DNS Cache Poisoners
Lazy, Stupid, or Evil?

Duane Wessels
The Measurement Factory/CAIDA
wessels@measurement-factory.com

NANOG 36
February 13, 2006
Motivation

- During March/April 2005, SANS Internet Storm Center reports a number of DNS cache poisoning “attacks” are occurring.
  - http://isc.sans.org/presentations/dnspoisoning.php

- Poisoned nameservers have bogus NS records for the com zone.

- SANS ISC theorizes it may have been a vector for spyware propagation.

- Microsoft Windows NT, 2000, 2003, and Symantec firewall products are affected.
The Poisoning Attack

- An authoritative nameserver is configured (intentionally or not) to return bogus and out-of-bailiwick NS authority records. See example next four slides.

- A caching resolver trusts and caches the bogus referral.

- Future queries for names in the poisoned zone go to the bogus nameserver.

- The bogus nameserver returns incorrect answers to queries that it should not be receiving.
Bad Referral Example (1 of 4)

Start at the Root with `dig +trace longislandauction.com`

```
; <<>> DiG 9.3.2 <<>> +trace longislandauction.com
;; global options:  printcmd
. 141529 IN NS M.ROOT-SERVERS.NET.
. 141529 IN NS I.ROOT-SERVERS.NET.
. 141529 IN NS E.ROOT-SERVERS.NET.
. 141529 IN NS D.ROOT-SERVERS.NET.
. 141529 IN NS A.ROOT-SERVERS.NET.
. 141529 IN NS H.ROOT-SERVERS.NET.
. 141529 IN NS C.ROOT-SERVERS.NET.
. 141529 IN NS G.ROOT-SERVERS.NET.
. 141529 IN NS F.ROOT-SERVERS.NET.
. 141529 IN NS B.ROOT-SERVERS.NET.
. 141529 IN NS J.ROOT-SERVERS.NET.
. 141529 IN NS K.ROOT-SERVERS.NET.
. 141529 IN NS L.ROOT-SERVERS.NET.
;; Received 436 bytes from 206.168.0.2#53(206.168.0.2) in 3 ms
```
**Bad Referral Example (2 of 4)**

*m.root-servers.net* returns a referral for *com*

<table>
<thead>
<tr>
<th>com.</th>
<th>172800 IN NS</th>
<th>K.GTLD-SERVERS.NET.</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>L.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>M.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>A.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>B.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>C.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>D.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>E.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>F.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>G.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>H.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>I.GTLD-SERVERS.NET.</td>
</tr>
<tr>
<td>com.</td>
<td>172800 IN NS</td>
<td>J.GTLD-SERVERS.NET.</td>
</tr>
</tbody>
</table>

;; Received 499 bytes from 202.12.27.33#53(M.ROOT-SERVERS.NET) in 142 ms
Bad Referral Example (3 of 4)

k.gtld-servers.net returns a referral for longislandauction.com

longislandauction.com. 172800 IN NS auth1.ns.sargasso.net.
longislandauction.com. 172800 IN NS auth2.ns.sargasso.net.
longislandauction.com. 172800 IN NS auth3.ns.sargasso.net.

;; Received 162 bytes from 192.52.178.30#53(K.GTLD-SERVERS.NET) in 118 ms
Bad Referral Example (4 of 4)

auth1.ns.sargasso.net returns a bad referral for com with its answer

longislandauction.com. 300 IN A 127.127.127.127
com. 300 IN NS auth1.ns.sargasso.net.
com. 300 IN NS auth2.ns.sargasso.net.
com. 300 IN NS auth3.ns.sargasso.net.

;; Received 178 bytes from 198.77.14.65#53(auth1.ns.sargasso.net) in 80 ms
What if we trusted the bad referral?

# dig @auth1.ns.sargasso.net www.aol.com

;; QUESTION SECTION:

;www.aol.com. IN A

;; ANSWER SECTION:

www.aol.com. 300 IN A 127.127.127.127

;; AUTHORITY SECTION:

com. 300 IN NS auth1.ns.sargasso.net.
com. 300 IN NS auth2.ns.sargasso.net.
com. 300 IN NS auth3.ns.sargasso.net.

;; ADDITIONAL SECTION:

auth1.ns.sargasso.net. 3600 IN A 198.77.14.65
auth2.ns.sargasso.net. 3600 IN A 69.56.183.51
auth3.ns.sargasso.net. 3600 IN A 198.77.15.67
Vulnerable Implementations

The following caching resolvers are known to be susceptible to this type of poisoning:

- Windows NT
  - vulnerable by default
  - SP4 and later can become not-vulnerable after editing registry

- Windows 2000
  - SP1, SP2 vulnerable by default
  - SP3 and later not-vulnerable by default

- Windows 2003
  - not-vulnerable by default

- Symantec gateway/firewall products
  - google for SYM04-010 and SYM05-005
How Many Poisoners Are Out There?
How To Find Poisoners

- Start with a (large) list of DNS names or zones.

