Security and Stability Advisory Committee

Activities Update

ICANN Singapore Meeting
March 2014

#ICANN49

ICANN

NO. 49
23-27 MARCH 2014
Singapore

Agenda

1. SSAC Overview and Activities – Patrik Fältström
2. SAC 064: SSAC Advisory on Search List Processing – Patrik Fältström
3. SAC 065: SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure – Merike Kaeo
4. Discussion & Questions

Security and Stability Advisory Committee (SSAC) Overview

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

2014 Work Plan: Current Activities

- SSAC Membership Committee
- DNSSEC Workshop
- Identifier Abuse Metrics
- SSAC Outreach to Law Enforcement
- IGF Workshop
- Public Suffix Lists

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

SAC064: SSAC Advisory on DNS “Search List” Processing

Patrik Fältström

Overview

In SAC 064, the SSAC:

- Examines how current operating systems and applications process search lists;
- Highlights security and stability implications with some search list behaviors; and
- Proposes a strawman to improve search list processing.

Background

- What is search list processing?
  - a feature that allows a user to enter a partial name in an application, with the operating system expanding the name through entries in a search list.
  - a search list of "somedomain1.com; somedomain2.com" and a user types "system" into her browser's address box, the operating system would try "system.somedomain1.com", "system.somedomain2.com", and "system." in some order.

Issues

Issue 1: Non-Standardization

Name	Behavior
never	*never* apply the search list, the original name is queried.
always	*always* apply the search list, the synthesized names are queried in the DNS, and the original name is *never* queried in the DNS.
pre	The search list is *first* applied to the original name in DNS queries, and if iterations of the application of the search list generate a NXDOMAIN response, the original name is queried in the DNS.
post	The original name is queried in the DNS. If it generates an NXDOMAIN response, the search list is applied to the original name in DNS queries.
www / search	“www” is prepended to the original QNAME, or the string is used as a search term to the default search engine.

Issues, Cont.

Issue 2: Query Leakage and Privacy Issues

- Applications and resolver libraries in the “post” behavior leak queries that may result in them reaching the root servers.
- Applications move between different environments (e.g., from corporate to home network) where different search lists are set, queries will be appended with search list entries that may not match the user’s original intent, causing unintended and unnecessary queries.

Issues, Cont.

