Distributed, Stealthy Brute Force Password Guessing Attempts

PASSWORDS14, Trondheim 8 December 2014

Peter N. M. Hansteen

BSDly.net
<peter@bsdly.net>

<peter.hansteen@evry.com>

Twitter: @pitrh

The Hail Mary Cloud: A Widely Distributed, Low Intensity Password Guessing SSH Botnet

The Hail Mary Cloud was a widely distributed, low intensity password guessing botnet that targeted Secure Shell (ssh) servers on the public Internet.

The first activity may have been as early as 2005 [Mobin and Paxson (2013)], our first recorded data start in late 2008. Links to full data and extracts are found in this presentation.

We present the basic behavior and algorithms, and point to possible policies for staying safe(r) from similar present or future attacks, as well as some attacks on other services.

But first, the devil we knew -

The Traditional SSH Bruteforce Attack

If you run an Internet-facing SSH service, you have seen something like this in your logs:

```
Sep 26 03:12:34 skapet sshd[25771]: Failed password for root from 200.72.41.31 port 40992 ssh2
Sep 26 03:12:34 skapet sshd[5279]: Failed password for root from 200.72.41.31 port 40992 ssh2
Sep 26 03:12:35 skapet sshd[5279]: Received disconnect from 200.72.41.31: 11: Bye Bye
Sep 26 03:12:44 skapet sshd[29635]: Invalid user admin from 200.72.41.31
Sep 26 03:12:44 skapet sshd[24703]: input_userauth_request: invalid user admin
Sep 26 03:12:44 skapet sshd[24703]: Failed password for invalid user admin from 200.72.41.31
port 41484 ssh2
Sep 26 03:12:44 skapet sshd[29635]: Failed password for invalid user admin from 200.72.41.31
port 41484 ssh2
Sep 26 03:12:45 skapet sshd[24703]: Connection closed by 200.72.41.31
Sep 26 03:13:10 skapet sshd[11459]: Failed password for root from 200.72.41.31 port 43344 ssh2
```

This is the classic, rapid-fire type of bruteforce attack.

Actually, most of them target root exclusively.

The Likely Business Plan

Either preceded by a port scan or just blasting away, the miscreants' likely plan is

1. Try for likely user names, hope for guessable password
2. Keep guessing until successful
3. ***PROFIT!***

They usually come in faster than most of us can type, so

Traditional Anti-Bruteforce Rules

Rapid-fire bruteforce attacs are easy to head off, here's the OpenBSD PF style, with state tracking options to set limits:

/etc/pf.conf

```
table <bruteforce> persist
block quick from <bruteforce>
pass inet proto tcp to $int_if:network port $tcp_services \
        keep state (max-src-conn 100, max-src-conn-rate 15/5, \
         overload <bruteforce> flush global)
```

`max-src-conn:` # of connections from one host

`max-src-conn-rate`: rate of new connections: 15 connections per 5 seconds .

`overload <bruteforce>`: offenders go to the blocked table

flush global: kill all connections

Basically, ***problem solved*** - the noise generally disappears instantly. If you like, tweak rules to local tastes and needs.

(and yes, Linux and other scan do similar, won't get into them)

What's That? Something New!

On November 19th, 2008 (or shortly thereafter), I noticed this:

```
Nov 19 15:04:22 rosalita sshd[40232]: error: PAM: authentication error for illegal user alias from s514.nxs.nl
Nov 19 15:07:32 rosalita sshd[40239]: error: PAM: authentication error for illegal user alias from c90678d3.static.spo.virtua.com.br
Nov 19 15:10:20 rosalita sshd[40247]: error: PAM: authentication error for illegal user alias from 207-47-162-
126.prna.static.sasknet.sk.ca
Nov 19 15:13:46 rosalita sshd[40268]: error: PAM: authentication error for illegal user alias from 125-236-218-109.adsl.xtra.co.nz
Nov 19 15:16:29 rosalita sshd[40275]: error: PAM: authentication error for illegal user alias from 200.93.147.114
Nov 19 15:19:12 rosalita sshd[40279]: error: PAM: authentication error for illegal user alias from 62.225.15.82
Nov 19 15:22:29 rosalita sshd[40298]: error: PAM: authentication error for illegal user alias from 121.33.199.39
Nov 19 15:25:14 rosalita sshd[40305]: error: PAM: authentication error for illegal user alias from 130.red-80-37-213.staticip.rima-tde.net
Nov 19 15:28:23 rosalita sshd[40309]: error: PAM: authentication error for illegal user alias from 70-46-140-187.orl.fdn.com
Nov 19 15:31:17 rosalita sshd[40316]: error: PAM: authentication error for illegal user alias from gate-dialog-simet.jgora.dialog.net.pl
Nov 19 15:34:18 rosalita sshd[40334]: error: PAM: authentication error for illegal user alias from 80.51.31.84
Nov 19 15:37:23 rosalita sshd[40342]: error: PAM: authentication error for illegal user alias from 82.207.104.34
Nov 19 15:40:20 rosalita sshd[40350]: error: PAM: authentication error for illegal user alias from 70-46-140-187.orl.fdn.com
Nov 19 15:43:39 rosalita sshd[40354]: error: PAM: authentication error for illegal user alias from 200.20.187.222
Nov 19 15:46:41 rosalita sshd[40374]: error: PAM: authentication error for illegal user amanda from 58.196.4.2
Nov 19 15:49:31 rosalita sshd[40378]: error: PAM: authentication error for illegal user amanda from host116-164.dissent.birch.net
Nov 19 15:55:47 rosalita sshd[40408]: error: PAM: authentication error for illegal user amanda from robert71.lnk.telstra.net
Nov 19 15:59:08 rosalita sshd[40412]: error: PAM: authentication error for illegal user amanda from static-71-166-159-
177.washdc.east.verizon.net
```

... and so on, the alphabetic progression went on and on.

Several hosts try to access the same user, up to minutes apart. When any one host comes back it's more likely than not several user names later. The full sequence (it stopped December 30th), is available here.

The Initial Reaction

Was disbelief.

For the first few days I tried tweaking PF rules. (How do I make this match?)

Short version: You can't. You will soon hit limits (especially time limits) that interfere with normal use.

Next, I started analyzing my data, and came up with -

Business Plan, Distributed Version

Executive Summary: Have more hosts take turns, round robin-ish, at long enough intervals to stay under the radar, guessing for weak passwords.

The plan is much like before, but now we have more host on the attacking side, so

1. Pick a host from our pool, assign a user name and password (from list, dictionary or pool). For each host,
    1. Try logging in to the chosen target with the assigned user name and password
    2. If successful, report back to base (we theorize); else wait for instructions (again we speculate)
2. Go to 1.
3. For each success at 2.2, ***PROFIT!***

You're The Target

Still it boils down to the same basics:

1. Your Unix computer (Linux, OpenBSD, FreeBSD or other) is a desirable, powerful thing.
2. If your password is weak, you will be 0WN3D, sooner rather than later.

There's a whole fleet out there, and they're coordinated.

Introducing dt_ssh5, Linux /tmp Resident

Of course there was a piece of malware involved. A Linux binary called *dt_ssh5* did the grunt work.

The *dt_ssh5* file was found installed in */tmp* on affected systems, likely because the */tmp* directory tends to be world readable and world writeable.

Three basic lessons:

1. Stay away from guessable passwords
2. Watch for weird files (stuff you didn't put there yourself) anywhere in your file system, even in */tmp*.
3. Internalize the fact that `PermitRootLogin yes` is a bad idea.

The Waves We Saw, 2008 - 2014

We saw eight sequences of SSH attempts (complete list of articles in References), plus two for other services (POP3 and Wordpress).

The 2009-09-30 sequence was notable for trying only root, the 2012-04-01 sequence for being the first to attempt access to OpenBSD hosts.

We may have missed earlier sequences, early reports place the first similar attempts as far back as 2005 (Mobin and Paxson).

2008-11-19 15:04:22 - 2008-12-30 11:09:03

Top ten hosts (of 1193):

Attempts	Host	User Names	First Seen	Last Seen
351	217.96.70.66	2	2009-11-20 04:56	2009-12-30 04:21
270	coloc82-044.singnet.com.sg	2	2009-11-20 05:06	2009-12-30 09:24
269	static-98-119-110-139.lsanca.dsl-w.verizon.net	2	2009-11-20 18:08	2009-12-30 11:09
263	c-71-63-229-140.hsd1.mn.comcast.net	2	2009-11-20 14:41	2009-12-30 09:52
248	211.154.254.120	2	2009-11-20 08:32	2009-12-29 21:08
244	170.56.255.20	2	2009-11-20 03:43	2009-12-20 16:23
221	123.14.10.64	2	2009-11-20 08:18	2009-12-17 18:50
217	190.144.61.58	2	2009-11-20 14:31	2009-12-26 11:24
215	200.118.119.48	2	2009-11-20 06:47	2009-12-30 07:35

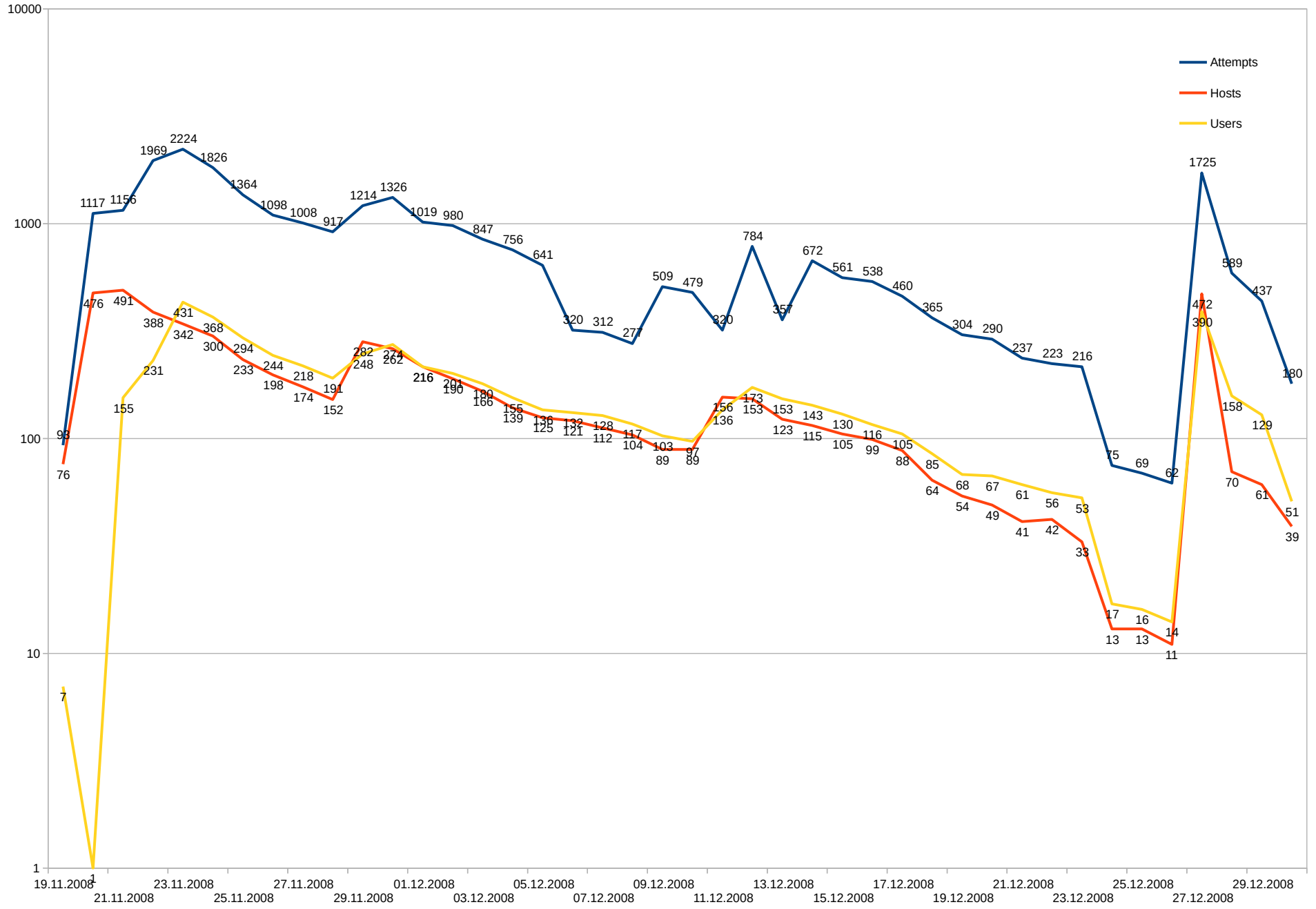
Full list at http://home.nuug.no/~peter/passwords14/2008nov19/gropers_ranked.csv

