Street Art: Banksy

The Theory

- At APNIC we measurement aspects of technology deployment by using Google Ads to deliver a test script to a very large profile of users
  - We measure penetration of DNSSEC and IPv6, and many other aspects of the end user's view of the Internet through these scripts
  - We have some 500,000 tests executed per day
  - And each of them use uniquely generated URLs
  - And the URLs direct the end user back to our servers
  - So, in theory we should see each unique URL retrieved exactly once

The Theory

- At APNIC we measurement aspects of technology deployment by using Google Ads to deliver a test script to a very large profile of users
  - We measure penetration of DNSSEC and IPv6, and many other aspects of the end user's view of the Internet through these scripts
  - We have some 500,000 tests executed per day
  - And each of them use uniquely generated URLs
  - And the URLs direct the end user back to our servers
  - So, in theory we should see each unique URL retrieved exactly once

Right?

Here's what we see at times 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
```

Here's what we see at times 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
```

10:21 120.194.53.xxx – Origin AS = 24445

CMNET-V4HENAN-AS-AP Henan Mobile Communications Co.,Ltd

Here's what we see at times 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
```

Here's what we see at times 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
```

10:21 120.194.53.xxx – Origin AS = 24445

CMNET-V4HENAN-AS-AP Henan Mobile Communications Co.,Ltd

68 seconds later -- SAME URL, different IP!

11:29 221.176.4.xxx – Origin AS = 9808

CMNET-GD Guangdong Mobile Communication Co.Ltd.

Searching for Stalkers

We've combed over our collected data since the start of 2014 to see what evidence we can gather about URL stalking…

Some Numbers

In the first 149 days of 2014 we saw:

- 61,576,774 unique end-user IP addresses presented to our servers from these test scripts
- 110,684 of these end-user IP addresses presented HTTP GET strings to us that were subsequently presented to us from a different client IP address!

That's some 1 in 500* users that seem to have attracted some kind of digital stalker!

* Or maybe a bit more, due to NATs hiding multiple end users behind a single public IP address

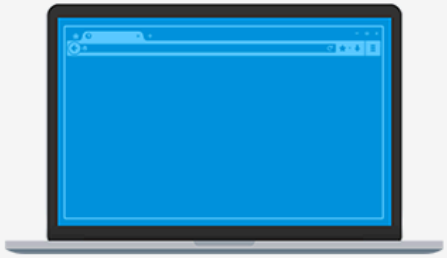
mozilla

Take the tour to see what's new »

Committed to you, your privacy and an open Web

Keep your Firefox in Sync

Access your bookmarks, passwords and more from any device.



Get started with Sync

Create an account from the menu panel

Privacy? Really?

It's hard to believe that today's Internet respects personal privacy when it seems that around 1 in 500 users have attracted some kind of digital stalker who is tracking the URLs they visit.

Stalking Rates by Country

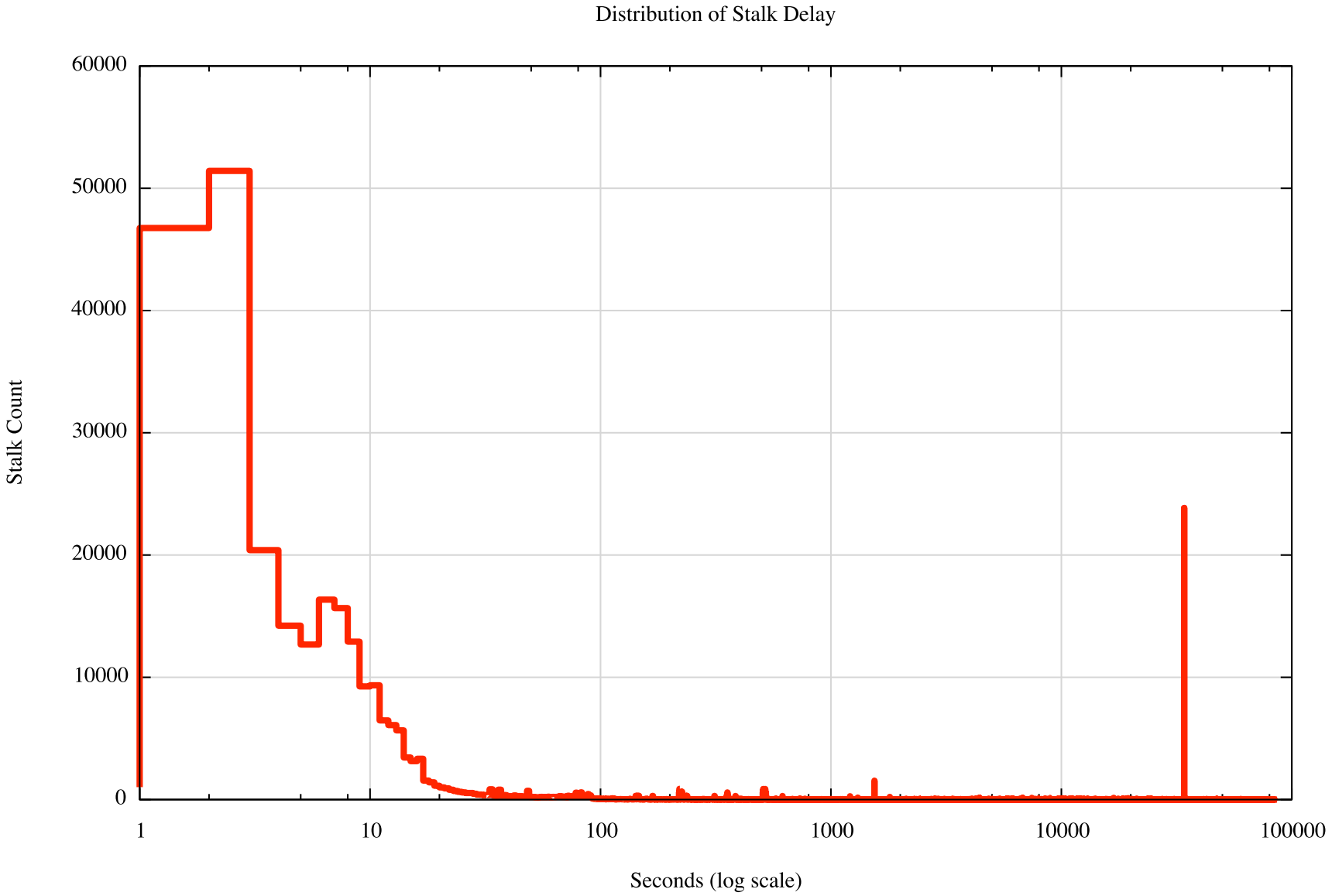
CC	Samples	Stalked	Rate/100,000	Country
LA	7,905	245	3,099	Lao People's Democratic Republic
MO	12,382	315	2,544	Macao Special Administrative Region of China
CN	3,409,338	49,552	1,453	China
HK	161,586	2,110	1,306	Hong Kong Special Administrative Region of China
MP	2,642	34	1,287	Northern Mariana Islands
VU	1,866	21	1,125	Vanuatu
GQ	488	5	1,025	Equatorial Guinea
GL	306	3	980	Greenland
ST	215	2	930	Sao Tome and Principe
JP	644,620	4,797	744	Japan
TW	507,789	3,714	731	Taiwan
AL	157,154	823	524	Albania
US	3,596,202	17,096	475	United States of America
MY	623,434	2,232	358	Malaysia
SG	1,334,252	4,562	342	Singapore
MK	156,424	480	307	The former Yugoslav Republic of Macedonia
CA	537,928	1,441	268	Canada
KH	56,676	137	242	Cambodia
ME	70,407	168	239	Montenegro
TG	1,268	3	237	Togo
SR	16,719	38	227	Suriname
GB	3,181,253	6,696	210	United Kingdom of Great Britain and Northern Ireland
PM	495	1	202	Saint Pierre and Miquelon
IR	21,519	39	181	Iran (Islamic Republic of)
MM	13,482	24	178	Myanmar
FJ	6,472	10	155	Fiji
IQ	215,083	322	150	Iraq
LR	710	1	141	Liberia
BJ	1,492	2	134	Benin
MN	29,906	39	130	Mongolia

