Fast flux hosting and DNS

Kitisak Jirawannakool

National Electronics and Computer Technology Center (NECTEC)

Agenda

- About me
- What is fast flux?
- Types of fast flux
- Case study
- Mitigation and Detection
- Conclusion

Contact me

Name : Kitisak Jirawannakool

Facebook : http://www.facebook.com/kitisak.note

Email : kitisak.jirawannakool@nectec.or.th
jkitisak@gmail.com

Weblog : http://foh9.blogspot.com

Twitter : @kitisak

About me

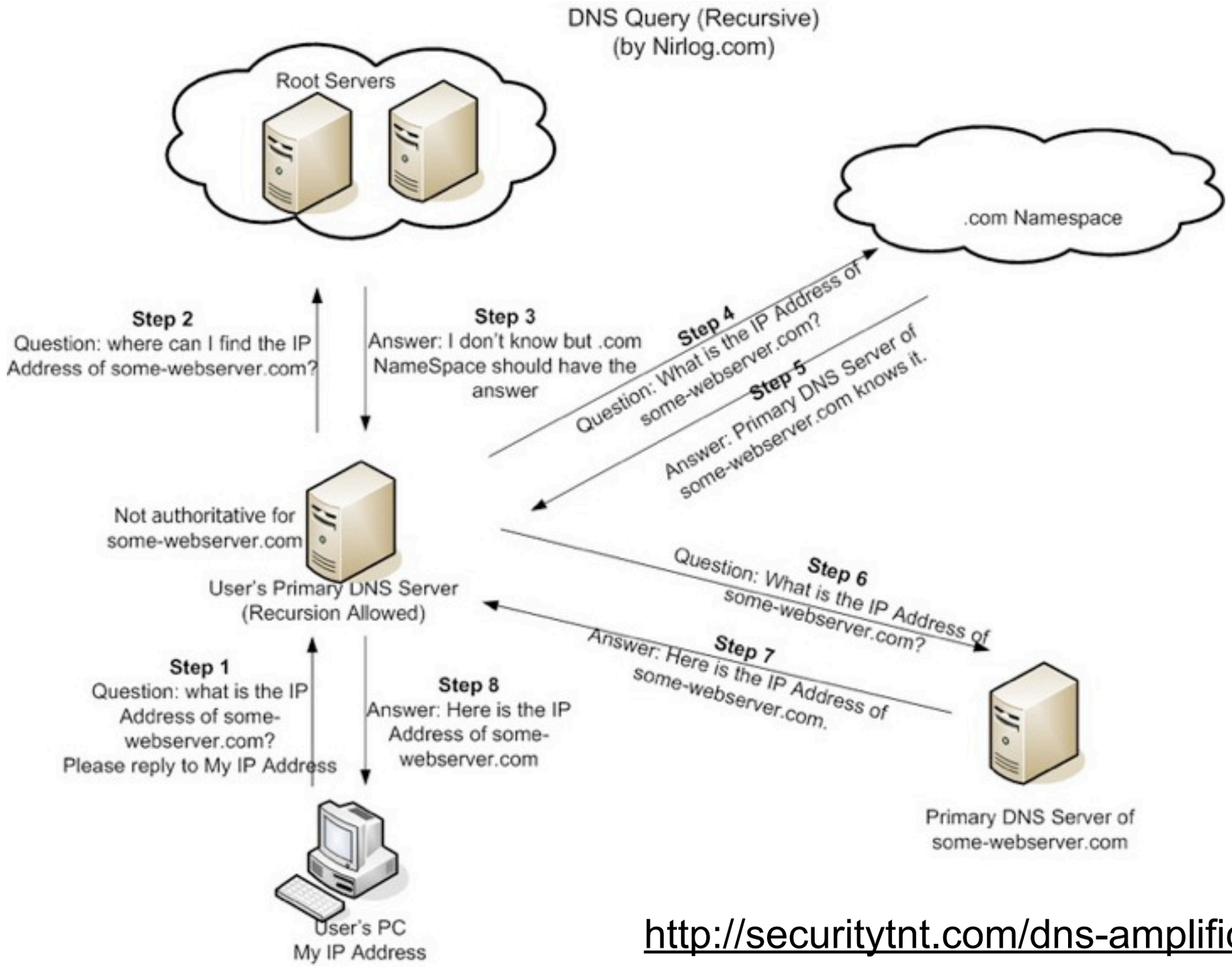
- Education
  - Bachelor : Comp. Eng. KKU
  - Master : Comp. Sci. CU
- Certification and Award
  - COMTIA Security+
  - Asia Pacific Information Security Leader Achievements 2011 (ISLA) by (ISC)2
- Membership
  - APWG, ShadowServer, OWASP, MSCP, MedSec, CSA - Thailand Chapter (Secretariat), TISA (Subcommittee)

About me (Experience)

- >10 years in IT Security
  - Incidents response
  - Research
  - Speaker and writer
  - …
- Working for the security section at the National Health Information System project, under NECTEC
- OWASP Thailand Chapter Leader

