Here's looking at you...

Geoff Huston

The Theory

- We use Google Ads to deliver a test script to a very large profile of users
  - We measure the DNS, DNSSEC, IPv6, performance, and many other aspects of the end user's view of the Internet
  - We have some 500,000 ads delivered per day
  - And each of them use uniquely generated URLs
  - So, in theory we should see each unique URL retrieved once
  - Right?

Here is what we see in the web logs…

```
[22/Jan/2014:00:10:21 +0000]
   120.194.53.xxx
   "GET /1x1.png?
   t10000.u3697062917.s1390349413.i333.v1794.rd.td
[22/Jan/2014:00:11:29 +0000]
   221.176.4.xxx
   "GET /1x1.png?
   t10000.u3697062917.s1390349413.i333.v1794.rd.td
```

68 seconds later:

-- SAME URL

-- 120.194.53.xxx – Origin AS = 24445

-- 221.176.4.xxx – Origin AS = 9808

How widespread is this?

48 days in 2013:

- 29,171,864 unique URLS presented to end users
- 612,089 of these URLS were re-presented to us from a different client IP address

That's 2.1% of URLs fetches that seem to have attracted a digital stalker!

The Top Repeaters

Rank	IP Address	Count	AS	AS Name
1	119.147.146.xxx	11,241	4134	CHINANET-BACKBONE No.31,Jin-rong Street CN
2	182.18.208.xxx	1,0982	23944	SKYBB-AS-AP AS-SKYBroadband SKYCable Corporation PH
3	182.18.209.xxx	5,046	23944	SKYBB-AS-AP AS-SKYBroadband SKYCable Corporation PH
4	124.6.181.xxx	5,046	4775	GLOBE-TELECOM-AS Globe Telecoms PH
5	112.198.64.xxx	4,641	4775	GLOBE-TELECOM-AS Globe Telecoms PH
6	203.177.74.xxx	3,315	4775	GLOBE-TELECOM-AS Globe Telecoms PH
7	120.28.64.xxx	3,230	4775	GLOBE-TELECOM-AS Globe Telecoms PH
8	211.125.138.xxx	3,098	9619	SSD Sony Global Solutions Inc. JP
9	210.94.41.xxx	1,414	6619	SAMSUNGSDS-AS-KR SamsungSDS Inc. KR
10	222.127.223.xxx	1,269	4775	GLOBE-TELECOM-AS Globe Telecoms PH
11	210.143.35.xxx	1,177	2516	KDDI KDDI CORPORATION JP
12	202.156.10.xxx	1,154	10091	SCV-AS-AP StarHub Cable Vision Ltd SG
13	14.1.193.xxx	1,128	45960	YTLCOMMS-AS-AP YTL COMMUNICATIONS SDN BHD MY
14	183.90.103.xxx	1,069	55430	STARHUBINTERNET-AS-NGNBN Starhub Internet Pte Ltd SG
15	202.246.252.xxx	995	2526	HITNET HITACHI,Ltd. Information Technology Division. JP
16	192.51.44.xxx	887	2510	INFOWEB FUJITSU LIMITED JP
17	183.90.41.xxx	774	55430	STARHUBINTERNET-AS-NGNBN Starhub Internet Pte Ltd SG
18	110.34.0.xxx	704	4007	Subisu Cablenet (Pvt) Ltd, Baluwatar, Kathmandu, Nepal NP
19	110.232.92.xxx	638	23679	NUSANET-AS-ID Media Antar Nusa PT. ID
20	37.19.108.xxx	603	44143	VIPMOBILE-AS Vip mobile d.o.o. RS
21	24.186.96.xxx	573	6128	CABLE-NET-1 - Cablevision Systems Corp. US
22	161.53.179.xxx	535	2108	CARNET-AS Croatian Academic and Research Network HR
23	193.254.230.xxx	534	25304	UNITBV Universitatea TRANSILVANIA Brasov RO
24	121.54.54.xxx	500	10139	SMARTBRO-PH-AP Smart Broadband, Inc. PH
25	77.244.114.xxx	484	42779	AZERFON Azerfon AS AZ

Web Proxies?

