SSAC Fast Flux Activities

Dave Piscitello
ICANN SSAC

Long and Winding Road…

- January 2008: SAC 025 Fast Flux Hosting and DNS
  - Result of 4 month study and cooperative work with APWG
  - Characterizes Fast Flux (FF) as an evasion technique
  - Describes the anatomy of single and double flux attacks
  - Initial findings include:
    - Frequent NS record changes and short TTLs are indicators of potential abuses of name services
    - Preventing automated changes to DNS information and changes that set longer minimum TTLs for NS A records appear to be effective
- January – October 2008
  - SSAC studies FF with anticrime community (APWG, ISOI)
  - SSAC participates in GNSO FF WG (report pending)

Lessons learned

- Evasion technique has evolved
  - Not all flux attacks are "fast"
- Original characterization of fast flux attacks is too narrow
  - Short TTLs for NS records are found in production networks as well as attack networks
  - Certain production networks frequently change IP addresses of name servers
  - Some attack networks "flux" slowly
    - E.g., networks can "flux" in response to loss of communication between bots and their command and control computers
- Original set of characteristics: too coarse, too few…
  - Community has studied fast flux intensely over past 9 months
  - Time to re-examine and refine original definition of fast flux

Short TTLs in Production Networks

Short TTLs in A and CNAME records, longer TTLs in NS records

```
aol.com.          60       IN      A       207.200.94.38
aol.com.          60       IN      A       205.188.142.182
aol.com.          3600     IN      NS      dns-06.ns.aol.com.
aol.com.          3600     IN      NS      dns-07.ns.aol.com.

gmail.com.        60       IN      A       66.249.91.83
gmail.com.        60       IN      A       64.233.161.83
gmail.com.        60       IN      A       209.85.171.83
gmail.com.        345600   IN      NS      ns2.google.com.
gmail.com.        345600   IN      NS      ns4.google.com.
gmail.com.        345600   IN      NS      ns3.google.com.
```

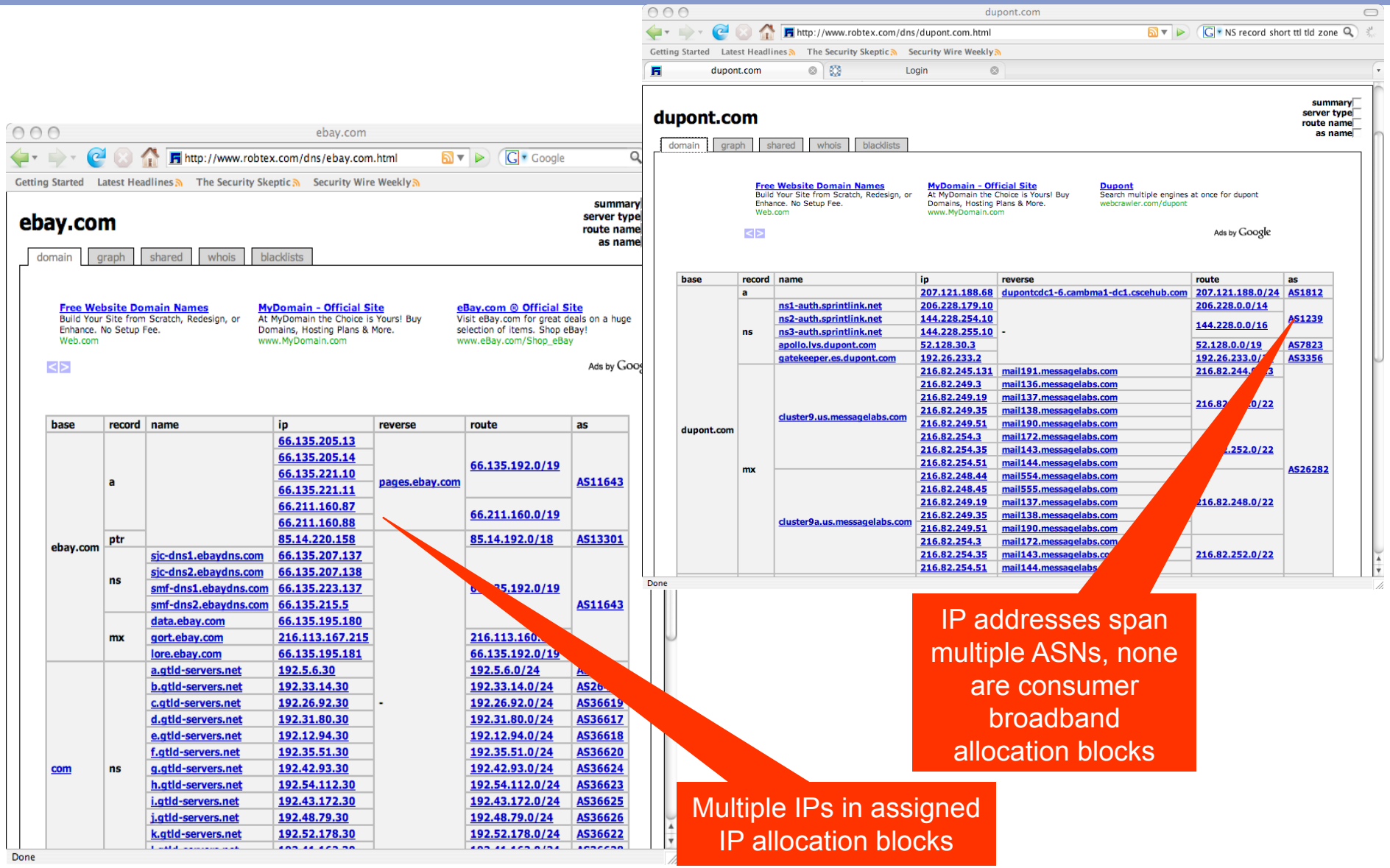
Short TTLs in A and CNAME records

```
www.irs.gov.                  600 IN  CNAME  www.irs.gov.edgesuite.net.
www.irs.gov.edgesuite.net. 10800 IN  CNAME  a321.g.akamai.net.
a321.g.akamai.net.            20 IN  A      204.2.148.144
a321.g.akamai.net.            20 IN  A      204.2.148.106
g.akamai.net.               1000 IN  NS     n0g.akamai.net.
g.akamai.net.               1000 IN  NS     n4g.akamai.net.
```