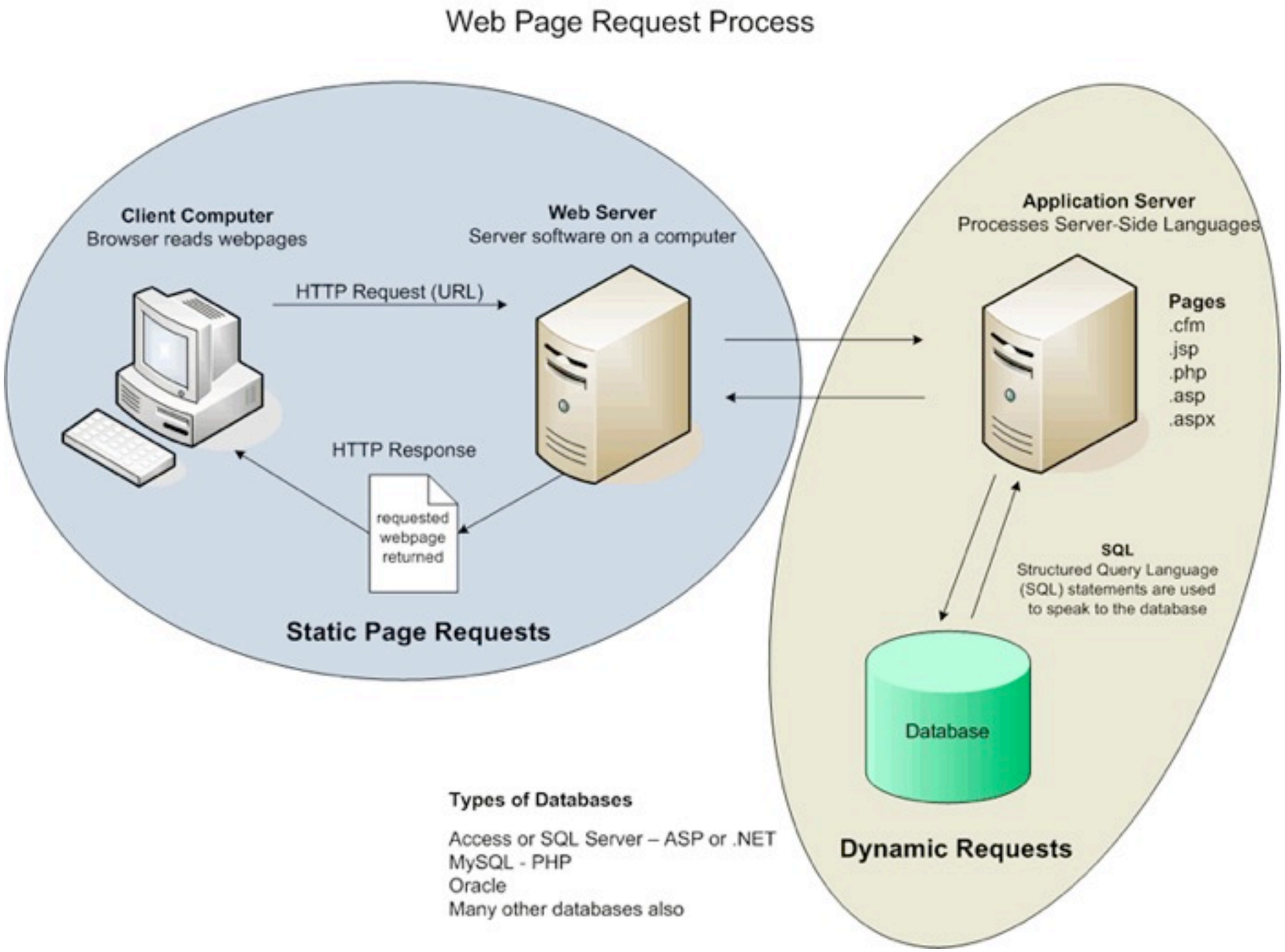
International Collaborations

How does DNS work?



http://securitytnt.com/dns-amplification-attack/

Web Page Request Process



http://cmairscreate.com/webPageRequest.html

What is Fast Flux Hosting?

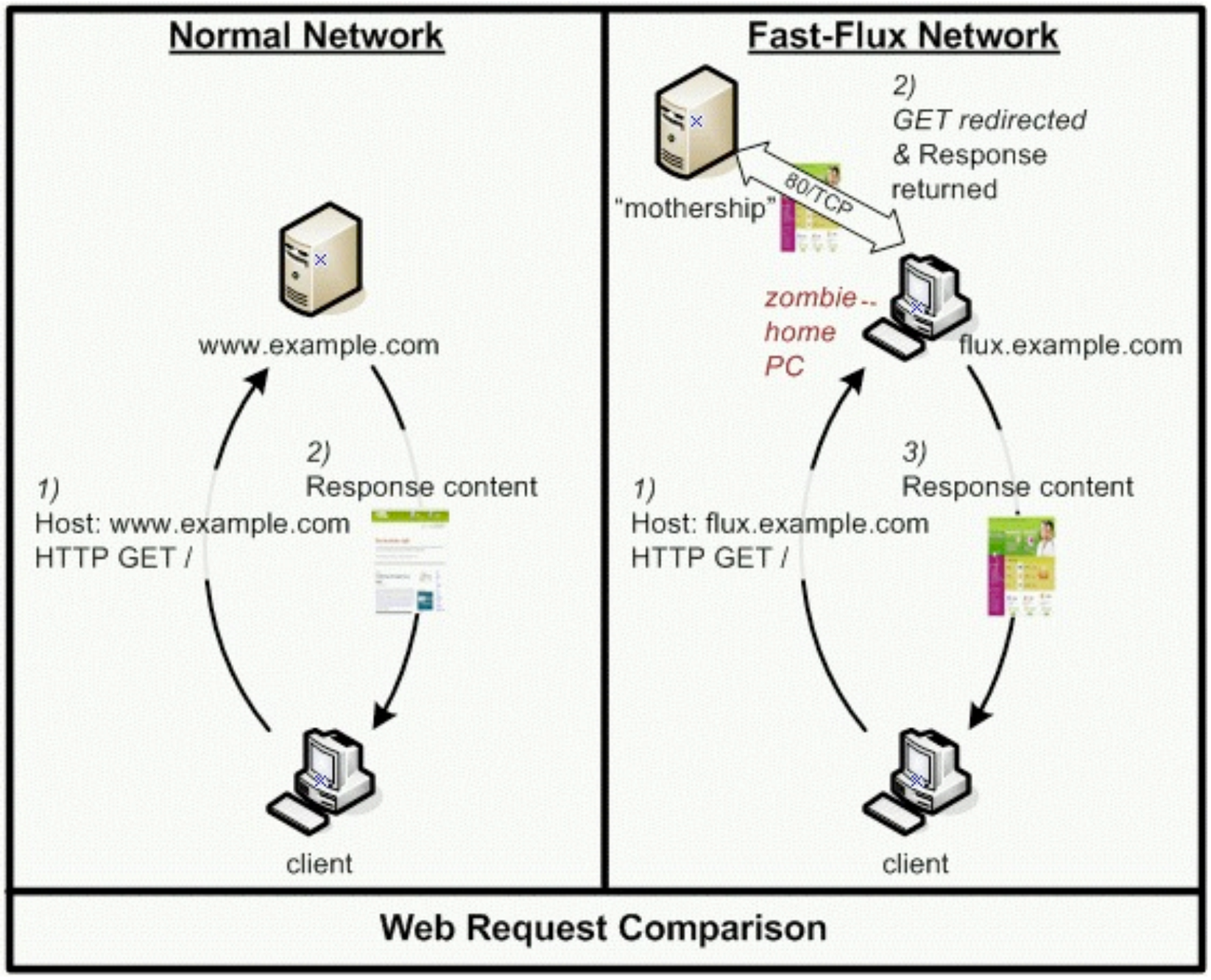
- An evasion technique
- Goal
  - Avoid detection and take down of web sites used for illegal purposes
- Technique
  - Host illegal content at many sites
  - Rapidly change pointers (IP addresses) so that no one site is used long enough to isolate and shut down

