Malware comes of age: The arrival of the true computer parasite

Steven Furnell[1] and Jeremy Ward[2]

[1] Network Research Group, School of Computing, Communications & Electronics,
University of Plymouth, Plymouth, United Kingdom
[2] Symantec (UK) Ltd, Hines Meadow, St Cloud Way, Maidenhead, United Kingdom

It is now twenty years since Fred Cohen published his seminal research paper suggesting the potential threat of computer viruses[i]. In the years since this publication, the risk that Cohen described has unquestionably been borne out, and alongside hackers, the threat of the computer virus is the security issue that has most clearly permeated the public mind. This reputation is certainly not without foundation - viruses consistently take the top spot in surveys of reported security breaches. Two recent examples of this are the 2004 Computer Crime and Security Survey (from the US Computer Security Institute) and the 2004 Information Security Breaches Survey (from the UK Department of Trade & Industry). Both asked respondents to indicate the type of security incidents that they had encountered in the previous year, and viruses were the top-rated problem in both cases, accounting for 78% and 50% of replies respectively (both figures being approximately 20% ahead of any other of the rated threats in either survey). Such figures clearly suggest that malware is one of the most troublesome and frequently encountered cyber threats.

Although frequently used as a catch-all term, the virus is of course only one form of malware, and other categories, such as worms and Trojan Horse programs, had already emerged long before Cohen's paper. However, it was with Cohen's work that a biological analogy first arose, and this has been a lasting contribution to the way in which much of the subsequent literature has considered malware in general (note: although Cohen authored the paper, it was actually his research supervisor, Prof. Leonard Adleman (the 'A' in RSA encryption), who suggested the use of the term 'virus').

The analogy between a computer 'virus' and a biological virus is a good one. Both entities rely for their continued propagation and existence on their ability to insert their own code into an existing set of programmed instructions; and neither have any meaningful existence in the absence of a system they have infected. However, until now the computer virus, unlike many of its biological counterparts, has not been a successful parasite. The criteria of success in a biological parasite are that:

- it spreads rapidly and effectively;
- it does not cause such a violent adverse reaction in its host that it is rapidly destroyed;
- it is able to extract valuable resources from its host.

It is our contention in this paper that computer malware, having long ago met the first characteristic, has developed the second over the past few years, and now meets the third criterion. Malware has, therefore 'come of age' as a truly successful parasite.

The security industry has, of course, responded with a range of prevention, detection and inoculation products, spawning a whole new market in terms of anti-virus

technologies. However, the genie is now very much out of the bottle, and as protection methods have been devised, so the malware has evolved, ensuring that it remains a continuous problem. This article examines the nature of this evolution, highlighting that as well as the more obvious development that has occurred in terms of replication techniques, the nature of payload activities is also significantly changing. A key issue here is the tendency for modern malware to open up backdoors on infected systems, which can in turn lead to further criminal opportunities. As a result, malware is able to generate profit for its creators – thus becoming a true parasite on the infected system.

Malware evolution

There has been a clear and widely observed evolution in terms of the infection and replication mechanisms that have enabled computer viruses to meet the first criterion of success as a parasite. Aside from an underlying fundamental change, which moved malware distribution away from reliance upon manual exchange of disks to leveraging of the Internet, the last ten years have witnessed some distinct phases:

- Mid 1990s – a move away from infection of boot sectors and program files towards macro viruses, which enabled the malware to be embedded in files that users were more likely to exchange with each other.
- Late 1990s – the appearance of automated mass mailing functionality, removing the reliance upon users to manually send infected files.
- Today – avoiding the need to dupe the user into opening an infected email attachment, by exploiting vulnerabilities that enable infection without user intervention.

As a result, malware distribution has become faster and more widespread, and far more people are coming into actual contact with it, rather than just hearing the second-hand experiences of others. As an indication of this, we can consider the significant increase in malware-infected email messages, as reported by MessageLabs, which scans millions of emails per day as part of its managed email security service. Back in the first six months of 2002, these scans revealed that an average of one in every 392 emails contained a virus. By 2004, however, the first six months were very different indeed – with one in every 12 messages being infected[ii].

