Metasploit Minus Metasploit

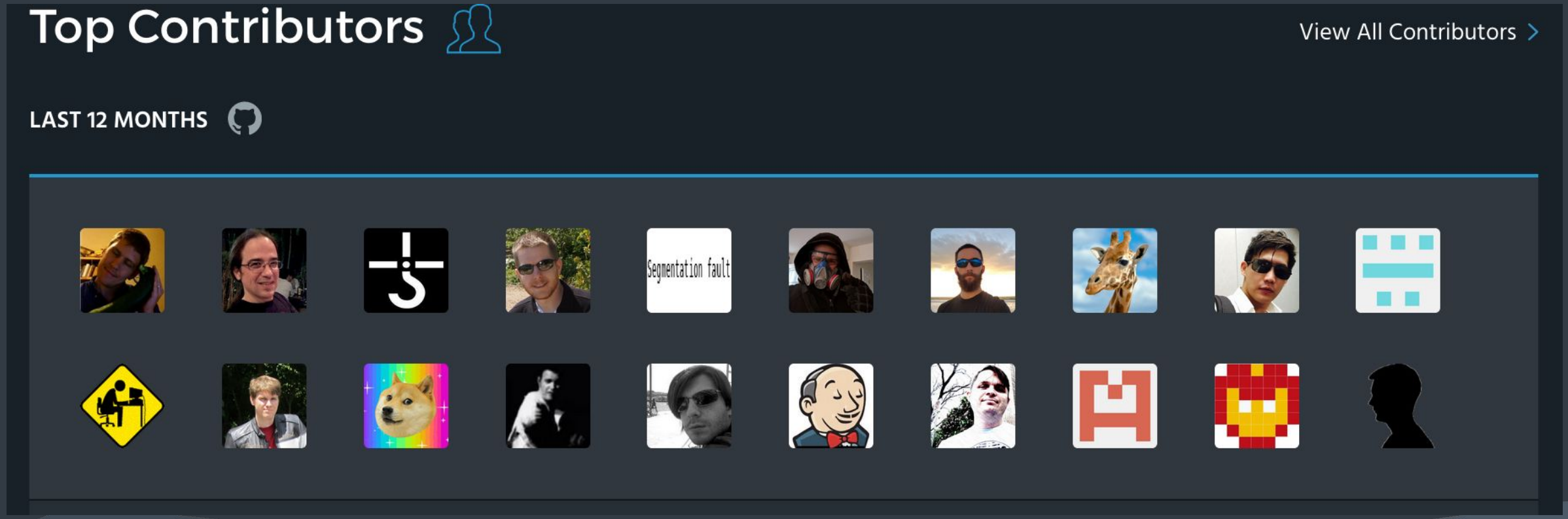
Building APIs and abstractions for the future