The top 30 countries in terms of observed URL stalking rates

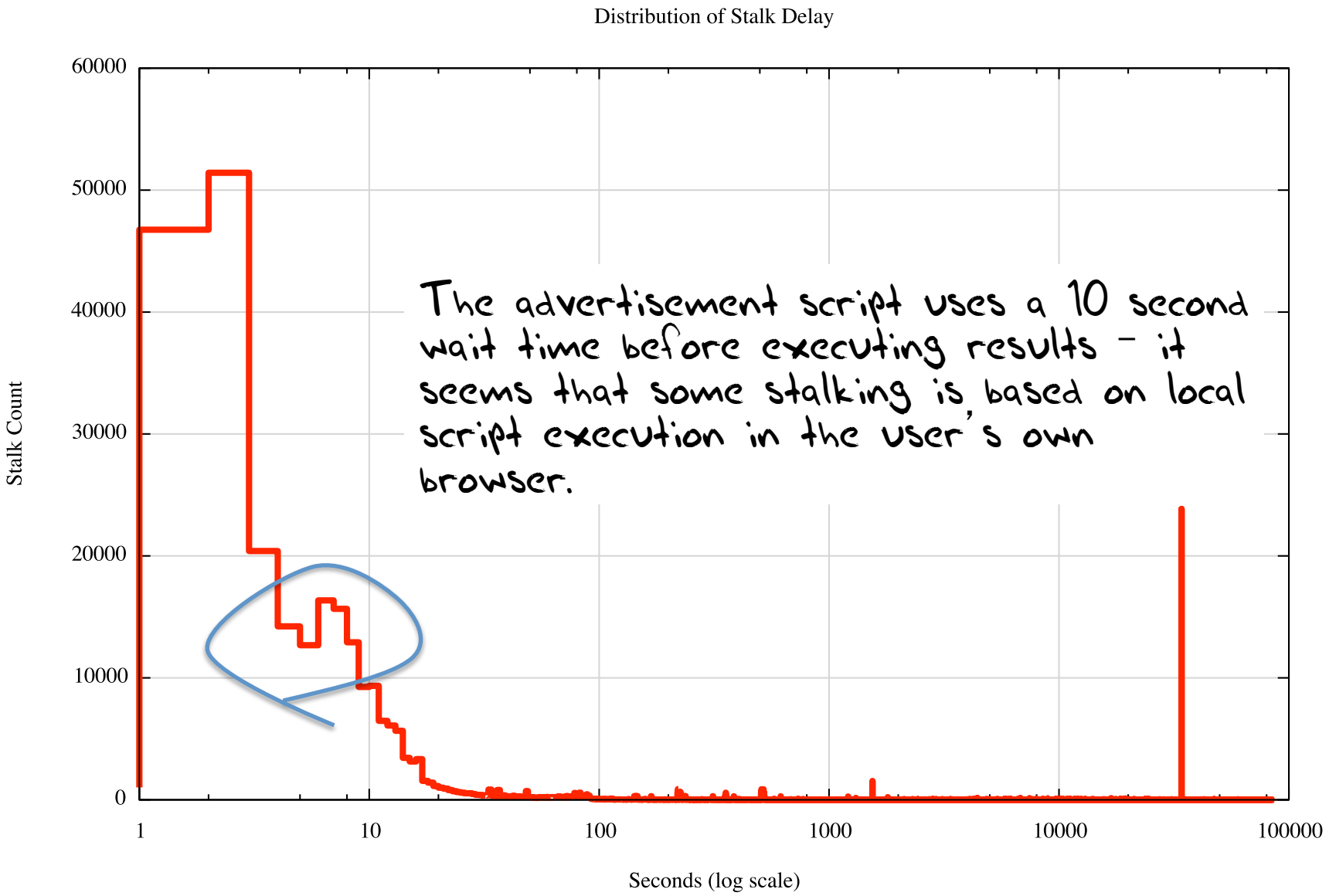
Counting Stalkers

- 213,657,379 unique URLs were presented back to us in this experiment, and we saw some 378,775 URLS that were presented to us more than once, from different source IP addresses
- The subsequent presentations came from 1,579 distinct source networks (/24s)

