



# Fast Flux

Adli Wahid

Head, MyCERT

[adli@cybersecurity.org.my](mailto:adli@cybersecurity.org.my)



# Agenda

---

- About MyCERT
- Fast-Flux
- Example
- Response/Mitigation Issues
- Interesting Projects

# MyCERT

- ❑ Cyber999
  - Incident Response / Handling
- ❑ Cyber Early Warning
  - Advisories and alert
  - Research network
    - Honeynet
- ❑ **Technical Co-ordination**
  - **National CERT**
  - **Works with Law Enforcement Agencies, CSIRTs,**
  - **Currently Chair of APCERT**

# Fast-Flux

---

- Have you read this ?
  - **[SAC025]:Fast Flux Hosting and DNS**

# Fast-Flux

- ❑ Briefly
  - Technique for **hiding** hosts
  - **Multiple IP addresses** assigned to full qualified domain name
  - Combined with **redirection** / **reverse proxy**
- ❑ Used by the bad guys
  - Host illegal sites, phishing, serving malware
  - StormWorm
- ❑ Goal
  - To make life difficult for everyone :-)

# thebestcasinosonly.org



**ONLINE CASINO**  
Real Money



- Home
- About Black Jack
- About Poker
- About Slots
- About Roulette

Welcome to the internet's leading resource for finding the finest and fairest casinos in the market today. Whether a beginner, novice, or professional, we will make sure that you arrive at the casino that is right for you.

We keep our visitors updated with the latest promotions and bonuses, as well as provide inside tips and techniques for the most popular casino games

Feel free to browse through some of the most beautifully designed and reliable online gaming sites on the internet today.



## ALL STARS CASINO

**U.S. Players Are Welcome!**

Play in your own language!

Click your flag to Play



ALL Stars Casino is a rewarding, classy gaming site that delivers a solid and exciting gaming experience. ALL Stars Casino relies on the strength of its fantastic

# Flux Variance

---

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

# thebestcasinosonly.org

```

$ dig thebestcasinosonly.org

; <<>> DiG 9.3.1 <<>> thebestcasinosonly.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34670
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;thebestcasinosonly.org.                IN      A

;; ANSWER SECTION:
thebestcasinosonly.org. 180      IN      A      24.131.245.17
thebestcasinosonly.org. 180      IN      A      24.196.99.141
thebestcasinosonly.org. 180      IN      A      61.33.123.33
thebestcasinosonly.org. 180      IN      A      67.14.250.74
thebestcasinosonly.org. 180      IN      A      67.165.248.201
thebestcasinosonly.org. 180      IN      A      68.118.88.8
thebestcasinosonly.org. 180      IN      A      69.145.50.205
thebestcasinosonly.org. 180      IN      A      72.24.66.110
thebestcasinosonly.org. 180      IN      A      75.35.119.75
thebestcasinosonly.org. 180      IN      A      75.64.184.207

;; AUTHORITY SECTION:
thebestcasinosonly.org. 86398    IN      NS      ns2.c0fbfef6e372ca34a.com.
thebestcasinosonly.org. 86398    IN      NS      ns1.c0fbfef6e372ca34a.com.

;; ADDITIONAL SECTION:
ns1.c0fbfef6e372ca34a.com. 172800  IN      A      76.83.111.64