Adam Cammack and James Barnett

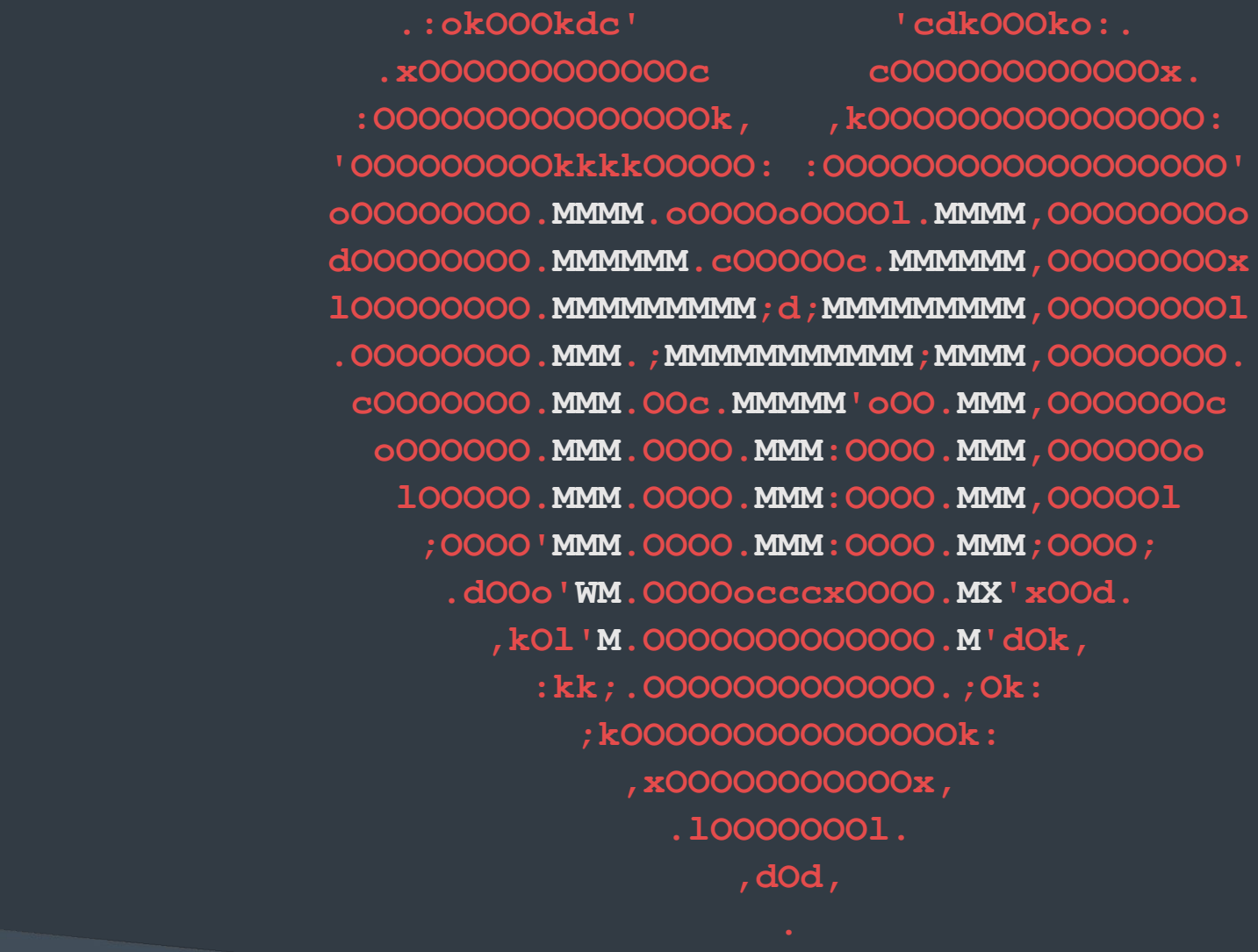
RAPID7

Who We Are

- Engineers on the Metasploit team
- Made possible by our awesome community



msf5 > banner

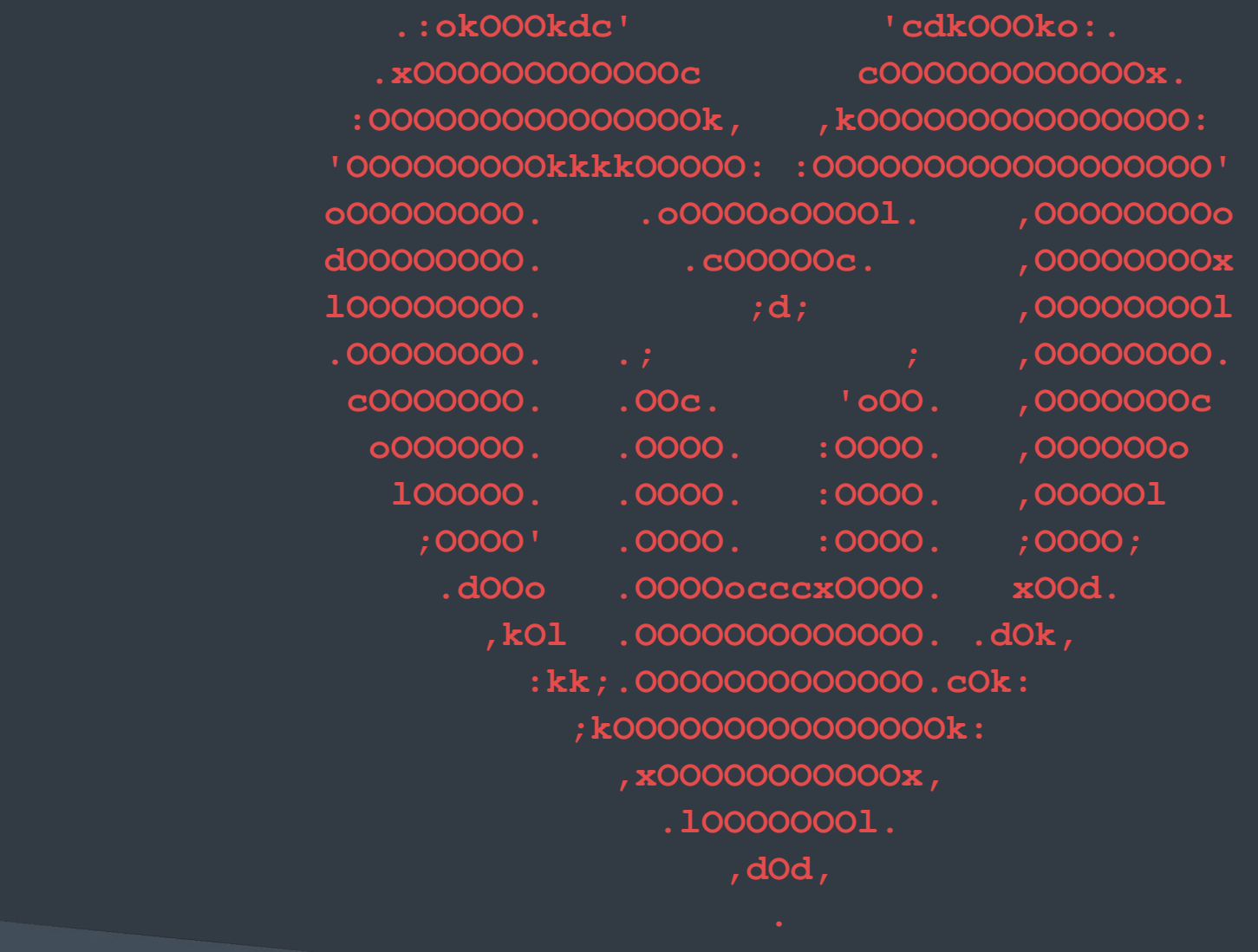


RAPID7

msf5 > banner

RAPID7

msf5 > banner



RAPID7

Be Flexible

Handle ALL the Cases

- Different types of tasks
  - Scanning
  - Exploiting
  - Post-exploit gathering
- Network traffic should be re-routable
- Exploit traffic should be malleable
- Payloads should support transformations

Separate Modules and Payloads

- Modules should only know enough to trigger the exploit
- Maintain a wide library of payloads
- C2 for a wide library of payloads
- Large number of module/payload combinations

Current Architecture

Everything Touches the DB

- Very Rails-oriented
- Tightly coupled to the database
- ONE MSF per database
- Searching and filtering haphazardly organized

Modules Are Plugins

- Read into memory, modified, and eval'd
- Loaded multiple times at startup
- Everything executes in the context of everything else
- Shared functionality via mixins
- And then there's the datastore…

Networking Is Complicated

- All listeners go through the switch board
- Pivoting through sessions and proxies
- Socket, service, and client abstractions
- Ring buffers for sessions

