

FEATURE

Virus Writers – Part 1

Sarah Gordon

IBM Research

There are six questions I am often asked. The first is ‘when will you update your research on virus writers?’ The answer is ‘all of the time’. Several years of research produced The Generic Virus Writer study, the results of which were presented at the *Virus Bulletin* Conference in 1994. This initial qualitative research provided many valuable insights into the cognitive development of some of the world’s most prolific virus writers – at that time.

These insights allowed me to show that virus writers were *not*, despite some claims, a homogenous group. Understanding their differences and discarding stereotypes, the research began to play a role in helping others to understand this pressing problem – and begin developing some strategies for combating it. It enabled us to realize that they, and perhaps others like them, could be expected to ‘age out’ of virus writing. Good to know; there were not that many virus writers at that time and any leaving that proclivity behind would significantly ease the problem.

The second question is really two-fold: ‘what exactly is “ageing out”, and how can “normal” kids do things which most adults view as anti-social?’ The idea behind ageing out is relatively simple, and is well-accepted in other areas of research into anti-social behaviours [1, 2, 3].

Let us begin with one of the theories of moral development [4]. It is not the only one, but it is the one chosen as an instrument for the original study. As a child begins to mature, his moral/ethical development goes through a number of stages, with ages roughly correlated to levels in these stages:

Level 1: Pre-conventional morality.

Stage 1 – The ‘rightness’ of an act depends upon the immediate consequence of it. Rules are obeyed to avoid punishment.

Stage 2 – Naïve instrumental hedonism. Being good is the way to get a reward or satisfy a need.

Level 2: Conventional morality.

Stage 3 – Actions are judged on the merit of their intent. ‘Right’ is having a right motive and a concern for others. Conform to avoid disapproval or dislike of others.

Stage 4 – Acceptance of authority. ‘Right’ is keeping the rules of society. Conform to avoid censure by legitimate authorities, with resulting guilt.

Level 3: Post-conventional morality.

Stage 5 – Judgements become more flexible; rules must be impartial, and ‘the welfare of the many’ becomes paramount. Abide by laws for the welfare of the community.

Stage 6 – Normative ethics, based upon self-chosen principles. ‘Right’ is an obligation to the universal principles of equality, justice and respect for persons.

This is the short form of this particular theory. It is not without some weaknesses, primarily it disregards cultural differences that determine what is ‘moral’ in non-Western societies, resulting in a form of moral absolutism [5]. However, the strengths of this particular instrument are well-documented [6].

The existence of a normal, ethical, developmental stage/age relationship does not necessarily moderate individual behaviour consistently in any given situation until an individual is older, and capable of integrating thought and action in a more mature way. This brings us to the second part of the question ‘How can otherwise “normal teenagers” do irresponsible “wrong” things like “writing viruses”?’

I am sure most readers can think back to a time when they, or their children, behaved in some reckless or anti-social way. Just as one could know it is ‘wrong’ to stay out after curfew when his parents have told him it is (a) illegal and (b) against the house rules, one can know it is ‘wrong’ to write viruses – yet, still *do* the ‘wrong’ thing.

Usually, in those people who are within ethical norms, the anti-social behaviours tend to go away as they grow up. (Whether or not those who commit the acts are labelled ‘delinquent’ often depends on whether they are caught; it can also depend on race or socio-economic status.) When these behaviours go away, it is sometimes referred to as ‘ageing out’. Sometimes the behaviours may recur from time to time; usually they go away completely.

If it were really the case that the virus writers profiled were ‘normal young people’ in terms of general development, as the research suggested, we would expect them to ‘age out’ of virus writing. Would they? I pressed on, past the usual hurdles in longitudinal study, following up on the subjects over several years. (The only subject with whom I was unable to maintain contact was the adult employed virus writer and distributor.) To date, the original ex-virus writer has remained an ex-virus writer. The college student has aged out of virus writing. I would expect the last to follow suit, but this remains to be seen.

‘Ageing out’ will probably continue to be one factor in lessening the number of active virus writers. However, they do not all do it. That follow-up study also discussed developing trends, and predicted a future that was a bit darker. Okay, a lot darker.

The Darker Venture

Question three is ‘how old are these guys?’. I have talked with virus writers who claim to have started in their pre-teen years, and given their level of skill and familiarity with viruses, I see no reason to disbelieve them; however, youth does seem to be diminishing as a primary attribute.

Whereas in the early days, virus writing groups were generally populated by young men in their mid-teens to early twenties, the mean age of the virus writers in one currently active and well-known virus writing group is 23; the oldest member is 33. I have talked with virus writers who are in their forties. This is indicative of one disturbing new trend featured in *The Generic Virus Writer II* – involvement of those who are older and possibly more ethically mature in virus writing. How can this be?

