

The Snooper Project
Analysis of speculative probing of non-responsive
IP addresses

Ingvar Mattsson
<ingvar@hexapodia.net>

October 1, 2008

Contents

1	The Snooper Project - background and goal	4
1.1	Brief background	4
1.2	Technical background	4
1.3	The ongoing Snooper Project	4
1.4	Report goal	4
1.5	Thanks	5
1.6	Technical aids	5
2	General observations	6
3	Anomaly detection and analysis	7
3.1	Anomaly detection	7
3.2	Analysis	7
3.3	February 2007	7
3.4	March 2007	8
3.5	April 2007	8
3.6	May 2007	8
3.7	June 2007	8
3.8	July 2007	9
3.9	August 2007	9
3.10	September 2007	9
3.11	October 2007	9
3.12	November 2007	9
3.13	December 2007	10
3.14	January 2008	10
3.15	February 2008	10
3.16	Conclusions	10
4	Graphs	11
5	Statistics	17
5.1	Statistics for 2007-02	17
5.2	Statistics for 2007-03	19
5.3	Statistics for 2007-04	21
5.4	Statistics for 2007-05	23
5.5	Statistics for 2007-06	25
5.6	Statistics for 2007-07	27
5.7	Statistics for 2007-08	29
5.8	Statistics for 2007-09	31
5.9	Statistics for 2007-10	33
5.10	Statistics for 2007-11	35
5.11	Statistics for 2007-12	37
5.12	Statistics for 2008-01	39
5.13	Statistics for 2008-02	41

6	A more detailed look at some active sources	43
6.1	2007-06, 83.27.37.238	43
6.2	2007-06, 77.81.81.83	43
6.3	2007-06, 217.147.224.66	44
6.4	2007-09, 219.148.119.11	55
7	The date/protocol/port list	58
7.1	2007-02	58
7.2	2007-03	58
7.3	2007-04	59
7.4	2007-05	59
7.5	2007-06	59
7.6	2007-07	60
7.7	2007-08	60
7.8	2007-09	61
7.9	2007-10	62
7.10	2007-11	63
7.11	2007-12	64
7.12	2008-01	65
7.13	2008-02	65

1 The Snooper Project - background and goal

1.1 Brief background

The Snooper project is an on-going attempt to get a feel for how anonymous scans are done and how wide-spread they are. It is done by combining a firewall DROP rule and `tcpdump` and by composing statistics for the last 7 days (on a daily basis) and the last 28 days (on a weekly basis).

All packet captures are kept, for long-term analysis, and this paper will present the results from analysing packets from 2007-02-05 to 2008-02-29.

1.2 Technical background

The packet capture is done on a linux machine, with a secondary IP address on one of the interfaces, then using iptables firewall rules as follows (the IP address of the snooper virtual IP is kept as the SNOOP shell variable).

```
iptables -A INPUT -d $SNOOP -j DROP
iptables -A INPUT -s $SNOOP -j DROP
iptables -A OUTPUT -s $SNOOP -j DROP
```

The linux machine is hosted on an ADSL connection, this may influence the probe pattern seen.

The actual packet capture is accomplished by using `tcpdump`, capturing a set number of packets¹ for each capture file, then restarting `tcpdump`. This allows for fairly accurate timestamping of capture files (each capture file is named after the start date and time, like 2008-08-07T17:57:45).

1.3 The ongoing Snooper Project

The continuously rolling Snooper Project² prepares retrospective reports for the last seven days every night and a 28-day retrospective every Friday.

The data analysis is written completely in Common Lisp, using my PCAP-reading library³ to read the PCAP data files generated by `tcpdump`.

These are eventually archived in a semi-manual fashion. There is a script to do the archiving, but the script is run manually. This report has been prepared exclusively from long-term archived files.

1.4 Report goal

The intent with this report is to present some aggregate statistics for probing against inactive IP addresses (thus the firewall DROP rules) and correlating these with vulnerability reports, to try to build a picture of how fast a reported vulnerability goes into bulk scanning. I will also present a list of “top ten” sources that I have seen.

I will also have a closer look at some of the more prolific probing hosts to see if any similarities between the patterns they exhibit can be found.

¹currently 100 packets

²<http://www.hexapodia.net/snooper/>

³<http://src.hexapodia.net/pcap.tar.gz>

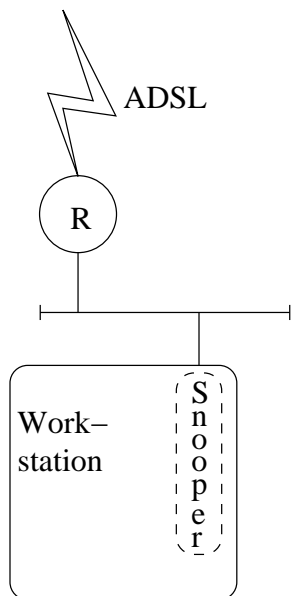


Table 1: Brief sketch of the Snooper Project network

The Snooper network lives on a 'business-grade' ADSL network, the ADSL router is marked as "R" in the image, with the network and virtual snooper interface connected by Ethernet.

There are some obvious weaknesses with the data collection. The collector machine has changed IP address (and ISP) three times during the data collection period, though this doesn't seem to have caused a massive discrepancy in the port spread (it's certainly had an effect on the raw number of packets received each day, though). The actual connection is a 'business-grade ADSL', rather than being housed in a data centre⁴.

A lot of the analysis (especially the correlation with vulnerability reports) is done manually and may well miss some reports, but I try to be thorough.

1.5 Thanks

I extend my thanks to James E. Prewett, John Sim, Brian Nisbet, Richard Bryant, Aidan Burrows, Peter van Eynde and Richard Clayton for agreeing to read and comment on early revisions of this report.

1.6 Technical aids

In preparing this report, I have used \LaTeX for the document preparation, GNU Emacs as the primary editor, SBCL and SLIME as my code development environment, Gnuplot for some graphing needs, Wireshark for quick looks at packet dumps, tcpmerge and tcpdump for quick packet mangling and ImageMagick for image conversions.

⁴However, looking at the most prolific IPs, there is only four instances of another ADSL user with the same ISP appearing on the list

2 General observations

One of the things I was wondering about as I started the Snooper Project was if I would see any probe behaviour at all or if I would only see ICMP ECHO scans. When I quite rapidly started seeing probes both of UDP and TCP ports, I reached the conclusion that ICMP ECHO was essentially irrelevant. However, now that I am looking at more long-ranging statistics, I have had to modify this position slightly.

Most hosts that start with an ICMP scan will send one or two ICMP ECHO and drop off completely when they don't receive a positive response. Some will (see p. 43) both ping-scan and probe for ports. Then there's the high-volume probing hosts that scan and scan and scan... Sometimes in an easily discernable pattern, sometimes in what looks like multiple scan patterns with slightly different periods.

It would be interesting to set up another one (or few) snooper project host(s), on different networks, and see if this pattern holds true on a wider range of hosts. It would also be interesting to see if the same hosts show up as the most prolific sources.

The more prolific (I am almost tempted to say "industrial") probe sources seem to all probe for a small number of ports with associated protocols that have had security problems in the past (HTTP, various SMB ports, MS-RPC).

3 Anomaly detection and analysis

3.1 Anomaly detection

To find times when certain destination ports have suddenly risen in popularity, I have run some trend analyses on the data. The core analytic method is an exponential average that has been calculated on the number of probes per hour. This is done individually for each UDP and TCP port.

Table 2: Exponential average

In the following formula, A is the average (subscript o for the old, subscript n for the new) and N is the number of probes seen in an hour, irrespective of the source.

$$A_n = N + (A_o - N)e^{-1/24}$$

To determine if a specific port is of interest, the number of probes for a given IP protocol and destination port is compared to the moving average and whenever this was higher than 6 and more than twice the moving average⁵, it was flagged as a protocol/port combination to be noted.

3.2 Analysis

The method chosen to try to make sense of these peaks of activity is to try to find vulnerability reports around the time the peak occurs. I have been using BugTraq archives⁶ for this. While it is possible that the use of more than one mailing list may have produced more results, I suspect that BugTraq is good enough.

3.3 February 2007

The anomalies reported in February 2007 are tcp/135, tcp/445, tcp/2967 and tcp/5900.

Looking through the BugTraq archives for this month, we can see that there was a new release of Samba⁷, to plug several vulnerabilities, early in the month. This probably explains the many peaks for tcp/135 and the single peak for tcp/445.

The repeated peaks for tcp/2697 from February 23rd onwards are less easy to explain. However, tcp/2697 is used by the Symantec AV client and there was a vulnerability announced⁸ on February 23rd. Even if the text of the vulnerability report indicated that this was a local-only exploit, it may have prompted attackers to try, anyway.

There is no obvious explanation for tcp/5900 (peaking on February 25th), there was a report of a DoS vulnerability in one VNC client⁹, but this doesn't

⁵It is probably of interest that the number of day/protocol/port tuples of interest depends more on the "higher than 6" criteria. Using $N > 10$ instead of $N > 6$ generated 255 tuples over the period no matter if we required N to be twice or thrice the average, but using $N > 6$ generated 740 tuples for both absolute value requirements.

⁶<http://seclists.org/bugtraq/> and down from there

⁷<http://seclists.org/bugtraq/2007/Feb/0047.html>

⁸<http://seclists.org/bugtraq/2007/Feb/0453.html>

⁹<http://seclists.org/bugtraq/2007/Feb/0012.html>

really explain the surge of new traffic, as this would presumably be directed at the server.

3.4 March 2007

There's a mixed surge of tcp/135, tcp/445 and tcp/2967 throughout the month that I can't pin-point to anything specific.

Towards the end of the month, there are two surges for tcp/80 and there were several HTTP-based problems reported on March 27th¹⁰¹¹¹².

3.5 April 2007

Nothing super-noteworthy in April. There's a lot of peaking of tcp/135, tcp/445, tcp/2967 and tcp/5900. The increased VNC activity may, possibly, be related to a new version of tightvnc that was released to fix an integer overflow¹³, announced on April 4th.

3.6 May 2007

May offers fewer triggered anomalies, but we see a few new ones. On May 1st, we see tcp/51927, though I can't say I can find anything that seems to be a corresponding vulnerability.

On May 10th, there's a surge for tcp/3306 (MySQL). This neatly fits with a vulnerability report (two DoS vulnerabilities), posted May 8th¹⁴. There's a brief spiking in tcp/1433 (MS SQL Server) towards the end of the month.

3.7 June 2007

June 2007 starts with surges for MS SQL Server and SMB probing. There is a spike of HTTP probes on June 8th, there are a few web vulnerabilities reported around this time¹⁵.

There are assorted SMB peaks until the 15th, when udp/1026 and udp/1027 spike. UDP/1026 seems to be related to Messenger and may be either Messenger spam or an attempt to convince Messenger users to visit a specific URL. UDP/1027 seems to be the same.

On the 16th, there's a spike of VNC-related probes. This cannot be correlated with any reports.

Onwards through the month, there are several re-occurrences of spikes for tcp/135, tcp/1433, tcp/2967 and udp/1026. On June 24th, there's a spike for tcp/3306 (MySQL). Again, there is no obvious correlation with a vulnerability report near this time (see, however, the mysql vulnerabilities reported in July (p. 9).

¹⁰<http://seclists.org/bugtraq/2007/Mar/0416.html>

¹¹<http://seclists.org/bugtraq/2007/Mar/0406.html>

¹²<http://seclists.org/bugtraq/2007/Mar/0408.html>

¹³<http://seclists.org/bugtraq/2007/Apr/0102.html>

¹⁴<http://seclists.org/bugtraq/2007/May/0096.html>

¹⁵<http://seclists.org/bugtraq/2007/Jun/0106.html> <http://seclists.org/bugtraq/2007/Jun/0099.html>
<http://seclists.org/bugtraq/2007/Jun/0110.html> <http://seclists.org/bugtraq/2007/Jun/0112.html>
<http://seclists.org/bugtraq/2007/Jun/0121.html>

The tail end of the month is more of the same (assorted MS protocol ports, with a re-occurrence of a MySQL spike on the 29th).

3.8 July 2007

July starts with a spike of tcp/25. Looking at BugTraq, there is no obvious mailer-related vulnerability published.¹⁶

July 2nd sees another VNC peak. Then there's mostly assorted Microsoft protocols, until July 20th, when there's a spike for MySQL (possibly related to a vulnerability report from July 4th¹⁷ or July 17th¹⁸).

3.9 August 2007

August 2nd sees another VNC spike, though no obvious correlation to a vulnerability report.

Up until August 23rd, it is various Microsoft protocol ports and tcp/2967 that dominate, when tcp/5168 shows up. This seems to be a vulnerability in Trend Micro ServerProtect¹⁹.

From there, there's again more Microsoft protocols, until August 28th, when we see tcp/7212 making itself noticed (GhostSurf, no obvious vulnerability report tied in with this). This port also re-appears on August 29th, 30th and 31st.

3.10 September 2007

The month starts with a varied field. September 1st sees more GhostSurf (tcp/7212), MS SQL probes (tcp/1433) and VNC (tcp/5900).

Moving on to September 3rd, we see a spike for tcp/8000 (apparently WinAmp ShoutCast, iRDMI or maybe as an alternate HTTP port), but again, there is no obvious correlation to a vulnerability report.

The rest of the month sees the normal harvest of SMB, VNC and GhostSurf, with some tcp/2968 (Symantec AV Client) included as a bonus.

3.11 October 2007

The whole of October sees the same Microsoft protocols/VNC/Ghostsurf mix. Looking through the BugTraq vulnerability reports, nothing sticks out.

3.12 November 2007

November 2007 sees assorted Microsoft protocols, GhostSurf and VNC. There are Samba vulnerabilities²⁰ reported.

¹⁶There is a vulnerability reported for MailMarshal on September 4th, <http://seclists.org/bugtraq/2007/Sep/0025.html>

¹⁷<http://seclists.org/bugtraq/2007/Jul/0032.html>

¹⁸<http://seclists.org/bugtraq/2007/Jul/0164.html>

¹⁹<http://isc.sans.org/diary.html?storyid=3306>, <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=588>, <http://secunia.com/advisories/26523/>, there are two Trend Micro OfficeScan vulnerability reports that may be related, at <http://seclists.org/bugtraq/2007/Jul/0164.html> and <http://seclists.org/bugtraq/2007/Jul/0164.html>

²⁰<http://seclists.org/bugtraq/2007/Nov/0241.html>, <http://seclists.org/bugtraq/2007/Nov/0242.html>

There's some spikes for tcp/2967 (Symantec AV Corp), on the 12th, 16th, 20th and 24th.

3.13 December 2007

This month sees more of the same (spikes for Messenger spams, assorted SMB ports, Symantec AV Corp). Curiously, on the 20th there's a spike for tcp/53022, a port I cannot identify at all. This port re-spikes on the 21st, 24th, 25th, 26th, 27th and 28th.

3.14 January 2008

More of the classic SMB/Messenger/MS SQL mix until the 7th, when tcp/9788 surfaces. This seems to be related to "Filesphere". Again, there's no obvious vulnerability report.

There's also a spike for tcp/7788 on the 7th, this seems to be "PTC license server". Yet again, no obvious vulnerability report.

More of the usual SMB/GhostSurf mix through to the 13th, when we see UDP packets destined for SMB ports (udp/135 and udp/137).

Things continue with the normal mix until the 22nd, when tcp/18109²¹ spikes. It's noticeable that the VNC activity is fairly stable through the month, with a spike on the 27th.

3.15 February 2008

February sees, again, the normal mix of Microsoft protocol probe surges, Ghost-Surf and a surge for VNC on the 13th. There's no obvious correlation with vulnerability reports.

3.16 Conclusions

To some extent, increases in probe activity can be correlated with reported vulnerabilities, but it seems as if once there's exploits for anything, these will resurface now and again, without any obvious correlation to new vulnerabilities.

²¹I have not been able to find out what application(s) use tcp/18109 and no vulnerability reports mentioning it

4 Graphs

I have produced a ‘stream graph’²² of probe activity during the analysed period.

