BUILDING YOUR OWN DFIR SIDEKICK

CHATOPS FOR INCIDENT RESPONSE

HI, I'M SCOTT

I DO INCIDENT RESPONSE @ GitHub

THIS IS HUBOT

HE DOES BASICALLY EVERYTHING

@

GitHub

"MAKING IT EASIER TO WORK TOGETHER THAN TO WORK ALONE...."

- CHATOPS & INCIDENT RESPONSE
- HUBOT VARIABLE THREAT RESPONSE
- DEPLOYING & DEVELOPING HUBOT

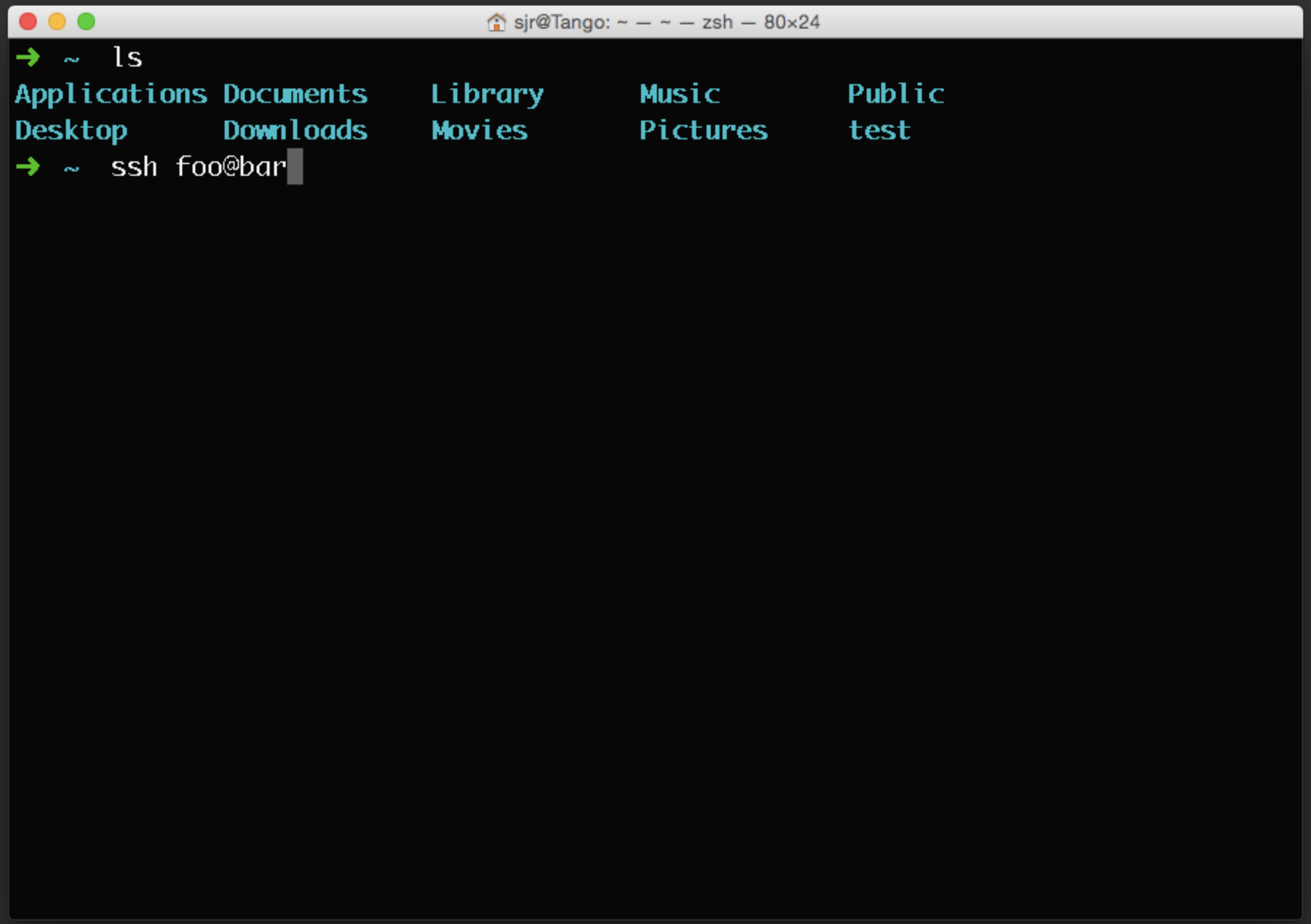
A BRIEF INTRODUCTION TO CHATOPS

WHAT IS CHATOPS?!

DEVOPS + CHAT = CHATOPS

COLLABORATIVE TERMINAL EXPERIENCE

SO WHAT REALLY IS CHATOPS?!


sjr@Tango: ~ — ~ — zsh — 80×24
➜ ~ ls
Applications Documents Library Music Public
Desktop Downloads Movies Pictures test
➜ ~ ssh foo@bar


MARIO
000000
×00
WORLD
1-1
TIME
SUPER
MARIO BROS.
©1985 NINTENDO
1 PLAYER GAME
2 PLAYER GAME
TOP- 000000

technicalpickles commented on Oct 18, 2013 — Collaborator

Looks like test/hello-world_test.coffee was copied from https://github.com/hubot-scripts/hubot-example/blob/master/test/hello-world_test.coffee . I don't expect this would work (but script/test should confirm), so may as well remove it.

technicalpickles commented on an outdated diff on Oct 18, 2013 — Show outdated diff

technicalpickles commented on an outdated diff on Oct 18, 2013 — Show outdated diff

technicalpickles commented on an outdated diff on Oct 18, 2013 — Show outdated diff

sroberts added some commits on Nov 9, 2013

- `Added index.coffee per PR comments` d0c6fd7
- `Made package.json name and description a bit more logical` a5b4203
- `Removed sample test` bf25967

sroberts commented on Nov 11, 2013 — Owner

@technicalpickles Alright, I think I'm more up to date. Hows this look?

I'm also wondering what the best way to DL those community scripts is. Do you have a better idea than that shell script?

technoskald commented on Nov 11, 2013 — Collaborator

I'm not the Git expert you two are, but with the new structure of the Hubot community script repo, can't you just add the ones you like as subtrees or summat?

Labels
None yet

Milestone
No milestone

Assignee
No one—assign yourself

Notifications
Unsubscribe
You're receiving notifications because you modified the open/close state.

3 participants

Lock pull request

Ops - Need urgent attention? See `/help`.

9:18 AM

/gpanel chassis reboot [redacted] magic_word=[redacted]

Hubot 9:18 AM

```
Host deployed: [redacted].github.net
Chassis state: installed
Rebooting [redacted]
```

[gPanel] booting Dell Inc. PowerEdge [redacted] into installed...

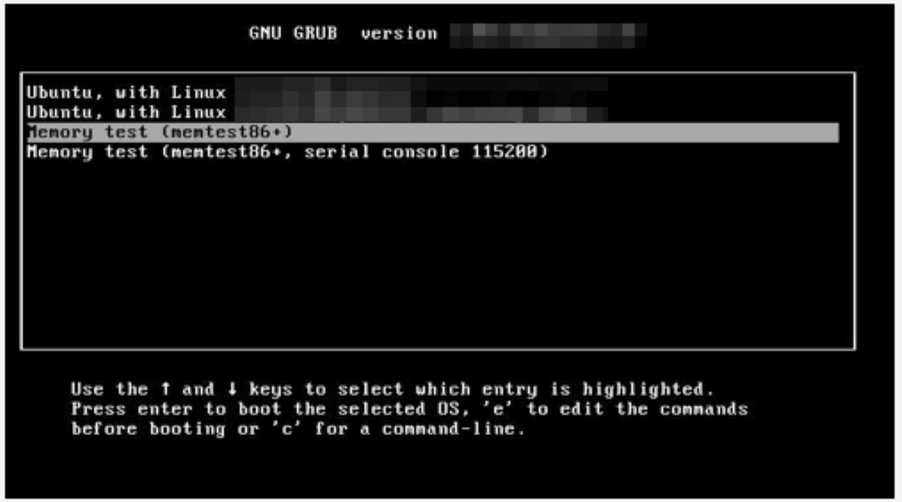
Hubot 9:25 AM

[gPanel] booting Dell Inc. PowerEdge [redacted] into installed...

9:31 AM

/drac me [redacted]

