STATEMENT OF

JOHN G. MALCOLM

DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U. S. DEPARTMENT OF JUSTICE

BEFORE THE HOUSE COMMITTEE ON
GOVERNMENT REFORM, SUBCOMMITTEE
ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERMENTAL
RELATIONS AND THE CENSUS

SEPTEMBER 10, 2003

Mr. Chairman and Members of the Subcommittee, thank you for this opportunity to testify about the Department of Justice's continuing effort to protect our nation's critical infrastructure from the growing problem of destructive Internet-borne computer "viruses" and "worms." This issue is of critical importance to our country's computer networks and its economy, and I commend the Subcommittee for holding this hearing.

In my testimony today, I would like to briefly outline the nature of the threat from malicious computer code commonly known as viruses and worms, the Congressional response to this problem, and the Department of Justice's current efforts both to combat the effects of computer viruses and worms and to arrest and prosecute the perpetrators of these crimes.

The nature of the threat

Although computer viruses have been around for a long time, the ubiquity of Internet access and household ownership of computers in the United States

have manifestly increased the deleterious impact of viruses and worms on our critical infrastructure and on our daily lives. Similarly, we have seen a significant increase in network intrusions; denial of service attacks and system damage; extortion threats involving computer systems and networks; and other criminal conduct that demonstrate that, unfortunately, criminals have taken to the Internet as eagerly as law-abiding citizens. It seems that nearly every week, we learn the name of a new computer virus or worm that exploits flaws in commonly used software and quickly spreads through the Internet. As the public relies increasingly on high-speed electronic communications, email attachments, and peer-to-peer file sharing programs, viruses and worms will continue to spread.

First, a brief explanation of what computer viruses and worms are, and how they spread from network to network. A virus is a small computer program that attaches itself to a legitimate program or file on a target machine, which is usually described as a 'host' for the virus. The virus is then copied from machine to machine when that infected program or file is shared. A worm is also a computer program, but unlike a virus, a worm does not need a host file. A computer worm usually has the ability to copy and spread itself to other computers on other networks. As a result, computer worms generally spread faster than computer viruses, and some have spread around the world in a matter of hours or, in some cases, minutes.

The behavior of malicious code, whether a virus or a worm, is determined

by the ‘payload’ of the program, which is the embedded instructions that tell the virus or worm what to do once it arrives on a system. The worm or virus may be relatively benign or it may delete essential system files, change critical data or otherwise disrupt the normal functioning of a computer system. Worms and viruses, which spread rapidly and use up available bandwidth, routinely clog networks. When this occurs, essential e-commerce and other legitimate network traffic are prevented from following their normal course.

Each year, the incidents of world-wide epidemics of computer viruses and worms increase. In recent memory, we have seen the ILOVEYOU virus in 2000, the Code Red worm and the NIMDA virus in 2001; the Klez worm in 2002; and so far in 2003, the Slammer worm; the MiMail worm; the MSBlaster worm; and SoBig.F. These viruses and worms are merely the tip of the iceberg – they are just the ones that have received the most public attention. Hundreds more are released every year, posing a daily challenge to those responsible for protecting networks and investigating network attacks.

The effect of these viruses and worms should not be underestimated. For example, in the United States, the Slammer worm shut down the automatic teller machine system and caused significant transportation delays when electronic ticketing used for airline travel was affected. The “LovSan” or “Blaster” worm and its variants have affected hundreds of thousands of computers. The original variant of the worm shut down Maryland’s Motor Vehicle Agency and other

entities. The MiMail worm affected computers nationwide, including computers at U.S. government agencies, by cleverly masquerading as a message from a company's or agency's system administrator. Previous outbreaks, such as the NIMDA virus and Code Red worm, have been blamed for significant losses to businesses across the country, as servers became infected and were rendered unable to perform tasks related to banking and electronic commerce.

Since the Internet is seamless and borderless, the harmful impact of worms and viruses is not limited to our country. At the international level, news services reported that the Slammer worm was responsible for severely hampering an Asian stock market for the better part of a day, and disrupted a Canadian political party's vote for its national leader. The Blaster worm knocked nearly 20,000 Swedish Internet users offline, and harmed hundreds of thousands of home and business users around the world.

Clones, or new varieties of malicious code, continue to crop up, raising concerns that more damaging variants are right around the corner. These varieties of existing viruses and worms are developed in an underground community of creators who share emerging vulnerabilities, develop exploits directed to those vulnerabilities, and refine the malicious code. Although such "copycat" creators of viruses and worms do not always develop the original code, their activity is no less dangerous. In many cases, succeeding generations of a virus or worm will build on its capabilities, adding additional harmful payloads or

enhancing the capability of the virus to spread. For instance, the teenager in Minnesota who was just charged with creating a copycat version of the Blaster worm is alleged to have modified the original Blaster virus and caused significant additional damage.

The worldwide damage to computers and data, as well as the productive time lost, as a result of viruses and worms measures in the millions, and by some estimates, in the billions of dollars. This damage has an undeniable, adverse effect on important sectors of our economy and potentially undercuts the security of the nation's critical infrastructure. Resources are lost due to the inability of businesses and employees to use the Internet, unexpected shutdowns of computer systems in homes and offices, and time spent repairing damaged and infected systems.