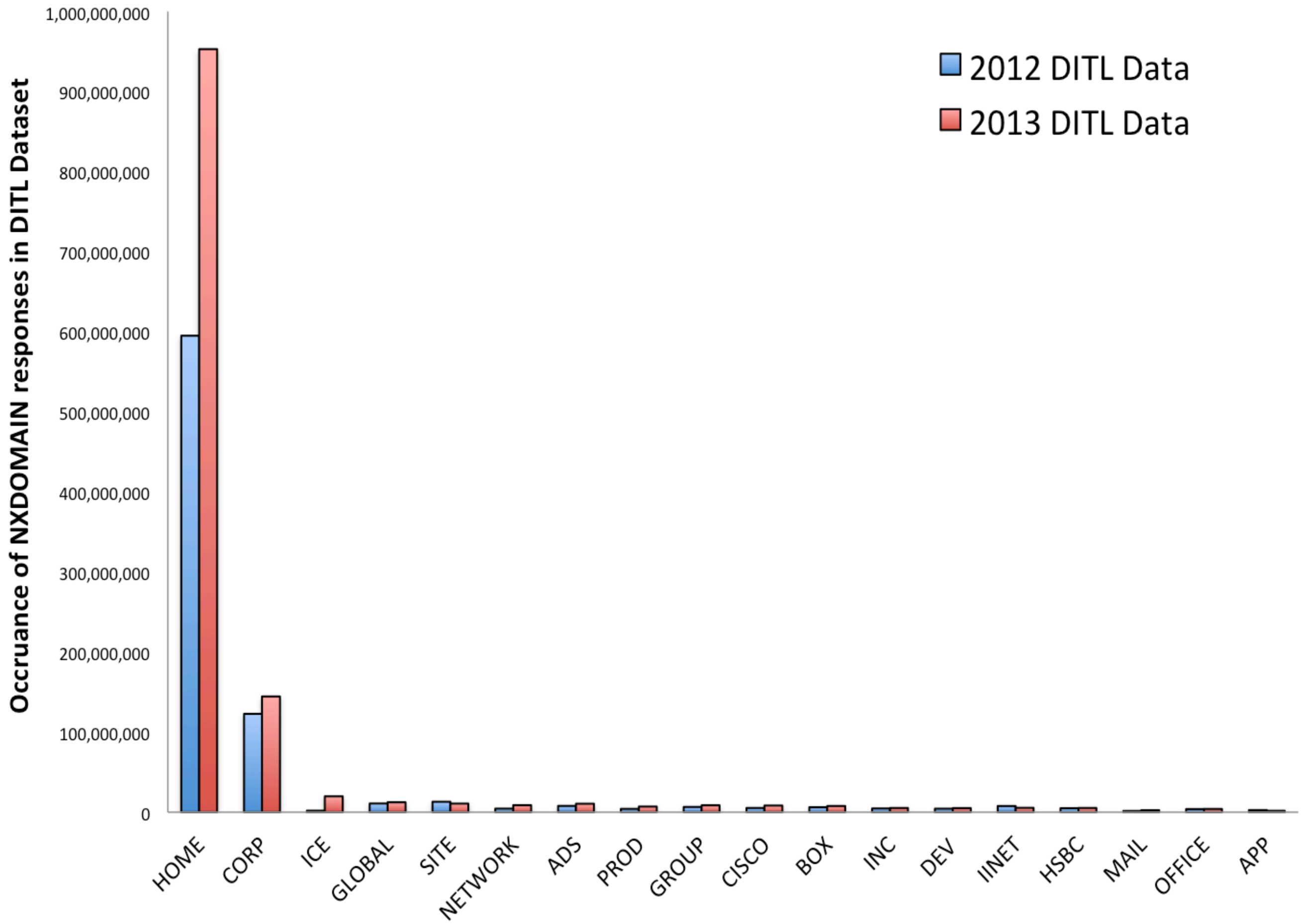


Figure 1: NXDOMAIN traffic to some proposed TLDs (source 2012, 2013 DITL)

Issues, Cont.

