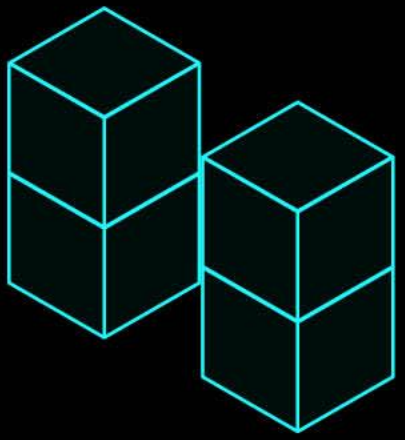
CYBERTHREAT 2023



Analyzing volatile memory on a Google Kubernetes Engine node

Marcus Hallberg
Security engineer - Detection & Response
Spotify

National Cyber Security Centre
a part of GCHQ

SANS

CYBERTHREAT 2023

Disclaimer

- This talk presents personal research and applications of open source tools.
- Spotify is not liable for this content or published code.
- Questions, remarks or other actions should be aimed towards the presenter.

National Cyber Security Centre
a part of GCHQ

SANS

CYBERTHREAT 2023

Agenda

- Main takeaways
- Container workloads at Spotify
- Google Kubernetes Engine
- What are memory snapshots?
- How can we create a memory snapshot on GKE?
- Demo and analysis

National Cyber Security Centre
a part of GCHQ

SANS

CYBERTHREAT 2023

Main takeaways

- Accessing and analysing volatile memory on a GKE node.
- Complete setup using open source tools.
- All code used - https://github.com/Monrava/cyberthreat2023

Source: https://gifdb.com/images/high/funny-sassy-cat-waiting-hurry-up-1drmhnti7ucgiqee.webp

National Cyber Security Centre
a part of GCHQ

SANS

Container workloads at Spotify

CYBERTHREAT 2023

5 GCP Regions

4096 nodes/cluster

+4000 services

+3000 namespaces

National Cyber Security Centre
a part of GCHQ

SANS

Source https://image.cnbcfm.com/api/v1/image/107149511-1668071326472-gettyimages-997042320-148347209.jpeg?v=1668140224&w=740&h=416&ffmt=webp&vtcrop=y

CYBERTHREAT 2023

The problem:

- We get an alert that a user accessed a container in GKE.
- What did user do once they accessed the container?
- There are no commercial tools available.

National Cyber Security Centre
a part of GCHQ

SANS

Source https://e0.pxfuel.com/wallpapers/26/241/desktop-wallpaper-art-owl-coffee-alarm-clock.jpg