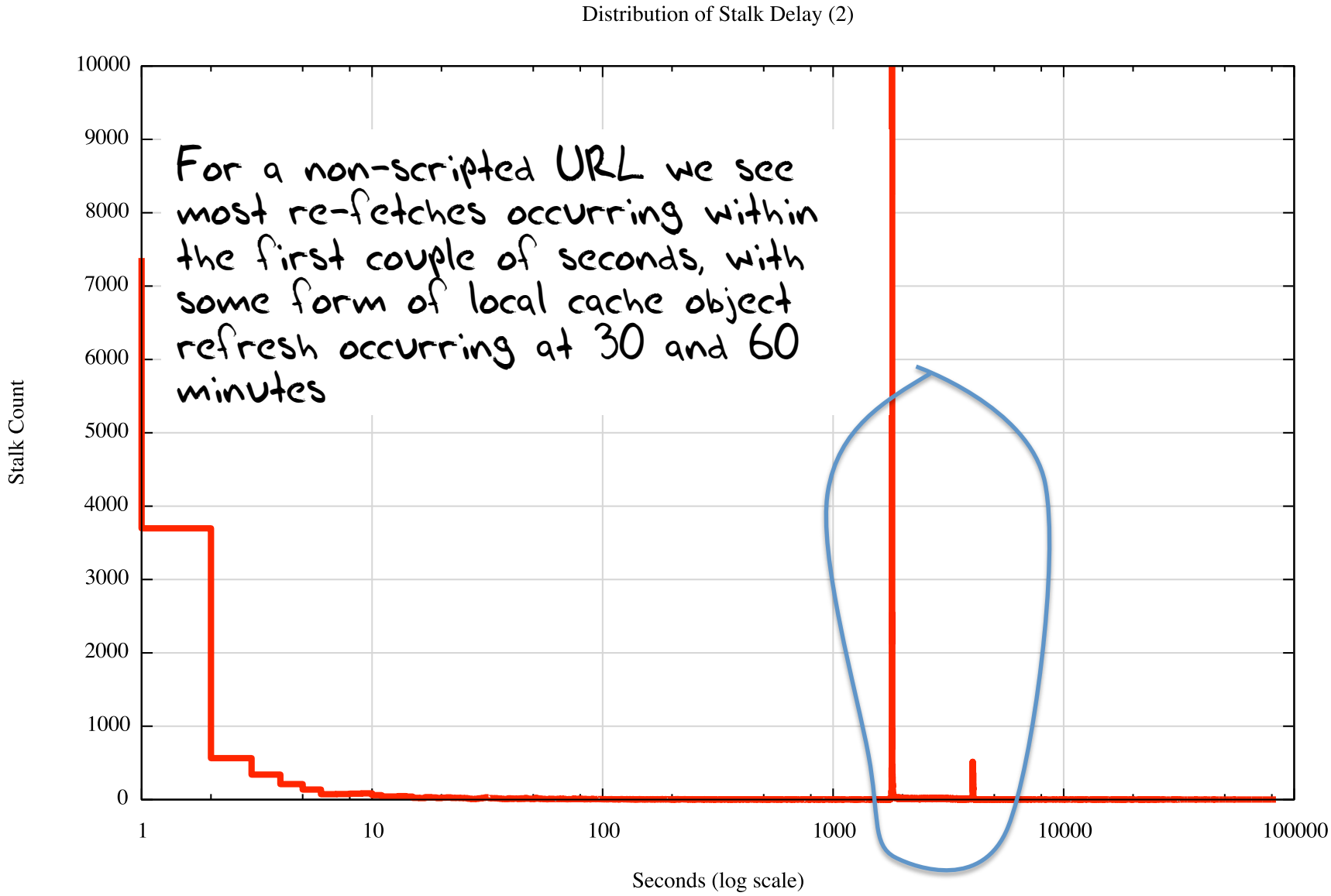
Stalking Delay



Stalking Delay



Stalking Delay (2)



Is it me … or you?

The first result leads to the view that there is some amount of local scriptware on users' browsers that feeds visited URL streams to a third party

The second result indicates that there is some amount of intercepting middleware that feeds proxy caches, with automatic refresh cycles

Top Stalkers

Rank	IP Net	Count	AVG Delay	AS	Description
1	119.147.146.0	184,286	74.6	4134	CHINANET-BACKBONE No.31,Jin-rong Street,CN
2	165.12.252.0	65,591	6.9	9509	DEWRSB-AU-AP Dept of Employment, Workplace Relations, AU
3	181.66.157.0	23,851	34,128.6	6147	Telefonica del Peru S.A.A., PE
4	66.249.93.0	23,397	19,353.5	15169	GOOGLE - Google Inc., US
5	66.249.85.0	10,685	14,399.7	15169	GOOGLE - Google Inc., US
6	66.249.81.0	9,367	32,502.5	15169	GOOGLE - Google Inc., US
7	150.101.123.0	8,178	423.6	4739	INTERNODE-AS Internode Pty Ltd, AU
8	221.176.4.0	7,790	295.5	9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN
9	66.249.80.0	7,333	18,814.5	15169	GOOGLE - Google Inc., US
10	66.249.88.0	7,241	24,535.5	15169	GOOGLE - Google Inc., US
11	59.167.157.0	4,982	292.9	4739	INTERNODE-AS Internode Pty Ltd, AU
12	69.41.14.0	2,745	1,152.6	47018	CE-BGPAC - Covenant Eyes, Inc. US
13	64.233.172.0	2,548	19,095.9	15169	GOOGLE - Google Inc., US
14	64.125.188.0	2,070	1,181.7	6461	ABOVENET - Abovenet Communications Inc, US
15	93.186.23.0	1,876	20.7	18705	RIMBLACKBERRY - Research In Motion Limited, CA
16	93.186.16.0	1,873	3.3	18705	RIMBLACKBERRY - Research In Motion Limited, CA
17	115.164.209.0	1,519	1,544.0	4818	DIGIIX-AP DiGi Telecommunications Sdn. Bhd., MY
18	93.186.31.0	1,490	8.9	18705	RIMBLACKBERRY - Research In Motion Limited, CA
19	66.249.82.0	1,451	21,705.5	15169	GOOGLE - Google Inc., US
20	208.184.77.0	1,058	1,001.4	6461	ABOVENET - Abovenet Communications Inc, US
21	64.124.98.0	1,055	1,377.7	6461	ABOVENET - Abovenet Communications Inc, US
22	8.35.201.0	726	3.6	15169	GOOGLE - Google Inc., US
23	206.53.152.0	493	7.2	18705	RIMBLACKBERRY - Research In Motion Limited, CA
24	183.60.153.0	484	349.2	4134	CHINANET-BACKBONE No.31 Jin-rong Street, CN
25	199.30.24.0	419	13,339.7	8075	MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US

