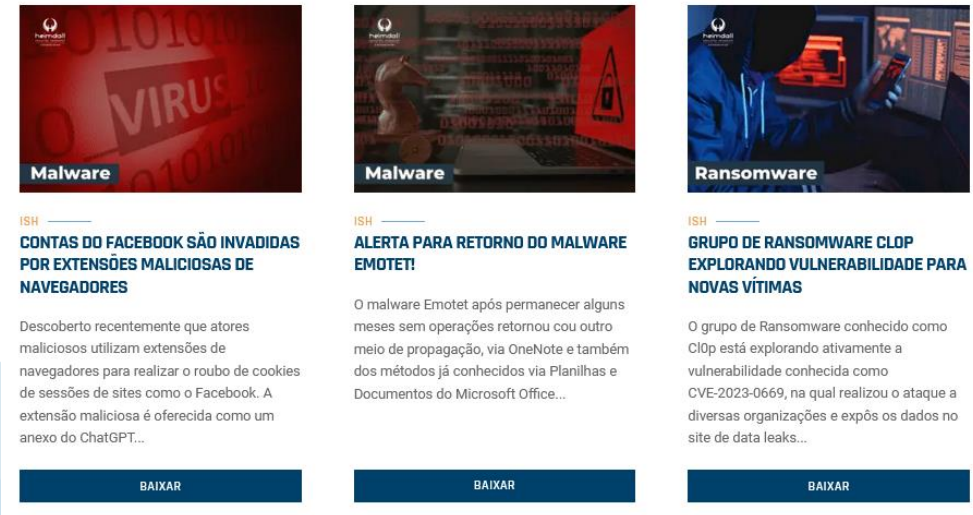
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

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



heimdall
security research

Sumário

Lista de Figuras

1 O Corretor de Acesso Inicial

A Microsoft afirmou que um corretor de acesso inicial conhecido por trabalhar com grupos de ransomware mudou recentemente para ataques de phishing do Microsoft Teams para violar redes corporativas.

O grupo de ameaça com motivação financeira por trás da campanha é rastreado como **Storm-0324**, um ator malicioso conhecido por ter implantado os ransomware Sage e GrandCrab no passado. De acordo com a Microsoft o grupo também forneceu à notória gangue do crime cibernético FIN7 acesso a redes corporativas depois de comprometê-las usando JSSLoader, Gozi e Nymaim.

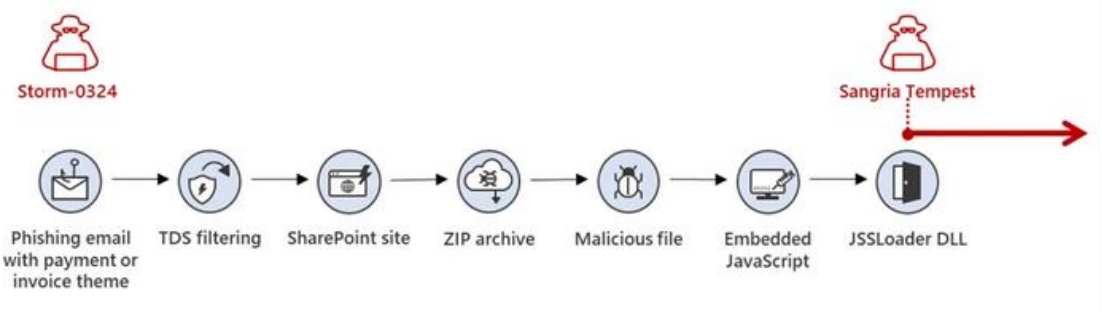


Figura 1 – Cadeia de ataque do ator Storm-0324.

O grupo de ameaça FIN7 (conhecido como Sangria Tempest e ELBRUS) foi visto implantando o ransomware Cl0p nas redes das vítimas, sendo também vinculado as operações de ransomware Maze, BlackMatter e REvil.

