

***Security and Stability Advisory
Committee (SSAC)
Steve Crocker, Chair***

***APTLD Meeting
Kuala Lumpur
May 22, 2008***

ICANN Mission Statement

- To co-ordinate, overall, the global Internet's system of unique identifiers, and to ensure stable and secure operation of the Internet's unique identifier systems. In particular, ICANN co-ordinates:
 1. Allocation and assignment of the three sets of unique identifiers for the Internet:
 - Domain names (forming a system called the DNS)
 - Internet protocol (IP) addresses and autonomous system (AS) numbers
 - Protocol port and parameter numbers
 2. Operation and evolution of the DNS root name server system
 3. Policy development reasonably and appropriately related to these technical functions



ICANN

Asia - Pacific

Illustrative

North Amer

South Amer

Europe

Africa

- 8 Policy & Laws
- 7 Law Enforcement
- 6 Response
- 5 Operations
- 4 Products/Networks
- 3 Implementation
- 2 Protocols
- 1 Architecture

FBI

CERT

NANOG

ICANN

AUCERT

Root Server Operators

Advisory role across multiple levels and countries (DNS and addressing only)

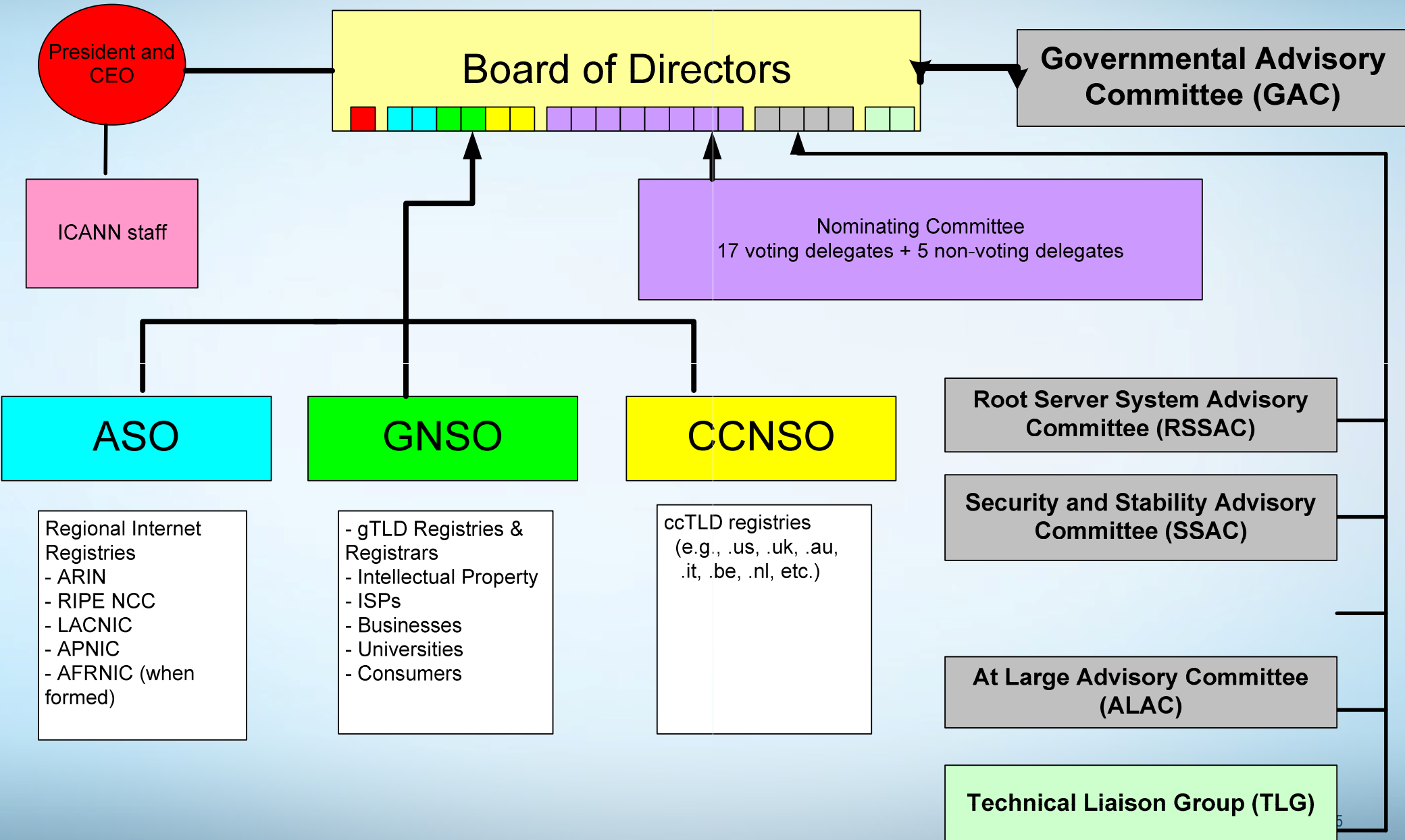
IETF

IAB

Major Activities and Initiatives

- Internationalized Domain Names (IDNs)
- New gTLDs
- DNSSEC
- IPv6 Adoption

Public-private policy forum establishes a bottom-up and balanced mechanism for interest groups to arrive at consensus on issues within a limited technical administrative mandate



What is SSAC?

- The Security and Stability Advisory Committee advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.
 - operational matters
 - administrative matters
 - registration matters
- <http://www.icann.org/committees/security/>

Security and Stability Advisory committee (SSAC)

- Volunteer committee of outside experts
 - Highly technical, broad representation
- Independence of views
- Tasks come from Board, staff, other groups and, most frequently, inside SSAC