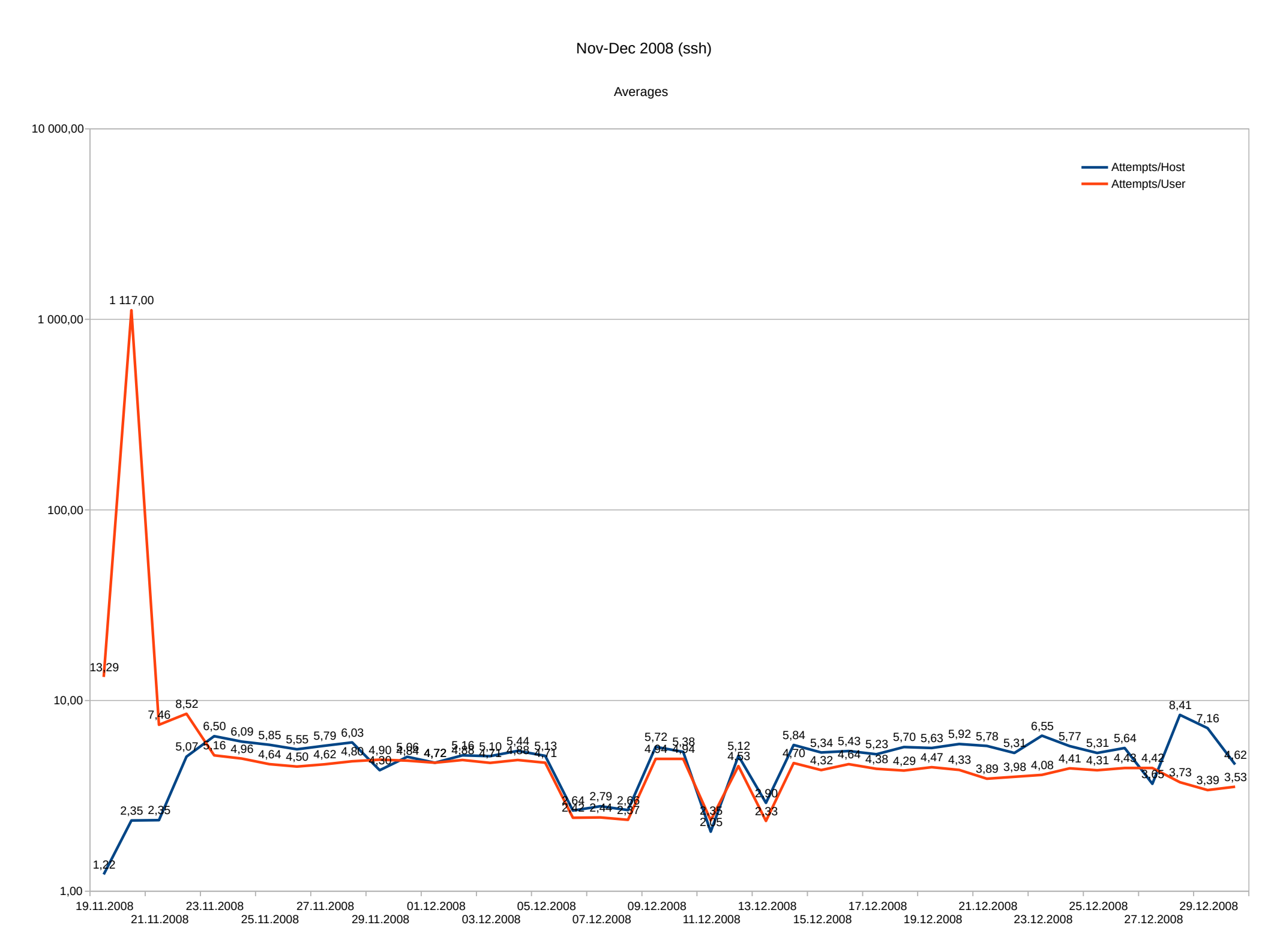
2008-11-19 15:04:22 - 2008-12-30 11:09:03

Top ten user IDs (of 6100):

Attempts	User ID
1697	root
128	admin
30	emilie
30	elise
26	denise
26	corinne
26	cecilia
26	astrid
25	dorothy
25	colette

Full list at http://home.nuug.no/~peter/passwords14/2008nov19/groped-users-by-frequency.txt


Nov-Dec 2008 (ssh)
Attempts
Hosts
Users
10000
1000
100
10
1
19.11.2008
21.11.2008
23.11.2008
25.11.2008
27.11.2008
29.11.2008
01.12.2008
03.12.2008
05.12.2008
07.12.2008
09.12.2008
11.12.2008
13.12.2008
15.12.2008
17.12.2008
19.12.2008
21.12.2008
23.12.2008
25.12.2008
27.12.2008
29.12.2008


Nov-Dec 2008 (ssh)
Averages
10 000,00
1 000,00
100,00
10,00
1,00
Attempts/Host
Attempts/User
19.11.2008
21.11.2008
23.11.2008
25.11.2008
27.11.2008
29.11.2008
01.12.2008
03.12.2008
05.12.2008
07.12.2008
09.12.2008
11.12.2008
13.12.2008
15.12.2008
17.12.2008
19.12.2008
21.12.2008
23.12.2008
25.12.2008
27.12.2008
29.12.2008

2009-04-07 03:56:25 - 2009-04-12 21:01:37

Top ten hosts (of 1104):

Attempts	Host	User Names	First Seen	Last Seen
203	216.45.58.210	191	2009-04-07 06:18	2009-04-12 15:54
155	221.130.177.154	140	2009-04-07 14:02	2009-04-12 19:04
152	75.125.217.2	140	2009-04-07 19:53	2009-04-12 18:09
140	216.195.56.227	135	2009-04-07 07:01	2009-04-09 14:29
119	websvr01.dbhosting.nl	2	2009-04-08 00:42	2009-04-11 15:24
110	200.69.217.177	82	2009-04-07 06:37	2009-04-12 20:41
109	66.63.165.200	97	2009-04-07 09:13	2009-04-12 19:25
99	85.17.154.236	95	2009-04-07 20:42	2009-04-12 19:02
98	webmail.jknet.com.br	2	2009-04-07 06:39	2009-04-12 06:24
97	72.30.5446.static.theplanet.com	2	2009-04-07 05:05	2009-04-12 16:57

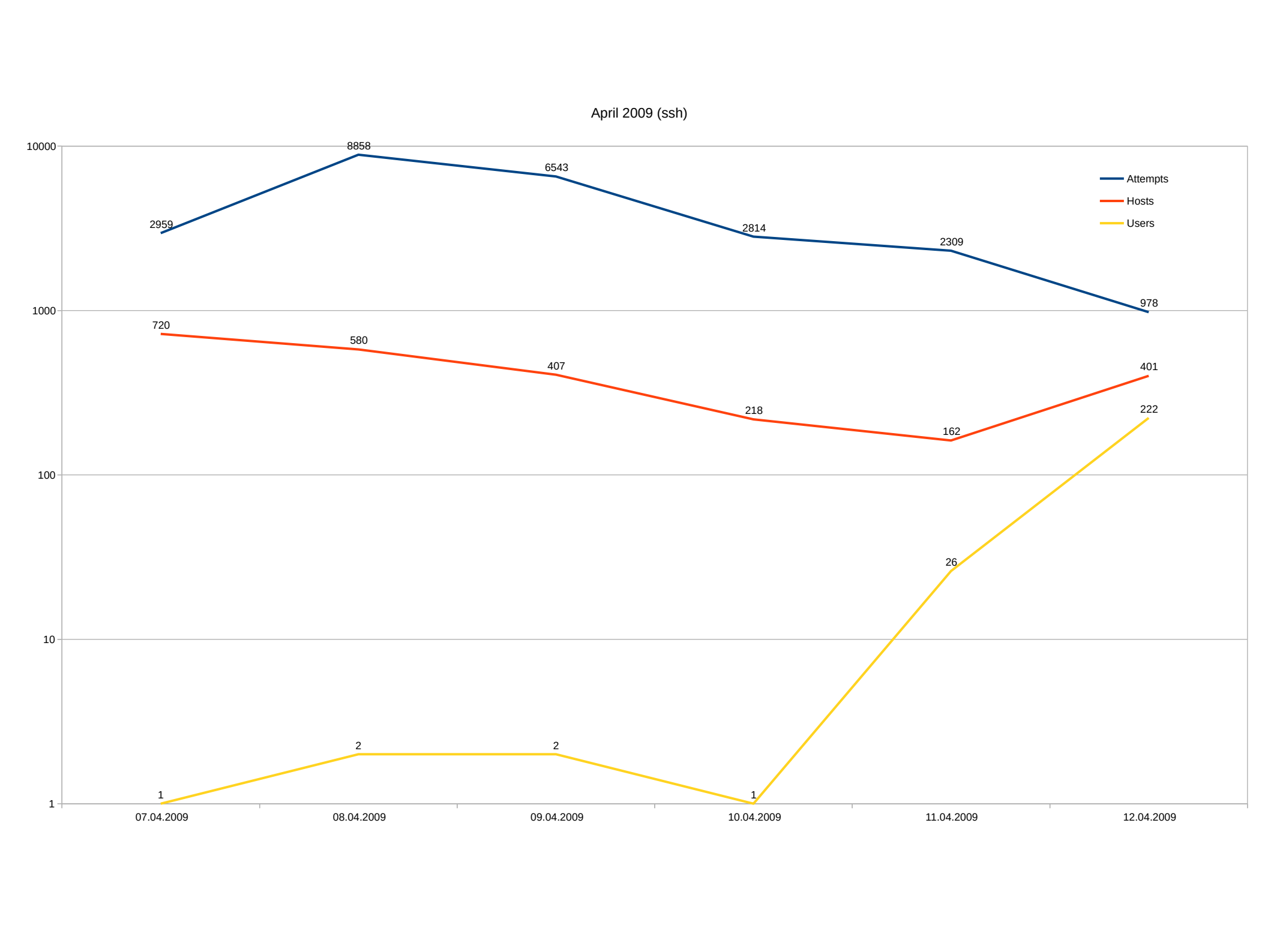
Full list at http://home.nuug.no/~peter/passwords14/aprilbrutes/gropers_ranked.csv

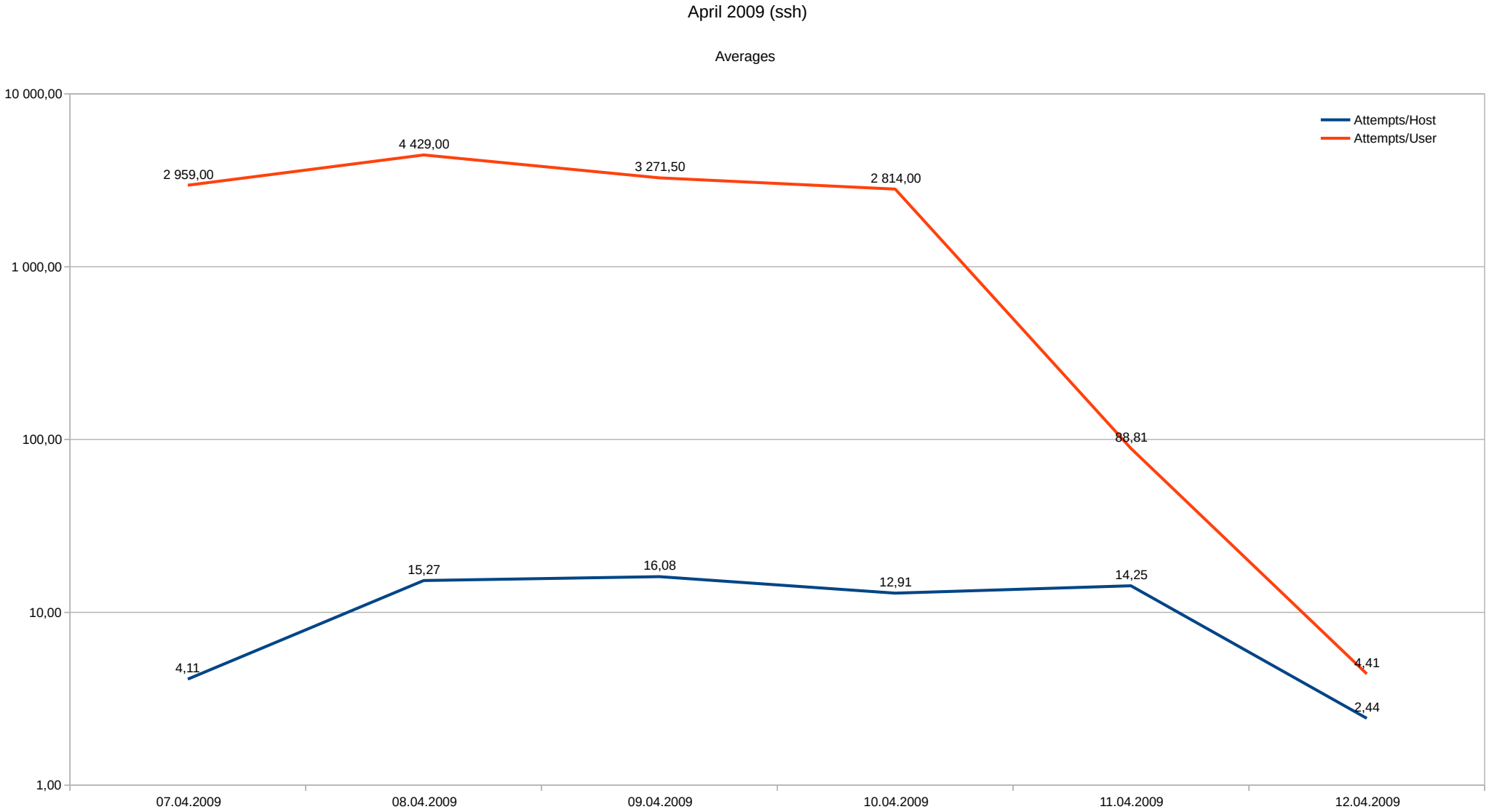
2009-04-07 03:56:25 - 2009-04-12 21:01:37

