
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/diary.php?date=2005-04-03>
 - <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*

```
com.          172800  IN      NS      K.GTLD-SERVERS.NET.
com.          172800  IN      NS      L.GTLD-SERVERS.NET.
com.          172800  IN      NS      M.GTLD-SERVERS.NET.
com.          172800  IN      NS      A.GTLD-SERVERS.NET.
com.          172800  IN      NS      B.GTLD-SERVERS.NET.
com.          172800  IN      NS      C.GTLD-SERVERS.NET.
com.          172800  IN      NS      D.GTLD-SERVERS.NET.
com.          172800  IN      NS      E.GTLD-SERVERS.NET.
com.          172800  IN      NS      F.GTLD-SERVERS.NET.
com.          172800  IN      NS      G.GTLD-SERVERS.NET.
com.          172800  IN      NS      H.GTLD-SERVERS.NET.
com.          172800  IN      NS      I.GTLD-SERVERS.NET.
com.          172800  IN      NS      J.GTLD-SERVERS.NET.
```

```
;; 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:

| zone | # | zone | # |
|------|-----|---------|---|
| . | 217 | cc | 2 |
| com | 49 | cn | 1 |
| net | 29 | to | 1 |
| org | 24 | default | 1 |
| au | 3 | | |

- 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

Location Edit View Go Bookmarks Tools Settings Window Help

Location:  http://www.google.com/

www.google.com

This page is parked free, courtesy of [GoDaddy.com](#)

Popular Searches

Travel

- [Hotels](#)
- [Cruises](#)
- [Cheap Flights](#)
- [Car Rental](#)
- [Travel Insurance](#)

Lifestyle

- [Dating](#)
- [Personals](#)
- [Singles](#)
- [Chat](#)
- [Vacations](#)

Business

- [Bankruptcy](#)
- [CRM](#)
- [How to Make Money](#)
- [Conference Calls](#)
- [Business Cards](#)

Financial Planning

- [Loans](#)
- [Credit Cards](#)
- [Debt Consolidation](#)
- [Stocks](#)
- [Payday Loans](#)

Real Estate

- [Mortgages](#)
- [Home Insurance](#)
- [Home Equity Loans](#)
- [Homes For Sale](#)
- [Credit Reports](#)

Shopping

- [Flowers](#)
- [Gifts](#)
- [Books](#)
- [Jewelry](#)
- [Pets](#)

E-Commerce

- [VoIP](#)
- [Broadband](#)
- [Web Hosting](#)
- [Domain Names](#)
- [Web Design](#)

Autos

- [Used Cars](#)
- [Car Loans](#)
- [Auto Repair](#)
- [Car Insurance](#)
- [Cars For Sale](#)

Personal Finances

- [Jobs](#)
- [Student Loans](#)
- [Life Insurance](#)
- [Personal Loans](#)
- [Work from Home](#)



LIMITED-TIME OFFER

\$1.99 No Qty Limit
Domains

Now, with any non-domain purchase!

FREE with every domain name:

- ▶ NEW! Hosting** with Web builder
- ▶ NEW! Quick Blog
- ▶ Complete Email
- ▶ AND MORE!



Find a domain name now:

 .com

Advanced Search

*Plus ICANN fee of 25 cents per domain name year.

**Turbo-Charged
Hosting & Servers**

Plans starting from **\$3.95/mo**

▶ NEW! Premium Plans

The image shows a screenshot of a web browser window. The address bar displays "http://www.google.com/". The page header features the "google.com" logo and a notification: "We recently registered our domain name at NameScout.com." A "namescout.com" logo is also present in the top right. The date "February 05, 2006" is shown on the left, and a search bar with a "Go" button is on the right. The main content area is divided into two columns. The left column, titled "Sponsored Links:", contains several promotional items with blue underlined titles and green underlined links: "Search Engine Submission" (with a link to "Search Engine Submission"), "Pay Per Click Service" (with a link to "Pay Per Click Service"), "All the Search Engines" (with a link to "All the Search Engines"), "Vegas Affiliate Program" (with a link to "Vegas Affiliate Program"), "Super Affiliate Program" (with a link to "Super Affiliate Program"), "Submit Your URL" (with a link to "Submit Your URL"), and "Web-Feet.co.uk Web Design". The right column, titled "Related Categories:", lists various search engine categories such as "Global Search Engines", "MetaSearch Engines", "Pay Per Click Search Engines", "Add URL to Search Engines", "Submission to Search Engines", "Submit to Search Engines", "Internet Search Engines", "Multi Search Engines", "Meta Search Engines", "Image Search Engines", "Other Search Engines", "New Search Engines", "Best Search Engines", "UK Search Engines", "Australian Search Engines", "Picture Search Engines", and "Different Search Engines". The browser's status bar at the bottom indicates "Page loaded."

