Atacando e auditando containers Docker

Fernando Silva
@FernandoDebrand

Sobre mim!

Fernando Silva

Software Developer Analyst

KINGHOST

Análise e Desenvolvimento de Sistemas

Fecomércio RS | Senac

UFRGS

open source

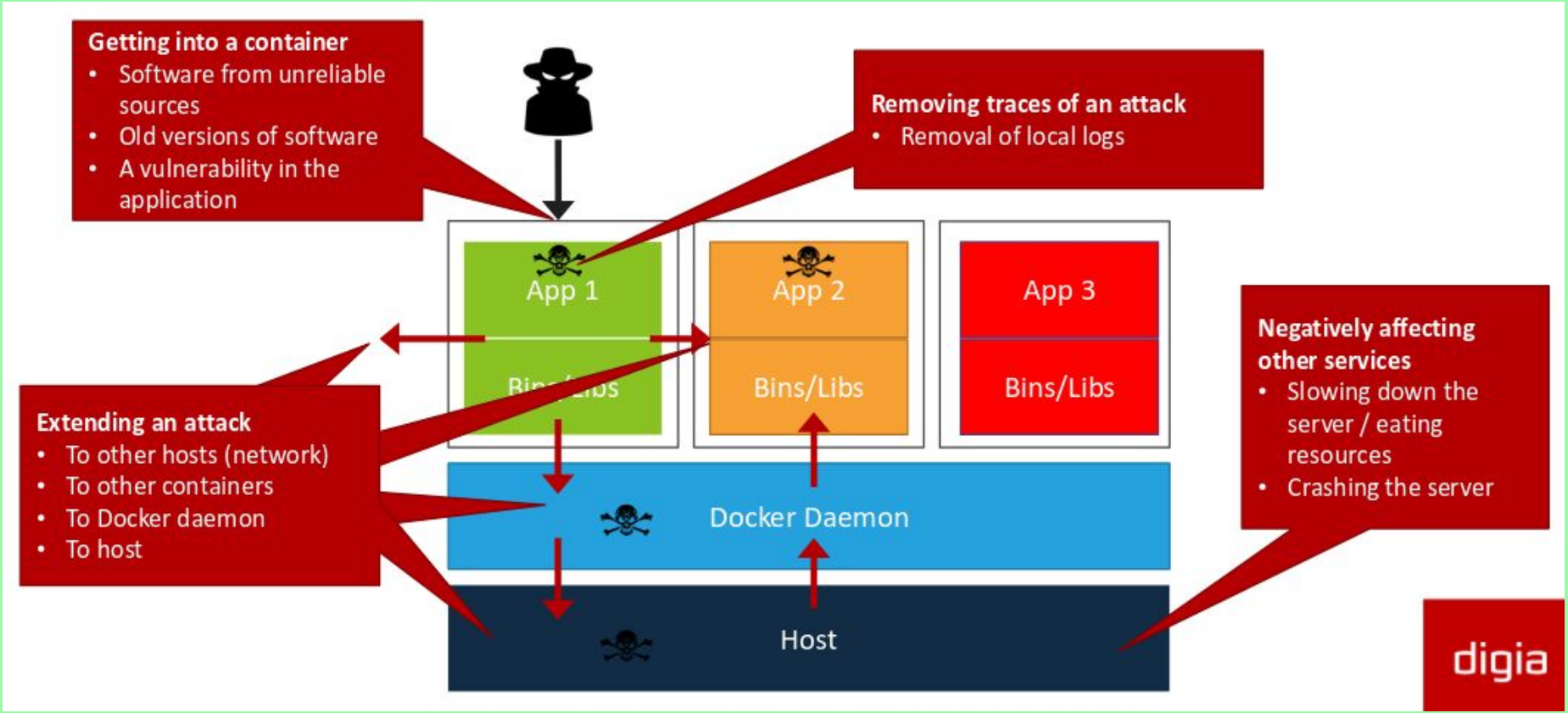
software ivre Brasil

CYBER SECURITY

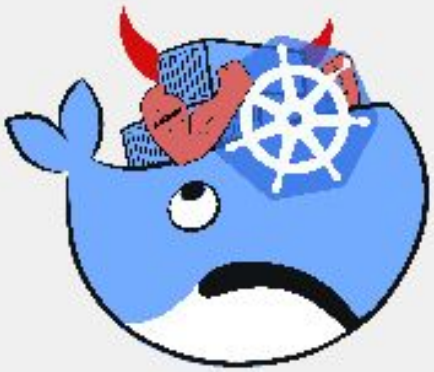
Visão Geral

- Vetores de ataques
- Como hackers estão explorando conteinerização
- Anatomia dos ataques
- Auditoria de ambientes contenerizados

