FEATURE 2

Virus Writers – Part 3

Sarah Gordon
IBM Research

So far in this series we have covered five of the most frequently asked questions concerning virus writers. In this, the third and final part of the series, we will examine the question that seems to raise the most heated debate of all: why do they do it?

Justifications

As a starting point, let us approach the topic from the viewpoint of the virus writers. In their own words, how do they *justify* their actions? Notably, the arguments outlined below have remained relatively unchanged over the last few years. Such arguments were frequently encountered upon some of the FidoNet virus echoes and BBS in the early days. Here, borrowed (and paraphrased) from the satirical commentary 'Why Computer Viruses are Not and Never Were a Problem' [33], is an examination of the most prevalent justifications that appeared several years ago:

'We are doing research. This is just our research. You can't tell us not to do research – We have the right to do it. We have the right to write viruses, too, and to make them available – It's about freedom. We have the *right* to do this research and the *freedom* to make viruses available – You want to keep this "top secret" virus knowledge to yourselves, but we will set it free. We will educate the people. Information wants to be free – We are not really hurting anyone, we don't force anyone to download our viruses, and we don't force anyone to use them. That is up to the individual – You AV guys are all bad, in it for the money, you need us – You just don't understand!'.

Of course, one need not go back through the archives to see examples of these arguments. You need only read *current* Usenet news posts, to see some of the same old arguments made today, by new people who believe with all their hearts that they know something the rest of us do not. Here are some more contemporary examples [34]. Note that I am unable to credit the authors due to the fact that I could not authenticate them:

'The only justification my code needs is furthering education, and knowledge. These are the greatest strengths the human race has… – my goal is accomplished… my reaserch (sic) and making available this information to those who are interested… '.

As you can see, not a lot has changed. At this point, however, I would like to make an aside, and interject a few comments. I hear these arguments all the time, for the virus writers reading this, take note, please.

Programming computer viruses is not some super-élite, arcane art-form. It does not require some top-secret type of programming skills known only to the cognoscenti. Virtually anyone with the interest can learn how to do it, and just doing it does not make it 'research'. Good research implies certain goals, guidelines and appropriate scientific technique [35]; this is worlds apart from randomly injecting a small piece of self-replicating code into an unsuspecting, unconsenting and uncontrolled computer-using population. It is just plain irresponsible to experiment with viruses in such uncontrolled environments, given the potential for viral interaction with the computers of human subjects. This includes experimentation using your college or employer's network without their consent. No matter how you look at it, it is *irresponsible.*

It is also irresponsible to set self-replicating programs free where this interaction is an inevitable consequence of that action. Some would argue that placing viruses on the WWW is in fact setting them 'free', that placing viruses on the Internet for other people to experiment with is irresponsible because the program's author cannot control what someone else does with the viruses once they are made available [36, 37]. This is a question with philosophical and cultural colourings beyond the scope of this article, but please think about it!

However, there is certainly a potentially expensive, destructive cycle that follows the life of an ItW computer virus. There are issues of negligence and liability when it comes to making these types of programs available, with concern being shown by more and more organizations as evidenced in these examples of Membership Agreements and Disclaimers [38–41]. This is one reason why many Internet Service Providers now have 'acceptable use policies' which prohibit the distribution of computer viruses [42–44]. They do not want to risk being involved in lawsuits related to negligence. To any virus writer reading this article: if you *must* experiment, keep your experiment to yourself, or you might find yourself in the middle of just such a legal action.

Now that is cleared up, let us continue with some of the current justifications: 'If my code was used to damage someone's computer, that is the responsibility of the person who's (sic) immature behaviour has resulted in damage. Open your mind, and expand your horizons… its (sic) a huge world out there, if you can just get over your fears – … this is nauseating… you feel you have the right to censor, and condemn the creativity of young, brilliant minds. you fear what you dont (sic) understand… '.

There are other justifications expressed from time to time. One is, was, and has been, and probably will be, 'if it was not for us, you guys wouldn't have a job'.

This is not quite true. There is a relationship, certainly, but a relationship does not imply the existence of a positive justification. Consider the following statement: ‘If it were not for people who shoplift, the store detectives would be out of a job.’ Yet, shoplifters are not heroes and we do not consider new and novel ways of absconding with merchandise to be admirable or acceptable. Or: ‘If people didn’t throw trash on the ground at Disneyworld, the street cleaners would be out of a job’. Yet, we surely do not look upon those that throw lit cigarettes on the ground with admiration, do we?

