



OWASP 2023
GLOBAL
AppSec

WASHINGTON

DC

OCT 30 • NOV 3





OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3



CREDENTIAL SHARING AS A SERVICE: THE DARK SIDE OF NO CODE

Michael Bargury @mbrg0
Zenity

mbgsec.com

About me

- CTO and Co-founder @ Zenity
- OWASP LCNC Top 10 project lead
- Dark Reading columnist
- OWASP, BlackHat, Defcon, BSides

- Hiring top researchers, engs & pms!



@mbrg0



mbgsec.com





Outline

- No Code in a nutshell
- No Code attacks observed in the wild and recreated with **POWERPWN**
 - Living off the land – account takeover, lateral movement, PrivEsc, data exfil
 - Phishing made easy
 - Hiding in plain sight
- How to defend
- The latest addition to your red team arsenal



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

No-Code in a Nutshell

@mbrg0

mbgsec.com

C# devs today

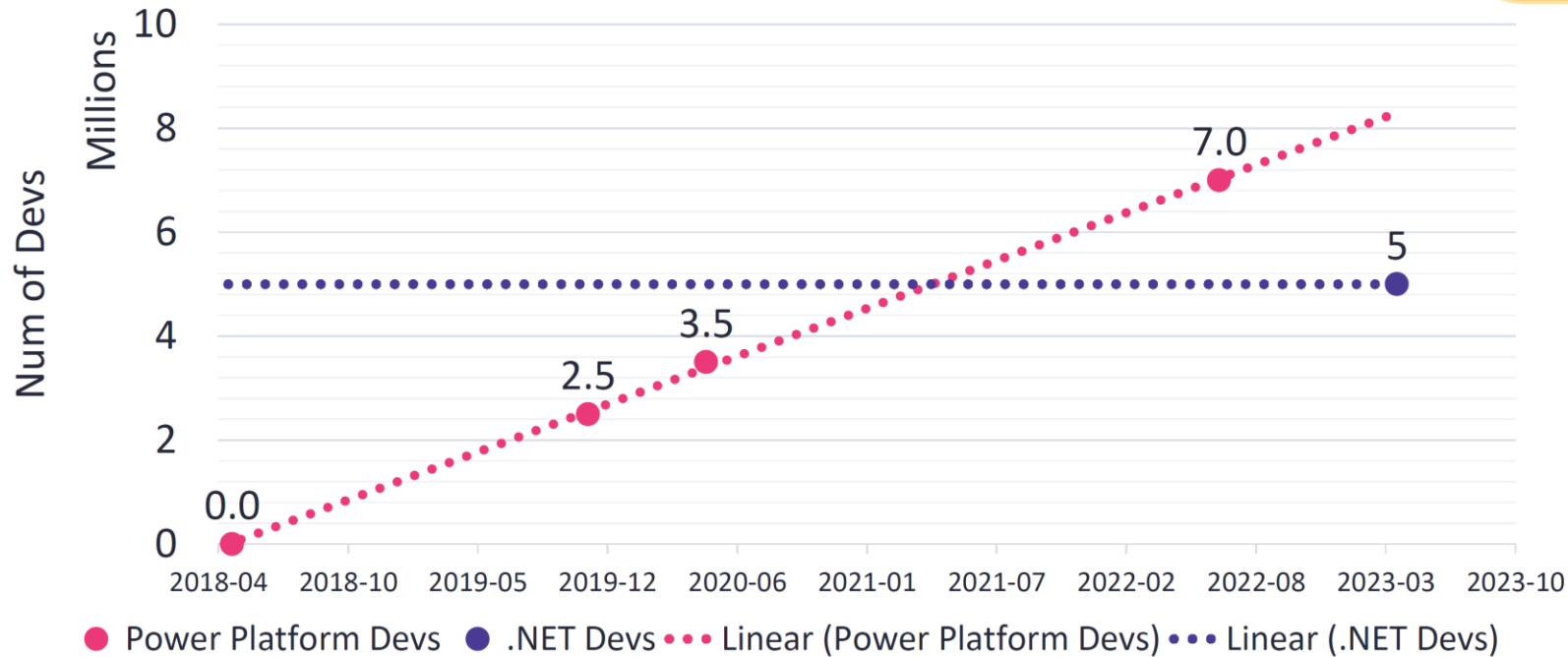


Credential Sharing as a Service: The Dark Side of No Code

Michael Bargury
RSAC 2023

~8M active Power devs today!

More MSFT low-code devs than .NET devs, today!



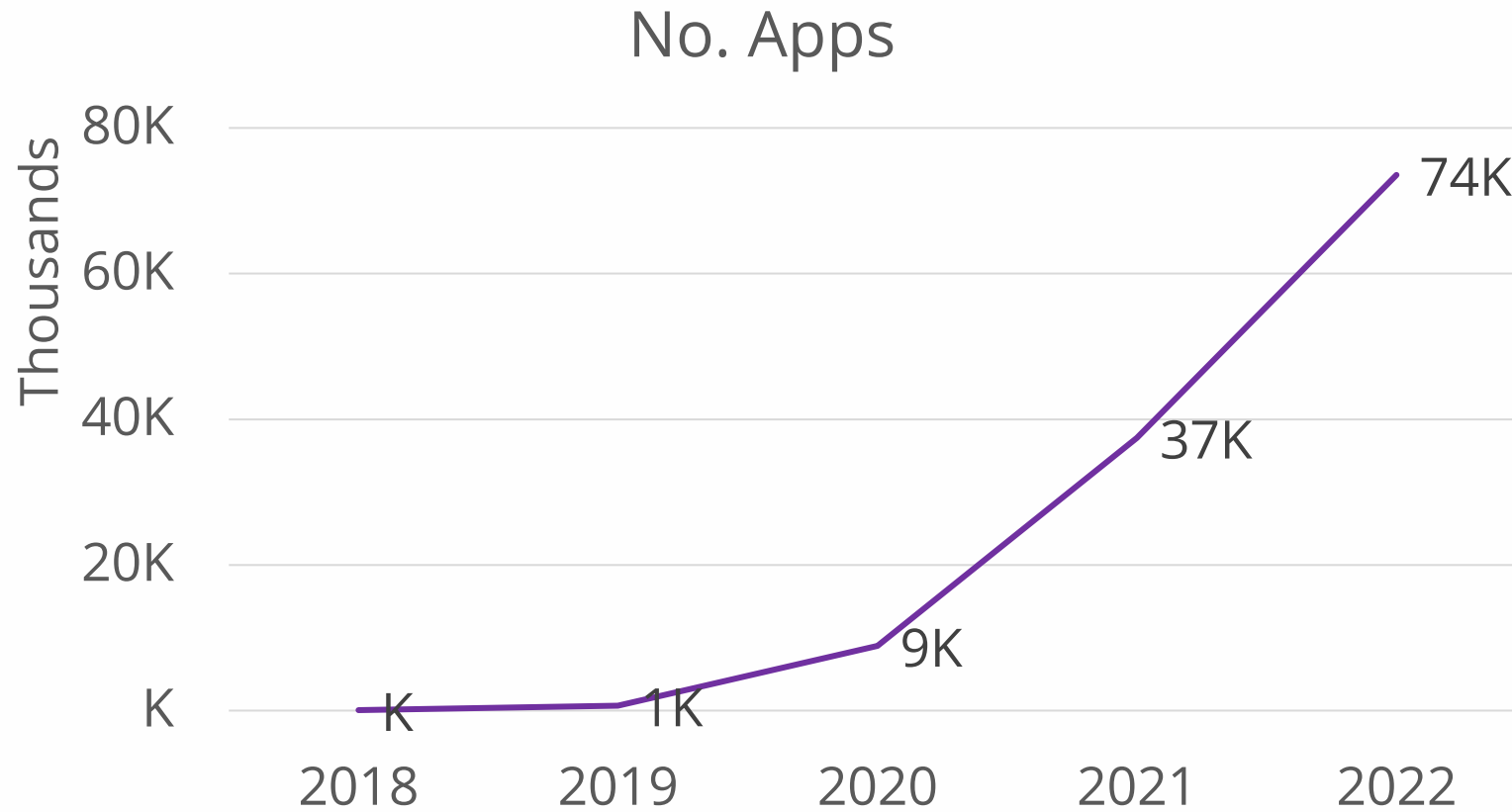
Sources: Microsoft Build 2018, Ignite 2019, Build 2020, Protocol 2022



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

Michael Bargury
RSAC 2023

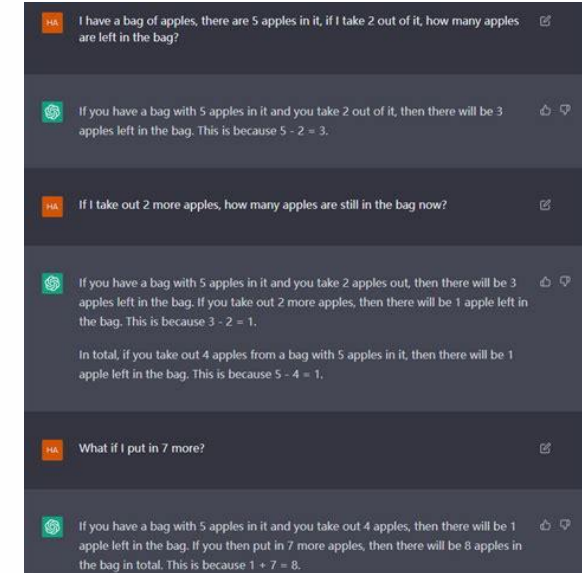
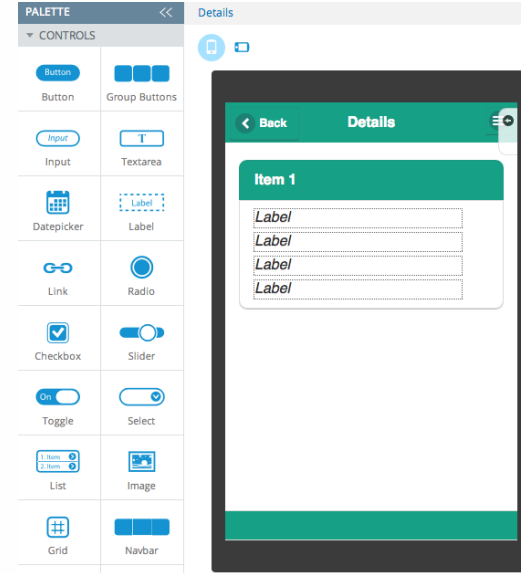
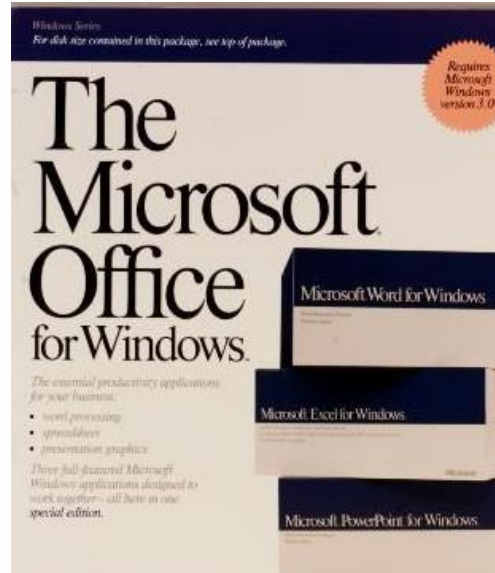
Exponential Growth in Citizen Development



Why No Code?



“Everyone is a developer”



Tech evolution

Build everything

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

The image displays three overlapping screenshots from a no-code automation platform. The top-right screenshot shows a workflow configuration with three steps: a trigger 'When a new email arrives' (1s), an action 'Apply to each attachment' (7s), and another action 'Upload to Google Drive' (5s). The middle screenshot shows the configuration for a 'Trigger' event '1. New Mention in Slack', with a 'Choose account' section listing two Slack accounts: '@michaelbargury (pwntoso)' and '@michaelbargury (CTOs)'. The bottom-left screenshot shows an 'Insert' menu with a search bar and a list of UI components including 'Text label', 'Text input', 'Vertical gallery', 'Rectangle', 'Date picker', 'Button', 'Input', 'Display', 'Layout', 'Media', 'Icons', 'Shapes', 'Charts', 'AI Builder', and 'Mixed Reality'.