Sure enough, we saw more and more of this type of involvement of older people, and predicted this would continue and increase. This involvement seems to take various shapes, sometimes not malicious, just curious. For example, it is not uncommon for some adults involved in testing of anti-virus software to alter a virus in an ill-conceived but well-meaning attempt to see ‘how good virus detection is’. No matter how well-intentioned, this can lead to problems, which are documented in [7].

Several macro virus variants appear to owe their creation to ordinary users’ experimentation. This is sometimes carried out as part of a quest to ‘understand’ the virus; or it is done with what appears to be no good motive, as such viruses have been released into the wild seemingly intentionally.

It is unclear whether these trends are due to a change in people (unlikely), technology (possibly), or simply that experimenting with viruses is seen as ‘less wrong’ as we approach the year 2000. In general, when objectionable or questionable behaviours are tolerated, even tacitly, they can take on a ‘legitimate’ tinge of acceptability [8]. Research is currently in progress to shed some light on this. My guess is that it is a combination of the three.

Data taken from *The Generic Virus Writer II* seemed to indicate that there is indeed a ‘New Age’ virus writer beginning to take shape – older, more network-aware and more technologically advanced than some of his predecessors. Did I say older and network-aware? I did. The fourth question people ask me is ‘what’s next in viruses?’. Well, I hate to say I told you so, but...

Melissa Magic

With regard to the virus *writer* known as VicodinES, several self-proclaimed virus writers have expressed sentiments along these lines:

If Vicodines did it, I’m sure he didn’t realise how many problems this would cause. I know that Vicodines spread some of his viruses, but he always said that he doesn’t want to destroy anything, he said ‘he just loves to annoy people around the world’. He hates destructive payloads, but he likes simple ‘annoying’ and rather humorous payloads like this ‘I think that [username] is a big stupid jerk.’ payload. I’m sure he wouldn’t have released this virus if he had known how much problems it would cause. [9]

At the same time, some of the same virus writers express anger at the idea of a virus being distributed to unknowing and unwilling individuals: many virus writers have wiped their hard drives, vowing to lay low until things cool down.

In the words of one virus writer:

I hear how some vX people say that they’d kill the author of melissa as it is his fault for other vx people getting hunted now also, for vX webpages being closed and so on., even though my own webpage has been closed also it doesn’t make me feel very good when i hear others talk about my friends like that. sure all of that has been caused by melissa, but i’m sure the author (of the virus) didn’t want this to happen, he wanted to spread his virus (like many of these, now pissed off, vX people do also),and teach vX people some new things – not bring their sites down and get them arrested. [10]

Another had this to say:

31th March – Melissa fucked us. Melissa has been tracked down to its author thanx to Micro\$oft GUID... They know have a proff that VicodinES is the author. Now the media hype has sarterd again, and the word virus is everywhere.... And, TOTALLY unrelated to that, sok went down as well as codbreakers.... Weird, uh ?? My server is still running and kicking asses, you can use my board communicate if you want... (It’s here for that, USE IT !!) Now I really wouldn’t be VicodenES, because I think media will make him an example and he WILL be bashed... [11]

Yet another had this to say:

to be honest guys,whoever wrote and spread melissa fucked all of us...to add more viruses to this thing would be lame as fuck and pointless....we would all just end up joining the now RIP authors.. for fucks sake get real people...we dont need any more grief . [12]

Profiles of individual virus writers are under re-evaluation, and are scheduled for presentation at The Blackhat Briefings in July 1999. Part 2 of this article (next month) will answer question five ‘How have they changed?’ and the most frequently asked question six: ‘Why do they do it?’.

1. Hollister, R. G. and Hill, J. *Problems in the Evaluation of Community Initiatives*. New York: Russell Sage Foundation. 1995.
2. Pfohl, S. *Images of Deviance and Social Control: A Sociological History*. 2nd ed., McGraw-Hill. 1994.
3. Keel, Robert. *The Evolution of Classical Theory: Rational Choice, Deterrence, Incapacitation and Just Dessert*. Rational Choice and Deterrence Theory. The Sociology of Deviant Behavior. 1999.
4. Craig, G. J. *Kohlberg’s Stages of Moral Development*. Human Development. Seventh Edition. Prentice Hall. 1996.
5. Colby, A. & Kohlberg, et. al. *A longitudinal study of moral development*. Monographs of the Society for Research in Child Development, 48 (1-2 Serial 200). 1983.
6. Baumrind, D. *A Dialectical Materialist’s Perspective on Knowing Social Reality*. New Directions for Child Development. 1978.
7. Gordon, S. *Real World Anti-virus Reviews and Evaluations - the Current State of Affairs*. Presentation. 19th National Information Systems Security Conference. National Institute of Standards and Technology, National Computer Security Center. Baltimore Maryland. 1996.
8. Craig, G. J. *Development in Modern Life: The effects of television*. *Human Development*. Seventh Edition. Prentice Hall. 1996.
9. Private communication. Used with permission. 1999.
10. Private communication. Used with permission. 1999.
11. Publicly available communication. 1999.
12. Publicly available communication. 1999.