

The Viral Mind: Understanding the Motives of Malicious Coders

D.D. Shelby 2002-05-21

The Viral Mind: Understanding the Motives of Malicious Coders

by *D. D. Shelby*

last updated May 21, 2002

A Personal Perspective

Over the years I have seen many people offer opinions on why virus writers do what they do. While I accept that many of these people have indeed spoken to a small number of malware authors, it has become all too apparent that much of their text has been based on opinion and not fact. In this article, I will draw upon my own experiences as a virus writer and as a member of the virus (and anti-virus) community to explore some of the reasons that people would devote their time to developing viruses.

As I mentioned, I have some experience as a virus writer, so before I start discussing the motivation of other virus writers, I should explain my own. My reasons are quite simple: boredom and a wish to see what can and cannot be done to and with an operating system. Now that operating system is on a personal computer at present but things are changing rapidly, soon many household appliances will have the ability to connect to the Internet and run executable code. This has the potential to offer new vectors of infection and new degrees of damage.

A Brief History of Viruses

Boredom and curiosity are pretty simple motivations, but there is more at work than that. Since the early days of viral coding, I believe the reasons people involve themselves in such potentially dangerous hobbies has changed. As was my case, the early virus writers were motivated by the same things that drove early hackers: curiosity and a fascination with the technology. A case in point would be the code explorer who was amazed that they could get program A to copy itself to program B and even more so by the fact they could make program B still work normally. These guys were no more than just interested users who had a little time to spare and an excellent knowledge of how the operating system worked. At that time the main OS was DOS, a simple command line system that had some serious limitations but was easily exploited by the inquisitive programmer.

As time passed, the various versions of Windows arrived starting with DOS front-end versions that were no more than a simple GUI added to DOS. They looked different and, compared to the systems of the earlier years, gave the user the warm fuzzy feeling of interaction. Not to be outdone, the virus coders wished to ensure that their code worked with these early GUIs and continued to explore possibilities including how to damage such systems.

The viruses became more graphical in their displays and, in some cases, much more damaging in their effects. I believe that the graphical aspect allowed the coder to incorporate part of his or her persona in their work, such as the words of William Blake the author being added to [Maltese Amoeba](#). Admittedly there were some interesting things added to the viruses but, by and large, the additions became more sinister in their nature. Take for example the [Pathogen series of viruses](#) that when running would display "Smoke me a kipper I'll be back for breakfast, unfortunately some of your data won't". This message was an attempt on the part of the author to instill fear or apprehension in the user so that they would likely not forget their run in with that piece of code.

Virus writing slowly but surely became a game of names. Many virus authors took on unusual and ominous sounding names that were intended, I believe, to make the air of mystery all that much more impenetrable. It also may have indicated that the stakes of the virus-writing game were much higher, as the authors chose to further obfuscate their real life details so to avoid the chance of capture for any crime they may have committed. The drawback to the security of the general computer user was that this malicious code had an air of mystery that further added to the mystique. Writing viruses rapidly became interesting to many people who then proceeded to try and become one of these evil underground dwellers who could destroy a computer the other side of the world with no more than a few keystrokes. The truth behind it – one that was rarely noticed - was that a computer virus is a program - nothing more, nothing less. Regardless of this mundane reality, to the new breed of virus coder they represented power: unlimited and often destructive POWER.

As Windows evolved and, some say, increased the havoc that viruses could wreak, virus creators learned how to send mail, encrypt files, launch attacks against Web servers, update their code from Web pages or newsgroups, and a number of other nefarious things. As the office packages became easier to use, malicious coders also learned that many of these functions were available in simple Macro code, so the movement shifted towards the easier methods of writing a virus. At the same time, many of the older virus coders stuck with

assembler in its newer 32-bit guise as it took intelligence and a fundamental understanding of the operating system to write viruses in such languages. These purists would often berate newcomers for their quick-fix attempts at virus coding with such "lame" things as simple macro code.