Types of Fast Flux

- Single flux
  - Basic fast flux hosting
    - IP addresses of illegal web sites are fluxed
  - Name Server (NS) fluxing
    - IP addresses of DNS name servers are fluxed

- Double flux
  - IP addresses of web sites and name servers are fluxed

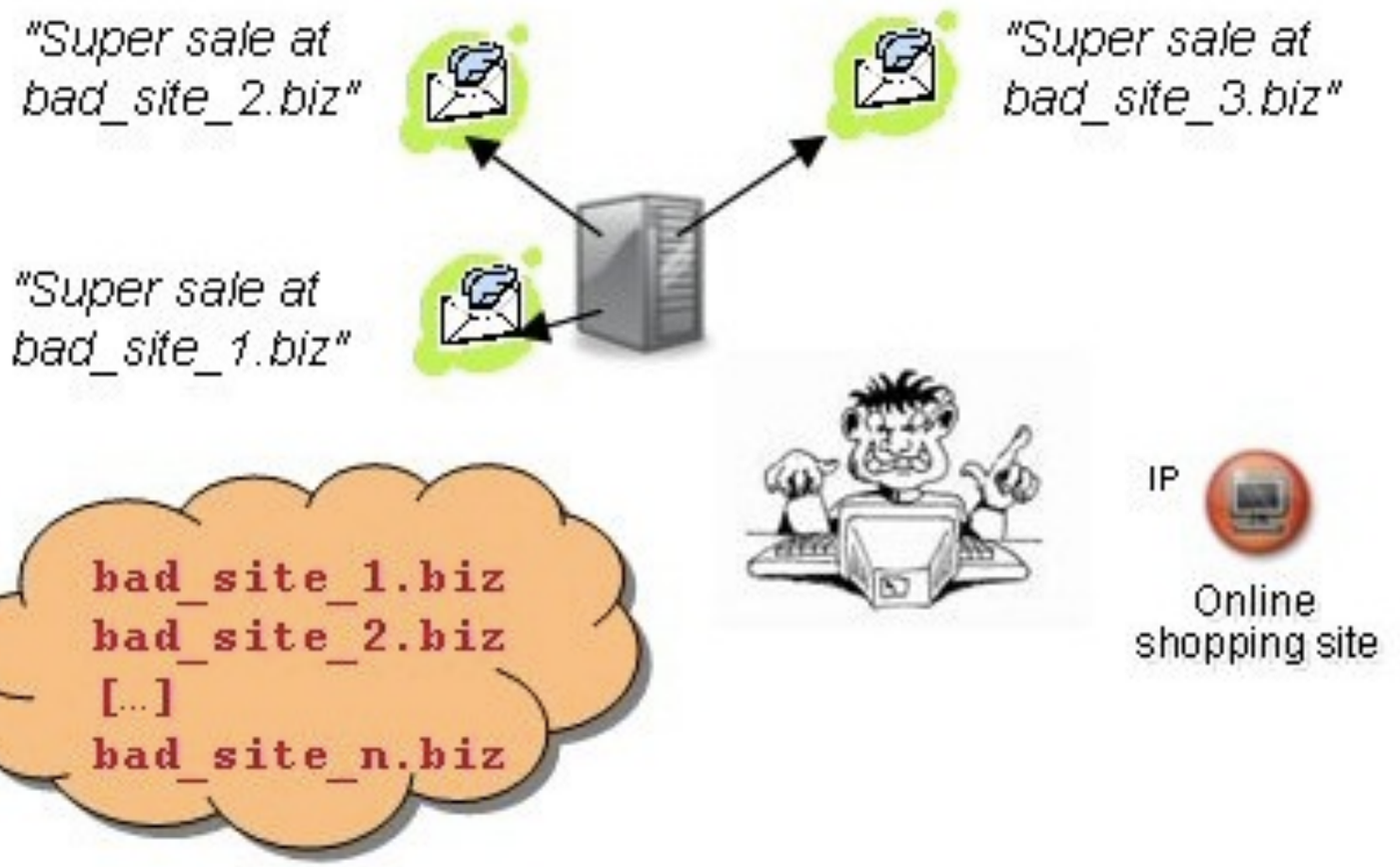
Fast Flux



http://www.honeynet.org/node/134

Several domains for a single IP (Single flux)

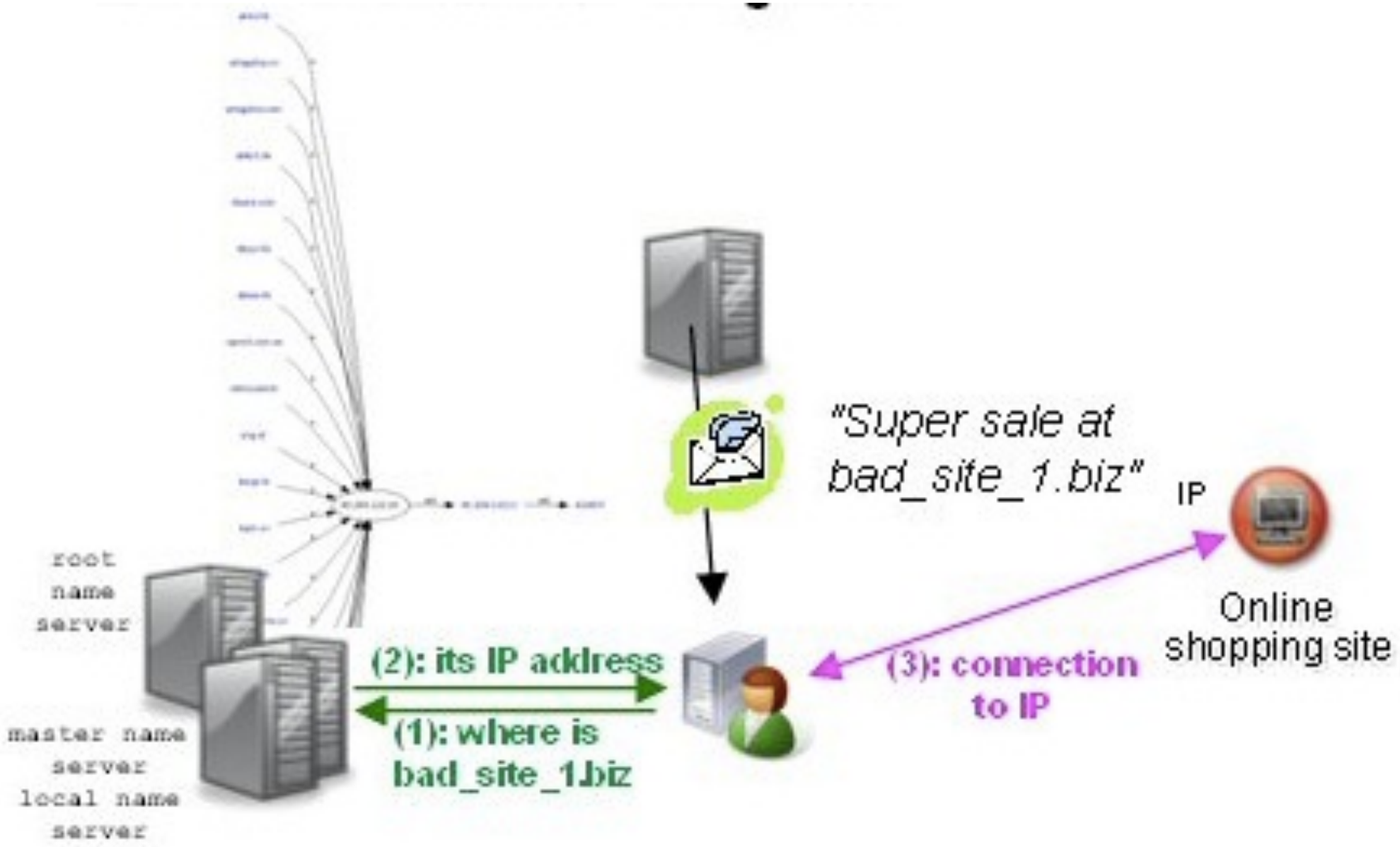
- A spammer owns a lot of domain names
- Only one machine contains his site
- The URL is changed for each message