Alongside replication methods, there has also been an evolution in terms of payload actions. In the early days, the objective was to be seen to be seen – virus writers were typically motivated by ego and thus wanted their creations to get attention. With no prior art in the area, the bar for achieving this was set low, and thus a virus did not have to do anything too drastic in order for such attention to be gained. Unfortunately, it did not take long for payloads to evolve from being a mere distractions or nuisance to being overtly malicious. Destructive malware quickly became the norm, with corruption of hard disks and even the PC BIOS being possible payload actions. Malware also developed characteristics of effective biological parasites. For example, the ability to mutate using polymorphic techniques, to better evade anti-virus programs. Now various strains even attempt to terminate anti-virus processes and block access to vendors' AV websites.

Such traits are valuable in a parasite, in that they help it to meet the second criterion by making it more difficult for the host to destroy. However, if a computer virus has an obviously destructive associated payload it will be actively tracked down and destroyed. Even in the past, therefore, payload elements would very rarely manifest themselves the instant that a virus infected a system. To do so would effectively undermine the replication strategy, as the virus would not have had the opportunity to spread further before being detected. As such, the most successful replicators were often those viruses that lay dormant for a fairly long time before invoking their payloads. However, a key difference in many of today's malware is that even when the payload is triggered, users remain oblivious – thus ensuring that these viruses meet the third criterion of a true parasite by remaining concealed from their hosts.

The invisible enemy

It would be fair to say that most end-user perceptions of a virus still seem to be based upon the idea of something that infects the system, and then disrupts operations or destroys data in some way. Without signs of something being obviously wrong, most will not remotely suspect that their system has fallen victim to malware. Contributing to potential misunderstandings is the fact that most media attention has tended to focus upon the outbreak aspect, such as the immediate disruption caused by a mass-mailing worm. Many users will doubtless observe the consequent media reports, but unless their system falls over, they will assume that they have dodged the bullet. This, in turn, could lead to a level of complacency – "what's all the fuss about?" – that leads them to discount the likelihood of malware being able to affect their system.

However, it is important to recognise that the real threat is often to be found not in the initial infection, but in the bit that gets left behind. Rather than trashing the system, the current modus operandi is to open a 'backdoor' that allows the system to be compromised in potentially more insidious ways. Indeed, creating a backdoor has become an increasingly significant phenomenon over the past three years, as can be seen in Figure 2 (numbers taken from Symantec DeepSight Alert – see Table 1, below).
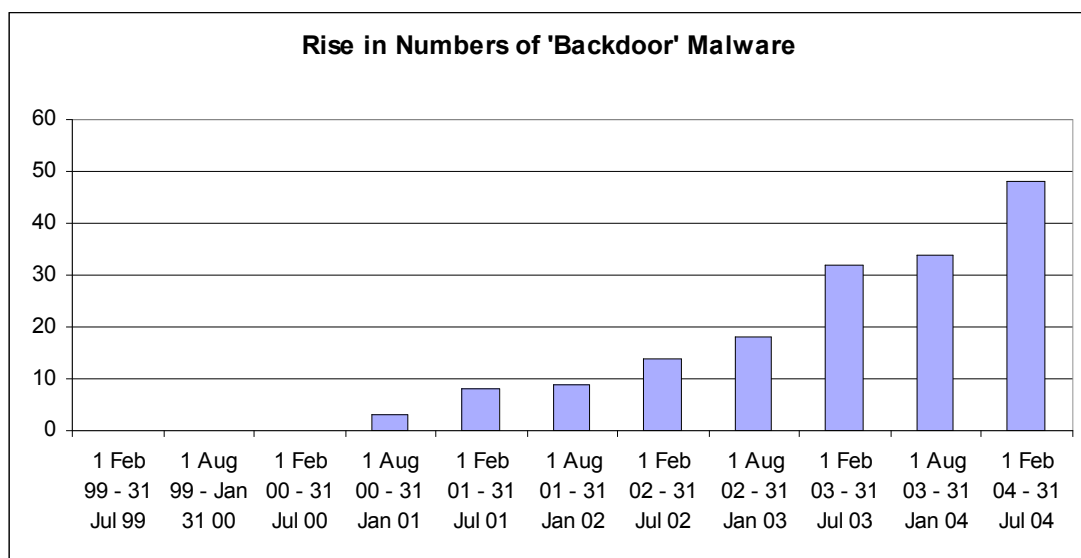
Figure 2 : The rise of the 'Backdoor'

