Social Science Computer Review
Volume 25 Number 1
Spring 2007 78-98
© 2007 Sage Publications
10.1177/0894439306292346
http://ssc.sagepub.com
hosted at
http://online.sagepub.com

Viruses, Worms, and Trojan Horses

Serious Crimes, Nuisance, or Both?

Lorine A. Hughes
Gregory J. DeLone
University of Nebraska at Omaha

This study examines the functionality and propagation patterns of computer viruses, worms, and Trojan horses detected during a 12-month period beginning on January 1, 2004. Using data obtained from threat reports prepared by a major vendor of computer security products, the authors find that these unique forms of cybercrime warrant general concern but that their overall threat to corporate, government, and end computer users thus far has been exaggerated. The authors conclude that greater attention must be paid to the role of the computer user in the spread of viruses and other malicious software and to the small handful of chronic offenders who contribute disproportionately to the problem.

Keywords: *computer crime; cybercrime; malware; viruses; worms; Trojan horses*

Advances in computer technology have ushered in the information age. As computers have become increasingly accessible and powerful, our reliance on them has grown immensely (Day, Janus, & Davis, 2005; see also Central Intelligence Agency, 2005). For all that computers offer, however, we may pay a high price. Computer crime expert Donn Parker (1976, pp. 17-21) notes that computers can be related to criminal behavior in four different ways. In addition to being the "object of the [physical] attack" or used to produce information that is intended to "intimidate, deceive, or defraud victims" and thereby poses some sort of "symbolic" threat, computers sometimes are used as an "instrument" to assist in the commission of offenses that previously could be perpetrated only with direct access to the victim or victim's property. Computers also may play a role in "creating a unique environment in which unauthorized activities can occur, or where the computer creates unique forms of assets subject to abusive acts." Although the offenses that fall into this last category often bear a close resemblance to traditional forms of crime (e.g., theft, larceny, fraud, embezzlement, vandalism, extortion, and sabotage), they differ in terms of "the positions of the perpetrators, the environments of the act, the methods used in the abuse, and the form of assets." With computers, for example, it now is easier for very small groups or lone offenders to commit large-scale extortion and other crimes that traditionally have been difficult—if not impossible—to accomplish without the physical or financial backing of a larger organization (see Ratliff, 2005).

Authors' Note: The authors wish to thank Jim Short, Pete Simi, and the anonymous reviewers for their comments on a previous draft of this article. Correspondence concerning this article should be addressed to Lorine A. Hughes, Department of Criminal Justice, 310 NE Hall, Lincoln, NE 68588-0561; e-mail: `lahughes@mail.unomaha.edu`.

Although a variety of these new forms of computer crimes (or "cybercrimes") exists, those that are perpetrated through the use of viruses, worms, and Trojan horses are the most prevalent and appear to be among the most troubling to computer users (Furnell, 2002). Indeed, many of us have experienced firsthand the havoc wreaked by such malicious software ("malware"); countless others are at risk. Beyond the immediate effects of these attacks, victims may suffer economic strain, lowered levels of personal and organizational productivity, and emotional distress (see Trend Micro, 2002). Because those who are responsible for their creation and dispersal often go undetected and unpunished, victims also are unlikely to be compensated financially or to experience either justice or revenge.

Perhaps because of the stealthy and technical nature of "rogue computer programs" and the difficulty of obtaining relevant data, we know little about the scope and impact of the problem. Much of the information on computer threats—and computer crimes in general—is derived from sensationalized media accounts and surveys of businesses regarding financial losses and organizational security practices (Wall, 2002). Data from the U.S. federal government are of limited value, mainly because of their heavy focus on software vulnerabilities and threats that may affect the national infrastructure and "federal interest" computers. Attempts to broaden the reach of federal computer crime laws to deal specifically with viruses, Trojan horses, and worms often have failed,[1] leaving a legal vacuum for states to fill. The result is a varied and idiosyncratic body of law that has been largely impotent in the fight against increasingly cross-jurisdictional offenses (Davis, 1994; McCall, 1988).

Partly because of the inadequacy of existing laws, law enforcement agencies throughout the United States have been slow to respond to computer crimes or to provide the necessary intelligence for better understanding of these offenses. Jurisdictional issues, and practical considerations such as limited financial resources and the lack of properly trained personnel, also hamper law enforcement efforts to address most forms of computer crime (Stambaugh et al., 2000). Not surprisingly, then, local law enforcement has tended to exclude computer crimes from its domain or to focus only on those that are most amenable to traditional methods of policing. In the latter cases, the computer typically is incidental, rather than central, to the crime (e.g., child "grooming" or luring; see R. G. Smith, Grabosky, & Urbas, 2004).[2]

Although some (mainly British) scholars have examined issues related to hacking and investigated the legal aspects of computer crimes and law enforcement responses, criminological inquiries into this relatively new area of offending have been largely restricted (but see Hollinger, 1997; Wall, 2003).

> The hitherto lack of criminological commentary about cybercrimes suggests that criminologists are clearly frustrated by the absence of familiar tools that generate "reliable data"—in much the same way as when called to respond to any new type of harmful behaviour about which there has been (usually a media-inspired) public panic. (Wall, 2002, p. 187; see also Wall, 2001)

Faced with the paucity of police data, criminologists with an interest in computer crimes are forced to rely on other sources of information.[3] Limited funding opportunities and technical expertise often dissuade criminologists from collecting alternate forms of data, however, as does the field's clear preference for study of more visible street crimes.[4] The resulting lack of empirical research on computer crimes has prevented informed debate on the nature of these offenses and the level of threat they pose, allowing untested claims to be advanced freely. This is especially true with respect to criminological discussions of computer viruses and other types of malicious software, which often do no more than rehash basic definitions, describe a handful of high-profile cases, and point to the difficulties involved in research into the topic.[5] In this article, we draw on threat reports issued by a major vendor of computer security products to provide an empirical assessment of the propagation patterns and functionality of computer malware detected during a 12-month period beginning on January 1, 2004. Findings reveal that these programs warrant general concern and greater criminological attention but that their overall threat thus far has been exaggerated.

Viruses, Worms, and Trojan Horses

Although computer viruses first appeared in the 1980s (Furnell, 2002),[6] it was not until the 1990s that malicious software came to be seen as a major cause for concern. Previously, viruses typically carried benign “payloads” (functionality) and employed inefficient methods of propagation (e.g., via floppy disks). With advancing technologies and increasing Internet connectivity, however, there emerged the possibility for widespread dissemination of increasingly destructive viruses. Moreover, the development of virus-writing kits meant that viruses could be created and circulated at a much faster rate, as these kits allowed their users to bypass the esoteric computing language that had previously held in check the total number of virus writers and the speed with which they worked.[7]

Discovery of the first computer virus in the wild was followed shortly thereafter by the spread of other threats designed to reach a broad audience, including Trojan horses and worms.[8] Two new classes of threats, adware and spyware, were recently added.[9] Adware consists of programs that “facilitate delivery of advertising content to the user through their own window, or by utilizing another program’s interface” (Symantec, 2005a; see also Taylor, Caeti, Fritsch, & Liederbach, 2005), in some cases also gathering usage information from the infected computer and sending it to a remote location. By definition, spyware has “the ability to scan systems or monitor activity and relay [usage or personal] information to other computers or locations in cyber-space” (Symantec, 2005a). Adware and spyware are spread in the same furtive way, typically being placed onto a computer when the user downloads a seemingly legitimate program in which either or both types of threats are hidden (e.g., weather tool bar) or visits a Web site that surreptitiously downloads the malicious code. Both also can be spread through e-mail and instant messaging. What distinguishes viruses from these and other computer crimes and abuses is that the former, like their epidemiological counterparts, require a host to survive and replicate. Once attached to a host (a file or disk), a virus will unleash its payload and affect the infected computer in any number of ways, depending on the specific environment in which the virus operates (Taylor et al., 2005) and “ranging from the harmless but irritating display of messages on the screen to the trashing of data or the manipulation of other programs within the system” (Furnell, 2002, p. 145).

