

RSAC Conference™ 2023

San Francisco | April 24 – 27 | Moscone Center

SESSION ID: DAS-R06

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



#RSAC

Michael Bargury

CTO & Co-founder

Zenity

@mbrg0

Disclaimer



Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2023 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

Outline



- Low-code / no-code in a nutshell
- The low-code / no-code SDLC and (lack of) security controls
- Low Code attacks observed in the wild
 - Living off the land – account takeover, lateral movement, PrivEsc, data exfil
 - Hiding in plain sight
 - Leveraging predictable misconfiguration from the outside
- How to defend

RSAConference™2023



**Stronger
Together**

Low-Code / No-Code in a Nutshell

EVERYONE is a developer

Why Low Code?

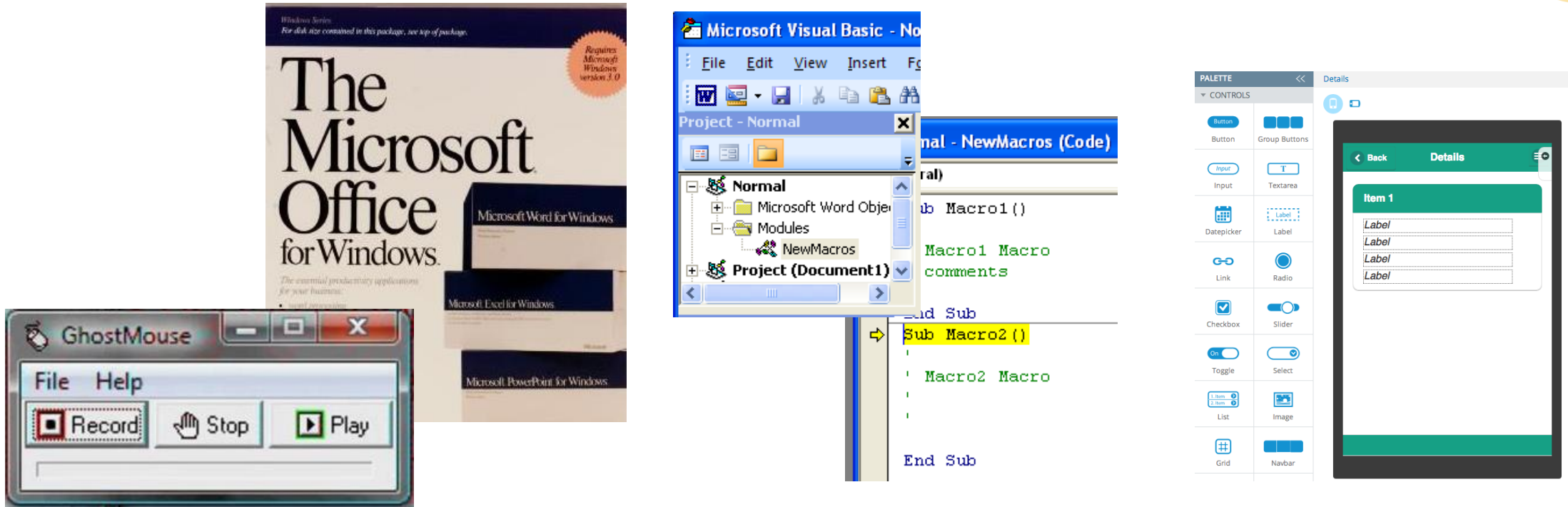
Business Needs



IT Capacity



If this sounds familiar, its because it is

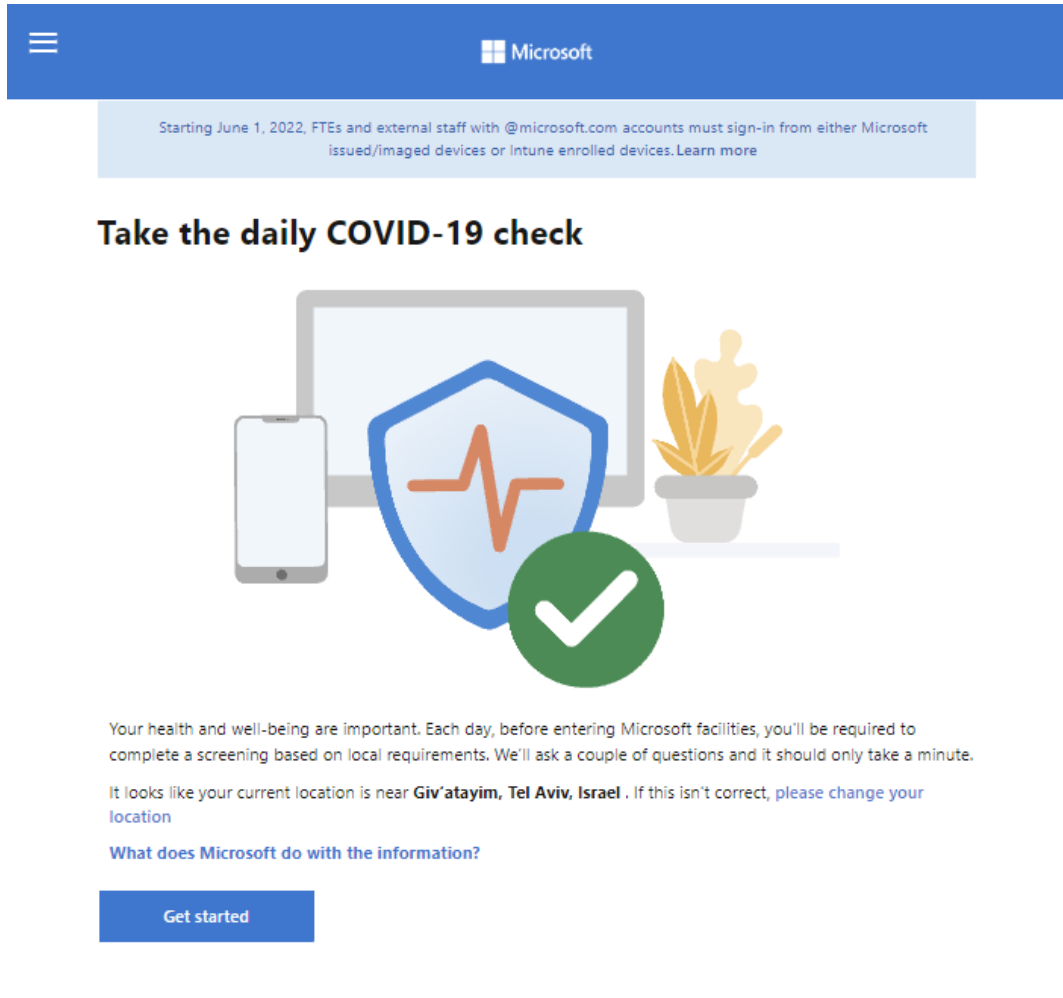


Tech evolution

COVID health check app by Microsoft

#RSAC

Stronger Together



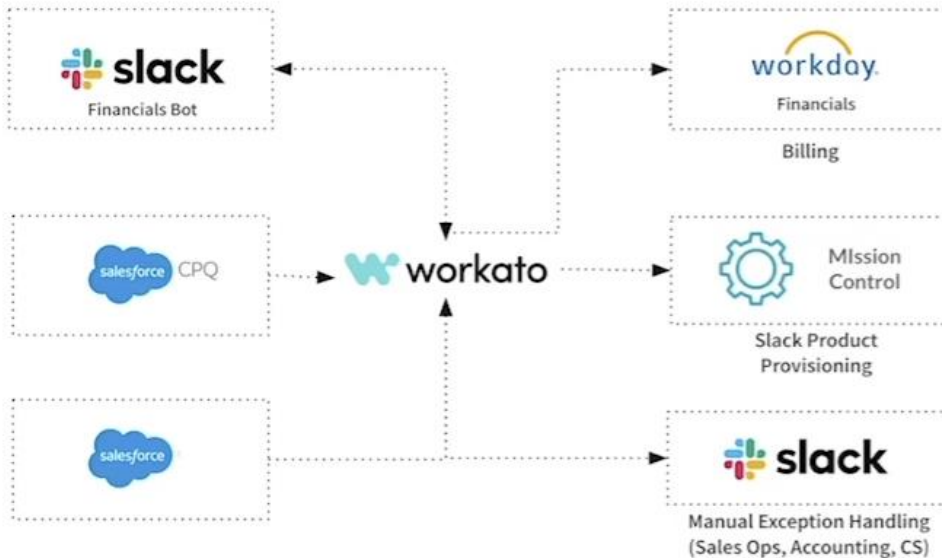
The screenshot shows the Microsoft COVID health check app interface. At the top, there is a blue navigation bar with a hamburger menu icon on the left and the Microsoft logo in the center. Below the navigation bar, a light blue banner contains the text: "Starting June 1, 2022, FTEs and external staff with @microsoft.com accounts must sign-in from either Microsoft issued/imaged devices or Intune enrolled devices. Learn more". The main heading is "Take the daily COVID-19 check". Below the heading is an illustration featuring a laptop, a smartphone, a shield with a red heartbeat line, and a green checkmark in a circle. To the right of the shield is a small potted plant. Below the illustration, the text reads: "Your health and well-being are important. Each day, before entering Microsoft facilities, you'll be required to complete a screening based on local requirements. We'll ask a couple of questions and it should only take a minute." This is followed by: "It looks like your current location is near **Giv'atayim, Tel Aviv, Israel**. If this isn't correct, [please change your location](#)". Below this is the question "What does Microsoft do with the information?" and a blue "Get started" button.

<https://aka.ms/healthcheck>

Order-to-cash automation by Slack



Automating order to cash fulfillment



💰 90% no touch orders

💰 95% orders processed in less than 5 minutes

❤️ Delightful experience from Sales Opportunity to Product Fulfillment

“Choose tools that make developing and managing Integrations a joy.”

Monica Wilkinson
Lead Architect

<https://www.workato.com/the-connector/how-slack-automated-order-to-cash/>

Business users become business developers

#RSAC

Stronger
Together

Microsoft | Inside Track Search content Audience ▾ Topic ▾ Content Suites Videos Blog Careers

How citizen developers modernized Microsoft product launches

Mar 20, 2020 | Serah Delaini



“... A Business Operations program manager, and her team, were searching for a way to optimize the launch process for the 150 employees who ran product launches across the company.

... Within months, the app would become a widely used internal tool”

<https://www.microsoft.com/insidetrack/blog/how-citizen-developers-modernized-microsoft-product-launches/>

