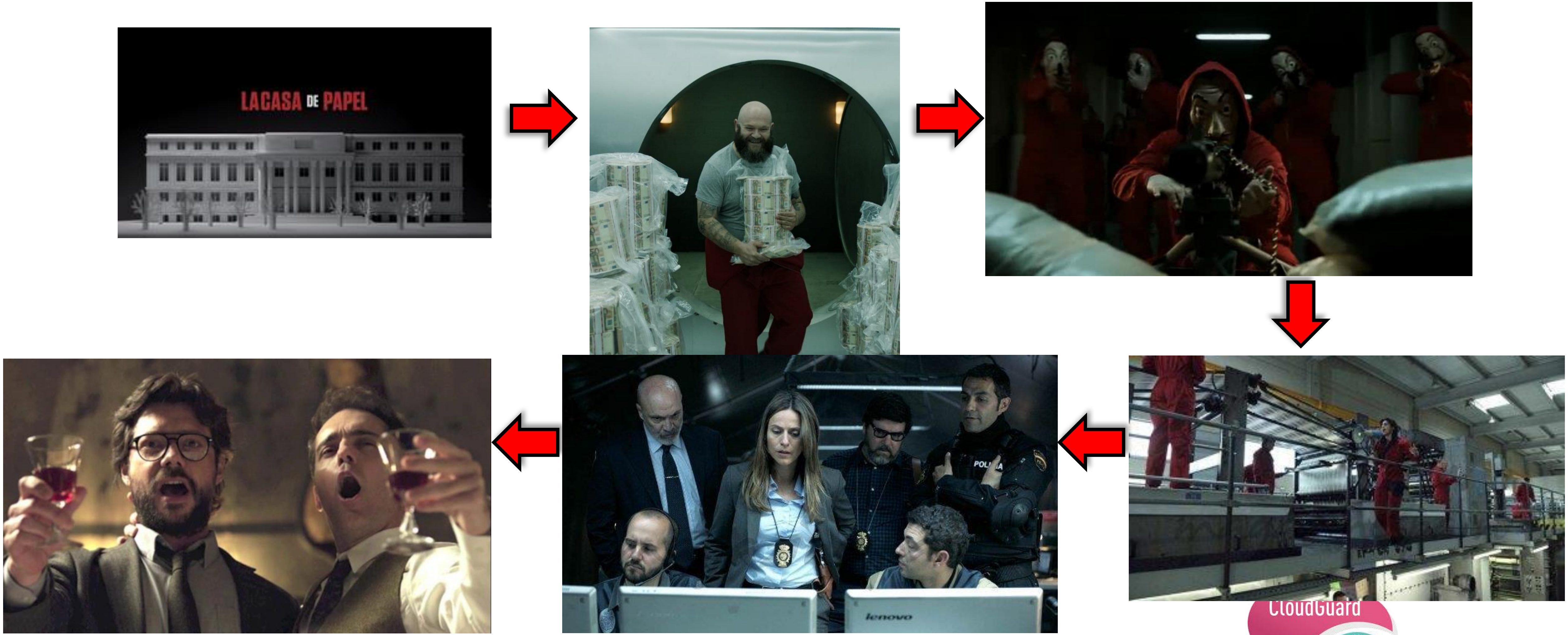
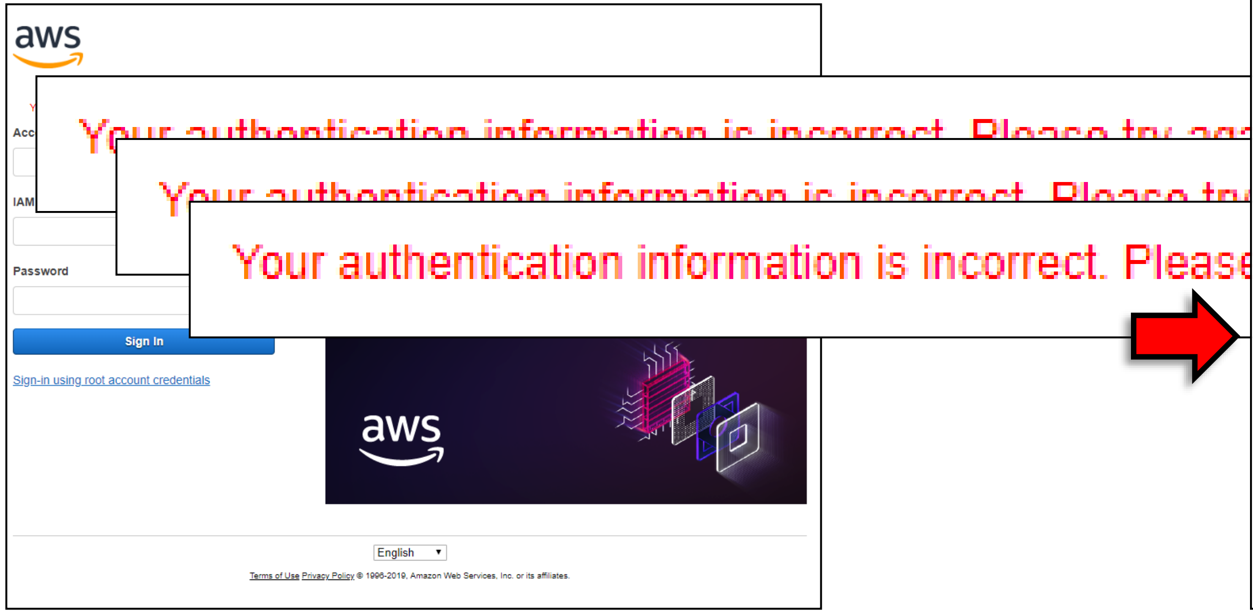
Ghost Robbers In The Cloud Finding Crypto Miners

Shira Shamban
Dome9 Security (acquired by CheckPoint)

