

Credential Sharing as a Service:

The Dark Side of No Code

Michael Bargury @ Zenity

SANS Cybersecurity Leadership UK Summit 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



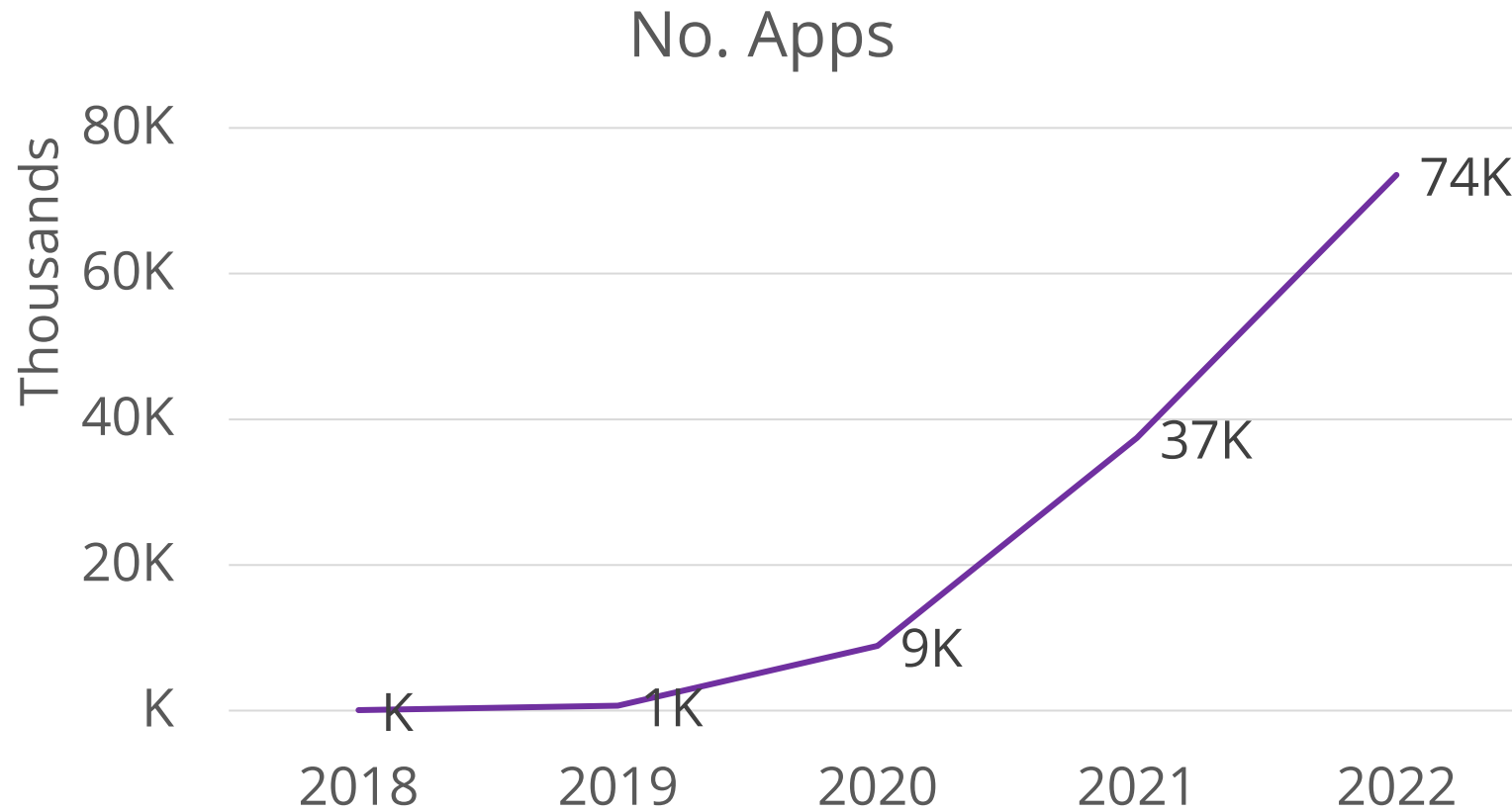
Outline

- Low Code / No Code growth and evolution
- 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



Business-Led Development Is Here

Exponential Growth in Business Development



The Low-Code/No-Code Evolution: How did we get here?

