

**Computer Viruses: The Disease, the Detection, and  
the Prescription for Protection**

**Testimony of Richard D. Pethia  
Director, CERT® Coordination Center  
Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213**

**Before the Subcommittee on Telecommunications  
and the Internet  
Energy & Commerce Committee  
November 6, 2003**

## **Introduction**

Mr. Chairman and Members of the Subcommittee:

My name is Rich Pethia. I am the director of the CERT® Coordination Center (CERT/CC). Thank you for the opportunity to testify on the important issue of cyber security. Today I will discuss viruses and worms and the steps we must take to protect our systems from them.

The CERT/CC was formed in 1988 as a direct result of the first Internet worm. It 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 with a mission 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.

In September of this year, the Department of Homeland Security, in conjunction with Carnegie Mellon University, created the US-CERT. The US-CERT is a growing partnership between the CERT/CC and DHS's National Cyber Security Division (NCSD) and is forging strong partnerships with many different types of organizations that conduct cyber security analysis and response efforts – From government laboratories, to academic institutions, to major hardware and software suppliers. The US-CERT is focused on preventing and mitigating cyber attacks and reducing cyber vulnerabilities. It provides the needed focal point for these over two hundred private, public, and academic organizations that conduct cyber security incident watch, warning, response, and prevention functions.

## **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 email attachment, before they spread. Users are often enticed to open email attachments, sometimes because of an intriguing or legitimate-sounding subject line and sometimes, when address books have been compromised, because the email appears to be from someone the user knows. Worms and viruses can bypass security measures, such as firewalls, and clog systems to the point that response is slow or shut off.

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 attached to the end of this testimony show the speed and magnitude of the Blaster worm compared to previous worms, as well as indications of Blaster's and Sobig.F's continued impact. Figure 1, *Blaster, Slammer, and Code Red Growth Over Day 1*, shows 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 US-CERT have to analyze the problem and warn the Internet community. Likewise, system administrators and users have little time to protect their systems.

Figure 3, *Blaster-Infected Systems Scanning per Hour: Long-Lasting Effects*, demonstrates how far-reaching worms and viruses can be. 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. However, it is a different 30,000 computers (an average of 150,000 in any given day), depending on the time of day. Peaks represent activity in different parts of the world, cycling through business days. 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 twelve months.

In the 2003 CSI/FBI Computer Crime and Security Survey ([www.gocsi.com](http://www.gocsi.com)), viruses were the most cited form of attack (82% 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 \$6,000,000. The Australian Computer Crime and Security Survey found similar results, with 80% of respondents affected by viruses or worms. Of the victims, 57% reported financial losses, totaling \$2,223,900. According to the Australian survey, one-third (33%) of the victims recovered in less than one day, and 30% recovered in one to seven days. The other 37% 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 over \$500 million (*Business Week*, 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 email messages that crossed the Internet. In our own experience, Sobig.F has accounted for 87% of all email to our [cert@cert.org](mailto:cert@cert.org) address from August 18 through the end of that month. We received more than 10,000 infected messages a day, or one message every 8.6 seconds. Figure 4, *Emails messages per Day to cert@cert.org*, shows this in a graph. Sobig.F was so effective because it could send multiple emails at the same time, resulting in thousands of messages a minute. Moreover, Sobig has been refined many times, making it harder to stop (the "F" stands for the 6th version).

### **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 forecasts what we can expect in the future.

My most important message today is that the Internet is vulnerable to these types of attack today, and the damage is likely to increase. While the viruses and worms we have seen in the past have caused considerable damage by infecting computers, and clogging networks and mail servers, few have been programmed to do more than just propagate. In the future, it is likely that we will see more malicious attacks with viruses and worms carrying payloads that delete or corrupt data and program files or leak sensitive information. These attacks could easily be aimed at computers used by government organizations 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 is 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.

### **Current 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 171,000,000 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 in very short periods of time. 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 We Do?**

The actions needed to deal effectively with this growing problem are embodied in the strategy developed by the US-CERT. They include:

- Improved warning and response to incidents with increased coordination of response information

- Reducing vulnerabilities
- Enhancing prevention and protection efforts

### **Improved warning and response**

Improved warning and response functions are critically needed to combat fast moving automated attacks such as viruses and worms. To improve current response activities, the US-CERT is building a collaborative partnership between computer security incident response teams, managed security service providers, information technology vendors, security product and service providers and other organizations that participate in cyber watch, warning, and response functions. Working together, and using common information sharing and dissemination principles, the partnership is significantly increasing the nation's ability to protect against and respond to large-scale cyber incidents. Emphasis is currently be placed on the development and use of common alerting protocols and collaboration and communication mechanisms to support the rapid identification and analysis of new attacks and the timely production and dissemination and remediation information.

