redlure

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

> whoami

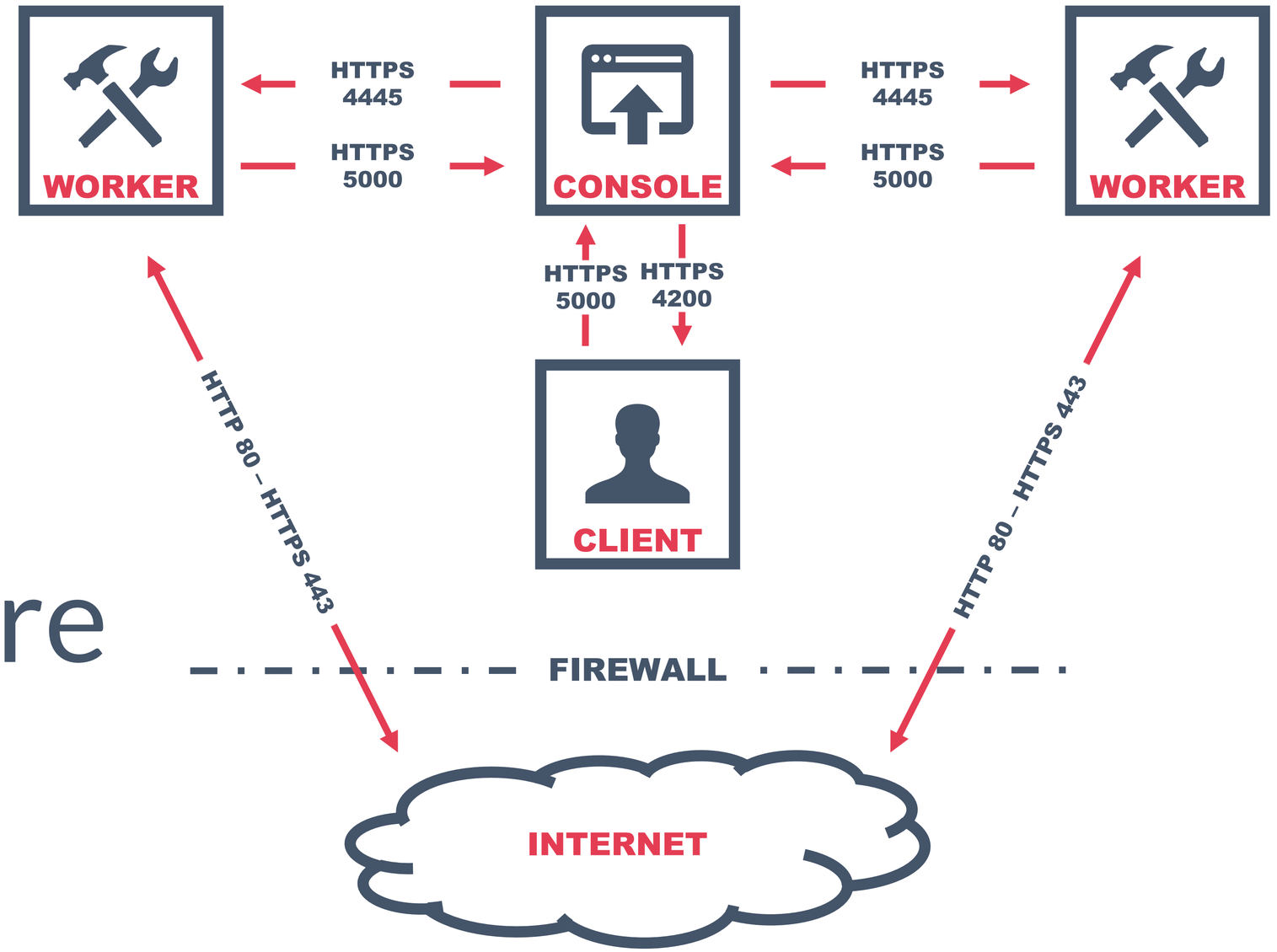
- Senior Cybersecuity Analyst
- Penetration testing
- Offensive tooling
- Digital forensics/incident response

… Phishing

> what is redlure?

- Manage campaigns in parallel
- Chain templated webpages together
- Scale up/down quickly
- Centralize management
- Sensitive data encryption
- Integrate payload delivery
- Improve metrics

> redlure architecture




ENOUGH TALKING!
SHOW ME A DEMO!!
imgflip.com

> todo

- Relay emails through workers
- Dynamic webpages/scenarios based on visiting user-agent
- Redirect specified IPs associated with defensive products
- Delayed weaponization of hosted payload
- Bypass Office365 Safe Links (if this is still a thing…)

> Questions?

https://github.com/redlure
https://schneiderdowns.com/redlure

Contact Info:

- mcreel@schneiderdowns.com
- Twitter: @Tw1sm
- https://schneiderdowns.com/cybersecurity