Is virus writing really that bad?

White Paper written by:
Paul Ducklin, Head of Global Support,
Sophos, Australia

Global Secure Systems

Is virus writing really that bad?

Paul Ducklin, Head of Global Support, Sophos Anti-Virus, Australia
Presented at the Fourth Anti-Virus Asia Researchers (AVAR) Conference 2001
Hong Kong - November 2001

SUMMARY

In a world in which some anti-virus companies regularly overstate the risks posed by individual viruses in order to hype up the threat, it can be hard to judge the seriousness of the problem. So this paper tries to answer the question 'is virus writing really that bad?' with a balanced view of the situation. Even though some of the so-called good guys come in for firm criticism, we conclude that the answer is a very definite yes.

What do people think of virus writers?

At Sophos, we deal with thousands of people every month who have been infected, entirely unwittingly, by computer viruses. As you can imagine, these people, almost without exception, have a very low opinion of virus writers.

Even when the virus involved is not particularly dangerous and can be removed easily, victims still feel a sense of invasion and discomfort at having been attacked by an unknown assailant. "I wish I could get my hands on the guy who did this to me," is a common cry. This fact is important: even viruses which do nothing more than spread are seen as dangerous and intrusive, and we shall return to it later.

> Many computer virus researchers have a low opinion of virus writers. They are seen as irresponsible and unethical at best, malevolent and overtly criminal at worst.

Many of those who are involved in (or on the fringes of) computer virus research share the same low opinion of virus writers. They are seen as irresponsible and unethical at best; malevolent and overtly criminal at worst. As one anti-virus professional (who shall remain nameless here) is popularly claimed to have said: "They're scumbag w**k**s and they belong in jail."

Not everyone in the anti-virus field is quite so vehement. For example, Sarah Gordon, currently at Symantec, has consistently taken a more conciliatory view. In a survey of virus writers, she claims that:

> ...The virus writer has been characterized by some as a bad, evil, depraved, maniac; terrorist, technopathic, genius gone mad, sociopath. This image has been heightened not only by the media, but by some of the actions of the virus writers themselves. Public communications from the writers, in the form of echo-mail messages, often seem to indicate they are intent on doing as much damage as humanly possible. Their electronic publications have in the past reinforced this, and the very fact that they release viruses may seem to confirm it: these people are bad. [But it can be argued that] this is a gross oversimplification of the situation, and that the virus writing aspect of these individuals is not sufficient to characterize them into one group simply labelled 'unethical people'... (1)

Some regard Gordon as overly sympathetic to the virus writing counterculture, even though she regularly states in her writings that virus distribution is wrong and cannot be condoned.

Virus writers, of course, have a very different outlook. Whilst most of their justifications for writing viruses are puerile and not worthy of comment, at least one aspect of virus writing and distribution has drawn support (albeit theoretical and guarded) from people outside the virus scene.

Proponents of an unregulated internet, by means of which the freedom of speech could more or less be assured, have argued that viruses are program code; that program code is speech; and therefore that the circulation of viruses on the internet is not something any freedom-minded individual should oppose. Virus writers have not been slow to capitalise on this source of support.

This sort of argument has been heard the loudest in the United States of America, where the First Amendment to the Constitution guarantees free speech. Whilst the US courts seem unable to agree whether program code really is speech or not, some legal experts show little regard for the free-speech claims of the virus counterculture (2,3):

> ...Internet speech doesn't have more constitutional protection than speech disseminated in a more old-fashioned and limited manner. In particular, direct threats or other messages that by their very utterance cause harm receive no more protection on the Internet than anyplace else. Releasing a computer virus through e-mail deserves no greater immunity than crying 'Fire' in a crowded theater... (4)

This common sense view matches that held by most actual victims of viruses. Viruses cause harm; therefore viruses are bad; therefore virus writing is bad. This seems like a reasonably uncontroversial viewpoint.

Should we regulate against virus writing?

Unfortunately, there are two potential problems with the syllogism 'viruses are bad; therefore virus writing is bad'. Both of these problems are much-argued topics. We shall summarise the arguments here.

First, what happens if you do not agree that viruses are bad? You may accept that most viruses are bad — but if we can find even a single example of a good (or perhaps a benign or neutral) virus, then clearly writing such a virus cannot be bad. If this were the case, then regulations against virus writing would clearly be wrong (or at least very hard to devise).

Many good viruses have been suggested. Fred Cohen is one computer virus researcher who thinks that good viruses can exist (5,6). For example, he proposes a compression virus, which spreads from program to program, compressing the host during infection and thus saving on disk space. Because it is viral, it finds its way through your files automatically, saving more and more disk space as it goes.

But much of Fred Cohen's virus research is theoretical, and just doesn't pan out in the real world. For example, not all programs can be safely compressed — some programs, such as anti-virus utilities, check their own integrity before running, to detect any unauthorised changes. This includes (as it should) changes made by Cohen's good virus.

