Inflight Modifications of Content: Who are the Culprits?

- *Chao Zhang*
- Keith W. Ross

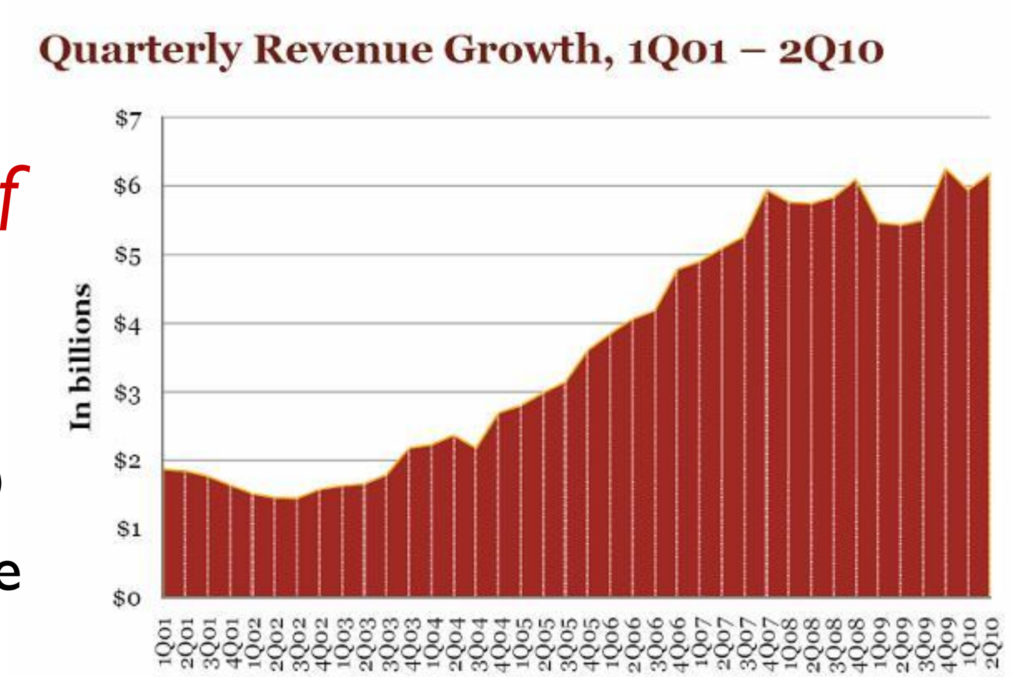
Polytechnic of NYU

- Cheng Huang
- David A. Maltz
- Jin Li

Microsoft Research

Motivation

- Online advertising becomes main source of revenue
- *High revenue attracts eyes of third-party*
  - Bahama botnet stealing traffic from Google *(blog.clickforensics.com, Sep 17, 2009)*
  - Web Tripwires demonstrate inflight modification *(NSDI, 2008)*



http://mashable.com/2010/10/12/

Contribution

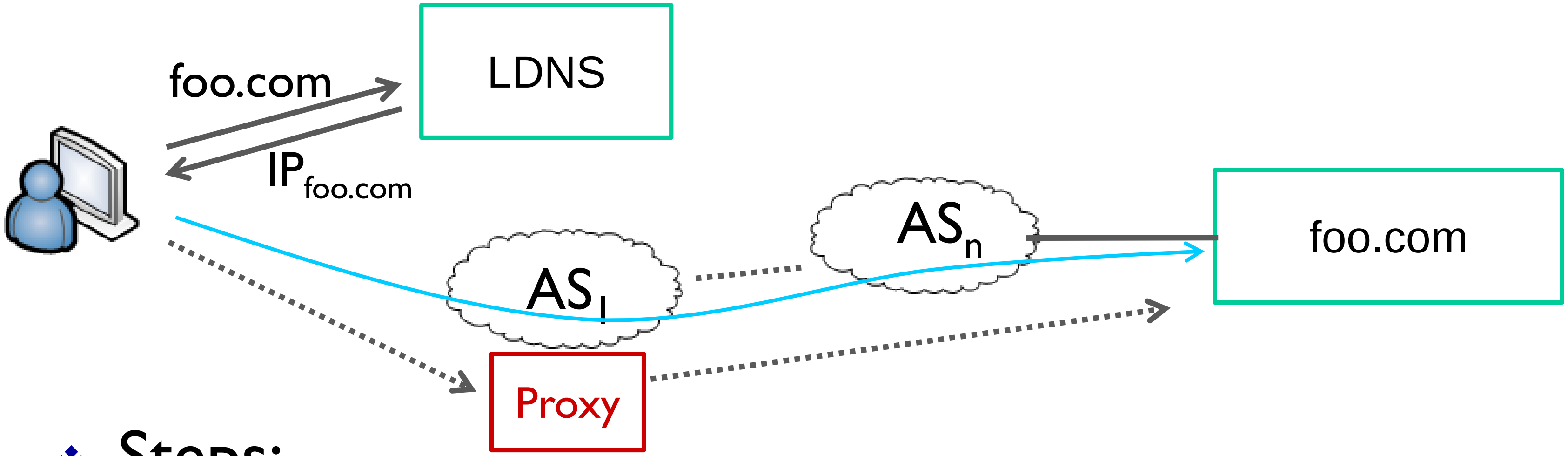
- *Nearly 2% clients from US are affected by inflight modification*
- *44 LDNS in 9 ISPs redirect clients to malicious servers*

ISP	# of cmpmzd LDNS	affected clients (%)
Hughes Network Systems	14	95.5
Frontier Communications	13	92.7
Cavalier Telephone	7	87.0
FiberNet of West Virginia	1	70.3
Spacenet, Inc.	1	97.8
Onvoy	3	76.1
WideOpenWest	3	68.6
Cincinnati Bell Telephone	1	92.6
South Dakota Network	1	88.5

Outline

- *Identifying the Inflight Modification*
- Digging the Root Causes
- Summary

Processing of Fetching a Page



- Steps:
  - DNS resolution
  - HTTP request to foo.com
  - Content to client
- Sometimes, clients are redirected to web

Q: Do Proxies Modify Pages?

