Attacking and Defending Kubernetes

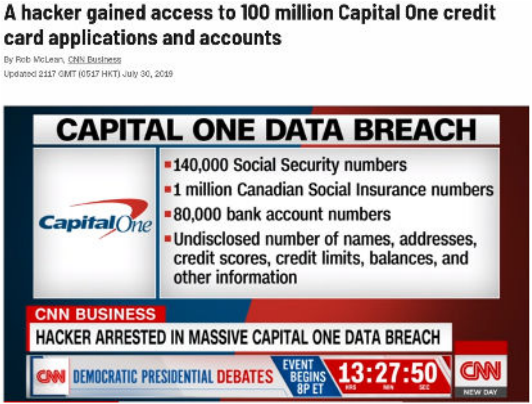
Linux Stammtisch

kubernetes

Andy Wirtz, ATIX AG

June 22nd, 2021

Capital One



A hacker gained access to 100 million Capital One credit card applications and accounts

By Rob McLean, CNN Business

Updated 2117 GMT (0517 HKT) July 30, 2019

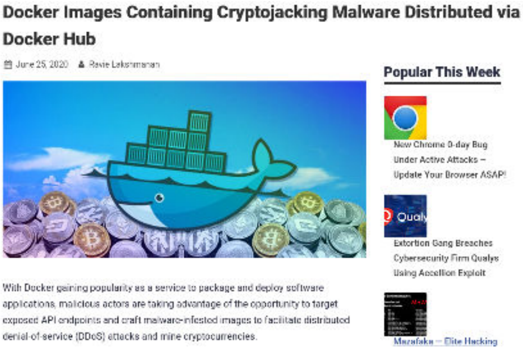
CAPITAL ONE DATA BREACH

- 140,000 Social Security numbers
- 1 million Canadian Social Insurance numbers
- 80,000 bank account numbers
- Undisclosed number of names, addresses, credit scores, credit limits, balances, and other information

Capital One
CNN BUSINESS
HACKER ARRESTED IN MASSIVE CAPITAL ONE DATA BREACH
CNN
DEMOCRATIC PRESIDENTIAL DEBATES
EVENT BEGINS 8P ET
13:27:50
HRS MIN SEC
CNN
NEW DAY

https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

Docker Hub & Microsoft Azure



Docker Images Containing Cryptojacking Malware Distributed via Docker Hub

June 25, 2020 Ravie Lakshmanan

With Docker gaining popularity as a service to package and deploy software applications, malicious actors are taking advantage of the opportunity to target exposed API endpoints and craft malware-infested images to facilitate distributed denial-of-service (DDoS) attacks and mine cryptocurrencies.

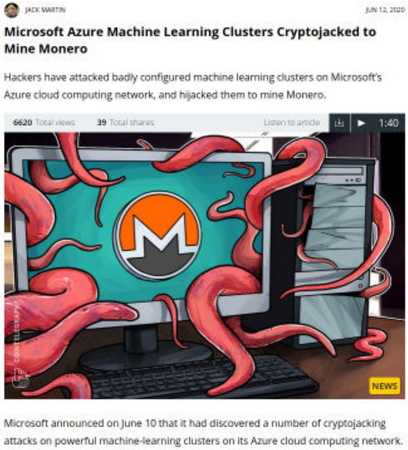
Popular This Week

New Chrome 0-day Bug Under Active Attacks – Update Your Browser ASAP!

Extortion Gang Breaches Cybersecurity Firm Qualys Using Accellion Exploit

Mazafaka — Elite Hacking

https://thehackernews.com/2020/06/cryptocurrency-docker-image.html



JACK MARTIN JUN 12, 2020

Microsoft Azure Machine Learning Clusters Cryptojacked to Mine Monero

Hackers have attacked badly configured machine learning clusters on Microsoft's Azure cloud computing network, and hijacked them to mine Monero.

