Attacks on the Internet in 2003

Congressional Testimony
Richard Pethia
Director, CERT Coordination Center

Disguised under ominous names like Blaster, Slammer, and Sobig.F, malicious computer code has brought more havoc to the Internet in 2003 than ever before. Releases of malicious code by unknown perpetrators have prompted heightened concern about the vulnerability of the Internet at the same time this worldwide system becomes ever more important to global communications and economics. The following document is an abridgment of testimony that CERT Coordination Center Director Richard Pethia presented to the U.S. Congress September 10 on the viruses and worms that have swept through the Internet in 2003 and actions needed to confront them.

The complete version of Mr. Pethia's testimony is available at http://www.cert.org/congressional_testimony/ Pethia-Testimony-9-10-2003/

The Internet is vulnerable to attack today, and will remain so in the foreseeable future.

Introduction

The CERT Coordination Center (CERT/CC) was formed in 1988 as a direct result of the first Internet worm. [The worm] was the first computer security incident to make headline news, serving as a wake-up call for network security. In response, the CERT/CC was established by the Defense Advanced Research Projects Agency at Carnegie Mellon University's Software Engineering Institute in Pittsburgh. Our mission is to serve as a focal point to help resolve computer security incidents and vulnerabilities, to help others establish incident response capabilities, and to raise awareness of computer security issues and help people understand the steps they need to take to better protect their systems. We activated the center in just two weeks, and we have worked hard to maintain our ability to react quickly. The CERT/CC staff has handled 260,000 incidents, cataloged and worked on resolutions to more than 11,000 computer vulnerabilities, and published hundreds of security alerts.

Today, with continued sponsorship from the Department of Defense and from the Department of Homeland Security, we continue our work and disseminate security information and warnings through multiple channels—a Web site (www.cert.org), an online vulnerability database, and an electronic mailing list of more than 161,000 addresses. We have relationships with major media outlets that help us distribute accurate information about major security events to the broad community. We also work with over 600 technology vendors to facilitate their response to product vulnerabilities and warn the community of vulnerabilities that require immediate attention.

The CERT/CC is now recognized by both government and industry as a neutral, authoritative source of data and expertise on information assurance. In addition to handling reports of computer security breaches and vulnerabilities in network-related technology, we identify and publish preventive security practices, conduct research, and provide training to system administrators, managers, and incident response teams.

Growing Risk from Worms and Viruses

Worms and viruses are in a more general category of programs called "malicious code." Both exploit weaknesses in computer software, replicating themselves and/or attaching themselves to other programs. They spread quickly and easily from system to system. By definition, worms are programs that spread with no human intervention after they are started. Viruses are programs that require some action on the part of the user, such as opening an e-mail attachment, before they spread....

Today, worms and viruses are causing damage more quickly than those created in the past and are spreading to the most vulnerable of all systems – the computer systems of home users. The Code Red worm spread around the world faster in 2001 than the so-called Morris worm moved through U.S. computers in 1988, and faster than the Melissa virus in 1999. With the Code Red worm, there were days between first identification and widespread damage. Just months later, the Nimda worm caused serious damage within an hour of the first report of infection. In January of this year, Slammer had significant impact in just minutes.

The figures ... show how quickly Slammer infected a significant number of computer systems. It shows that Blaster was slightly slower than Slammer, but still much faster than Code Red. After 24 hours, Blaster had infected 336,000 computers; Code Red infected 265,000; and Slammer had infected 55,000. Figure 2, “Comparing Blaster and Code Red in the First 18 Hours,” shows the growth in the number of computers reached by the Blaster and Code Red worms in the first 18 hours. In both cases, 100,000 computers were infected in the first 3 to 5 hours. The fast exploitation limits the time security experts like those at the CERT/CC have to analyze the problem and warn the Internet community. Likewise, system administrators and users have little time to protect their systems.

After the initial surge of infections from the Blaster worm and subsequent patching, the impact reached a steady state of 30,000 computers in any given hour.... The Blaster worm is still active and continues to have impacts on computer systems across the globe.

Impact of Worms and Viruses

At best, worms and viruses can be inconvenient and costly to recover from. At worst, they can be devastating. Virus and worm attacks alone have resulted in millions of dollars of loss in just the last 12 months.

In the 2003 Computer Security Institute/Federal Bureau of Investigation Computer Crime and Security Survey (www.gocsi.com), viruses were the most cited form of attack (82 percent of respondents were affected), with an estimated cost of $27,382,340. The lowest reported cost to a victim was $40,000, and the highest was $6 million. The Australian Computer Crime and Security Survey found similar results, with 80 percent of respondents affected by viruses or worms. Of the victims, 57 percent reported financial losses, totaling $2,223,900. According to the Australian survey, one-third (33 percent) of the victims recovered in less than one day, and 30 percent recovered in one to seven days. The other 37 percent took more time, including two organizations that believe they might never recover.

So far, damages from the Blaster worm are estimated to be at least $525 million, and Sobig.F damages are estimated to be from $500 million to more than $1 billion (*Business Week,* the London-based mi2g at *www.mi2g.com,* among other reports in the media). The cost estimates include lost productivity, wasted hours, lost sales, and extra bandwidth costs. The *Economist* (August 23, 2003) estimated that Sobig.F was responsible for one of every 16 e-mail messages that crossed the Internet. In our own experience, Sobig.F has accounted for 87 percent of all e-mail to our cert@cert.org address since August 18. We have received more than 10,000 infected messages a day, or one message every 8.6 seconds.

Implications for the Future

The significance of our recent experience with Blaster and Sobig.F lies beyond their specific activity. Rather, the worms represent a larger problem with Internet security and forecast what we can expect in the future.

