FEATURE 2

Viruses on the Internet

Sarah Gordon

Author's note: This article explores attitudes to virus distribution facilitated by the Internet. Our increased reliance on the Internet for communication, and the retrieval of information from untrusted systems, can be expected to bring more cases of point-and-click giving users new viruses of many types, including those which take advantage of existing security holes in insecure applications.

The World Wide Web is a wonderful place. In June 1996, I decided to explore it to research this article; specifically to gauge the success of the 1995 'let's get rid of Internet virus sites!' campaign which had been sponsored by the *NCSA* and some anti-virus product developers.

My first search brought me fifty thousand matches. After regaining my composure, I realised many of these must be related to other types of virus. Fortunately, a narrowed search proved I was right. Surely we are winning the battle to encourage responsible behaviour on the Internet!

Or are we? With my refined search, I found 2000 matches to computer and virus (or virii, as virus distributors like to call them). The first site I came across was one that offered the classic 'computer virus joke' file:

```
Arnold Schwarzenegger Virus. Terminates, stays
resident. It'll be back.
Freudian Virus. Computer becomes obsessed with
marrying its own motherboard.
Star Trek Virus. Invades your system in places
where no virus has gone before.
```

What was to come was not so amusing. As I pointed and clicked, I found other 'virii' sites. Some pages were not fully operational, but many more were. Some were old pages I had run across months ago which had been taken down during the brief flurry of 'stop the virus sites'.

At that time, I predicted that the sites would come back, or reappear under other names. I hate to say it, but… *I told you so*. The sites have returned, and the methods we have tried to use to stop them have not worked.

Anatomy Lessons

What exactly can be found by following the downward spiral of the World Wide Web? More than some people would have you believe, to be sure.

I began with a site reference on university coursework. This was of particular interest to me, as I had just returned from the IFIP Conference in Samos where I heard a Swedish professor explain that making viruses was part of his curriculum. When I mentioned that two of the virus writers with whom I had spoken were students at his university, he told me he had heard about them, but he did not seem to think it noteworthy.

The following, a description of coursework from an American university, illustrates the casual attitude toward viruses which seems to prevail at many universities.

> *Computer Virus analysis*
>
> *Take a computer virus and analyse it thoroughly. You will have to isolate the virus code and disassemble it … Once you have it disassembled, you now have a program listing which IS the virus. Go through it, one assembly language statement at a time, and figure out what it does and how it works. It is best to do this on a fairly simple virus … I have a copy of the Natas virus if you want to try that one.*

This was the most responsible entry. While some would say using viruses as part of a learning exercise is 'good experience', others say it is 'poor science'. Deciding whether or not Natas is a 'fairly simple virus' remains a task for the reader. From this site, it was all downhill.

Under the banner 'Free Speech On-line Blue Ribbon Campaign', I was welcomed to 'The Virus Page: VIRUS PROGRAMMING and VIRII'. I was invited to join the Blue Ribbon Anti-Censorship Campaign and given access to all sorts of virus tutorials. There was information on disinfecting infected files, TSR, COM infections, non-overwriting COM infections, infection on closing, EXE infections, directory stealth, memory stealth, and a memorable tutorial, 'The Dangers of Thunderbyte'.

Polymorphic viruses were part of the plan as well, with 'Implementation, Detection, and Prevention'. Other instructions included infection of *Windows* executables, calling *Windows* API in assembly language from VLAD, heuristics, ANTI-AV Tricks (Tunnelling), Inbar Raz's Guide to Anti-Debugging Techniques and (from our own side), 'Anticipated trends in Virus Writing – Some ideas from the AV folks'.

There were also assembly language links, programming tools including A86 assembler v4.02, A86 debugger, a 32-bit *Windows* disassembler, *ViruScan for Windows 3.x*, *TBAV for Windows 3.x*, and, to my utter horror, *F-PROT*.

Does anyone actually get anti-virus software from sites which offer the latest and greatest virus source and executables right alongside anti-virus software? You would hope not, but I learned that some people do!

Some company employees of major firms told me that they 'trust' the virus sites because there is so much 'information' there. These are the people who are responsible, in some cases, for securing your systems. There were links to other

pages, too numerous to mention, most of them virus-related. There was even a link to Alan Solomon's hacking and virus laws page.