6620 Total views 39 Total shares Listen to article ▶ 1:40

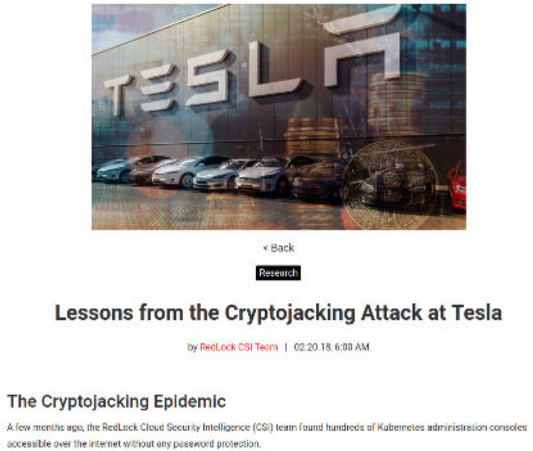
NEWS

Microsoft announced on June 10 that it had discovered a number of cryptojacking attacks on powerful machine-learning clusters on its Azure cloud computing network.

https://cointelegraph.com/news/microsoft-azure-machine-learning-clusters-cryptojacked-to-mine-monero

#kubernetes #security

Tesla & Jenkins



< Back

Research

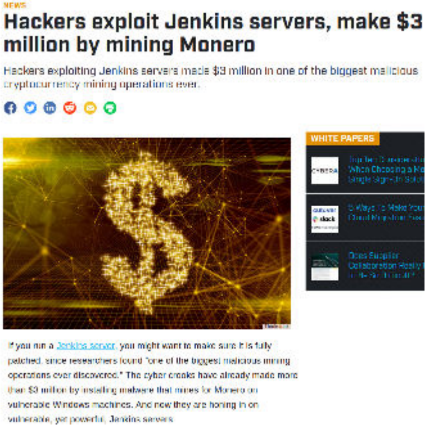
Lessons from the Cryptojacking Attack at Tesla

by RedLock CSI Team | 02.20.18, 6:00 AM

The Cryptojacking Epidemic

A few months ago, the RedLock Cloud Security Intelligence (CSI) team found hundreds of Kubernetes administration consoles accessible over the internet without any password protection.

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



NEWS

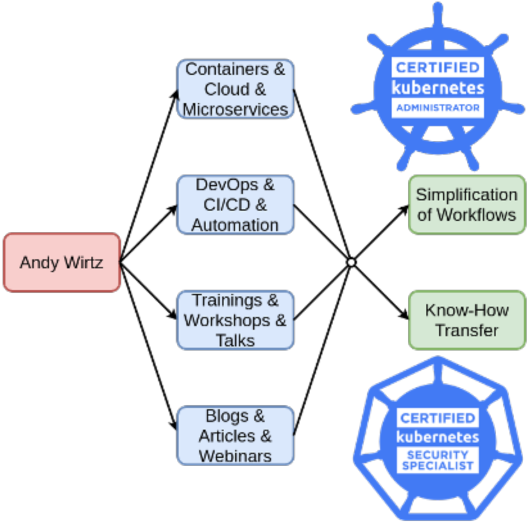
Hackers exploit Jenkins servers, make $3 million by mining Monero

Hackers exploiting Jenkins servers made $3 million in one of the biggest malicious cryptocurrency mining operations ever.

If you run a Jenkins server, you might want to make sure it is fully patched, since researchers found "one of the biggest malicious mining operations ever discovered." The cyber crooks have already made more than $3 million by installing malware that mines for Monero on vulnerable Windows machines. And now they are honing in on vulnerable, yet powerful, Jenkins servers.

https://www.csoonline.com/article/3256314/hackers-exploit-jenkins-servers-make-3-million-by-mining-monero.html

Andy Wirtz – Senior IT Consultant at ATIX AG, Germany



Andy Wirtz

Containers & Cloud & Microservices

DevOps & CI/CD & Automation

Trainings & Workshops & Talks

Blogs & Articles & Webinars

Simplification of Workflows

Know-How Transfer

- Phone: +49 (0)89 452 35 38-248
- Email: `wirtz@atix.de`
- `www.xing.com/profile/Andy_Wirtz2`
- `www.linkedin.com/in/andy-wirtz`