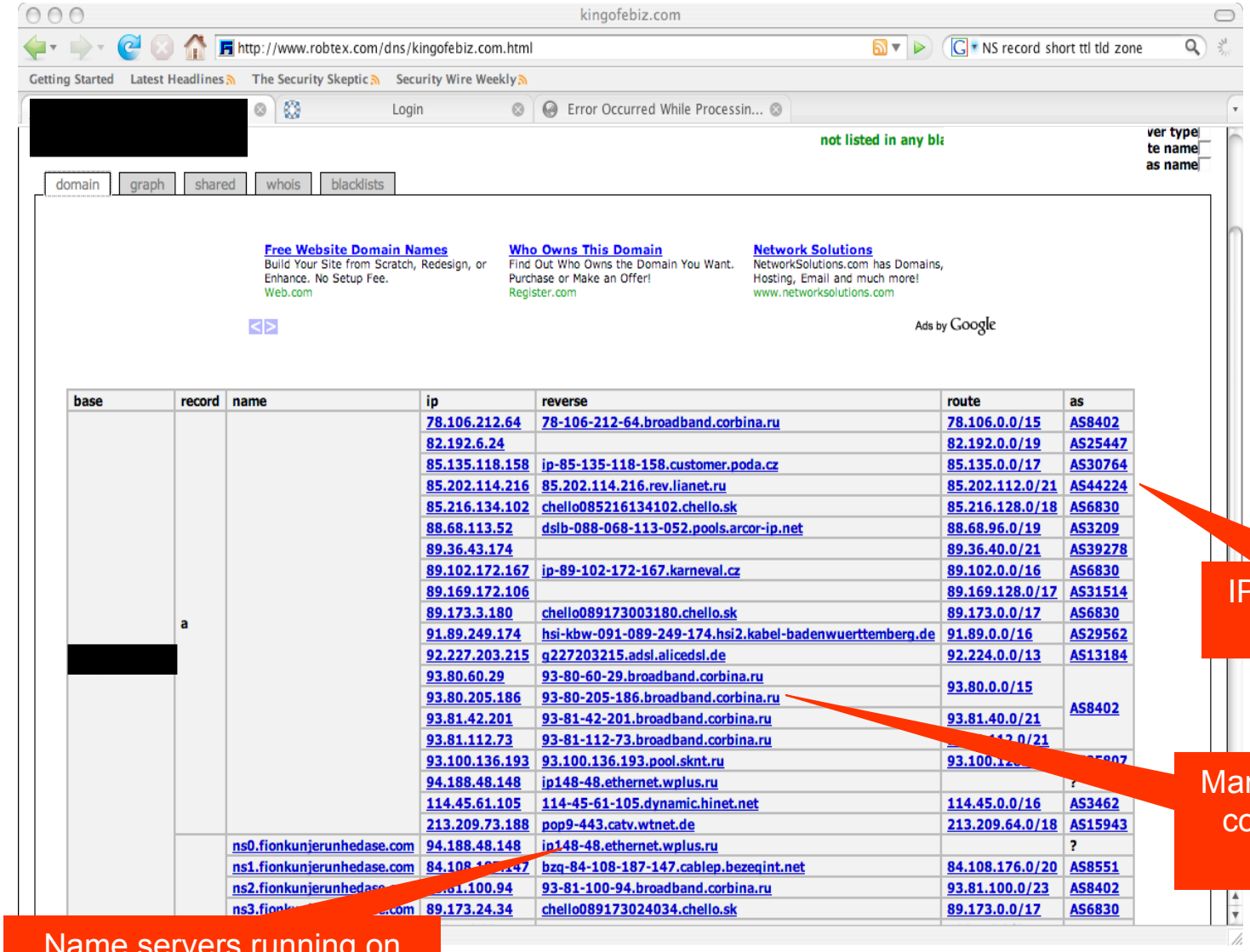
Know the Enemy: Study Attacker Mentality