CYBERTHREAT 2023

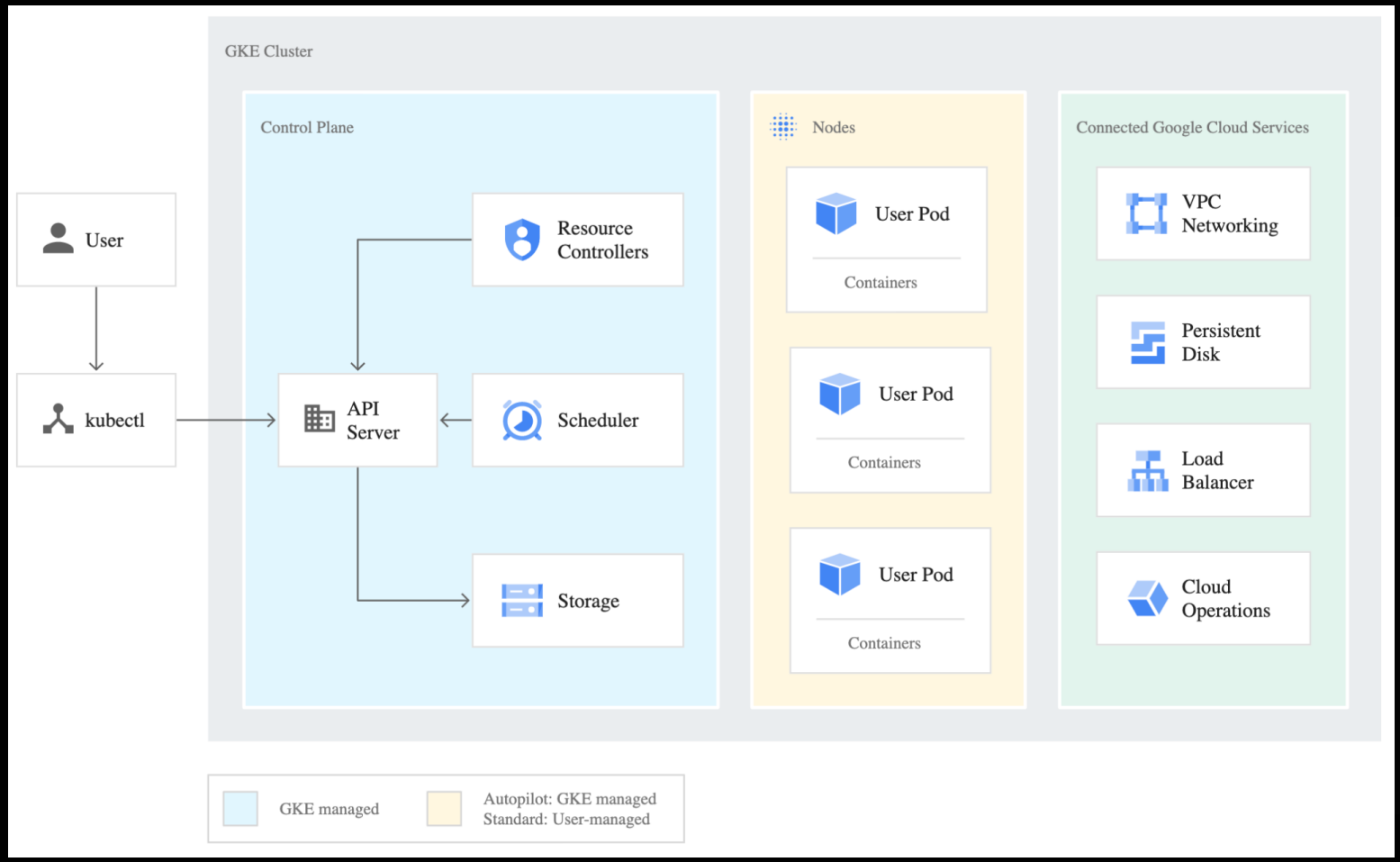

```
"principalEmail": "          @spotify.com"
"granted": true,
"permission": "io.k8s.core.v1.pods.exec.create",
"resource": "core/v1/namespaces/default/pods/pod-node-affinity-zeroday-attacker-pod/exec"
"callerIp": "195.178.178.197",
"callerSuppliedUserAgent": "kubectl/v1.25.4 (darwin/am
"resourceName": "core/v1/namespaces/default/pods/pod-n
"cluster_name": "zeroday-gke-cluster",
"project_id": "PROJECT_NAME",
"location": "europe-west1-b"
"timestamp": "2023-04-11T12:23:43.423331Z",
"logName": "projects/PROJECT_NAME/logs/cloudaudit.goog
"id": "d42f3772-56da-4658-b996-3eaf024b6b59",
"receiveTimestamp": "2023-04-11T12:23:57.235797324Z"
```


National Cyber Security Centre
a part of GCHQ

SANS

Google Kubernetes Engine

CYBERTHREAT 2023



National Cyber Security Centre
a part of GCHQ

SANS

Source https://cloud.google.com/kubernetes-engine/docs/concepts/cluster-architecture

What are memory snapshots?

CYBERTHREAT 2023

Memory snapshots

- What are they?
- Are they still used?
- Why would we take memory snapshots on GKE nodes?

National Cyber Security Centre
a part of GCHQ

SANS

Source https://kodakdigitizing.com/blogs/news/what-is-a-polaroid-picture-1

CYBERTHREAT 2023

The problem:

- We get an alert that a user accessed a container in GKE.
- What did user do once they accessed the container?
- There are no commercial tools available.

