Novas vulnerabilidades no Microsoft Teams expõem riscos na colaboração digital

written by O Cidadão | 5 de Novembro, 2025

Com mais de **320 milhões de utilizadores ativos mensais**, o **Microsoft Teams** é uma das principais ferramentas de comunicação e colaboração corporativa a nível mundial. No entanto, os resultados desta investigação demonstram como os cibercriminosos podem explorar os próprios mecanismos de confiança que sustentam estas plataformas, **transformando-as num novo vetor de ataque digital.**

"A confiança é essencial para a colaboração, mas não é suficiente para garantir segurança", alerta Rui Duro, Country Manager para Portugal da Check Point Software. ***"Os atacantes estão a explorar precisamente essa confiança para manipular decisões e comprometer operações empresariais."***

A colaboração como nova superfície de ataque

Durante anos, o email foi o principal alvo de ataques baseados em engenharia social. Agora, os aplicativos de colaboração como **Microsoft Teams, Slack e Zoom** estão a assumir esse papel central nas empresas e, por isso, estão a tornar-se infraestruturas críticas de negócio.

Grupos de ameaça persistente avançada (APT) e cibercriminosos motivados financeiramente reconhecem que, se conseguirem manipular o que as pessoas veem e acreditam dentro dessas plataformas, podem contornar as defesas tradicionais. O estudo da Check Point confirma uma tendência crescente: os atacantes exploram as suposições de confiança que os utilizadores fazem quando interagem em canais digitais familiares.

O que foi descoberto

A Check Point Research conduziu uma análise aprofundada ao Microsoft Teams, investigando tanto utilizadores externos convidados como potenciais ameaças internas. As conclusões revelaram múltiplas falhas que permitiam:

Editar mensagens sem deixar rasto – explorando identificadores únicos do sistema, era possível alterar o conteúdo de mensagens enviadas sem que aparecesse a etiqueta “Editado”. Isto permitia reescrever o histórico de conversas sem deteção.

Falsificar notificações – os investigadores demonstraram que um atacante poderia manipular campos de notificação, fazendo parecer que um alerta provinha de um executivo ou colega de confiança.

Alterar nomes de utilizador em conversas privadas – ao modificar o tópico da conversa, o atacante podia mudar o nome exibido no chat, levando ambos os participantes a acreditar que estavam a comunicar com outra pessoa.

Falsificar identidade em chamadas de áudio/vídeo – através da

manipulação de pedidos de início de chamada, era possível alterar o nome mostrado ao destinatário, criando identidades falsas em tempo real.

Embora a Microsoft tenha entretanto corrigido todas as falhas, estas vulnerabilidades colocaram em risco **a confiança fundamental nas comunicações empresariais.** Os potenciais impactos vão muito além de simples perturbações: incluem impersonação de executivos, fraudes financeiras, distribuição de malware, campanhas de desinformação e sabotagem de comunicações sensíveis.

A Check Point Research notificou a Microsoft sobre as vulnerabilidades em 23 de março de 2024. A empresa reconheceu as falhas, registadas sob o código CVE-2024-38197, e lançou atualizações de correção progressivas ao longo de 2024, culminando com a correção final em outubro de 2025, relativa às chamadas de áudio e vídeo.

Estas vulnerabilidades representam um caso paradigmático do novo contexto de risco digital: **as plataformas de colaboração** são agora o novo campo de batalha cibernético. Tal como o email se tornou o ponto de entrada preferido para ataques de phishing e BEC (Business Email Compromise), as aplicações de trabalho colaborativo **são hoje alvos críticos de manipulação.**

Os ataques não dependem de explorações técnicas complexas, atuam sobre os sinais de confiança humana: o nome de um remetente, uma notificação, uma citação de mensagem. Se esses sinais forem comprometidos, as decisões empresariais podem ser manipuladas.

Para além do Teams: um problema sistémico

Embora a Microsoft tenha resolvido as vulnerabilidades identificadas, a investigação da Check Point revela que esta não é uma questão isolada. Os atacantes estão a direcionar os seus esforços para um conjunto crescente de aplicações de colaboração e produtividade, incluindo **assistentes de IA,**

plataformas de automação e ferramentas de desenvolvimento. O padrão é claro: **onde existe confiança digital, há exploração potencial.**

O caminho a seguir: defesa em camadas

A mensagem central é inequívoca: a confiança, por si só, não é suficiente. As defesas nativas destas aplicações foram concebidas para facilitar a colaboração e a produtividade, **não para detetar ataques sofisticados**.

A Check Point recomenda a **adoção de um modelo de segurança em camadas**, que inclua:

· Proteção contra malware e ficheiros maliciosos – bloqueando cargas e links partilhados em plataformas colaborativas.

· Prevenção de perda de dados (DLP) – salvaguardando informações sensíveis em conversas, ficheiros e ligações.

· Deteção e resposta a ameaças – monitorizando anomalias e sessões suspeitas.

· Proteção unificada entre aplicações – estendendo a segurança além do Teams, abrangendo email, browsers e outras ferramentas de colaboração.

"Os atacantes já não estão apenas a invadir sistemas,a estão a invadir as conversas", sublinha Rui Duro da Check Point. ***"As empresas devem preparar-se para um futuro onde ver não é necessariamente acreditar."***

Transparência e colaboração contínua

A Check Point Research reforça o seu compromisso com a transparência e colaboração responsável, partilhando as descobertas com fabricantes como a Microsoft e promovendo a adoção de **práticas preventivas em todo o setor.**

Para aprofundar estas conclusões e compreender o novo cenário

de ameaças, a Check Point convida os profissionais a participar no webinar dedicado às vulnerabilidades do Microsoft Teams: *https://pages.checkpoint.com/2025-nov-ww-critical-microsoft-teams-vulnerabilities-uncovered.html*

OC/AJS