Top ten user IDs (of 249):

Attempts	User ID
5711	admin
3454	james
2316	root
10	abner
10	abigail
10	abiba
10	abia
10	abbie
10	aaron
10	aaralyn

Full list at http://home.nuug.no/~peter/passwords14/aprilbrutes/groped-users-by-frequency.txt


April 2009 (ssh)
10000
1000
100
10
1
Attempts
Hosts
Users
2959
8858
6543
2814
2309
978
720
580
407
218
162
401
1
2
2
1
26
222
07.04.2009
08.04.2009
09.04.2009
10.04.2009
11.04.2009
12.04.2009


April 2009 (ssh)
Averages
10 000,00
1 000,00
100,00
10,00
1,00
Attempts/Host
Attempts/User
2 959,00
4 429,00
3 271,50
2 814,00
88,81
4,41
4,11
15,27
16,08
12,91
14,25
2,44
07.04.2009
08.04.2009
09.04.2009
10.04.2009
11.04.2009
12.04.2009

2009-09-30 21:15:36 - 2009-10-15 13:42:07

Top 10 hosts (of 1071):

Attempts	Host	User Names	First Seen	Last Seen
729	212.243.41.9	352	30.10.09 05:21	13.01.10 12:36
477	217.70.139.42	217	30.10.09 13:47	25.11.09 01:05
457	58.247.222.163	213	03.11.09 23:47	18.01.10 09:38
444	80.169.105.159	220	29.10.09 00:27	15.01.10 06:19
438	202.102.245.109	213	30.10.09 06:41	04.01.10 20:38
418	220.162.241.11	202	30.10.09 04:50	17.01.10 15:25
394	116.55.226.131	185	05.11.09 16:25	07.01.10 04:00
384	211.115.234.143	177	05.11.09 02:05	22.01.10 07:17
381	80.243.172.54	181	03.11.09 20:03	17.01.10 11:33
375	58.60.106.24	183	04.11.09 05:08	22.01.10 00:43

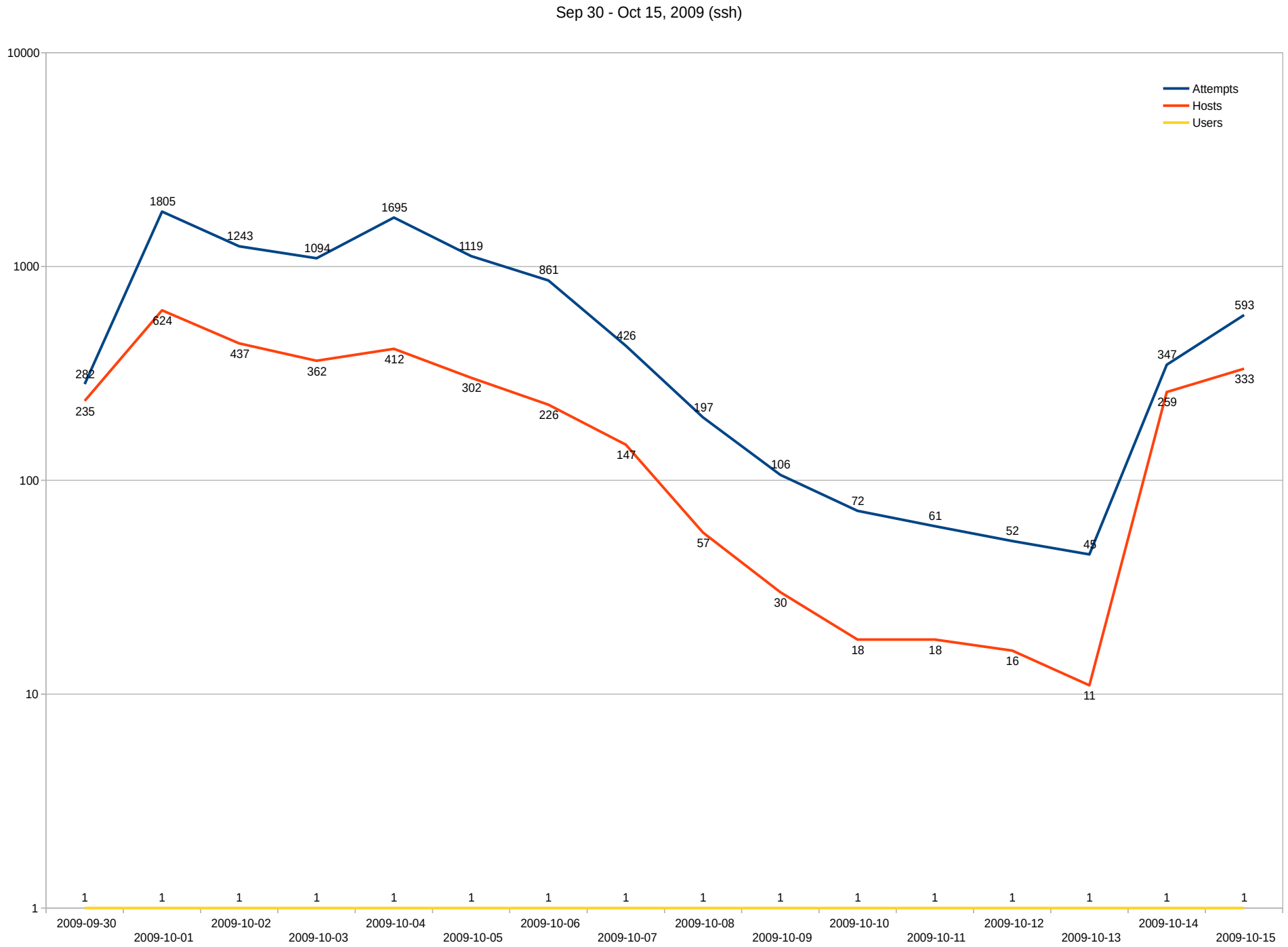
Full list at http://home.nuug.no/~peter/passwords14/2009sept30/gropers_ranked.csv

2009-09-30 21:15:36 - 2009-10-15 13:42:07

Top 1 user IDs (of 1):

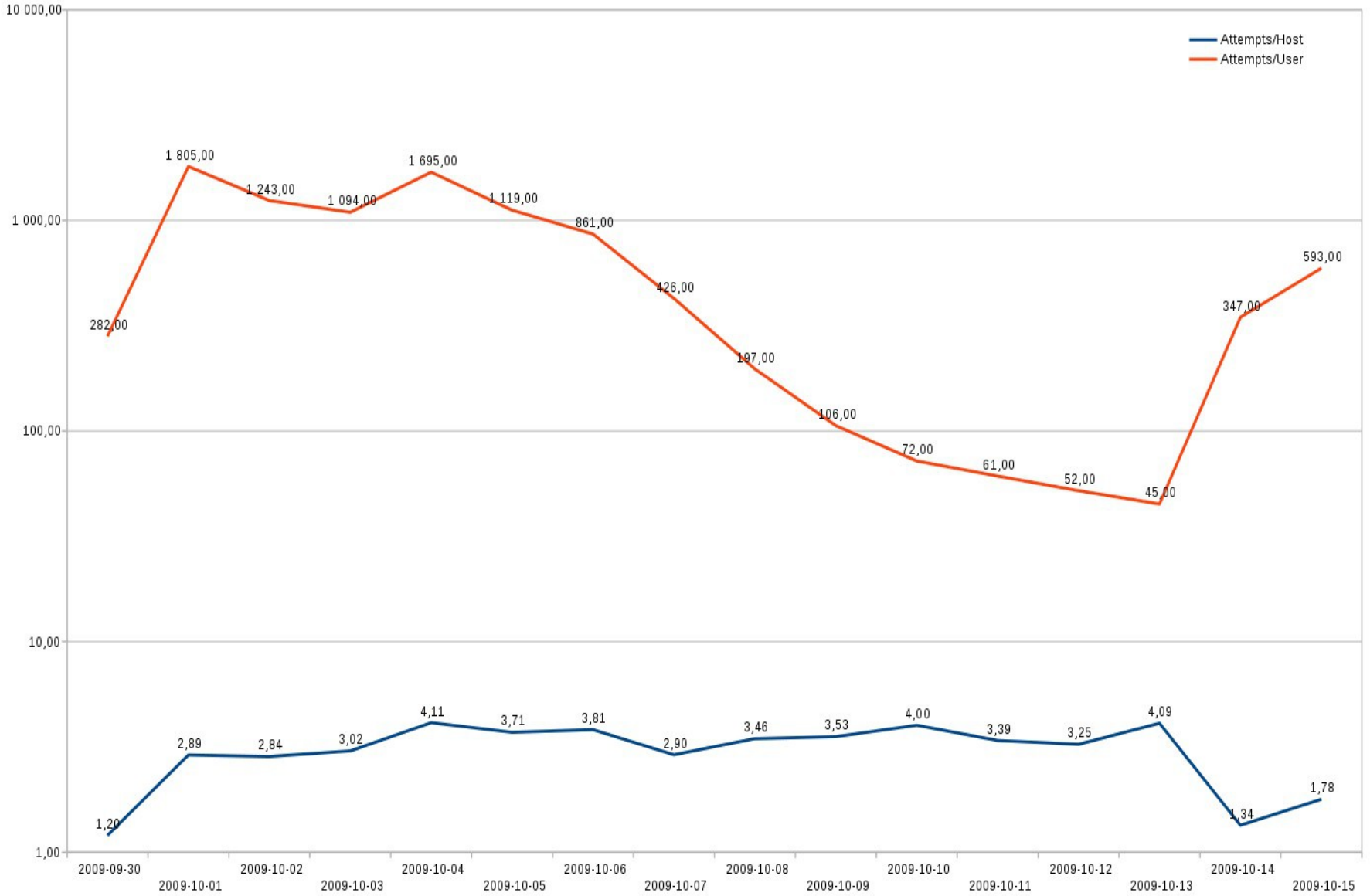
Attempts	User ID
9998	root

Full list at http://home.nuug.no/~peter/passwords14/2009sept30/groped-users-by-frequency.txt


Sep 30 - Oct 15, 2009 (ssh)
10000
1000
100
10
1
Attempts
Hosts
Users
282
1805
1243
1094
1695
1119
861
426
197
106
72
61
52
45
347
593
235
624
437
362
412
302
226
147
57
30
18
18
16
11
259
333
1
2009-09-30
2009-10-01
2009-10-02
2009-10-03
2009-10-04
2009-10-05
2009-10-06
2009-10-07
2009-10-08
2009-10-09
2009-10-10
2009-10-11
2009-10-12
2009-10-13
2009-10-14
2009-10-15

Sep 30 - Oct 15, 2009

Averages



2009-10-28 23:58:35 - 2010-01-22 09:56:24

Top ten host names (of 6209)

Attempts	Host	User Names	First Seen	Last Seen
88	211.154.254.120	1	2009-10-01 09:04	2009-10-15 11:45
80	61.131.208.44	1	2009-10-01 00:29	2009-10-15 13:20
69	219.134.65.39	1	2009-09-30 21:41	2009-10-15 11:04
66	www.pbs-hosting.net	1	2009-09-30 22:53	2009-10-10 10:04
62	rl80.1blu.de	1	2009-10-01 06:05	2009-10-12 09:41
61	189-112-076-005.static.ctbctelecom.com.br	1	2009-10-01 17:13	2009-10-15 07:34
55	static-71-242-245-111.phlapa.east.verizon.net	1	2009-09-30 21:29	2009-10-15 11:50
55	bcl02861.empresas.ya.com	1	2009-10-01 14:28	2009-10-09 11:48
54	218.248.69.185	1	2009-10-01 09:46	2009-10-15 08:58
51	222.210.17.151	1	2009-10-01 04:12	2009-10-15 12:10