- A strong indicator of a proxy device is that it is located in the same AS as the end client.
- So lets filter that list and look at those repeaters that use a different AS from the original request
- And here's what we see

Different Origin AS Repeaters

Rank	IP Address	Count	AS	AS Name
1	119.147.146.xxx	8,886	4134	CHINANET-BACKBONE No.31,Jin-rong Street CN
2	220.181.158.xxx	493	23724	CHINANET-IDC-BJ IDC, China Telecommunications Corporation CN
3	123.125.161.xxx	446	4808	CHINA169-BJ CNCGROUP IP China169 Beijing Province Network CN
4	210.133.104.xxx	285	7677	DNP Dai Nippon Printing Co., Ltd JP
5	202.214.150.xxx	266	2497	IIJ Internet Initiative Japan Inc. JP
6	112.65.211.xxx	248	17621	CNCGROUP-SH China Unicom Shanghai network CN
7	221.176.4.xxx	226	9808	CMNET-GD Guangdong Mobile Communication Co.Ltd. CN
8	62.84.94.xxx	204	16130	FiberLink Networks LB
9	212.40.141.xxx	203	31126	SODETEL-AS SODETEL SAL LB
10	101.69.163.xxx	163	4837	CHINA169-BACKBONE CNCGROUP China169 Backbone CN
11	59.162.23.xxx	158	4755	TATACOMM-AS TATA Communications IN
12	8.35.201.xxx	156	15169	GOOGLE - Google Inc. US
13	118.186.36.xxx	149	23724	CHINANET-IDC-BJ IDC, China Telecommunications Corporation CN
14	190.96.112.xxx	147	262150	Empresa Provincial de Energia de Cordoba AR
15	202.155.113.xxx	143	4795	INDOSATM2-ID INDOSATM2 ASN ID
16	118.228.151.xxx	142	4538	ERX-CERNET-BKB China Education and Research Network Center CN
17	123.125.73.xxx	136	4808	CHINA169-BJ CNCGROUP IP China169 Beijing Province Network CN
18	69.41.14.xxx	133	47018	CE-BGPAC - Covenant Eyes, Inc. US
19	118.97.198.xxx	131	17974	TELKOMNET-AS2-AP PT Telekomunikasi Indonesia ID
20	112.215.11.xxx	128	17885	JKTXLNET-AS-AP PT Excelcomindo Pratama ID
21	122.2.0.xxx	125	9299	IPG-AS-AP Philippine Long Distance Telephone Company PH
22	176.28.78.xxx	123	197893	ELSUHD-AS Elsuhd Net Ltd. Communications and Computer Services IQ
23	14.139.97.xxx	120	55824	RSMANI-NKN-AS-AP National Knowledge Network IN
24	211.155.120.xxx	116	23724	CHINANET-IDC-BJ IDC, China Telecommunications Corporation CN
25	121.96.61.xxx	114	6648	BAYAN Bayan Telecommunications, Inc. PH

Maybe its National Infrastructure

- We've all heard about the Great Firewall of China
- And other countries may be doing similar things
- So perhaps these repeaters are the result of some form of national / regional content cache program
- So lets filter this further by using geolocate information to find those cases where the original end client and the digital stalker locate to different countries

