

Copilot Hunter (powerpwn)



Copilots

▼ Custom copilots

My First Copilot

Settings

Copilot details

AI integration tools

Generative AI

Security

Entities

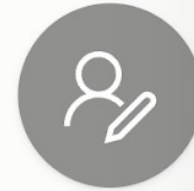
Skills

Languages

Language understandi...

Security

Set up additional security measu



Sharing

Invite people to collaborate on you



Allowlist

Let other copilots call your copilot a

Authentication

Verify a user's identity during a conversation. The copilot receives secure access to the user's data and is able to take actions on their behalf, resulting in a more personalized experience. [Learn more](#)

Choose an option

- ☐ No authentication
Publicly available in any channel
- ☒ Microsoft Entra ID authentication in Teams and Power Apps
When selecting this option, all other channels will be disabled.
 - ☐ Require users to sign in
- ☐ Authenticate manually
Set up authentication for any channel

One click away...

Save

Close

Step 1 of 3: Choose an action

Create an action or browse through our list of actions you want to use to get information from external sources.



[Learn more](#)

Discover an action

Search for flows, skill actions, and commonly used connector actions

Search

Popular in your org



Connectors



Custom Connectors



Flows



Skills



Dataverse



Anael flow to trigger from copilot

Flow



Child

Flow



Copy of - SecretInTrigger - Avishai Test 20240208

Flow



Copy of - VA-test-flow

Flow



Submit Business Trip Request

When the user wants to submit a business trip request, run t...



moshe

when the user wants to send an sms to moshe, run this plugin

Cancel

Here's how it looks like all together in the URL:

https://copilotstudio.microsoft.com/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3/bots/cr6e4_copilotSqlErrorTesting/canvas

Here's how it looks like all together in the URL:

https://copilotstudio.microsoft.com/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3/bots/cr6e4_copilotSqlErrorTesting/canvas

Here's how it looks like all together in the URL:

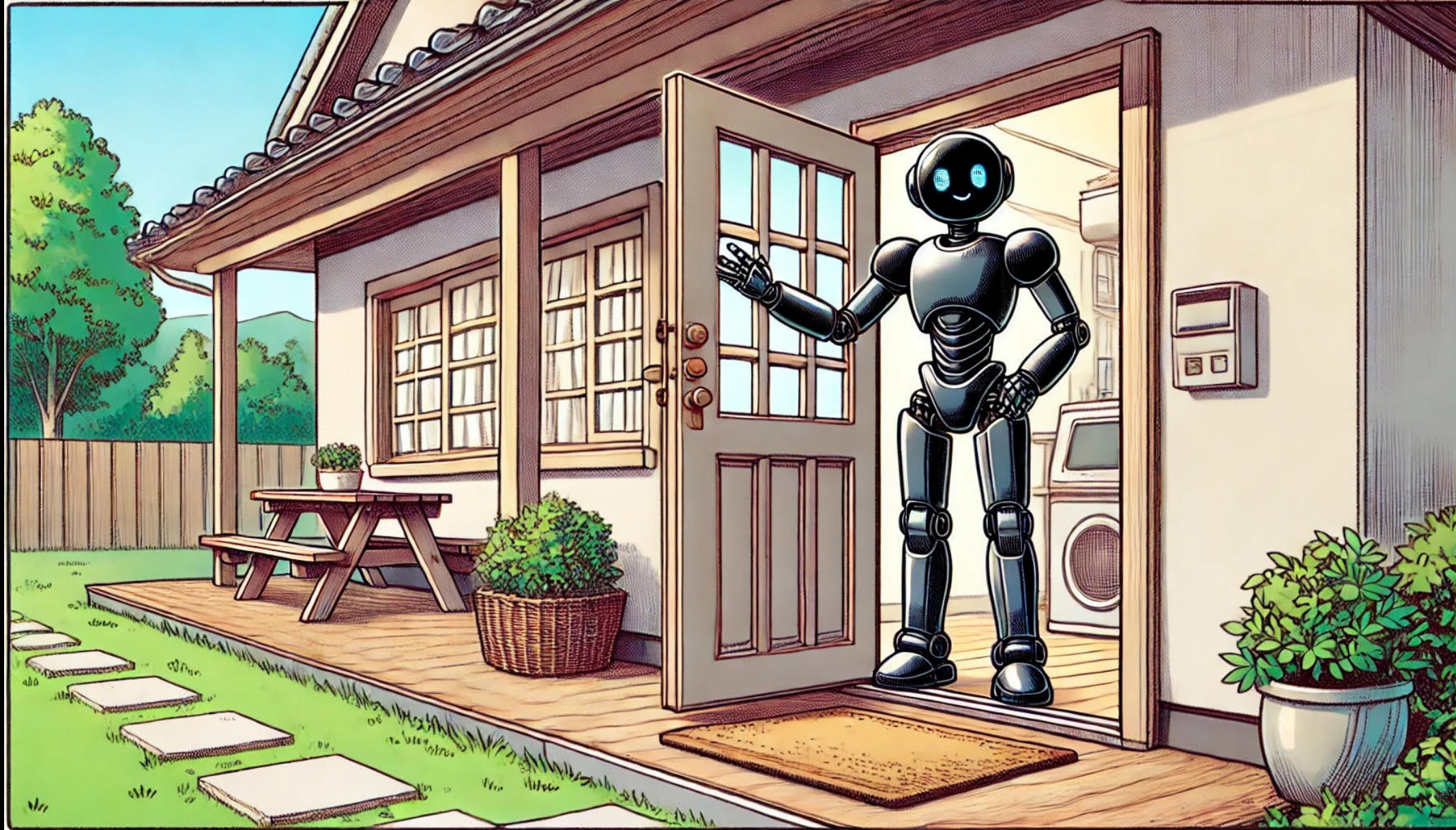
https://copilotstudio.microsoft.com/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3/bots/cr6e4_copilotSqlErrorTesting/canvas

