PHISHING VIA MICROSOFT TEAMS: VETORES DE ATAQUE, FERRAMENTAS OFENSIVAS E ESTRATÉGIAS DE MITIGAÇÃO

Henrique Botan Bauermann[1], Rodrigo Caio Koelln Alfonsin[2], Vitor Mallmann[3],Vinicius Brenner[4]

[1]Itaipu Parquetec, Foz do Iguaçu, Paraná, Brasil (henrique.bauermann@itai.org.br)
[2]Itaipu Parquetec, Foz do Iguaçu, Paraná, Brasil
[3]Itaipu Parquetec, Foz do Iguaçu, Paraná, Brasil
[4]Itaipu Parquetec, Foz do Iguaçu, Paraná, Brasil

Resumo: O Microsoft Teams tornou-se um vetor emergente de phishing corporativo, explorando a confiança implícita da plataforma. A partir de revisão técnica, este trabalho analisa a vulnerabilidade IDOR que permite o envio de arquivos maliciosos, ferramentas como TeamsPhisher e TeamsEnum, a plataforma de Phishing-as-a-Service Kali365 e campanhas dos grupos Storm-1811 e Storm-2372, mapeando as TTPs ao MITRE ATT&CK e propondo medidas de mitigação e detecção para organizações.

Palavras-chave: Engenharia social; MITRE ATT&CK; Segurança da informação; Cibersegurança; Blue-Team;

INTRODUÇÃO

O Microsoft Teams é uma das plataformas de colaboração corporativa mais adotadas no mundo, reunindo comunicação persistente, chamadas de voz e vídeo, compartilhamento de tela e integração com SharePoint e aplicativos de terceiros. Essa mesma riqueza funcional reflete o conjunto de capacidades que agentes de ameaça necessitam para vigiar, comunicar-se e comprometer organizações-alvo. Enquanto o phishing por e-mail acumulou décadas de infraestrutura defensiva — filtros de spam, bancos de reputação de domínios, treinamento de usuários e alertas integrados a navegadores —, o Teams surgiu como canal de alta confiança, no qual mensagens aparentemente oriundas de colegas ou da equipe de TI carregam legitimidade implícita que o e-mail não proporciona com a mesma confiabilidade (Cloud Security Alliance, 2026).

A exploração do Teams como vetor de phishing ganhou escala a partir de 2023, quando pesquisadores da JUMPSEC identificaram uma vulnerabilidade de controle de acesso que permite a usuários externos contornarem restrições nativas de envio de arquivos (Corbridge e Ellson, 2023). Pouco depois, essa descoberta foi incorporada a ferramentas automatizadas de código aberto, como o TeamsPhisher e o TeamsEnum, reduzindo drasticamente a barreira técnica para a execução desses ataques (Reid, 2023; Kanbach, 2023). Desde então, múltiplos grupos de ameaça — tanto financeiramente motivados quanto patrocinados por Estados — adotaram o Teams como canal primário de entrega ou persistência (Cloud Security Alliance, 2026; Toulas, 2023). A plataforma passou a ser explorada não apenas para distribuição estática de links maliciosos, mas também como palco de engenharia social interativa em tempo real, levando à implantação de backdoors sofisticados como o A0Backdoor.

Este trabalho tem como objetivo consolidar, a partir da literatura técnica disponível, os vetores de ataque, as ferramentas ofensivas e as campanhas documentadas que exploram o Microsoft Teams, mapeando as respectivas táticas, técnicas e procedimentos (TTPs) ao framework MITRE ATT&CK e propondo recomendações práticas de mitigação e detecção para organizações que dependem da plataforma em seus ambientes corporativos.

