Kubernetes Security

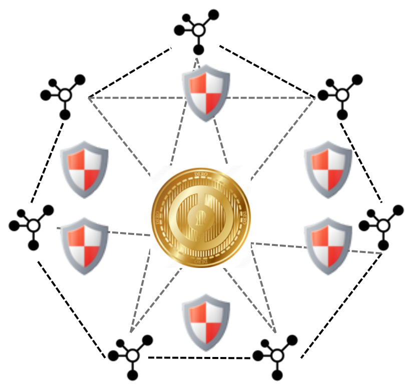
Defending Against Dero

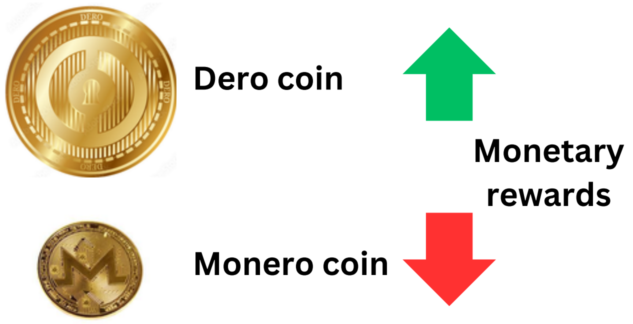
Cryptojacking is the unauthorized use of someone else's computing resources to mine cryptocurrencies, leading to resource drain and potential financial losses for organizations.

Target Device — **Malware Infection** — **Resource Hijack** — **Cryptocurrency Mining** — **Stolen Profits**

Decentralized Cryptocurrency Revolution

- Defending Your Assets
- Privacy and Security
- Foundation for Decentralization
- Strengthening Security

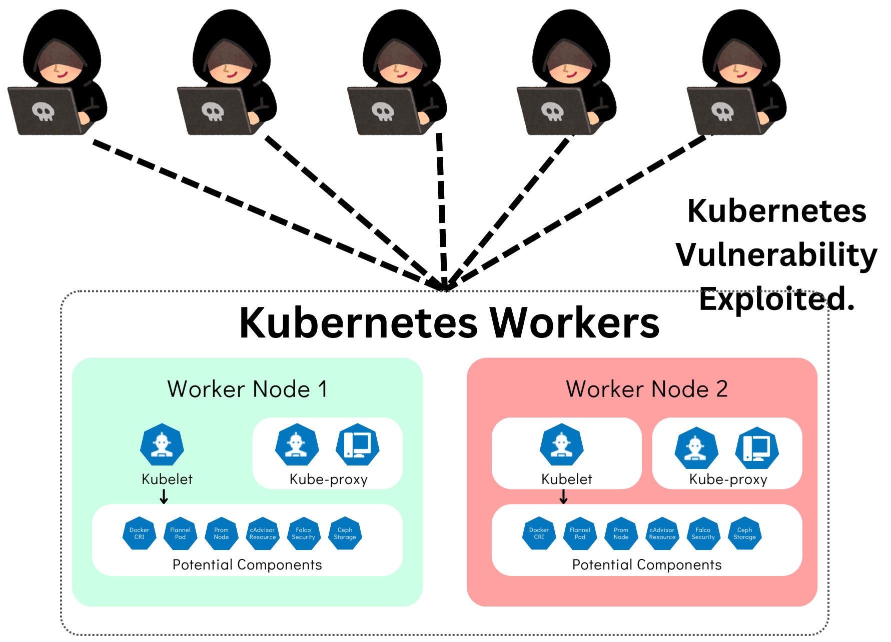




Dero, a pioneering digital currency, prioritizes privacy and security with its advanced Directed Acyclic Graph (DAG) technology.

Experience higher rewards and enhanced anonymity compared to traditional cryptocurrencies like Monero.

Kubernetes Vulnerability Exploited



secure and not vulnerable

vulnerable to exploitation.

CrowdStrike uncovers the first-ever Dero cryptojacking operation targeting Kubernetes.

CrowdStrike has been constantly observing the Dero cryptojacking operation since February 2023. The operation targets Kubernetes clusters with anonymous access enabled on the API and listens on non-standard ports. The modified Monero campaign also competes with the Dero campaign.

CROWDSTRIKE →

Cryptojacking Target

Impact of the Attack

Increase in Cryptojacking Incidents

2021	**51.1 million**	↑	**23% from 2020**
2022	**140 million**	↑	**43% from 2021**

Resource Drain — **Resource Drain** — **Performance Hit** — **Financial Loss**

Protection Strategies

- ✓ Disable anonymous access to the Kubernetes control plane API.
- ✓ Regularly review and improve configurations.
- ✓ Install Antivirus and Malware Protection Software
- ✓ Monitor for suspicious activity and unauthorized pods.
- ✓ Educate users about cryptojacking risks.
- ✓ Use Ad Blockers in Your Browser