In terms of what the backdoors may be used for, we can consider the following examples from the last few months:

- Bobax.D (19 May) - Selects a number of ports at random, and opens them to accept incoming connections. An SMTP server runs on the opened ports, allowing the infected system to be used as a spam relay[iii].
- Beagle.AB (15 July) - Opens up a backdoor on port 1080, allowing the infected computer to be used as an email relay[iv].
- Mydoom.M (26 July) – Drops a copy of the Zincite.A backdoor program, which in turn opens up port 1034 for incoming connections. Remote attackers are then able to download and execute files, as well as get a list of other infected IP addresses that have been saved[v] [vi].
- Gaobot.BAJ (August 2004) – Just one of the many incarnations of Gaobot, this variant uses port 6667 to connect to a remote IRC server, and waits for commands from a remote attacker (which can include file download and execution, network scanning, and launch of DoS attacks)[vii].

All of the functionality described above is, of course, in addition to other functionality inherent in the malware; for example to help it propagate to other systems, and to ensure that it persists in the infected system (e.g. by attempting to disrupt anti-virus protection). Even from this brief set of examples, it should be clear that the backdoors can be achieved in a variety of ways, and subsequently put to a number of uses.

Having given a few specific examples, it is also relevant to consider the extent to which the problem scales to the wider context – and also to illustrate the claim about the backdoor increasingly being the main (or only) aim of the payload. One option here would simply be to reference the huge catalogue of malware that has been collated by the anti-virus community, and thereby determine the proportion with backdoor functionality. However, the downside is that this would not easily differentiate between those malware strains that are in widespread circulation, and those that are rarely encountered outside the confines of anti-virus laboratories. As such, a better option is to examine the nature of the malware incidents that are actually being encountered in practice, and a good source of such information is provided by Symantec's DeepSight Alert Service. The service analyses potential vulnerabilities in more than 18,000 distinct versions of 4,600 products from 2,200 vendors, and tracks information about malware from over 140 different sources[viii]. By extracting the data that DeepSight has collected in relation to malware incidents, it is possible to investigate the nature of the payloads, and determine whether there has been a discernable change over time. Table 1 summarises the findings, looking at the situation over the last five years, and considering 6 month blocks from early 1999 through to mid-2004. In assessing the DeepSight data collected during this period, an alert was considered to be relevant if it pertained to malware which had a risk index of 2 or above. This value is assigned on a scale of 1-5 (very low to very severe), and is based upon the analysis of three major components of the malware threat[ix]:

- the extent to which it is "in-the-wild";
- the damage that it causes if encountered;

- the rate at which it spreads.

For each relevant DeepSight report, the originating malware was analysed and placed into one of four categories, according to the type of payload:

- those that are destructive or irritating (and would therefore make themselves known to the user of an infected system);
- those that are destructive and open a backdoor;
- those that only open a backdoor;
- those that do not appear to contain any payload.

Dates	No. Malicious Code	Payload Type			
		Destructive / Irritating without Backdoor	Destructive / Irritating with Backdoor	Only Backdoor	No Payload
1 Feb 99 - 31 Jul 99	1	1	0	0	0
1 Aug 99 - Jan 31 00	1	1	0	0	0
1 Feb 00 - 31 Jul 00	4	4	0	0	0
1 Aug 00 - 31 Jan 01	3	0	3	0	0
1 Feb 01 - 31 Jul 01	15	6	8	0	1
1 Aug 01 - 31 Jan 02	59	46	0	9	4
1 Feb 02 - 31 Jul 02	123	105	8	6	4
1 Aug 02 - 31 Jan 03	149	120	5	13	11
1 Feb 03 - 31 Jul 03	123	82	23	9	9
1 Aug 03 - 31 Jan 04	161	112	23	11	15
1 Feb 04 - 31 Jul 04	360	275	40	8	37