- Output is reports, advisories, comments
- No formal authority. Traction comes from quality of our advice.

SSAC Members

Stephen Crocker <steve@stevetricrocker.com> – Chair

Dave Piscitello <dave.piscitello@icann.org> – ICANN Senior Security Technologist

Jim Galvin <galvin+dnssac@elistx.com> – eList eXpress

Alain Aina (Consultant)

Jaap Akkerhuis (NLnet Labs)

Jeffrey Bedser (Internet Crimes Group)

Lyman Chapin (Interisle), RSTEP Liaison

KC Claify (CAIDA)

Steve Conte (ICANN)

Patrik Faltstrom (Cisco Systems)

Robert Guerra (Privaterra), ALAC Liaison

Rodney Joffe (Neustar)

Olaf Kolkman (NLNet Labs), IAB Point of Contact

Mark Kosters (ARIN)

Warren Kumari (Google)

Matt Larson (VeriSign)

Danny McPherson (Arbor Networks, Inc.)

Ram Mohan (Afilias)

Russ Mundy (SPARTA, Inc.)

Frederico Neves (NIC.br)

Ray Plzak (ARIN), Vice-Chair

Ramaraj Rajashekhar (Sequoia Capital, India)

Barbara Roseman (ICANN), IANA Liaison

Mike St. Johns

Shinta Sato (JPRS)

Mark Seiden (Yahoo!)

Doron Shikmoni (ForeScout, ISOC-IL)

Bruce Tonkin (Melbourne IT)

Stefano Trumpy (IIT/CNR), GAC Liaison

Paul Vixie (ISC)

Rick Wesson (Support Intelligence)

Suzanne Woolf (ISC)

Themes and Reports

- Protection of registration
 - hijacking, inadvertent reuse, etc.
- Transition to IPv6
- Wild card use
- Fast Flux
- WHOIS
- Etc.

- <http://www.icann.org/committees/security/ssac-documents.htm>

Recent SSAC Reports

- [SAC022]:Domain Name Front Running
- [SAC023]:Is the WHOIS Service a Source for email Addresses for Spammers?
- **[SAC024]:Report on Domain Name Front Running**
- **[SAC025]:Fast Flux Hosting and DNS**
- **[SAC026]:SSAC Statement to ICANN and Community on Deployment of DNSSEC**
- [SAC027]:SSAC Comment to GNSO regarding WHOIS studies
- [SAC029]:SSAC Endorsement of Proposed Amendment to the ORG registry agreement, Security Extensions for the DNS – DNSSEC
 - <http://www.icann.org/announcements/announcement-23apr08.htm>