Vetores de ataque



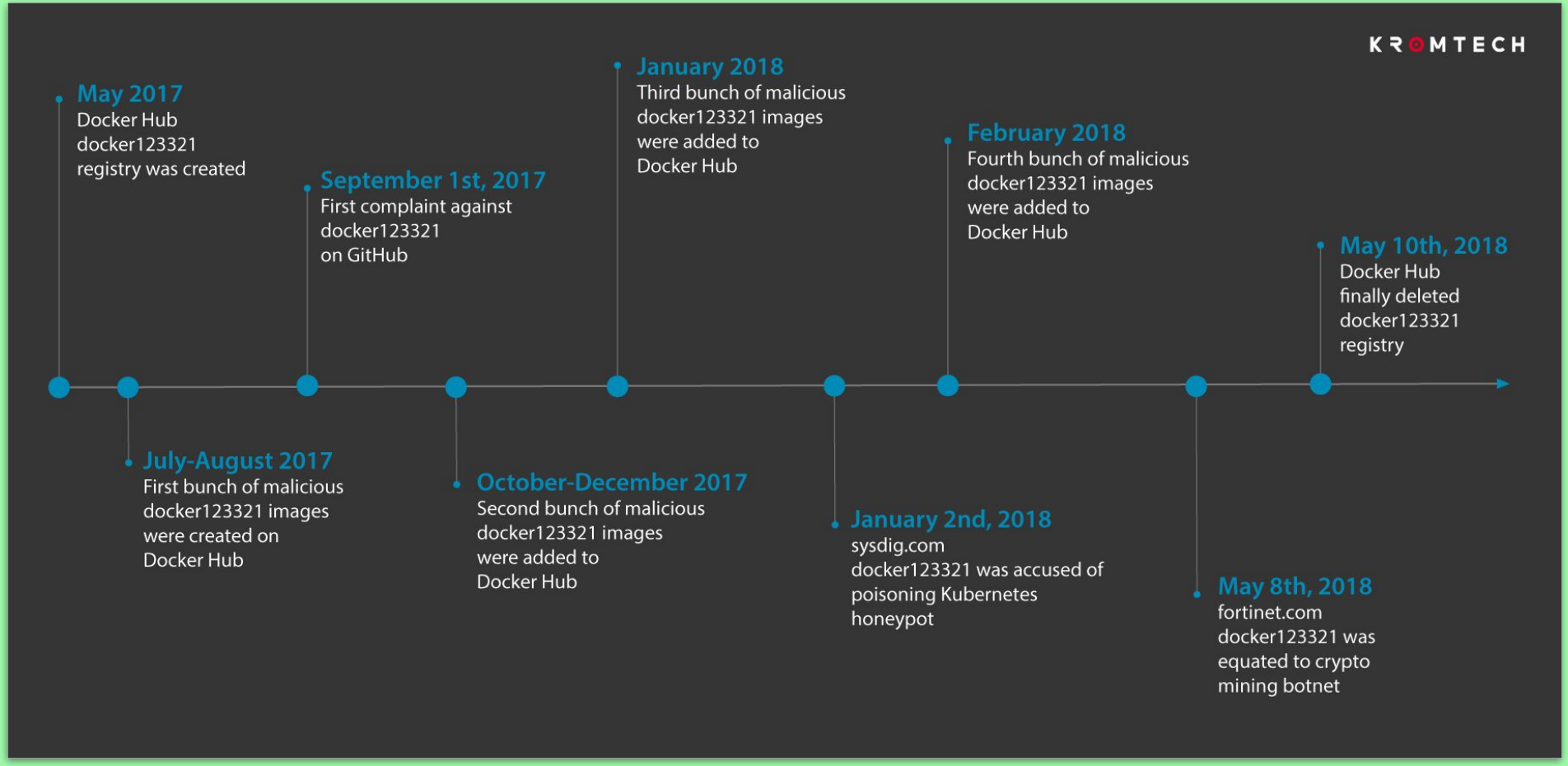
Como hackers estão explorando conteinerização



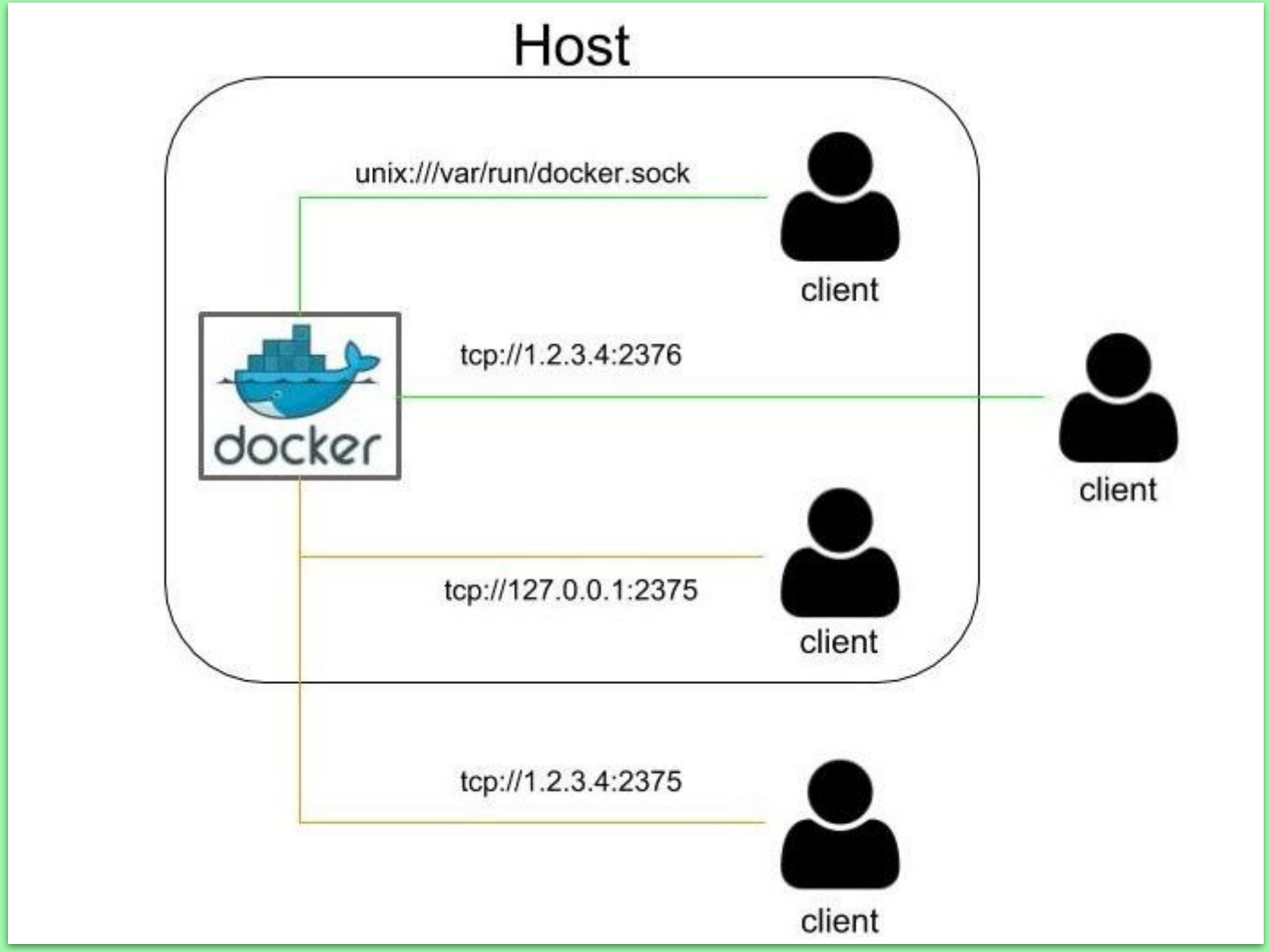
Cryptojacking invades cloud. How modern containerization trend is exploited by attackers