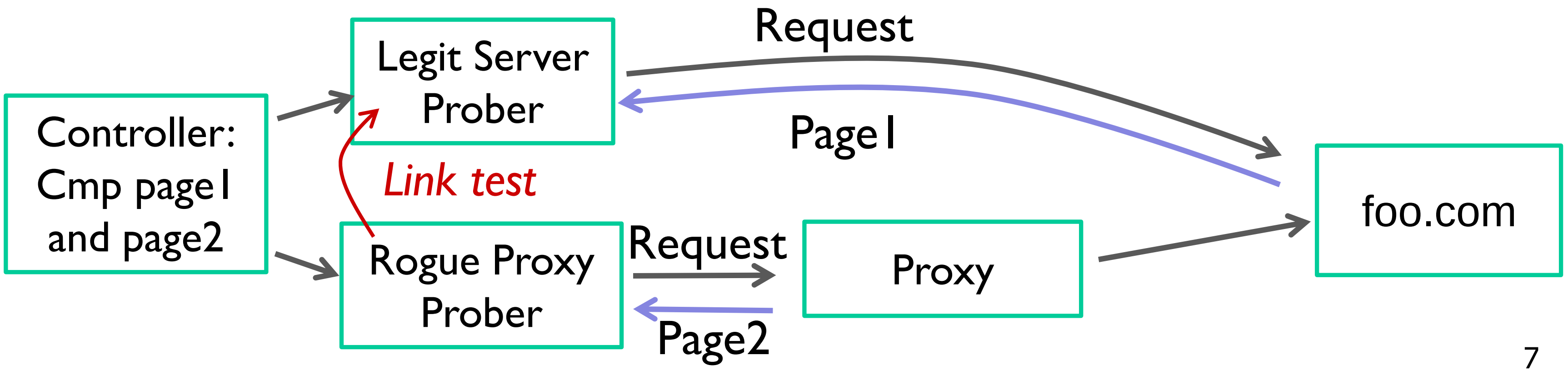
Collecting Proxies List

- Instrument clients in the wild
- Each client reports:
  - Its IP
  - The IPs of foo.com returned by the LDNS
- In two months, we collected
  - I5M unique clients
  - 4,437 proxies for foo.com

Q: Which proxy servers are modifying the content?

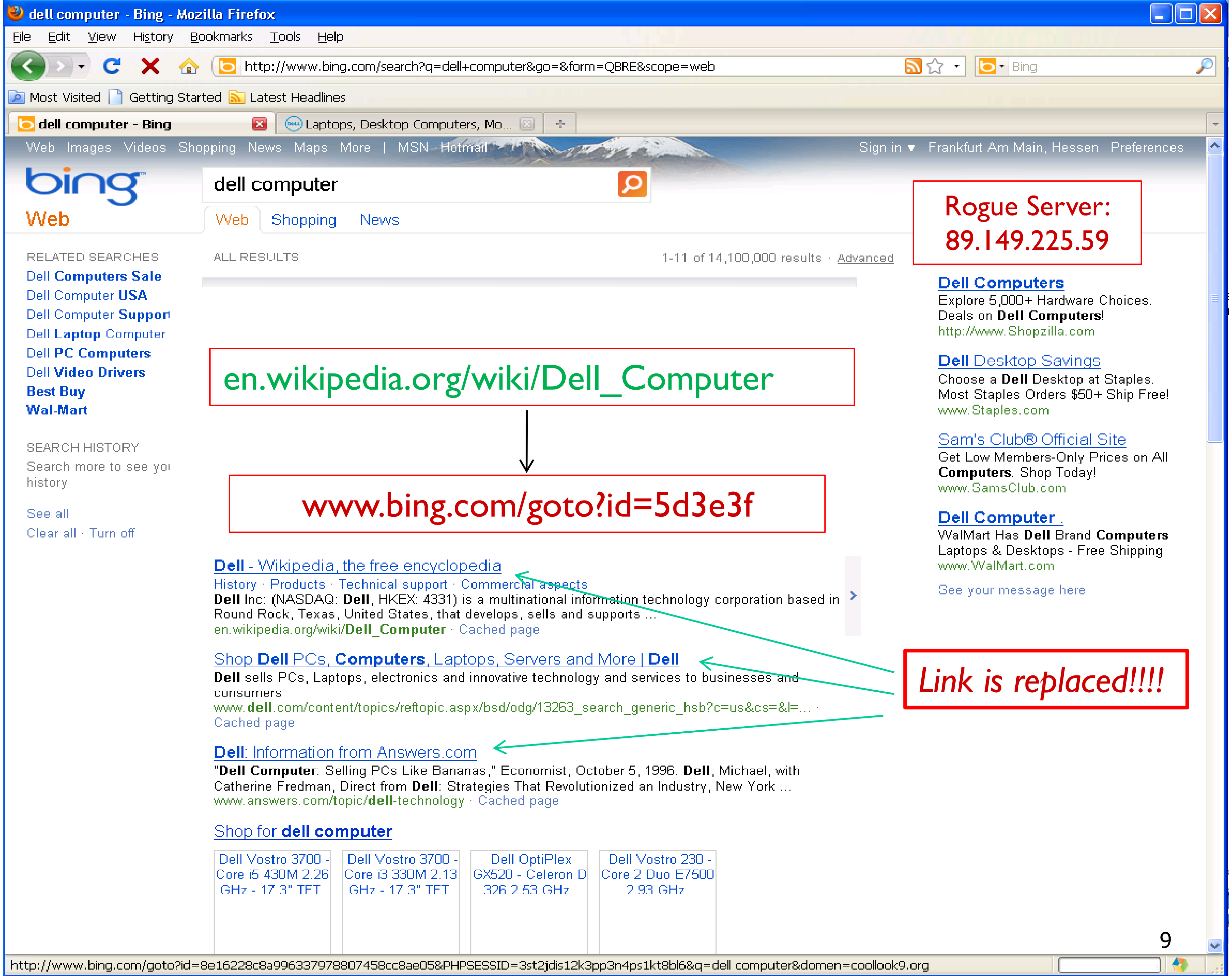
Identifying Rogue Proxies: Revealer Framework

- Fetch pages from two servers, compare
- Benign, if content is the same
- *Different content doesn't necessarily mean that the proxy is malicious*
  - *Search result page with ads*
  - different ads can be identified by links
  - test the link again by emulate user click
- Capture all HTTP traffic
  - Analyze abnormal redirection



Types of Modifications

- *Modify search result links*
- Modify advertisements links
- Insert JavaScript
- Redirect requests



dell computer - Bing - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.bing.com/search?q=dell+computer&go=&form=QBRE&scope=web

Most Visited · Getting Started · Latest Headlines

dell computer - Bing · Laptops, Desktop Computers, Mo...

Web Images Videos Shopping News Maps More | MSN Hotmail · Sign in · Frankfurt Am Main, Hessen · Preferences

bing Web

dell computer

Web · Shopping · News

RELATED SEARCHES

- Dell **Computers Sale**
- Dell Computer **USA**
- Dell Computer **Suppor**
- Dell **Laptop** Computer
- Dell **PC Computers**
- Dell **Video Drivers**
- **Best Buy**
- **Wal-Mart**

SEARCH HISTORY

Search more to see yo history

See all

Clear all · Turn off

ALL RESULTS · 1-11 of 14,100,000 results · Advanced

en.wikipedia.org/wiki/Dell_Computer

↓

www.bing.com/goto?id=5d3e3f

Dell - Wikipedia, the free encyclopedia
History · Products · Technical support · Commercial aspects
Dell Inc. (NASDAQ: **Dell**, HKEX: 4331) is a multinational information technology corporation based in Round Rock, Texas, United States, that develops, sells and supports ...
en.wikipedia.org/wiki/**Dell_Computer** · Cached page

