Secure, Stable and Resilient Identifiers

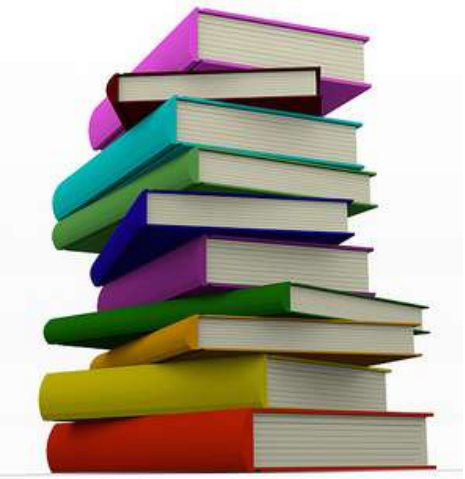
ICANN Security Team | Riga, Latvia 2015

Who is ICANN?

ICANN coordinates the administration of global identifier systems

- The Internet Corporation for Assigned Names and Numbers (ICANN)
- Operate the Internet Assigned Numbers Authority (IANA) maintaining most of the unique identifiers used on the Internet today
- We love Acronyms!

What is ICANN

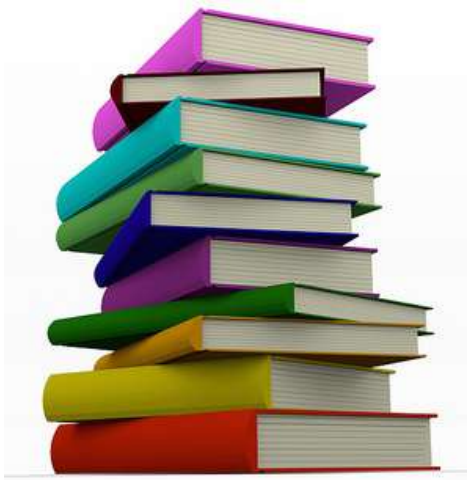


ICANN coordinates the administration of global identifier systems

- Non Profit 501c public benefit corporation
- Office locations:
  - Hub Offices: Istanbul, Los Angeles, Singapore
  - Engagement Offices: Beijing, Brussels, Geneva, Montevideo, Seoul, Washington D.C.

Also quite a few “Home Offices”. Amman, Brisbane, Cairo, London.. Too many to list.

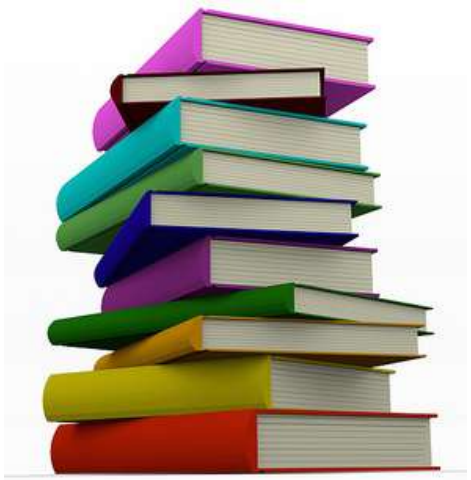
What is ICANN



ICANN coordinates the administration of global identifier systems

- ICANN is also a policy forming body
  - We operate through contracts with operators of DNS infrastructure
  - The policies that guide those contracts are made through bottom up policy forums.
  - Three large meetings a year but policy discussions are ongoing year round

Participation in ICANN

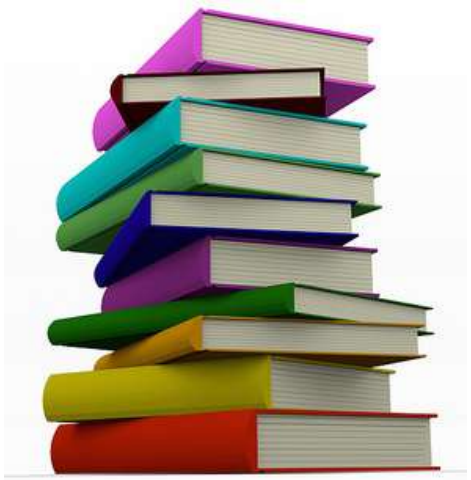


ICANN coordinates the administration of global identifier systems

- Open to entire Internet ecosystem
- Receive updates via MyICANN.ORG
- Join public comment forum on ICANN's web site
- Attend ICANN's public meetings in person or online
- Join one of ICANN's Supporting Organizations or Advisory Committees


So what are Identifiers?