The bottom line here is that while it is true that if virus writers did not release viruses, the users would not need anti-virus software (allowing most virus researchers to shift into other, equally interesting, areas of work), attempting to paint some lovely picture of healthy symbiosis is simply not supported by the facts.

Motivating Factors

So far, we have taken a brief overview of the justifications many virus writers use, and noted that most, if not all, of these reasons are far from new. Similarly, several of the motivational factors for virus writing are also unchanged.

Today, as yesterday, in some cases virus writers are motivated by simple intellectual curiosity. This is understandable, especially considering the free availability of viruses and the media attention given to viruses and virus writers. Virus writing continues to take place as a form of political expression; Stoned_June4th (Beijing) and Macedonia being two examples.

Viruses as an expression of love and admiration for the opposite sex or for peers continue to be keyed into existence. In the early days we saw viruses like Gergana, Neuroquila and the MtE ‘demo virus’. More recently, we find ‘love’ expressed a bit more directly via viruses like Ivana, which proudly proclaims:

```
  ‘Na kraju, samo jos da kazem: volim te,
Ivana [by utik]
     ‘And finally, I would like to say: I love
you, Ivana [by utik] [45]
```

Another motivation behind virus creation is to designate ‘turf’. In the past, viruses like NPOX and Vice planted the viral flag for NuKE; today, we have such ignoble creations as WM97/Antimarc [46]. In other cases, virus writing and distribution is positively correlated with being told ‘thou shalt not’. It is widely agreed upon by behavioural scientists that the ‘thou shalt not’ approach may not prove very effective in situations where direct and immediate consequences cannot be observed [47]. Thus, despite much saber rattling on the part of the anti-virus industry and lawmakers, legislating away the virus creation problem seems an unlikely solution.

Being ‘one of the boys’ appears to continue in importance, too; the need for peer approval is illustrated by gravitation toward ‘groups’, with group affiliation providing a form of social identity [48]. While there have been several cases of female virus writers documented over the past several years [49–53], females do not appear to have made a significant contribution to the population of those viruses in the wild. Currently, while females play a minor role in the virus-writing community as a whole, their presence appears to be a moderating influence in the community. There appears to be very little gender-related sexual bias within the community. Further research into gender issues related to group involvement and technology, and virus writing specifically, might provide some additional insights.

Finally, some virus writing has been the direct result of various forms of provocation by anti-virus researchers themselves. This was more common during the early days of the virus problem, when a (thankfully) small number of anti-virus researchers would insult the virus writers, calling them names [54–59] or claim they were too stupid to create a virus that ‘did xyz’. Shortly thereafter, we would find a virus doing or attempting to do ‘xyz’.

Disparaging remarks have been made regarding the young person’s appearance, or physical characteristics. While there is simply no point to this sort of ‘discussion’ [60], this cycle does unfortunately repeat itself from time to time today [61, 62], though with lower frequency. Such negative interactions continue to produce negative responses as well as negative impacts on users and should be avoided. Young people learn through transitive interaction, not debasement.

Recently, there has been a trend toward adapting the ‘open source’ mindset for publication of viral code, and this has not been lost on the virus-writing community. This is apparently done in an effort to warn users of the dangers of certain design philosophies. To quote one virus writer, ‘Some good virus writers like my friend VicodinES (who retired) are here to demonstrate the vulnerability of badly written softwares, like all Microsoft offerings. They don’t like destruction.’

It should be noted that it is not virus writers alone who think there may be some merit to the publication of viral source code. Some users report that on-line publication facilitates a wide understanding of exactly what viruses and payloads do; some believe such publication is actually essential in keeping corporate security people up to date.

However, not everyone shares this view. In particular, many in the anti-virus community believe such public dissemination of information is irresponsible. David Chess of *IBM’s Thomas J. Watson Research Center* has this to say about the issue. ‘The moderators should never let such things through. Unlike bug exploits, where at least a case may be made that it’s a valid last resort if a vendor has been notified of a bug and ignored it, viruses don’t go away when you just fix a bug’ (63).

It should be further noted that the differences between open source and availability for software in general, for security exploits and for computer viruses are substantial. Beyond the scope of this article, the effect on the user when these worldviews collide will be discussed in Vancouver at VB'99 in 'When Worlds Collide' [64].

For now, it should suffice to say that if virus writers are attempting to influence *Microsoft* or any other corporation by showing real or alleged vulnerabilities in the product line, it would seem a more responsible course of action would be to do so *without* the replicative mechanism. Certainly, it must be done in a private way that does not endanger other computer users' rights to safe computing.

Some virus writers are more honest with themselves. Here is an example of the reasoning given to me recently by one active virus writer [65], who will remain anonymous.