MATERIAL E MÉTODOS

O trabalho consiste em uma revisão técnica-descritiva de fontes especializadas em segurança ofensiva e inteligência de ameaças. Foram utilizados como base o advisory original da JUMPSEC sobre a vulnerabilidade de Referência Direta a Objetos Insegura, IDOR (Corbridge e Ellson, 2023), a documentação pública das ferramentas ofensivas TeamsPhisher (Reid, 2023) e TeamsEnum (Kanbach, 2023), reportagens técnicas sobre sua weaponização (Toulas, 2023), o alerta de serviço público do FBI/IC3 sobre a plataforma de Phishing-as-a-Service Kali365 (FBI/IC3, 2026) e o relatório de pesquisa da Cloud Security Alliance sobre a campanha do A0Backdoor e a industrialização dos ataques a plataformas de colaboração (Cloud Security Alliance, 2026).

As táticas, técnicas e procedimentos identificados em cada fonte foram extraídos, sistematizados e mapeados às categorias correspondentes do framework MITRE ATT&CK Enterprise (MITRE, 2025). A partir desse mapeamento, foi construída uma linha do tempo da evolução dos ataques — da exploração isolada da vulnerabilidade IDOR até a industrialização via Phishing-as-a-Service —, permitindo consolidar um panorama unificado dos

vetores de ataque e orientar a formulação das recomendações de mitigação e detecção apresentadas na seção final.

RESULTADOS E DISCUSSÃO

A vulnerabilidade IDOR no Microsoft Teams

Em junho de 2023, pesquisadores da equipe de Red Team da JUMPSEC identificaram uma vulnerabilidade que permite a introdução de malware em qualquer organização que utilize o Teams em sua configuração padrão (Corbridge e Ellson, 2023). A falha decorre do fato de que controles de segurança críticos são implementados exclusivamente no lado do cliente, sendo, portanto, contornáveis por manipulação direta das requisições HTTP. Por padrão, o Teams permite que usuários com contas Microsoft entrem em contato com usuários de outras organizações (external tenancies); embora mensagens externas sejam sinalizadas com um banner de aviso, usuários são frequentemente induzidos a aceitá-las, especialmente quando o remetente se passa por uma entidade conhecida.

Ao tentar enviar arquivos a usuários de organizações externas, o Teams exibe a interface de envio desabilitada — mas essa restrição existe apenas na camada de apresentação. A exploração baseia-se em uma técnica clássica de IDOR: ao interceptar a requisição POST de envio de mensagem, na rota /v1/users/ME/conversations/<RECIPIENT_ID>/messages, e substituir o identificador externo do destinatário pelo identificador interno correspondente, o arquivo é entregue diretamente na caixa de entrada da vítima. O payload é hospedado em um domínio SharePoint legítimo e exibido como arquivo nativo, não como link, o que aumenta consideravelmente a taxa de abertura (Corbridge e Ellson, 2023).

A gravidade da vulnerabilidade reside em sua capacidade de contornar praticamente todos os controles modernos de segurança contra phishing por e-mail: a técnica elimina a necessidade de domínios maduros, servidores web, páginas de destino, CAPTCHAs, categorização de domínios e filtragem de URLs. O payload é servido por um domínio SharePoint confiável, herdando sua reputação de segurança, e a entrega ocorre sem que a vítima precise clicar em um link de e-mail — comportamento amplamente treinado como perigoso. A JUMPSEC reportou a falha à Microsoft, que validou sua legitimidade, mas concluiu que ela não atingia o nível para correção imediata. A eficácia real da técnica foi comprovada pelos próprios pesquisadores em ambiente de produção, tendo sido utilizada para entregar um payload de C2 e obter acesso inicial durante um red team engagement autorizado em um cliente real.

Ferramentas ofensivas derivadas

O TeamsEnum, desenvolvido por Bastian Kanbach, é uma ferramenta de enumeração de usuários do Microsoft Teams disponibilizada publicamente no GitHub (Kanbach, 2023). Trata-se de um script Python que identifica usuários existentes e seu status de presença online por meio da API do Teams, suportando múltiplos mecanismos de autenticação: por senha para contas corporativas sem MFA, por código de dispositivo quando MFA está habilitado, e por token para sessões já autenticadas. Um aspecto crítico identificado é que, mesmo quando a configuração "Block all external domains" está ativa no painel administrativo, ainda é possível utilizar uma conta corporativa para distinguir entre usuários existentes e inexistentes — a mera confirmação da existência de um alvo já constitui informação de reconhecimento valiosa para um adversário.