SAC024

Report on Domain Name Front Running

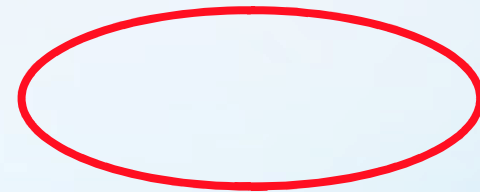
Background

- SSAC issued Domain Name Front Running Advisory (October 2007)
- Advisory offers preliminary findings:
 - Some Internet users claim that parties associated with the domain name registration process participate in domain name front running (DNFR)
 - No Internet user had presented sufficient information to support or disprove such claims
- Advisory called for community input

Disposition of Claims

- SSAC members reviewed each claim using information provided by claimant
 - Registration records, domain history, current status of domain, DNS checks, and current use of domain name used to create chronology of registration related events
- Majority of claimants were contacted by email for additional information
- Majority of claimants were informed of SSAC's interpretation of the chronology of events leading to the claim that front running occurred

Analysis and Classification of 120 Claims



No "smoking gun"

SSAC identified alternate, plausible explanations for all of the claims

Noteworthy statistics

- Of the 120 domains studied...
 - 38% are “live” and host advertising
 - 27% are registered using private/proxy services
 - 15% were available at time SSAC studied the domain
 - SSAC found that many of these were tasted and returned to the available pool
 - 14% were available for purchase in after market
 - Many of these domains host advertising
 - One domain is locked (redemption grace period)
 - 6% relate to a back-order process
 - 2% appear to be candidates for UDRP

Observations (from the Report)

- 74% of front running claims can be attributed to domain tasting and secondary market activities
 - *The community does not understand the complexities of the domain registration process and the domain name marketplace*
- Domain names believed to be of limited or exclusive interest are not as unique as claimants imagine.
 - *Competition for domain names containing commonly used or popular words, phrases and even surnames is intense*
- Measurable interest in typo-squat and visually deceptive names (often to host PPC)
- Tasting of non-renewed domains is a problem for many Internet users
 - Interest in tasting deleted names intensifies this problem

Conclusions

- SSAC can neither confirm, nor deny, any incident of DNFR **based on community responses**
- **SSAC is continuing to look at DNFR**
- Many Internet users do not approve of domain name kiting, front running, hijacking, and tasting and conclude that the registration process is not trustworthy
 - SSAC observes a deteriorating trust relationship between registrants and registrars
- Any agent who collects information about an Internet user's interest in a domain name and who discloses it in a public way violates a trust relationship
 - This violation is exacerbated when agents put themselves or third parties in an advantageous market position with respect to acquiring that domain name at the expense of its client

Recommendations

- All parties should help educate registrants about the global market for domain names, the existence of after markets and how these affect registrants
 - Eliminate the use of industry jargon wherever possible
- Registrars should
 - Clearly state how they treat information Internet users submit when checking the availability of a domain name
 - Seek to eliminate the apparent confusion over the nature and benefits of back ordering domain names
- Registrants should appreciate that
 - Domain names are a speculated and sought-after commodity
 - Availability checks may disclose an interest in a name
 - Preparing in advance and registering a name at the time they perform an availability check is the surest course of action