Available in every major enterprise

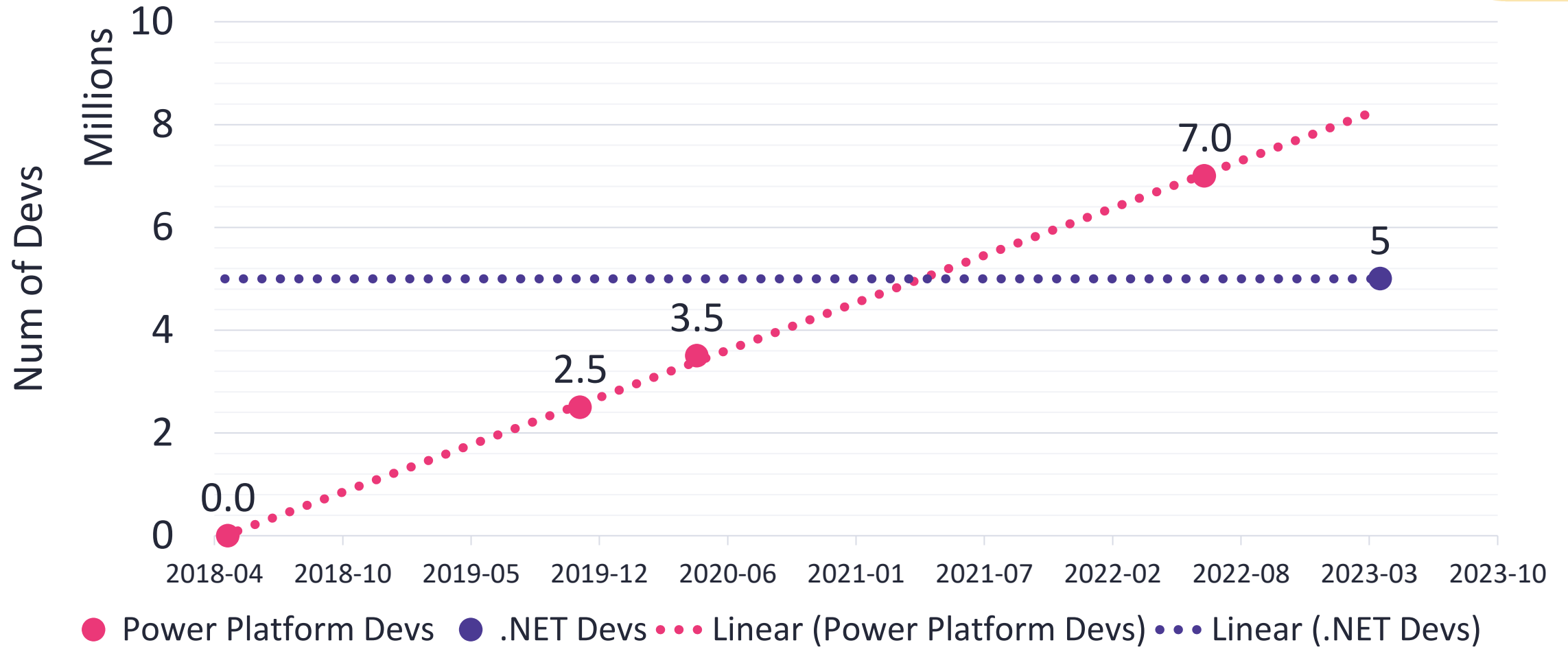


The vast majority of enterprise apps



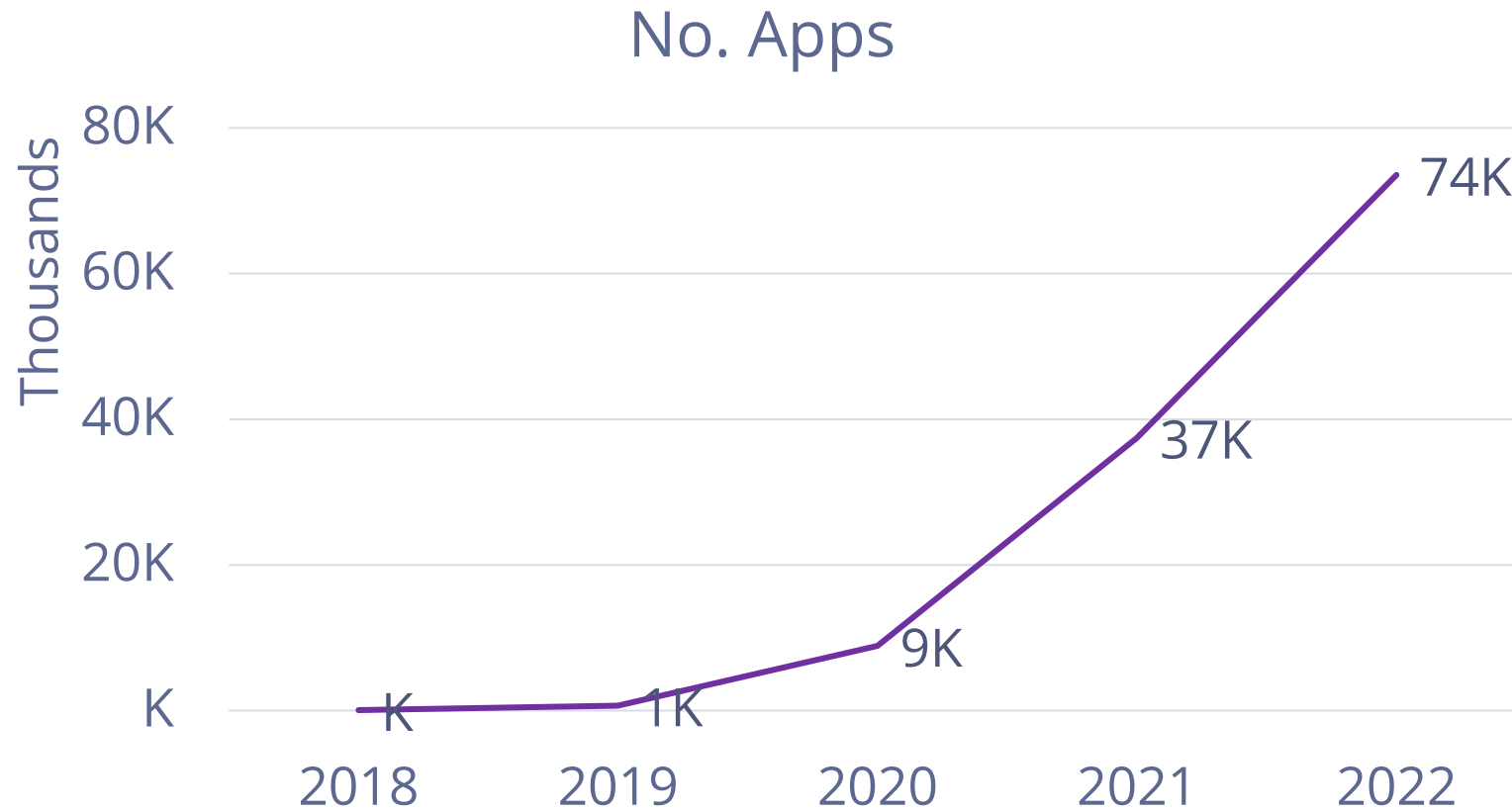
- *“By 2025, 70% of new applications deployed for the enterprise will use low-code or no-code tools” Gartner 2021*
- *“By 2023, the number of active citizen developers at large enterprises will be at least four times the number of professional developers.” Gartner 2021*
- *“we are going to have 500 million applications that are going to get created, new, by 2023. Just to put that in perspective, that's more than all of the applications that were created in the last 40 years.” Satya Nadella, Microsoft Ignite 2019*

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



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

Exponential Growth in Business Development



Recap – you can't opt out of citizen development

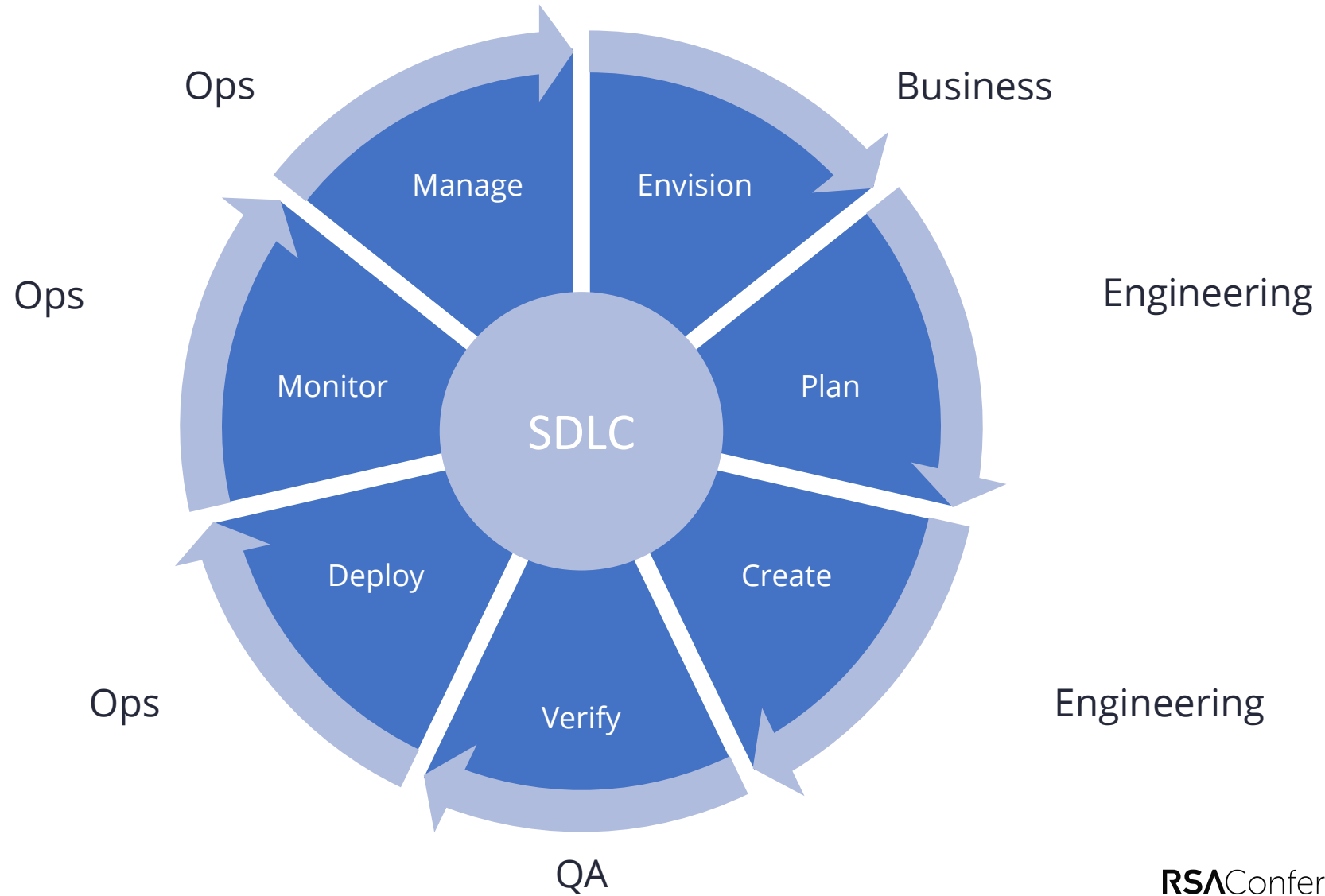


- The next big productivity boost (Excel-level impact)
- Powers critical business workflows, predicted to power 70% of enterprise apps by 2025
- Available on every major enterprise, yours too
- Millions of new (business) developers and growing fast
- Tens of thousands of apps in a large enterprise