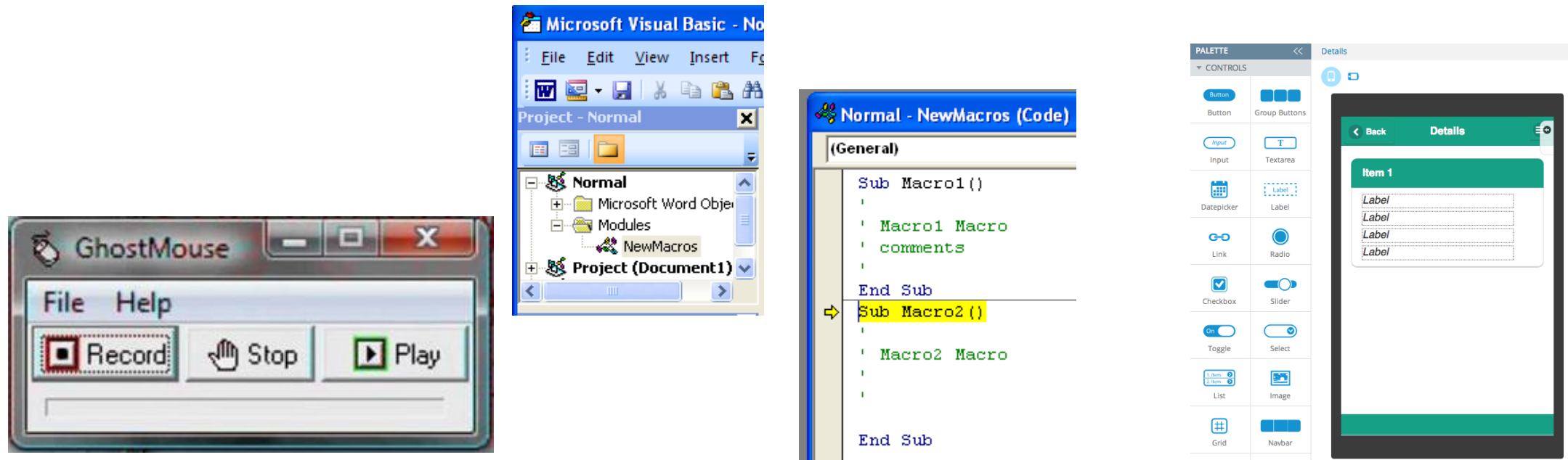
Business Needs



IT Capacity



If it sounds familiar, its because it is



Tech evolution

Build everything

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

The image displays three overlapping screenshots from the Zapier automation platform. The top screenshot shows a Zap workflow 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 the 'Trigger' step, '1. New Mention in Slack', with options to 'Choose app & event' and 'Choose account'. The bottom screenshot shows the 'Choose account' dialog for Slack, listing 'Slack @michaelbargury (pwntoso)' and 'Slack @michaelbargury (CTOs)'. On the left, a partial view of the Zapier 'Insert' menu is visible, listing various widget types like 'Text label', 'Form', 'Input', 'Display', etc.

Available in every major enterprise



zapier*



mx mendix

/// make
formerly Integromat



servicenow™



Betty Blocks



Microsoft

o outsystems

Appian

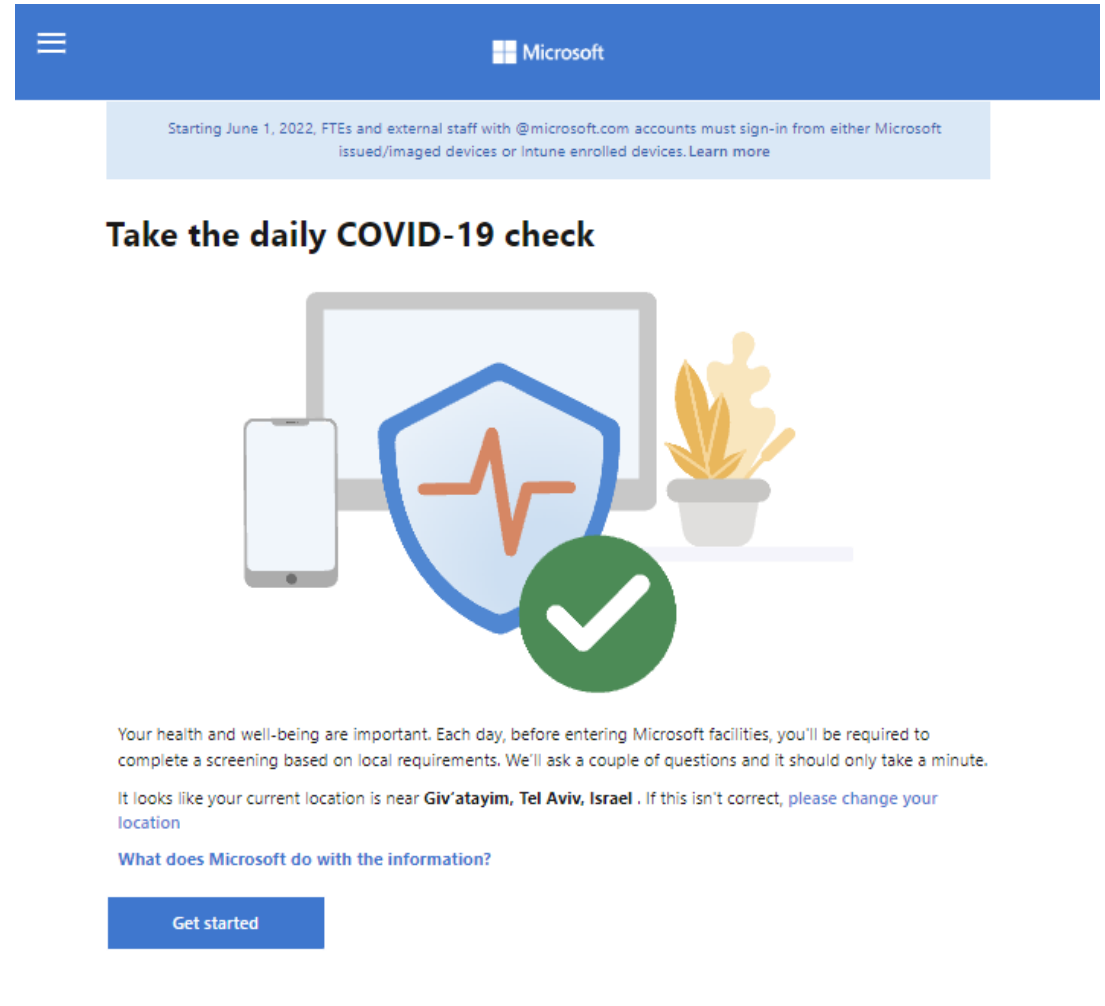
Build Business Apps Faster

How low code / no code accelerates development:

- Ease of use lowers barrier to entry
- Off-the-shelf integrated components
- Key app features are baked-in (AuthN, AuthZ, ..)
- Connectors to on-prem, cloud and SaaS
- “Save” to deploy
- No infra to maintain

COVID health check app by Microsoft

<https://aka.ms/healthcheck>



The screenshot shows the Microsoft COVID-19 health check app interface. At the top, there is a blue header with a hamburger menu icon on the left and the Microsoft logo on the right. Below the header, 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 this is an illustration featuring a smartphone, a laptop, a shield with a red heartbeat line, and a green checkmark in a circle, all set against a background of a desk with a potted plant.

The text below the illustration 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. 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 a link: "What does Microsoft do with the information?".

At the bottom of the main content area is a blue button labeled "Get started".