Shop **Dell** PCs, **Computers**, Laptops, Servers and More | **Dell**
Dell sells PCs, Laptops, electronics and innovative technology and services to businesses and consumers
www.**dell**.com/content/topics/reftopic.aspx/bsd/odg/13263_search_generic_hsb?c=us&cs=&l=... · Cached page

Dell: Information from Answers.com
"**Dell Computer**: Selling PCs Like Bananas," Economist, October 5, 1996. **Dell**, Michael, with Catherine Fredman, Direct from **Dell**: Strategies That Revolutionized an Industry, New York ...
www.answers.com/topic/**dell**-technology · Cached page

Shop for **dell computer**

Dell Vostro 3700 - Core i5 430M 2.26 GHz - 17.3" TFT	Dell Vostro 3700 - Core i3 330M 2.13 GHz - 17.3" TFT	Dell OptiPlex GX520 - Celeron D 326 2.53 GHz	Dell Vostro 230 - Core 2 Duo E7500 2.93 GHz

Rogue Server: 89.149.225.59

Dell Computers
Explore 5,000+ Hardware Choices. Deals on **Dell Computers**!
http://www.Shopzilla.com

Dell Desktop Savings
Choose a **Dell** Desktop at Staples. Most Staples Orders $50+ Ship Free!
www.Staples.com

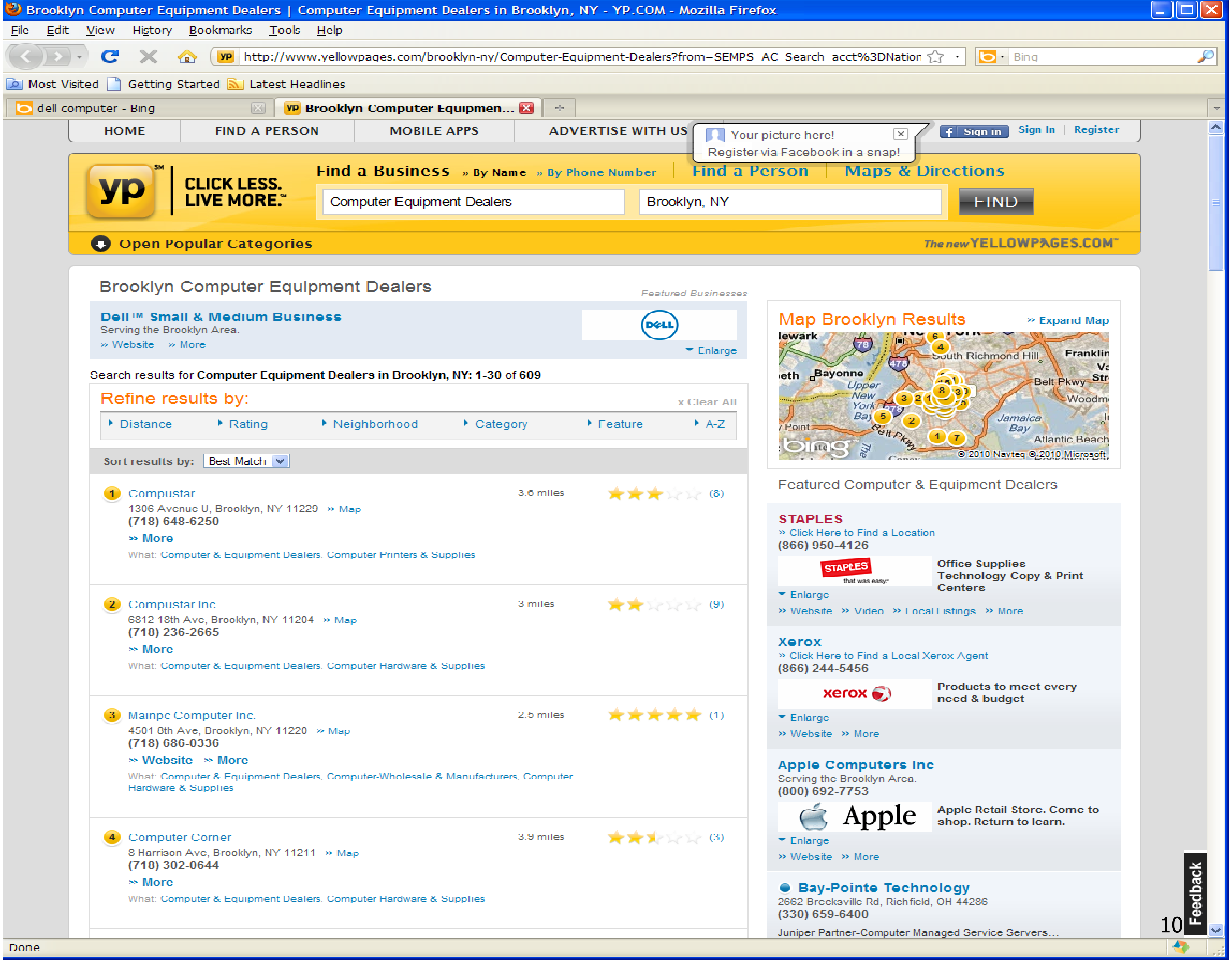
Sam's Club® Official Site
Get Low Members-Only Prices on All **Computers**. Shop Today!
www.SamsClub.com

Dell Computer
WalMart Has **Dell** Brand **Computers** Laptops & Desktops - Free Shipping
www.WalMart.com

See your message here

Link is replaced!!!!

http://www.bing.com/goto?id=8e16228c8a996337978807458cc8ae05&PHPSESSID=3st2jdis12k3pp3n4ps1kt8bl6&q=dell computer&domen=coollook9.org



Brooklyn Computer Equipment Dealers | Computer Equipment Dealers in Brooklyn, NY - YP.COM - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.yellowpages.com/brooklyn-ny/Computer-Equipment-Dealers?from=SEMPS_AC_Search_acct%3DNatior
Bing
Most Visited
Getting Started
Latest Headlines
dell computer - Bing
Brooklyn Computer Equipmen...
HOME
FIND A PERSON
MOBILE APPS
ADVERTISE WITH US
Sign in
Sign In | Register
CLICK LESS. LIVE MORE.
FIND
Open Popular Categories
The new YELLOWPAGES.COM
Done
Feedback

Your picture here!
Register via Facebook in a snap!