Money Heist – Let’s Review…



Finders Keepers, Losers Weepers



aws

Acc

IAM

Password

Your authentication information is incorrect. Please try aga

Your authentication information is incorrect. Please try

Your authentication information is incorrect. Please

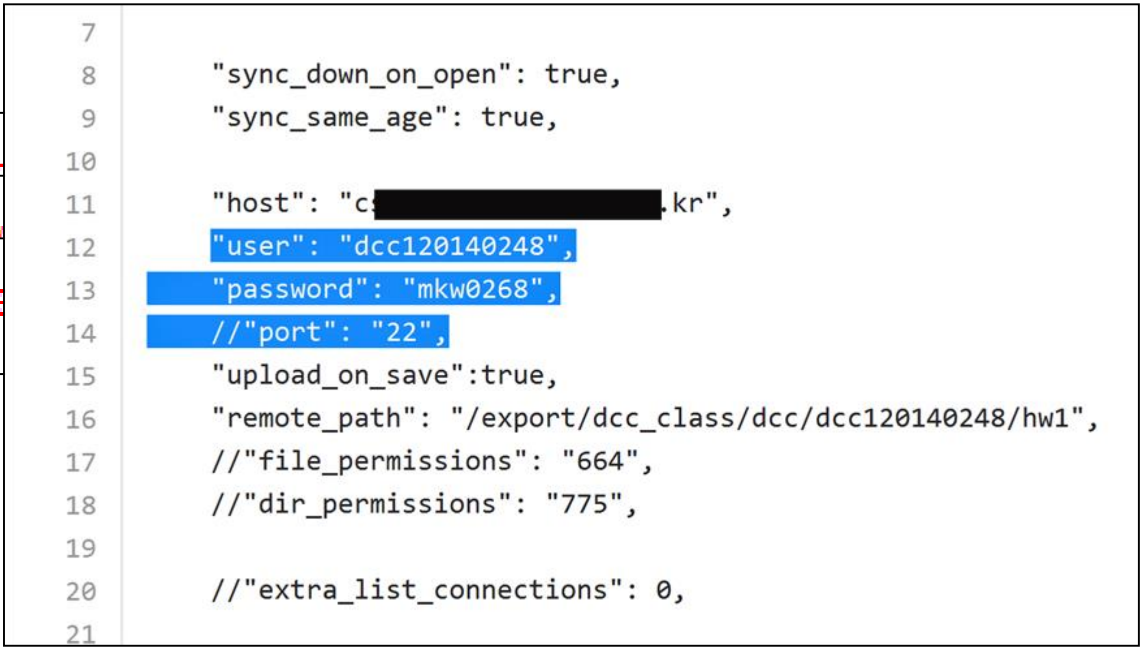
Sign In

Sign-in using root account credentials

aws

English

Terms of Use Privacy Policy © 1996-2019, Amazon Web Services, Inc. or its affiliates.



```
    "sync_down_on_open": true,
    "sync_same_age": true,

    "host": "c[redacted].kr",
    "user": "dcc120140248",
    "password": "mkw0268",
    //"port": "22",
    "upload_on_save":true,
    "remote_path": "/export/dcc_class/dcc/dcc120140248/hw1",
    //"file_permissions": "664",
    //"dir_permissions": "775",

    //"extra_list_connections": 0,
```

The 21st Century Gold Rush

“Overtaking Ransomware, Cryptominers affected over **42% of organizations worldwide**, compared to 20.5% at the end of 2017”

CheckPoint

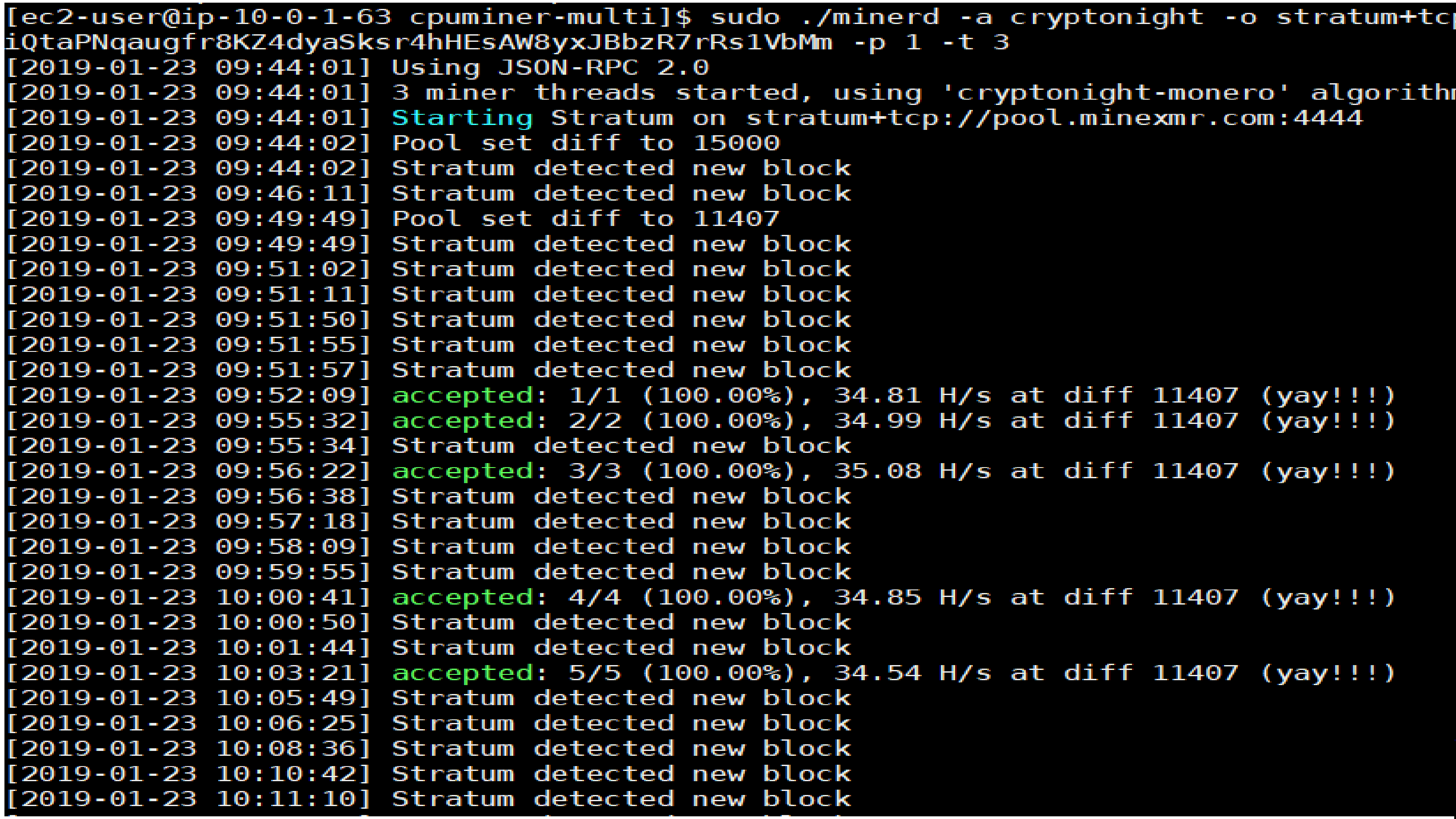
CheckPoint

“During the first six months of 2018, Cryptomining attacks are estimated to have ‘earned’ their users more than **$2.5 billion**”