'i fully agree with you about it being irresponsible, i don't know why i release them on a web page. viruses have always fascinated me since i got infected myself the first time (it was parity boot b), since that i'm (lets call it) addicted to studying them by collecting and writing them myself. i don't feel good if i have nothing to do with viruses, no matter if VX or AV wise (AV, i'm doing alot of "anonymous" antivirus support for people on alt.comp.virus and i have been active on #nohack for some time helping people to get rid of their mIRC_worm infections..

so it doesn't make a big difference for me, i just like the VX people more then AV's – AV's like nick fitzgerald who believe that anybody who doesn't share their opinion has no right to exist). when someone says that he is writing viruses just for "educational purposes" it is a lie in my opinion (i think i have said that in some interview a long time ago also, and it was a lie).

i have often thought about why i'm really doing this (i could probably spend my time with more productive things) though till now i never really found out why. the best thing i came up with is that it is a "hobby"... you don't really know why you go play tennis, why you watch football matches, why you collect stamps... you just like doing it, and if you can't do it for some time you feel bad i guess you can't understand this.. do you smoke? i don't, and never did, so i really can't imagine why its so hard for people to stop smoking... i believe them anyway because i know that if i'd start smoking i'd also understand how/why they think so.'

I do not smoke, but I do understand. Becoming fascinated with viruses is not an alien concept to me. Like many other anti-virus experts (and virus writers), I became interested because I suffered the impact of a virus.

However, after understanding and appreciating the impact viruses can have on human beings in terms of their work and personal lives, many of which center around computers, it never occurred to me that creating and releasing more and more viruses was an acceptable way to behave. Too much depends upon the stability of computers for this sort of silly experimentation and potentially dangerous game.

Yet, for some virus writers, our societal dependence on computers is *exactly* the motivation for virus creation and distribution, and it is not a game to them. According to some virus writers, our society entrusts far too much important information to computerized technologies, to the point where there is a moral responsibility to take a form of action which forces us to reconsider this dependence. To them, the end justifies the means, and while this implementation of the civil disobedience *is* new, the concept is ages old.

The Songs Remain the Same

Why, you might ask, are we seeing the same old arguments, over and over? This is mostly due to the replacement factor, a direct result of the 'ageing out' phenomenon I described in part one of this series. This factor has a tremendous effect on the overall virus writing subculture.

By and large, the members of the virus writing community are in a constant state of flux. As mature adults exit from one side of the population, new, ethically normal but undeveloped adolescents enter at the other.

In turn, this continual flux provides a certain lack of development within the community. Hence, each new batch of virus writers is essentially discovering these arguments for themselves, leading to oft-repeated debates between the 'white hats' and the 'black hats'. Finally, those members who remain in the community are all somewhat ethically underdeveloped, further skewing the population, and making the role models there decidedly less than perfect.

It does not appear to be the case that virus writers are becoming more malicious *per se*. There may be more malicious viruses circulating nowadays, but this is probably attributable not so much to the fact that *people* are more malicious as to the fact that the *number* of people (some of whom by sheer chance are more malicious than the norm) having access to Internet technologies has increased dramatically. People are not getting worse. There is just more opportunity for those bad apples that have already rotted and fallen off the tree.

The Way Things Are

Despite the similarities, there are some differences in virus writing which are unfortunately becoming more and more common. These were first noted in 'The Generic Virus Writer II', presented at the *Virus Bulletin Conference* in 1996, where I introduced the concept of the 'New Age Virus Writer'. This concept became a prime-time news headline with the introduction of the Melissa virus into hundreds of thousands of networked computers.

Today, more and more virus writers have an increased awareness of connectivity issues that simply was not present in the early days. It should not be surprising that an increase in networked environments would lead to an increase in opportunities for people to learn about networks. The sorts of innovations that have come to exist in the past five years certainly add a new dimension to the problem of viruses.

Payloads now have the capacity for compromising an entire network, and more than a few virus writers are beginning to explore more general security issues. Melissa was not a one-shot-deal; Explorezip (see p.3 of this issue) indicates very much the shape of things to come.

This trend will probably continue over the next several years, and it is likely that there will be an increased cross-over between the security and virus worlds. In light of this, response time to new viruses will become paramount, as the presence of viruses on the corporate LAN may well become more than the current nuisance it is now and a matter of considerable urgency.

What has happened to the original groups that held all of these beliefs and had these motivations? In some cases, individuals have simply repositioned themselves, taking a ‘leadership’ role. In most cases, however, the members of old groups have grown up, realized that creating and releasing computer viruses is not a good or admirable thing, and moved on.