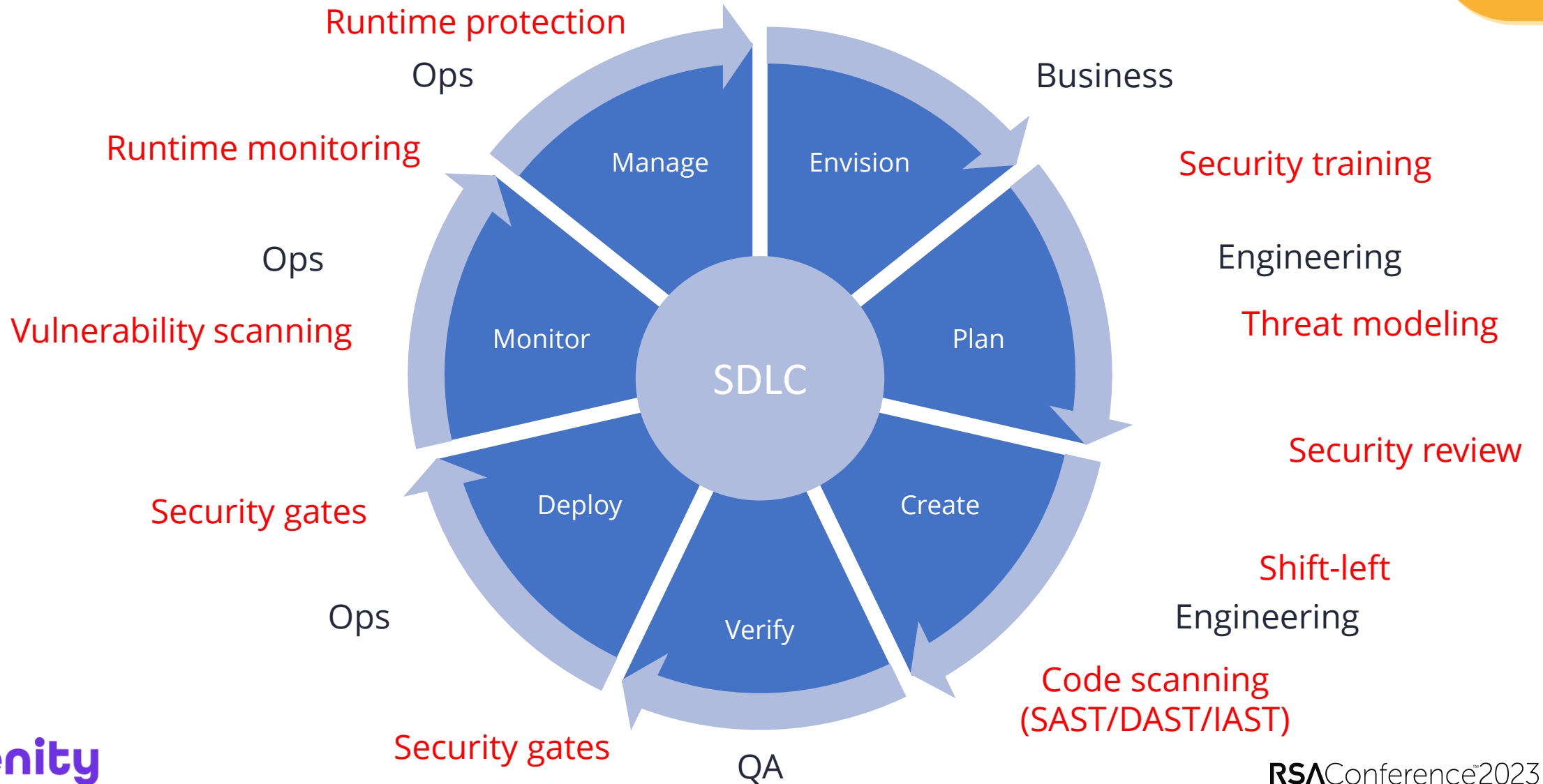
No Code No Control

**We can't handle low-code / no-code security by
doing more of what we're already doing**

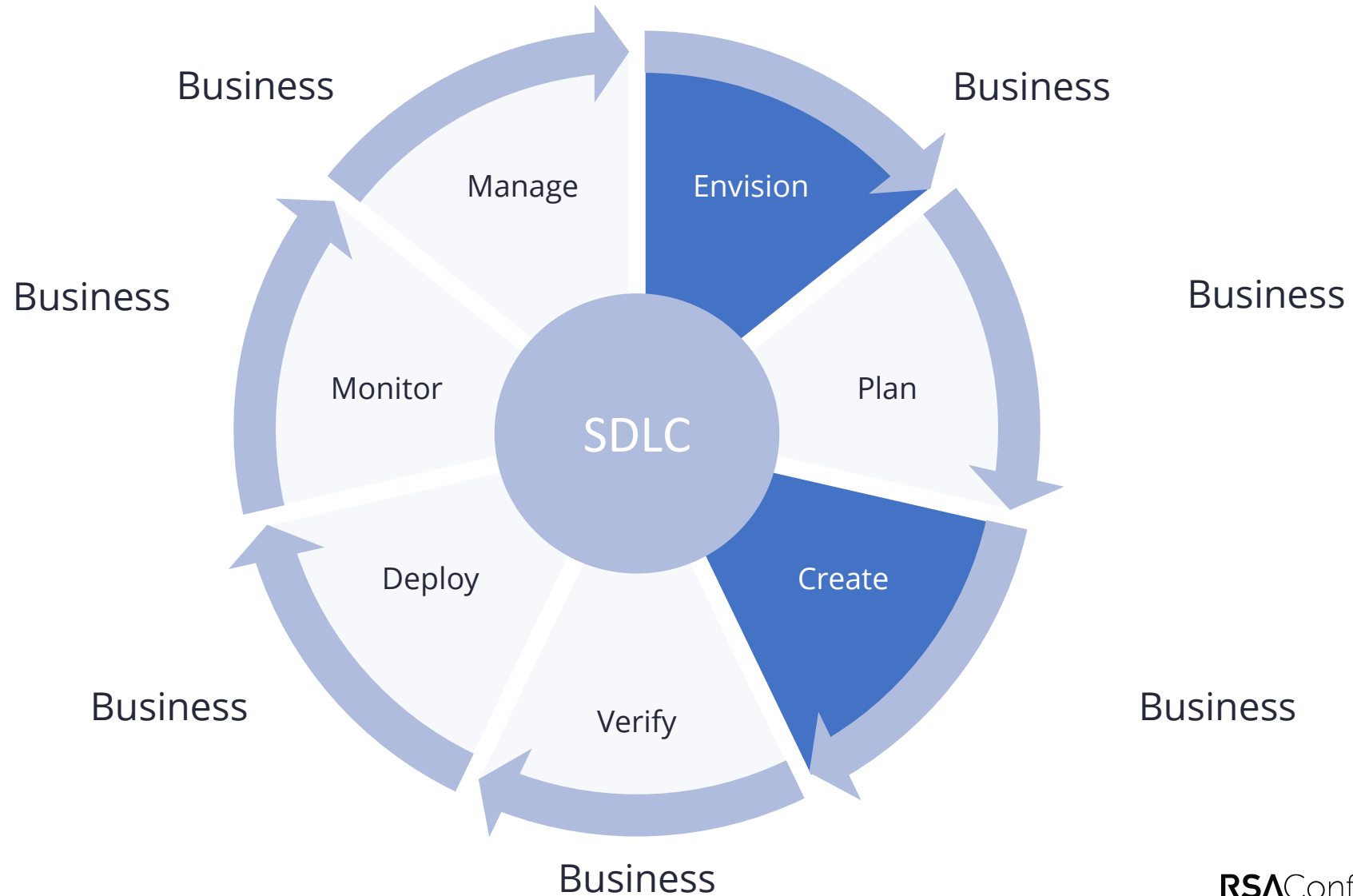
Pro-Code SDLC



Secure SDLC



Replace SDLC with “Hit Save to Deploy”



Lacking security controls

Existing security control	Low-code / no-code
Security training	Can we expect business users to be security savvy?
Threat modeling	Can't scale to 000s apps/year
Security review	Can't scale to 000s apps/year
Code scanning	No code to scan
Artifact scanning	Mostly unavailable, overwhelming FPs
Security gates	Lacking CI/CD
Vulnerability scanning	No awareness to low-code leads to overwhelming FPs
Runtime monitoring	Lacking logs
Runtime protection	Lacking instrumentation

Recap – security controls are severely lacking



- Has access to business, health, financial data
- Runs as SaaS
- Lacking SDLC
- Lacking security controls
- Developers with no security savviness
- 10-100x the scale of application development

RSAConference™2023



**Stronger
Together**

Low Code Attacks In The Wild

Living off the land

A simple example



youtu.be/5naPxs0fEJc

Step by step

Add a new app connection

Add a new app connection

- Slack
- Forms for Slack
- Dislack



slack

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



i New connection added

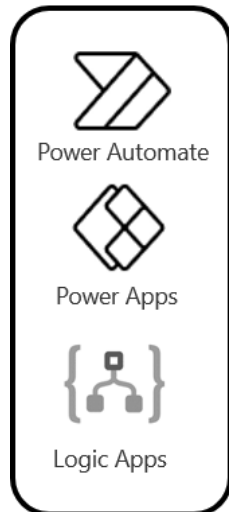
My connections 1

Slack @michaelbargury (pwntoso)
@michaelbargury (pwntoso) - added 21 seconds ago

Share 0 Zaps **KS** by Kris S. ...

Behind the scenes

RESTful API
defined in
swagger

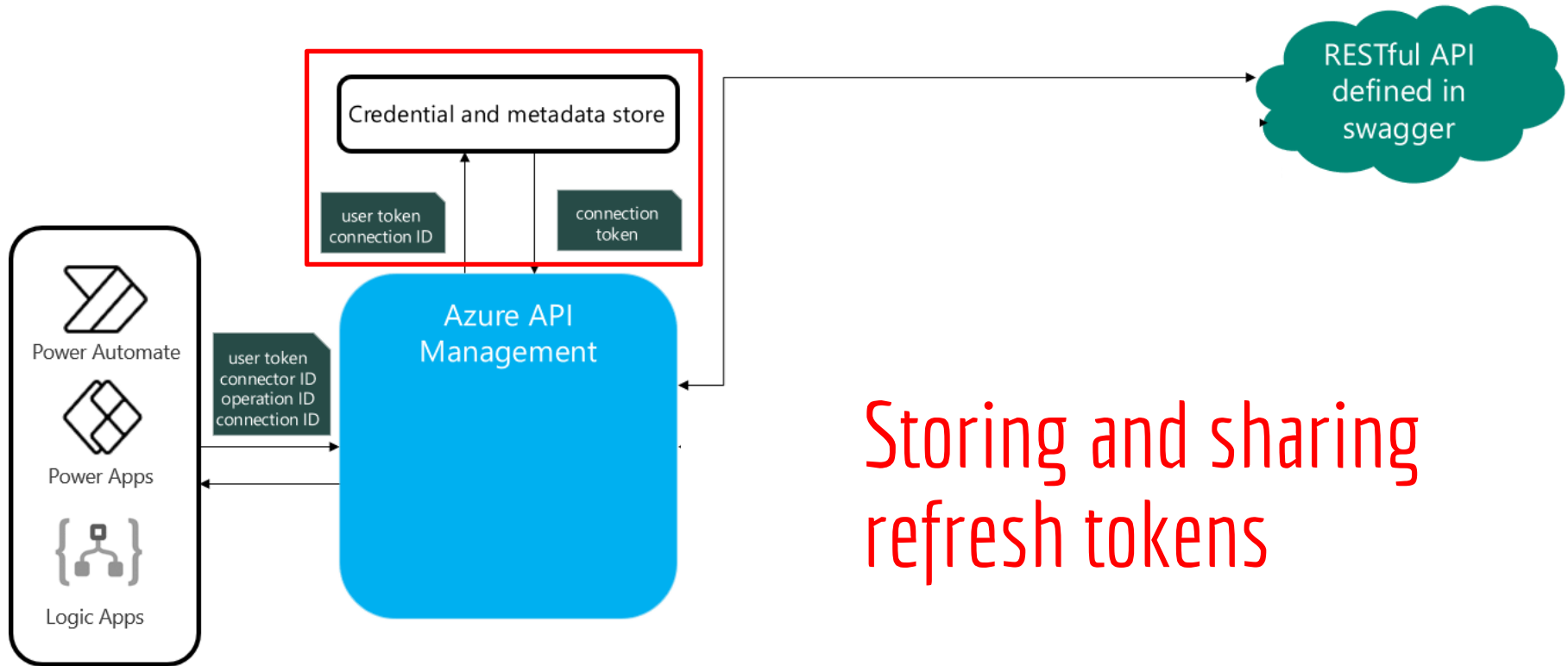


How does the app authenticate to slack?

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!

Add new Facebook Lead Ads leads to rows on Google Sheets
Premium

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

Add info to a Google Sheet from new Webhook POST requests
Premium
Webhooks by Zapier + Google Sheets

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

Send emails via Gmail when Google Sheets rows are updated
Google Sheets + Gmail

Create Forms
Premium

Get Slack notifications for new information from a Webhook
Premium
Webhooks by Zapier + Slack

Send an email when a new message is added in Microsoft Teams
By Microsoft Power Automate Community
Automated 35000

Lots of apps means lots of credentials

Connections in Zenity Stage (default)

Name	Account	Last Used
Zenity Zenity	ystage.com Microsoft Dataverse (legacy)	1 mo ago
{BaseResourceUrl} HTTP with Azure AD	Bitbucket Bitbucket (preview)	
Microsoft Teams	ystage.com Azure Resource Manager	
SQL Server y.io	ystage.com Office 365 Management API	
SQL Server ystage.com	ConnectionToFadiStorageAccount Azure Blob Storage	
SQL Server ystage.com	SQL Server ...-sql-server.database.wind...	
SQL Server ystage.com	ystage.com Azure Blob Storage	
SharePoint ystage.com	ystage.com Microsoft Dataverse	
Power Platform for Admins ystage.com	Connective eSignatures Connective eSignatures (preview)	
Power Platform for Admins ystage.com	Connective eSignatures Connective eSignatures (preview)	
	23 DB2	
	h@gmail.com Dropbox	
	ty.io Azure Key Vault	1 d ago
	MSN Weather MSN Weather	5 mo ago
	ystage.com Office 365 Outlook	1 h ago
	ystage.com Office 365 Users	5 d ago
	6681@gmail.com OneDrive	9 mo ago
	Outlook.com Outlook.com	57 min ago
	RSS RSS	4 mo ago
	ystage.com Salesforce	2 wk ago
	Mail Mail	9 mo ago
	Mail Mail	7 mo ago
	aviv-demo-2 ServiceNow	8 mo ago
	Aviv-Demo ServiceNow	9 mo ago