- "Why use my resources when I can use yours?"
  - Your (compromised) PCs are my bots
  - Your (compromised) servers host my web sites
  - Your (compromised) domain registration accounts hide my DNS configurations
  - Your credit cards pay for my domains and hosting services
- Any public IP address from any provider or assigned IP space will do
  - Dynamically assigned public addresses enhance deception
  - The more the better applies to both IP addresses and Autonomous Systems

Production Networks with Multiple IPs and ASs



Sample Fast Flux Attack Domain



base	record	name	ip	reverse	route	as
[redacted]	a		78.106.212.64	78-106-212-64.broadband.corbina.ru	78.106.0.0/15	AS8402
			82.192.6.24		82.192.0.0/19	AS25447
			85.135.118.158	ip-85-135-118-158.customer.poda.cz	85.135.0.0/17	AS30764
			85.202.114.216	85.202.114.216.rev.lianet.ru	85.202.112.0/21	AS44224
			85.216.134.102	chello085216134102.chello.sk	85.216.128.0/18	AS6830
			88.68.113.52	dslb-088-068-113-052.pools.arcor-ip.net	88.68.96.0/19	AS3209
			89.36.43.174		89.36.40.0/21	AS39278
			89.102.172.167	ip-89-102-172-167.karneval.cz	89.102.0.0/16	AS6830
			89.169.172.106		89.169.128.0/17	AS31514
			89.173.3.180	chello089173003180.chello.sk	89.173.0.0/17	AS6830
			91.89.249.174	hsi-kbw-091-089-249-174.hsi2.kabel-badenwuerttemberg.de	91.89.0.0/16	AS29562
			92.227.203.215	g227203215.adsl.alicedsl.de	92.224.0.0/13	AS13184
			93.80.60.29	93-80-60-29.broadband.corbina.ru	93.80.0.0/15	AS8402
			93.80.205.186	93-80-205-186.broadband.corbina.ru		
			93.81.42.201	93-81-42-201.broadband.corbina.ru	93.81.40.0/21	
			93.81.112.73	93-81-112-73.broadband.corbina.ru		
			93.100.136.193	93.100.136.193.pool.sknt.ru	93.100.12[redacted]	
			94.188.48.148	ip148-48.ethernet.wplus.ru		?
			114.45.61.105	114-45-61-105.dynamic.hinet.net	114.45.0.0/16	AS3462
			213.209.73.188	pop9-443.catv.wtnet.de	213.209.64.0/18	AS15943
		ns0.fionkunjerunhedase.com	94.188.48.148	ip148-48.ethernet.wplus.ru		?
		ns1.fionkunjerunhedase.com	84.108.[redacted]	bzq-84-108-187-147.cablep.bezeqint.net	84.108.176.0/20	AS8551
		ns2.fionkunjerunhedase.com	[redacted].100.94	93-81-100-94.broadband.corbina.ru	93.81.100.0/23	AS8402
		ns3.fionkunjerunhedase.com	89.173.24.34	chello089173024034.chello.sk	89.173.0.0/17	AS6830

