FEATURE

The Real Virus Problem

Jim Bates

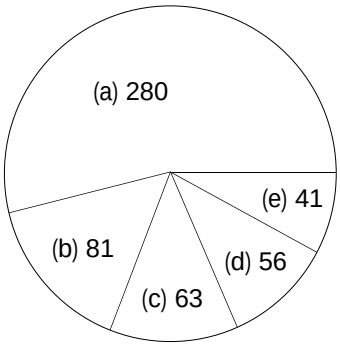
There has always been a pressing need for reliable information concerning computer virus activity in the real world: only by accurate assessment of the problem can an effective defence be created. Thanks mainly to the marketing efforts of the anti-virus industry around the world, the true extent of the problem has been efficiently concealed beneath a ragbag of pseudo-scientific projections, surveys, reports, forecasts and speculations. Here I present the findings of a recent survey of UK computer programmers, conducted without any input from the software vendors.

Vital Statistics

The infamous Tippett Prediction appeared to forecast virus infections of galactic proportions by the end of this century. Since then, most of the information concerning virus prevalence has either been unabashed hyperbole and exaggeration designed primarily to frighten users into buying a particular anti-virus package, or simply gathered in such a way as to invalidate the statistics.

One of the biggest problems in this area is that, following the grossly overestimated predictions about Michelangelo prevalence, predictions from within the industry are seen to be self-serving at best. Many anti-virus companies experienced record sales in the scanning frenzy which preceded 'Michelangelo Day' in 1992, and ever since, the public has been understandably wary of industry-generated figures.

Academic discussion of the pros and cons of rare and exotic virus techniques, coupled with the magpie collection complex displayed by vendors and researchers intent upon playing the numbers game, may be very stimulating. Such counting, however, bears little direct relevance to the problems faced by computer users. Similarly irresponsible attitudes to virus writers themselves encourage a whole group of prospective 'researchers' to think it perfectly acceptable to write viruses for 'research purposes' and then pass them on to others, to swell their collections.



Breakdown of virus type: (a) Never had a virus. (b) Had a boot sector virus. (c) Unsure of virus type (d) Had a parasitic virus (e) Had both boot sector and parasitic viruses.

Those researchers genuinely concerned with helping users have had to rely upon verified reports of virus infections coming in through their own channels, as well as upon occasional statistics produced by other trusted organisations such as the Police. Until now, this is all they have had to enable them to evaluate the extent of the problem. We may, however, be seeing the beginning of a new trend, with the publication of the results of a survey conducted by the *Institution of Analysts and Programmers* (*IAP*). This organisation is dedicated to the promotion of excellence amongst computer professionals, and their survey represents the first truly independent attempt which I have seen to evaluate the real extent of the virus problem.

Setting the Scene

Several fascinating revelations from the results of the survey confirm the reliability of the approach adopted by responsible researchers in the UK. First, existing figures seem to indicate that under 2% of known viruses are actually at large and causing problems for real computer users. Second, it appears that there is a slight preponderance of boot sector over parasitic viruses, despite the fact that parasitic types form the vast majority of most collections. Finally, it is thought that most of the real problems arise from a handful of aged viruses (old, that is, when compared to the age of the virus problem).

The *IAP* survey consisted of a simple questionnaire sent out to around 2,500 members (mainly in the UK) and 521 (circa 20%) were returned. I understand that this is a better than average response to such things. The figures which follow include approximate percentages, in order to give an idea of just where changes are occurring in this field.

In the Wild

Of those replying, 280 (54%) reported no virus incidents. When asked how long ago the infection occurred, the remaining 241 were split 166 to 75 (69% to 31%) - the larger group indicating infection within the past year.

The survey then went on to determine which types of virus had been noted. Here, 81 (34%) definitely identified boot sector viruses only, 56 (23%) said parasitic viruses only, 41 (17%) experienced both types, and the remaining 63 (26%) did not know what type of virus had infected their computer. There were eight different boot sector viruses and 14

different parasitic varieties reported, so even if the 63 people who were unsure of the type all had different viruses (extremely unlikely), well under 100 different viruses would have been reported at large. This seems to confirm the current suggestion of approximately 40 to 45 common viruses causing almost all real-world problems.