Worms are autonomous, self-replicating threats that do not infect or alter computer programs in the same way as viruses; their main objective is to spread to other computers through e-mail, instant messaging programs, network systems, software vulnerabilities, and peer-to-peer file-sharing networks (e.g., KaZaA, Winny, etc.; Taylor et al., 2005). Much of the initial concern over worms centered on their propagation routines and the associated consumption of valuable computer and network resources. The implications of entire systems being brought to a halt by the promulgation of worms—as happened in the case of the infamous Morris Internet Worm[10]—were far reaching and extended beyond government interest in national security and the integrity of the nation's infrastructure to businesses and other organizations that depend on computers to conduct their day-to-day activities (e.g., colleges and universities, NASA, etc.). Although apocalyptic predictions related to the development of flash, Warhol, and other "super worms" have yet to materialize (see Dyson, 2005; McCollum, 2003; Staniford, Grim, & Jonkman, 2001; Weaver, 2005), the success of such worms as Beagle, Mydoom, Mytob, and Sobig.F demonstrates the effectiveness of relatively unsophisticated e-mail propagation routines, especially when coupled with social engineering strategies that trick people into believing that the threat they are receiving consists of information or photographs related to sex and nudity, celebrities (often naked and somehow involved with sex), a secret crush or joke, a potential personal embarrassment, money, computer security, and so forth.[11] At the same time, however, the recent emergence and dispersion of the Blaster worm (also known as LovSan and MSBlast) highlights the continuing problem of worms that rely on some of the more technologically advanced methods of spread.[12]

In recent years, worms have attracted increasing attention for the problems they cause beyond those related to their replication and distribution. Reflecting the emerging trend toward "blended threats," which "combine the characteristics of viruses, worms, Trojan Horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack" (Symantec, 2005a; see also Taylor et al., 2005, p. 140), modern-day worms frequently exhibit a type of functionality previously associated exclusively with Trojan horses. As in the legendary tale about the hollow wooden horse that the Greeks used to smuggle their soldiers into Troy, a Trojan horse is a destructive program that masquerades as a legitimate file or application to gain entry to a computer (or, more recently, mobile phone, personal digital assistant, or gaming device). Once in the system, a Trojan horse may perform any number of undesirable actions, including deleting or damaging files, launching a denial of service attack (i.e., preventing the use of the targeted computer or the Internet), making beeping sounds, starting and stopping processes, stealing information (e.g., passwords), and opening a back door that allows an outside attacker to control the compromised computer remotely and perform such actions as launching a distributed denial of service attack in which all infected computers are transformed into zombies that overwhelm a targeted Web site with simultaneous requests for information or by sending large amounts of data. This recently happened to Yahoo!, CNN, Microsoft, and several major e-commerce sites, including Amazon, eBay, and E*trade (Kumar, 2004; Lemos, 2001; Livingston, 2001; Yasin, 2001).

The first Trojan horse, PC-Write, appeared in 1986 (Dickey, 2003; see also Microsoft TechNet, 2004). Disguised as the latest version of a popular word processing application, the Trojan was downloaded onto the computers of many unsuspecting users, whose hard drives were then reformatted and wiped out (i.e., all files were lost). More recent Trojan horses likewise disrupt the normal operation of computers, albeit not always to the same extent or using the same methods. Following the growth of the Internet and user connectivity, however, the functionality of Trojan horses increasingly has been expanded to include the release of information and other activities that appear to be oriented toward more instrumental goals. Beyond cybertagging and vandalism, theft, trespassing, invasion of privacy, and the other immediate damages caused by Trojan horses and those who release them into the wild, then, it is important to recognize the role that these threats may play in the furtherance of such crimes as fraud, identity theft, and even extortion (see Ratliff, 2005; Symantec, 2005b).

Although Trojan horses are often confused with viruses and worms (and viruses and worms confused with one another), there are important technical distinctions between them. Nevertheless, Trojan horses and other types of malware are all similar in that they "take advantage of the very conveniences and features that make the Internet so appealing" (Taylor et al., 2005, p. 119) and may cause problems for computer users and those who rely on them. Because of the lack of systematic study of the topic, however, it is unclear whether these programs are nothing more than minor irritations or pose a significant threat that warrants serious official and public concern and criminological attention.

Major Threat or Minor Irritation?

Because "there is no centralized database that collects information on the damage that viruses [and other types of malware] cause" (Taylor et al., 2005, p. 119), it is impossible to say with any certainty whether the effects of these programs constitute a major threat or have been largely overblown by the media and other doomsayers. Recent events and analyses, however, suggest that there are good reasons for concern. Reports and press releases from the major antivirus companies—including McAfee, Sophos, Symantec, and Trend Micro—reveal a substantial increase in the number and complexity of malware attacks. Symantec's (2005b) September 2005 *Internet Security Threat Report* also shows a shift during the first 6 months of the year toward more profit-oriented attacks and attacks that target individual computers rather than the servers and networks to which they are connected. Although such trends are alarming in terms of their implications for the millions of people who rely on computers for personal use (Day et al., 2005; see also Pew Internet & American Life Project, 2005), the pecuniary losses incurred by these home users likely pale in comparison to the costs that viruses and other malware create for corporate organizations, financial and medical institutions, government agencies, and colleges and universities. Findings from the 10th annual Computer Crime and Security Survey, conducted by the Computer Security Institute in cooperation with the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad, suggest that the fiscal losses to these entities are staggering. Respondents reported $130,104,542 in losses from 13 different types of computer security incidents, with the greatest amounts attributed to viruses ($42,787,767), unauthorized access ($31,233,100), and theft of proprietary information ($30,933,000). Because of the survey's inability to account for "implicit losses (such as the lost future sales due to negative media coverage following a breach)," however, these figures may underestimate the true costs of such attacks (L. W. Gordon, Loeb, Lucyshyn, & Richardson, 2005, p. 15; see also Campbell, Gordon, Loeb, & Zhou, 2003).[13] They also may be biased downward by the general reluctance among banks and computer experts in many businesses to admit to incidents that might negatively affect consumer confidence (Baker, 1993; Furnell, 2002; Marion, 1989; Parker, 1976; see also Wall, 2002).