Find a Business » By Name » By Phone Number | Find a Person | Maps & Directions

Computer Equipment Dealers | Brooklyn, NY

Brooklyn Computer Equipment Dealers

Featured Businesses

Dell™ Small & Medium Business
Serving the Brooklyn Area.
» Website » More
Enlarge

Search results for **Computer Equipment Dealers in Brooklyn, NY: 1-30** of **609**

Refine results by: x Clear All

Distance | Rating | Neighborhood | Category | Feature | A-Z

Sort results by: Best Match

1. **Compustar** — 3.6 miles — ★★★☆☆ (8)
1306 Avenue U, Brooklyn, NY 11229 » Map
(718) 648-6250
» More
What: Computer & Equipment Dealers, Computer Printers & Supplies

2. **Compustar Inc** — 3 miles — ★★☆☆☆ (9)
6812 18th Ave, Brooklyn, NY 11204 » Map
(718) 236-2665
» More
What: Computer & Equipment Dealers, Computer Hardware & Supplies

3. **Mainpc Computer Inc.** — 2.5 miles — ★★★★★ (1)
4501 8th Ave, Brooklyn, NY 11220 » Map
(718) 686-0336
» Website » More
What: Computer & Equipment Dealers, Computer-Wholesale & Manufacturers, Computer Hardware & Supplies

4. **Computer Corner** — 3.9 miles — ★★½☆☆ (3)
8 Harrison Ave, Brooklyn, NY 11211 » Map
(718) 302-0644
» More
What: Computer & Equipment Dealers, Computer Hardware & Supplies

Map Brooklyn Results » Expand Map

Featured Computer & Equipment Dealers

STAPLES
» Click Here to Find a Location
(866) 950-4126
Office Supplies-Technology-Copy & Print Centers
Enlarge
» Website » Video » Local Listings » More

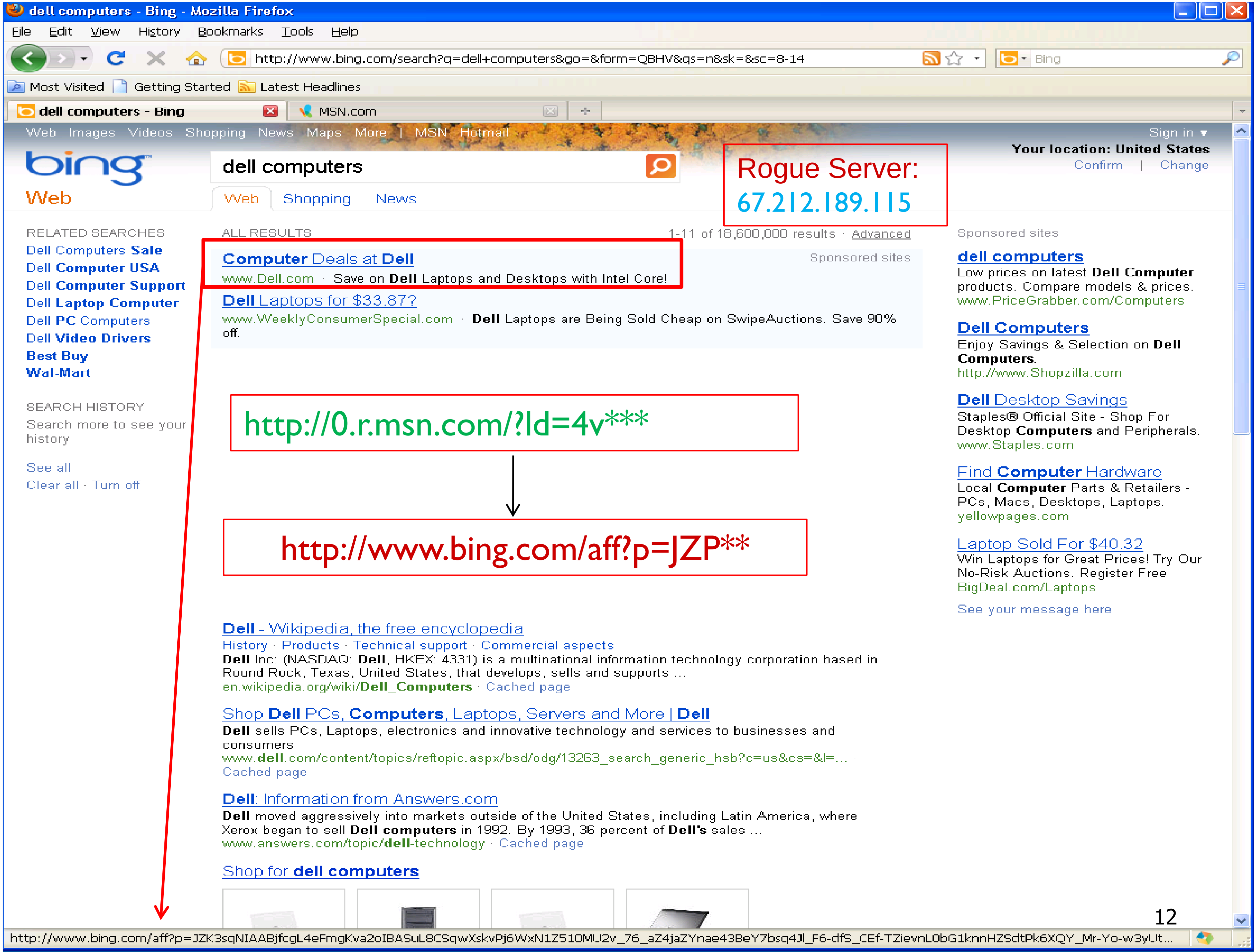
Xerox
» Click Here to Find a Local Xerox Agent
(866) 244-5456
Products to meet every need & budget
Enlarge
» Website » More

Apple Computers Inc
Serving the Brooklyn Area.
(800) 692-7753
Apple Retail Store. Come to shop. Return to learn.
Enlarge
» Website » More

Bay-Pointe Technology
2662 Brecksville Rd, Richfield, OH 44286
(330) 659-6400
Juniper Partner-Computer Managed Service Servers...

Types of Modifications

- Modify search result links
- *Modify advertisements links*
- Insert JavaScript
- Redirect requests


dell computers - Bing - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.bing.com/search?q=dell+computers&go=&form=QBHV&qs=n&sk=&sc=8-14
Bing
Most Visited
Getting Started
Latest Headlines
dell computers - Bing
MSN.com
Web Images Videos Shopping News Maps More | MSN Hotmail
Sign in
bing
Web
dell computers
Web Shopping News

Your location: United States
Confirm | Change

Rogue Server:
67.212.189.115

RELATED SEARCHES
- Dell Computers **Sale**
- Dell **Computer USA**
- Dell **Computer Support**
- Dell **Laptop Computer**
- Dell **PC** Computers
- Dell **Video Drivers**
- **Best Buy**
- **Wal-Mart**

SEARCH HISTORY
Search more to see your history

See all
Clear all · Turn off

ALL RESULTS 1-11 of 18,600,000 results · Advanced

Sponsored sites

Computer Deals at Dell
www.Dell.com · Save on **Dell** Laptops and Desktops with Intel Core!

