

# The Database Exposure Survey 2005

David Litchfield [davidl@ngssoftware.com]  
21<sup>st</sup> December 2005



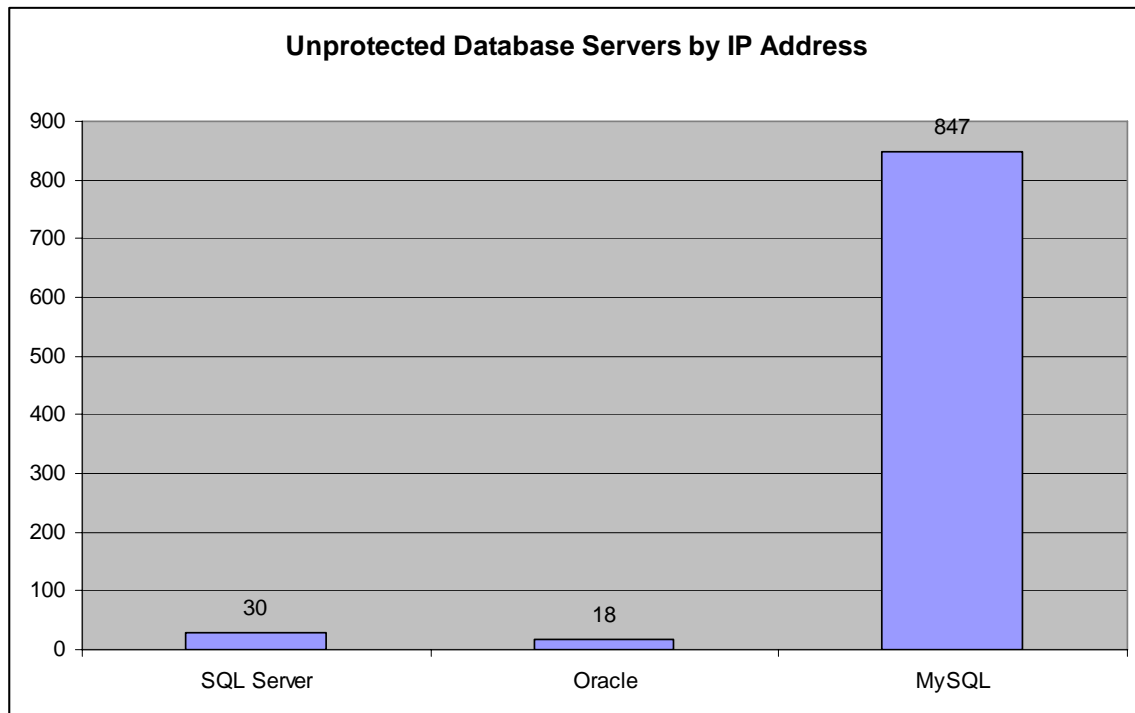
An NGSSoftware Insight Security Research (NISR) Publication  
©2005 Next Generation Security Software Ltd  
<http://www.ngssoftware.com>