Isolating Modules

Modules as Processes

- Enhanced isolation
- Parallelism
- Support for any language

Modules as Processes

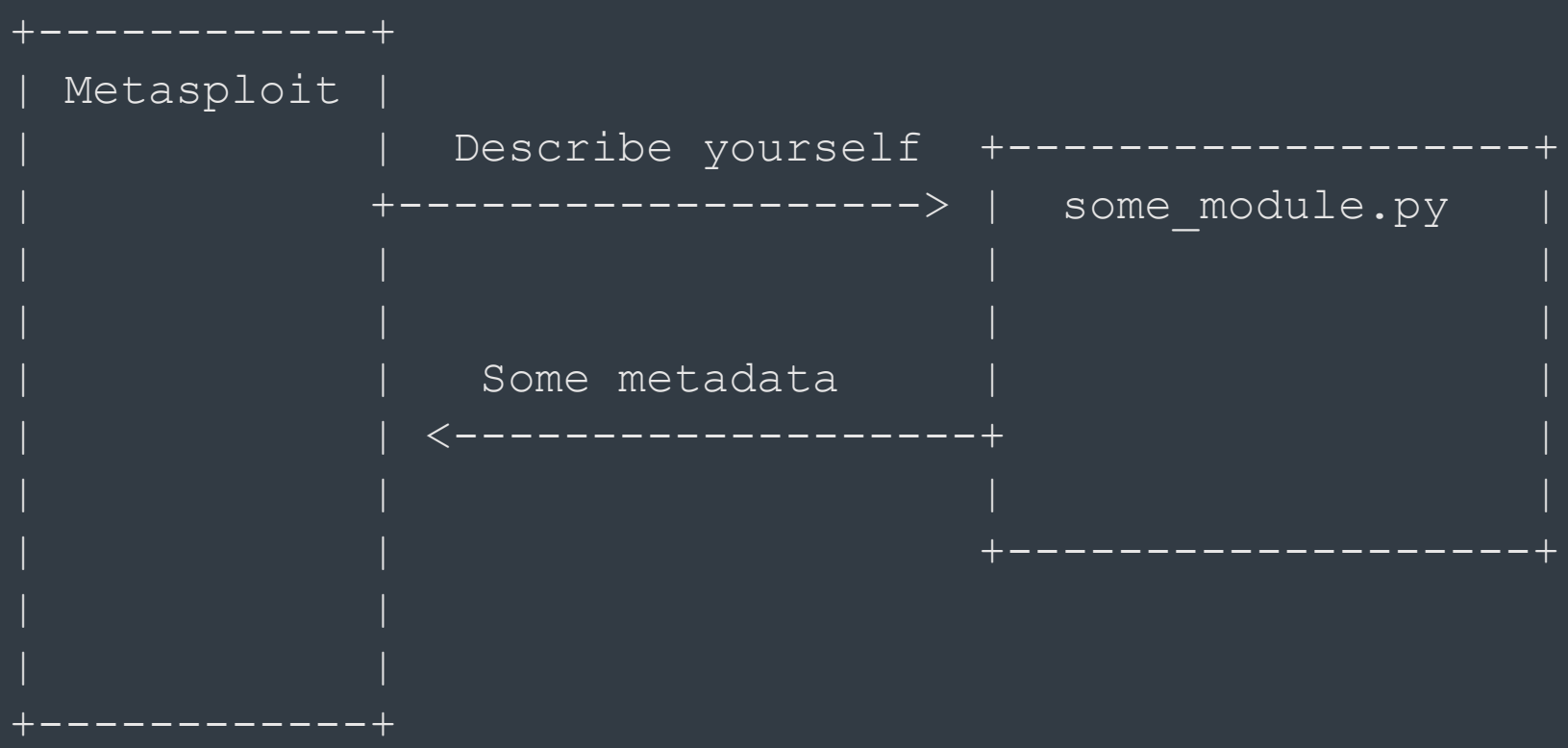
Full Isolation

- OS process per task
- Communicates via JSON over stdin/stdout
- Network transparency