Applicable legislation

Causing damage to our nation's computer networks is a federal crime, one that carries substantial penalties for those convicted. The principal federal law enforcement weapon in the battle against computer viruses and worms is the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Specifically, subsection (a)(5) makes it a federal crime to knowingly cause the transmission of a program, information, code or command, and as a result of such conduct, intentionally cause damage, without authorization, to a protected computer if the conduct

caused (or causes) --

1. a loss of at least $5,000 to one or more persons during any one-year period;

2. the impairment or modification of the medical diagnosis or treatment of one or more persons;

3. physical injury to any person;

4. a threat to public health or safety; or

5. damage to a government computer system used for the administration of justice, national defense, or national security.

The scope of the prohibition is broad and recognizes that the risk of damage from a computer virus or worm is significant, and could impact critical national or personal interests. Penalties for felony violations of the law range from 5 years in prison to 20 years for subsequent offenders, to life imprisonment for those whose knowing or reckless violations result in someone's death. We expect new sentencing guidelines to go into effect shortly that more closely correlate the sentencing structure for these crimes with their serious nature. These guidelines will provide for significant sentencing enhancements for abuse of specific skills employed in sophisticated means to facilitate the crime; the number of victims; the risk of serious bodily injury or death; and the degree of damage caused by the criminal conduct.

<u>The Department of Justice's Response to the Problem</u>

The Department of Justice has devoted significant resources to investigating and prosecuting persons who release malicious code on the Internet. Those efforts have met with some success. For example, in 2001, David Smith of New Jersey was sentenced to 20 months in federal prison after pleading guilty to unleashing the "Melissa" computer virus that infected untold numbers of computer networks and caused millions of dollars in damage. It bears mentioning, however, that tracking the source of viruses and worms on the Internet is difficult and presents unique challenges to investigators because of the speed with which such programs spread, and the fundamental characteristics of computer networks. Particularly in “peer-to-peer” networking applications, it is difficult to determine precisely where an outbreak began, since simultaneous file transfers can occur to other computers in far corners of the world.

Although tracking the sources of viruses and worms is difficult, the Department of Justice is committed to fully and effectively investigating such attacks. The USA PATRIOT Act has significantly enhanced the Department’s ability to respond in computer crime investigations. Specifically, the reaffirmed applicability of pen register/trap and trace orders to Internet non-content traffic and the single-order pen register/trap authority afforded to the Department under this Act adds important procedural tools to investigations of computer crime.

The Criminal Division’s Computer Crime and Intellectual Property Section, which I supervise, maintains a number of prosecutors who help coordinate

investigations into computer crimes of all sorts, including virus and worm attacks. They, in turn, work with Computer Hacking and Intellectual Property (CHIPS) units and Computer and Telecommunications Coordinators (CTCs) in each of the 93 U.S. Attorneys' offices. Together, this network of prosecutors, working with law enforcement agencies such as the Secret Service and the FBI, provide an integrated approach to addressing computer crime.

The recent arrest by federal authorities in Minnesota of an 18-year old suspected of releasing a variant of the Blaster worm illustrates that this conduct is treated seriously and consonant with the harm that it causes. This is not the end of the Blaster worm investigation because the original author of the worm has not yet been apprehended, and new variants of the worm appear almost daily. We will do everything we can to bring the perpetrator of the Blaster worm and copycat offenders to justice.

Because the perpetrators of these offenses may live in other countries, these investigations frequently have an international component that draws upon the Department's contacts with law enforcement counterparts abroad. Indeed, international cooperation is a foundation of the Department of Justice's strategy for combating cybercrime including viruses and worms. Department personnel, including attorneys and FBI agents, have been instrumental in training legislators and law enforcement in foreign countries on drafting cybercrime laws and developing investigative techniques.

We worked with international partners to negotiate the Council of Europe Convention on Cybercrime, which requires parties to criminalize the use of viruses and worms to intentionally damage computers and networks. The Convention requires countries that join the Convention to have minimum procedural tools to investigate such attacks, and to facilitate international cooperation in investigating such attacks. These efforts are rewarded when evidence is obtained from foreign countries that further domestic investigations, or when we are able to furnish similar assistance to other countries.

In addition to international outreach, Department attorneys and agents regularly meet with industry, trade groups and state and local law enforcement to improve communication with federal law enforcement. The Department of Justice pursues the message of a 'culture of security' where both individual users and corporations view computer security as a key component of a successful computing experience. Preventing computer virus and worm epidemics by keeping operating system software updated and by practicing 'safe computing' will always be the first line of defense against malicious code.

The Department has also pursued educational programs directed to youth that we describe as 'cyberethics." This program delivers the message to young people that certain moral responsibilities attach to skill and knowledge about computers. We understand that some of our brightest students are attracted to

the world of computing and the intellectual rigor of that course of study. However, there is a bright line between responsible intellectual inquiry and criminal conduct that hurts people and damages property.

The Department of Justice continues to make progress in the battle against computer crime and intellectual property theft. Recognizing the challenges ahead, we look forward to continued success in our efforts.

Conclusion

Mr. Chairman, I want to thank you again for this opportunity to testify about the problem of computer viruses and worms and the Department of Justice's efforts to protect critical infrastructure. Government agencies, industry, and individual citizens alike are threatened by this abuse of computing power. The Department of Justice is actively pursuing the perpetrators of these crimes and is dedicated to ensuring that they know that there are serious consequences for their actions.

Mr. Chairman, that concludes my prepared statement. I would be pleased to answer any questions that you may have at this time.