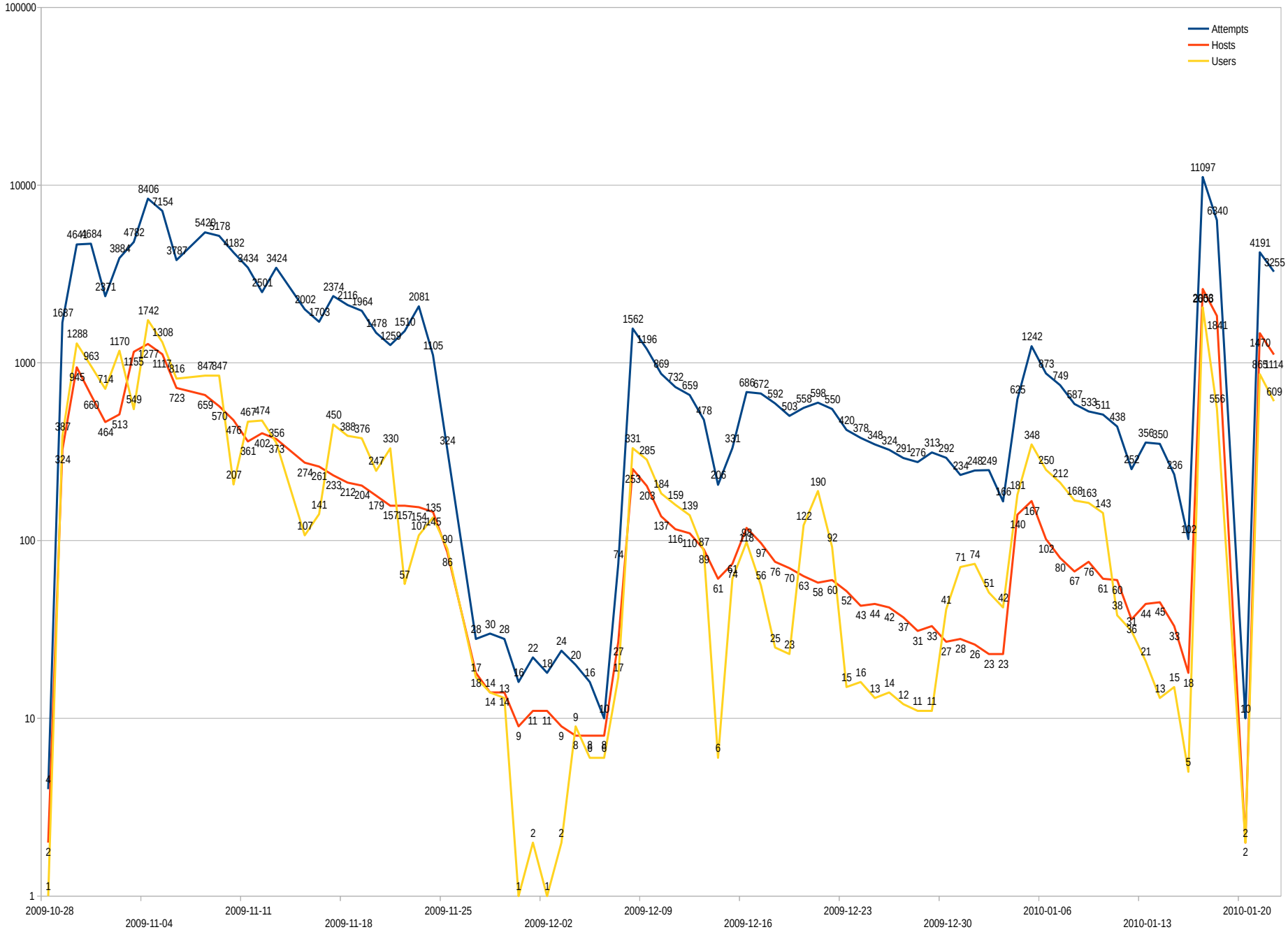
Full list at http://home.nuug.no/~peter/passwords14/2009Oct28/gropers_ranked.csv

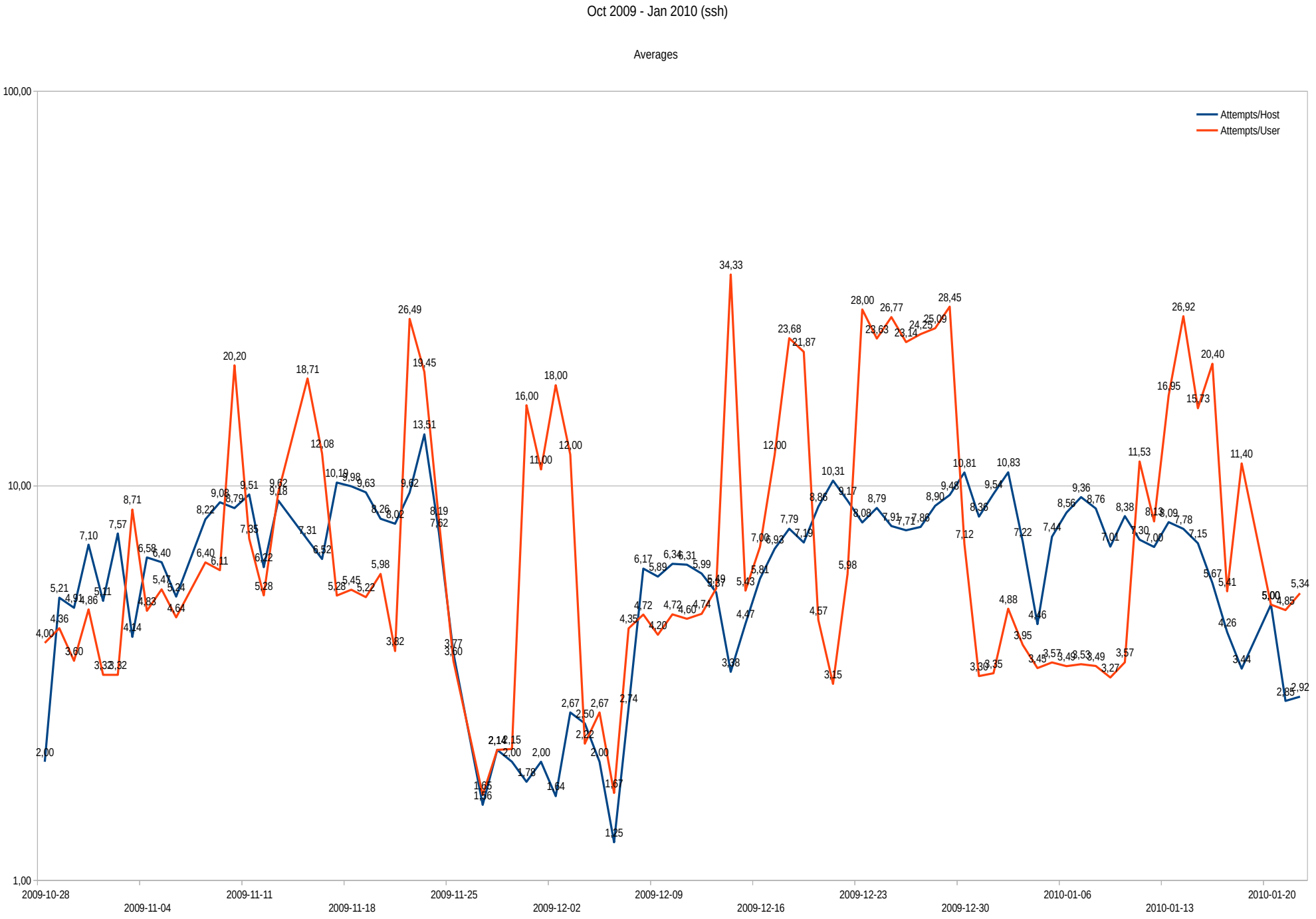
2009-10-28 23:58:35 - 2010-01-22 09:56:24

Top ten user IDs (of 8110)

Attempts	User ID
4309	root
654	admin
360	test
234	mysql
223	student
215	postgres
194	oracle
186	user
181	backup
168	ftp

Full list at http://home.nuug.no/~peter/passwords14/2009Oct28/groped-users-by-frequency.txt


Oct 2009 - Jan 2010 (ssh)
Attempts
Hosts
Users
100000
10000
1000
100
10
1
2009-10-28
2009-11-04
2009-11-11
2009-11-18
2009-11-25
2009-12-02
2009-12-09
2009-12-16
2009-12-23
2009-12-30
2010-01-06
2010-01-13
2010-01-20


Oct 2009 - Jan 2010 (ssh)
Averages
Attempts/Host
Attempts/User
100,00
10,00
1,00
2009-10-28
2009-11-04
2009-11-11
2009-11-18
2009-11-25
2009-12-02
2009-12-09
2009-12-16
2009-12-23
2009-12-30
2010-01-06
2010-01-13
2010-01-20

2010-06-17 01:55:34 - 2010-08-11 13:23:01

Top ten hosts (of 6262):

Attempts	Host	User Names	First Seen	Last Seen
131	58.247.222.163	63	2010-06-17 06:19	2010-07-27 19:16
113	220.178.16.99	56	2010-06-18 18:10	2010-08-11 06:09
111	74.63.208.18	55	2010-06-18 09:01	2010-07-24 11:31
111	202.109.115.169	57	2010-06-17 14:35	2010-08-10 19:23
107	220.178.16.98	54	2010-06-17 03:25	2010-08-10 19:59
107	114.247.18.6	51	2010-06-17 14:14	2010-07-27 19:30
98	59.40.182.68	50	2010-06-17 17:12	2010-08-11 01:18
95	202.116.160.171	47	2010-06-17 16:09	2010-08-11 03:56
93	123.127.150.200	47	2010-06-17 11:11	2010-08-10 07:08
92	200.171.178.213	45	2010-06-17 07:45	2010-07-27 08:55

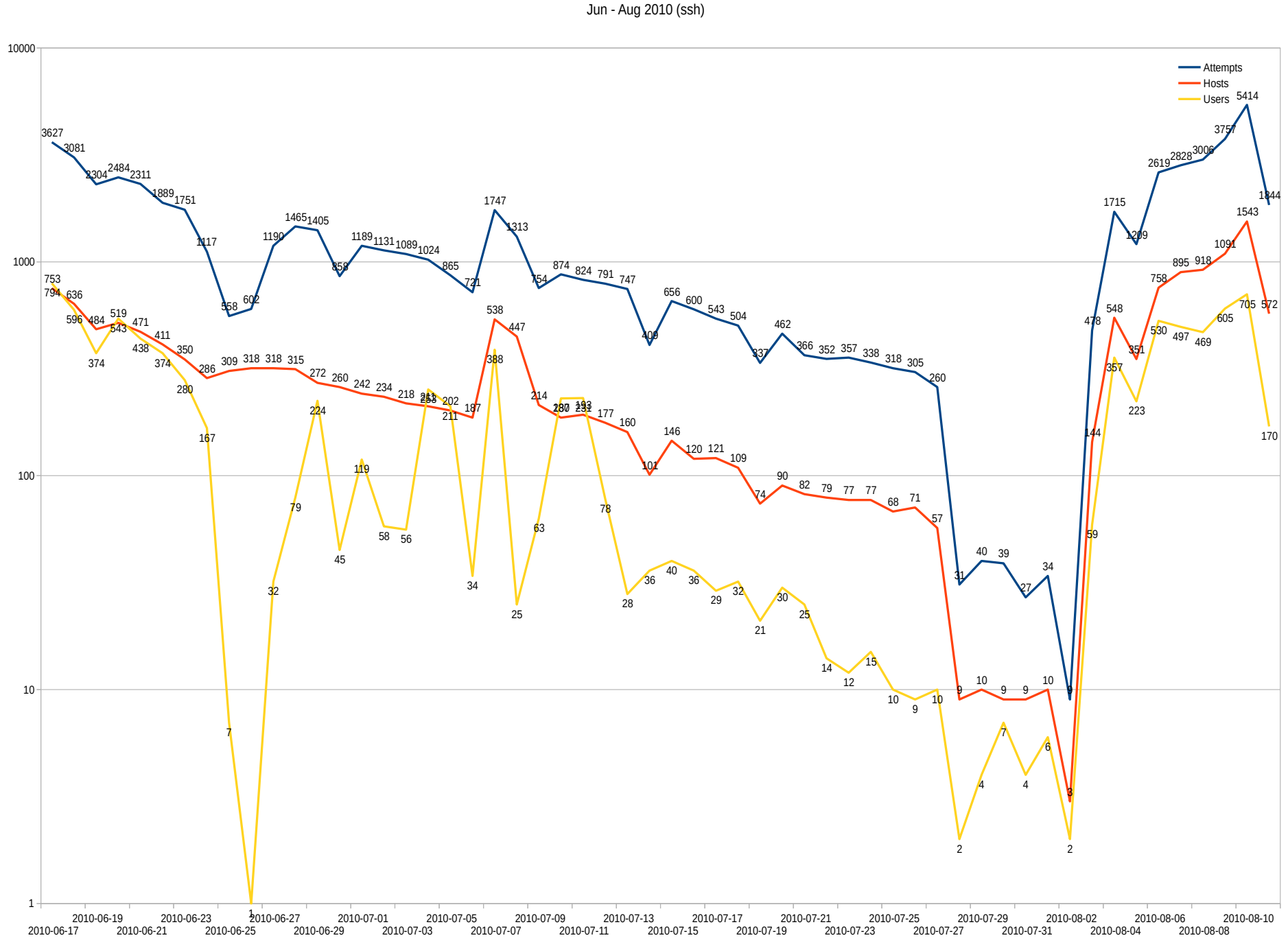
Full list at http://home.nuug.no/~peter/passwords14/hailmary-2010-06/gropers_ranked.csv