Reflecting government interest in protecting the nation's critical infrastructure, media reports of the threat of computer crimes and abuses to our increasingly digital economic, communication, and information systems were followed by quick legislative action (Hollinger & Lanza-Kaduce, 1988; see also Taber, 1980). First passed by Congress in 1984, the Computer Fraud and Abuse Act has been the main law used to deal with computer crimes at the federal level. As amended to incorporate computer malware, this statute

> criminalizes knowingly causing the transmission of a program, code, or command, and as a result, intentionally causing damage to a protected computer. . . . Subsections 1030(a)(5)(A)(ii) and 1030(a)(5)(A)(iii) prohibit intentional access without authorization that results in damage, but do not require intent to damage. (Jacobson & Green, 2002, p. 281)

Prosecutions of computer malware writers under the act have been relatively rare, mainly because of the "burden and complexity of the government's case" (Montana, 2000, p. 58), the traditionally narrow focus of the law on information stored on federal interest computers, and the existence of legislative loopholes stemming from vague terminology (Baker, 1993; Colombell, 2002; Davis, 1994; McCall, 1988).[14] Problems related to detection and enforcement, particularly in cases originating in foreign countries (those both with and without related laws), also have made it difficult to bring the perpetrators of these crimes to trial (see R. G. Smith et al., 2004). For these reasons, the federal government has actively pursued the development of agencies that assess electronic threats to the national infrastructure, communicate information and warnings about critical network and software vulnerabilities, and coordinate responses to cyberattacks and other breaches of security. The two primary agencies, the National Infrastructure Protection Center (NIPC) and U.S. Computer Emergency Response Team, operate under the aegis of the Federal Bureau of Investigation and U.S. Department of Homeland Security, respectively, and were established and developed amid growing fears of cyberterrorism and cyberwar (see D. E. Denning, 2000; Shimeall, Williams, & Dunlevy, 2001-2002), political "hacktivism" and cyberprotests (especially from China; see NIPC, 2001), and a possible connection between certain types of cyberattacks and organized crime (see Adams, 1996; Ratliff, 2005).

"Most state computer crime laws are comprehensive statutes, and often take the form of an independent title in a state's criminal code called the 'Computer Crimes Act' or the 'Computer Crime Prevention Act'" (Schmalleger, 2006, p. 412). However, some states have simply modified existing laws to incorporate computer crimes, and a few others have developed new computer crime laws within traditional statutory categories (Schmalleger, 2006; see also Davis, 1994). Although a number of scholars view the more specialized laws as having significant practical and symbolic advantages over the Band-Aid approach to dealing with unauthorized computer access and other types of computer crimes, they contend that stiffer penalties and legislation tailored specifically to computer malware are needed (in more than just a few states) to deter and punish individuals who engage in such harmful activities (Baker, 1993; Davis, 1994; Gemignani, 1990; Marion, 1989; Sokolik, 1980; Tramontana, 1990; see also Jacobson & Green, 2002; Raskin & Schaldach-Paiva, 1996; Young, 1995).

Although greater government concern and intervention may be warranted, skeptics argue that there is no evidence to substantiate the claim that computer viruses and other types of malware constitute a significant threat (S. Gordon, Ford, & Wells, 1997; G. Smith, 1998;

Vmyths.com, 2003; see also Davis, 1994; P. J. Denning, 1990; Furnell, 2002; Hansen, 1990; Wall, 1998). Although they acknowledge the existence of computer malware and concede that viruses, worms, and Trojan horses may indeed create serious problems, they argue that the dangers of these programs have been largely exaggerated by individuals and groups who stand to benefit, financially or otherwise, from the fear that such hype generates and by academics lacking sufficient technical expertise to distinguish between reality and make-believe.[15] Smith (1998) argues further that one need only to consider the technical and economic realities confronted by computer viruses and those who create them to appreciate the nonsensical nature of much of the claims surrounding these programs. This view is echoed in a recent security watch report by the senior associate editor of CNET Reviews, the editorial portion of a well-known technology Web site (`CNET.com`). Although the author alerts us to the existence of "virus gangs" on the Internet, he portrays the individual members of these gangs not as dangerous criminals, but as "thugs" whose "interest in marking territory and showing off their elite skills" somewhat ironically prompts "everyone to patch their system in advance of something even worse" (Vamosi, 2004, para. 9).[16]

For these and other skeptics, the real dangers of computer malware stem from a general lack of awareness. Because viruses, worms, and Trojan horses are not well understood, mythological assertions have been difficult to dispel. Consequently, they argue, more time and resources are devoted to worrying about these programs than to safeguarding against the seemingly greater harm caused by the errors or malicious activities of insiders and other computer end users (see L. W. Gordon et al., 2005). For businesses, the government, and others who rely on computers, however, the possibility of external attacks destroying data, invading privacy, and performing a variety of other harmful actions hardly seems trivial.

Because of the lack of empirical research on computer malware, the extent to which such programs constitute a significant threat is largely unknown. Criminological attention to this issue—indeed, to computer crimes and abuses more generally—has been particularly deficient. This article presents results from a systematic analysis of the payload and propagation patterns of Trojan horses, worms, and viruses detected during a 1-year period. The goal is to inform the larger debate surrounding these programs and to establish a baseline for future research.

Data and Method

Data for this research are from malware threat reports issued by a major vendor of computer security products during a 1-year period beginning on January 1, 2004, and ending on December 31, 2004. These reports document the "attributes for each new form of malicious code that emerges both in the wild and in a 'zoo' (or controlled laboratory) environment" and are based on analyses of malicious code samples submitted to the firm from any of the more than "120 million client, server, and gateway systems" that employ the firm's antivirus products in both "consumer and corporate environments" (Symantec, 2004, p. 2).[17] Following the removal of all generic threat reports and duplicates resulting from updates and name changes, there remained more than 930 reports to analyze ($N = 935$). Although these data clearly are not as ideal as if they were derived from an independent source and must be viewed cautiously, they provide an alternative to the problematic types of data that have been used in the past (see Taber, 1980) and, given the practical difficulties of obtaining sufficiently detailed information about computer malware and their creators, may be the best available.

All security threat reports were obtained and coded within a day or two of their publication. To ensure that the codes reflected the most recent information concerning the functionality and distribution of the malware, they were updated to take into account any change that had been made to the reports in the following 6 to 18 months.[18] Each report includes five threat assessment measures related to the distribution, removal, and control of the malware under consideration: number of infections ("number of computers known to be infected"), number of sites (number of organizations with infected computers), geographic distribution (low = "localized or non-wild" threat, medium = "threat in a few geographic regions," high = "global threat"), threat containment using current antivirus technology (easy = "well-contained," moderate = "partially contained," difficult = "uncontainable"), and removal (easy = "requires little or no expertise," moderate = "requires some expertise," difficult = "requires an experienced technician"). Also included are three composite "threat metrics" related to the current and potential spread of the malware under consideration and to its potential damage: wild ("measures the extent to which a virus is already spreading" and is based on number of infections and sites, geographic distribution, threat containment, and the complexity of the threat), distribution ("measures how quickly a threat is able to spread"), and damage ("measures the amount of harm that a given threat might inflict" and is based on its payload, errors in its code, and ease of repair). These three measures are combined to produce a rating of overall threat of the malware to computer users, with 1 = *very low*, 2 = *low*, 3 = *moderate*, 4 = *severe*, and 5 = *very severe*. Because the rated threat of some of these programs—particularly those with a high rate of initial spread—often fluctuates considerably, we include only the most recent ranking, that is, the one that remains stable over time and reflects the rated level of threat after the initial period in which continuous upgrading and downgrading takes place.

In addition to these measures, we examined the reports for information related to the propagation routine and payload of the various types of computer malware. Because the same program may use multiple methods to spread and may be capable of performing more than one type of function, it was necessary to create a separate category for each possibility. In all, we constructed eight dichotomous measures of computer malware propagation: e-mail, Web, software vulnerability, instant messaging, peer-to-peer file-sharing network, computer network, remote command, and other (e.g., back doors opened by other malware). Dichotomous measures were also constructed for each of the 35 primary payload categories. These range from simple annoyances and displays of messages or images to the deletion or downloading of files, denial of service and distributed denial of service attacks, remote access, and theft of information (including system information, passwords, and keystrokes, whether in general or for financially related Web sites).