IP addresses span multiple ASNs,

Many IP addresses from consumer broadband allocation blocks,

Name servers running on dynamically assigned IPs

"resource-full" Fast Flux Attack Networks

2008_06_unique_asns_per_host.csv

	A	B
1	UNIQUE ASNs PER HOST - JUNE 2008	
2	begcasino.com	377
3	amoreocasino.com	375
4	byecasino.com	372
5	casinoeuroprime.com	371
6	butcasino.com	368
7	atacasino.com	368
8	boacasino.com	367
9	besttopgamer.net	367
10	bocecasino.com	366
11	bigvegasvip.com	366
12	bktcasino.com	365
13	bltcasino.com	365
14	armcasino.com	365
15	casinoroyalgrand.com	365
16	burcasino.com	365
17	augcasino.com	365
18	casinoroyalroad.com	364
19	casinoexoticslots.com	363
20	avocasino.com	363
21	blkcasino.com	363
22	bigvegasmoney.com	363
23	bigvegascasinos.com	363
24	arvcasino.com	362
25	boqcasino.com	362
26	bkgcasino.com	362
27	bplcasino.com	361
28	555lasvegas.com	361
29	befcasino.com	361
30	asccasino.com	361
31	auxcasino.com	360
32	baroccocasino.com	359
33	buncasino.com	358
34	atecasino.com	357
35	beluckygamer.com	357
36	asvcasino.com	357
37	bsccasino.com	357

2008_06_distinct_hosts.csv

	A	B
1	UNIQUE IP ADDRESSES PER DOMAIN	
2	breathless-exploit.com	1742
3	breathless-detection.com	1721
4	blucpan.com	1713
5	brand-new-feat.com	1710
6	burnmade.com	1709
7	bornprove.com	1704
8	breadbegan.com	1701
9	assistance-best.com	1694
10	breakthrourequired.com	1691
11	breathlessuncovering.com	1691
12	asopein.com	1689
13	butisland.com	1689
14	bottomcow.com	1686
15	assistancepleasant.com	1680
16	brisinnovation.com	1679
17	brothercotton.com	1677
18	bleogry.net	1676
19	broadimagine.com	1673
20	blissful-years.com	1672
21	bright-advanced.com	1672
22	aspectfast.com	1670
23	bright-innovative.com	1667
24	assistance-pleasant.com	1666
25	ascorow.com	1665
26	boomifunds.com	1664
27	booming-funds.com	1664
28	bringdivide.com	1662
29	ask-meds.com	1658
30	blissful-times.com	1658
31	broadeconomical.com	1658
32	brownfoxpro.com	1657
33	boardborn.com	1656
34	broadhear.com	1654
35	answedynamic.com	1653
36	buildeffect.com	1649

Findings

- Certain techniques associated with "fast flux" are common to attack and production networks
  - Short TTLs
  - Rapid NS record changes
  - Multiple IPs and ASNs
- What additional characteristics can we apply to positively identify attack networks?
  - Characteristics of the member nodes?
  - Distribution of the member nodes?
  - Domain registration?

Characteristics of Fast Flux Attack Nets

- Some network nodes run on compromised hosts
  - Nodes include proxies, DNS and web servers, C&Cs
- Network nodes change to sustain the network's lifetime, to spread network software, and to conduct attacks
  - Member nodes are monitored to determine that a host has been shut down
- Network node IP addresses changed (frequently) via DNS (low TTLs)
- Network nodes distributed across multiple ASNs
- Network nodes distributed across multiple IP allocation blocks
  - in-addrs of IPs fall within consumer broadband allocation blocks
- WHOIS characteristics
  - Domain registration is "recent"
  - Contact information quality and accuracy is poor
  - Registration was fraudulently altered or purchased

Not all characteristics must be present to positively identify a network as a fast flux attack network