Location Edit View Go Bookmarks Tools Settings Window Help

Location: <http://www.findnrank.com/?ref=aosgs>

Find N Rank

[Make This Your Homepage](#) [Add This Page to Your Favorites](#)

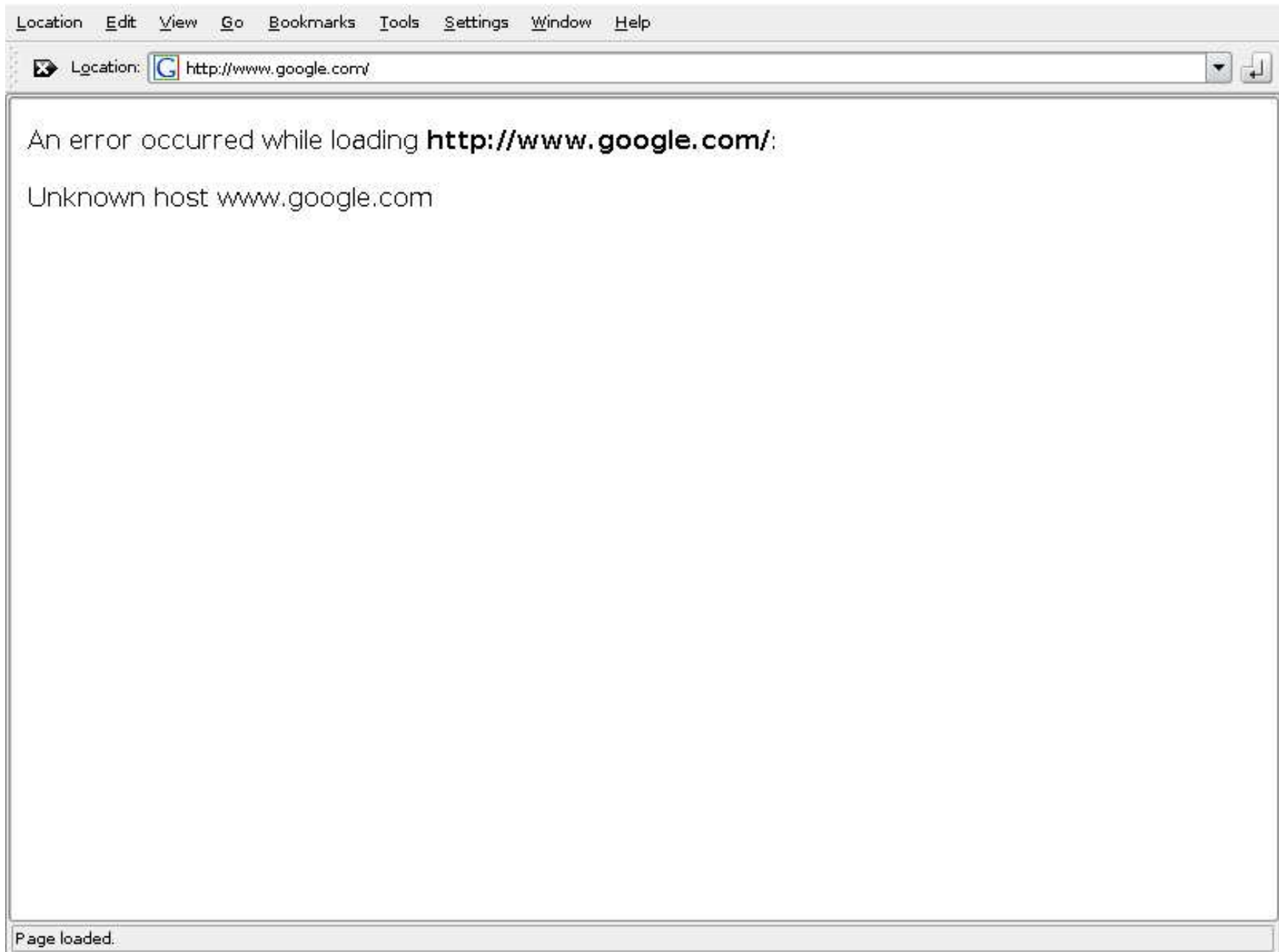
Top Searches

| CASINO | MISC. | MONEY | INSURANCE | POPULAR |
|-----------------------------------|----------------------------------|------------------------------|-------------------------------------|----------------------------------|
| 1. Casino | 1. Web Hosting | 1. Debt Help | 1. Health Insurance | 1. Viagra |
| 2. Gambling | 2. Moving | 2. Loans | 2. Life Insurance | 2. Online Dating |
| 3. Slots | 3. Long Distance | 3. Finance | 3. Auto Insurance | 3. Inkjet |
| 4. Sports Betting | 4. Weight Loss | 4. Money | 4. Home Insurance | 4. Credit Cards |
| 5. Online Casino | 5. Flowers | 5. Lawyer | 5. Insurance | 5. Ringtones |

Directory

- [Arts](#)
- [Concerts](#), [Movies](#), [MP3](#), [Music](#), [Radio](#), [Television](#), [Video](#)
- [Home](#)
- [Consumers](#), [Home Loans](#), [Homeowners Insurance](#), [Family](#)
- [Regional](#)
- [Africa](#), [Asia](#), [Australia](#), [Europe](#), [North America](#), [South America](#)
- [Business](#)
- [Industries](#), [Finance](#), [Jobs](#), [Loans](#), [Software](#), [Standards](#)
- [Kids and Teens](#)
- [Computers](#), [Entertainment](#), [Games](#), [Music](#), [School](#)
- [Science](#)
- [Astronomy](#), [Biology](#), [Paleontology](#), [Psychology](#), [Physics](#)

dns2.nai.com



ns.domainredirect.com



Location Edit View Go Bookmarks Tools Settings Window Help

Location:  http://www.google.com/

NATIONWIDE SHIPPING!

Online Consultations
Lowest Prices
Discreet Packaging
Buy in Bulk and Save!