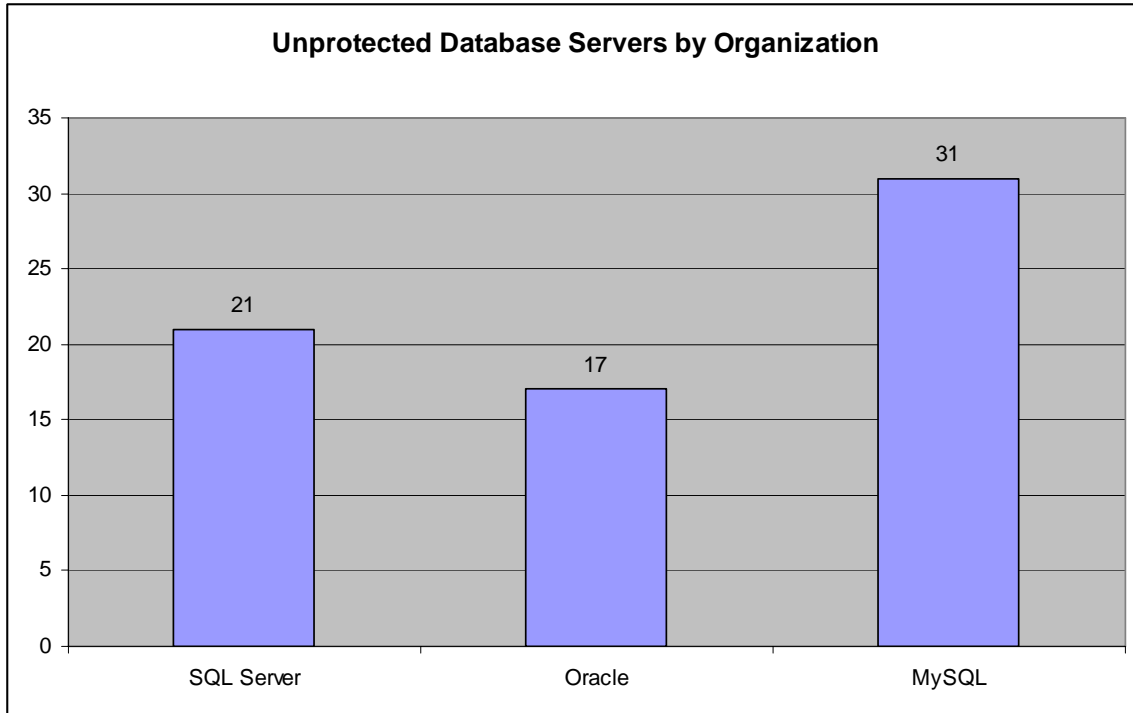
## Introduction

RFC 876 describes the results of a scan of mail servers on the Internet to check for bugs and non-compliance with the SMTP protocol. This RFC became the seed for the idea for a new survey to determine how many database servers are “out there” on the Internet and which are *not* protected by a firewall. This research will help assess the potential threat posed by worms that target database servers such as Slammer, Spida and SpoolCLL. The database servers chosen for this survey were MySQL, Microsoft SQL Server and Oracle.

## Executive Summary of the Results

This survey checked approximately half a million systems [see Appendix A for data gathering details] and found that, whilst there are considerably more MySQL servers exposed than Oracle or Microsoft SQL Server, no one particular “camp” can claim to be much better than the other: when the data is rearranged by organization the numbers are “normalized”. This can be seen in the two graphs that follow. They depict the number of database servers found in the sample that were not protected by a firewall with the first graph breaking the numbers down by IP address and the second by organization.