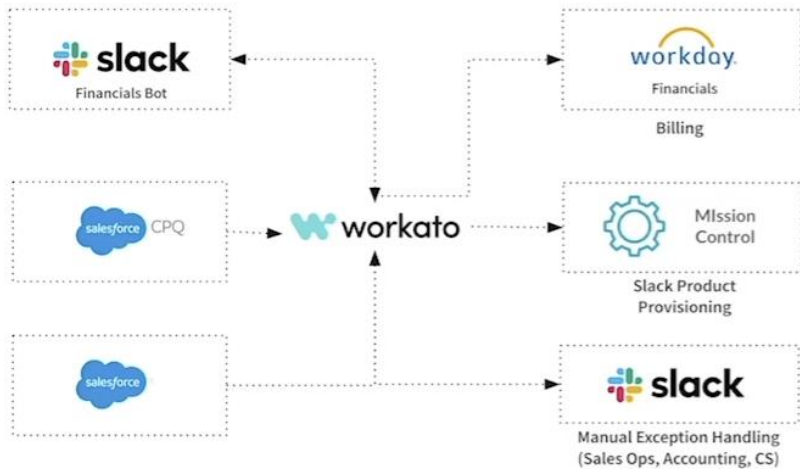
For issues or concerns contact IT Global Helpdesk globalhd@microsoft.com

[Microsoft Data Privacy Notice](#) [Identity Terms of Use](#) [Feedback](#)

© 2021 Microsoft



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

Order-to-cash automation by Slack

Business users become business developers



"... 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"

A Humble Beginning – Low Code as Extendibility

“With Dynamics, ..., we also launched this very powerful platform, the Power Platform -- ... which acts as the extensibility framework for Microsoft Graph, extensibility framework for Dynamics, as well as Microsoft 365, and embeddable by every SaaS ISV.”

Satya Nadella, Microsoft Build 2018

Shift to Empowerment of Business Users

"Anyone can be a developer, completely transforming how your business operates"

"... we need to empower citizen developers with tools that are low-code/no-code tools so that they can build out these applications In fact, there are already 2.5 million citizen developers using Power Platform ..."

"Once Excel was introduced, a lot of people were able to build spreadsheets and become numerical and analytical ... think about all the white-collar-ish jobs that were created ... we want the same thing to happen with low-code/no-code."

Satya Nadella, Microsoft Ignite 2019

Business Users are Leading The Way

“By 2025, 70% of new applications deployed for the enterprise will use low-code or no-code tools, up from less than 25% in 2020.”

“With Power Platform, we have the leading business process automation and productivity suite for domain experts in every industry, with 20 million monthly active users.”

Satya Nadella, Microsoft Inspire 2022



The Race for a New Excel

Big vendors
have a strong
incentive to
empower
business users



Companies are
lacking IT
resources and
need a
solution for
accelerated
development



The tech is
already there -
business users
are actually
using it

Recap

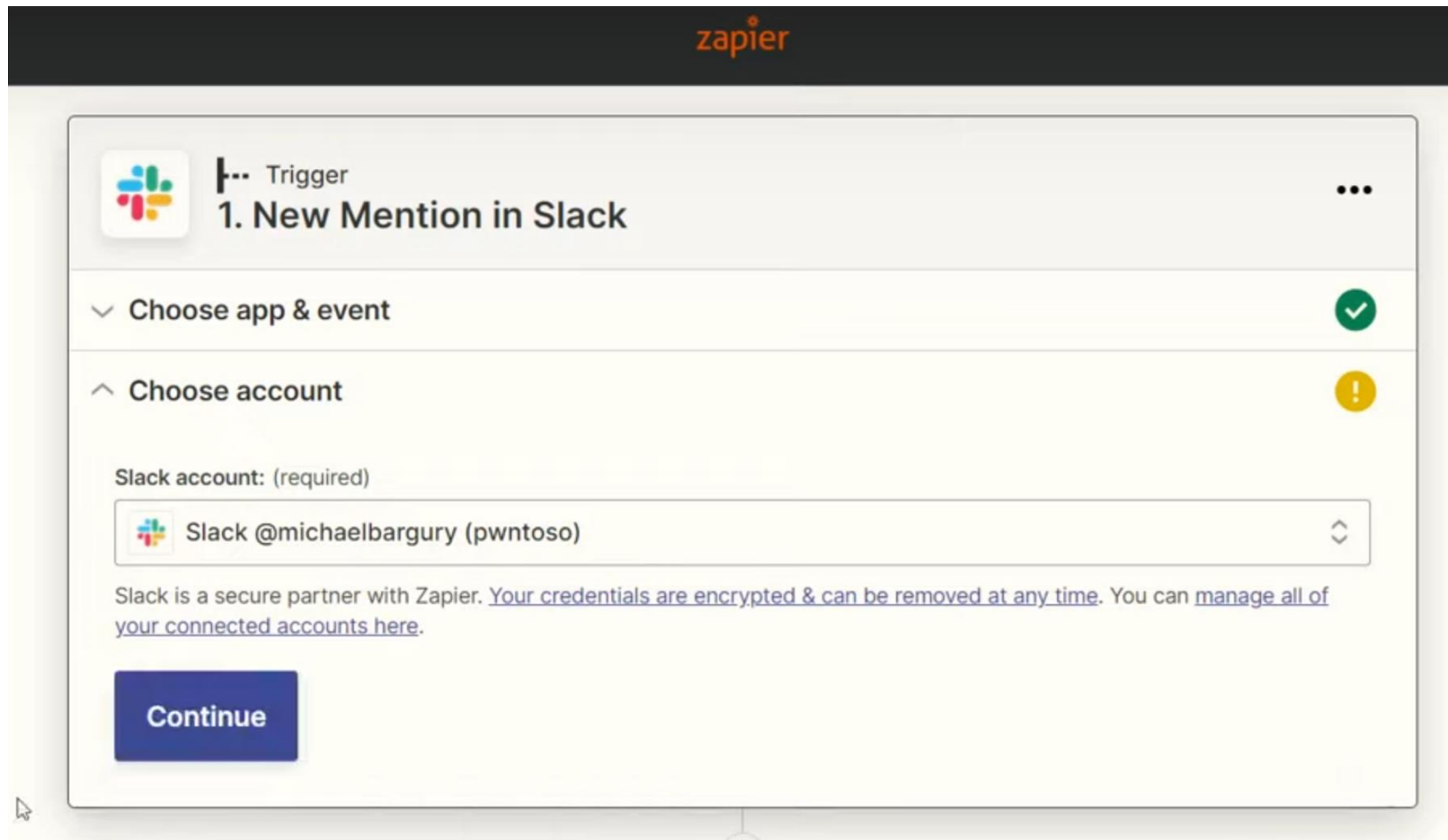
- ✓ Available on every major enterprise
- ✓ Has access to business data and powers business processes
- ✓ Runs as SaaS (difficult to monitor)
- ✓ Underrated by IT/Sec

Low Code Attacks In The Wild

Living off the land



Wait. What?