#kubernetes #security

Agenda

1 Attack Kubernetes

2 Demo of an Attack Path

3 Defend Kubernetes

4 Mitigate the Attack Path

5 Security Checklist

#kubernetes #security

Agenda

1 Attack Kubernetes

2 Demo of an Attack Path

3 Defend Kubernetes

4 Mitigate the Attack Path

5 Security Checklist

Kubernetes

Virtual data center

- for container apps
- manages compute resources

Wide spread use

- interesting for attackers
- various attack surfaces

API Server
Node
Network
Resources

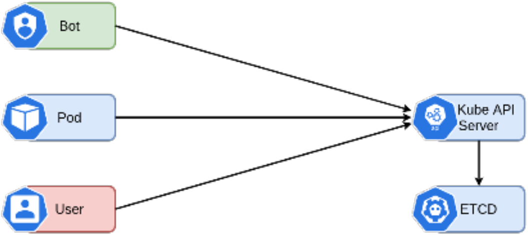
Kubernetes API Server

Access control

- to Kubernetes objects
- can be annulled

Unwarranted access

- read secrets, write workloads
- administer cluster



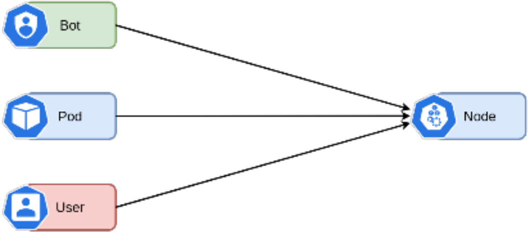
Container Hosts

Container isolation

- of process, network, filesystem
- can be softened

Container outbreak

- access host file system
- root in container = root on host



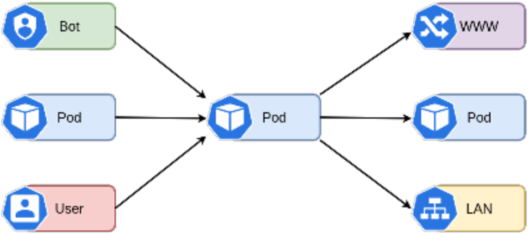
Container Network

Container communication

- in a flat network
- can be unlimited

Unwanted communication

- download malware
- talk to other apps



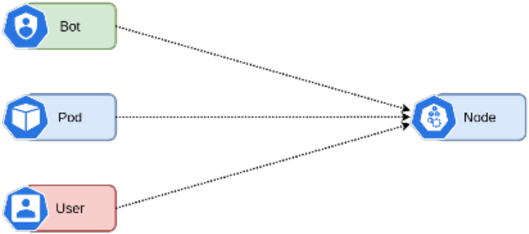
Compute Resources

Allocatable resources

- are CPU, memory, storage
- can be misused

Consume resources

- crypto mining
- fork bombs



Agenda

1 Attack Kubernetes

2 Demo of an Attack Path

3 Defend Kubernetes

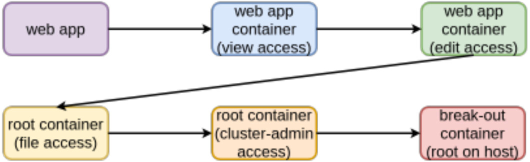
4 Mitigate the Attack Path

5 Security Checklist

Goals

Privilege escalation to control

- Kubernetes
- container hosts


web app
web app container (view access)
web app container (edit access)
root container (file access)
root container (cluster-admin access)
break-out container (root on host)

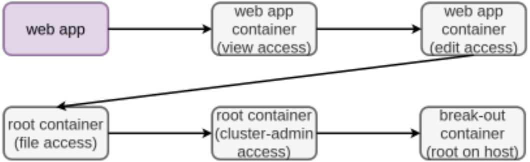
Crypto Mining without detection

- divert compute resources
- share over network

Web application

Command injection

- ping servers
- execute additional commands


web app
web app container (view access)
web app container (edit access)
root container (file access)
root container (cluster-admin access)
break-out container (root on host)

Access via reverse shell

- target machine initiates connection
- user’s computer listens

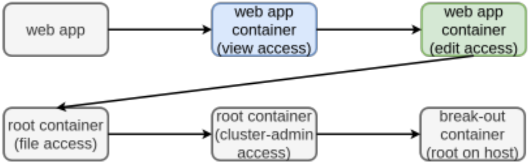
Web application container

View access to Kubernetes

- read ServiceAccounts
- read Secrets

Edit access to Kubernetes

- create root container on master
- log into new container


web app
web app container (view access)
web app container (edit access)
root container (file access)
root container (cluster-admin access)
break-out container (root on host)