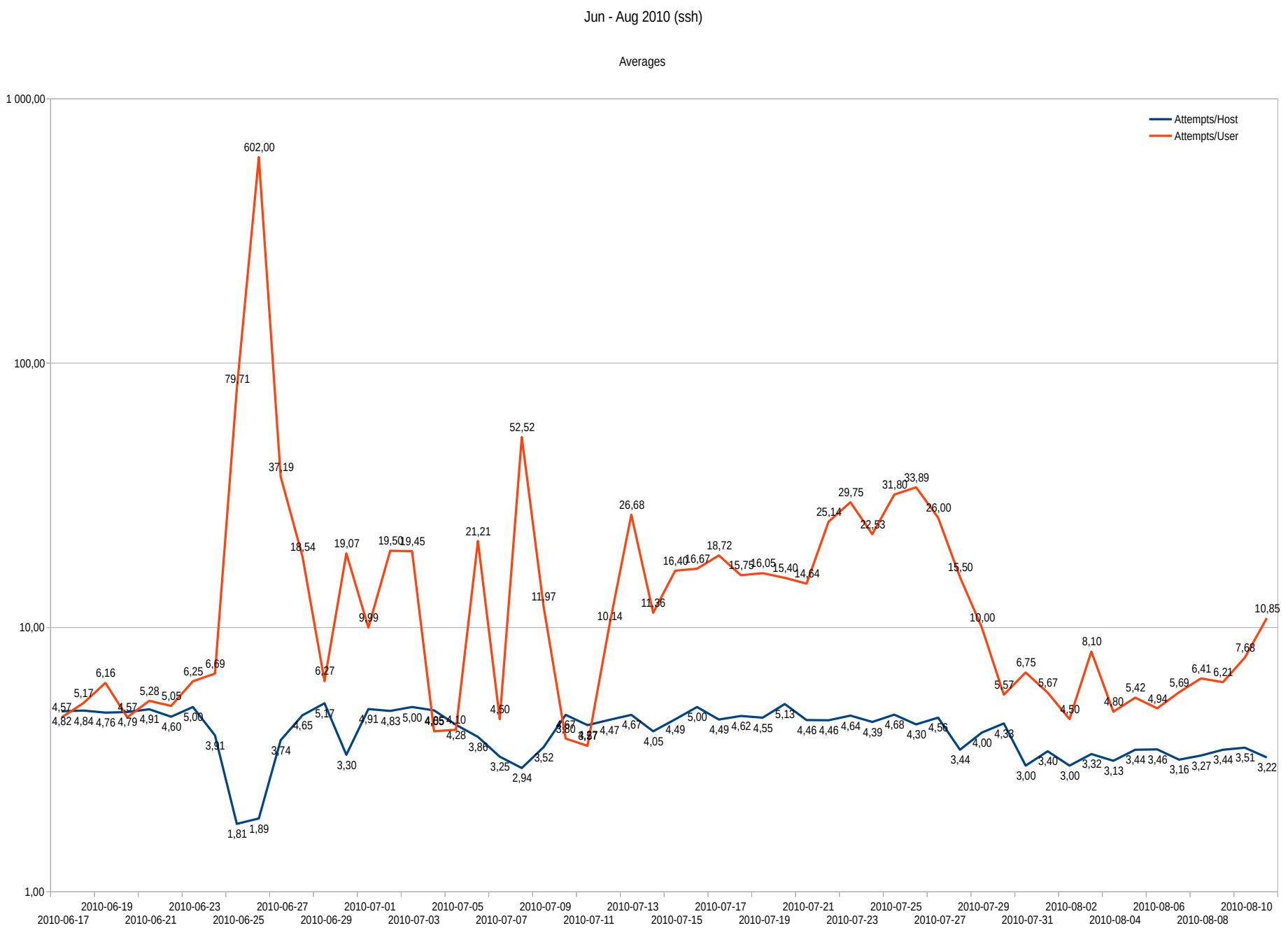
2010-06-17 01:55:34 - 2010-08-11 13:23:01

Top ten user IDs (of 3887):

Attempts	User ID
2727	root
470	admin
231	test
151	testuser
142	student
138	user
133	postgres
131	oracle
128	test1
128	mysql

Full list at http://home.nuug.no/~peter/passwords14/hailmary-2010-06/groped-users-by-frequency.txt


Jun - Aug 2010 (ssh)
Attempts
Hosts
Users
10000
1000
100
10
1
2010-06-17
2010-06-19
2010-06-21
2010-06-23
2010-06-25
2010-06-27
2010-06-29
2010-07-01
2010-07-03
2010-07-05
2010-07-07
2010-07-09
2010-07-11
2010-07-13
2010-07-15
2010-07-17
2010-07-19
2010-07-21
2010-07-23
2010-07-25
2010-07-27
2010-07-29
2010-07-31
2010-08-02
2010-08-04
2010-08-06
2010-08-08
2010-08-10


Jun - Aug 2010 (ssh)
Averages
Attempts/Host
Attempts/User
1 000,00
100,00
10,00
1,00
2010-06-17
2010-06-19
2010-06-21
2010-06-23
2010-06-25
2010-06-27
2010-06-29
2010-07-01
2010-07-03
2010-07-05
2010-07-07
2010-07-09
2010-07-11
2010-07-13
2010-07-15
2010-07-17
2010-07-19
2010-07-21
2010-07-23
2010-07-25
2010-07-27
2010-07-29
2010-07-31
2010-08-02
2010-08-04
2010-08-06
2010-08-08
2010-08-10

2011-10-23 04:13:00 - 2011-10-29 05:40:07

Top ten hosts (of 369):

Attempts	Host	User Names	First Seen	Last Seen
143	109.237.210.147	36	2011-10-23 05:17	2011-10-29 05:40
126	85.22.60.6	45	2011-10-23 04:40	2011-10-29 05:35
122	69.162.65.138	26	2011-10-23 04:47	2011-10-29 05:20
113	69.162.70.2	35	2011-10-23 06:08	2011-10-29 05:22
102	190.152.145.53	30	2011-10-23 04:15	2011-10-29 04:04
101	88.191.89.25	27	2011-10-23 04:20	2011-10-29 05:28
92	118.122.179.71	29	2011-10-23 07:52	2011-10-29 04:58
88	69.162.119.162	33	2011-10-23 05:06	2011-10-29 04:57
86	91.191.170.146	14	2011-10-23 05:24	2011-10-28 08:20
85	61.31.204.90	21	2011-10-23 07:39	2011-10-29 04:46

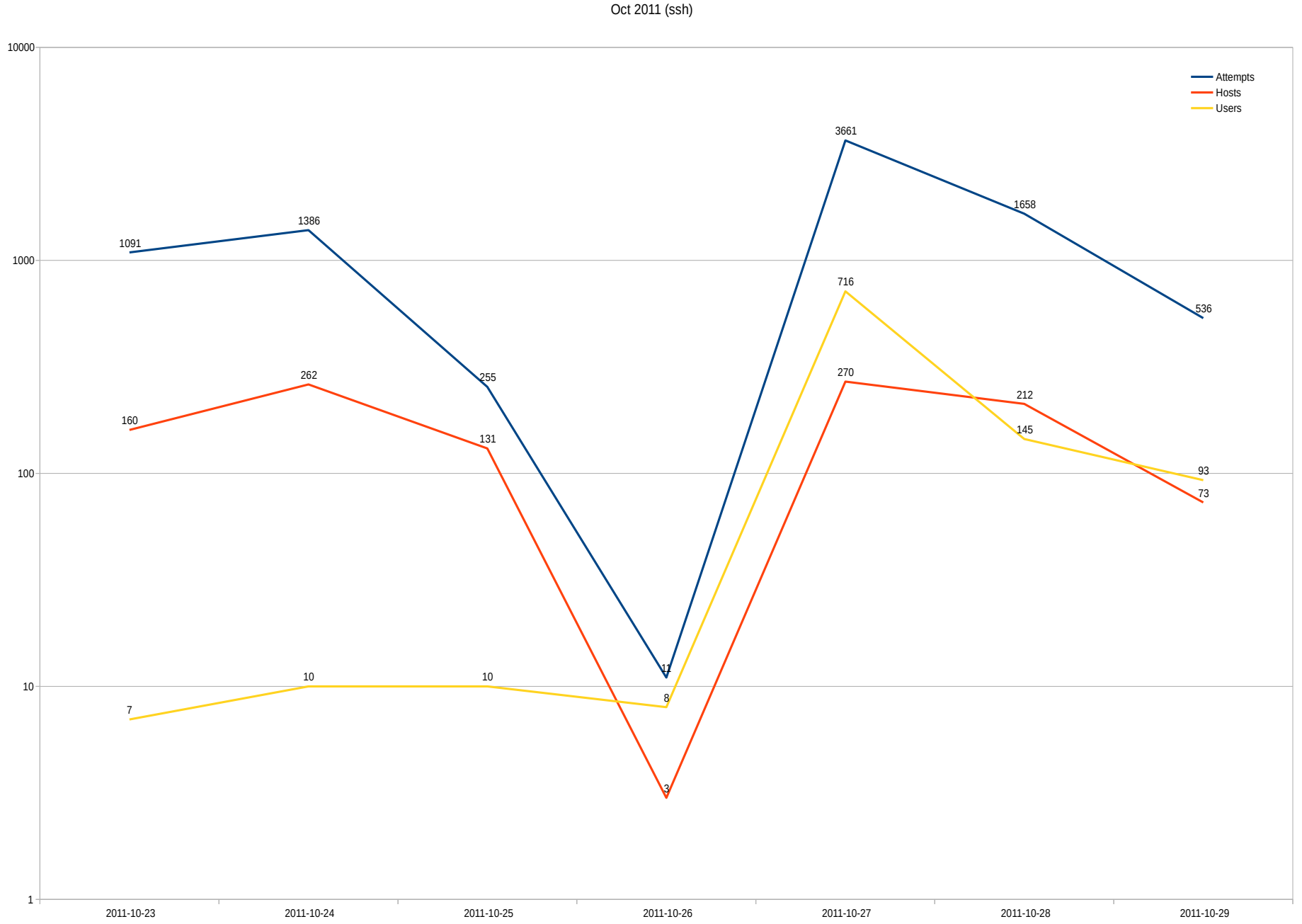
Full list at http://home.nuug.no/~peter/passwords14/hailmary/2011-10/gropers_ranked.csv

2011-10-23 04:13:00 - 2011-10-29 05:40:07

Top ten user IDs (of 944):

Attempts	User ID
3321	root
41	admin
26	test
16	mysql
15	info
13	testuser
11	user
9	sshd
8	www

Full list at http://home.nuug.no/~peter/passwords14/hailmary/2011-10/groped-users-by-frequency.txt


Oct 2011 (ssh)
10000
1000
100
10
1
Attempts
Hosts
Users
1091
1386
255
11
3661
1658
536
160
262
131
3
270
212
73
7
10
10
8
716
145
93
2011-10-23
2011-10-24
2011-10-25
2011-10-26
2011-10-27
2011-10-28
2011-10-29


Oct 2011 (ssh)
Averages
1 000,00
100,00
10,00
1,00
Attempts/Host
Attempts/User
155,86
138,60
25,50
1,38
6,82
5,29
1,95
3,67
13,56
7,82
7,34
5,11
11,43
5,76
2011-10-23
2011-10-24
2011-10-25
2011-10-26
2011-10-27
2011-10-28
2011-10-29

2011-11-03 20:56:18 - 2011-11-26 17:42:19

Top ten hosts (of 290):