The graph doesn’t have (yet) a colour key, but in general red tones are TCP ports and blue tones are UDP ports. Each pixel line corresponds to 12 hours and the two images overlap from 2007-07-29 to 2007-09-14. The non-filtered stream graphs can be seen at p. 12 and 13

A slightly massaged data-set (any protocol/port tuple that has totalled at least 500 probes in sequential 12-hour segments) has been generated as a comparison, it shows quite clearly that most of the probes is to a limited number of ports (see p. 14 and p. 15).

I have prepared a graph of the number of ICMP ECHO received, on a per-day basis. As a general guideline, each individual source of ICMP ECHO will send two ICMP ECHO in any given day.

²²<http://www.leebyron.com/else/streamgraph/>

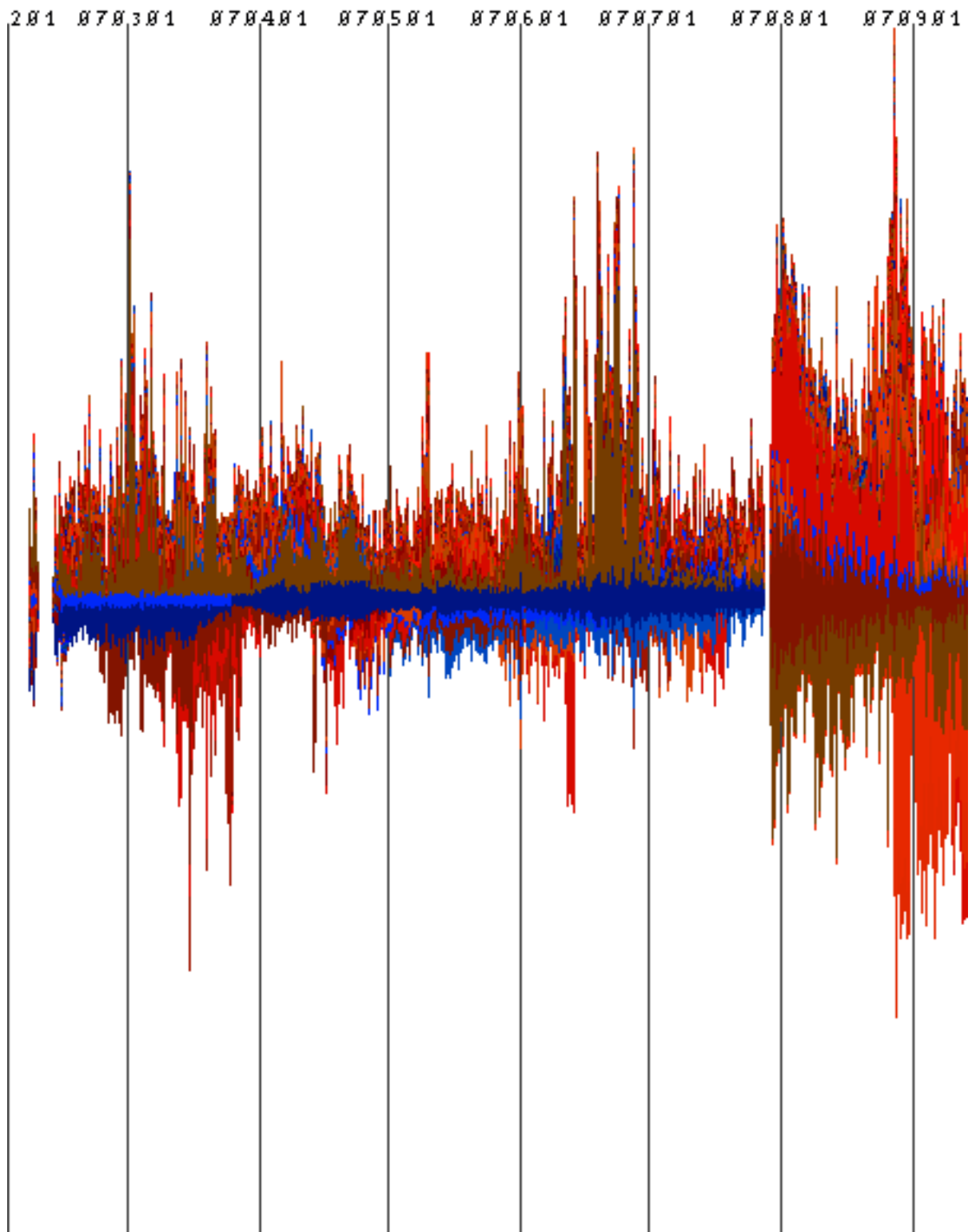


Table 3: Stream graph displaying all packets captured, colour-coded by protocol and port. Red tones indicate TCP packets, blue tones indicate UDP packets. The graph spans from 2007-02-01 to 2007-09-14

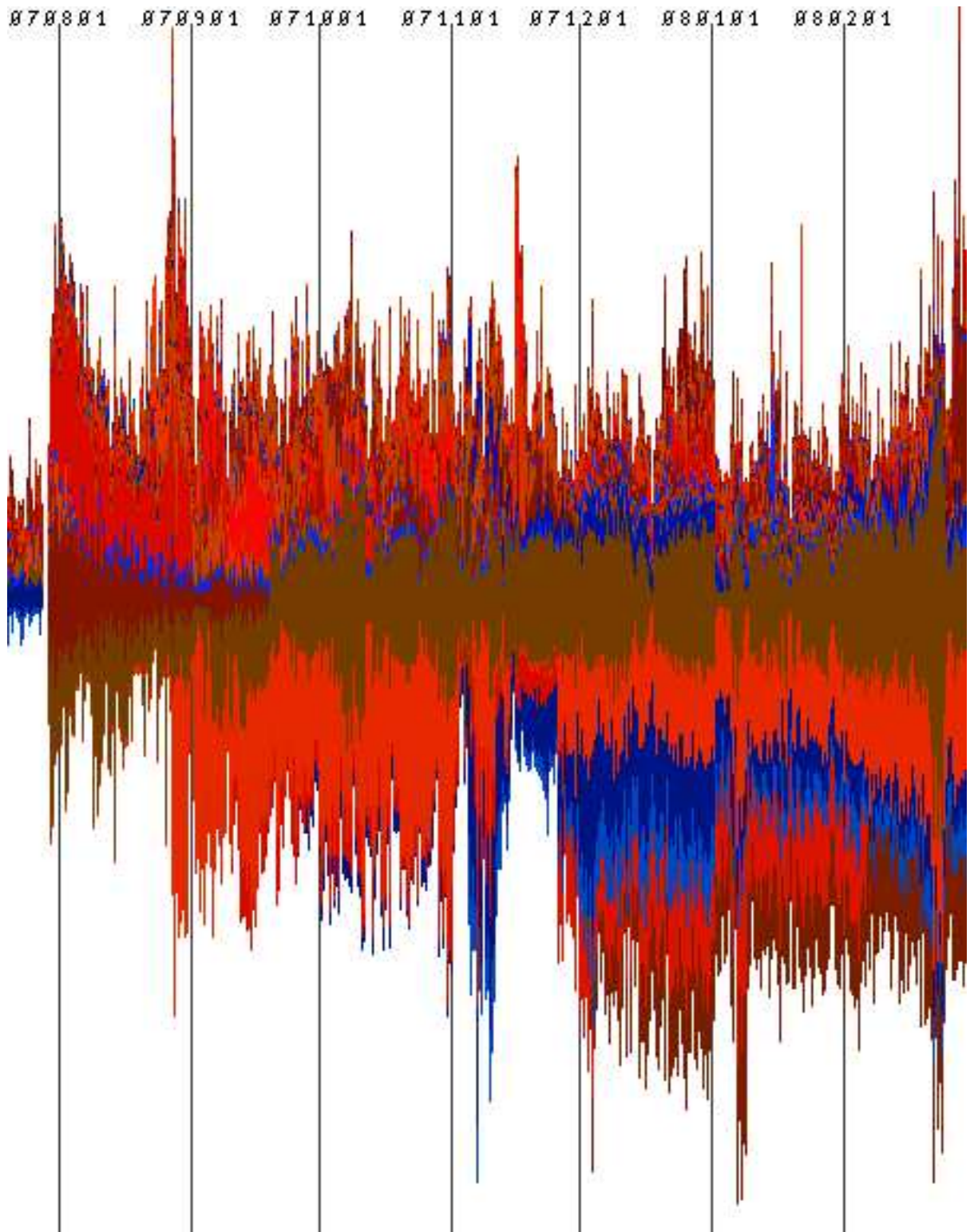


Table 4: Stream graph displaying all packets captured, colour-coded by protocol and port. Red tones indicate TCP packets, blue tones indicate UDP packets. The graph spans from 2007-07-29 to 2008-02-29

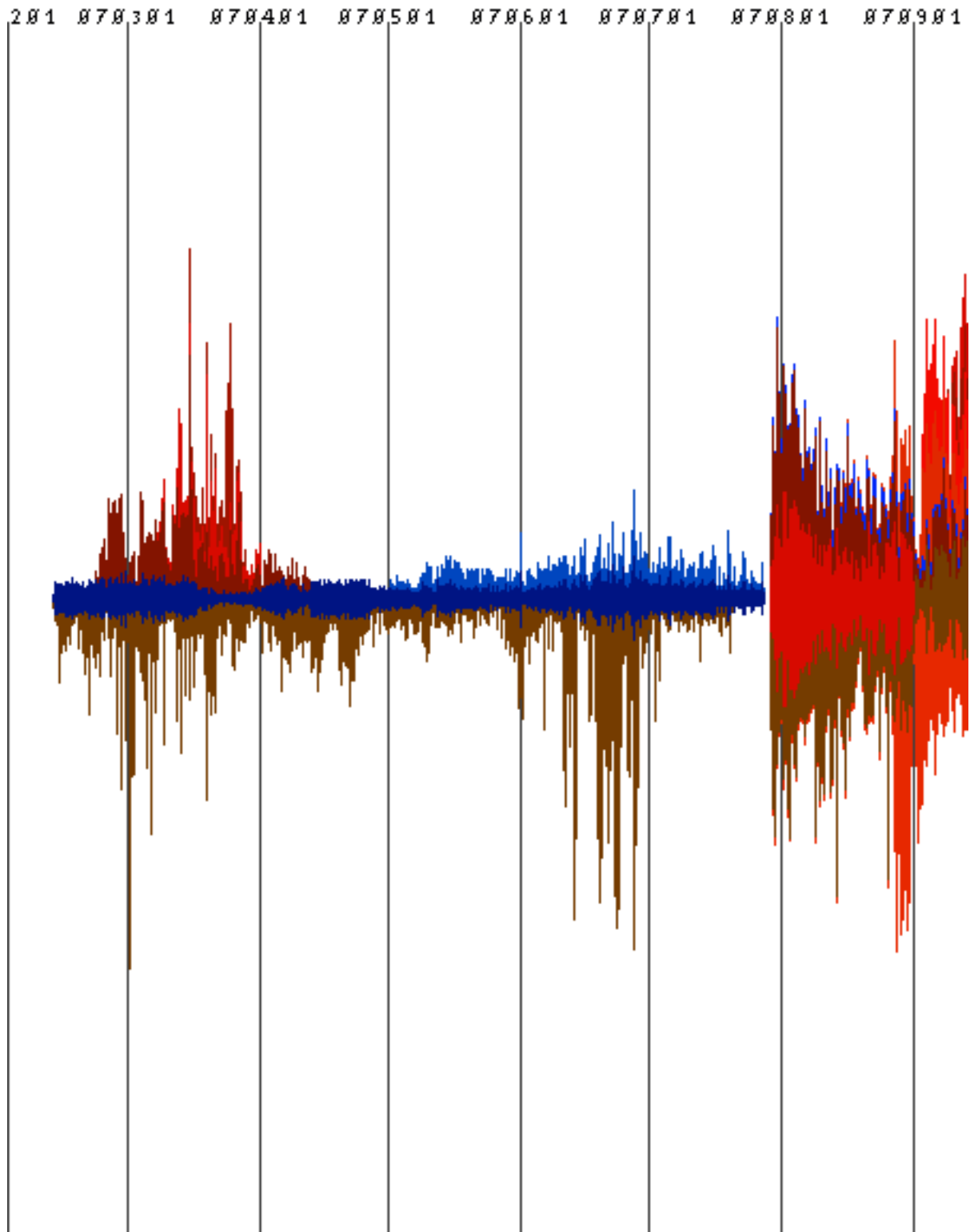


Table 5: Filtered stream graph displaying high-volume probes, colour-coded by protocol and port. Red tones indicate TCP packets, blue tones indicate UDP packets. The graph spans from 2007-02-01 to 2007-09-14

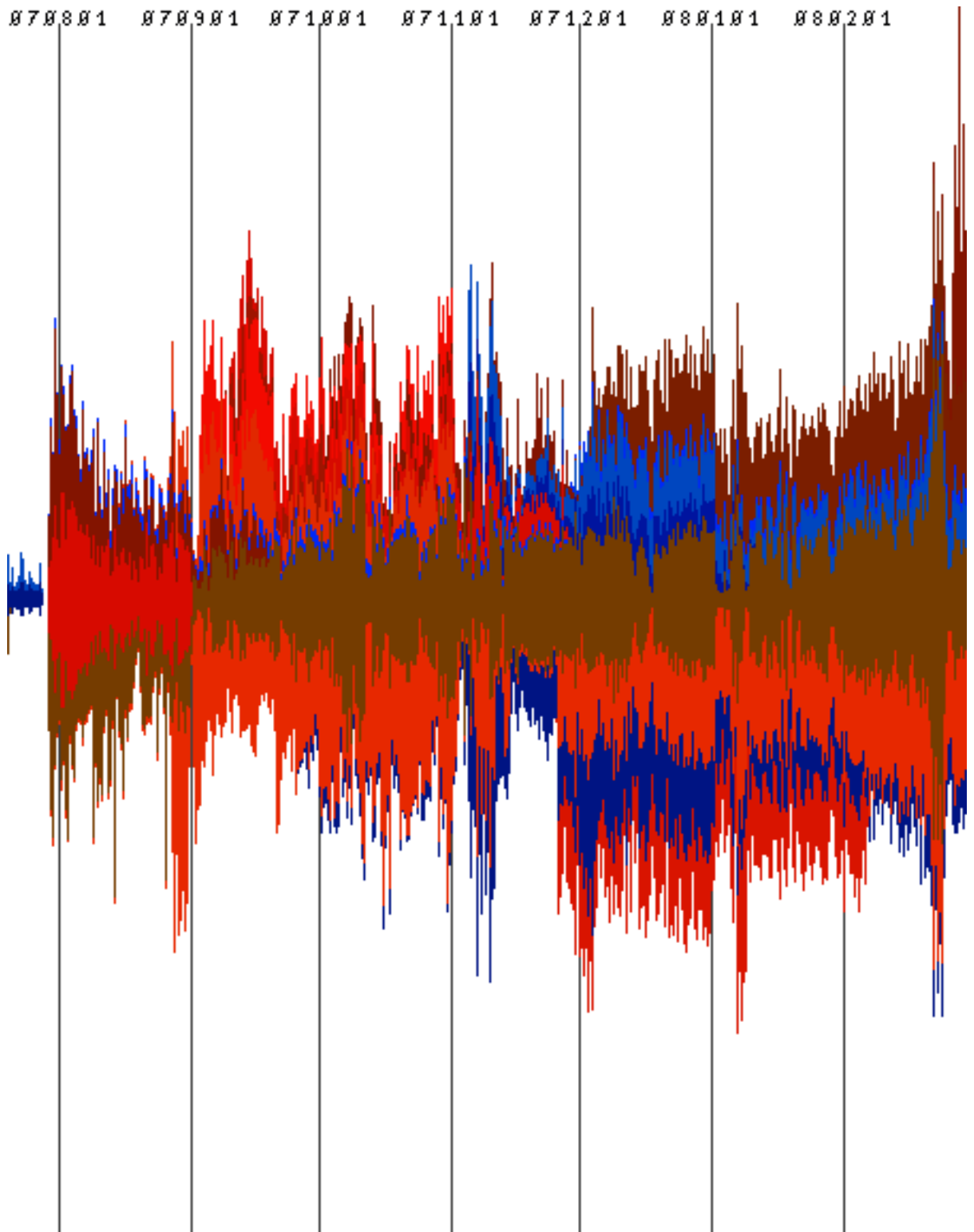


Table 6: Filtered stream graph displaying high-volume probes, colour-coded by protocol and port. Red tones indicate TCP packets, blue tones indicate UDP packets. The graph spans from 2007-07-29 to 2008-02-29