Top Stalkers

Rank	IP Net	Count	AVG Delay	AS	Description
1	119.147.146.0	184,286	74.6	4134	CHINANET-BACKBONE No.31,Jin-rong Street,CN
2	165.12.252.0	65,591	6.9	9509	DEWRSB-AU-AP Dept of Employment, Workplace Relations, AU
3	181.66.157.0	23,851	34,128.6	6147	Telefonica del Peru S.A.A., PE
4	66.249.93.0	23,397	19,353.5	15169	GOOGLE - Google Inc., US
5	66.249.85.0	10,685	14,399.7	15169	GOOGLE - Google Inc., US
6	66.249.81.0	9,367	32,502.5	15169	GOOGLE - Google Inc., US
7	150.101.123.0	8,178	423.6	4739	INTERNODE-AS Internode Pty Ltd, AU
8	221.176.4.0	7,790	295.5	9808	CMNET-GD Guangdong Mobile Communication Co.Ltd., CN
9	66.249.80.0	7,333	18,814.5	15169	GOOGLE - Google Inc., US
10	66.				
11	59.				
12	69.				JS
13	64.233.172.0	2,548	19,095.9	15169	GOOGLE - Google Inc., US
14	64.125.188.0	2,070	1,181.7	6461	ABOVENET - Abovenet Communications Inc, US
15	93.186.23.0	1,876	20.7	18705	RIMBLACKBERRY - Research In Motion Limited, CA
16	93.186.16.0	1,873	3.3	18705	RIMBLACKBERRY - Research In Motion Limited, CA
17	115.164.209.0	1,519	1,544.0	4818	DIGIIX-AP DiGi Telecommunications Sdn. Bhd., MY
18	93.186.31.0	1,490	8.9	18705	RIMBLACKBERRY - Research In Motion Limited, CA
19	66.249.82.0	1,451	21,705.5	15169	GOOGLE - Google Inc., US
20	208.184.77.0	1,058	1,001.4	6461	ABOVENET - Abovenet Communications Inc, US
21	64.124.98.0	1,055	1,377.7	6461	ABOVENET - Abovenet Communications Inc, US
22	8.35.201.0	726	3.6	15169	GOOGLE - Google Inc., US
23	206.53.152.0	493	7.2	18705	RIMBLACKBERRY - Research In Motion Limited, CA
24	183.60.153.0	484	349.2	4134	CHINANET-BACKBONE No.31 Jin-rong Street, CN
25	199.30.24.0	419	13,339.7	8075	MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation, US

Yes, i've cleared the last octet to (ever so slightly) obscure the stalker's IP address

Web Proxies?

Could this be a variant of a web proxy or active middleware content service that is harvesting URLs off the wire?

- A strong indicator of a local proxy device is that it is located in the same AS as the end client.
- Let's filter that list of URL stalkers and look at those stalkers that use a different Origin AS from the original request
- Here's what we see…

Different Origin AS Stalkers

Rank	IP Net	#	Avg Delay	AS	Description
1	119.147.146.0	132,456	75.1	4134	CHINANET-BACKBONE No.31 Jin-rong Street,CN
2	221.176.4.0	4,954	280.6	9808	CMNET-GD Guangdong Mobile,CN
3	69.41.14.0	2,745	1,152.6	47018	CE-BGPAC - Covenant Eyes Inc.,US
4	64.125.188.0	2,070	1,181.7	6461	ABOVENET - Abovenet Communications Inc,US
5	208.184.77.0	1,058	1,001.4	6461	ABOVENET - Abovenet Communications Inc,US
6	64.124.98.0	1,055	1,377.7	6461	ABOVENET - Abovenet Communications Inc,US
7	183.60.153.0	365	393.4	4134	CHINANET-BACKBONE No.31 Jin-rong Street,CN
8	223.27.200.0	315	3.5	45796	BBCONNECT-TH-AS-AP BB Connect Co. Ltd.,TH
9	101.226.33.0	239	2,591.2	4812	CHINANET-SH-AP China Telecom (Group),CN
10	180.153.206.0	222	2,292.9	4812	CHINANET-SH-AP China Telecom (Group),CN
11	180.153.214.0	161	2,436.1	4812	CHINANET-SH-AP China Telecom (Group),CN
12	101.226.66.0	143	3,068.0	4812	CHINANET-SH-AP China Telecom (Group),CN
13	112.64.235.0	142	3,304.6	17621	CNCGROUP-SH China Unicom Shanghai network,CN
14	180.153.201.0	105	3,079.3	4812	CHINANET-SH-AP China Telecom (Group),CN
15	180.153.163.0	94	3,739.5	4812	CHINANET-SH-AP China Telecom (Group),CN
16	101.226.89.0	77	2,392.5	4812	CHINANET-SH-AP China Telecom (Group),CN
17	111.206.125.0	71	47.4	4808	CHINA169-BJ CNCGROUP IP network China169,CN
18	60.199.178.0	63	103.9	9924	TFN-TW Taiwan Fixed Network Telco,TW
19	101.226.65.0	59	3,820.2	4812	CHINANET-SH-AP China Telecom (Group),CN
20	125.88.25.0	53	374.0	4134	CHINANET-BACKBONE No.31 Jin-rong Street,CN
21	112.65.193.0	47	2,004.0	17621	CNCGROUP-SH China Unicom Shanghai network,CN
22	101.226.51.0	42	2,829.4	4812	CHINANET-SH-AP China Telecom (Group),CN
23	8.35.201.0	33	35.6	15169	GOOGLE - Google Inc.,US
24	180.153.205.0	33	2,788.1	4812	CHINANET-SH-AP China Telecom (Group),CN
25	180.153.114.0	31	2,021.8	4812	CHINANET-SH-AP China Telecom (Group),CN