```

<http://project.honeynet.org>

# Many IPs

```
$ dig thebestcasinosonly.org

; <<>> DiG 9.3.1 <<>> thebestcasinosonly.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34670
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 2, ADDITIONAL: 1

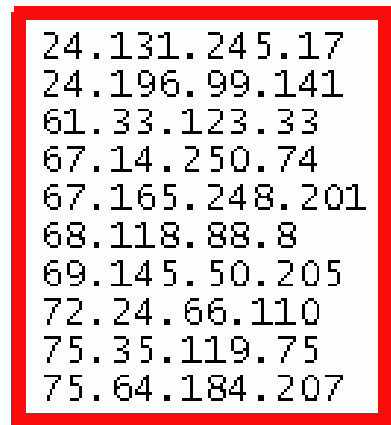
;; QUESTION SECTION:
;thebestcasinosonly.org.                IN      A

;; ANSWER SECTION:
thebestcasinosonly.org. 180     IN      A      24.131.245.17
thebestcasinosonly.org. 180     IN      A      24.196.99.141
thebestcasinosonly.org. 180     IN      A      61.33.123.33
thebestcasinosonly.org. 180     IN      A      67.14.250.74
thebestcasinosonly.org. 180     IN      A      67.165.248.201
thebestcasinosonly.org. 180     IN      A      68.118.88.8
thebestcasinosonly.org. 180     IN      A      69.145.50.205
thebestcasinosonly.org. 180     IN      A      72.24.66.110
thebestcasinosonly.org. 180     IN      A      75.35.119.75
thebestcasinosonly.org. 180     IN      A      75.64.184.207

;; AUTHORITY SECTION:
thebestcasinosonly.org. 86398   IN      NS     ns2.c0fbfef6e372ca34a.com.
thebestcasinosonly.org. 86398   IN      NS     ns1.c0fbfef6e372ca34a.com.

;; ADDITIONAL SECTION:
ns1.c0fbfef6e372ca34a.com. 172800 IN      A      76.83.111.64
```

**Many 'A' Records returned (5-15)**



Source: [project.honeynet.org](http://project.honeynet.org)

# Short TTLs

```

$ dig thebestcasinosonly.org

; <<>> DiG 9.3.1 <<>> thebestcasinosonly.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34670
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;thebestcasinosonly.org.                IN      A

;; ANSWER SECTION:
thebestcasinosonly.org. 180     IN      A      24.131.245.17
thebestcasinosonly.org. 180     IN      A      24.196.99.141
thebestcasinosonly.org. 180     IN      A      61.33.123.33
thebestcasinosonly.org. 180     IN      A      67.14.250.74
thebestcasinosonly.org. 180     IN      A      67.165.248.201
thebestcasinosonly.org. 180     IN      A      68.118.88.8
thebestcasinosonly.org. 180     IN      A      69.145.50.205
thebestcasinosonly.org. 180     IN      A      72.24.66.110
thebestcasinosonly.org. 180     IN      A      75.35.119.75
thebestcasinosonly.org. 180     IN      A      75.64.184.207

;; AUTHORITY SECTION:
thebestcasinosonly.org. 86398   IN      NS      ns2.c0fbfef6e372ca34a.com.
thebestcasinosonly.org. 86398   IN      NS      ns1.c0fbfef6e372ca34a.com.

;; ADDITIONAL SECTION:
ns1.c0fbfef6e372ca34a.com. 172800 IN      A      76.83.111.64

```

**Short Time-To-Live (<1800 sec)**

180  
180  
180  
180  
180  
180  
180  
180  
180  
180

Source: [project.honeynet.org](http://project.honeynet.org)

# Double Fast Flux

```

$ dig thebestcasinosonly.org

; <<>> DiG 9.3.1 <<>> thebestcasinosonly.org
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34670
;; flags: qr rd ra; QUERY: 1, ANSWER: 10, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;thebestcasinosonly.org.                IN      A

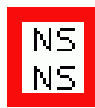
;; ANSWER SECTION:
thebestcasinosonly.org. 180     IN      A       24.131.245.17
thebestcasinosonly.org. 180     IN      A       24.196.99.141
thebestcasinosonly.org. 180     IN      A       61.33.123.33
thebestcasinosonly.org. 180     IN      A       67.14.250.74
thebestcasinosonly.org. 180     IN      A       67.165.248.201
thebestcasinosonly.org. 180     IN      A       68.118.88.8
thebestcasinosonly.org. 180     IN      A       69.145.50.205
thebestcasinosonly.org. 180     IN      A       72.24.66.110
thebestcasinosonly.org. 180     IN      A       75.35.119.75
thebestcasinosonly.org. 180     IN      A       75.64.184.207

;; AUTHORITY SECTION:
thebestcasinosonly.org. 86398   IN      NS      ns2.c0fbfef6e372ca34a.com.
thebestcasinosonly.org. 86398   IN      NS      ns1.c0fbfef6e372ca34a.com.

;; ADDITIONAL SECTION:
ns1.c0fbfef6e372ca34a.com. 172800 IN      A       76.83.111.64