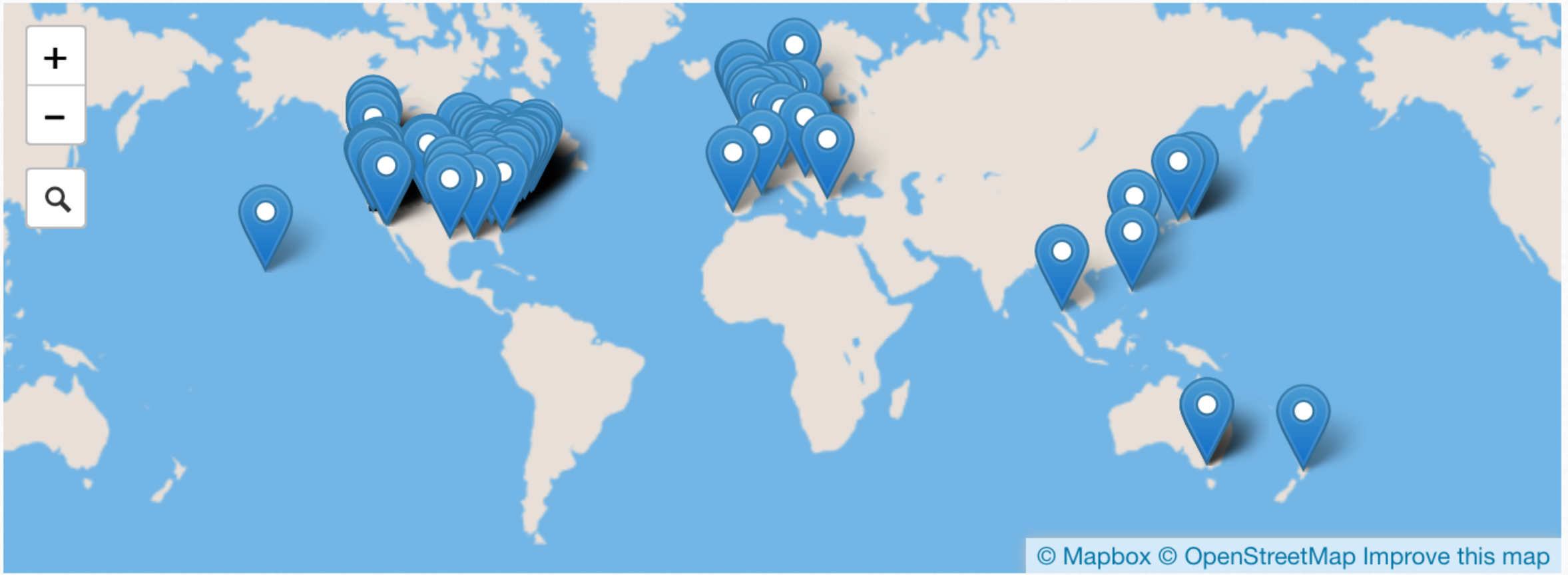
Hubot 9:31 AM



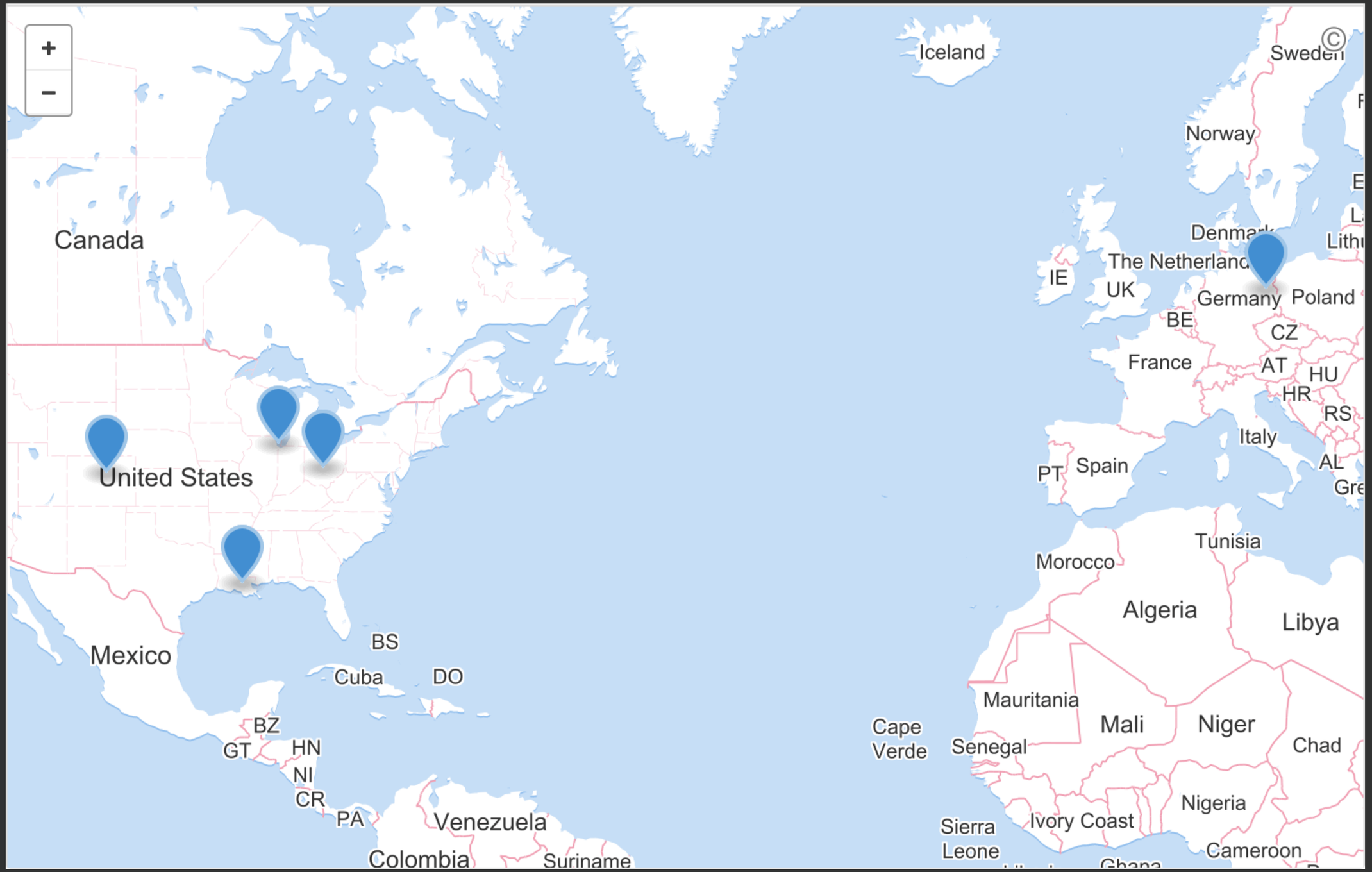

Group 3
0.00 / 416.81
Unclefrank
Health 4724 / 4724
Mana 5998 / 5998
Magmadar
MT Targets
Magmadar
Shokr
Magmadar
Shadospectr...
Determined's Target
Demon Armor
23 minutes
Touch of Shadow
15 minutes
Arcane Brilliance
53 minutes
Prayer of Fortitude
54 minutes
Prayer of Spirit
54 minutes
Gift of the Wild
56 minutes
Magmadar Cavern
Pigglywiggly
Newone
Pootypoo
Amblix
trade with me for one
Sergeant Smellysocks
Scout Timebomb
<Overwhelm>
Stone Guard Cosmosis
Sergeant Arrogance
Sergeant Dralath
<Overwhelm>
Champion Poomanchu
<Overwhelm>
Legionnaire Rexy
<Overwhelm>
Senior Sergeant Diobolique
<Overwhelm>
Grunt Gbonez
<Overwhelm>
Group 1
Shokr
Shadospectre
Hause
Gragan
Bigugly
Group 2
Belinack
Therealoxy
Delamis
Azarot
Sathia
Group 3
Pigglywiggly
Newone
Pootypoo
Amblix
Unclefrank
Group 4
Draloth
Tornak
Smellysocks
Timebomb
Keppo
Group 5
Cosmosis
Taedis
Delnar
Gbonez
Undedfred
Group 6
Diobolique
Melanoma
Icewater
Gbone
OFFLINE
Group 7
Kuruption
Uncleturkey
Determined
Jhonkau
Arrogance
Group 8
Poomanchu
Vyri
Rexy
Narcisa
User
Traveler's Backp...
Traveler's Backp...
Backpack
Sergeant Tornak
<Overwhelm>
Newone gains 424 Mana from Newone's Life Tap.
Pootypoo gains 509 Mana from Pootypoo's Life Tap.
[Raid] [Poomanchu]: np
[Raid] [Icewater]: Im in teh secksy group!
[Raid] [Sathia]: got it bel! look sexy guys!
[Azarot] says: oh i forgot i got 4 [Major Mana Potion]
[Raid] [Poomanchu]: im frapsing this to show people how to play a shaman correctly
[Azarot] says: trade with me for one
Magmadar
Level ?? Beast (Boss)
Warsong Outriders 13 / 6000

WHY CHATOPS ANYWAY?

GEOGRAPHICALLY DISTRIBUTED



237 hubbers are spread across **94 cities** right now


+
−
Iceland
Sweden
Norway
Canada
Denmark
The Netherlands
IE
UK
Germany
Poland
BE
CZ
France
AT
HU
HR
RS
Italy
PT
Spain
AL
Tunisia
Morocco
Algeria
Libya
United States
BS
Cuba
DO
Mexico
Mauritania
Mali
Niger
Chad
Cape Verde
Senegal
BZ
GT
HN
NI
CR
PA
Venezuela
Colombia
Suriname
Nigeria
Ivory Coast
Sierra Leone
Cameroon
Ghana

ASYNCHRONOUS

MULTI DEVICE

github: The Danger Room

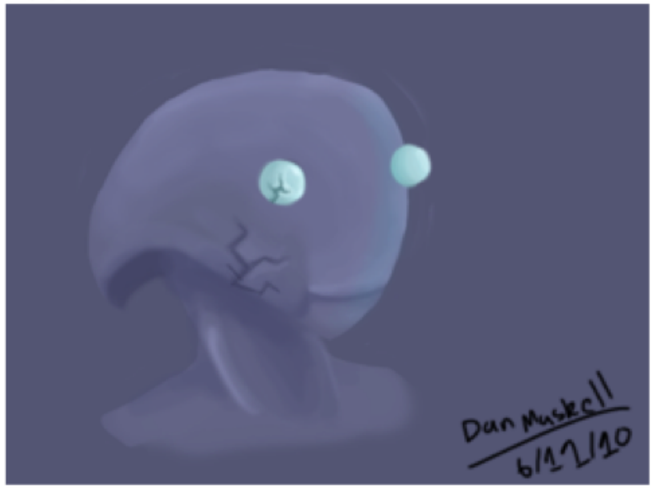
The Danger Room GitHub has tidy little bit of GUI

Hubot convert 1 gallon to liters

Hubot
: 3.78541178 liters

Hubot image me robawt

Hubot



hubot tell me the rules

Hubot
1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.

2. A robot must obey any orders given to it by human beings, except where such orders would conflict with the First Law.

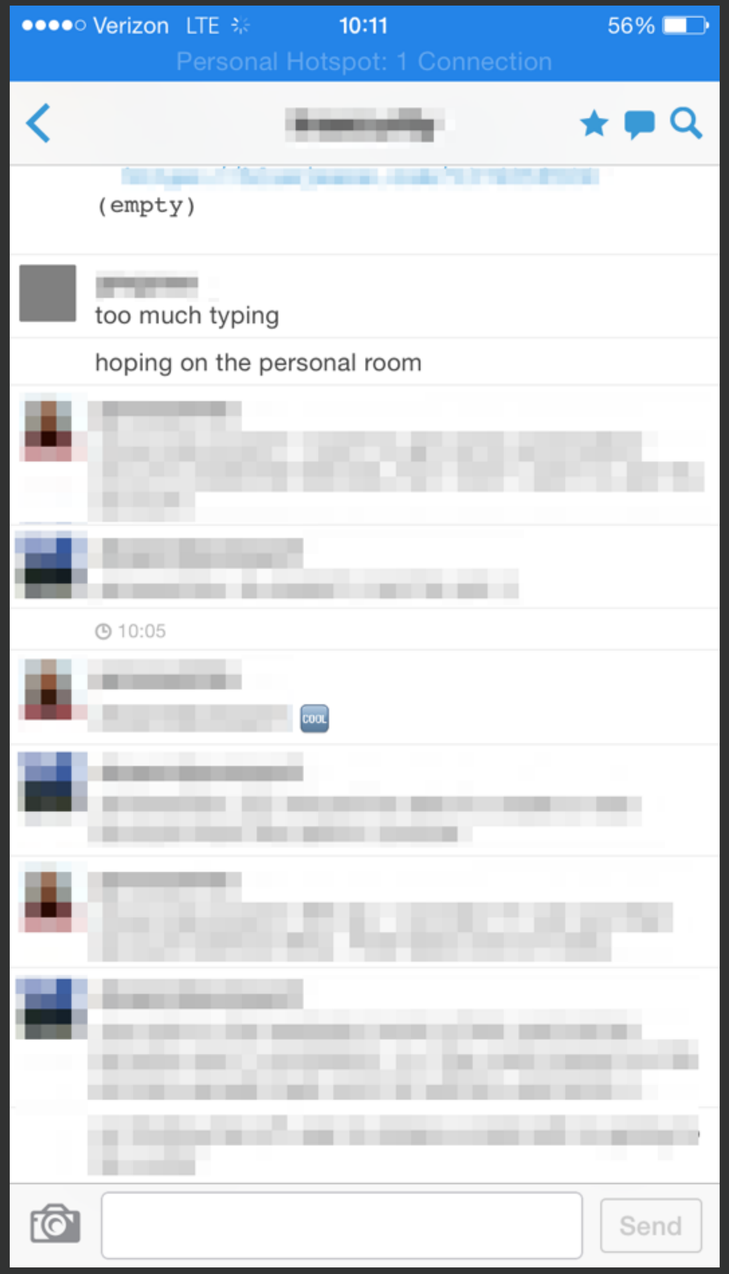
3. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.

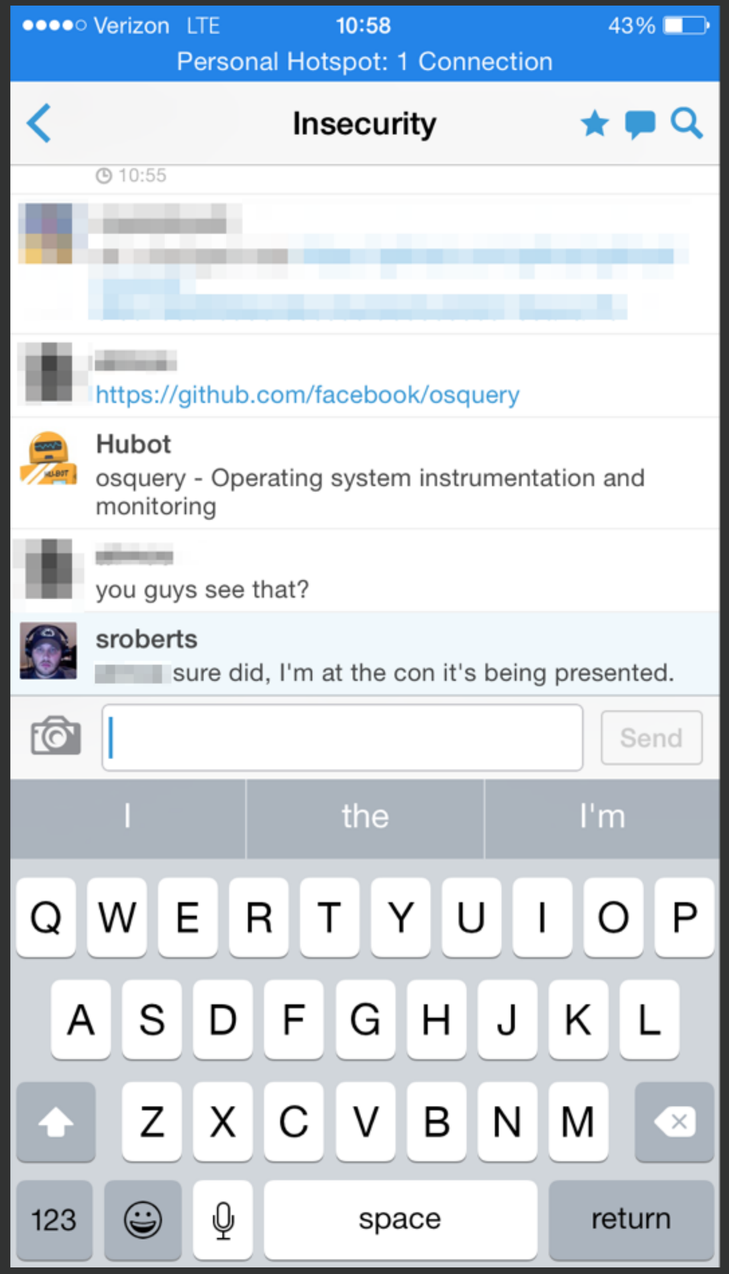
Who's Here?