Brand Name Medications

***Brand Name Medications prescribed by real doctors and discretely shipped to your door in 48 hours or less

CALL : (309) 273-2150

EliteMedications.com



EliteMedications.com

Home Price List FAQ About Report Spam **I to be true.....it is! Our prices are the best** View Cart Order Status Contact Us

WIN free prescriptions for one year!

Enter Your Email Address Here:

Submit

Bookmark this site


Products

- Weight Loss
 - Adipex
 - Bontril
 - Bontril SR
 - Didrex

| | | |
|--|---|---|
|  Xanax 30 (pills) x 1mg Place your order today! ONLY \$164 ADD TO CART |  Adipex 30 (pills) x 37.5mg Place your order today! ONLY \$149 ADD TO CART |  Viagra 5 (pills) x 100mg Place your order today! ONLY \$119 ADD TO CART |
|  Ultram 30 (pills) x 50mg Place your order today! ONLY \$80 ADD TO CART |  Bontril 90 (pills) x 35mg Place your order today! ONLY \$99 ADD TO CART |  Didrex 90 (pills) x 50mg Place your order today! ONLY \$199 ADD TO CART |

Page loaded.

Location Edit View Go Bookmarks Tools Settings Window Help


Location:  http://www.google.com/

Welcome! Search: Search

Home
[Baby Store](#)
[Book Store](#)
[Camera & Photo Store](#)
[Computer Store](#)
[Game Store](#)
[DVD Store](#)
[Electronics Store](#)
[Kitchen Store](#)
[Magazine Store](#)
[Music Store](#)
[Garden Store](#)
[Software Store](#)
[Tools Store](#)
[Toys Store](#)
[Video Store](#)

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...](#)

My Shopping Bag:
 Items: 0
Total: \$0
[View Bag](#)

Free Shipping!
Hot Deals

Best Sites:
[LightWave6.com](#)
[lway.org](#)
[Internet-Film.org](#)
[EraLine.com](#)
[NewspaperNow.com](#)
[00-00-00-00.com](#)
[www.my999.com](#)
[SinaCity.com](#)

Page loaded.