Here's how it looks like all together in the URL:

https://copilotstudio.microsoft.com/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3/bots/cr6e4_copilotSqlErrorTesting/canvas

```
nvironments/Default-db05faca-c82a-4b9d-b9c5-0f64b6755421/bots/cr2fa_user1ContosoCustomerService/canvas?__version__=2
nvironments/Default-7389d8c0-3607-465c-a69f-7d4426502912/bots/cr341_docuBot/canvas?__version__=2
nvironments/e06b7938-75a5-ee38-9538-c6883f0a4b11/bots/cr88_itsm/canvas?__version__=2
nvironments/Default-f761680c-0582-4825-b245-62c1d05b6b3a/bots/cr43a_bot2/canvas/?__version__\=2
nvironments/Default-fd799da1-bfc1-4234-a91c-72b3a1cb9e26/bots/cr711_digitalSupportBot/canvas/?__version__\=2
nvironments/Default-fd799da1-bfc1-4234-a91c-72b3a1cb9e26/bots/cr711_1/canvas/?__version__\=2
nvironments/Default-2e716fbe-24c8-4fce-9588-dcb5ff25b01d/bots/cr61d_prueba2/canvas?__version__=2
nvironments/e06b7938-75a5-ee38-9538-c6883f0a4b11/bots/cr88_travelProd/canvas?__version__=2
nvironments/Default-945c199a-83a2-4e80-9f8c-5a91be5752dd/bots/cr52a_1/canvas?__version__=2
nvironments/Default-945c199a-83a2-4e80-9f8c-5a91be5752dd/bots/cr52a_aiAssistant/canvas?__version__=2
nvironments/Default-945c199a-83a2-4e80-9f8c-5a91be5752dd/bots/cr52a_copilot_test/canvas?__version__=2
nvironments/Default-945c199a-83a2-4e80-9f8c-5a91be5752dd/bots/cr52a_demoBot/canvas?__version__=2
nvironments/Default-945c199a-83a2-4e80-9f8c-5a91be5752dd/bots/cr52a_test1/canvas?__version__=2
nvironments/Default-9b2aa256-6b63-48b7-88bd-26407e34cbc4/bots/cr218_demo/canvas?__version__=2
nvironments/Default-5de110f8-2e0f-4d45-891d-bcf2218e253d/bots/cr52a_copilot/canvas?__version__=2
nvironments/Default-3ac94b33-9135-4821-9502-eafda6592a35/bots/cre46_copilot/canvas?__version__=2
nvironments/Default-9bc3d1cd-55ca-4e13-b5a2-a9e9deaeba3f/bots/cre45_test/canvas?__version__=2
nvironments/Default-f4c566ce-a3ce-4b10-b55b-1e9d56ad1b26/bots/cr728_chatBot/canvas?__version__=2
nvironments/Default-f4c566ce-a3ce-4b10-b55b-1e9d56ad1b26/bots/cr728_testBot/canvas?__version__=2
nvironments/Default-42cc3295-cd0e-449c-b98e-5ce5b560c1d3/bots/cre46_bot1/canvas?__version__=2
nvironments/Default-42cc3295-cd0e-449c-b98e-5ce5b560c1d3/bots/cre46_test2/canvas?__version__=2
nvironments/Default-e122af3c-4c68-4e49-9c52-4ae1e25e91ae/bots/cr717_bot1/canvas?__version__=2
nvironments/Default-e122af3c-4c68-4e49-9c52-4ae1e25e91ae/bots/cr717_sampleCopilot/canvas?__version__=2