Tree view [Close]

Screens Components

Search

+ New screen ▾

> App

Screen1 ...

Add an item from the Insert pane or connect to data

Copilot PREVIEW [Close]



What do you want to do?

Describe what you want to do with this app, and AI will do it for you.

- Add a text label
- Add a gallery
- Add a button
- Add an email screen

What do you want to do with this app? [Submit]

Make sure AI-generated content is accurate and appropriate before using. [See terms](#)

Source:
@RezaDorrani

Available in every major enterprise



Recap

- ✓ Available on every major enterprise
- ✓ Has access to business data and powers business processes
- ✓ Runs on somebody else's infra
- ✓ Built by citizen devs



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

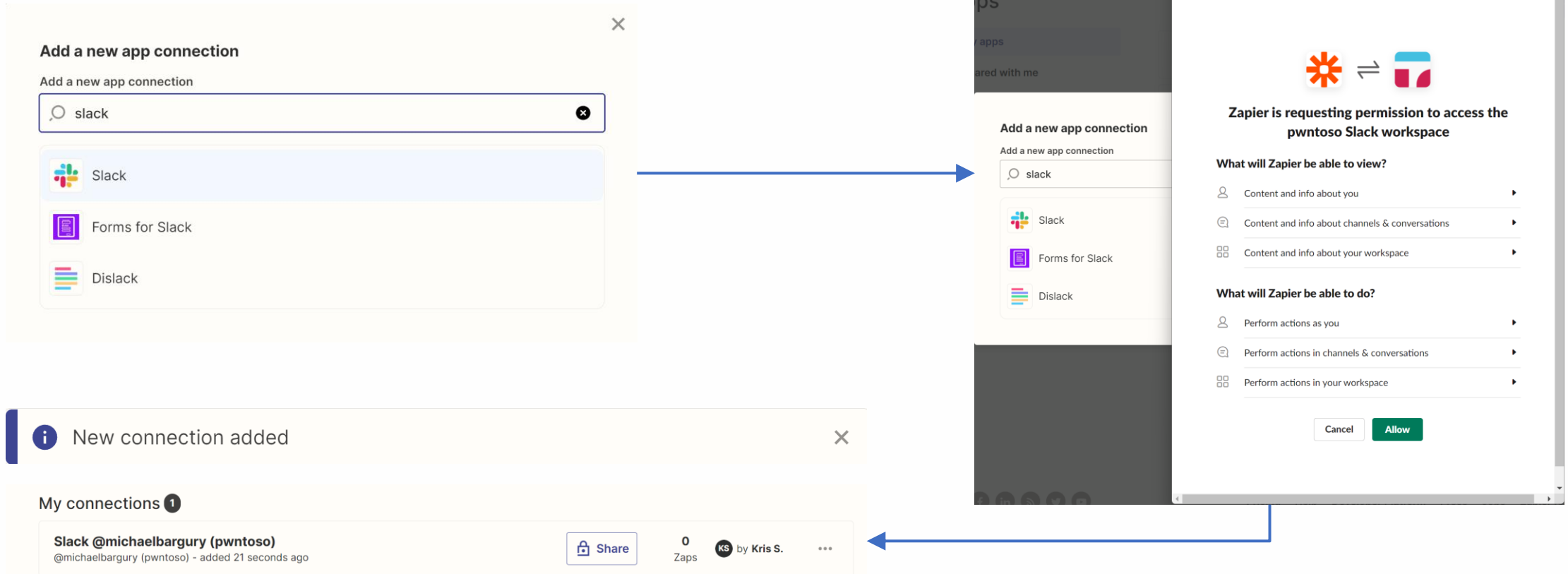
No Code Attacks In The Wild: Living off the land

@mbrg0

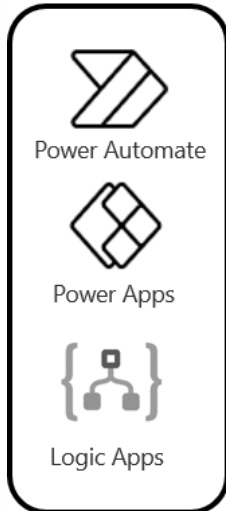
mbgsec.com



Step by step



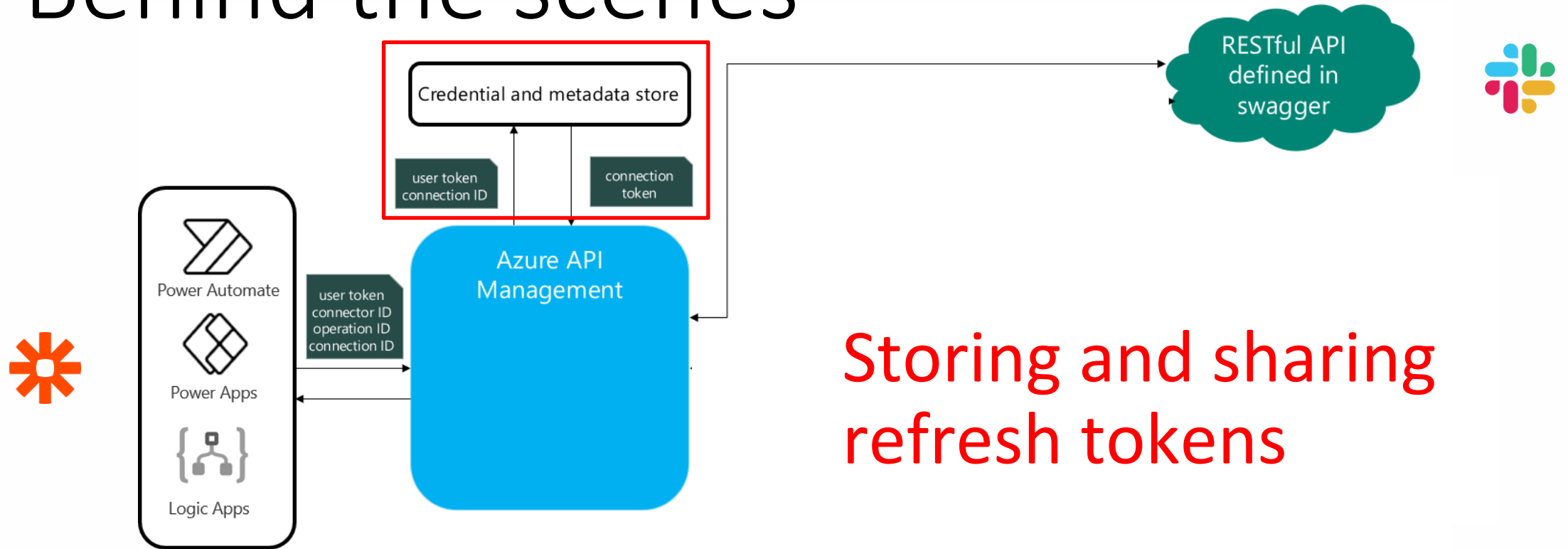
Behind the scenes



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

 Premium


Add info to a Google Sheet from new Webhook POST requests

 Premium

Create SQL Server rows from new Google Forms responses

 Premium


Get Slack notifications for new information from a Webhook

 →

Send myself a reminder in 10 minutes

By Microsoft


Instant
460902

 Webhooks by

Save Gmail attachments to your Google Drive

By Microsoft


Automated
32731

 →

Send an email to responder when response submitted in Microsoft Forms

By Microsoft Power Automate Community


Automated
214763

 →

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

By Microsoft Power Automate Community

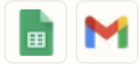
Automated
350

 →

Save Outlook.com email attachments to your OneDrive

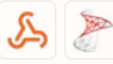
By Microsoft Power Automate Community

Automated
168098

 →











































Send emails via Gmail when Google Sheets rows are updated

Google Sheets + Gmail

 →

Add SQL Server rows with new caught webhooks

Webhooks by Zapier + SQL Server

Name	Icon	Account/Service	Icon	Account/Service	Icon	Account/Service	Time
		[redacted]ystage.com Azure Resource Manager		[redacted]tage.com Office 365 Outlook			1 h ago
Zenity Zenity		[redacted]ystage.com Office 365 Management API		[redacted]tage.com Office 365 Users			5 d ago
(BaseResourceUrl) HTTP with Azure AD		ConnectionToFadiStorageAccount Azure Blob Storage		[redacted]6681@gmail.com OneDrive			9 mo ago
[redacted]stage.com Microsoft Teams		[redacted]ure-sql-server.database.wind... SQL Server		Outlook.com Outlook.com			57 min ago
[redacted]y.io SQL Server		[redacted]ystage.com Azure Blob Storage		RSS RSS			4 mo ago
[redacted]stage.com SQL Server		[redacted]ystage.com Microsoft Dataverse		[redacted]tage.com Salesforce			2 wk ago
[redacted]stage.com SQL Server		Connective eSignatures Connective eSignatures (preview)		Mail Mail			9 mo ago
[redacted]stage.com SharePoint		Connective eSignatures Connective eSignatures (preview)		Mail Mail			7 mo ago
[redacted]stage.com Power Platform for Admins		23 DB2		aviv-demo-2 ServiceNow			8 mo ago
[redacted]stage.com Power Platform for Admins		[redacted]h@gmail.com Dropbox		Aviv-Demo ServiceNow			9 mo ago
[redacted]stage.com Power Apps for Makers		File System File System		Aviv-Demo ServiceNow			8 mo ago
[redacted]stage.com Power Apps for Admins		Notifications Notifications		SFTP SFTP			9 mo ago
[redacted]stage.com Planner		Vendor Server FTP		SFTP - SSH SFTP - SSH			8 mo ago
[redacted]stage.com OneNote (Business)		FTP FTP		[redacted]tage.com SharePoint			3 h ago

Credential Sharing as a Service

The screenshot displays the Power Automate interface. On the left is a navigation sidebar with options like Home, Action items, My flows, Create, Templates, Connectors, Data, Monitor, AI Builder, Process advisor, Solutions, and Learn. The main area is titled 'Connections in Zenity Stage (default)' and contains a table of connections:

Name	Modified
ConnectionToFadStorageAccount Azure Blob Storage	10 mo ago
SQL Server azure-sql-server.database.wind...	8 mo ago
stage.com Azure Blob Storage	11 mo ago
stage.com Microsoft Dataverse	
Connective eSignatures Connective eSignatures (preview)	
Connective eSignatures Connective eSignatures (preview)	
23 DBZ	
File System File System	
Notifications Notifications	
Vendor Server FTP	
FTP FTP	
ba2g@gmail.com Gmail	1 wk ago Connected

Below the connections table is a 'zapier' logo and an 'Apps' section with 'My apps' and 'Custom integrations'.