O TeamsPhisher, desenvolvido por um integrante do red team da Marinha dos EUA e publicado em julho de 2023, automatiza completamente a entrega de mensagens de phishing e anexos a usuários cujas organizações permitem comunicações externas (Reid, 2023; Toulas, 2023). A ferramenta integra a técnica de contorno IDOR da JUMPSEC, técnicas de criação de threads de grupo que contornam a tela de aviso de remetente externo, e as funções de autenticação e enumeração do TeamsEnum. O fluxo operacional ocorre da seguinte maneira: dado um anexo, uma mensagem e uma lista de alvos, o TeamsPhisher autentica-se com uma conta Microsoft Business válida, faz upload do arquivo para o SharePoint pessoal do remetente, enumera cada usuário-alvo para confirmar sua existência e capacidade de receber mensagens externas, cria um thread de grupo incluindo o destinatário duas vezes — técnica que contorna a tela de confirmação de remetente externo — e envia a mensagem com o link do SharePoint. Por fim, remove o alvo do chat criado, eliminando a notificação de remetente externo. A ferramenta oferece ainda recursos como envio de links seguros acessíveis apenas pelo destinatário-alvo, personalização da saudação com o primeiro nome do alvo, modo de prévia sem envio real e controle de atraso entre mensagens para evitar limitação de taxa.

A weaponização do Teams como vetor de phishing em escala começou em julho de 2023, quando o Storm-0324, um broker de acesso inicial financeiramente motivado, passou a utilizar o TeamsPhisher para enviar iscas de phishing com links maliciosos para arquivos hospedados no SharePoint diretamente via chat do Teams (Cloud Security Alliance, 2026). A Microsoft documentou essa atividade em setembro de 2023 e implementou restrições padrão nas mensagens externas, mas essas restrições aplicaram-se apenas à comunicação Teams-a-Teams, sem abordar o modelo mais amplo

de acesso de convidados. Atores subsequentes adaptaram suas táticas: em vez de depender do envio automatizado de links estáticos, migraram para engenharia social interativa em que o atacante impersona um técnico de suporte de TI e conduz a vítima ativamente pela instalação de software de acesso remoto.

Campanhas ativas e grupos de ameaça
O grupo mais sofisticado documentado é rastreado pela BlueVoyant como Blitz Brigantine (também referido como Storm-1811 ou STAC5777), avaliado com confiança moderada a alta como continuação das atividades associadas ao ecossistema de ransomware Black Basta após a dissolução dessa operação em fevereiro de 2025 (BlueVoyant, 2026). Cabe notar que a atribuição ao grupo, bem como os detalhes técnicos apresentados a seguir, têm como origem primária a pesquisa da própria BlueVoyant (2026), citada diretamente quando possível; a Cloud Security Alliance (2026), também utilizada como fonte, identifica sua síntese como "unofficial AI-assisted research".

O primeiro estágio é a inundação de e-mails (email bombing): o atacante inscreve o endereço de e-mail corporativo do alvo em grande volume de serviços de newsletter e confirmações de assinatura, gerando centenas ou milhares de mensagens legítimas em curto intervalo. O objetivo não é entregar um payload por e-mail, mas criar um estado de crise que torna o usuário mais suscetível a uma oferta de ajuda.

O segundo estágio é a engenharia social via Teams. O atacante contata a vítima pelo Microsoft Teams se passando por técnico de suporte de TI interno, com mensagem contextualmente crível que referencia o problema de e-mail vivenciado pela vítima naquele momento.