Fast Flux Hosting and DNS

Joint Work with the
Anti-Phishing Working Group
28 January 2008
SAC 025

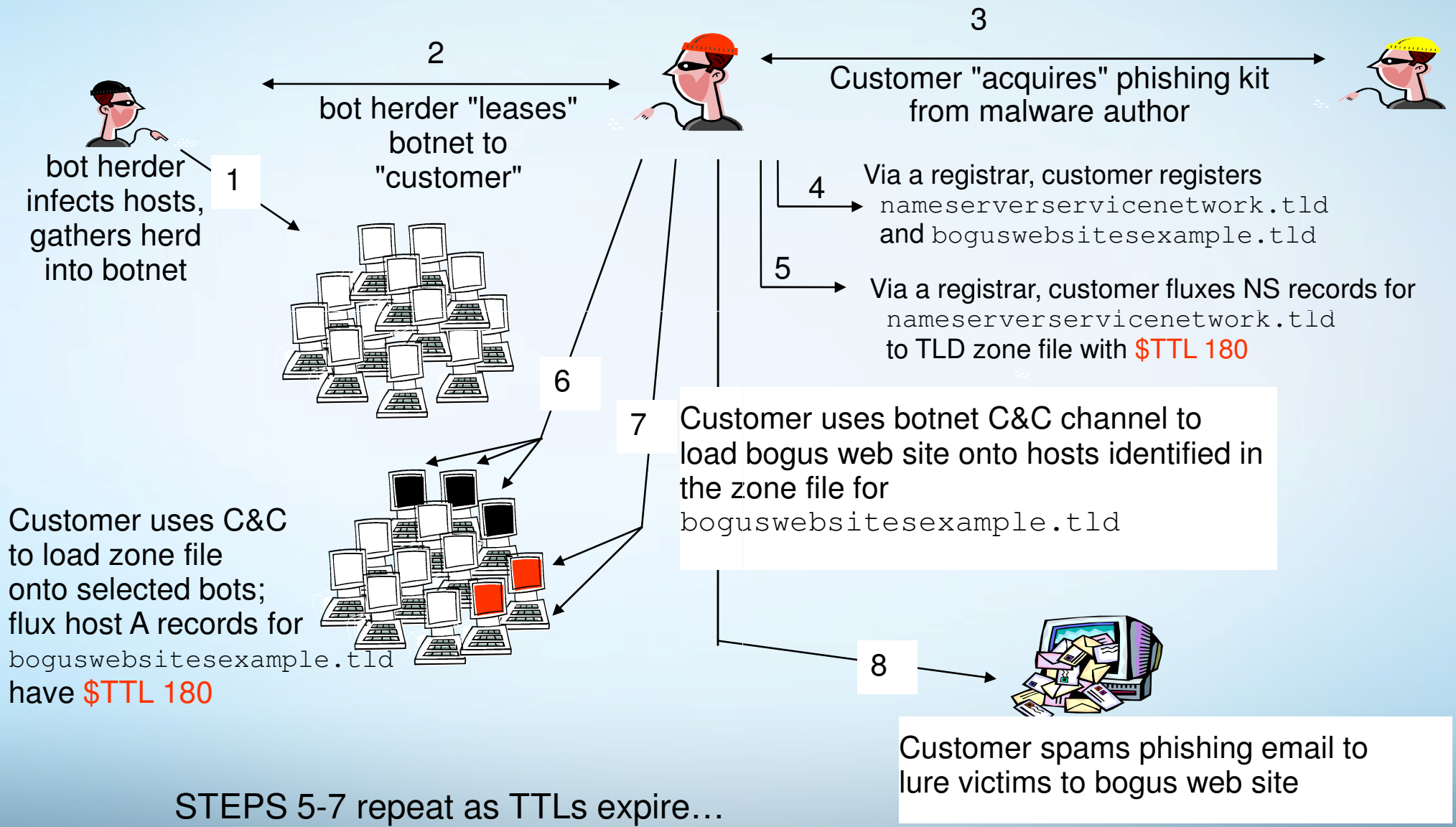
What is Fast Flux Hosting?

- 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

Variations on a theme...

- 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

Anatomy of an attack



Mitigation Alternatives

- Shut down the bots (botnets) that host fast flux
- Shut down the fast flux hosts
- Remove domains used in fast flux hosting from service

Shut down the bots

- Bots number in the 100,000s or 1Ms
- Current mitigation techniques
 - Anti-malware on desktops and at gateways
 - Education and awareness
 - Not close to stemming the tide
- Possible additional techniques include
 - Process and executable white listing
 - Network access/admission controls for private networks and public Internet service
 - Inclusion of bot detection in “unified threat management” security

Shut down fast flux hosts

- Today, responders and law enforcement collect information (and obtain court orders) to shut down fast flux hosts
 - Fast flux is designed to thwart these activities
 - Fast flux hosts operate well beyond average illegal site lifetime of 4 days
- Possible additional measures
 - Adopt procedures that accelerate the suspension of a domain name
 - Improve information sharing among responders, CERTS, LEAs (will facilitate accelerated suspension procedures)