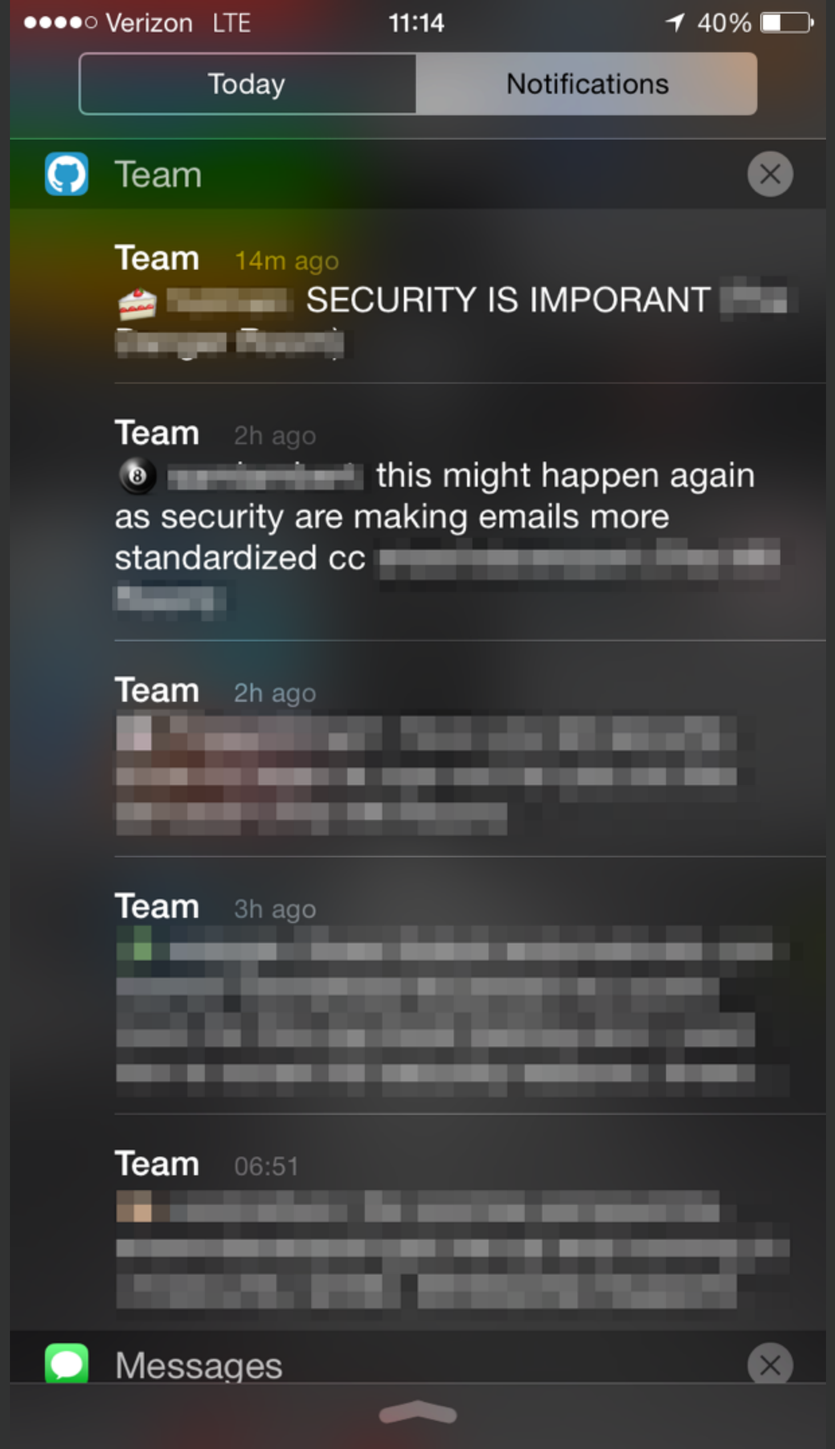
Latest Documents

- 899 Pine St San...
- image.jpg
- Screen shot 20...
- Photo on 2011...
- VISION Consulti...

The Danger Room


Verizon LTE 10:11 56%
Personal Hotspot: 1 Connection
(empty)
too much typing
hoping on the personal room
10:05
Send


Verizon LTE 10:58 43%
Personal Hotspot: 1 Connection
Insecurity
10:55
https://github.com/facebook/osquery
Hubot
osquery - Operating system instrumentation and monitoring
you guys see that?
sroberts
sure did, I'm at the con it's being presented.
Send
I
the
I'm
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
return


●●●●○ Verizon LTE
11:14
40%
Today
Notifications
Team
Team 14m ago
SECURITY IS IMPORANT
Team 2h ago
this might happen again as security are making emails more standardized cc
Team 2h ago
Team 3h ago
Team 06:51
Messages

HIDES THE "UGLY"

OR AT LEAST MAKES INTERFACES CONSISTENT

"THIS WAS ALWAYS MY MAIN MOTIVATION WITH HUBOT - TEACHING BY DOING BY MAKING THINGS VISIBLE."

-

@TOMAYKO

HOW GITHUB USES CHATOPS

DEPLOY
+
MONITOR SERVERS

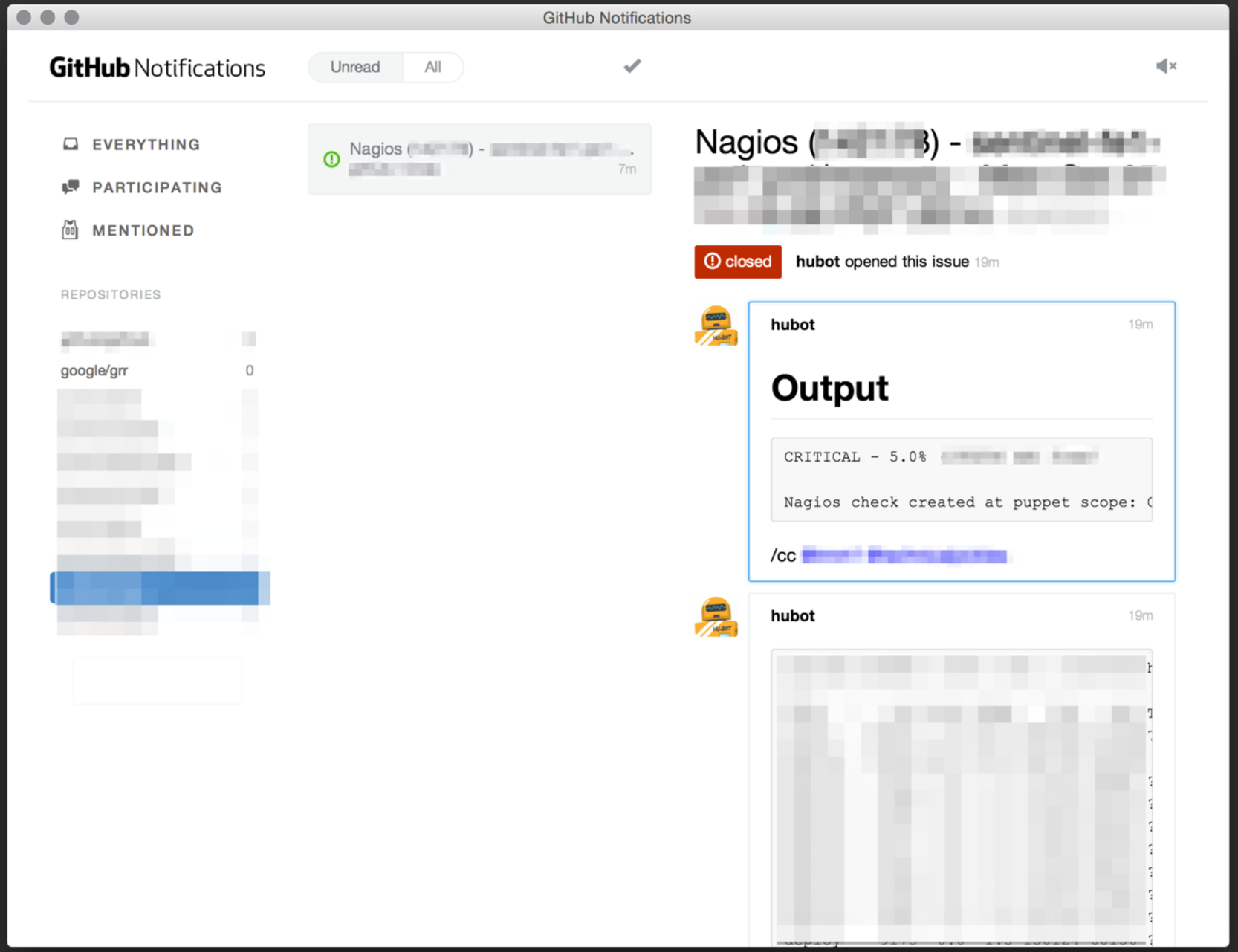
VIA PUPPET

DEPLOY
+
MONITOR CODE

VIA CAPISTRANO + JENKINS CI

MONITOR SYSTEMS

VIA NAGIOS


GitHub Notifications
GitHub Notifications
Unread
All
EVERYTHING
PARTICIPATING
MENTIONED
REPOSITORIES
google/grr
0
Nagios (
) -
7m
Nagios (
) -
closed
hubot opened this issue 19m
hubot
19m
Output
CRITICAL - 5.0%
Nagios check created at puppet scope:
/cc
hubot
19m

GitHub, Inc. github.com/hubot

Search GitHub | Explore | Gist | Blog | Help | sroberts

hubot

Joined on Nov 14, 2010

87 Followers | **0** Starred | **0** Following

Contributions | Repositories | Public activity

Follow

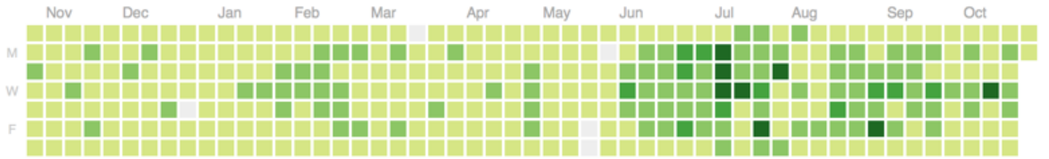
Popular repositories

Spoon-Knife
This repo is for demonstration purposes ... 1 ★

Repositories contributed to

github/developer.github.com
GitHub Developer site 710 ★

Contributions



Summary of Pull Requests, issues opened, and commits. Learn more.

Less More

Year of contributions	Longest streak	Current streak
17,898 total	154 days	154 days
Oct 27, 2013 – Oct 27, 2014	May 27 – October 27	May 27 – October 27

Contribution activity

Period: **1 week**

28 commits

UPDATE OUR STATUS SITE

(HOPEFULLY RARELY)

LOOKUP FUNNY PICTURES

AND GIFS TOO!

08:47 **kylemxl** it is indeed a morning.

08:48 **sroberts** ! img me wednesday morning

08:48 **woodhouse** http://www.desicomments.com/dc2/03/189130/189130.gif (54KB)

Slack

STARRED

security_at_scale

CHANNELS

+11 more...

DIRECT MESSAGES

+12 More...

PRIVATE GROUPS

+2 more...

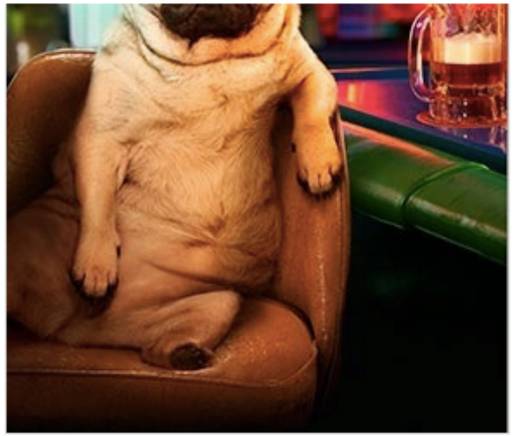
sroberts

online

#general

Search

27



10:07 http://25.media.tumblr.com/tumblr_mcmthlSKeN1r0wqrdo1_500.gif (499KB)

SHOUTOUT TO MATTJAY

SO WHAT ABOUT DFIR?!