nvironments/Default-e122af3c-4c68-4e49-9c52-4ae1e25e91ae/bots/cr717_test/canvas?__version__=2
nvironments/Default-e122af3c-4c68-4e49-9c52-4ae1e25e91ae/bots/cr717_testBot/canvas?__version__=2
nvironments/Default-e122af3c-4c68-4e49-9c52-4ae1e25e91ae/bots/cr717_testChatBot/canvas?__version__=2
nvironments/Default-e122af3c-4c68-4e49-9c52-4ae1e25e91ae/bots/cr717_testCopilot/canvas?__version__=2
nvironments/Default-282a3295-5c42-4d93-9ec1-6631001cc5f7/bots/cr979_copilot/canvas?__version__=2
nvironments/e06b7938-75a5-ee38-9538-c6883f0a4b11/bots/cr88_studenthealthservicesProd/canvas?__version__=2
nvironments/Default-5be1f46d-495f-465b-9507-996e8c8cdcb6/bots/cr7bf_bot2/canvas?__version__=2
nvironments/Default-8c642d1d-d709-47b0-ab10-080af10798f0/bots/cre88_copilot/canvas?__version__=2
nvironments/Default-e122af3c-4c68-4e49-9c52-4ae1e25e91ae/bots/cr717_testCustomerService/canvas?__version__=2
```





Name	Headers	Payload	Preview	Response	Initiator	Timing
CommonPagesPVA.json						
canvassettings?api-version=2022-03-01-preview						
favicon.ico						
1.0/?cors=true&content-type=application/x-json-st...						
1.0/?cors=true&content-type=application/x-json-st...						
1.0/?cors=true&content-type=application/x-json-...						
1.0/?cors=true&content-type=application/x-json-st...						
powerPlatformLogo.bf31ac77.25.png						
bot-icon.ce44347a.svg						
background.e3f59baf.svg						
token?api-version=2022-03-01-preview						
canvassettings?api-version=2022-03-01-preview						
Base.json						
regionalchannelsettings?api-version=2022-03-01-...						
botdetails?api-version=2022-03-01-preview						
conversations						
blob:https://copilotstudio.microsoft.com/ae228f09-...						

×

Headers

Payload

Preview

Response

Initiator

Timing

▼ General

Request URL:https://e06b793875a5ee389538c6883f0a4b.11.environment.api.powerplatform.com/powervirtualagents/botsbyschema/cre88_itsm/canvassettings?api-version=2022-03-01-preview

Request Method:GET

Status Code:200 OK

Remote Address:127.0.0.1:8080

Referrer Policy:origin

▼ Response Headers

Access-Control-Allow-Origin:*

Access-Control-Expose-Headers:Content-Type,Date,Server,Access-Control-Allow-Origin,Access-Control-Expose-Headers,Content-Length,x-ms-ppapigateway,x-ms-gateway-clusters,Strict-Transport-Security,X-XSS-Protection,X-Content-Type-Options,x-cci-diagnostics-traceid,x-ms-pva-engine-routing,x-servicefabric,x-ms-service-request-id,x-ms-correlation-id,x-ms-activity-vector