On the right side of the interface, there is an 'Assets' section with a table of assets:

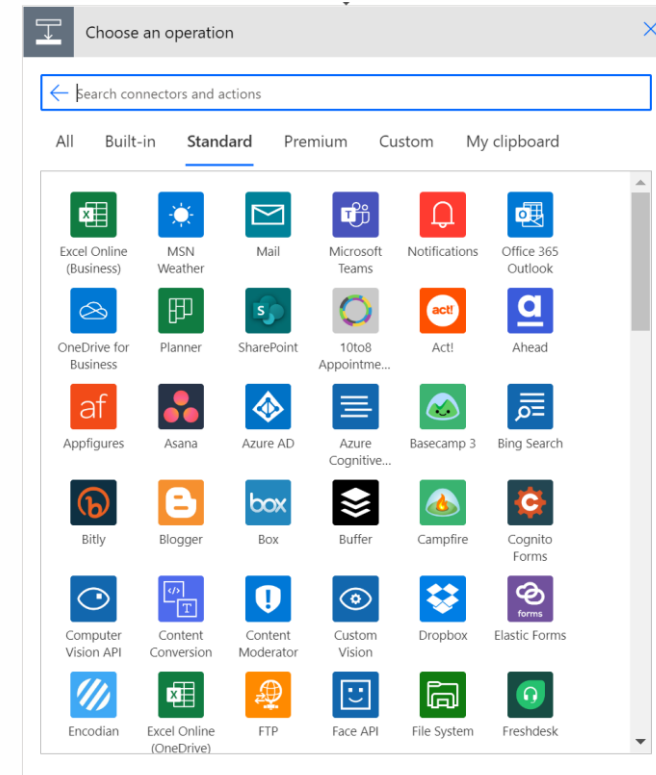
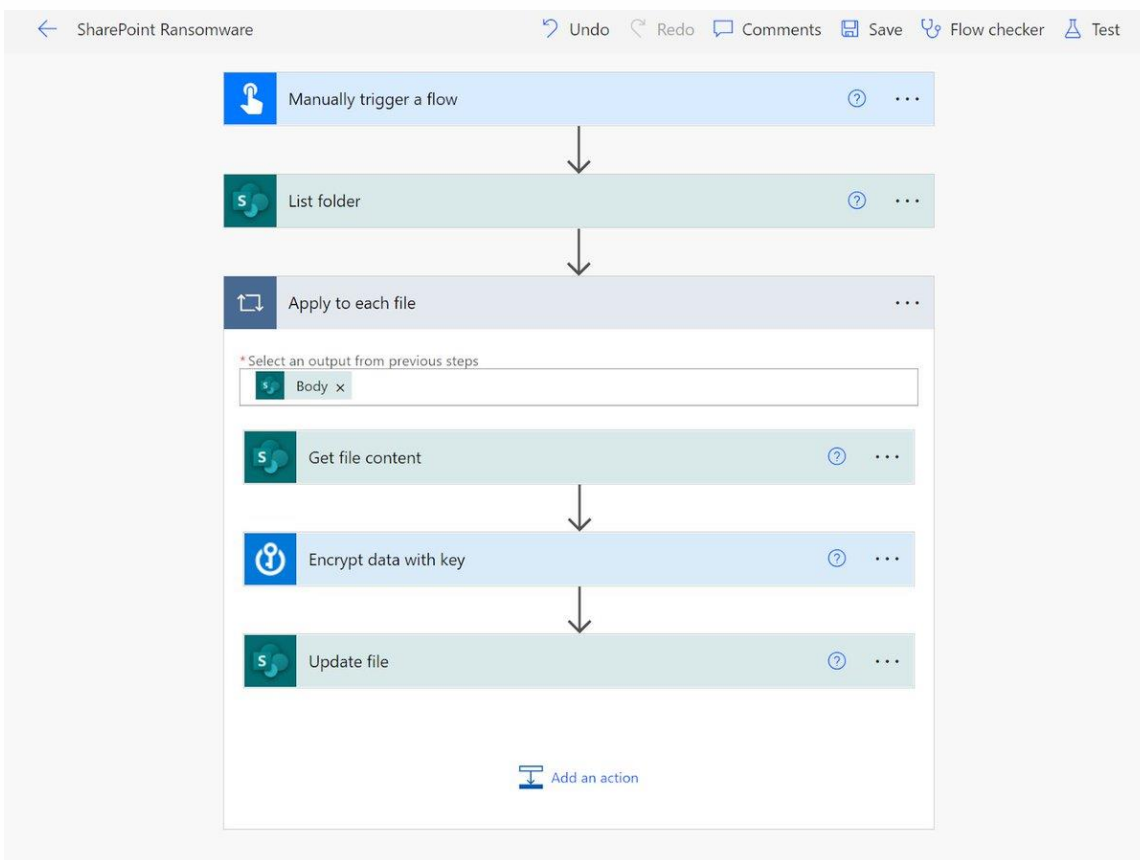
Asset	Status	Created	Recipes
Management	Connected	May 22 at 1:47 am	4
dev_HTTP account	Connected	Feb 6 at 1:21 am	0
dev_HTTP account	Connected	Feb 6 at 1:21 am	0
dev_twitter	Connected	Feb 10 at 1:40 am	1
FTP at test.rebox.net	Connected	Apr 9, 2021, at 7:05 am	932
@gmail.com gmail	Connected	Apr 9, 2021, at 5:05 am	1

Credential Sharing as a Service

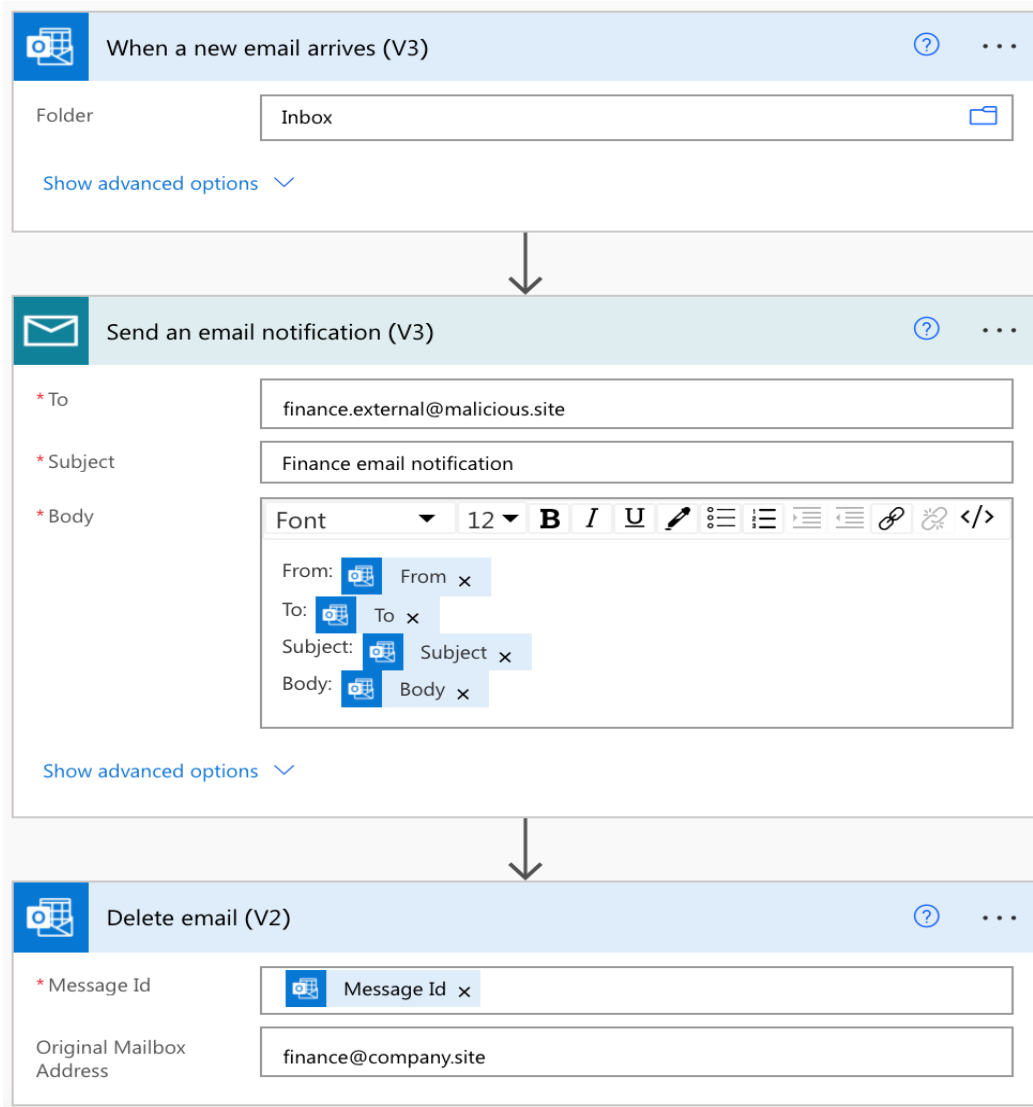
The screenshot displays the Power Automate interface. On the left is a navigation pane with options like Home, Action items, My flows, Create, Templates, Connectors, Data, Monitor, AI Builder, Process advisor, Solutions, and Learn. The main area is titled 'Connections in Zenity Stage (default)' and lists various connectors such as Azure Blob Storage, SQL Server, Microsoft Dataverse, and eSignatures. A large, semi-transparent image of a baby's face is overlaid on the connections list. Below the connections list is an 'Apps' section showing 'My apps' (Shared with me, Custom integrations) and specific app integrations for Gmail (2 Connections, 5 Zaps) and Google Sheets (1 Connection, 2 Zaps). A table on the right side of the interface shows a list of connections with columns for Name, Status (all 'Connected'), and Recipes. A green callout box in the bottom right corner contains a checkmark icon and the text 'Privilege escalation'.

Name	Status	Recipes
ConnectionToFadIStorageAccount Azure Blob Storage	Connected	4
SQL Server azure-sql-server.database.win	Connected	0
stage.com Azure Blob Storage	Connected	0
stage.com Microsoft Dataverse	Connected	1
Connective eSignatures Connective eSignatures (preview)	Connected	932
Connective eSignatures Connective eSignatures (preview)	Connected	1
23 DB2	Connected	
File System File System	Connected	
Notifications Notifications	Connected	
Vendor Server FTP	Connected	
FTP FTP	Connected	
ba2g@gmail.com Gmail	Connected	

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 Dummy Edit

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

Show advanced options

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

Lateral movement

Power Pwn

Black Hat Arsenal USA 2023 DEFCON 30

Stars 173 Follow michael.bargury owasp.org

Power Pwn is an offensive security toolset for Microsoft Power Platform.

Install with `pip install powerpwn`.

Check out our [Wiki](#) for docs, guides and related talks!



	command	
dump	Recon for available data connections and dump their content.	
gui	Show collected resources and data via GUI.	
backdoor	Install a backdoor on the target tenant	
nocodemalware	Repurpose trusted execs, service accounts and cloud services to power a malware	
phishing	Deploy a trustworthy phishing app.	

Introducing **powerpwn**

Find us on GitHub!

github.com/mbrg/power-pwn





OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

CREDENTIAL SHARING AS A SERVICE: THE DARK SIDE OF NO CODE

@mbrg0



black hat[®]
USA 2023

AUGUST 9-10, 2023
BRIEFINGS

All You Need Is Guest

Michael Bargury @mbrg0
Zenity

BlackHat
USA 2023

mbgsec.com

#BHUSA @BlackHatEvents



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30 - NOV 3

CREDENTIAL SHARING AS A SERVICE: THE DARK SIDE OF NO CODE

@mbrg0

POWERPWN DEMO

github.com/mbrg/power-pwn



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

No Code Attacks In The Wild: Phishing made easy

@mbrg0

mbgsec.com

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



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30 - NOV 3

CREDENTIAL SHARING AS A SERVICE: THE DARK SIDE OF NO CODE

@mbrg0

POWERPWN DEMO

github.com/mbrg/power-pwn


black hat[®]
USA 2023

AUGUST 9-10, 2023
BRIEFINGS

Sure, Let Business Users Build Their Own. What Could Go Wrong?