Dell Laptops for $33.87?
www.WeeklyConsumerSpecial.com · **Dell** Laptops are Being Sold Cheap on SwipeAuctions. Save 90% off.

http://0.r.msn.com/?ld=4v***

↓

http://www.bing.com/aff?p=JZP**

Dell - Wikipedia, the free encyclopedia
History · Products · Technical support · Commercial aspects
Dell Inc. (NASDAQ: **Dell**, HKEX: 4331) is a multinational information technology corporation based in Round Rock, Texas, United States, that develops, sells and supports ...
en.wikipedia.org/wiki/**Dell**_**Computers** · Cached page

Shop **Dell** PCs, **Computers**, Laptops, Servers and More | **Dell**
Dell sells PCs, Laptops, electronics and innovative technology and services to businesses and consumers
www.**dell**.com/content/topics/reftopic.aspx/bsd/odg/13263_search_generic_hsb?c=us&cs=&l=... · Cached page

Dell: Information from Answers.com
Dell moved aggressively into markets outside of the United States, including Latin America, where Xerox began to sell **Dell computers** in 1992. By 1993, 36 percent of **Dell's** sales ...
www.answers.com/topic/**dell**-technology · Cached page

Shop for **dell computers**

Sponsored sites

dell computers
Low prices on latest **Dell Computer** products. Compare models & prices.
www.PriceGrabber.com/Computers

Dell Computers
Enjoy Savings & Selection on **Dell Computers**.
http://www.Shopzilla.com

Dell Desktop Savings
Staples® Official Site - Shop For Desktop **Computers** and Peripherals.
www.Staples.com

Find **Computer** Hardware
Local **Computer** Parts & Retailers - PCs, Macs, Desktops, Laptops.
yellowpages.com

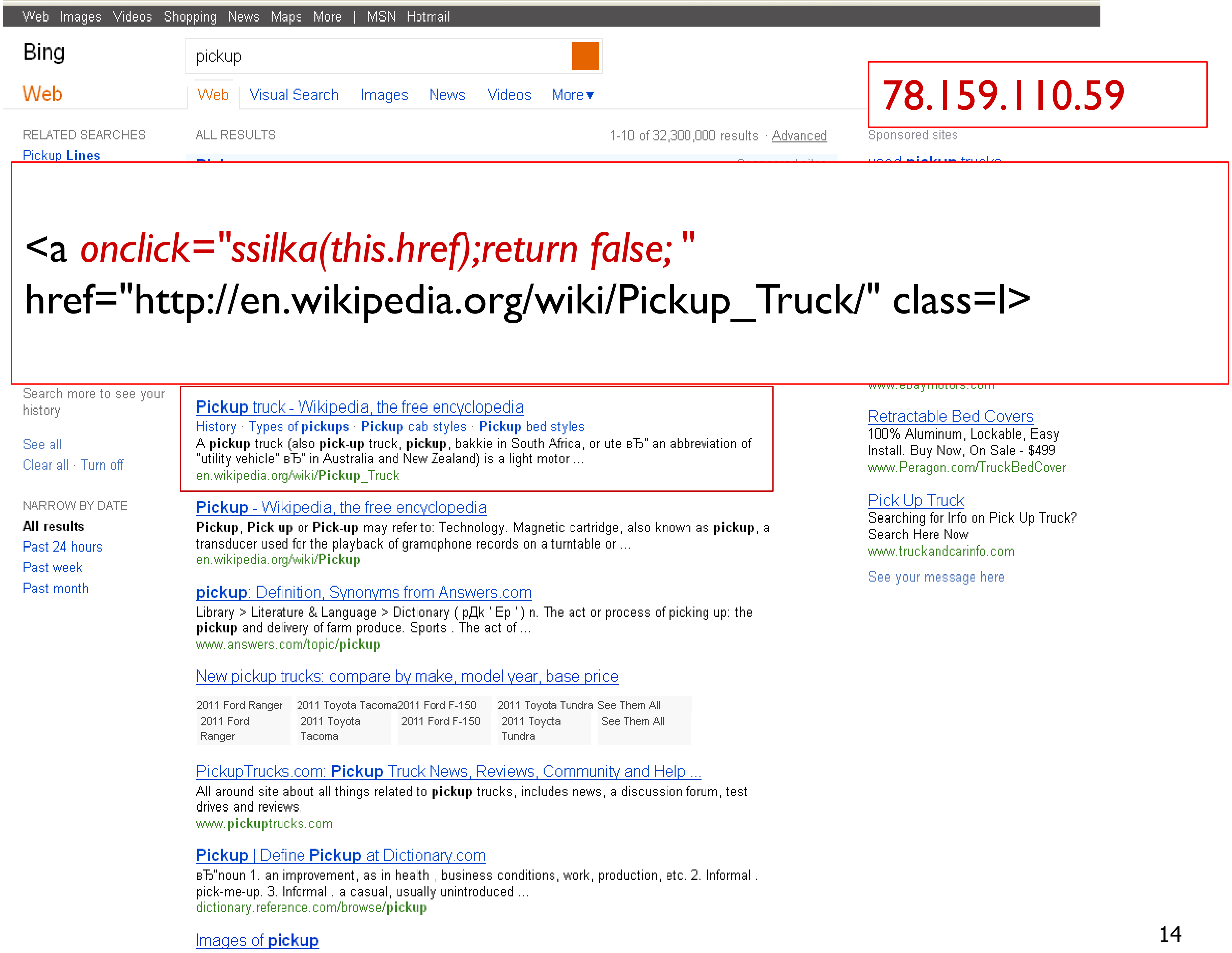
Laptop Sold For $40.32
Win Laptops for Great Prices! Try Our No-Risk Auctions. Register Free
BigDeal.com/Laptops

See your message here

http://www.bing.com/aff?p=JZK3sqNIAABjfcgL4eFmgKva2oIBASuL8CSqwXskvPj6WxN1Z510MU2v_76_aZ4jaZYnae43BeY7bsq4Jl_F6-dfS_CEf-TZievnL0bG1knnHZSdtPk6XQY_Mr-Yo-w3yUt...

Types of Modifications

- Modify search result links
- Modify advertisements links
- *Insert JavaScript*
- Redirect requests



78.159.110.59

```
<a onclick="ssilka(this.href);return false; " href="http://en.wikipedia.org/wiki/Pickup_Truck/" class=l>
```

Pickup truck - Wikipedia, the free encyclopedia
History · Types of pickups · Pickup cab styles · Pickup bed styles
A pickup truck (also pick-up truck, pickup, bakkie in South Africa, or ute вЂ" an abbreviation of "utility vehicle" вЂ" in Australia and New Zealand) is a light motor ...
en.wikipedia.org/wiki/Pickup_Truck

Pickup - Wikipedia, the free encyclopedia
Pickup, Pick up or Pick-up may refer to: Technology. Magnetic cartridge, also known as pickup, a transducer used for the playback of gramophone records on a turntable or ...
en.wikipedia.org/wiki/Pickup

pickup: Definition, Synonyms from Answers.com
Library > Literature & Language > Dictionary (рДk ' Ep ') n. The act or process of picking up: the pickup and delivery of farm produce. Sports . The act of ...
www.answers.com/topic/pickup

New pickup trucks: compare by make, model year, base price

2011 Ford Ranger	2011 Toyota Tacoma	2011 Ford F-150	2011 Toyota Tundra	See Them All
2011 Ford Ranger	2011 Toyota Tacoma	2011 Ford F-150	2011 Toyota Tundra	See Them All