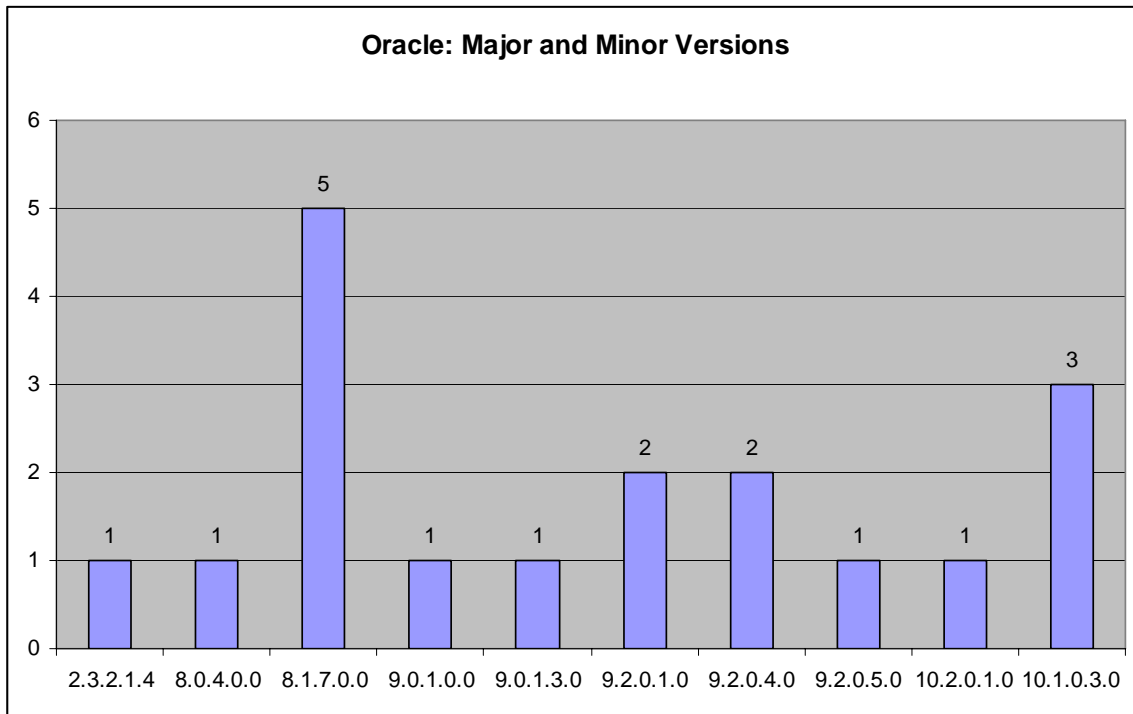


We can immediately see that there's a stark difference between the two graphs; this is due to the popularity of MySQL in hosting companies where they have server farms or multiple IP addresses bound to the same physical system.

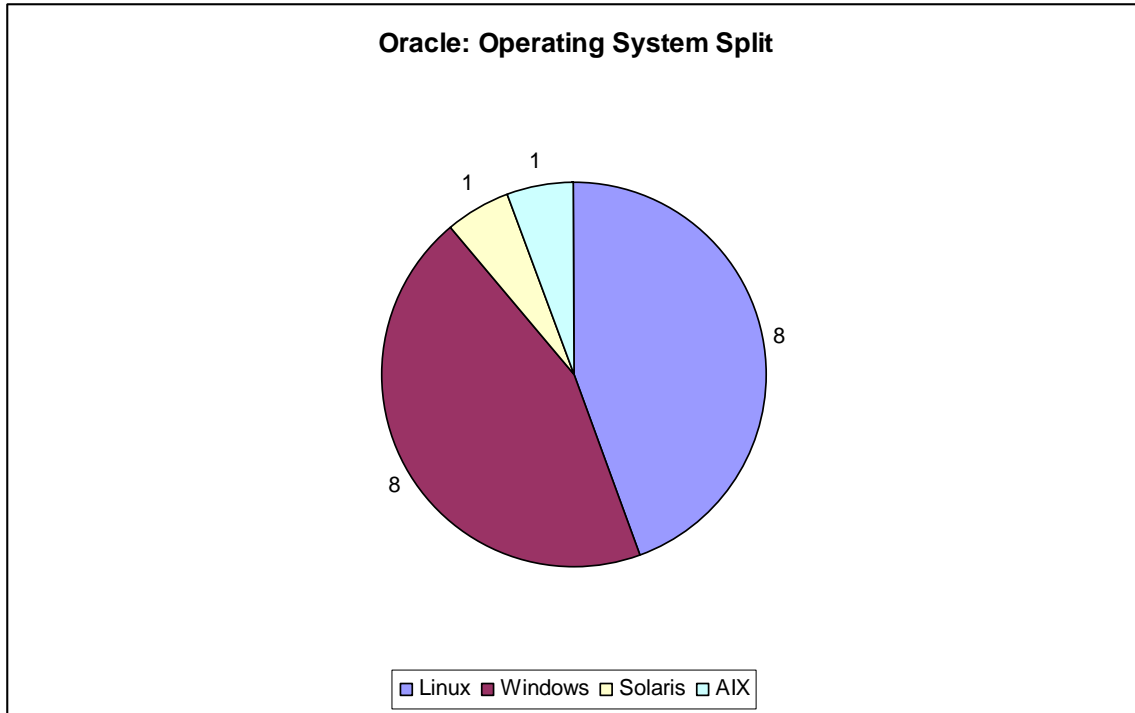
If these results form an accurate representation of what actually exists out there then, if extrapolated, it suggests that there are c. 140,000 Oracle servers that are not firewalled and 210,000 Microsoft SQL Servers that are not firewalled.

## Results for Oracle

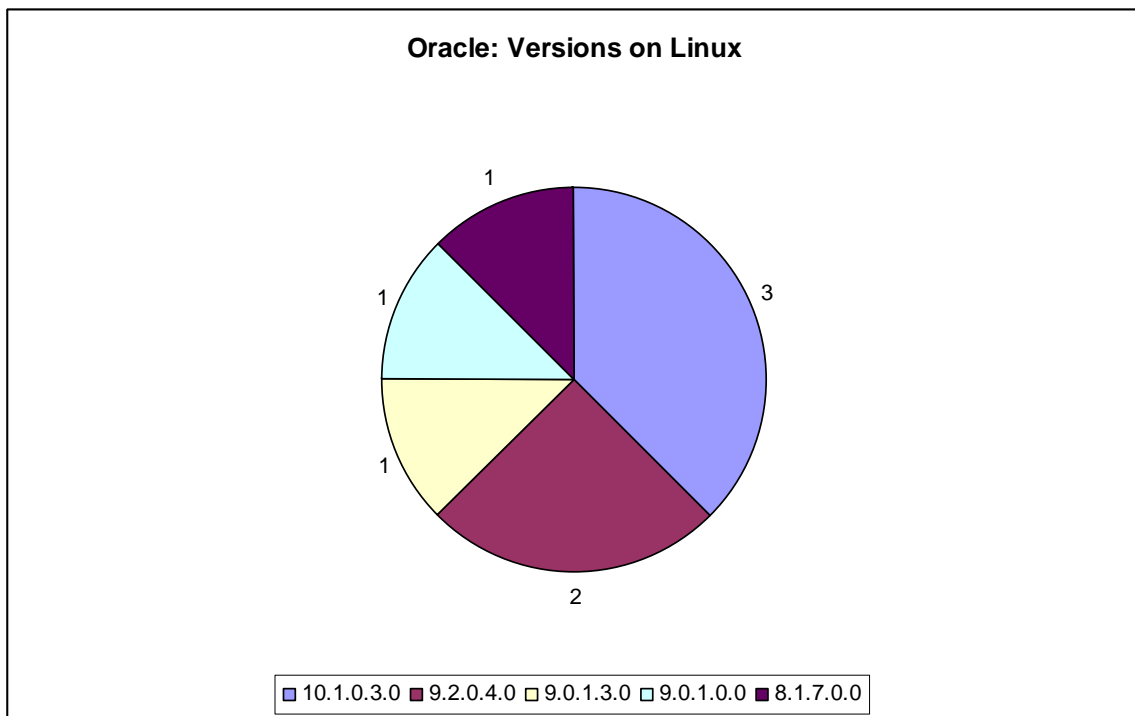
The results of this survey put to bed the myth that Oracle servers are never found exposed on the Internet. When you consider that 75,000 Microsoft SQL Servers were infected by the Slammer worm [1], with an estimated 140,000 un-firewalled Oracle servers “out there” there is a real risk of an Oracle worm. What exacerbates this potential problem is that Oracle creates a large number of default accounts with default passwords, and further, many of the servers found during the survey are running old versions of Oracle which are vulnerable to a particular flaw that allows attackers to gain control of the server without a user ID and password. Indeed many of the servers found in the survey seem not to be running patched systems.

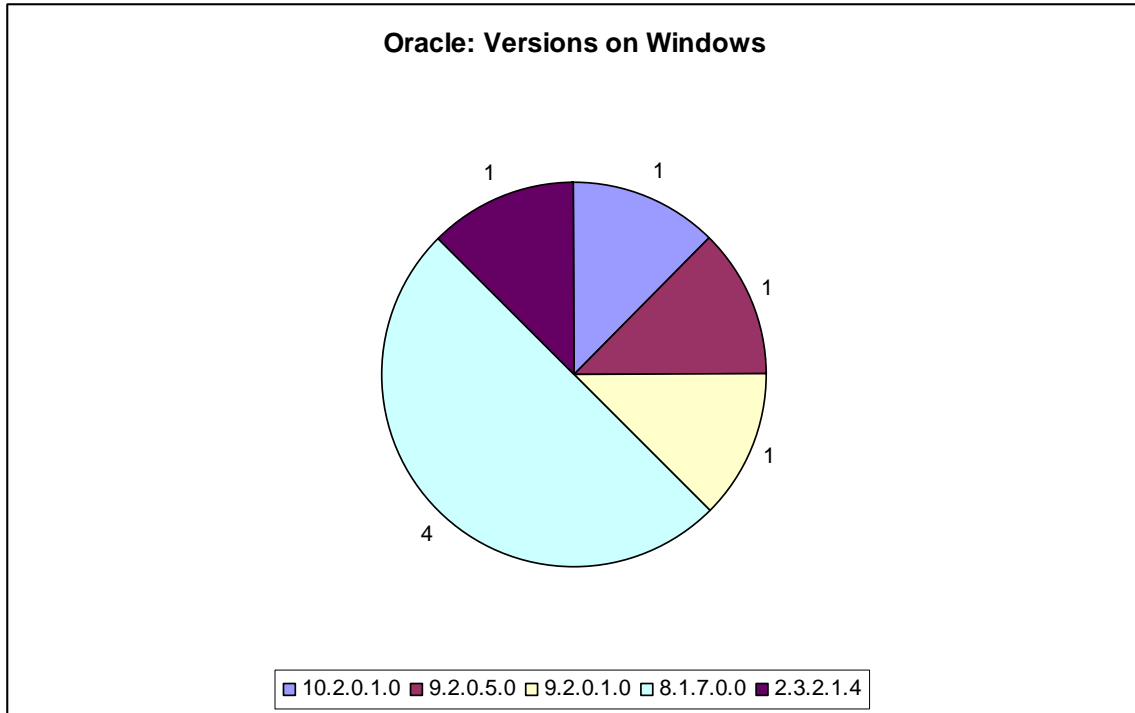


With regards to the distribution of Oracle servers over operating systems, just over half were found to be running on a Unix-variant, mostly Linux, and the rest on Windows:



If we break down the versions found for Linux and Windows we get the following two graphs:

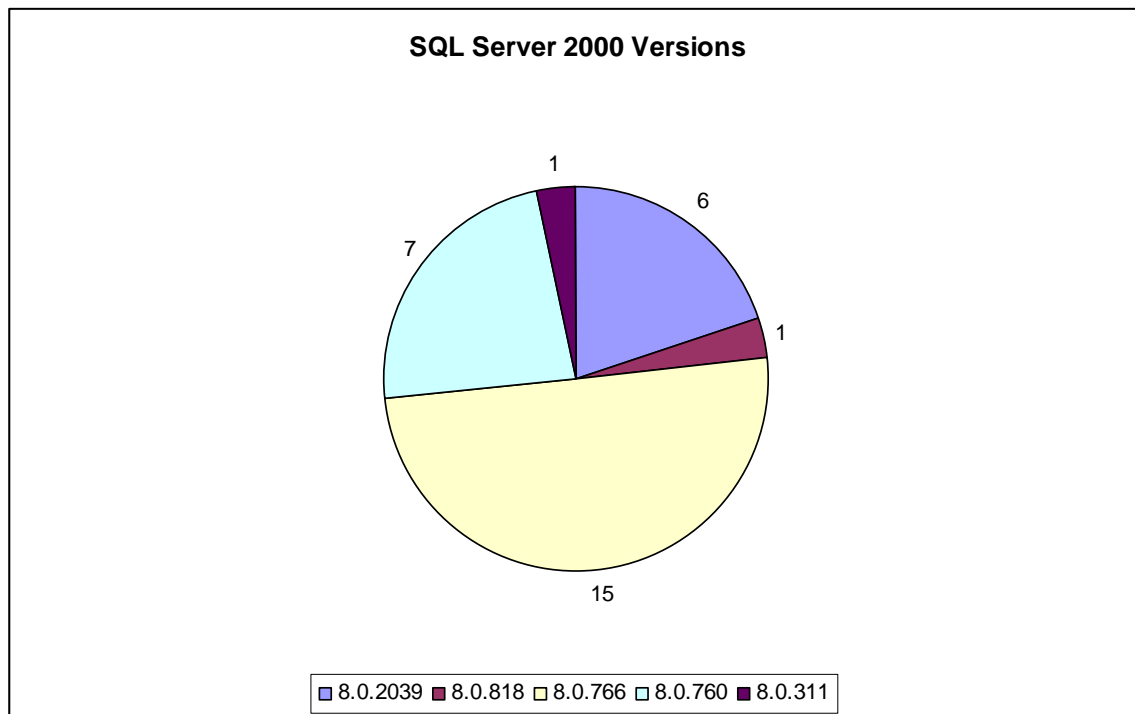




The version of Oracle running on the sole AIX box discovered was 8.0.4.0.0 and 9.2.0.1.0 on the Solaris box.

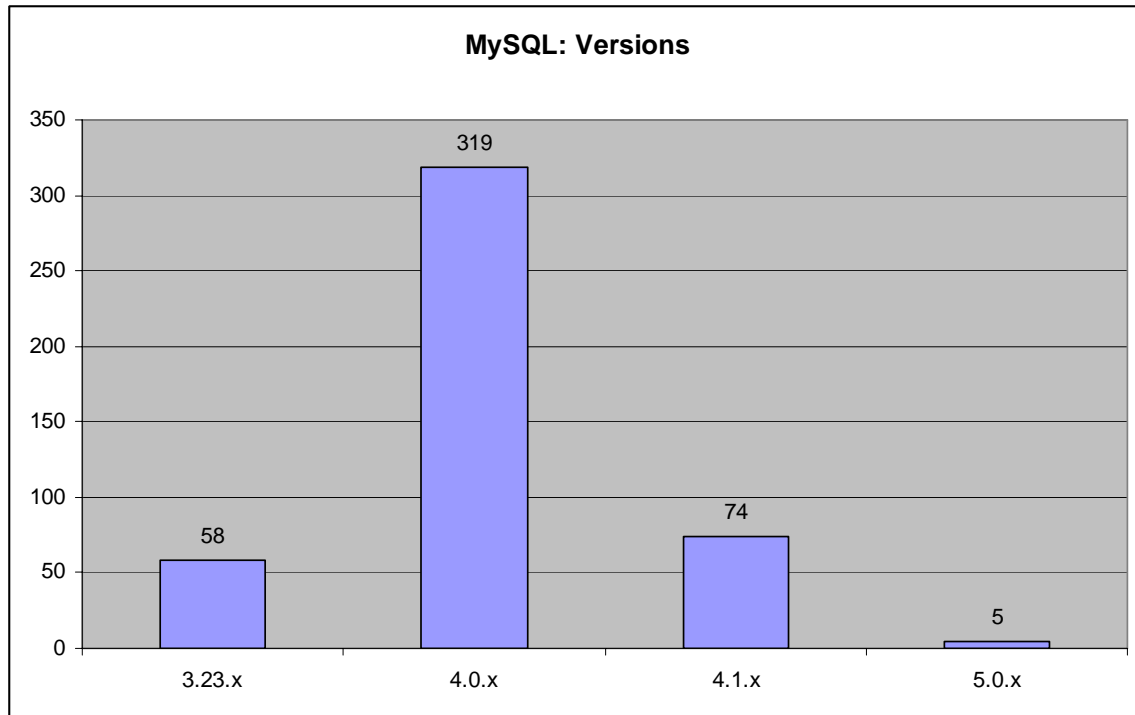
## Results for SQL Server

The survey found no servers running SQL Server 7 (or earlier) but did find one SQL Server 2005 system. The remaining 29 systems were running SQL Server 2000. All SQL Server 2000 systems found except one were patched against MS02-39 – the hole the Slammer worm exploited. That said only 6 systems of the 30 found had Service Pack 4 installed (Version 8.0.2039) and thus were the only servers that were fully-patched. This shows that the poor patching practices that allowed Slammer to be as “successful” as it was still exist in the SQL world. With an estimated 210,000 un-firewalled Microsoft SQL Servers out there, SQL administrators cannot afford to be complacent.



## Results for MySQL

Though 847 MySQL Servers were found, only 391 restricted access by address; the remaining 456 could be accessed. This may cause some to question as to whether these systems should be included in the results. They should be: even though restricting access drastically reduces “attack surface” a potential attacker can still interact with the server by the very act of connecting - the server logs the connection and performs a DNS lookup on the connecting host. A theoretical vulnerability in this “functionality” could leave a server compromised. From the distribution of versions out there it becomes apparent that patching practices in the MySQL world are no better than anyone else.



### Conclusion

For me there are three interesting points that can be drawn from this survey

- SQL Administrators didn't learn anything from Slammer – they're still not keeping up to date with patches.
- Oracle servers are as exposed as the "rest of them" and patching practices seem as poor as they are in the SQL world.
- There are more exposed MySQL servers than I would have expected and, like SQL Server and Oracle, most of the systems found were discovered to by running older, un-patched versions.

It is expected that many of the servers found during this survey are not firewalled due to risk acceptance – in other words a business decision has been taken to have these systems open so business can be enacted; but please, if you must expose your database servers to the world and their dog, keep them patched!

[1] <http://www.cs.berkeley.edu/~nweaver/sapphire/>

### **Appendix A - How the data was gathered**

8000 IP addresses were chosen at random and the sixty addresses from there were checked to see if a database server was present. This gave a total of 480,000 IP addresses checked. Only those systems that returned a valid server banner were considered – having the “right” TCP port open was considered as not sufficient. TCP ports 1433 (Microsoft SQL Server), 1521 (Oracle) and 3306 (MySQL) were checked.