Table 1 : Malware incidents from DeepSight Alerting System

One of the first things to become apparent is the increasing extent to which malware incidents are being experienced. However, this is really no surprise – especially in view of the various security incident surveys that have been released in recent years. Something that may be less obvious to the casual observer is the shift in the nature of payload behaviour. Looking at Figure 3, it is notable that although the percentage of destructive malware is still far greater, the last few years have witnessed non-destructive strains increasing from virtually nothing to account for a relatively significant proportion of the encountered incidents.
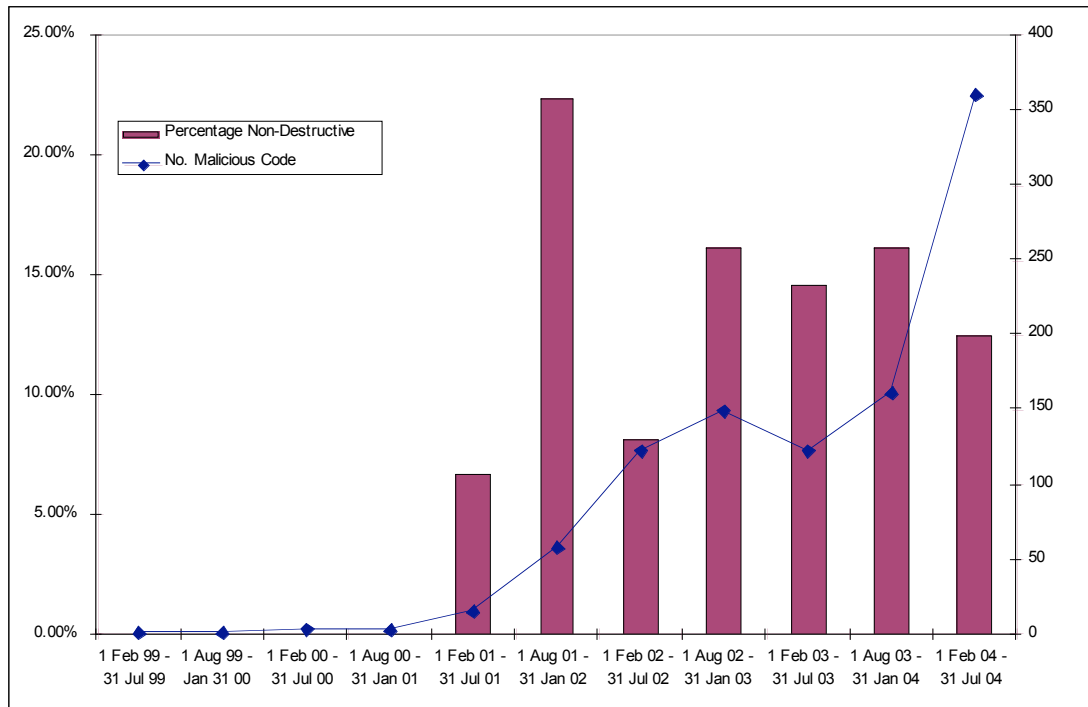
Figure 3 : The rise of malware