Maybe it's ISP and/or National Infrastructure

- We've all heard about the Great Firewall of China
  - And other countries may be doing similar things
- Possibly this URL stalking is the result of some form of ISP or national content cache program

- Let's filter this list further by using geo-location information to find those cases where the original end client's IP address and the stalker's IP address locate to different countries

Different Country Stalkers

Rank	IP Net	#	AVG Delay	AS	Description
1	119.147.146.0	102,199	66.8	4134	CHINANET-BACKBONE No.31 Jin-rong Street,CN
2	69.41.14.0	831	1,202.0	47018	CE-BGPAC - Covenant Eyes Inc.,US
3	64.124.98.0	749	1,400.4	6461	ABOVENET - Abovenet Communications Inc,US
4	208.184.77.0	444	911.0	6461	ABOVENET - Abovenet Communications Inc,US
5	223.27.200.0	315	3.5	45796	BBCONNECT-TH-AS-AP BB Connect Co. Ltd.,TH
6	183.60.153.0	301	469.3	4134	CHINANET-BACKBONE No.31 Jin-rong Street,CN
7	64.125.188.0	109	2,967.6	6461	ABOVENET - Abovenet Communications Inc,US
8	60.199.178.0	63	103.9	9924	TFN-TW Taiwan Fixed Network Telco,TW
9	8.35.201.0	33	35.6	15169	GOOGLE - Google Inc.,US
10	65.49.68.0	13	1.8	6939	HURRICANE - Hurricane Electric Inc.,US
11	71.58.164.0	8	0.5	7922	COMCAST-7922 - Comcast Cable Communications Inc.,US
12	218.186.15.0	7	4.3	10091	SCV-AS-AP StarHub Cable Vision Ltd,SG
13	8.37.224.0	6	0.2	54994	WANGSU-US - Chinanetcenter (USA),US
14	125.88.123.0	6	43.7	4134	CHINANET-BACKBONE No.31 Jin-rong Street,CN
15	175.156.206.0	5	4.6	4773	MOBILEONELTD-AS-AP MobileOne Ltd. Singapore,SG
16	94.242.251.0	5	16.6	5577	ROOT root SA,LU
17	65.49.2.0	5	1.8	6939	HURRICANE - Hurricane Electric Inc.,US
18	37.130.227.0	4	6.2	13213	UK2NET-AS UK2 - Ltd,GB
19	185.2.138.0	4	8.0	13213	UK2NET-AS UK2 - Ltd,GB
20	77.247.181.0	4	8.8	43350	NFORCE NFOrce Entertainment BV,NL
21	109.201.138.0	4	32.5	43350	NFORCE NFOrce Entertainment BV,NL
22	77.109.138.0	4	10.0	13030	INIT7 Init Seven AG,CH
23	107.219.51.0	4	0.0	7018	ATT-INTERNET4 - AT&T Services Inc.,US
24	68.96.8.0	4	0.0	22773	ASN-CXA-ALL - Cox Communications Inc.,US
25	77.109.141.0	4	6.5	13030	INIT7 Init Seven AG,CH

Different Country Stalkers

Rank	IP Net	#	AVG Delay	AS	Description
1	119.147.146.0	102,199	66.8	4134	CHINANET-BACKBONE No.31 Jin-rong Street,CN
2	69.41.14.0	831	1,202.0	47018	CE-BGPAC - Covenant Eyes Inc.,US
3	64.124.98.0	749	1,400.4	6461	ABOVENET - Abovenet Communications Inc,US
4	208.184.77.0	444	911.0	6461	ABOVENET - Abovenet Communications Inc,US
5	223.27.200.0	315	3.5	45796	BBCONNECT-TH-AS-AP BB Connect Co. Ltd.,TH
6	183.60.153.0	301	469.3	4134	CHINANET-BACKBONE No.31 Jin-rong Street,CN
7	64.125.188.0	109	2,967.6	6461	ABOVENET - Abovenet Communications Inc,US
8	60.199.178.0	63	103.9	9924	TFN-TW Taiwan Fixed Network Telco,TW

Create account Log in

Article Talk Read Edit View history Search

WIKIPEDIA
The Free Encyclopedia

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

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."

22	77.109.138.0	4	10.0	13030	INIT7 Init Seven AG,CH
23	107.219.51.0	4	0.0	7018	ATT-INTERNET4 - AT&T Services Inc.,US
24	68.96.8.0	4	0.0	22773	ASN-CXA-ALL - Cox Communications Inc.,US
25	77.109.141.0	4	6.5	13030	INIT7 Init Seven AG,CH

What are we seeing here?

- State-based Espionage?
- Compromised Middleware?
- Commercial espionage?
- Commercial data collection?
- Viral spyware?

Street Art: Banksy

Where are the Stalked?

CC	Stalk Count	Country
AD	1	Andorra
AE	105	United Arab Emirates
AF	2	Afghanistan
AG	8	Antigua and Barbuda
AL	620	Albania
AM	32	Armenia
AO	3	Angola
AR	141	Argentina
AT	39	Austria
AU	1094	Australia
AW	11	Aruba
AZ	17	Azerbaijan
BA	85	Bosnia and Herzegovina
BB	9	Barbados
BD	18	Bangladesh
BE	53	Belgium
BG	379	Bulgaria
BH	10	Bahrain
BN	6	Brunei Darussalam
BO	8	Bolivia
BR	262	Brazil
BS	3	Bahamas
BT	2	Bhutan
BY	28	Belarus
BZ	3	Belize
CA	995	Canada
CD	2	The Congo
CH	48	Switzerland
CI	4	Cote d'Ivoire
CL	45	Chile
CM	5	Cameroon
CN	44496	China
CO	195	Colombia
CR	8	Costa Rica
CV	1	Cape Verde
CY	42	Cyprus
CZ	71	Czech Republic
DE	198	Germany
DK	22	Denmark
DO	19	Dominican Republic
DZ	62	Algeria
EC	38	Ecuador
EE	16	Estonia
EG	199	Egypt
ES	120	Spain
FI	54	Finland
FJ	6	Fiji
FR	330	France
GB	6816	United Kingdom
GE	31	Georgia
GH	12	Ghana
GL	4	Greenland
GQ	2	Equatorial Guinea
GR	288	Greece
GT	3	Guatemala
GU	6	Guam
GY	4	Guyana
HK	2827	Hong Kong SAR of China
HN	8	Honduras
HR	49	Croatia
HU	220	Hungary
ID	493	Indonesia
IE	15	Ireland
IL	99	Israel
IN	396	India
IQ	265	Iraq
IR	47	Iran
IT	253	Italy
JM	14	Jamaica
JO	3	Jordan
JP	5782	Japan
KE	11	Kenya
KG	13	Kyrgyzstan
KH	108	Cambodia
KR	128	Republic of Korea
KW	2	Kuwait
KZ	414	Kazakhstan
LA	11	Lao People's Democratic Republic
LB	4	Lebanon
LK	16	Sri Lanka
LR	3	Liberia
LT	90	Lithuania
LU	3	Luxembourg
LV	31	Latvia
LY	7	Libya
MA	409	Morocco
MD	22	Republic of Moldova
ME	128	Montenegro
MK	408	Yugoslav Republic of Macedonia