Data Analysis

To assess the level of threat posed by computer malware, we first examine the distribution of the various types and the operating systems they target. We then focus on the scope

Table 1
Type of Malware

Type of Malware	*n*	%
Virus	36	3.9
Worm	468	50.1
Trojan horse	350	37.4
Macro virus	30	3.2
Macro worm	2	0.2
Zoo virus	8	0.9
Zoo worm	4	0.4
Zoo Trojan horse	19	2.0
Zoo macro virus	9	1.0
Worm/virus	6	0.6
Trojan horse/virus	1	0.1
Trojan horse/worm	1	0.1
Zoo virus/zoo Trojan horse	1	0.1
Total	935	100.0

and controllability of these programs, as indicated in the security threat reports. Finally, we turn our attention to their propagation routines and payloads. Here, we are less concerned with the extent of the threat than with how they spread and what they do.

Table 1 presents the frequency and percentage distribution of the various types of computer malware reported for the year 2004. Of the total number of cases, approximately half (50.1%) were worms. Trojan horses comprised slightly more than one third of all cases (37.4%), whereas viruses made up less than 5% (3.9%). Even when combined with malware that is dually classified (worm/virus and Trojan horse/virus) and with viruses not in the wild (“zoo”) or that are written into the macros of a particular application such as Microsoft Word (macro viruses), computer viruses still constitute a small proportion of all threats (9.8%). This suggests that much of what we hear about computer viruses in the media and elsewhere is based on a misnomer. Although computer viruses may have been the most prevalent type of malware in previous years, they have since given way to worms and Trojan horses.

Table 2 shows the frequency and percentage distribution of the operating systems affected by these malware. Given the high usage of Microsoft Windows relative to other operating systems and the general disdain for Microsoft among the hacker community (see Furnell, 2002), it is not surprising that Microsoft Windows is the most targeted operating system. Of the 927 cases for which sufficient information was available, 880 (94.9%) affected only Microsoft Windows operating systems. Another 15 (1.6%) affected both Microsoft Windows and Macintosh operating systems. Less than 1% (0.3%) affected only Macintosh operating systems. A small, but possibly growing, proportion of the malware reportedly targeted the EPOC operating systems of mobile phones (1.8%) and Windows CE for the Pocket PC (0.2%). The remaining threats affected DOS, UNIX, and Linux operating systems, either exclusively or in some combination with each other, OS/2, and/or Microsoft Windows.

Table 3 and Table 4 show the frequency and percentage distribution of each component of the threat assessment and threat metrics measures, respectively. Consistent with arguments advanced by the skeptics, these data indicate that most computer malware poses

Table 2
Systems Affected

Systems Affected	*n*	%
DOS	1	0.1
UNIX	2	0.2
Windows	880	94.9
Macintosh	3	0.3
Windows CE (pocket PC)	2	0.2
EPOC (mobile phone)	17	1.8
DOS and Windows	1	0.1
UNIX and Windows	3	0.3
Macintosh and Windows	15	1.6
UNIX and Linux	1	0.1
Windows and Windows CE	1	0.1
DOS, UNIX, Windows, Macintosh, Linux, OS/2	1	0.1
Subtotal	927	100.0
Not provided	8	
Total	935	

relatively little risk to the computer user. Although nearly half of all threats were considered to have at least a medium level of ability to propagate or to cause damage (distribution and damage in Table 4), only a few threats were widely disseminated or difficult to remove or contain (Table 3 and wild in Table 4). Thus, it is not surprising that the overwhelming majority of threats were rated as very low or low (63.1% and 36.7%, respectively), with only 2 (0.2%) rated as moderate and none rated as severe or very severe (Table 5).

In the remaining analyses, we focus attention on the propagation routines and payloads of the various types of computer malware. Removal of zoo threats, and the threats that were limited to the macros of specific applications, resulted in a total of 862 cases. Of these, 33 (3.8%) reportedly had bugs in their code and did not necessarily spread and/or function properly. Because these threats often were only partially defective, we did not omit them from the analyses.

Table 6 presents data on the methods by which computer malware spread. Because this information frequently was not provided for viruses and Trojan horses, these data mainly reflect the propagation patterns of worms. E-mail is the most common method, followed by computer networks, software vulnerabilities, and peer-to-peer file-sharing networks. Relatively few threats are spread through Web sites, instant messaging programs, remote commands, and other methods such as back doors opened previously by another malware. The predominance of e-mail as a method of malware distribution is not surprising given the popularity of e-mail relative to other Internet activities (Pew Internet & American Life Project, 2005; see also U.S. Department of Commerce, 2004). Computer end users thus may play the most important role in the spread of malware.

For analytical purposes, we rank ordered the payload categories according to the proportion of computer malware reported to perform each function. Table 7a includes the five most prevalent payloads. Although no single action is reported to have been associated with more than half of all cases for which sufficient information is available, approximately 48%

Table 3
Threat Assessment

Infections[a]	*n*	%
0 to 49	808	91.0
50 to 999	56	6.3
More than 1,000	24	2.7
Total	888	100.0
Sites		
0 to 2	778	87.6
3 to 9	31	3.5
More than 10	79	8.9
Total	888	100.0
Geographical distribution		
Low	870	98.0
Medium	11	1.2
High	7	0.8
Total	888	100.0
Threat containment		
Easy	877	98.8
Moderate	10	1.1
Difficult	1	0.1
Total	888	100.0
Removal		
Easy	419	47.2
Moderate	458	51.6
Difficult	11	1.2
Total	888	100.0

Note: Information on each of these components was not provided for 47 cases.
a. Given the nature of the reports, we were unable to partition threat assessment measures into fewer, more precise categories.

of all threats were capable of downloading a file or files onto the infected computer, either independently or on remote command. The nature of these files is unclear, but at least 41 (4.8%) were other malware (data not presented).

The four remaining threats are perhaps among the most serious. Out of 853 cases, 388 (45.5%) opened back doors that allowed unauthorized remote access to the infected computer. The back doors varied greatly in terms of the extent of access they provided, though most allowed the remote attacker to perform more than a couple of actions (e.g., download a file, delete files, end processes, and capture Web cam or screen images).[19] However, only 23 cases (3.5%) were reported to provide the remote attacker with complete control of the computer.[20]

An alarming number of threats were reported to release information from the compromised computer. Although system information was the most commonly targeted, the “keylogging” (i.e., recording of typed keystrokes into a log file that is forwarded to the attacker, often through e-mail) capability of numerous threats also placed user information, passwords, and financial information at risk. Financial information frequently was targeted by programs that monitored the user’s Internet browser for certain words in the title bar (e.g., fidelity, e-Gold, bank) and logged keystrokes only when these were present. Not all of these threats targeted

Table 4
Threat Metrics

Wild	*n*	%
Low	846	95.3
Medium	39	4.4
High	3	0.3
Total	888	100.0
Damage		
Low	450	50.7
Medium	427	48.1
High	11	1.2
Total	888	100.0
Distribution		
Low	498	56.1
Medium	175	19.7
High	215	24.2
Total	888	100.0

Note: Information on each of these components was not provided for 47 cases.