Remove domains used in fast flux hosting from service

- Practiced today (but not uniformly)
 - Authenticate contacts before permitting changes to NS records
 - Prevent automated changes to NS records
 - Enforce a minimum TTL (e.g., 30 minutes)
 - Implement or expand abuse monitoring systems to report excessive DNS configuration changes
 - Enforce a Universal Terms of Service agreement that prohibits use of a registered domain and hosting services to abet illegal activities

Possible, additional measures

- Quarantine (and honeypot) domain names
- Rate-limit changes to name servers associated with a registered domain
- Separate "short TTL updates" from normal registration change processing
- Use suspended domains to educate consumers

Findings

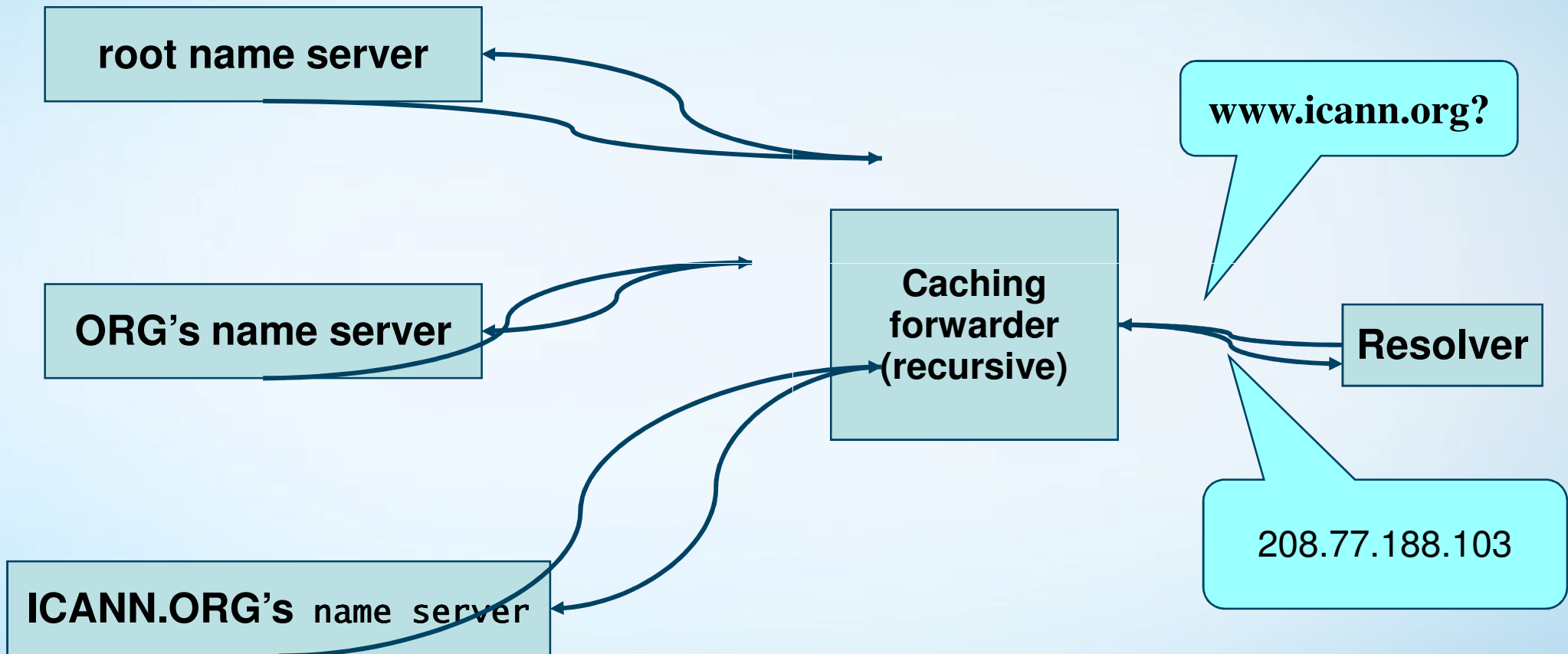
- Fast flux hosting exploits domain name resolution and registration services to abet illegal activities
- Current methods to thwart fast flux hosting by detecting and dismantling botnets *are not effective*
- Fast flux hosting hampers current methods to detect and shut down illegal web sites
- Frequent 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*

Recommendation

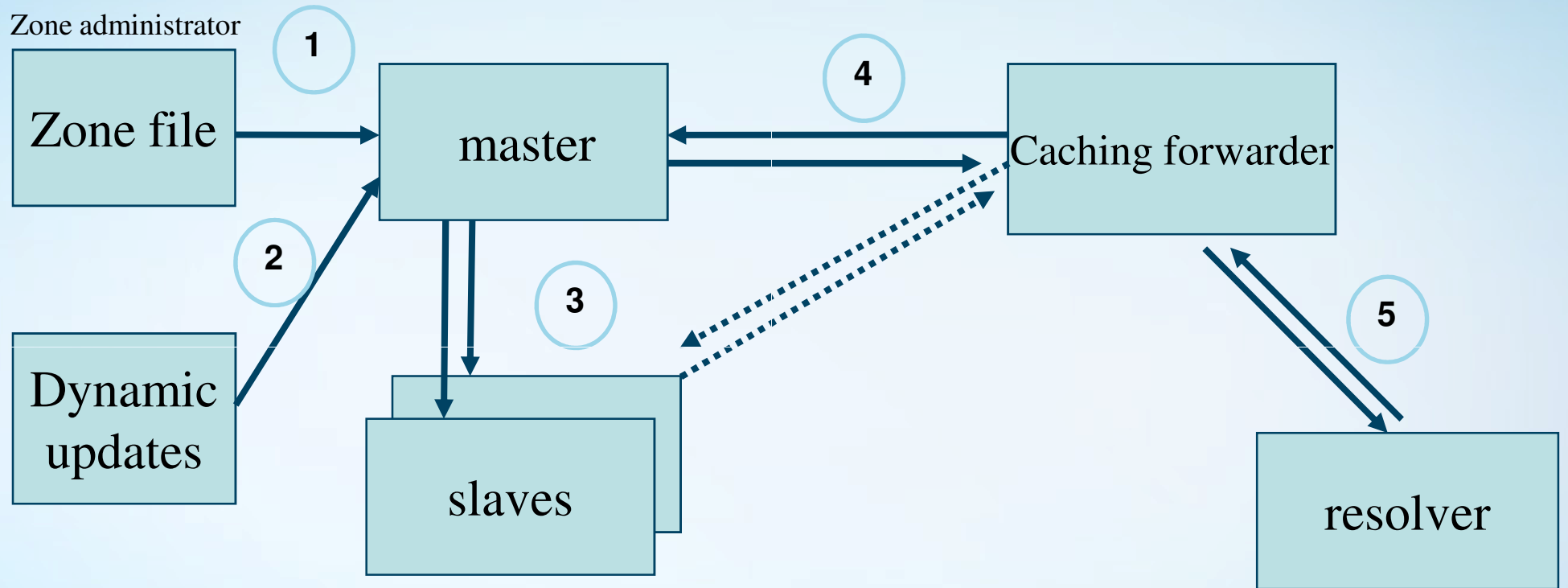
- SSAC encourages ICANN, registries and registrars to
 - consider the practices mentioned in this Advisory,
 - establish best practices to mitigate fast flux hosting
 - consider incorporating such practices in future accreditation agreements.

DNS Security Protocol (DNSSEC)