The screenshot shows the Zapier interface for configuring a trigger. At the top, the Zapier logo is visible. The main content area is titled "Trigger" and "1. New Mention in Slack". Below this, there are two sections: "Choose app & event" which is completed with a green checkmark, and "Choose account" which has a yellow warning icon. Under "Choose account", there is a dropdown menu labeled "Slack account: (required)" with the selected account "Slack @michaelbargury (pwntoso)". Below the dropdown, there is a note: "Slack is a secure partner with Zapier. [Your credentials are encrypted & can be removed at any time.](#) You can [manage all of your connected accounts here.](#)" At the bottom of the configuration area is a blue "Continue" button.

zapier

Trigger
1. New Mention in Slack

✓ Choose app & event

⚠ Choose account

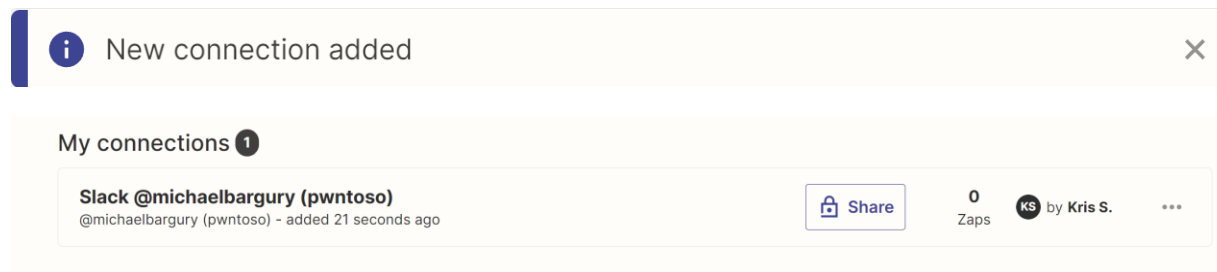
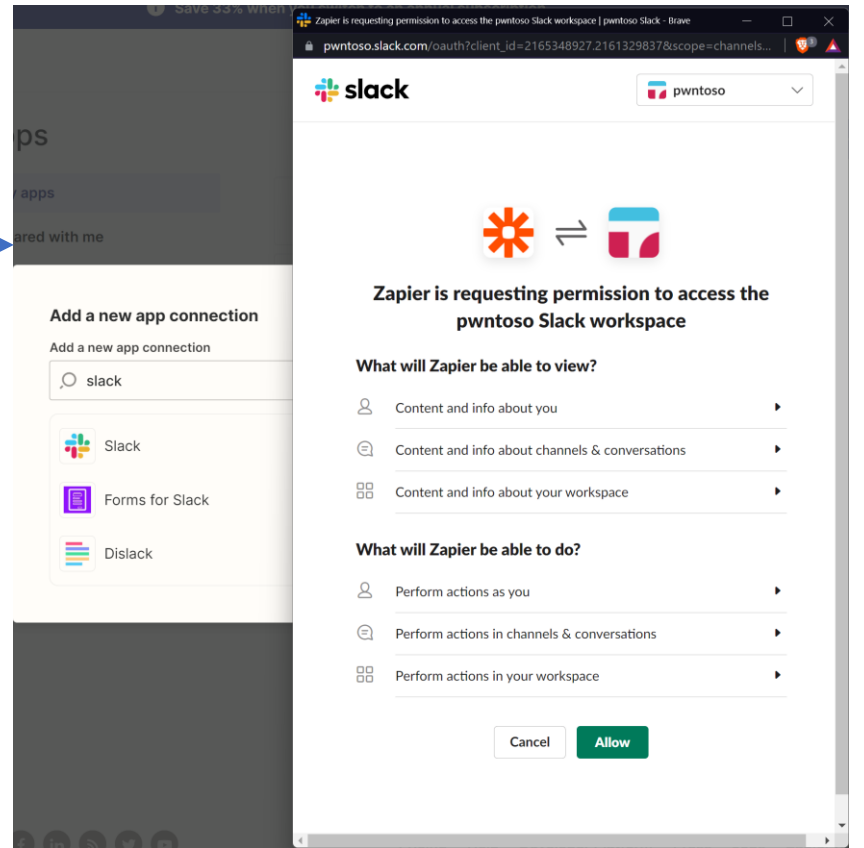
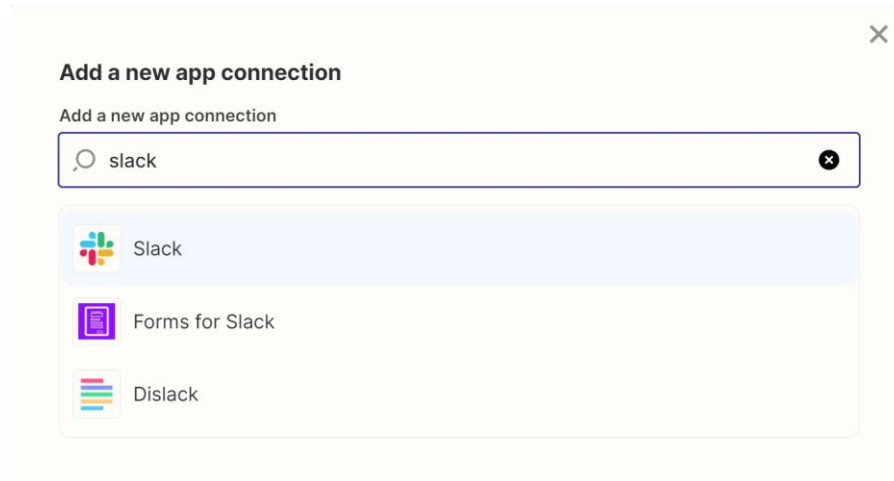
Slack account: (required)

Slack @michaelbargury (pwntoso)