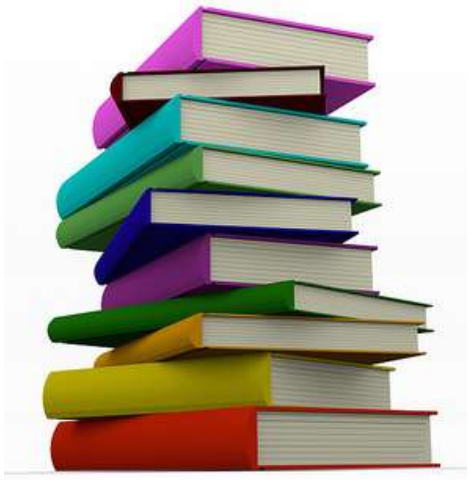
One Internet, Many Identifier Systems



ICANN coordinates the administration of global identifier systems

- Addresses identify locations of Internet devices or hosts
  - IP version 4
  - IP version 6
- Domain names provide user friendly identification of hosts
  - Latin script (A-Z, 0-9, and hyphen)
  - Internationalized Domain Names accommodate non-Latin languages or scripts

One Internet, Many Identifier Systems



Identifier systems are managed in databases or "registries"

- Port numbers identify Internet application endpoints, e.g.,
  - A browser and a web server
  - Called and calling parties of an Internet telephony connection
- Parameters identify numbers that Internet protocols need to operate correctly
  - Uniform resource identifiers
  - Character encodings
  - Values for specific protocol fields

What Can I Do With a Domain Name?

- An engineer's answer
  - Assign user friendly names to a computer (server)
  - that hosts Internet applications:
  - Web, blog, file server, email, IP telephony

- A business person's answer
  - Create a merchant or other commercial online presence
  - Join a commodities market: buy, sell, auction domain names
  - Run a commercial service

- A government official's answer
  - Provide services for public interest

- A criminal's answer
  - Misuse, exploit or disrupt public or business services


Identifier System
Security, Stability & Resilienc

The group

- Seven dedicated staff constituting decades of Internet technology and security experience
- Focus primarily on the SSR of the Identifiers
- Trying to take a bigger picture approach to recognizing and mitigating risks to the system through both technical and policy solutions.

Our Toolbox

- Threat Awareness:
  - Understanding emerging and long term threats.
  - Being aware of critical issues that are active.
  - If a large piece of the network goes dark we want to know about and if appropriate offer assistance.
- Analysis and Research
  - Collaboration with research community as well as internal projects.

Our Toolbox

- Education and Outreach:
  - Trainings to operators within the Identifier Industry on operations and security matter
  - Helping Op-sec, LEA understand the Industry and vice versa
  - Publications, Blogs etc..
  - Presentations and talks like this..

Our Toolbox

- Community:
  - As a group we are active participants in many Policy, Operational and Security communities.
  - We often act as “trusted introducers” between communities and as SME’s to help them understand each other.(Translation services ☺)

Our Toolbox

- Daily Operations:

  - The day job also includes:
    - Advising ICANN staff, board and community on SSR issues
    - ICANN's vulnerability disclosure processes
    - Putting out fires..
    - Rescuing cats.


What keeps us awake?

Maliciously Registered Domain Names

- Phishing
- Malware C&C
- Data exfiltration
- Malware distribution (drive-by pages)
- Exploit attacks
- Scams (419, reshipping etc.)
- Counterfeit goods
- Illegal pharma and piracy
- Infrastructure (ecrime name resolution)

Abuses of Other People's Domains & DNS

Attackers compromise legitimate domain registrations.

