

# Malware Infection Vectors: Past, Present, and Future

Paul Schmehl 2002-08-06

## New Infection Vectors for Malware

by Paul Schmehl

last updated August 6, 2002

---

The vectors that malicious software use to invade systems are constantly evolving: adapting to new technologies, changing to avoid defense mechanisms and adding on to attack new weaknesses. While not an attempt to predict the future, this article will look at what infection vectors have been historically effective, how they've changed over time and what they probably will do in the future.

## A Short History of Viruses

Professor [Fred Cohen](#) is generally credited as being the first to discuss the possibility of viruses when he published his now-famous 1984 paper, "[Computer Viruses - Theory and Experiments](#)". In this paper, Dr. Cohen theorized on what viruses could do, how they could enter systems, and what could be done to prevent them from causing damage. In his introduction and abstract, he states: "Analysis shows that the only systems with potential for protection from a viral attack are systems with limited transitivity and limited sharing, systems with no sharing, and systems without general interpretation of information (Turing capability)." (For more information on Turing capability and the Turing test, please see [http://www.pcwebopaedia.com/TERM/A/Alan\\_Turing.html](http://www.pcwebopaedia.com/TERM/A/Alan_Turing.html).)

Cohen's words could not have been more prescient. Whether he foresaw the peer-to-peer (P2P) sharing networks of today (such as KaZaA, Morpheus, etc.), only Dr. Cohen could say, but there is no doubt that those networks have the potential to spread viruses more readily than any previous vector that has been used.

### From Theory...

The first worm (a program that can move between computers without their users interacting) was discussed in a paper entitled "[Notes on the 'Worm' Programs - Some Early Experience with a Distributed Computation](#)", by John F. Shoch of the Xerox [PARC \(Palo Alto Research Center\)](#), revealed the unsettling fact that sometimes programs can take on a life of their own, completely apart from their creator's intentions.

## ... To Practice

In 1986, two years after Dr. Cohen's groundbreaking paper was published, the first "in the wild" virus was discovered. Its name was "Brain" (or "Pakistani Brain"), which was a boot sector virus, the first of several to gain notoriety. [N.B.: Throughout this article, at least one variant of the viruses marked with an asterisk are still listed on the [WildList](#). Note also that I am often using the popular names for viruses rather than the more correct [CARO names](#).] Initially it could only infect floppy disks (remember them?), but later variants were able to infect hard disks as well.

Still, spreading an infection depended entirely upon physical "transportation". As one person with an infected computer made copies of a file, document or program that someone else wanted and then gave them the infected floppy, the virus would spread to the second machine, and so on. This was a very inefficient way to spread viruses. As a result, for almost twelve years virus infections were almost non-existent in the media and were almost unknown to the general public. They spread mainly on university campuses, where sharing floppies was routine and computers were more prevalent.

Veterans of the virus wars nod their heads knowingly when they hear mention of viruses like "Stealth\_C"\* , "Monkey B"\* , "NYB"\* and "Stoned Empire Monkey"\* , but the average person would have no idea what these cryptic names referred to. (Probably the first "famous" virus is Michelangelo, which became famous because the press, in a pattern that is still repeated today, hyped the virus much beyond its true threat to computers. Even though it was still a virus that required floppy disk exchange to spread, the press latched on to the ominous "D-Day" (March 6th) when the computer's hard disk would be "formatted" by overwriting a part of the disk with random characters.) I remember being called to a student lab one time, to investigate a "persistent" Stealth\_C infection that they just couldn't seem to get rid of. It turned out that the floppy disks that were being used to initialize the hard disks and install the operating systems on all the lab machines were infected. Before we were through, we had cleaned over fifty floppies that had been passed around as the labs were being set up. Fifty infections isn't even a good "seeding" for today's viruses!

## New Methods of "Transportation" Begin to Appear

In 1988, the [Morris Internet Worm](#) was turned loose, bringing servers around the world to their

knees as it consumed processes until the target computer ground to a halt. As a precursor of today's multi-functional malware, the Morris worm holds some valuable lessons. Beneath the mystique of its rapid spread, the worm pointed out the need to maintain secure networks, keep systems patched to current patch levels, allow complete access only to trusted users, and control the types of information that can be shared, all of which Dr. Cohen pointed out six years before the worm's release, and all of which the Morris Worm's successors continue to illustrate.

In 1994 an Australian programmer, Peter Tattam, released a program named [Trumpet Winsock](#) and the Internet revolution was born. (Of course, I would be remiss not to mention Tim Berners-Lee at CERN, who, in 1992, created hypertext and thus invented "the world Web Web" that we know today. Perhaps he and Peter should share the honors of having jointly launched "the revolution".) To be sure, the Internet had existed for quite some time before that (since 1969), but Peter's program brought dial-up connectivity to the masses and launched the phenomenal growth that has increased from 1000 hosts in 1984 (and perhaps 1,000,000+ in 1992) to the estimated 580.78 million that are connected to the Internet today (according to [NUA Internet Surveys On-Line](#)). Suddenly the average citizen could sit down at a computer in their home and compose a message that magically appeared at their friend's house in less than a second. And they could "surf" the Web, visiting sites all over the world without leaving the comfort of their home.

It wouldn't take long for virus writers to exploit the Web as a new vector of infection. First the Word Macro viruses appeared: starting with Cap\*, followed by Concept\*, then Class\*, Groov\*, Ethan\*, and on and on and on. The avalanche had begun. Then Melissa\* arrived on the scene (a virus so famous that it has its very own [domain!](#)), taking advantage of the ubiquity of e-mail to speed its infection. Suddenly viruses were international news. The days of passing infection from machine to machine by hand were over, and the days of automated, distributed infection had begun.