Some former virus writers have taken jobs in various computer-related industries; some have found other professional fields more rewarding. In a few years, most of the current crop (at least, the ethically normal ones, which we hope would be most of them) will probably ‘age out’ of this behaviour. However, unfortunately, there are always new ones to take their places.

Those that continue writing and making viruses available to the general public will be seen as ‘irresponsible’ at best, and criminal at worst (depending on one’s geographic location and what one does with the viruses once they are written). That said, it is interesting to note that while some have argued for stronger legal action, research into adolescent at-risk behaviour finds that youths are *not* significantly motivated by fear of legal reprisal or involvement with the criminal justice system. They are more likely to be influenced by peers, family and significant others whom they like and respect.

The Last Word

Fear of the law does not appear to be a major demotivator for many virus writers and it appears that for now, the community continues to play itself out over and over again. Until we begin to tackle the root causes of virus writer motivation, this will continue to be the case; a multi-disciplinary approach is required to solve a multi-faceted problem. Anything less is oversimplification.

[33] Gordon, S. 1994. Why Viruses are Not and Never Were a Problem. *From the Proceedings of the 1994 EICAR Conference*. St Albans, U.K.

[34] Public communication. 1999. Alt.Comp.Virus.

[35] Lawrence Berkeley National Laboratory. (1999). ELSI in Science. The need to KNOW vs. the need to GROW. http://www.lbl.gov/Education/ELSI/research-main.html.

[36] Gordon, S. 1993. Virus Exchange BBS: A Legal Crime? Legal, Ethical and Technical Aspects of Computer and Network Use and Abuse. *American Association for the Advancement of Science*. Irvine, California.

[37] VIRUS-L Digest. 1994. Volume 7, Issue 83.

[38] Owens, M. 1999. Killing Two Birds With One Stone. *Good To Know*. http://www.trade-attorney.com/goodtoknow.html.

[39] Membership Agreement. http://www.sexyclips.com/agreement.html.

[40] Disclaimer. http://www.snapit.com/PEG_disclaimer.html.

[41] Disclaimer. http://www.roweandmaw.co.uk/5const.htm.

[42] Acceptable Use Policy. http://www.verio.com/policies/aup.shtml.

[43] Acceptable Use Policy. http://www.telemanage.ca/disclaimer.html.

[44] Acceptable Use Policy. http://www.vas.net/policies.html.

[45] Ivana description from: http://www.Europe.DataFellows.com/v-descs/ivana.htm.

[46] W97M/Antimarc description from: http://www.Europe.DataFellows.com/v-descs/antimarc.html/.

[47] Klein, H. 1975. Behaviourally oriented treatment for juvenile offenders. *Corrective & Social Psychiatry & Journal of Behavior Technology, Methods & Therapy*. Vol 2, pp. 17-21.

[48] Kipke, M. & Unger, J. 1997. *Adolescence*. Street Youth, Their Peer Group Affiliation and Differences According to Residential Status, Subsistence Patters and Use of Services. Vol. 32, Issue 127.

[49] Anonymous. 1995. Private email and in-person communications. Used with permission.

[50] Anonymous. 1996. Private in-person communication. Used with permission.

[51] Anonymous. 1997. Private in-person communication. Used with permission.

[52] Anonymous. 1999. Private IRC communication. Used with permission.

[53] Anonymous. 1999. Private email communication. Used with permission.

[54] VIRUS-L Digest. 1991. Volume 4, Issue 126.

[55] VIRUS-L Digest. 1992. Volume 5, Issue 174.

[56] Skulason, F. 1992. Virus Trends. *From the Proceedings of the Virus Bulletin Conference*. Edinburgh, Scotland.

[57] VIRUS-L Digest. 1994. Volume 7, Issue 56.

[58] VIRUS-L Digest. 1994. Volume 7, Issue 4.

[59] Bennehaum, David. 1998. Heart of Darkness. *WIRED*.

[60] Solomon, A. 1994. The Computer Virus Underground. *From the Proceedings of the International Virus Bulletin Conference*. Jersey.

[61] Sterling, B. 1997. Sterling Versus Virus Writers. http://www.av.ibm.com/.

[62] Dufner, E. *Dallas Morning News*. 1999. Virus Writers make a science of mischief.

[63] Chess, D. 1999. Private email communication. Used with permission.

[64] Gordon, S. & Ford, R. 1999. When Worlds Collide. Preprint.

[65] Anonymous. 1999. Private email communication. Used with permission.