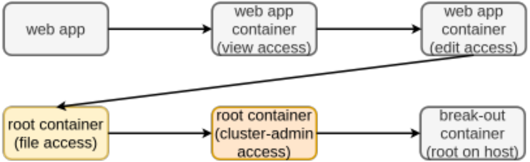
Root container

Root user in container on master

- use hostPath
- read admin.conf

Cluster-admin access to Kubernetes

- create break-out container
- log into new container


web app
web app container (view access)
web app container (edit access)
root container (file access)
root container (cluster-admin access)
break-out container (root on host)

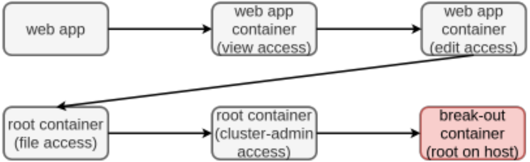
Break-out container

Root user on host

- create mining container
- use docker

Cleanup

- delete root container
- delete break-out container


web app
web app container (view access)
web app container (edit access)
root container (file access)
root container (cluster-admin access)
break-out container (root on host)

Agenda

1 Attack Kubernetes

2 Demo of an Attack Path

3 Defend Kubernetes

4 Mitigate the Attack Path

5 Security Checklist

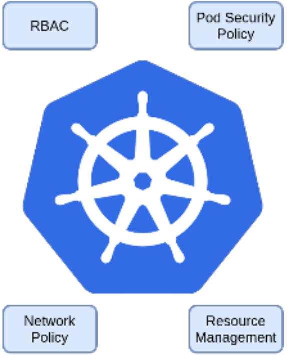
Security Basics

Defence in depth

- attackers pick their targets
- layered security needed

Best practices

- limit attack surface
- principle of least privilege



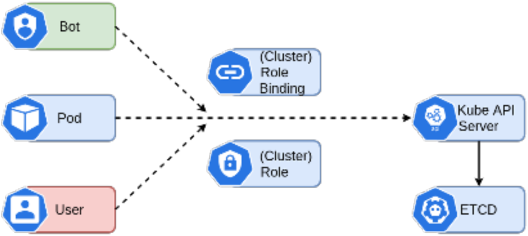
Role-Based Access Control

Kubernetes bouncer

- for Kubernetes resources and others
- namespace- or cluster-wide

Least privilege access

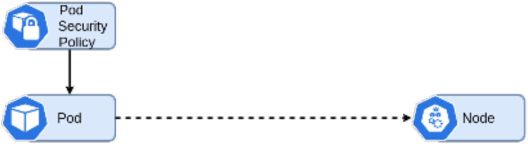
- no access for apps and humans
- access for tools (CD, monitoring)



PodSecurityPolicies

Container prison

- drop capabilities
- ensure separation



Prevent outbreak

- deny privileged/root/privilege escalation
- ensure isolation & RO root filesystem

