Managing Security Incidents in an IPv6 World

Troopers 15 – IPv6 Security Summit
March 16, 2015

Merike Kaeo

CISO, IID

merike@internetidentity.com

Topics For Today

- Introduction and Background
- Anatomy of Security Incident
- How Does IPv6 Impact Incident Handling
- Lets Take a Look at Passive DNS
- Where Do We Go From Here

Introduction and Background

A Little Background – Merike Kaeo

- Work History
  - National Institute of Health (1988-1993)
  - Cisco (1993-2000)
  - Double Shot Security (2000-2012)
- Industry Recognition
  - Authored “Designing Network Security” by Cisco Press (1999 / 2003)
  - Active Contributor to IETF Standards
  - IPv6 Forum Fellow since 2007
  - Member of FCC CSRIC III (Botnet Remediation) and FCC CSRIC IV (DNS/Routing)

Anatomy of Security Incidents

Incident Response

- It is always best to have a plan in place before something bad happens
- DO NOT PANIC!
- If you set appropriate guidelines now, it will make things a lot easier when a security incident happens

Create a checklist that can be followed when a significant security incident does occur!!

Security Incident Lifecycle

PREPARATION

- Prepare the network
- Create tools
- Test tools
- Prepare procedures
- Train team
- Practice

IDENTIFICATION

- How do you know about the attack?
- What tools can you use?
- What's your process for communication?

CONTAINMENT

- What kind of attack is it?

ERADICATION

- Where is the attack coming from?
- Where and how is it affecting the network?

RECOVERY

- What options do you have to remedy?
- Which option is the best under the circumstances?

POST MORTEM

- What was done?
- Can anything be done to prevent it?
- How can it be less painful in the future?

Most Common Threats and Attacks

- Unauthorized access – insecure hosts, cracking
- Eavesdropping a transmission – access to the medium
  - Looking for passwords, credit card numbers, or business secrets
- Hijacking, or taking over a communication
  - Inspect and modify any data being transmitted
- IP spoofing, or faking network addresses
  - Impersonate to fool access control mechanisms
  - Redirect connections to a fake server
- DOS attacks
  - Interruption of service due to system destruction or using up all available system resources for the service (CPU, memory, bandwidth)

Examples of Sophisticated Attacks

- DNS Changer
  - Install malware on PCs and MACs, changes the DNS, and tries to reconfigure the home gateway's DNS.
  - Point the DNS configurations to DNS resolvers in specific address blocks and use it for their criminal enterprise.
- BroBot DDoS
  - Computers linked to high-bandwidth websites and web-hosting data centers compromised mostly thru outdated versions of Joomla, WordPress and cPanel applications.
  - Then near-invisible code is embedded onto these hosts into the extensions' HTML
- DNS Amplification DDoS
  - Utilize forged (spoofed) traffic and unmanaged open recursive resolvers to launch large bandwidth attacks

How does IPv6 Impact Incident Handling?

Does Operations Understand IPv6?

- It *is* similar to IPv4…..but NOT ☺ [Training is Important!!]
- IPv4 and IPv6 interface addressing nuances
  - Which IPv6 address used to source traffic?
  - When is IPv4 address used vs IPv6 address for a dual-stacked host?
  - Where are special transition addresses used?
- More IPv6 nuances
  - Every mobile device is a /64
  - Extension headers
  - Path MTU Discovery
  - Fragmentation

Required Host IPv6 Addresses

- Each host must assign the following addresses to identify itself:
  - Its link-local address for each interface
  - Any assigned unicast addresses
  - The loopback address
  - The all-nodes multicast address
  - Solicited-node multicast address for each assigned unicast or anycast address
  - Multicast addresses for all other group memberships

Sample MacOS Interface

```
Tidal-Wave:~ merike$ ifconfig

lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        inet 71.39.132.244 netmask 0xfffffff8 broadcast 71.39.132.247
        inet6 fe80::20d:93ff:fe2f:554c%en0 prefixlen 64 scopeid 0x4
        inet6 2001:440:1880:5001:20d:93ff:fe2f:554c prefixlen 64 autoconf
        ether 00:0d:93:2f:55:4c
        media: autoselect (10baseT/UTP <half-duplex>) status: active
```

Mac OSX Interface Today…..

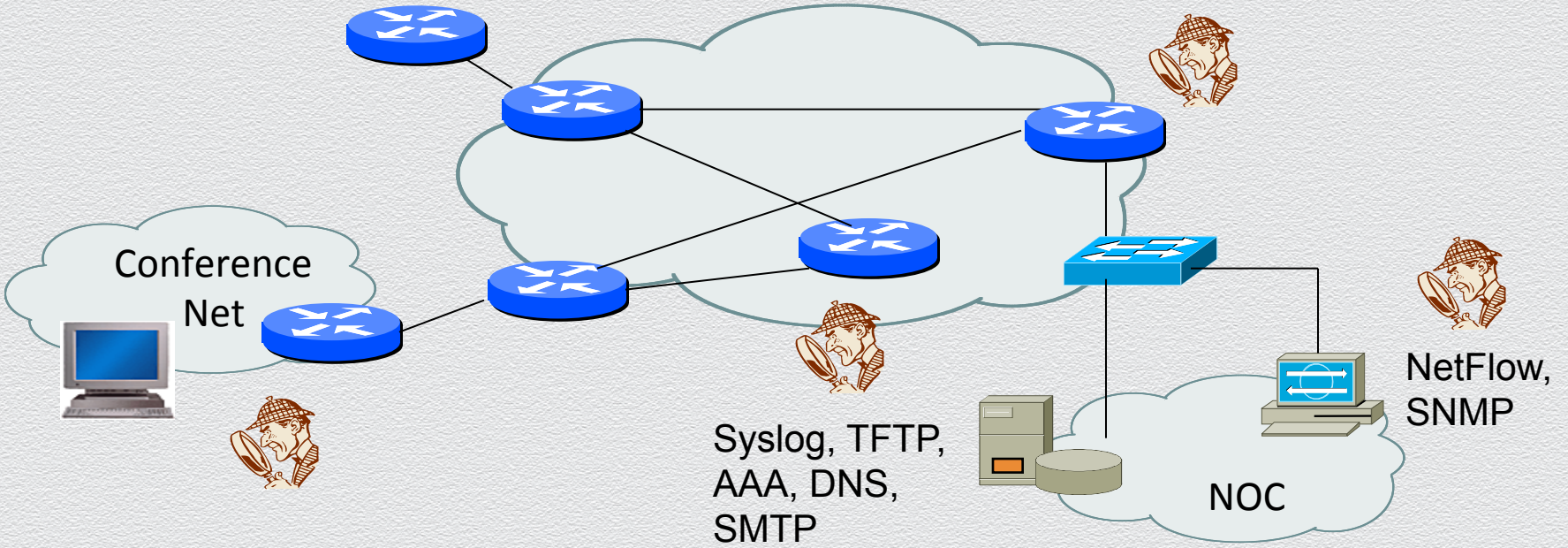
```
Merikes-MacBook-Air:~ merike$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=3<RXCSUM,TXCSUM>
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether 94:94:26:04:cc:f2
        inet6 fe80::9694:26ff:fe04:ccf2%en0 prefixlen 64 scopeid 0x4
        inet6 2a02:8071:f00:64:9694:26ff:fe04:ccf2 prefixlen 64 autoconf
        inet6 2a02:8071:f00:64:14f3:a9a6:60d5:a7d4 prefixlen 64 autoconf temporary
        inet 169.254.25.203 netmask 0xffff0000 broadcast 169.254.255.255
        media: autoselect
        status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
        ether 06:94:26:04:cc:f2
        media: autoselect
        status: inactive
Merikes-MacBook-Air:~ merike$
```