Michael Bargury @mbrg0
Zenity

BlackHat
USA 2023

mbgsec.com



OWASP 2023
GLOBAL
AppSec

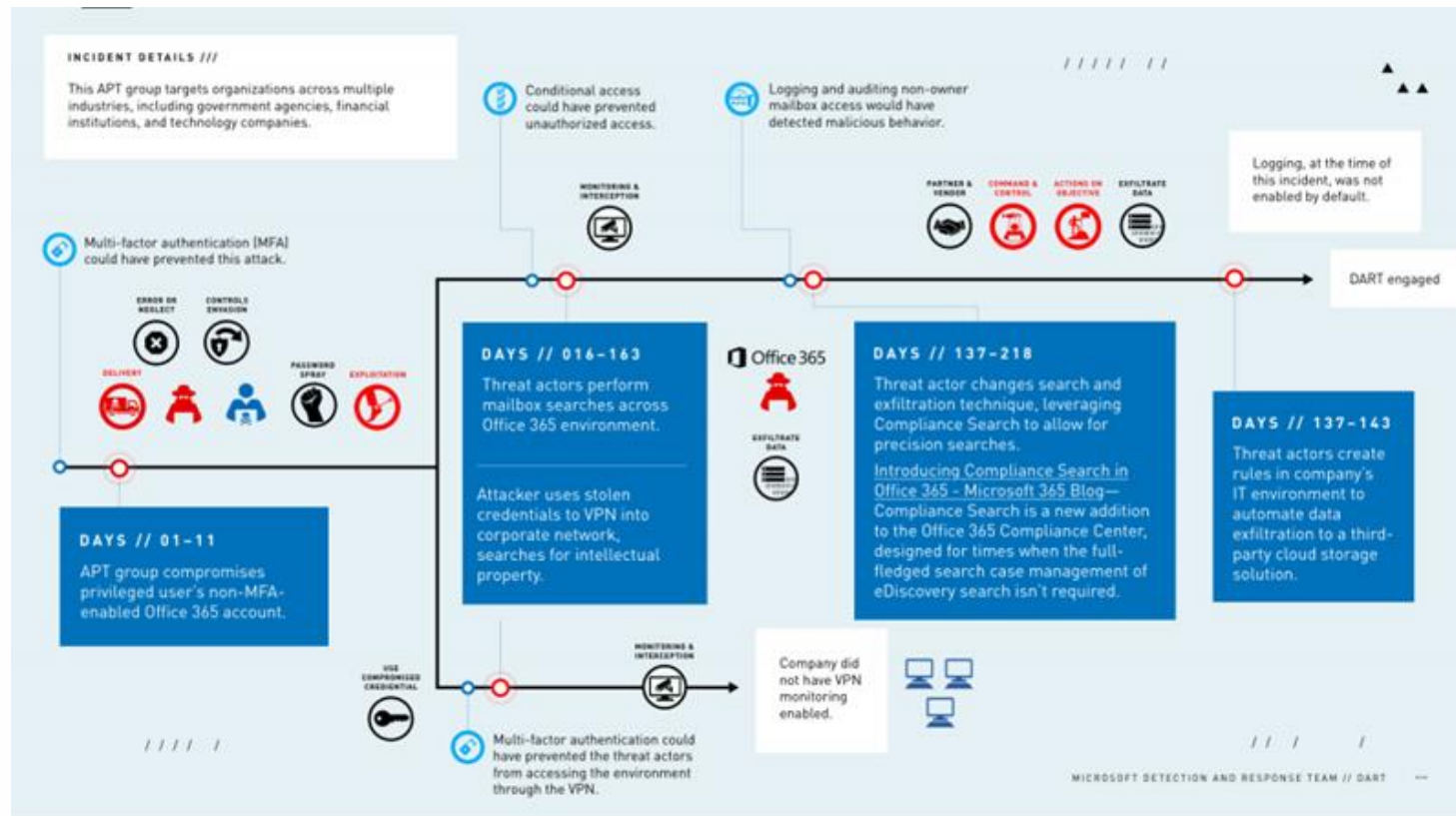
WASHINGTON
DC
OCT 30-NOV 3

No Code Attacks In The Wild: A backdoor that survives user deletion

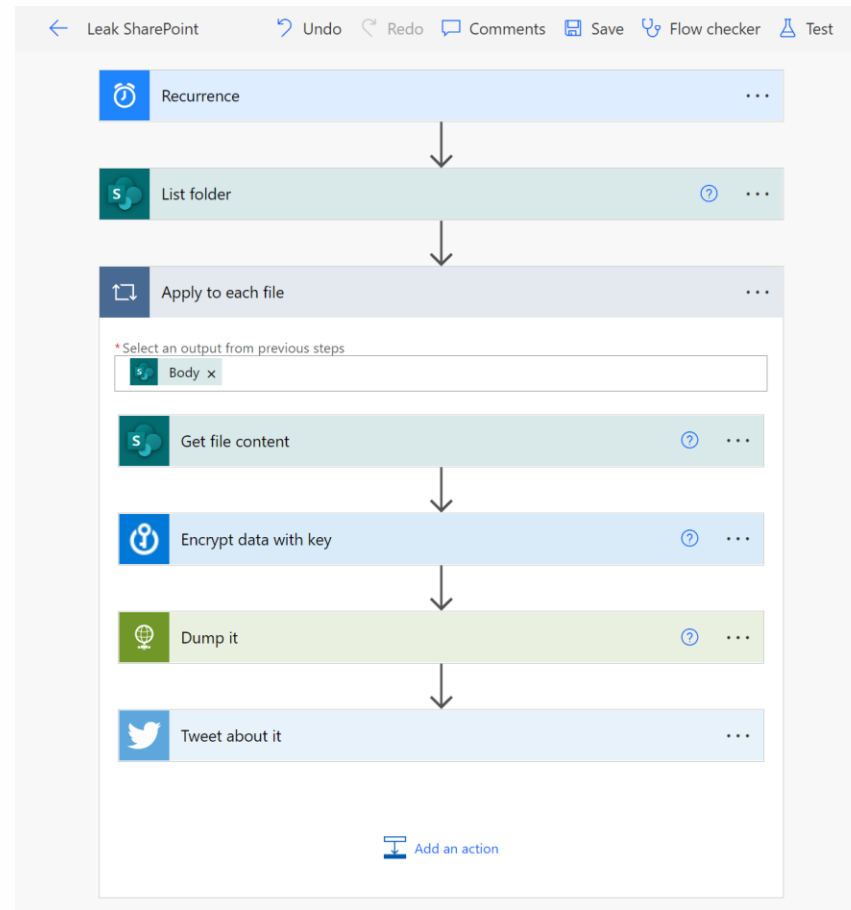
@mbrg0

mbgsec.com

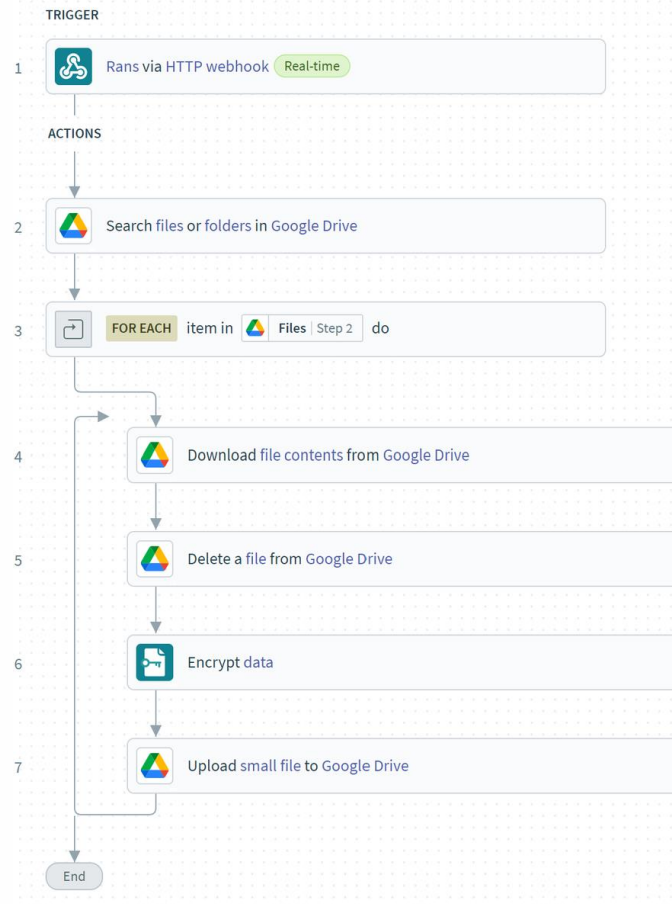
This has been done before



Dump files and tweet about it on a schedule



Encrypt on command



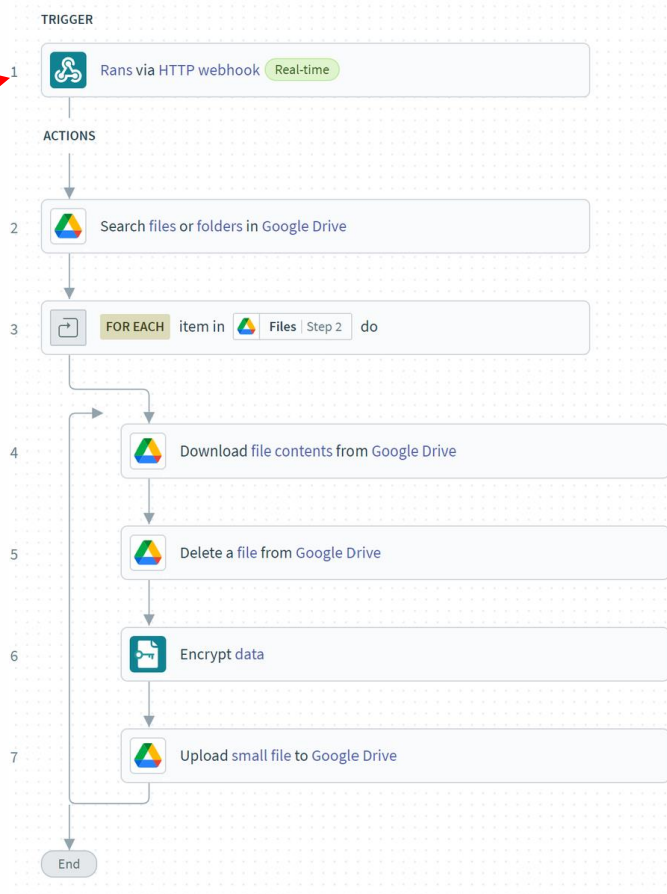
Persistence

What do we want?