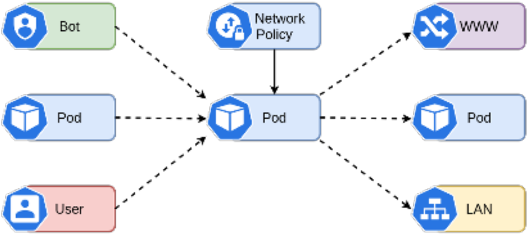
NetworkPolicy

Container firewall

- for ingress and egress
- with labels, namespaces, ip-blocks

Restrict communication

- default deny all
- allow-list specific traffic



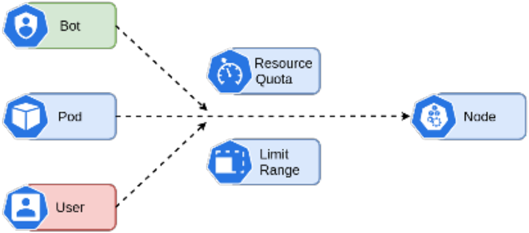
Resource Management

Kubernetes limiter

- quotas for namespaces
- limits for containers, pods, pvcs

Assign resources

- split resources for tenants
- define min, max, default resources



Agenda

1 Attack Kubernetes

2 Demo of an Attack Path

3 Defend Kubernetes

4 Mitigate the Attack Path

5 Security Checklist

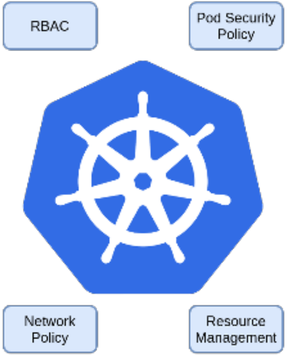
Security Basics

Defence in depth

- attackers pick their targets
- layered security needed

Best practices

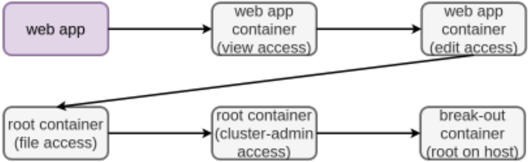
- limit attack surface
- principle of least privilege



Mitigate 1

Mitigate reverse shell for container

- scan container images for vulnerabilities
- remove unnecessary software
- restrict traffic with NetworkPolicies


web app
web app container (view access)
web app container (edit access)
root container (file access)
root container (cluster-admin access)
break-out container (root on host)

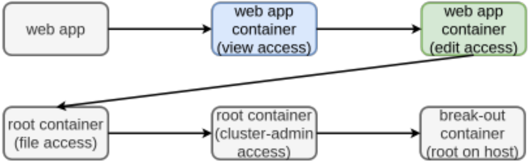
Mitigate installation of new software

- scan container images for vulnerabilities
- remove unnecessary software
- restrict traffic with NetworkPolicies

Mitigate 2

Mitigate privlige escalation to edit access

- avoid existence of unnecessary secrets
- restrict traffic with NetworkPolicies
- restrict access to API server with RBAC


web app
web app container (view access)
web app container (edit access)
root container (file access)
root container (cluster-admin access)
break-out container (root on host)

Mitigate root container on master

- restrict with NetPol and RBAC
- don’t tolerate container on master
- forbid root container with PSP

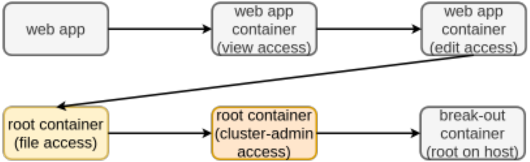
Mitigate 3

Mitigate shell for root container

- forbid root container with PSP
- restrict traffic with NetworkPolicies
- restrict access to API server with RBAC

Mitigate privlige escalation to cluster-admin

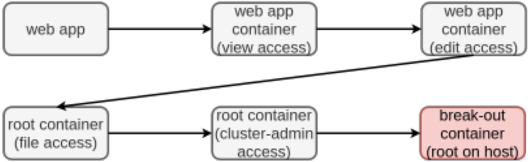
- don’t tolerate container on master
- forbid root container with PSP
- forbid hostPath with PSP


web app
web app container (view access)
web app container (edit access)
root container (file access)
root container (cluster-admin access)
break-out container (root on host)

Mitigate 4

Mitigate break-out container

- restrict with NetPol and RBAC
- forbid privileged container with PSP
- forbid hostPID with PSP


web app
web app container (view access)
web app container (edit access)
root container (file access)
root container (cluster-admin access)
break-out container (root on host)

Mitigate docker run

- restrict with NetPol and RBAC
- forbid privileged container with PSP
- forbid hostPID with PSP

Agenda

1 Attack Kubernetes

2 Demo of an Attack Path

3 Defend Kubernetes

4 Mitigate the Attack Path

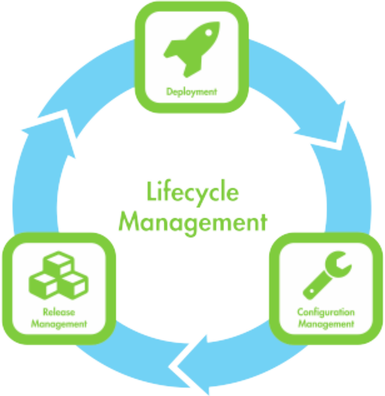
5 Security Checklist

Container Hosts

Server Lifecycle Management

- dedicated container hosts
- reduction of the attack surface
- runtime security tools
- restriction of access to the container hosts