- Discover the set of authoritative nameservers for a zone by following referrals starting at the root.

- Query each authoritative nameserver.

- Compare the NS RR set in each reply to the previously-learned referrals for parent zones.

- This technique only finds parent-zone poisoning. Furthermore, we are limiting our search to TLD poisoning at this point.
February 2006 Survey

- Input is 6,332,966 names captured from nameservers operated by us.

- Found 284 “poisoning” nameservers — these return bogus referrals to a TLD, or the root.

- The following zones are poisoned:

<table>
<thead>
<tr>
<th>zone</th>
<th>#</th>
<th>zone</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>217</td>
<td>cc</td>
<td>2</td>
</tr>
<tr>
<td>com</td>
<td>49</td>
<td>cn</td>
<td>1</td>
</tr>
<tr>
<td>net</td>
<td>29</td>
<td>to</td>
<td>1</td>
</tr>
<tr>
<td>org</td>
<td>24</td>
<td>default</td>
<td>1</td>
</tr>
<tr>
<td>au</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Some nameservers poison multiple zones
Some Poisoners

dns.internic.ca
ns1.afternic.com
ns0.directnic.com
ns1.domainsarefree.com
ns1.my-name-server.com
ns0.expireddomainservices.com
park1.dnsmadeeasy.com
ns.sg.gs
ns2.pipipapa.net
redirns1.bgdns.net
ns2.parabolastudios.com
ns2.dnscheck.net
ns1.domainmonger.com
jar2.hostalia.com

ns1-expired.nictrade.se
ns1.pairnic.com
ns2.newdomllc.com
ns1.domainmonger.com
ns1.dr-parkingservices.com
dns1.arishost.com
ns1.opt.to
ns1.hi2000.net
ns3.typein.net
ns2.darkscape.net
uabdc1.uab.edu
ns2.domaincontender.com
ns1.totalnic.net
ns1.2n4c0.com
Never attribute to malice what can adequately be explained by stupidity

- Many of the nameservers that return bad referrals appear to be companies in the DNS business:
  - registrars
  - resellers
  - speculators
  - typo profiteers

- Others appear to be legitimate companies.

- They should know better.

- Many of the names leading to poisoners are either expired or parked.
Is the Sky Falling?

• With so many poisoners out there, why don’t we hear about more problems?

• Fortunately, most implementations do not allow the root zone to be poisoned.

• If you were surfing the Web with a poisoned DNS cache, would you know it?

• Let’s simulate it...

• For every bad referral found, we
  – Put the nameserver’s IP address in /etc/resolv.conf
  – Fire up a web browser and request www.google.com and www.microsoft.com
  – Take screenshots
We recently registered our domain name at NameScout.com.

February 05, 2006

Sponsored Links:

Search Engine Submission
Free traffic for 1 full year and be entered for 24,000 free visitors.
Search Engine Submission

Pay Per Click Service
Increase targeted traffic to your Website instantly.
Pay Per Click Service

All the Search Engines
All the Pay Per Click SE Savings Find Local Pay Per Click SE Here!
All the Search Engines

Vegas Affiliate Program
Shows, Tours, Merchandise, Poker Books, Cards, Chips and much more.
Vegas Affiliate Program

Super Affiliate Program
Learn Affiliate Marketing Secrets See Profits within Just 24-hr!
Super Affiliate Program

Submit Your URL
Need Website Traffic? Submit to 500,000 High Traffic Sites Free!
Submit Your URL

Web-Feet.co.uk Web Design
Find N Rank

Top Searches

<table>
<thead>
<tr>
<th>CASINO</th>
<th>MISC.</th>
<th>MONEY</th>
<th>INSURANCE</th>
<th>POPULAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Casino</td>
<td>Web Hosting</td>
<td>Debt Help</td>
<td>Health Insurance</td>
<td>Viagra</td>
</tr>
<tr>
<td>Gambling</td>
<td>Moving</td>
<td>Loans</td>
<td>Life Insurance</td>
<td>Online Dating</td>
</tr>
<tr>
<td>Slots</td>
<td>Long Distance</td>
<td>Finance</td>
<td>Auto Insurance</td>
<td>Inkjet</td>
</tr>
<tr>
<td>Sports Betting</td>
<td>Weight Loss</td>
<td>Money</td>
<td>Home Insurance</td>
<td>Credit Cards</td>
</tr>
<tr>
<td>Online Casino</td>
<td>Flowers</td>
<td>Lawyer</td>
<td>Insurance</td>
<td>Ringtones</td>
</tr>
</tbody>
</table>

Directory

Arts
Concerts, Movies, MP3, Music, Radio, Television, Video

Business
Industries, Finance, Jobs, Loans, Software, Standards

Home
Consumers, Home Loans, Homeowners Insurance, Family

Kids and Teens
Computers, Entertainment, Games, Music, School

Regional
Africa, Asia, Australia, Europe, North America, South America

Science
Astronomy, Biology, Paleontology, Psychology, Physics
An error occurred while loading http://www.google.com/:
Unknown host www.google.com
Blue Collar Comedy Tour: The Movie
A MUST-HAVE!!!
GET THIS MOVIE! This is the funniest movie you'll ever see! It tops even "Rat Race!" Jeff, Bill, Ron and Larry are hilarious even when they're not on stage! "He just made enough money to buy anything he wants in the store, and he gets the remote-controlled"

More...