Lots of apps means lots of credentials

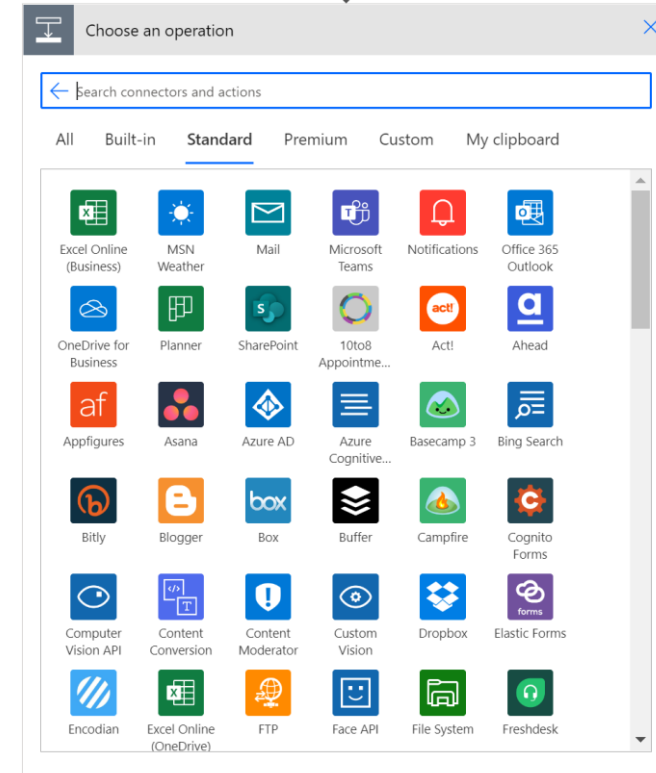
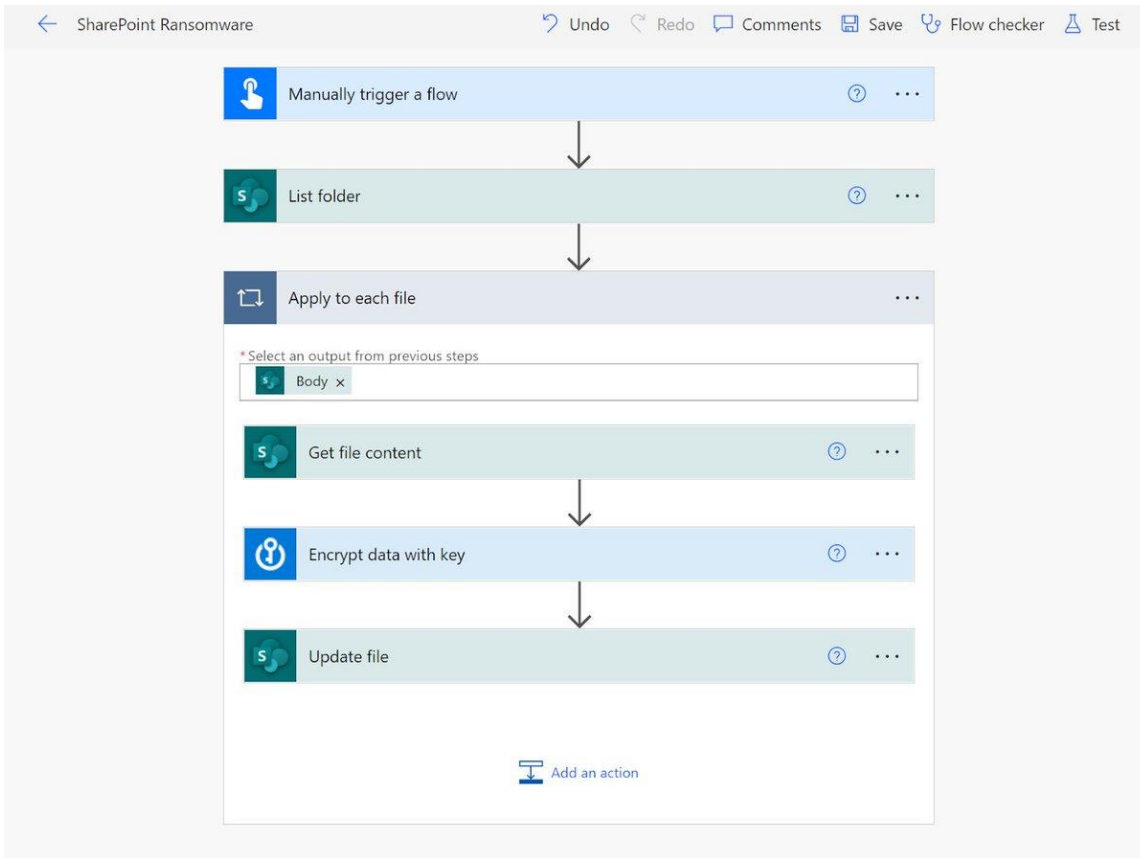
Connections in Zenity Stage (default)

The screenshot shows a list of connections in Zenity Stage. A large meme image of a baby with a grumpy expression is overlaid on the middle of the list. The connections include various services like Microsoft Dataverse, Bitbucket, Azure, Office, Connective eSignatures, SQL Server, SharePoint, Power Platform for Admins, Microsoft Teams, Azure Key Vault, MSN Weather, Outlook, Gmail, Salesforce, Mail, and ServiceNow. Each entry shows the app name, icon, and last accessed time.

Name	Last Accessed
Zenity	
(BaseResourceUrl) HTTP with Azure AD	
Microsoft Teams	
SQL Server	
SQL Server	
SQL Server	
SharePoint	
Power Platform for Admins	
Power Platform for Admins	
Microsoft Dataverse (legacy)	1 mo ago
Bitbucket	
Azure	
Office	
Connective eSignatures	
SQL Server	
Azure	
Microsoft Dataverse	
Connective eSignatures	
Connective eSignatures	
23 DB2	
Dropbox	
Azure Key Vault	1 d ago
MSN Weather	5 mo ago
Outlook	1 h ago
Outlook	5 d ago
6681@gmail.com	9 mo ago
com	57 min ago
com	4 mo ago
stage.com	2 wk ago
Salesforce	
Mail	9 mo ago
Mail	7 mo ago
aviv-demo-2 ServiceNow	
Aviv-Demo ServiceNow	

Privilege escalation

Ransomware thru action connections



Ransomware

Exfiltrate email thru the platform's email account

When a new email arrives (V3)

Folder:

Show advanced options

Send an email notification (V3)

*To:

*Subject:

*Body:

Font 12 **B** *I* U [Rich Text Editor Icons]

From:

To:

Subject:

Body:

Show advanced options

Delete email (V2)

* Message Id:

Original Mailbox Address:

☑ 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...
✓ win11	⋮	2.14.173.21294	—	Connected	0	0	Owner	Kris S...

No Code Malware:

github.com/mbrg/defcon30

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 that's signed out)