The increasing trend for malware to contain non-destructive payloads can be illustrated by plotting the relative numbers. This is illustrated in Figure 4, with the chart being derived from the formula: $N*(n/N)$, where N is the total number of new malware codes, and n is the number of new codes without a destructive payload (i.e. those that only open a backdoor, or have no apparent payload functionality). The correlation coefficient is 0.9017, making the trend highly significant.
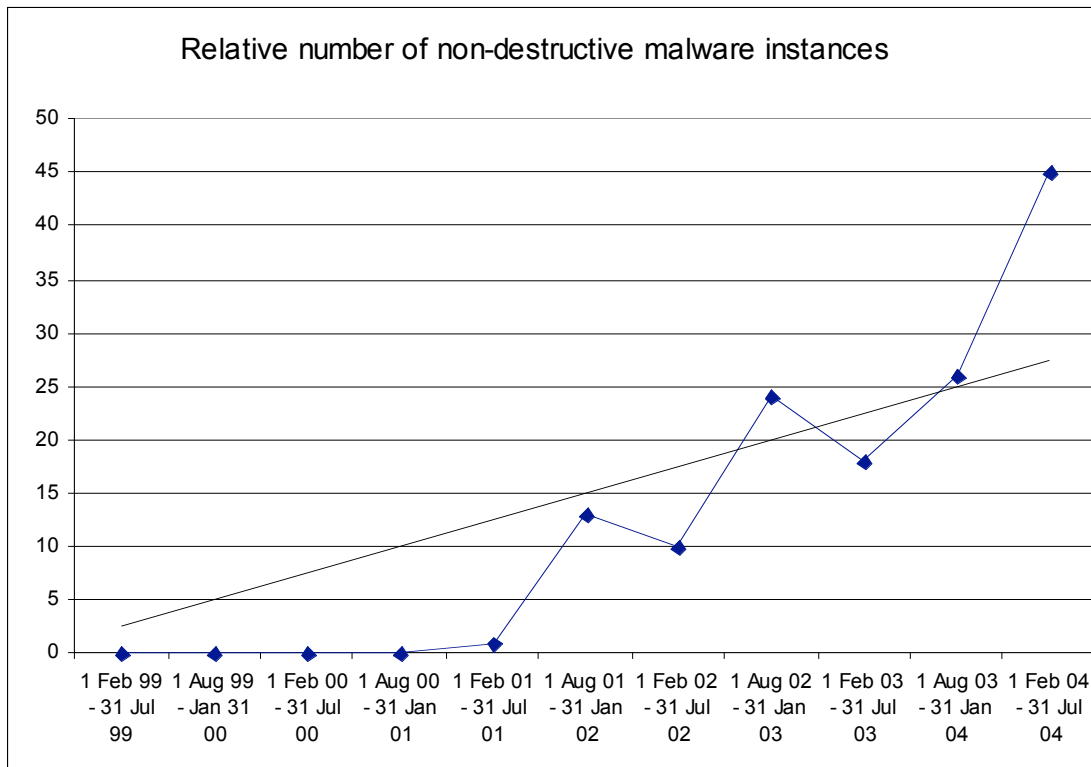
Figure 4 : The rise in non-destructive malware

The profitable parasite

If malware is becoming less destructive, then it is fair to wonder about the motivation of its authors. Malware writers have never been known for their public-spirited activity, so if they are electing not to directly harm our systems there must be something in it for them. Perhaps unsurprisingly, the answer turns out to be money.

For each backdoor that a worm or virus introduces, the attacker acquires an asset in terms of a compromised system. As their number increases, these systems can represent a massive resource in terms of their collective computing power and network bandwidth. With successfully replicating malware, the size of the resulting 'botnet' could easily run into thousands of zombie PCs. Over the first 6 months of 2004, the number of botnets monitored by Symantec rose from under 2,000 to more than 30,000[x].

Having acquired such resources, the hackers can turn them to financial advantage in a number of ways. One established approach is to sell or rent the botnet to spammers as a means of sending junk mail and bypassing IP address blacklists, with reports suggesting that they can be rented for as little as $100 an hour[xi]. Another proven option is extortion, based upon the threat of using the collective 'fire power' of the compromised systems to launch a Distributed Denial of Service attack. Notable victims in this respect have included online gambling sites, which have reported being targets of demands for $50,000 from Russian organised crime syndicates[xii]

Another important factor is that those releasing the malware that introduce the backdoors will not necessarily be those that ultimately exploit the compromised

systems. A supply chain is emerging. Botnet 'herders' will pay hackers for their botnets. Indeed, botnets are turning up in the marketplace – with evidence of them appearing on online auction sites. Your compromised system really can be sold to the highest bidder! The fact that the malware now effectively feeds off the infected system means that it now meets the third criterion of an effective parasite.

In considering where the money is being made, it is relevant to ask whose systems are getting compromised. Unsurprisingly, the answer is often those with the least ability to protect themselves – such as small and medium enterprises, and domestic users, all of whom often lack the money and expertise to tackle the problem effectively. Indeed, findings published earlier this year by network management firm Sandvine suggested that as much as 80% of spam now originates from residential broadband networks[xiii]. Such findings suggest that the business community may be as proactive as it likes in maintaining effective anti-virus and other network security protection – the problem is never going to disappear while domestic systems are less secure. Indeed, organisations will remain at indirect risk of malware attack whilst their employees use computers at home.

Evolution continues

Even though malware has been a recognised threat within the general IT community for well over 15 years, it is effectively a bigger problem now than it has ever been before. This situation has arisen, despite improvements in protective technologies, because many systems do not use these technologies effectively, and many others remain open to be exploited by resolvable vulnerabilities that can let new strains in.