A further breakdown of the virus types indicated that just five viruses accounted for around 93% of all boot sector infections (Form 38%, New Zealand 31%, Michelangelo 9%, Tequila 8%, Spanish Telecom 8%) whilst another four viruses caused around 65% of parasitic infections (Cascade 26%, Jerusalem 17%, Yankee Doodle 11%, Dark Avenger 11%). Thus the overall picture shows that of the 234 people who were able to identify the virus, 188 (80%) had been hit by one of just nine viruses.

This again tallies with most observed data from other sources, and is a far cry from the threat of 'thousands of viruses' which some vendors claim are in the wild.

"It would seem from this that an anti-virus policy alone is no real defence against the threat."

Changing Times

The survey revealed some interesting variations on the point at which infections were noted, and additional analysis was made of this. The most common virus reported from more than one year ago was Tequila (31 instances) followed by Cascade (14 reports), New Zealand (11) and Form (10). Since there were 100 reports within this time frame, these figures also represent percentages. The results for the past year show dramatic changes. The most common virus now is Form with 41 reports (21%), followed by New Zealand with 31 (16%) and Spanish Telecom with 11 (6%).

As well as obtaining these figures for actual virus infections, users were also asked how those affected had dealt with the problem. The response showed that over 82% had used proprietary anti-virus software, while around 14% had dealt with the problem in-house. Just 3% had contacted an outside consultant for further help.

Another series of questions asked how users handled the threat of virus infection. Rather surprisingly, 41% had an anti-virus policy and had been hit, 41% had *no policy* and had been hit, 13% had no policy and had not been hit, and the remaining 5% had an anti-virus policy and had not been hit. It would seem from this that an anti-virus policy alone is no real defence against the threat. The type of anti-virus measures which users implement were analysed as follows: 10% banned incoming software, 25% had some form of quarantine arrangement, 30% maintained control of software sources and 27% conducted regular software audits.

Helping with Enquiries

A final question concerned the reporting of virus attacks. This contained the biggest surprise - fewer than 6% of the respondents actually reported the incident to the police!

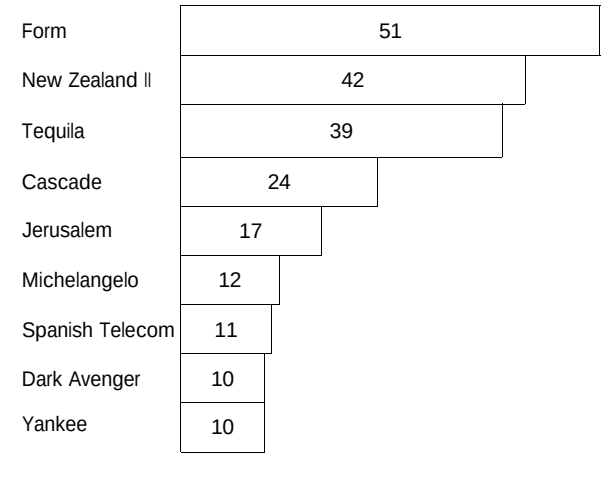
These figures certainly confirm that a virus problem does exist, since nearly half of all respondents had experienced an attack. However, the extent of the problem indicates that the level of user awareness, at least in the UK, has contained the problem within far narrower limits than those suggested by many vendors of anti-virus software.

All the viruses reported are relatively simple ones; there is a distinct absence of the more exotic types beloved of the academic researchers and virus collectors (Commander Bomber, Starship, DIR II, Tremor and so on). It seems that the presence or absence of an anti-virus policy has little effect in preventing infections. This can only be due to poor implementation and user education: a well designed virus defecne will prevent infection.

I was most disappointed to read just how few people report the problem to the police, as this has been a major source of statistical information on virus prevalence for some time now. However small their sample may have been, its usefulness is amply demonstrated by the similarity of the *IAP* survey. I would urge all users to reconsider any policy which prevents reporting virus outbreaks.

Each report is treated in the strictest confidence and provides the only possibility of bringing the perpetrators to book. If you need further information, call the *Computer Crime Unit* at *New Scotland Yard* on +44 (0)71 230 1177.

I am particularly indebted to Michael Ryan, Director General of *The Institution of Analysts and Programmers* (+44 (0)81 567 2118), for allowing me access to these figures and analyses.



UK's 'Most unwanted' list: The top nine viruses account for 80% of all virus outbreaks among those polled.