Enter custom value

✓ Lateral movement

Assess your risk with ZapCreds

account_name	app_name	app_icon	connection_created	connection_title	connection_owner
Marketing	Dropbox		2021-06-06T10:54:52Z	Dropbox johnw@gmail.com	John.Webb@mycompany.com
Marketing	Gmail		2021-06-06T10:00:14Z	Gmail Bobby.Atkinson@mycompany.com	Bobby.Atkinson@mycompany.com
Marketing	Gmail		2021-06-06T07:53:42Z	Gmail Lola.Burton@mycompany.com	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_owner'])
```

github.com/mbrg/zapcreds

Phishing made easy



- Set up a bait app that does something useful
- Host it under a trusted Microsoft domain
- Fool users to use it
- Take over their account

Account takeover

Phishing made easy

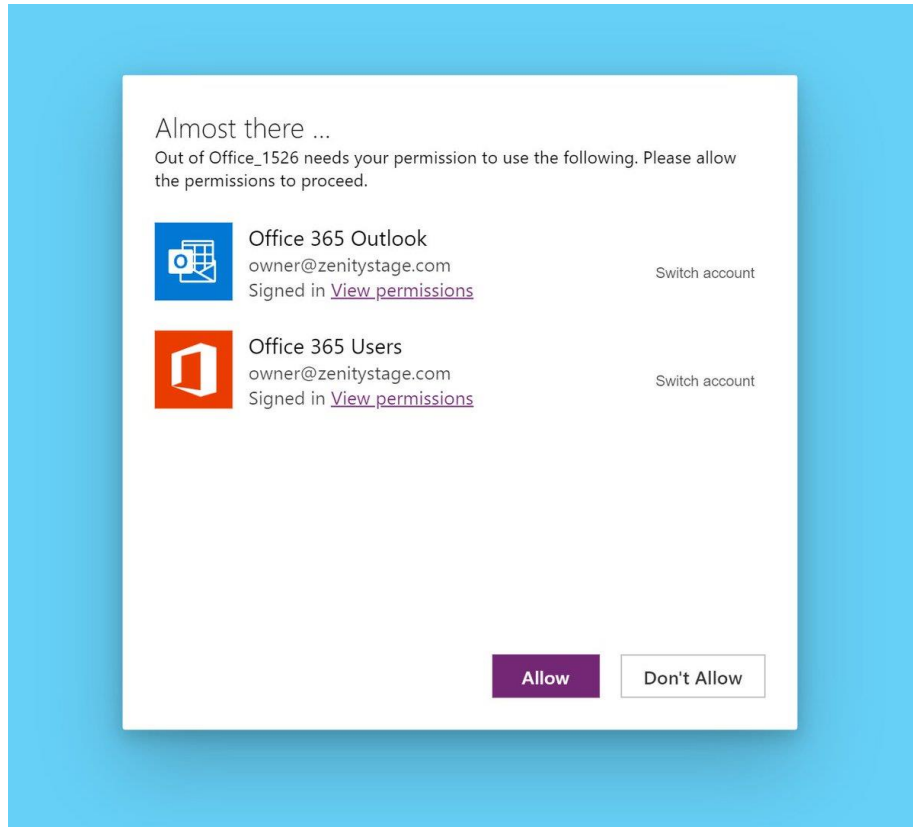
#RSAC

Stronger
Together



youtu.be/vjZpNJRC_10

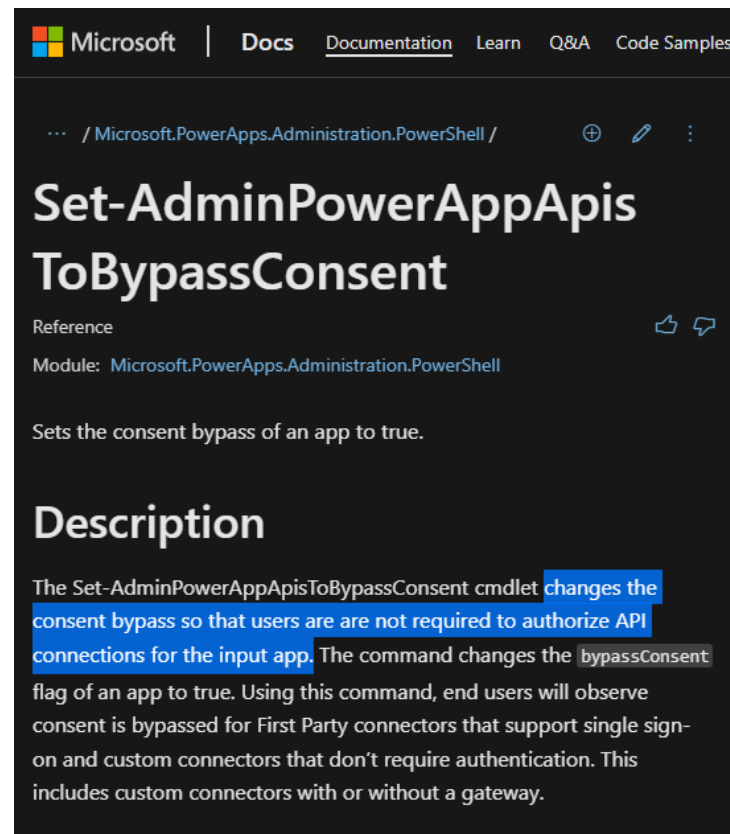
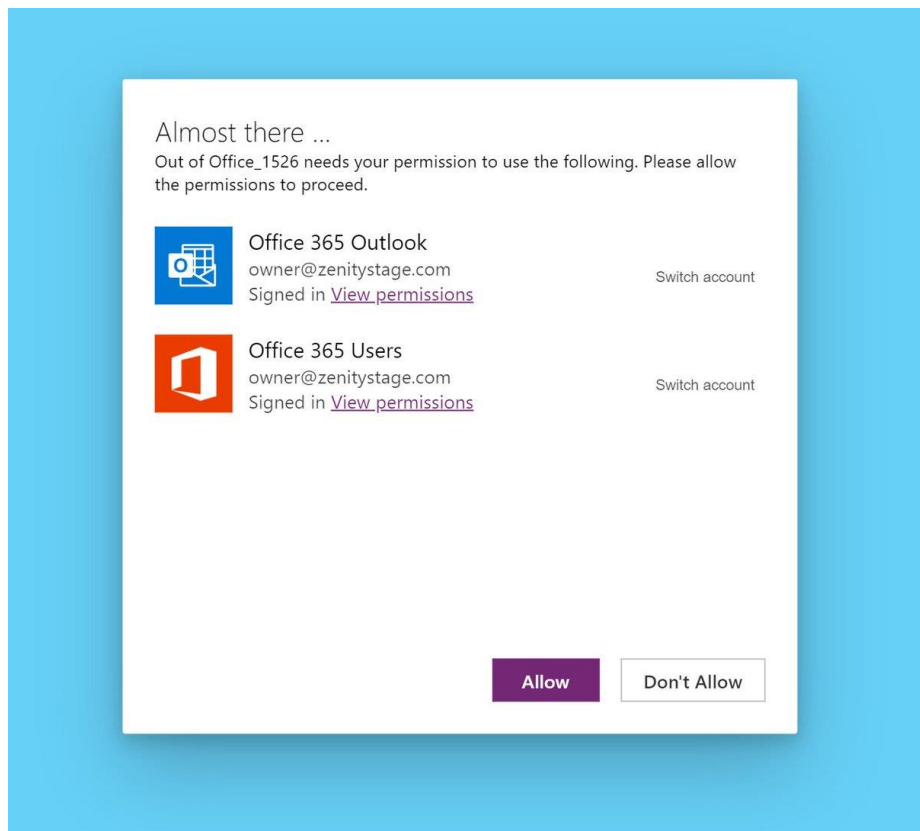
Approval window to the rescue!



Approval window to the rescue? Don't opt out!

#RSAC

Stronger Together



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

RSAConference™2023

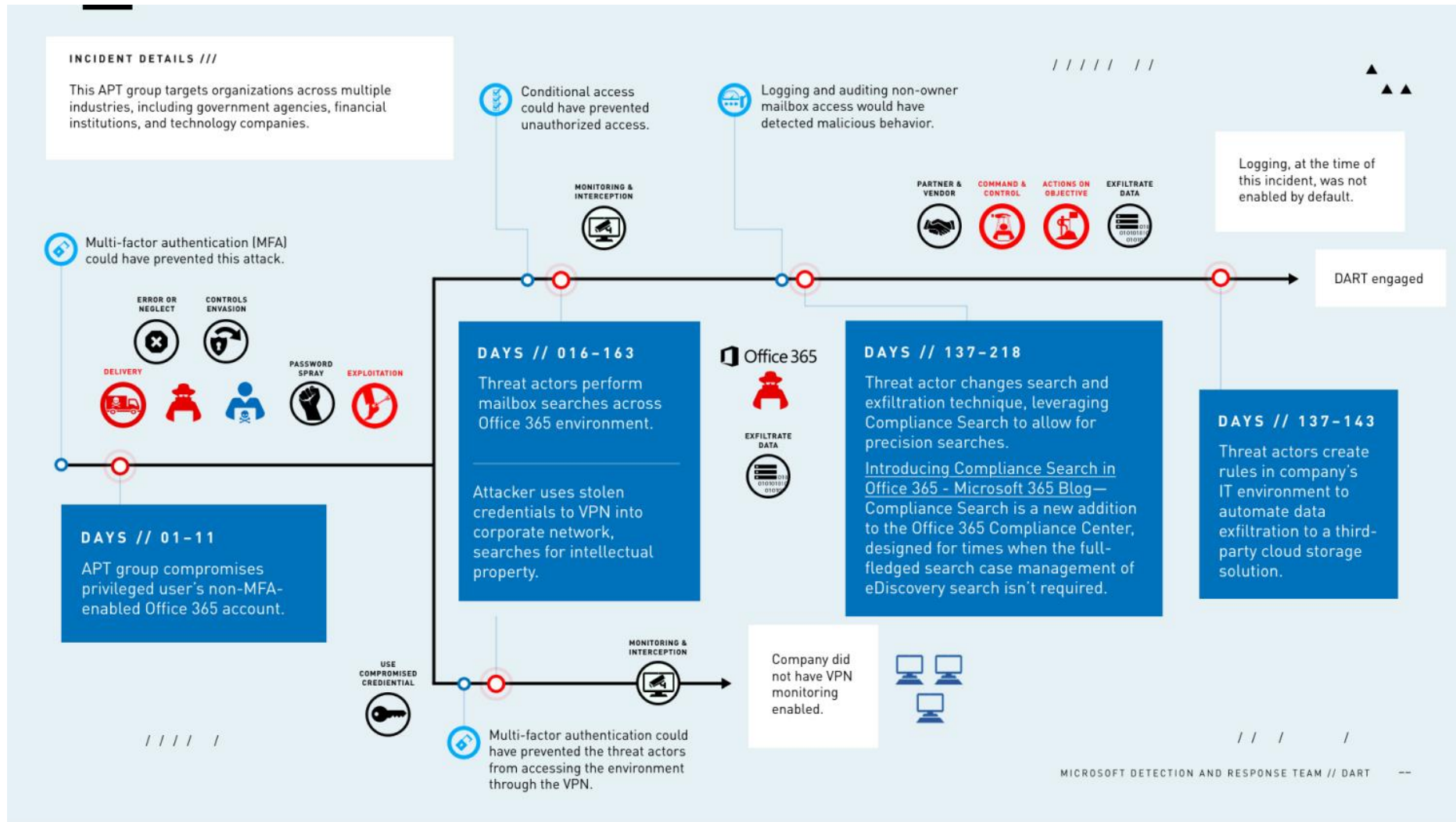


**Stronger
Together**

Low Code Attacks In The Wild

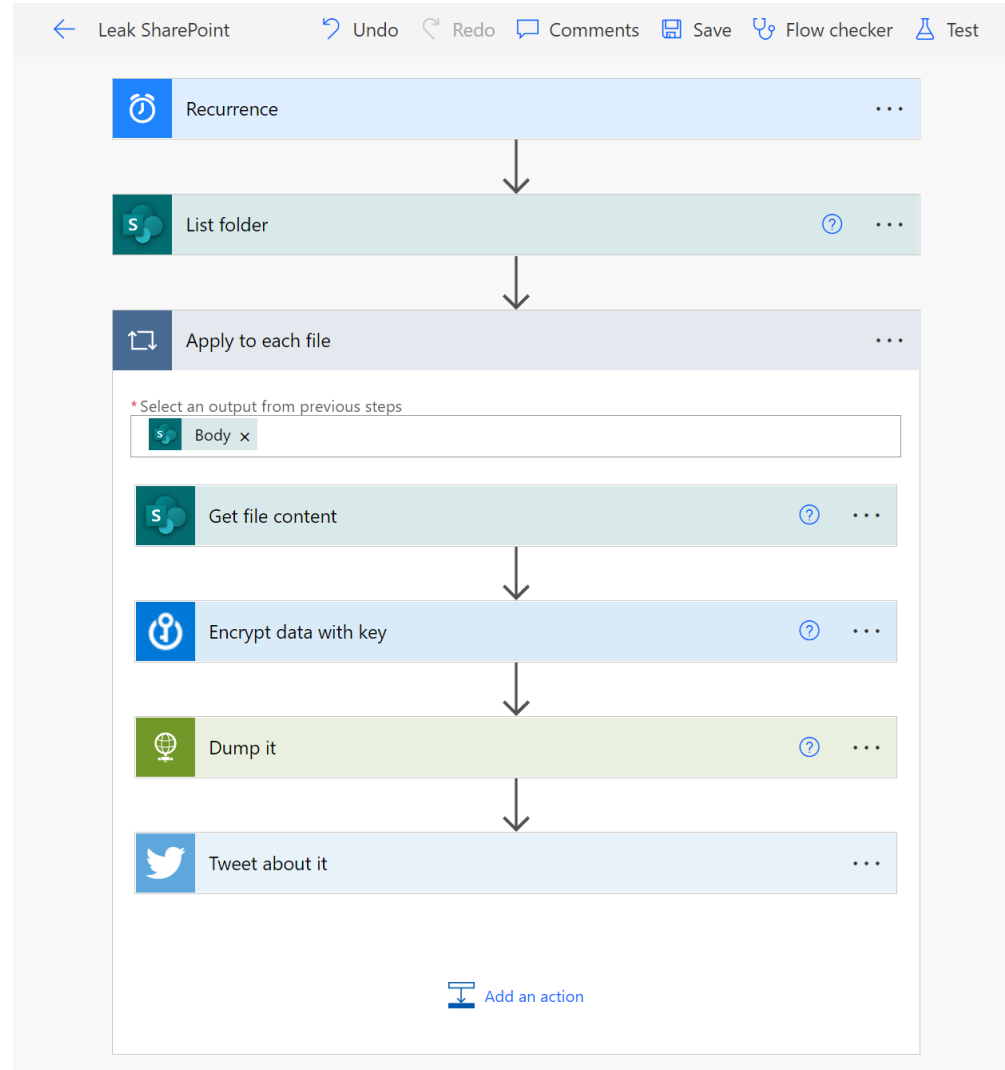
Hiding in plain sight

Why install malware when you can get your way with no code?

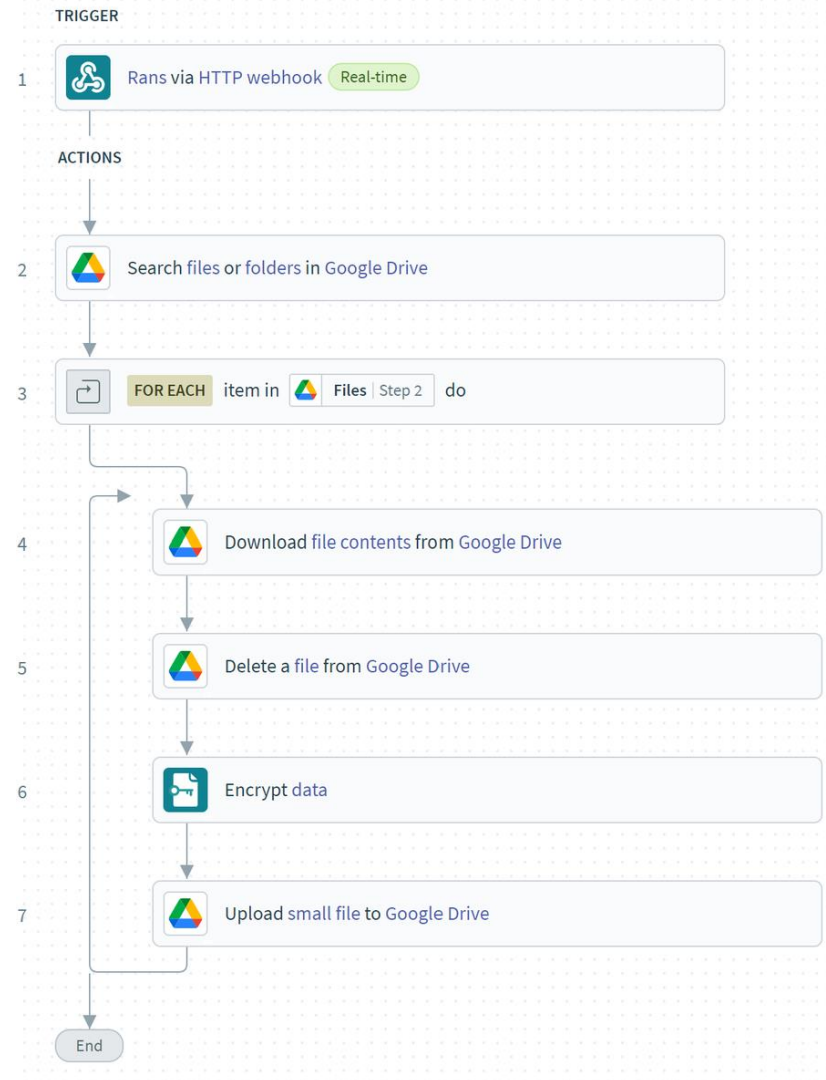


zenity.io/blog/hackers-abuse-low-code-platforms-and-turn-them-against-their-owners/

Dump files and tweet about it on a schedule



Encrypt on command



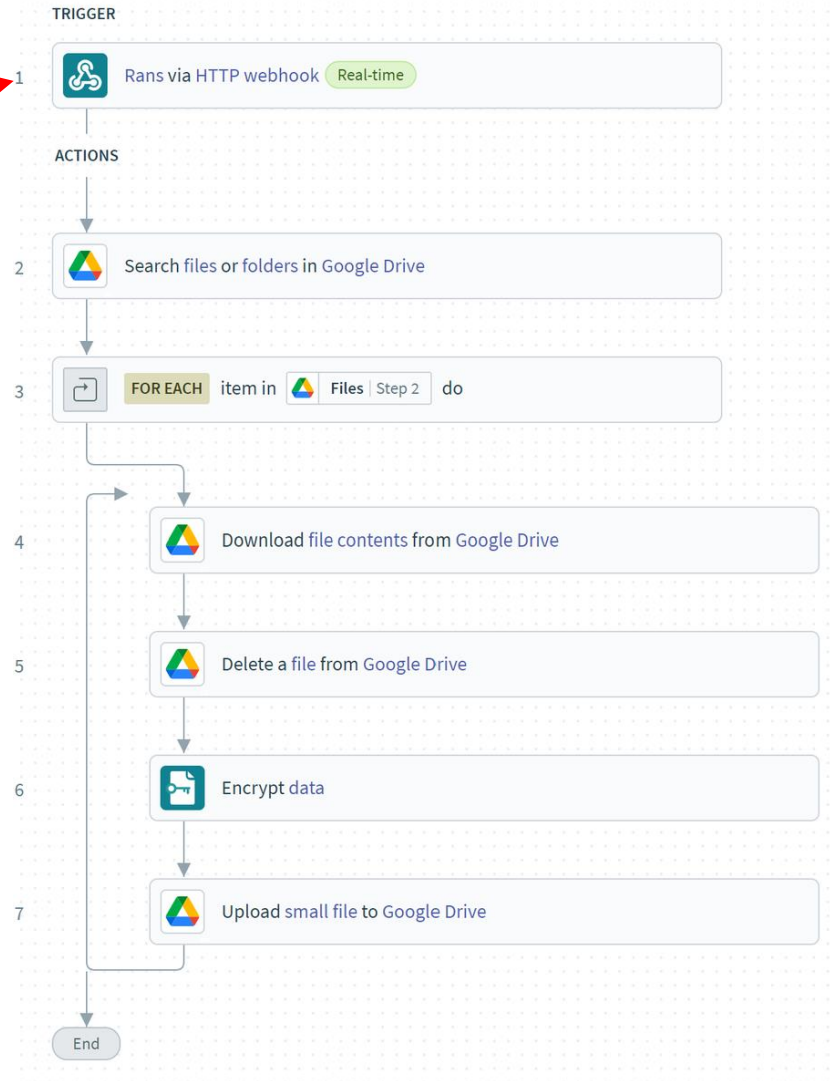
Persistence

What do we want?

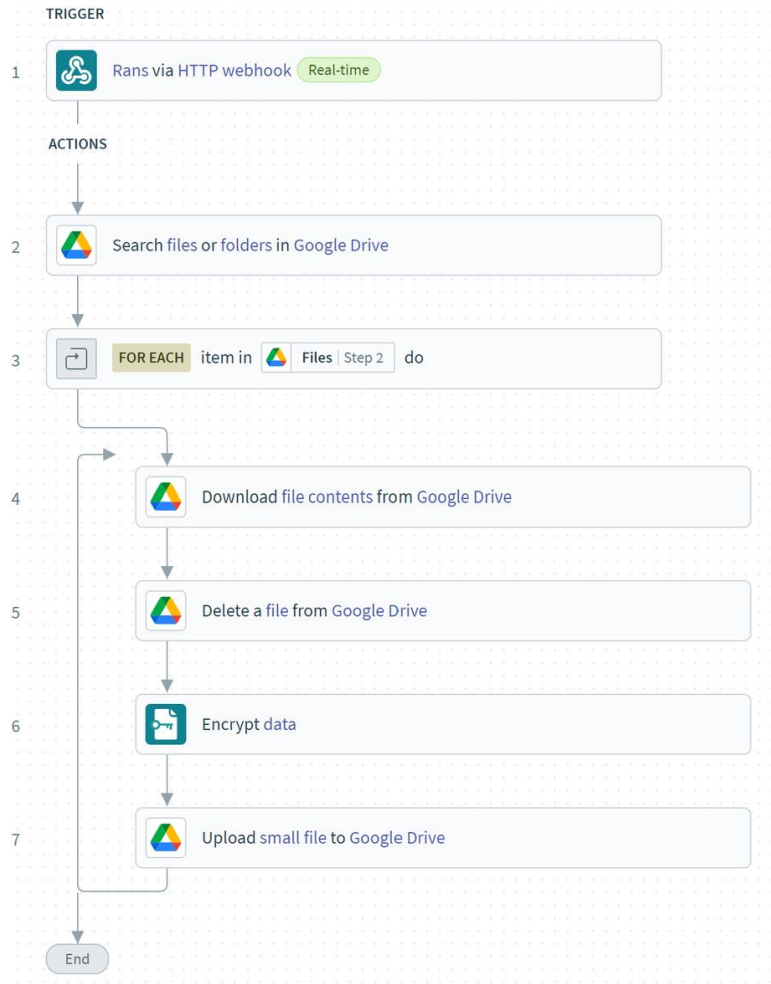
- Remote execution
- Arbitrary payloads
- Maintain access (even if user account access get revokes)
- Avoid detection
- Avoid attribution
- No logs

Persistency v1

Persistency

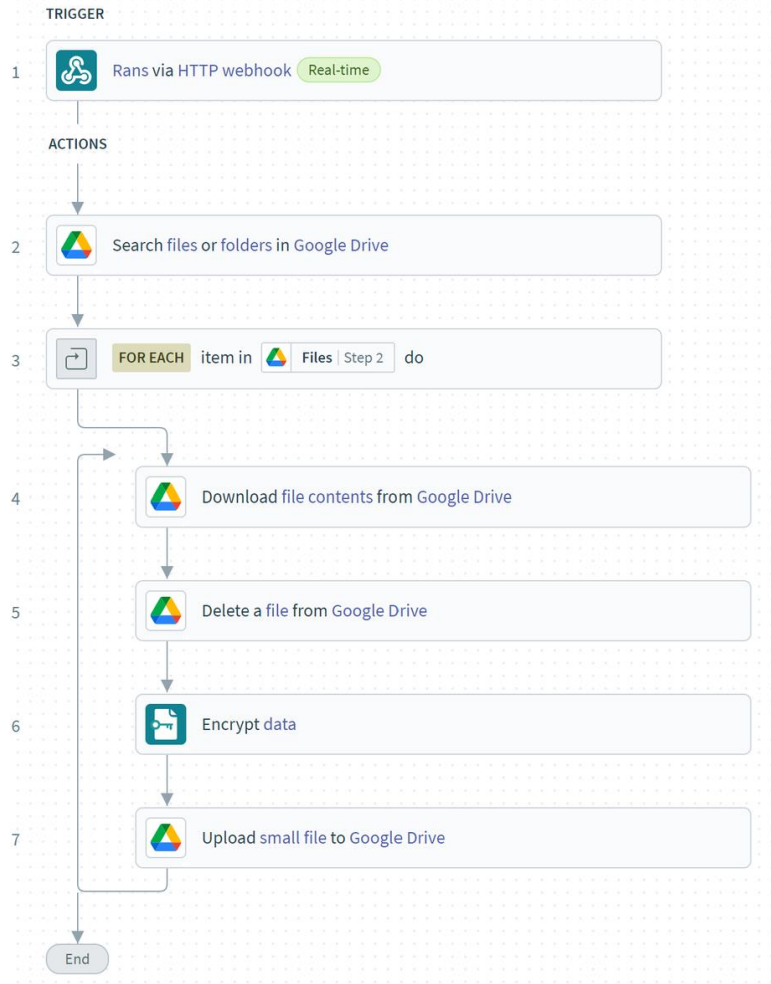


Persistency v1