The fact that it is effectively impossible to control a virus after it has been released suggests we should believe all viruses are bad.

Despite Cohen's claims, the fact that it is effectively impossible to control a virus after it has been released suggests we should believe all viruses are bad. If you do not wish simply to accept this, you may find it useful to work through Vesselin Bontchev's systematic discussion of the topic in (7). Most, if not all, of the functions proposed for 'good' viruses can be carried out more easily, controllably and reliably using traditional tools such as logon scripts or system management software.

Second, what happens if you can find situations in which virus writing may be helpful? Even if the virus you write is harmful, you may be able to learn about virus prevention by creating it, and you can take strict precautions to ensure it is destroyed once your experiments are complete.

There are actually situations in which deliberately creating new viruses in a secure laboratory can be useful. For example, many virus-writing toolkits exist which allow inexperienced virus writers to produce new viruses easily. But these toolkits often generate viruses that are sufficiently similar, and detection identities can be written to detect reliably all possible outputs of the toolkit. Determining the similarities between the viruses produced by a generator is usually much easier if you actually use the generator to create a representative sample of viruses. And testing your generic detection of toolkit viruses is almost impossible to do in a statistically significant way without running the generator.

Interestingly, despite the apparent benefits of deliberately creating viruses in a laboratory setting, the anti-virus community is divided on this issue.

In a survey carried out for their Virus Bulletin conference paper in 2001, Hartmann, Perry and Zwienenberg asked about 50 anti-virus researchers whether it was acceptable to generate viruses for test purposes (8). Approximately 35% said it was not, even when testing the generic detection of viruses made by a virus generating toolkit.

Notwithstanding this 35% (since some of them are involved in anti-virus software development, you may wonder how, or if, they test their products), it seems reasonable to conclude that:

- All viruses are bad;
- Virus writing may be good, neutral or bad;
- Virus writing is bad if the viruses escape;
- Virus writing is neutral or good if they do not escape.

This suggests that virus writing (or virus generation) should only be undertaken by knowledgeable and responsible researchers under isolated and controlled conditions. Unless these conditions apply, and are carefully enforced (for example, through the use of a physically secure and separate virus laboratory), virus writing is bad.

So, if virus writing is possibly good, but only when the good guys do it safely, should codes of practice for anti-virus research be regulated? Suggestions for a mechanism of this sort have come from unexpected sources, including the London School of Economics. Alistair Kelman writes:

> As a staunch defender of Free Speech and the rights of young people to experiment with their lives, in recent months I have had to face up to some unpalatable facts — virus writing is evil and cannot be justified in any circumstances. It follows that prosecution of virus writers is something which should be universally accepted as appropriate action. Virus writing needs to be recognised as a criminal act by international conventions and virus writers should always be subject to extradition. Just like murderers and terrorists, virus writers should find no escape across national boundaries. And the investigation of computer viruses needs to be a regulated activity with failure to apply for regulation being a criminal offence... (9)

Kelman claims that virus writing can never be justified, which unfortunately misses the point that it can be used to improve anti-virus products when carried out in a secure environment.

Furthermore, considering the dramatic pace of the anti-virus industry, a regulatory framework such as that suggested by Kelman could become a bureaucratic nightmare in which the State would end up stifling innovation, slowing down anti-virus research, and increasing the cost of anti-virus software.

In short, we should not regulate against virus writing, or even attempt to regulate anti-virus research. Where the State, the police and the legal system should be involved is in identifying, prosecuting and convicting those who deliberately spread viruses (whether they have written them or not) outside a laboratory.

Can virus disseminators be punished?

The same people who wish they could get their hands on the perpetrator after a virus attack often ask us why they hardly ever hear of those who write and distribute viruses getting into trouble.

Unfortunately, prosecutions of virus writers are rare, even in countries in which there are well-established laws which prohibit unauthorised access to, or modification of, other people's computers. Only a few significant cases exist, which we shall look at now.

Robert Morris wrote the infamous Internet Worm in 1988 (10). This was a virus which spread from computer to computer automatically, mounting a series of attacks on systems which were visible from each infected host. There were three different attacks: the first guessed passwords using a small (under 500 word) dictionary attack; the second used a debugging backdoor in the sendmail program; the third exploited a buffer overflow in the fingerd daemon.

Allegedly due to a bug in the virus, it spread very much more rapidly than Morris anticipated — so fast that the internet (which consisted of thousands rather than today's many millions of systems) became largely unuseable until the virus was analysed and preventative measures taken around the network.

Morris was prosecuted. He was sentenced to three years of probation, 400 hours of community service, and a fine of US$10,050 (11).