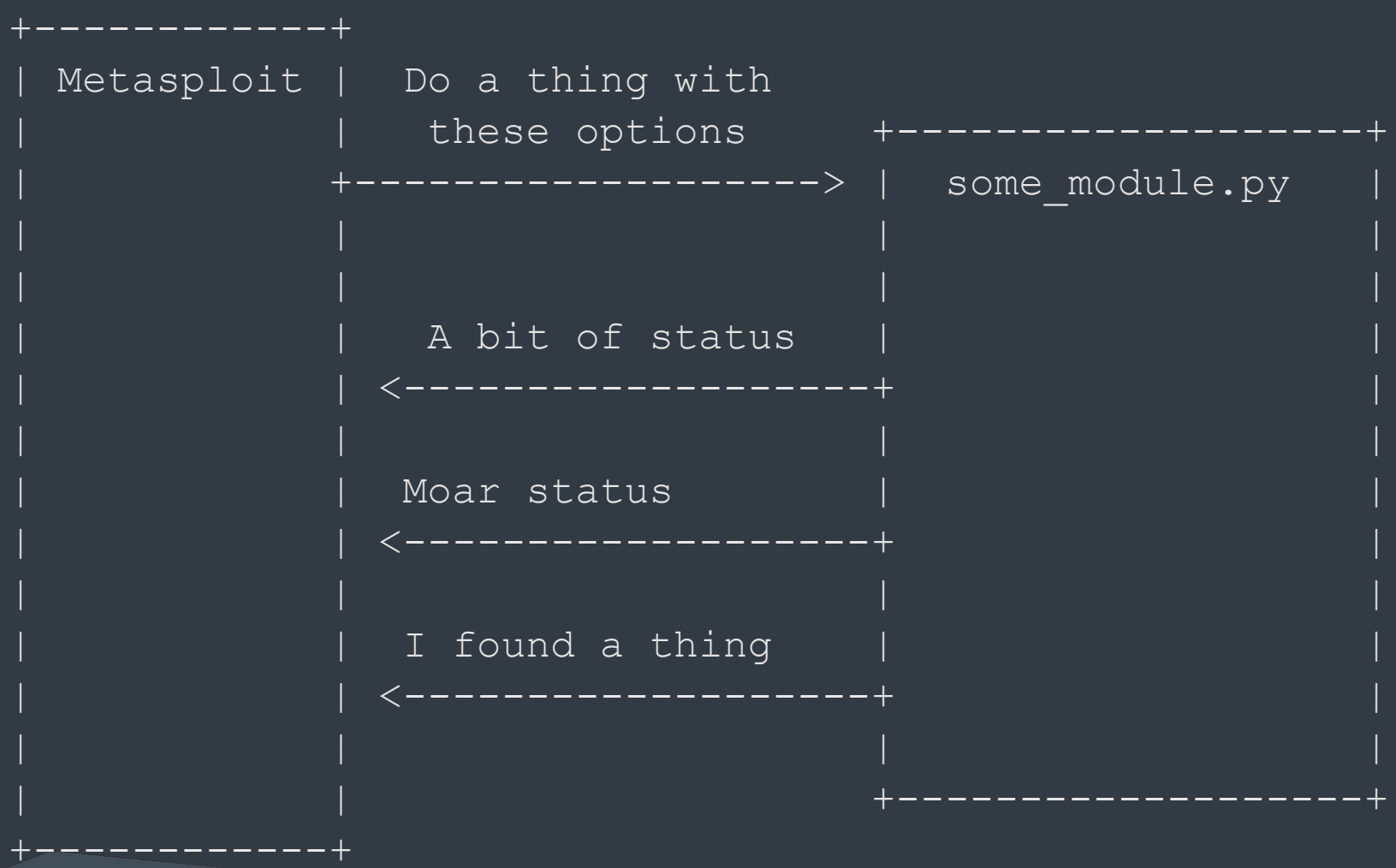
Better Performance

- Separate file descriptor pool
- Separate memory space
- No GIL - separate
- Horizontal scaling