National Cyber Security Centre
a part of GCHQ

SANS

Source https://e0.pxfuel.com/wallpapers/26/241/desktop-wallpaper-art-owl-coffee-alarm-clock.jpg

How can we create a memory snapshot on GKE?

CYBERTHREAT 2023

How do we create a GKE memory snapshot?

- Step 1 - Kernel memory dump:
  - /proc/kcore
  - AVML
- Step 2 - Symbol file:
  - vmlinux
  - dwarf2json
- Step 3 - Analysis (Volatility3)

National Cyber Security Centre
a part of GCHQ

SANS

The How:
Step 1 - Kernel memory dump

- /proc/kcore

This file represents the physical memory of the system and is stored in the ELF core file format.

The total length of the file is the size of physical memory (RAM) plus 4 KiB.

- AVML (Or other tool able to take dumps of this file)

CYBERTHREAT 2023

The How:
Step 1 - Kernel memory dump

- How do we access /proc/kcore?

```
container {
  name  = "avml-container"
  image = var.container_image_avml
  security_context {
      privileged = "true"
      capabilities {
        add = ["CAP_NET_ADMIN", "CAP_SYS_ADMIN"]
      }
    }
```

National Cyber Security Centre
a part of GCHQ

SANS

CYBERTHREAT 2023

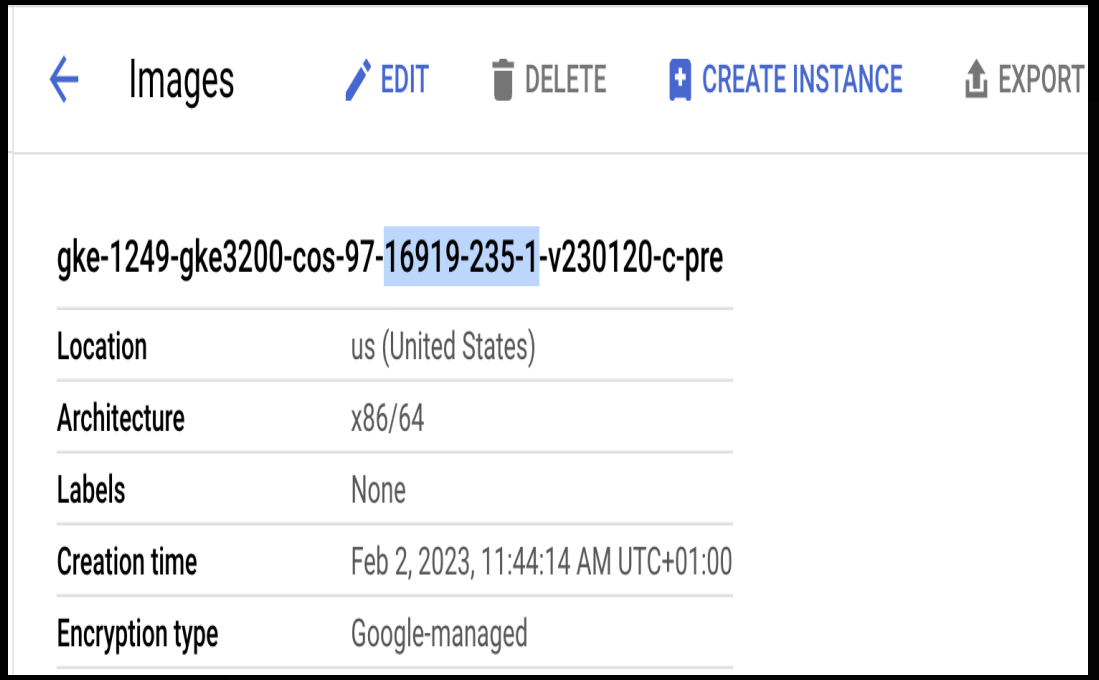
The How:
Step 2 - Symbol file

- vmlinux - what is it?

  https://storage.googleapis.com/cos-tools/$build_id/vmlinux

  https://storage.googleapis.com/cos-tools/**16919.235.1**/vmlinux

- dwarf2json



National Cyber Security Centre
a part of GCHQ

SANS

Source: https://cloud.google.com/container-optimized-os/docs/concepts/versioning#milestones_and_build_numbers