Slack is a secure partner with Zapier. [Your credentials are encrypted & can be removed at any time.](#) You can [manage all of your connected accounts here.](#)

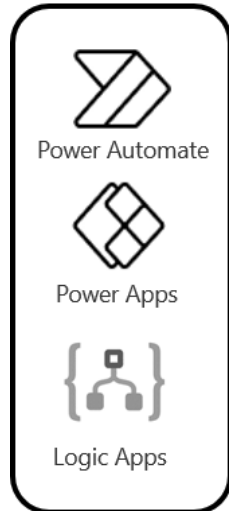
Continue

Step by step



Behind the scenes

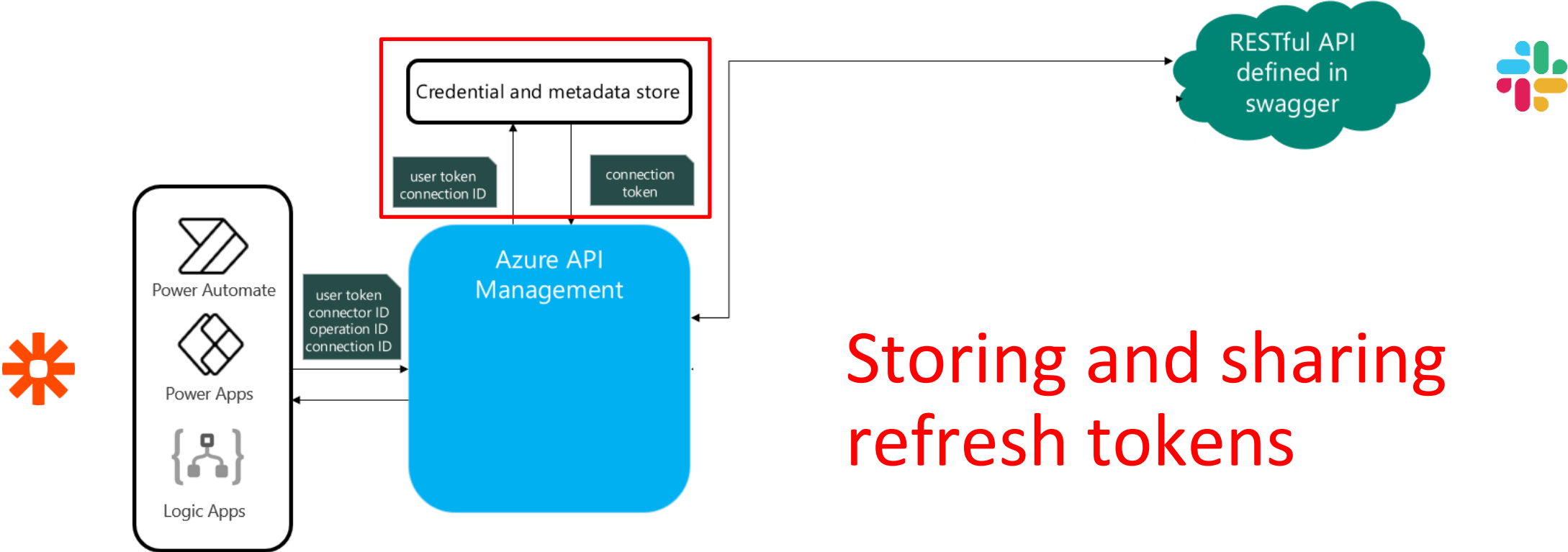
RESTful API
defined in
swagger



How does the app
authenticate to slack?

How do different users get
authenticated by the same
app?

Behind the scenes



Ready, set, AUTOMATE!

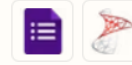


Premium

Add new Facebook Lead Ads leads to rows on Google Sheets



Add info to a Google Sheet from new Webhook POST requests



Premium

Create SQL Server rows from new Google Forms responses



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

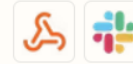
Automated
214763



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
32731



Add SQL Server rows with new caught webhooks

Webhooks by Zapier + SQL Server



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

Credential Sharing as a Service

The image displays two overlapping software interfaces. The background interface is Microsoft Power Automate, showing a list of connections in the 'Zenity Stage (default)' environment. The foreground interface is Zapier, showing a list of apps with connection and zap counts.

Power Automate Connections:

Name	Modified
ConnectionToFadiStorageAccount 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)	
23 DB2	
File System File System	
Notifications Notifications	
Vendor Server FTP	
FTP FTP	
pa2g@gmail.com Gmail	1 wk ago

Zapier Apps:

App	Connections	Zaps
Gmail	2	5
Google Sheets	1	2

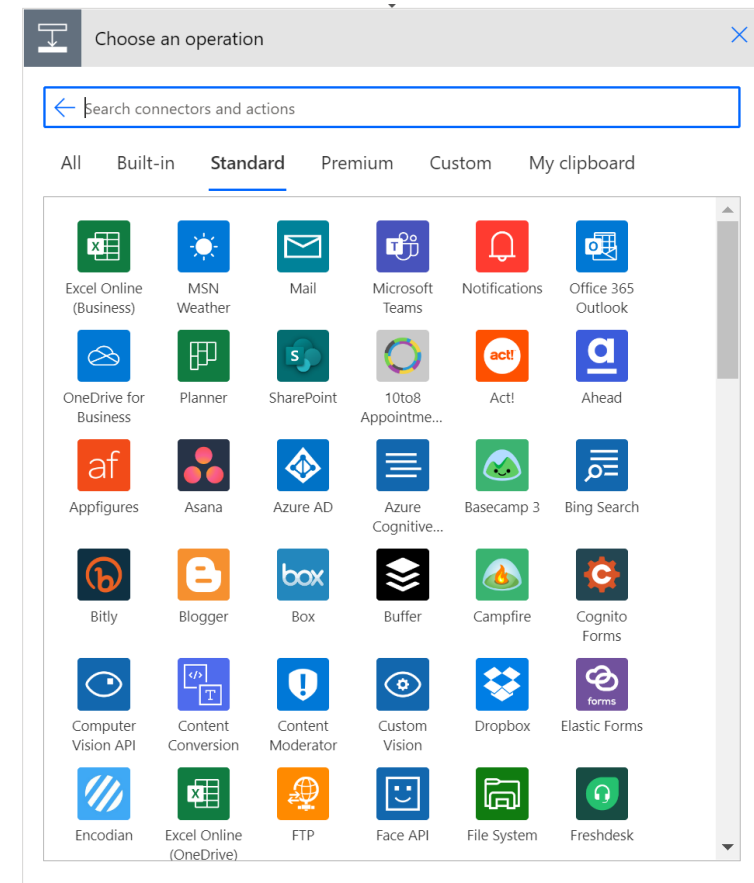
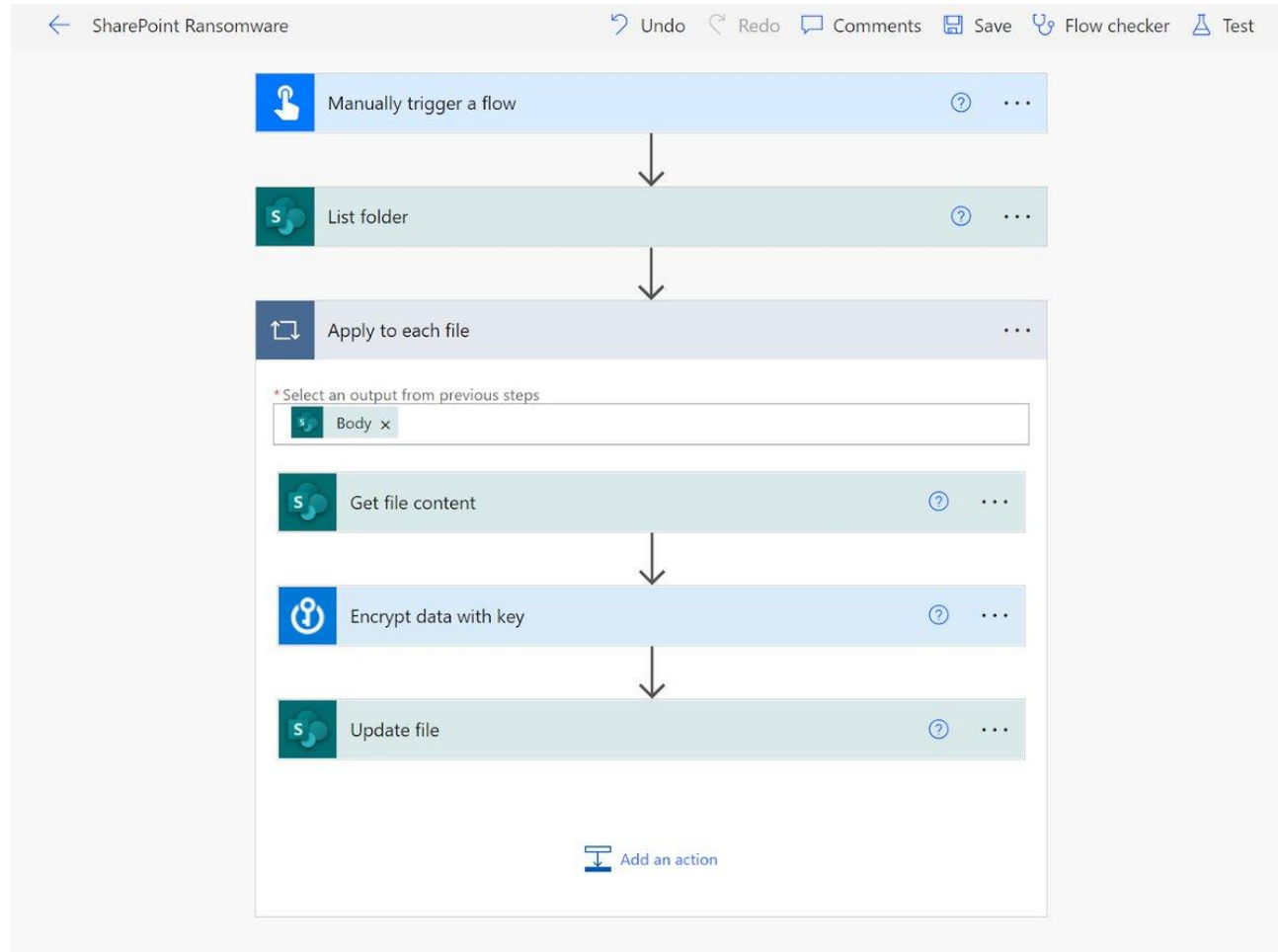
Credential Sharing as a Service

The screenshot displays the Microsoft 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 'ConnectionToFadiStorageAccount Azure Blob Storage', 'SQL Server', 'stage.com Azure Blob Storage', 'stage.com Microsoft Dataverse', 'Connective eSignatures', '23 DB2', 'File System', 'Notifications', 'Vendor Server FTP', and 'FTP'. A central overlay image shows a baby with a pouting face. On the right, there's an 'Assets' section with a table of connections and their associated recipes. Below this is an 'Apps' section with 'My apps', 'Shared with me', and 'Custom integrations'. The 'Shared with me' section lists 'Gmail' (2 Connections, 5 Zaps) and 'Google Sheets' (1 Connection, 2 Zaps). A green callout box in the bottom right corner contains a checkmark icon and the text 'Privilege escalation'.

Asset Name	Status	Created	Recipes
Management	Connected	May 22 at 1:47 am	4
	Connected	Feb 6 at 1:21 am	0
	Connected	Feb 6 at 1:21 am	0
	Connected	Feb 10 at 1:40 am	1
	Connected	Apr 9, 2021, at 7:05 am	932
	Connected	Apr 9, 2021, at 5:05 am	1

Privilege escalation

Ransomware thru action connections



Ransomware

When a new email arrives (V3) ? ...

Folder 📁

Show advanced options ▾



Send an email notification (V3) ? ...

* To

* Subject

* Body

Font 12 **B** *I* U 🖋️ ☰ ☷ ☹️ ☺️ 🔗 🔗 </>

From: From x

To: To x

Subject: Subject x

Body: Body x

Show advanced options ▾



Delete email (V2) ? ...

* Message Id

Original Mailbox Address

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

Lateral movement

Can we fool users to create connections for us?