O terceiro estágio é o abuso do Windows Quick Assist. O atacante persuade a vítima a abrir essa ferramenta de suporte remoto, legítima, assinada pela Microsoft e integrada ao Windows 10 e 11, e a fornecer um código de sessão de seis caracteres. Por ser reconhecida como mecanismo padrão de suporte de TI, ela raramente aciona alertas de antivírus ou EDR. Uma vez obtido o acesso remoto, o A0Backdoor é implantado silenciosamente. Trata-se de malware residente em memória, projetado para operar sem gravar seus componentes principais em disco, evitando ferramentas de análise estática. Seu canal de comando e controle é especialmente sofisticado: em vez de se conectar a um endereço IP remoto por HTTP ou HTTPS, o A0Backdoor codifica comunicações em consultas DNS de registro MX direcionadas a resolvedores públicos como o 1.1.1.1 da Cloudflare — tráfego que toda organização precisa permitir para funcionar, criando um canal encoberto de difícil detecção.

O Storm-2372, grupo com vínculos russos ativo desde agosto de 2024, opera por um caminho técnico completamente diferente: envia convites falsos de reunião no Teams para induzir as vítimas a completar um fluxo de autenticação por código de dispositivo (device code flow), capturando tokens OAuth de acesso e atualização em vez de depender de acesso remoto ao dispositivo. Com os tokens capturados, o grupo obtém acesso persistente a serviços Microsoft 365, Outlook, Teams e OneDrive, sem necessitar das credenciais do usuário nem enfrentar desafios adicionais de MFA. Esse padrão foi posteriormente formalizado e disponibilizado como serviço pela plataforma Kali365.

Phishing-as-a-Service: o caso Kali365

Em maio de 2026, o FBI emitiu um Aviso de Serviço Público alertando sobre a plataforma emergente de Phishing-as-a-Service Kali365, observada pela primeira vez em abril de 2026 (FBI/IC3, 2026). Distribuída principalmente via Telegram, a plataforma permite que atores de ameaça obtenham tokens de acesso do Microsoft 365 e contornem protocolos de autenticação multifator sem interceptar credenciais, oferecendo iscas geradas por IA, modelos de campanha automatizados, painéis de rastreamento em tempo real e capacidades de captura de tokens OAuth.

O mecanismo segue quatro etapas: o atacante envia um e-mail de phishing se passando por serviços confiáveis de produtividade em nuvem, contendo um código de dispositivo com instruções para acessar uma página legítima de verificação da Microsoft; a vítima navega até a página real da Microsoft e cola o código, autorizando inadvertidamente o dispositivo do atacante; o atacante captura os tokens de acesso e atualização OAuth; e, com os tokens em mãos, o acesso persiste a Outlook, Teams e OneDrive sem senha ou novos desafios de MFA.

Uma lacuna estrutural amplifica o risco tanto do Kali365 quanto de outros grupos: o modelo de proteção por tenant do Microsoft Defender. As proteções de Safe Links e Safe Attachments são aplicadas pelo tenant de recurso, aquele que hospeda o ambiente Teams onde o conteúdo é compartilhado, e não pelo tenant que licencia o usuário-vítima (Cloud Security Alliance, 2026). Um atacante que registra uma conta Microsoft 365 Business Basic por aproximadamente US$ 6 por mês obtém um ambiente funcional sem o Defender for Office 365. Quando usuários-vítima aceitam convites de convidado desse tenant, os arquivos e links compartilhados passam pelo contexto do tenant do atacante e não são inspecionados pelas políticas Defender da organização-alvo, criando uma zona

efetivamente sem proteção mesmo em organizações com licenciamento premium.

Mapeamento ao MITRE ATT&CK

A Tabela 1 consolida as principais táticas, técnicas e procedimentos (TTPs) identificados nos ataques via Microsoft Teams, mapeadas ao framework MITRE ATT&CK Enterprise.