HINT: WE WERE ALREADY DOING IT

MANAGING OUR PAGER ALERTS

VIA PAGERDUTY

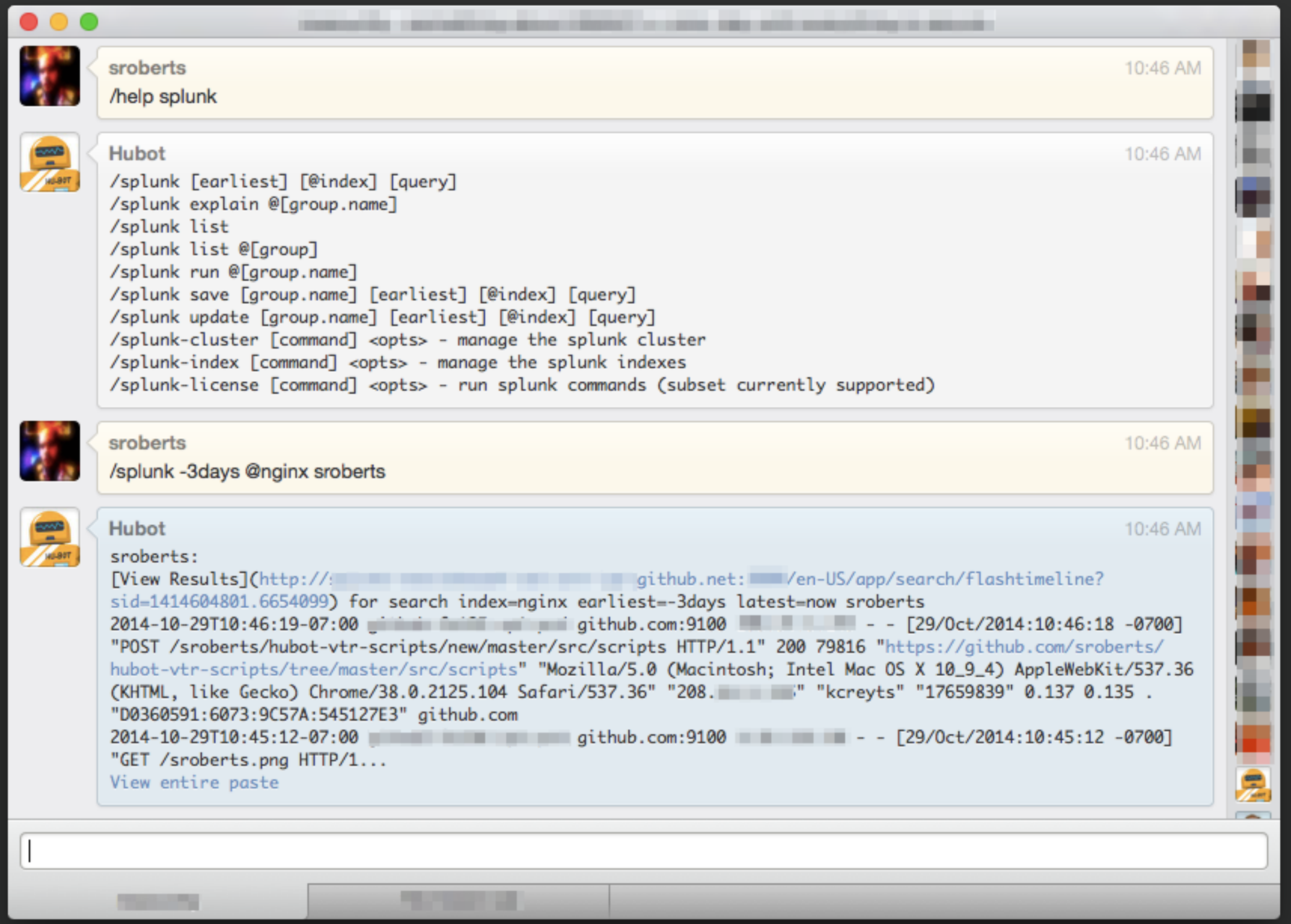
SHOWING PROCESS LISTS ON HOSTS

CHANGING FIREWALL RULES

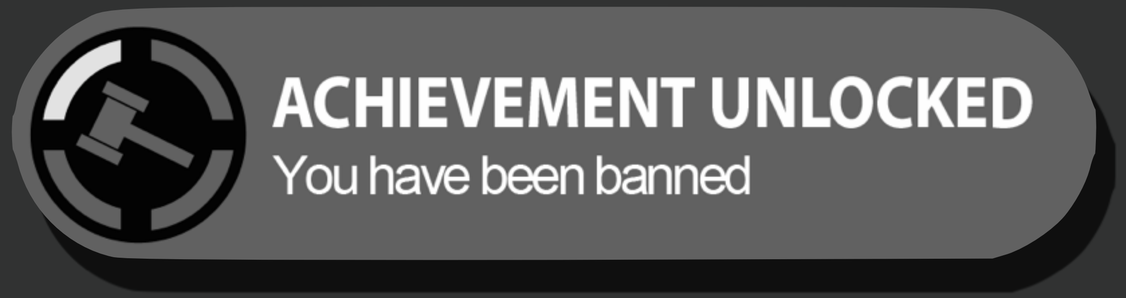
GETTING WHOIS INFORMATION

GETTING APP LOGS + STATS

VIA SPLUNK + GRAPHITE


sroberts
10:46 AM
/help splunk
Hubot
10:46 AM
/splunk [earliest] [@index] [query]
/splunk explain @[group.name]
/splunk list
/splunk list @[group]
/splunk run @[group.name]
/splunk save [group.name] [earliest] [@index] [query]
/splunk update [group.name] [earliest] [@index] [query]
/splunk-cluster [command] <opts> - manage the splunk cluster
/splunk-index [command] <opts> - manage the splunk indexes
/splunk-license [command] <opts> - run splunk commands (subset currently supported)
sroberts
10:46 AM
/splunk -3days @nginx sroberts
Hubot
10:46 AM
sroberts:
[View Results](http://
github.net:
/en-US/app/search/flashtimeline?sid=1414604801.6654099) for search index=nginx earliest=-3days latest=now sroberts
2014-10-29T10:46:19-07:00
github.com:9100
- - [29/Oct/2014:10:46:18 -0700] "POST /sroberts/hubot-vtr-scripts/new/master/src/scripts HTTP/1.1" 200 79816 "https://github.com/sroberts/hubot-vtr-scripts/tree/master/src/scripts" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/38.0.2125.104 Safari/537.36" "208.
" "kcreyts" "17659839" 0.137 0.135 . "D0360591:6073:9C57A:545127E3" github.com
2014-10-29T10:45:12-07:00
github.com:9100
- - [29/Oct/2014:10:45:12 -0700] "GET /sroberts.png HTTP/1...
View entire paste

"SWINGING THE BANHAMMER"



OTHER "SECRET" STUFF

JUST COME ASK ME IF YOU'RE CURIOUS

"MAKING IT EASIER TO WORK TOGETHER THAN TO WORK ALONE...."

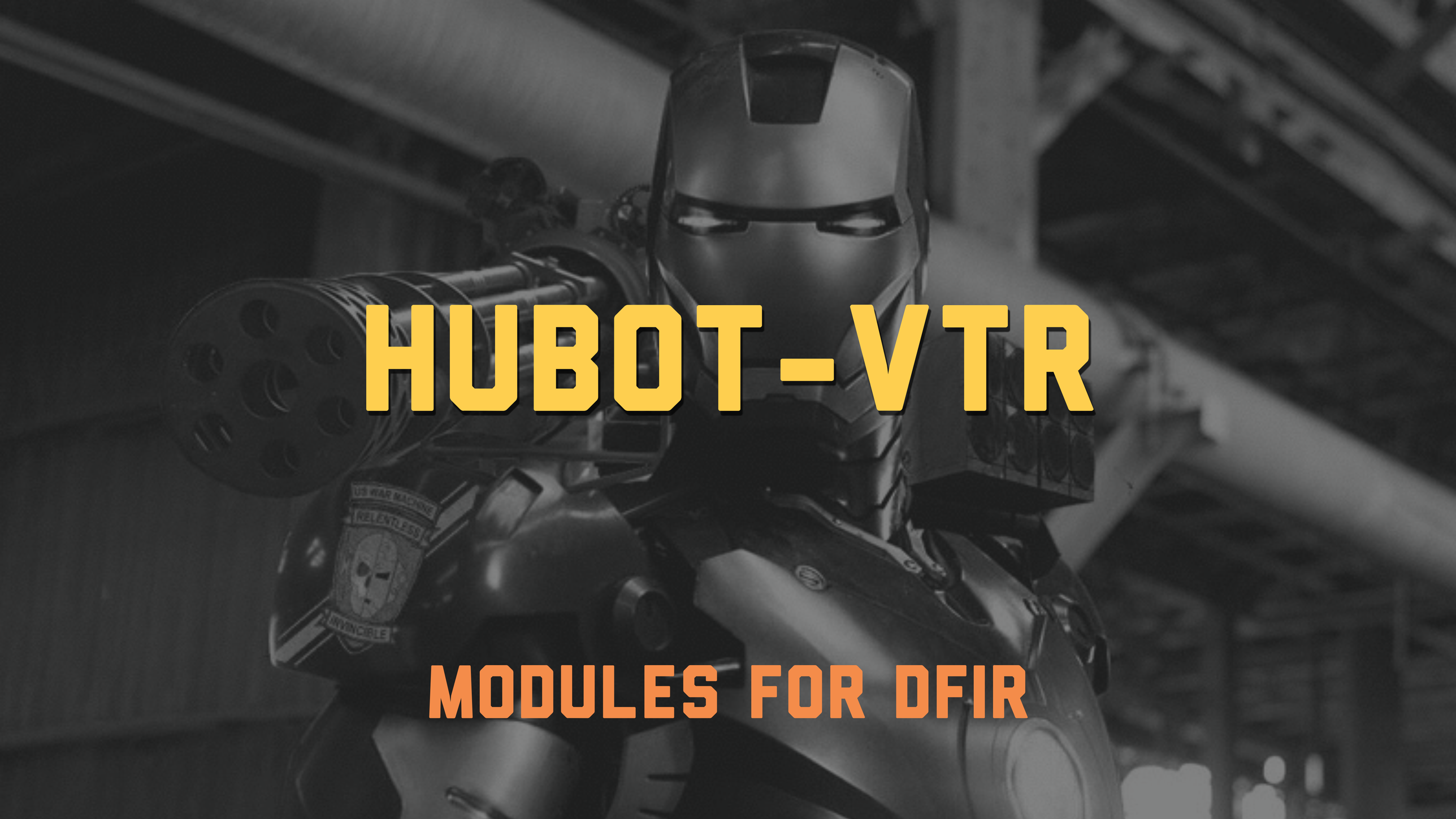
"MAKING IT EASIER TO RESPOND TO INCIDENTS TOGETHER THAN TO RESPOND ALONE...."

HUBOT VTR

HUBOT

- NODE.JS BASED CHAT BOT
- COFFEESCRIPT BASED ACTIONS
- DEPLOYABLE ANYWHERE YOU CAN RUN NODE.JS (UNIX, WINDOWS, HEROKU, ETC)

- DISK FORENSICS
- NETWORK FORENSICS
- OPEN SOURCE INTELLIGENCE
- MALWARE ANALYSIS



HUBOT-VTR

MODULES FOR DFIR

CODE NAME GENERATOR

BECAUSE YOU CAN'T CALL IT "THAT THING FROM JANUARY" FOREVER

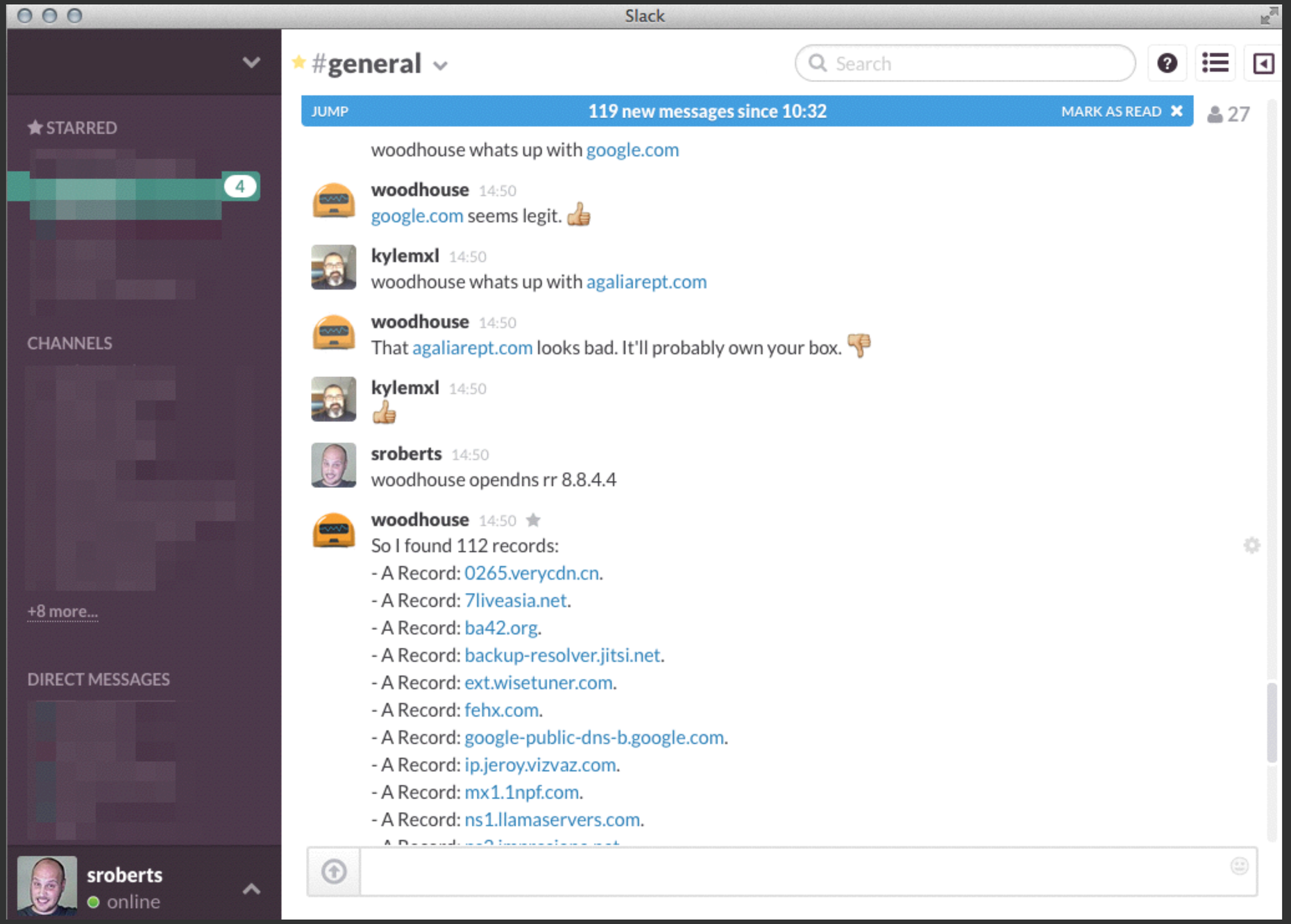
GEOLOCATING IPS

BUT NOT FOR ATTRIBUTION...

REVERSE DNS LOOKUPS

CHECKING RESOURCE REPUTATIONS

MYWOT, GOOGLE, VIRUSTOTAL, + OPENDNS


Slack
#general
Search
STARRED
4
CHANNELS
+8 more...
DIRECT MESSAGES
sroberts
online
JUMP
119 new messages since 10:32
MARK AS READ
27
woodhouse whats up with google.com
woodhouse 14:50
google.com seems legit.
kylemxl 14:50
woodhouse whats up with agaliarept.com
woodhouse 14:50
That agaliarept.com looks bad. It'll probably own your box.
kylemxl 14:50
sroberts 14:50
woodhouse opendns rr 8.8.4.4
woodhouse 14:50
So I found 112 records:
- A Record: 0265.verycdn.cn.
- A Record: 7liveasia.net.
- A Record: ba42.org.
- A Record: backup-resolver.jitsi.net.
- A Record: ext.wisetuner.com.
- A Record: fehx.com.
- A Record: google-public-dns-b.google.com.
- A Record: ip.jeroy.vizvaz.com.
- A Record: mx1.1npf.com.
- A Record: ns1.llamaservers.com.