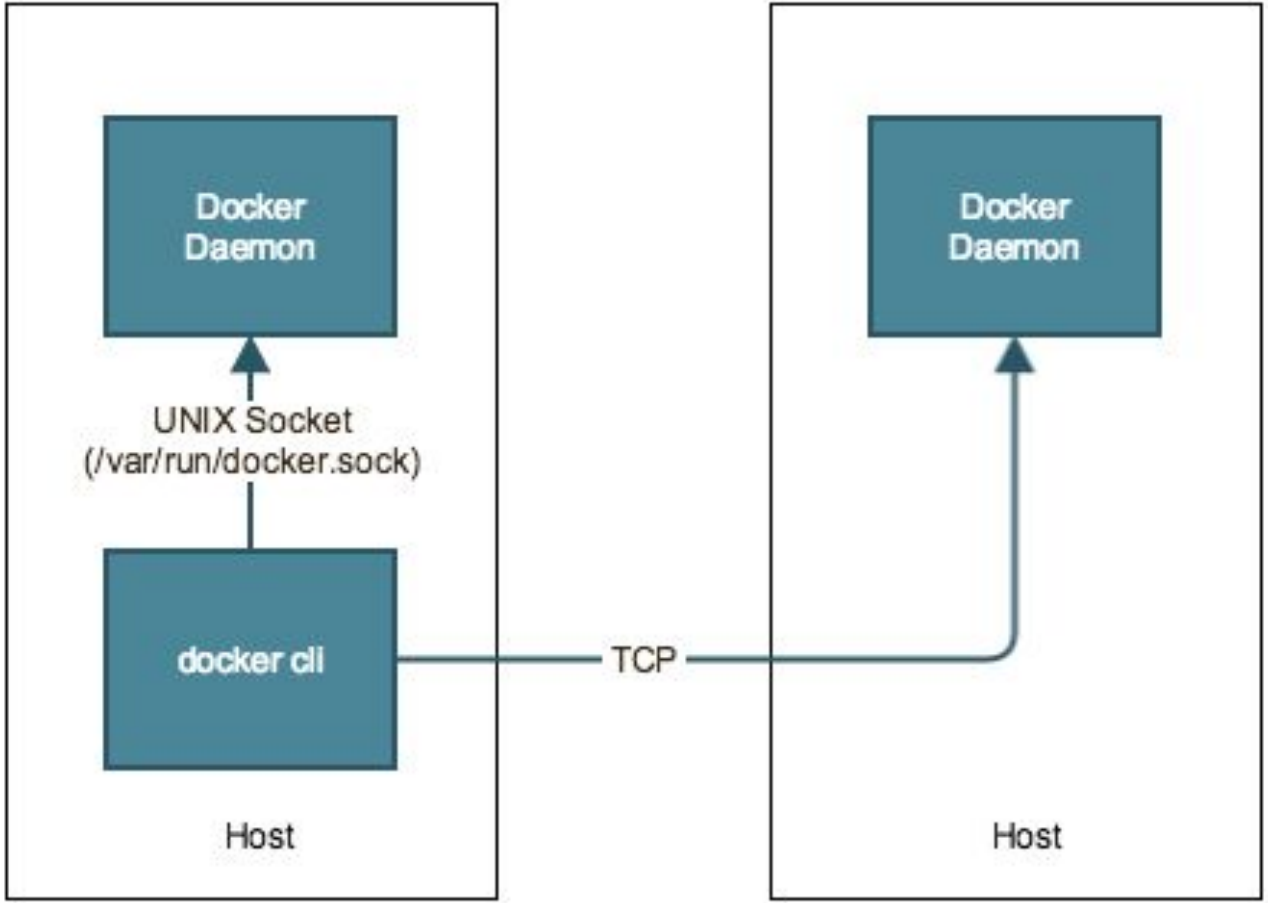
2018-06-12 | By Security Center

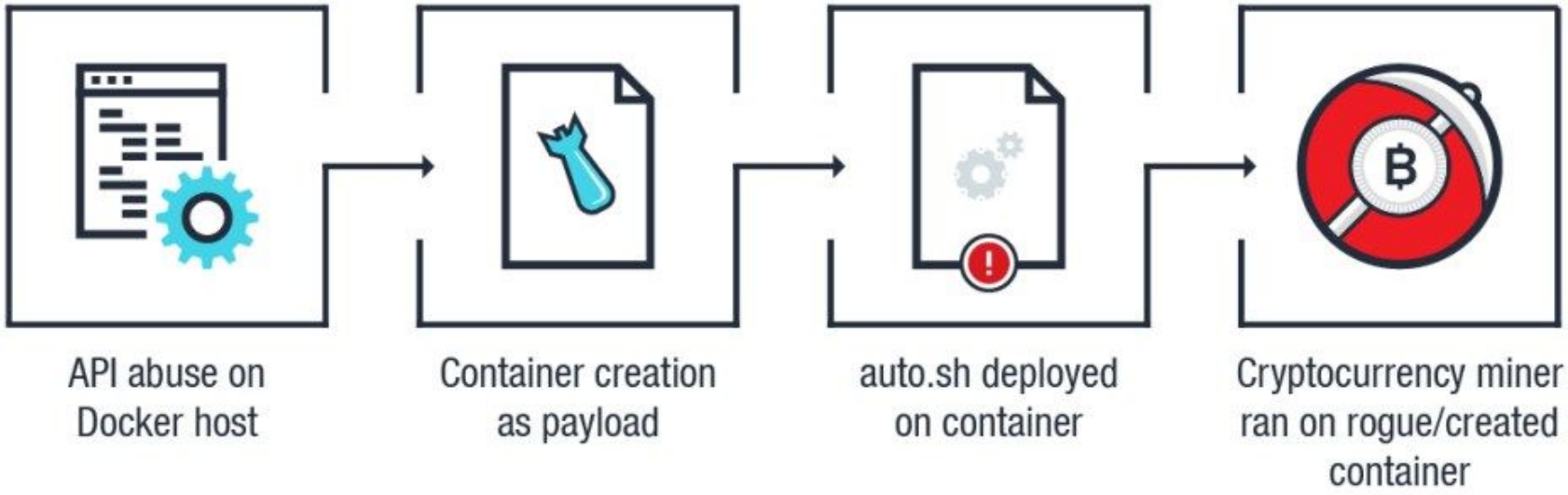
17 imagens Docker disponibilizadas por uma única conta durante 10 meses no Docker Hub, com mais de 5 milhões de pulls, podem ter minerado US $90.000 em criptomoedas Monero.


KROMTECH
May 2017
Docker Hub
docker123321
registry was created
July-August 2017
First bunch of malicious
docker123321 images
were created on
Docker Hub
September 1st, 2017
First complaint against
docker123321
on GitHub
October-December 2017
Second bunch of malicious
docker123321 images
were added to
Docker Hub
January 2018
Third bunch of malicious
docker123321 images
were added to
Docker Hub
January 2nd, 2018
sysdig.com
docker123321 was accused of
poisoning Kubernetes
honeypot
February 2018
Fourth bunch of malicious
docker123321 images
were added to
Docker Hub
May 8th, 2018
fortinet.com
docker123321 was
equated to crypto
mining botnet
May 10th, 2018
Docker Hub
finally deleted
docker123321
registry

Anatomia dos ataques

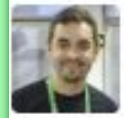

Host
unix:///var/run/docker.sock
client
tcp://1.2.3.4:2376
client
docker
tcp://127.0.0.1:2375
client
tcp://1.2.3.4:2375
client


Docker
Daemon
UNIX Socket
(/var/run/docker.sock)
docker cli
TCP
Host
Docker
Daemon
Host


API abuse on Docker host
Container creation as payload
auto.sh deployed on container
Cryptocurrency miner ran on rogue/created container

Malicious image in docker hub #1554

Closed **fernandodebrando** opened this issue 5 days ago · 3 comments



fernandodebran... commented 5 days ago

Malicious image found in the account https://hub.docker.com/r/l0s3r in the docker hub.

jmwong commented 5 days ago

Thanks for the report **@fernandodebrando**. Could you elaborate on those images? Have you seen it being used in an attack?

API do Docker Aberta na Internet?

Open API Docker Containers

Search for product:docker returned 1,307 results on 04-12-2018

Top Countries

1.	China	572
2.	United States	248
3.	Germany	51
4.	India	45
5.	Ireland	42
6.	France	41
7.	United Kingdom	36
8.	Singapore	32
9.	Japan	29
10.	Korea, Republic of	27