How it Works


Metasploit
Describe yourself
some_module.py
Some metadata

How it Works



Isolating Data Storage

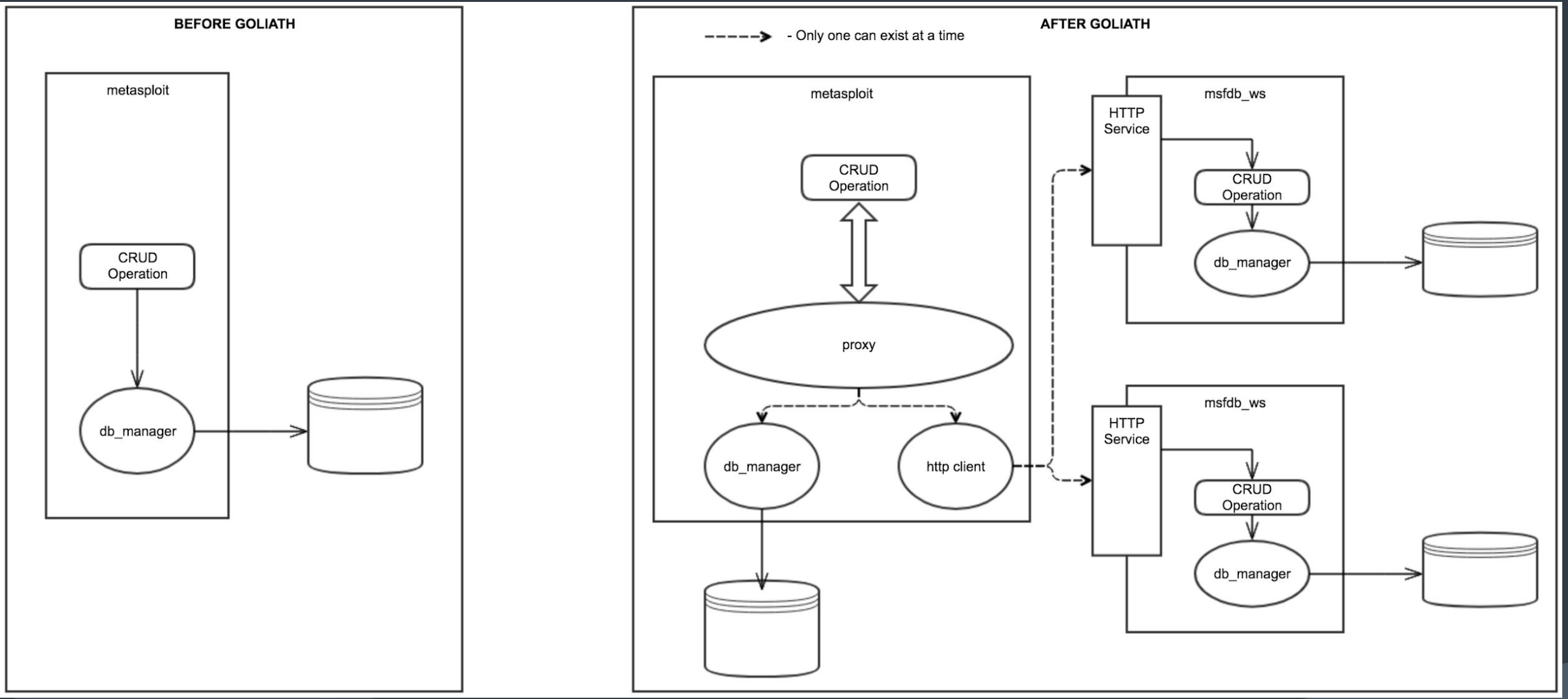
Objectives of Project Goliath

- Make the Metasploit datastore portable
- Improve the data model
- Make sessions shareable