http://blogs.mcafee.com/mcafee-labs/from-fast-flux-to-rockphish-part-1

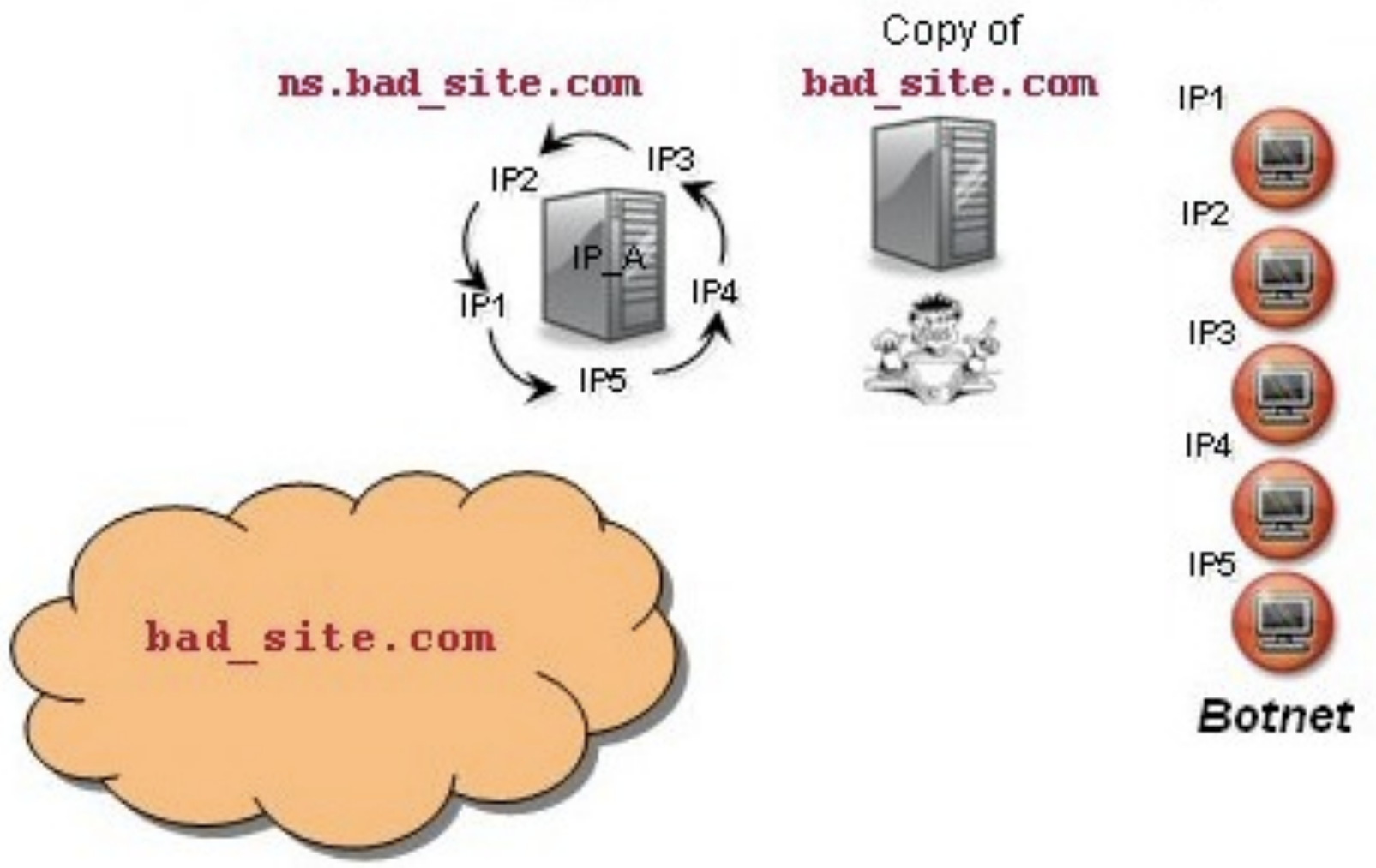
Several domains for a single IP (Single flux)

- When a victim tries to follow the linked provided



Several IPs for a single domain (Single flux)

- Attacker has just one domain and a network of compromised machines (botnet)
- Short DNS expiry dates

