Alerta

Técnica

Vulnerabilidad en chat externo de Microsoft Teams

COLCERT AL-20251201 - 087

TLP:CLEAR

NIVEL DE RIESGO

ALTO

Una nueva funcionalidad de **Microsoft Teams** llamada "**Chat with Anyone**" habilitada por defecto desde noviembre de 2025, permite que cualquier persona inicie un chat únicamente con una dirección de correo electrónico, incluso si el destinatario no tiene cuenta en Teams.

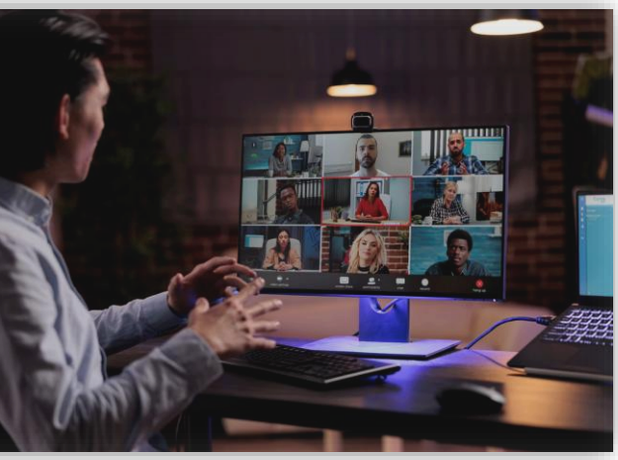
Aunque esta característica busca facilitar la colaboración externa, se ha identificado que puede ser utilizada por actores maliciosos para **realizar *phishing***, **engañar a usuarios**, y **entregar archivos o enlaces maliciosos**. El riesgo aumenta porque, cuando el usuario acepta la invitación y accede como "invitado" (guest) al entorno del ciberdelincuente, las medidas de seguridad, protección y filtrado de su organización dejan de aplicarse, incluyendo:

- ❑ Análisis seguro de enlaces (Safe Links).
- ❑ Análisis de archivos (Safe Attachments).
- ❑ Filtros antimalware y antispoofing.
- ❑ Controles de DLP.
- ❑ Políticas de monitoreo interno.

Esto crea una brecha de seguridad que puede ser aprovechada para ataques directos, incluso en organizaciones con altos estándares de protección.

Descripción Técnica

"**Chat with Anyone**" es una opción que permite que un usuario de **Teams** inicie un chat con solo enviar un mensaje a un correo electrónico externo. La víctima recibe una invitación y, si la acepta, ingresa como usuario invitado al *tenant* del remitente. Un *tenant* (o inquilino) es el espacio propio dentro de una plataforma en la nube.



¿Cuál es el problema?

Cuando un usuario se une como invitado a un *tenant* externo ya no está protegido por las configuraciones de seguridad de su propia organización. Todo lo que comparta o reciba (mensajes, enlaces, archivos) dependerá exclusivamente de las políticas del *tenant* del atacante, el cual puede tener todas las protecciones deshabilitadas. El actor de amenaza puede usar un *tenant* económico o de prueba para realizar campañas de *phishing* altamente convincentes dentro de Teams.

¿Por qué es grave?