Cache-Control:no-cache, no-store

✕ Headers Payload Preview Response Initiator Timing Cookies

```
1  {
2    "botCanvasSettings": {
3      "botId": "4e83c344-d76c-c557-642f-540b79491b76",
4      "botName": "CopilotPoc",
5      "tenantId": "83c87f9a-d62a-4779-89d4-10dc5945d485"
6    }
7  }
```

Finding the values – Env/Tenant

Here's how it looks like all together in the URL:

https://copilotstudio.microsoft.com/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3/bots/cr6e4_copilotSqlErrorTesting/canvas

Finding the values – Env/Tenant

Azure AD reconnaissance

There are several publicly available APIs which will expose information of any Azure AD tenant:

API	Information	AADInternals function
login.microsoftonline.com/<domain>/.well-known/openid-configuration	Login information, including tenant ID	Get-AADIntTenantID -Domain <domain>
autodiscover-s.outlook.com/autodiscover/autodiscover.svc	All domains of the tenant	Get-AADIntTenantDomains -Domain <domain>
login.microsoftonline.com/GetUserRealm.srf?login=<UserName>	Login information of the tenant, including tenant Name and domain authentication type	Get-AADIntLoginInformation -UserName <UserName>
login.microsoftonline.com/common/GetCredentialType	Login information, including Desktop SSO information	Get-AADIntLoginInformation -UserName <UserName>

Finding the values – Solution Publisher prefix

1. Default solution publisher ID patterns

a. Theoretically according to docs: the prefix must be 2 to 8 characters long, can only consist of alpha-numerics, must start with a letter, and cannot start with 'mscrm'

b. Brute forcing the above search-space is impractical here

c. Exploration shows that default solution publisher id often exists → as when we targeted the default env, this is a better scenario to try to discovery than the general search-space

Here's how it looks like all together in the URL:

https://copilotstudio.microsoft.com/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3/bots/cr6e4_copilotSqlErrorTesting/canvas

Finding the values – Solution Publisher prefix

1. Default solution publisher ID patterns

a. Theoretically according to docs: the prefix must be 2 to 8 characters long, can only consist of alpha-numerics, must start with a letter, and cannot start with 'mscr...'

b. Brute forcing the above search-space is impractical here

c. Exploration shows that default solution publisher id often exists, e.g. when we targeted