Persistency laundry list:

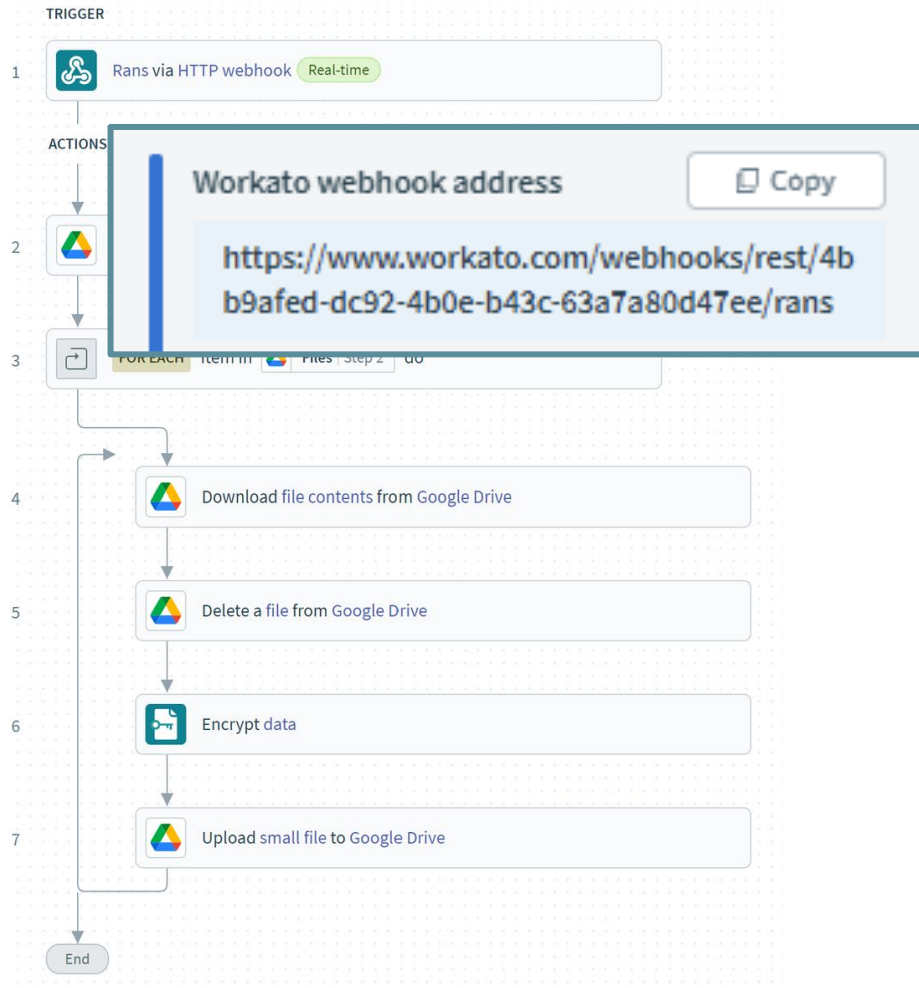
Persistency v1



Persistency laundry list:

- Remote execution
- Arbitrary payloads

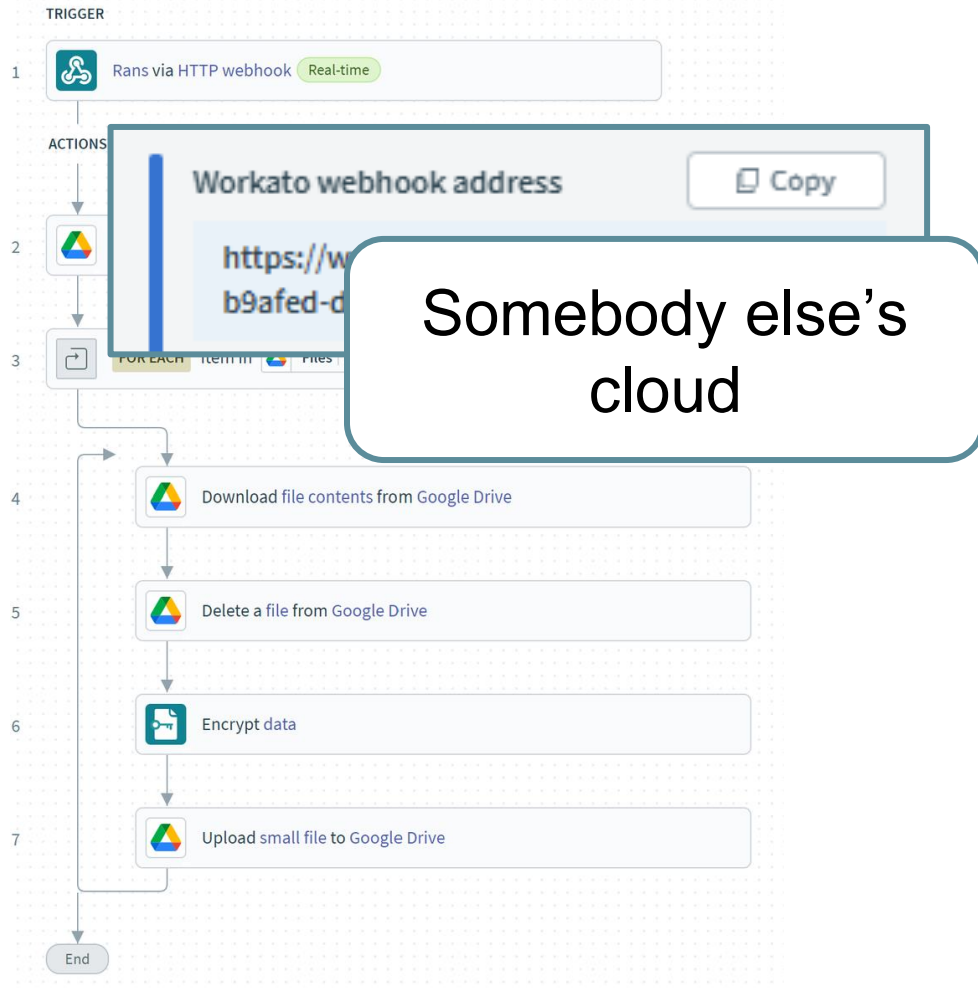
Persistency v1



Persistency laundry list:

- Remote execution
- Arbitrary payloads
- Maintain access

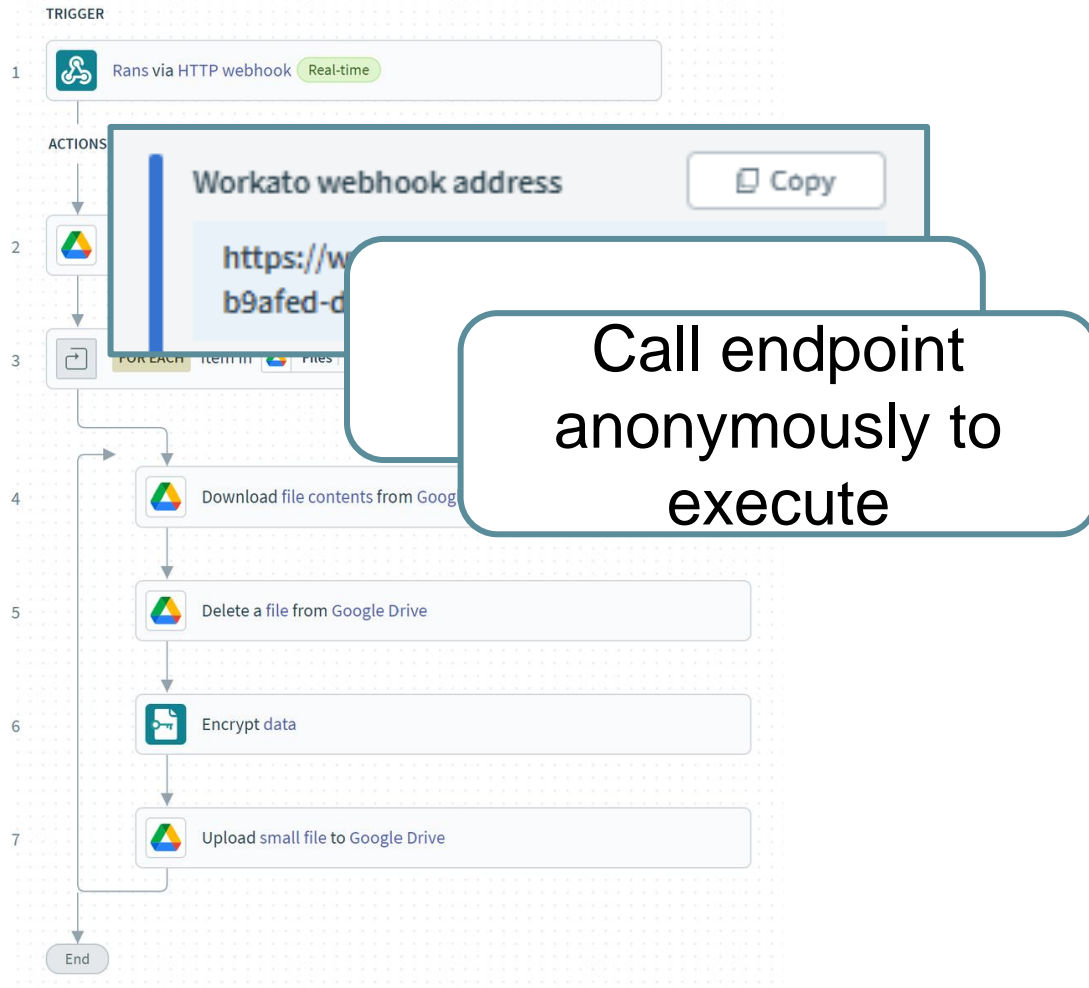
Persistency v1



Persistency laundry list:

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

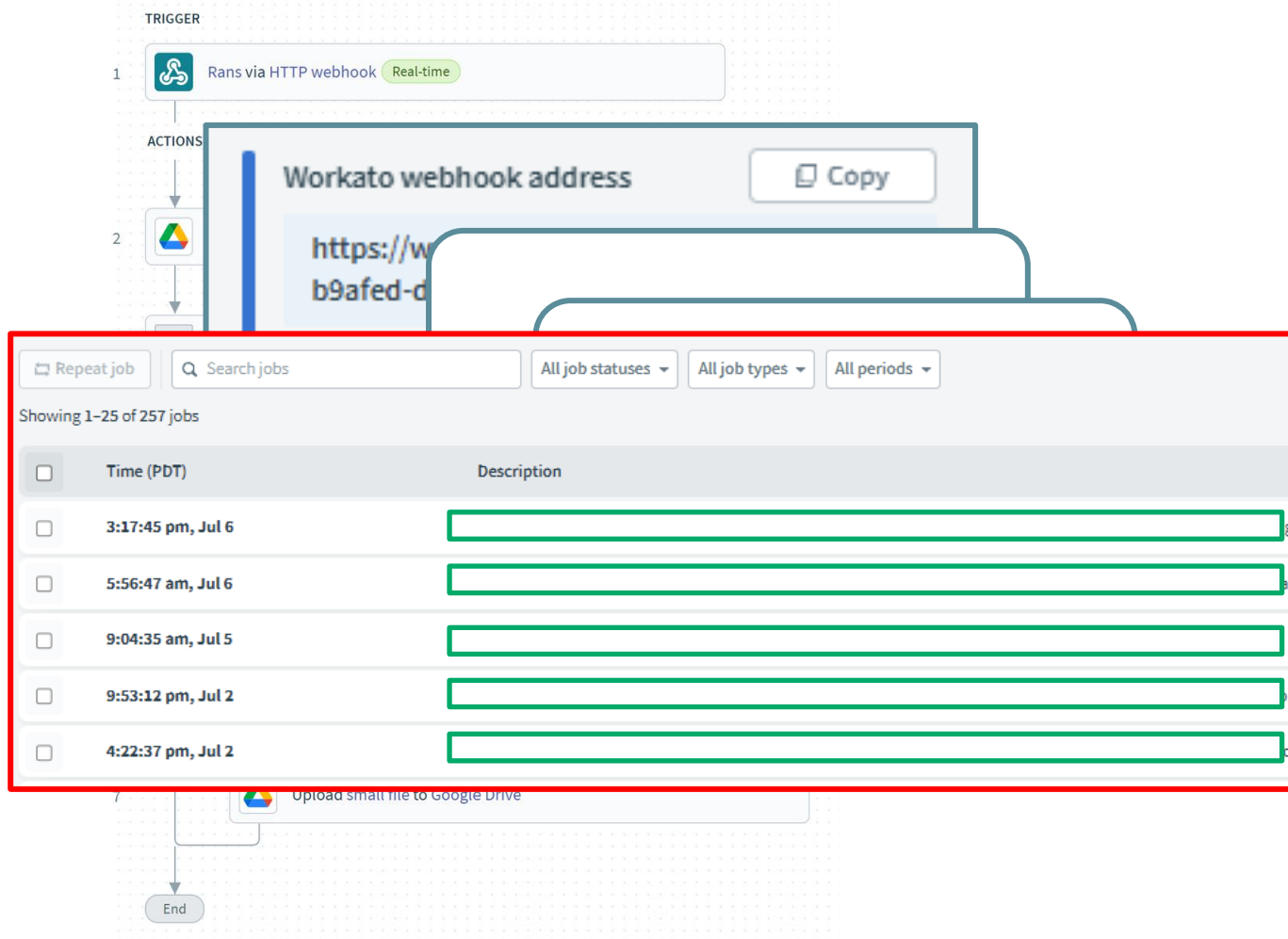
Persistency v1



Persistency laundry list:

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

Persistency v1



Persistency laundry list:

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

Towards 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](#)

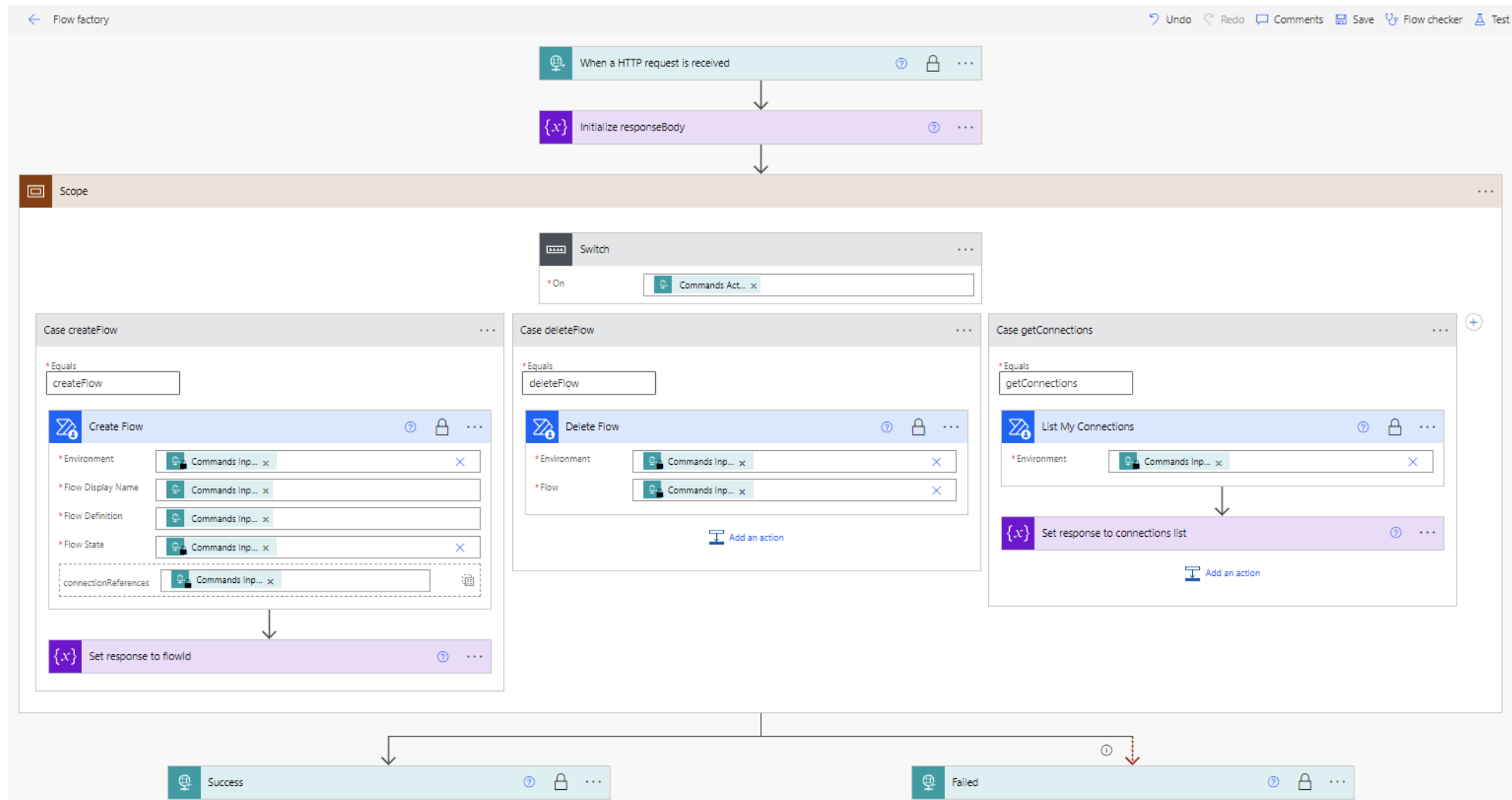


<https://docs.microsoft.com/en-us/connectors/flowmanagement/>

Executing arbitrary commands

The image displays three overlapping dialog boxes from a software interface, each with a blue header and a Zenity logo icon. The top-left dialog is titled "Create Flow" and contains the following fields: "* Environment" (a dropdown menu with "Select environment"), "* Flow Display Name" (a text input), "* Flow Definition" (a text input), "* Flow State" (a text input), and "connectionReferences" (a dashed box containing a text input). The middle dialog is titled "Resubmit Flow" and contains: "* Environment" (dropdown), "* Flow" (dropdown), "* Trigger Name" (text input with placeholder "Name of the flow trigger to resubmit."), and "* Run ID" (text input with placeholder "The ID of the flow run to"). The bottom-right dialog is titled "Delete Flow" and contains: "* Environment" (dropdown) and "* Flow" (dropdown).

Test your defense with Powerful



Test your defense with Powerful

#RSAC

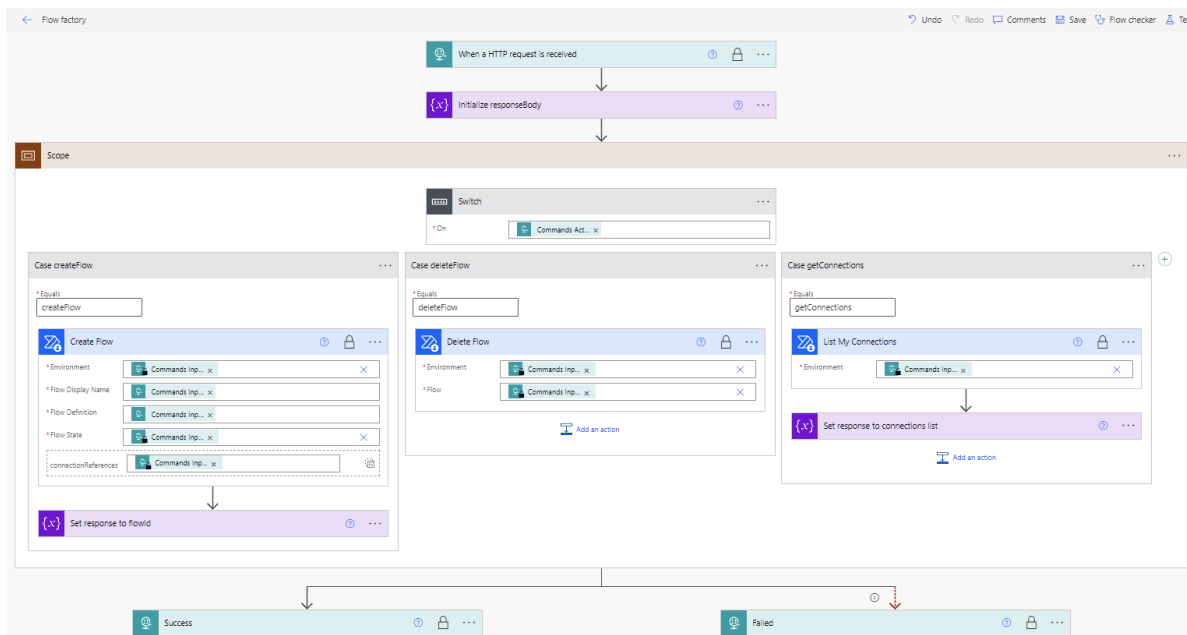
Stronger
Together