To the end user, or infectee, the method by which the malicious code had been written with was irrelevant; they were being infected by so many different things that any differentiation became pointless. The anti-virus companies released press stories about the thousands of new viruses and so added to the air of mystery and taboo and indeed to the attraction of becoming a virus writer for the young kid with too much time on their hands.

In the late 90's it all got serious very quickly, a simple piece of macro code known as Melissa, written by a bored thirty-something, went off round the world like wildfire, infecting millions of computer systems and bringing the attention of federal authorities to the virus scene. Realizing the potential for prison sentences, some virus writers took flight, some ignored the new developments, and indeed some positively basked in the increased danger of it all. The stakes had increased almost overnight.

At the same time, there emerged a new group of virus coder: the script kiddies, as they became known. They saw the media attention devoted to the Melissa virus and realized it would be a way for them to gain notoriety. Sadly they confused fame with infamy, and set about modifying much of the available macro code in an effort to become one of the great virus coders. They had very little if any skills to speak of but with fifteen minutes of simple work they could send their code off round the world in a matter of hours. Sure, they got the attention they so desperately craved but they also started getting visits from their federal authorities.

A number of the more *time served* virus coders and members of the virus scene also realized that this was great media material and started doing interviews with both the press and TV stations and another group the "media whore" was soon created. (Following the publication of this article, I expect to be included in this group by a number of my peers.) Some of this group had little thought for what they said to the press and TV and didn't take into account that their every word was likely to be monitored by interested parties who didn't see viruses as funny or any kind of *game*.

The Motives of Virus Writers

So, now that we have discussed the historical context of virus writing, where does that leave us in our attempts to understand why virus writers do what they do? From my experience I believe that there are a number of reasons people do this. These reasons differ with the individuals involved and, as a result, the type of virus developed will differ, as will the degree of proliferation and the site of release of the virus.

Just Having Fun

First and foremost, many coders write viruses simply for fun. This may sound ridiculous considering the amount of damage these pieces of code can do; but to the author, those consequences are something that may happen in a far away place and likely have no real bearing on their actual situation. I think this may be a dissociate problem where having not seen the results of their handiwork they feel no compassion for any problems they may cause. "Hey some geek 5000 miles away just lost all his files, so what I don't know him"

Seeking Fame and Fortune

The second reason for authoring viruses is for the infamy that comes with having a virus or piece of code posted on the [Wildlist](#), a non-profit site that announces which viruses are currently circulating in the wild, or amongst the general population of users. To be able to look at the Wildlist and say to one's self "hey I did that" or "I'm really somebody now" can be a real boost to the ego. This is the attitude typically displayed by the script kiddie: while they commit childish pranks in full knowledge of the damage that they may cause, when they are caught and brought to trial, they hide behind their youth, disingenuously using it as an excuse for their ignorance. This subset of virus writers is the most dangerous, as they will do anything within their powers to make a name for themselves with no regard for people's data or privacy. Worse yet, this type of coder does not even require a particular skill set to achieve this. As a result, just about anybody who wants to do this will be able to.

This group of people would include the dreaded "Kit clicker", a sub-set of script kiddies who use kits to build prefabricated viruses. One well-known example of this group was the use of the [the Kalamar kit](#) to construct the Anna Kournikova worm.

The kit coder has almost no technical ability or understanding and generally will only uses such tools to try and achieve some degree of fame. This group is universally despised by both virus writers and the anti-virus communities alike. While it may be said that some of these people

may be just *experimenting* to see what happens although this is usually in the lower age range (circa 14 to 18 years of age), the use of a *kit* by an adult or anyone with any degree of coding experience is just plain infantile. Kits are considered by VXers to be interesting things to code but have very little use, but beyond that the *Kit Clicker* deserves nothing but contempt.

The third group consists of the fame junkies, people who seek the same sort of affirmation as the preceding group, only on an ongoing rather than a one-time basis. These individuals are not a significant threat in terms of the quality of code they produce. However, the sheer volume of malicious code they turn out represents a real problem to the anti-virus companies. Think about it, if these idiots produce a total of say 20 pieces of code a day between them that means that 20 code analysts will be tied up for the day disassembling the code to add detection to their products databases. Some of this will be driven by market forces in that if one product vendor adds the virus to their database then the others will feel compelled to do the same, so that they would not appear to consumers to be lagging behind the competition.