Different Country Stalkers

Rank	IP Address	Count	AS	AS Name
1	119.147.146.xxx	7,001	4134	CHINANET-BACKBONE No.31,Jin-rong Street CN
2	8.35.201.xxx	156	15169	GOOGLE - Google Inc. US
3	190.216.130.xxx	84	3549	GBLX Global Crossing Ltd. AR
4	190.27.253.xxx	82	19429	ETB - Colombia CO
5	61.92.16.xxx	62	9269	HKBN-AS-AP Hong Kong Broadband Network Ltd. HK
6	208.80.194.xxx	53	13448	WEBSENSE Websense, Inc. US
7	112.140.187.xxx	33	45634	SPARKSTATION-SG-AP 10 Science Park Road SG
8	69.41.14.xxx	32	47018	CE-BGPAC - Covenant Eyes, Inc. US
9	126.117.225.xxx	31	17676	GIGAINFRA Softbank BB Corp. JP
10	113.43.175.xxx	29	17506	UCOM UCOM Corp. JP
11	202.249.25.xxx	26	4717	AI3 WIDE Project JP
12	139.193.204.xxx	25	23700	BM-AS-ID PT. Broadband Multimedia, Tbk ID
13	180.13.45.xxx	22	4713	OCN NTT Communications Corporation JP
14	201.221.124.xxx	21	27989	BANCOLOMBIA S.A CO
15	123.125.161.xxx	21	4808	CHINA169-BJ CNCGROUP China169 Beijing Province Network CN
16	220.181.158.xxx	17	23724	CHINANET-IDC-BJ IDC, China Telecommunications Corporation CN
17	208.184.77.xxx	17	6461	MFNX MFN - Metromedia Fiber Network US
18	183.179.254.xxx	16	9269	HKBN-AS-AP Hong Kong Broadband Network Ltd. HK
19	203.192.154.xxx	16	10026	PACNET Pacnet Global Ltd JP
20	139.193.223.xxx	13	23700	BM-AS-ID PT. Broadband Multimedia, Tbk ID
21	175.134.140.xxx	12	2516	KDDI KDDI CORPORATION JP
22	210.187.58.xxx	12	4788	TMNET-AS-AP TM Net, Internet Service Provider MY
23	195.93.102.xxx	12	1668	AOL-ATDN - AOL Transit Data Network GB
24	221.82.58.xxx	12	17676	GIGAINFRA Softbank BB Corp. JP
25	167.205.22.xxx	12	4796	BANDUNG-NET-AS-AP Institute of Technology Bandung ID

Different Country Stalkers

Rank	IP Address	Count	AS	AS Name
1	119.147.146.xxx	7,001	4134	CHINANET-BACKBONE No.31,Jin-rong Street CN
2	8.35.201.xxx	156	15169	GOOGLE - Google Inc. US
3	190.216.130.xxx	84	3549	GBLX Global Crossing Ltd. AR
4	190.27.253.xxx	82	19429	ETB - Colombia CO
5	61.92.16.xxx	62	9269	HKBN-AS-AP Hong Kong Broadband Network Ltd. HK
6	208.80.194.xxx	53	13448	WEBSENSE Websense, Inc. US
7	112.140.187.xxx	33	45634	SPARKSTATION-SG-AP 10 Science Park Road SG
8	69.41.14.xxx	32	47018	CE-BGPAC - Covenant Eyes, Inc. US
9	126.117.225.xxx	31	17676	GIGAINFRA Softbank BB Corp. JP
10	113.43.175.xxx	29	17506	UCOM UCOM Corp. JP

WIKIPEDIA
The Free Encyclopedia

Create account Log in

Article Talk Read Edit View history Search

Smoking gun

From Wikipedia, the free encyclopedia

For other uses, see Smoking Gun.

The term "**smoking gun**" was originally, and is still primarily, a reference to an object or fact that serves as conclusive evidence of a crime or similar act. In addition to this, its meaning has evolved in uses completely unrelated to criminal activity: for example, scientific evidence that is highly suggestive in favor of a particular hypothesis is sometimes called smoking gun evidence. Its name originally came from the idea of finding a smoking (i.e., very recently fired) gun on the person of a suspect wanted for shooting someone, which in that situation would be nearly unshakable proof of having committed the crime. A piece of evidence that falls just short of being conclusive is sometimes referred to as a "smoldering gun."