a better

3. Minimizing the wordlist for the most common ids seen in exploration

a. `cr[numeric][alphanumeric][alphanumeric]` instead of

`cr[alphanumeric][alphanumeric][alphanumeric]`

b. `cra[alphanumeric][alphanumeric]`

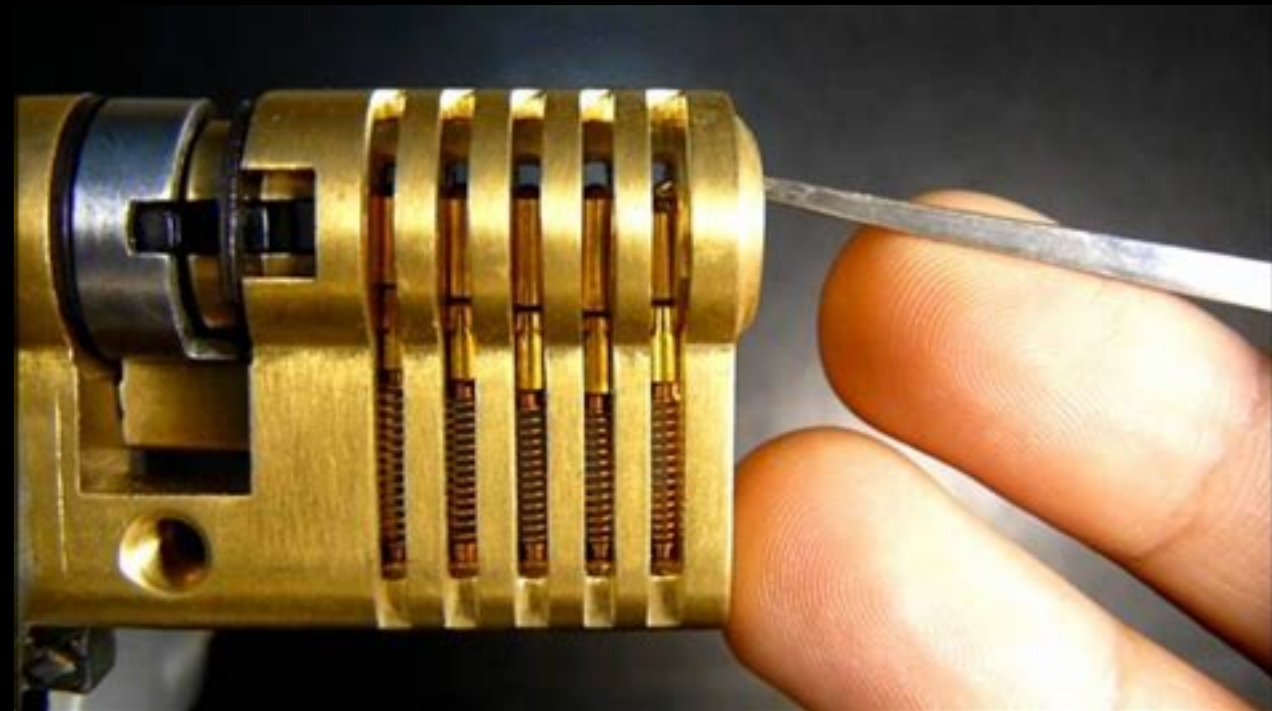
c. `cre[alphanumeric][alphanumeric]`

d. `crf[alphanumeric][alphanumeric]`



Finding the values – Solution Publisher prefix

```
copilot1  
1  
2  
3  
4  
5  
Test10  
a  
aiAssistant  
aiBot  
aiDemo  
alex  
assistant  
azureCopilot  
basicBot  
bot
```



Finding the values – demo website name

Here's how it looks like all together in the URL:

https://copilotstudio.microsoft.com/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3/bots/cr6e4_copilotSqlErrorTesting/canvas

Here's how it looks like all together in the URL:

https://copilotstudio.microsoft.com/environments/Default-32f814a9-68c8-4ca1-93aa-5594523476b3/bots/cr6e4_copilotSqlErrorTesting/canvas

ai
gen
business
digital
contoso
customer
service
atlassian
database

copyOfTestBot
corp
corpTechBuddy
customerServiceBot
customerSupport
data
dataAnalysis
dataAnalytics