Tabela 1. TTPs mapeadas ao MITRE ATT&CK

Técnica (ID ATT&CK)	Uso observado
Spearphishing via serviço (T1566.003)	Envio de mensagens e arquivos maliciosos via Teams, contornando controles de e-mail
Account Discovery: Cloud Account (T1087.004)	TeamsEnum enumera contas cloud válidas e presença mesmo com domínios externos bloqueados
Exploração de controle de acesso – IDOR (T1190)	Troca do ID externo pelo interno na requisição POST para liberar envio de arquivos
Remote Access Software (T1219)	Abuso do Windows Quick Assist para controle remoto sem acionar alertas
Roubo de token de aplicação (T1528)	Captura de tokens OAuth via device code flow (Storm-2372, Kali365)
Tunelamento DNS via MX (T1071.004)	(T1071.004)C2 do A0Backdoor encoberto em consultas DNS de registro MX
Impersonation (T1656)	Impersonação de suporte de TI via Teams para induzir uso do Quick Assist

Medidas de mitigação e detecção

No plano administrativo, a primeira linha de defesa é a revisão das políticas de comunicação externa no Teams Admin Center, em Usuários → Acesso Externo. Organizações sem necessidade de negócio para comunicação com tenants externos devem bloquear todos os domínios externos por padrão; aquelas que necessitam de comunicação externa devem substituir a permissão irrestrita por uma lista de domínios de parceiros explicitamente autorizados. Políticas de acesso entre tenants no Microsoft Entra ID oferecem camada complementar de controle sobre permissões de convite e colaboração de convidados.

O Windows Quick Assist deve ser avaliado como candidato a restrição por política em ambientes onde não é necessário para operações de TI, via Política de Grupo ou Microsoft Intune. Onde for necessário, deve-se estabelecer um processo de verificação formal: qualquer sessão remota deve ser iniciada apenas após abertura de chamado no sistema oficial de tickets e confirmada por um segundo canal, nunca em resposta a mensagem não solicitada no Teams. Para mitigar ataques de código de dispositivo, recomenda-se criar política de Acesso Condicional que bloqueie esse fluxo para todos os usuários, com exceções limitadas e auditadas, complementada por políticas de bloqueio de transferência de autenticação.

No plano técnico de detecção, equipes de segurança devem configurar alertas para volumes e padrões incomuns de consultas DNS de registro MX, especialmente a resolvedores públicos em alta frequência, como potencial indicador de tunelamento DNS. Plataformas de segurança de e-mail devem alertar sobre tráfego súbito de confirmações de assinatura, já que um usuário reportando inundação de caixa de entrada pode estar no início de uma cadeia de ataque. Requisições ao endpoint de aceitação de mensagens externas também podem ser monitoradas via proxy para gerar visibilidade sobre a frequência dessas transações. O Microsoft Defender for Office 365 Plan 2 passou a incluir Segurança de Colaboração para o Teams com disponibilidade geral em 2025, oferecendo Safe Links, Safe Attachments e detonação de URLs em tempo real, embora essa proteção não cubra interações com tenants externos que não possuam Defender.

Por fim, o componente humano é central em todos os vetores documentados, uma vez que nenhum deles depende de exploração técnica sofisticada para ser bem-sucedido; todos requerem, em algum grau, que a vítima tome uma ação. Programas de simulação de phishing devem incorporar cenários via Teams, cobrindo especificamente impersonação de suporte de TI, solicitações não solicitadas de Quick Assist e convites de reunião externos. Usuários devem ser orientados a reconhecer o padrão de email bombing seguido de contato por Teams como sinal de alerta

claro, suspendendo a interação, encerrando qualquer sessão de acesso remoto já iniciada e verificando a identidade do solicitante por canal alternativo previamente estabelecido.

CONCLUSÃO

O Microsoft Teams consolidou-se, entre 2023 e 2026, como vetor de ataque prioritário para múltiplos grupos de ameaça, tanto financeiramente motivados quanto patrocinados por Estados. A trajetória documentada evidencia progressão clara e acelerada: da descoberta de uma vulnerabilidade IDOR que contorna controles de envio de arquivos, à automação do ataque por ferramentas como TeamsPhisher e TeamsEnum, ao surgimento de plataformas de Phishing-as-a-Service como o Kali365, e finalmente ao uso do Teams como palco de engenharia social interativa que culmina na implantação de backdoors avançados como o A0Backdoor, com canal de C2 encoberto em tráfego DNS legítimo.