Orcharhino

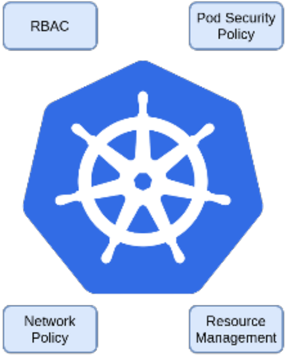


#kubernetes #security

Kubernetes

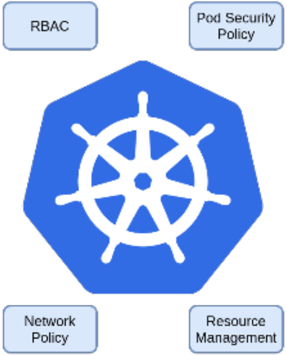
Kubernetes Lifecycle Management

- protection of the kubernetes components
- restriction of access to the kubernetes API
- usage of authentication and authorization
- usage of admission control
- enabling of audit logs
- checking via security benchmarking



Ecosystem

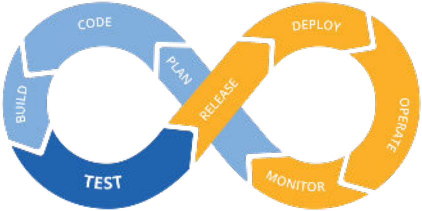
kube-bench


RBAC
Pod Security Policy
Network Policy
Resource Management

Container applications

Application Lifecycle Management

- seperation of code and data
- restriction of access to the kubernetes API
- container sandboxing
- container hardening
- vulnerability scanning of container images
- mutual TLS



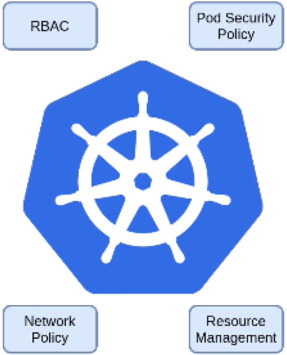
Summary

Defence in depth

- attackers pick their targets
- layered security needed

Best practices

- limit attack surface
- principle of least privilege



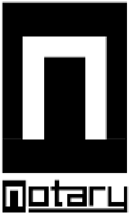
Outlook

Secure applications

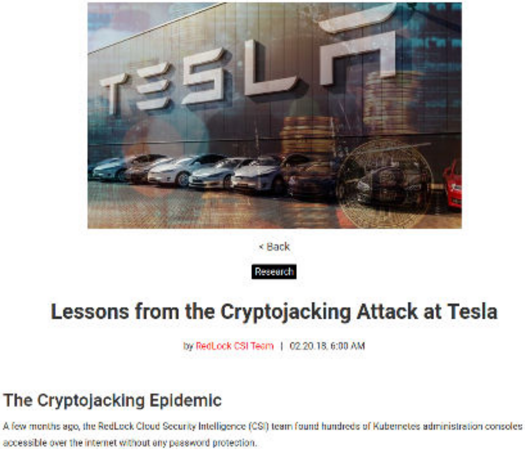
- container image scanning and signing
- sandbox technologies

Use agents

- policy agent for compliance
- RT security agent for anomaly detection



Tesla & Jenkins



< Back

Research

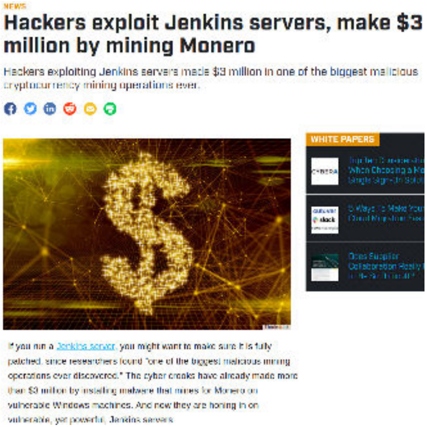
Lessons from the Cryptojacking Attack at Tesla

by RedLock CSI Team | 02.20.18, 6:00 AM

The Cryptojacking Epidemic

A few months ago, the RedLock Cloud Security Intelligence (CSI) team found hundreds of Kubernetes administration consoles accessible over the internet without any password protection.