Distinguishing Good Actors from Bad

- Why do good actors "fast flux"?
  - Resilient and adaptive are desirable characteristics!
- We know that good actors
  - Use short TTLs
  - Operate networks that use multiple IP assignment blocks
  - Operate networks that span multiple autonomous systems
- However, good actors typically
  - Use IP space that RIRs have assigned to them
  - Do not hack into other actors' systems
  - Do not hack into registrar account login pages
  - Do not use stolen credit cards to register domains
  - Do not host name and web servers on dynamically assigned IPs

Dealing with Fast Flux Attacks

- Focus of ongoing studies

  (Some of these topics are being considered in GNSO FFWG):

  - Data sharing and analysis among registry, registrar and anticrime/antiphishing communities
  - Reduce fraudulent registrations and account theft
  - Accelerated domain suspension processing
  - Algorithms and automated means of detecting domains used in fast flux attacks
    - How effective are current detection algorithms?
    - Can automation adapt to change as quickly as attackers?
    - What is an acceptable false positive rate?
    - Can we couple automation with manual inspection to further reduce probability of false positives?

Example FF detection formula

- Mannheim formula
  - method for separating FF and non-FF domains with a very high detection accuracy (99.98%)
  - Apply to multiple resolutions of a domain name (FQDN) to see if additional A records or ASNs appear

f(x) = 1.32*n(A) + 18.54*n(ASN) + 0 *n(NS)
n(A) = # of unique IPs, n(ASN) = # of ASNs,…
FF attack network when f(x) > 142.38

DNS RESOURCE RECORD					ASN
yes2-quality-meds.com	120	IN	A	85.216.214.249	AS6830
yes2-quality-meds.com	120	IN	A	87.123.186.241	AS8881
yes2-quality-meds.com	120	IN	A	87.228.66.14	AS31514
yes2-quality-meds.com	120	IN	A	89.208.196.46	AS12695
yes2-quality-meds.com	120	IN	A	90.184.33.198	AS39554
yes2-quality-meds.com	120	IN	A	91.67.118.9	AS31334
yes2-quality-meds.com	120	IN	A	93.80.26.145	AS4802
yes2-quality-meds.com	120	IN	A	123.192.214.49	AS4780
yes2-quality-meds.com	120	IN	A	123.203.32.77	AS9269
yes2-quality-meds.com	120	IN	A	202.126.117.42	AS4766
yes2-quality-meds.com	120	IN	A	218.190.85.230	AS9304
yes2-quality-meds.com	120	IN	A	218.254.228.85	AS9908
yes2-quality-meds.com	120	IN	A	61.18.221.154	AS9908
yes2-quality-meds.com	120	IN	A	61.224.207.108	AS3462
yes2-quality-meds.com	120	IN	A	69.245.174.253	AS33491
yes2-quality-meds.com	120	IN	A	75.139.130.32	AS20115
yes2-quality-meds.com	120	IN	A	78.53.155.176	AS13184
yes2-quality-meds.com	120	IN	A	79.120.53.160	AS12714
yes2-quality-meds.com	120	IN	A	82.119.105.151	AS6830

