FEATURE 1

Virus Writers – Part 2

Sarah Gordon
IBM Research

I will put off my discussion of why virus writers write viruses until Part 3, next month. This article will examine the question 'How have they changed?'. If you've been counting, this is question number five.

In October 1993, the number of virus writers who were actively contributing to the problem of computer viruses found in the wild comprised a relatively small percentage of the global computing population. The number of their viruses actually causing many problems was quite small too, especially considering the number of viruses known to exist – the number of computer viruses which were reported spreading in the wild was 71 [13], with a total virus count of about 3200 [14]. During this time, there were virus writers known and unknown; working on their own, and working in groups like Phalcon/Skism, RABID, NuKe, Trident and SLAM. They used handles like Dark Angel, Attitude Adjuster and Aristotle. They wrote viruses, placing them on publicly accessible BBSs, FTP sites, and WWW sites, and they kept some to themselves [15].

In some cases, they sent viruses only to anti-virus researchers, because while they wanted to show they could write proof of concept viruses, they did not want to release them to the general public. They wrote viruses that were not released in any way into cyberspace (for lack of a better term), and never caused anyone any problem (other than necessitating their inclusion in scanners 'just in case'); they wrote viruses that they did release into cyberspace, causing all sorts of problems. They made source code available, and they kept code 'just for their private individual use' or 'just for use within their own group'. They dedicated their viruses to various people, they used some viruses to promote their own groups or identities, and they left some viruses completely anonymous. They attended secondary schools and Universities, and they were professionally employed [16]. They began to beta-test viruses [17].

In May 1999, there are approximately 150 viruses found in the wild [18], with approximately 30,000 known to exist. Some virus writers are pretty well known, signing their creations, while some prefer to do their deeds in secret. Some labour alone, while others work in groups like 29a, SLAM (all-new, all-revised, and not related in any way to the original), The Codebreakers, and The NoMercy Virus Team. They use names like DarkMan, VicodinES and Knowdeth. Some put their viruses up on FTP or WWW sites; some prefer to keep them for themselves. Some restrict their distribution to within their own groups. In some cases, they send viruses only to AV researchers. Some virus writers today release their viruses to unsuspecting users; others do not actively release them. Some make code available, while others prefer to keep it to themselves. Some viruses are dedicated to individuals or causes; other viruses are used to self-promote. Some remain anonymously authored. Virus writers attend secondary schools and Universities. Some are professionally employed. Beta-testing of viruses is pretty common. Sound familiar?

New Bottles, Old Wine?

Some people claim interesting 'new' ideas have come out of the virus writing community. Has the 'creativity' of virus writers actually started to take on a whole new face? The answer, as is so common when analysing virus writers and their behaviours, is both yes and no. One purportedly new idea is something called (in its current incarnation), Project Zero. It was designed as an 'experiment' which should show what would happen if nobody in the VX community released viruses to the public any more for an arbitrary time period of, for example, one year [19].

While this may seem noble, one goal of such a project could be to lull the anti-virus developers and users into a false sense of security. Despite its emergence as a 'novel idea', the same idea was tossed around by NuKE affiliates in the old days [20]. Be it vortex or vacuum, the idea is the same, just dressed up in millennium garb.

Another 'new' idea is that viruses are actually 'evolutionary programs'. In particular, several virus writers have recently mentioned to me [21] their belief that replicating code could be used to explore various concepts of artificial life. This is certainly true, but not a new idea; it was explored long ago in [22, 23], to cite just two examples. Additionally, these types of experiments in authentic artificial life concepts are worlds apart from 'virus writing' and should probably not be mentioned in the same breath.

Then there is the idea of viruses that could be good entities, also frequently cited as a 'new' idea – discussed several years ago in [24, 25]. Padgett Peterson, well-known anti-virus and general security expert says it best: 'I have never seen a virus do anything that is not easier and more reliable to do without a virus (except be a virus, of course)' [26].

But Wait, this is New! Really!

One interesting and actually somewhat new idea which has come to light recently may show a slight change in the *modus operandi* of the virus writing community. In the early months of 1999, we saw alleged virus writers and distributors attempting to spread confusion by going 'public' on the Internet, registering such domains as datafellowes.com and vgrep.com.

The Codebreakers Internet site, which vanished abruptly in the midst of the Melissa investigation, was reincarnated as codebreakers.net on a site hosted by a large web hosting company in Florida. The site was no amateur-looking hodge-podge. It was particularly well done, with excellent graphics and a 'research' feel to it. It was registered to someone claiming to represent 'DataFellows, Ltd' [27]. At this time, the site appears to have been discontinued, for unspecified reasons. Contact information for the domain refers to an email address located at a different web hosting company in Cupertino, CA. According to the person we asked at *Data Fellows*, Finland, neither the site nor these contact details had anything to do with the 'real' company.