Table 5
Overall Threat Level

Threat Level	*n*	%
Very low	559	63.1
Low	325	36.7
Moderate	2	0.2
Severe	0	0.0
Very severe	0	0.0
Total	886	100.0

Note: A total of 49 cases were not rated.

Table 6
Method of Spread

	Yes		No	
	n	%	*n*	%
E-mail	243	46.8	276	53.2
Computer network	152	29.3	367	70.7
Software vulnerability	134	25.7	387	74.3
Peer-to-peer file-sharing network	117	22.7	398	77.3
Other (e.g., back door opened by other malware)	67	12.6	466	87.4
Remote command	64	10.1	568	89.9
Web	42	8.0	481	92.0
Instant messaging	35	6.7	487	93.3

Table 7a
Payload (40% to 50% Prevalence)

	Yes		No	
	n	%	*n*	%
Download file or files	350	47.9	381	52.1
Remote access	388	45.5	465	54.5
Release information	322	44.5	401	55.5
System information (CPU, IP address, etc.)	232	33.9	453	66.1
Financial information	156	23.9	496	76.1
Passwords	136	20.8	518	79.2
User information	119	18.4	527	81.6
Degrade performance or system instability	276	43.1	364	56.9
Delete or modify file or files	285	43.0	378	57.0

users with accounts at financial institutions in the United States or other developed countries; users with Brazilian bank accounts were targeted at least as often, if not more.

Roughly the same proportion of all threats was reported to degrade computer performance (43.1%) or delete or modify files (43.0%). Both of these functions can cause significant problems for businesses and other organizations and for home computer users (especially those with important data stored on their machines). Performance degradation often was associated with mass-mailing worms, whereas the deletion of files regularly appeared as a remote capability or as a tool to prevent the updating of computer security programs. In some cases, the deletion of files was clearly meant to be malicious, with either random files or all files needed to run computer applications being targeted (62 or 7.4%).

Table 7b includes the next 15 most commonly reported actions performed by the computer malware. These functions generally are less severe than the most prevalent threats, ranging from denial of service to minor annoyances. However, approximately 1 in 3 (34.7%) reportedly compromised antivirus or other security programs, often by ending processing or disabling associated keys in the computer registry. A slightly lower proportion (31.1%) was reported to prevent security updates from Microsoft or antivirus Web sites. Nearly 1 in 4 (22.9%) was reported to alter the function of a program. Much to the chagrin of online businesses and other organizations with an online component, about the same proportion (23.3%) possessed the capacity to perform denial of service attacks. Reflecting both the existence of so-called "benevolent" malware and the periodic flare-ups between various virus gangs, close to 1 in 3 (31.3%) threats reportedly deleted existing malware from the infected computer or otherwise disabled it. Approximately 1 out of every 5 threats was reported to display a message and/or image (20.9%),[21] end one or more nonsecurity processes (20.7%), perform an annoying action (19.5%), and/or open or close a specific program (19.2%). Relatively few threats were reported to act as a proxy or Web server, that is, as an intermediary between a client application such as Internet browser and a computer server (13.2%), relay messages through e-mail or instant messaging programs (11.6%), hijack Internet browsers and point them to a random or specified Web site (11.2%), or set up a file transfer system that permits files to be retrieved from or placed onto the compromised computer (10.9%).

Table 7b
Payload (10% to 39% Prevalence)

	Yes		No	
	n	%	*n*	%
Compromise security program	224	35.0	416	65.0
End processes	243	34.7	458	65.3
Delete other malware	192	31.3	422	68.7
Prevent security update	185	31.1	409	68.9
Denial of service	157	23.3	516	76.7
Alter program function	143	22.9	481	77.1
Display message	138	20.9	522	79.1
End nonsecurity process	132	20.7	505	79.3
Annoyance (beep, change display or mouse, etc.)	129	19.5	533	80.5
Open or close program or programs	124	19.2	521	80.8
Proxy or Web server	114	13.2	748	86.8
Damage or crash system	72	13.1	477	86.9
Spam, e-mail, or instant message relay	75	11.6	573	88.4
Browser hijack (change browser page)	73	11.2	580	88.8
FTP setup	73	10.9	595	89.1

The least common computer malware functions are presented in Table 7c. Nearly 1 in 10 threats were reported to attack other individual computers (9.1%), often by repeatedly sending and/or requesting information and thereby consuming a large amount of resources. Roughly the same proportion reportedly visited Web sites (8.9%) or launched a distributed denial of service attack (8.3%). The visited Web sites often contained pornographic materials or malicious code. Chat rooms were entered by 40 threats (6.2%), usually to spread themselves or to receive remote commands. Relatively few threats involved direct interaction between the remote attacker and the user of the compromised computer (3.6%). Only 45 (6.9%) of the threats reportedly monitored the user's Internet or other computer-related activities, perhaps because adware and spyware are more effective trackers. Fortunately for the end user, few threats were reported to drop or generate other malware (2.9% and 5.7%, respectively), disrupt the Internet connection (5.4%), hide themselves (4.5%), set or disable a macro (3.6%), delete or reformat the hard drive (2.9%), redirect Internet traffic to the compromised computer (0.1%), or perform a brute force dictionary attack in which an attempt is made to guess the password of a protected computer or server by systematically entering each word in the dictionary (0.1%). Despite the recent concern over cyberhacktivism, only 19 (2.2%) threats were reported to communicate with the computer user through means other than the more commonly used method of displaying messages and/or images.

To determine the extent to which these findings reflect general patterns in the data or may be attributed to the dominance of those few threats with multiple variants, we excluded from the analyses all but the first variant of each threat reported in 2004 (*n* = 504 with all threats and *n* = 437 after the removal of zoo threats and macros; data not presented). Although the general placement of each of the functions into one of the three tiers of prevalence remains unchanged, a few important differences emerge. With the exception of delete

Table 7c
Payload (0% to 9% Prevalence)

	Yes		No	
	n	%	*n*	%
Attack other Pcs	60	9.1	602	90.9
Visit Web sites or servers	58	8.9	591	91.1
Distributed denial of service	54	8.3	598	91.7
Monitor user activity	45	6.9	611	93.1
Enter or join chat room	40	6.2	609	93.8
Generate other malware	49	5.7	812	94.3
Disrupt Internet connection	35	5.4	614	94.6
Hide self	39	4.5	819	95.5
Interact with user	23	3.6	623	96.4
Set or disable macro	23	3.6	624	96.4
Drop other malware	25	2.9	836	97.1
Reformat or delete computer hard drive	25	2.9	837	97.1
Other communication	19	2.2	842	97.8
Brute force dictionary attack	1	0.1	861	99.9
Redirects Internet traffic to PC	1	0.1	861	99.9

or modify files and several of the least serious actions (e.g., display message, alter program function, annoyance, browser hijack), the proportion of all payload functions decreases—hence, the even lower levels of risk revealed by all three measures provided in the security threat reports. Reflecting the especially large number of worm variants produced during periods of cyberconflict between the major virus gangs, the proportion of worms also decreases (and is now second to Trojan horses), as does the proportion of threats that delete existing malware from the targeted computer. Finally, the proportion of threats that spread via the World Wide Web and instant messaging programs increases, whereas the proportion of those that rely on software vulnerabilities, computer networks, and remote commands decreases considerably. Together, these findings suggest that, similar to the amount of crime that can be attributed to the relatively small proportion of chronic offenders (Wolfgang, Figlio, & Sellin, 1972), there exists a handful of threats that contribute disproportionately to the overall computer malware problem. These threats are also the ones that tend to spread via some of the more technologically advanced methods of propagation.