Attempts	Host	User Names	First Seen	Last Seen
347	69.162.70.2	168	2011-11-03 20:56	2011-11-23 15:07
229	221.224.13.25	109	2011-11-06 07:13	2011-11-23 14:44
204	210.42.35.1	96	2011-11-06 06:44	2011-11-23 13:28
177	60.28.199.166	89	2011-11-06 08:46	2011-11-23 14:39
144	118.97.50.11	72	2011-11-06 06:48	2011-11-19 14:33
142	189.14.99.226	72	2011-11-04 20:03	2011-11-23 09:12
138	148.244.65.25	69	2011-11-06 06:47	2011-11-23 12:22
131	222.122.45.110	63	2011-11-06 06:58	2011-11-19 19:18
128	65.161.248.26	61	2011-11-06 07:41	2011-11-18 23:44
128	219.240.36.110	62	2011-11-06 07:32	2011-11-21 03:29

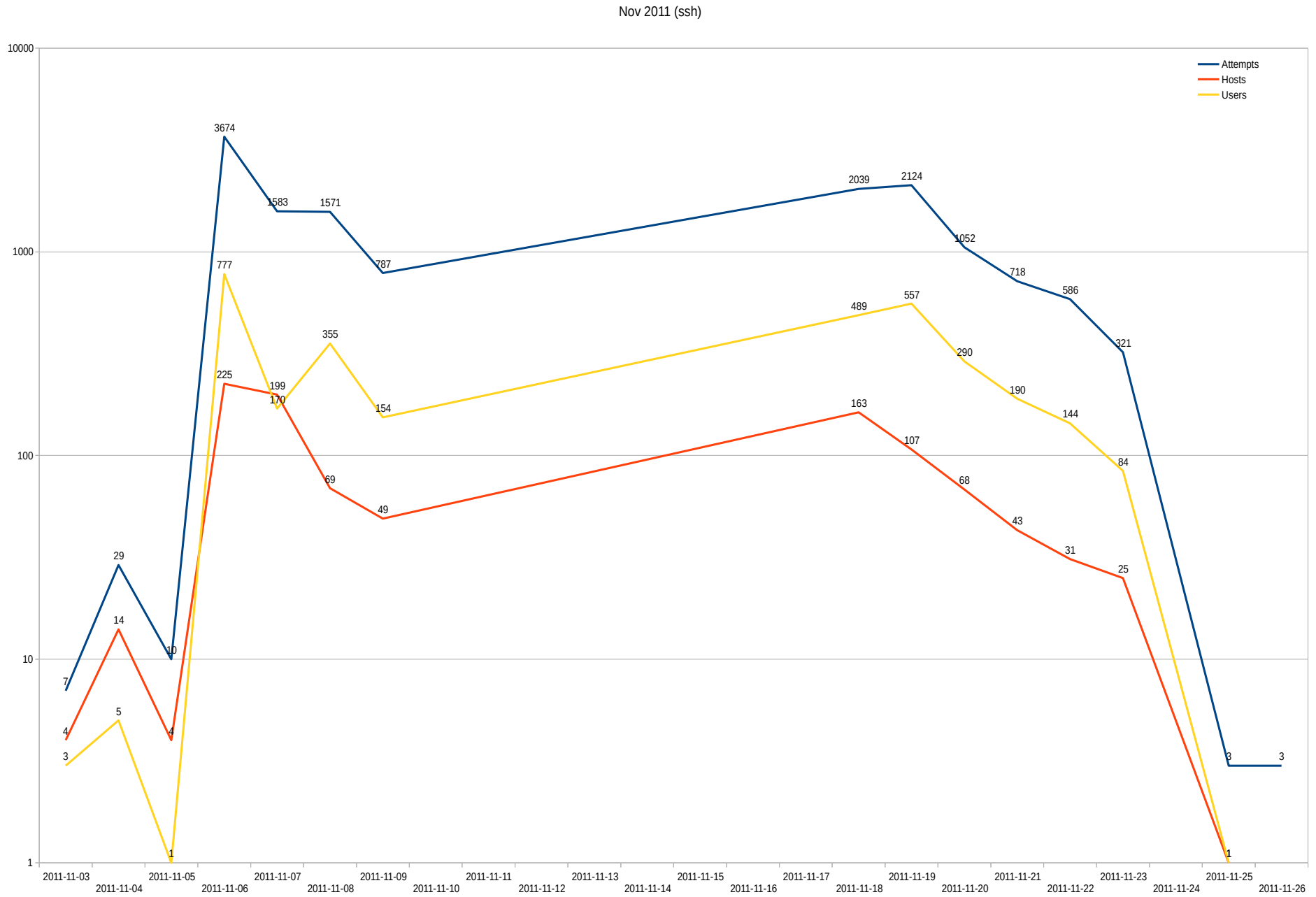
Full list at http://home.nuug.no/~peter/passwords14/hailmary/2011-11-combined/gropers_ranked.csv

2011-11-03 20:56:18 - 2011-11-26 17:42:19

Top ten user IDs (of 2474):

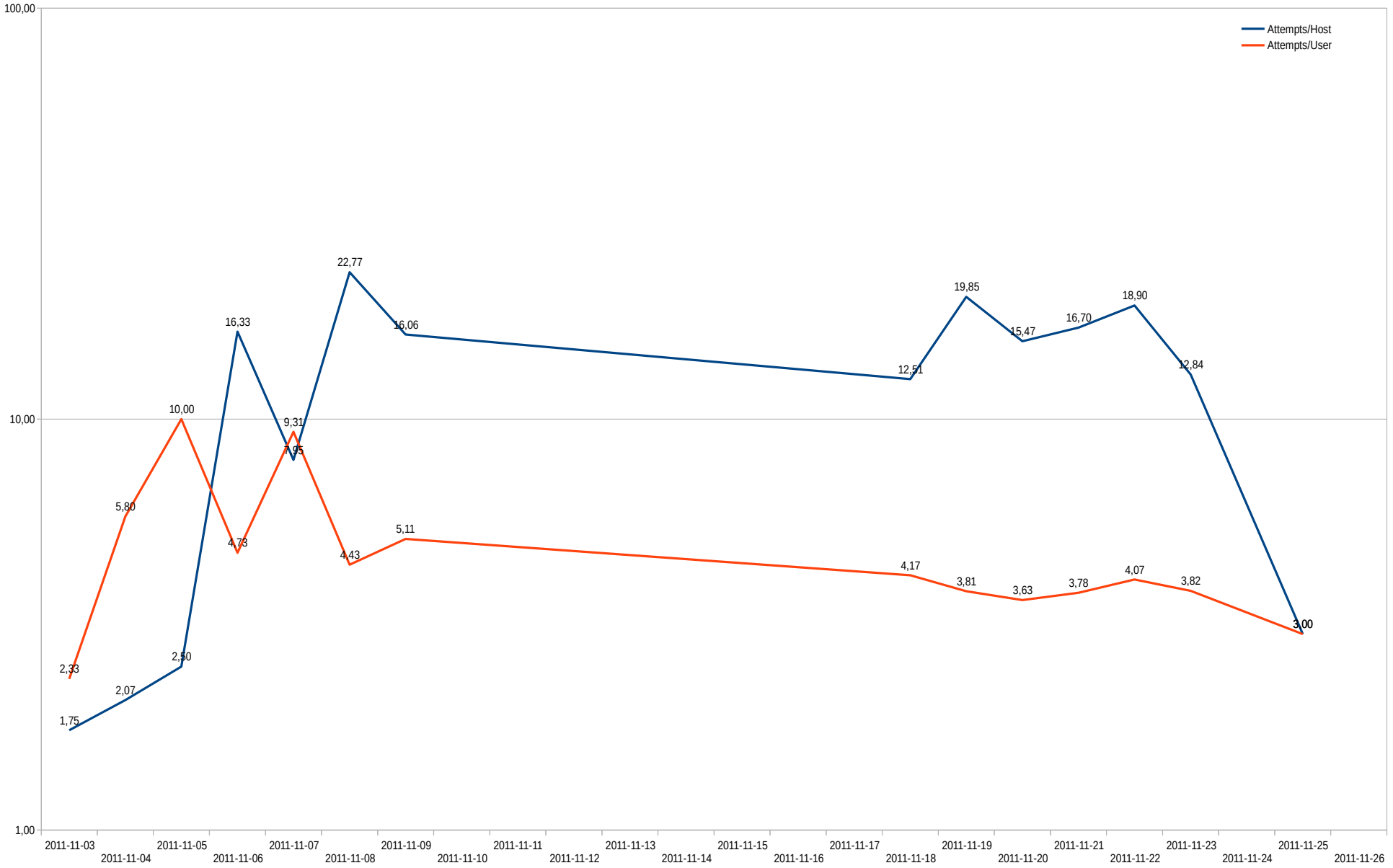
Attempts	User ID
633	root
152	admin
47	ftp
46	info
35	guest
25	apache
23	alex
22	backup
20	mysql
19	ftpuser

Full list at http://home.nuug.no/~peter/passwords14/hailmary/2011-11-combined/groped-users-by-frequency.txt


Nov 2011 (ssh)
Attempts
Hosts
Users
10000
1000
100
10
1
2011-11-03
2011-11-04
2011-11-05
2011-11-06
2011-11-07
2011-11-08
2011-11-09
2011-11-10
2011-11-11
2011-11-12
2011-11-13
2011-11-14
2011-11-15
2011-11-16
2011-11-17
2011-11-18
2011-11-19
2011-11-20
2011-11-21
2011-11-22
2011-11-23
2011-11-24
2011-11-25
2011-11-26
7
29
10
3674
1583
1571
787
2039
2124
1052
718
586
321
3
3
4
14
4
225
199
69
49
163
107
68
43
31
25
1
3
5
1
777
355
154
489
557
290
190
144
84
1

Nov 2011 (ssh)

Averages



2012-04-01 12:33:04 - 2012-04-06 14:52:11

Top ten hosts (of 23):

Attempts	Host	User Names	First Seen	Last Seen
3597	58.214.5.51	1030	2012-04-01 12:33	2012-04-03 00:36
868	61.160.76.123	45	2012-04-01 12:33	2012-04-02 17:56
30	58.51.95.75	4	2012-04-01 22:04	2012-04-01 22:05
24	59.60.7.111	1	2012-04-03 09:52	2012-04-06 05:52
17	212.22.171.6	9	2012-04-05 21:15	2012-04-05 21:30
15	91.197.131.24	4	2012-04-05 20:22	2012-04-05 20:22
15	69.60.116.73	8	2012-04-04 17:11	2012-04-04 17:12
15	60.174.65.242	6	2012-04-05 14:04	2012-04-05 14:11
15	221.182.2.16	6	2012-04-02 18:46	2012-04-02 18:47
15	218.108.224.84	2	2012-04-05 11:27	2012-04-05 11:28

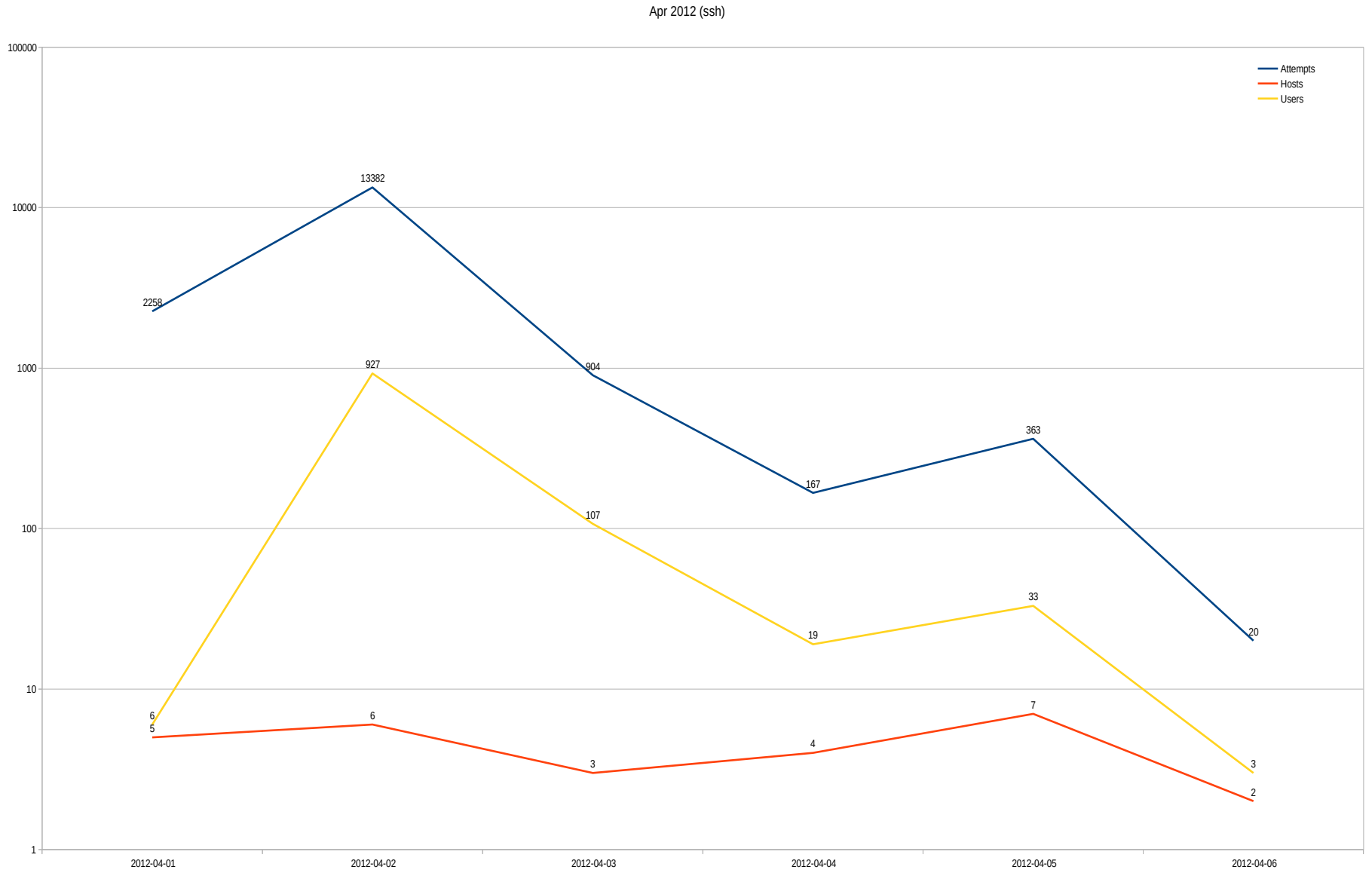
Full list at http://home.nuug.no/~peter/passwords14/hailmary/2012-04/gropers_ranked.csv

