

The Snooper Project
Analysis of Speculative Probing of
Non-Responsive IP Addresses 2008-01-01 –
2008-12-31

Ingvar Mattsson
<ingvar@hexapodia.net>

April 20, 2009

Contents

1	The Snooper Project - background and goal	4
1.1	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	7
3	Anomalies	8
3.1	Purpose	8
3.2	Methodology	8
3.3	2008-01	8
3.4	2008-02	9
3.5	2008-03	9
3.6	2008-04	10
3.7	2008-05	10
3.8	2008-06	11
3.9	2008-07	11
3.10	2008-08	11
3.11	2008-09	11
3.12	2008-10	12
3.13	2008-11	12
3.14	2008-12	12
4	Graphs	13
A	Month-by-month statistic overview	19
A.1	Statistics for 2008-01	19
A.2	Statistics for 2008-02	21
A.3	Statistics for 2008-03	23
A.4	Statistics for 2008-04	25
A.5	Statistics for 2008-05	27
A.6	Statistics for 2008-06	29
A.7	Statistics for 2008-07	31
A.8	Statistics for 2008-08	33
A.9	Statistics for 2008-09	35
A.10	Statistics for 2008-10	37
A.11	Statistics for 2008-11	39
A.12	Statistics for 2008-12	41
B	A detailed look at a few probe sequences	43
B.1	Ping and SMB probes, 2008-10	43
B.2	Slammer probes, 2008-12-10	43

C	Full list of detected anomalies	44
C.1	2008-01	44
C.2	2008-02	44
C.3	2008-03	45
C.4	2008-04	46
C.5	2008-05	46
C.6	2008-06	47
C.7	2008-07	48
C.8	2008-08	48
C.9	2008-09	49
C.10	2008-10	49
C.11	2008-11	49
C.12	2008-12	50
D	Ports and application map	51

1 The Snooper Project - background and goal

1.1 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 2008-01-01 to 2008-12-31.

The base assumption at the start of the Snooper Project (early February 2007) was that a completely unresponsive IP address would still see a fair bit of probing. An underlying thought was to comprehensively demonstrate that the filtering of ICMP packets (in general) and ICMP ECHO (specifically) was not a significant increase in safety for hosts and networks.

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, as there may be a difference in how organised probe sources scan different types of address ranges.

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

¹currently 100 packets

²<http://www.hexapodia.net/snooper/>

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

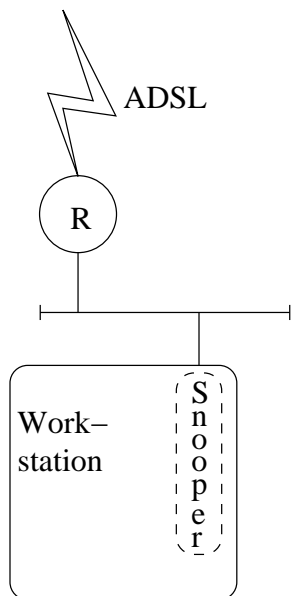


Table 1: Brief sketch of the Snooper Project network

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.

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.

There are some obvious weaknesses with the data collection. The actual connection is a 'business-grade ADSL', rather than being housed in a data centre. There was also at least one multi-day period of "not on the network" and that may well have skewed the statistics closer to the end of the year. This period is instantly visible in the stream graphs presented on pp. 15, 17.

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

First, thanks are extended to Leigh Honeywell for general encouragement.

I'd also like to thank Kent Engström, ... for assisting in reading through draft versions 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.

2 General observations

One of the things I wanted to see, when I started the Snooper Project, back in 2007, was to what extent probes started with ICMP ECHO or went straight into payload packets. My conclusion after the first report was that there's a definite component of "to some extent, ICMP probing happens before actual vulnerability probing", but that the data was sufficiently clear on the fact that just blocking ICMP ECHO doesn't do you much good in terms of stopping attacks.

A brief look at the monthly summary for January, 2008, is quite clear on "blocking ICMP ECHO is not a sufficient protective measure" (3791 distinct probe sources, 1952 ICMP packets seen). As most ICMP probes are at least two ICMP packets, filtering out ICMP would, at most, discourage 976 source hosts. While that is almost 26% of the probing hosts, the probe source count is still quite high.

The 2008 statistics do, however, indicate that sources that cannot solicit an ICMP ECHO response will not attack, so it is less clear from the 2008 statistics that filtering ICMP responses is useless.

3 Anomalies

3.1 Purpose

By looking at probe intensity trends and correlate rise in activity to suspected vulnerabilities using that port, at or around that day, we may gain an insight in how scanning/probing relates to new or re-surfaced vulnerabilities.

3.2 Methodology

To detect a trend, I've used a moving average with a "seasonal component"⁴⁵. Each protocol/port combination have been processed separately, to make it easier to determine when a given port has had an increase in probe activity.

Table 2: Exponential average with weighed seasonal component

In the following formula, A_t is the moving average for time t (the time increment is one hour) and W_t is the weighed average for a given time. N_t is the number of probes for time t . Without too much research⁶, the weight (α) between "current" and "seasonal" has been set to 0.9.

$$A_{t+1} = N_{t+1} + (A_t - N_{t+1})e^{-1/24} \quad W_t = \alpha A_t + (1 - \alpha)A_{t-24}$$

An increase in rate has been deemed significant if (and only if) N_{t+1} is both higher than 6 and more than twice W_t . Comparing with last year's experimentation⁷, the sensitivity seems to be more related to the "higher than N" than the amount it exceeds the moving average. However, poking around with the criteria, these values seem to be a good compromise between "detects probe rate increase" and "doesn't generate too many false indications".

The flagged anomalies, worthy of further investigation, have been correlated with BugTraq and SecurityFocus.com. For SecurityFocus.com, a homebrew script has been used to generate a database table of vulnerability release dates and a CGI script that accepts a target date and lists all CVE IDs released in a window of 10 days before until five days after the specified date. BugTraq has been referenced by manually searching mailing list archives, primarily focussing around the anomaly date and trying to spot keywords related to the expected vulnerable service.

3.3 2008-01

The year starts on a high note for TCP/135 (SMB services) and UDP/1027 (seems to be targetted at MSN Messenger, presumably SPIM) on the 1st. SPIM, SQL Slammer and SMB probes continue to set the pattern until the 6th, where TCP/2967 surges. Now, TCP/2967 seems to be the Symantec AV client and there's no obvious vulnerability in the time window and though there was a ClamAV vulnerability reported on 2007-12-29, this is probably not related.

On the seventh, we see TCP/7212, TCP/9788 and TCP/7788 spike, this seems to be FileSPHERE (TCP/9788) and the PTC License Server (TCP/7788).

⁴http://www.usenix.org/publications/library/proceedings/cinci93/full_papers/hoogen.txt

⁵<http://www.usenix.org/events/lisa2000/brutlag.html>

⁷"The Snooper Report", p. 7; <http://www.hexapodia.net/snooper/snooper/report-20070201-20080229.pdf>

No real information about why these would spike, as there seems to be no related vulnerability published. TCP/7212 is GhostSurf, a P2P application that seems to, in at least some versions, default to being a wide-open proxy. It'd make sense probing for that not long after Xmas, as there'd be at least some expectations of newly installed computers, with as-yet non-modified default installs.

This pattern continues on the 8th and 9th. From the 10th until the 21st, we see assorted SMB-related ports and what is probably SPIM. On the 21st, we see a rise for TCP/445 (MS CIFS) and this *may* be related to a vulnerability in MS LSASS⁸, even though that seems to be a local-only exploit (TCP/445 has been implicated for earlier LSASS vulnerabilities).

On the 22nd, we see a rise for TCP/18019, something noted in the previous report as “unidentified” and that is still the case. The 22nd also sees a rise for TCP/2967, but no obvious vulnerability ties in with this.

There's more SMB floating around until the 27th, when TCP/5900 (VNC) has a rise and this may be correlated to a remote exploit in UltraVNC, published on the 25th⁹, though the exploit only affects the viewer.

The remainder of the month is more GhostSurf and SMB.

3.4 2008-02

February continues with daily peaks of SMB traffic, until the 12th, when GhostSurf (TCP/7212) re-surfaces. On the 13th, there's a spike for VNC, maybe correlated to a vulnerability reported in UltraVNC on the 8th¹⁰. Again, these are viewer-only, so the rough co-incidence in time may well be just random.

More SMB and GhostSurf until the 19th, where we see a spike for TCP/2967 (Symantec AV). There's no obvious vulnerability report for this, but again comes not long after a vulnerability in ClamAV¹¹.

Some more GhostSurf and assorted Microsoft protocols show up until the 22nd, when TCP/2968 (ENPP, whatever that is) shows up. The month then continues with a mix of Microsoft protocols and GhostSurf.

3.5 2008-03

March start with the normal mix of SMB, GhostSurf and occasional probes for Symantec AV clients. Then, on the 9th, there's a probe peak for TCP/23 (telnet). This cannot readily be attributed to any vulnerability, however.

A mix of telnet probes and Symantec AV continues apace until the 19th, when TCP/1433 jumps in. Now, that's registered to MS SQL Server, but the “classic” on that port is SQL Slammer and UDP-based, not TCP-based. There is no obvious vulnerability report connected with this, however.

A mix of telnet, Symantec AV and the occasional Messenger or MS SQL probe continues through to the end of the month, with no obvious correlation to vulnerability reports.

⁸<http://www.securityfocus.com/bid/27099>

⁹<http://www.securityfocus.com/bid/27561>

¹⁰<http://www.securityfocus.com/bid/27687>

¹¹<http://www.securityfocus.com/bid/27751>

3.6 2008-04

The whole month of April is an eclectic mix of peaking probe rates, mostly involving Symantec AV, telnet and the other “normal” ports.

Looking on the vulnerability side, there may finally be some explanations for the prevalence of telnet probes.

On April 8th¹², a hard-coded password vulnerability in the Nortel CS1000 communications server was published. It’s hard to get exact details on this vulnerability, so it may be that telnet was not an exploit vector.

On April 29th¹³, there is a vulnerability published about a log-file obfuscation vector through login, obviously accessible via an open telnet port. This is, essentially, a new vector to a vulnerability published on 2007-07-13¹⁴ that relies on the same path through the syslog subsystem.

On the Symantec AV side, there’s a vulnerability published on April 2nd¹⁵ that may, possibly, be related to the popularity of probes aimed at the AV client.

3.7 2008-05

May starts with the normal mix we almost never see vulnerabilities for (in this specific case: TCP/7212, TCP/9788 and UDP/1026). Then, on the 4th, we see VNC (TCP/5900) pop up. There’s no obvious vulnerability correlated with this however.

On the 8th, telnet (TCP/23) re-appears. Again, no obvious vulnerability correlated with this. The EUsecWest 2008 speaker announcement, on May 8th¹⁶ may, possibly, have sparked an interest, but is more inspiration than vulnerability.

The “normal mix” is temporarily augmented by TCP/23 and TCP/135 and this continues until the 17th, when SQL Server (TCP/1433) makes a re-appearance. As tiresome as it is, there is again no obvious vulnerability to tie this to.

This state of affairs continues until the 28th, when TCP/8000 (usually used for HTTP, but not formally assigned to anything). Looking at BugTraq and SecurityFocus, there is one vulnerability¹⁷ that rings true, though only BugTraq uses TCP/8000 as destination port.

The 29th sees TCP/23, UDP/1027 and TCP/7212, then on the 30th, we see TCP/8080 jump to the foreground. This MAY be related to a TomCat vulnerability published on June 2nd¹⁸ or possibly related to one or more vulnerabilities in Computer Associates eTrust gateway, published on June 4th¹⁹. There’s also a spike for TCP/445 (CIFS Raw). This is most probably a reaction to a Samba vulnerability report from May 28th²⁰. The rest of the month sees TCP/8080, TCP/9788 and TCP/7212.

¹²<http://www.securityfocus.com/bid/28691>

¹³<http://www.securityfocus.com/bid/28983>

¹⁴<http://www.securityfocus.com/bid/26097>

¹⁵<http://www.securityfocus.com/bid/28507>

¹⁶<http://seclists.org/bugtraq/2008/May/0115.html>

¹⁷<http://seclists.org/bugtraq/2008/May/0232.html>, <http://www.securityfocus.com/bid/29317>

¹⁸<http://www.securityfocus.com/bid/29502>

¹⁹<http://www.securityfocus.com/bid/29528>, <http://seclists.org/bugtraq/2008/Jun/0039.html>,

<http://seclists.org/bugtraq/2008/Jun/0040.html>, <http://seclists.org/bugtraq/2008/Jun/0041.html>

²⁰<http://seclists.org/bugtraq/2008/May/0315.html>, <http://www.securityfocus.com/bid/29404>

3.8 2008-06

June starts with the usual mix of ports, not easily attributable to any specific vulnerability. Then, comes the 14th, we see both TCP/3128 (usually Squid or other web proxies) and TCP/1433 come to the fore. Alas, there is nothing we can tie this to.

The month continues with the usual blend, until TCP/8724 (??) pops up on the 24th. At the moment, I can't even tie this to any specific application, so trying to find a vulnerability to tie it to is the proverbial needle in the equally proverbial haystack.

That, however, brings the flagged anomalies in June to an end.

3.9 2008-07

July starts off with a somewhat reduced version of "the normal mix". TCP/23 dominates the flagged anomalies until the 14th, when TCP/8000 comes to the fore. Unfortunately, there's no easily-correlatable vulnerability, but these things happen.

The remainder of July continues in roughly the same fashion. Nothing that seems correlatable with anything else.

3.10 2008-08

August starts slow, with nothing flagged before the 6th, where we see lots of telnet (still no obvious vulnerability, alas). On the 12th, it's time for a newcomer among the flagged ports, UDP/1028. This is, apparently, another Microsoft protocol port and it seems it's used for (among other things) DCOM. More likely, someone tyoped a config file.

There's a scattering of telnet, CIFS and Messenger spam, until te 24th, when another newcomer is flagged, UDP/26828. Since I can't actually identify the port, I can't (yet) correlate it to any vulnerability reports.

The remainder of the month is a mix of same-old same-old.

3.11 2008-09

The month starts with TCP/9788 and TCP/7212, then shifts briefly into SMB ports (TCP/135) on the 5th, over into telnet (TCP/23) on the 10th and then back to the FileSphere/GhostSurf until the 17th, when TCP/8000 pops up. This is normally a web-server port, but no obvious vulnerabilities anywhere near in time (there's the SAP-related vulnerability in May, but...).

On the 19th, we see a rate spike for TCP/1080, usually associated with SOCKS. We can, indeed, see one vulnerability for a SOCKS-providing software published on the same day (CCProxy²¹), even though hte vulnerability itself is the HTTP part of the proxy.

Nothing at all until the 26th, when TCP/1433 jumps out, without any obvious vulnerability correlation. The month then fizzles out with some TCP/23 and some TCP/2967.

²¹<http://www.securityfocus.com/bid/31416>

3.12 2008-10

October starts with TCP/8000 on the 4th, then continues with a steady flagging for TCP/23 (with a small moment of TCP/135 and TCP/445 on the 9th) until the 19th, when TCP/5900 pops up out of the noise. Lo and behold, on the 20th, there's a vulnerability report for RealVNC²².

The rest of the month is a mix of TCP/23, TCP/135 and TCP/139 that cannot be correlated to any vulnerability reports.

3.13 2008-11

November starts with a mix of YCP/23 and TCP/135 (telnet and assorted SMB). It then continues in the same fashion all through the month. Unfortunately, these (and web-based exploits) are among the hardest to pin to any specific vulnerability.

Bit of a let-down, as these things go, but we can but shrug and soldier on.

3.14 2008-12

December starts with UDP/44923, unfortunately I can't find out what service this port is associated with.

The month then continues with telnet (TCP/23) being flagged up. After that, it's a mix of telnet and various SMB ports. Again, no specific vulnerability report can be pinned to any flagged anomaly.

²²<http://www.securityfocus.com/bid/31832>

4 Graphs

The following graphs are attempts at illustrating various aspects of the captured data in graphical form. The stream graphs have “count” on the vertical axis and “time” on the horizontal axis, with an attempt to group different ports so that they form a continuously filled field for the duration. Due to the sheer size of a key, they are unfortunately un-keyed, but should still show the difference between TCP and UDP probes and give a rough idea of varying probe intensities over the year.

The other presented graphs probably do not need any specific introduction.

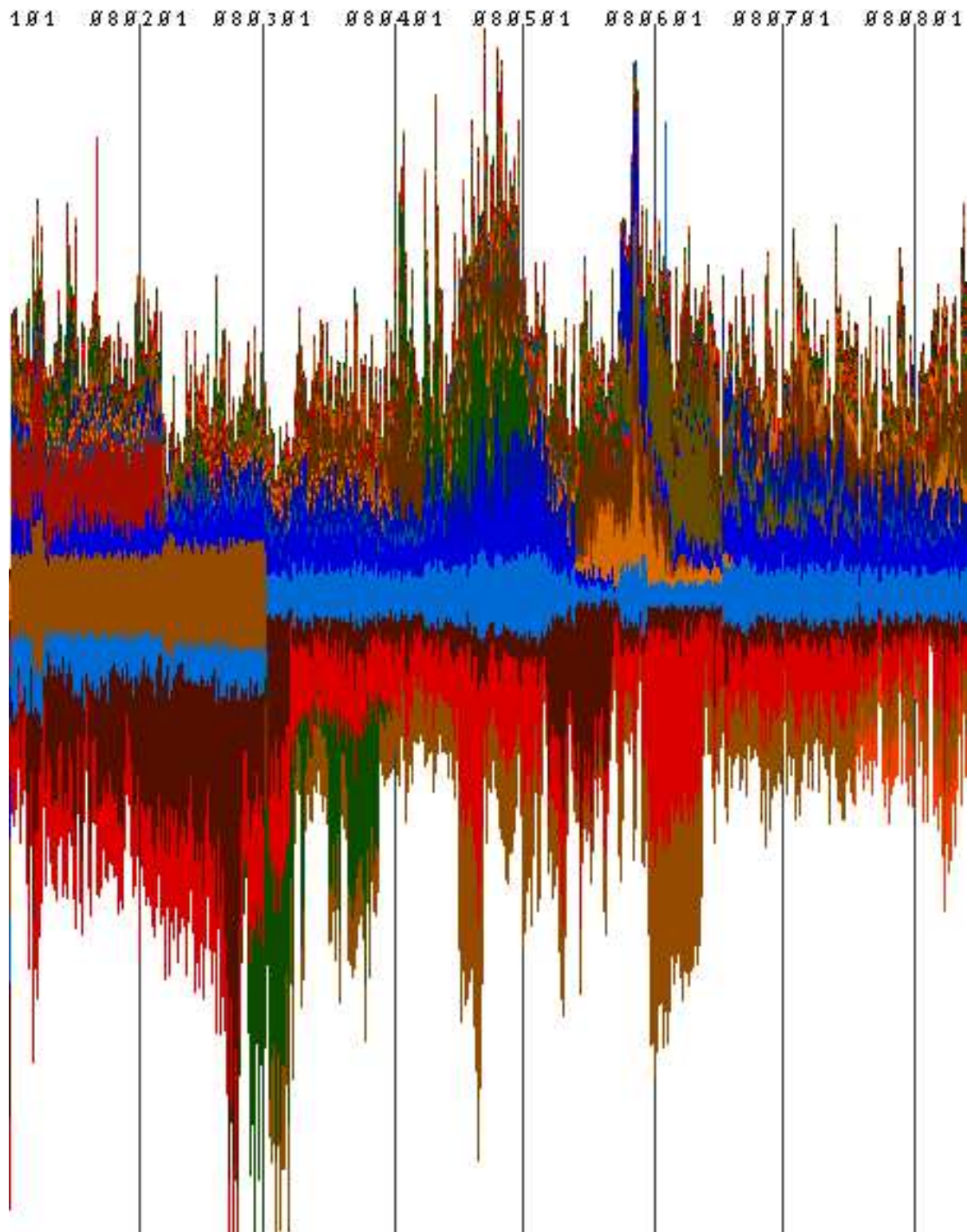


Table 3: Stream graph displaying all packets captured, colour-coded by protocol and port. Red tones indicate TCP packets, blue tones indicate UDP packets. The graph spans from 2008-01-01 to 2008-08-13.

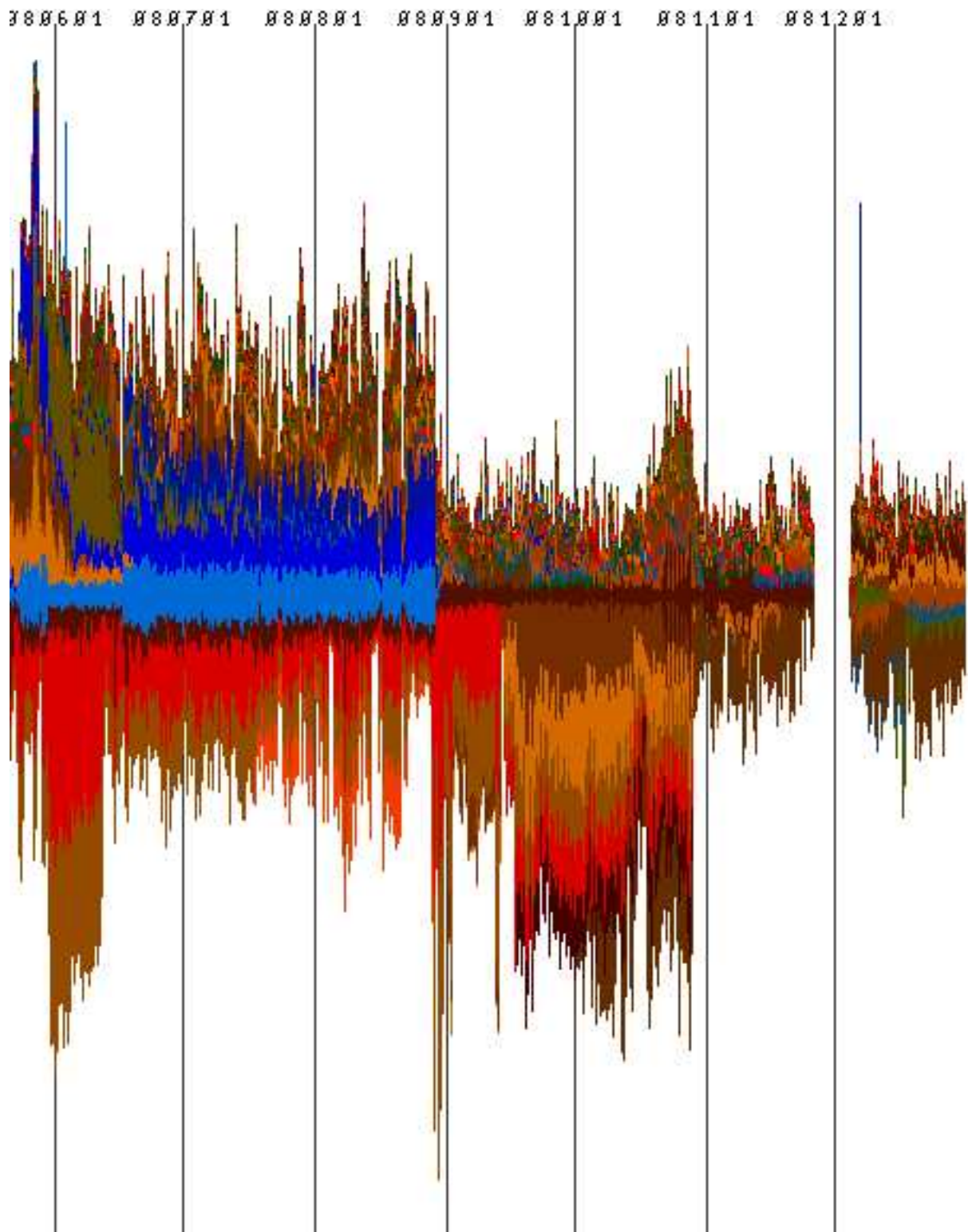


Table 4: Stream graph displaying all packets captured, colour-coded by protocol and port. Red tones indicate TCP packets, blue tones indicate UDP packets. The graph spans from 2008-01-01 to 2008-08-13.

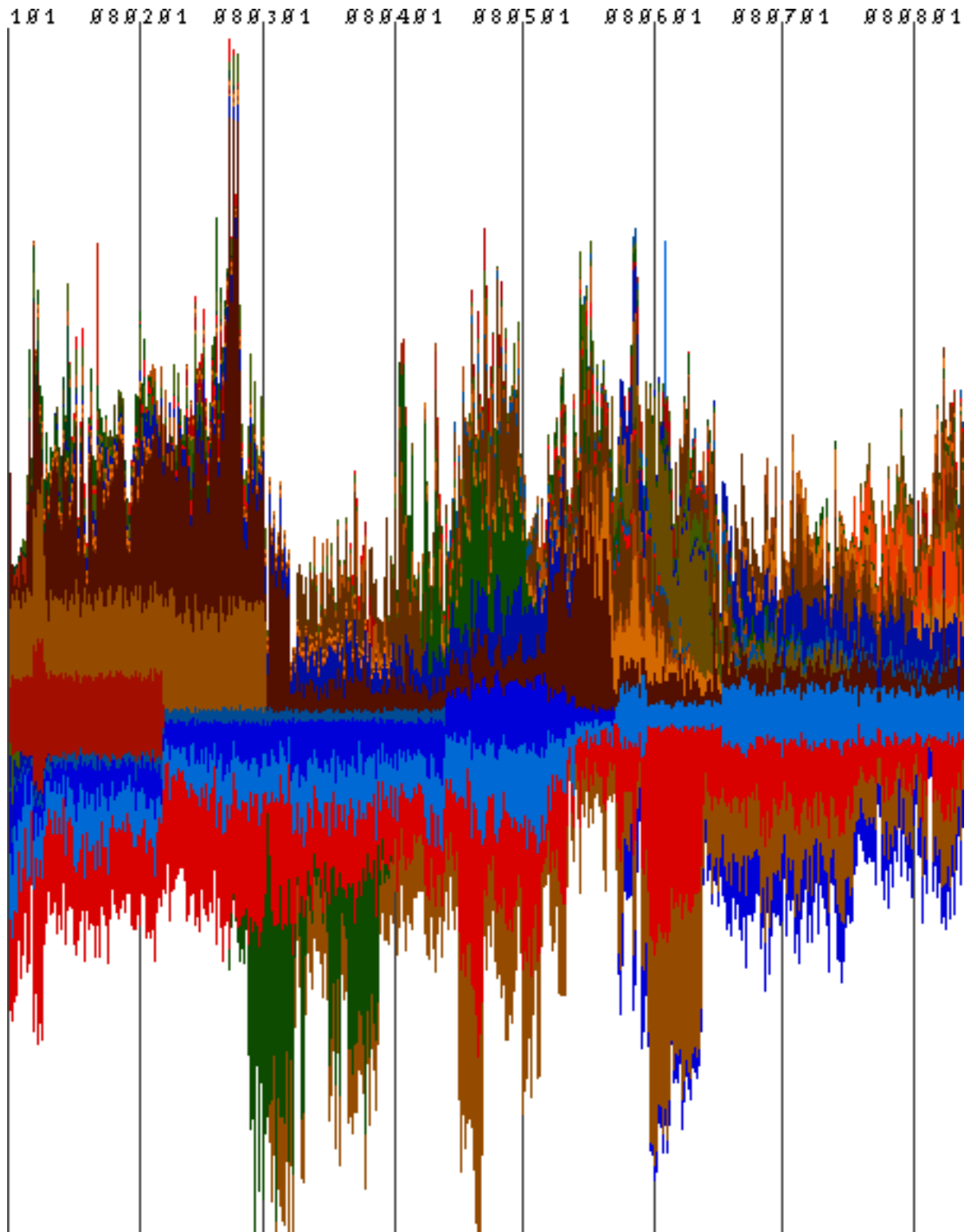


Table 5: Stream graph displaying all proto/port combinations with at least 30 packets captured, colour-coded by protocol and port. Red tones indicate TCP packets, blue tones indicate UDP packets. The graph spans from 2008-05-21 to 2008-12-31.

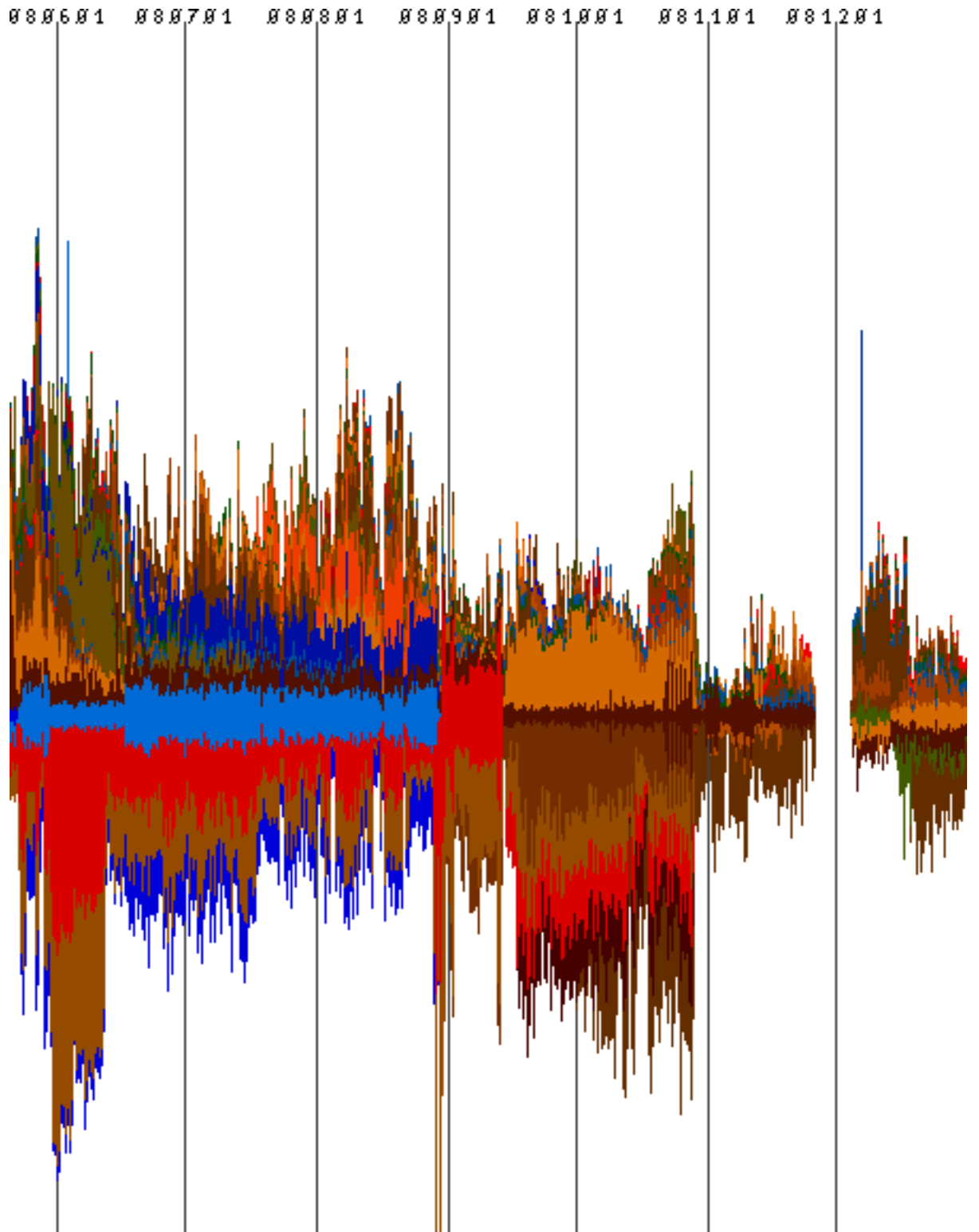


Table 6: Stream graph displaying all proto/port combinations with at least 30 packets captured, colour-coded by protocol and port. Red tones indicate TCP packets, blue tones indicate UDP packets. The graph spans from 2008-05-21 to 2008-12-31.

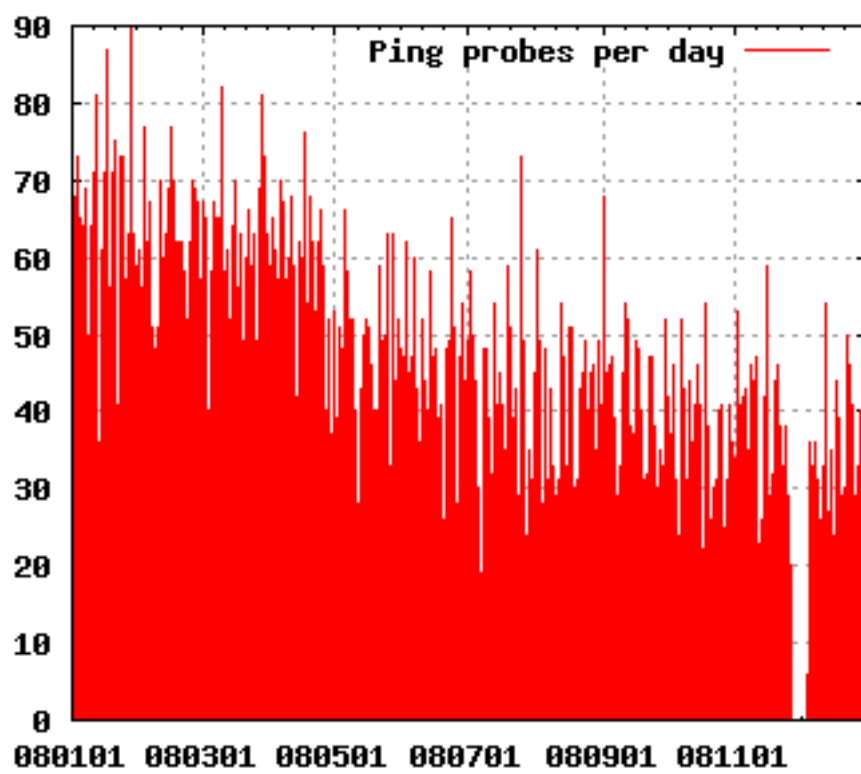


Table 7: ICMP echos received each day throughout 2008.

A Month-by-month statistic overview

The following section contains some statistical overviews of the year, tabulated month by month.

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.

A.1 Statistics for 2008-01

Table 8: Statistical breakdown, 2008-01

TCP packets, total	12809
UDP packets, total	2973
ICMP packets, total	1952
Distinct sources	3791
Distinct TCP ports	95
Distinct UDP ports	23

Table 9: Top 12 TCP packets, 2008-01

port	count
tcp/135	2771
tcp/7212	2595
tcp/9788	2416
tcp/7788	2376
tcp/2967	412
tcp/445	289
tcp/139	178
tcp/5900	174
tcp/1433	166
tcp/22	164
tcp/2968	155
tcp/3128	137

Table 10: Top 12 UDP packets, 2008-01

port	count
udp/1026	1349
udp/1027	825
udp/137	272
udp/1028	257
udp/1434	248
udp/53	3
udp/1357	3
udp/63555	1
udp/8677	1
udp/20984	1
udp/15362	1
udp/27757	1

Table 11: Top 12 probe sources, 2008-01

host	count
121.18.13.107	6539
121.18.13.100	553
218.63.236.143	282
83.105.36.56	150
222.239.255.43	125
218.234.41.8	116
121.14.136.101	104
218.3.134.250	98
218.233.198.25	95
222.73.204.17	94
91.125.70.12	68
218.10.137.142	63

A.2 Statistics for 2008-02

Table 12: 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 13: 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 14: 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 15: 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

A.3 Statistics for 2008-03

Table 16: Statistical breakdown, 2008-03

TCP packets, total	12416
UDP packets, total	3642
ICMP packets, total	1899
Distinct sources	5823
Distinct TCP ports	85
Distinct UDP ports	33

Table 17: Top 12 TCP packets, 2008-03

port	count
tcp/2967	3527
tcp/7212	2330
tcp/9788	1995
tcp/135	1394
tcp/23	1097
tcp/1433	397
tcp/445	197
tcp/5900	174
tcp/22	162
tcp/1080	131
tcp/3128	126
tcp/6588	120

Table 18: Top 12 UDP packets, 2008-03

port	count
udp/1026	1334
udp/1027	1207
udp/1028	751
udp/1434	227
udp/137	89
udp/53	5
udp/7100	3
udp/8947	1
udp/9502	1
udp/9275	1
udp/8700	1
udp/8772	1

Table 19: Top 12 probe sources, 2008-03

host	count
121.18.13.107	4039
218.63.236.143	278
218.234.41.8	119
222.239.255.43	119
218.233.198.25	116
218.3.134.250	106
121.14.136.101	95
83.80.218.184	84
202.97.238.194	61
83.34.33.95	57
221.209.110.13	56
202.97.238.204	53

A.4 Statistics for 2008-04

Table 20: Statistical breakdown, 2008-04

TCP packets, total	12242
UDP packets, total	4380
ICMP packets, total	1728
Distinct sources	5204
Distinct TCP ports	87
Distinct UDP ports	6

Table 21: Top 12 TCP packets, 2008-04

port	count
tcp/9788	2494
tcp/7212	2488
tcp/2967	2244
tcp/23	1852
tcp/135	821
tcp/1433	422
tcp/445	242
tcp/5900	228
tcp/8000	207
tcp/3128	187
tcp/2968	170
tcp/22	145

Table 22: Top 6 UDP packets, 2008-04

port	count
udp/1026	1635
udp/1027	1397
udp/1028	1004
udp/1434	248
udp/137	94
udp/10000	2

Table 23: Top 12 probe sources, 2008-04

host	count
121.18.13.107	2246
61.164.148.109	2097
125.65.112.135	374
221.12.22.20	374
221.12.22.25	310
83.105.23.49	190
83.105.84.151	135
125.65.112.192	124
83.105.96.205	114
83.105.58.87	106
83.83.133.6	95
121.14.136.101	90

A.5 Statistics for 2008-05

Table 24: Statistical breakdown, 2008-05

TCP packets, total	12200
UDP packets, total	3435
ICMP packets, total	1449
Distinct sources	4088
Distinct TCP ports	97
Distinct UDP ports	20

Table 25: Top 12 TCP packets, 2008-05

port	count
tcp/135	2377
tcp/7212	2190
tcp/9788	2059
tcp/23	1535
tcp/8000	923
tcp/8080	650
tcp/2967	452
tcp/3128	363
tcp/1433	300
tcp/445	251
tcp/22	210
tcp/5900	154

Table 26: Top 12 UDP packets, 2008-05

port	count
udp/1026	1266
udp/1027	1096
udp/1028	757
udp/1434	212
udp/137	83
udp/53	5
udp/1369	2
udp/1358	2
udp/2000	1
udp/1484	1
udp/1383	1
udp/1427	1

Table 27: Top 12 probe sources, 2008-05

host	count
221.12.22.25	1782
61.164.148.109	1723
60.172.223.15	956
122.224.134.55	645
125.65.112.135	485
121.15.220.104	212
125.65.165.139	196
83.117.21.64	156
125.65.112.192	100
121.14.136.101	97
83.105.52.137	89
213.120.111.122	86

A.6 Statistics for 2008-06

Table 28: Statistical breakdown, 2008-06

TCP packets, total	12150
UDP packets, total	2987
ICMP packets, total	1357
Distinct sources	3335
Distinct TCP ports	87
Distinct UDP ports	24

Table 29: Top 12 TCP packets, 2008-06

port	count
tcp/7212	3131
tcp/9788	2991
tcp/8080	1655
tcp/23	1191
tcp/135	725
tcp/8000	410
tcp/3128	386
tcp/445	338
tcp/2967	234
tcp/1433	227
tcp/5900	174
tcp/22	121

Table 30: Top 12 UDP packets, 2008-06

port	count
udp/1026	1050
udp/1027	944
udp/1028	593
udp/1434	215
udp/137	82
udp/53	75
udp/8724	3
udp/6817	2
udp/4554	2
udp/7298	2
udp/3677	2
udp/8479	2

Table 31: Top 12 probe sources, 2008-06

host	count
61.164.148.109	3866
122.224.134.55	2024
121.15.220.104	931
125.65.165.139	875
125.65.112.135	316
221.12.22.25	221
60.172.223.15	205
125.65.112.192	88
195.11.55.180	78
121.14.136.101	72
125.211.198.8	63
125.211.198.21	59

A.7 Statistics for 2008-07

Table 32: Statistical breakdown, 2008-07

TCP packets, total	8298
UDP packets, total	4195
ICMP packets, total	1289
Distinct sources	4187
Distinct TCP ports	265
Distinct UDP ports	16

Table 33: Top 12 TCP packets, 2008-07

port	count
tcp/7212	1629
tcp/9788	1618
tcp/23	1077
tcp/135	645
tcp/8118	580
tcp/8000	398
tcp/3128	385
tcp/8080	384
tcp/1433	184
tcp/2967	162
tcp/445	142
tcp/22	137

Table 34: Top 12 UDP packets, 2008-07

port	count
udp/1026	1458
udp/1027	1231
udp/1028	1131
udp/1434	241
udp/137	97
udp/135	11
udp/44671	6
udp/9034	4
udp/5257	4
udp/5426	3
udp/5473	3
udp/5568	2

Table 35: Top 12 probe sources, 2008-07

host	count
61.164.148.109	3808
125.65.165.139	728
125.65.112.135	287
83.105.97.193	163
125.65.112.217	115
83.104.226.72	101
207.44.226.156	94
125.65.112.192	87
121.14.136.101	75
83.105.96.205	72
74.52.134.9	64
59.36.101.9	63

A.8 Statistics for 2008-08

Table 36: Statistical breakdown, 2008-08

TCP packets, total	9537
UDP packets, total	3507
ICMP packets, total	1243
Distinct sources	3808
Distinct TCP ports	154
Distinct UDP ports	8

Table 37: Top 12 TCP packets, 2008-08

port	count
tcp/9788	1780
tcp/7212	1681
tcp/8118	1118
tcp/23	713
tcp/135	610
tcp/1080	559
tcp/3128	469
tcp/8000	450
tcp/8080	296
tcp/1433	271
tcp/445	157
tcp/22	124

Table 38: Top 8 UDP packets, 2008-08

port	count
udp/1026	1209
udp/1028	1017
udp/1027	983
udp/1434	197
udp/137	80
udp/26828	16
udp/49153	4
udp/5060	1

Table 39: Top 12 probe sources, 2008-08

host	count
61.164.148.102	2255
61.164.148.109	1590
222.208.183.218	1261
125.65.165.139	798
222.180.37.14	346
221.192.199.34	340
83.105.58.87	102
59.36.101.9	85
83.105.117.97	78
83.117.21.64	77
121.14.136.101	74
125.65.112.172	53

A.9 Statistics for 2008-09

Table 40: Statistical breakdown, 2008-09

TCP packets, total	10711
UDP packets, total	449
ICMP packets, total	1214
Distinct sources	1823
Distinct TCP ports	85
Distinct UDP ports	5

Table 41: Top 12 TCP packets, 2008-09

port	count
tcp/9788	2122
tcp/7212	2109
tcp/1080	1770
tcp/8000	1238
tcp/8800	722
tcp/23	499
tcp/135	487
tcp/3128	248
tcp/1433	231
tcp/2967	159
tcp/445	154
tcp/22	139

Table 42: Top 5 UDP packets, 2008-09

port	count
udp/1434	195
udp/137	90
udp/1027	62
udp/1026	56
udp/1028	46

Table 43: Top 12 probe sources, 2008-09

host	count
222.180.37.14	4052
221.192.199.34	2455
222.208.183.218	1211
125.65.165.139	281
61.164.148.102	251
59.36.101.9	76
121.14.136.101	71
83.105.52.137	69
121.14.212.72	41
83.104.237.166	39
222.73.204.17	30
125.65.112.177	28

A.10 Statistics for 2008-10

Table 44: Statistical breakdown, 2008-10

TCP packets, total	13098
UDP packets, total	328
ICMP packets, total	1146
Distinct sources	1838
Distinct TCP ports	93
Distinct UDP ports	9

Table 45: Top 12 TCP packets, 2008-10

port	count
tcp/23	2044
tcp/8000	1775
tcp/1080	1631
tcp/7212	1395
tcp/8800	1389
tcp/9788	1305
tcp/135	845
tcp/6081	410
tcp/3128	397
tcp/8080	289
tcp/2967	200
tcp/25	194

Table 46: Top 9 UDP packets, 2008-10

port	count
udp/1434	237
udp/137	62
udp/1027	9
udp/1026	9
udp/1028	5
udp/53724	2
udp/161	2
udp/5060	1
udp/53	1

Table 47: Top 12 probe sources, 2008-10

host	count
221.192.199.34	4010
222.180.37.14	2861
222.208.183.218	1322
83.102.206.133	323
125.65.165.139	253
83.105.58.87	246
83.105.96.205	227
83.105.23.49	226
83.105.124.217	201
83.105.103.57	180
125.65.165.132	140
83.105.26.145	99

A.11 Statistics for 2008-11

Table 48: Statistical breakdown, 2008-11

TCP packets, total	4148
UDP packets, total	267
ICMP packets, total	983
Distinct sources	1557
Distinct TCP ports	74
Distinct UDP ports	4

Table 49: Top 12 TCP packets, 2008-11

port	count
tcp/23	1491
tcp/135	671
tcp/8000	260
tcp/1433	247
tcp/3128	242
tcp/1080	214
tcp/2967	154
tcp/22	138
tcp/25	97
tcp/445	94
tcp/139	64
tcp/5900	63

Table 50: Top 4 UDP packets, 2008-11

port	count
udp/1434	199
udp/137	51
udp/1027	10
udp/1026	7

Table 51: Top 12 probe sources, 2008-11

host	count
222.208.183.218	553
83.105.53.1	497
83.102.206.133	258
83.105.124.217	171
83.105.23.49	100
125.65.165.139	74
125.65.112.177	70
125.65.165.132	68
83.105.96.205	66
121.14.136.101	63
221.195.73.68	53
83.105.52.137	51

A.12 Statistics for 2008-12

Table 52: Statistical breakdown, 2008-12

TCP packets, total	5178
UDP packets, total	444
ICMP packets, total	963
Distinct sources	1499
Distinct TCP ports	82
Distinct UDP ports	8

Table 53: Top 12 TCP packets, 2008-12

port	count
tcp/23	1717
tcp/135	547
tcp/3128	505
tcp/445	476
tcp/8000	464
tcp/1080	335
tcp/1433	180
tcp/22	162
tcp/2967	141
tcp/25	99
tcp/139	79
tcp/80	61

Table 54: Top 8 UDP packets, 2008-12

port	count
udp/1434	246
udp/44923	113
udp/137	50
udp/1026	20
udp/1027	10
udp/5060	3
udp/20375	1
udp/22785	1

Table 55: Top 12 probe sources, 2008-12

host	count
222.208.183.218	1146
83.105.53.1	555
83.105.23.49	235
83.105.96.205	171
221.195.73.68	159
83.105.124.217	117
83.105.58.87	116
125.65.165.139	102
83.105.11.233	94
83.105.55.41	86
121.14.136.101	63
125.65.112.177	55

B A detailed look at a few probe sequences

B.1 Ping and SMB probes, 2008-10

Here's one host both probing for assorted SMB vulnerabilities and trying to use ICMP for probing. However, I suspect this may well be a dynamically allocated source IP, based on the difference in dates.

Time	Source IP	Source port	Dest. port
2008-10-06 15:16:55	83.148.100.70	TCP/1127	TCP/139
2008-10-06 15:16:58	83.148.100.70	TCP/1127	TCP/139
2008-10-06 15:17:04	83.148.100.70	TCP/1127	TCP/139
2008-10-16 22:25:02	83.148.100.70	ICMP/NIL	ICMP/NIL
2008-10-16 22:25:04	83.148.100.70	ICMP/NIL	ICMP/NIL
2008-10-21 14:07:53	83.148.100.70	TCP/3569	TCP/135
2008-10-21 14:07:56	83.148.100.70	TCP/3569	TCP/135
2008-10-21 14:08:02	83.148.100.70	TCP/3569	TCP/135
2008-10-21 21:03:58	83.148.100.70	TCP/2551	TCP/135
2008-10-21 21:04:01	83.148.100.70	TCP/2551	TCP/135
2008-10-21 21:04:07	83.148.100.70	TCP/2551	TCP/135
2008-10-21 21:25:38	83.148.100.70	TCP/3089	TCP/135
2008-10-21 21:25:41	83.148.100.70	TCP/3089	TCP/135
2008-10-21 21:25:47	83.148.100.70	TCP/3089	TCP/135
2008-10-21 21:59:35	83.148.100.70	TCP/2519	TCP/135
2008-10-21 21:59:38	83.148.100.70	TCP/2519	TCP/135
2008-10-21 21:59:44	83.148.100.70	TCP/2519	TCP/135

B.2 Slammer probes, 2008-12-10

In honour of the Nobel Day, here's the SQL Slammer probes received that day.

Time	Source IP	Source port	Dest. port
2008-12-10 02:45:49	202.99.11.99	UDP/1231	UDP/1434
2008-12-10 03:43:12	222.85.151.244	UDP/4229	UDP/1434
2008-12-10 05:48:00	218.3.114.7	UDP/2653	UDP/1434
2008-12-10 11:14:06	202.103.11.41	UDP/1047	UDP/1434
2008-12-10 12:17:14	76.29.42.187	UDP/2831	UDP/1434
2008-12-10 15:54:22	61.150.92.188	UDP/3898	UDP/1434
2008-12-10 21:16:19	123.30.51.252	UDP/1445	UDP/1434
2008-12-10 23:11:22	221.233.242.4	UDP/1035	UDP/1434

C Full list of detected anomalies

C.1 2008-01

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

C.2 2008-02

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

2008-02-19 TCP/7212	2008-02-24 UDP/1026
2008-02-20 TCP/135	2008-02-26 TCP/135
2008-02-20 TCP/7212	2008-02-26 TCP/2967
2008-02-20 UDP/1026	2008-02-27 TCP/135
2008-02-21 TCP/135	2008-02-27 TCP/2967
2008-02-22 TCP/135	2008-02-27 TCP/7212
2008-02-22 TCP/2968	2008-02-28 TCP/135
2008-02-22 TCP/7212	2008-02-28 TCP/2967
2008-02-23 TCP/135	2008-02-28 TCP/7212
2008-02-23 TCP/7212	2008-02-29 TCP/135
2008-02-24 TCP/135	2008-02-29 TCP/2967
2008-02-24 TCP/445	2008-02-29 TCP/445

C.3 2008-03

2008-03-01 TCP/135	2008-03-18 TCP/23
2008-03-01 TCP/7212	2008-03-18 TCP/2967
2008-03-01 TCP/2967	2008-03-19 TCP/1433
2008-03-02 TCP/135	2008-03-19 TCP/23
2008-03-02 TCP/2967	2008-03-20 TCP/23
2008-03-02 TCP/7212	2008-03-20 TCP/135
2008-03-03 TCP/135	2008-03-21 TCP/2967
2008-03-03 TCP/7212	2008-03-22 TCP/2967
2008-03-03 TCP/2967	2008-03-22 TCP/23
2008-03-04 TCP/7212	2008-03-22 TCP/135
2008-03-04 TCP/135	2008-03-23 TCP/1433
2008-03-04 TCP/2967	2008-03-23 TCP/2967
2008-03-05 TCP/135	2008-03-24 TCP/23
2008-03-05 TCP/7212	2008-03-24 UDP/1026
2008-03-05 TCP/2967	2008-03-24 TCP/23
2008-03-06 TCP/135	2008-03-24 TCP/2967
2008-03-06 TCP/7212	2008-03-25 UDP/1027
2008-03-06 TCP/2967	2008-03-25 TCP/2967
2008-03-07 TCP/7212	2008-03-26 TCP/2967
2008-03-07 TCP/2967	2008-03-26 TCP/23
2008-03-08 TCP/7212	2008-03-27 TCP/1433
2008-03-09 TCP/23	2008-03-27 TCP/2967
2008-03-10 TCP/2967	2008-03-27 UDP/1027
2008-03-12 TCP/23	2008-03-29 TCP/1433
2008-03-15 TCP/23	2008-03-30 TCP/23
2008-03-16 TCP/2967	2008-03-31 TCP/2968
2008-03-16 TCP/23	2008-03-31 TCP/23
2008-03-16 TCP/2967	2008-03-31 UDP/1027
2008-03-17 TCP/2967	2008-03-31 TCP/135

C.4 2008-04

2008-04-01 TCP/23	2008-04-20 TCP/7212
2008-04-02 TCP/23	2008-04-20 TCP/9788
2008-04-02 TCP/2967	2008-04-20 TCP/2967
2008-04-03 TCP/23	2008-04-20 TCP/135
2008-04-03 TCP/2967	2008-04-21 UDP/1026
2008-04-03 TCP/135	2008-04-21 TCP/7212
2008-04-04 TCP/2968	2008-04-21 TCP/9788
2008-04-04 TCP/2967	2008-04-21 UDP/1027
2008-04-05 TCP/135	2008-04-22 TCP/23
2008-04-05 TCP/23	2008-04-22 TCP/2967
2008-04-07 TCP/2967	2008-04-22 TCP/135
2008-04-08 UDP/1026	2008-04-22 TCP/23
2008-04-08 TCP/2967	2008-04-22 UDP/1026
2008-04-09 UDP/1027	2008-04-22 TCP/2967
2008-04-09 UDP/1026	2008-04-23 TCP/1433
2008-04-10 UDP/1026	2008-04-23 TCP/23
2008-04-10 TCP/23	2008-04-24 TCP/2967
2008-04-10 TCP/2967	2008-04-25 TCP/23
2008-04-11 TCP/2967	2008-04-25 UDP/1027
2008-04-13 TCP/2967	2008-04-25 UDP/1026
2008-04-14 TCP/135	2008-04-25 TCP/23
2008-04-15 TCP/2967	2008-04-25 TCP/2967
2008-04-16 TCP/2967	2008-04-26 TCP/23
2008-04-16 TCP/9788	2008-04-26 TCP/2967
2008-04-16 TCP/7212	2008-04-27 UDP/1026
2008-04-16 TCP/9788	2008-04-27 TCP/7212
2008-04-16 TCP/23	2008-04-27 TCP/23
2008-04-17 TCP/2967	2008-04-27 TCP/7212
2008-04-17 TCP/7212	2008-04-27 TCP/2967
2008-04-17 TCP/9788	2008-04-28 TCP/2968
2008-04-17 TCP/23	2008-04-28 TCP/23
2008-04-17 TCP/2967	2008-04-28 TCP/2967
2008-04-18 TCP/9788	2008-04-29 TCP/23
2008-04-18 TCP/7212	2008-04-29 TCP/9788
2008-04-18 TCP/23	2008-04-29 TCP/2967
2008-04-18 TCP/2967	2008-04-29 TCP/7212
2008-04-19 UDP/1027	2008-04-30 UDP/1026
2008-04-19 TCP/9788	2008-04-30 TCP/23
2008-04-19 TCP/7212	2008-04-30 TCP/2967
2008-04-19 TCP/2967	2008-04-30 TCP/135
2008-04-20 UDP/1026	

C.5 2008-05

2008-05-01 TCP/7212	2008-05-15 TCP/135
2008-05-01 TCP/9788	2008-05-15 TCP/445
2008-05-01 UDP/1026	2008-05-16 TCP/135
2008-05-01 TCP/7212	2008-05-16 TCP/23
2008-05-01 TCP/9788	2008-05-17 TCP/1433
2008-05-01 TCP/2967	2008-05-17 TCP/135
2008-05-02 TCP/7212	2008-05-17 TCP/23
2008-05-03 TCP/9788	2008-05-18 TCP/135
2008-05-03 TCP/7212	2008-05-19 TCP/23
2008-05-04 TCP/5900	2008-05-19 TCP/135
2008-05-04 UDP/1026	2008-05-20 TCP/23
2008-05-05 TCP/9788	2008-05-20 TCP/135
2008-05-05 TCP/7212	2008-05-21 TCP/23
2008-05-05 UDP/1027	2008-05-21 TCP/135
2008-05-05 UDP/1026	2008-05-21 TCP/23
2008-05-05 TCP/1433	2008-05-22 TCP/23
2008-05-06 UDP/1026	2008-05-23 TCP/23
2008-05-07 TCP/135	2008-05-24 TCP/9788
2008-05-07 UDP/1026	2008-05-24 TCP/23
2008-05-08 TCP/23	2008-05-24 UDP/1026
2008-05-08 TCP/135	2008-05-25 UDP/1026
2008-05-08 TCP/9788	2008-05-26 TCP/23
2008-05-08 TCP/7212	2008-05-27 TCP/8000
2008-05-09 TCP/135	2008-05-27 TCP/7212
2008-05-10 TCP/7212	2008-05-27 TCP/23
2008-05-10 TCP/135	2008-05-28 TCP/8000
2008-05-10 TCP/9788	2008-05-29 TCP/23
2008-05-11 TCP/7212	2008-05-29 UDP/1027
2008-05-11 TCP/23	2008-05-29 TCP/7212
2008-05-11 TCP/135	2008-05-30 TCP/8080
2008-05-12 TCP/135	2008-05-30 TCP/445
2008-05-12 TCP/23	2008-05-30 TCP/9788
2008-05-13 TCP/23	2008-05-30 TCP/7212
2008-05-13 TCP/135	2008-05-31 TCP/8080
2008-05-14 TCP/135	2008-05-31 TCP/7212
2008-05-14 TCP/23	2008-05-31 TCP/9788
2008-05-14 TCP/7212	2008-05-31 TCP/8080
2008-05-15 TCP/23	

C.6 2008-06

2008-06-01 TCP/8080	2008-06-02 TCP/8080
2008-06-01 TCP/9788	2008-06-03 TCP/135
2008-06-01 TCP/7212	2008-06-03 TCP/9788
2008-06-02 TCP/9788	2008-06-03 TCP/7212
2008-06-02 TCP/7212	2008-06-03 TCP/8080

2008-06-04 TCP/23	2008-06-11 TCP/9788
2008-06-04 TCP/7212	2008-06-11 TCP/7212
2008-06-04 TCP/8080	2008-06-11 TCP/8080
2008-06-04 TCP/9788	2008-06-12 TCP/8080
2008-06-05 TCP/7212	2008-06-13 TCP/8080
2008-06-05 TCP/9788	2008-06-14 TCP/1433
2008-06-06 TCP/9788	2008-06-14 TCP/3128
2008-06-06 TCP/7212	2008-06-14 TCP/23
2008-06-07 TCP/8080	2008-06-15 TCP/135
2008-06-07 TCP/9788	2008-06-15 TCP/445
2008-06-07 TCP/7212	2008-06-16 TCP/23
2008-06-07 TCP/23	2008-06-18 TCP/135
2008-06-08 TCP/9788	2008-06-18 TCP/23
2008-06-08 TCP/7212	2008-06-19 TCP/445
2008-06-08 TCP/8080	2008-06-20 TCP/23
2008-06-09 TCP/23	2008-06-21 UDP/1026
2008-06-09 TCP/8080	2008-06-21 TCP/23
2008-06-09 TCP/7212	2008-06-21 UDP/1027
2008-06-09 TCP/9788	2008-06-21 UDP/1026
2008-06-10 TCP/2967	2008-06-22 TCP/23
2008-06-10 TCP/9788	2008-06-22 UDP/1026
2008-06-10 TCP/7212	2008-06-24 TCP/8724
2008-06-10 TCP/8080	2008-06-25 TCP/23
2008-06-10 TCP/23	

C.7 2008-07

2008-07-01 TCP/23	2008-07-16 TCP/23
2008-07-01 UDP/1026	2008-07-20 TCP/23
2008-07-01 TCP/23	2008-07-21 UDP/1026
2008-07-03 TCP/23	2008-07-22 TCP/135
2008-07-04 TCP/7212	2008-07-23 TCP/23
2008-07-04 TCP/23	2008-07-24 TCP/23
2008-07-10 TCP/23	2008-07-26 TCP/2967
2008-07-13 TCP/23	2008-07-26 TCP/23
2008-07-14 TCP/23	2008-07-28 TCP/9788
2008-07-14 TCP/8000	2008-07-28 TCP/23
2008-07-14 TCP/7212	2008-07-30 TCP/23
2008-07-15 TCP/23	2008-07-31 UDP/135

C.8 2008-08

2008-08-06 TCP/23	2008-08-10 TCP/23
2008-08-07 TCP/23	2008-08-12 TCP/23
2008-08-08 TCP/135	2008-08-12 UDP/1028
2008-08-08 TCP/23	2008-08-12 UDP/1026

2008-08-14 UDP/1026
2008-08-17 TCP/23
2008-08-21 TCP/445
2008-08-23 TCP/23
2008-08-24 UDP/26828
2008-08-28 TCP/9788
2008-08-28 TCP/7212

2008-08-29 TCP/9788
2008-08-29 TCP/7212
2008-08-30 TCP/9788
2008-08-30 TCP/7212
2008-08-30 TCP/139
2008-08-31 TCP/9788
2008-08-31 TCP/7212

C.9 2008-09

2008-09-01 TCP/7212
2008-09-01 TCP/9788
2008-09-02 TCP/7212
2008-09-02 TCP/9788
2008-09-05 TCP/135
2008-09-10 TCP/23
2008-09-12 TCP/9788
2008-09-12 TCP/7212

2008-09-13 TCP/9788
2008-09-13 TCP/7212
2008-09-17 TCP/8000
2008-09-17 TCP/7212
2008-09-19 TCP/1080
2008-09-26 TCP/1433
2008-09-29 TCP/23
2008-09-30 TCP/2967

C.10 2008-10

2008-10-04 TCP/8000
2008-10-06 TCP/23
2008-10-07 TCP/23
2008-10-08 TCP/23
2008-10-09 TCP/135
2008-10-09 TCP/23
2008-10-09 TCP/445
2008-10-10 TCP/23
2008-10-12 TCP/23
2008-10-13 TCP/23
2008-10-14 TCP/23
2008-10-15 TCP/23
2008-10-16 TCP/23
2008-10-17 TCP/23
2008-10-18 TCP/23
2008-10-19 TCP/23
2008-10-19 TCP/5900
2008-10-20 TCP/23
2008-10-21 TCP/23
2008-10-22 TCP/135

2008-10-22 TCP/23
2008-10-22 TCP/135
2008-10-22 TCP/139
2008-10-23 TCP/23
2008-10-23 TCP/135
2008-10-24 TCP/23
2008-10-24 TCP/135
2008-10-25 TCP/23
2008-10-25 TCP/135
2008-10-26 TCP/23
2008-10-26 TCP/135
2008-10-27 TCP/23
2008-10-28 TCP/135
2008-10-28 TCP/25
2008-10-28 TCP/135
2008-10-28 TCP/23
2008-10-29 TCP/23
2008-10-30 TCP/23
2008-10-31 TCP/23

C.11 2008-11

2008-11-01 TCP/23
2008-11-01 TCP/135
2008-11-02 TCP/23
2008-11-02 TCP/135
2008-11-03 TCP/23
2008-11-04 TCP/23
2008-11-06 TCP/23
2008-11-07 TCP/135
2008-11-08 TCP/23
2008-11-09 TCP/23
2008-11-09 TCP/135

2008-11-10 TCP/23
2008-11-11 TCP/135
2008-11-11 TCP/23
2008-11-12 TCP/23
2008-11-15 TCP/23
2008-11-18 TCP/23
2008-11-19 TCP/23
2008-11-20 TCP/23
2008-11-21 TCP/23
2008-11-23 TCP/135
2008-11-23 TCP/23

C.12 2008-12

2008-12-07 UDP/44923
2008-12-08 TCP/23
2008-12-09 TCP/23
2008-12-10 TCP/23
2008-12-11 TCP/23
2008-12-12 TCP/23
2008-12-13 TCP/23
2008-12-14 TCP/23
2008-12-15 TCP/23
2008-12-16 TCP/445
2008-12-16 TCP/23
2008-12-17 TCP/445

2008-12-17 TCP/23
2008-12-18 TCP/445
2008-12-19 TCP/23
2008-12-20 TCP/23
2008-12-21 TCP/23
2008-12-22 TCP/23
2008-12-23 TCP/23
2008-12-24 TCP/135
2008-12-25 TCP/23
2008-12-26 TCP/23
2008-12-30 TCP/23

D Ports and application map

This is more for my own reference than a canonical mapping, but maybe it will make it slightly quicker to write next year's report, having these already collated. These have been compiled from various on-line sources.

Protocol	Port	Application
TCP	23	Telnet
TCP	135	SMB
UDP	135	SMB
TCP	445	MS Naked CIFS
UDP	1026	MSN Messenger
UDP	1027	MSN Messenger
UDP	1028	Microsoft, may be DCOM
TCP	1080	SOCKS
TCP	2967	Symantec AntiVirus client
TCP	2968	ENPP (?)
TCP	3128	Squid web proxy
TCP	5900	VNC
TCP	7212	GhostSurf
TCP	7788	PTC License server
TCP	8000	Alternative HTTP port
TCP	8080	Alternative HTTP port
TCP	9788	FileSphere
TCP	18019	Unidentified
UDP	26828	Unidentified
UDP	44923	Unidentified