A trip to one of the links showed the same viewpoint, or possibly pseudo-viewpoint, one I saw repeated many times:

> Disclaimer: These files are for research and educational purposes only. I take no responsibility for any misuse of these programs which can result in ARREST OR DAMAGE TO YOUR COMPUTER. Please keep in mind that viruses are harmful and may destroy your computer: if you destroy other people's computers, you will be held responsible. Download at your own risk!

That site had files. The files were viruses, nicely catalogued. It also had generators, constructors and source code files. The warnings are nice. But who's kidding whom? Virus distribution in this manner is nothing less than irresponsible.

When I asked some of the people involved, the responses were generally that if the person who downloaded the viruses was incompetent to manage them, it would be that person's problem; that it is always the user's own choice to download. Virus sites are well and truly on the Internet, and they are here to stay.

"there are real problems in becoming the censor of user communications, both from a legal and an ethical standpoint"

A Problem with the American Legal System…

…is the outcry of some anti-virus researchers. Indeed, this is a possibility worth considering. People may take this position because some American-based public Internet Service Providers (ISPs) and on-line services hide behind the whimper 'it's not illegal'. Does this demonstrate a terrible ethnocentricity on the part of these providers? After all, the Internet is global.

An examination of one of these same providers' publicly available FTP logs shows computer viruses being siphoned to the UK just last week. Japan is another popular location on the receiving end of viruses from American ISP clients.

However, is action on the part of the service provider part of the solution? Is 'it is not illegal' adhering to the outdated paradigm 'If it's not illegal it must be OK'? Some would argue that it is, and that ISPs and on-line services should take more responsibility for the actions of their users and for the welfare of the computing public. Others recognize that there is, in fact, no viable solution.

There are real problems in becoming the censor of user communications, both from a legal and an ethical standpoint. These problems place ISPs, on-line providers and bulletin board operators in situations which may be impossible to resolve.

In 1994, representatives of several unnamed commercial ISPs and on-line services were questioned by various people regarding their policies on allowing viruses to be distributed or made available from their servers[1]. Reactions varied from 'it's legal' and 'we cannot become censors of our users', to 'we will not knowingly allow such things to be made available on our site'. It is interesting to note, however, that all the sites queried still have viruses and other 'questionable' material available from time to time.

Of course, service providers' views are based not only on the laws, but on the feelings of their customers and potential customers. 'Is it OK to make viruses available for public consumption, via the Internet?' – I have asked this question countless times, in public forums, on BBSs, at Conferences. Opinions seem to fall into two categories:

- it's nobody's business what anyone else does as long as it doesn't hurt anyone directly
- you can't do that because I don't like it

Defining 'directly' seems to vary from culture to culture; that discussion is best left for another publication.

I thought it might be interesting to query individuals in the IT field and ask the same question. The responses reflect what I have heard from the computing community in general. Only two responses stated that virus distribution should be illegal. The first said:

> *Maybe virus distribution should be illegal, but policing it will always be a problem. The Internet offers a new perspective on the 'Global Village' concept. These are issues yet to be resolved – who knows if they ever will be? A person who makes viruses available should share the responsibility, but the key word is 'should'. That opens a new arena of conflict: we must learn to be wary and learn how to avoid these problems. The ideal would be nice; people providing only helpful, useful items on the Internet. There should probably be some sort of punishment for malicious intent, but I hesitate to invite excessive government regulation to the Internet.*

A similar response:

> *I don't believe in censorship in many cases. I do believe in restricting the public market. If a person wants to write a virus, he should have the freedom to do so. If he wants to send it to his friends, still his business. If he would like to place it on his own FTP site and distribute it, as long as it is clearly marked as virus, then he should be allowed. Any distribution of the virus into the public should be illegal.*
>
> *It is the responsibility of the individual if he is on the Internet to watch out for harmful code. It should be assumed that files being downloaded may be infected.*

Then, there were those who took a more casual attitude:

> *Since I've never had a virus, and don't work on systems that most viruses infect, I'm just not that familiar with, or interested in, viruses. I find that most*

people who are very interested in viruses are those who got one and were determined to 'out' their intruder, to figure out everything they could about the creator or the processes involved.