Conclusion and Discussion

"Advanced, post-industrial societies and economies are critically dependent on linked computer information and communication systems" (Shimeall et al., 2001-2002). Potential threats to these systems thus raise serious concerns. As the Internet has expanded and our reliance on it increased, the dangers of computer viruses and other types of malware have been widely touted, by the media, the government, and others. At the same time, however, a growing chorus of voices criticizes this position for being based on an irrational fear of what often turns out to pose little to no real threat.

Findings from this study show that neither position is entirely wrong and that the risk of danger probably depends on who is affected. On one hand, the data reveal that most threats are not widely distributed, do not cause significant damage, and are fairly easy to contain and remove. Their potential to spread and effect major hardships is equally limited. On the other hand, however, the most prevalent actions performed by existing malware tend to be among the most serious in terms of their ability to release information, provide unauthorized computer access, destroy data, and result in financial losses. Clearly, these types of threats have major implications, for businesses, for home users with important information stored on their computers, and for researchers, government agencies, and other organizations (e.g., hospitals and universities) with an obligation to protect the confidentiality of their digital records. Even if such threats affect only a small proportion of the population of computer users, this nevertheless translates into a large number of victimizations. Though the likelihood is not high, the consequences can be disastrous. In 2004, for example, the Sasser worm interrupted regular travel services in the United States and affected the French Stock Exchange, the U.K. Maritime and Coastguard Agency, a leading bank in Finland, Taiwan’s postal service, and one of the largest hospitals in Korea (Keizer, 2004).

Of course, it is important to reiterate that the source of the data on which these findings are based is not without biases and clearly has a vested interest in continuing the angst surrounding computer malware. A similar parallel can be drawn to police data and other forms of commonly used sources of criminological information, however. In addition, because findings provide a great deal of support to claims made by those skeptical of the alleged threat of computer malware, greater confidence can be had in these data. Until there are better ways to learn about computer malware and other computer crimes and abuses, criminologists will need to find creative ways to gain insight into these little understood phenomena (which clearly warrant their attention). Research should focus in particular on trends over time. Although viruses, worms, and Trojan horses may be of relatively limited threat today, these programs are continually evolving and may pose a significant future risk, especially if those that contribute disproportionately to the problem increase in number and begin to employ even more sophisticated methods of spread (Furnell, 2002, pp. 186-191). To the extent that malicious code and software continue to proliferate primarily through popular computer applications (e.g., e-mail and peer-to-peer file sharing), however, it will be necessary to consider the role of the end user in their spread. Indeed, addressing the problem may be more a matter of educating computer users about safe and unsafe computing practices and improving software to guide these people toward more secure use of systems and to better contain the results of insecure choices than furthering legislative and law enforcement responses, which thus far have been largely ineffective and are likely to always be so. This is not to say that the expenditure of large amounts of financial and human resources for the sake of target hardening is wasteful, nor do we recommend an end to the development of special computer crime task forces or to the practice of earmarking federal grant monies for the creation of technologies to assist law enforcement in combating and reacting to various cyberthreats and security breaches. Rather, our findings lead us to argue quite simply that practices that promote the development of proper routine (computer) activities by end users must be considered an important part of the solution to the problem of viruses, worms, and Trojan horses. Local, national, and global efforts to increase user awareness of the potential dangers of cyberspace and how best to avoid them nevertheless can coexist with innovative legal and law enforcement strategies to fight cybercrimes, including the development of incentive structures and programs for actions undertaken to benefit the common good (see Powell, 2005). Widespread educational campaigns occurring in a school setting, at the organizational level, and through the media actually may benefit traditional approaches by preventing the escalation of minor nuisances into major problems and thereby allowing resources to be targeted more specifically on those few offenders and offenses that pose the most serious threat. Such selective targeting might enhance international cooperation and lead to the development of cross-border treaties that are sensitive to variations in the laws and practices of different nations and to the privacy and civil liberties of computer users throughout the world.

Notes

1. Prior to the passage of the National Information Infrastructure Protection Act (1994), which amends the 1984 Computer Fraud and Abuse Act to include computer malware, the Computer Virus Eradication Act was proposed in 1988 and 1989, stalling both times (for a history of federal legislation, see Adams, 1996; Baker, 1993; Hansen, 1990; Jacobson & Green, 2002; May, 2004).

2. Apprehension of offenders who commit these crimes requires the least amount of technical expertise, yet it is this type of police work that appears to receive the most media attention and public support.

3. The National Incident-Based Reporting System does, however, including a category to indicate “whether the computer was the object of the crime” and “to indicate whether the offender(s) used computer equipment to perpetrate a crime” (U.S. Department of Justice, 2000, p. 19). Because “it is the national UCR Program’s position that Computer Crime actually involves the historical common-law offenses of larceny, embezzlement, trespass, etc., which are being perpetrated through the use of a new tool, the computer” (U.S. Department of Justice, 2000, p. 19), no new classification for computer crimes has been created.

4. This preference is evident in the relatively limited number of computer crime sessions at the annual meetings of the American Society of Criminology. Since 1999 (and including 2005), there have been 16 sessions dedicated to computer crimes and related issues. Other topics have that many or more in a single year. Moreover, in the most recent program, half of the papers dealing with computer crimes are included in the residual Other Varieties of Offending subcategory of the Varieties of Offending session. The other half are included in the Identity Theft and Computer Crime subcategory of the same session.

5. The lack of criminological understanding of computer malware can have potentially serious effects, as made clear by a recent case involving two university professors who cited as examples of real computer viruses a number of hoaxes that were part of an April Fool’s Day tradition maintained by *Datamation* magazine. This work, “Trends and Experiences in Computer Crime: Findings From a National Study,” was presented at the 1996 Academy of Criminal Justice Science meetings in Las Vegas and published in condensed form (as “Computer Crime: An Emerging Challenge for Law Enforcement”) in the December 1996 hard copy edition of the FBI Law Enforcement Bulletin (“The Nutty Professors,” 2003).

6. The first computer virus was intended to “have the potential to improve computing technology” and is credited to Fred Cohen, a University of Southern California graduate student (Furnell, 2002, p. 152; but see Barrett, 2003; Kaspersky Lab, 2005; “Timeline,” 2005). The first malicious virus, Brain, appeared in 1986 (Furnell, 2002).

7. Individuals who “rely upon scripts and programs written by other, more competent hackers” are often referred to as “script kiddies” and are “generally viewed with scorn by more accomplished members of the hacking community” (Furnell, 2002, p. 44).

8. Another type of malware is the “software bomb,” which is malicious code that is implanted in a particular program within a specific computer system and lays dormant until triggered by a specific event or time. We do not include software bombs in this discussion because they differ from viruses, Trojan horses, and worms in that they are “more likely to be specifically placed within a particular target system, with the aim of having an equally specific effect on it” (Furnell, 2002, p. 149; see also Stephenson, 2000).

9. Although adware and spyware are included here in the discussion of computer threats, they generally are not “considered malware because they are not programs written with malicious intent” (Microsoft TechNet, 2004).