ns1.frakes.net

The screenshot shows a web browser window with the address bar containing `http://www.google.com/start.php`. The browser's menu bar includes `Location`, `Edit`, `View`, `Go`, `Bookmarks`, `Tools`, `Settings`, `Window`, and `Help`. The main content area displays a webpage with a large image of a man in a dark jacket. A modal dialog box titled "Missing Plugin - Konqueror" is overlaid on the page. The dialog contains the following text: "No plugin found for 'Shockwave Flash Media'." followed by "Do you want to download one from www.macromedia.com?" Below this text is a checkbox labeled "Do not ask again" which is currently unchecked. At the bottom of the dialog are two buttons: "Download" and "Do Not Download". The background webpage text is partially visible, including "Jothan, Jothan", "Welcome to Jothan Frak", "Did you mean to go to [WW](#)", and a paragraph starting with "1/10/06 Vint Cerf to speak at Domain Roundtable this coming April 19-21. This is a big deal, and I am thrilled at the chance to have gotten him to come speak at the conference. It will be a great win for the audience. Marc Ostrovsky of IREIT, a long time domain name legend will be speaking at the conference on the term 'Internet Real Estate', one he coined back in 1994. The show was great last year, and the upcoming show should be fantastic. If you are into domains, I strongly reccomend attending (though I am a bit biased, I must admit, because of being the executive event". The browser's status bar at the bottom left shows "Page loaded."

Location Edit View Go Bookmarks Tools Settings Window Help

Location:  http://www.google.com/

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 yor 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 emailid where we will send you the instructions for your site.

Enter your Email

Entering your Name is optional

First Name : Last Name :

Page loaded.

ns2.pairnic.com

Location Edit View Go Bookmarks Tools Settings Window Help

Location: <http://www.google.com/>

pairNIC

what's
Services
Register
transfer
login
Beginner's
faq
pricing
Webhosting
About
Service
contact

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!

Page loaded.

ns3.gi.net

The image shows a screenshot of the Google.com homepage as it appeared in the early 2000s, viewed within a web browser window. The browser's address bar shows the URL "http://www.google.com/". The page features the Google logo and the slogan "We search, so you don't have to." Below the logo is a search bar with the text "Find it:" and a "Search" button. The main content area is organized into a grid of categories, each with a list of related services or products. The categories include Travel, Gambling, Money Savers, Services, Health & Beauty, Educate Yourself, Gifts & Apparel, Sports Tickets, Computers, Professional Services, New Technology, and Legal Assistance. The browser's status bar at the bottom indicates "Page loaded."

Location Edit View Go Bookmarks Tools Settings Window Help