I have a Macintosh at home. I am not very concerned about getting a virus at home, though I use Internet services daily (I don't use BBSs at all though). I run Disinfectant occasionally, but more out of a sense of duty, than fear. I don't have Word, or any other (known) macro infecting program. I think as these things go, based on my user habits and stuff, I have a low propensity for actually getting a virus. But I may be wrong.

These views seem typical of most Americans I have queried, but, despite the claim you will often hear that the USA distributes all the viruses (it used to be Bulgaria – I suspect neither deserved the amount of 'credit' bestowed upon it), I found virus distribution on the Internet to be culturally diverse. The US was there, but along with Canada, Austria, Portugal, Germany, Sweden, Norway and the UK. Viruses were available via FTP, WWW, or in casual trading centres such as IRC: they seem to have become the POGS of the Information Age.

New acquisitions are made with relative anonymity and virtually no interference. The logs of a real server, recorded 1–18 June 1996, showed various viruses, including Monkey and variants of Stealth, being retrieved by willing users. It is possible, of course, to identify users who obtain viruses via anonymous FTP or WWW should one desire to do so.

IRC BOTS dispensing viruses seem to have, at least for now, disappeared. I was pleased to hear this, but then reminded by a cynical friend that there was no need for VirusBOTS. After all, why spend the time getting limited information from a BOT when you can get all the viruses, source, and tools you want directly from the World Wide Web?

We still have the question 'How can we prevent this sort of irresponsible behaviour?' The problem seems to be that we don't really know whom we should be asking to stop it. Although, for the most part, virus download areas eventually fall into disrepair and disappear, there is a continual influx of 'young blood', keeping the number of sites in some sort of steady state.

The ISPs, companies, or universities which host these sites will not, for the most part, stop allowing such activities. For every site which acts responsibly, and does prevent such behaviour, there is a person determined to exercise his rights, oblivious to the concept of duty and responsibility…

As the college has taken this page away from me, I am searching for a new home for this information. Please, if you have any suggestions, email and tell me, I'd like to make the page available as soon as humanly possible. I'm sorry about this, but don't let it discourage your learning, because I won't let it discourage mine.

-The Demon X(a/n)^th

Supply and Demand

Who are the people commonly said to share in the Vx Internet pie? The four groups in contention for this dubious honour appear to be the virus writers and distributors themselves; the average user; the employee (who may be in charge of tech support or product evaluation); and finally, the anti-virus product developer.

The group with the most potential interest in VxWWW sites are the virus writers and distributors themselves[2]. Much of the information stored on such sites is of reasonably high quality, and can provide interesting pointers (in the form of source code or text files) to new techniques. For those who trade viruses, the attraction of such sites is obvious.

How much impact these sites have among virus writers is questionable; however, in the same way that a frisson of fear went through the industry when the VxBBSs began to appear (though the boards had little discernible effect), it is entirely possible that the impact of viruses on the WWW will not lead to vast numbers of new viruses or variants. Only time will tell.

"making viruses available via the Internet may be the 'right' of some people in some countries, but it is not responsible behaviour"

The second group, which encompasses the average user, is in the unenviable position of having the intrigue of viruses thrown at him by the media, the scare put into him by some companies, and the WWW at his disposal to get 'information' which he may think will help him protect himself.

What he does not realise is that this point-and-click could cost him his data: infected documents and Trojanised information abound on the Internet. The biggest risk which is posed to the 'average' user by these boards is that of accidental infection.

The third group with an interest in VxWWW sites comprises those interested in obtaining viruses for product testing. Although some anti-virus companies have gone so far as to recommend this, such actions are demonstrably wrong. After all, without investing a significant amount of time and expertise, it is next to impossible to verify a virus collection obtained from a third party, or to remove all Trojans, joke programs, first generation samples, simulated viruses and corrupted files.

Tests carried out on a virus collection which is not clean (i.e. does not contain real viruses) are meaningless at best, and can be completely misleading[3]. Thus, these sites are of little use as a source of scanner fodder; the problems outstrip any possible benefits.

The final group, the anti-virus product developers, are presented with a unique situation. Ever since the beginning of 'public' virus distribution, the mainstream anti-virus industry has scorned those who trawl the boards for the latest viruses. This was done initially because many VxBBSs required a user to upload new viruses to gain connect time, and also to prevent the legitimization of particular boards. However, the issues are no longer as clear.