The fame junkie will typically do as many press interviews with as many sources as will speak with them or print their self-aggrandizing hype in an effort to gain some sort of infamy or adulation from other coders. Typically the code itself is of low standard and rarely presents any significant threat to the end user or even show any proof of concept.

Experienced Coders Pushing the Envelope

The next group includes more dangerous viral coders, individuals who have attained quite extensive experience in programming and are more than able to circumvent the procedures used by the anti-virus industry. When they create their malware, they will often add specialist routines or functions that allow updating or high-level obfuscation to prevent disassembly of the base code. This virus program is generally written more from a point of research than a wish to see harm or infect end users. That having been said, a small number of people from this group will often allow their code to either be spread by other VXers (a VXer is somebody who writes viruses, exchanges viruses, studies viruses, or is generally interested in the development and proliferation of viruses) or will make their accomplishment available on a Web site as a proof of concept without considering what reckless downloaders might use that code for. From a moral point of view they are closely related to the first group in that they do not see first hand the effect of their code, and so are easily able to rationalize their actions as valid research. While they may not inflict the damage themselves, they give others the means by which to inflict damage.

The Disgruntled Loner

The final and by far the most dangerous type of virus coder is the lone madman. These individuals have no respect for law or morality, and care little for the losses or damage they may cause. They usually have significant personal issues. Furthermore, they are often deeply anti-social and are often loners who do not associate with other virus coders in any manner. Their motivation is to cause the most harm or create a virus that will spread the furthest in an effort to "get at" the world they despise so much.

These people are rarely encountered by the mainstream of virus creator, as they have very few social skills and do not mix well with others. Currently there are not too many people in this group (or at least no more so than in mainstream society as a whole). Thankfully, to this point in time, their ability does not match their ambition; however, in the future, if operating systems and software become easier to exploit, the chances of this type of individual having access to dangerous code is increasing rapidly.

Hobbyists

Having stated all of this, many current virus coders see what they do only as a hobby. It may take up some small amount of their time or they may devote many hours per week to their work. Typically, younger virus coders spend more time at their work than the more seasoned or older coder who may well have family commitments or other things they find more interesting or productive.

While it may seem as though this group is the same as the first group, some hobbyists take virus writing very seriously, such as a number of collectors who will spend hours checking log files for a piece of code they are missing or the coder who will check and recheck their routines to ensure that they work on all platforms (Beta testing so to speak). This can be done solely by the coder; however, other people in from the community will often take part in an effort to help out a friend. For hobbyists, the study of viruses is a pastime to take up a few hours in the dark evening (I would include myself in this group), or to discover new ideas or information. This group has no real intent of harming anybody or wasting too much time on the whole thing.

What the Future Holds

As yet there are a number of exploitable platforms and methods of distribution that have not

been used by the virus writing community. This may be due to a lack of information, or it may be a simple moral question. Indeed it may even be self-preservation - a wish not to be imprisoned. This may be the current situation, but I have reason to believe this may well change in the not too distant future as fame attracts more and more younger and less stable people into viral experimentation. The media attention and notoriety that viruses give their author will increase until the point that the governments of the world decide that "enough is enough" and legislate to prevent such action. While this will likely not stop the determined coder, it would almost certainly stop the kid who just wants his "fifteen minutes of fame".

The world of the virus coder is full of myths and legends that have been generated by misinformed persons out for a good headline or to scare the using public into buying software they do not need and will not indeed save their data anyways. The average age of virus writers is increasing as is the base level of programming quality and distribution methodology and in the near future I expect to see many more events such as the Melissa problem as the pool of ignorant users and malicious coders increases. It has become a matter of **when** and not **if**.

[Privacy Statement](#)

Copyright 2006, SecurityFocus