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

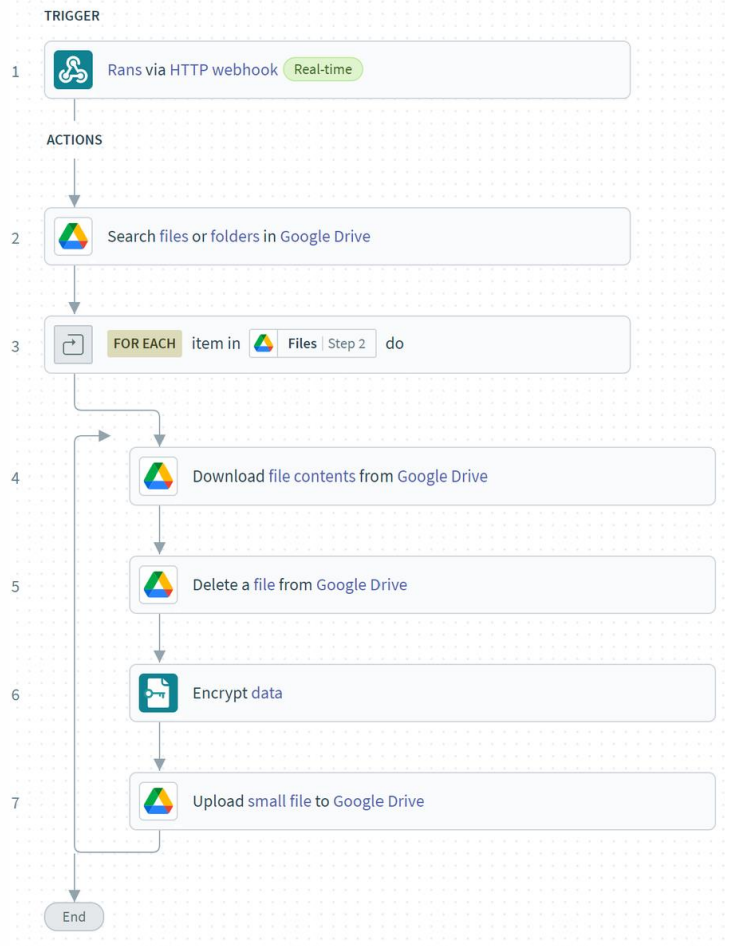
Persistency v1

Persistency

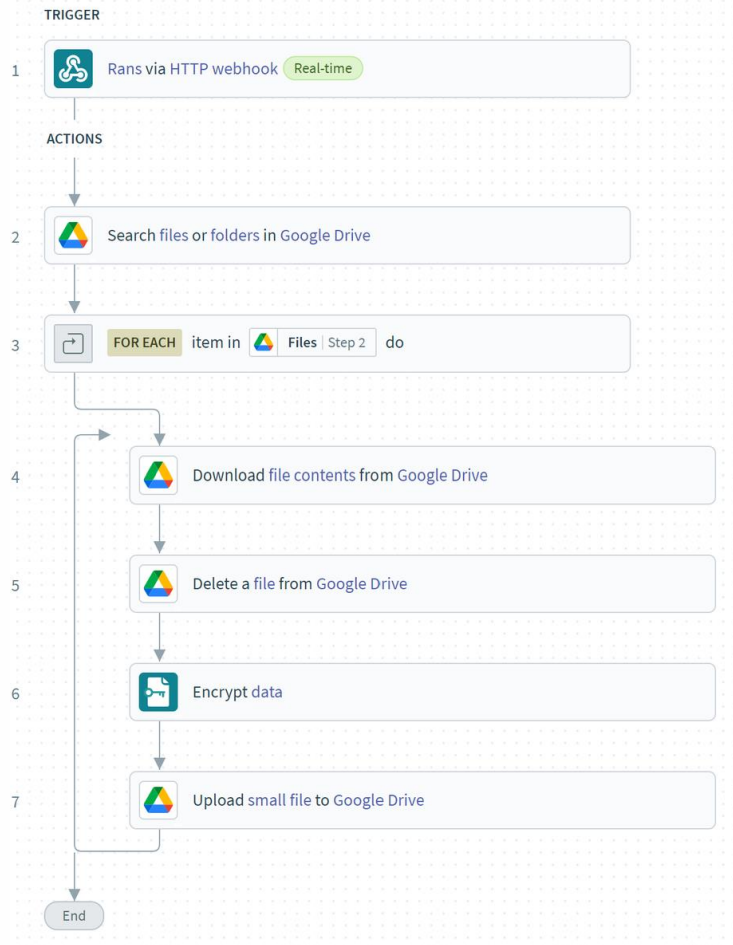


Persistency v1

What do we want?



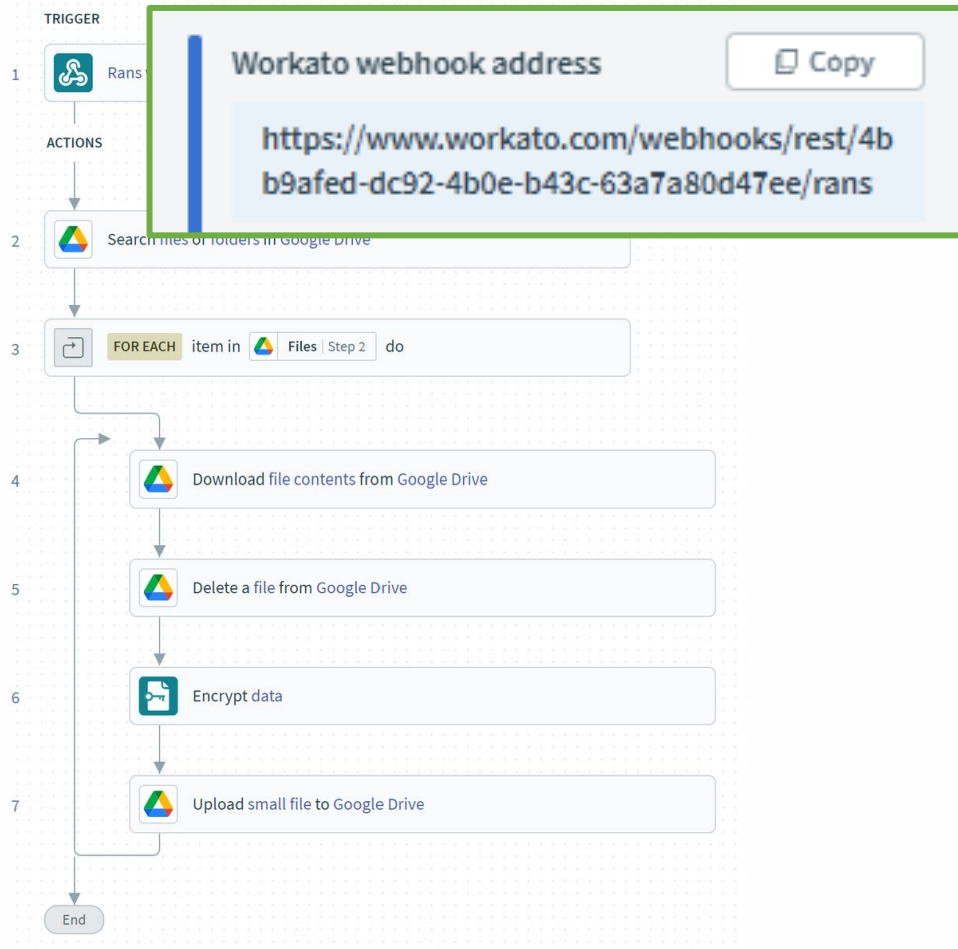
Persistency v1



What do we want?

- Remote execution
- Arbitrary payloads

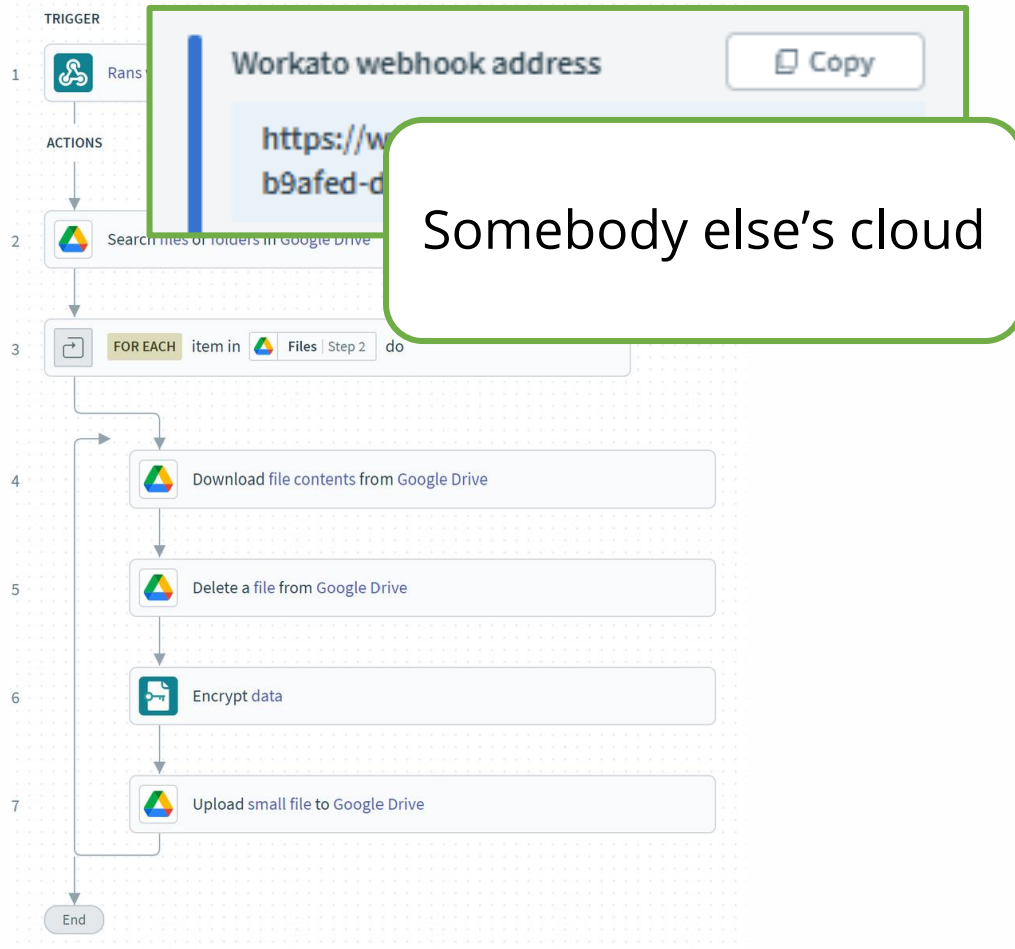
Persistency v1



What do we want?

- Remote execution
- Arbitrary payloads
- Maintain access

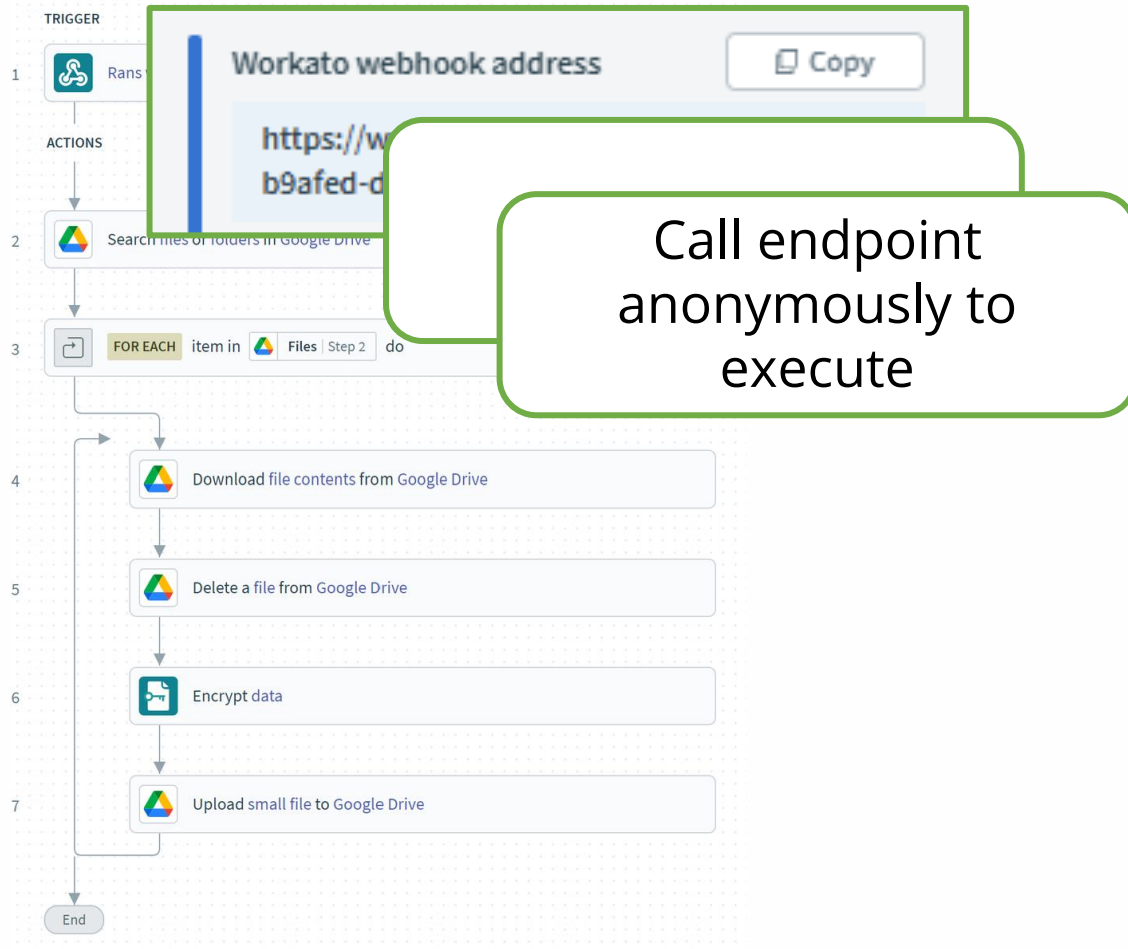
Persistency v1



What do we want?