CYBERTHREAT 2023

The How:
Step 3 - Analysis

- Volatility3

volatilityfoundation/
volatility3

Volatility 3.0 development

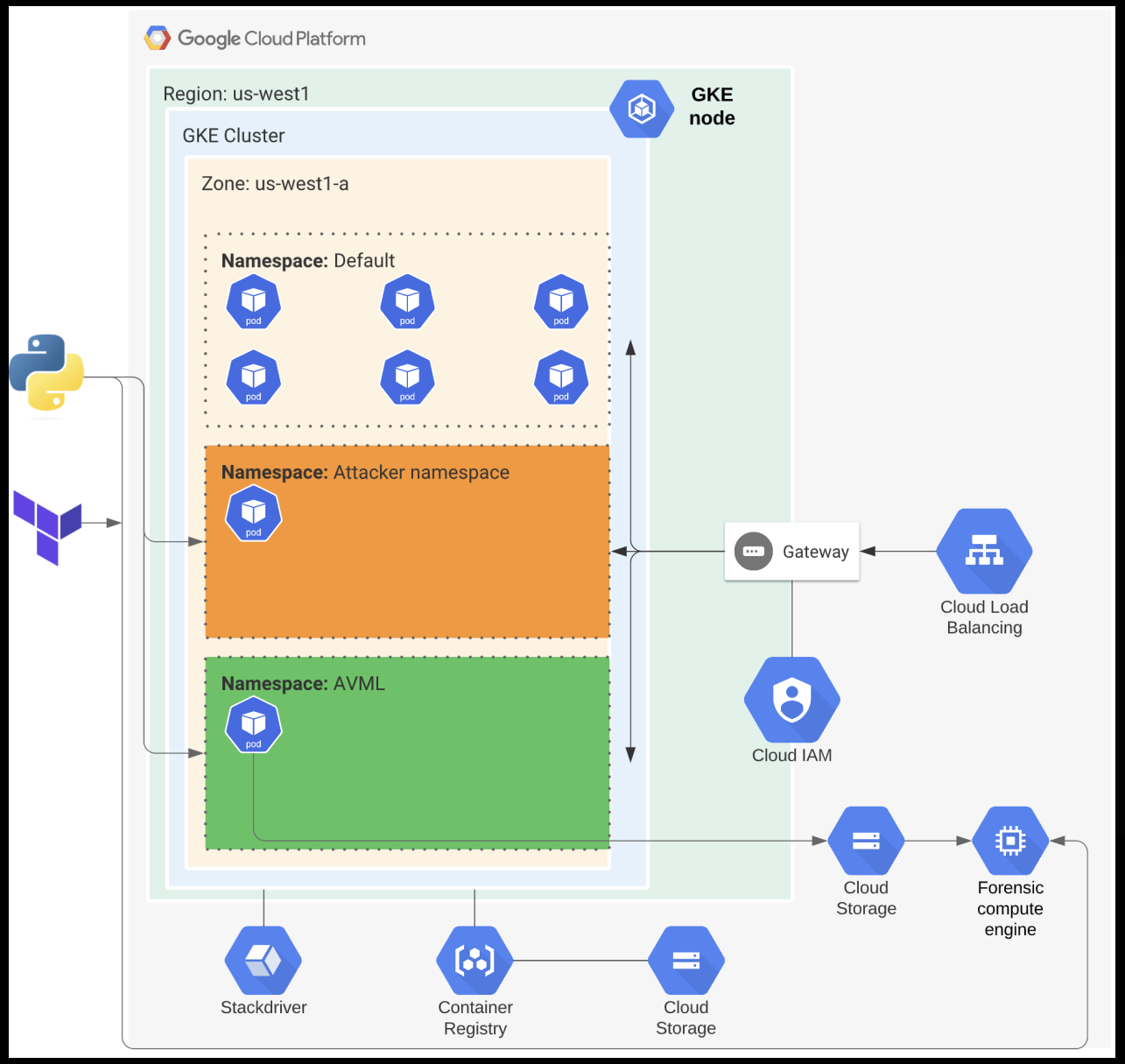
46 Contributors | 83 Used by | 2k Stars | 321 Forks

