ICANN's Role in the Security and Stability of the DNS

Pre-ATLAS II Capacity Building Program

Webinar: 1300 UTC 15 May 2014

ICANN’s Role in the Security and Stability of the DNS

Webinar Outline:

1. Definition of Security and Stability
2. ICANN's Role in the Security and Stability of the DNS
3. Why is security and stability important?
4. What is the Security and Stability Advisory Committee (SSAC)?
5. Example of a security attack.
6. Questions

ICANN’s Limited Technical Mission

ICANN’s limited technical mission is described as:

- To coordinate the allocation of the Internet’s unique identifier systems;
- To preserve and enhance the Stability, Security and Resiliency of these systems;
- To maintain and operate the L-Root nameserver instance as steward for the Community;
- To manage ICANN’s own internal systems and to provide a publicly accessible portal to disseminate and share information.

Source: ICANN Security, Stability and Resiliency Framework FY14 March 2013
https://www.icann.org/en/about/staff/security/ssr/ssr-plan-fy14-06mar13-en.pdf

Definitions

- **Security** – the capacity to protect and prevent misuse of Internet unique identifiers.
- **Stability** – the capacity to ensure that the system operates as expected, and that users of the unique identifiers have confidence that the system operates as expected.
- **Resiliency** – the capacity of the unique identifier system to effectively withstand/tolerate/survive malicious attacks and other disruptive events without disruption or cessation of service.

Source: ICANN Security, Stability and Resiliency Framework FY14 March 2013
https://www.icann.org/en/about/staff/security/ssr/ssr-plan-fy14-06mar13-en.pdf

ICANN is not:

- A law enforcement agency, a court of law or a government agency
  - Law enforcement and governments participate as stakeholders in ICANN's processes and policy development
- Responsible for policing the Internet or operationally combatting criminal behaviour
- Responsible for determining what constitutes illicit conduct on the Internet
- Involved in use of the Internet related to cyber-espionage and cyber-war
- Authorised to unilaterally suspend or terminate domain names
  - ICANN is able to enforce its contracts with third parties, including domain name registration providers

Source: ICANN Security, Stability and Resiliency Framework FY14 March 2013

https://www.icann.org/en/about/staff/security/ssr/ssr-plan-fy14-06mar13-en.pdf

ICANN does:

- Play a role in supporting the work of law enforcement or government agencies in carrying out legitimate actions at their request.
- Participate with the operational security community in studying, analyzing and identifying malicious use or abuse of the DNS.
- Play the same part as any interested stakeholder with regards to Internet protocols
  - evolution of Internet protocols and related standards are not under the purview of ICANN but reside with the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB)

Source: ICANN Security, Stability and Resiliency Framework FY14 March 2013
https://www.icann.org/en/about/staff/security/ssr/ssr-plan-fy14-06mar13-en.pdf

How Security, Stability & Resiliency Fits into ICANN

Security at ICANN can be viewed as:

- A Core Value for ICANN (in accordance with the Affirmation of Commitments)
- One of the Four Focus Areas of the Strategic Plan
- An overall thematic area cutting across the organization
- A department within ICANN (the Security Team)
- An essential element in projects and activities
- A key stakeholder group within the ICANN Community (the Security and Stability Advisory Committee – SSAC)

Why is security and stability important?

- Contributes to the stability of the global economic environment
- Assists the prosperity of developing and developed nations
- Supports national security, emergency response and the preservation of law and order
- Facilitates the correct functioning of critical infrastructure
- Enhances opportunities for business and commerce
- Enables the free flow of information
- Protects the interests of individual users of the internet

Security and Stability Advisory Committee (SSAC)

Charter: To advise the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems.