PickupTrucks.com: Pickup Truck News, Reviews, Community and Help ...
All around site about all things related to pickup trucks, includes news, a discussion forum, test drives and reviews.
www.pickuptrucks.com

Pickup | Define Pickup at Dictionary.com
вЂ"noun 1. an improvement, as in health , business conditions, work, production, etc. 2. Informal . pick-me-up. 3. Informal . a casual, usually unintroduced ...
dictionary.reference.com/browse/pickup

Images of pickup

www.ebaymotors.com

Retractable Bed Covers
100% Aluminum, Lockable, Easy Install. Buy Now, On Sale - $499
www.Peragon.com/TruckBedCover

Pick Up Truck
Searching for Info on Pick Up Truck? Search Here Now
www.truckandcarinfo.com

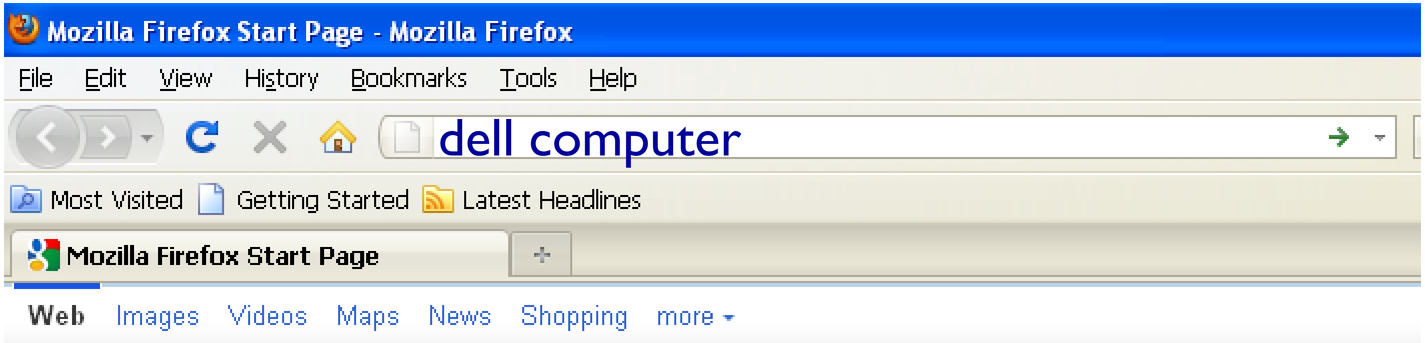
See your message here

Types of Modifications

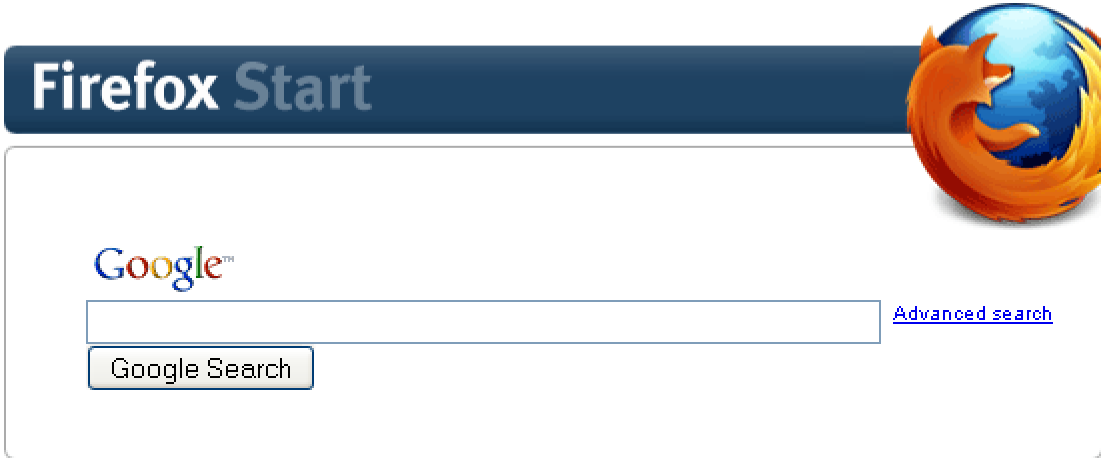
- Modify search result links
- Modify advertisements links
- Insert JavaScript
- *Redirect requests*

Redirect Requests

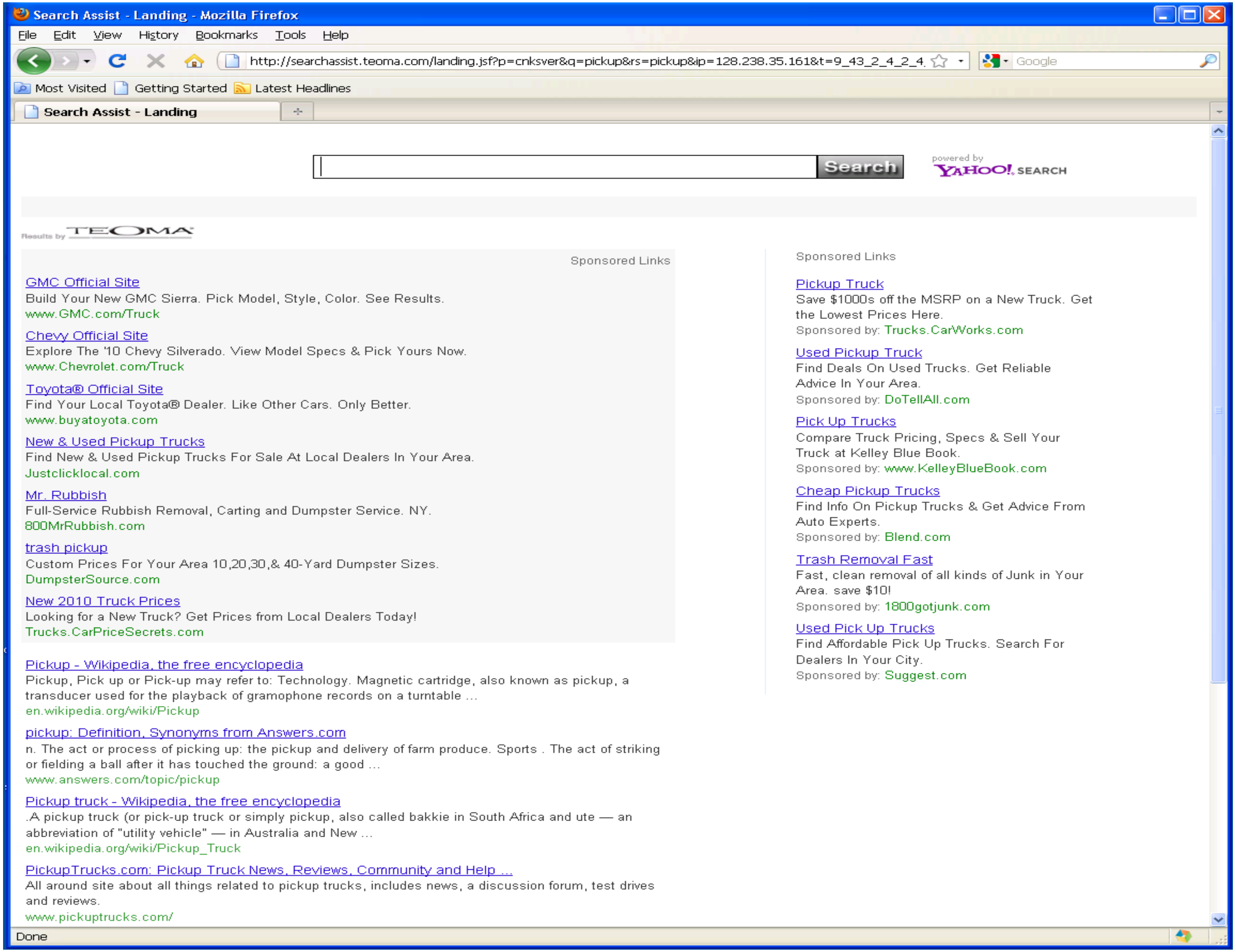
- Redirect search requests originating from *Address Bar*