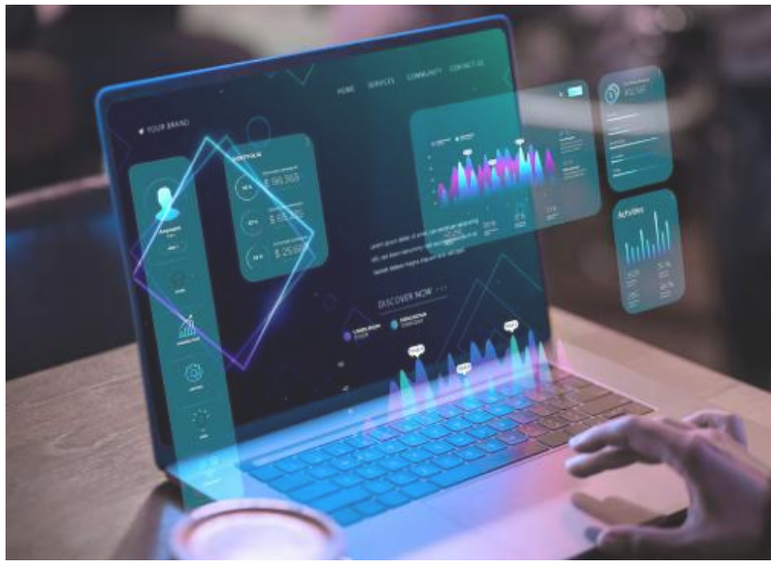
Teams es percibido por los usuarios como un entorno "confiable" y "corporativo". Al recibir una invitación aparentemente legítima, muchos usuarios pueden **aceptar sin sospecha**, **hacer clic en enlaces maliciosos**, **descargar archivos peligrosos** y **compartir información sensible**. Esto abre la posibilidad de ataques como **captura de credenciales**, **instalación de troyanos**, **exfiltración de datos**, **movimientos laterales** y **compromiso de cuentas corporativas**.

¿Cómo puede ser explotado por atacantes?

Los ciberdelincuentes pueden seguir un flujo similar:

1. Crear un ***tenant* de Microsoft 365** con una licencia económica o versión de prueba.
2. Enviar invitaciones de chat a colaboradores y empleados de múltiples organizaciones.
3. Redactar mensajes que aparenten ser comunicaciones profesionales de otras áreas de la organización objetivo o incluso de un líder de proceso.
4. Cuando el usuario acepta la invitación, el atacante puede enviar:
   - ❑ Un archivo infectado.
   - ❑ Un enlace a una página falsa.
   - ❑ Un documento señuelo para capturar credenciales.
5. La organización del usuario no puede bloquear el contenido porque no tiene control sobre el entorno invitante.
6. Si el usuario es engañado, el adversario **puede comprometer la cuenta**, **el dispositivo**, **las comunicaciones** o **la red corporativa**. Este tipo de ataque puede pasar desapercibido en monitoreos convencionales.

Impacto para Colombia y la región



- ❑ **Sectores afectados**: todos los sectores, pero principalmente gobierno, salud, financiero, educación, TIC, comercio, industria y turismo.

- ❑ **Riesgo alto**: el riesgo es considerado alto porque la vulnerabilidad permite que los ciberdelincuentes interactúen directamente con los usuarios dentro de una plataforma corporativa confiable (Microsoft Teams), utilizando invitaciones que parecen legítimas. Al aceptar el chat externo, el usuario queda expuesto en un entorno donde no aplican las protecciones de su organización, lo que facilita el phishing dirigido, la entrega de archivos maliciosos y la manipulación social.

- ❑ **Posibles consecuencias**:
  - ○ Compromiso de cuentas corporativas.
  - ○ Captura de credenciales críticas.
  - ○ Descarga de archivos maliciosos que pueden permitir control remoto del equipo.
  - ○ Fuga o exposición de información sensible.
  - ○ Paralización temporal de operaciones.
  - ○ Fraudes internos o acceso indebido a sistemas críticos.
  - ○ Escalamiento del incidente hacia *ransomware* u otros ataques más graves.

- ❑ **Implicaciones en seguridad digital**: esta vulnerabilidad pone en evidencia la creciente tendencia de ataques que utilizan plataformas legítimas como canal principal, evitando así muchas barreras tradicionales de seguridad. Para la región, implica la necesidad de reforzar políticas de colaboración externa, monitoreo entre *tenants*, educación a usuarios sobre riesgos dentro de herramientas “confiables” y la adopción de controles que limiten la interacción con entornos externos no verificados.

