

A dark, stormy sea with a large sailing ship in the background and a skull in the foreground. The sky is filled with dark, heavy clouds and several birds are flying. The overall mood is ominous and mysterious.

# A Hackers Guide To Kubernetes and the cloud

# ABOUT ME

- 18 Years in IT/Information Security
- Managing Consultant at NCC Group PLC
- Contributor at Security Stack Exchange
- Contributing author to the CIS Docker and Kubernetes Standards





# TOPICS

- Threat Models
- Attack Surface
- External Attackers
- Compromised Containers
- Top 10 Things to do



# Threat Model



















# Attack Surface

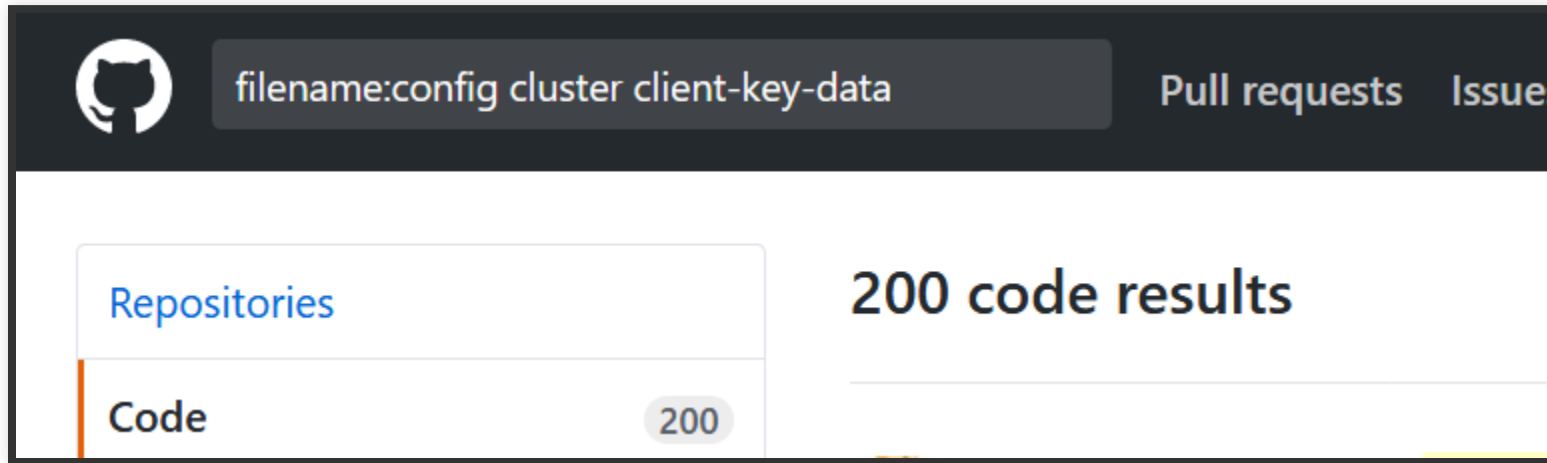






# CLOUDY CLUSTERS

# OTHER MEANS OF ACQUIRING ACCESS - GITHUB!



# External Attackers





# EXTERNAL NETWORK VISIBILITY

- 2379/tcp open etcd
- 4194/tcp open cAdvisor
- (6 | 8)443/tcp open API Server
- 8080/tcp open Insecure API Server
- 10250/tcp open kubelet
- 10255/tcp open kubelet (Read Only)
- [various] open [Network plugins]

# ATTACKING THE API SERVER

ATTACKING  
ETCD

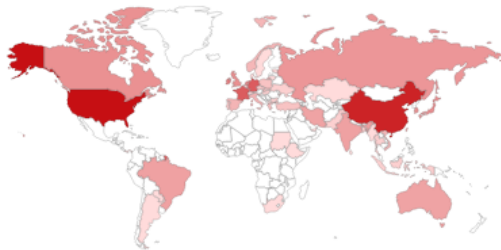


SHODAN &  
FRIENDS

### TOTAL RESULTS

1,874

### TOP COUNTRIES



United States	680
China	471
France	137
Germany	136
Ireland	57

### TOP ORGANIZATIONS

Amazon.com	286
Hangzhou Alibaba Advertising Co.,Ltd.	160
Digital Ocean	154
Psychz Networks	62
OVH SAS	31

### TOP OPERATING SYSTEMS

Linux 3.x	13
-----------	----

### TOP PRODUCTS

etcd	1,830
------	-------

## 104.254.244.82

**1&1 Internet AG**

Added on 2018-02-23 21:35:54 GMT

United States, Wayne

[Details](#)

etcd

Name: kube-etcd-0000

Version: 3.1.0

Uptime: 7441h27m17.554682808s

Peers: http://104.254.244.82:23

## 54.194.20.187

ec2-54-194-20-187.eu-west-1.compute.amazonaws.com

**Amazon.com**

Added on 2018-02-23 21:25:44 GMT

Ireland, Dublin

[Details](#)

cloud

etcd

Name: 8e19c8ff13c34a82bbf0c5c5e

Version: 2.3.1

Uptime: 5246h57m20.810080435s

Peers: http://10.0.30.75:2380

## 13.84.129.237

**Microsoft Azure**

Added on 2018-02-23 21:24:48 GMT

United States, San Antonio

[Details](#)

cloud

etcd

Name: etcd02

Version: 2.2.5

Uptime: 4h8m34.56225026s

Peers: http://10.3.0.8:2380

## 119.23.79.186

**Hangzhou Alibaba Advertising Co.,Ltd.**

Added on 2018-02-23 21:20:37 GMT

China, Hangzhou

[Details](#)

etcd

Name: x1

Version: 3.2.0+git

Uptime: 583h4m22.51149815s

Peers: http://0.0.0.0:2380

# ATTACKING THE KUBELET





# Malicious Container

# INCREASED ATTACK SURFACE

- Container Filesystem Access
- "Internal" Network Position
- Kernel Attacks

ATTACKING  
SERVICE  
ACCOUNT  
TOKENS



LEVERAGING  
ACCESS IN THE  
CLOUD

THE  
IMPORTANCE OF  
SECURE  
DEFAULTS!

# Key Security Considerations





# 1. INSECURE PORT

```
--insecure-port=0  
--insecure-bind-address - Not Set
```

# 2. CONTROL ACCESS TO THE KUBELET

```
--anonymous-auth=false  
--authorization-mode - Not set to "AlwaysAllow"  
--read-only-port=0  
--cadvisor-port=0
```

# 3. CONTROL ACCESS TO ETCD

```
--client-cert-auth=true  
--auto-tls=false  
--peer-client-cert-auth=true  
--peer-auto-tls=false
```



# 4. RESTRICT SERVICE TOKEN USE

# 5. RESTRICT PRIVILEGED CONTAINERS

# 6. API SERVER AUTHENTICATION

```
--anonymous-auth=false  
--basic-auth-file - Not Set  
--token-auth-file - Not Set
```



# 7. API SERVER AUTHORISATION

```
--authorization-mode=RBAC
```

# 8. PODSECURITYPOLICY

# 9. NETWORKPOLICY



# 10. REGULAR UPGRADES!

# HONOURABLE MENTION - CLOUD RIGHTS

# RESOURCES

- CIS Security Guide for Kubernetes - <https://learn.cisecurity.org/benchmarks>

# CONCLUSION

- Default Security Options very important.
- Always think about your threat model and attack surface :)
- Get the basics right



# QUESTIONS

- Twitter - @raesene
- E-mail -  
rory.mccune@nccgroup.trust