dell computer



Redirect to a Different Search Engine



Sponsored Links

[GMC Official Site](#)
Build Your New GMC Sierra. Pick Model, Style, Color. See Results.
www.GMC.com/Truck

[Chevy Official Site](#)
Explore The '10 Chevy Silverado. View Model Specs & Pick Yours Now.
www.Chevrolet.com/Truck

[Toyota® Official Site](#)
Find Your Local Toyota® Dealer. Like Other Cars. Only Better.
www.buyatoyota.com

[New & Used Pickup Trucks](#)
Find New & Used Pickup Trucks For Sale At Local Dealers In Your Area.
Justclicklocal.com

[Mr. Rubbish](#)
Full-Service Rubbish Removal, Carting and Dumpster Service. NY.
800MrRubbish.com

[trash pickup](#)
Custom Prices For Your Area 10,20,30,& 40-Yard Dumpster Sizes.
DumpsterSource.com

[New 2010 Truck Prices](#)
Looking for a New Truck? Get Prices from Local Dealers Today!
Trucks.CarPriceSecrets.com

[Pickup - Wikipedia, the free encyclopedia](#)
Pickup, Pick up or Pick-up may refer to: Technology. Magnetic cartridge, also known as pickup, a transducer used for the playback of gramophone records on a turntable ...
en.wikipedia.org/wiki/Pickup

[pickup: Definition, Synonyms from Answers.com](#)
n. The act or process of picking up: the pickup and delivery of farm produce. Sports . The act of striking or fielding a ball after it has touched the ground: a good ...
www.answers.com/topic/pickup

[Pickup truck - Wikipedia, the free encyclopedia](#)
.A pickup truck (or pick-up truck or simply pickup, also called bakkie in South Africa and ute — an abbreviation of "utility vehicle" — in Australia and New ...
en.wikipedia.org/wiki/Pickup_Truck

[PickupTrucks.com: Pickup Truck News, Reviews, Community and Help ...](#)
All around site about all things related to pickup trucks, includes news, a discussion forum, test drives and reviews.
www.pickuptrucks.com/

Sponsored Links

[Pickup Truck](#)
Save $1000s off the MSRP on a New Truck. Get the Lowest Prices Here.
Sponsored by: Trucks.CarWorks.com

[Used Pickup Truck](#)
Find Deals On Used Trucks. Get Reliable Advice In Your Area.
Sponsored by: DoTellAll.com

[Pick Up Trucks](#)
Compare Truck Pricing, Specs & Sell Your Truck at Kelley Blue Book.
Sponsored by: www.KelleyBlueBook.com

[Cheap Pickup Trucks](#)
Find Info On Pickup Trucks & Get Advice From Auto Experts.
Sponsored by: Blend.com

[Trash Removal Fast](#)
Fast, clean removal of all kinds of Junk in Your Area. save $10!
Sponsored by: 1800gotjunk.com

[Used Pick Up Trucks](#)
Find Affordable Pick Up Trucks. Search For Dealers In Your City.
Sponsored by: Suggest.com

Redirect Requests

- Two types of redirection
  - Redirect to a different search engine
  - *Insert additional rounds of redirection*

Normal	With Modification
www.google.com/search?ie=UTF-8****	www.google.com/search?ie=UTF-8***
www.dell.com	wwww13.notfoundhelp.net/search?***
	www.kqzyfj.com/click****
	www.apmebf.com/7j115uoxwE***
	www.emjcd.com/ep122dlutD/****
	altfarm.mediaplex.com/ad/ck/*****
	lt.dell.com/lt/lt.aspx?CID=4350***

Online ad companies

Scale of Rogue Servers

- Total # of rogue servers: 349

Type	# of Servers
Modify search result links	41
Modify ad links	80
JavaScript injection	72
Redirect requests from address bar	154

- 15M unique clients worldwide
  - 1% were directed to malicious servers
  - *2% clients from US are affected*

Identifying the Inflight Modification :Summary

- Collect thousands of proxies from wild
- Develop a framework to determine whether a proxy modify content
- Find 4 types of modifications
- 2% clients from US are affected

Outline

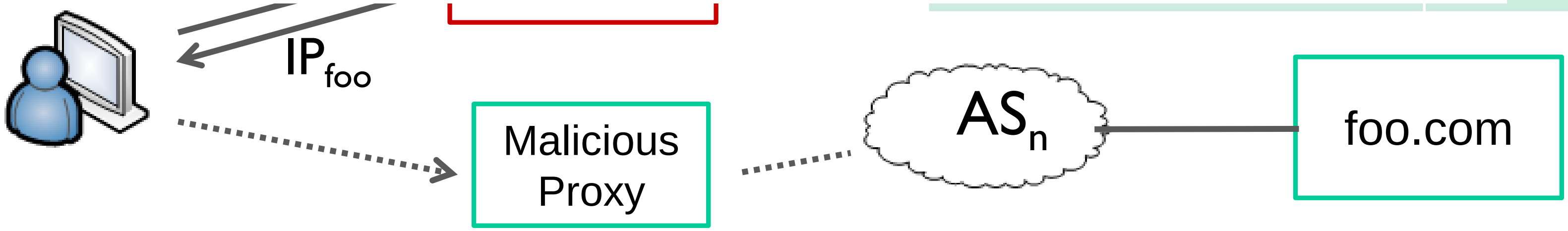
- Identifying the Inflight Modification
- *Digging the Root Causes*
- Summary

Narrow Down Horizon

- Active probing the malicious web servers
- Only accept a few domains
- Clients only connect to malicious servers when accessing particular sites