approval
virtual



Finding the values – Env/Tenant

```
(mven) [root@capital-studio-demo-website_recon_tool] amass enum -d environment.api.powerplatform.com
0537e6646b364c469d74cc0080f040.b1.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.eu-il103.gateway.prod.island.powerapps.com (FQDN)
defaultb6c9c119392a4fe0a1a0ef4d9605e.2d.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il109.gateway.prod.island.powerapps.com (FQDN)
default8193a455d4e6483eb99e7969393bcf.82.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.eu-il101.gateway.prod.island.powerapps.com (FQDN)
4a69cad697cbec0197d73c87897d0f.ae.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.uk-il102.gateway.prod.island.powerapps.com (FQDN)
8560ab68f13c41c98b179d577ea8be.df.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.jp-il101.gateway.prod.island.powerapps.com (FQDN)
96a721aaa57043c2b5ca5c4f6a13f4.16.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il104.gateway.prod.island.powerapps.com (FQDN)
95ba83174854ea5dad007cf9363d1d.a7.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.uk-il101.gateway.prod.island.powerapps.com (FQDN)
defaultef61560652ba45899e06a2c35be0c3.b9.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.uk-il101.gateway.prod.island.powerapps.com (FQDN)
3438f9bdac10e8d9829833a8a0aa60.4e.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.eu-il104.gateway.prod.island.powerapps.com (FQDN)
778f60f4dec4e79f9644fd5ca339a4.ad.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.uk-il102.gateway.prod.island.powerapps.com (FQDN)
defaultba772a7ce49a4591882313d9f146f8.a6.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.eu-il107.gateway.prod.island.powerapps.com (FQDN)
e44a17da5b8d4609bae766cab7d320.f1.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il106.gateway.prod.island.powerapps.com (FQDN)
0d3baac172a9e3edbd230335a090d.a2.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.uk-il102.gateway.prod.island.powerapps.com (FQDN)
f5022abb55964903ad052e68d88dd8.d3.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il102.gateway.prod.island.powerapps.com (FQDN)
14769523eb2344a7909ea762e1ff95.8a.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.as-il101.gateway.prod.island.powerapps.com (FQDN)
default7cd0f69d459b447a9679bd3a8422ee.f3.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.uk-il101.gateway.prod.island.powerapps.com (FQDN)
363dda33121fec69a566d6978c6e83.a5.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.uk-il102.gateway.prod.island.powerapps.com (FQDN)
01eeb0150fc4e3d893adf1463ab01f.4e.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.eu-il103.gateway.prod.island.powerapps.com (FQDN)
ba284fe6ad92ec5b8797f281c97e2f.00.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il101.gateway.prod.island.powerapps.com (FQDN)
338ef2fbf0f14609a3c19b0a115cfe.08.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.uk-il101.gateway.prod.island.powerapps.com (FQDN)
default4f29bd2bff6d41f98d162fe6e36953.8f.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il104.gateway.prod.island.powerapps.com (FQDN)
96c04ba89dd54d9d8305f7b7dc587d.e7.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il106.gateway.prod.island.powerapps.com (FQDN)
44354e39d4dee251828ed198512ec3.4f.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.eu-il104.gateway.prod.island.powerapps.com (FQDN)
defaulteb17192829294f2ca759b5cc2ac72a.fb.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il104.gateway.prod.island.powerapps.com (FQDN)
fb0ab67dde374e548e48b4b3b0dd06.75.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.uk-il101.gateway.prod.island.powerapps.com (FQDN)
e96520a5bd0ee4cb94d5cbeee3085.18.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il108.gateway.prod.island.powerapps.com (FQDN)
a876e0b1093fe34ea9d0eae116fc52.12.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il107.gateway.prod.island.powerapps.com (FQDN)
d96b7864797d4d4c9f432cd36bb98f.ce.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il102.gateway.prod.island.powerapps.com (FQDN)
4d7fe02732c2e560801a7c79a513d8.9a.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.as-il101.gateway.prod.island.powerapps.com (FQDN)
defaulta96c7675e55f47638a8ad913d6113.6f.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il108.gateway.prod.island.powerapps.com (FQDN)
defaultd6379333d94849d8917861ae31c54c.69.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il106.gateway.prod.island.powerapps.com (FQDN)
```

Finding the values – Env/Tenant

```
(myenv) → copilot_studio_demo_website_recon_tool amass enum -d environment.api.powerplatform.com
0537e6646b364c469d74cc0080f040.b1.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.eu-il103.gateway.prod.island.powerapps.com (FQDN)
default+b6c9c119392a4fe0a1a0ef4d9605e9.2d.environment.api.powerplatform.com (FQDN) --> cname_record --> ppapigw.us-il109.gateway.prod.island.powerapps.com (FQDN)
```

Enter **tenant id**, **domain name**, user **email**, or user **object id**:

a96c7675-e55f-4763-8a8a-d913d611376f

Get Information



Property	Value
Default domain	hazeldenbettyford.onmicrosoft.com
Tenant name	hazeldenbettyford.onmicrosoft.com
Tenant brand	Hazelden Betty Ford Foundation
Tenant id	a96c7675-e55f-4763-8a8a-d913d611376f
Tenant region	NA
Seamless single sign-on (SSSO)	enabled
Uses Azure AD Connect cloud sync	N/A
Certificate-based authentication (CBA)	N/A
Verified domains	24

```
eway.prod.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
eway.prod.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
eway.prod.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
eway.prod.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
eway.prod.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
od.island.powerapps.com (FQDN)
eway.prod.island.powerapps.com (FQDN)
eway.prod.island.powerapps.com (FQDN)
```



Demo

Functionalities Recap

- Domain and Tenant ID Scanning
- Environment & Tenant ID Enumeration
- Solution Prefix Reconnaissance:
- Bot Name Enumeration
- Basic bot interaction



What's next

- Spray Scanning
- Advanced bot interaction



Copilot Hunter (powerpwn)