```
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"])
```

Test your defense with Powerful

Persistency laundry list:

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



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

RSAConference™2023



**Stronger
Together**

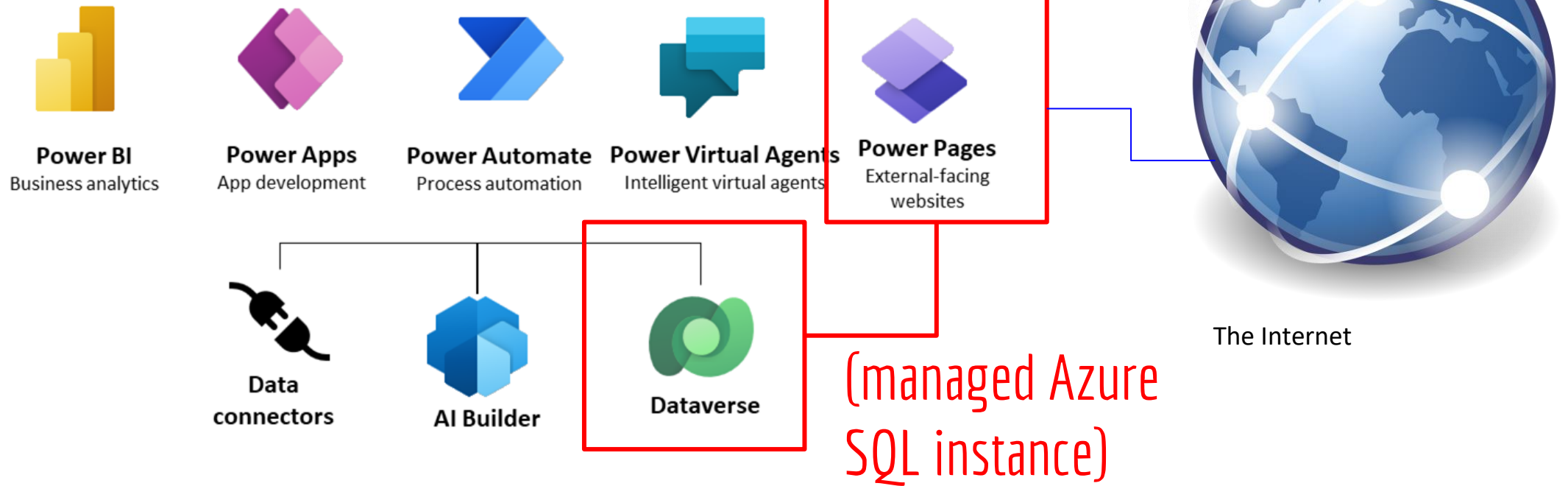
Low Code Attacks In The Wild

Outside looking in

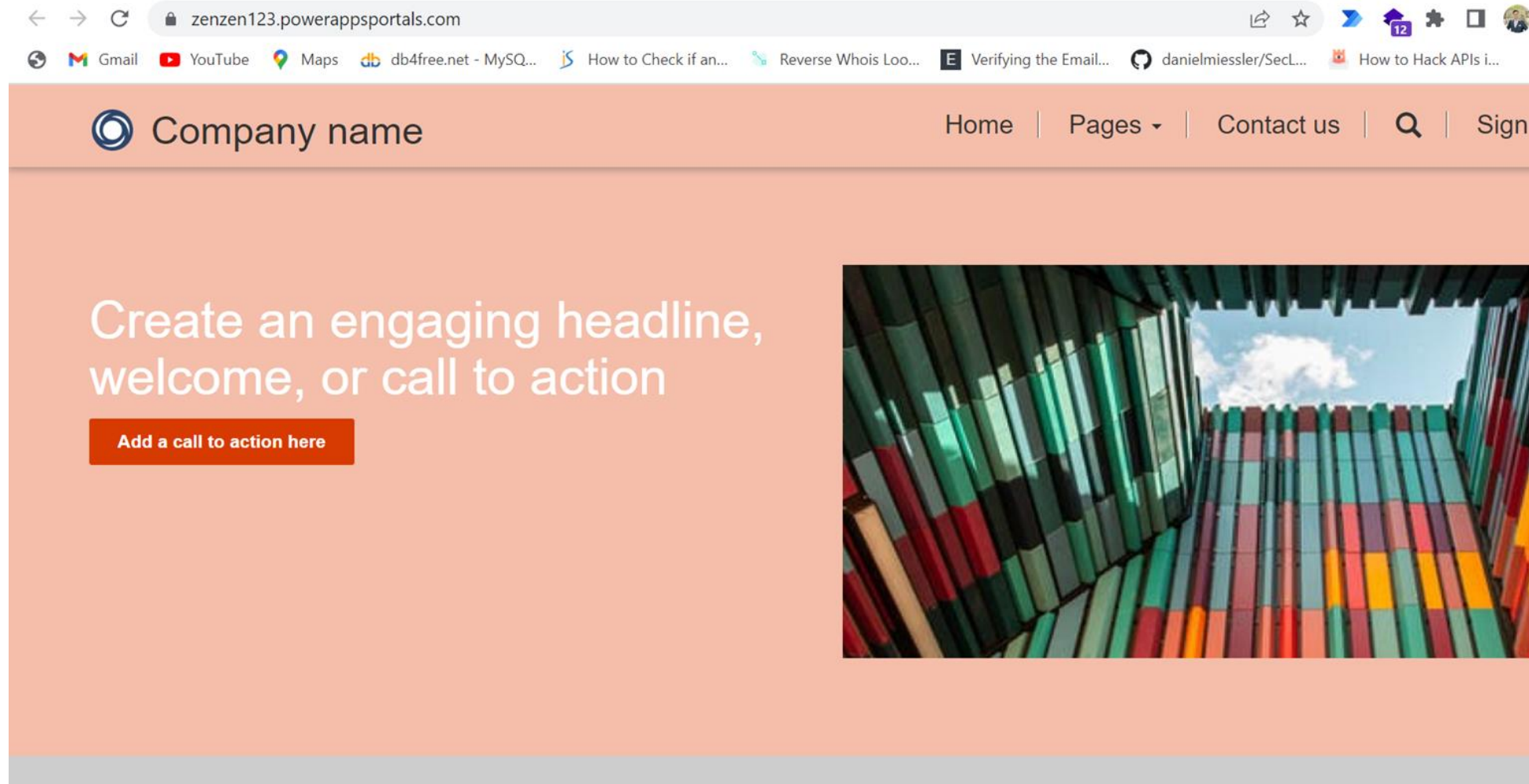
Power Portals/Pages



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



Power Portals/Pages



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>
```