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

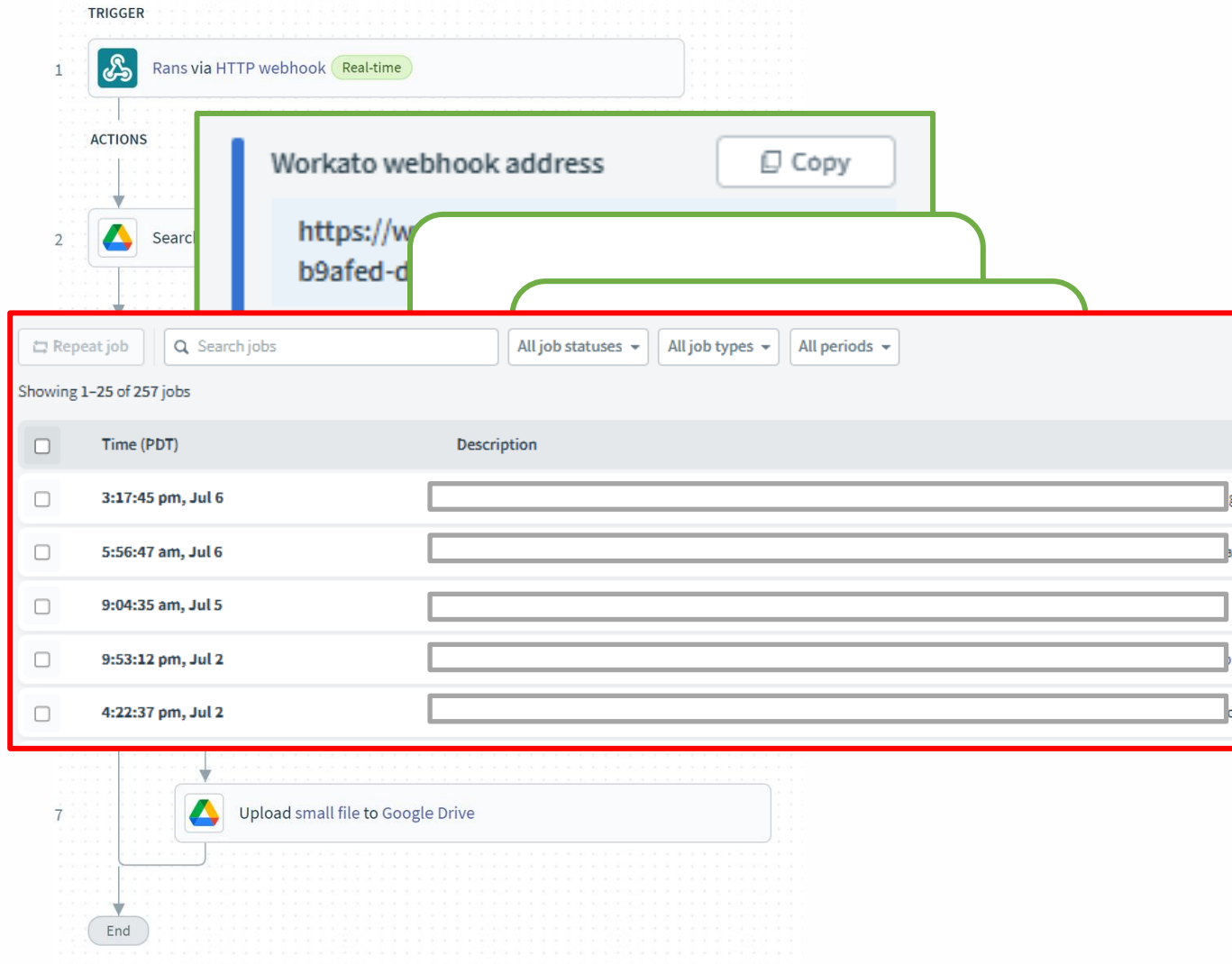
Persistency v1



What do we want?

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

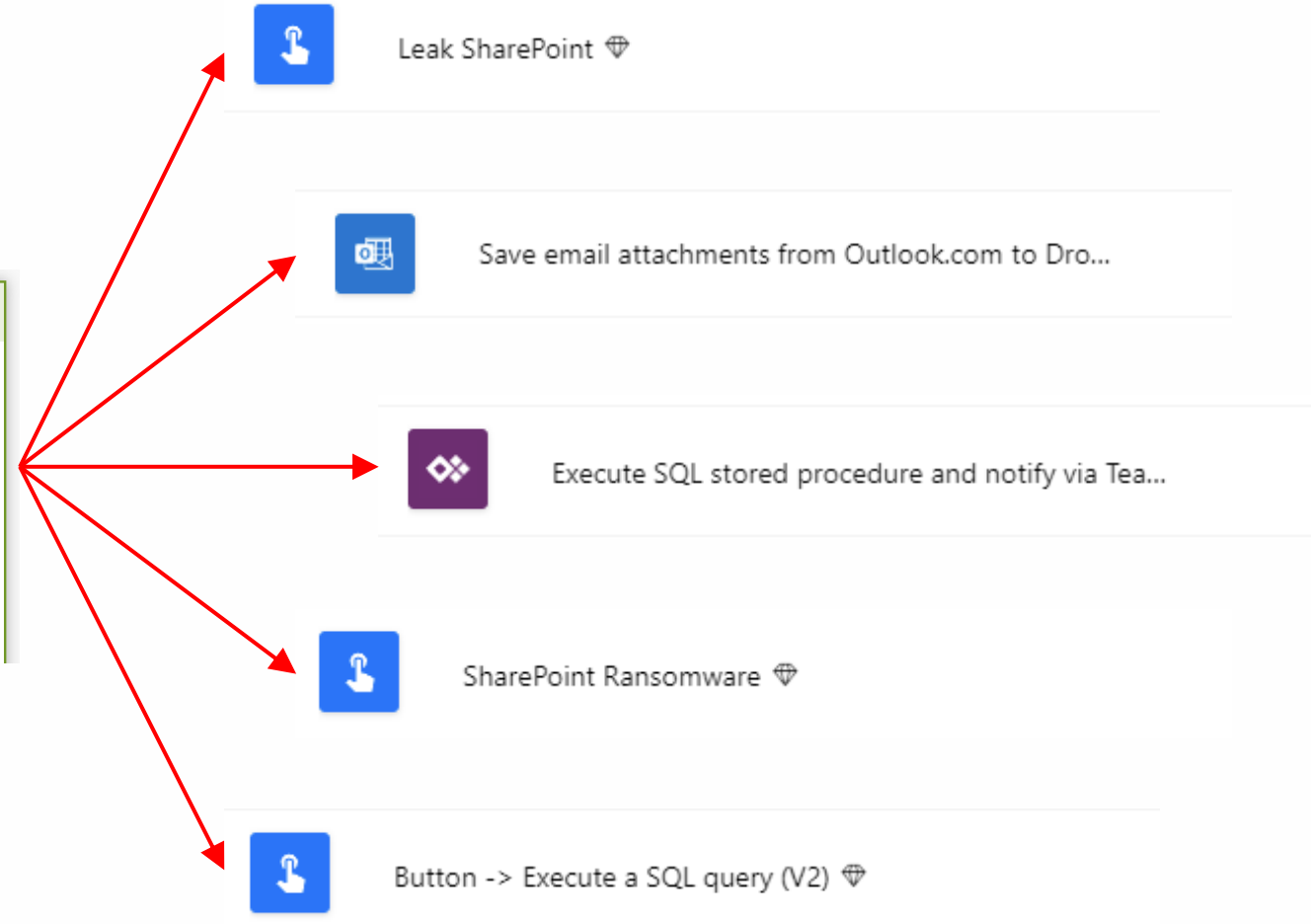
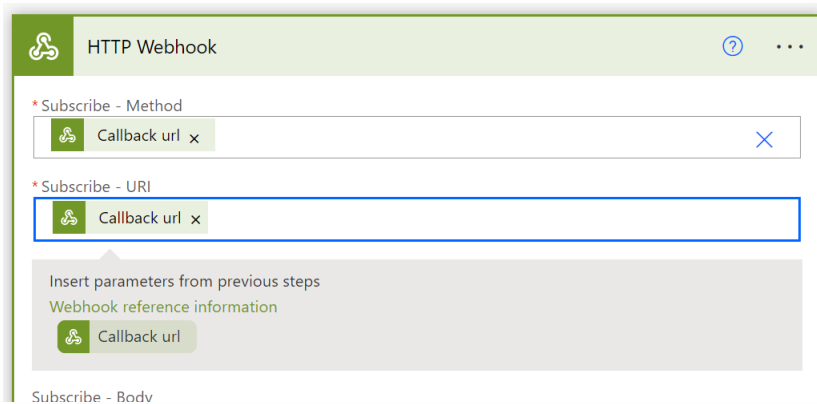
Persistency v1



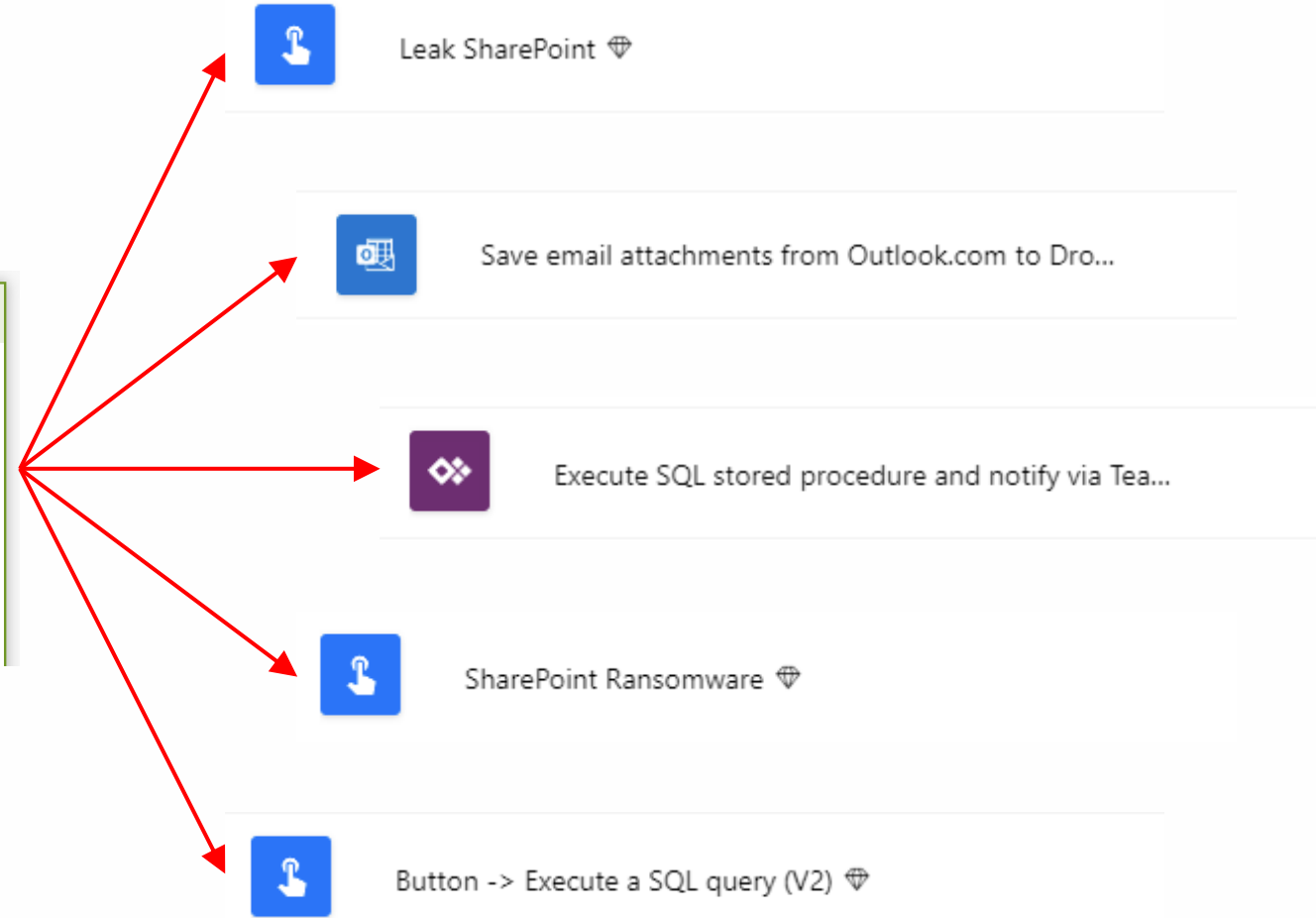
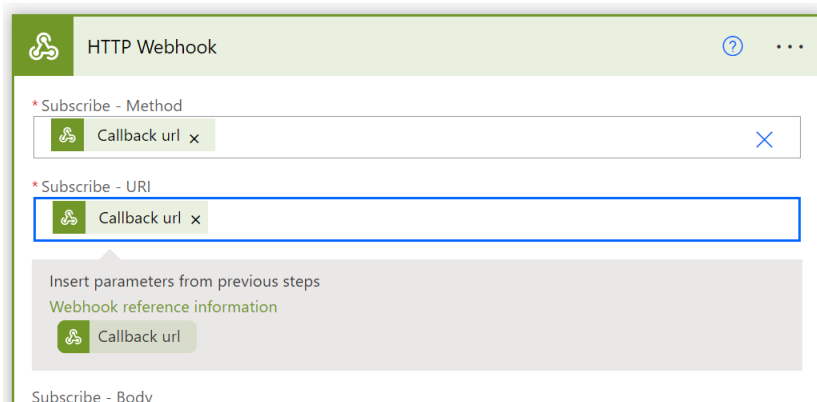
What do we want?