National Cyber Security Centre
a part of GCHQ

SANS

Testing setup

CYBERTHREAT 2023



National Cyber Security Centre
a part of GCHQ

SANS

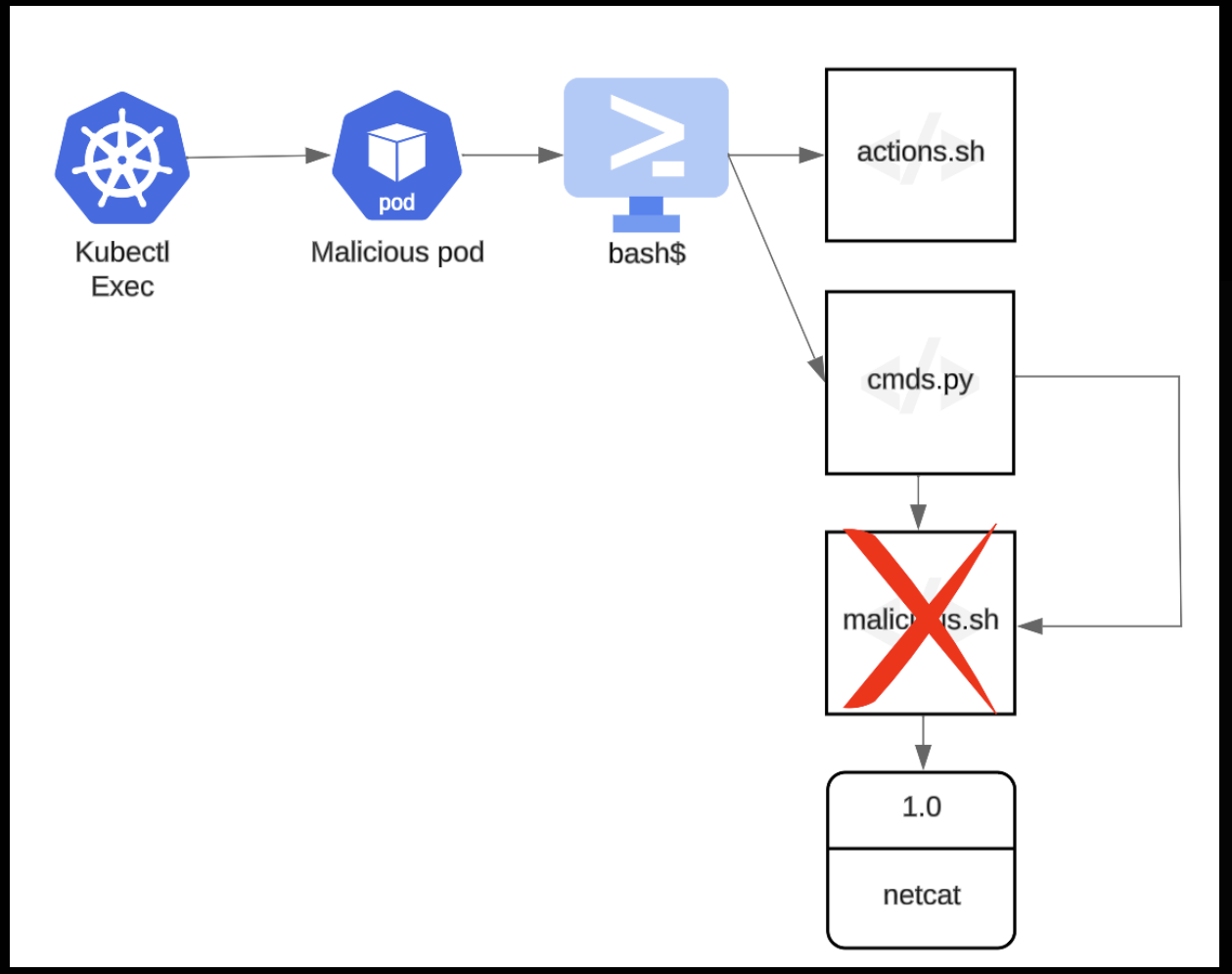
Test and analysis

CYBERTHREAT 2023

What we tested

- Various commands using bash
  - Running processes
  - Checking external IP address
  - Running scripts