"Em julho de 2023, Storm-0324 começou a utilizar iscas de phishing enviadas pelo Teams com links maliciosos que levavam a um arquivo malicioso hospedado no Sharepoint" disse a Microsoft.

Para a atividade, o Storm-0324 utiliza de uma ferramenta disponível publicamente chamada TeamsPhisher. O ator faz isso explorando uma vulnerabilidade de segurança no Microsoft Teams.

Porém, é valido mencionar que a vulnerabilidade também foi explorada pelo APT29, a divisão de hackers Russos (SVR) em ataques contra dezenas de organizações, incluindo agências governamentais em todo o mundo.

Embora a Microsoft não tenha fornecido detalhes sobre o objetivo final dos ataques do Storm-0324 desta vez, os ataques APT29 tiveram como objetivo roubar as credenciais dos alvos depois de enganá-los para que aprovassem prompts de autenticação multifator (MFA).

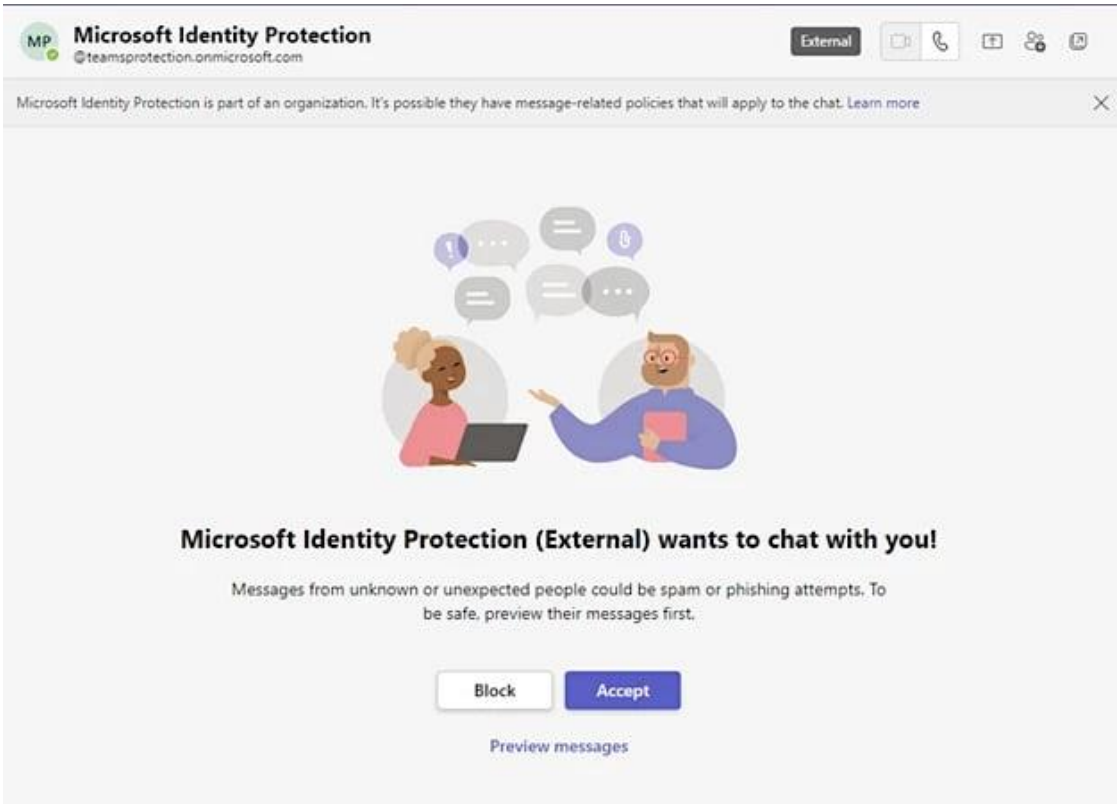


Figura 2 – Phishing utilizado pelos APT29.