Cornell (which is where Morris was a student at the time of the Internet Worm) was also the site of virus-related arrests in 1992. Those arrested were accused of deliberately infecting software with a Macintosh virus before uploading it to an archive at Stanford, from where it was downloaded and spread inadvertently by other users.

They received no sympathy from John Norstad (who was at the time the author and maintainer of a free Macintosh anti-virus program, Disinfectant):

> ...Norstad took the opportunity in his release announcement to mention that three Cornell University students have been indicted on an assortment of felony and misdemeanor counts, including first-degree computer tampering, in connection with the release of the MBDF virus this spring. They are presently awaiting trial. Norstad hopes that this news will remind potential virus writers that computer viruses are taken seriously, and that writing them and releasing them is a crime that can, should, and will be punished under the law... (12)

The trio were sentenced to several hundred hours of community service (13).

Christopher Pile was prosecuted in the UK in 1995 (13). He wrote a polymorphic toolkit which could be linked with a regular virus to turn it into a polymorphic one which was randomly variable and much harder to detect. He wrote an instruction manual for this polymorphic engine, which he called SMEG (Simulated Metamorphic Encryption Generator), in which he encouraged the use of SMEG in producing hard-to-detect viruses (14).

Pile went further: he also wrote two viruses (Pathogen and Queeg) which made use of the SMEG engine; he included disk-formatting code as part of the side-effects of the viruses; and he deliberately planted infected files where he knew they would be downloaded and run by unsuspecting users.

After an investigation which traced the virus back to Pile, he pleaded guilty to 11 charges under the UK's Computer Misuse Act. A number of companies testified that they had been infected and suffered loss of data. Pile was sentenced to 18 months in prison.

David Smith of New Jersey, who wrote the Melissa virus, which was designed to spread rapidly via email, was also identified after a police investigation.

His virus, released in 1999, immediately distributed itself to the first 50 entries in an infected computer's address book (for many users, these entries included groups of email addresses, so more than 50 individual mails were often sent out). This resulted in a worldwide pandemic which became troublesome within hours of the first reports of the virus.

Like Pile and Morris before him, Smith pleaded guilty to the charges he faced as a result of his crimes (he not only set the virus loose, but used a stolen AOL account with which to do so). He admitted to causing damage of over US$80,000,000.

Surprisingly, according to Business Week, Smith has still not been sentenced (15).

Onel de Guzman, allegedly the author of the LoveLetter virus (which spread in a similarly aggressive way to Melissa), was also identified and arrested soon after his virus was released. But so far he has escaped the plight of Pile or Smith. De Guzman ultimately had all charges against him dropped because laws in the Philippines under which he could have been prosecuted were not enacted until June 2000, shortly after the appearance of the virus he was accused of having released (16).

This was not de Guzman's first brush with authority: his university thesis was rejected (and he subsequently dropped out of college) because it proposed a project to develop a password stealing program which could be used to obtain free internet access illegally (17).

The most recent virus-related prosecution is that of Jan de Wit, the Dutch author and disseminator of the SST-A virus. This virus arrived in an email claiming to contain a picture of tennis pin-up Anna Kournikova. In fact, the email's attachment was a thinly-disguised Visual Basic Script program which attempted to send a copy of itself to every entry in the user's email address book.

The penalty handed down to de Wit in September 2001 was 150 hours community service or 75 days in prison. Compared to the sentences handed out to Morris, Pile and the Cornell trio of 1992, some people regard this sentence as rather light (18).

Are harsher penalties in order?

One of the reasons given for de Wit's comparatively light sentence is that the damage figures compiled for his sentencing were correspondingly small. Apparently, only 55 infections with a total of US$166,827 worth of damage were documented in evidence presented to the court.

But what seems surprising here is that US$166,000 is regarded as a small amount of damage for a computer virus. Unfortunately, the anti-virus industry itself must take some of the blame for this perception.

Vast damage figures, some of which beggar belief, have been proposed for previous viruses. Some sources suggest that the LoveLetter virus cost US$10,000,000,000 (16). Even the CodeRed virus (which could be removed effectively, albeit temporarily, simply by rebooting your computer) has been claimed to have cost US$2,600,000,000 (19).

As long as the anti-virus industry gives credibility to figures of this sort (the above CodeRed figure, for example, was dutifully republished by the vendors of Norton Anti-Virus), damage which amounts only to hundreds of thousands of dollars will continue to be regarded as small in comparison.

Astonishing damage figures attributed to viruses are not new. During Pile's sentencing, the judge heard evidence from a number of companies who had suffered infection from his viruses. Two of them proposed a reasonable-sounding damage figure of GBP1,000 each. A third company (whose figure was rejected as unsubstantiated by the judge) decided to include three weeks of network downtime on two continents, and declared its total cost as GBP250,000 (14).

Vast damage figures, some of which beggar belief, have been proposed for previous viruses.