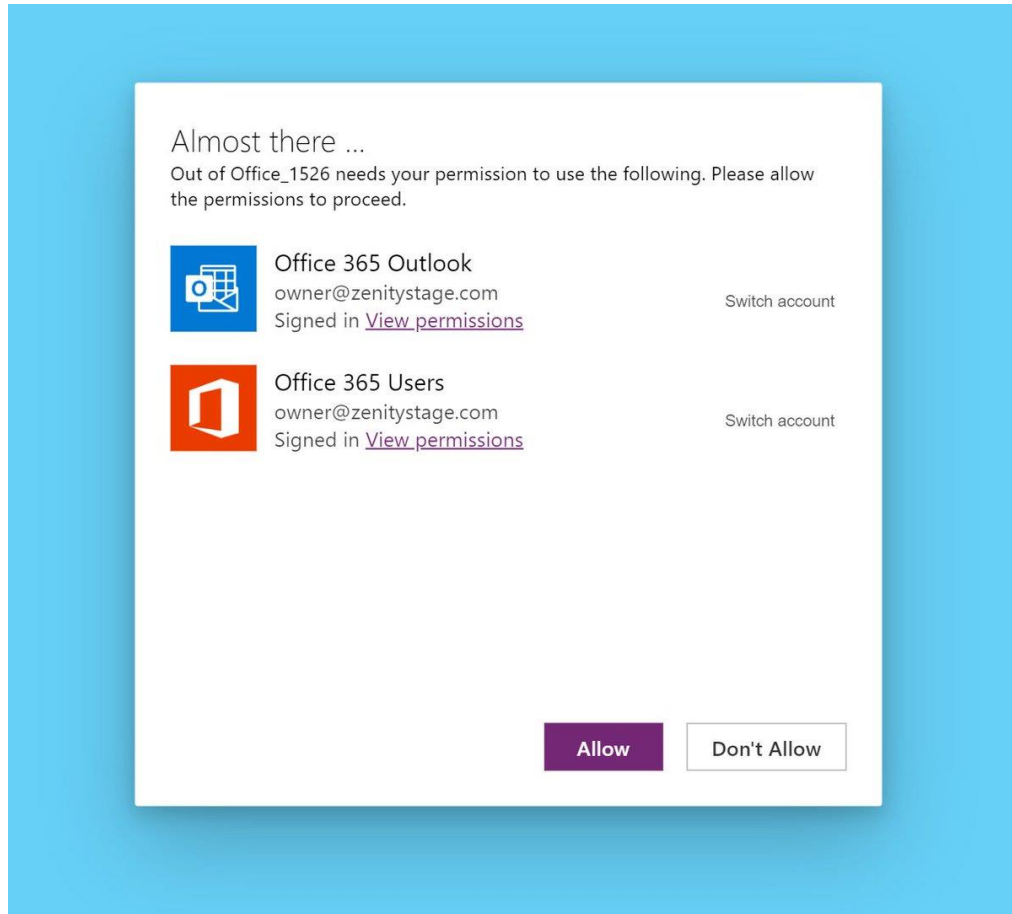
- Set up a bait app that does something useful
- Generate connections on-the-fly
- Fool users to use it
- Pwn their connection (i.e. account)

Account takeover

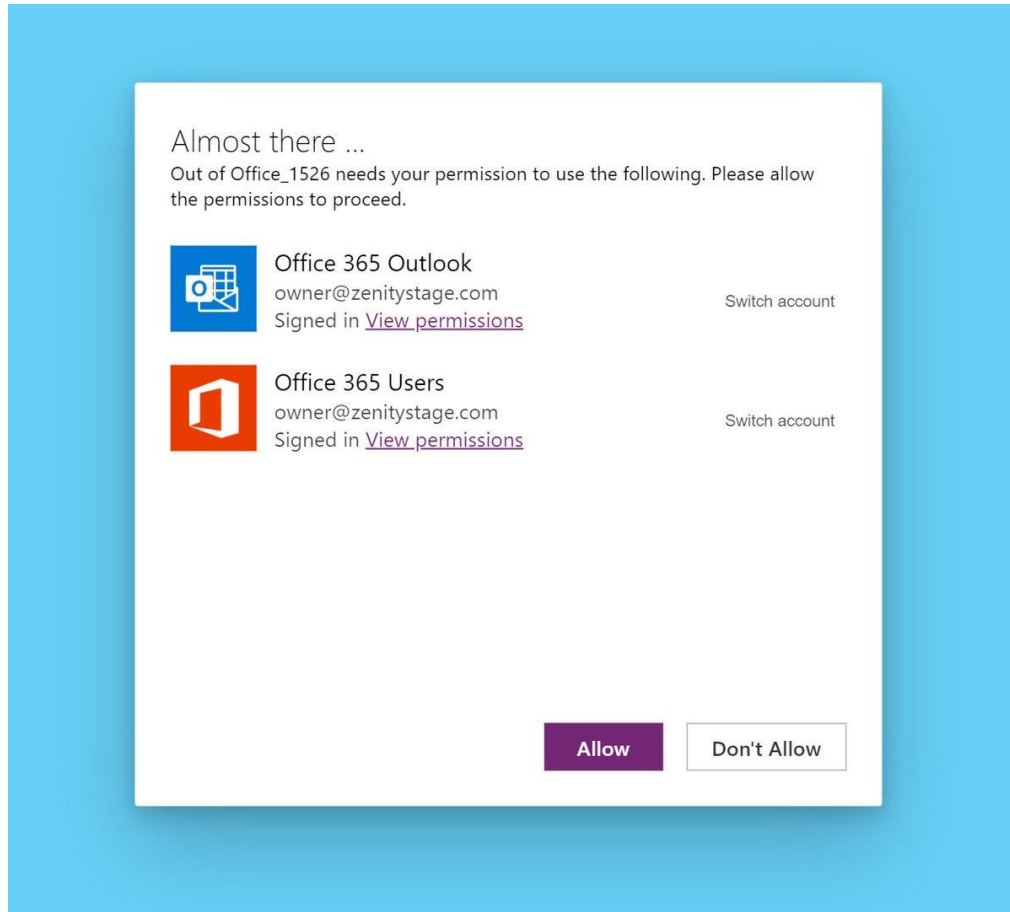


youtu.be/vJZpNJRC_10

Saved by the prompt?