It WILL Be Your Fault

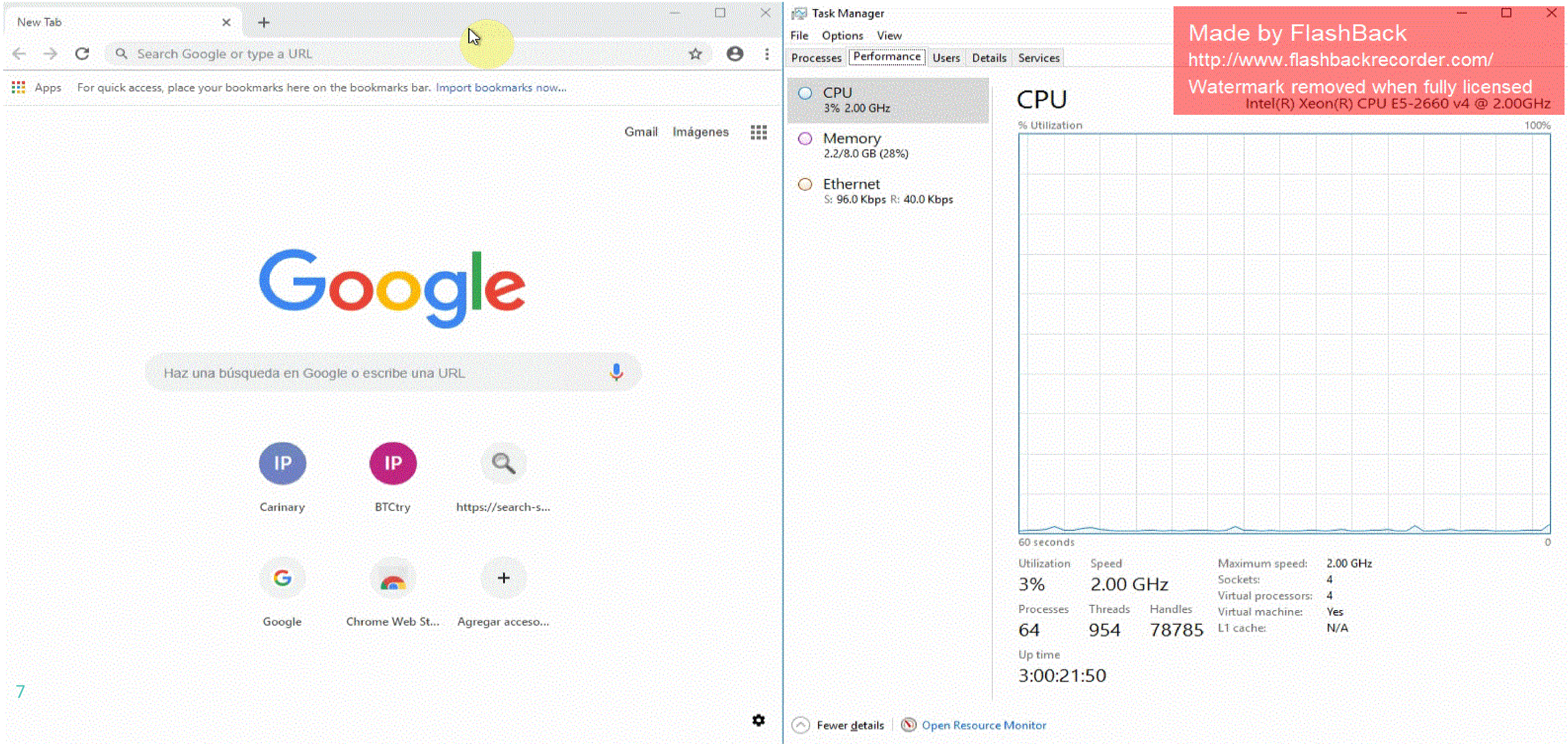
“Through 2022, at least 95% of cloud security failures will be the customer’s fault” Gartner

MMM



```
[ec2-user@ip-10-0-1-63 cpuminer-multi]$ sudo ./minerd -a cryptonight -o stratum+tcp://pool.minexmr.com:4444 -
iQtaPNqaugfr8KZ4dyaSksr4hHEsAW8yxJBbzR7rRs1VbMm -p 1 -t 3
[2019-01-23 09:44:01] Using JSON-RPC 2.0
[2019-01-23 09:44:01] 3 miner threads started, using 'cryptonight-monero' algorithm.
[2019-01-23 09:44:01] Starting Stratum on stratum+tcp://pool.minexmr.com:4444
[2019-01-23 09:44:02] Pool set diff to 15000
[2019-01-23 09:44:02] Stratum detected new block
[2019-01-23 09:46:11] Stratum detected new block
[2019-01-23 09:49:49] Pool set diff to 11407
[2019-01-23 09:49:49] Stratum detected new block
[2019-01-23 09:51:02] Stratum detected new block
[2019-01-23 09:51:11] Stratum detected new block
[2019-01-23 09:51:50] Stratum detected new block
[2019-01-23 09:51:55] Stratum detected new block
[2019-01-23 09:51:57] Stratum detected new block
[2019-01-23 09:52:09] accepted: 1/1 (100.00%), 34.81 H/s at diff 11407 (yay!!!)
[2019-01-23 09:55:32] accepted: 2/2 (100.00%), 34.99 H/s at diff 11407 (yay!!!)
[2019-01-23 09:55:34] Stratum detected new block
[2019-01-23 09:56:22] accepted: 3/3 (100.00%), 35.08 H/s at diff 11407 (yay!!!)
[2019-01-23 09:56:38] Stratum detected new block
[2019-01-23 09:57:18] Stratum detected new block
[2019-01-23 09:58:09] Stratum detected new block
[2019-01-23 09:59:55] Stratum detected new block
[2019-01-23 10:00:41] accepted: 4/4 (100.00%), 34.85 H/s at diff 11407 (yay!!!)
[2019-01-23 10:00:50] Stratum detected new block
[2019-01-23 10:01:44] Stratum detected new block
[2019-01-23 10:03:21] accepted: 5/5 (100.00%), 34.54 H/s at diff 11407 (yay!!!)
[2019-01-23 10:05:49] Stratum detected new block
[2019-01-23 10:06:25] Stratum detected new block
[2019-01-23 10:08:36] Stratum detected new block
[2019-01-23 10:10:42] Stratum detected new block
[2019-01-23 10:11:10] Stratum detected new block
```

How?



CPU
3% 2.00 GHz

Memory
2.2/8.0 GB (28%)