IPv6 Reserved Addresses (RFC 6890)

Description	Network
unspecified	:: /128
loopback	::1 /128
IPv4-IPv6 Translation address	64::ff9b::/96
IPv4-compatible IPv6 address	::/96
IPv4-mapped IPv6 address	::ffff:0:0/96
discard-only prefix	100::/64
TEREDO	2001::/32
benchmarking	2001:2::/48
ORCHID	2001:10::/28
6to4	2002::/16
reserved	::/8
unique-local address	fc00::/7
multicast address	ff00::/8
documentation addresses	2001:db8::/32

Can You Listen to the Network using IPv4 / IPv6 ?

- Sources (data collection points)
- Protocols to use for data collection
- Tools used to collect data



Fundamental Applications and Tools

- Preparation / Identification
  - SNMP
  - Netflow / sFlow / IPFIX
  - Syslog or other application based logs
  - TACACS / RADIUS
- Investigation
  - Ping / Traceroute / DIG / WHOIS / pDNS
- Containment / Eradication
  - Route and Packet Filtering
  - Blacklists (i.e. SPAM or Domains)

SNMP

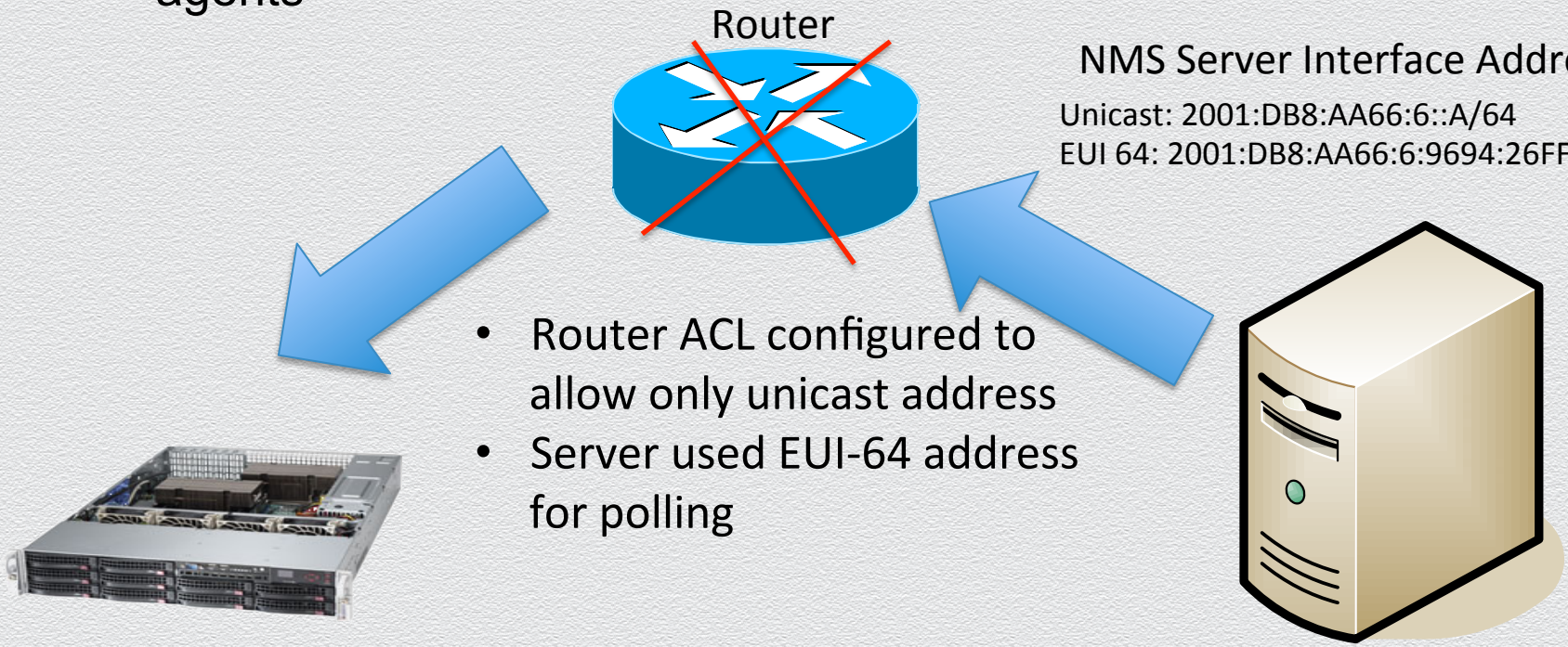
- Status of MIBs (are IPv6 MIBs implemented?)
  - IP Protocol Version Independent MIBs make IPv6-specific MIBs obsolete
  - RFC 4292 (IP Forwarding Table MIB) / RFC 4293 (MIB for the IP)
- Transport Issue (can communication use IPv6?)
  - Agent to Collector
  - Collector to Viewer
- Viewers / Tools (do they support IPv6?)