Where are the Stalked?

ML	2	Mali
MM	26	Myanmar
MN	24	Mongolia
MO	306	Macao SAR of China
MP	28	Northern Mariana Islands
MR	2	Mauritania
MT	20	Malta
MU	17	Mauritius
MX	485	Mexico
MY	2828	Malaysia
NA	3	Namibia
NG	20	Nigeria
NL	114	Netherlands
NO	17	Norway
NP	18	Nepal
NZ	293	New Zealand
OM	12	Oman
PA	30	Panama
PE	202	Peru
PH	679	Philippines
PK	135	Pakistan
PL	1776	Poland
PR	12	Puerto Rico
PS	51	Occupied Palestinian Territory
PT	33	Portugal
PY	1	Paraguay
QA	49	Qatar
RO	916	Romania
RS	311	Serbia
RU	343	Russian Federation
RW	2	Rwanda
SA	141	Saudi Arabia
SD	1	Sudan
SE	62	Sweden
SG	7027	Singapore
SI	37	Slovenia
SK	35	Slovakia
SN	11	Senegal
SR	27	Suriname
ST	3	Sao Tome and Principe
SV	3	El Salvador
TG	2	Togo
TH	557	Thailand
TJ	3	Tajikistan
TN	29	Tunisia
TR	350	Turkey
TT	11	Trinidad and Tobago
TW	3922	Taiwan
TZ	4	United Republic of Tanzania
UA	185	Ukraine
UG	5	Uganda
US	3007	United States of America
UY	7	Uruguay
VE	54	Venezuela
VN	2429	Vietnam
YE	3	Yemen
ZA	6	South Africa
ZM	1	Zambia
ZW	1	Zimbabwe

Where are the Stalked?

- This is an impressive list of countries
  - Which says a lot about the ubiquity of Google Ads (and YouTube watchers)!
  - But it also says a lot about the reach of the particular stalking activity we are seeing here
- Is this list skewed towards any particular country?

Where are the stalked?

CN	**44496**	**China**
SG	**7027**	**Singapore**
GB	**6816**	**United Kingdom of Great Britain and Northern Ireland**
JP	**5782**	**Japan**
TW	**3922**	**Taiwan**
US	**3007**	**United States of America**
MY	**2828**	**Malaysia**
HK	**2827**	**Hong Kong Special Administrative Region of China**
VN	**2429**	**Vietnam**
PL	**1776**	**Poland**
AU	**1094**	**Australia**
CA	**995**	**Canada**
RO	**916**	**Romania**
PH	**679**	**Philippines**
AL	**620**	**Albania**
TH	**557**	**Thailand**
ID	**493**	**Indonesia**
MX	**485**	**Mexico**
KZ	**414**	**Kazakhstan**
MA	**409**	**Morocco**
MK	**408**	**The former Yugoslav Republic of Macedonia**
IN	**396**	**India**
BG	**379**	**Bulgaria**
TR	**350**	**Turkey**
RU	**343**	**Russian Federation**

This is the top 25 countries where we have observed end systems that appear to have attracted this particular stalker

Where are the stalked?

CC	Stalk	Total	Rate/100000	Country
MO	414	13,080	3,165	Macao Special Administrative Region of China
CN	54,770	3,275,057	1,672	China
MP	41	2,474	1,657	Northern Mariana Islands
HK	3,454	209,588	1,647	Hong Kong Special Administrative Region of China
ST	3	205	1,463	Sao Tome and Principe
GL	4	318	1,257	Greenland
TW	4,855	546,492	888	Taiwan
JP	7,377	839,634	878	Japan
GQ	4	506	790	Equatorial Guinea
MY	3,356	68,9486	486	Malaysia
AL	942	211,644	445	Albania
PM	2	470	425	Saint Pierre and Miquelon
LR	3	743	403	Liberia
MK	562	146,663	383	The former Yugoslav Republic of Macedonia
SG	8,229	2184,466	376	Singapore
IR	64	22,508	284	Iran (Islamic Republic of)
KH	144	53,815	267	Cambodia
ME	175	66,077	264	Montenegro
SR	38	15,793	240	Suriname
AW	11	4,906	224	Aruba
FJ	16	7,157	223	Fiji
MM	29	14,212	204	Myanmar
LA	16	8,040	199	Lao People's Democratic Republic
CA	1,157	593,756	194	Canada
AG	10	5,264	189	Antigua and Barbuda