Open API Docker Containers

Search for product:docker country:"BR" returned 26 results on 04-12-2018

Top Cities

1. Sao Paulo	19
2. Campinas	2
3. Rio De Janeiro	1
4. Florianopolis	1
5. Belo Horizonte	1

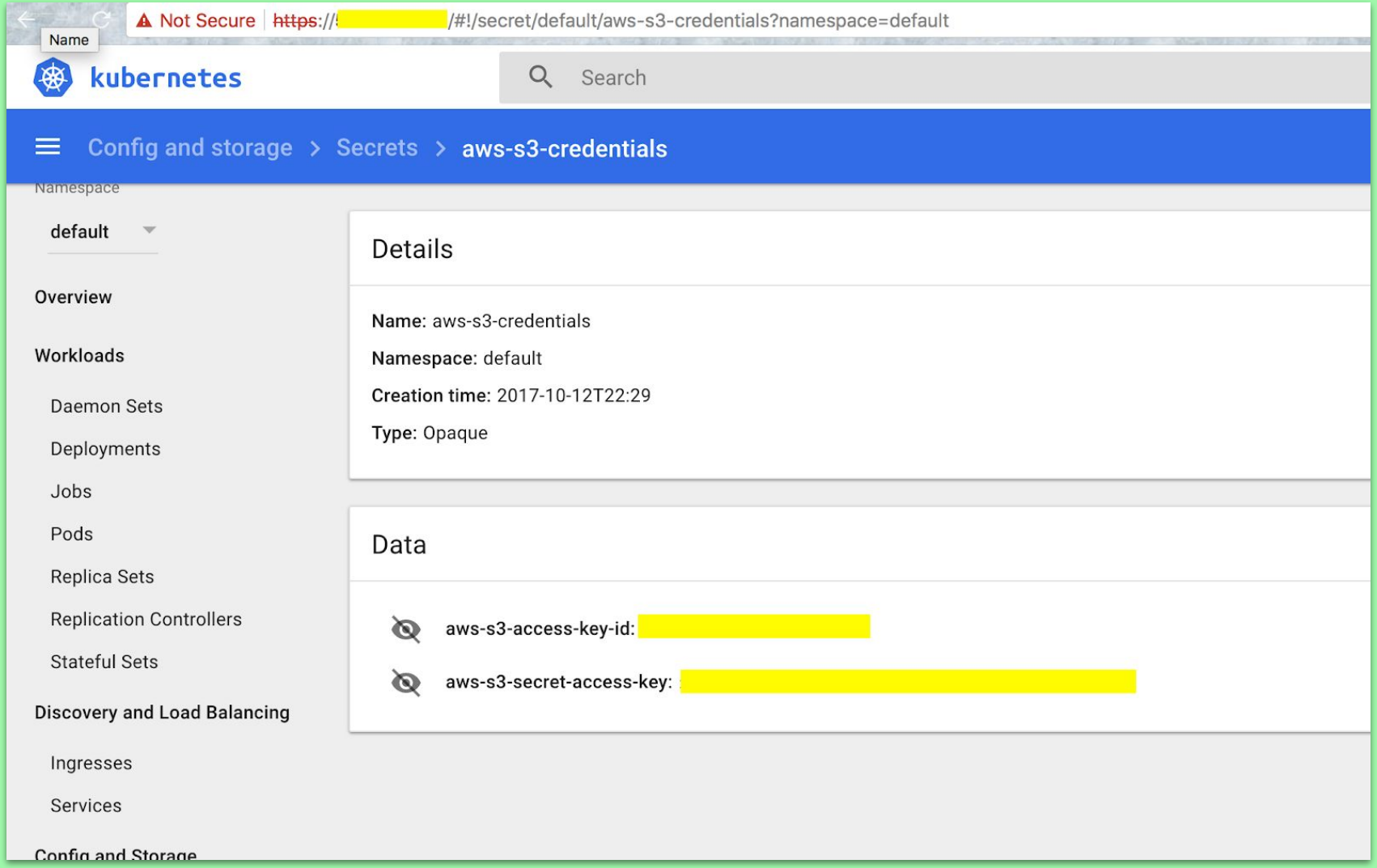
Nuvem da Tesla foi invadida e usada para minerar criptomoeda

https://blog.redlock.io/cryptojacking-tesla

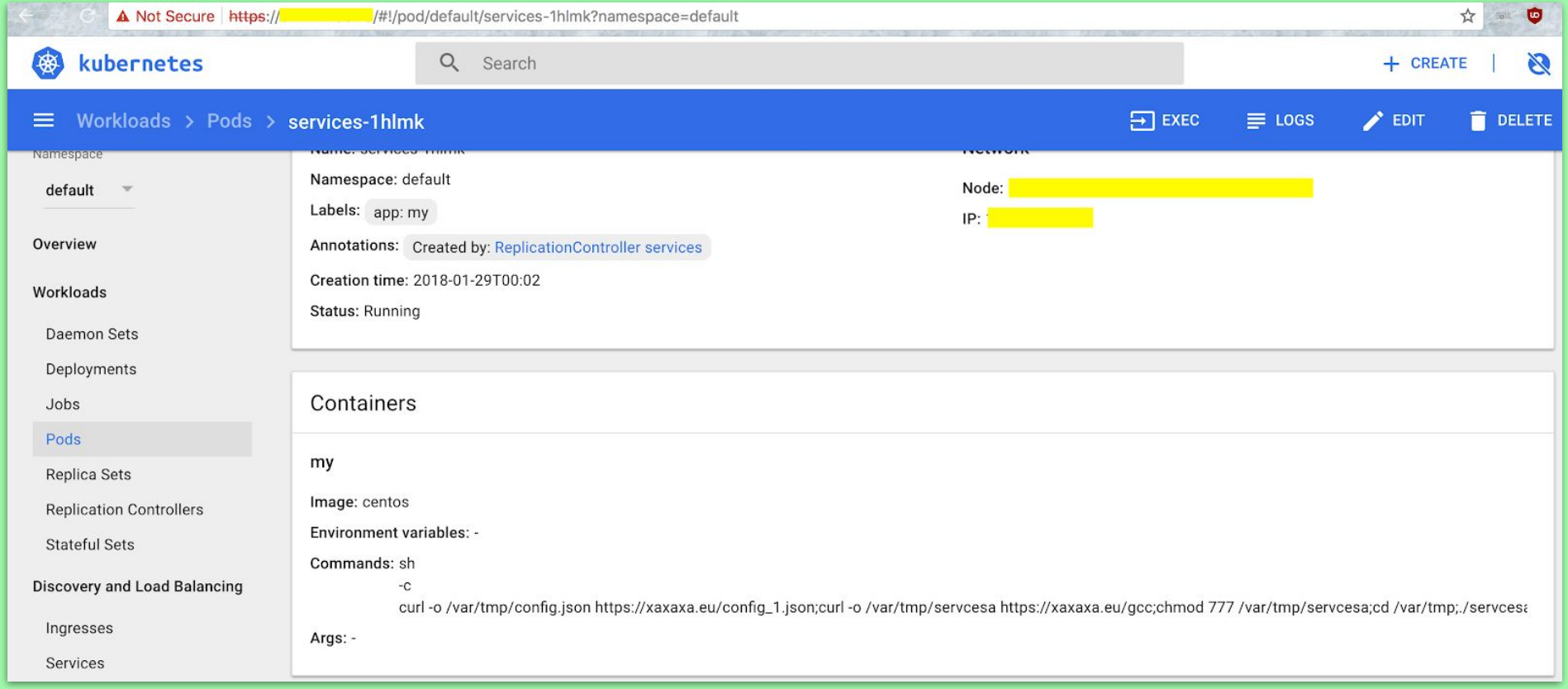
Anatomia dos ataques

Tesla é vítima de cryptojacking

Os **hackers se infiltraram no console Kubernetes** da Tesla, que **não era protegido por senha**. Em um pod Kubernetes, as credenciais de acesso foram expostas ao ambiente AWS da Tesla, que continha um bucket do Amazon S3 (Amazon Simple Storage Service) que tinha dados confidenciais, como telemetria.