De acordo com a publicação da Microsoft, a empresa teria lançado melhorias para se defender contra este tipo de ameaça, bem como os usuários e agentes de ameaças que utilizam esta técnica de phishing do Teams são reconhecidos como usuários "**EXTERNOS**" quando o acesso externo é habilitado nas configurações de uma organização.

Foi implementado ainda melhorias na experiência de Aceitar/Bloquear em bate-papos individuais dentro do Teams, para enfatizar a externalidade de um usuário e seu endereço de e-mail para que os usuários do Teams possam ter mais cuidado ao não interagir com remetentes desconhecidos ou maliciosos.

2 RECOMENDAÇÕES

A Microsoft recomenda que para se proteger de ataques de phishing direcionados pelo Storm-0324 são:

- Pilote e comece a implantar métodos de autenticação resistentes a phishing para usuários.
- Implemente a força da autenticação de acesso condicional para exigir autenticação resistente a phishing para funcionários e usuários externos para aplicativos críticos.
- Especifique organizações confiáveis do Microsoft 365 para definir quais domínios externos têm permissão ou bloqueio para bate-papo e reuniões.
- Mantenha a auditoria do Microsoft 365 habilitada para que os registros de auditoria possam ser investigados, se necessário.
- Entenda e selecione as melhores configurações de acesso para colaboração externa para sua organização.
- Permitir apenas dispositivos conhecidos que cumpram as linhas de base de segurança recomendadas pela Microsoft.
- Eduque os usuários sobre engenharia social e ataques de phishing de credenciais, incluindo a abstenção de inserir códigos MFA enviados por meio de qualquer forma de mensagens não solicitadas.
- Eduque os usuários do Microsoft Teams para verificar a marcação 'Externa' nas tentativas de comunicação de entidades externas, ser cautelosos com o que eles compartilham e nunca compartilhar as informações da conta ou autorizar solicitações de entrada por chat.
- Eduque os usuários a revisar a atividade de login e marcar tentativas de login suspeitas como “Não fui eu”.
- Implemente o Controle de Aplicativos de Acesso Condicional no Microsoft Defender para Aplicativos de Nuvem para usuários que se conectam de dispositivos não gerenciados.
- Configure o Microsoft Defender para Office 365 para verificar novamente os links ao clicar. O Safe Links fornece verificação de URL e reescrita de mensagens de email recebidas no fluxo de email e verificação no momento do clique de URLs e links em mensagens de email, outros aplicativos do Microsoft Office, como Teams, e outros locais, como o SharePoint Online. A verificação do Safe Links ocorre além da proteção antispam e antimalware regular em mensagens de email de entrada no Microsoft Exchange Online Protection (EOP). A

verificação de links seguros pode ajudar a proteger sua organização contra links maliciosos usados em phishing e outros ataques.

- Habilite a limpeza automática zero hora (ZAP) no Microsoft Office 365 para colocar em quarentena os e-mails enviados em resposta à inteligência de ameaças recém-adquirida e neutralizar retroativamente mensagens maliciosas de phishing, spam ou malware que já foram entregues em caixas de correio.
- Pratique o princípio do menor privilégio e mantenha a higiene das credenciais. Evite o uso de contas de serviço em nível de administrador em todo o domínio. A restrição de privilégios administrativos locais pode ajudar a limitar a instalação de RATs e outros aplicativos indesejados.
- Ative a proteção fornecida pela nuvem e o envio automático de amostras no Microsoft Defender Antivirus. Esses recursos usam inteligência artificial e aprendizado de máquina para identificar e impedir rapidamente ameaças novas e desconhecidas.
- Para obter recomendações adicionais sobre como proteger sua organização contra-ataques de ransomware, consulte nossa visão geral de ameaças sobre ransomware operado por humanos.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Publicação Microsoft – Sotm-0324**

heimdall
security research
A DIVISION OF ISH