2012-04-01 12:33:04 - 2012-04-06 14:52:11

Top ten user IDs (of 1081):

Attempts	User ID
1182	root
54	bin
16	user1
16	user
16	uselman
16	up2date
16	unix
16	u
16	ts
16	trix

Full list at http://home.nuug.no/~peter/passwords14/hailmary/2012-04/groped-users-by-frequency.txt


Apr 2012 (ssh)
100000
10000
1000
100
10
1
Attempts
Hosts
Users
2258
13382
904
167
363
20
6
927
107
19
33
3
5
6
3
4
7
2
2012-04-01
2012-04-02
2012-04-03
2012-04-04
2012-04-05
2012-04-06


Apr 2012 (ssh)
Averages
10 000,00
1 000,00
100,00
10,00
1,00
Attempts/Host
Attempts/User
451,60
2 230,33
301,33
41,75
51,86
10,00
376,33
14,44
8,45
8,79
11,00
6,67
2012-04-01
2012-04-02
2012-04-03
2012-04-04
2012-04-05
2012-04-06

2014-07-08 00:00:53 - 2014-11-24 11:50:05

Top ten hosts (of 984):

Attempts	Host	User Names	First Seen	Last Seen
1007	isis.vdsinside.com	632	2014-09-06 19:01	2014-09-26 19:00
178	host-92-44-17-43.reverse.superonline.net	154	2014-08-29 15:00	2014-08-31 01:01
152	46.149.111.57	145	2014-09-07 18:01	2014-09-25 10:01
143	46.149.111.58	138	2014-09-06 17:01	2014-09-25 14:00
140	46.149.111.23	134	2014-09-06 17:01	2014-09-25 14:01
137	177.96.247.62.dynamic.adsl.gvt.net.br	8	2014-09-02 10:00	2014-09-02 20:02
135	46.149.111.77	131	2014-09-06 22:00	2014-09-25 14:00
133	46.149.111.21	129	2014-09-06 23:01	2014-09-25 08:00
133	46.149.111.19	129	2014-09-08 05:00	2014-09-25 08:01
132	46.149.111.83	128	2014-09-07 17:00	2014-09-25 00:01

Full list at http://home.nuug.no/~peter/passwords14/pop3gropers/gropers_ranked.csv

2014-07-08 00:00:53 - 2014-11-24 11:50:05

Top ten user IDs (of 3992):

Attempts	User ID
70	admin
65	test
36	sales
34	info
28	renato
28	fonseca
28	dani
27	servidor
26	lia
26	laura

Full list at http://home.nuug.no/~peter/passwords14/pop3gropers/groped-users-by-frequency.txt

Innovation: Stealth

Active only first 2 min of each hour

```
Jul 24 15:00:08 skapet spop3d[26766]: authentication failed: no such user: 5ce830d - ns35.hostinglotus.net (122.155.16.125)
Jul 24 15:00:11 skapet spop3d[4351]: authentication failed: no such user: 6b272a3f - samhain.z8.ru (80.93.62.126)
Jul 24 15:00:47 skapet spop3d[16430]: authentication failed: no such user: 9402e3231 - server.esbi.com.tr (92.42.38.73)
Jul 24 15:01:14 skapet spop3d[32245]: authentication failed: no such user: 6a64fe17e - n22.netmark.pl (188.116.35.5)
Jul 24 15:01:21 skapet spop3d[6908]: authentication failed: no such user: 2d74e83 - server1.ommforhire.com (173.233.93.184)
Jul 24 15:01:25 skapet spop3d[16471]: authentication failed: no such user: annaduraikolcu - 10.183.96.66.static.eigbox.net (66.96.183.10)
Jul 24 15:02:01 skapet spop3d[13654]: authentication failed: no such user: 1adf6645 - p30.progreso.pl (77.79.246.210)
Jul 24 16:00:16 skapet spop3d[25654]: authentication failed: no such user: aleks - fe58.hc.ru (79.174.73.74)
Jul 24 16:00:48 skapet spop3d[25599]: authentication failed: no such user: 55ef390a - 198.154.210.164
Jul 24 16:00:56 skapet spop3d[25360]: authentication failed: no such user: admin - 81.31.150.163
Jul 24 16:01:01 skapet spop3d[30376]: authentication failed: no such user: 8cada7110 - h2136188.stratoserver.net (85.214.43.20)
Jul 24 16:01:35 skapet spop3d[29880]: authentication failed: no such user: anna4ab15f - h2.hosting9000.com (178.33.191.210)
Jul 24 16:01:39 skapet spop3d[28881]: authentication failed: no such user: arran6 - 91.202.171.103
Jul 24 16:02:02 skapet spop3d[20188]: authentication failed: no such user: abtavl - 50.97.161.230-static.reverse.softlayer.com (50.97.161.230)
```

But on the other hand -

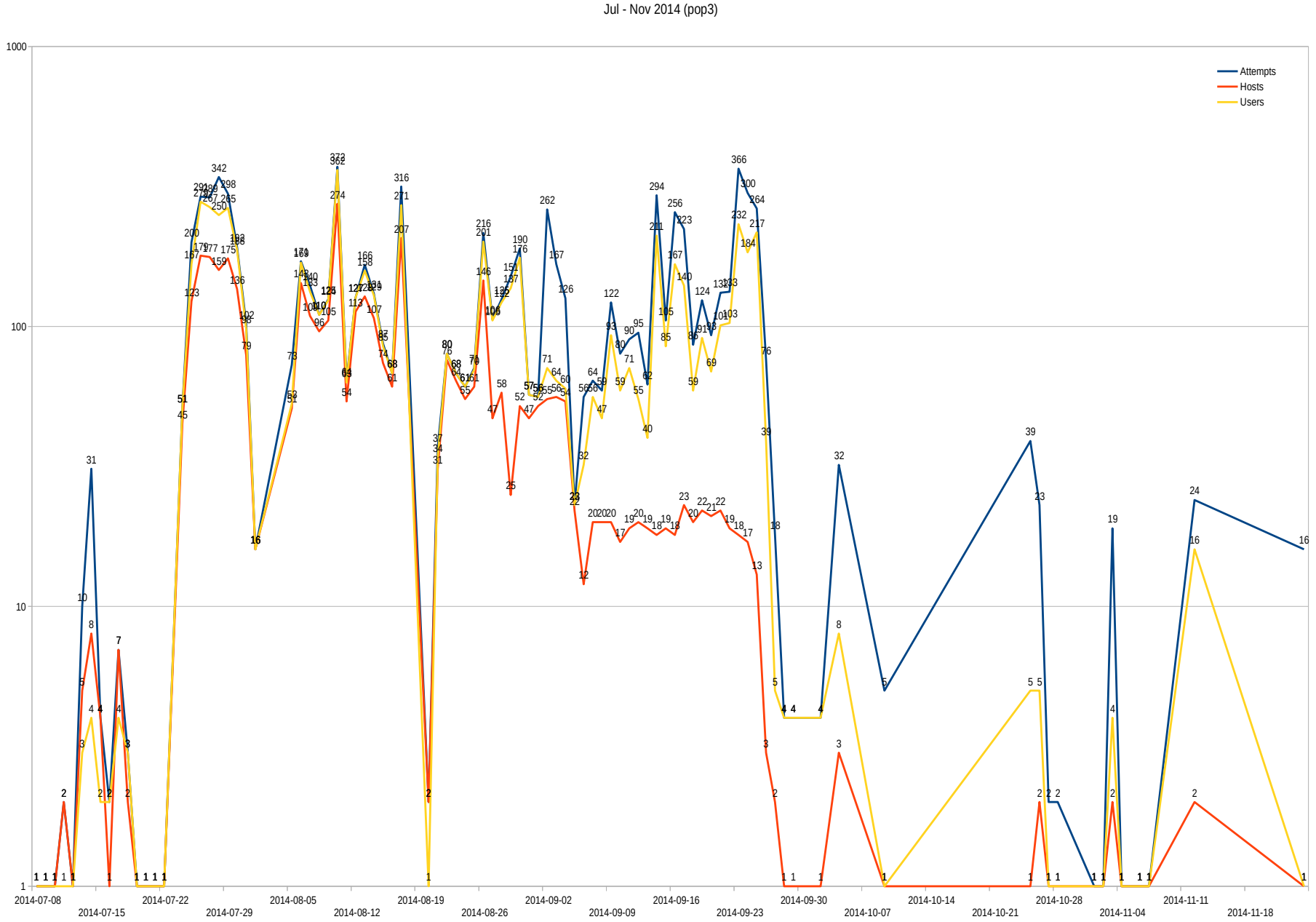
Innvation: List shopping

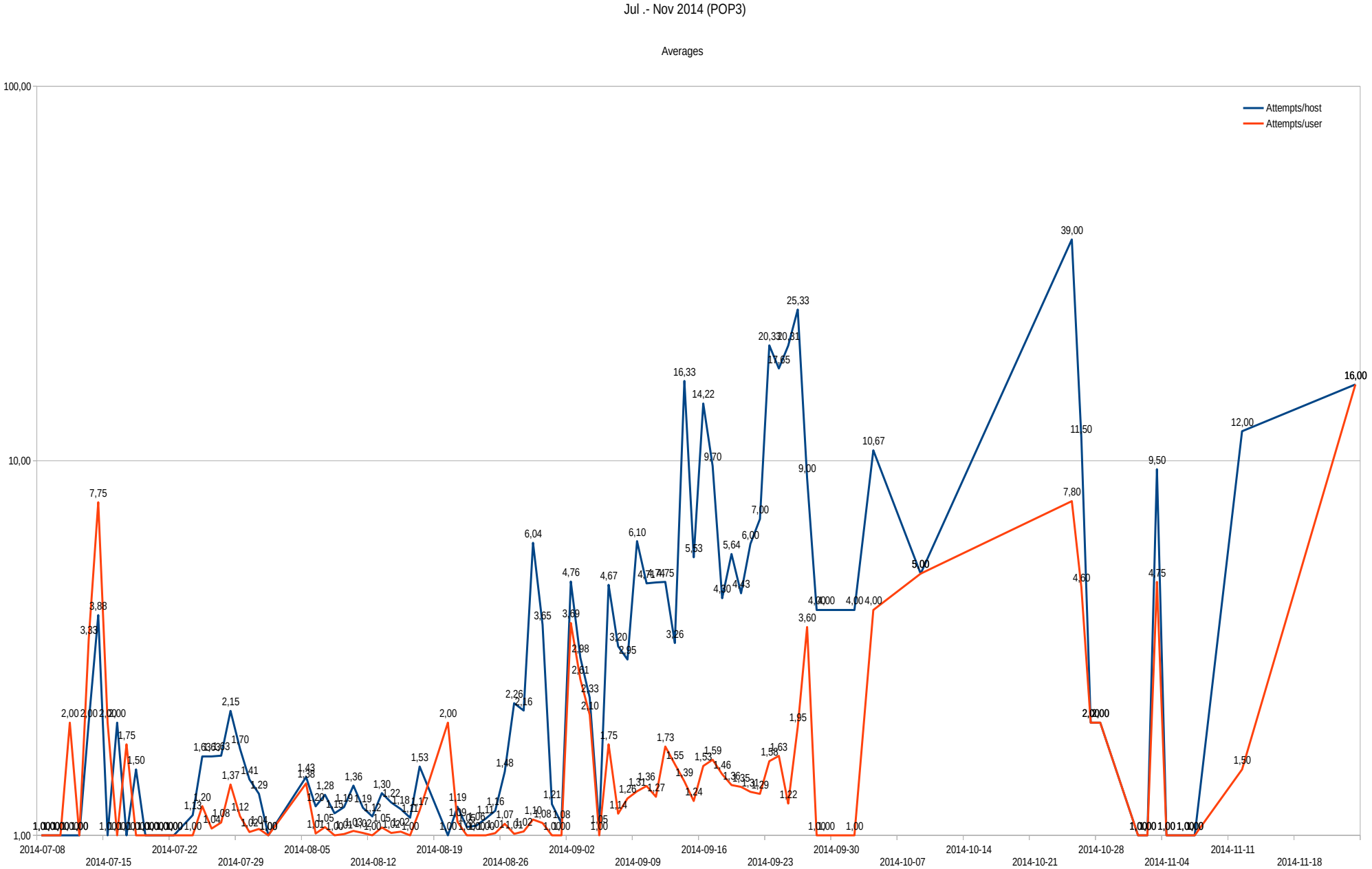
Caveat emptor, 2014 edition:

A large portion of the user names the *pop3gropers* used were the user name parts of my spamtrap list at

http://www.bsdly.net/~peter/traplist.shtml

Which contains my >28,000 *'imaginary friends'*; non-existent spamtrap mail addresses collected mainly from bounces


Jul - Nov 2014 (pop3)
Attempts
Hosts
Users
1000
100
10
1
2014-07-08
2014-07-15
2014-07-22
2014-07-29
2014-08-05
2014-08-12
2014-08-19
2014-08-26
2014-09-02
2014-09-09
2014-09-16
2014-09-23
2014-09-30
2014-10-07
2014-10-14
2014-10-21
2014-10-28
2014-11-04
2014-11-11
2014-11-18

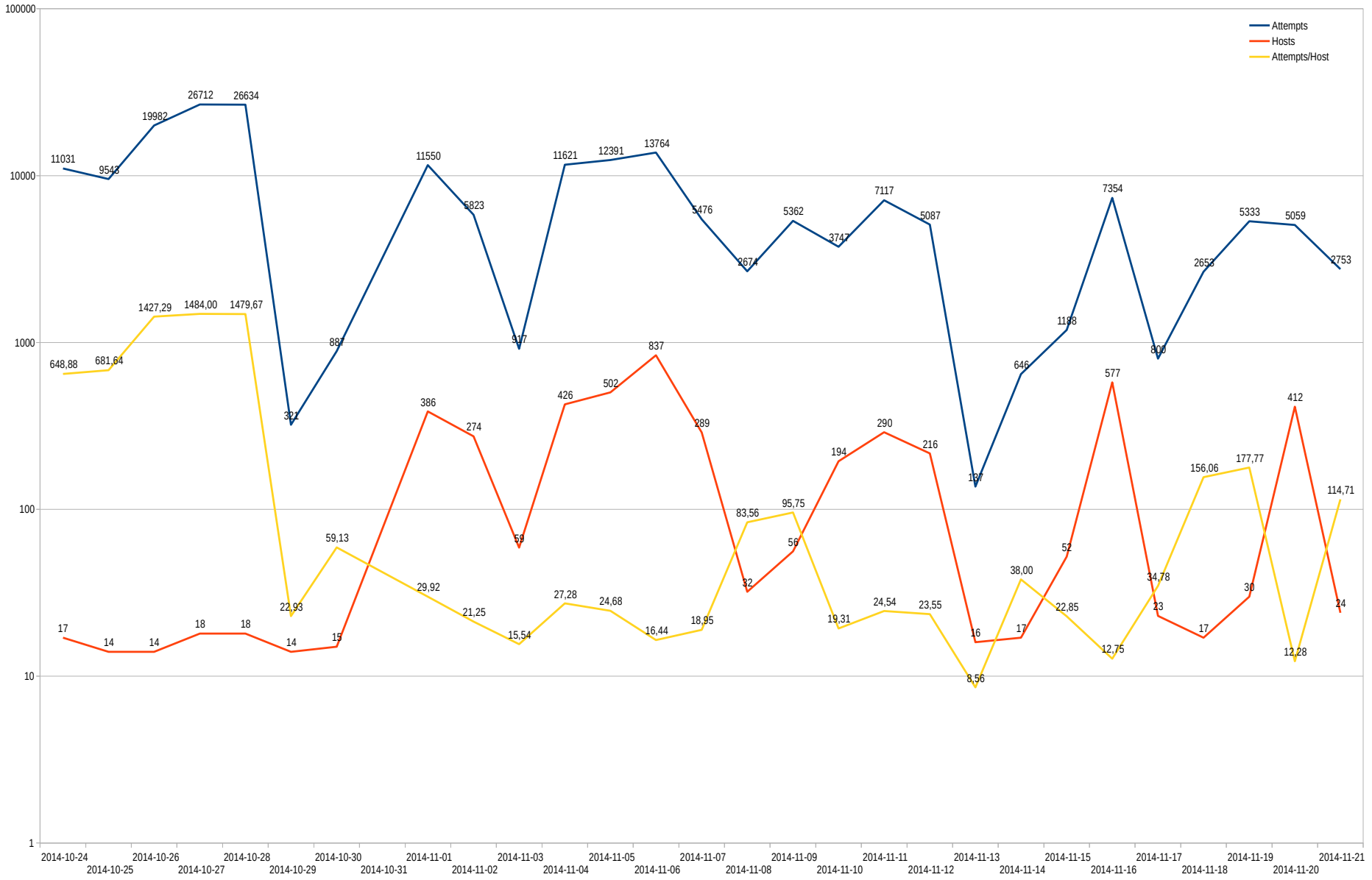

Jul .- Nov 2014 (POP3)
Averages
Attempts/host
Attempts/user
100,00
10,00
1,00
2014-07-08
2014-07-15
2014-07-22
2014-07-29
2014-08-05
2014-08-12
2014-08-19
2014-08-26
2014-09-02
2014-09-09
2014-09-16
2014-09-23
2014-09-30
2014-10-07
2014-10-14
2014-10-21
2014-10-28
2014-11-04
2014-11-11
2014-11-18

2014-10-24 00:00:15 - 2014-11-21 08:10:52

Top 10 (of 2293):

Attempts	Host	First Seen	Last Seen
72953	69.30.245.226	24/10/2014 09:31:09	28/10/2014 13:36:11
6964	80.82.70.134	24/10/2014 00:00:15	20/11/2014 16:13:00
3980	162.248.79.130	28/10/2014 13:26:12	28/10/2014 19:50:34
2340	94.102.49.102	18/11/2014 16:09:48	21/11/2014 11:43:13
2274	93.174.93.10	18/11/2014 15:07:27	21/11/2014 12:56:57
1985	89.248.162.235	18/11/2014 15:10:56	21/11/2014 11:43:45
1726	141.255.167.121	24/10/2014 14:32:58	03/11/14 07:40 PM
1685	93.174.93.204	24/10/2014 00:00:28	02/11/14 12:59 AM
1581	80.82.78.166	24/10/2014 01:07:08	24/10/2014 23:56:12
1444	89.248.174.31	19/11/2014 09:14:20	21/11/2014 12:56:19

Full list at http://home.nuug.no/~peter/passwords14/wordpress-posts/gropers_ranked.csv


Oct - Nov 2014 (WordPress XMLRPC)
Attempts
Hosts
Attempts/Host
100000
10000
1000
100
10
1
11031
9543
19982
26712
26634
321
887
11550
5823
917
11621
12391
13764
5476
2674
5362
3747
7117
5087
197
646
1198
7354
800
2653
5333
5059
2753
648,88
681,64
1427,29
1484,00
1479,67
22,93
59,13
29,92
21,25
15,54
27,28
24,68
16,44
18,95
83,56
95,75
19,31
24,54
23,55
8,56
38,00
22,85
12,75
34,78
23
156,06
177,77
12,28
114,71
17
14
14
18
18
14
15
386
274
59
426
502
837
289
32
56
194
290
216
16
17
52
577
23
17
30
412
24
2014-10-24
2014-10-25
2014-10-26
2014-10-27
2014-10-28
2014-10-29
2014-10-30
2014-10-31
2014-11-01
2014-11-02
2014-11-03
2014-11-04
2014-11-05
2014-11-06
2014-11-07
2014-11-08
2014-11-09
2014-11-10
2014-11-11
2014-11-12
2014-11-13
2014-11-14
2014-11-15
2014-11-16
2014-11-17
2014-11-18
2014-11-19
2014-11-20
2014-11-21

Keep Them Out, Keep Them Guessing

Here, most geeks would wax lyrical about the relative strengths of different encryption schemes and algorithms.

Being a simpler mind, I prefer a different metric for how good your scheme is, or effectivness of obfuscation (also see entropy):

How many bytes does a would-be intruder have to get exactly right?

Authentication method	Number of bytes
Password	Password length (varies, how long is yours?)
Alternate Port	Port number (2 bytes, it's a 16 bit value, remember)
Port Knocking	Number of ports in sequence * 2 (still a 16 bit value)
Single Packet Authentication	2 bytes (the port) plus Max 1440 (IPv4/Ethernet) or 1220 (IPv6/Ethernet)
Key Only	Number of bytes in key (depending on key strength, up to several kB)

You can of course combine several methods (and piss off your users), or use *two factor authentication* (OpenSSH supports several schemes).

Questions?

(if you're not sick of this already)

If you enjoyed this, support OpenBSD!

Buy OpenBSD CDs and other items, donate!

OpenBSD.org Orders Page: http://www.openbsd.org/orders.html

OpenBSD Donations Page: http://www.openbsd.org/donations.html

OpenBSD Hardware Wanted Page: http://www.openbsd.org/want.html

Remember: Free software takes real work and real money to develop and maintain.

If you want to support me, buy the book!

References

These slides at
http://home.nuug.no/~peter/passwords14/

With data:
http://home/nuug.no/~peter/passwords14-talk.zip

Mobin Javed and Vern Paxson, "
Detecting stealthy, distributed SSH brute-forcing ," ACM International Conference on Computer and Communication Security (CCS), November 2013.

References (cont'd)

The blog posts (field notes), data links within:

Peter N. M. Hansteen, (2008-12-02) A low intensity, distributed bruteforce attempt (slashdotted)

Peter N. M. Hansteen, (2008-12-06) A Small Update About The Slow Brutes

Peter N. M. Hansteen, (2008-12-21) Into a new year, slowly pounding the gates (slashdotted)

Peter N. M. Hansteen, (2009-01-22) The slow brutes, a final roundup

Peter N. M. Hansteen, (2009-04-12) The slow brute zombies are back (slashdotted)

Peter N. M. Hansteen, (2009-10-04) A Third Time, Uncharmed (slashdotted)

Peter N. M. Hansteen, (2009-11-15) Rickrolled? Get Ready for the Hail Mary Cloud! (slashdotted)

Peter N. M. Hansteen, (2011-10-23) You're Doing It Wrong, Or, The Return Of The Son Of The Hail Mary Cloud

Peter N. M. Hansteen, (2011-10-29) You're Doing It Wrong, Returning Scoundrels

Peter N. M. Hansteen, (2012-04-06) If We Go One Attempt Every Ten Seconds, We're Under The Radar (slashdotted)

Peter N. M. Hansteen, (2012-04-11) Why Not Use Port Knocking?

Peter N. M. Hansteen, (2013-02-16) There's No Protection In High Ports Anymore. If Indeed There Ever Was. (slashdotted)

Peter N. M. Hansteen, (2014-08-21) Password Gropers Take the Spamtrap Bait (slashdotted)

References (cont'd)

Other Useful Texts

Marcus Ranum: The Six Dumbest Ideas in Computer Security, September 1, 2005

Michael W. Lucas: SSH Mastery, Tilted Windmill Press 2013

Michael W. Lucas: Absolute OpenBSD, 2nd edition No Starch Press 2013

Peter N. M. Hansteen, The Book of PF, 3rd edition, No Starch Press 2013, also the online PF tutorial it grew out of, several formats http://home.nuug.no/~peter/pf/ , more extensive slides at http://home.nuug.no/~peter/pf/newest/

OpenBSDs web http://www.openbsd.org/ -- lots of useful information.