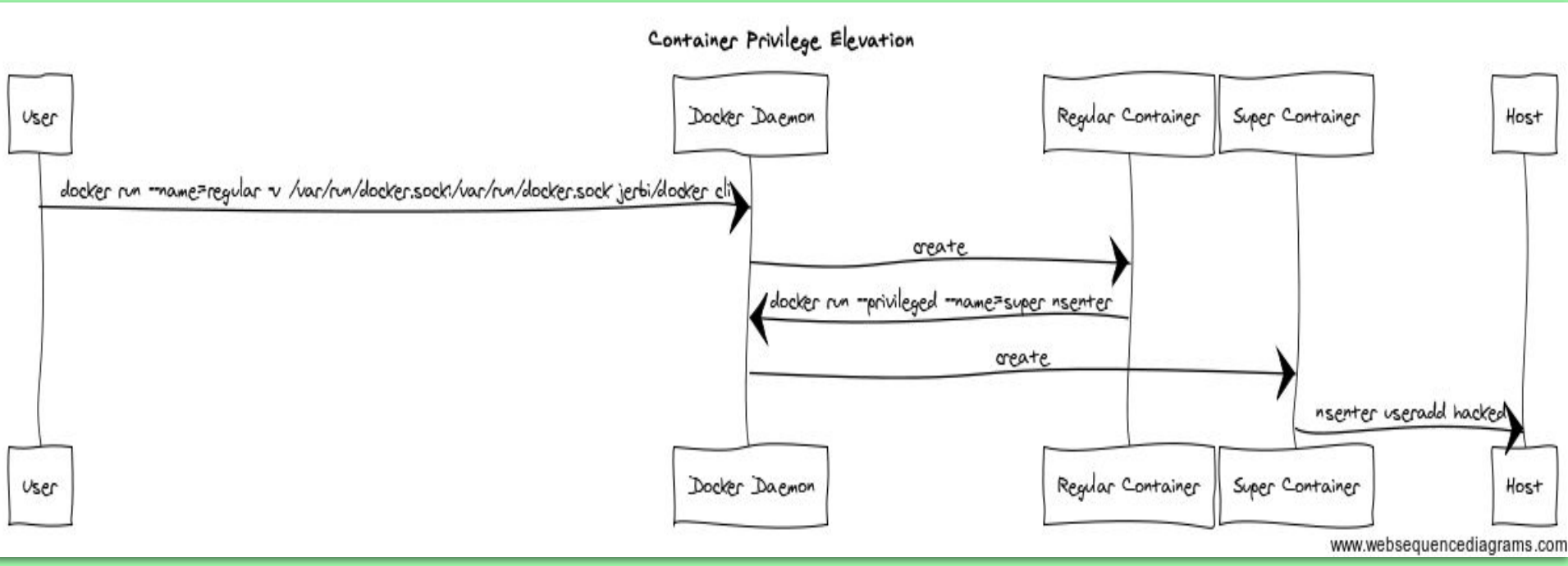

Not Secure
https://[redacted]/#!/secret/default/aws-s3-credentials?namespace=default
Name
kubernetes
Search
Config and storage > Secrets > aws-s3-credentials
Namespace
default
Overview
Workloads
Daemon Sets
Deployments
Jobs
Pods
Replica Sets
Replication Controllers
Stateful Sets
Discovery and Load Balancing
Ingresses
Services
Config and Storage
Details
Name: aws-s3-credentials
Namespace: default
Creation time: 2017-10-12T22:29
Type: Opaque
Data
aws-s3-access-key-id: [redacted]
aws-s3-secret-access-key: [redacted]

