Current Counter-measures and Responses by the Domain Name System Community

Paul Twomey
President and CEO

22 April 2007

APEC-OECD Malware Workshop
Manila, The Philippines
What I want to do today in 15 Minutes:

• Outline ICANN and its role in security and stability in the Internet’s system of unique identifiers
• Illustrate how malware is affecting Root Server, TLD and DNS servers
• Explain some initiatives in the domain name arena and ways through the ICANN process for you to input
ICANN mission statement

- To coordinate, 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 coordinates:
  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
Security must be a multi-stakeholder and layered responsibility

<table>
<thead>
<tr>
<th>8 Policy &amp; Laws</th>
<th>7 Law Enforcement</th>
<th>6 Response</th>
<th>5 Operations</th>
<th>4 Products/Networks</th>
<th>3 Implementation</th>
<th>2 Protocols</th>
<th>1 Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>OECD/APEC</td>
<td>APEC</td>
<td>OECD/EU</td>
<td>OECD/APEC</td>
<td>OECD/APEC</td>
<td>IETF</td>
<td>IAB</td>
<td>ICANN</td>
</tr>
</tbody>
</table>

Governments

- Advisory role across multiple levels and countries (DNS and addressing only)
- Root Server Operators

Illustrative

North Amer

- Intel, Microsoft etc

South Amer

Europe

Africa

Asia - Pacific

- FBI
- Italian PCPS
- KrCERT

- APRICOT

ICANN

- OECD/APEC

IAB

- OECD/EU

OECD/APEC
Internet infrastructure threats

1. Physical disruption of major lines and switching centers
2. Loss of routing infrastructure continuity and/or fidelity
3. Loss of DNS service continuity and/or fidelity
4. Flooding of network or specific sites, i.e., denial of service attack

Not all Internet-based systems are Internet infrastructure...
Routing infrastructure

• Status
  – Routing information is maintained in routing registries
    • These are reasonably well protected against physical attack
    – Inputs to the routing registries can be compromised
    – False routing information can be inserted
  • Potential protection
    – Secure BGP has been defined and implemented

  Does not look feasible – too much hardware required

Routing security requires a multi-stakeholder engagement.
DNS infrastructure root servers – status

• Root servers point to top level domains
  – 20 generic TLDs (gTLDs) – .com, .org, etc.
    • U.S. Government has .gov and .mil
  – 243 country codes (ccTLDs) – .de, .jp, .uk, etc.

• Root servers are heavily replicated
  – 13 independent businesses
  – Many-fold replication and distribution
DNS infrastructure servers – threats

**Threats**

- **Loss of Service**
  - Network outage
  - Machine or site failures
  - Overwhelming traffic (denial of service attack)
  - Business failure

- **Hijacking**
  - Cache poisoning
  - False registration
  - Fake zone transfer
  - Fake registrar-registry interaction
  - Private roots

- **Loss of coherence**
  - Unauthorized roots and TLDs
  - Private character set extensions

**Countermeasures**

- Excess capacity
- Distribution, replication
- Strong connectivity
- Multiplicity of businesses
- DDoS counters (long term)

- Protocol changes, DNSSEC
- Tight registrar controls
- TSIG (crypto)
- Crypto authentication
- DNSSEC

- DNSSEC; policy/political pressure
- DNSSEC; policy/political pressure

Lots of work is under way. But threats are growing and this will take more time and money than many expect.
System threats

• Denial of service attacks target high-value sites
  – DNS servers are among the obvious targets
  – These will get more sophisticated
  – Action is required – see later slides

• Domain and address theft is growing
  – Spammers like to hide their identity
  – The legal framework doesn’t provide protection

Address theft, per se, is not actionable(!)
The denial of service problem

• Denial of service attacks are increasing
  – This will get worse – probably much worse
• Law enforcement is important but necessarily at the wrong end of the problem
• Technical changes in the Internet would help a lot
Distributed denial of service on Root Servers

- On 6 February 2007 – most visible since 2002 attack but not as comprehensive as amplified DDoS attack on TLDs of 2006
- Six of the 13 root servers that form building blocks of the Internet were affected – two badly
- The attack highlighted the effectiveness of Anycast load balancing technology
- More analysis is needed before a full report on what happened can be drawn up – reasons behind the attack are unclear – a wake-up call
- Root server operators worked together in a fast, effective, and coordinated effort
- Recent SSAC recommendations for improving the security of the domain name system still need to be followed through – other measures should also be considered
- Coordination and preparation were key
- Did you notice?
Amplified DNS Distributed Denial of Service (DDOS) Attack January - February, 2006

- Authoritative TLD DNS servers attacked
- Variant of a well-known DDoS attack
- Exploited some of the 500,000+ innocent but vulnerable recursive servers
- Attacks generated from 2 - 8 Gbps of traffic at targeted Authoritative DNS Servers
- Failures occurred in networks in the path as well as transit providers to the authoritative TLD DNS servers
- Resulted in disruption of DNS services in every case
- Included many TLDs without any apparent motive in most cases
Anatomy of the Attack

1. Attacker directs zombies to begin attack.

2. All zombies send DNS query for record “foo” in domain “bar.<tld>” to open recursive servers and set source IP=10.10.1.1.