The need to put a financial figure on the effects of viruses on users also causes us to lose sight of the human costs which virus writers can extract from their victims. The side-effects of being infected by a virus may seem minor when compared to those of other relatively common crimes such as assault, mugging and burglary. Yet, as we mentioned above, many virus victims nevertheless feel a sense of invasion and discomfort at having been attacked by an unknown assailant.

Recently, Sophos technical support staff received an email of thanks from a man who had used Sophos Anti-Virus to disinfect a friend's computer. The friend was infirm and felt insecure outside his home. Access to the internet had given him the opportunity for more regular interaction with his friends; the virus infection had interfered with his internet connectivity and cut him off from this contact.

Suspicious of his sudden silence, our correspondent had gone round to find his friend incommunicado and emotionally withdrawn as a result of the virus attack, which was as motiveless as it was senseless and debilitating.

What can we do to improve the situation?

Revisiting what we have already discussed, we note that:

- All viruses are bad;
- Virus writing is bad if the viruses escape;
- Openly distributing viruses is rightly criminal in many countries;
- But those who commit this crime are rarely punished.

Perhaps the most obvious way to punish virus writers fairly (some have argued that Pile's sentence seemed as harsh as de Wit's seemed light) is for frequent prosecutions with modest penalties.

This would allow even apparently minor virus writing and distribution offences to be pursued quickly and effectively, without the risk of being seen as victimising those few whose viruses happen to become widespread enough to attract outrageous damage estimates. As Allan Dyer points out:

> ...I strongly believe that the probability of getting caught is as important as the severity of the sentence in deterring potential criminals. For example, it is illegal to smoke in lifts in Hong Kong, and lifts have signs saying the penalty is HK$5000. However, I often enter a lift and smell cigarette smoke, and I have never seen or heard of someone being fined. The chance of getting caught is (virtually) nil, so the heavy fine is no deterrent. If the fine was HK$100, but offenders were caught 50%+ of the time, the practice would quickly stop. Very few virus writers or distributors have been caught, so the severity of punishment is small deterrent... (20)

For this to work, users (and companies) need to be prepared to lodge complaints; anti-virus companies and the media need to make an effort to publish realistic estimates of the damage caused by viruses; and authorities such as schools, colleges and the police need to be prepared to act swiftly, efficiently and without drama.

Perhaps if virus writing could be dealt with like vandalism, speeding or graffiti, we would see fair and regular punishment which also acted as a real deterrent.

Perhaps if virus writing could be dealt with like vandalism, speeding or graffiti, we would see fair and regular punishment which also acted as a real deterrent.

References

1   Gordon, S. "The Generic Virus Writer". Proc. Fourth Virus Bulletin Conference, Jersey, 1994.

2   US District Court, Northern District of California. "Daniel J. Bernstein vs. US Department of State". California, 1995.

3   US District Court, District of New York: "Memorandum Order, in MPAA v. Reimerdes, Corley and Kazan". New York, 2000.

4   Tribe, L. "The Internet vs. The First Amendment". New York Times, 28 April 1999.

5   Cohen, F. "Computer Viruses - Theory and Experiments". IFIP Computer Security Conference, Toronto, 1984.

6   Cohen, F. "A Case for Benevolent Viruses". Pittsburgh, 1991.

7   Bontchev, V. "Are 'Good' Viruses Still a Bad Idea?". Hamburg, 1994.

8   Hartmann, J; Perry, D; Zwienenberg, R. "Accepted Methods of Anti-Virus Research". Proc. Eleventh Virus Bulletin Conference, Prague, 2001.

9   Kelman, A. "The Regulation of Virus Research and the Prosecution for Unlawful Research?". LSE Computer Security Research Centre, London, 1997.

10 Spafford, E. "The Internet Worm Program: An Analysis". Purdue University, Indiana, 1988.

11 "Timeline of Computer History". http://www.computerhistory.org/, Mountain View, California, 2001.

12 Anbinder, M. "Disinfectant 2.9 Released". TidBITS#132/06-Jul-92, 1992.

13 Jackson, D. "Virus Warning". University of Aberdeen Computing Centre Newsletter, Aberdeen, Scotland, 1995.

14 "Black Baron Behind Bars". Virus Bulletin, Abingdon, England, December 1995.

15 Poulsen, K. "Melissa Virus Prosecution in Limbo". Business Week, 30 July 2001.

16 "LoveBug Suspect off the Hook". CBS News, 21 August 2001.

17 de Guzman, O. "Email Password Sender Trojan". AMA Computer College, Manila, 2000.

18 "Kournikova virus author sentenced". http://www.sophos.com/, England, 27 September 2001.

19 "Code Red Computer Worm Cost Set at $ 2.6 Billion". http://enterprisesecurity.symantec.com/, USA, 04 September 2001.

20 Gordon, S. "Virus Writers — The End of Innocence". IBM, New York, 2000.