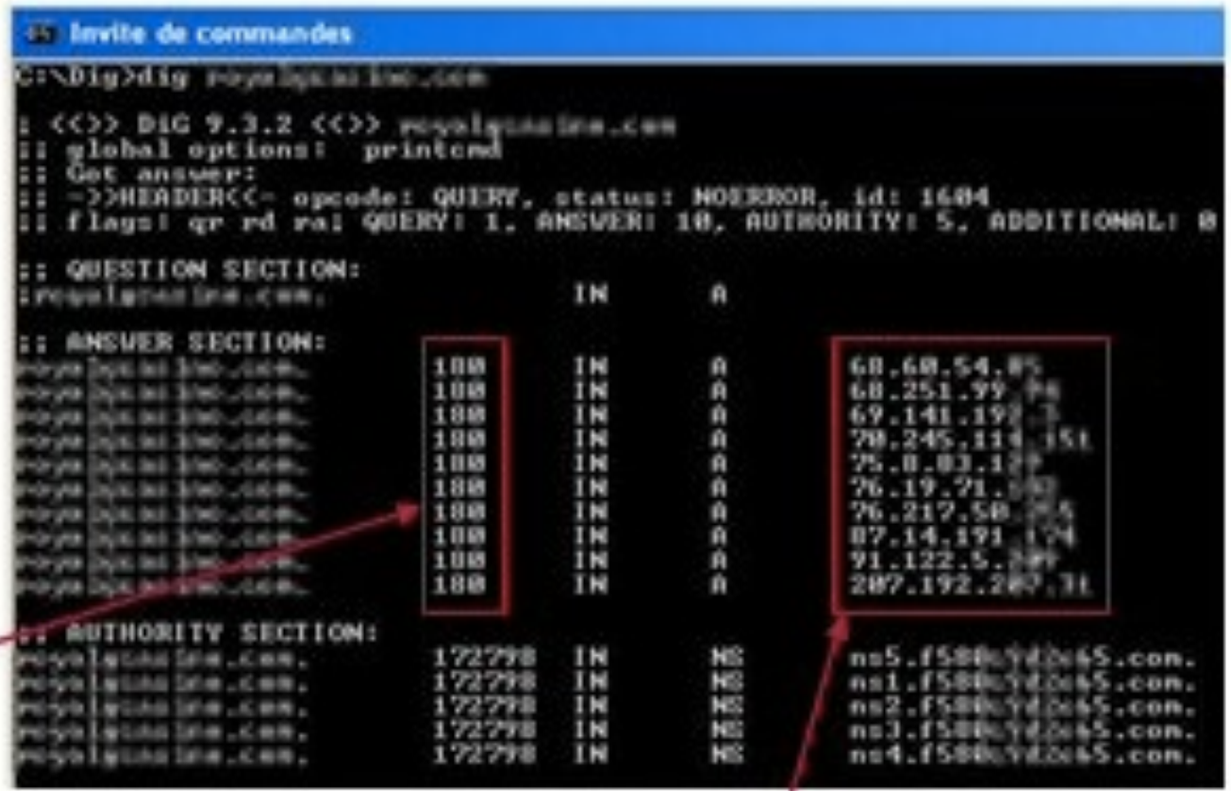


Several IPs for a single domain (Single flux)

- Victim tries to reach the mirror site (bad_site.com)

Several IPs for a single domain (Single flux)