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

Persistency v2



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**

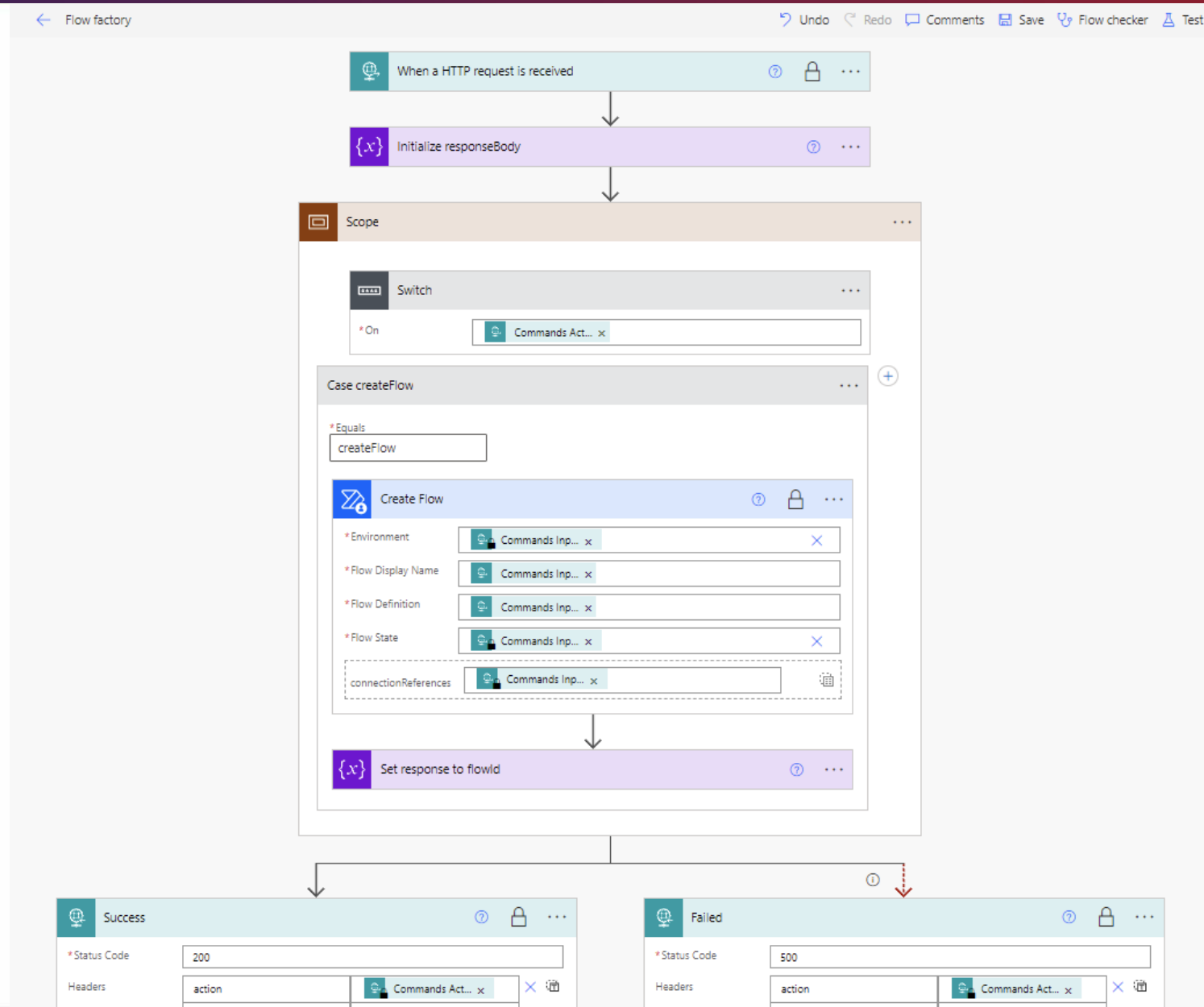
Executing arbitrary commands

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](#)





Create a flow

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

{x} Set response to flowId

Add an action

List authenticated sessions to use

Case getConnections

*Equals
getConnections

List My Connections

*Environment
Commands Inp... x

{x} Set response to connections list

Delete a flow

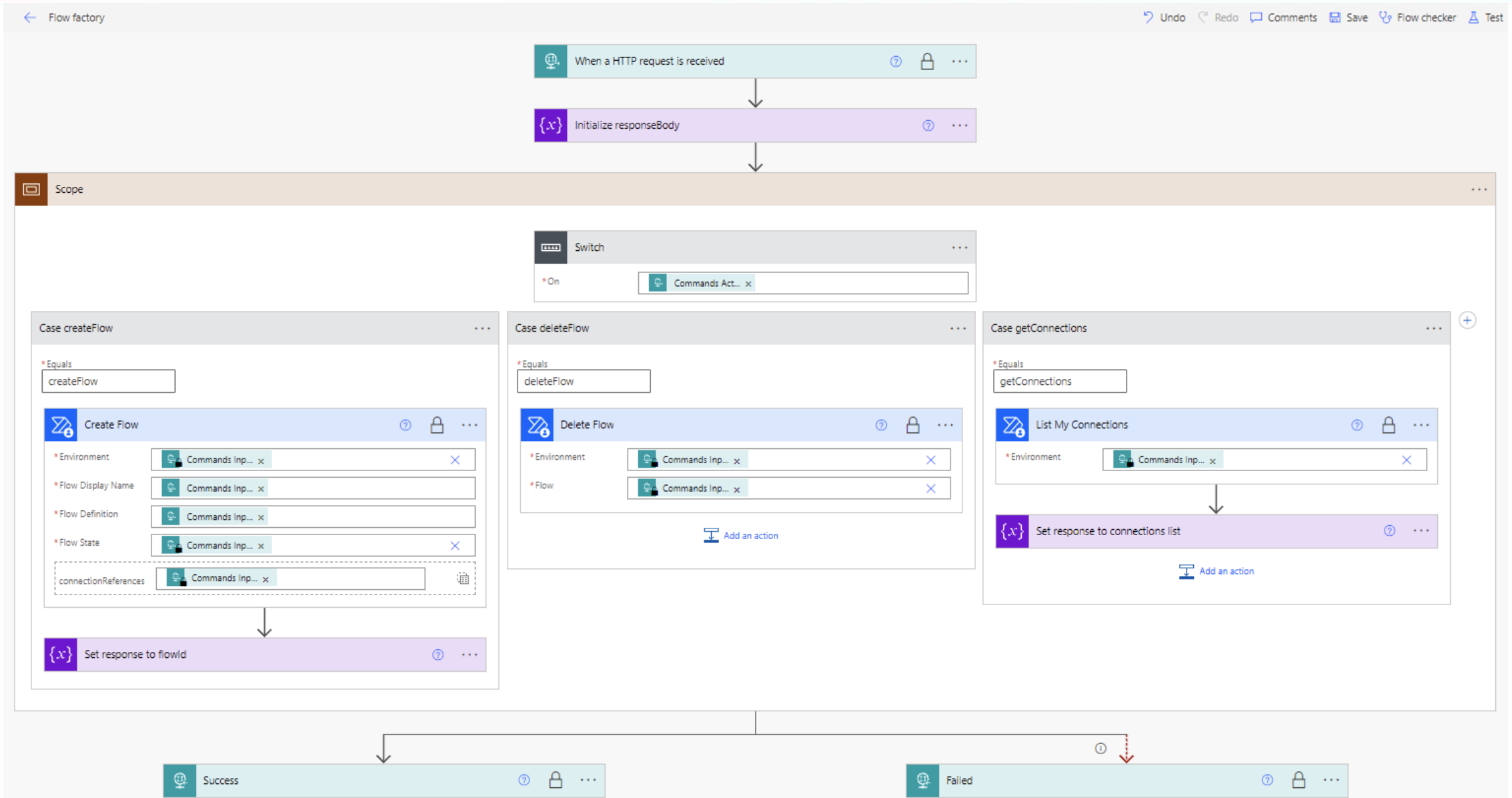
Case deleteFlow

*Equals
deleteFlow

Delete Flow

*Environment
Commands Inp... x

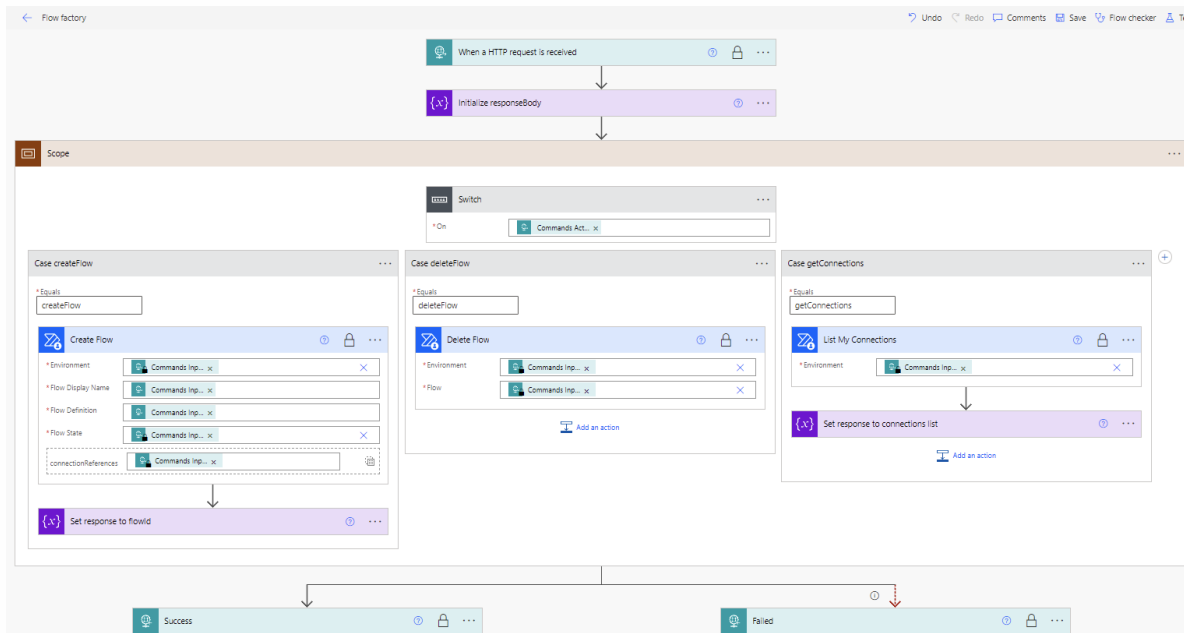
*Flow
Commands Inp... x



powerpwn (persistency v3)

What do we want?