Ethernet
S: 96.0 Kbps R: 40.0 Kbps

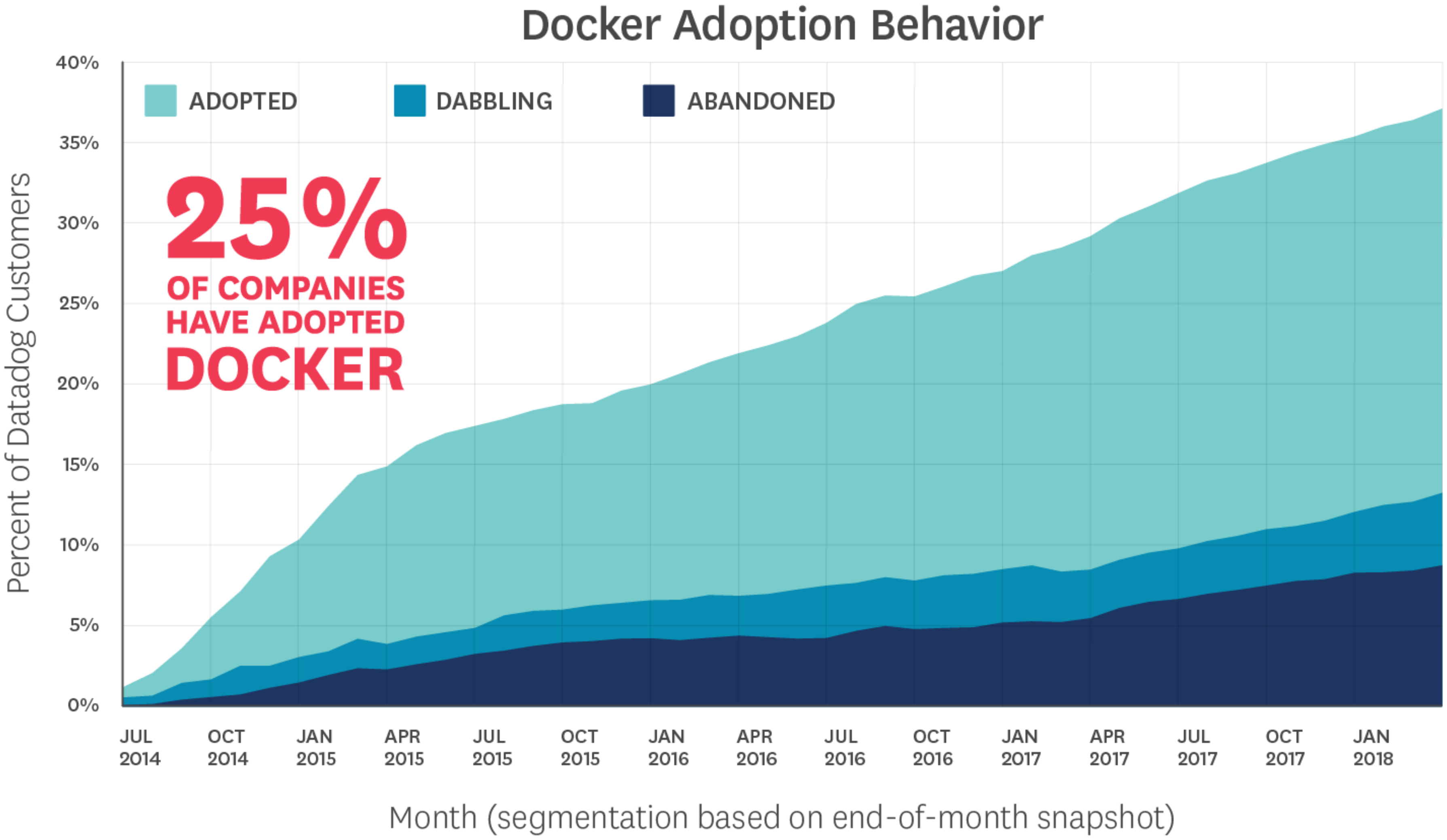
CPU
Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz

Utilization 3%
Speed 2.00 GHz
Processes 64
Threads 954
Handles 78785
Up time 3:00:21:50

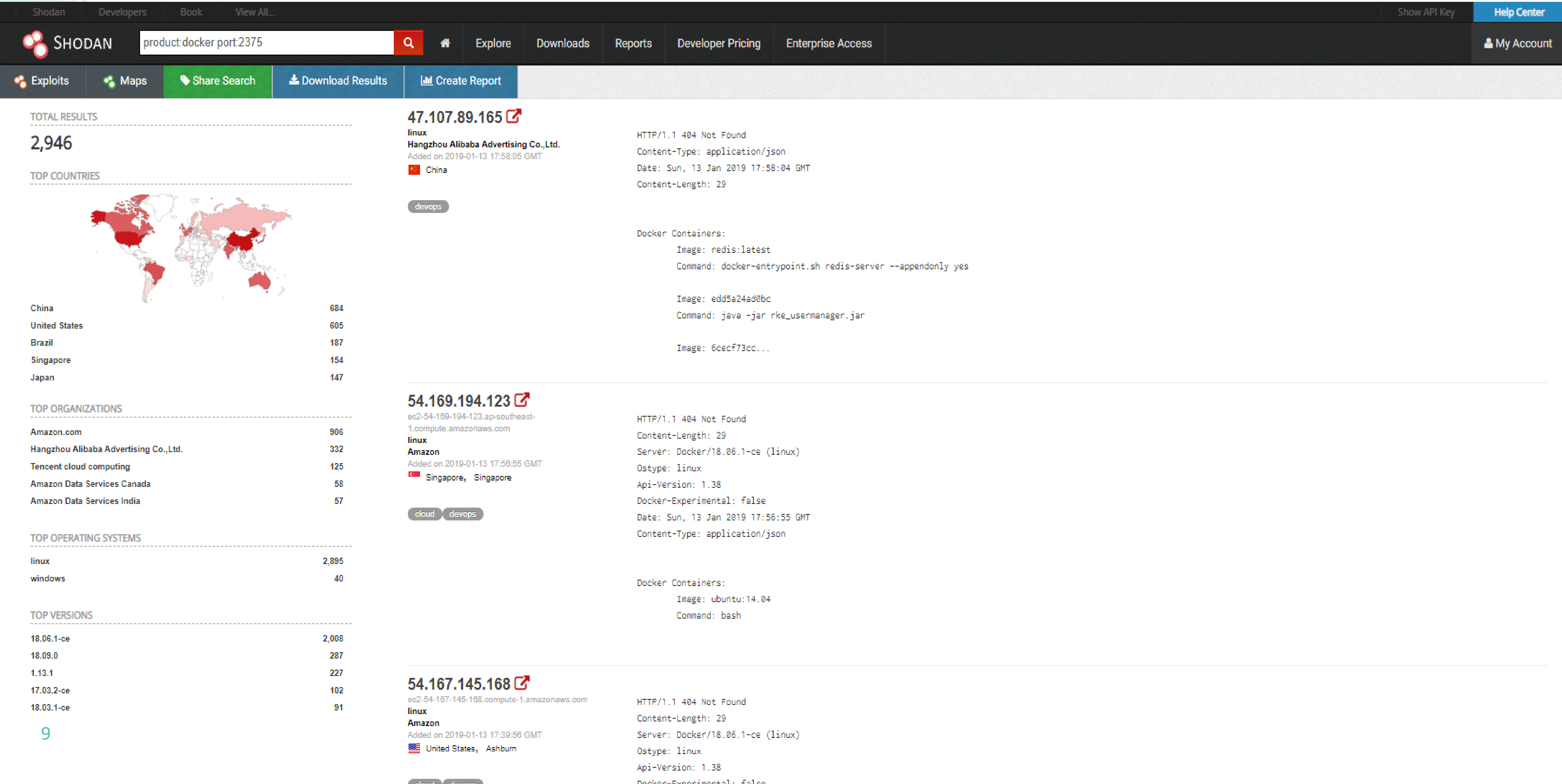
Maximum speed: 2.00 GHz
Sockets: 4
Virtual processors: 4
Virtual machine: Yes
L1 cache: N/A

Docker

Containers!



Source: Datadog



TOTAL RESULTS

2,946

TOP COUNTRIES

China	684
United States	605
Brazil	187
Singapore	154
Japan	147

TOP ORGANIZATIONS

Amazon.com	906
Hangzhou Alibaba Advertising Co.,Ltd.	332
Tencent cloud computing	125
Amazon Data Services Canada	58
Amazon Data Services India	57

TOP OPERATING SYSTEMS

linux	2,895
windows	40

TOP VERSIONS

18.06.1-ce	2,008
18.09.0	287
1.13.1	227
17.03.2-ce	102
18.03.1-ce	91

47.107.89.165

linux

Hangzhou Alibaba Advertising Co.,Ltd.