RESEARCH LINKS GENERATOR

ROBTEXT, CENTRALOPS, HURRICANE ELECTRIC...

SERVER PROFILING

VIA SHODAN

DW
⌘1
I
⌘2
g
⌘3

STARRED

CHANNELS
+11 more...

DIRECT MESSAGES
+13 More...

PRIVATE GROUPS
+2 more...

sroberts
online

#general

Search

27

15:48 r ! shodan 79.97.250.59

15:48 **woodhouse** Shodan Result for 79.97.250.59

- IP: 79.97.250.59
- Geo: null, null, Ireland

~ 79.97.250.59

- Hostname: 79.97.250.59
- Organization: UPC Ireland
- Port: 21
- Banner:
- 220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
- 530 Login or password incorrect!
- 214-The following commands are recognized:
USER PASS QUIT CWD PWD PORT PASV TYPE
LIST REST CDUP RETR STOR SIZE DELE RMD
MKD RNFR RNTO ABOR SYST NOOP APPE NLST
MDTM XPWD XCUP XMKD XRMD NOP EPSV EPRT
AUTH ADAT PBSZ PROT FEAT MODE OPTS HELP
ALLO MLST MLSD SITE P@SW STRU CLNT MFMT
HASH
214 Have a nice day.

~ 79.97.250.59

- Hostname:
- Organization: UPC Ireland
- Port: 23
- Banner:
-
System administrator is connecting from 174.79.246.153
Reject the connection request !!!

~ 79.97.250.59

- Hostname:
- Organization: UPC Ireland
- Port: 23
- Banner:
-

MALWARE RESEARCH

VIA VIRUSTOTAL

PASSIVE DNS

VIA VIRUSTOTAL

DETECTION GENERATION

VIA YARA + SNORT

FORCE MULTIPLER

DEPLOYMENT

DEVELOPMENT

DEPLOYMENT

LOCAL
OR
HEROKU

3 COMPONENTS

BRAIN

+

CONNECTOR

+

SCRIPTS

DEVELOPMENT

COFFEESCRIPT

ON

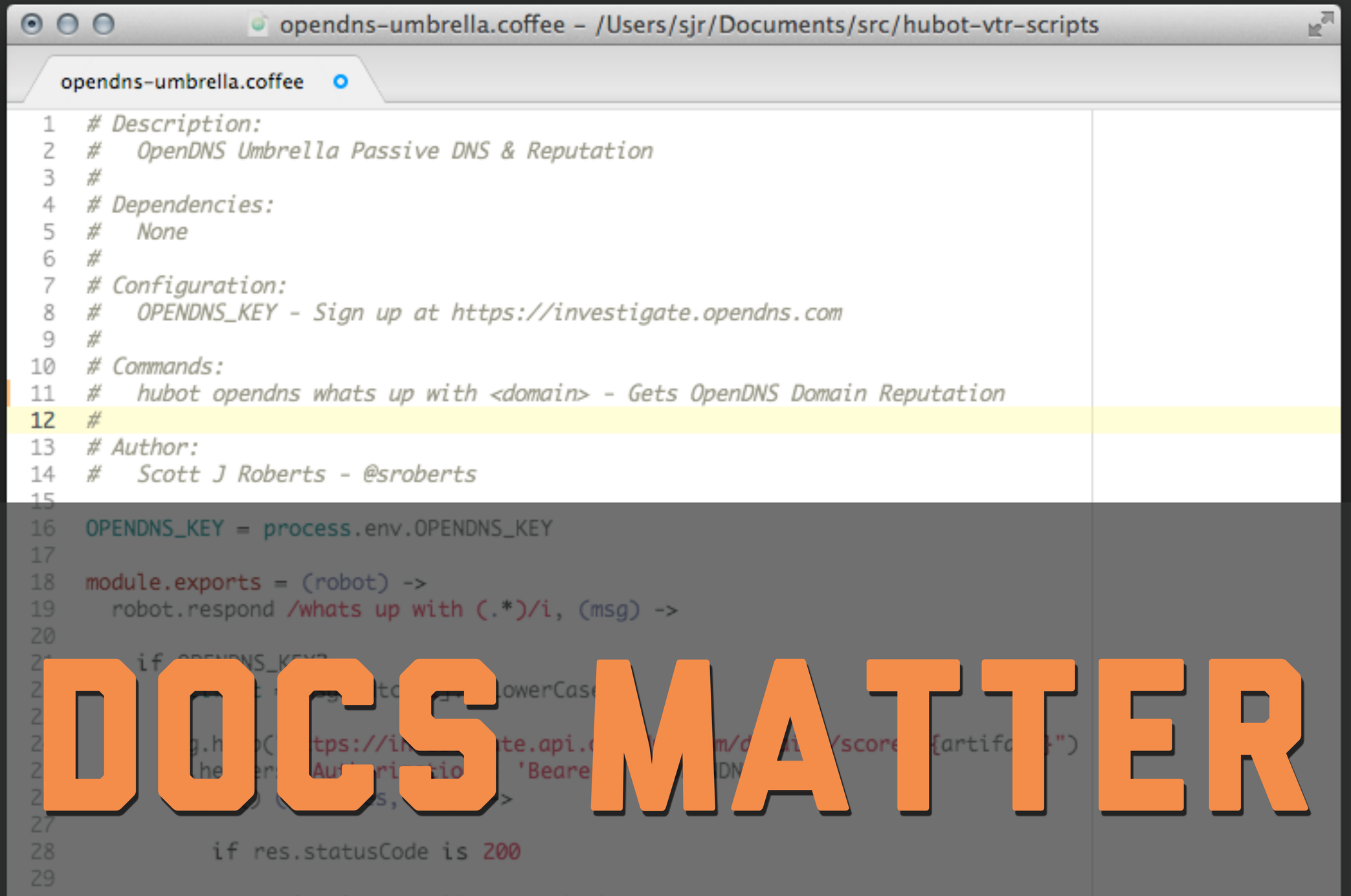
NODEJS

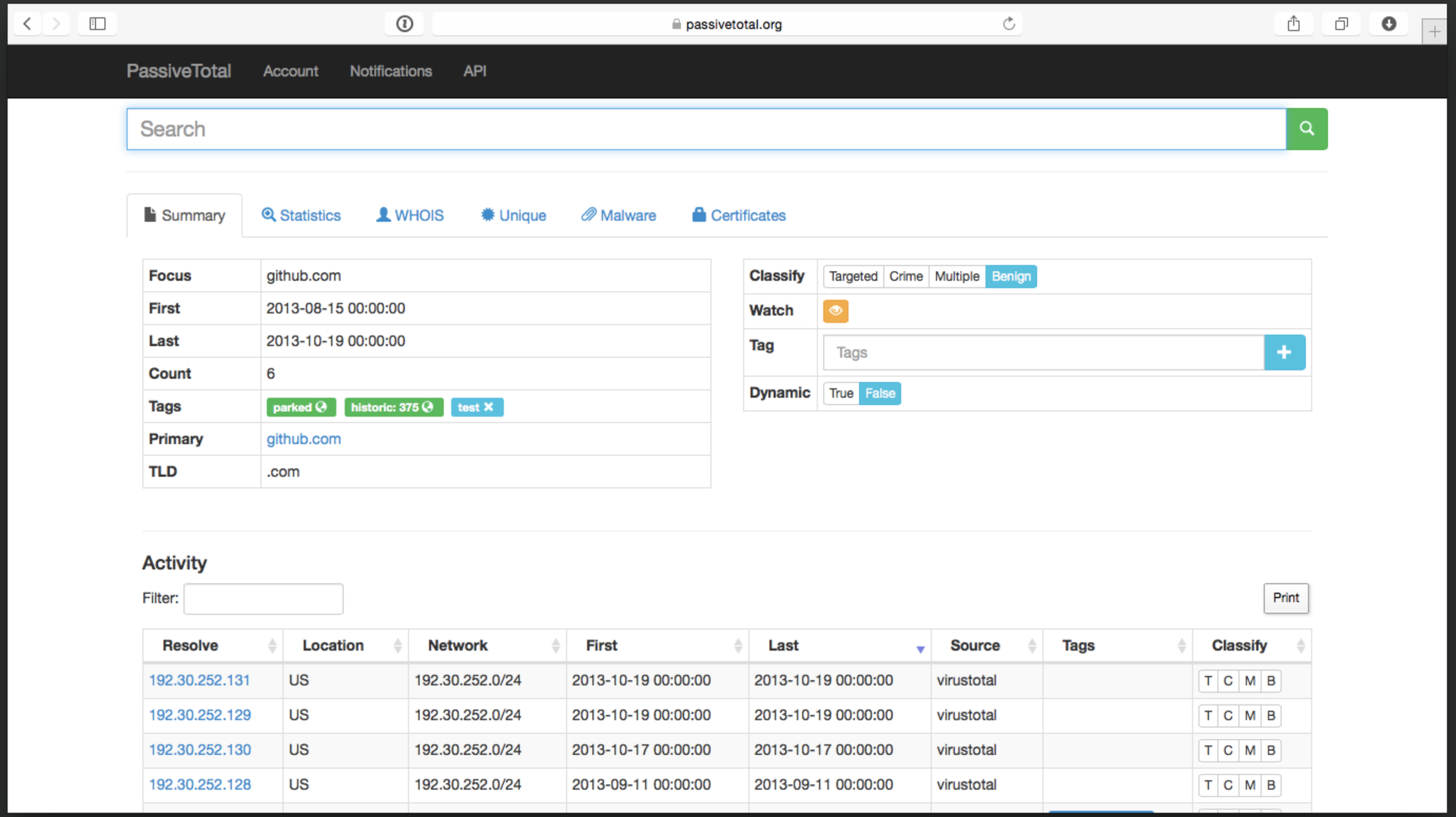
opendns-umbrella.coffee – /Users/sjr/Documents/src/hubot-vtr-scripts