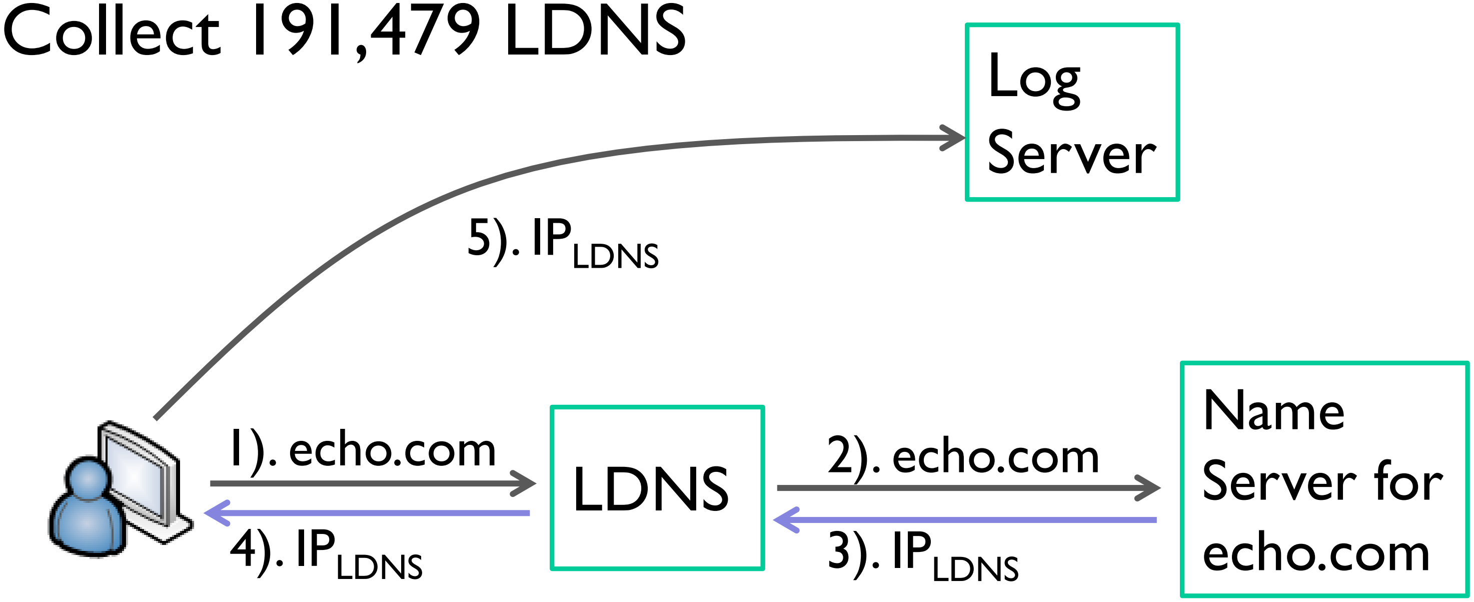
Web Service	Accept
Bing.com	✓
Google.com	✓
Search.yahoo.com	✓
Youtube.com	✗
Facebook.com	✗
Akamai.com	✗
limelightnetworks.com	✗
	✗
	✗

Q: DNS Resolution is Compromised?



Collect LDNS

- Create echo.com
- Name server for echo.com returns source IP of DNS query
- Collect 191,479 LDNS

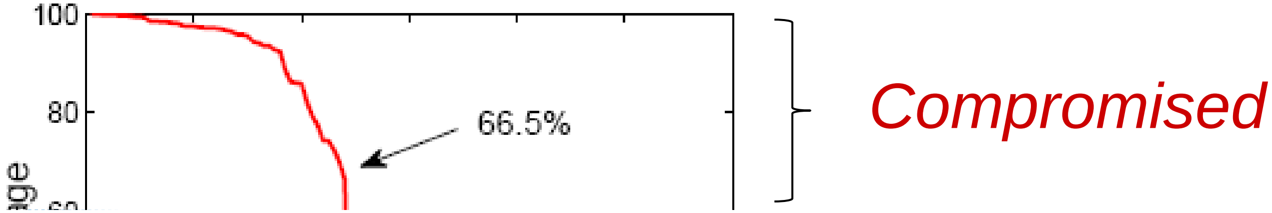


LDNS Analysis

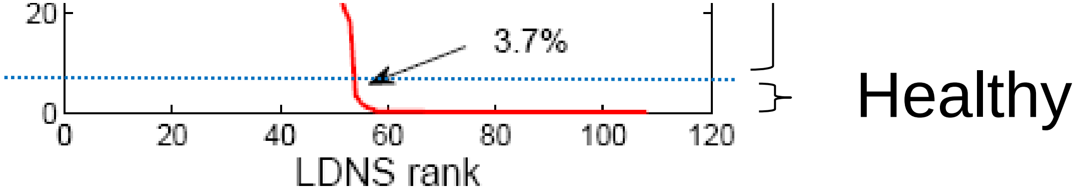
- *Which LDNS are compromised?*
- Who is behind?
- Does LDNS discriminate among users?
- Does public DNS help?

Which LDNS are compromised?

- Group by /24 prefix, remove ones with clients < 50
- Get 108 LDNS prefixes
- Aggregate all clients that use the same LDNS
- Calculate the percentage of affected clients
- *48 out of 108 LDNS are compromised*



Q: Who operates these LDNS?



Who is Behind?

- Not all LDNS are deployed by ISPs
- Define: *an LDNS deployed by ISP if more than 50% clients using it from the same ISP.*
- *44 / 48 compromised LDNS are official.*

ISP	# of cmpmzd LDNS	affected clients (%)
Hughes Network Systems	14	95.5
Frontier Communications	13	92.7
Cavalier Telephone	7	87.0
FiberNet of West Virginia	1	70.3
Spacenet, Inc.	1	97.8
Onvoy	3	76.1
WideOpenWest	3	68.6
		92.6
		88.5

A small # of ISPs operate these LDNS!

Do the LDNS Discriminate among Users?

- Will clients from other ISPs be affected if they use those compromised LDNS?

ISP	affected external clients (%)
Hughes Network Systems	82.0
Frontier Communications	97.9
Cavalier Telephone	84.7
FiberNet of West Virginia	---
Spacenet, Inc.	---
Onvoy	69.7

Compromised LDNS servers indiscriminately redirect all clients to the malicious servers!

Are clients forced to connect to malicious servers?

- In other words, will public DNS work in these ISP?

ISP	Ratio of affected external clients
Hughes Network Systems	0.2
Frontier Communications	0.1
Cavalier Telephone	0.0
FiberNet of West Virginia	0.0
Spacenet, Inc.	0.0
Onvoy	1.2
WideOpenWest	0.0

Using Public DNS Improves Service Availability!

Summary

- Find four types of modifications
  - Insert abnormal redirection in HTTP request
- Inflight modification is popular
  - Nearly 2% clients from U.S. are affected
- Most of affected clients are from 9 small-to-medium size ISPs
  - Some LDNS in ISPs direct clients to rogue servers
- Public DNS would help bypass modification