- 2001: SSAC initiated.
- 2002: Began operation.
- Provides guidance to ICANN Board, Supporting Organizations and Advisory Committees, staff and general community.
- Members as of March 2014: 40 (appointed by ICANN Board for 3-year terms)

SSAC Activities

- SSAC Membership Committee
- ICANN Meetings
    - DNSSEC Workshop
    - SSAC Outreach to Law Enforcement
- Annual SSAC Workshop
- SSAC Work Parties
    - Identifier Abuse Metrics
    - Public Suffix Lists
    - IANA Transition
    - JAS Report Comment

2013-2014 Publications by Category

DNS Security

[SAC064]: SSAC Advisory on DNS “Search List” Processing – 13 February 2014

[SAC063]: SSAC Advisory on DNSSEC Key Rollover in the Root Zone – 07 November 2013

[SAC062]: SSAC Advisory Concerning the Mitigation of Name Collision Risk – 07 November 2013

[SAC059]: SSAC Letter to the ICANN Board Regarding Interdisciplinary Studies – 18 April 2013
[SAC057] SSAC Advisory on Internal Name Certificates—March 2013

2013-2014 Publications by Category

DNS Abuse

[SAC065]: SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure – 18 February 2014

Internationalized Domain Names (IDNs)

[SAC060]: SSAC Comment on Examining the User Experience Implications of Active Variant TLDs Report—23 July 2013

Registration Data (WHOIS):

[SAC061] SSAC Comment on ICANN's Initial Report from the Expert Working Group on gTLD Directory Services—06 September 2013

[SAC058] SSAC Report on Domain Name Registration Data Validation Taxonomy—March 2013

One Example of a Security Attack: Distributed Denial of Service (DDoS)

- A DoS attack attempts to make a machine or network resource unavailable to users.
- DoS – Sent by one person or machine
- DDoS – Sent by more than one person or machine

One Example of a Security Attack: Distributed Denial of Service (DDoS)

- Contemporary DDoS attacks use DNS reflection and amplification to achieve attack data bit rates reportedly exceeding 300 gigabits per second.
- Underlying many of these attacks is packet-level source address forgery or spoofing, the attacker:
  - Generates and transmits data packets purporting to be from the victim's IP address
  - Uses query-response protocols to reflect and/or amplify responses to achieve attack data transfer rates exceeding the victim's network capacity
- DNS is especially suitable for such attacks.

One Example of a Security Attack: Distributed Denial of Service (DDoS)

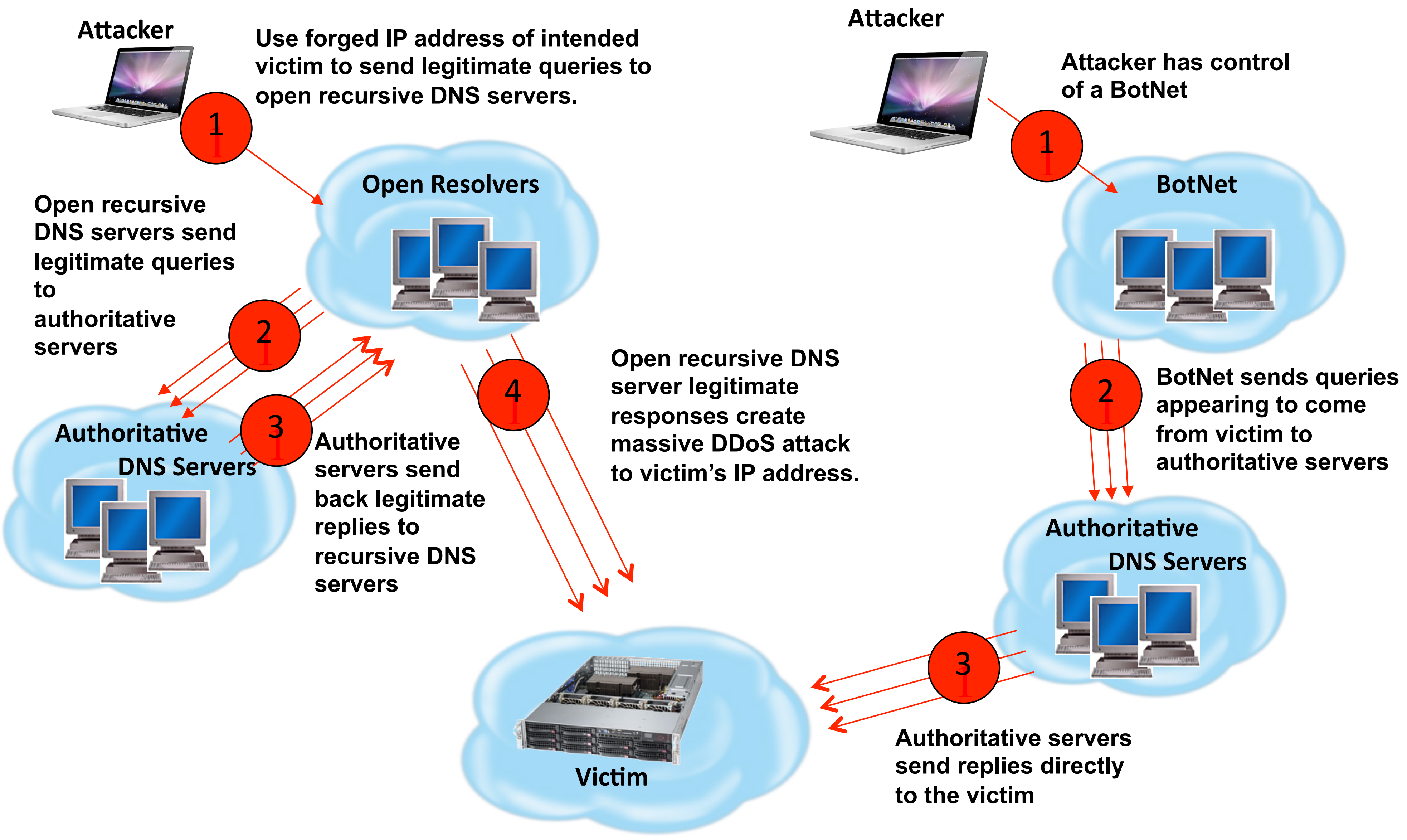
In the following diagram:

- An Authoritative Name Server is a name server that gives answers in response to questions asked about names in a zone.
  - By design, an authoritative name server must respond to every query
- A Recursive Name Server or Caching Name Server (*DNS cache*) stores DNS query results for a period of time. If it does not hold the response to a query, it will ask an Authoritative Name Server
- A Recursive Name Server may be:
  - Secure: only responds to queries from 'authorized' sources in the network; or
  - Open: responds to all queries, irrespective of their source

DNS Amplification Attacks Utilizing Forged IP Addresses

Abusing Open Recursive DNS Servers

Abusing Authoritative DNS Servers



Use forged IP address of intended victim to send legitimate queries to open recursive DNS servers.

Open recursive DNS servers send legitimate queries to authoritative servers

Authoritative servers send back legitimate replies to recursive DNS servers

Open recursive DNS server legitimate responses create massive DDoS attack to victim’s IP address.

Attacker has control of a BotNet

BotNet sends queries appearing to come from victim to authoritative servers

Authoritative servers send replies directly to the victim

Distributed Denial of Service (DDoS) Attack: Contributing Factors

- Critically, basic controls for network access and DNS security have not been as widely implemented as is necessary to maintain and grow a resilient Internet.

- There are increasingly higher-speed Internet connections combined with the growing power of individual end user devices results in an extraordinary and growing capacity for conducting extremely large scale and highly disruptive DDoS attacks using unsecured DNS infrastructure.

SAC065 Recommendations

1. ICANN should help facilitate an Internet-wide community effort to reduce the number of open resolvers and networks that allow network spoofing. This effort should involve measurement efforts and outreach.
   - Help to identify and publicize the scale of the problem
   - Provide information to assist network operators
2. All network operators should take immediate steps to prevent network address spoofing.
   - Check whether queries actually come from the address they say they do (called network ingress filtering)
3. Recursive DNS server operators should take immediate steps to secure open recursive DNS servers.
   - Respond only to queries from authorized sources on the network

SAC065 Recommendations (cont)

4. Authoritative DNS server operators should support efforts to investigate authoritative response rate limiting.
   - Some server vendors limit the number of responses which can be transmitted within a specified time period

5. DNS server operators should put in place operational processes to ensure that their DNS software is regularly updated and communicate with their software vendors to keep abreast of the latest developments.
   - Keep software up to date

SAC065 Recommendations (cont)

6. Manufacturers and/or configurators of customer premise networking equipment should take immediate steps to secure these devices and ensure that they are field upgradable when new software is available to fix security vulnerabilities, and aggressively replace the installed base of non-upgradeable devices with upgradeable devices.
   - Make sure customer network equipment does not respond to “unauthorized’ queries
   - Make sure all equipment has software that can be upgraded in the field
   - Replace any equipment that can’t be upgraded

Questions?

Pre-ATLAS II Capacity Building Program

Webinar: 1300 UTC 15 May 2014