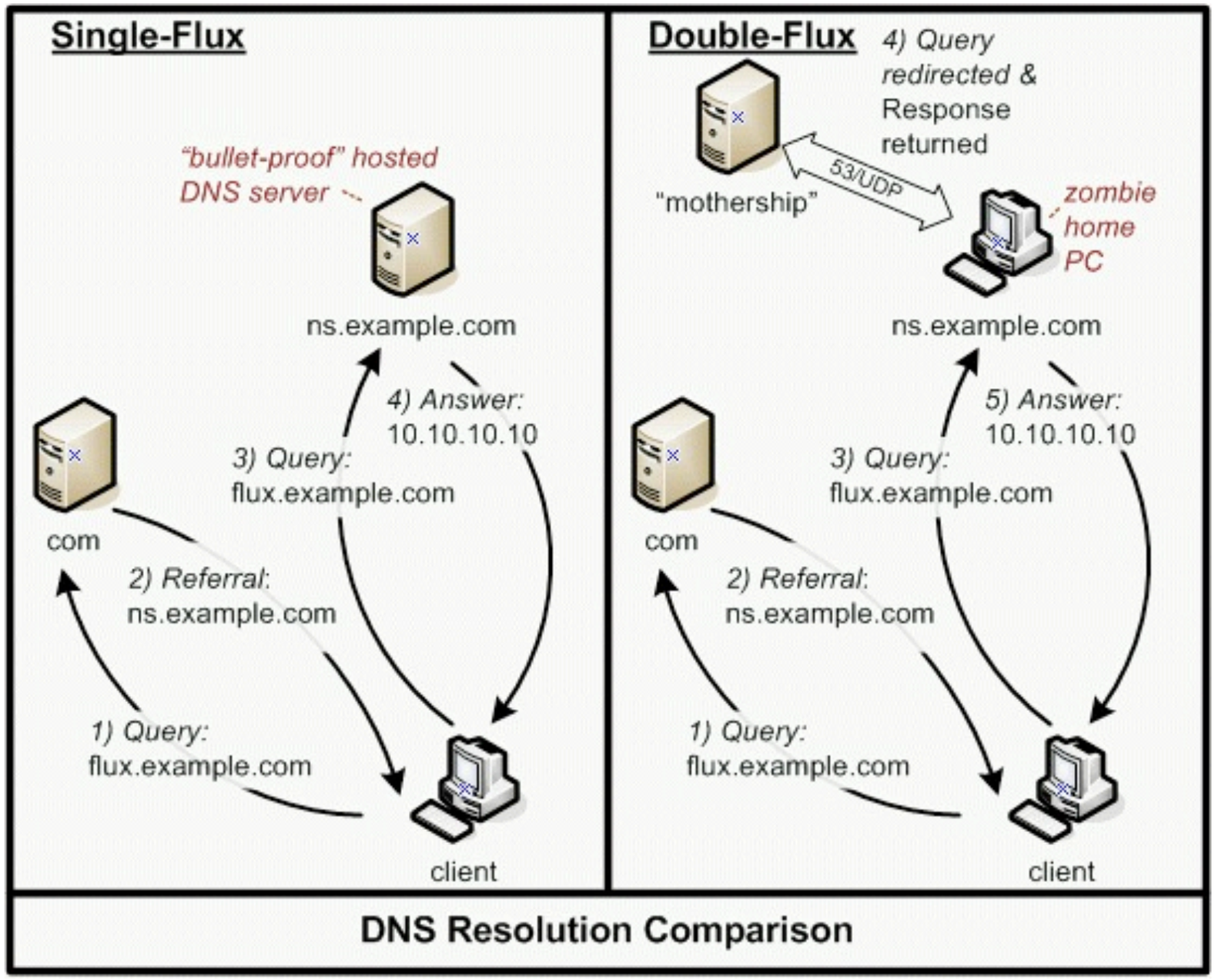
- Example of an online casino site



Time to Live < 1800 s

Many correspondences for a single canonical name
Very different IP adresses

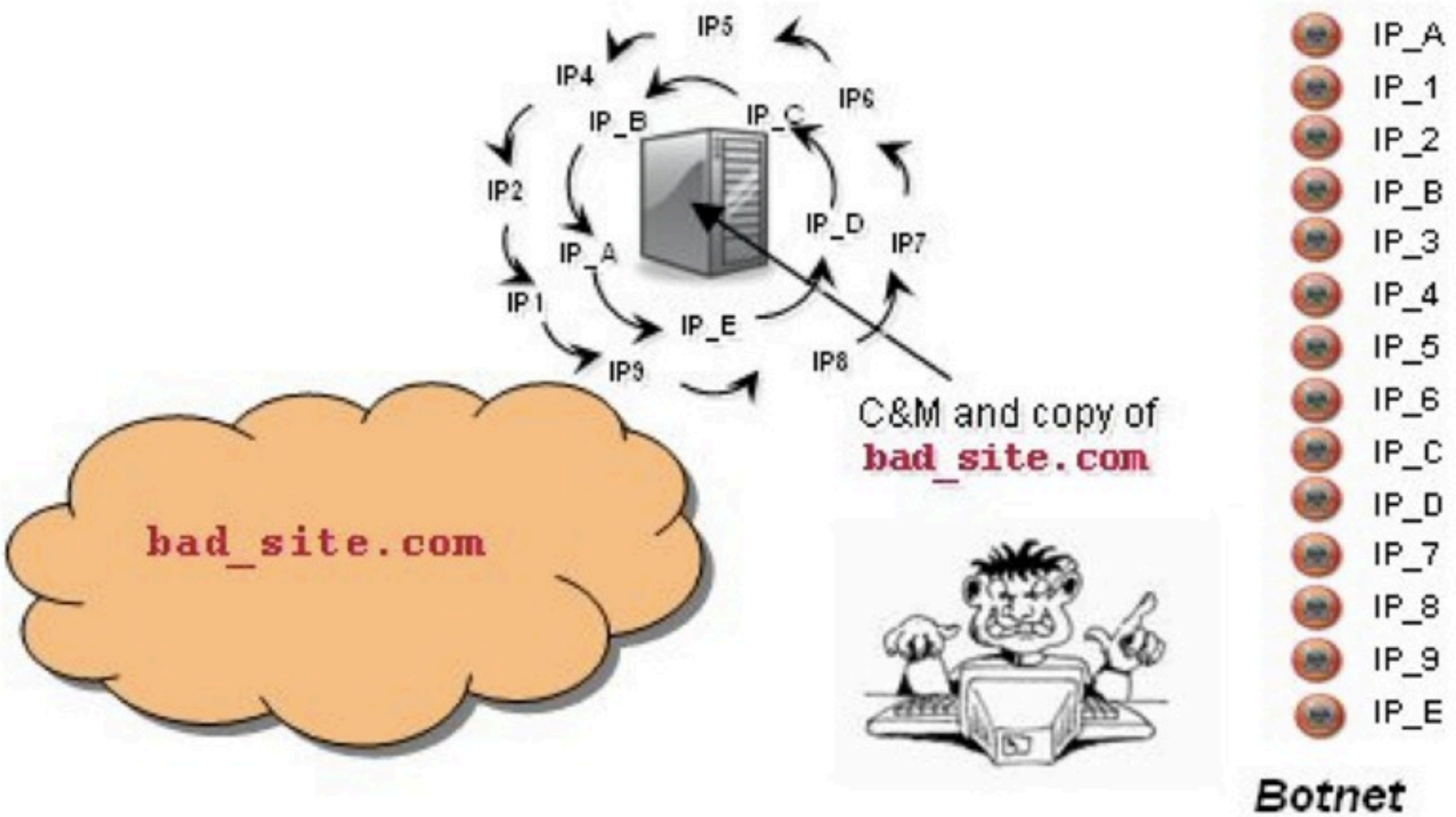
Double Fast Flux



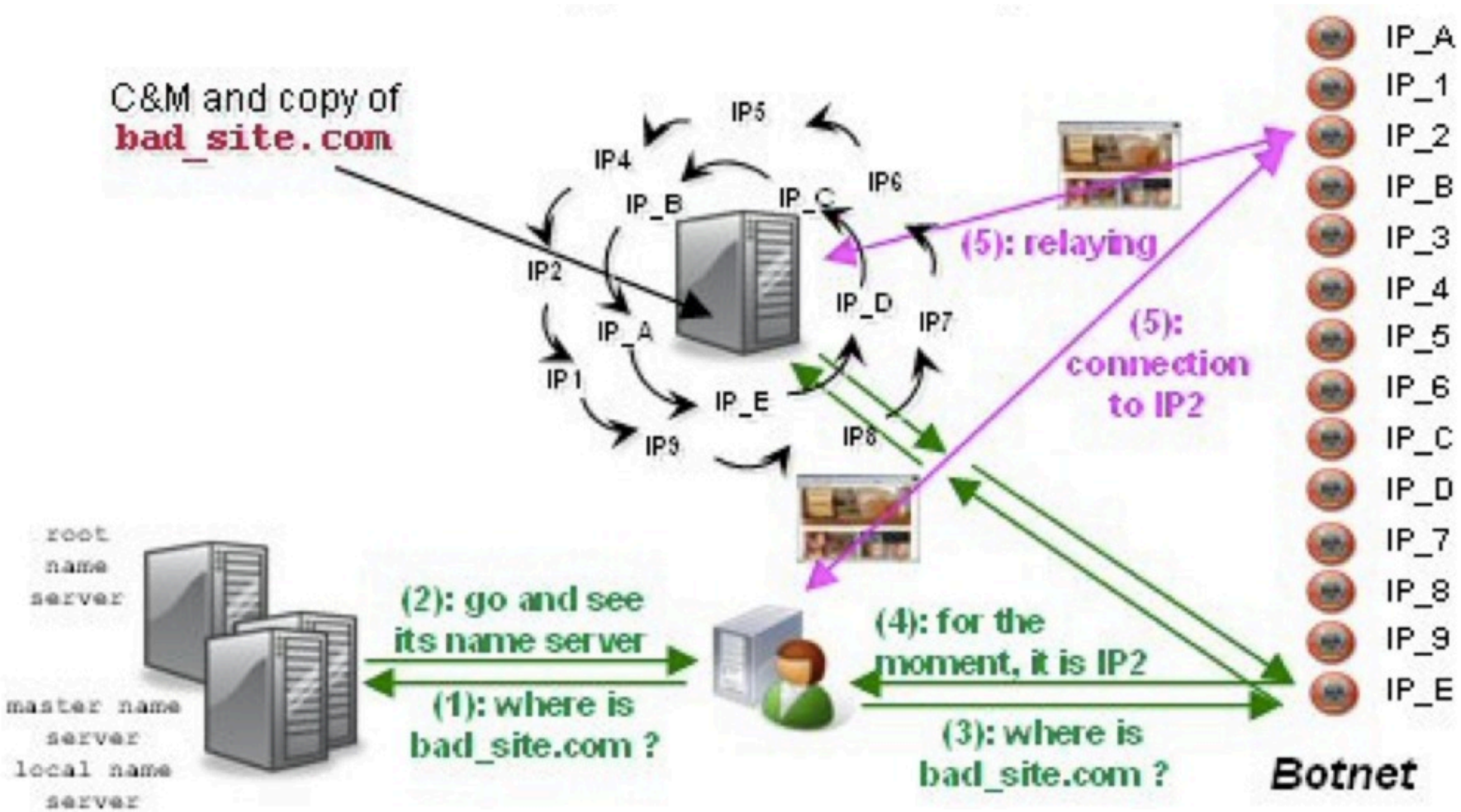
http://www.honeynet.org/node/135