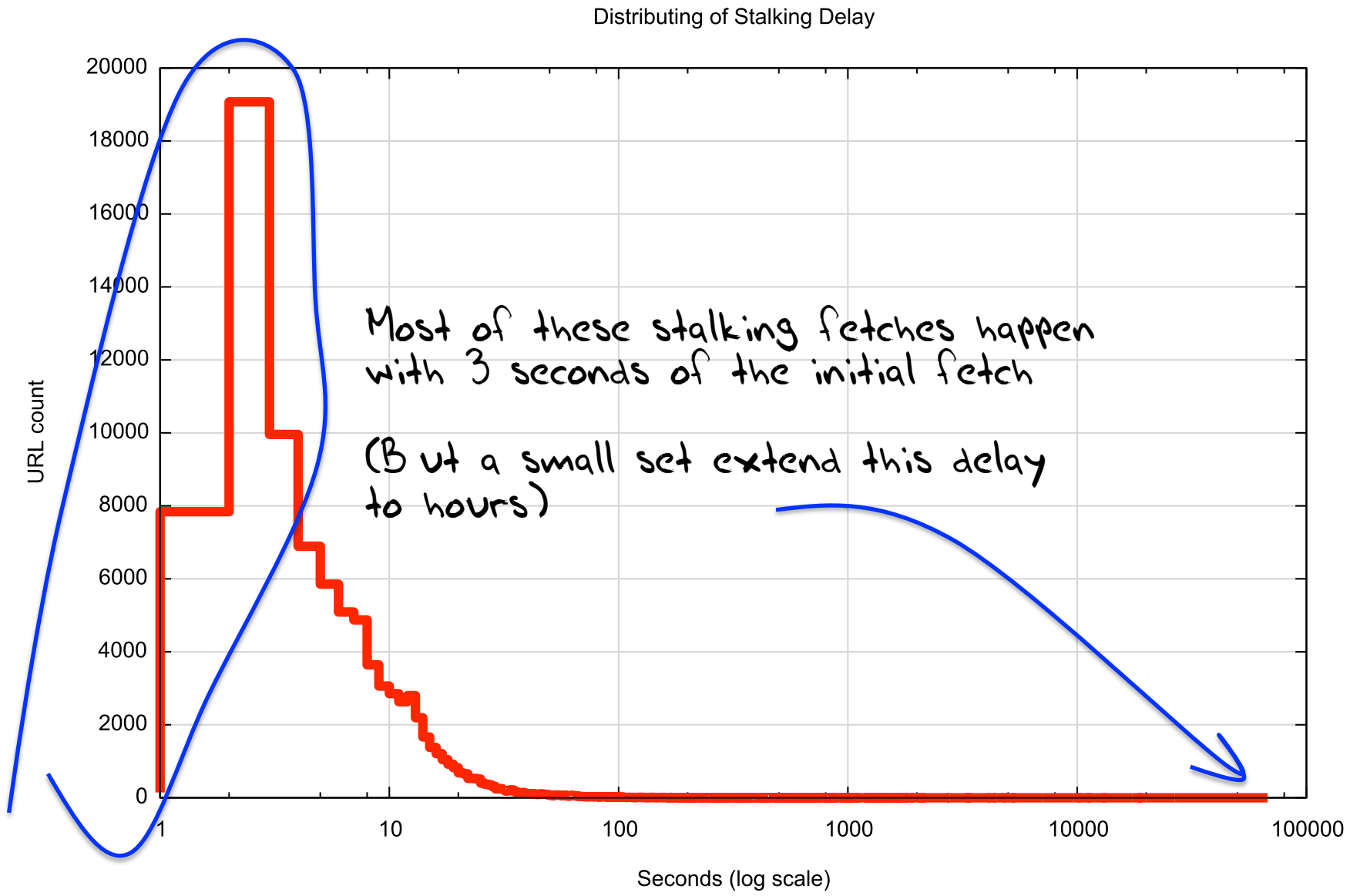
This is the top 25 countries with the highest relative rate of stalking from this particular stalker

Stalking Delay Distribution

Is this stalking instant, or delayed?

- The average interval between the initial URL fetch and the second fetch from this net is 74 seconds. What's the distribution in delay times?

Distribution of Stalking Delay



User Agent strings

- What User Agent string is used by the stalker?
- What User Agent strings are used by the stalked?

The Stalker's User Agent String

Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; MAXTHON 2.0)

Top 25 User Agent Strings of the stalked systems

6,068 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,458 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,389 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36
5,029 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
4,669 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
4,641 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
3,382 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
3,265 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0
3,084 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
2,915 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.76 Safari/537.36
2,813 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36
2,813 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0
2,765 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1
2,653 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.117 Safari/537.36
2,651 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36
2,416 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36
2,238 Mozilla/5.0 (Windows NT 6.1; rv:26.0) Gecko/20100101 Firefox/26.0
2,222 Mozilla/5.0 (Windows NT 5.1; rv:26.0) Gecko/20100101 Firefox/26.0
2,142 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
2,043 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0
2,028 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
1,965 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.76 Safari/537.36
1,876 Mozilla/5.0 (Windows NT 6.1; rv:27.0) Gecko/20100101 Firefox/27.0
1,846 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36
1,813 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.102 Safari/537.36

Top 25 User Agent Strings of the stalked systems

6,068 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,458 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,389 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36
5,029 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
4,669 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
4,641 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
3,382 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
3,265 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0
3,084 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML
2,915 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537
2,813 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML
2,813 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20
2,765 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537
2,653 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.117 Safari/537.36
2,651 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36
2,416 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36
2,238 Mozilla/5.0 (Windows NT 6.1; rv:26.0) Gecko/20100101 Firefox/26.0
2,222 Mozilla/5.0 (Windows NT 5.1; rv:26.0) Gecko/20100101 Firefox/26.0
2,142 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
2,043 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0
2,028 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
1,965 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.76 Safari/537.36
1,876 Mozilla/5.0 (Windows NT 6.1; rv:27.0) Gecko/20100101 Firefox/27.0
1,846 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36
1,813 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.102 Safari/537.36

Many of the stalked end systems appear to be using Windows OS platforms!

Top 25 User Agent Strings of the stalked systems

6,068 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,458 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,389 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36
5,029 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
4,669 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
4,641 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
3,382 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
3,265 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0
[illegible]Chrome/32.0.1700.107 Safari/537.36
[illegible]Gecko) Chrome/32.0.1700.76 Safari/537.36
[illegible]Chrome/33.0.1750.154 Safari/537.36
[illegible]/27.0
2,765 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.1 (KHTML, like Gecko) Chrome/21.0.1180.89 Safari/537.1
2,653 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.117 Safari/537.36
2,651 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36
2,416 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36
2,238 Mozilla/5.0 (Windows NT 6.1; rv:26.0) Gecko/20100101 Firefox/26.0
2,222 Mozilla/5.0 (Windows NT 5.1; rv:26.0) Gecko/20100101 Firefox/26.0
2,142 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
2,043 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0
2,028 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.63 Safari/537.36
1,965 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.76 Safari/537.36
1,876 Mozilla/5.0 (Windows NT 6.1; rv:27.0) Gecko/20100101 Firefox/27.0
1,846 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.131 Safari/537.36
1,813 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.102 Safari/537.36

Many of the stalked end systems appear to be Chrome!