```

**#'NS' Records Varies (Double-Flux >= 5)**



# IP Mapped to thebestcasinoonly.org

287 IP addresses!

12.206.40.180	24.170.47.176	67.10.209.213	69.0.73.84	70.240.228.214	75.0.40.101	75.68.235.7
12.206.54.141	24.178.108.58	67.11.53.229	69.104.17.202	70.240.76.64	75.132.196.148	76.105.73.135
12.207.68.178	24.178.70.101	67.122.209.32	69.104.79.110	70.242.226.137	75.132.221.72	76.105.94.93
12.216.56.160	24.192.190.232	67.14.250.74	69.105.29.239	70.247.72.253	75.15.177.242	76.160.14.167
165.247.3.62	24.192.229.71	67.163.9.207	69.105.53.104	70.247.73.240	75.15.246.201	76.160.18.66
172.166.156.216	24.196.99.141	67.165.248.201	69.111.195.192	70.247.75.152	75.15.252.175	76.160.23.48
172.168.162.140	24.197.105.54	67.175.219.231	69.111.195.23	70.249.187.167	75.16.105.1	76.167.164.252
172.190.186.191	24.2.123.87	67.181.91.202	69.139.115.247	70.250.217.237	75.16.110.30	76.18.15.226
172.190.51.251	24.240.70.148	67.182.11.96	69.139.31.14	70.251.246.111	75.176.40.117	76.188.22.61
172.192.138.83	24.27.203.131	67.188.91.127	69.143.2.111	70.255.250.189	75.21.184.230	76.193.35.241
172.192.6.73	24.62.54.140	67.64.114.126	69.145.50.205	70.78.11.19	75.21.191.180	76.195.181.88
172.193.41.102	24.94.62.190	68.116.214.113	69.146.142.65	71.12.14.160	75.21.226.71	76.195.183.56
190.84.147.136	24.98.156.181	68.118.88.8	69.151.200.212	71.135.45.74	75.21.242.103	76.195.9.80
196.217.101.105	4.131.83.22	68.121.85.57	69.151.200.241	71.135.71.54	75.22.20.182	76.197.59.104
200.114.214.92	4.180.60.136	68.126.254.99	69.177.90.100	71.136.13.167	75.26.49.34	76.198.93.93
201.244.248.187	4.180.60.159	68.126.255.178	69.182.21.234	71.136.14.44	75.31.160.172	76.202.254.102
201.245.252.74	4.227.241.192	68.185.180.87	69.183.12.223	71.137.136.140	75.31.163.161	76.203.17.200
203.170.111.16	4.245.120.173	68.204.134.168	69.208.138.101	71.138.48.230	75.31.27.32	76.215.129.131
203.170.115.64	61.33.123.33	68.205.108.135	69.208.138.23	71.140.115.153	75.32.50.25	76.216.115.188
204.13.181.145	65.184.237.226	68.248.1.10	69.209.136.66	71.141.91.134	75.36.125.248	76.22.239.167
204.13.181.171	65.205.65.83	68.250.211.151	69.215.135.107	71.198.93.144	75.37.161.145	76.227.0.122
204.13.181.183	65.24.108.223	68.251.185.64	69.215.136.146	71.205.219.86	75.4.141.137	76.23.121.71
204.13.181.211	65.24.109.83	68.33.3.123	69.215.140.43	71.225.137.78	75.4.61.10	76.24.146.172
207.255.83.226	65.25.6.83	68.37.193.126	69.215.173.148	71.232.66.87	75.4.70.107	76.27.116.145
208.104.21.244	65.33.192.199	68.37.220.199	69.221.7.14	71.238.40.7	75.41.4.178	76.83.85.235
208.104.84.227	66.139.11.139	68.37.91.78	69.221.92.49	71.74.239.158	75.45.238.22	76.98.91.185
208.104.88.123	66.142.170.139	68.44.187.232	69.232.65.116	71.76.219.163	75.46.10.146	76.99.113.84
208.188.16.15	66.142.185.118	68.45.116.157	69.232.68.109	71.76.56.14	75.46.37.253	76.99.254.64
208.188.17.164	66.16.189.26	68.46.93.192	69.246.178.123	71.79.201.101	75.46.80.126	82.3.234.196
208.188.17.239	66.177.221.151	68.57.63.155	69.251.167.240	71.79.247.170	75.46.95.208	84.125.43.159
208.191.144.174	66.177.24.253	68.73.87.136	69.251.44.158	71.79.252.196	75.47.107.97	84.222.244.186
210.57.250.102	66.188.122.229	68.75.6.70	70.128.42.114	71.81.244.187	75.49.116.215	84.223.131.250
210.57.252.229	66.190.101.125	68.88.13.108	70.129.135.238	72.181.75.188	75.5.2.164	84.223.134.181
210.57.252.80	66.190.102.134	68.88.143.59	70.131.147.172	72.186.86.145	75.51.92.217	86.31.118.11
216.255.60.248	66.214.56.40	68.88.254.147	70.131.153.35	72.187.156.200	75.54.135.226	89.172.26.164
219.91.185.247	66.215.208.135	68.89.175.186	70.226.14.253	72.234.104.254	75.6.138.195	96.2.169.94
24.131.245.17	66.215.91.66	68.89.176.169	70.226.224.180	74.138.21.51	75.6.180.189	98.194.20.186
24.131.245.44	66.229.173.145	68.89.177.5	70.226.23.230	74.140.246.17	75.63.63.97	98.194.66.50
24.14.72.252	66.234.209.142	68.89.189.67	70.233.250.4	75.0.235.83	75.64.184.207	98.199.193.16
24.15.131.102	66.56.26.35	68.90.218.145	70.236.18.72	75.0.36.19	75.65.189.26	98.202.2.4
24.15.179.161	66.65.217.252	68.91.122.22	70.236.29.243	75.0.37.193	75.65.33.136	99.244.112.14