3. Open resolvers ask bar.<tld> for record “foo”.

4. bar.<tld> responds with record “foo” (4000 byte DNS TXT RR).

5. Open resolvers send DNS response with (4000 byte DNS TXT RR) to target name server.

Target name server at IP = 10.10.1.1.
Detailed analysis of one attack

Graph of responses to monitoring probes by the authoritative nameservers for a TLD before, during, and after an attack in February 2005.

Vertical Axis shows the six TLD Server IP addresses. Red shows complete failure to answer, yellow indicates slow answers. For reference, Servers 1 and 4 show lesser impact than Servers 2, 3, 5, and 6. The horizontal axis shows actual time. This attack lasted 14 minutes.

Graphs courtesy of RIPE NCC.
Attack Metrics:

• 51,000 open recursive servers were involved
• 55 byte query resulted in a 4,200 byte response, for a 1:76 amplification
• 8gbps attack requires a total of 108mbps of queries.
• Each recursive server saw 2,100 bytes of queries, or 38 qps, and responded with 160kbps in answers
• Assuming compromised hosts have minimum 512kb DSL modem, only 200 compromised hosts were required
• Source networks would see no effect
• Recursive servers saw minimal traffic or query increase
• Victim network providers had catastrophic experience
• Victim DNS provider was sent the equivalent of 150 million queries per second

At best, 1 in 100 real queries were answered
Enabling Vectors

The following specific vectors that allowed the Reflective Recursive DNS DDoS attacks against the Authoritative TLD DNS servers have been identified by the ICANN SSAC:

- **Network Providers (ISPs)**
  - Failure to prohibit forging or spoofing of IP addresses by hosts
  - Failure to prohibit traffic from IP addresses they are not authorized to originate from exiting their networks

- **Recursive Server Operators**
  - Accepting and responding to DNS queries from IP addresses not under their control
  - Running nameserver versions with known vulnerabilities that allow destructive records to be configured by unauthorized parties
Recommendations

- ICANN’s Security and Stability Committee: http://www.icann.org/committees/security/


- Non-technical fact sheet: http://www.icann.org/announcements/announcement-08mar07.htm
DDoS – technical approaches raised by some

• Identification of sources of traffic
  – Tighten the routing security
• Refashion the protocols to know the identity of senders of traffic
• Distinguish between well managed computers on well managed networks vs others
  – “Well managed” means they aren’t zombies and their configuration is checked regularly
• Well managed networks quarantine computers which appear to be infected or misbehaving
• Well managed networks report misbehaviors and accept reports of misbehaviors
• Traffic among well managed networks gets preference
DDoS – customer approaches

- Pressure on the vendor to supply machines that are safe out of the box
- Establishment of an ethic that machines should be safe – it’s the vendor’s problem, not the user’s
Recommendations: implementation of DNS Security Protocol (DNSSEC)

• Sweden and Bulgaria have moved ccTLD to DNSSEC
  - importance of government, business, banking as well as registry involvement to launch successfully
• See presentations at:
  http://www.icann.org/meetings/lisbon/agenda-dnssec-28mar07.htm
Bandwidth demands for defense from DNS attacks are spiraling

– Normal DNS traffic continues to rise at about 100% every 16 months.

– Bandwidth required for attack vectors as a multiple of average daily traffic

– In 2000 it was 2 times normal bandwidth in 2006 it was 150 times
Responses and Opportunities in the generic Domain Name arena

- New DNS Update Service for .com and .net
- Whois policy
- New gTLD policy
- Review of Registrar Accreditation Agreements
On 11 April 2007, ICANN approved a “DNS Update Service” for the .COM and .NET Registries

– Registries used to publish updated data twice a day.

– This data includes domain names, nameservers, IP address additions, deletions and modifications.

– The approved service would enable registrars and others who currently obtain zone file access in the .COM and .NET TLDs twice daily, to receive updated zone information every five minutes for a fee.
Registrar responses have included:

- The service would shed light on the activity of those engaged in domain tasting and expose bad actors. (Note most domain tasting is completely legal)
- Phishers and others currently make nameserver changes to conduct fraudulent activity immediately after one publication and make the change back prior to the next publication - there has been a twelve-hour window to conduct this activity, this will now be 5 minutes.
- The service would advantage law enforcement to thwart phishing. (One opinion was that the additional extra notice period might not be a significant advantage.)
Whois policy process

• Whois issues are being addressed through the General Names Supporting Organization's (GNSO’s) policy development process (PDP)
• Numerous opportunities for public review and comment
• Important input from the Governmental Advisory Committee
• Still open for input.
New generic top-level domain timetable

• Potentially GNSO Policy Development Process may be completed by June meeting in Puerto Rico
• Governmental Advisory Committee principles developed in March
• Policy may be concluded by the end of the 4th Quarter 2007
• Next round of new gTLDs in early 2008?
Consider the impact of –

• Unique industry TLDs
• Industry cross-certified
• DNSSEC
• Other anti-phishing tools?
Opportunity now to review the gTLD Registrar Accreditation Agreement

- Call for review: http://www.icann.org/announcements/announcement-21mar07.htm
- Workshops and ongoing review
- Opportunity for input both directly, but also through the Governmental Advisory Committee - June meeting in Puerto Rico
Thank You

www.icann.org