20 IPs

17 ASNs

f(x) = 1.32*20 + 18.54*17 + 0

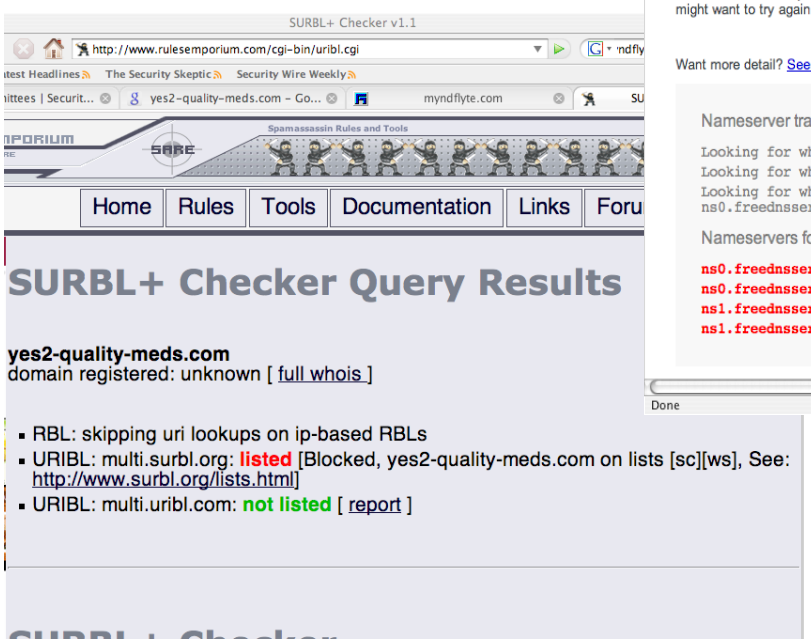
f(x) =341.58

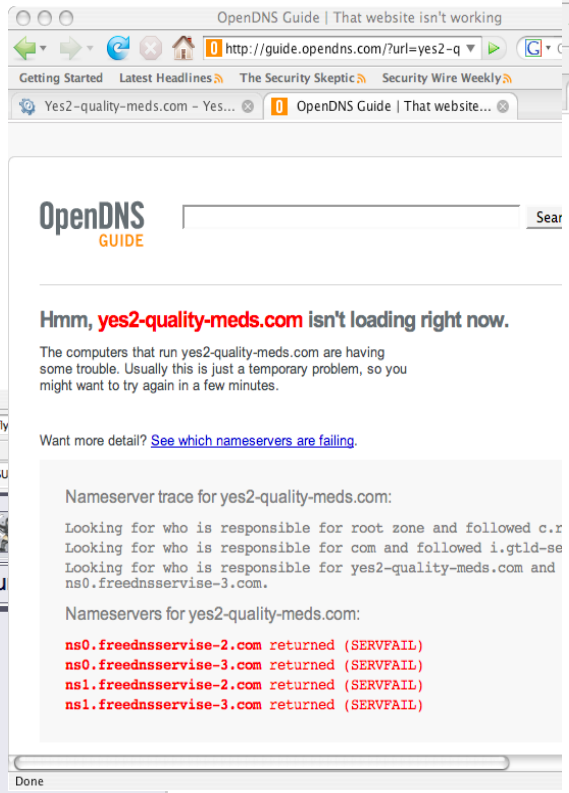
FQDN is an FF attack network

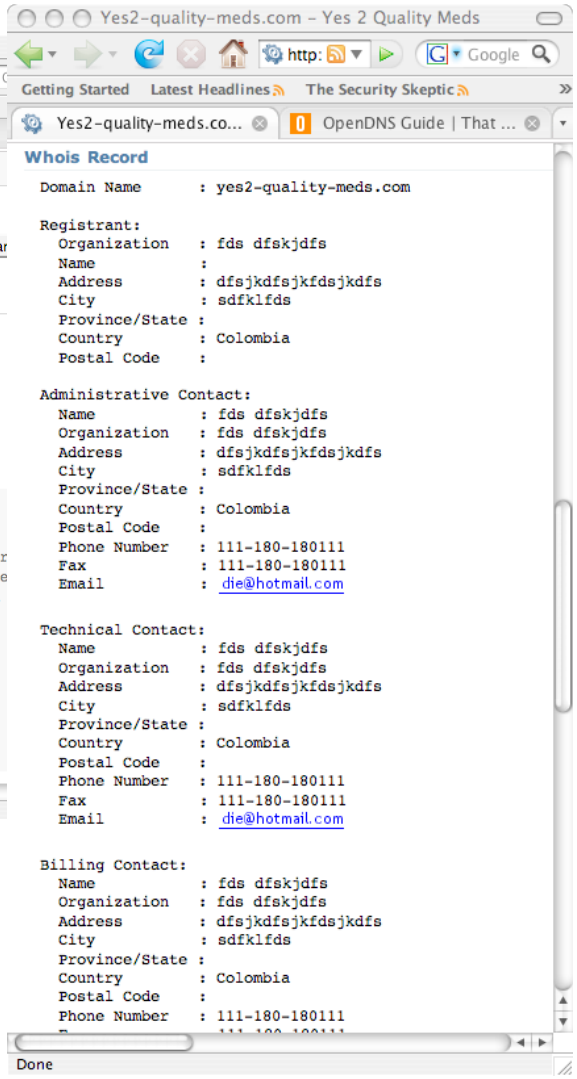
In practice, manual inspection can complement automation that uses this formula to increase detection accuracy…

Manual Inspection

We can complement automation with manual inspection to further reduce probability of false positives…







Questions?