Location: http://www.google.com/

google.com
We search, so you don't have to!

Find it: Search

Travel
Airline Tickets
Cruises
Car Rental
Hotels
Discount Vacations

Gambling
Sports Betting
Poker
Texas Holdem
Blackjack
Online Casino

Money Savers
Health Insurance
Debt Consolidation
Student Loans
Refinance
Free Credit Report

Services
Car Insurance
Mortgage
Business Opportunities
Life Insurance
Work From Home

Health & Beauty
Weight Loss
Health Care
Hair Replacement
Exercise Equipment
Skin Care Products

Educate Yourself
Real Estate Training
Ditech
Weight Loss
Alcohol Treatment
MCSE Certification

Gifts & Apparel
Birthday Gifts
Gift Certificates
Jewelry
Wedding Gifts
Gift Baskets

Sports Tickets
NASCAR Tickets
Hockey Tickets
Basketball Tickets
Baseball Tickets
Football Tickets

Computers
Computer Rental
Software Training
LCD Projectors

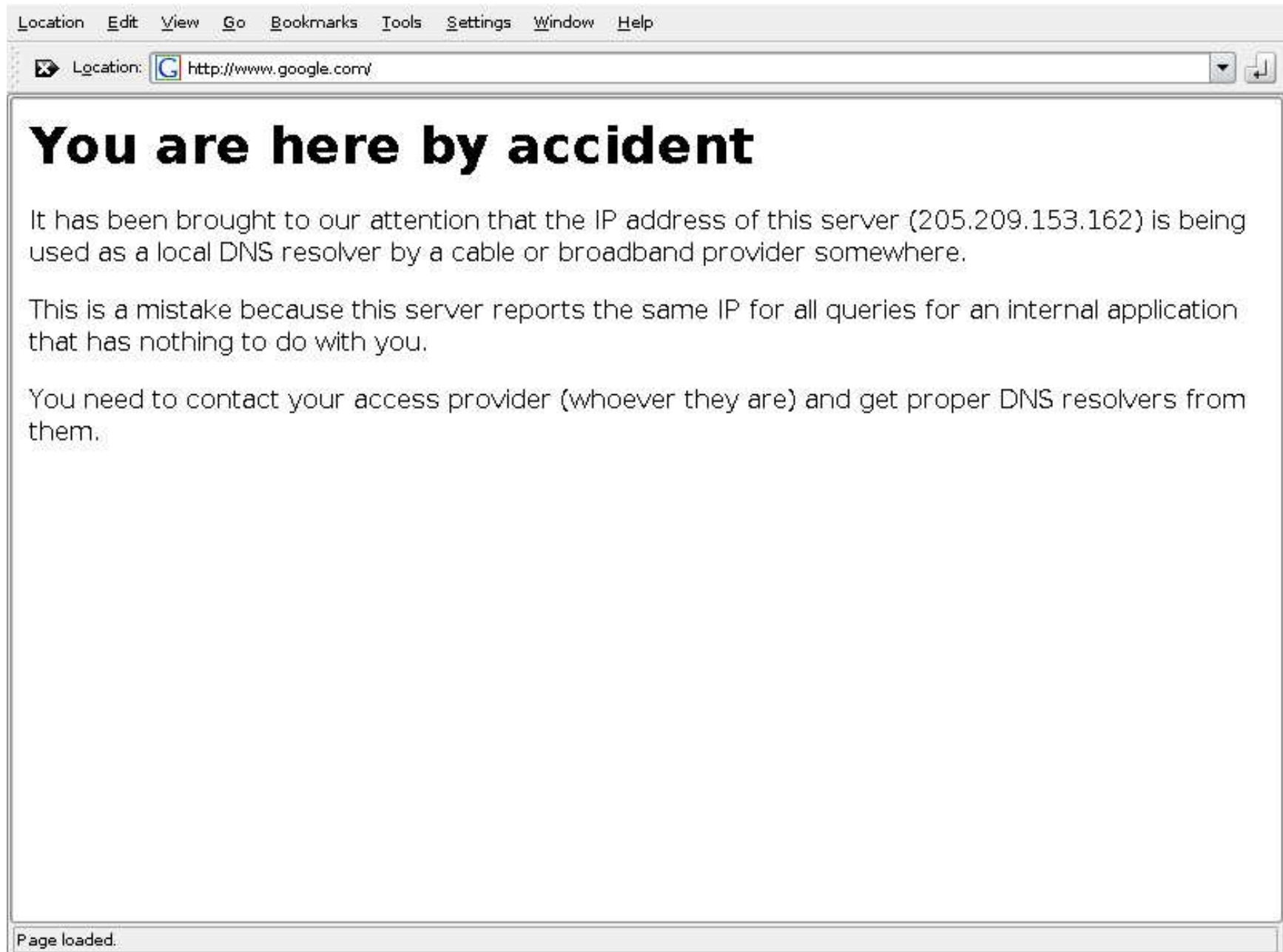
Professional Services
Website Design
Gourmet Food Gifts
Online Dating

New Technology
Mobile Phones
PDAs
DVD Rental

Legal Assistance
Patent Lawyers
Bankruptcy Lawyers
Probate Lawyers

Page loaded.

65.75.128.178.com



Lazy, Stupid, or Evil?

Laziness: ns1.hi2000.com

;; QUESTION SECTION:

;china-bamboo-wood.com. IN A

;; ANSWER SECTION:

china-bamboo-wood.com. 86400 IN A 202.101.43.181

;; AUTHORITY SECTION:

com. 86400 IN NS ns1.hi2000.com.

com. 86400 IN NS ns2.hi2000.com.

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
IN           NS       ns1.hi2000.com.
IN           NS       ns2.hi2000.com.
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:

| | | | | |
|-----------------------------|--------------------|-----------------|----------------|----------------------------|
| <code>gripelist.com.</code> | <code>86400</code> | <code>IN</code> | <code>A</code> | <code>64.202.173.35</code> |
|-----------------------------|--------------------|-----------------|----------------|----------------------------|

;; AUTHORITY SECTION:

| | | | | |
|-------------------|--------------------|-----------------|-----------------|-----------------------|
| <code>com.</code> | <code>86400</code> | <code>IN</code> | <code>NS</code> | <code>ns2.com.</code> |
| <code>com.</code> | <code>86400</code> | <code>IN</code> | <code>NS</code> | <code>ns3.com.</code> |
| <code>com.</code> | <code>86400</code> | <code>IN</code> | <code>NS</code> | <code>ns1.com.</code> |

;; ADDITIONAL SECTION:

| | | | | |
|-----------------------|--------------------|-----------------|----------------|---------------------------|
| <code>ns1.com.</code> | <code>86400</code> | <code>IN</code> | <code>A</code> | <code>66.249.1.244</code> |
| <code>ns2.com.</code> | <code>86400</code> | <code>IN</code> | <code>A</code> | <code>66.249.7.25</code> |
| <code>ns3.com.</code> | <code>86400</code> | <code>IN</code> | <code>A</code> | <code>66.249.1.100</code> |

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.
- Its 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