Added on 2019-01-13 17:58:05 GMT

China

devops

```
HTTP/1.1 404 Not Found
Content-Type: application/json
Date: Sun, 13 Jan 2019 17:58:04 GMT
Content-Length: 29


Docker Containers:
        Image: redis:latest
        Command: docker-entrypoint.sh redis-server --appendonly yes

        Image: edd5a24ad0bc
        Command: java -jar rke_usermanager.jar

        Image: 6cecf73cc...
```

54.169.194.123

ec2-54-169-194-123.ap-southeast-1.compute.amazonaws.com

linux

Amazon

Added on 2019-01-13 17:56:55 GMT

Singapore, Singapore

cloud devops

```
HTTP/1.1 404 Not Found
Content-Length: 29
Server: Docker/18.06.1-ce (linux)
Ostype: linux
Api-Version: 1.38
Docker-Experimental: false
Date: Sun, 13 Jan 2019 17:56:55 GMT
Content-Type: application/json


Docker Containers:
        Image: ubuntu:14.04
        Command: bash
```

54.167.145.168

ec2-54-167-145-168.compute-1.amazonaws.com

linux

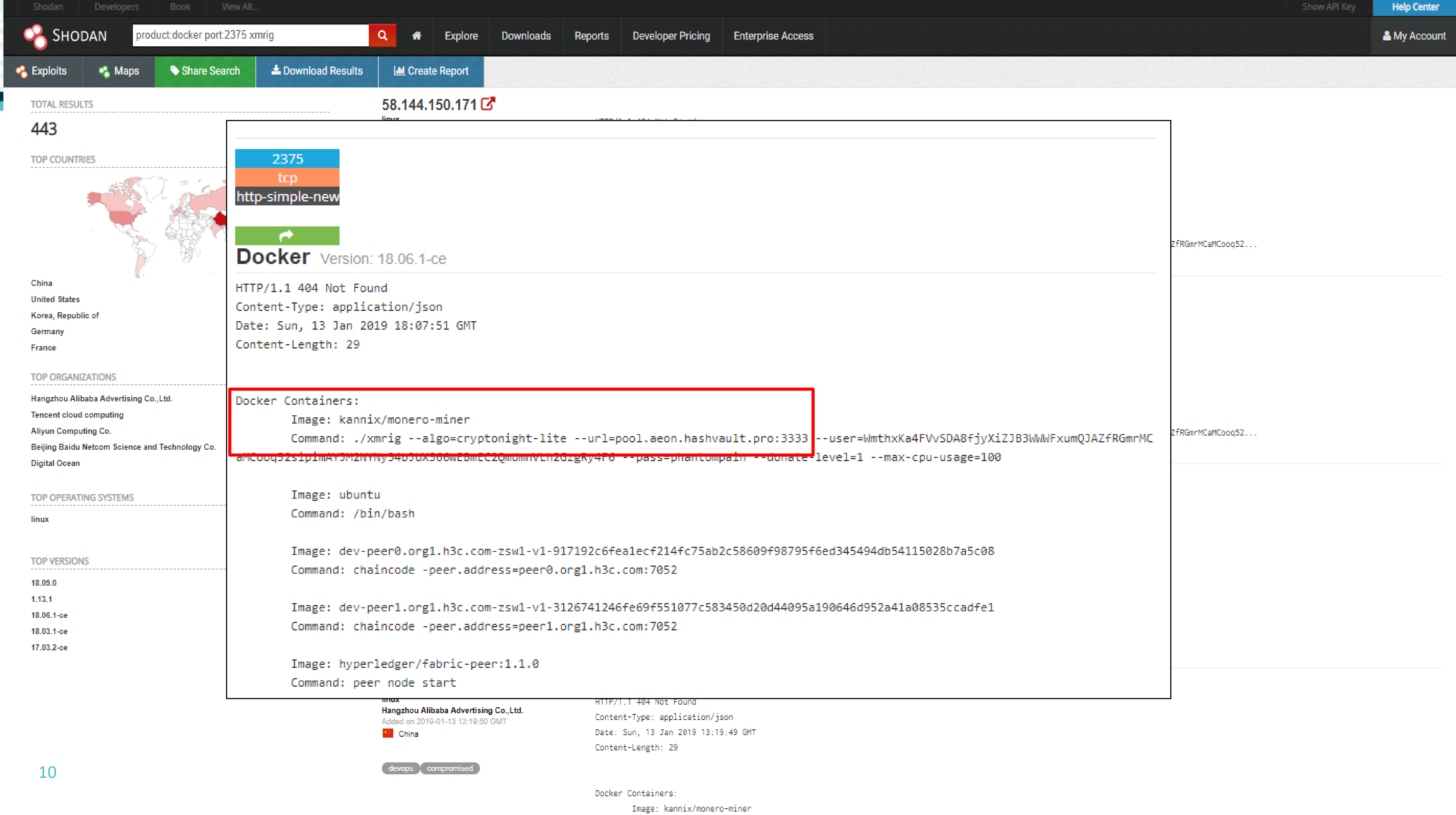
Amazon

Added on 2019-01-13 17:39:56 GMT

United States, Ashburn

cloud devops

```
HTTP/1.1 404 Not Found
Content-Length: 29
Server: Docker/18.06.1-ce (linux)
Ostype: linux
Api-Version: 1.38
Docker-Experimental: false
```



TOTAL RESULTS

443

TOP COUNTRIES

China
United States
Korea, Republic of
Germany
France

TOP ORGANIZATIONS

Hangzhou Alibaba Advertising Co.,Ltd.
Tencent cloud computing
Aliyun Computing Co.
Beijing Baidu Netcom Science and Technology Co.
Digital Ocean

TOP OPERATING SYSTEMS

linux

TOP VERSIONS

18.09.0
1.13.1
18.06.1-ce
18.03.1-ce
17.03.2-ce

58.144.150.171

linux

Docker Version: 18.06.1-ce

```
HTTP/1.1 404 Not Found
Content-Type: application/json
Date: Sun, 13 Jan 2019 18:07:51 GMT
Content-Length: 29


Docker Containers:
        Image: kannix/monero-miner
        Command: ./xmrig --algo=cryptonight-lite --url=pool.aeon.hashvault.pro:3333 --user=WmthxKa4FVvSDA8fjyXiZJB3WWWFxumQJAZfRGmrMC
aMCooq52sipimAYJM2NYNy34bJUX366WEBmEC2QmUmnVLh2GzgRy4P6 --pass=phantompain --donate-level=1 --max-cpu-usage=100

        Image: ubuntu
        Command: /bin/bash

        Image: dev-peer0.org1.h3c.com-zsw1-v1-917192c6fea1ecf214fc75ab2c58609f98795f6ed345494db54115028b7a5c08
        Command: chaincode -peer.address=peer0.org1.h3c.com:7052

        Image: dev-peer1.org1.h3c.com-zsw1-v1-3126741246fe69f551077c583450d20d44095a190646d952a41a08535ccadfe1
        Command: chaincode -peer.address=peer1.org1.h3c.com:7052

        Image: hyperledger/fabric-peer:1.1.0
        Command: peer node start
```