NCAA Football 2005
Not a review, just a summary of new features.
As I said in the title, this is not a review. I just want to save like-minded people some time, and summarize what makes 2005 different from the 2004 title. While this isn't platform specific, the biggest upgrade this year is for the Xbox, as EA and Micros

More...
Welcome to PowerSiteSystem Setup for google.com

Please Enter your Subscription Number to verify your payment
If you have paid using paypal, the subscription id can be found in your paypal receipt email or when you login to your paypal account and view the details of your payment. Example S-2RF693066K543900R

Subscription Id

Your Subscription id can be used for 1 time only, so make sure that you want to use your subscription for the setup of google.com

Please choose a username and password that you will use to manage your site, you will be unable to change this later so select a name that you can remember and make sure to note down your selected password so that you do not forget it.

Select Username
Select Password

Please enter your email id where we will send you the instructions for your site.

Enter your Email

Entering your Name is optional

First Name : Last Name :
This domain name registered through pairNIC

Smart people choose pairNIC. Here's why ...

Every pairNIC v2.6 domain name includes:

- Free Change of Ownership
- Free pairNIC Place Holder Page
- Free Custom DNS
- Free URL & E-Mail Forwarding
- Free Domain Name Security Features
- Complete, Secure Online Management with Billing Statements + More

Register or Transfer today!
We have great rates too!
You are here by accident

It has been brought to our attention that the IP address of this server (205.209.153.162) is being used as a local DNS resolver by a cable or broadband provider somewhere.

This is a mistake because this server reports the same IP for all queries for an internal application that has nothing to do with you.

You need to contact your access provider (whoever they are) and get proper DNS resolvers from them.
Lazy, Stupid, or Evil?
The administrator is too lazy to put each domain delegated to them into separate zone files. Instead, they create a com zone and list A records for each delegation (see next slide).

Laziness such as this is probably the source of most of the poison that we find.
Laziness: ns1.hi2000.com, cont

Their zone file probably looks like this...

$ORIGIN com.
@ IN SOA ns1.hi2000.com. hostmaster.hi2000.com ( 2003042101 ; serial
28800 ; refresh
14400 ; retry
3600000 ; expire
86400 ) ; minimum
china-bamboo-wood IN A 202.101.43.181
www.china-bamboo-wood IN A 202.101.43.132
newsunseed IN A 202.101.43.132
www.newsunseed IN A 202.101.43.132
...
Stupidity: ns1.frakes.net

;; ANSWER SECTION:
gripelist.com. 86400 IN A 64.202.173.35

;; AUTHORITY SECTION:
com. 86400 IN NS ns2.com.
com. 86400 IN NS ns3.com.
com. 86400 IN NS ns1.com.

;; ADDITIONAL SECTION:
ns1.com. 86400 IN A 66.249.1.244
ns2.com. 86400 IN A 66.249.7.25
ns3.com. 86400 IN A 66.249.1.100

Typos, combined with laziness, create an interesting situation. Looks like frakes.net is using the com zone technique, but forgot to make the nameservers fully qualified.

Note that ns1.com, etc are legitimate DNS names and have A records different than those returned by ns1.frakes.net.
Evilness

Our definition of an evil poisoning nameserver is one where it answers queries, with the wrong address, and proxies web traffic sent there so you still get what you expect.

To help find them, we give each source of poison an evilness ranking from 1–5. One point each for:

- Returning a bad referral
- Poisoning a TLD
- Answering an A query for “important names”
- Answering the query incorrectly.
- Answering the query such that the a web browser looks the same as with correct DNS.

Found a few “fours” but no “fives” yet.
Miscellany

- Some of the poison sources that we find are actually vulnerable implementations that have been previously poisoned.

- Remember: **authoritative nameservers should never accept recursive queries!**

- Some NS records have non-FQDN names. The name “ns” is a popular example.

- It’s a good thing even the vulnerable implementations don’t let the root zone become poisoned.
Bottom Line

• Several hundred misconfigured nameservers out there return bad referrals that can poison DNS caches.
  – Some perhaps with malicious intent

• About 75% of those try to poison the root zone, which usually has no effect.

• Probably 90% of nameservers out there today are not vulnerable to this type of poisoning.

• Most of the attempted poisoning can be attributed to laziness and stupidity.
For More Information

• Browse the Poisoners Database
  http://dns.measurement-factory.com/surveys/poisoners.html

• wessels@measurement-factory.com
The End