Script de mineração de criptomoeda em execução no pod Kubernetes da Tesla



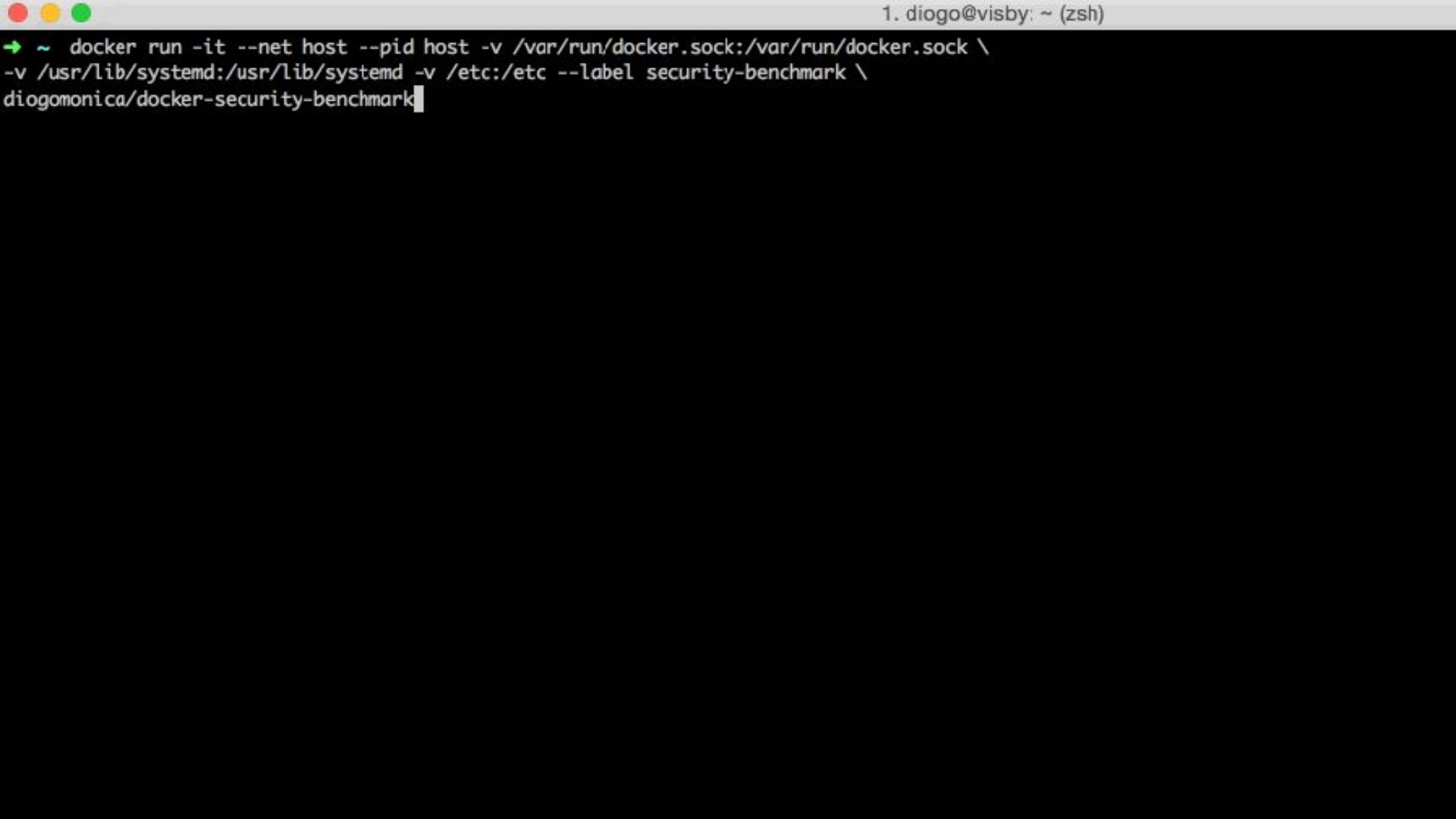
Outros ataques

- ➔ Ataque a montagens de volume inseguro
- ➔ Ataque de elevação de privilégio de container


Container Privilege Elevation
User
Docker Daemon
Regular Container
Super Container
Host
docker run --name=regular -v /var/run/docker.sock:/var/run/docker.sock jerbi/docker cli
create
docker run --privileged --name=super nsenter
create
nsenter useradd hacked
User
Docker Daemon
Regular Container
Super Container
Host
www.websequencediagrams.com