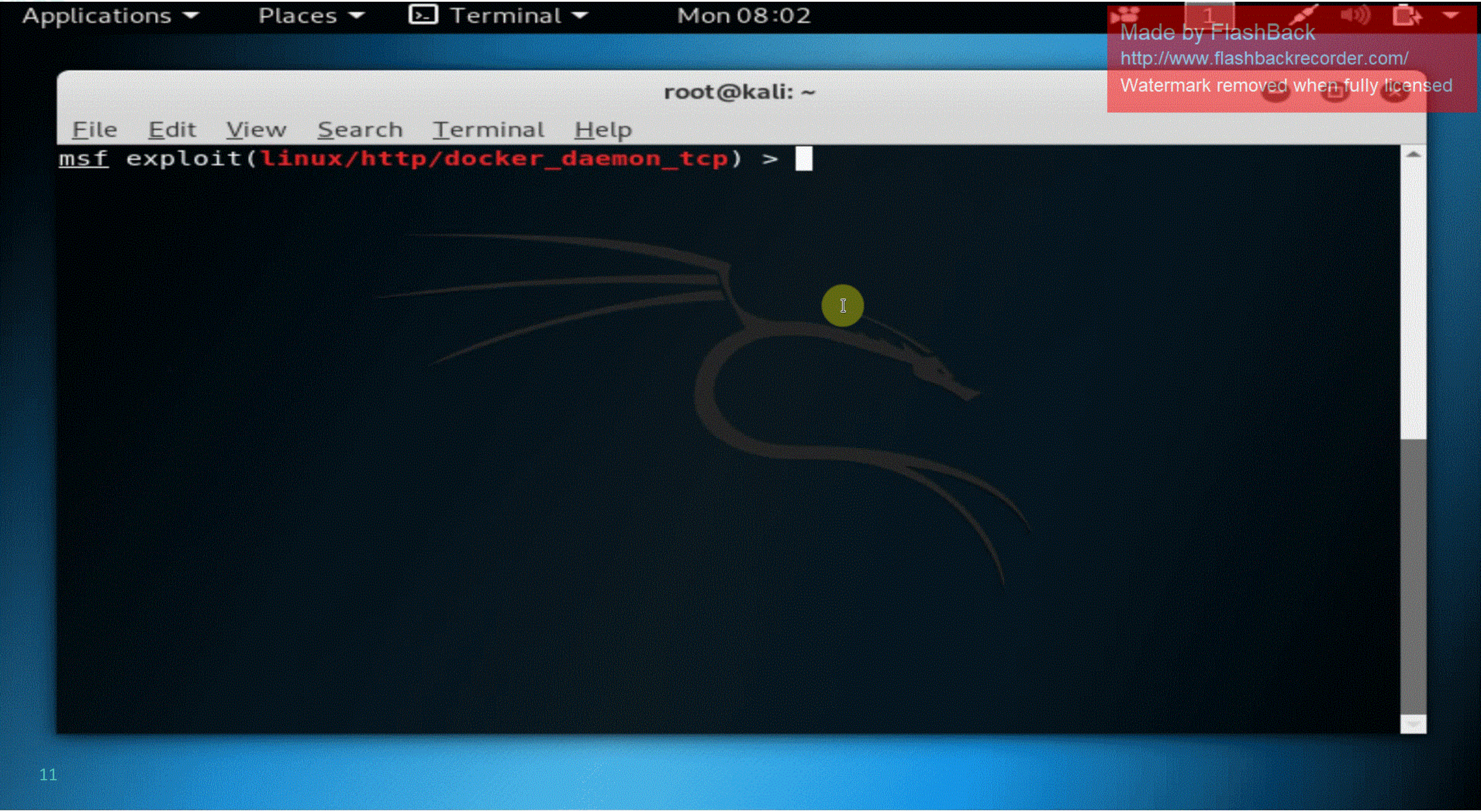
ZfRGmrMCaMCooq52...

ZfRGmrMCaMCooq52...

linux
Hangzhou Alibaba Advertising Co.,Ltd.
Added on 2019-01-13 13:19:50 GMT
China

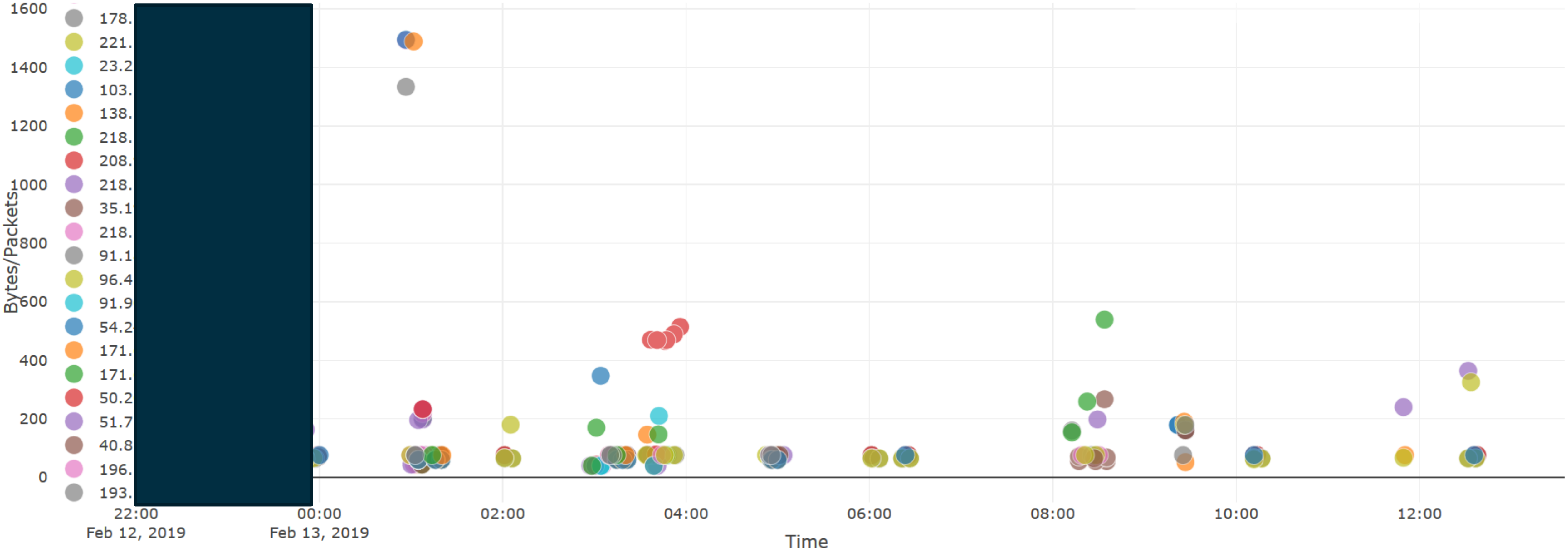
```
HTTP/1.1 404 Not Found
Content-Type: application/json
Date: Sun, 13 Jan 2019 13:19:49 GMT
Content-Length: 29


Docker Containers:
        Image: kannix/monero-miner
```



```
msf exploit(linux/http/docker_daemon_tcp) > 
```