Técnicas MITRE ATT&CK asociadas

TÉCNICA	CÓDIGO	DESCRIPCIÓN
***Spearphishing* vía servicio**	**T1566.003**	Envío de mensajes dirigidos usando servicios de terceros para engañar a usuarios y lograr que hagan clic en enlaces o abran archivos maliciosos. Es la forma de *phishing* que encaja con invitaciones de chat externas por Teams.
Ejecución por acción del usuario (User Execution)	**T1204**	El adversario induce al usuario a ejecutar código o abrir un enlace o archivo malicioso (por ingeniería social). En el contexto de Teams, ocurre cuando la víctima abre un adjunto malicioso o hace clic en un enlace dentro del chat.
Cuentas válidas (Valid Accounts)	**T1078**	Uso o abuso de cuentas legítimas (incluyendo cuentas en la nube) para obtener acceso o persistencia.
Relación de confianza (Trusted Relationship)	**T1199**	Aprovechar relaciones o conexiones "confiables" entre organizaciones o servicios para obtener acceso o menos escrutinio. En este caso, la invitación desde un *tenant* "externo" puede ser percibida como una relación de confianza que el atacante explota.

Mitigaciones MITRE

MITIGACIÓN	CÓDIGO	RELEVANCIA
User Training (Formación y concienciación de usuarios)	**M1017**	Capacitar a usuarios para identificar y reportar invitaciones sospechosas, mensajes de ingeniería social y enlaces/adjuntos maliciosos reduce significativamente la efectividad de *spearphishing* vía servicio y la ejecución por acción de usuario.
Multi-factor Authentication (MFA)	**M1032**	MFA dificulta el abuso de cuentas válidas, incluso si un atacante consigue credenciales o induce a un usuario a aceptar una invitación que redirige a un flujo de autenticación malicioso. Implementar MFA en accesos a Microsoft 365 reduce el riesgo de compromiso por captura de credenciales.
User Account Management (Gestión del ciclo de vida de cuentas)	**M1018**	Políticas de creación, revisión, desactivación y privilegios mínimos para cuentas limitan el impacto cuando se explotan relaciones de confianza, *tenants* externos o se abusa de cuentas legítimas.
Behavior Prevention on Endpoint (Prevención basada en comportamiento en endpoints / EDR)	**M1040**	Controles de endpoint pueden bloquear la ejecución de archivos maliciosos o comportamientos sospechosos resultantes de que un usuario abra un adjunto o enlace en Teams y facilitar la detección temprana si un *guest* entrega malware desde un *tenant* externo.

Recomendaciones

- **Deshabilitar la funcionalidad "Chat with Anyone" en Microsoft Teams**: si no es estrictamente necesario, se recomeinda deshabilitar esta capacidad desde la política de mensajería (TeamsMessagingPolicy) para evitar que los usuarios puedan iniciar o recibir conversaciones desde direcciones externas no verificadas. Esta es la medida preventiva más efectiva mientras Microsoft no lance un ajuste estructural.

- **Restringir la colaboración externa y el acceso entre *tenants***: configurar estrictamente las políticas de colaboración externa y acceso B2B en Entra ID, limitando qué organizaciones pueden enviar solicitudes de chat, permitiendo solo dominios confiables o bloqueando la funcionalidad por completo según el nivel de riesgo.

- **Monitorear el tráfico de Teams**: monitorear eventos relacionados con mensajes provenientes de usuarios externos, solicitudes de acceso B2B y actividad inusual entre *tenants*, identificando patrones que puedan indicar intentos de phishing o abuso de la funcionalidad.

- **Sensibilizar a los usuarios sobre los riesgos de aceptar chats externos**: capacitar a los empleados para reconocer mensajes sospechosos en Teams, evitar interactuar con contactos no solicitados, verificar remitentes y reportar cualquier invitación inesperada que llegue al entorno corporativo.

- **Aplicar Zero Trust en interacción entre tenants**: aplicar controles de confianza cero que evalúen cada solicitud de conexión entre *tenants*, evitando asumir que un chat externo es seguro por el simple hecho de que provenga de una cuenta Microsoft válida.

Fuentes

Ontinue, B2B Guest Access Creates an Unprotected Attack Vector, artículo de blog.
https://www.ontinue.com/resource/blog-microsoft-chat-with-anyone-understanding-phishing-risk/
Cyber Security News, 2025-11-27, Microsoft Teams' New "Chat with Anyone" Feature Exposes Users to Phishing and Malware Attacks, artículo de noticia.
https://cybersecuritynews.com/microsoft-teams-guest-chat-vulnerability/