Several IPs for a single name server (double-flux)

- IP_A to IP_E - fast flux on name servers
- IP_1 to IP_9 - fast flux on web site

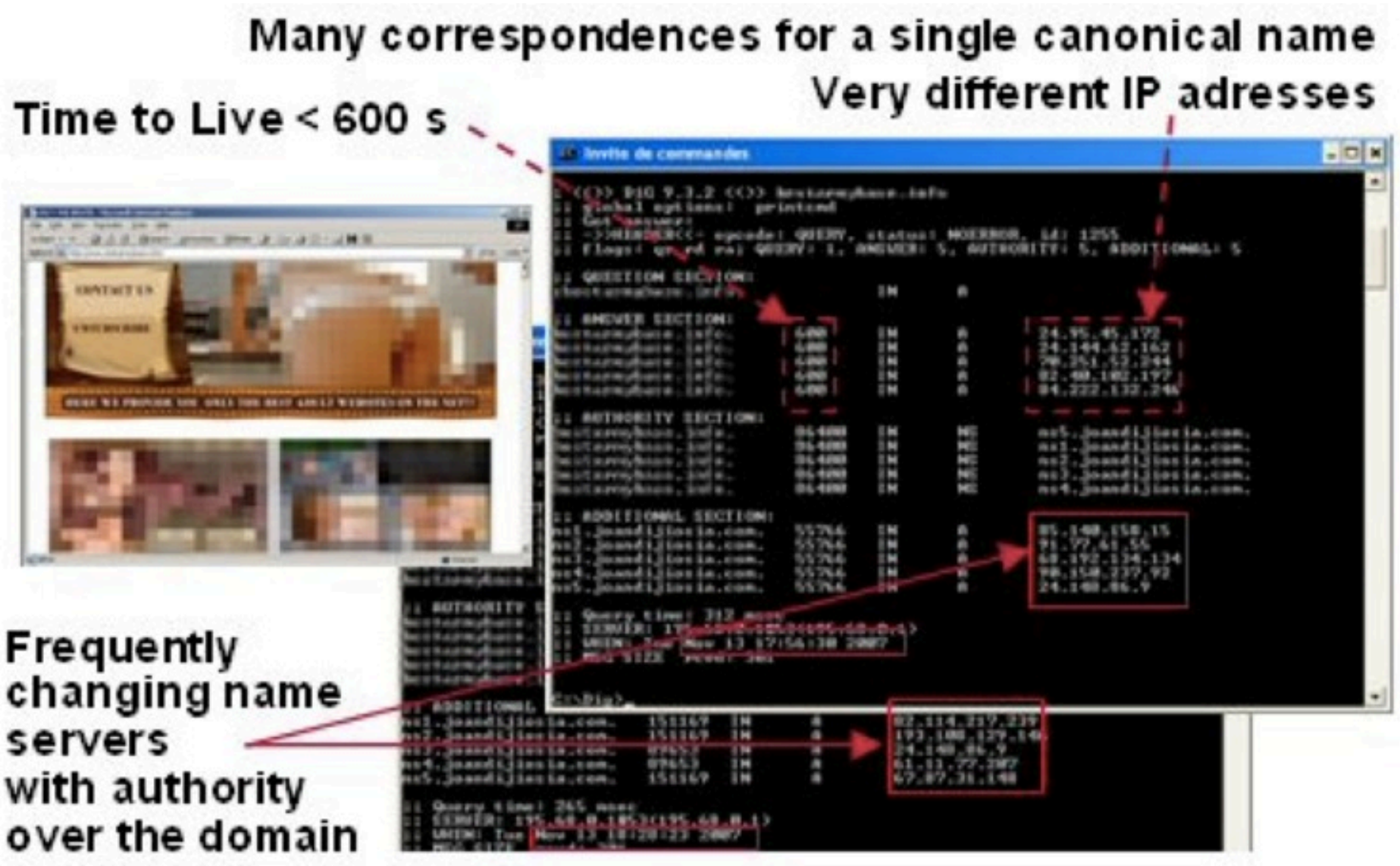


Several IPs for a single name server (double-flux)



Several IPs for a single name server (double-flux)