MVD – minimal viable detection

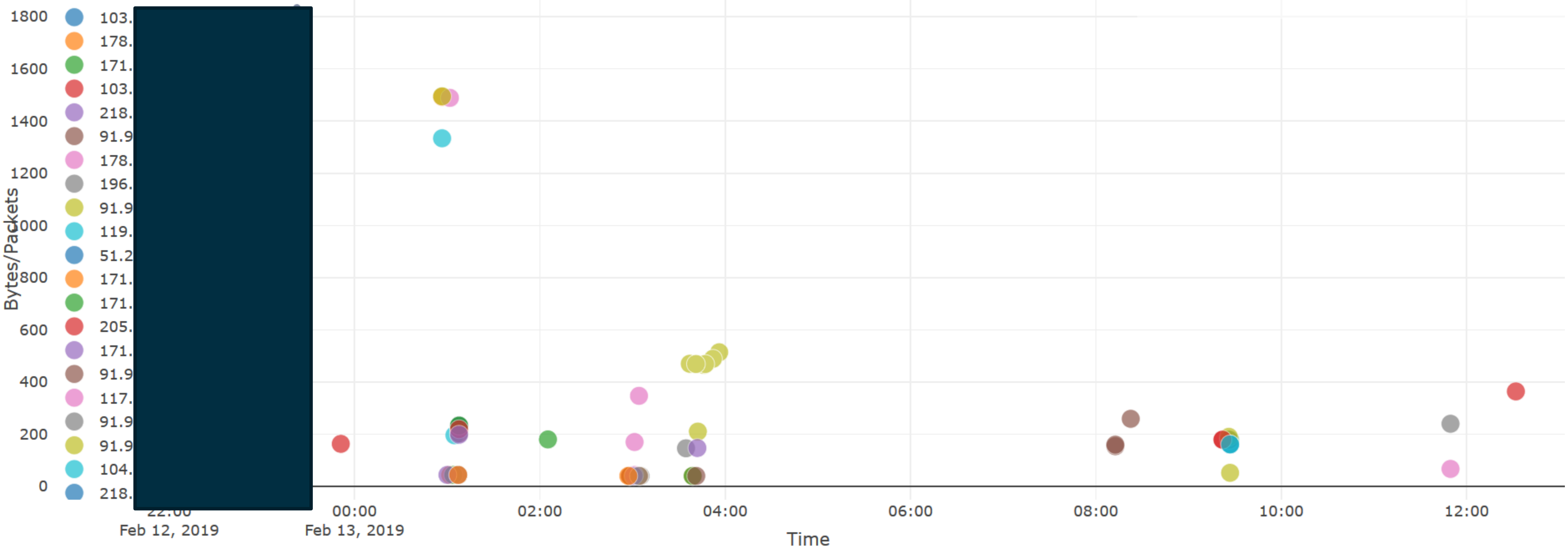

[redacted]