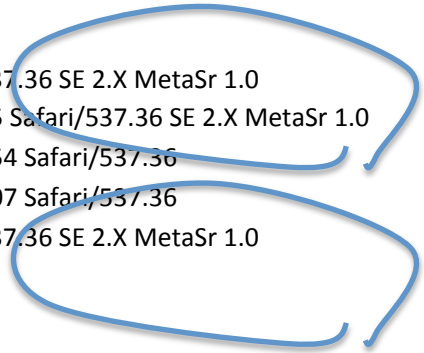
Chrome/Windows Virus?

Well, no – not in this case!

There is some further detail in the User Agent string that may help?

Top 25 User Agent Strings of the stalked systems

6,068 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,458 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,389 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36
5,029 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
4,669 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0



Top 25 User Agent Strings of the stalked systems

6,068 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,458 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,389 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36
5,029 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
4,669 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0

Sogou Explorer 2.X

WIKIPEDIA
The Free Encyclopedia

Sogou

From Wikipedia, the free encyclopedia

For the Japanese department store, see Sogo.

Sogou, Inc. is a subsidiary of Sohu.com, Inc. founded on 9 August 2010. It is the owner and developer of **Sogou** (Chinese: 搜狗; pinyin: *Sōugǒu*; literally: "Search dog") search engine, Sogou Input and Sogou browser.

Contents [show]

Products [edit]

Search engine and web applications [edit]

Sogou search engine (Sogou.com) was launched on 3 August 2004.

Sogou's web application products are designed to classify on-line information, such as music, picture, video clip, news, map and vertical information.

Sogou Input [edit]

Main article: Sogou Pinyin

Initially released in 2006, Sogou Pinyin is the most popular Chinese input software in China. It makes use of its search engine techniques which are the analysis and categorization of the most popular words or phrases on the Internet.

Sogou browser [edit]

Started in December 2008, Sogou browser adopts a "dual-core" (Google Chrome's WebKit and Internet Explorer's Trident layout engines) techniques and it connects to the cloud to recognize malicious websites and software.

Investment [edit]

On 17 September 2013, it was announced that Tencent has invested $448 million for a minority share in Chinese search engine Sogou.com, the subsidiary of Sohu, Inc.[2]

Sogou, Inc.
搜狗公司

Type	Public company, subsidiary
Founded	9 August 2010; 3 years ago
Headquarters	Beijing, China
Industry	Internet
Website	Sogou.com

Sogou
搜狗

Website screenshot [show]

Web address	www.sogou.com
Commercial?	yes
Available language(s)	Chinese
Users	400 million
Owner	Sogou, Inc. (subsidiary of Sohu, Inc.)
Launched	4 August 2004; 9 years ago
Alexa rank	▲ 137 (April 2014)[1]
Current status	Active

Top 25 User Agent Strings of the stalked systems

6,068 Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,458 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0
5,389 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36
5,029 Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36
4,669 Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.95 Safari/537.36 SE 2.X MetaSr 1.0

Sogou Explorer 2.X

WIKIPEDIA
The Free Encyclopedia

Sogou

From Wikipedia, the free encyclopedia

For the Japanese department store, see Sogo.

Sogou, Inc. is a subsidiary of Sohu.com, Inc. founded on 9 August 2010. It is the owner and developer of **Sogou** (Chinese: 搜狗; pinyin: *Sōugǒu*; literally: "Search dog") search engine, Sogou Input and Sogou browser.

Contents [show]

Products [edit]

Search engine and web applications [edit]

Sogou search engine (Sogou.com) was launched on 3 August 2004.

Sogou's web application products are designed to classify on-line information, such as music, picture, video clip, news, map and vertical information.

Sogou Input [edit]

Main article: Sogou Pinyin

Initially released in 2006, Sogou Pinyin is the most popular Chinese input software in China. It makes use of its search engine techniques which are the analysis and categorization of the most popular words or phrases on the Internet.

Sogou browser [edit]

Started in December 2008, Sogou browser adopts a "dual-core" (Google Chrome's WebKit and Internet Explorer's Trident layout engines) techniques and it connects to the cloud to recognize malicious websites and software.

Investment [edit]

On 17 September 2013, it was announced that Tencent has invested $448 million for a minority share in Chinese search engine Sogou.com, the subsidiary of Sohu, Inc.[2]

Sogou, Inc.
搜狗公司

Type	Public company, subsidiary
Founded	9 August 2010; 3 years ago
Headquarters	Beijing, China
Industry	Internet
Website	Sogou.com

Sogou
搜狗

Website screenshot [show]

Web address	www.sogou.com
Commercial?	yes
Available language(s)	Chinese
Users	400 million
Owner	Sogou, Inc. (subsidiary of Sohu, Inc.)
Launched	4 August 2004; 9 years ago
Alexa rank	▲ 137 (April 2014)[1]
Current status	Active

"It connects to the cloud to recognize malicious websites and software"

What are we seeing for stalking from 119.147.146.0/24?

- State-based Espionage?
- Compromised Middleware?
- Commercial espionage?
- Commercial data collection?
- Viral spyware?
- Cloud-Mania?

We see an average of around 1 in 500 of all visible end users are attracting an Internet stalker.

It's likely that most of these observed stalkers are either performing some content caching function, or performing URL checking for content rating and monitoring

Who else gets to see this data of user behaviour? Under what conditions?

Is this form of digital stalking something that we are comfortable with?

Are we even aware that it is happening at all?

This data set is just a tiny glimpse into the overall pattern of web activity

What’s happening in the larger world of various forms of tracking users’ behaviour on the Internet?

Thanks to:

Warren Kumari, of Google, who spent some time looking through user agent strings to identify a pointer to the Sogou browser in the collected data.

Thanks!

Street Art: Banksy