SNMP Walk Syntax

- It is different from IPv4
  - For IPv4 you only use the IP address of device
  - For IPv6 you need to enter “udp6:[<IPv6 Address>]”
    - In some cases you also need to specify the port number
    - You may also need to configure transport specific variables
      - (i.e. Rcommunity6 public)
- Examples:
  - snmpset -v 1 -c private "udp6:[<ipv6 address here>]:161" 1.3.6.1.4.1.318.1.1.26.4.4.1.4.1 i 7
  - snmpwalk -v 2c -c public udp6:[fe80::10] iso.org.dod.internet.2.1.1.5.0 SNMPv2-MIB::sysName.0 = STRING: CiscoRouter

SNMP and Addressing

- Know what IP address is being used by an SNMP server to poll the agents



NetFlow

- Must use Netflow-v9 to get IPv6 information
- Does netflow collect both IPv4 and IPv6 traffic?
  - Might depend on specific implementation
  - *NetFlow Analyzer by default give priority to ipv4 information. NetFlow Analyzer do not support flow export with both ipv4 and ipv6 data exported at the same time from an source device.* (https://forums.manageengine.com/topic/problems-with-flexible-netflow-ipv6-and-qos)
- Do netflow tools correlate between IPv4 and IPv6 traffic?
  - Are separate tables created for the different transports?

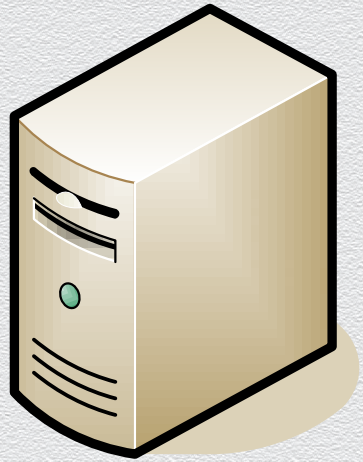
What Are Transition Mechanism Implications?

Client

Request IP address for a domain name

Does it return IPv4 or IPv6 ?