CHECK POINT CloudGuard

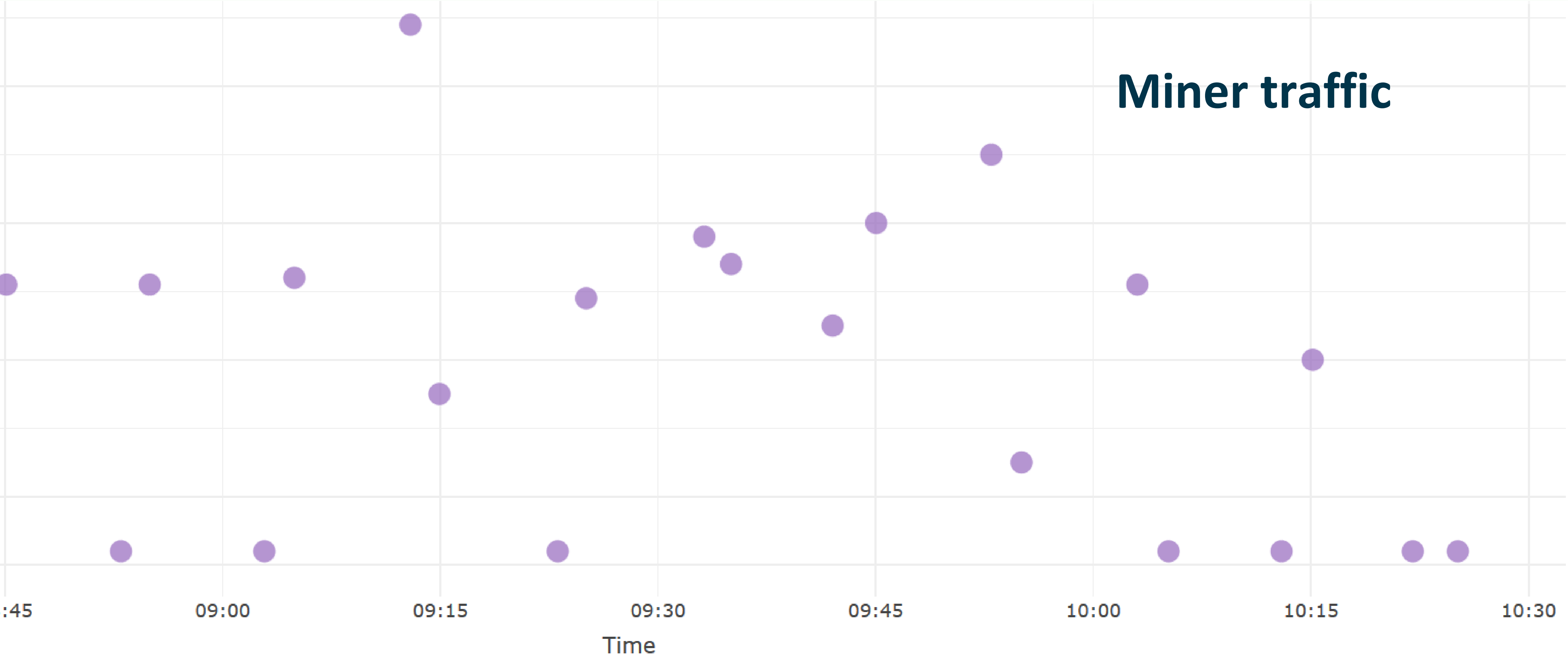
Dome9 SECURITY

MVD – minimal viable detection

Production environment –



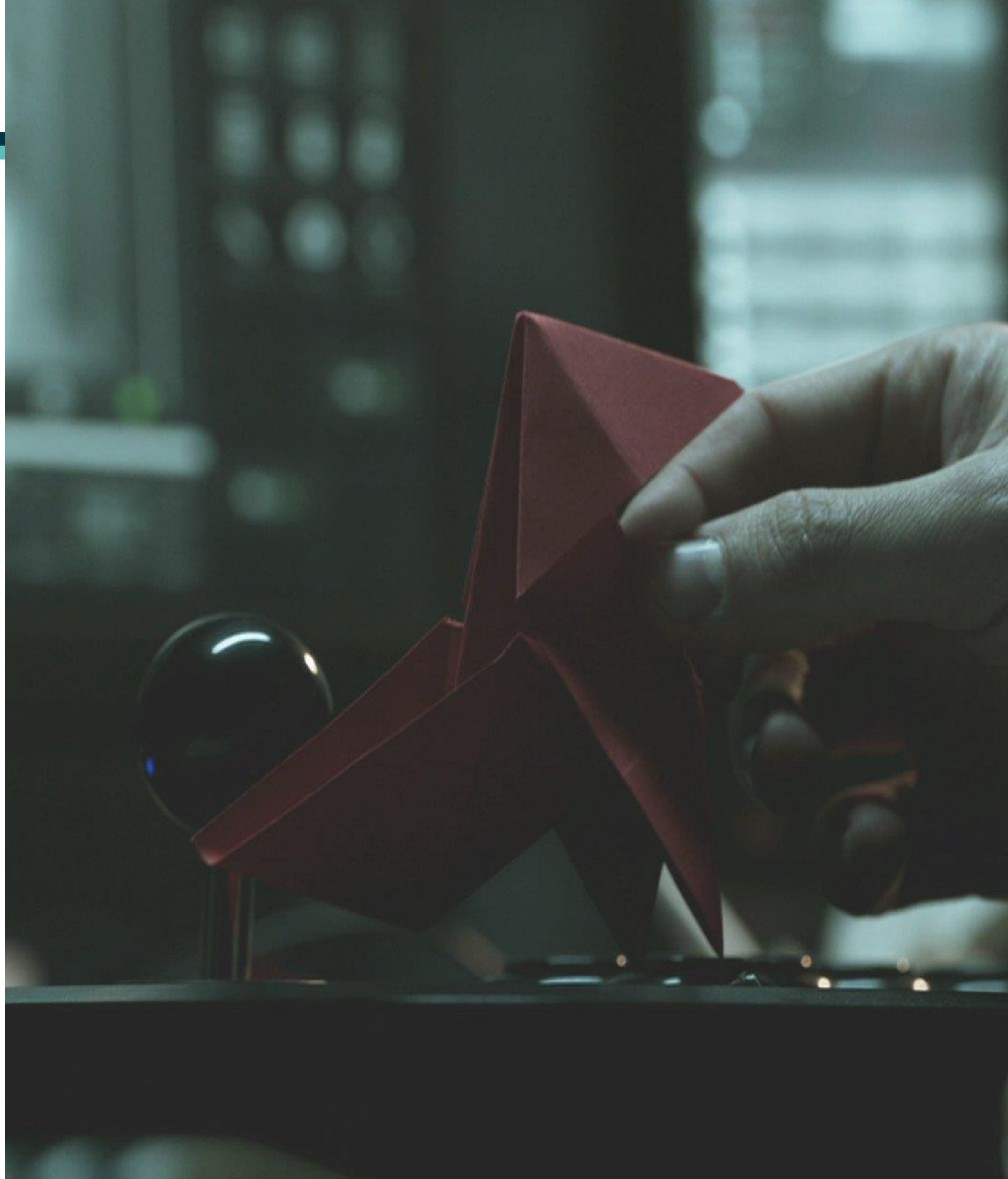
MVD – minimal viable detection



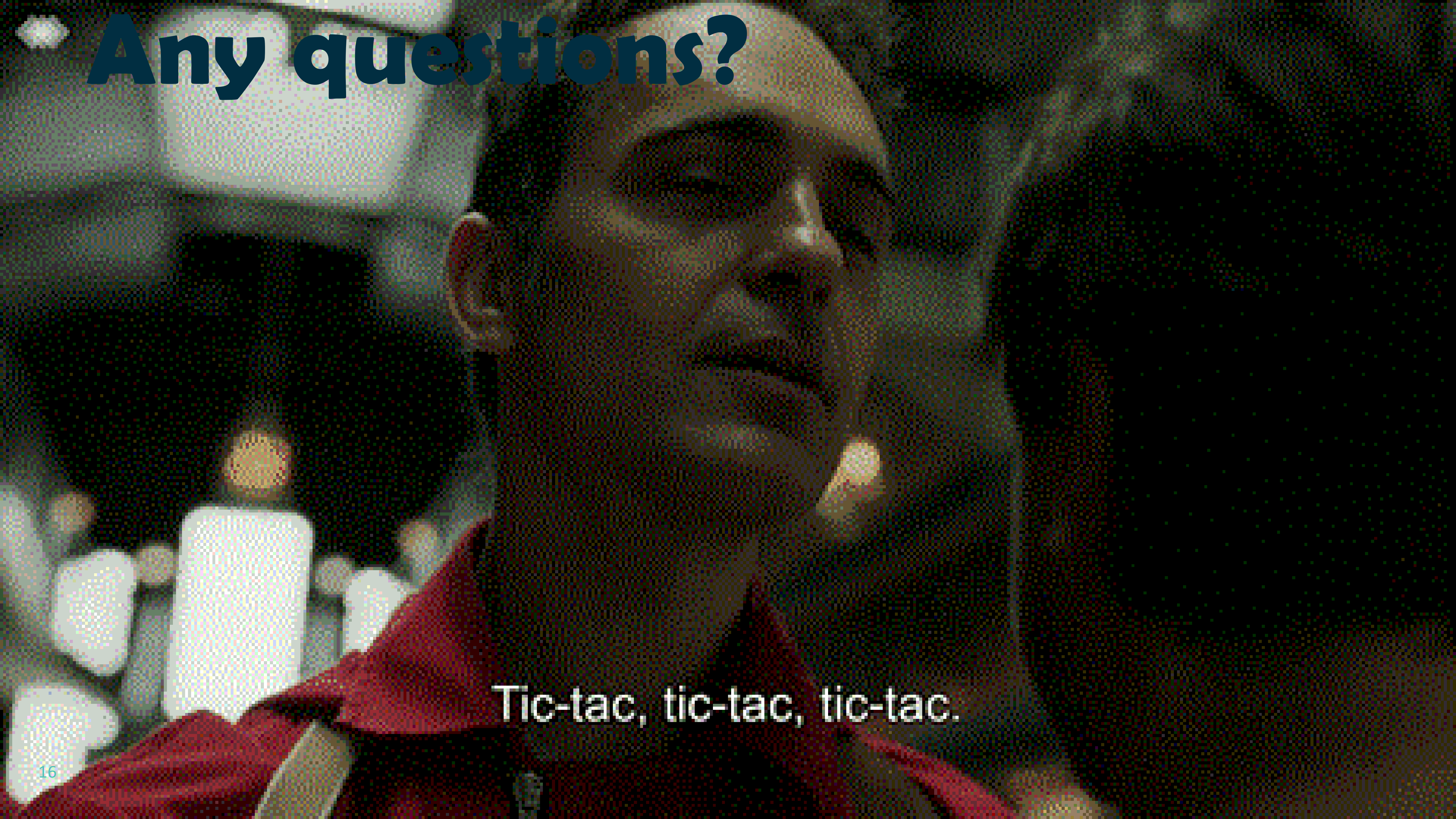
Miner traffic

Tell-Tale Signs…

- Scan the code
- Monitor CPU
- Monitor the cost
- Ports (Docker, miner)
- First-time asset
- First-time connections
- Mind the socket



Any questions?



Thank you!

Shira Shamban

shirasha@checkpoint.com

@ShambanIT

CHECK POINT CloudGuard Dome9 SECURITY