### **E-mail Becomes the "Vehicle of Choice"**

From Word viruses, the virus writers branched out to Excel (Laroux\*, Tristate\*, etc.), and it wasn't long before their attention turned to e-mail propagation using scripting (Visual Basic, JavaScript, etc.) While commercial minds were thinking of ways to use e-mail to advertise products, distribute colorful newsletters, and generally make the world a better place, virus writers saw the dark side of all these new enhancements and aspired to take advantage of them. HTML e-mail held possibilities that plain text never could. Now a virus could be spread

through an e-mail message without even having to use an attachment. This method has proven so effective that today the Kak\* worm, which was first discovered in the wild in late 1999, is still spreading to unsuspecting users three years later.

Soon the Loveletter\* virus appeared on the scene, proving once again that people could be fooled very easily by the right kind of "social engineering" (a term used to denote the use of deceit and trickery to persuade people to take an action that they wouldn't normally take). Then "Kournikova"\* followed. It wasn't long before the year 2000 was becoming known for its virus outbreaks rather than its computer clock problems.

## **Viruses Begin to "Branch Out"**

In addition to e-mail, virus writers began to exploit weaknesses in software - both programs and operating systems - to spread their wares. The Hybris\* virus appeared and proved that it was possible to use multiple vectors (such as Web, e-mail and newsgroups) to spread a single virus and that it was possible to distribute a virus using plug-ins, much like many popular Internet programs are distributed.

In 2002, Code Red\* and Nimda\* appeared on the scene and proved that machines could be used to spread viruses through Web pages, obscure Internet protocols (tftp) and e-mail, all without human intervention or assistance. (Further proving that Cohen was right. Those who didn't patch their machines were overwhelmed. Those that did patch their machines and those who chose operating systems and applications that weren't vulnerable to begin with were unaffected by the storms.) By the end of 2001, many system admins were reeling, exhausted from the constant pummeling of new virus releases, looking for any solution they could put their hands on.

## **So Where Are We Today?**

This brief and very incomplete history illustrates the main point of Fred Cohen's thesis: sharing information between computers is fraught with peril. Therefore we have to find ways to protect the sharing mechanisms in a way that shields us from malicious code (as much as is possible.)

In the brief time between the publishing of Dr. Cohen's article and today, we have seen viruses move from physical exchange to automated exchange, from floppy disks to every possible means of sharing information, and from "horse and buggy" transmission to light speed

propagation. As I write this article it is possible to get infected by in the wild viruses through e-mail, the Web, P2P networks, newsgroups, IRC, ICQ, IM (Instant Messenger), PDAs, wireless devices and telecommunications equipment. In fact, I'm finding it hard to think of a means of information sharing through which you **cannot** get infected today.

## And The Future?

By now it should be obvious that predicting the future of infection vectors is child's play. Wherever there is a method or means of sharing information digitally, there will be viruses. When engineers speak breathlessly of the next generation of cell phones - complete with downloadable Web pages updating sports scores and world news, and keeping users apprised of the movement in their stocks - somewhere there is a virus writer planning on using that medium to transport his or her malicious creation. One can only hope that the designers of the new appliances are building in enough security features to at least make viral infection a challenge. Sadly, if the past is any indication, product developers will continue to scoff at the idea that viruses will be a real threat and opt for "usability" over security.

Predicting how viruses will change over time is a little more difficult. Peering into the future with the knowledge of the past tells us that malware will continue to build on previous "successes". Whatever works in one creation will be incorporated in the next one, along with the new ideas about how to get around newly developed defenses. When the Outlook and Outlook Express address books became more difficult to exploit, viruses simply adapted. They began to mine the hard drive, particularly the Web browser cache, for e-mail addresses to use. When anti-virus professionals worked diligently to shut down Websites that hosted viruses, viruses began using locations that couldn't be shut down. When new weaknesses in programs were announced, virus writers added code to take advantage of those weaknesses.

### **Blended Threats, Second Wave Viruses, and Multi-Stage Viruses**

Some experts have coined the term "blended threats" to identify the threats of the future. This refers to the technique of combining multiple transport methods with multiple infection vectors. The dividing line between malware and network intrusions will blur to the point that they will essentially become one and the same. I believe that one trend that will become much more prevalent is "second wave" attacks. Once a virus has been successful at spreading and infecting, other programs will be written to take advantage of the things the first virus has left behind. Code Red and Nimda left behind renamed copies of the Windows command interpreter

sitting in Web-accessible directories that could be exploited through directory traversal weaknesses. Those command interpreters, for the most part, have not been exploited by other viruses. That will change.

We will probably see a "multi-stage" virus released within the next year. It will begin with an initial attack (perhaps requiring a few variants to "perfect" its techniques like Frethem\* did) and then follow up with a second attack that exploits the initial infection. Perhaps triple or even quadruple attacks will occur, each building on additional weaknesses that have been introduced by the predecessors until the machine is so compromised that it will have to be completely rebuilt in order to assure that it is virus free.

One trend that doesn't appear to be changing is the placement of destructive code in viruses. With notable examples (such as Michelangelo and CIH\*) most viruses don't destroy data. They're more an irritation than anything else. This appears to be the one thing about viruses that has remained relatively constant over time. Whether or not that will continue to be the case remains to be seen.

*Paul Schmehl is a Technical Support Services Manager with over 25 years experience. He is currently employed in IT management in higher education, in enterprise-wide technical support, help desk management and anti-virus protection. Involved in many new technology projects, Web site development and security-related issues. Paul is also a founding member of [AVIEN](#).*

[Privacy Statement](#)

Copyright 2006, SecurityFocus