- Happy Eyeballs
- DNS64

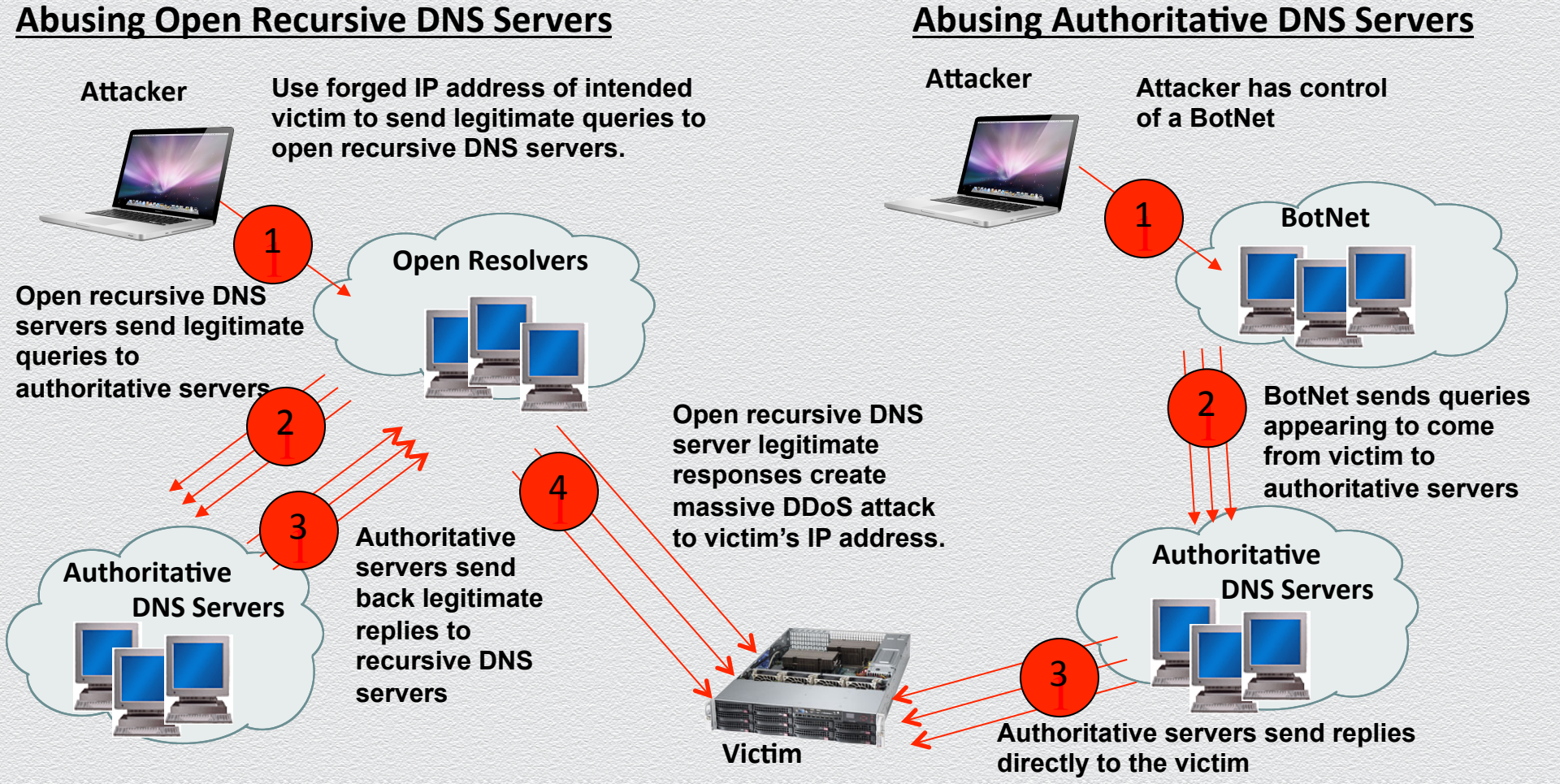


DNS Server

Growing Trends in DDoS

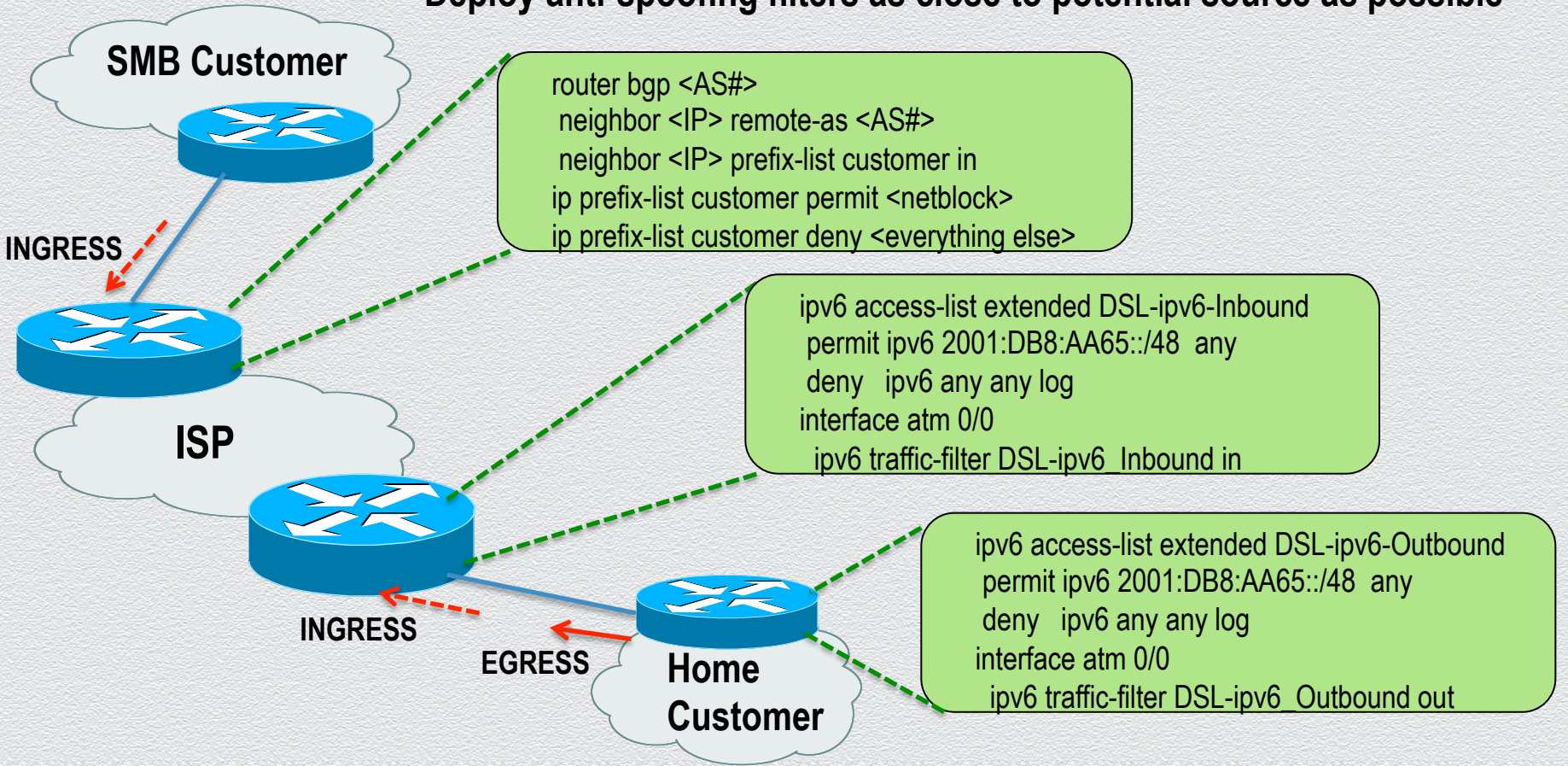
- Reflective DDoS attacks use *spoofed IP addresses* of legitimate users
- Combining spoofed addresses with legitimate protocol use makes mitigation extremely difficult – what do you block and where?
- Recent trends have been utilizing DNS as attack vector since it is a fundamentally used Internet technology
- Utilize resources of large hosting providers for added attack bandwidth
- Many other Internet protocols also susceptible

DNS Amplification Attacks Utilizing Forged (Spoofed) IP Addresses



Help Mitigate DDoS: Ingress/Egress Filters

Deploy anti-spoofing filters as close to potential source as possible



Let’s Take A Look At Passive DNS

What is Passive DNS

- Passive DNS replication is a technology invented in 2004 by Florian Weimer
  - Many uses!
  - Malware, e-crime, legitimate Internet services all use the DNS
- Inter-server DNS messages are captured by sensors and forwarded to a collection point for analysis.
- After being processed, individual DNS records are stored in a database

Passive DNS and Privacy

Client 1

DNS Resolver

Q1: what is IP address of www.nsrc.org ?

Q2: what is IP address of authoritative server for .org?

Authoritative ROOT

R2: IP address of authoritative server for .org

Q3: what is IP address for authoritative server for .nsrc

Authoritative ORG

R3: IP address of authoritative server for nsrc.org

Q4: what is IP address for authoritative server for www.

Authoritative NSRC

R4: IP address of authoritative server for www.ns

R1: IP address of www.nsrc.org

Client 2

Q5: what is IP address of www.nsrc.org ?