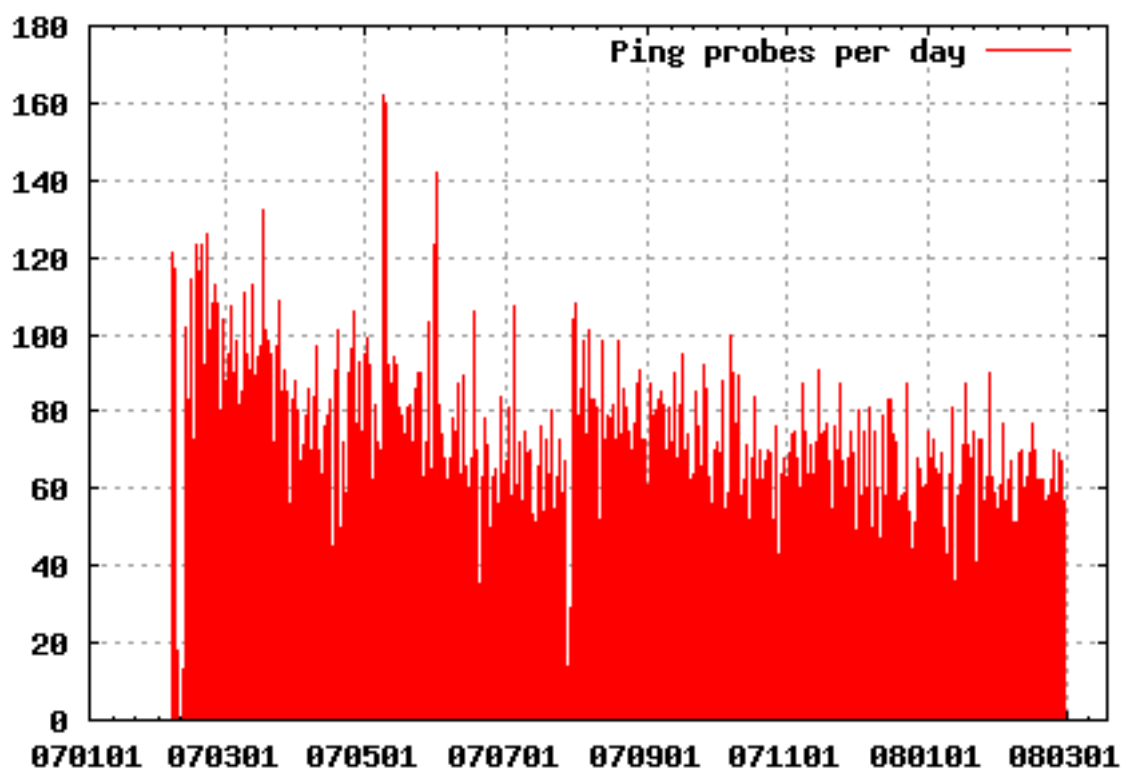


Table 7: Pings per day during the period

5 Statistics

This section presents some statistical breakdown of the seen probes on a per-month basis. The statistics that have been computed is the total of UDP, TCP and ICMP packets seen during the month, the number of distinct source IPs and distinct UDP and TCP destination ports.

5.1 Statistics for 2007-02

Table 8: Statistical breakdown, 2007-02

TCP packets, total	2472
UDP packets, total	954
ICMP packets, total	2018
Distinct sources	2722
Distinct TCP ports	75
Distinct UDP ports	19

Table 9: Top 12 TCP packets, 2007-02

port	count
tcp/135	737
tcp/2967	459
tcp/139	213
tcp/445	212
tcp/22	136
tcp/5900	117
tcp/25	70
tcp/4899	70
tcp/10000	64
tcp/1433	63
tcp/80	37
tcp/443	27

Table 10: Top 12 UDP packets, 2007-02

port	count
udp/1026	588
udp/1434	181
udp/1027	57
udp/137	31
udp/1028	17
udp/1029	14
udp/1030	12
udp/1031	10
udp/1033	10
udp/1032	9
udp/2	8
udp/4081	5

Table 11: Top 12 probe sources, 2007-02

host	count
217.147.28.218	192
218.27.16.183	62
202.99.172.163	43
217.147.37.110	23
217.146.246.10	21
217.147.43.64	20
217.144.163.121	18
84.9.188.121	18
217.144.198.177	17
217.147.36.29	17
204.16.209.159	17
217.144.202.240	16

5.2 Statistics for 2007-03

Table 12: Statistical breakdown, 2007-03

TCP packets, total	6316
UDP packets, total	1209
ICMP packets, total	2809
Distinct sources	3936
Distinct TCP ports	80
Distinct UDP ports	17

Table 13: Top 12 TCP packets, 2007-03

port	count
tcp/135	1739
tcp/2967	1213
tcp/139	890
tcp/445	859
tcp/5900	256
tcp/1433	252
tcp/22	217
tcp/80	148
tcp/4899	132
tcp/25	107
tcp/2968	82
tcp/10000	48

Table 14: Top 12 UDP packets, 2007-03

port	count
udp/1026	675
udp/1434	264
udp/1027	160
udp/137	38
udp/1028	16
udp/135	15
udp/1031	8
udp/4257	7
udp/1030	6
udp/1033	5
udp/1032	4
udp/1029	3

Table 15: Top 12 probe sources, 2007-03

host	count
217.147.28.218	853
217.147.230.16	314
217.147.230.27	277
217.147.231.254	237
217.146.216.14	116
218.27.16.156	79
217.147.44.6	75
217.147.232.146	70
217.147.43.48	63
217.146.246.10	51
218.27.16.183	49
217.146.214.8	44

5.3 Statistics for 2007-04

Table 16: Statistical breakdown, 2007-04

TCP packets, total	3711
UDP packets, total	1259
ICMP packets, total	2343
Distinct sources	3513
Distinct TCP ports	124
Distinct UDP ports	14

Table 17: Top 12 TCP packets, 2007-04

port	count
tcp/135	954
tcp/445	469
tcp/2967	448
tcp/139	379
tcp/5900	238
tcp/22	220
tcp/4899	172
tcp/1433	145
tcp/25	91
tcp/110	44
tcp/443	40
tcp/10000	38

Table 18: Top 12 UDP packets, 2007-04

port	count
udp/1026	787
udp/1434	243
udp/1027	176
udp/137	21
udp/1028	13
udp/53	3
udp/1033	3
udp/4081	3
udp/1029	2
udp/1030	2
udp/1032	2
udp/2	2

Table 19: Top 12 probe sources, 2007-04

host	count
217.145.145.90	89
217.147.230.27	84
217.146.214.8	63
217.144.205.19	52
217.147.18.140	45
66.98.254.217	44
217.144.205.205	40
217.144.163.121	36
204.16.211.16	34
204.16.208.63	33
218.27.16.156	33
217.144.217.136	31

5.4 Statistics for 2007-05

Table 20: Statistical breakdown, 2007-05

TCP packets, total	3429
UDP packets, total	1279
ICMP packets, total	2721
Distinct sources	2895
Distinct TCP ports	126
Distinct UDP ports	5

Table 21: Top 12 TCP packets, 2007-05

port	count
tcp/135	607
tcp/2967	418
tcp/445	346
tcp/5900	326
tcp/139	299
tcp/22	188
tcp/1433	184
tcp/4899	135
tcp/25	98
tcp/10000	73
tcp/2968	66
tcp/3306	62

Table 22: Top 5 UDP packets, 2007-05

port	count
udp/1026	583
udp/1027	404
udp/1434	258
udp/137	24
udp/1028	10

Table 23: Top 12 probe sources, 2007-05

host	count
204.16.209.14	109
217.147.45.7	106
204.16.208.33	96
217.146.214.8	93
204.16.208.63	82
58.19.183.42	73
204.16.209.15	68
217.145.145.90	54
204.16.210.172	45
222.161.2.48	45
121.28.24.62	42
218.27.148.122	39

5.5 Statistics for 2007-06

Table 24: Statistical breakdown, 2007-06

TCP packets, total	5783
UDP packets, total	2036
ICMP packets, total	2142
Distinct sources	2934
Distinct TCP ports	80
Distinct UDP ports	13

Table 25: Top 12 TCP packets, 2007-06

port	count
tcp/135	2855
tcp/445	596
tcp/5900	423
tcp/139	342
tcp/2967	316
tcp/1433	212
tcp/22	202
tcp/4899	150
tcp/5901	81
tcp/80	65
tcp/3306	64
tcp/2968	50

Table 26: Top 12 UDP packets, 2007-06

port	count
udp/1026	916
udp/1027	624
udp/1434	191
udp/1028	105
udp/1032	40
udp/1029	39
udp/1030	37
udp/1031	37
udp/137	35
udp/135	8
udp/13218	2
udp/13281	1

Table 27: Top 12 probe sources, 2007-06

host	count
217.147.224.66	2391
77.81.81.83	273
204.16.209.15	131
217.146.248.30	116
204.16.209.16	93
218.27.148.118	89
217.147.232.165	88
222.161.2.47	83
220.164.140.236	79
218.27.148.122	73
58.19.183.42	68
217.147.234.69	66

5.6 Statistics for 2007-07

Table 28: Statistical breakdown, 2007-07

TCP packets, total	3643
UDP packets, total	1538
ICMP packets, total	2044
Distinct sources	2918
Distinct TCP ports	83
Distinct UDP ports	15

Table 29: Top 12 TCP packets, 2007-07

port	count
tcp/445	660
tcp/135	657
tcp/2967	574
tcp/5900	402
tcp/139	280
tcp/22	153
tcp/4899	116
tcp/1433	101
tcp/25	94
tcp/3306	91
tcp/10000	34
tcp/2968	33

Table 30: Top 12 UDP packets, 2007-07

port	count
udp/1026	690
udp/1027	474
udp/1434	174
udp/1028	141
udp/137	30
udp/2	5
udp/4073	4
udp/1029	4
udp/1031	4
udp/4081	3
udp/1032	3
udp/1030	2

Table 31: Top 12 probe sources, 2007-07

host	count
220.164.140.242	230
83.105.82.243	212
217.164.54.56	95
217.147.232.165	86
222.161.2.52	82
218.27.16.155	80
218.27.148.165	76
218.27.148.162	63
217.145.64.250	54
217.146.216.64	36
61.138.185.98	35
222.161.2.53	30

5.7 Statistics for 2007-08

Table 32: Statistical breakdown, 2007-08

TCP packets, total	11757
UDP packets, total	694
ICMP packets, total	2591
Distinct sources	4607
Distinct TCP ports	177
Distinct UDP ports	6

Table 33: Top 12 TCP packets, 2007-08

port	count
tcp/445	3061
tcp/135	2340
tcp/2967	1862
tcp/7212	922
tcp/139	479
tcp/5900	411
tcp/8000	320
tcp/1433	274
tcp/5168	256
tcp/1080	228
tcp/8080	227
tcp/6588	135

Table 34: Top 6 UDP packets, 2007-08

port	count
udp/1434	341
udp/1026	138
udp/1027	118
udp/137	69
udp/1028	25
udp/53	3

Table 35: Top 12 probe sources, 2007-08

host	count
83.105.82.243	904
219.148.119.11	766
219.148.119.6	519
222.239.255.43	123
218.234.41.8	114
218.50.1.119	114
218.63.236.143	99
83.104.227.229	82
222.121.31.67	68
218.27.148.165	62
83.103.169.64	55
218.3.134.250	52

5.8 Statistics for 2007-09

Table 36: Statistical breakdown, 2007-09

TCP packets, total	12944
UDP packets, total	590
ICMP packets, total	2295
Distinct sources	3513
Distinct TCP ports	116
Distinct UDP ports	12

Table 37: Top 12 TCP packets, 2007-09

port	count
tcp/7212	2776
tcp/135	2316
tcp/8000	1458
tcp/8080	1357
tcp/445	946
tcp/2967	688
tcp/139	638
tcp/1433	492
tcp/5900	441
tcp/2968	416
tcp/5168	210
tcp/1080	187

Table 38: Top 12 UDP packets, 2007-09

port	count
udp/1434	291
udp/137	118
udp/1026	101
udp/1027	50
udp/1028	19
udp/53	4
udp/13675	2
udp/5060	1
udp/5632	1
udp/1357	1
udp/1369	1
udp/44654	1

Table 39: Top 12 probe sources, 2007-09

host	count
219.148.119.11	2474
219.148.119.2	1879
121.18.13.107	837
83.105.40.246	211
218.63.236.143	164
83.104.227.229	121
222.239.255.43	121
218.50.1.119	114
218.234.41.8	109
218.3.134.250	103
83.102.185.50	91
83.105.42.221	87

5.9 Statistics for 2007-10

Table 40: Statistical breakdown, 2007-10

TCP packets, total	14324
UDP packets, total	943
ICMP packets, total	2128
Distinct sources	3997
Distinct TCP ports	76
Distinct UDP ports	6

Table 41: Top 12 TCP packets, 2007-10

port	count
tcp/135	4142
tcp/7212	3607
tcp/8000	1157
tcp/8080	1058
tcp/445	900
tcp/2967	688
tcp/1433	538
tcp/139	442
tcp/2968	418
tcp/5900	410
tcp/22	134
tcp/1080	127

Table 42: Top 6 UDP packets, 2007-10

port	count
udp/1026	482
udp/1434	272
udp/137	149
udp/1027	25
udp/1028	14
udp/10081	1

Table 43: Top 12 probe sources, 2007-10

host	count
121.18.13.107	2518
121.18.13.100	1199
219.148.119.2	953
121.18.12.197	777
218.63.236.143	174
222.239.255.43	108
218.50.1.119	105
218.234.41.8	103
218.3.134.250	101
85.105.57.6	98
83.105.42.175	92
221.194.46.204	63

5.10 Statistics for 2007-11

Table 44: Statistical breakdown, 2007-11

TCP packets, total	9991
UDP packets, total	3582
ICMP packets, total	2117
Distinct sources	5238
Distinct TCP ports	80
Distinct UDP ports	13

Table 45: Top 12 TCP packets, 2007-11

port	count
tcp/135	3365
tcp/7212	1469
tcp/445	933
tcp/2967	690
tcp/1433	556
tcp/139	443
tcp/7788	387
tcp/5900	364
tcp/8000	340
tcp/8080	283
tcp/2968	220
tcp/22	135

Table 46: Top 12 UDP packets, 2007-11

port	count
udp/1026	1887
udp/1027	844
udp/1028	542
udp/1434	192
udp/137	109
udp/8984	1
udp/55287	1
udp/9656	1
udp/8921	1
udp/9500	1
udp/9287	1
udp/161	1

Table 47: Top 12 probe sources, 2007-11

host	count
121.18.13.107	1272
121.18.13.100	509
221.194.46.204	275
83.105.91.234	209
218.63.236.143	160
221.194.46.30	137
83.19.228.14	128
83.105.42.175	113
218.50.1.119	110
218.234.41.8	104
218.3.134.250	88
83.105.32.250	82

5.11 Statistics for 2007-12

Table 48: Statistical breakdown, 2007-12

TCP packets, total	13215
UDP packets, total	5576
ICMP packets, total	2007
Distinct sources	5323
Distinct TCP ports	67
Distinct UDP ports	17

Table 49: Top 12 TCP packets, 2007-12

port	count
tcp/135	3459
tcp/7212	2382
tcp/7788	2155
tcp/9788	1928
tcp/445	612
tcp/2967	373
tcp/53022	321
tcp/5900	278
tcp/2968	215
tcp/139	180
tcp/22	167
tcp/1433	151

Table 50: Top 12 UDP packets, 2007-12

port	count
udp/1026	2748
udp/1027	1592
udp/1028	829
udp/1434	267
udp/137	123
udp/53	6
udp/8112	1
udp/8236	1
udp/8091	1
udp/54729	1
udp/8778	1
udp/8255	1

Table 51: Top 12 probe sources, 2007-12

host	count
121.18.13.107	6255
202.111.175.193	302
218.63.236.143	204
222.239.255.43	129
218.234.41.8	127
218.3.134.250	89
221.208.208.96	72
121.14.136.101	68
221.209.110.50	67
218.233.198.25	62
221.209.110.13	57
218.10.137.140	57