At the recent *NCSA IVPC Conference* in Washington, one anti-virus company spokesperson publicly admitted obtaining viruses from Vx sites. I am totally against irresponsible virus distribution and joined with the majority of vendor representatives who chastised the errant company.

However, we do need to keep up with virus authors: accessing what they make available to the general public, to our customers. Knowing that people are in fact accessing and experimenting with these viruses may force a change of heart among the anti-virus community.

I believe much of the anti-virus community's reaction to the admission by the unnamed company was overreaction, based on our instinctive distaste for Vx sites in general. It is one thing to say you do not condone them while sneaking around giving or receiving viruses; unfortunately, some vendors are said to have been involved in this.

It is another matter altogether to admit that, due to the proliferation of these places, we must keep up with current trends. The only way to do that, some say, is to see what is there; to access and examine the viruses.

Unlike the VxBBSs of old, the viruses are there, free for all, only a point-and-click away… what are we supposed to do? Most anti-virus researchers do not obtain viruses from these places, claiming the mixed messages this would send outweigh the benefit of ethical behaviour related to viruses on the Internet. However, the issue is much less clear-cut than you might believe.

Clearly, the Internet is a fabulous place to obtain viruses, no matter who you are or what your intentions. Granted, you shouldn't use them to test anti-virus software. Such tests have been shown many times over to be flawed, and in some cases dangerous to the health of your company. You should not spread them to the unwilling and unknowing – even most virus writers acknowledge this. There is nothing a user can 'learn' from looking at viruses which cannot be learned from non-replicating programs.

Unless you are a product vendor or virus writer, the benefit to you from such sites is practically nil – and even if you are a vendor, the benefit is limited. The risks these sites provide to computer users in general, however, remain high. Owners and maintainers of such sites have no control over how the materials they make available are used. While this is the case with most FTPd or WWW materials, it is particularly undesirable in the case of viruses, as they are uncontrollable once released.

This leaves us with the question, again: 'What is the purpose of allowing such irresponsible behaviour?'. Maybe you believe it is an exercise in free speech, or that it is a 'right'. Making viruses available via the Internet may be the 'right' of some people in some countries, but it is not responsible behaviour. It is also, unfortunately, not showing any signs of slowing down.

Closing Thoughts

Finding a suitable conclusion to this article has been difficult, because I don't think that we are even close to finding answers. We don't know whom we should ask such simple questions as 'Why do we allow this kind of irresponsible behaviour on the Internet?'.

While it is a cliché to say that the Internet causes us to re-evaluate what we mean by censorship and freedom of speech, there is little doubt that the rapid development of the WWW has outstripped our ability as a society to control its contents.

Yes, there are viruses on the Internet, accessible via the World Wide Web, FTP, IRC, email, Usenet and other ways not discussed in this article – but we must keep our perspective. There are also infinitely more threatening problems, like child pornography, which I was unfortunate enough to encounter during my research for this article. The issues to which the Internet gives birth are much bigger than simply computer security and viruses. They envelop our communications with the fabric of cultural diversity, and force us to change the way we, in our own hometowns, think, live and do business.

There is no easy way to make us all think in the same way and magically solve the problem of irresponsible action on the Internet, be it child pornography, church-burning sound files, or computer viruses. We who work to fight computer viruses can only try to educate the public to protect itself from those who put the responsibility on the 'other guy'.

It is possible that, someday, those who view it as incumbent upon the 'other guy' to be technically competent, responsible, and ethical will realise that individual responsibility begins with not distributing or writing computer viruses in the first place.

Footnotes:

[1] *Virus-L Digest*, Fridrik Skulason. August 1994.

[2] 'Technologically Enabled Crime: Shifting Paradigms for the Year 2000.' Sarah Gordon. *Computers and Security*. November 1995.

[3] 'Analysis and Maintenance of a Clean Virus Library.' Vesselin Bontchev. *Virus Bulletin Conference Proceedings*. September 1993.

The views expressed in this article are those of the author, Sarah Gordon, a researcher at *Command Software*. Readers wishing more information on the subject may contact her via email at: sgordon@low-level.format.com.