At the same time, www.datafellowes.com appeared on the Internet, hosted by the same Florida-based company as codebreakers.net. As if registering a domain which is an obvious misspelling of an existing and well-known anti-virus software manufacturer were not enough, there have also been reports of misleading email associated with this domain. Several weeks ago, I received an email appearing to be from Mikko Hypponnen, an anti-virus researcher working for *Data Fellows*. The mail requested quite a few viruses. As Mikko is a *CARO* member, such a request seemed unlikely at best, and so I gave it extra scrutiny. Closer inspection showed that the message reply would have gone to datafellowes.com, not DataFellows.com.

Several other prominent anti-virus researchers also received similar requests. Who exactly was the mystery mail sender? I do not know. Clearly, had I complied with the request, I would have been sending viruses to someone who was not the real Hypponnen. Again, at the time of writing, the www.datafellowes.com site does not appear to be operational. Neither the company which hosted the site, nor *Data Fellows*, was at liberty to discuss details of the incident due to police involvement. Another example involves VGREP, a popular utility produced by *Sophos* and available at www.virusbtn.com. It provides a quick and easy reference for virus names. Imagine my surprise when I spotted 'Vgrep Anti-Virus Inc.' using vgrep@hotmail.com as an email address. Is this related to the Codebreakers and Datafellowes events? Only time will tell.

It seems that the 'bad guys' are attempting to confuse the issue by a troublesome (but not particularly creative) manipulation of procedure. The question remains – is this 'new'? Setting up BBSs which appeared to be 'legitimate research facilities' was a favourite ploy of some early virus writers [28]. The mid-1990s saw the same sorts of attacks using email when virus writers pretended to be everyone from Dark Avenger to well-known anti-virus researcher Frans Veldman, and everything in-between. Confusion is the name of the game. So, while the Internet provides some novel twists to the chase, the overall ploy is unchanged; the 'robbers' are pretending to be the 'cops'.

The operational characteristics and demographics of virus writers have undergone some subtle shifts, which began several years ago [29]. While geographic hot zones do pop up from time to time, the advent of cheap connectivity for many has resulted in more global alliances not centred around a particular BBS; the 'Net, as it were, in action. Once relatively regionalized [30], groups that do exist seem more geographically diverse; The Codebreakers group reportedly has seven members from Europe (Austria and Germany), three from the US and one from Australia. Where there are some strongly regionalized groups [31], these regionalizations seem based on language limitations.

Some virus writers are more willing to discuss issues now. This may be partly due to the general acceptability of 'counter-culture' ideas on the Internet *per se*, or the supposedly increased anonymity afforded by various forms of Internet communication [32]. There *is* more willingness to debate publicly – at least on the part of some virus writers and those who favour public availability of viruses. Next month, we examine motivations and justifications. Understanding why can provide some insights which will help us take action that can slow down the viral glut.

13. Richardson, K. 1994. Computer Viruses – The Breadth of the Problem. *Sophos Technical Report.*

14. The WildList. 1993. November. www.wildlist.org.

15. Gordon, S. 1994. Technologically Enabled Crime: Shifting Paradigms for the Year 2000. *Computers & Security.* Elsevier Science Publications .

16. Gordon, S. 1994. The Generic Virus Writer. *From the Proceedings of The 4th International Virus Bulletin Conference.* Jersey. Channel Islands.

17. Gordon, S. 1996. The Generic Virus Writer II. *From the Proceedings of The 6th International Virus Bulletin Conference*, Brighton, UK.

18. The WildList. 1999. February. www.wildlist.org.

19. Private Communication, 1995. Used with permission.

20. Private Communication, 1999. Used with permission.

21. Private Communication, 1999. Used with permission.

22. Dibbell, J. 1995. Viruses are Good For You. *WIRED.*

23. Myers, S. 1995. Computer Viruses: The Infection Spreads to Japan. *Computing Japan*.

24. Cohen, F. 1991. Trends in Computer Virus Research. ASP Press.

25. Stojakovic-Celustka, S. 1994. The Legend – Fred Cohen. *Alive. Volume 1, Issue 1.*

26. Peterson, P. 1999. Used with permission.

27. Internic. 1999. WHOIS. Registrant: DataFellows Ltd. (DATAFELLOWES-DOM)

28. Gordon, S. 1993. Virus Exchange BBS: A Legal Crime? *From the Proceedings of The Use and Abuse of Computer Networks: Ethical, Legal and Technological Aspects.* American Association for the Advancement of Science. National Conference of Lawyers and Scientists.

29. In (17).

30. In (28).

31. Gordon, S. 1999. Viruses in the Information Age. A presentation pre-print for The BlackHat Briefings. National Computer Security Center and Secure Computing. Las Vegas, Nevada.

32. Ahern, T. & Durrington, V. Effects of anonymity and group saliency on participation and interaction in a computer-mediated small-group discussion. *Journal of Research on Computing in Education*. Vol. 28, Issue 2.