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



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



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30 - NOV 3



Learn more: github.com/mbrg/defcon30
Twitter: @mbrg0

Low Code High Risk:

Enterprise Domination via Low Code Abuse

Michael Bargury @ Zenity



DEFCON 30

mbrgsec.com

DEF
CON



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30 - NOV 3

POWERPWN DEMO

github.com/mbrg/power-pwn

Summary

- No 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
 - Phishing made easy
 - Hiding in plain sight
- **powerpwn** - the latest addition to your red team arsenal
- How to defend your org



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3

How To Stay Safe

@mbrg0

mbgsec.com

Protect your org!

Build secure apps

Protect your org!

Build secure apps
1. Don't overshare

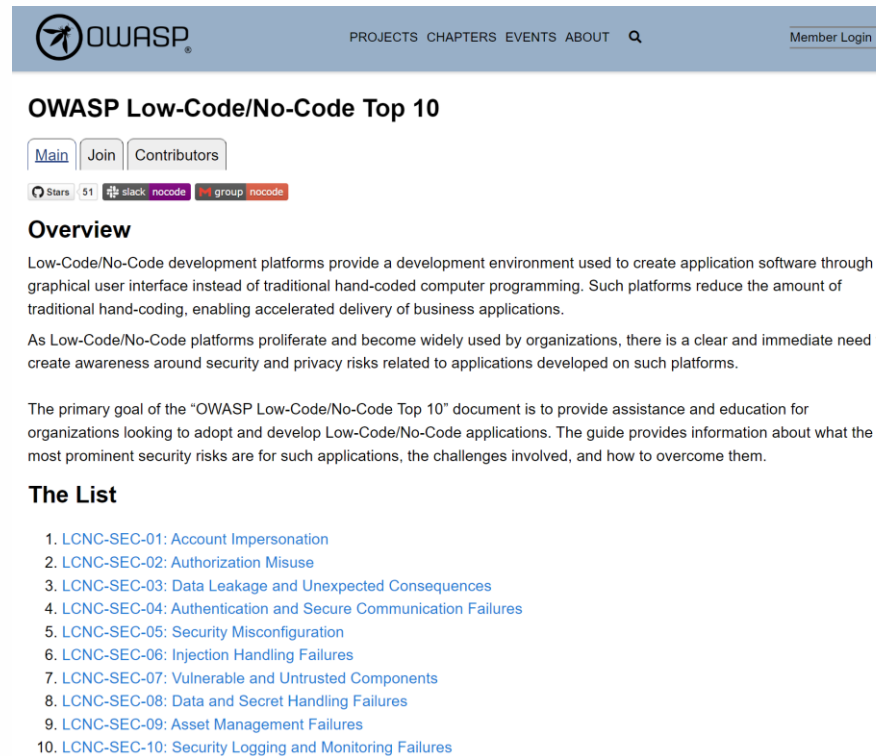


Links → mbgsec.com/blog/owasp-dc-links

Protect your org!

Build secure apps

1. Don't overshare
2. OWASP LCNC Top 10



The screenshot shows the OWASP website header with navigation links for PROJECTS, CHAPTERS, EVENTS, and ABOUT. Below the header, the page title is "OWASP Low-Code/No-Code Top 10". There are buttons for "Main", "Join", and "Contributors". Below these are social media links for Stars (51), slack, nocode, and group, nocode. The "Overview" section contains two paragraphs of text. The "The List" section contains a numbered list of 10 items, each with a link to a specific security issue.

OWASP

PROJECTS CHAPTERS EVENTS ABOUT

Member Login

OWASP Low-Code/No-Code Top 10

Main Join Contributors

Stars 51 slack nocode group nocode

Overview

Low-Code/No-Code development platforms provide a development environment used to create application software through a graphical user interface instead of traditional hand-coded computer programming. Such platforms reduce the amount of traditional hand-coding, enabling accelerated delivery of business applications.

As Low-Code/No-Code platforms proliferate and become widely used by organizations, there is a clear and immediate need to create awareness around security and privacy risks related to applications developed on such platforms.

The primary goal of the "OWASP Low-Code/No-Code Top 10" document is to provide assistance and education for organizations looking to adopt and develop Low-Code/No-Code applications. The guide provides information about what the most prominent security risks are for such applications, the challenges involved, and how to overcome them.

The List

1. [LCNC-SEC-01: Account Impersonation](#)
2. [LCNC-SEC-02: Authorization Misuse](#)
3. [LCNC-SEC-03: Data Leakage and Unexpected Consequences](#)
4. [LCNC-SEC-04: Authentication and Secure Communication Failures](#)
5. [LCNC-SEC-05: Security Misconfiguration](#)
6. [LCNC-SEC-06: Injection Handling Failures](#)
7. [LCNC-SEC-07: Vulnerable and Untrusted Components](#)
8. [LCNC-SEC-08: Data and Secret Handling Failures](#)
9. [LCNC-SEC-09: Asset Management Failures](#)
10. [LCNC-SEC-10: Security Logging and Monitoring Failures](#)

Links → mbgsec.com/blog/owasp-dc-links



Protect your org!

Build secure apps

1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

Links → mbgsec.com/blog/owasp-dc-links

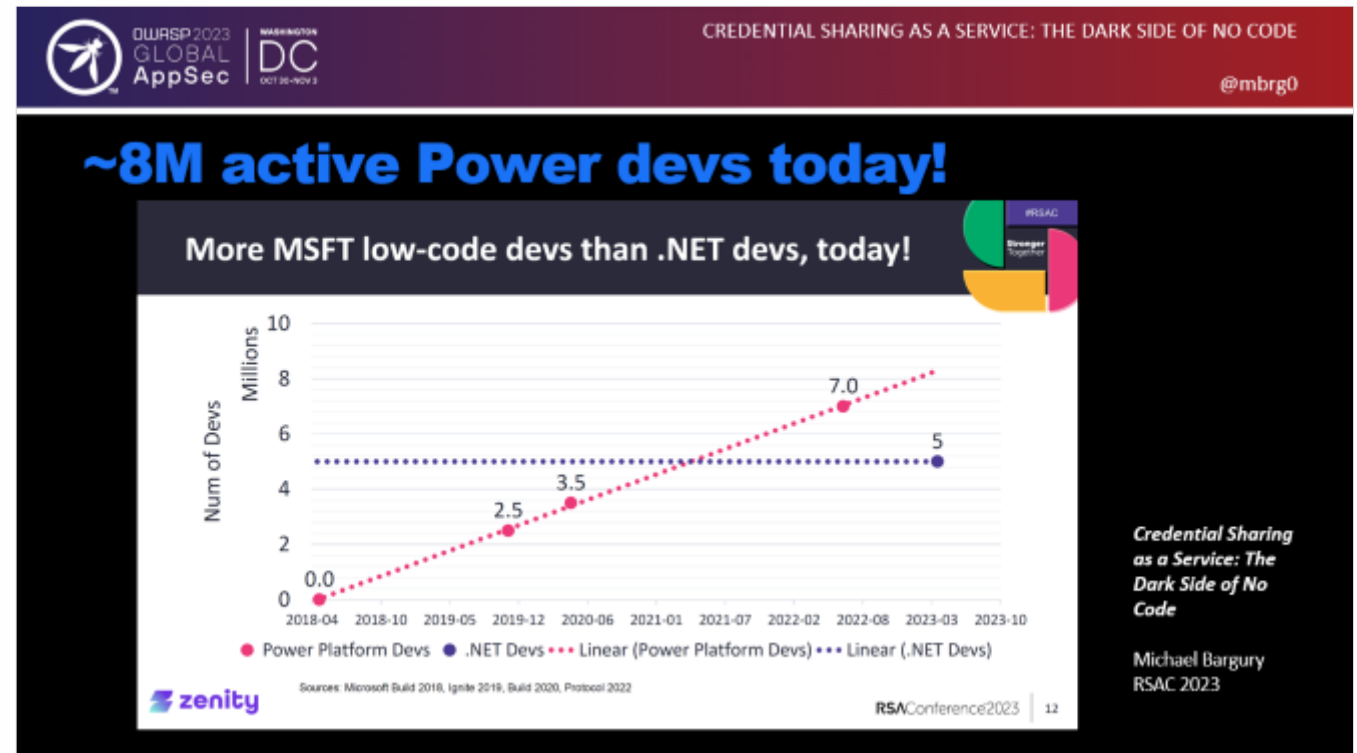
Protect your org!

Build secure apps

1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

3. AppSec



Links → mbgsec.com/blog/owasp-dc-links



Protect your org!

Build secure apps

1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

3. AppSec

Hack your env

Links → mbgsec.com/blog/owasp-dc-links

Protect your org!

Build secure apps

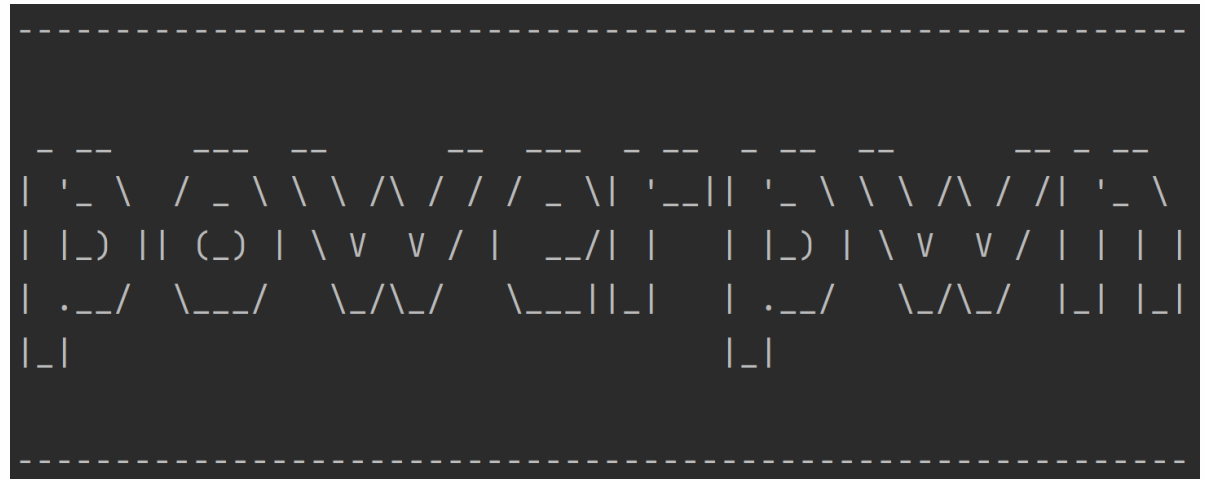
1. Don't overshare
2. OWASP LCNC Top 10

Harden your env

3. AppSec

Hack your env

4. powerpwn



Links → mbgsec.com/blog/owasp-dc-links



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30-NOV 3



CREDENTIAL SHARING AS A SERVICE: THE DARK SIDE OF NO CODE

Michael Bargury @mbrg0
Zenity

mbgsec.com



OWASP 2023
GLOBAL
AppSec

WASHINGTON
DC
OCT 30 - NOV 3

THANK YOU

