Chapter XIV

Computer Viruses: Winnowing Fact from Fiction

Stu Westin
University of Rhode Island, USA

It would be difficult to find a veteran end user who is unwilling to share at least one “war story” concerning a computer virus. Viruses are, and undoubtedly will continue to be, a fact of life in the end user computing community. Many tales of bouts with computer viruses contain a good measure of embellishment, and many computer mishaps attributed to viruses are truly due to “pilot error.” Regardless of these facts, computer viruses are a problem worth addressing. This paper considers the past and current status of computer viruses and “defensive computing,” and the degree to which the situation has been clouded by hype, misinformation, and misunderstanding.

While the coining of the term computer virus is attributable to Fred Cohen in conjunction with his 1983 academic research on a DEC VAX platform (Cobb, 1998), the phenomenon and did not become a concern to users of application systems until almost ten years later. In 1987, occurrences first appeared in several universities, and shortly thereafter in corporate settings. In today’s environment, the computer virus threat clearly impacts every computer user in one way or another. The degree of impact is not as clear, however.

The severity of the virus threat is particularly difficult to pin down. One reason is that a major source, if not the major source of literature and information on computer viruses is the vendors of anti virus (AV) software...
products. I do not mean to imply that these vendors knowingly disseminate erroneous information, but let’s face it, they have a vested interest in your perceiving the virus threat as a major one. Their stock prices and revenues are known to rise rapidly in reaction to virus scares (Wired News, 2000). AV vendors also have a vested interest in your perceiving that their products can protect you from a large number of viral threats.

Consider this latter issue. The anti virus vendors often list virus strains with minimal, inconsequential differences as being distinct viruses. In doing so, their product can be touted as protecting against more viruses than would otherwise be the case. An early example of this is the case of the Marijuana virus. When first released, the virus contained the phrase “legalize marijuana” as part of its message (this message is called the virus payload). In a later incarnation of the virus, the payload phrase was changed to “legalize marijuana” (note the Americanized spelling). Most anti virus vendors have listed these two versions as unique viruses, although the detection and removal procedures are identical (Rosenberger & Greenberg, 1996). Related to this is the fact that many single virus strains are known by multiple handles (sometimes dozens). This is often because viruses are “discovered,” named, and reported simultaneously from several different locations. The pseudonym problem is not a trivial one, and virus identification experts, understandably, tend to focus their energies on identification and collection rather than on nomenclature (Wells, 2001). The result of this situation is that it is difficult, if not impossible, to evaluate the true impact and infection rate of any particular virus.

Another possible source of confusion lies in the fact that a potentially harmful virus need not pose any real threat to the end user community. This is because only a small portion of known computer viruses actually exist in the wild – the term used to denote viruses that are doing their evil deeds in the real world of computing applications. An article in Information Security Magazine (Cobb, 1998) noted that there were, at that time, fewer than three hundred viruses in this wild category (for the purpose of comparison, at the time of this current writing there are 214 viruses officially considered to exist in the wild). Compare this to the 16,000 plus viruses that existed in virus research facilities (this virus category is referred to as in the zoo). According to Rosenberger & Greenberg (1996), however, most AV vendors use this latter (zoo) number when reporting the state of the virus situation.
Understanding Web Information Search Behavior: An Exploratory Model
www.igi-global.com/article/understanding-web-information-search-behavior/3774?camid=4v1a