My most important message is that the Internet is not only vulnerable to attack today, but it will stay vulnerable to attack in the foreseeable future. This includes computers used by government organi zations at all levels and computers used at research laboratories, in schools, in business, and at home. They are vulnerable to problems that have already been discovered, sometimes years ago, and they are vulnerable to problems that will be discovered in the future.

The implications for federal, state, and local governments, and for critical infrastructure operators, are that their computer systems are vulnerable both to attack and to being used to further attacks on others. With more and more government and private sector organizations increasing their dependence on the Internet, our ability to carry on business reliably is at risk.

Reactive Solutions are Limited

For the past 15 years, we have relied heavily on the ability of the Internet community as a whole to react quickly enough to security attacks to ensure that damage is minimized and attacks are quickly defeated. Today, however, it is clear that reactive solutions alone are no longer adequate. To briefly summarize the factors:

- The Internet now connects over 171 million computers and continues to grow at a rapid pace. At any point in time, there are millions of connected computers that are vulnerable to one form of attack or another.

- Attack technology has now advanced to the point where it is easy for attackers to take advantage of these vulnerable machines and harness them together to launch high-powered attacks.

- Many attacks are now fully automated and spread with blinding speed across the entire Internet community, regardless of geographic or national boundaries.

- The attack technology has become increasingly complex and in some cases intentionally stealthy, thus increasing the time it takes to discover and analyze the attack mechanisms in order to produce antidotes.

- Internet users have become increasingly dependent on the Internet and now use it for many critical applications as well as online business transactions. Even relatively short interruptions in service cause significant economic loss and can jeopardize critical services.

These factors, taken together, indicate that we can expect many attacks to cause significant economic losses and service disruptions within even the best response times that we can realistically hope to achieve. Aggressive, coordinated, continually improving response will continue to be necessary, but we must also move quickly to put other solutions in place.

Recommended Actions—What Can System Operators Do?

Addressing the threat of worms and viruses is not easy. With approximately 4,000 vulnerabilities being discovered each year, system and network administrators are in a difficult situation....

In the face of this difficult situation, there are steps system operators and their organizations can take to help protect systems:

Adopt security practices. It is critical that organizations, large and small, adopt the use of effective information security risk assessments, management policies, and security practices. While there is often discussion and debate over which particular body of practices might be in some way "best," it is clear that descriptions of effective practices and policy templates are widely available from both government and private sources, including the CERT/CC....

Keep skills and knowledge current. System operators should attend courses that enhance their skills and knowledge.... They need to keep current with attack trends and with tools that help them protect their systems against the attacks. The security problem is dynamic and ever changing with new attacks and new vulnerabilities appearing daily.

Help educate the users of their systems. System operators must provide security awareness programs to raise users' awareness of security issues, improve their ability to recognize a problem, instruct them on what to do if they identify a problem, and increase their understanding of what they can do to protect their systems.

Recommended Actions—What Can Technology Vendors Do?

The steps available to system operators will help, but will only solve parts of the problem. Technology vendors are in a position to prevent the spread of worms and viruses more effectively. Although some companies have begun moving toward improvement in the security of their products, there is a long way to go. Software developers do not devote enough effort to applying lessons learned about the causes of vulnerabilities. The CERT/CC continues to see the same types of vulnerabilities in newer versions of products that were in earlier versions.

Additional vulnerabilities come from the difficulty of securely configuring operating systems and applications. These products are complex and often shipped to customers with security features disabled, forcing the technology user to go through the difficult and error-prone process of properly enabling the security features they need....

It is critical for technology vendors to produce products that are impervious to worms and viruses in the first place. In today's Internet environment, a security approach based on "user beware" is unacceptable....

Recommended Actions—What Can the Government Do?

The government can help by taking a multi-pronged approach. Actions that I believe should be investigated include the following:

Provide incentives for higher quality/more security products. To encourage product vendors to produce the needed higher quality products, we encourage the government to use its buying power to demand higher quality software. The government should consider upgrading its contracting processes to include "code integrity" clauses—clauses that hold vendors more accountable for defects, including security defects, in released products and provide incentives for vendors that supply low defect products and products that are highly resistant to viruses....

Information assurance research. It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data....

Thus, the government should support a research agenda that seeks new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures....

More technical specialists. Government identification and support of cyber-security centers of excellence and the provision of scholarships that support students working on degrees in these universities are steps in the right direction....

More awareness and training for Internet users. The combination of easy access and user-friendly interfaces have drawn users of all ages and from all walks of life to the Internet. As a result, many Internet users have little understanding of Internet technology or the security practices they should adopt. To encourage "safe computing," there are steps we believe the government could take:

- Support the development of educational material and programs about cyberspace for all users. There is a critical need for education and increased awareness of the security characteristics, threats, opportunities, and appropriate behavior in cyberspace....

- Support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing....

The National Cyber Security Division (NCSD), formed by the Department of Homeland Security in June 2003, is a critical step towards implementation of these recommendations. The mission of NCSD and the design of the organization are well-aligned to successfully coordinate implementation of the recommendations that I have described here. However, implementing a "safer cyberspace" will require the NCSD and the entire federal government to work with state and local governments and the private sector to drive better software practices, higher awareness at all levels, increased research and development activities, and increased training for technical specialists.

Conclusion

Our dependence on interconnected computing systems is rapidly increasing, and even short-term disruptions from viruses and worms can have major consequences. Our current solutions are not keeping pace with the increased strength and speed of attacks, and our information infrastructures are at risk.... We can make significant progress by making changes in software design and development practices, increasing the number of trained system managers and administrators, improving the knowledge level of users, and increasing research into secure and survivable systems. Additional government support for research, development, and education in computer and network security would have a positive effect on the overall security of the Internet.

The opinions expressed in this article are those of the author and do not necessarily reflect the views or policies of the U.S. government.