- 2 “dig” commands launched a few minutes apart show us the result



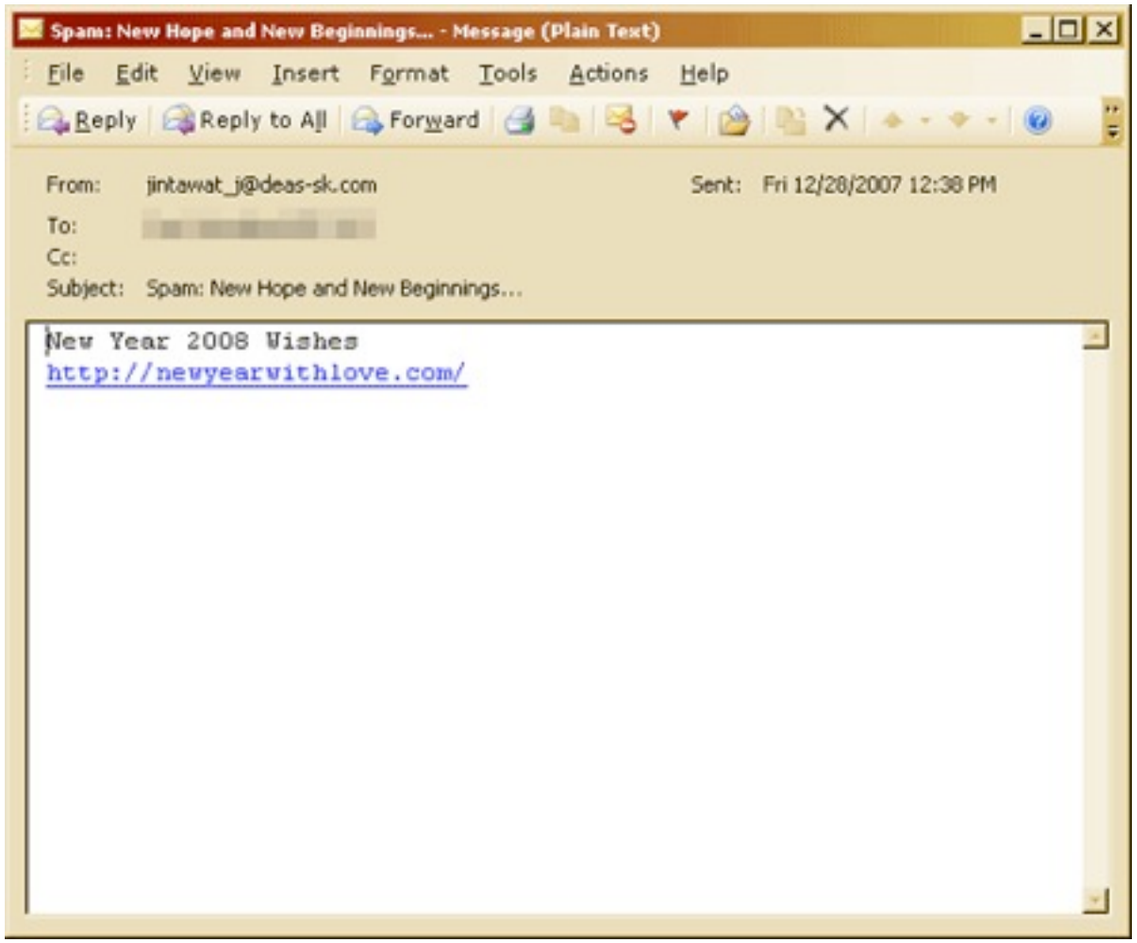
Case study 1

- Spam mails were sent
- Domain names of the fake web sites were added and shared to a root DNS server
- Single fast flux


```
angerfollow.com
beautybegan.com
byoperate.com
chickher.com
elementgrand.com
instantsilent.com
interestquiet.com
roundtoward.com
twoinstant.com
```

Case study 2

- Storm worm (Nuwar)
- Double fast flux



Answer records

name	class	type	data	time to live
newyearwithlove.com	IN	NS	ns9.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns8.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns7.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns6.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns5.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns4.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns3.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns2.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns13.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns12.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns11.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns10.newyearwithlove.com	131485s (1d 12h 31m 25s)
newyearwithlove.com	IN	NS	ns.newyearwithlove.com	131485s (1d 12h 31m 25s)

Mitigation

- Prevent automated (scripted) changes
- Set a minimum allowed TTL
- Implement or expand abuse monitoring
- Establish policies to enable blocking of TCP 80 and UDP 53 into user-land networks if possible (ISP)
- Block access to controller infrastructure (motherships, registration, and availability checkers) as they are discovered. (ISP)
- Improving domain registrar response procedures, and auditing new registrations for likely fraudulent purpose. (Registrar)
- Increase service provider awareness, foster understanding of the threat, shared processes and knowledge. (ISP)

Detection

- Fast flux hosting exploits domain name resolution and registration services to abet illegal activities
- Current methods to thwart fast flux hosting by detecting and dismantling botnets are not effective
- Fast flux hosting hampers current methods to detect and shut down illegal web sites
- Frequent modifications to NS records and short TTLs in NS A records in TLD zone files can be monitored to identify possible abuse
- Blocking automated changes to DNS info and enforcing a minimum TTL > 30 minutes are effective countermeasures but are not uniformly practiced

Detection (more)

- Implement IDS (Snort) with signature

```
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;)
```

  - Base64 of “helloflux” is “aGVsbG9mbHV4IAO”

- Trace the destination using

```
$ 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}
```

http://www.honeynet.org/node/144

Recommendations

- Timely response to domain takedown requests by shutdown authorities and/or law enforcement
- Proactively use available data to identify and shut down malicious domains
- Share fraudulent domain registration information with law–enforcement
- Protect your customers from being phished
- Prohibit/minimize use of fast–flux domains

How registrants can avoid falling victim to registrar impersonation (1/2)

- Do not click on hyperlinks included in email
- Use an email client that
  - offers anti-spam and antiphishing features
  - is able to reveal the hyperlink reference associated with displayed text or images include in an email

```
<A HREF="http://iwillscamu.tld">www.example.com</a>
<A HREF="http://192.168.2.3">www.example.com</a>
```

- Read email carefully (Poor grammar and punctuation)
- Do not trust an email simply because it is personalized
- Do not divulge personal or account information in any web submission form until you verify the page is legitimate

How registrants can avoid falling victim to registrar impersonation (2/2)

- Use SSL on web page and also verify the authenticity of the digital certificate associated with SSL pages
- If intend to purchase a domain name using a credit card, choose the registrar that provides a secure process to purchase and must protects customer's info
- Report suspected phishing emails to your registrar or antiphishing organizations such as the APWG, the Phish Report Network, PhishTank,or your local CERT

Follow me

Name : Kitisak Jirawannakool

Facebook : http://www.facebook.com/kitisak.note

Email : kitisak.jirawannakool@nectec.or.th

jkitisak@gmail.com

Weblog : http://foh9.blogspot.com

Twitter : @kitisak

Q/A