- Started processes
  - Netcat
  - Python3
  - Bash shell script

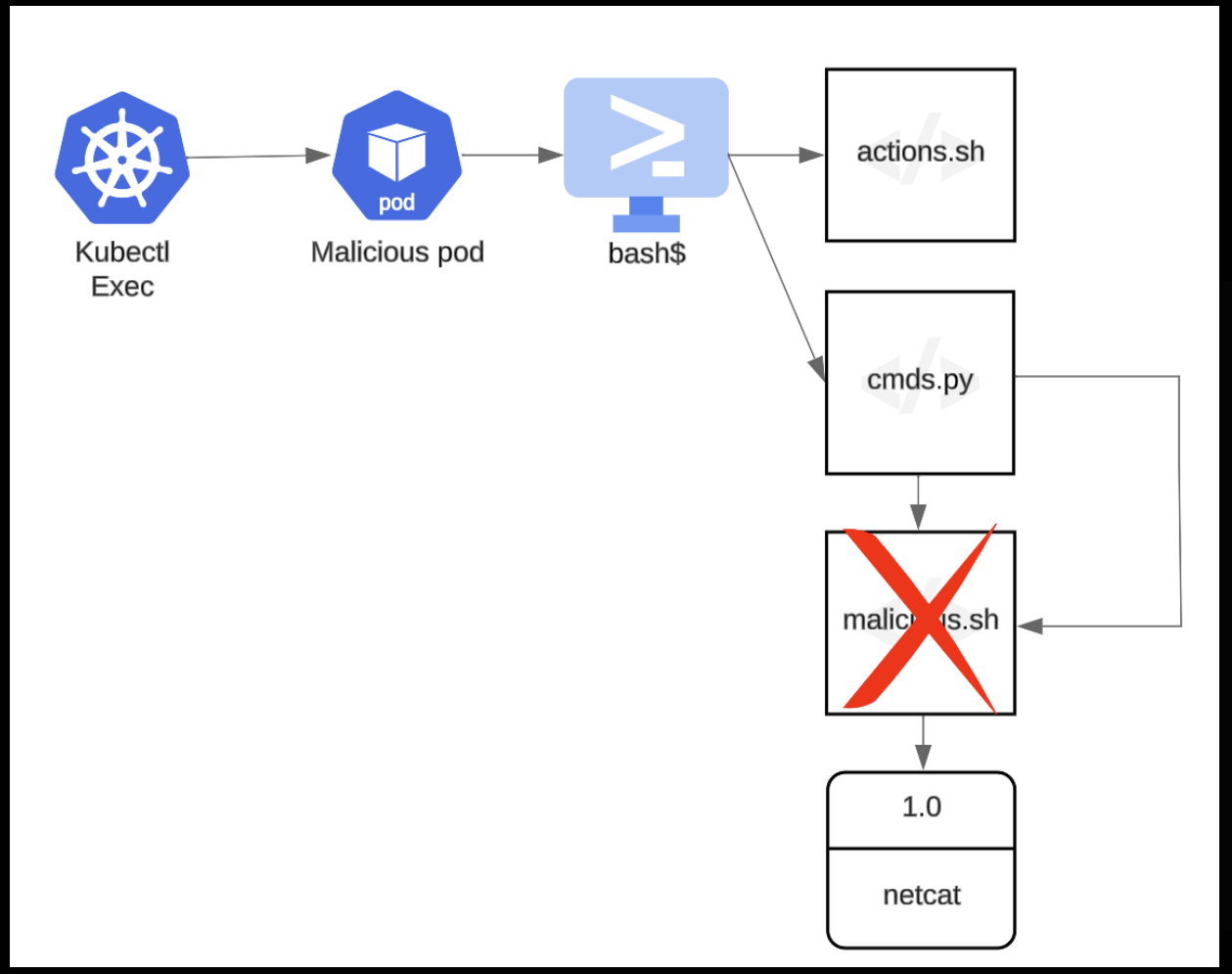


National Cyber Security Centre
a part of GCHQ

SANS

CYBERTHREAT 2023

What can we see from the GKE memory dump?