# Mitigation Issues

- ❑ Revisit the goal of all of this
  - Evasion
- ❑ Multi-pronged approach
- ❑ Take down/clean up bots/botnets
  - Too many
  - Need to work with ISPs
- ❑ Detection
  - Low TTLs
  - Enforcement of minimum time of updates
  - Need to work with Registrar

# Way forward

---

- ❑ Greater sharing of information
  - Framework for response
  - Establishing Trust

# Related Projects

---

- ❑ Passive DNS monitoring of A and NS records advertised
  - DNSParse
  - Passive DNS Replication

# End()

---

❑ Email [adli@cybersecurity.org.my](mailto:adli@cybersecurity.org.my)

# Resources

---

- ❑ Know Your Enemy: Fast-Flux Service Networks
  - <http://www.honeynet.org/papers/ff/>
- ❑ Fast-Flux Hosting and DNS – ICANN
  - <http://www.icann.org/committees/security/sac025.pdf>
- ❑ Passive DNS Replication
  - <http://cert.uni-stuttgart.de/stats/dns-replication.php>

# Our Websites and emails

**websites**

<http://www.cybersecurity.org.my>

for



Corporate website

<http://www.mycert.org.my>

for



Technical website

<http://www.esecurity.org.my>

for



Awareness Portal

<http://cnii.cybersecurity.org.my>

for



**emails**

[info@cybersecurity.org.my](mailto:info@cybersecurity.org.my)

→ for general inquiries

[cyber999@cybersecurity.org.my](mailto:cyber999@cybersecurity.org.my)

→ for incidence reporting

Our Corporate  
Website:



<http://www.cybersecurity.org.my/>


An agency under:




Ministry of Science, Technology & Innovation

Home About Us Services Events Knowledge Bank Community

Home > About Us > **Contact Information**


 **Postal Address** : CyberSecurity Malaysia (formerly known as NISER),  
Level 7, SAPURA @ MINES,  
7, Jalan Tasik, The Mines Resort City,  
43300 Seri Kembangan,  
Selangor Darul Ehsan,  
Malaysia.

 **Office Hours** : Monday - Friday 08:30 - 17:30 MYT  
(Note: Not operational every Saturday and Sunday)

 **Phone** : +603 - 8992 6888

 **Fax** : +603 - 8945 3205

 **Email** : *info [at] cybersecurity.org.my*

 **Map** : Click here to download CyberSecurity Malaysia location map.

Thank You 