A assimetria entre a maturidade defensiva consolidada no e-mail e a relativa imaturidade das defesas em torno das plataformas de colaboração representa uma vantagem estrutural que agentes de ameaça estão ativamente explorando. Organizações que investiram significativamente em segurança de e-mail, mas não aplicaram o mesmo rigor ao Teams, possuem uma lacuna explorável com ferramentas acessíveis e custo mínimo de infraestrutura; uma conta Microsoft 365 Basic de aproximadamente US$ 6 por mês pode ser suficiente para contornar o Defender de uma organização-alvo com licenciamento premium, simplesmente porque as proteções são aplicadas pelo tenant do recurso, e não pelo tenant da vítima.

A resposta adequada exige defesa em profundidade que combine controles administrativos restringindo o acesso externo ao estritamente necessário, restrição e monitoramento de ferramentas de suporte remoto passíveis de abuso, mitigação do fluxo de código de dispositivo, alertas de DNS para canais de C2 furtivos e, fundamentalmente, a extensão do treinamento de conscientização de segurança para cobrir os padrões específicos de engenharia social documentados para o Teams. Plataformas de colaboração de alta adoção constituirão vetores de ataque prioritários enquanto essa assimetria defensiva persistir.

REFERÊNCIAS

BLUEVOYANT. New A0Backdoor Linked to Teams Impersonation and Quick Assist Social Engineering. BlueVoyant Threat Fusion Cell, 2026. Disponível em: https://www.bluevoyant.com/blog/new-a0backdoor-linked-to-teams-impersonation-and-quick-assist-social-engineering. Acesso em: mai. 2026.

CLOUD SECURITY ALLIANCE (CSA) – AI SAFETY INITIATIVE. Microsoft Teams as Phishing Infrastructure: The A0Backdoor Campaign and the Industrialization of Collaboration-Platform Attacks. Unofficial AI-assisted Research. [s.l.]: CSA, mar. 2026. Disponível em: https://labs.cloudsecurityalliance.org/wp-content/uploads/2026/03/CSA_research_note_teams_phishing_a0backdoor_quick_assist_abuse_20260310-csa-styled-2.pdf. Acesso em: mai. 2026.

CORBRIDGE, M.; ELLSON, T. Advisory: IDOR in Microsoft Teams Allows for External Tenants to Introduce Malware. JUMPSEC Labs, jun. 2023. Disponível em: https://labs.jumpsec.com/advisory-idor-in-microsoft-teams-allows-for-external-tenants-to-introduce-malware/. Acesso em: mai. 2026.

FEDERAL BUREAU OF INVESTIGATION (FBI) – INTERNET CRIME COMPLAINT CENTER (IC3). Kali365 Phishing-as-a-Service Kit Hijacks Microsoft 365 Access Tokens. Alert Number: I-052126-PSA. Washington, D.C.: IC3, mai. 2026. Disponível em: https://www.ic3.gov/PSA/2026/PSA260521. Acesso em: mai. 2026.

KANBACH, B. TeamsEnum: User Enumeration of Microsoft Teams users via API. GitHub, 2023. Disponível em: https://github.com/lucidra-security/TeamsEnum. Acesso em: mai. 2026.

MITRE CORPORATION. MITRE ATT&CK Enterprise Matrix. [s.l.]: MITRE, 2025. Disponível em: https://attack.mitre.org/. Acesso em: mai. 2026.

REID, A. TeamsPhisher: Send phishing messages and attachments to Microsoft Teams users. GitHub, 2023. Disponível em: https://github.com/Octoberfest7/TeamsPhisher. Acesso em: mai. 2026.

TOULAS, B. New tool exploits Microsoft Teams bug to send malware to users. BleepingComputer, jul. 2023. Disponível em: https://www.bleepingcomputer.com/news/security/new-tool-exploits-microsoft-teams-bug-to-send-malware-to-users/. Acesso em: mai. 2026.