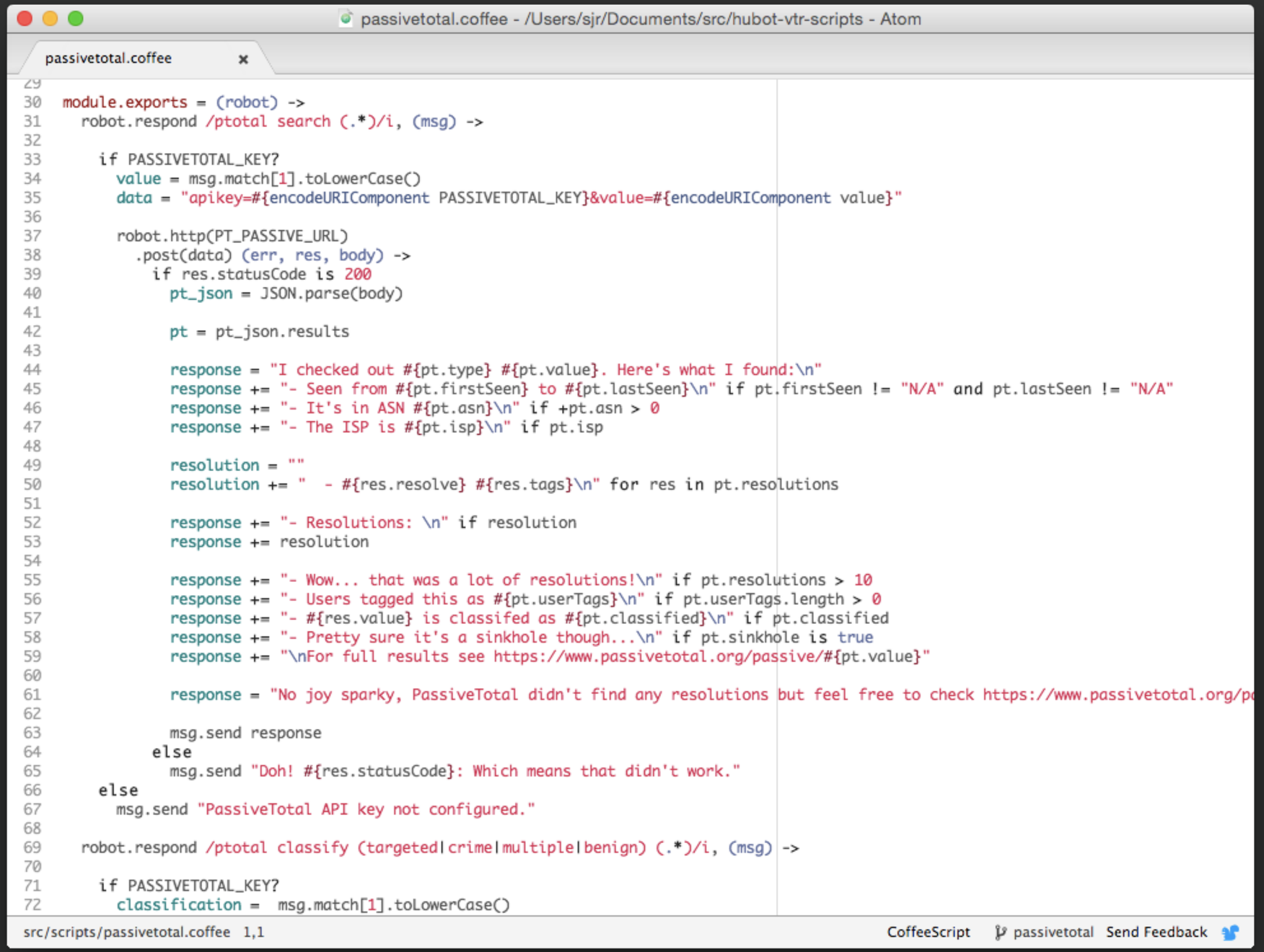
opendns-umbrella.coffee

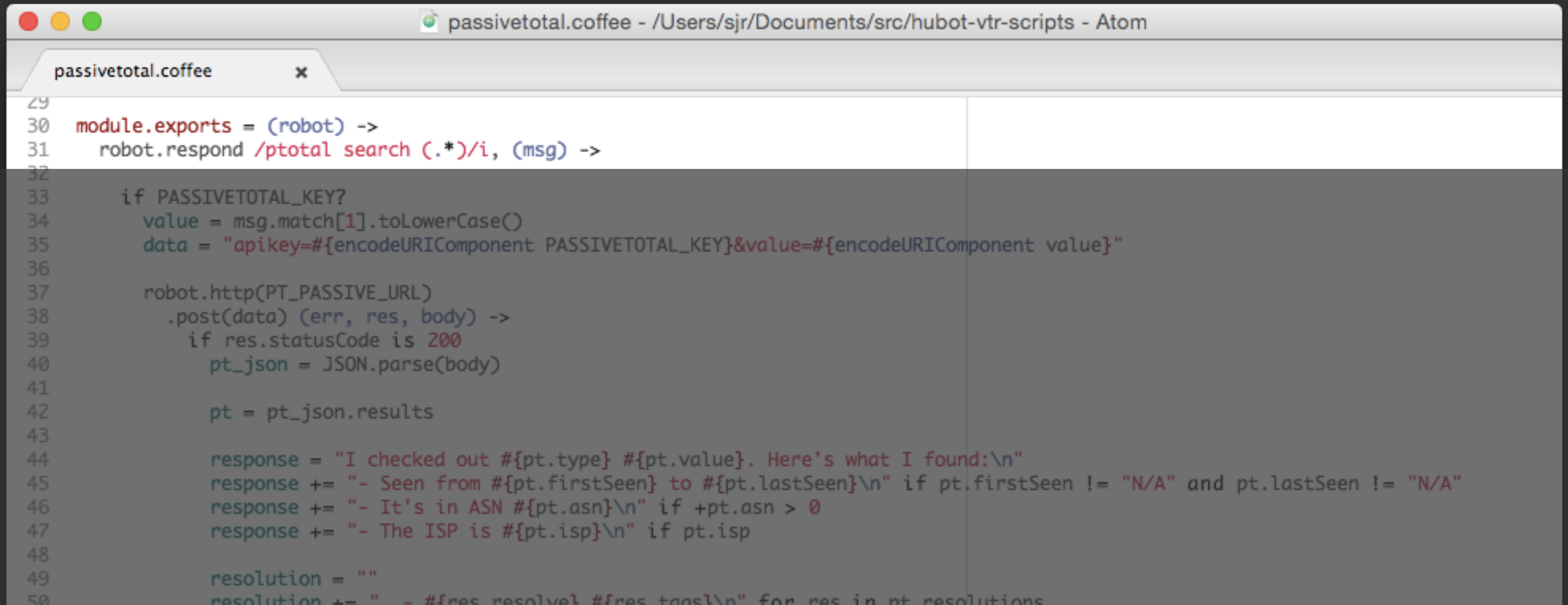
```coffeescript
# Description:
#   OpenDNS Umbrella Passive DNS & Reputation
#
# Dependencies:
#   None
#
# Configuration:
#   OPENDNS_KEY - Sign up at https://investigate.opendns.com
#
# Commands:
#   hubot opendns whats up with <domain> - Gets OpenDNS Domain Reputation
#
# Author:
#   Scott J Roberts - @sroberts

OPENDNS_KEY = process.env.OPENDNS_KEY

module.exports = (robot) ->
  robot.respond /whats up with (.*)/i, (msg) ->

    if OPENDNS_KEY?
      artifact = msg.match[1].toLowerCase()

      msg.http("https://investigate.api.opendns.com/domains/score/#{artifact}")
        .headers('Authorization': 'Bearer ' + OPENDNS_KEY)
        .get() (err, res, body) ->

          if res.statusCode is 200

            opendns_json = JSON.parse body

            for key, value of opendns_json

              switch value
                when "1" then msg.send "#{key} seems legit. :+1:"
                when "0" then msg.send "Not sure about that #{key}. Use at your own risk."
                when "-1" then msg.send "That #{key} looks bad. It'll probably own your box. :-1:"
                else
                  "No clue. You're on your own."

          else
            msg.send "Doh! #{res.statusCode}: Which means that didn't work."
    else
      msg.send "OpenDNS API key not configured."
```

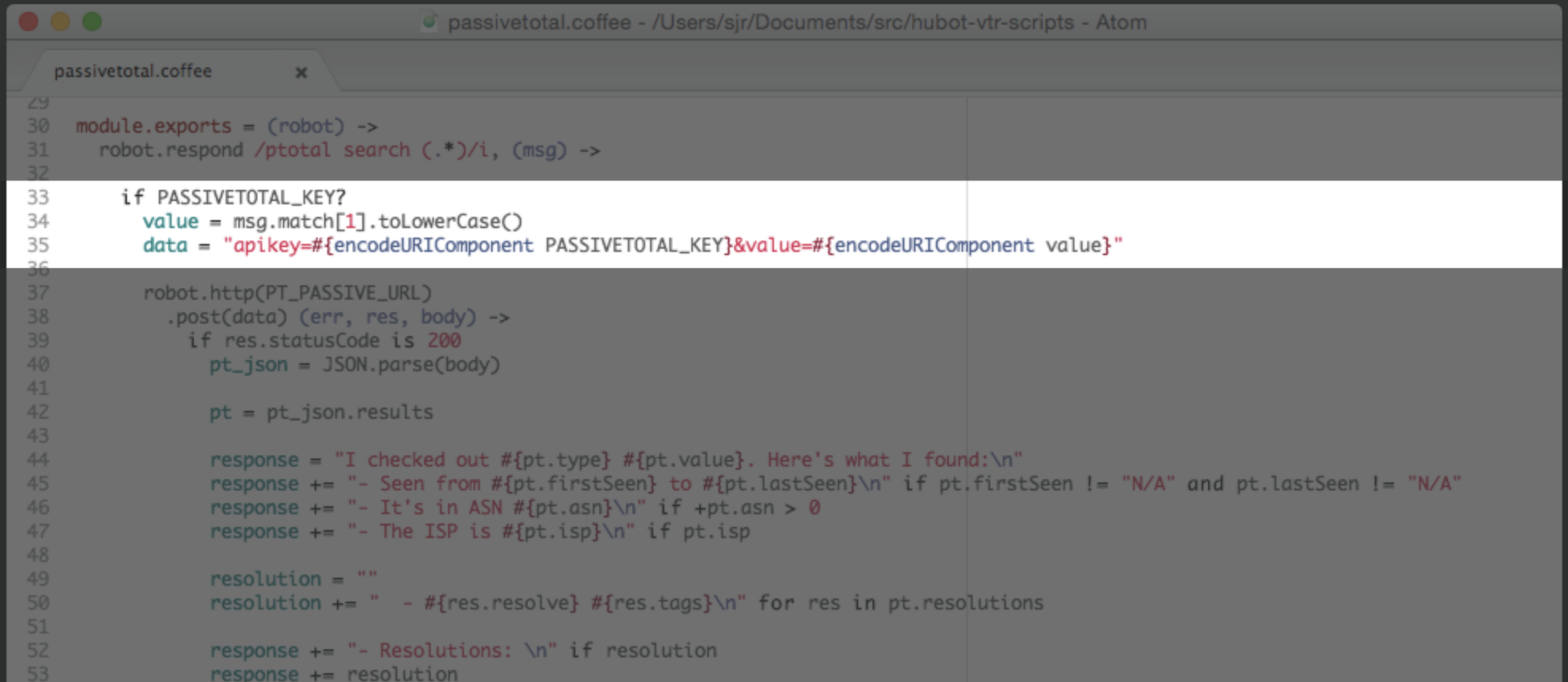
src/scripts/opendns-umbrella.coffee* 12,1 CoffeeScript opendns-umbrella Send Feedback

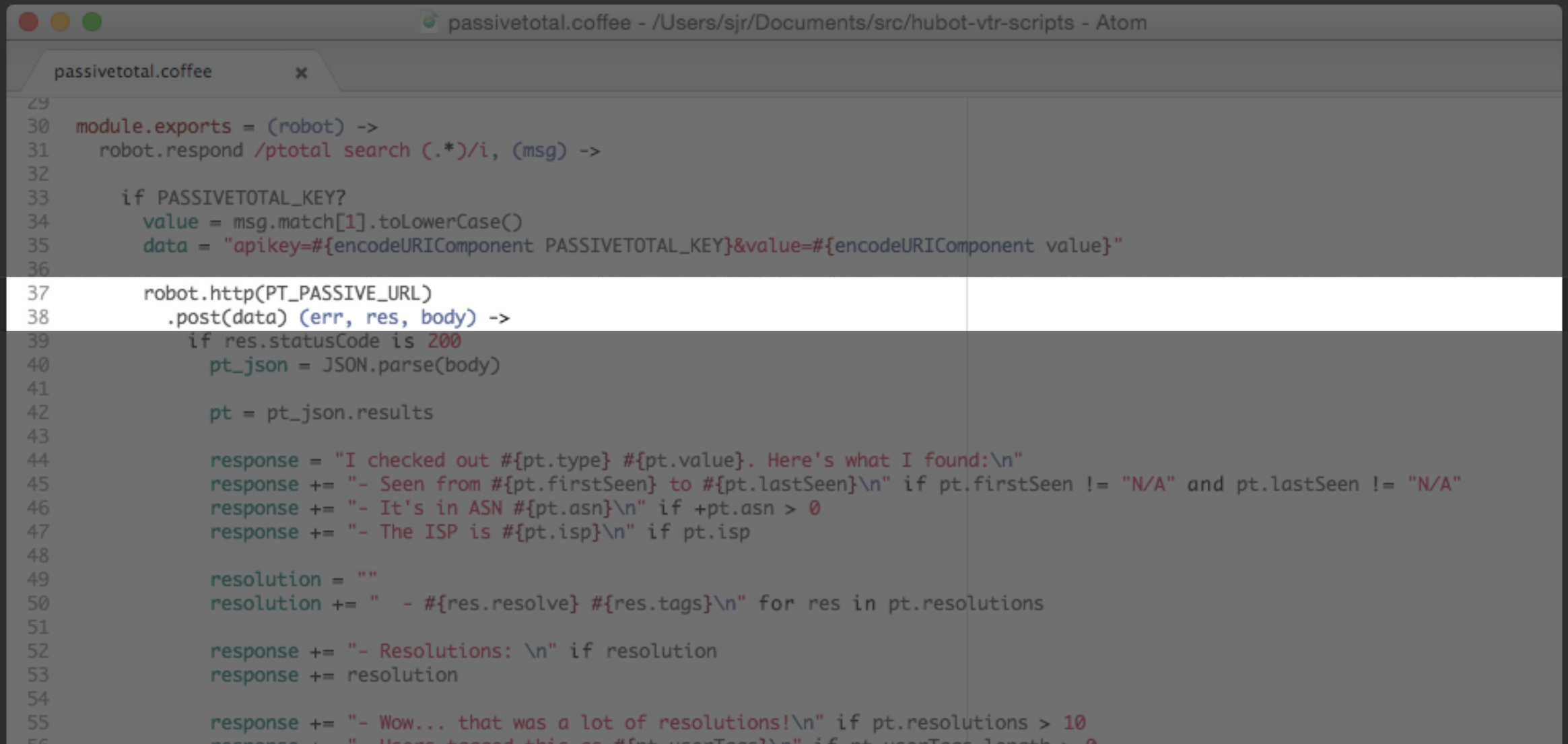

opendns-umbrella.coffee – /Users/sjr/Documents/src/hubot-vtr-scripts
opendns-umbrella.coffee
Description:
OpenDNS Umbrella Passive DNS & Reputation
#
Dependencies:
None
#
Configuration:
OPENDNS_KEY - Sign up at https://investigate.opendns.com
#
Commands:
hubot opendns whats up with <domain> - Gets OpenDNS Domain Reputation
#
# Author:
#   Scott J Roberts - @sroberts
OPENDNS_KEY = process.env.OPENDNS_KEY
module.exports = (robot) ->
robot.respond /whats up with (.*)/i, (msg) ->
if res.statusCode is 200
DOCS MATTER