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



NEWS

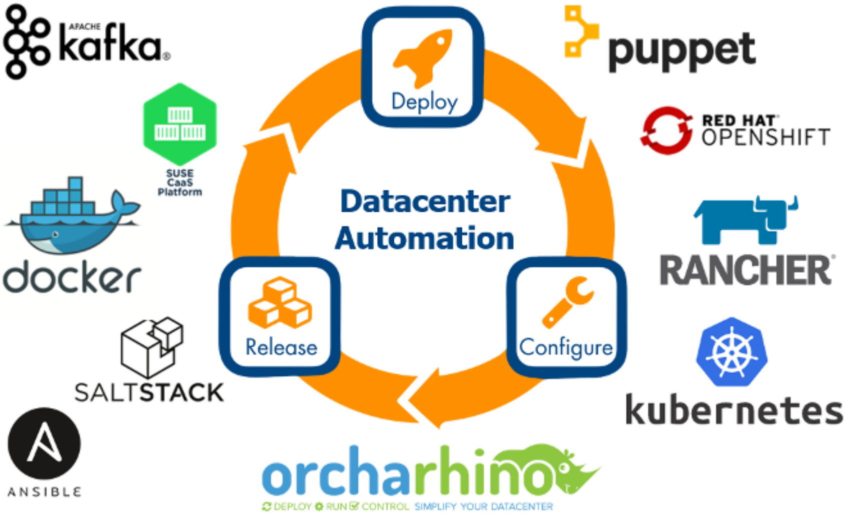
Hackers exploit Jenkins servers, make $3 million by mining Monero

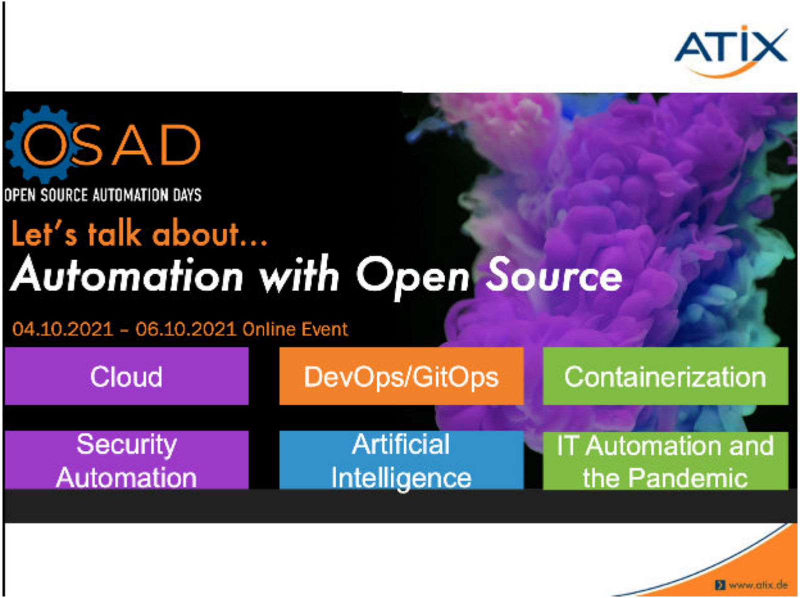
Hackers exploiting Jenkins servers made $3 million in one of the biggest malicious cryptocurrency mining operations ever.

If you run a Jenkins server, you might want to make sure it is fully patched, since researchers found "one of the biggest malicious mining operations ever discovered." The cyber crooks have already made more than $3 million by installing malware that mines for Monero on vulnerable Windows machines. And now they are honing in on vulnerable, yet powerful, Jenkins servers

https://www.csoonline.com/article/3256314/hackers-exploit-jenkins-servers-make-3-million-by-mining-monero.html

ATIX – SIMPLIFY YOUR DATACENTER





OSAD

OPEN SOURCE AUTOMATION DAYS

Let's talk about...

Automation with Open Source

04.10.2021 – 06.10.2021 Online Event

Cloud

DevOps/GitOps

Containerization

Security Automation

Artificial Intelligence

IT Automation and the Pandemic

www.atix.de