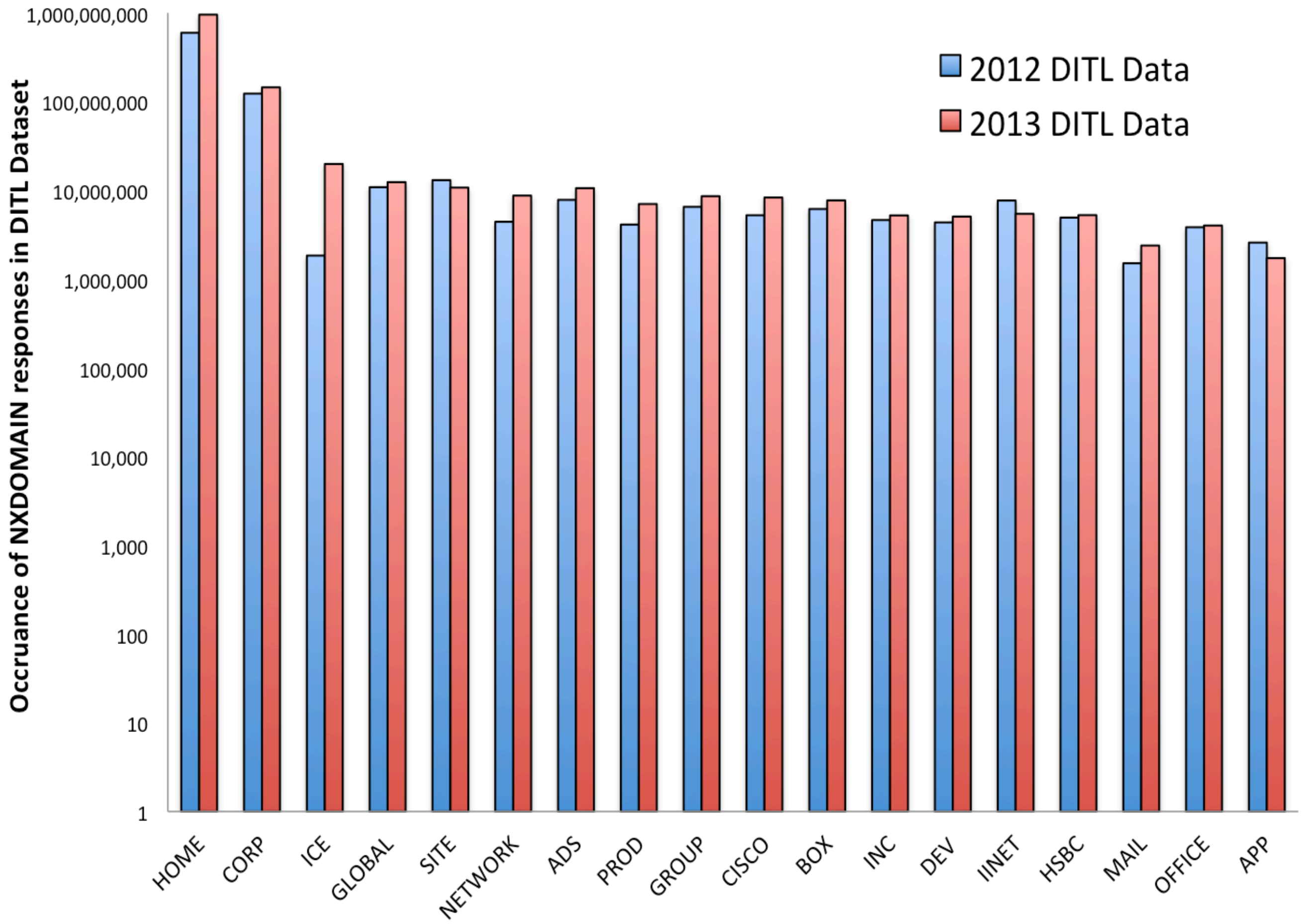


Figure 2: NXDOMAIN traffic to some proposed TLDs (source 2012, 2013 DITL). Note the log scale of the Y-Axis.

Issues, Cont.

Issue 3: Security and Name Collision Issues

```
1) User > Resolver:   A? www.corp.

2) Resolver > User:   NXDomain q: A? www.corp.

3) User > Resolver:   A? www.corp.corp.example.com.

4) Resolver > User:   NXDomain q: A? www.corp.corp.example.com.

5) User > Resolver:   A? www.corp.chicago.example.com.

6) Resolver > User:   NXDomain q: A? www.corp.chicago.example.com.

7) User > Resolver:   A? www.corp.example.com.

8) Resolver > User:   A? www.corp.example.com. 192.0.2.10
```

Strawman Proposal

- No automatically generated search lists:
  - Administrators (including DHCP server administrators) should configure the search list explicitly, and must not use implicit search lists.
- Unqualified single-label domain names are never queried directly:
  - When a user enters a single label name, that name may be subject to search list processing if a search list is specified, but must never be queried in the DNS in its original single-label form.
- Unqualified multi-label domain names never use search lists:
  - When a user queries a hostname that contain two or more labels separated by dots, such as www.server, applications and resolvers must query the DNS directly. Search lists must not be applied.

Recommendations

In SAC 064, the SSAC:

- Invites ICANN SO/ACs, the IETF, and the DNS operations community to consider the proposed behavior for search list processing and comment on its correctness, completeness, utility and feasibility;
- Recommends ICANN staff to work with the DNS community and the IETF to encourage the standardization of search list processing behavior; and
- Recommends in the context of mitigating name collisions, ICANN should consider additional steps to address search list processing behavior.