R5: IP address of www.nsrc.org

Q2, R2, Q3, R3, Q4, R4

Collector

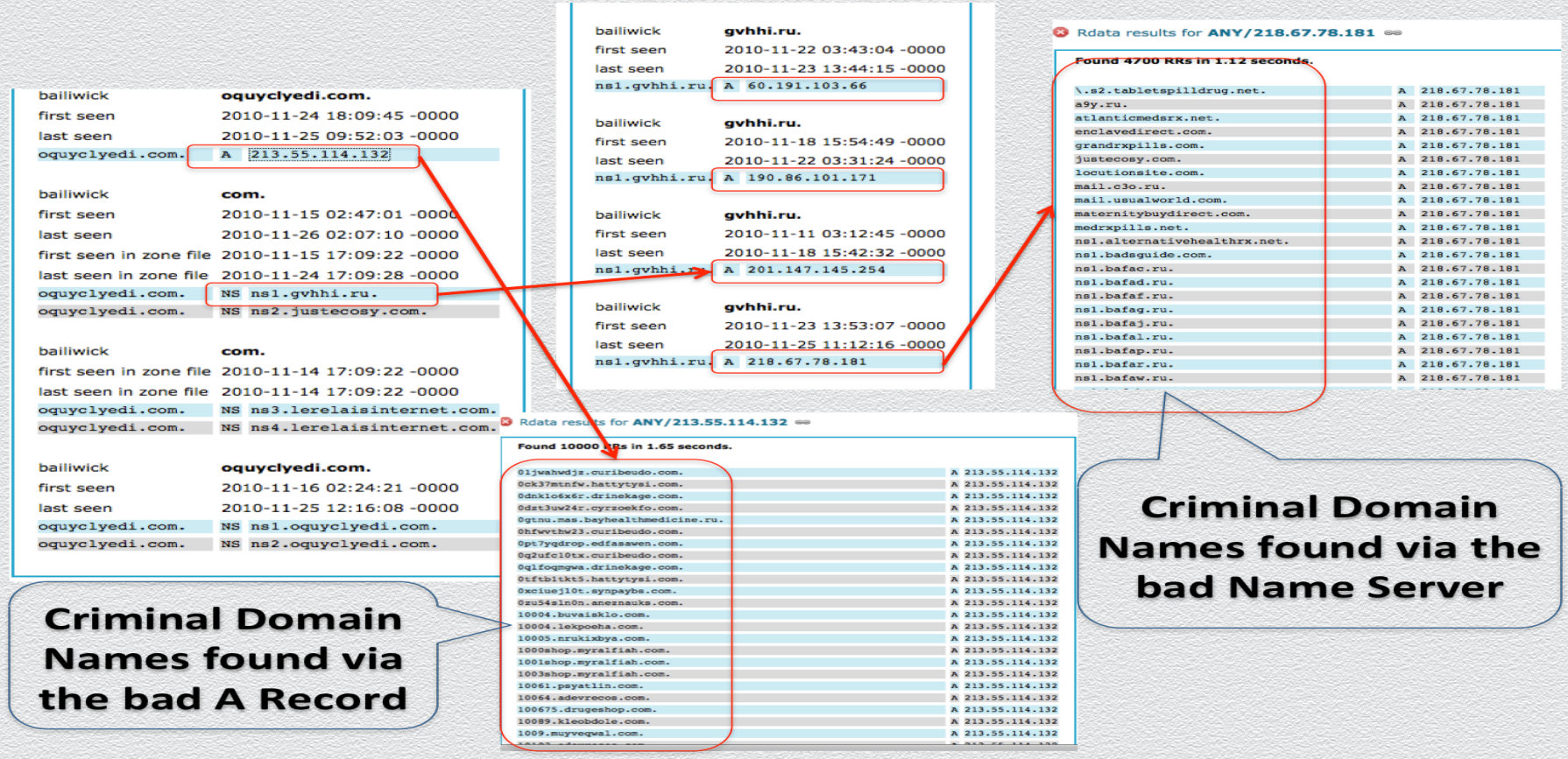
Passive DNS Sensor

Questions that can be answered using pDNS

- Where did this domain name point to in the past?
- What domain names are hosted by a given nameserver?
- What domain names point into a given IP network?
- What subdomains exist below a certain domain name?
- What new names are hosted in ccTLDs?

Passive DNS – Tool to Find the Badness

[https://www.dnsdb.info/]



Zeus hunting (fast-flux)

abuse.ch ZeuS Tracker

Home | FAQ | ZeuS Blocklist | ZeuS Tracker | Removals | ZTDNS

ZeuS Tracker :: C&C indingo.ru

The list below shows all ZeuS configs, ZeuS binaries, ZeuS dropzones and

Live Information

ZeuS C&C:	**indingo.ru**
Additional Note:	Hosted on a FastFlux botnet - ZeuS Tracker provides

	A record	TTL	Spamhaus SB
	125.88.110.49	300	LISTED
	60.19.30.134	300	LISTED
	60.19.30.135	300	LISTED
	61.197.232.43	300	Not listed
	67.209.65.212	300	Not listed

Level:	5 (Hosted on a FastFlux botnet)
Sponsoring registrar:	REGRU-REG-RIPN
Nameserver(s):	ns1.freetgp.net | ns2.freetgp.net
Date added:	2011-09-04
Last checked:	2011-09-05
Last updated:	never
BL status:	This host is being published on the ZeuS Blocklist!

RRset results for **indingo.ru/A**

Found 275 RRsets in 0.05 seconds.

bailiwick	indingo.ru.
count	93
first seen	2011-09-02 01:30:37 -0(
last seen	2011-09-04 03:47:38 -0(

indingo.ru.	A	60.19.30.134
indingo.ru.	A	60.19.30.135
indingo.ru.	A	61.197.232.43
indingo.ru.	A	63.226.215.202
indingo.ru.	A	78.[illegible]

bailiwick	indingo.ru.
count	15
first seen	2011-09-02 12:26:03 -0(
last seen	2011-09-05 00:03:46 -0(

indingo.ru.	A	60.19.30.134
indingo.ru.	A	60.19.30.135
indingo.ru.	A	61.197.232.43
indingo.ru.	A	63.226.215.202
indingo.ru.	A	113.161.87.176

bailiwick	indingo.ru.
count	119
first seen	2011-09-02 03:26:53 -0000
last seen	2011-09-05 13:18:36 -0000

indingo.ru.	A	60.19.30.134
indingo.ru.	A	60.19.30.135
indingo.ru.	A	61.197.232.43
indingo.ru.	A	63.226.215.202
indingo.ru.	A	125.88.110.49

Rdata results for **ANY/63.226.215.202**

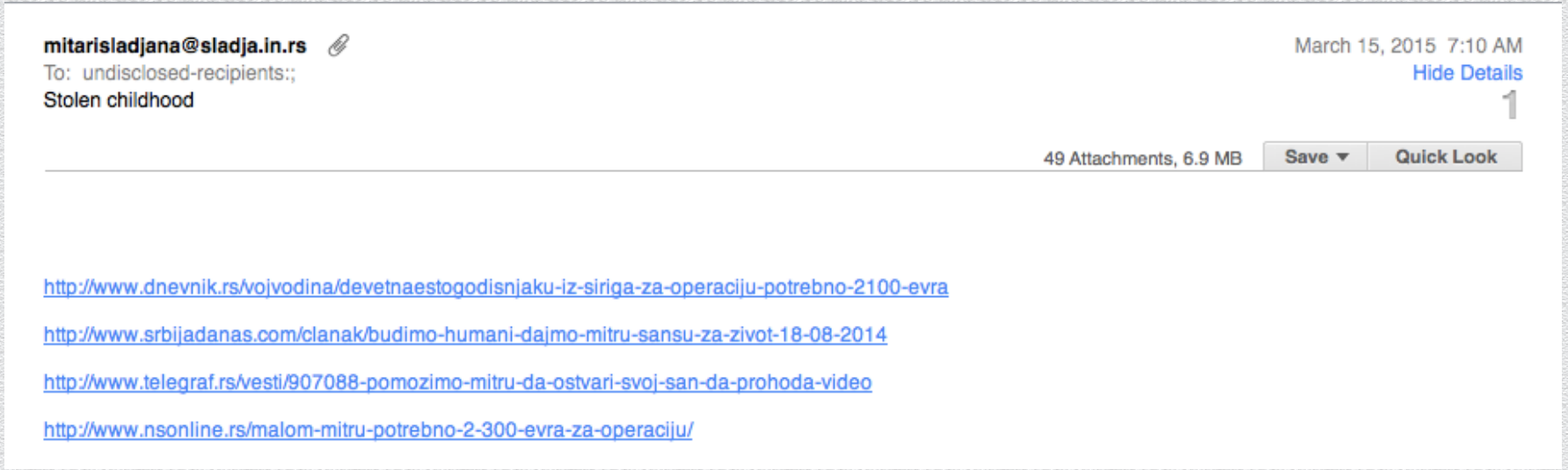
Found 28 RRs in 0.07 seconds.