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia

Lets zoom in for a second

And look at the distribution of the clients who were stalked by 119.147.146.xxx

Which countries were the clients located?

Rank	Count	Country
AE	27	United Arab Emirates
AG	2	Antigua and Barbuda
AL	32	Albania
AM	13	Armenia
AR	19	Argentina
AT	5	Austria
AU	21	Australia
AW	6	Aruba
AZ	8	Azerbaijan
BA	27	Bosnia and Herzegovina
BD	1	Bangladesh
BE	10	Belgium
BG	45	Bulgaria
BN	1	Brunei Darussalam
BO	1	Bolivia
BR	44	Brazil
BS	1	Bahamas
BY	7	Belarus
BZ	4	Belize
CA	125	Canada
CL	13	Chile
CN	4,622	China
CO	11	Colombia
CR	1	Costa Rica
CW	2	Curaçao
CY	1	Cyprus
CZ	37	Czech Republic
DE	21	Germany
DO	2	Dominican Republic
DZ	19	Algeria
EC	8	Ecuador
EG	22	Egypt
ES	38	Spain
FR	68	France
GB	45	United Kingdom
GE	12	Georgia
GR	25	Greece
GY	1	Guyana
HK	721	Hong Kong
HN	1	Honduras
HR	9	Croatia
HU	67	Hungary
ID	159	Indonesia
IE	16	Ireland
IL	8	Israel
IN	32	India
IQ	21	Iraq
IT	52	Italy
JM	5	Jamaica
JO	2	Jordan
JP	2,910	Japan
KE	1	Kenya
KG	1	Kyrgyzstan
KH	28	Cambodia
KR	27	Republic of Korea
KW	1	Kuwait
KZ	11	Kazakhstan
LA	6	Laos
LK	11	Sri Lanka
LT	12	Lithuania
LV	6	Latvia
MA	6	Morocco
MD	2	Republic of Moldova
ME	7	Montenegro
MK	69	Macedonia
MM	2	Myanmar
MN	36	Mongolia
MO	37	Macao
MP	4	Northern Mariana Islands
MT	4	Malta
MU	7	Mauritius
MX	107	Mexico
MY	375	Malaysia
NC	1	New Caledonia
NI	1	Nicaragua
NL	15	Netherlands
NO	8	Norway
NP	1	Nepal
NZ	20	New Zealand
OM	1	Oman
PA	11	Panama
PE	29	Peru
PH	166	Philippines
PK	1	Pakistan
PL	340	Poland
PR	7	Puerto Rico
PS	9	Occupied Palestinian Territory
PT	1	Portugal
RO	197	Romania
RS	62	Serbia
RU	32	Russian Federation
RW	1	Rwanda
SA	24	Saudi Arabia
SE	3	Sweden
SG	83	Singapore
SI	13	Slovenia
SK	13	Slovakia
SR	2	Suriname

SV	3	El Salvador
TH	138	Thailand
TN	3	Tunisia
TR	57	Turkey
TW	1,241	Taiwan
UA	37	Ukraine
US	371	United States of America
UZ	1	Uzbekistan
VC	1	Saint Vincent and the Grenadines
VE	16	Venezuela
VN	249	Vietnam
YE	1	Yemen

What the…?

- That's an impressive list of countries!
- And our collection of 30 million URLs across 49 days is a mere drop in the ocean of web fetches on the Internet
- So are we glimpsing here the tip of some much larger program of URL stalking?

Accident? Deliberate? Something Else?

- Why go to all the trouble to collect URLs but use the same IP address to perform the followup stalking?
- Is this some kind of deliberate leakage from a middleware device?
- Or the result of some kind of a virus?
- Or the outcome of TOR + virus?
- Or a smart, but at the same time remarkably dumb, digital stalking program?
- Or <*insert your favourite conspiracy theory here*>