5.12 Statistics for 2008-01

Table 52: Statistical breakdown, 2008-01

TCP packets, total	13021
UDP packets, total	3050
ICMP packets, total	1990
Distinct sources	3865
Distinct TCP ports	95
Distinct UDP ports	23

Table 53: Top 12 TCP packets, 2008-01

port	count
tcp/135	2832
tcp/7212	2633
tcp/9788	2452
tcp/7788	2408
tcp/2967	421
tcp/445	301
tcp/139	179
tcp/5900	177
tcp/1433	166
tcp/22	164
tcp/2968	160
tcp/3128	139

Table 54: Top 12 UDP packets, 2008-01

port	count
udp/1026	1385
udp/1027	847
udp/137	274
udp/1028	272
udp/1434	250
udp/53	3
udp/1357	3
udp/63555	1
udp/8677	1
udp/20984	1
udp/15362	1
udp/27757	1

Table 55: Top 12 probe sources, 2008-01

host	count
121.18.13.107	6641
121.18.13.100	553
218.63.236.143	286
83.105.36.56	150
222.239.255.43	127
218.234.41.8	118
121.14.136.101	106
218.3.134.250	99
218.233.198.25	97
222.73.204.17	94
91.125.70.12	68
218.10.137.142	66

5.13 Statistics for 2008-02

Table 56: Statistical breakdown, 2008-02

TCP packets, total	13920
UDP packets, total	2903
ICMP packets, total	1815
Distinct sources	4680
Distinct TCP ports	72
Distinct UDP ports	21

Table 57: Top 12 TCP packets, 2008-02

port	count
tcp/135	4792
tcp/7212	2987
tcp/9788	2637
tcp/2967	996
tcp/445	508
tcp/7788	422
tcp/5900	212
tcp/1433	210
tcp/22	184
tcp/139	117
tcp/1080	85
tcp/4899	84

Table 58: Top 12 UDP packets, 2008-02

port	count
udp/1026	1019
udp/1027	962
udp/1028	506
udp/1434	281
udp/137	119
udp/8566	1
udp/8457	1
udp/8732	1
udp/9810	1
udp/8792	1
udp/5632	1
udp/8563	1

Table 59: Top 12 probe sources, 2008-02

host	count
121.18.13.107	5863
218.63.236.143	178
83.39.193.21	113
121.14.136.101	107
201.90.166.130	106
83.71.191.89	93
222.239.255.43	81
218.234.41.8	76
222.73.204.18	76
195.101.186.205	73
218.233.198.25	73
58.60.239.51	69

6 A more detailed look at some active sources

In this section, I will show slightly redacted output from the PCAP traces, filtered on prolific sources or other interesting criteria. In general, a UDP or TCP dump will contain time, source host, source and destination ports and no more.

To the extent it is warranted, I have shortened these where there's a trivial pattern. Unfortunately, some of the behaviour looks as if there is a multiplicity of scanners, in that you have two or more simple patterns intertwined. I have not tried to separate these out.

6.1 2007-06, 83.27.37.238

This host has been included as it was a fairly clear example of a host that both pings and probes.

Time	Source IP	Source port	Dest. port
2007-06-08 15:46:25	83.27.37.238	ICMP Echo	
2007-06-08 15:46:25	83.27.37.238	TCP/41652	TCP/80
2007-06-08 15:46:26	83.27.37.238	ICMP Echo	
2007-06-08 15:46:26	83.27.37.238	TCP/41653	TCP/80

6.2 2007-06, 77.81.81.83

Time	Source IP	Source port	Dest. port
2007-06-05 00:39:56	77.81.81.83	UDP/13364	UDP/ 1027
2007-06-05 00:39:56	77.81.81.83	UDP/13364	UDP/ 1028
2007-06-05 00:39:56	77.81.81.83	UDP/13364	UDP/ 1029
2007-06-05 00:39:56	77.81.81.83	UDP/13364	UDP/ 1026
2007-06-05 00:39:56	77.81.81.83	UDP/13364	UDP/ 1030
2007-06-05 00:39:56	77.81.81.83	UDP/13364	UDP/ 1031
2007-06-05 00:39:56	77.81.81.83	UDP/13364	UDP/ 1032
2007-06-07 03:15:39	77.81.81.83	UDP/13364	UDP/ 1026
2007-06-07 03:15:39	77.81.81.83	UDP/13364	UDP/ 1027
2007-06-07 03:15:39	77.81.81.83	UDP/13364	UDP/ 1028
2007-06-07 03:15:39	77.81.81.83	UDP/13364	UDP/ 1029
2007-06-07 03:15:39	77.81.81.83	UDP/13364	UDP/ 1030
2007-06-07 03:15:39	77.81.81.83	UDP/13364	UDP/ 1031
2007-06-07 03:15:39	77.81.81.83	UDP/13364	UDP/ 1032
2007-06-07 06:20:35	77.81.81.83	UDP/13364	UDP/ 1026
2007-06-07 06:20:35	77.81.81.83	UDP/13364	UDP/ 1027
2007-06-07 06:20:35	77.81.81.83	UDP/13364	UDP/ 1028
2007-06-07 06:20:35	77.81.81.83	UDP/13364	UDP/ 1029
2007-06-07 06:20:35	77.81.81.83	UDP/13364	UDP/ 1030
2007-06-07 06:20:35	77.81.81.83	UDP/13364	UDP/ 1031
2007-06-07 06:20:35	77.81.81.83	UDP/13364	UDP/ 1032
2007-06-07 09:26:18	77.81.81.83	UDP/13364	UDP/ 1026
⋮	⋮	⋮	⋮
2007-06-07 18:40:39	77.81.81.83	UDP/13364	UDP/ 1030

Continued from last page

Time	Source IP	Source port	Dest. port
2007-06-07 18:40:39	77.81.81.83	UDP/13364	UDP/ 1031
2007-06-07 21:45:44	77.81.81.83	UDP/13364	UDP/ 1026
2007-06-07 21:45:44	77.81.81.83	UDP/13364	UDP/ 1027
2007-06-07 21:45:44	77.81.81.83	UDP/13364	UDP/ 1029
2007-06-07 21:45:44	77.81.81.83	UDP/13364	UDP/ 1030
2007-06-07 21:45:44	77.81.81.83	UDP/13364	UDP/ 1031
2007-06-07 21:45:44	77.81.81.83	UDP/13364	UDP/ 1032
2007-06-07 21:45:44	77.81.81.83	UDP/13364	UDP/ 1028
2007-06-08 00:50:54	77.81.81.83	UDP/13364	UDP/ 1028
2007-06-08 00:50:54	77.81.81.83	UDP/13364	UDP/ 1029
2007-06-08 00:50:54	77.81.81.83	UDP/13364	UDP/ 1026
2007-06-08 00:50:54	77.81.81.83	UDP/13364	UDP/ 1027
2007-06-08 00:50:54	77.81.81.83	UDP/13364	UDP/ 1030
2007-06-08 00:50:54	77.81.81.83	UDP/13364	UDP/ 1031
2007-06-08 00:50:54	77.81.81.83	UDP/13364	UDP/ 1032
2007-06-08 03:55:40	77.81.81.83	UDP/13364	UDP/ 1028
2007-06-08 03:55:40	77.81.81.83	UDP/13364	UDP/ 1029
2007-06-08 03:55:40	77.81.81.83	UDP/13364	UDP/ 1030
2007-06-08 03:55:40	77.81.81.83	UDP/13364	UDP/ 1032
2007-06-08 03:55:40	77.81.81.83	UDP/13364	UDP/ 1026
⋮	⋮	⋮	⋮
2007-06-11 21:25:19	77.81.81.83	UDP/13364	UDP/ 1026
2007-06-12 00:30:33	77.81.81.83	UDP/13364	UDP/ 1026
2007-06-12 00:30:33	77.81.81.83	UDP/13364	UDP/ 1027
2007-06-12 00:30:33	77.81.81.83	UDP/13364	UDP/ 1028
2007-06-12 00:30:33	77.81.81.83	UDP/13364	UDP/ 1029
2007-06-12 00:30:33	77.81.81.83	UDP/13364	UDP/ 1030
2007-06-12 00:30:33	77.81.81.83	UDP/13364	UDP/ 1031
2007-06-12 00:30:33	77.81.81.83	UDP/13364	UDP/ 1032
2007-06-12 03:35:30	77.81.81.83	UDP/13364	UDP/ 1026
2007-06-12 03:35:30	77.81.81.83	UDP/13364	UDP/ 1027
2007-06-12 03:35:30	77.81.81.83	UDP/13364	UDP/ 1028
2007-06-12 03:35:30	77.81.81.83	UDP/13364	UDP/ 1029
2007-06-12 03:35:30	77.81.81.83	UDP/13364	UDP/ 1030
2007-06-12 03:35:30	77.81.81.83	UDP/13364	UDP/ 1031
2007-06-12 03:35:30	77.81.81.83	UDP/13364	UDP/ 1032
2007-06-12 06:40:41	77.81.81.83	UDP/13364	UDP/ 1029
2007-06-12 06:40:41	77.81.81.83	UDP/13364	UDP/ 1026
2007-06-12 06:40:41	77.81.81.83	UDP/13364	UDP/ 1030
2007-06-12 06:40:41	77.81.81.83	UDP/13364	UDP/ 1031
2007-06-12 06:40:41	77.81.81.83	UDP/13364	UDP/ 1027
2007-06-12 06:40:41	77.81.81.83	UDP/13364	UDP/ 1028
2007-06-12 06:40:41	77.81.81.83	UDP/13364	UDP/ 1032

6.3 2007-06, 217.147.224.66

Time	Source IP	Source port	Dest. port
2007-06-10 16:05:33	217.147.224.66	TCP/3606	TCP/135
2007-06-10 16:15:09	217.147.224.66	TCP/3620	TCP/135
2007-06-10 16:24:56	217.147.224.66	TCP/3575	TCP/135
2007-06-10 16:46:03	217.147.224.66	TCP/3068	TCP/135
2007-06-10 16:56:33	217.147.224.66	TCP/3586	TCP/135
2007-06-10 17:07:42	217.147.224.66	TCP/4124	TCP/135
2007-06-10 17:18:17	217.147.224.66	TCP/3032	TCP/135
2007-06-10 17:28:35	217.147.224.66	TCP/3582	TCP/135
2007-06-10 17:39:33	217.147.224.66	TCP/3159	TCP/135
2007-06-10 17:51:00	217.147.224.66	TCP/3057	TCP/135
2007-06-10 18:01:41	217.147.224.66	TCP/3591	TCP/135
2007-06-10 18:12:33	217.147.224.66	TCP/4125	TCP/135
2007-06-10 18:23:19	217.147.224.66	TCP/3025	TCP/135
2007-06-10 18:34:04	217.147.224.66	TCP/3596	TCP/135
2007-06-10 18:44:39	217.147.224.66	TCP/4162	TCP/135
2007-06-10 18:55:14	217.147.224.66	TCP/3004	TCP/135
⋮	⋮	⋮	⋮
2007-06-11 13:57:32	217.147.224.66	TCP/4660	TCP/135
2007-06-11 14:07:53	217.147.224.66	TCP/3296	TCP/135
2007-06-11 14:17:38	217.147.224.66	TCP/4436	TCP/135
2007-06-11 14:27:42	217.147.224.66	TCP/4462	TCP/135
2007-06-11 14:37:31	217.147.224.66	TCP/3840	TCP/135
2007-06-11 14:47:15	217.147.224.66	TCP/4695	TCP/135
2007-06-11 14:52:09	217.147.224.66	TCP/3089	TCP/445
2007-06-11 14:59:33	217.147.224.66	TCP/4771	TCP/135
2007-06-11 15:03:54	217.147.224.66	TCP/4832	TCP/445
2007-06-11 15:09:47	217.147.224.66	TCP/3903	TCP/135
2007-06-11 15:14:31	217.147.224.66	TCP/3226	TCP/445
2007-06-11 15:20:13	217.147.224.66	TCP/4570	TCP/135
2007-06-11 15:24:37	217.147.224.66	TCP/4331	TCP/445
2007-06-11 15:30:19	217.147.224.66	TCP/3292	TCP/135
2007-06-11 15:34:42	217.147.224.66	TCP/4165	TCP/445
2007-06-11 15:40:52	217.147.224.66	TCP/3434	TCP/135
2007-06-11 15:45:24	217.147.224.66	TCP/4356	TCP/445
2007-06-11 15:51:52	217.147.224.66	TCP/3543	TCP/135
2007-06-11 15:55:56	217.147.224.66	TCP/4908	TCP/445
2007-06-11 16:06:15	217.147.224.66	TCP/4042	TCP/445
2007-06-11 16:15:53	217.147.224.66	TCP/3030	TCP/445
2007-06-11 16:25:33	217.147.224.66	TCP/4586	TCP/445
2007-06-11 16:35:20	217.147.224.66	TCP/3437	TCP/445
2007-06-11 16:45:01	217.147.224.66	TCP/4809	TCP/445
2007-06-11 16:54:48	217.147.224.66	TCP/3335	TCP/445
2007-06-11 17:04:31	217.147.224.66	TCP/3437	TCP/445
2007-06-11 17:14:12	217.147.224.66	TCP/4008	TCP/445
2007-06-11 17:24:09	217.147.224.66	TCP/3712	TCP/445
2007-06-11 17:34:12	217.147.224.66	TCP/3279	TCP/445
2007-06-11 17:44:10	217.147.224.66	TCP/4280	TCP/445
2007-06-11 17:54:14	217.147.224.66	TCP/3168	TCP/445

Continued from last page

Time	Source IP	Source port	Dest. port
2007-06-11 18:03:57	217.147.224.66	TCP/3187	TCP/445
2007-06-11 18:13:40	217.147.224.66	TCP/3159	TCP/445
2007-06-11 18:23:25	217.147.224.66	TCP/3131	TCP/445
2007-06-11 18:33:08	217.147.224.66	TCP/3468	TCP/445
2007-06-11 18:42:48	217.147.224.66	TCP/3710	TCP/445
2007-06-11 18:52:30	217.147.224.66	TCP/4821	TCP/445
2007-06-11 19:02:10	217.147.224.66	TCP/3928	TCP/445
2007-06-11 19:11:52	217.147.224.66	TCP/3155	TCP/445
2007-06-11 19:21:34	217.147.224.66	TCP/3978	TCP/445
2007-06-11 19:31:21	217.147.224.66	TCP/3714	TCP/445
2007-06-11 19:41:16	217.147.224.66	TCP/4604	TCP/445
2007-06-11 19:50:55	217.147.224.66	TCP/3004	TCP/445
2007-06-11 20:00:38	217.147.224.66	TCP/4273	TCP/445
2007-06-11 20:10:25	217.147.224.66	TCP/4828	TCP/445
2007-06-11 20:20:06	217.147.224.66	TCP/4549	TCP/445
2007-06-11 20:29:50	217.147.224.66	TCP/3705	TCP/445
2007-06-11 20:39:38	217.147.224.66	TCP/4096	TCP/445
2007-06-11 20:49:22	217.147.224.66	TCP/3341	TCP/445
2007-06-11 20:59:18	217.147.224.66	TCP/3646	TCP/135
2007-06-11 21:00:51	217.147.224.66	TCP/4152	TCP/445
2007-06-11 21:10:18	217.147.224.66	TCP/3082	TCP/135
2007-06-11 21:11:44	217.147.224.66	TCP/3589	TCP/445
2007-06-11 21:20:58	217.147.224.66	TCP/3636	TCP/135
2007-06-11 21:22:24	217.147.224.66	TCP/4119	TCP/445
2007-06-11 21:31:41	217.147.224.66	TCP/4189	TCP/135
2007-06-11 21:33:04	217.147.224.66	TCP/4920	TCP/445
2007-06-11 21:42:19	217.147.224.66	TCP/3081	TCP/135
2007-06-11 21:43:43	217.147.224.66	TCP/3553	TCP/445
2007-06-11 21:52:52	217.147.224.66	TCP/3613	TCP/135
2007-06-11 21:54:16	217.147.224.66	TCP/4104	TCP/445
2007-06-11 22:03:28	217.147.224.66	TCP/4190	TCP/135
2007-06-11 22:04:53	217.147.224.66	TCP/4990	TCP/445
⋮	⋮	⋮	⋮
2007-06-12 16:24:51	217.147.224.66	TCP/4966	TCP/445
2007-06-12 16:28:18	217.147.224.66	TCP/4609	TCP/135
2007-06-12 16:35:31	217.147.224.66	TCP/3519	TCP/445
2007-06-12 16:39:10	217.147.224.66	TCP/3504	TCP/135
2007-06-12 16:46:23	217.147.224.66	TCP/4951	TCP/445
2007-06-12 16:50:33	217.147.224.66	TCP/4799	TCP/135
2007-06-12 16:58:18	217.147.224.66	TCP/4361	TCP/445
2007-06-12 17:02:00	217.147.224.66	TCP/3634	TCP/135
2007-06-12 17:09:18	217.147.224.66	TCP/3896	TCP/445
2007-06-12 17:12:48	217.147.224.66	TCP/3415	TCP/135
2007-06-12 17:19:58	217.147.224.66	TCP/3569	TCP/445
2007-06-12 17:23:33	217.147.224.66	TCP/3948	TCP/135
2007-06-12 17:30:34	217.147.224.66	TCP/3422	TCP/445
2007-06-12 17:33:51	217.147.224.66	TCP/3592	TCP/135

Continued from last page

Time	Source IP	Source port	Dest. port
2007-06-12 17:41:54	217.147.224.66	TCP/3545	TCP/445
2007-06-12 17:45:25	217.147.224.66	TCP/3438	TCP/135
2007-06-12 17:52:52	217.147.224.66	TCP/4987	TCP/445
2007-06-12 17:56:47	217.147.224.66	TCP/4575	TCP/135
2007-06-12 18:04:08	217.147.224.66	TCP/4889	TCP/445
2007-06-12 18:07:59	217.147.224.66	TCP/3425	TCP/135
2007-06-12 18:15:20	217.147.224.66	TCP/4791	TCP/445
2007-06-12 18:19:24	217.147.224.66	TCP/4640	TCP/135
2007-06-12 18:31:35	217.147.224.66	TCP/4540	TCP/135
2007-06-12 18:38:19	217.147.224.66	TCP/3882	TCP/445
2007-06-12 18:42:35	217.147.224.66	TCP/3058	TCP/135
2007-06-12 18:49:31	217.147.224.66	TCP/4673	TCP/445
2007-06-12 18:53:58	217.147.224.66	TCP/4691	TCP/135
2007-06-12 19:01:01	217.147.224.66	TCP/3499	TCP/445
2007-06-12 19:05:15	217.147.224.66	TCP/3422	TCP/135
2007-06-12 19:12:04	217.147.224.66	TCP/3789	TCP/445
2007-06-12 19:16:33	217.147.224.66	TCP/4750	TCP/135
2007-06-12 19:22:56	217.147.224.66	TCP/4157	TCP/445
2007-06-12 19:26:55	217.147.224.66	TCP/3599	TCP/135
2007-06-12 19:32:56	217.147.224.66	TCP/3590	TCP/445
2007-06-12 19:36:55	217.147.224.66	TCP/3412	TCP/135
2007-06-12 19:43:12	217.147.224.66	TCP/4051	TCP/445
2007-06-12 19:47:05	217.147.224.66	TCP/4461	TCP/135
2007-06-12 19:53:21	217.147.224.66	TCP/4921	TCP/445
2007-06-12 19:57:34	217.147.224.66	TCP/4047	TCP/135
2007-06-12 20:03:57	217.147.224.66	TCP/3862	TCP/445
2007-06-12 20:08:25	217.147.224.66	TCP/3612	TCP/135
2007-06-12 20:14:38	217.147.224.66	TCP/4692	TCP/445
2007-06-12 20:19:55	217.147.224.66	TCP/4379	TCP/135
2007-06-12 20:27:48	217.147.224.66	TCP/4755	TCP/445
2007-06-12 20:32:00	217.147.224.66	TCP/4581	TCP/135
2007-06-12 20:38:39	217.147.224.66	TCP/4371	TCP/445
2007-06-12 20:43:00	217.147.224.66	TCP/4722	TCP/135
2007-06-12 20:49:40	217.147.224.66	TCP/4901	TCP/445
2007-06-12 20:59:30	217.147.224.66	TCP/4675	TCP/445
2007-06-12 21:09:07	217.147.224.66	TCP/3341	TCP/445
2007-06-12 21:18:39	217.147.224.66	TCP/3854	TCP/445
2007-06-12 21:28:10	217.147.224.66	TCP/3322	TCP/445
2007-06-12 21:37:40	217.147.224.66	TCP/3593	TCP/445
2007-06-12 21:47:10	217.147.224.66	TCP/4113	TCP/445
2007-06-12 21:56:41	217.147.224.66	TCP/4366	TCP/445
2007-06-12 22:06:19	217.147.224.66	TCP/3064	TCP/445
2007-06-12 22:15:53	217.147.224.66	TCP/4673	TCP/445
2007-06-12 22:25:26	217.147.224.66	TCP/3070	TCP/445
2007-06-12 22:34:57	217.147.224.66	TCP/3871	TCP/445
2007-06-12 22:44:32	217.147.224.66	TCP/4112	TCP/445
2007-06-12 22:54:01	217.147.224.66	TCP/3038	TCP/445
2007-06-12 23:03:31	217.147.224.66	TCP/3564	TCP/445

Continued from last page

Time	Source IP	Source port	Dest. port
⋮	⋮	⋮	⋮
2007-06-13 02:53:26	217.147.224.66	TCP/4170	TCP/445
2007-06-13 03:03:25	217.147.224.66	TCP/3355	TCP/445
2007-06-13 03:13:14	217.147.224.66	TCP/4387	TCP/445
2007-06-13 03:24:18	217.147.224.66	TCP/3518	TCP/135
2007-06-13 03:26:11	217.147.224.66	TCP/3312	TCP/445
2007-06-13 03:36:34	217.147.224.66	TCP/3636	TCP/135
2007-06-13 03:36:37	217.147.224.66	TCP/3636	TCP/135
2007-06-13 03:38:34	217.147.224.66	TCP/4814	TCP/445
2007-06-13 03:48:06	217.147.224.66	TCP/4148	TCP/135
2007-06-13 03:49:56	217.147.224.66	TCP/4721	TCP/445
2007-06-13 03:59:02	217.147.224.66	TCP/3046	TCP/135
2007-06-13 04:00:38	217.147.224.66	TCP/3461	TCP/445
2007-06-13 04:10:18	217.147.224.66	TCP/3017	TCP/135
2007-06-13 04:11:59	217.147.224.66	TCP/3396	TCP/445
2007-06-13 04:20:54	217.147.224.66	TCP/4414	TCP/135
2007-06-13 04:22:23	217.147.224.66	TCP/3881	TCP/445
2007-06-13 04:31:18	217.147.224.66	TCP/4152	TCP/135
2007-06-13 04:32:58	217.147.224.66	TCP/3308	TCP/445
2007-06-13 04:42:16	217.147.224.66	TCP/4879	TCP/135
2007-06-13 04:43:41	217.147.224.66	TCP/3507	TCP/445
2007-06-13 04:53:17	217.147.224.66	TCP/4975	TCP/135
2007-06-13 04:54:47	217.147.224.66	TCP/4450	TCP/445
2007-06-13 05:04:03	217.147.224.66	TCP/3601	TCP/135
2007-06-13 05:05:14	217.147.224.66	TCP/3795	TCP/445
2007-06-13 05:14:40	217.147.224.66	TCP/4106	TCP/135
2007-06-13 05:16:05	217.147.224.66	TCP/4576	TCP/445
2007-06-13 05:25:44	217.147.224.66	TCP/4067	TCP/135
2007-06-13 05:26:55	217.147.224.66	TCP/4488	TCP/445
2007-06-13 05:35:46	217.147.224.66	TCP/3579	TCP/135
2007-06-13 05:36:59	217.147.224.66	TCP/4073	TCP/445
2007-06-13 05:45:53	217.147.224.66	TCP/4053	TCP/135
2007-06-13 05:47:07	217.147.224.66	TCP/4501	TCP/445
2007-06-13 05:56:11	217.147.224.66	TCP/4937	TCP/135
2007-06-13 05:57:32	217.147.224.66	TCP/3316	TCP/445
2007-06-13 06:07:04	217.147.224.66	TCP/3615	TCP/135
2007-06-13 06:08:16	217.147.224.66	TCP/4693	TCP/445
2007-06-13 06:17:31	217.147.224.66	TCP/3554	TCP/135
2007-06-13 06:18:43	217.147.224.66	TCP/4444	TCP/445
2007-06-13 06:28:22	217.147.224.66	TCP/3430	TCP/135
2007-06-13 06:29:24	217.147.224.66	TCP/4679	TCP/445
2007-06-13 06:38:46	217.147.224.66	TCP/3040	TCP/135
2007-06-13 06:39:42	217.147.224.66	TCP/3232	TCP/445
2007-06-13 06:49:24	217.147.224.66	TCP/4127	TCP/135
2007-06-13 06:50:25	217.147.224.66	TCP/3361	TCP/445
2007-06-13 07:00:13	217.147.224.66	TCP/4964	TCP/135
2007-06-13 07:01:04	217.147.224.66	TCP/4349	TCP/445

Continued from last page

Time	Source IP	Source port	Dest. port
2007-06-13 07:10:33	217.147.224.66	TCP/4133	TCP/135
2007-06-13 07:11:18	217.147.224.66	TCP/3261	TCP/445
2007-06-13 07:21:07	217.147.224.66	TCP/3511	TCP/135
2007-06-13 07:21:59	217.147.224.66	TCP/4644	TCP/445
2007-06-13 07:32:06	217.147.224.66	TCP/3047	TCP/135
2007-06-13 07:32:52	217.147.224.66	TCP/4570	TCP/445
2007-06-13 07:42:40	217.147.224.66	TCP/4031	TCP/135
2007-06-13 07:43:25	217.147.224.66	TCP/4606	TCP/445
2007-06-13 07:53:22	217.147.224.66	TCP/3617	TCP/135
2007-06-13 07:54:10	217.147.224.66	TCP/3913	TCP/445
2007-06-13 08:04:17	217.147.224.66	TCP/3597	TCP/135
2007-06-13 08:05:04	217.147.224.66	TCP/4394	TCP/445
2007-06-13 08:15:52	217.147.224.66	TCP/3050	TCP/135
2007-06-13 08:16:26	217.147.224.66	TCP/3814	TCP/445
2007-06-13 08:26:40	217.147.224.66	TCP/3293	TCP/135
2007-06-13 08:27:13	217.147.224.66	TCP/4505	TCP/445
2007-06-13 08:37:16	217.147.224.66	TCP/4142	TCP/135
2007-06-13 08:37:46	217.147.224.66	TCP/4353	TCP/445
2007-06-13 08:47:13	217.147.224.66	TCP/3591	TCP/135
2007-06-13 08:47:43	217.147.224.66	TCP/3334	TCP/445
2007-06-13 08:57:53	217.147.224.66	TCP/4110	TCP/135
2007-06-13 08:58:17	217.147.224.66	TCP/3232	TCP/445
2007-06-13 09:08:53	217.147.224.66	TCP/4930	TCP/135
2007-06-13 09:09:19	217.147.224.66	TCP/3279	TCP/445
2007-06-13 09:19:05	217.147.224.66	TCP/3571	TCP/135
2007-06-13 09:19:27	217.147.224.66	TCP/3773	TCP/445
2007-06-13 09:29:25	217.147.224.66	TCP/4038	TCP/135
2007-06-13 09:29:49	217.147.224.66	TCP/4685	TCP/445
2007-06-13 09:39:34	217.147.224.66	TCP/3050	TCP/135
2007-06-13 09:39:59	217.147.224.66	TCP/3334	TCP/445
2007-06-13 09:50:41	217.147.224.66	TCP/4829	TCP/135
2007-06-13 09:51:00	217.147.224.66	TCP/3856	TCP/445
2007-06-13 10:01:40	217.147.224.66	TCP/3864	TCP/135
2007-06-13 10:02:01	217.147.224.66	TCP/3339	TCP/445
2007-06-13 10:13:13	217.147.224.66	TCP/4828	TCP/135
2007-06-13 10:13:35	217.147.224.66	TCP/3331	TCP/445
2007-06-13 10:25:31	217.147.224.66	TCP/4086	TCP/135
2007-06-13 10:25:44	217.147.224.66	TCP/3781	TCP/445
2007-06-13 10:37:00	217.147.224.66	TCP/4016	TCP/135
2007-06-13 10:37:10	217.147.224.66	TCP/4578	TCP/445
2007-06-13 10:48:09	217.147.224.66	TCP/4943	TCP/135
2007-06-13 10:48:19	217.147.224.66	TCP/3312	TCP/445
2007-06-13 10:59:49	217.147.224.66	TCP/4040	TCP/135
2007-06-13 10:59:56	217.147.224.66	TCP/3875	TCP/445
2007-06-13 11:10:37	217.147.224.66	TCP/3517	TCP/135
2007-06-13 11:10:47	217.147.224.66	TCP/3917	TCP/445
2007-06-13 11:21:27	217.147.224.66	TCP/3489	TCP/135
2007-06-13 11:21:40	217.147.224.66	TCP/3879	TCP/445

Continued from last page

Time	Source IP	Source port	Dest. port
2007-06-13 11:32:30	217.147.224.66	TCP/4888	TCP/135
2007-06-13 11:32:35	217.147.224.66	TCP/3858	TCP/445
2007-06-13 11:43:42	217.147.224.66	TCP/3359	TCP/445
2007-06-13 11:43:46	217.147.224.66	TCP/4859	TCP/135
2007-06-13 11:55:35	217.147.224.66	TCP/3297	TCP/445
2007-06-13 11:55:38	217.147.224.66	TCP/3297	TCP/445
2007-06-13 11:55:39	217.147.224.66	TCP/3840	TCP/135
2007-06-13 12:07:58	217.147.224.66	TCP/4345	TCP/445
2007-06-13 12:08:01	217.147.224.66	TCP/3555	TCP/135
2007-06-13 12:19:01	217.147.224.66	TCP/3879	TCP/445
2007-06-13 12:19:04	217.147.224.66	TCP/4913	TCP/135
2007-06-13 12:30:53	217.147.224.66	TCP/3286	TCP/445
2007-06-13 12:30:54	217.147.224.66	TCP/3991	TCP/135
2007-06-13 12:40:51	217.147.224.66	TCP/3739	TCP/445
2007-06-13 12:40:54	217.147.224.66	TCP/4984	TCP/135
2007-06-13 12:51:40	217.147.224.66	TCP/4469	TCP/445
2007-06-13 12:51:46	217.147.224.66	TCP/4108	TCP/135
2007-06-13 13:07:07	217.147.224.66	TCP/4867	TCP/135
2007-06-13 13:10:24	217.147.224.66	TCP/4119	TCP/135
2007-06-13 13:10:24	217.147.224.66	TCP/4573	TCP/445
2007-06-13 13:23:26	217.147.224.66	TCP/4594	TCP/135
2007-06-13 13:26:18	217.147.224.66	TCP/4819	TCP/135
2007-06-13 13:26:18	217.147.224.66	TCP/4773	TCP/445
2007-06-13 13:39:43	217.147.224.66	TCP/4849	TCP/135
2007-06-13 13:42:24	217.147.224.66	TCP/4673	TCP/135
2007-06-13 13:42:25	217.147.224.66	TCP/3854	TCP/445
2007-06-13 13:57:34	217.147.224.66	TCP/4780	TCP/135
2007-06-13 13:57:34	217.147.224.66	TCP/3382	TCP/445
2007-06-13 14:14:59	217.147.224.66	TCP/4663	TCP/135
2007-06-13 14:17:48	217.147.224.66	TCP/4256	TCP/135
2007-06-13 14:18:02	217.147.224.66	TCP/4789	TCP/445
2007-06-13 14:34:35	217.147.224.66	TCP/4318	TCP/135
2007-06-13 14:37:41	217.147.224.66	TCP/4486	TCP/135
2007-06-13 14:37:52	217.147.224.66	TCP/3666	TCP/445
2007-06-13 14:51:01	217.147.224.66	TCP/4609	TCP/135
2007-06-13 14:53:44	217.147.224.66	TCP/4129	TCP/135
2007-06-13 14:53:58	217.147.224.66	TCP/4953	TCP/445
2007-06-13 15:06:18	217.147.224.66	TCP/4421	TCP/135
2007-06-13 15:08:32	217.147.224.66	TCP/3629	TCP/135
2007-06-13 15:08:42	217.147.224.66	TCP/4770	TCP/445
2007-06-13 15:08:45	217.147.224.66	TCP/4770	TCP/445
2007-06-13 15:20:17	217.147.224.66	TCP/4729	TCP/135
2007-06-13 15:22:55	217.147.224.66	TCP/4293	TCP/135
2007-06-13 15:23:08	217.147.224.66	TCP/4236	TCP/445
2007-06-13 15:34:30	217.147.224.66	TCP/4567	TCP/135
2007-06-13 15:37:06	217.147.224.66	TCP/4308	TCP/135
2007-06-13 15:37:22	217.147.224.66	TCP/4781	TCP/445
2007-06-13 15:48:35	217.147.224.66	TCP/4130	TCP/135

Continued from last page

Time	Source IP	Source port	Dest. port
2007-06-13 15:50:45	217.147.224.66	TCP/3079	TCP/135
2007-06-13 16:01:15	217.147.224.66	TCP/3925	TCP/135
2007-06-13 16:03:23	217.147.224.66	TCP/3081	TCP/135
2007-06-13 16:13:26	217.147.224.66	TCP/3171	TCP/135
2007-06-13 16:15:30	217.147.224.66	TCP/3092	TCP/135
2007-06-13 16:28:23	217.147.224.66	TCP/3925	TCP/135
2007-06-13 16:39:09	217.147.224.66	TCP/3180	TCP/135
2007-06-13 16:56:10	217.147.224.66	TCP/4448	TCP/135
2007-06-13 17:09:28	217.147.224.66	TCP/3167	TCP/135
2007-06-13 17:11:45	217.147.224.66	TCP/3939	TCP/135
2007-06-13 17:22:30	217.147.224.66	TCP/3168	TCP/135
⋮	⋮	⋮	⋮
2007-06-27 06:54:16	217.147.224.66	TCP/4689	TCP/135
2007-06-27 07:00:30	217.147.224.66	TCP/3308	TCP/135
2007-06-27 07:03:15	217.147.224.66	TCP/3969	TCP/135
2007-06-27 07:07:18	217.147.224.66	TCP/3632	TCP/135
2007-06-27 07:12:46	217.147.224.66	TCP/4529	TCP/445
2007-06-27 07:12:49	217.147.224.66	TCP/4529	TCP/445
2007-06-27 07:13:46	217.147.224.66	TCP/4868	TCP/135
2007-06-27 07:16:31	217.147.224.66	TCP/3545	TCP/135
2007-06-27 07:20:33	217.147.224.66	TCP/4566	TCP/135
2007-06-27 07:27:04	217.147.224.66	TCP/3531	TCP/135
2007-06-27 07:29:47	217.147.224.66	TCP/3625	TCP/135
2007-06-27 07:33:50	217.147.224.66	TCP/3116	TCP/135
2007-06-27 07:40:20	217.147.224.66	TCP/3591	TCP/135
2007-06-27 07:42:33	217.147.224.66	TCP/3987	TCP/139
2007-06-27 07:42:36	217.147.224.66	TCP/3987	TCP/139
2007-06-27 07:43:04	217.147.224.66	TCP/3887	TCP/135
2007-06-27 07:56:18	217.147.224.66	TCP/4261	TCP/135
2007-06-27 08:00:19	217.147.224.66	TCP/3625	TCP/135
2007-06-27 08:06:46	217.147.224.66	TCP/4678	TCP/135
2007-06-27 08:13:28	217.147.224.66	TCP/3661	TCP/135
2007-06-27 08:19:55	217.147.224.66	TCP/3704	TCP/135
2007-06-27 08:22:38	217.147.224.66	TCP/3478	TCP/135
2007-06-27 08:26:36	217.147.224.66	TCP/3361	TCP/135
2007-06-27 08:33:00	217.147.224.66	TCP/3270	TCP/135
2007-06-27 08:39:48	217.147.224.66	TCP/4641	TCP/135
2007-06-27 08:46:10	217.147.224.66	TCP/3156	TCP/135
2007-06-27 08:48:57	217.147.224.66	TCP/4009	TCP/135
2007-06-27 08:49:25	217.147.224.66	TCP/4654	TCP/445
2007-06-27 08:49:28	217.147.224.66	TCP/4654	TCP/445
2007-06-27 08:52:51	217.147.224.66	TCP/4316	TCP/135
2007-06-27 08:59:14	217.147.224.66	TCP/3715	TCP/135
2007-06-27 09:01:59	217.147.224.66	TCP/3837	TCP/135
2007-06-27 09:05:56	217.147.224.66	TCP/3251	TCP/135
2007-06-27 09:12:16	217.147.224.66	TCP/3596	TCP/135
2007-06-27 09:15:01	217.147.224.66	TCP/4674	TCP/135

Continued from last page

Time	Source IP	Source port	Dest. port
2007-06-27 09:18:56	217.147.224.66	TCP/4993	TCP/135
2007-06-27 09:25:18	217.147.224.66	TCP/4013	TCP/135
2007-06-27 09:31:57	217.147.224.66	TCP/4494	TCP/135
2007-06-27 09:32:17	217.147.224.66	TCP/3741	TCP/445
2007-06-27 09:32:20	217.147.224.66	TCP/3741	TCP/445
2007-06-27 09:38:18	217.147.224.66	TCP/3212	TCP/135
2007-06-27 09:40:58	217.147.224.66	TCP/4571	TCP/135
2007-06-27 09:44:52	217.147.224.66	TCP/4677	TCP/135
2007-06-27 09:53:54	217.147.224.66	TCP/4820	TCP/135
2007-06-27 09:57:48	217.147.224.66	TCP/3564	TCP/135
2007-06-27 10:06:45	217.147.224.66	TCP/3981	TCP/135
2007-06-27 10:10:39	217.147.224.66	TCP/4648	TCP/135
2007-06-27 10:16:40	217.147.224.66	TCP/4482	TCP/135
2007-06-27 10:19:26	217.147.224.66	TCP/3558	TCP/135
2007-06-27 10:23:10	217.147.224.66	TCP/4607	TCP/135
2007-06-27 10:27:40	217.147.224.66	TCP/3522	TCP/139
2007-06-27 10:27:44	217.147.224.66	TCP/3522	TCP/139
2007-06-27 10:29:07	217.147.224.66	TCP/4722	TCP/135
2007-06-27 10:31:57	217.147.224.66	TCP/3339	TCP/135
2007-06-27 10:35:25	217.147.224.66	TCP/3485	TCP/135
2007-06-27 10:41:25	217.147.224.66	TCP/4852	TCP/135
2007-06-27 10:47:56	217.147.224.66	TCP/3798	TCP/135
2007-06-27 10:53:50	217.147.224.66	TCP/3790	TCP/135
2007-06-27 10:56:56	217.147.224.66	TCP/3970	TCP/135
2007-06-27 11:00:18	217.147.224.66	TCP/3034	TCP/135
2007-06-27 11:06:20	217.147.224.66	TCP/3316	TCP/135
2007-06-27 11:09:28	217.147.224.66	TCP/3193	TCP/135
2007-06-27 11:12:44	217.147.224.66	TCP/3951	TCP/135
2007-06-27 11:18:35	217.147.224.66	TCP/3593	TCP/135
2007-06-27 11:21:49	217.147.224.66	TCP/4117	TCP/135
2007-06-27 11:24:51	217.147.224.66	TCP/4199	TCP/135
2007-06-27 11:30:44	217.147.224.66	TCP/4630	TCP/135
2007-06-27 11:43:11	217.147.224.66	TCP/4782	TCP/135
2007-06-27 11:56:05	217.147.224.66	TCP/4202	TCP/135
2007-06-27 12:09:34	217.147.224.66	TCP/4694	TCP/135
2007-06-27 12:11:11	217.147.224.66	TCP/4400	TCP/135
2007-06-27 12:14:56	217.147.224.66	TCP/4453	TCP/135
2007-06-27 12:37:02	217.147.224.66	TCP/4153	TCP/135
2007-06-27 12:54:23	217.147.224.66	TCP/4481	TCP/135
2007-06-27 13:06:37	217.147.224.66	TCP/4085	TCP/135
2007-06-27 13:25:02	217.147.224.66	TCP/4311	TCP/135
2007-06-27 13:31:51	217.147.224.66	TCP/4988	TCP/135
2007-06-27 13:35:17	217.147.224.66	TCP/4426	TCP/135
2007-06-27 13:38:09	217.147.224.66	TCP/4086	TCP/135
2007-06-27 13:58:54	217.147.224.66	TCP/3734	TCP/135
2007-06-27 14:26:12	217.147.224.66	TCP/4524	TCP/135
2007-06-27 14:40:09	217.147.224.66	TCP/3467	TCP/135
2007-06-27 14:41:51	217.147.224.66	TCP/4580	TCP/135

Continued from last page

Time	Source IP	Source port	Dest. port
2007-06-27 14:43:21	217.147.224.66	TCP/3481	TCP/135
2007-06-27 14:46:17	217.147.224.66	TCP/4084	TCP/135
2007-06-27 14:53:51	217.147.224.66	TCP/4325	TCP/135
2007-06-27 14:57:16	217.147.224.66	TCP/4761	TCP/135
2007-06-27 15:09:27	217.147.224.66	TCP/4099	TCP/135
2007-06-27 15:38:20	217.147.224.66	TCP/3604	TCP/135
2007-06-27 15:51:00	217.147.224.66	TCP/4915	TCP/135
2007-06-27 15:55:09	217.147.224.66	TCP/3267	TCP/135
2007-06-27 16:02:36	217.147.224.66	TCP/4350	TCP/135
2007-06-27 16:07:42	217.147.224.66	TCP/4822	TCP/445
2007-06-27 16:07:45	217.147.224.66	TCP/4822	TCP/445
2007-06-27 16:08:13	217.147.224.66	TCP/3140	TCP/445
2007-06-27 16:11:54	217.147.224.66	TCP/4614	TCP/135
2007-06-27 16:22:20	217.147.224.66	TCP/3654	TCP/135
2007-06-27 16:36:05	217.147.224.66	TCP/4679	TCP/135
2007-06-27 16:41:32	217.147.224.66	TCP/3964	TCP/139
2007-06-27 16:41:36	217.147.224.66	TCP/3964	TCP/139
2007-06-27 16:58:00	217.147.224.66	TCP/3297	TCP/135
2007-06-27 17:07:22	217.147.224.66	TCP/4229	TCP/445
2007-06-27 17:07:25	217.147.224.66	TCP/4229	TCP/445
2007-06-27 17:07:51	217.147.224.66	TCP/4262	TCP/135
2007-06-27 17:11:31	217.147.224.66	TCP/4319	TCP/135
2007-06-27 17:17:18	217.147.224.66	TCP/4183	TCP/135
2007-06-27 17:25:33	217.147.224.66	TCP/3877	TCP/135
2007-06-27 17:27:38	217.147.224.66	TCP/4938	TCP/135
2007-06-27 17:39:07	217.147.224.66	TCP/4315	TCP/135
2007-06-27 17:41:35	217.147.224.66	TCP/3226	TCP/135
2007-06-27 17:54:33	217.147.224.66	TCP/4292	TCP/135
2007-06-27 17:55:08	217.147.224.66	TCP/4147	TCP/135
2007-06-27 18:06:25	217.147.224.66	TCP/4775	TCP/135
2007-06-27 18:22:34	217.147.224.66	TCP/4505	TCP/135
⋮	⋮	⋮	⋮
2007-06-28 07:15:28	217.147.224.66	TCP/3974	TCP/135
2007-06-28 07:15:57	217.147.224.66	TCP/4218	TCP/135
2007-06-28 07:26:27	217.147.224.66	TCP/3582	TCP/135
2007-06-28 07:26:58	217.147.224.66	TCP/3547	TCP/135
2007-06-28 07:29:05	217.147.224.66	TCP/3809	TCP/139
2007-06-28 07:29:08	217.147.224.66	TCP/3809	TCP/139
2007-06-28 07:37:09	217.147.224.66	TCP/4333	TCP/135
2007-06-28 07:37:37	217.147.224.66	TCP/4340	TCP/135
2007-06-28 07:47:58	217.147.224.66	TCP/3832	TCP/135
2007-06-28 07:58:57	217.147.224.66	TCP/3703	TCP/135
2007-06-28 07:59:22	217.147.224.66	TCP/3893	TCP/135
2007-06-28 08:14:22	217.147.224.66	TCP/4424	TCP/139
2007-06-28 08:14:26	217.147.224.66	TCP/4424	TCP/139
2007-06-28 08:20:36	217.147.224.66	TCP/3637	TCP/135
2007-06-28 08:21:00	217.147.224.66	TCP/3327	TCP/135

Continued from last page

Time	Source IP	Source port	Dest. port
2007-06-28 08:31:36	217.147.224.66	TCP/3416	TCP/135
2007-06-28 08:31:57	217.147.224.66	TCP/4047	TCP/135
2007-06-28 08:53:34	217.147.224.66	TCP/3451	TCP/135
2007-06-28 09:15:09	217.147.224.66	TCP/3700	TCP/135
2007-06-28 09:15:23	217.147.224.66	TCP/4239	TCP/135
2007-06-28 09:25:46	217.147.224.66	TCP/3719	TCP/135
2007-06-28 09:25:57	217.147.224.66	TCP/4001	TCP/135
2007-06-28 09:36:52	217.147.224.66	TCP/4648	TCP/135
2007-06-28 09:37:06	217.147.224.66	TCP/4981	TCP/135
2007-06-28 09:47:52	217.147.224.66	TCP/4775	TCP/135
2007-06-28 09:48:05	217.147.224.66	TCP/4760	TCP/135
2007-06-28 09:58:32	217.147.224.66	TCP/4252	TCP/135
2007-06-28 09:58:43	217.147.224.66	TCP/3966	TCP/135
2007-06-28 10:09:28	217.147.224.66	TCP/3647	TCP/135
2007-06-28 10:09:39	217.147.224.66	TCP/4892	TCP/135
2007-06-28 10:20:08	217.147.224.66	TCP/3873	TCP/135
2007-06-28 10:20:21	217.147.224.66	TCP/4086	TCP/135
2007-06-28 10:31:08	217.147.224.66	TCP/4826	TCP/135
2007-06-28 10:31:24	217.147.224.66	TCP/4738	TCP/135
2007-06-28 10:42:04	217.147.224.66	TCP/3748	TCP/135
2007-06-28 10:42:20	217.147.224.66	TCP/4301	TCP/135
2007-06-28 10:53:13	217.147.224.66	TCP/4874	TCP/135
2007-06-28 10:53:29	217.147.224.66	TCP/4086	TCP/135
2007-06-28 11:04:20	217.147.224.66	TCP/3693	TCP/135
2007-06-28 11:04:36	217.147.224.66	TCP/3883	TCP/135
2007-06-28 11:15:23	217.147.224.66	TCP/4627	TCP/135
2007-06-28 11:15:38	217.147.224.66	TCP/4228	TCP/135
2007-06-28 11:26:25	217.147.224.66	TCP/4981	TCP/135
2007-06-28 11:26:40	217.147.224.66	TCP/4087	TCP/135
2007-06-28 11:36:36	217.147.224.66	TCP/3740	TCP/135
2007-06-28 11:46:32	217.147.224.66	TCP/4512	TCP/135
2007-06-28 13:18:34	217.147.224.66	TCP/4905	TCP/135
2007-06-28 13:18:37	217.147.224.66	TCP/4905	TCP/135
2007-06-28 17:56:30	217.147.224.66	TCP/3956	TCP/139
2007-06-28 17:56:33	217.147.224.66	TCP/3956	TCP/139
2007-06-29 08:11:24	217.147.224.66	TCP/3536	TCP/139
2007-06-29 08:11:28	217.147.224.66	TCP/3536	TCP/139
2007-06-29 09:27:56	217.147.224.66	TCP/3269	TCP/139
2007-06-29 09:28:00	217.147.224.66	TCP/3269	TCP/139
2007-06-29 09:31:03	217.147.224.66	TCP/3378	TCP/139
2007-06-29 09:31:07	217.147.224.66	TCP/3378	TCP/139
2007-06-29 10:01:50	217.147.224.66	TCP/4000	TCP/445
2007-06-29 10:01:53	217.147.224.66	TCP/4000	TCP/445
2007-06-29 10:10:11	217.147.224.66	TCP/3789	TCP/135
2007-06-29 10:10:14	217.147.224.66	TCP/3789	TCP/135
2007-06-29 10:12:37	217.147.224.66	TCP/3202	TCP/135
2007-06-29 10:12:40	217.147.224.66	TCP/3202	TCP/135
2007-06-29 10:58:11	217.147.224.66	TCP/3627	TCP/135

Continued from last page

Time	Source IP	Source port	Dest. port
2007-06-29 10:58:14	217.147.224.66	TCP/3627	TCP/135
2007-06-29 11:20:43	217.147.224.66	TCP/4494	TCP/445
2007-06-29 11:20:46	217.147.224.66	TCP/4494	TCP/445
2007-06-29 11:25:13	217.147.224.66	TCP/4795	TCP/139
2007-06-29 11:25:16	217.147.224.66	TCP/4795	TCP/139
2007-06-29 13:03:51	217.147.224.66	TCP/3900	TCP/139
2007-06-29 13:03:54	217.147.224.66	TCP/3900	TCP/139
2007-06-29 13:14:02	217.147.224.66	TCP/3981	TCP/135
2007-06-29 13:14:05	217.147.224.66	TCP/3981	TCP/135
2007-06-29 13:29:42	217.147.224.66	TCP/4084	TCP/445
2007-06-29 13:29:46	217.147.224.66	TCP/4084	TCP/445
2007-06-29 14:03:01	217.147.224.66	TCP/4447	TCP/445
2007-06-29 14:03:04	217.147.224.66	TCP/4447	TCP/445
2007-06-29 14:18:05	217.147.224.66	TCP/4085	TCP/139
2007-06-29 14:18:08	217.147.224.66	TCP/4085	TCP/139
2007-06-29 14:18:14	217.147.224.66	TCP/3763	TCP/139
2007-06-29 14:18:17	217.147.224.66	TCP/3763	TCP/139
2007-06-30 08:40:49	217.147.224.66	TCP/4069	TCP/445
2007-06-30 08:40:52	217.147.224.66	TCP/4069	TCP/445
2007-06-30 09:15:12	217.147.224.66	TCP/4979	TCP/135
2007-06-30 09:15:15	217.147.224.66	TCP/4979	TCP/135
2007-06-30 09:20:26	217.147.224.66	TCP/4305	TCP/445
2007-06-30 09:20:30	217.147.224.66	TCP/4305	TCP/445
2007-06-30 09:28:30	217.147.224.66	TCP/3486	TCP/445
2007-06-30 09:28:33	217.147.224.66	TCP/3486	TCP/445
2007-06-30 10:33:44	217.147.224.66	TCP/3277	TCP/139
2007-06-30 10:33:47	217.147.224.66	TCP/3277	TCP/139
2007-06-30 10:44:23	217.147.224.66	TCP/4621	TCP/135
2007-06-30 10:44:26	217.147.224.66	TCP/4621	TCP/135
2007-06-30 11:15:39	217.147.224.66	TCP/4768	TCP/139
2007-06-30 11:15:43	217.147.224.66	TCP/4768	TCP/139
2007-06-30 11:41:58	217.147.224.66	TCP/4757	TCP/139
2007-06-30 11:42:02	217.147.224.66	TCP/4757	TCP/139
2007-06-30 12:10:13	217.147.224.66	TCP/4190	TCP/139
2007-06-30 12:10:16	217.147.224.66	TCP/4190	TCP/139
2007-06-30 13:07:58	217.147.224.66	TCP/3782	TCP/139
2007-06-30 13:08:01	217.147.224.66	TCP/3782	TCP/139
2007-06-30 13:38:46	217.147.224.66	TCP/3596	TCP/445
2007-06-30 13:38:49	217.147.224.66	TCP/3596	TCP/445
2007-06-30 14:14:04	217.147.224.66	TCP/3437	TCP/139
2007-06-30 14:14:07	217.147.224.66	TCP/3437	TCP/139
2007-06-30 15:05:00	217.147.224.66	TCP/3667	TCP/139
2007-06-30 15:05:04	217.147.224.66	TCP/3667	TCP/139

6.4 2007-09, 219.148.119.11

Time	Source IP	Source port	Dest. port
2007-09-01 13:03:49	219.148.119.11	TCP/12200	TCP/7212

Continued from last page

Time	Source IP	Source port	Dest. port
2007-09-01 13:10:56	219.148.119.11	TCP/12200	TCP/7212
2007-09-01 13:20:12	219.148.119.11	TCP/12200	TCP/7212
2007-09-01 13:24:54	219.148.119.11	TCP/12200	TCP/7212
2007-09-01 13:29:30	219.148.119.11	TCP/12200	TCP/7212
2007-09-01 13:34:07	219.148.119.11	TCP/12200	TCP/7212
2007-09-01 13:38:44	219.148.119.11	TCP/12200	TCP/7212
⋮	⋮	⋮	⋮
2007-09-02 09:19:55	219.148.119.11	TCP/12200	TCP/7212
2007-09-02 09:24:32	219.148.119.11	TCP/12200	TCP/7212
2007-09-02 09:34:04	219.148.119.11	TCP/12200	TCP/7212
2007-09-02 09:43:46	219.148.119.11	TCP/12200	TCP/7212
2007-09-02 10:20:20	219.148.119.11	TCP/12200	TCP/8000
2007-09-02 10:20:20	219.148.119.11	TCP/12200	TCP/6588
2007-09-02 10:38:07	219.148.119.11	TCP/12200	TCP/1080
2007-09-02 10:53:10	219.148.119.11	TCP/12200	TCP/8000
2007-09-02 10:53:10	219.148.119.11	TCP/12200	TCP/6588
2007-09-02 10:53:10	219.148.119.11	TCP/12200	TCP/7212
2007-09-02 10:53:10	219.148.119.11	TCP/12200	TCP/1080
2007-09-02 11:10:56	219.148.119.11	TCP/12200	TCP/8000
2007-09-02 11:10:56	219.148.119.11	TCP/12200	TCP/6588
2007-09-02 11:10:56	219.148.119.11	TCP/12200	TCP/7212
2007-09-02 11:10:56	219.148.119.11	TCP/12200	TCP/1080
2007-09-02 11:28:58	219.148.119.11	TCP/12200	TCP/8000
2007-09-02 11:28:58	219.148.119.11	TCP/12200	TCP/6588
2007-09-02 11:28:58	219.148.119.11	TCP/12200	TCP/7212
2007-09-02 11:28:58	219.148.119.11	TCP/12200	TCP/1080
2007-09-02 11:47:32	219.148.119.11	TCP/12200	TCP/8000
⋮	⋮	⋮	⋮
2007-09-02 22:54:09	219.148.119.11	TCP/12200	TCP/1080
2007-09-02 23:13:08	219.148.119.11	TCP/12200	TCP/8000
2007-09-02 23:13:08	219.148.119.11	TCP/12200	TCP/6588
2007-09-02 23:13:08	219.148.119.11	TCP/12200	TCP/7212
2007-09-02 23:13:08	219.148.119.11	TCP/12200	TCP/1080
2007-09-02 23:31:29	219.148.119.11	TCP/12200	TCP/8000
2007-09-02 23:31:29	219.148.119.11	TCP/12200	TCP/6588
2007-09-02 23:31:29	219.148.119.11	TCP/12200	TCP/7212
2007-09-02 23:31:29	219.148.119.11	TCP/12200	TCP/1080
2007-09-02 23:49:36	219.148.119.11	TCP/12200	TCP/8000
2007-09-02 23:49:36	219.148.119.11	TCP/12200	TCP/6588
2007-09-02 23:49:36	219.148.119.11	TCP/12200	TCP/7212
2007-09-02 23:49:36	219.148.119.11	TCP/12200	TCP/1080
2007-09-03 00:07:30	219.148.119.11	TCP/12200	TCP/8000
2007-09-03 00:07:30	219.148.119.11	TCP/12200	TCP/6588
2007-09-03 00:07:30	219.148.119.11	TCP/12200	TCP/7212
2007-09-03 00:07:30	219.148.119.11	TCP/12200	TCP/1080
2007-09-03 00:24:34	219.148.119.11	TCP/12200	TCP/7212
2007-09-03 00:34:27	219.148.119.11	TCP/12200	TCP/8080

Continued from last page

Time	Source IP	Source port	Dest. port
2007-09-03 00:47:06	219.148.119.11	TCP/12200	TCP/8000
2007-09-03 00:47:06	219.148.119.11	TCP/12200	TCP/8080
2007-09-03 01:14:11	219.148.119.11	TCP/12200	TCP/8000
2007-09-03 01:14:11	219.148.119.11	TCP/12200	TCP/8080
2007-09-03 01:26:45	219.148.119.11	TCP/12200	TCP/8000
2007-09-03 01:26:45	219.148.119.11	TCP/12200	TCP/8080
2007-09-03 01:40:13	219.148.119.11	TCP/12200	TCP/8080
2007-09-03 01:53:00	219.148.119.11	TCP/12200	TCP/8080
2007-09-03 02:04:53	219.148.119.11	TCP/12200	TCP/8000
2007-09-03 02:04:53	219.148.119.11	TCP/12200	TCP/8080
⋮	⋮	⋮	⋮
2007-09-20 04:49:31	219.148.119.11	TCP/12200	TCP/8000
2007-09-20 04:49:31	219.148.119.11	TCP/12200	TCP/8080
2007-09-20 05:21:42	219.148.119.11	TCP/12200	TCP/8000
2007-09-20 05:21:42	219.148.119.11	TCP/12200	TCP/8080
2007-09-20 05:35:48	219.148.119.11	TCP/12200	TCP/8000
2007-09-20 05:53:11	219.148.119.11	TCP/12200	TCP/8000
2007-09-20 05:53:11	219.148.119.11	TCP/12200	TCP/8080

7 The date/protocol/port list

7.1 2007-02

2007-02-07 TCP/135	2007-02-25 TCP/135
2007-02-13 TCP/135	2007-02-25 TCP/2967
2007-02-18 TCP/135	2007-02-25 TCP/5900
2007-02-19 TCP/445	2007-02-26 TCP/135
2007-02-20 TCP/135	2007-02-26 TCP/2967
2007-02-21 TCP/135	2007-02-27 TCP/135
2007-02-23 TCP/2967	2007-02-27 TCP/2967
2007-02-24 TCP/2967	2007-02-28 TCP/135

7.2 2007-03

2007-03-01 TCP/135	2007-03-15 TCP/139
2007-03-02 TCP/135	2007-03-15 TCP/2967
2007-03-03 TCP/135	2007-03-15 TCP/445
2007-03-04 TCP/135	2007-03-16 TCP/135
2007-03-04 TCP/2967	2007-03-16 TCP/445
2007-03-04 TCP/445	2007-03-18 TCP/2967
2007-03-05 TCP/135	2007-03-19 TCP/135
2007-03-05 TCP/2967	2007-03-19 TCP/2967
2007-03-06 TCP/135	2007-03-19 TCP/445
2007-03-06 TCP/2967	2007-03-20 TCP/135
2007-03-07 TCP/135	2007-03-20 TCP/445
2007-03-09 TCP/135	2007-03-21 TCP/135
2007-03-09 TCP/2967	2007-03-21 TCP/445
2007-03-10 TCP/139	2007-03-22 TCP/139
2007-03-11 TCP/2967	2007-03-23 TCP/2967
2007-03-12 TCP/135	2007-03-24 TCP/139
2007-03-12 TCP/2967	2007-03-25 TCP/139
2007-03-12 TCP/5900	2007-03-25 TCP/2967
2007-03-12 UDP/135	2007-03-26 TCP/135
2007-03-13 TCP/135	2007-03-26 TCP/2967
2007-03-13 TCP/445	2007-03-27 TCP/445
2007-03-14 TCP/135	2007-03-27 TCP/80
2007-03-14 TCP/1433	2007-03-28 TCP/139
2007-03-14 TCP/2967	2007-03-29 TCP/80
2007-03-15 TCP/135	

7.3 2007-04

2007-04-01 TCP/135	2007-04-14 TCP/135
2007-04-01 TCP/139	2007-04-15 TCP/2967
2007-04-01 TCP/2967	2007-04-16 TCP/135
2007-04-01 TCP/5900	2007-04-16 TCP/2967
2007-04-03 TCP/135	2007-04-19 TCP/135
2007-04-03 TCP/2967	2007-04-19 TCP/445
2007-04-06 TCP/135	2007-04-20 TCP/445
2007-04-06 TCP/5900	2007-04-21 TCP/135
2007-04-07 TCP/135	2007-04-22 TCP/135
2007-04-10 TCP/135	2007-04-23 TCP/135
2007-04-13 TCP/135	2007-04-26 TCP/445
2007-04-13 TCP/2967	2007-04-28 TCP/139

7.4 2007-05

2007-05-01 TCP/51927	2007-05-24 TCP/5900
2007-05-03 TCP/139	2007-05-29 TCP/1433
2007-05-10 TCP/139	2007-05-29 TCP/2967
2007-05-10 TCP/22	2007-05-30 TCP/135
2007-05-10 TCP/3306	2007-05-31 TCP/135
2007-05-24 TCP/2967	2007-05-31 TCP/2967
2007-05-24 TCP/445	2007-05-31 TCP/445

7.5 2007-06

2007-06-01 TCP/135	2007-06-18 TCP/1433
2007-06-01 TCP/1433	2007-06-19 TCP/135
2007-06-03 TCP/135	2007-06-19 TCP/2967
2007-06-06 TCP/135	2007-06-20 TCP/135
2007-06-06 TCP/445	2007-06-21 TCP/135
2007-06-06 UDP/135	2007-06-21 UDP/1026
2007-06-08 TCP/80	2007-06-22 TCP/135
2007-06-11 TCP/135	2007-06-22 UDP/1026
2007-06-12 TCP/135	2007-06-23 TCP/135
2007-06-12 TCP/445	2007-06-24 TCP/135
2007-06-13 TCP/135	2007-06-24 TCP/3306
2007-06-13 TCP/445	2007-06-26 TCP/135
2007-06-14 TCP/135	2007-06-27 TCP/135
2007-06-14 TCP/139	2007-06-27 TCP/139
2007-06-15 UDP/1026	2007-06-27 UDP/1026
2007-06-15 UDP/1027	2007-06-27 UDP/1027
2007-06-16 TCP/5900	2007-06-28 TCP/135
2007-06-16 TCP/5901	2007-06-28 TCP/445
2007-06-17 TCP/135	2007-06-29 TCP/135
2007-06-18 TCP/135	2007-06-29 TCP/3306

7.6 2007-07

2007-07-02 TCP/135	2007-07-20 TCP/135
2007-07-02 TCP/25	2007-07-20 TCP/3306
2007-07-02 TCP/36721	2007-07-21 TCP/3306
2007-07-03 TCP/135	2007-07-23 UDP/1026
2007-07-03 UDP/1026	2007-07-23 UDP/1027
2007-07-05 TCP/139	2007-07-25 TCP/2967
2007-07-05 UDP/1026	2007-07-29 TCP/135
2007-07-05 UDP/1027	2007-07-29 TCP/2967
2007-07-06 TCP/2967	2007-07-29 TCP/445
2007-07-13 TCP/135	2007-07-30 TCP/135
2007-07-14 TCP/2967	2007-07-30 TCP/2967
2007-07-16 TCP/445	2007-07-30 TCP/445
2007-07-16 UDP/1027	2007-07-31 TCP/135
2007-07-17 TCP/1433	2007-07-31 TCP/2967
2007-07-19 UDP/1026	2007-07-31 TCP/445
2007-07-19 UDP/1027	

7.7 2007-08

2007-08-01 TCP/2967	2007-08-10 TCP/2967
2007-08-01 TCP/445	2007-08-10 TCP/445
2007-08-02 TCP/135	2007-08-11 TCP/135
2007-08-02 TCP/2967	2007-08-11 TCP/2967
2007-08-02 TCP/445	2007-08-11 TCP/445
2007-08-02 TCP/5900	2007-08-12 TCP/135
2007-08-03 TCP/135	2007-08-12 TCP/2967
2007-08-03 TCP/139	2007-08-12 TCP/445
2007-08-03 TCP/2967	2007-08-13 TCP/135
2007-08-03 TCP/445	2007-08-13 TCP/2967
2007-08-04 TCP/135	2007-08-14 TCP/2967
2007-08-04 TCP/2967	2007-08-14 TCP/445
2007-08-04 TCP/445	2007-08-15 TCP/135
2007-08-05 TCP/445	2007-08-15 TCP/2967
2007-08-06 TCP/135	2007-08-15 TCP/445
2007-08-06 TCP/139	2007-08-16 TCP/135
2007-08-06 TCP/2967	2007-08-16 TCP/2967
2007-08-06 TCP/445	2007-08-16 TCP/445
2007-08-07 TCP/445	2007-08-17 TCP/135
2007-08-08 TCP/135	2007-08-17 TCP/2967
2007-08-08 TCP/2967	2007-08-18 TCP/2967
2007-08-08 TCP/445	2007-08-18 TCP/445
2007-08-09 TCP/135	2007-08-19 TCP/445
2007-08-10 TCP/135	2007-08-20 TCP/135
2007-08-10 TCP/139	2007-08-20 TCP/2967
	2007-08-20 TCP/445
	2007-08-21 TCP/2967

2007-08-21 TCP/445
2007-08-22 TCP/135
2007-08-22 TCP/2967
2007-08-22 TCP/445
2007-08-22 TCP/5900
2007-08-23 TCP/139
2007-08-23 TCP/5168
2007-08-24 TCP/135
2007-08-24 TCP/445
2007-08-25 TCP/2967
2007-08-25 TCP/445
2007-08-26 TCP/135
2007-08-26 TCP/2967
2007-08-27 TCP/139
2007-08-27 TCP/2967
2007-08-27 TCP/445

2007-08-27 TCP/5900
2007-08-27 TCP/7212
2007-08-28 TCP/135
2007-08-28 TCP/1433
2007-08-28 TCP/7212
2007-08-29 TCP/445
2007-08-29 TCP/7212
2007-08-30 TCP/135
2007-08-30 TCP/139
2007-08-30 TCP/445
2007-08-30 TCP/7212
2007-08-31 TCP/135
2007-08-31 TCP/139
2007-08-31 TCP/2967
2007-08-31 TCP/445
2007-08-31 TCP/7212

7.8 2007-09

2007-09-01 TCP/1433
2007-09-01 TCP/5900
2007-09-01 TCP/7212
2007-09-02 TCP/7212
2007-09-03 TCP/135
2007-09-03 TCP/7212
2007-09-03 TCP/8000
2007-09-04 TCP/135
2007-09-04 TCP/2968
2007-09-04 TCP/445
2007-09-04 TCP/7212
2007-09-05 TCP/1433
2007-09-06 TCP/135
2007-09-06 TCP/2967
2007-09-06 TCP/445
2007-09-06 TCP/7212
2007-09-07 TCP/135
2007-09-07 TCP/139
2007-09-07 TCP/445
2007-09-08 TCP/135
2007-09-08 TCP/2967
2007-09-09 TCP/135
2007-09-10 TCP/135
2007-09-11 TCP/139
2007-09-11 TCP/2967
2007-09-11 TCP/7212
2007-09-12 TCP/135

2007-09-12 TCP/139
2007-09-12 TCP/2968
2007-09-12 TCP/445
2007-09-13 TCP/135
2007-09-14 TCP/445
2007-09-14 TCP/5900
2007-09-15 TCP/5900
2007-09-15 TCP/7212
2007-09-16 TCP/135
2007-09-16 TCP/2967
2007-09-16 TCP/7212
2007-09-17 TCP/135
2007-09-17 TCP/1433
2007-09-17 TCP/445
2007-09-17 TCP/5900
2007-09-19 TCP/135
2007-09-19 TCP/1433
2007-09-19 TCP/2967
2007-09-19 TCP/2968
2007-09-20 TCP/135
2007-09-20 TCP/5900
2007-09-21 TCP/135
2007-09-21 TCP/445
2007-09-21 TCP/5900
2007-09-21 TCP/7212
2007-09-22 TCP/135
2007-09-22 TCP/2967
2007-09-22 TCP/7212

2007-09-23 TCP/135
2007-09-23 TCP/139
2007-09-23 TCP/5900
2007-09-23 TCP/7212
2007-09-24 TCP/135
2007-09-24 TCP/2967
2007-09-24 TCP/7212
2007-09-25 TCP/135
2007-09-25 TCP/2968
2007-09-25 TCP/445
2007-09-25 TCP/7212
2007-09-26 TCP/135

2007-09-26 TCP/7212
2007-09-27 TCP/135
2007-09-27 TCP/1433
2007-09-27 TCP/7212
2007-09-28 TCP/135
2007-09-28 TCP/139
2007-09-29 TCP/135
2007-09-29 TCP/445
2007-09-30 TCP/135
2007-09-30 TCP/139
2007-09-30 TCP/2968
2007-09-30 TCP/7212

7.9 2007-10

2007-10-01 TCP/135
2007-10-01 TCP/5900
2007-10-01 TCP/7212
2007-10-02 TCP/135
2007-10-02 TCP/1433
2007-10-02 TCP/2968
2007-10-02 TCP/5900
2007-10-02 TCP/7212
2007-10-03 TCP/135
2007-10-03 TCP/445
2007-10-03 TCP/7212
2007-10-04 TCP/135
2007-10-04 TCP/1433
2007-10-04 TCP/7212
2007-10-05 TCP/135
2007-10-05 TCP/445
2007-10-05 TCP/7212
2007-10-06 TCP/135
2007-10-07 TCP/135
2007-10-07 TCP/2967
2007-10-08 TCP/135
2007-10-08 TCP/2968
2007-10-08 TCP/445
2007-10-09 TCP/135
2007-10-10 TCP/135
2007-10-10 TCP/445
2007-10-11 TCP/135
2007-10-11 TCP/445
2007-10-11 TCP/7212
2007-10-12 TCP/7212
2007-10-13 TCP/135

2007-10-13 TCP/445
2007-10-13 TCP/7212
2007-10-14 TCP/135
2007-10-14 TCP/2967
2007-10-14 TCP/7212
2007-10-15 TCP/135
2007-10-15 TCP/7212
2007-10-16 TCP/135
2007-10-16 TCP/445
2007-10-16 TCP/5900
2007-10-16 TCP/7212
2007-10-17 TCP/135
2007-10-17 TCP/5900
2007-10-17 TCP/7212
2007-10-18 TCP/135
2007-10-18 TCP/7212
2007-10-19 TCP/135
2007-10-19 TCP/7212
2007-10-20 TCP/135
2007-10-20 TCP/7212
2007-10-21 TCP/135
2007-10-21 TCP/2968
2007-10-21 TCP/7212
2007-10-22 TCP/135
2007-10-22 TCP/2967
2007-10-22 TCP/445
2007-10-22 TCP/7212
2007-10-23 TCP/135
2007-10-23 TCP/7212
2007-10-24 TCP/135
2007-10-24 TCP/139
2007-10-24 TCP/1433
2007-10-24 TCP/2967

2007-10-24 TCP/7212
2007-10-25 TCP/135
2007-10-25 TCP/139
2007-10-25 TCP/2967
2007-10-25 TCP/7212
2007-10-26 TCP/135
2007-10-26 TCP/2968
2007-10-26 TCP/7212
2007-10-27 TCP/135
2007-10-27 TCP/2968

2007-10-28 TCP/135
2007-10-28 TCP/7212
2007-10-29 TCP/135
2007-10-29 TCP/7212
2007-10-30 TCP/135
2007-10-30 TCP/445
2007-10-30 TCP/7212
2007-10-31 TCP/135
2007-10-31 TCP/445
2007-10-31 TCP/7212

7.10 2007-11

2007-11-01 TCP/135
2007-11-02 TCP/135
2007-11-02 TCP/445
2007-11-03 TCP/135
2007-11-03 TCP/2968
2007-11-04 TCP/135
2007-11-04 TCP/1433
2007-11-04 TCP/2967
2007-11-04 UDP/1026
2007-11-05 TCP/135
2007-11-05 UDP/1026
2007-11-05 UDP/1027
2007-11-06 TCP/445
2007-11-06 TCP/7212
2007-11-06 UDP/1026
2007-11-07 TCP/135
2007-11-07 TCP/139
2007-11-07 TCP/7212
2007-11-07 UDP/1027
2007-11-08 TCP/135
2007-11-08 TCP/139
2007-11-08 TCP/1433
2007-11-08 TCP/445
2007-11-08 TCP/5900
2007-11-08 TCP/7212
2007-11-08 UDP/1026
2007-11-09 TCP/135
2007-11-09 TCP/139
2007-11-09 TCP/445
2007-11-09 TCP/7212
2007-11-10 TCP/135
2007-11-10 TCP/1433
2007-11-10 TCP/445

2007-11-10 TCP/7212
2007-11-10 UDP/1026
2007-11-10 UDP/1027
2007-11-11 TCP/135
2007-11-11 TCP/139
2007-11-11 TCP/445
2007-11-11 UDP/1026
2007-11-12 TCP/135
2007-11-12 TCP/2967
2007-11-12 UDP/1026
2007-11-13 TCP/135
2007-11-14 TCP/135
2007-11-15 TCP/135
2007-11-16 TCP/135
2007-11-16 TCP/2967
2007-11-17 TCP/135
2007-11-18 TCP/135
2007-11-18 TCP/1433
2007-11-18 TCP/445
2007-11-19 TCP/135
2007-11-19 TCP/139
2007-11-20 TCP/135
2007-11-20 TCP/2967
2007-11-21 TCP/135
2007-11-21 TCP/445
2007-11-21 TCP/5900
2007-11-22 TCP/135
2007-11-22 TCP/1433
2007-11-22 TCP/2967
2007-11-23 TCP/135
2007-11-23 UDP/1026
2007-11-24 TCP/135
2007-11-24 TCP/2967
2007-11-25 TCP/135
2007-11-26 TCP/135

2007-11-27 TCP/135
2007-11-27 TCP/445
2007-11-28 TCP/135

2007-11-29 TCP/135
2007-11-29 UDP/1026
2007-11-30 TCP/135

7.11 2007-12

2007-12-01 TCP/135
2007-12-01 UDP/1026
2007-12-01 UDP/1027
2007-12-02 TCP/135
2007-12-02 UDP/1026
2007-12-03 TCP/135
2007-12-03 UDP/1026
2007-12-04 TCP/135
2007-12-04 TCP/2967
2007-12-04 UDP/1026
2007-12-04 UDP/1027
2007-12-05 TCP/135
2007-12-05 UDP/1026
2007-12-05 UDP/1027
2007-12-06 TCP/135
2007-12-07 TCP/135
2007-12-07 UDP/1026
2007-12-08 TCP/135
2007-12-08 UDP/1026
2007-12-09 TCP/135
2007-12-10 TCP/135
2007-12-10 UDP/1027
2007-12-10 UDP/1028
2007-12-11 TCP/135
2007-12-12 TCP/135
2007-12-12 UDP/1026
2007-12-13 TCP/135
2007-12-13 TCP/2967
2007-12-13 UDP/1026
2007-12-14 TCP/135
2007-12-14 UDP/1026
2007-12-15 TCP/135
2007-12-16 TCP/135
2007-12-16 UDP/1026
2007-12-17 TCP/445
2007-12-17 UDP/1026
2007-12-18 TCP/135
2007-12-19 UDP/1026

2007-12-20 TCP/2968
2007-12-20 TCP/53022
2007-12-21 TCP/135
2007-12-21 TCP/53022
2007-12-21 TCP/5900
2007-12-21 UDP/1026
2007-12-22 TCP/135
2007-12-22 UDP/1026
2007-12-22 UDP/1027
2007-12-23 TCP/135
2007-12-23 TCP/445
2007-12-24 TCP/135
2007-12-24 TCP/445
2007-12-24 TCP/53022
2007-12-25 TCP/135
2007-12-25 TCP/53022
2007-12-25 TCP/5900
2007-12-25 UDP/1026
2007-12-26 TCP/135
2007-12-26 TCP/445
2007-12-26 TCP/53022
2007-12-27 TCP/135
2007-12-27 TCP/53022
2007-12-28 TCP/135
2007-12-28 TCP/445
2007-12-28 TCP/53022
2007-12-28 UDP/1026
2007-12-29 TCP/135
2007-12-29 TCP/2967
2007-12-29 TCP/2968
2007-12-29 TCP/5900
2007-12-29 TCP/5901
2007-12-30 TCP/135
2007-12-30 TCP/139
2007-12-30 UDP/1026
2007-12-31 TCP/135
2007-12-31 TCP/445
2007-12-31 UDP/1026

7.12 2008-01

2008-01-01 TCP/135	2008-01-13 TCP/139
2008-01-01 TCP/445	2008-01-13 UDP/137
2008-01-01 UDP/1027	2008-01-14 TCP/135
2008-01-02 UDP/1026	2008-01-15 TCP/135
2008-01-04 TCP/135	2008-01-15 UDP/137
2008-01-04 TCP/1433	2008-01-16 TCP/135
2008-01-05 TCP/135	2008-01-16 UDP/1026
2008-01-05 UDP/1026	2008-01-18 TCP/135
2008-01-06 TCP/135	2008-01-20 TCP/135
2008-01-06 TCP/2967	2008-01-20 UDP/1026
2008-01-06 UDP/1026	2008-01-21 TCP/445
2008-01-07 TCP/135	2008-01-22 TCP/135
2008-01-07 TCP/7212	2008-01-22 TCP/18019
2008-01-07 TCP/7788	2008-01-22 TCP/2967
2008-01-07 TCP/9788	2008-01-23 TCP/135
2008-01-08 TCP/7212	2008-01-24 TCP/135
2008-01-08 TCP/7788	2008-01-25 TCP/135
2008-01-08 TCP/9788	2008-01-26 TCP/135
2008-01-08 UDP/137	2008-01-27 TCP/135
2008-01-09 TCP/7212	2008-01-27 TCP/5900
2008-01-09 TCP/7788	2008-01-28 TCP/135
2008-01-09 TCP/9788	2008-01-29 TCP/7212
2008-01-10 TCP/135	2008-01-30 TCP/135
2008-01-11 TCP/135	2008-01-30 TCP/7212
2008-01-12 TCP/135	2008-01-31 TCP/135
2008-01-13 TCP/135	

7.13 2008-02

2008-02-01 TCP/135	2008-02-13 TCP/5900
2008-02-02 TCP/135	2008-02-14 TCP/135
2008-02-03 TCP/135	2008-02-14 TCP/445
2008-02-04 TCP/135	2008-02-14 TCP/7212
2008-02-05 TCP/135	2008-02-15 TCP/135
2008-02-06 TCP/135	2008-02-15 TCP/7212
2008-02-07 TCP/135	2008-02-16 TCP/135
2008-02-08 TCP/135	2008-02-17 TCP/135
2008-02-09 TCP/135	2008-02-17 TCP/7212
2008-02-10 TCP/135	2008-02-18 TCP/135
2008-02-11 TCP/135	2008-02-18 TCP/7212
2008-02-12 TCP/135	2008-02-19 TCP/135
2008-02-12 TCP/139	2008-02-19 TCP/2967
2008-02-12 TCP/7212	2008-02-19 TCP/7212
2008-02-13 TCP/135	2008-02-20 TCP/135

2008-02-20 TCP/7212
2008-02-20 UDP/1026
2008-02-21 TCP/135
2008-02-22 TCP/135
2008-02-22 TCP/2968
2008-02-22 TCP/7212
2008-02-23 TCP/135
2008-02-23 TCP/7212
2008-02-24 TCP/135
2008-02-24 TCP/445
2008-02-24 UDP/1026

2008-02-26 TCP/135
2008-02-26 TCP/2967
2008-02-27 TCP/135
2008-02-27 TCP/2967
2008-02-27 TCP/7212
2008-02-28 TCP/135
2008-02-28 TCP/2967
2008-02-28 TCP/7212
2008-02-29 TCP/135
2008-02-29 TCP/2967
2008-02-29 TCP/445