Datastore As a Service

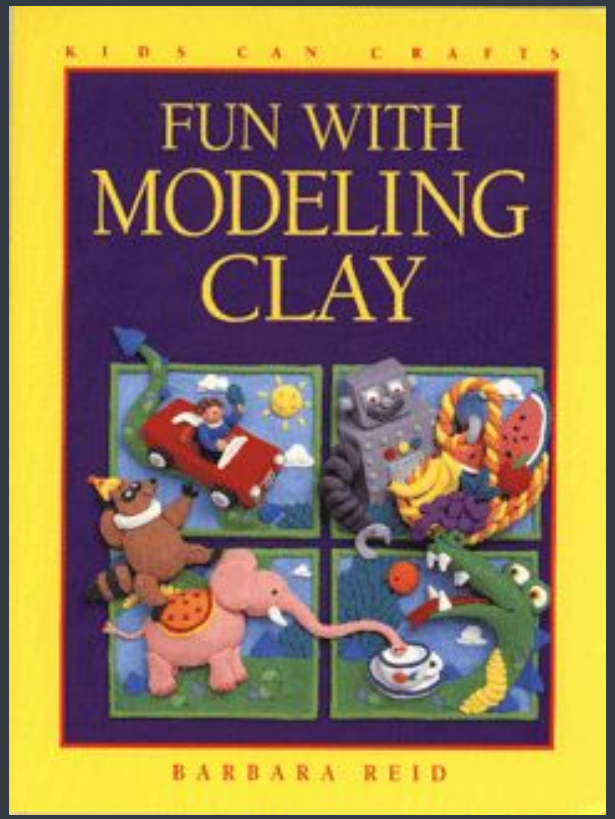
- Collaborate with others
- Host data store anywhere
- Integrate with other tools

Architecture



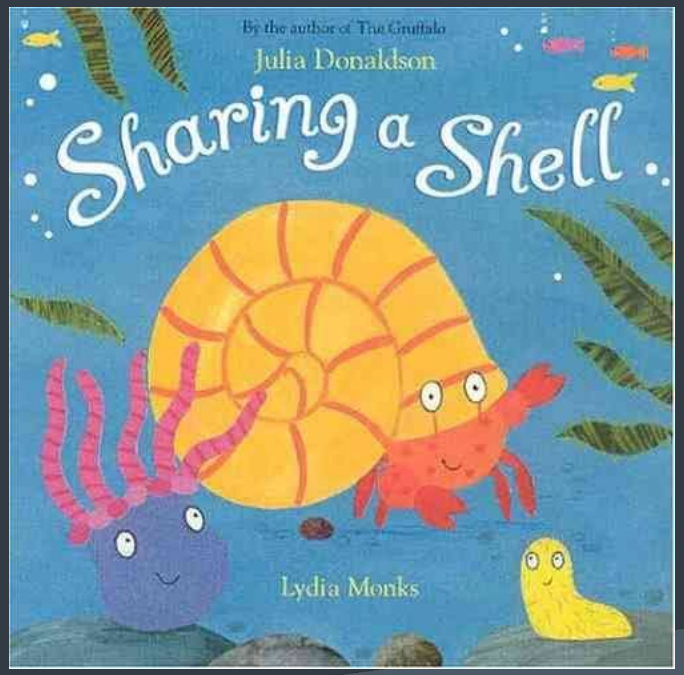
Data Model Improvements

- Flexibility
- Searchability
- Re-usability



Session Sharing

- Separate session management from framework
- Share sessions among team members
- Host session manager in the cloud



RAPID7

Demo

RAPID7

Questions?

https://blog.rapid7.com/2017/12/28/regifting-python-in-metasploit/
https://www.metasploit.com
https://github.com/rapid7/metasploit-framework
http://garfieldminusgarfield.net

RAPID7