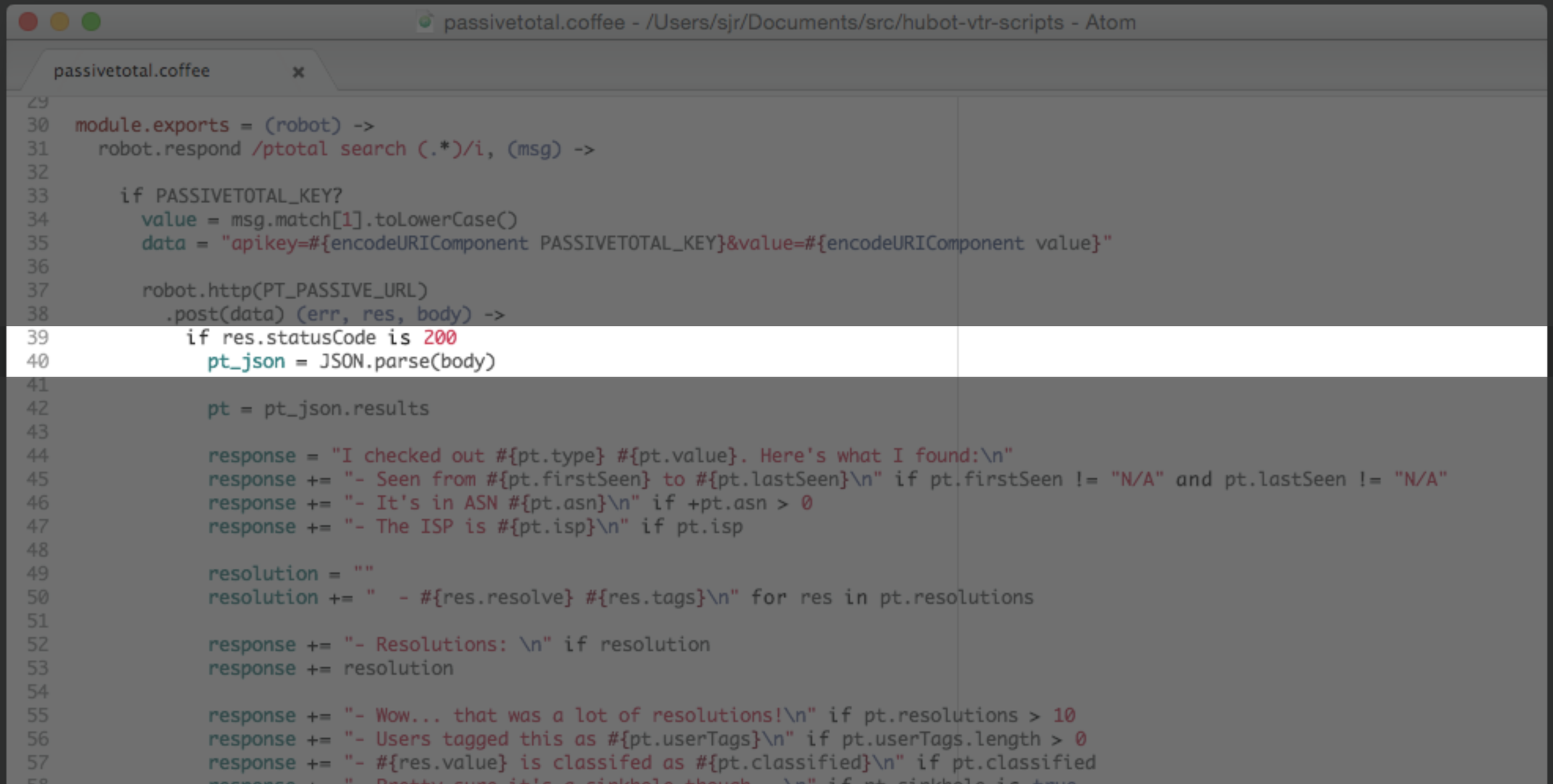

passivetotal.org
PassiveTotal
Account
Notifications
API
Search
Summary
Statistics
WHOIS
Unique
Malware
Certificates
Focus
github.com
First
2013-08-15 00:00:00
Last
2013-10-19 00:00:00
Count
6
Tags
parked
historic: 375
test
Primary
github.com
TLD
.com
Classify
Targeted
Crime
Multiple
Benign
Watch
Tag
Tags
Dynamic
True
False
Activity
Filter:
Print
Resolve
Location
Network
First
Last
Source
Tags
Classify
192.30.252.131
US
192.30.252.0/24
2013-10-19 00:00:00
2013-10-19 00:00:00
virustotal
T C M B
192.30.252.129
US
192.30.252.0/24
2013-10-19 00:00:00
2013-10-19 00:00:00
virustotal
T C M B
192.30.252.130
US
192.30.252.0/24
2013-10-17 00:00:00
2013-10-17 00:00:00
virustotal
T C M B
192.30.252.128
US
192.30.252.0/24
2013-09-11 00:00:00
2013-09-11 00:00:00
virustotal
T C M B


passivetotal.coffee - /Users/sjr/Documents/src/hubot-vtr-scripts - Atom
passivetotal.coffee
module.exports = (robot) ->
robot.respond /ptotal search (.*)/i, (msg) ->
if PASSIVETOTAL_KEY?
value = msg.match[1].toLowerCase()
data = "apikey=#{encodeURIComponent PASSIVETOTAL_KEY}&value=#{encodeURIComponent value}"
robot.http(PT_PASSIVE_URL)
.post(data) (err, res, body) ->
if res.statusCode is 200
pt_json = JSON.parse(body)
pt = pt_json.results
response = "I checked out #{pt.type} #{pt.value}. Here's what I found:\n"
response += "- Seen from #{pt.firstSeen} to #{pt.lastSeen}\n" if pt.firstSeen != "N/A" and pt.lastSeen != "N/A"
response += "- It's in ASN #{pt.asn}\n" if +pt.asn > 0
response += "- The ISP is #{pt.isp}\n" if pt.isp
resolution = ""
resolution += " - #{res.resolve} #{res.tags}\n" for res in pt.resolutions
response += "- Resolutions: \n" if resolution
response += resolution
response += "- Wow... that was a lot of resolutions!\n" if pt.resolutions > 10
response += "- Users tagged this as #{pt.userTags}\n" if pt.userTags.length > 0
response += "- #{res.value} is classifed as #{pt.classified}\n" if pt.classified
response += "- Pretty sure it's a sinkhole though...\n" if pt.sinkhole is true
response += "\nFor full results see https://www.passivetotal.org/passive/#{pt.value}"
response = "No joy sparky, PassiveTotal didn't find any resolutions but feel free to check https://www.passivetotal.org/p
msg.send response
else
msg.send "Doh! #{res.statusCode}: Which means that didn't work."
else
msg.send "PassiveTotal API key not configured."
robot.respond /ptotal classify (targeted|crime|multiple|benign) (.*)/i, (msg) ->
if PASSIVETOTAL_KEY?
classification = msg.match[1].toLowerCase()
src/scripts/passivetotal.coffee 1,1
CoffeeScript
passivetotal
Send Feedback


passivetotal.coffee - /Users/sjr/Documents/src/hubot-vtr-scripts - Atom
passivetotal.coffee
29
30 module.exports = (robot) ->
31   robot.respond /ptotal search (.*)/i, (msg) ->
32
33   if PASSIVETOTAL_KEY?
34   value = msg.match[1].toLowerCase()
35   data = "apikey=#{encodeURIComponent PASSIVETOTAL_KEY}&value=#{encodeURIComponent value}"
36
37   robot.http(PT_PASSIVE_URL)
38   .post(data) (err, res, body) ->
39   if res.statusCode is 200
40   pt_json = JSON.parse(body)
41
42   pt = pt_json.results
43
44   response = "I checked out #{pt.type} #{pt.value}. Here's what I found:\n"
45   response += "- Seen from #{pt.firstSeen} to #{pt.lastSeen}\n" if pt.firstSeen != "N/A" and pt.lastSeen != "N/A"
46   response += "- It's in ASN #{pt.asn}\n" if +pt.asn > 0
47   response += "- The ISP is #{pt.isp}\n" if pt.isp
48
49   resolution = ""
50   resolution += " - #{res.resolve} #{res.tags}\n" for res in pt.resolutions

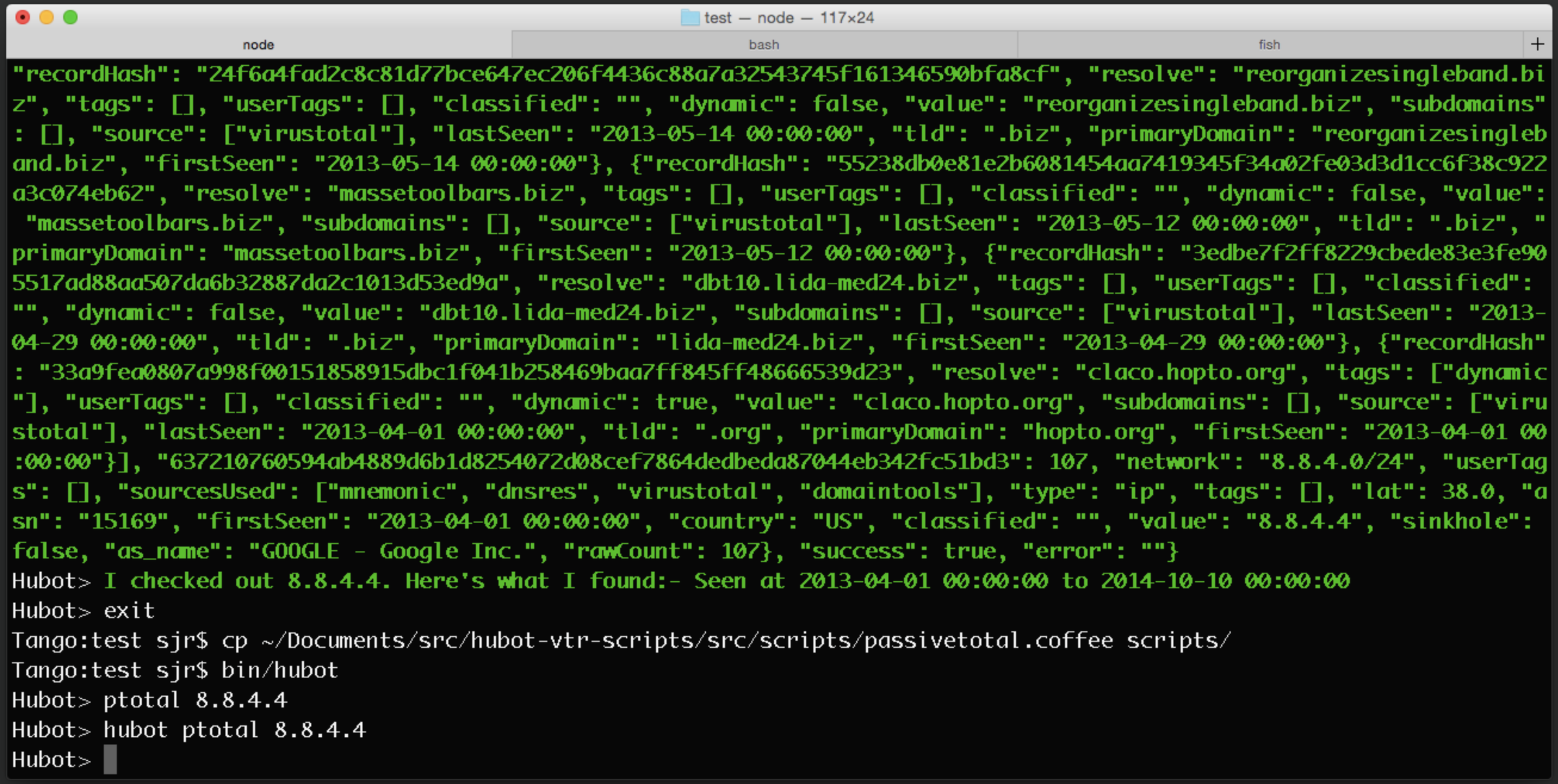

passivetotal.coffee - /Users/sjr/Documents/src/hubot-vtr-scripts - Atom
passivetotal.coffee
module.exports = (robot) ->
robot.respond /ptotal search (.*)/i, (msg) ->
if PASSIVETOTAL_KEY?
value = msg.match[1].toLowerCase()
data = "apikey=#{encodeURIComponent PASSIVETOTAL_KEY}&value=#{encodeURIComponent value}"
robot.http(PT_PASSIVE_URL)
.post(data) (err, res, body) ->
if res.statusCode is 200
pt_json = JSON.parse(body)
pt = pt_json.results
response = "I checked out #{pt.type} #{pt.value}. Here's what I found:\n"
response += "- Seen from #{pt.firstSeen} to #{pt.lastSeen}\n" if pt.firstSeen != "N/A" and pt.lastSeen != "N/A"
response += "- It's in ASN #{pt.asn}\n" if +pt.asn > 0
response += "- The ISP is #{pt.isp}\n" if pt.isp
resolution = ""
resolution += " - #{res.resolve} #{res.tags}\n" for res in pt.resolutions
response += "- Resolutions: \n" if resolution
response += resolution