SAC065: SSAC Advisory on DDoS Attacks Leveraging DNS Infrastructure

Merike Kaeo

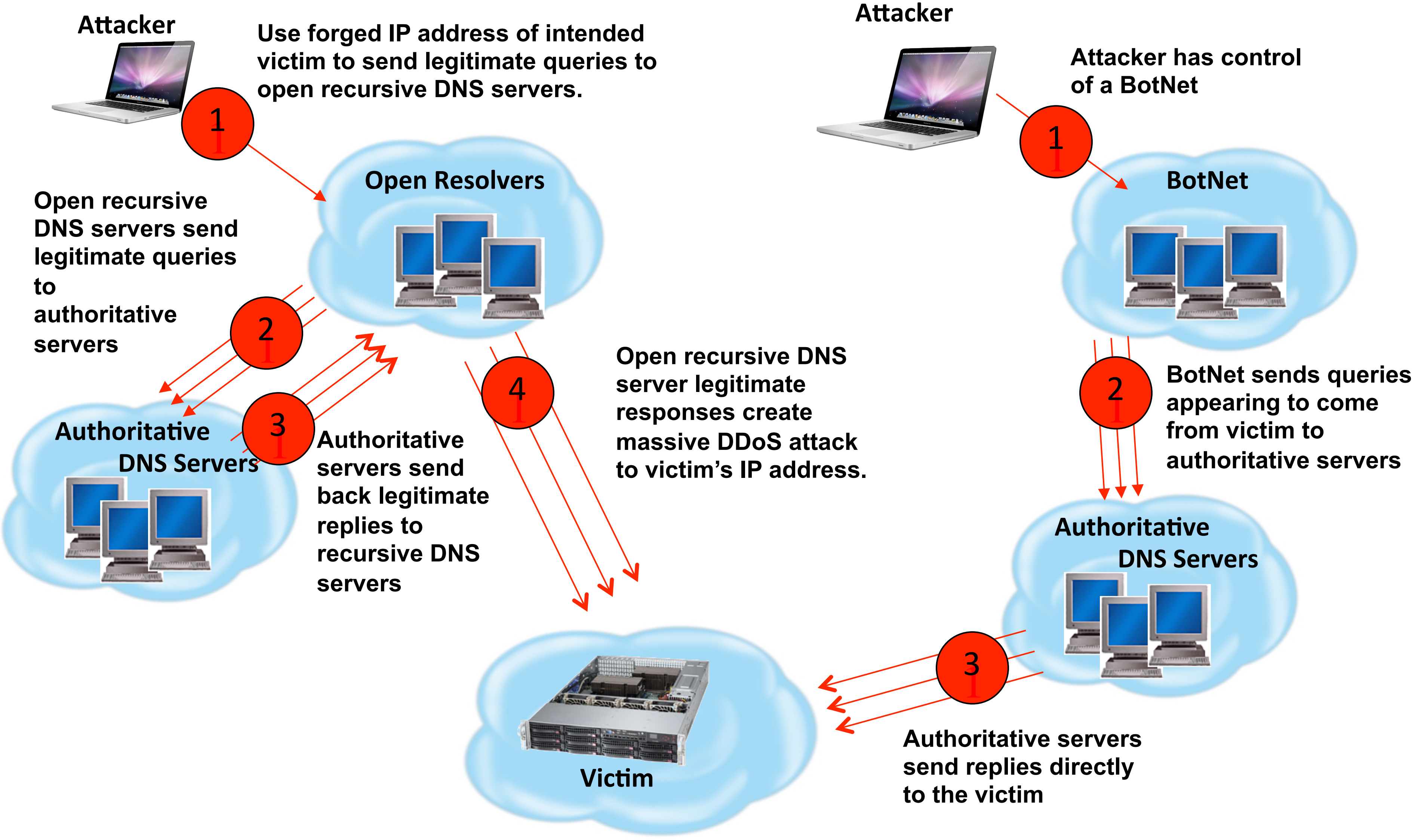
Overview

- 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 UDP packets purporting to be from the victim’s IP address;
  - Uses query-response protocols (e.g., DNS, NTP, or SNMP) to reflect and/or amplify responses to achieve attack data transfer rates exceeding the victim’s network capacity; and
  - DNS is especially suitable for such attack.

DNS Amplification Attacks Utilizing Forged IP Addresses

Abusing Open Recursive DNS Servers

Abusing Authoritative DNS Servers



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

2 Open recursive DNS servers send legitimate queries to authoritative servers

3 Authoritative servers send back legitimate replies to recursive DNS servers

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

1 Attacker has control of a BotNet

2 BotNet sends queries appearing to come from victim to authoritative servers

3 Authoritative servers send replies directly to the victim

Overview, Cont.

- 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.
- 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.

Summary

In SAC 065, the SSAC:

- Explores several unresolved critical design and deployment issues that have enabled increasingly large and severe Distributed Denial of Service (DDoS) attacks using the DNS; and
- Recommends ICANN and operators of Internet infrastructure and manufacturers take specific actions.

Recommendations

The SSAC Recommends that:

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;
2. All network operators should take immediate steps to prevent network address spoofing;
3. Recursive DNS server operators should take immediate steps to secure open recursive DNS servers;
4. Authoritative DNS server operators should support efforts to investigate authoritative response rate limiting.

Recommendations, Cont.

The SSAC Recommends that:

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; and
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.

Thank You and Questions

#ICANN49

ICANN

NO. 49
23-27 MARCH 2014
Singapore