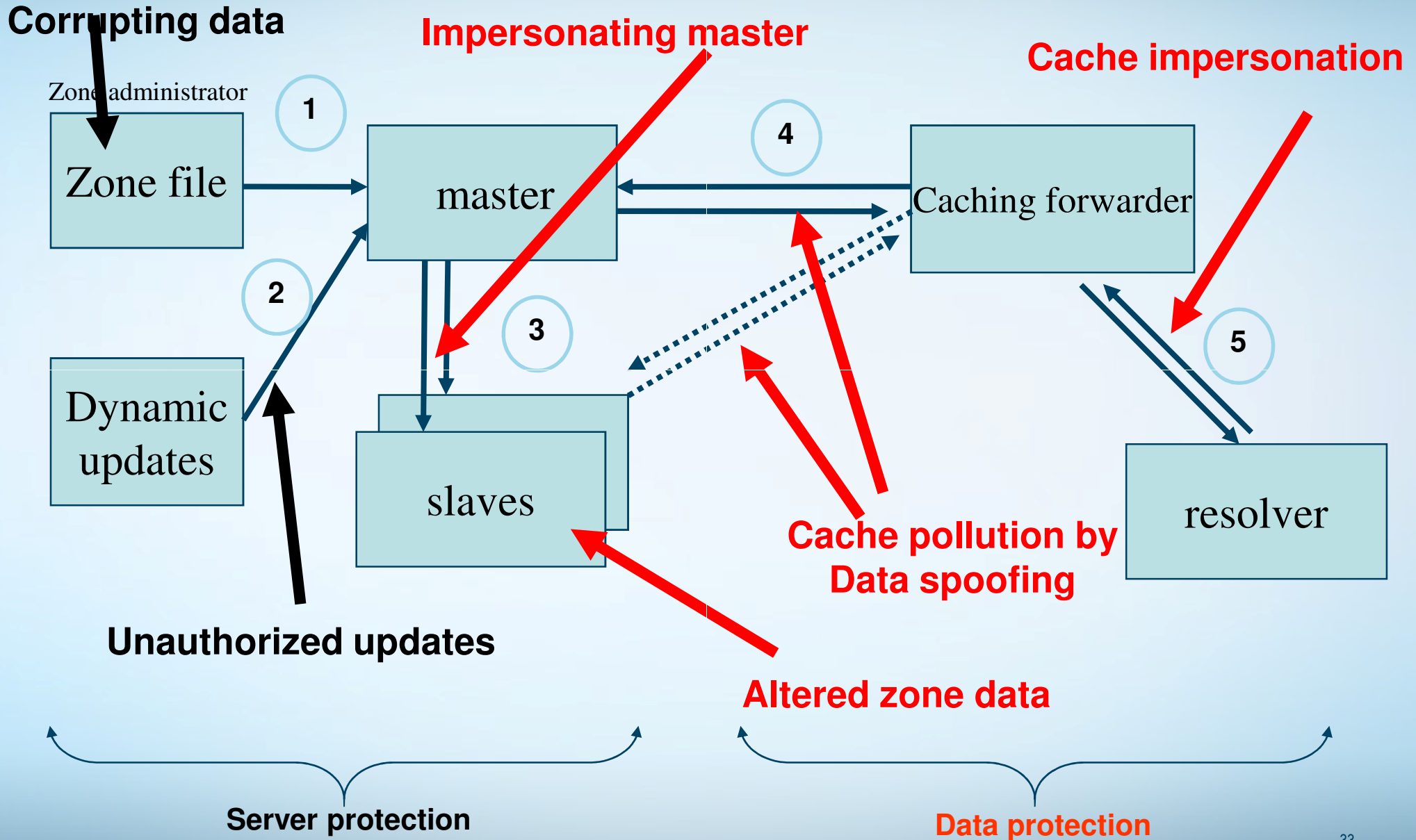
What is WWW.ICANN.ORG's address?



DNS: Data Flow



DNS Vulnerabilities



How bad can it get?

- In wireless environments, it's easy to substitute DNS responses.
- Redirect to a false site
 - Steal passwords
- Redirect to a man-in-the-middle site
 - See and copy an entire session
 - Web, email, IM, etc.

Where Does DNSSEC Come In?

- DNSSEC secures the name to address mapping
 - Transport and Application security are just other layers.

DNSSEC hypersummary

- Data authenticity and integrity by signing the Resource Records Sets with private key
- Public DNSKEYs used to verify the RRSIGs
- Children sign their zones with their private key
 - Authenticity of that key established by signature/checksum by the parent (DS)
- Ideal case: one public DNSKEY distributed

Deployment Status

- Signed: Sweden (.SE), Bulgaria (.BG), Puerto Rico (.PR), Brazil (.BR)
 - RIPE's portion of in-addr.arpa too
- Under Development: Japan (.JP), Korea (.KR), Mexico (.MX), Taiwan (.TW), United Kingdom (.UK)
- .MIL, .GOV, .EDU, .ORG all moving forward
- More coming

Final Words

- Implement DNSSEC
- Put in controls to limit fast flux
- What is your policy re front running?
- How can SSAC help you?
- <http://www.icann.org/committees/security>