10. The Morris Worm (otherwise known as the Internet Worm and the Cornell Internet Worm) was created by Robert T. Morris, who at the time was a graduate student at Cornell University. Morris released his worm into the Advanced Research Projects Agency Network of the U.S. Department of Defense on November 2, 1988, apparently intending no harm. A design flaw caused the worm to spread much faster than expected, soon resulting in the overloading of numerous computer systems (see P. J. Denning, 1990; Montz, 1990; Spafford, 1990). Morris was the first person convicted under the Computer Fraud and Abuse Act of 1986. He is now an associate professor in the Department of Electrical Engineering & Computer Science at MIT.

11. A recent study conducted by the Pew Internet & American Life Project (2005; see also U.S. Department of Commerce, 2004) indicates that e-mailing is the most common online activity engaged in by the growing population of Internet users.

12. The Blaster worm took advantage of a flaw in the Microsoft Windows operating system and is estimated to have resulted in at least $525 million in damages (Pethia, 2003).

13. Another implied cost is the "productivity lost from everyone having to chat and e-mail their friends about the latest threat" (Taylor, Caeti, Fritsch, & Liederbach, 2005, p. 145).

14. The term *protected computer* now incorporates any computer "used in interstate or foreign commerce or communications" (18 U.S.C. 1030), essentially covering all computers connected to the Internet. This and other amendments made by the National Information Infrastructure Protection Act, and the USA Patriot Act, have eliminated some of the problems associated with earlier legislative responses at the federal level (Colombell, 2002; Jacobson & Green, 2002; see also the Computer Crime and Intellectual Property Section, 2005).

15. Ross Anderson (2001) argues that society and most business firms overspend on computer security measures, in part because of the lack of built-in security features in many computer applications and because of "perverse economic incentives" among software companies to "create insecure systems" (p. 7) and ensure "customer lock-in" (p. 3).

16. Interestingly, Marion (1989, p. 630) argues that the lack of computer crime prosecutions can be partly attributed to the tendency of police and prosecutors to view computer criminals in the same way (i.e., as "more clever than dangerous").

17. The firm was established in 1989 and today is among the world leaders in computer security. In addition, the firm has been recognized by both *Fortune* and *Forbes* magazines for its business practices.

18. Reports were rechecked at the end of June 2005. Three new reports of Trojan horses were discovered in October 2005 and were included in the analysis.

19. The reports frequently contained only general reference to "remote access" and did not specify which actions the attacker could perform. This is a large part of the reason behind the large number of missing (i.e., indeterminable) cases for most of the payload categories. The categories with no missing data—hide self, brute force dictionary attacks, proxy or Web server, redirect Internet traffic, drop malware, generate malware, and other communication—did not involve the use of an indeterminable code; that is, they were automatically coded as 0 if not reported.

20. With the exception of the payload categories that did not involve the use of an indeterminable code, all payload categories were coded as 1 when the threat provided full remote access.

21. Most of these were error messages or notification of infection by the malware; relatively few were political in nature.

References

Adams, J. M. (1996). Controlling cyberspace: Applying the Computer Fraud and Abuse Act to the Internet. *Computer and High Technology Law Journal*, *12*, 403-434.

Anderson, R. (2001, December). *Why information security is hard: An economic perspective*. Paper presented at the 17th Annual Computer Security Applications, New Orleans, LA.

Baker, G. D. (1993). Trespassers will be prosecuted: Computer crime in the 1990s. *Computer/Law Journal*, *12*, 61-100.

Barrett, N. (2003). *Students delete history*. Retrieved November 5, 2005, from http://www.vnunet.com/itweek/comment/2086036/students-delete-history

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*, 431-448.

Central Intelligence Agency. (2005). *The world factbook*. Retrieved July 26, 2005, from `http://www.cia.gov/cia/publications/factbook/rankorder/2153rank.html`

Colombell, M. R. (2002). The legislative response to the evolution of computer viruses. *Richmond Journal of Law and Technology*, *8*. Retrieved October 28, 2005, from `http://law.richmond.edu/jolt/v8i3/article18.html`

Computer Crime and Intellectual Property Section. (2005). *Computer crime*. Retrieved June 28, 2005, from `http://www.usdoj.gov/criminal/cybercrime/compcrime.html`

Davis, B. S. (1994). It's virus season again, has your computer been vaccinated? A survey of computer crime legislation as a response to malevolent software. *Washington University Law Quarterly*, *72*, 411-440.

Day, J. C., Janus, A., & Davis, J. (2005). *Computer and Internet use in the United States: 2003*. *Current population reports*. Washington, DC: U.S. Census Bureau.

Denning, D. E. (2000, Autumn). Cyberterrorism: The logic bomb versus the truck bomb. *Global Dialogue*, pp. 29-37.

Denning, P. J. (1990). The Internet worm. In P. J. Denning (Ed.), *Computers under attack: Intruders, worms, and viruses* (pp. 193-200). New York: Addison-Wesley.

Dickey, K. (2003). Tales of Trojan horses: Why you should beware of those bearing gifts. *Avoid & Defeat Viruses*, *9,* 12-16. Retrieved October 2, 2005, from `http://www.smartcomputing.com/editorial/article.asp?article=articles/archive/l0902/03l02/03l02.asp`

Dyson, J. (2005). What me worry (about the Warhol worm)? Retrieved July 18, 2005, from `http://www.treachery.net/~jdyson/what_me_worry.html`

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. Boston: Addison-Wesley.

Gemignani, M. (1990). Viruses and criminal law. In P. J. Denning (Ed.), *Computers under attack: Intruders, worms, and viruses* (pp. 489-494). New York: Addison-Wesley.

Gordon, L. W., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI computer crime and security survey*. San Francisco: Computer Security Institute.

Gordon, S., Ford, R., & Wells, J. (1997, October). *Hoaxes & hypes*. Paper presented at the 7th Virus Bulletin International Conference, San Francisco.

Hansen, R. L. (1990). The Computer Virus Eradication Act of 1989: The war against computer crime continues. *Software Law Journal*, *3*, 717-753.

Hollinger, R. C. (Ed.). (1997). *Crime, deviance and the computer*. Aldershot, UK: Dartmouth.

Hollinger, R. C., & Lanza-Kaduce, L. (1988). The process of criminalization: The case of computer crime laws. *Criminology*, *26,* 101-126.

Jacobson, H., & Green, R. (2002). Computer crimes. *American Criminal Law Review*, *39*, 273-325.

Kaspersky Lab. (2005). *History of malicious programs*. Retrieved November 1, 2005, from `http://www.viruslist.com/en/viruses/encyclopedia?chapter=153311030`

Keizer, G. (2004). *Sasser worm impacted businesses around the world*. Retrieved November 28, 2005, from `http://www.techweb.com/wire/26804909`

Kumar, V. A. (2004). Sophistication in distributed denial-of-service attacks on the Internet. *Current Science*, *87*, 885-888.

Lemos, R. (2001). *Attack knocks out Microsoft Web sites*. CNet News.com. Retrieved July 27, 2005, from `http://news.com.com/Attack+knocks+out+Microsoft+Web+sites/2100-1001_3-251573.html`

Livingston, B. (2001). *We can prevent those distributed denial of service attacks with* "*egress filtering*." Retrieved October 5, 2005, from `http://archives.cnn.com/2000/TECH/computing/03/01/prevent.ddos.idg/`

Marion, C. C. (1989). Computer viruses and the law. *Dikinson Law Review*, *93*, 625-642.

May, M. (2004). *Federal computer crime laws*. The SANS Institute. Retrieved October 7, 2005, from `http://www.sans.org/rr/whitepapers/legal/1446.php`

McCall, C. (1988). Computer crime statutes: Are they bridging the gap between law and technology? *Criminal Justice Journal*, *11*, 203-233.