Based upon what we have seen in the past, there is little doubt that malware will continue to develop. The threat that we face tomorrow has the potential to be significantly worse than that of today. In this respect the mobile environment is very likely to become a 'hot zone' in the future – and indeed recent weeks have witnessed the emergence of notable proof-of-concept programs on major mobile platforms[xiv]. From one perspective, we might say that mobile devices are just another technology, but there is one very notable difference - this time, in an all-to-close parallel to their biological counterparts, viruses will have the opportunity to become 'airborne'. 'Physical' contact, through a wired network infrastructure, will no longer be required for infection to occur.

To summarise, we have seen in the last few years the evolution of computer viruses from a laboratory phenomenon, of interest to a small number of technically literate people, into a truly effective parasite that is capable of spreading rapidly and efficiently. It is able to resist efforts to destroy it and to conceal itself in an infected system. And now it is also able to gather for its creator resources that give it a truly significant reason for existence. If we thought malware writers were persistent or creative in the past, imagine what the future will bring, now that there is money in it!

Symantec is exhibiting at Infosecurity Europe 2005 which is Europe's number one information Security Event. Now in its 10th anniversary year, Infosecurity Europe continues to provide an unrivalled education programme, new products & services, over 250 exhibitors and 10,000 visitors from every segment of the industry. Held on

the 26th – 28th April 2005 in the Grand Hall, Olympia, this is a must attend event for all IT professionals involved in Information Security. www.infosec.co.uk

About the authors

Dr Steven Furnell is the head of the Network Research Group at the University of Plymouth, UK. He has been actively involved in security research for over 12 years, and has authored numerous papers on the topic, as well as the book 'Cybercrime: Vandalizing the Information Society', in which the evolution of malware, and several case examples, are examined in detail.

Dr Jeremy Ward is Service Development Director at Symantec (UK). He has been working in information security for 22 years in both government and industry, but before that was a research entomologist – hence the interest in parasites! He sits on a number of government and industry working groups, such as the OECD's Working Party on Information Security and Privacy, the Home Office Government and Industry Forum on Information Security, and the CBI' s Information Security panel.

[i] Cohen, F. 1984. ``Computer Viruses - Theory and Experiments'', originally appearing in IFIP-SEC 84 and also appearing as invited paper in Computers and Security, vol. 6 no. 1, Pages 22-35. See also http://www.all.net/books/virus/index.html

[ii] MessageLabs. 2004. Email security intelligence report: January–June 2004. http://www.messagelabs.com/emailthreats/intelligence/whitepapers/pdf/sixreport.pdf

[iii] "W32.Bobax.D", Symantec Security Response, 19 May 2004. http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.bobax.d.html.

[iv] "W32.Beagle.AB@mm", Symantec Security Response, 15 July 2004. http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.beagle.ab@mm.html.

[v] "W32.Mydoom.M@mm", Symantec Security Response, 26 July 2004. http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.mydoom.m@mm.html.

[vi] "Backdoor.Zincite.A", Symantec Security Response, 26 July 2004. http://securityresponse.symantec.com/avcenter/venc/data/pf/backdoor.zincite.a.html.

[vii] "W32.Gaobot. BAJ", Symantec Security Response, 2 August 2004. http://securityresponse.symantec.com/avcenter/venc/data/pf/w32.gaobot.baj.html.

[viii] http://securityresponse.symantec.com/avcenter/alerting_offerings.html

[ix] "Threat severity assessment", Symantec Security Response. http://securityresponse.symantec.com/avcenter/threat.severity.html.

[x] Symantec Internet Security Threat Report. Trends for January 1 - June 30 2004. Published September 2004.

[xi] "Fraudsters selling use of home PCs", Metro News, 8 July 2004. http://www.metronews.ca/tech_news.asp?id=1862

[xii] "Russian Mafia target online gambling sites", Online Casino News.com, http://www.onlinecasinonews.com/ocnv2_1/article/article.asp?id=4460

[xiii] Sandvine. 2004. *Trend analysis: Spam Trojans and their impact on broadband service providers*, Sandvine Incorporated, June 2004.

[xiv] Dwan, B. 2004. "The mobile phone virus", *Network Security*, July 2004, pp14-15.