Can we scale it?

Recall the portal url:

zenzen123.powerappsportals.com

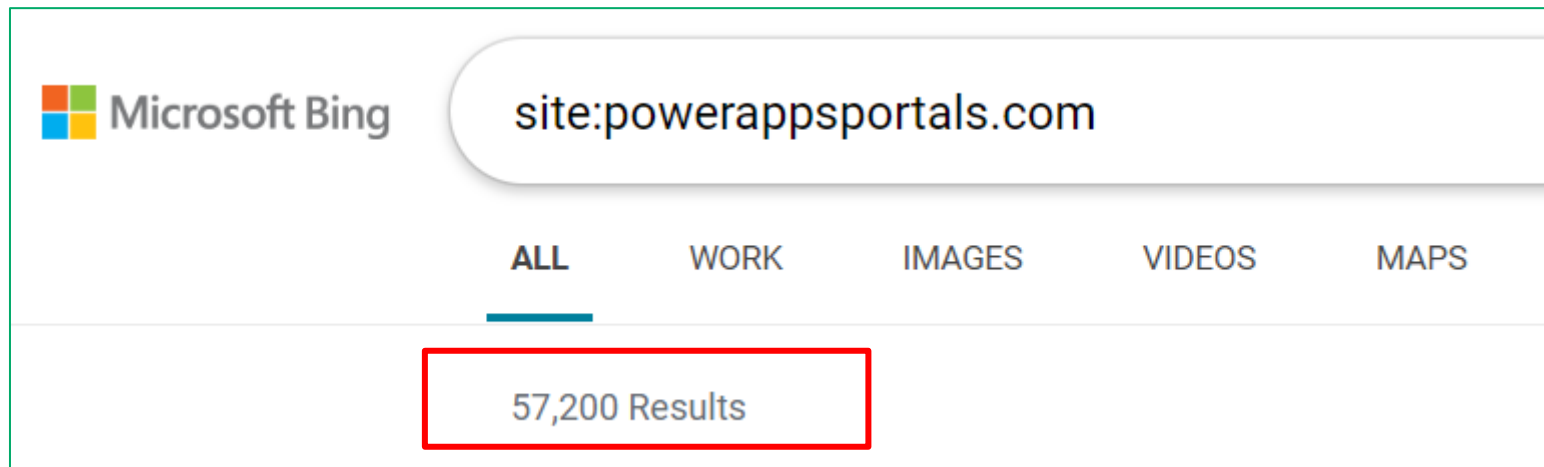
zenity.io/blog/the-microsoft-power-apps-portal-data-leak-revisited-are-you-safe-now/

Can we scale it?

Recall the portal url:

zenzen123.powerappsportals.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?



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

Integrations Help

Do more with Storage by 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 tha",
    "might use to stash a bit of state. we use it to p",
    "`StoreClient` in our Code steps of Zapier - you c",
    "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 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 you
    "might use to stash a bit of state. we use it to power our
    "`StoreClient` in our Code steps of Zapier - you can find
    "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/record": [
    "A data with a patch object",
    "The schema specifies the keys you can use to update records.",
    "For example {\"increment_by\": 1, \"set_value_if\": \"<key_>\", \"remove_child_value\": \"<key_>\", \"set_child_value\": \"<value_>\", \"list_push\": \"<value_>\", \"list_pop\": \"<key_>\"}."
  ],
  "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=>

```
{"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": "", "Number": "APIkey"}
{"bitcoinusd": "4", "dedupe": "d.com", "postlinjection": "2021-05-02"}
https://zoom.us/j/94?pwd=09\
{"YTAAuth": "perm:", "ZDAuth": "r.com| -LW7"}
```

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

RSAConference™2023



**Stronger
Together**

How To Stay Safe

Summary



- You can't opt out of citizen development
 - 70% of enterprise apps by 2025
 - Available on every major enterprise, yours too
 - Millions of new (business) developers and growing fast
- Security controls are severely lacking
 - Lacking SDLC
 - Developers with no security savviness
 - 10-100x the scale of application development
- Attackers are taking advantage of it by
 - Living off the land – account takeover, lateral movement, PrivEsc, data exfil
 - Hiding in plain sight
 - Leveraging predictable misconfiguration from the outside

OWASP Low-Code / No-Code Top 10

- [LCNC-SEC-01: Account Impersonation](#)
- [LCNC-SEC-02: Authorization Misuse](#)
- [LCNC-SEC-03: Data Leakage and Unexpected Consequences](#)
- [LCNC-SEC-04: Authentication and Secure Communication Failures](#)
- [LCNC-SEC-05: Security Misconfiguration](#)
- [LCNC-SEC-06: Injection Handling Failures](#)
- [LCNC-SEC-07: Vulnerable, Unmanaged and Untrusted Components](#)
- [LCNC-SEC-08: Data and Secret Handling Failures](#)
- [LCNC-SEC-09: Asset Management Failures](#)
- [LCNC-SEC-10: Security Logging and Monitoring Failures](#)

Do these 4 things to reduce your risk



- Expand Secure Development standards to low-code / no-code
 - Approved use cases and training
 - Security assurance
- Monitor low-code / no-code applications
 - Shared credentials and used identities
 - Data accessed
 - External-facing endpoints (webhooks, Microsoft ODATA, Zapier Storage)
- Leverage the OWASP LCNC Top 10 (bit.ly/owasp-lcnc-top10)
- Leverage Open-Source tools
 - ZapCreds – identify overshared credentials on Zapier github.com/mbrg/zapcreds
 - Powerful – reproduce persistence using Microsoft Power Platform github.com/mbrg/powerful
 - Power-Pwn – reproduce malicious usage of Microsoft Power Automate Desktop github.com/mbrg/power-pwn

RSAC Conference™ 2023

San Francisco | April 24 – 27 | Moscone Center

SESSION ID: DAS-R06

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



#RSAC

Michael Bargury

CTO & Co-founder

Zenity

@mbrg0