Saved by the prompt? No.



Microsoft | Docs [Documentation](#) [Learn](#) [Q&A](#) [Code Samples](#)

... / Microsoft.PowerApps.Administration.PowerShell /

Set-AdminPowerAppApisToBypassConsent

Reference [👍](#) [🗨](#)

Module: `Microsoft.PowerApps.Administration.PowerShell`

Sets the consent bypass of an app to true.

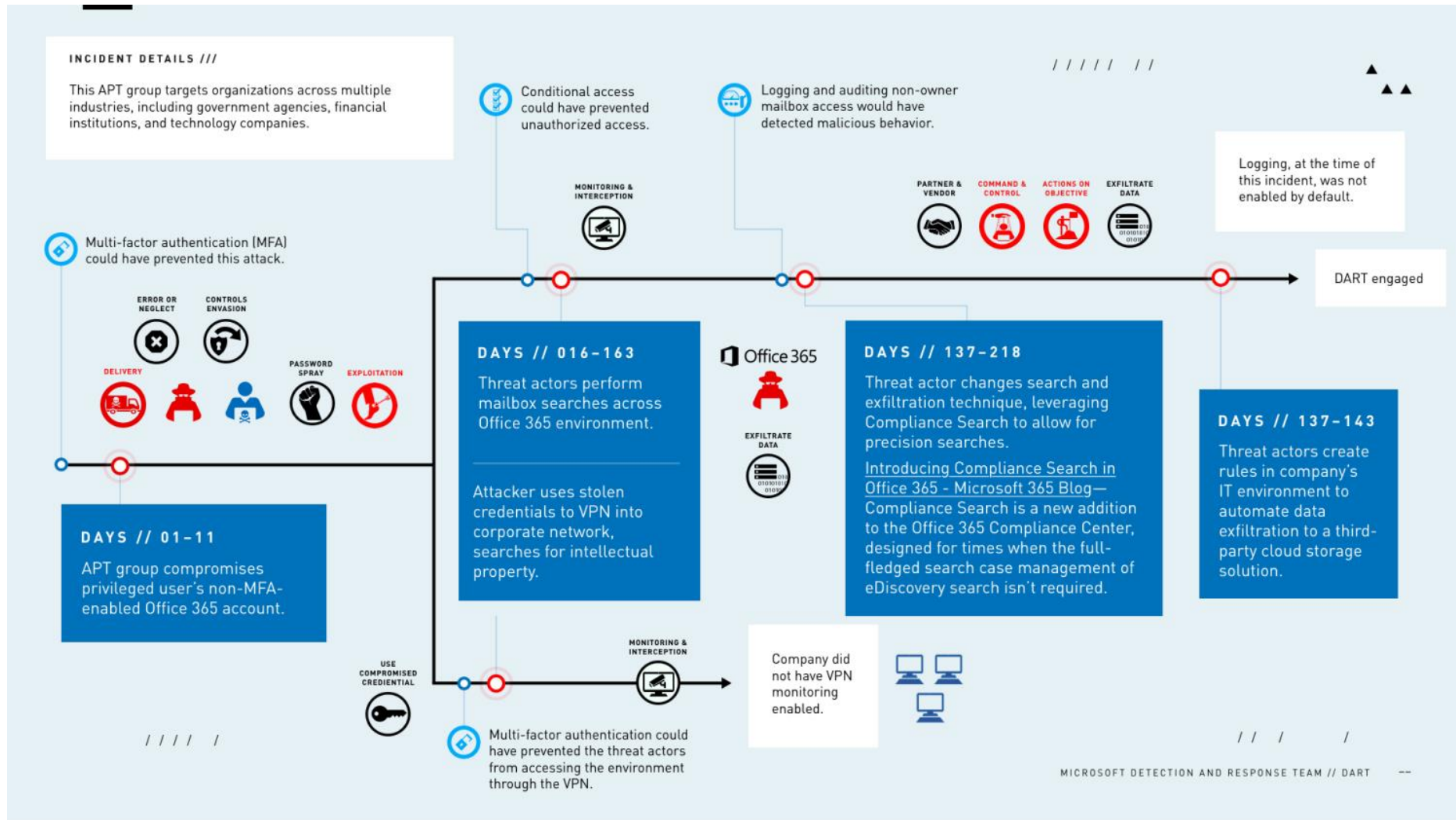
Description

The `Set-AdminPowerAppApisToBypassConsent` cmdlet changes the consent bypass so that users are not required to authorize API connections for the input app. The command changes the `bypassConsent` flag of an app to true. Using this command, end users will observe consent is bypassed for First Party connectors that support single sign-on and custom connectors that don't require authentication. This includes custom connectors with or without a gateway.

Hiding in plain sight

Persistence

This has been done before



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

Summary

- Low Code is huge in the enterprise
 - Probably already in your org
 - Shift focus to business users
- Attackers are taking advantage of it by living off the land
 - Account takeover
 - Lateral movement
 - PrivEsc
 - Data exfil
 - Persistence
- How to defend your org

How To Stay Safe?

Do these 4 things to reduce your risk

1. Leverage the [OWASP LCNC Top 10](#)
2. Expand Secure Development standards to low-code / no-code
 1. Approved use cases
 2. Training
 3. Security assurance
 4. Threat modeling
3. Inventory low-code / no-code applications
 1. Identities used
 2. Data accessed
4. Leverage Open-Source tools
 1. ZapCreds – identify overshared credentials on Zapier <https://github.com/mbrg/zapcreds>
 2. Powerful – reproduce persistence using Microsoft Power Platform <https://github.com/mbrg/powerful>
 3. Power-Pwn – reproduce malicious usage of Microsoft Power Automate Desktop <https://github.com/mbrg/power-pwn>



Learn more: github.com/mbrg0/talks
Twitter: @mbrg0

Credential Sharing as a Service:

The Dark Side of No Code

A solid purple horizontal bar that spans across the width of the text below it.

Michael Bargury @ Zenity

SANS Cybersecurity Leadership UK Summit 2023