asfun.ru.	A	63.226.215.202
coolsofa.ru.	A	63.226.215.202
cutesin.ru.	A	63.226.215.202
earlyship.ru.	A	63.226.215.202
ebaliu.com.	A	63.226.215.202
eepeohothe.ru.	A	63.226.215.202
greatjazz.ru.	A	63.226.215.202
indingo.ru.	A	63.226.215.202
itchysauce.ru.	A	63.226.215.202
jupaizeuph.ru.	A	63.226.215.202
krufop.com.	A	63.226.215.202
lamewire.ru.	A	63.226.215.202
munaeghohz.ru.	A	63.226.215.202
nahwisohch.ru.	A	63.226.215.202
one5xz7rf6fb61afyhx.com.	A	63.226.215.202
paperrain.net.	A	63.226.215.202
secondconcert.ru.	A	63.226.215.202
toplake.ru.	A	63.226.215.202

... more domains
... more IP resources

Could have AAAA records but haven't found any (YET!)

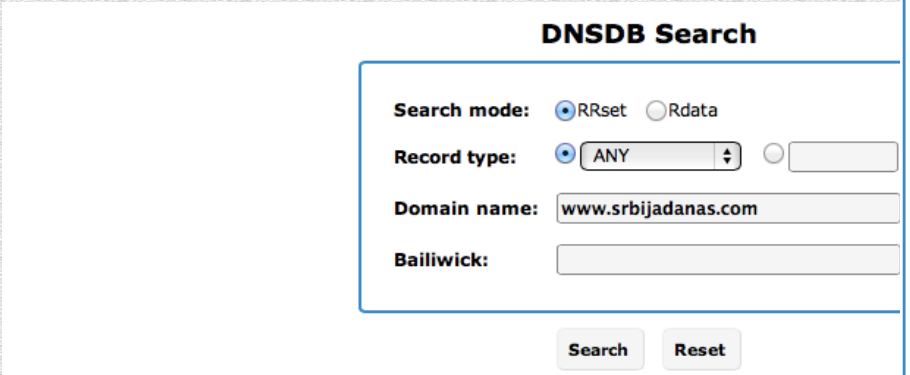
Let’s look at SPAM



Let’s see what we can find from one of those domains in a pDNS Database:

www.srbijadanas.com

DNSDB Results:



RRset results for **www.srbijadanas.com/ANY**

Returned 8 RRsets in 0.04 seconds.

bailiwick	**srbijadanas.com.**
count	4
first seen	2010-09-22 05:04:14 -0000
last seen	2012-10-13 07:07:18 -0000
www.srbijadanas.com.	A 74.117.222.24

bailiwick	**srbijadanas.com.**
count	7
first seen	2013-02-11 16:16:47 -0000
last seen	2013-04-29 13:19:44 -0000
www.srbijadanas.com.	A 107.20.206.69

bailiwick	**srbijadanas.com.**
count	3
first seen	2012-03-27 11:42:57 -0000
last seen	2012-05-21 00:38:37 -0000
www.srbijadanas.com.	A 173.212.56.174

bailiwick	**srbijadanas.com.**
count	1
first seen	2012-07-22 06:18:37 -0000
last seen	2012-07-22 06:18:37 -0000
www.srbijadanas.com.	A 173.212.56.221

bailiwick	**srbijadanas.com.**
count	6
first seen	2012-01-07 07:34:17 -0
last seen	2012-03-07 19:35:07 -0
www.srbijadanas.com.	A 173.212.56.230

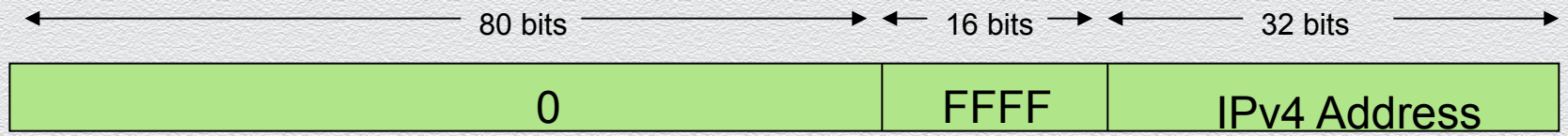
This is interesting!!

bailiwick	**srbijadanas.com.**
count	18
first seen	2011-01-10 03:30:46 -0000
last seen	2011-09-06 05:31:46 -0000
www.srbijadanas.com.	A 207.44.234.87

bailiwick	**srbijadanas.com.**
count	97413
first seen	2014-01-19 18:36:08 -0000
last seen	2015-03-15 21:24:54 -0000
www.srbijadanas.com.	CNAME srbijadanas.com.

