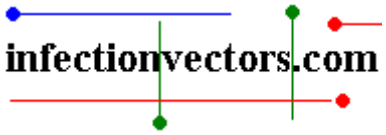

Poison Ivy Farmers: Virus Collections
infectionvectors.com
May 2005

Overview

Anyone who has worked in virus research for any length of time has likely been approached for a sample or two (maybe an entire catalog). People trying hard will say they are for "research," and undoubtedly that is true, although the nature of such research may not fit with one's sense of ethics when it comes to distributing such code. Virus collections have a certain mystique to them, amateur collectors are drawn to them the same way a certain subset of the population likes having dangerous exotic pets.

Distribution List

There are many legitimate needs for actually distributing viruses; obviously anti-virus companies rely upon sharing samples to ensure that they are on top of the latest threats. In addition, reverse engineering tool development requires that researchers be apprised of the compression and packing tactics used by virus writers. The allure of the amateur collection, however, is another beast entirely. The risks of publishing collections have been documented and fought by security professionals for years.

One interview with a noted collector/commentator, Cicatrix, was posted to a famous virus-collection site:

```
[netlux] You are a very big (if not the biggest) virus collector. Why
did you choosed to be a virus collector in the first place?

[Cicatrix] I certainly don't consider myself the biggest virus
collector. Guys like Falcon and Poltergeist (WCIVR) and Omega (Arrested
Development) are in a league of their own. And of course the biggest
virus collectors are the AV software producers.

Initially it started out as something not everyone did or have.
Computer viruses had a certain air of magic about them. As I found out
later this was mostly media induced hype. Later on it continued like
most hobbies I guess, the more you have the more you want. It was
intriguing what some smart people could do to a computer with just a
couple of bytes. It was a challenge to get deeper and deeper into the
scene, with one virus I got onto a BBS with 200 viruses. Those 200
viruses got me into BBS's with 1000 viruses, etc. etc.[1]
```

The collector has been around as long as there has been interest in the computer virus world. Sara Gordon, who has likely completed the most thorough research to date on the

virus writing culture, cataloged the group very early on, through a questionnaire printed in the Virus-L newsletter.[2] In the October 12, 1993 edition, she writes:

```
These questions are being asked to help document how different people
perceive various aspects of the virus problem. Any and all responses
will be appreciated. It is not necessary to include any identifying
information, but you can if you wish. Affiliation/Position would be
appreciated, such as Virus Writer, Virus Exchange BBS Sysop, Virus
Collector, Professor of Law, Student of Psychology, etc.
```

This is an interesting perspective, as she notes that the questions will consider the "problem" with computer viruses, establishing the ethical or even legal (as Law professors are included) trouble with distributing virus code. It is also interesting to see the title of "Virus Collector" as it indicates a distinction that is probably not as respected today. Given the plethora of sites where one can obtain a virus collection instantly these days, such a set of programs is less impressive to assemble. Furthermore, as overall understanding of computer viruses (and virus writers, thanks to much of the work Sara Gordon completed) is shrouded in less secrecy than just a decade ago, taking away much of the "magic" afforded to the trade.

Freedom of Information?

Certainly, the free trade of information is used to defend posting collections and sharing files amongst enthusiasts. The ethical considerations are often eliminated when an ISP acts on behalf of the Internet community to remove malicious content, as has been the case many times over. However, the central tenet of the opposition to posting live viruses, code, debugs, etc. is still missing international legal enforcement. Paul Ferguson posted the following in his, "Establishing Ethics in the Computer Virus Arena" in September of 1992:

```
To those who posted them, it may have been an innocent act on their
part to make the information available to others in a public forum. For
whatever reason, posting of code that has the ability to replicate (or
even destroy) on an unsuspecting user's system is, in my opinion,
inherently wrong.[3]
```

This sentiment is still strong in the antivirus community. In May of 2000, a proposed class on cyber ethics targeted filling the gap between perception and reality when it comes to computer crime laws.[4] The overriding belief among those that fight computer viruses appears to be that there is no responsible way to publicly distribute or create virus code. In 2003, the announcement that a college in Canada would offer a class on how to write a virus sparked controversy and outrage from the security community.[5]

Pet Scorpion

Much like the arguments about dangerous pets, there are not clear, far-reaching laws concerning the nature of owning/posting viral code. The misunderstood nature of viruses by the general public (and probably many collectors) makes them valuable to those

tempted to organize the intangible assets of malicious code samples. The same type of ever-present threat of a pet tiger exists when leaving the collection connected to the Internet – much less when the collection is posted to a public site. The danger, as mentioned, however, is exactly what drives the collector; so additional pleas from the community are unlikely to sway anyone.

On the more humorous side of virus collections, ThinkGeek published the "Virus Starter Collection" as a gag item. The picture crafted for the "ad" shows a stylish custom box with small horns that contains classic virus code for the new collector. This "pet virus" description has been passed around in various forms since being posted in the online store.[6]

References

1. Netlux Interview with Cicatrix
http://vx.netlux.org/lib/iv034.html

2. Virus-L Digest Printed in SecurityDigest, 12 October 1993.
http://securitydigest.org/virus/mirror/www.phreak.org-virus_l/1993/vlnl06.131

3. "Establishing Ethics In The Computer Virus Arena" Paul W. Ferguson, Jr., September 1992.
http://www.textfiles.com/virus/virethic.txt

4. "Should cyber ethics be taught in school?" Daniel Keegan, IDG.net (civic.com). 9 May 2000. http://archives.cnn.com/2000/TECH/computing/05/09/cyber.ethic.conference.idg/

5. "University defends virus-writing class" George Hulme, InformationWeek29 May 2003.
http://www.informationweek.com/story/showArticle.jhtml?articleID=10100515

"Class on virus writing draws industry ire" Andrew Brandt, 30 May 2003 PCWorld.com.
http://www.pcworld.com/news/article/0,aid,110938,00.asp

6. ThinkGeek "Virus Starter Collection"
http://www.thinkgeek.com/stuff/41/virus.shtml