McCollum, T. (2003). Super worms could pose new security threats. *IT Audit*, *6*. Retrieved November 28, 2005, from http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=5435

Microsoft TechNet. (2004). *The antivirus defense-in-depth guide*. Retrieved October 2, 2005, from http://www.microsoft.com/technet/security/topics/serversecurity/avdind_2.mspx

Montana, J. C. (2000). Viruses and the law: Why the law is ineffective. *Information Management Journal*, *34*, 57-60.

Montz, L. B. (1990). The worm case: From indictment to verdict. In P. J. Denning (Ed.), *Computers under attack: Intruders, worms, and viruses* (pp. 260-263). New York: Addison-Wesley.

National Infrastructure Protection Center. (2001). *Cyber protests: The threat to the U.S. information infrastructure*. Retrieved October 27, 2005, from http://www.au.af.mil/au/awc/awcgate/nipc/cyberprotests.pdf

The nutty professors. (2003). *Crypt Newsletter*. Retrieved July 16, 2005, from http://www.soci.niu.edu/~crypt/other/quant.htm

Parker, D. B. (1976). *Crime by computer*. New York: Scribner.

Pethia, R. D. (2003). *Viruses and worms: What can we do about them?* Testimony before the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relation and the Census. Retrieved September 16, 2003, from http://www.cert.org/congressional_testimony/Pethia-Testimony-9-10-2003/

Pew Internet & American Life Project. (2005). *Online activities—Daily*. Retrieved September 30, 2005, from http://www.pewInternet.org/trends/Daily_Activities_8.05.05.htm

Powell, B. (2005). *Is cybersecurity a public good? Evidence from the financial services industry* (Paper 57). Oakland, CA: The Independent Institute.

Raskin, X., & Schaldach-Paiva, J. (1996). Computer crimes. *American Criminal Law Review*, *33*, 541-573.

Ratliff, E. (2005, October 10). The zombie hunters: On the trail of cyberextortionist. *The New Yorker*, pp. 44-49.

Schmalleger, F. (2006). *Criminal law today: An introduction with capstone cases* (3rd ed.). Upper Saddle River, NJ: Pearson/Prentice Hall.

Shimeall, T., Williams, P., & Dunlevy, C. (2001-2002). Countering cyber war. *NATO Review*, *49*, 16-18. Retrieved July 16, 2005, from http://www.cert.org/archive/pdf/counter_cyberwar.pdf

Smith, G. (1998). An electronic Pearl Harbor? Not likely. *Issues in Science and Technology*, *15*, 68-73.

Smith, R. G., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial.* Cambridge, UK: Cambridge University Press.

Sokolik, S. L. (1980). Computer crime—The need for deterrent legislation. *Computer/Law Journal*, *2*, 353-383.

Spafford, E. H. (1990). Crisis and aftermath. In P. J. Denning (Ed.), *Computers under attack: Intruders, worms, and viruses* (pp. 223-243). New York: Addison-Wesley.

Stambaugh, H., Beaupre, D., Icove, D. J., Baker, R., Cassaday, W., & Williams, W. P. (2000). State and local law enforcement needs to combat electronic crime. In *Research in brief* (pp. 1-6). Washington, DC: U.S. Department of Justice, National Institute of Justice, Office of Justice Programs.

Staniford, S., Grim, G., & Jonkman, R. (2001). *Flash worms: Thirty seconds to infect the Internet. Silicon defense*. Retrieved July 18, 2005, from http://richie.idc.ul.ie/eoin/SILICON%20DEFENSE%20-%20Flash%20Worm%20Analysis.htm

Stephenson, P. (2000). *Investigating computer-related crime*. Boca Raton, FL: CRC.

Symantec. (2004). *Symantec Internet security threat report: Trends for January 1, 2004–June 30, 2004* (Vol. 6). Cupertino, CA: Author.

Symantec. (2005a). *Security risks*. Retrieved October 5, 2005, from http://securityresponse.symantec.com/avcenter/security_risks/

Symantec. (2005b). *Symantec Internet security threat report: Trends for January 05–June 05* (Vol. 8). Cupertino, CA: Author.

Taber, J. K. (1980). A survey of computer crime studies. *Computer/Law Journal*, *2*, 275-327.

Taylor, R. W., Caeti, T. J., Fritsch, E. J., & Liederbach, J. (2005). *Digital crime and digital terrorism*. Upper Saddle River, NJ: Prentice Hall.

Timeline. (2005). CBSNews. Retrieved November 28, 2005, from http://www.cbsnews.com/htdocs/cyber_crime/timeline.html

Tramontana, J. (1990). Computer viruses: Is there a legal antibiotic? *Rutgers Computer and Technology Law Journal*, *16*, 253-381.

Trend Micro. (2002). *The real cost of a virus outbreak: Why is antivirus needed?* Retrieved July 16, 2005, from http://www.go-red.com/pdf/white_paper_realcost.pdf

U.S. Department of Commerce. (2004). *A nation online: Entering the broadband age*. Retrieved November 6, 2006, from http://www.ntia.doc.gov/reports/anol/NationOnlineBroadband04.htm

U.S. Department of Justice. (2000). *National incident-based reporting system volume 1: Data collection guidelines*. Washington, DC: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, Uniform Crime Reporting Program.

Vamosi, R. (2004). *Does a virus gang own the Internet?* CNET Reviews. Retrieved June 27, 2005, from http://reviews.cnet.com/4520-3513_7-5133725.html

Vmyths.com. (2003). *Truth about computer hysteria*. Rhode Island Soft Systems, Inc. Retrieved November 3, 2005, from http://www.vmyths.com/

Wall, D. S. (1998). Policing and the regulation of the Internet. *Criminal Law Review*, (*Special Edition 1998*), 79-91.

Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 1-17). London: Routledge.

Wall, D. S. (2002). Insecurity and the policing of cyberspace. In A. Crawford (Ed.), *Crime and insecurity*: *The governance of safety in Europe* (pp. 186-209). Portland, OR: Willan.

Wall, D. S. (2003). *Cyberspace crime.* Aldershot, UK: Dartmouth.

Weaver, N. C. (2005). *Warhol worms: The potential for very fast Internet plagues*. Retrieved July 18, 2005, from http://www.cs.berkeley.edu/~nweaver/warhol.html

Wolfgang, M. E., Figlio, R. M., & Sellin, T. (1972). *Delinquency in a birth cohort*. Chicago: University of Chicago Press.

Yasin, R. (2001). *Tools stunt DoS attacks: Monitors dam packet floods at ISP routers*. InternetWeek. Retrieved July 27, 2005, from http://internetweek.cmp.com/newsleads01/lead020501.htm

Young, L. F. (1995). Combating unauthorized Internet access. *Jurimetrics Journal*, *35*, 257-261.

Lorine A. Hughes is an assistant professor in the Department of Criminal Justice at the University of Nebraska at Omaha. Her research interests include youth gangs, sex offenders, and computer crime. She may be reached at lahughes@mail.unomaha.edu.

Gregory J. DeLone is an assistant professor in the Department of Criminal Justice at the University of Nebraska at Omaha, where he teaches organization and administration, policing, drugs and crime, statistics, and philosophy of criminal justice. His PhD is in public administration. He may be reached at gdelone@mail.unomaha.edu.