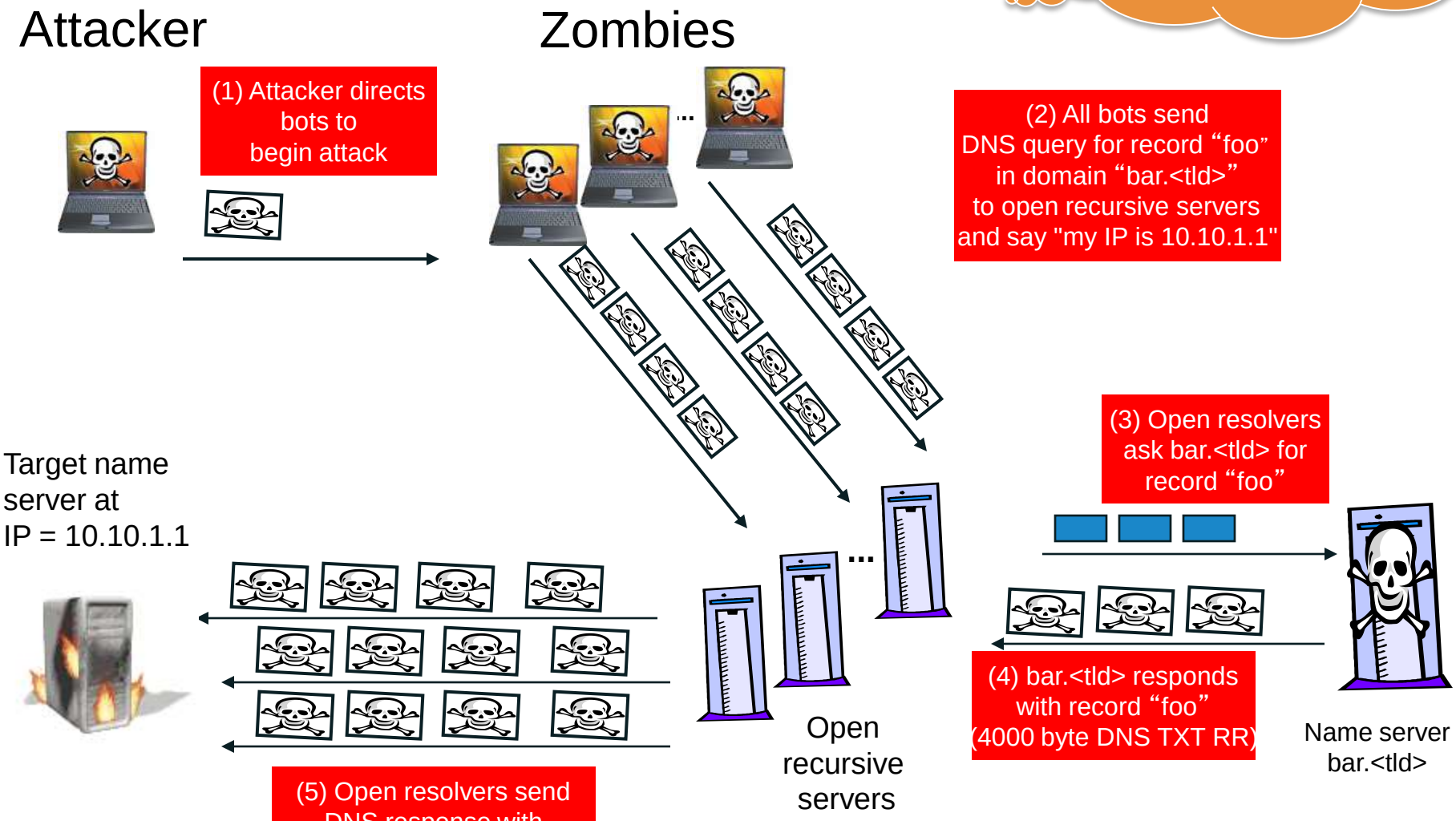
- Host criminal DNS infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism (e.g., defacement)
- Tunneling (covert communications)
- Attack obfuscation
- Host file modification (infected devices)
- Changing default resolvers (DNSChanger)
- Poisoning (resolver/ISP)
- Man in Middle attacks (insertion, capture)

How Can Bad Actors Attack DNS?

Attack	Description
Cache Poisoning	Dupe a resolver into adding false DNS records to its cache (example: basic cache poisoning)
Indirection attack	Use malware to poison a client computer's /etc/hosts file (example: DNSChanger)
Distributed Denial of service (DDoS) attack	A resource depletion attack where 1000s of bots send DNS queries to a target NS
DDoS amplification (reflection) attack	1000s of bots issue queries that evoke a very large response message, they all "spoof" the address of a targeted name server, and the targeted NS is flooded with very large DNS response messages requested by the compromised computers
Exploitation attacks	Exploit a software flaw that causes DNS server software to fail or behave in an unintended way

DDoS Amplification Attack

What identifiers are abused?



Summary

- The Internet uses many identifier systems
- DNS let us use names instead of numbers
  - The DNS is a critical Internet database
- The DNS is open and thus *open to abuse*
  - A public database, populated and supported by thousands of individual authorities
- Registration of names is also open to abuse
- Address registrations and routing system are open to abuse
- Maintaining the security and stability of Internet identifier systems is an important element of ICANN's mission

Engage with ICANN

Update email address

Thank You and Questions

Reach us at:
Email: security@icann.org
Website: http://www.icann.org

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations