



**Vector Report 2005**  
**infectionvectors.com**  
**December 2005**

**Overview**

2005 did not see an explosive network worm outbreak like years prior. In fact, the year came fairly close to avoiding network-based worm emergencies altogether. If not for Zotob in August, the year's record would be rather clean. The press coverage that Zotob received made it seem like a pretty big outbreak, but even this worm was not especially damaging on a global scale.<sup>1</sup> That is a big change from years past.

In recent history, network administrators have had to put up with the likes of:

|          |      |
|----------|------|
| Code Red | 2001 |
| Opaserv  | 2002 |
| Blaster  | 2003 |
| Sasser   | 2004 |

Attackers attack the weakest point of any target. Just like water always flows along the path of least resistance, so do bad guys. Sometimes cracking a target is more trouble than it's worth, but a criminal is not looking to hand around a system any longer than is necessary.

**Early Warning**

The first article published on infectionvectors.com to make predictions on the coming year had this to say:

Mass email will continue to have its share of the virus market throughout 2005, and probably 2006. Innovations like those seen with 2004's Beagle worm will push the medium to new heights. The simplicity and public availability of mass mail engines ensures its survival as a popular worm mechanism.

The report went so far as to predict no noticeable decline in the number of infections due to mass mailers.<sup>3</sup> That is, of course, difficult to prove. However, one can see that the power of mass mailers has not been curtailed, as predicted by numerous outlets in late 2004. Sophos produced a "Threat Management Report" wrapping up 2005. The report listed the top 10 malware threats for the entire year – all 10 spots are taken by mass mailers (6, 7, 9, & 10 are filled by Mytob, which has a mass mail routine as well as network routines).

Mass mail will continue to be a lucrative medium for malware authors as the state of email security is at best slightly better than it was at this time in 2004. Last year, experts predicted the use of firewalls and patching system would mean the end of mass mailers – in fact, it seems to have hurt the network worm most of all. As seen in the next sections, network worms enjoyed much less success in 2005.

## The OS

Operating system flaws were the natural targets for many outbreaks until recently. Aiming at a Windows flaw was not very challenging, hence the reputation Microsoft enjoys for its products (something that appears to be turning around slowly but surely). As take from the infectionvectors.com report “Just In Time: Microsoft Time to Exploit 3:” one can see that the number of worms based on the published security bulletins is not an overwhelming list:

| Malware<br>(Common Name/Symantec) | Associated Flaw<br>(MS Bulletin #) | Days Between Malware<br>Release and Bulletin |
|-----------------------------------|------------------------------------|--|
| Phel                              | MS05-001                           | -15  |
| Globe                             | MS05-002                           | 1  |
| VBS_RUNEXPLT                      | MS05-016                           | 10   |
| Phel.Q                            | MS05-026                           | 19   |
| Jevprox                           | MS05-037                           | 0  |
| Zotob                             | MS05-039                           | 4  |
| Dasher                            | MS05-051                           | 63   |
| Delf                              | MS05-054                           | -23  |

Note, however, that what would probably be considered the most damaging malware did become public before the corresponding patch did.

## The Apps

Aiming at application flaws is a little trickier. It is certainly not as attractive to a worm coder, as the installation base of most applications is lower than that of many operating systems (Microsoft Office certainly is an exception to that rule, which is likely the reason that so many Office Macro worms exist). However, Slammer/Sapphire is an example of a successful worm that aimed right at an application. Microsoft SQL Server 2000 was the subject of a vulnerability report in the summer of 2002.<sup>4</sup> A buffer overrun explored in that technical briefing made MS SQL Server the victim of the fastest spreading (one that spread like proverbial wildfire) worm ever.<sup>5</sup>

Web server worms also aim at a particular application, sometimes the server itself (whether Apache, IIS, etc.) sometimes a web tool running on the server (as in the phpbb discussed below). IIS was targeted most notably in 2001 when CodeRed slid the following request into the vulnerable Indexing Service:



remains a very profitable business for Internet criminals. This also points to the relative trust readers place in email messages.

### **Baby New Year**

What type of prediction is sensible for 2006? First off, email-based worms will not go away next year, much to the chagrin of experts predicting their death this year. They will likely occupy over half of the 2006 top 10 lists. Furthermore, phishing crimes have not seen the limit of their profitability either. Next year's scams will likely involve a combination of email and browser-based attacks (taking advantage of both IE and its top rival, Firefox).

Criminals have found a good niche in Web crime – aim where the lowest-common-denominator tools cannot reach: the user. Crimes that target email, slowly fixed browser flaws, and the unmanaged/under-managed millions of web server (used for quick hits in phishing ventures) will continue to succeed. Without a successful awareness campaign or technical overhaul, both of which are extremely unlikely, 2006 will look just like 2005.

## References

1. Bruce Schneier noted that Zotob was not a big deal, but was still the biggest outbreak of the year up to that point. "Schneier on security" weblog, Bruce Schneier, November 11, 2005.  
[http://www.schneier.com/blog/archives/2005/11/the\\_zotob\\_worm.html](http://www.schneier.com/blog/archives/2005/11/the_zotob_worm.html)
2. The "Demise of the Mass Mailer" report was published in January of 2005:  
[http://www.infectionvectors.com/hotzone/mass\\_mailer\\_demise.htm](http://www.infectionvectors.com/hotzone/mass_mailer_demise.htm)
3. Sophos' end of year report is a very good review for anyone interested in malware research. It can be retrieved in PDF format as well. The press release:  
<http://www.sophos.com/pressoffice/news/articles/2005/12/toptensummary05.html>
4. Microsoft MS02-039 "Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Remote Code Execution" Q323875. July 24, 2002.  
<http://www.microsoft.com/technet/security/bulletin/MS02-039.msp>
5. David Moore, et al. "The Spread of the Sapphire/Slammer Worm."  
<http://www.cs.berkeley.edu/~nweaver/sapphire/>
6. "Bofra exploit hits our ad serving supplier." The Register, 21 November 2004.  
[http://www.theregister.co.uk/2004/11/21/register\\_adserver\\_attack/](http://www.theregister.co.uk/2004/11/21/register_adserver_attack/)
7. Well outside the scope of this article, a good review of SQL injection techniques and defenses can be found at securitydocs.com.  
Sagar Joshi, 23 November 2005, "SQL Injection Attack and Defense."  
SecurityDocs.com.  
<http://www.securitydocs.com/library/3587>