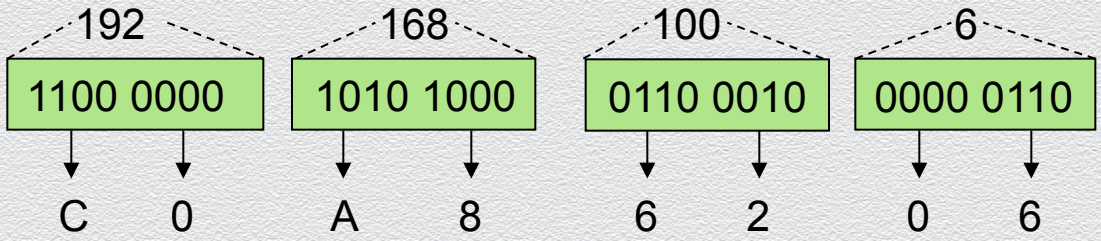
bailiwick	**srbijadanas.com.**
count	2
first seen	2010-09-15 02:58:01 -0000
last seen	2010-09-15 02:58:01 -0000
www.srbijadanas.com.	AAAA ::ffff:74.117.222.24

IPv4-Mapped Addresses



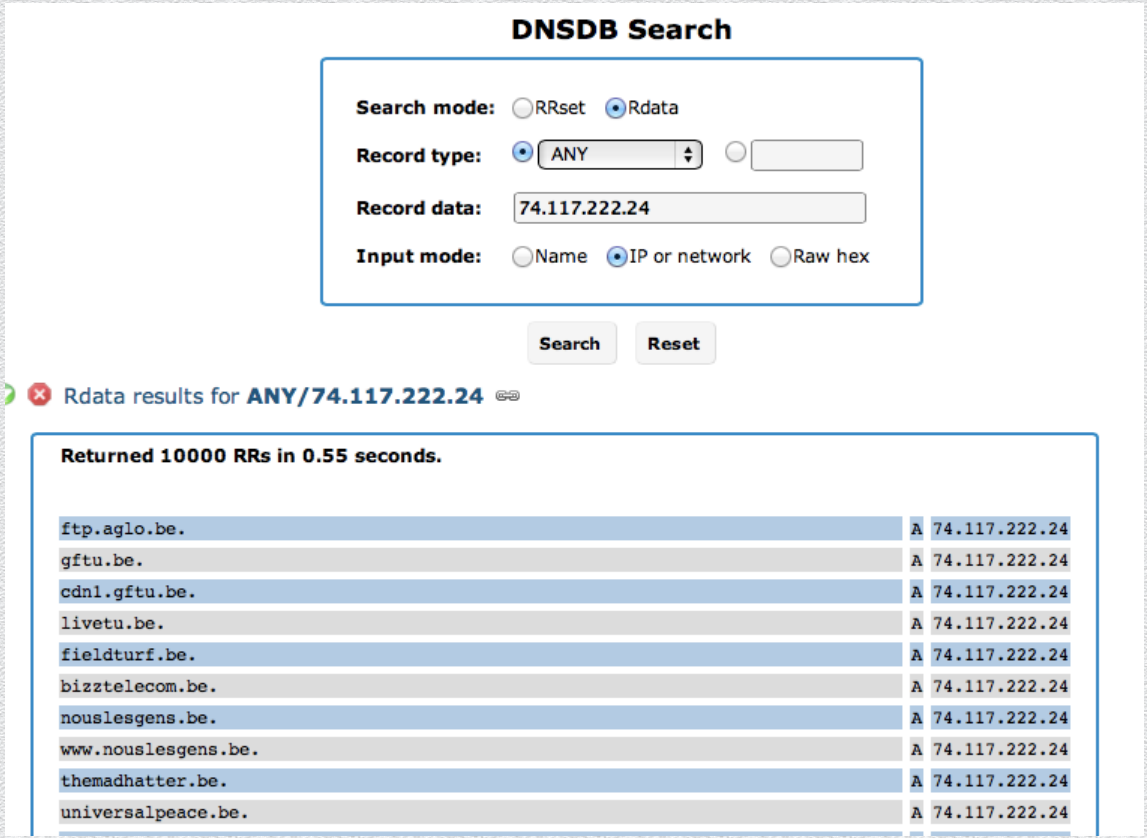
0:0:0:0:0:FFFF:192.168.100.6 → ::FFFF:C0A8:6206

XXXX XXXX : XXXX XXXX : XXXX XXXX : XXXX XXXX



An IPv4-mapped address should not be seen on the global Internet!!

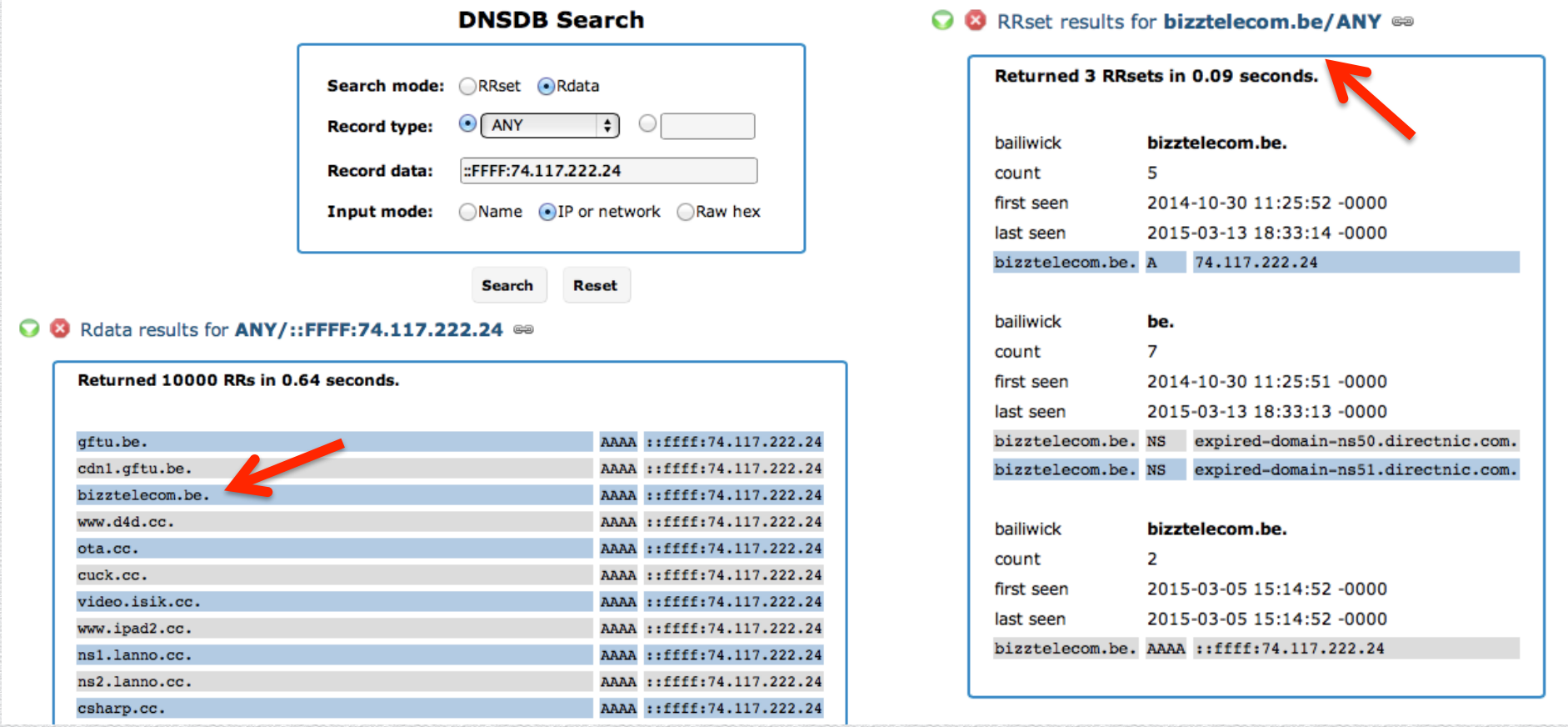
Find Associated Domains [IPv4]:



TODAY'S TREND

- Most all malicious domains utilize A records although these could be legitimate
- Many AAAA records associated with legitimate domains

Find Associated Domains [IPv6]:



Further Investigation…

- Correlate domains seen in IPv4 and in IPv6
  - IPv4 and IPv4-mapped addresses both associated with > 10,000 domains
  - Not all domains are same as seen in IPv4 and IPv6
- Investigate same domains seen in IPv4 and IPv6
- Investigate domains seen separately from IPv4 vs IPv6 address
- Might be legitimate hosting company

Passive DNS can be used to correlate some IPv4 and IPv6 related information

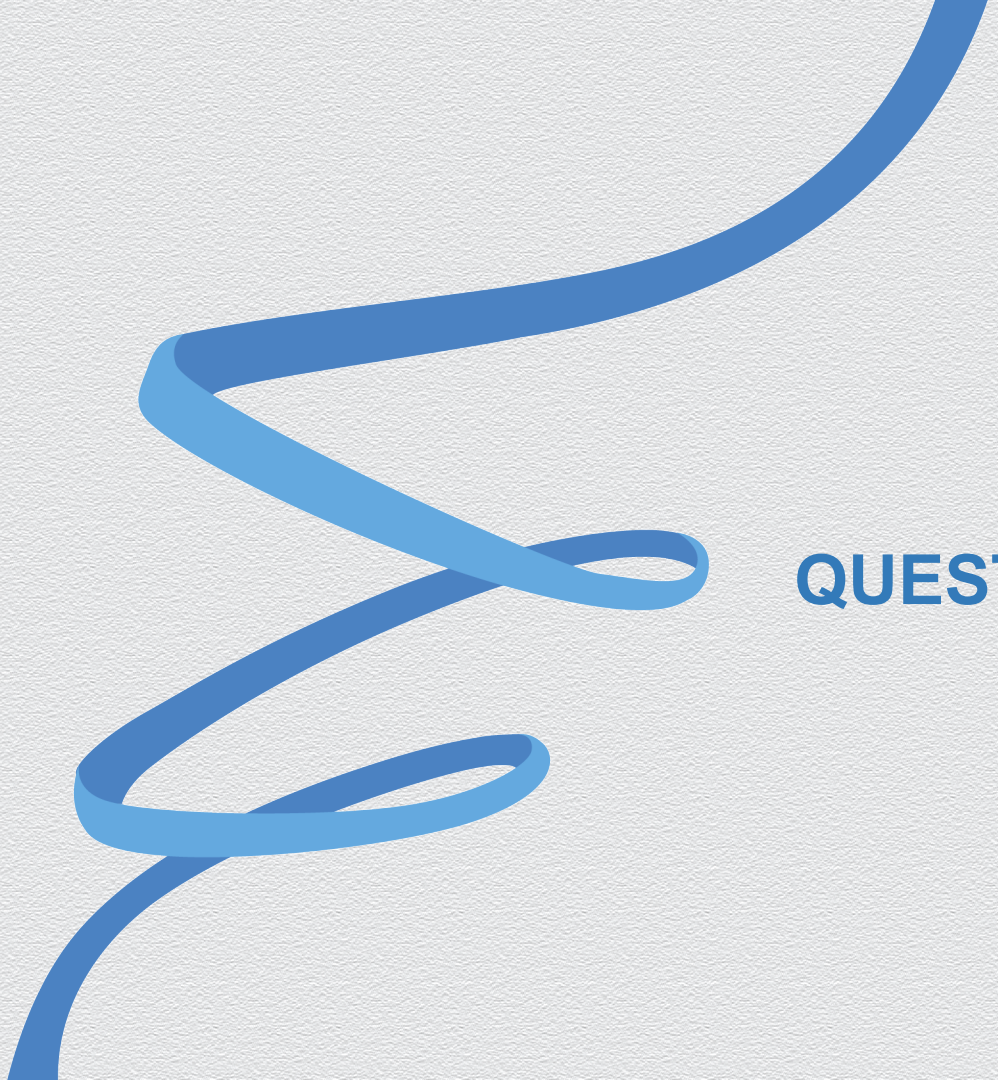
Where Do We Go From Here?

Operational Observations

- Some IPv6 attacks known but not discussed
- Recent SMTP over IPv6 discussions where lack of reputation information blocks legitimate traffic that would not be blocked on IPv4
  - Many folks turn off SMTP use over IPv6 as response
  - https://www.maawg.com/sites/maawg/files/news/M3AAWG_Inbound_IPv6_Policy_Issues-2014-09.pdf
- Many IPv6 invalid source addresses observed
  - https://ripe67.ripe.net/presentations/288-Jen_RIPE67.pdf
  - How would you tell configuration error from deliberate spoofing?

Trust But Verify….

- Understand what is able to be monitored for IPv4 and/or IPv6 traffic and know how the traffic patterns can be correlated
- Test dual-stack and transition technology behavior to know when DNS replies utilize A and/or AAAA records
- Tools for incident response improving for IPv6 but there is still more improvement needed
  - Not all management functionality can utilize IPv6 transport
  - Some networks being built for IPv6 only and are motivating vendors :)
- Correlation is important!!



QUESTIONS?