National Cyber Security Centre
a part of GCHQ

SANS

CYBERTHREAT 2023

PID	Process	CommandTime	Command
82141	bash	2023-11-16 12:33:43.000000	ls -la /proc/
82141	bash	2023-11-16 12:33:43.000000	unshare -Urm
82141	bash	2023-11-16 12:33:43.000000	echo $SHELL
82141	bash	2023-11-16 12:33:43.000000	cat /proc/1/cgroup
82141	bash	2023-11-16 12:33:43.000000	HISTFILE=~/.bash_history
82141	bash	2023-11-16 12:33:43.000000	
82141	bash	2023-11-16 12:33:43.000000	#1700138023
82141	bash	2023-11-16 12:33:43.000000	#!/bin/bash -i
82141	bash	2023-11-16 12:33:43.000000	ps aux
82141	bash	2023-11-16 12:33:43.000000	nohup watch -n1 curl -s ifconfig.co &
82141	bash	2023-11-16 12:33:43.000000	grep Cap /proc/1/status
82141	bash	2023-11-16 12:33:43.000000	set -o history
82141	bash	2023-11-16 12:33:43.000000	whoami
82141	bash	2023-11-16 12:33:43.000000	ls -la
82141	bash	2023-11-16 12:33:43.000000	history
82141	bash	2023-11-16 12:33:43.000000	./actions.sh
82141	bash	2023-11-16 12:33:43.000000	ls /root
82141	bash	2023-11-16 12:33:43.000000	pwd
82141	bash	2023-11-16 12:33:43.000000	ls -la
82141	bash	2023-11-16 12:33:43.000000	df -h
82141	bash	2023-11-16 12:33:43.000000	exit

Bash history plugin (Commands are captured in memory)

0x9e2601848fc0	58495	58495	58054	watch
0x9e2603f94ec0	58531	58531	57701	bash
0x9e2528de1f80	58687	58687	58054	python3
0x9e260ace1f80	58754	58754	58687	sh
0x9e260ace2f40	58756	58756	58754	nc
0x9e260ace5e80	58763	58763	58687	bash
0x9e25018d5e80	58839	58839	57892	avml

PSList plugin (Both container activities)

National Cyber Security Centre
a part of GCHQ

SANS

Source: https://volatility3.readthedocs.io/en/latest/volatility3.plugins.linux.html

CYBERTHREAT 2023

```
*** 0x9e2601848fc0  58495   58495   58054   watch
*** 0x9e2528de1f80  58687   58687   58054   python3
**** 0x9e260ace1f80 58754   58754   58687   sh
***** 0x9e260ace2f40    58756   58756   58754   nc
```

PSTree plugin (Attacker container)

PSaux plugin (Both container activities)

```
58054   watch   watch -n1 curl -s ifconfig.co
57701   bash    /bin/bash
58054   python3 python3 cmds.py
58687   sh  /bin/sh -c ./malicious_script.sh
58754   nc  /bin/nc -l 10514
58687   bash    [bash]
```

National Cyber Security Centre
a part of GCHQ

SANS

Lessons learned

CYBERTHREAT 2023

What have we learned?

- AVML + Dwarf2json + Volatility3
  - NodeSelector
  - Acquire vmlinux for GKE/COS using build_id
  - Be aware of updates to kernel or compiler

- Avoid overutilization
  - Cluster rebalancing - evicted
  - ContainerStatusUnknown with exit code 137

National Cyber Security Centre
a part of GCHQ

SANS

CYBERTHREAT 2023

- Get in touch
  - Tw/X: @monrava89
  - LinkedIn: in/hallbergmarcus
  - @: mhallberg@spotify.com

- Code
  - https://github.com/Monrava/cyberthreat2023

National Cyber Security Centre
a part of GCHQ

SANS