Auditoria de ambientes conteneriz

Docker Bench for Security

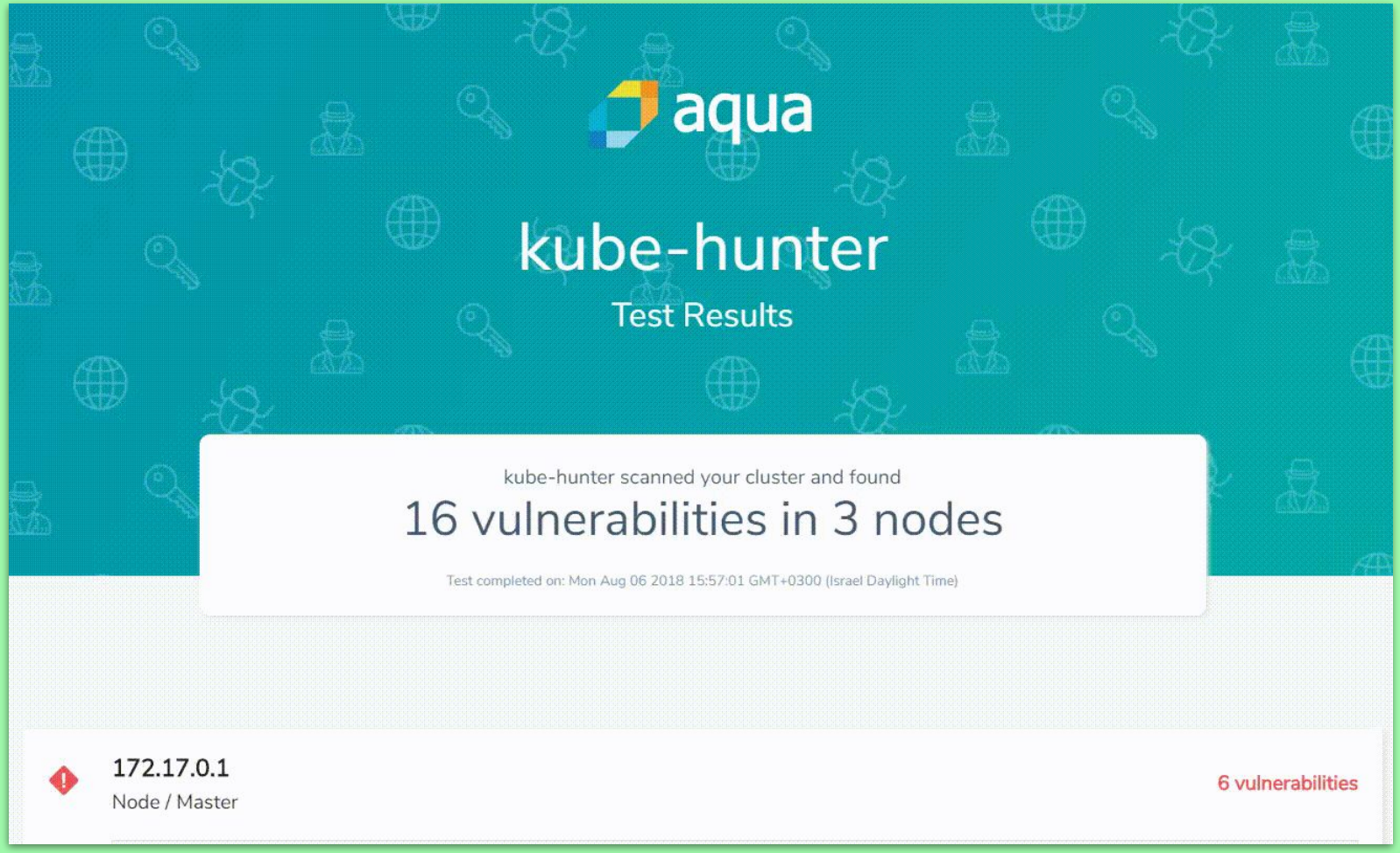

1. diogo@visby: ~ (zsh)
➜ ~ docker run -it --net host --pid host -v /var/run/docker.sock:/var/run/docker.sock \
-v /usr/lib/systemd:/usr/lib/systemd -v /etc:/etc --label security-benchmark \
diogomonica/docker-security-benchmark

kube-bench

kube-hunter

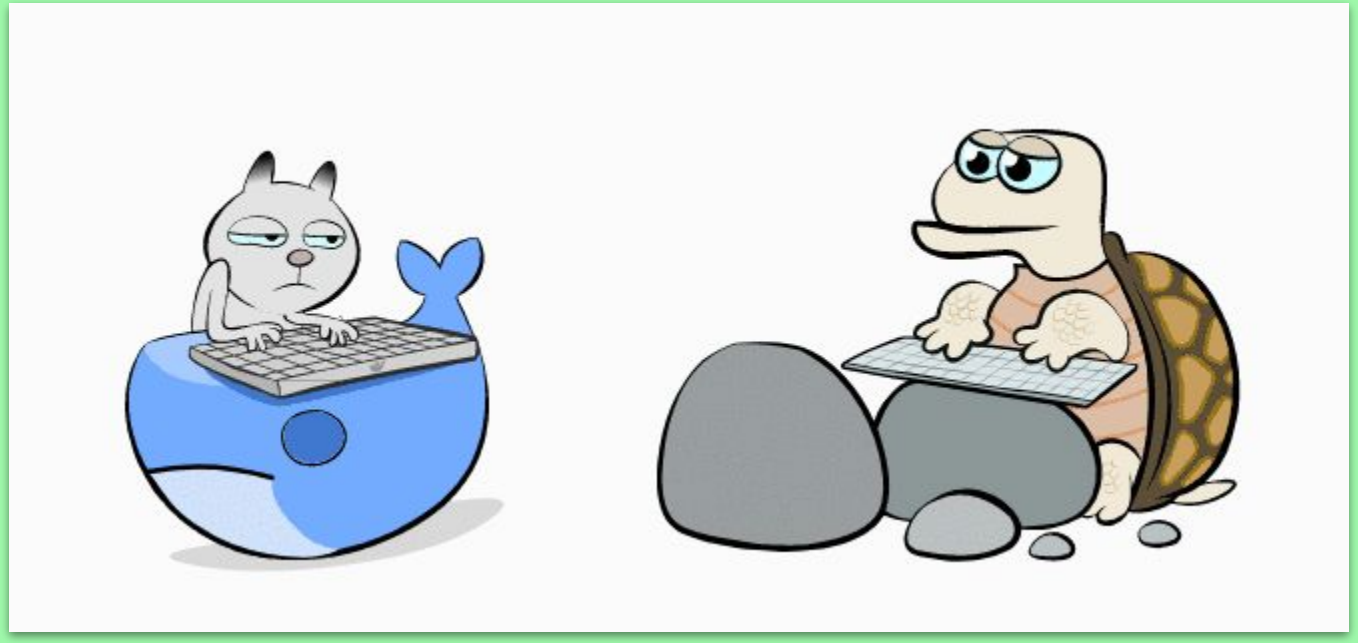
An Open Source Tool for

Kubernetes Penetration Testing


aqua
kube-hunter
Test Results
kube-hunter scanned your cluster and found
16 vulnerabilities in 3 nodes
Test completed on: Mon Aug 06 2018 15:57:01 GMT+0300 (Israel Daylight Time)
172.17.0.1
Node / Master
6 vulnerabilities


aqua
MicroScanner
Free Image Vulnerability
Scanner for Developers

Demonstração



Como proteger a API Docker?

Proteja o soquete do daemon do Docker

TLS precisa ser ativado especificando o sinalizador **tlsverify** e apontando o **tlscacert** do Docker para um **certificado de CA confiável**.

Há um processo passo-a-passo explicado como proteger em https://docs.docker.com/engine/security/https.

Referências / Links

- https://kubernetes-security.info/
- https://www.owasp.org/images/f/f2/Owasp-Helsinki-20170613-Docker-Security.pdf
- https://kubernetes.io/docs/setup/minikube/
- https://blog.aquasec.com/kube-hunter-kubernetes-penetration-testing
- https://github.com/aquasecurity/microscanner
- https://github.com/docker/docker-bench-security
- https://container-solutions.com/docker-security-admin-controls-2/
- https://container-solutions.com/understanding-volumes-docker/
- https://medium.com/@FernandoDebrand/seguranca-e-hacking-de-containers-docker-a6eaab43238c
- https://medium.com/@FernandoDebrand/docker-hackers-conteinerizacao-a9e2b267676a
- https://github.com/aquasecurity/kube-bench

OBRIGADO!

Perguntas?

fernando.poa.br

speakerdeck.com/fernandodebrando

VENHA FAZER PARTE
DO NOSSO TIME
king.host/talentos