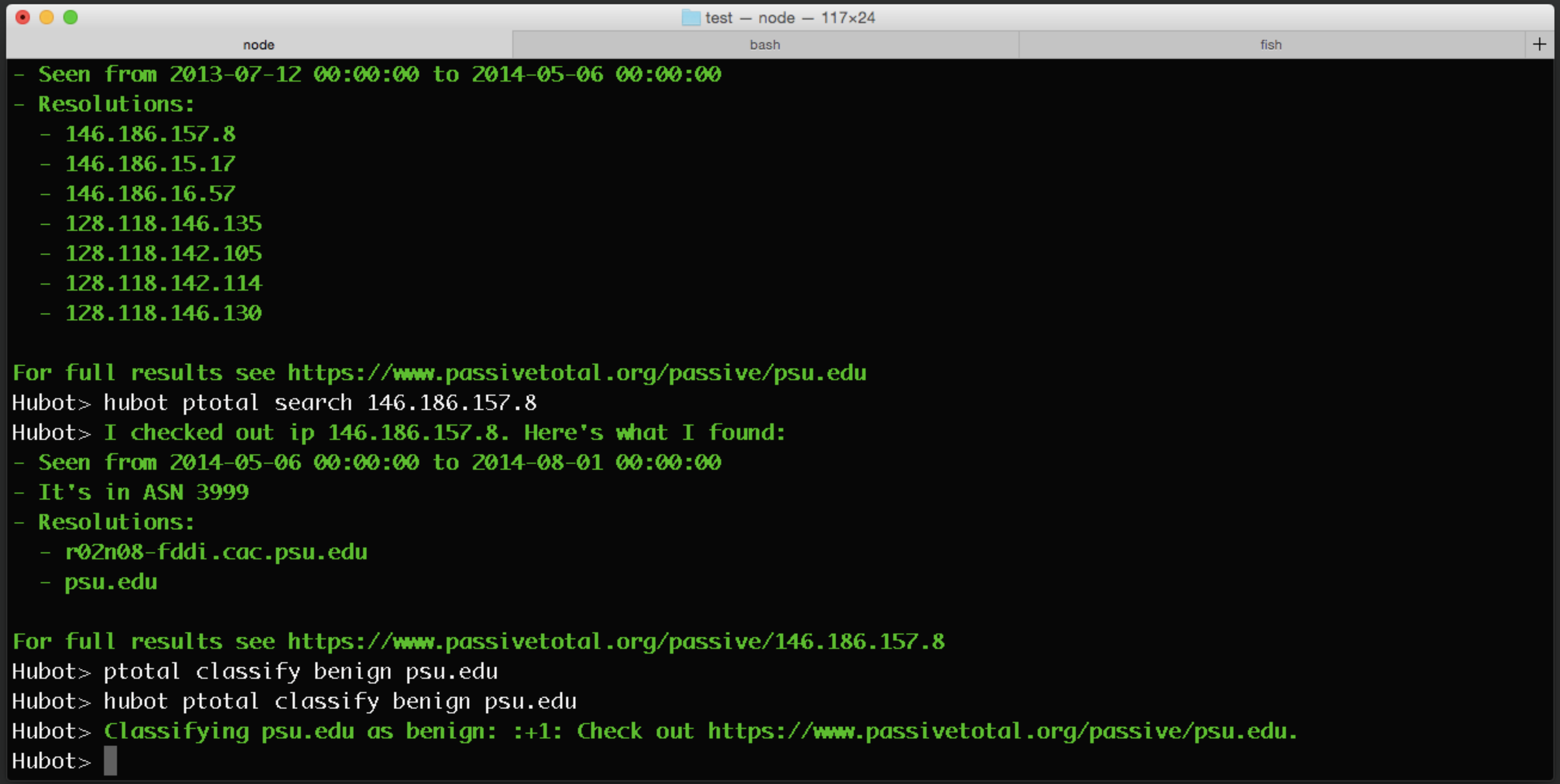

passivetotal.coffee - /Users/sjr/Documents/src/hubot-vtr-scripts - Atom
passivetotal.coffee
module.exports = (robot) ->
robot.respond /ptotal search (.*)/i, (msg) ->
if PASSIVETOTAL_KEY?
value = msg.match[1].toLowerCase()
data = "apikey=#{encodeURIComponent PASSIVETOTAL_KEY}&value=#{encodeURIComponent value}"
robot.http(PT_PASSIVE_URL)
.post(data) (err, res, body) ->
if res.statusCode is 200
pt_json = JSON.parse(body)
pt = pt_json.results
response = "I checked out #{pt.type} #{pt.value}. Here's what I found:\n"
response += "- Seen from #{pt.firstSeen} to #{pt.lastSeen}\n" if pt.firstSeen != "N/A" and pt.lastSeen != "N/A"
response += "- It's in ASN #{pt.asn}\n" if +pt.asn > 0
response += "- The ISP is #{pt.isp}\n" if pt.isp
resolution = ""
resolution += " - #{res.resolve} #{res.tags}\n" for res in pt.resolutions
response += "- Resolutions: \n" if resolution
response += resolution
response += "- Wow... that was a lot of resolutions!\n" if pt.resolutions > 10


passivetotal.coffee - /Users/sjr/Documents/src/hubot-vtr-scripts - Atom
passivetotal.coffee
29
30 module.exports = (robot) ->
31   robot.respond /ptotal search (.*)/i, (msg) ->
32
33   if PASSIVETOTAL_KEY?
34   value = msg.match[1].toLowerCase()
35   data = "apikey=#{encodeURIComponent PASSIVETOTAL_KEY}&value=#{encodeURIComponent value}"
36
37   robot.http(PT_PASSIVE_URL)
38   .post(data) (err, res, body) ->
39   if res.statusCode is 200
40   pt_json = JSON.parse(body)
41
42   pt = pt_json.results
43
44   response = "I checked out #{pt.type} #{pt.value}. Here's what I found:\n"
45   response += "- Seen from #{pt.firstSeen} to #{pt.lastSeen}\n" if pt.firstSeen != "N/A" and pt.lastSeen != "N/A"
46   response += "- It's in ASN #{pt.asn}\n" if +pt.asn > 0
47   response += "- The ISP is #{pt.isp}\n" if pt.isp
48
49   resolution = ""
50   resolution += " - #{res.resolve} #{res.tags}\n" for res in pt.resolutions
51
52   response += "- Resolutions: \n" if resolution
53   response += resolution
54
55   response += "- Wow... that was a lot of resolutions!\n" if pt.resolutions > 10
56   response += "- Users tagged this as #{pt.userTags}\n" if pt.userTags.length > 0
57   response += "- #{res.value} is classifed as #{pt.classified}\n" if pt.classified

```coffeescript
  if PASSIVETOTAL_KEY?
    value = msg.match[1].toLowerCase()
    data = "apikey=#{encodeURIComponent PASSIVETOTAL_KEY}&value=#{encodeURIComponent value}"

    robot.http(PT_PASSIVE_URL)
      .post(data) (err, res, body) ->
        if res.statusCode is 200
          pt_json = JSON.parse(body)

          pt = pt_json.results

          response = "I checked out #{pt.type} #{pt.value}. Here's what I found:\n"
          response += "- Seen from #{pt.firstSeen} to #{pt.lastSeen}\n" if pt.firstSeen != "N/A" and pt.lastSeen != "N/A"
          response += "- It's in ASN #{pt.asn}\n" if +pt.asn > 0
          response += "- The ISP is #{pt.isp}\n" if pt.isp

          resolution = ""
          resolution += "  - #{res.resolve} #{res.tags}\n" for res in pt.resolutions

          response += "- Resolutions: \n" if resolution
          response += resolution

          response += "- Wow... that was a lot of resolutions!\n" if pt.resolutions > 10
          response += "- Users tagged this as #{pt.userTags}\n" if pt.userTags.length > 0
          response += "- #{res.value} is classifed as #{pt.classified}\n" if pt.classified
          response += "- Pretty sure it's a sinkhole though...\n" if pt.sinkhole is true
          response += "\nFor full results see https://www.passivetotal.org/passive/#{pt.value}"

          response = "No joy sparky, PassiveTotal didn't find any resolutions but feel free to check https://www.passivetotal.org/p

          msg.send response
        else
          msg.send "Doh! #{res.statusCode}: Which means that didn't work."
    else
      msg.send "PassiveTotal API key not configured."

  robot.respond /ptotal classify (targeted|crime|multiple|benign) (.*)/i, (msg) ->

    if PASSIVETOTAL_KEY?
      classification =  msg.match[1].toLowerCase()
```

```
47            response += "- The ISP is #{pt.isp}\n" if pt.isp
48
49            resolution = ""
50            resolution += "  - #{res.resolve} #{res.tags}\n" for res in pt.resolutions
51
52            response += "- Resolutions: \n" if resolution
53            response += resolution
54
55            response += "- Wow... that was a lot of resolutions!\n" if pt.resolutions > 10
56            response += "- Users tagged this as #{pt.userTags}\n" if pt.userTags.length > 0
57            response += "- #{res.value} is classifed as #{pt.classified}\n" if pt.classified
58            response += "- Pretty sure it's a sinkhole though...\n" if pt.sinkhole is true
59            response += "\nFor full results see https://www.passivetotal.org/passive/#{pt.value}"
60
61            response = "No joy sparky, PassiveTotal didn't find any resolutions but feel free to check https://www.passivetotal.org/p
62
63            msg.send response
64          else
65            msg.send "Doh! #{res.statusCode}: Which means that didn't work."
66      else
67        msg.send "PassiveTotal API key not configured."
68
69    robot.respond /ptotal classify (targeted|crime|multiple|benign) (.*)/i, (msg) ->
70
71      if PASSIVETOTAL_KEY?
72        classification =  msg.match[1].toLowerCase()
```


test — node — 117×24
node
bash
fish
"recordHash": "24f6a4fad2c8c81d77bce647ec206f4436c88a7a32543745f161346590bfa8cf", "resolve": "reorganizesingleband.biz", "tags": [], "userTags": [], "classified": "", "dynamic": false, "value": "reorganizesingleband.biz", "subdomains": [], "source": ["virustotal"], "lastSeen": "2013-05-14 00:00:00", "tld": ".biz", "primaryDomain": "reorganizesingleband.biz", "firstSeen": "2013-05-14 00:00:00"}, {"recordHash": "55238db0e81e2b6081454aa7419345f34a02fe03d3d1cc6f38c922a3c074eb62", "resolve": "massetoolbars.biz", "tags": [], "userTags": [], "classified": "", "dynamic": false, "value": "massetoolbars.biz", "subdomains": [], "source": ["virustotal"], "lastSeen": "2013-05-12 00:00:00", "tld": ".biz", "primaryDomain": "massetoolbars.biz", "firstSeen": "2013-05-12 00:00:00"}, {"recordHash": "3edbe7f2ff8229cbede83e3fe905517ad88aa507da6b32887da2c1013d53ed9a", "resolve": "dbt10.lida-med24.biz", "tags": [], "userTags": [], "classified": "", "dynamic": false, "value": "dbt10.lida-med24.biz", "subdomains": [], "source": ["virustotal"], "lastSeen": "2013-04-29 00:00:00", "tld": ".biz", "primaryDomain": "lida-med24.biz", "firstSeen": "2013-04-29 00:00:00"}, {"recordHash": "33a9fea0807a998f00151858915dbc1f041b258469baa7ff845ff48666539d23", "resolve": "claco.hopto.org", "tags": ["dynamic"], "userTags": [], "classified": "", "dynamic": true, "value": "claco.hopto.org", "subdomains": [], "source": ["virustotal"], "lastSeen": "2013-04-01 00:00:00", "tld": ".org", "primaryDomain": "hopto.org", "firstSeen": "2013-04-01 00:00:00"}], "637210760594ab4889d6b1d8254072d08cef7864dedbeda87044eb342fc51bd3": 107, "network": "8.8.4.0/24", "userTags": [], "sourcesUsed": ["mnemonic", "dnsres", "virustotal", "domaintools"], "type": "ip", "tags": [], "lat": 38.0, "asn": "15169", "firstSeen": "2013-04-01 00:00:00", "country": "US", "classified": "", "value": "8.8.4.4", "sinkhole": false, "as_name": "GOOGLE - Google Inc.", "rawCount": 107}, "success": true, "error": ""}
Hubot> I checked out 8.8.4.4. Here's what I found:- Seen at 2013-04-01 00:00:00 to 2014-10-10 00:00:00
Hubot> exit
Tango:test sjr$ cp ~/Documents/src/hubot-vtr-scripts/src/scripts/passivetotal.coffee scripts/
Tango:test sjr$ bin/hubot
Hubot> ptotal 8.8.4.4
Hubot> hubot ptotal 8.8.4.4
Hubot>


test — node — 117×24
node
bash
fish
- Seen from 2013-07-12 00:00:00 to 2014-05-06 00:00:00
- Resolutions:
  - 146.186.157.8
  - 146.186.15.17
  - 146.186.16.57
  - 128.118.146.135
  - 128.118.142.105
  - 128.118.142.114
  - 128.118.146.130
For full results see https://www.passivetotal.org/passive/psu.edu
Hubot> hubot ptotal search 146.186.157.8
Hubot> I checked out ip 146.186.157.8. Here's what I found:
- Seen from 2014-05-06 00:00:00 to 2014-08-01 00:00:00
- It's in ASN 3999
- Resolutions:
  - r02n08-fddi.cac.psu.edu
  - psu.edu
For full results see https://www.passivetotal.org/passive/146.186.157.8
Hubot> ptotal classify benign psu.edu
Hubot> hubot ptotal classify benign psu.edu
Hubot> Classifying psu.edu as benign: :+1: Check out https://www.passivetotal.org/passive/psu.edu.
Hubot>

HUBOT'S "VOICE"

IN CONCLUSION...

CHATOPS CAN MAKE INCIDENT RESPONSE COLLABORATIVE

&

HUBOT VTR PUTS DFIR TOOLS & TASKS IN CHAT

FIND OUT MORE

HUBOT.GITHUB.COM

&

GITHUB.COM/SROBERTS/HUBOT-VTR-SCRIPTS

CONTACT ME

GITHUB & TWITTER: @SROBERTS

SROBERTS.GITHUB.IO

THANKS!!!