### **Reducing vulnerabilities**

A key component of the US-CERT strategy is to collaborate with the private sector to develop new tools and methods for detecting and remediating vulnerabilities in products commonly used in our information infrastructures. Technology vendors are in a position to help prevent the spread of worms and viruses. Although some companies have begun moving toward improvement in the security in 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 same types of vulnerabilities continue to appear 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. While the current practices allow the user to start using the product quickly and reduce the number of calls to the product vendor's service center when a product is released, it results in many Internet-connected systems that are misconfigured from a security standpoint. This opens the door to worms and viruses.

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. The systems are too complex and the attacks happen too fast for this approach to work. Fortunately, good software engineering practices can dramatically improve our ability to withstand attacks. The solutions required are a combination of the following:

- **Virus-resistant/virus-proof software.** There is nothing intrinsic about computers or software that makes them vulnerable to viruses. Viruses propagate and infect systems because of design choices that have been made by computer and software designers. Designs are susceptible to viruses and their effects when they allow the import of executable code, in one form or another, and allow that code to be executed without constraint on the machine that received it. Unconstrained execution allows program developers to easily take full advantage of a system's capabilities, but does so with the side effect of making the system vulnerable to virus attack. To effectively control viruses in the long term, vendors must provide systems and software that constrain the execution of imported code, especially code that comes from unknown or untrusted sources. Some

techniques to do this have been known for decades. Others, such as “sandbox” techniques, are more recent.

- **Dramatically reducing implementation errors.** Most vulnerabilities in products come from software implementation errors. They remain in products, waiting to be discovered, and are fixed only after they are found while the products are in use. In many cases, identical flaws are continually reintroduced into new versions of products. The great majority of these vulnerabilities are caused by low level design or implementation (coding) errors. Vendors need to be proactive, study and learn from past mistakes, and adopt known, effective software engineering practices that dramatically reduce the number of flaws in software products.
- **High-security default configurations.** With the complexity of today’s products, properly configuring systems and networks to use the strongest security built into the products is difficult, even for people with strong technical skills and training. Small mistakes can leave systems vulnerable and put users at risk. Vendors can help reduce the impact of security problems by shipping products with “out of the box” configurations that have security options turned on rather than require users to turn them on. The users can change these “default” configurations if desired, but they would have the benefit of starting from a secure base configuration.

### **Enhancing prevention and protection efforts**

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. They are challenged with keeping up with all the systems they have and all the patches released for those systems. Patches can be difficult to apply and might even have unexpected side effects. We have found that, after a vendor releases a security patch, it takes a long time for system operators to fix all the vulnerable computer systems. It can be months or years before the patches are implemented on 90-95 percent of the vulnerable computers. For example, the US-CERT still receives reports of outbreaks of the Melissa virus, which exploits vulnerabilities that are more than four years old.

There are a variety of reasons for the delay. The job might be too time-consuming, too complex, or just given too low a priority. Because many managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Moreover, business policies sometimes lead organizations to make suboptimal tradeoffs between business goals and security needs. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply.

In the face of this difficult situation, the US-CERT is working with the private sector to encourage system operators to take several critical steps.

**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.

What is often missing today is management commitment: senior management’s visible endorsement of security improvement efforts and the provision of the resources needed to implement the required improvements.

**Keep skills and knowledge current.** System operators should attend courses that enhance their skills and knowledge, and they should be given the necessary time and support to do so. 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 Else Can the Government Do?**

The founding of the National Cyber Security Division and the US-CERT were critical first steps in the US government taking leadership over the cyber security of our nation. Government must continue to show leadership by implementing several key additional actions. These actions include:

**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. The lower operating costs that come from use of such products should easily pay for the incentive program.

Also needed in this area are upgraded acquisition processes that put more emphasis on the security characteristics of systems being acquired. In addition, to support these new processes, acquisition professionals need to be given training not only in current government security regulations and policies, but also in the fundamentals of security concepts and architectures. This type of skill building is essential in order to ensure that the government is acquiring systems that meet the spirit, as well as the letter, of the regulations.

**Invest in 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. In doing so, it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches.

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. Among the activities should be the creation of

- A unified and integrated framework for all information assurance analysis and design
- Rigorous methods to assess and manage the risks imposed by threats to information assets
- Quantitative techniques to determine the cost/benefit of risk mitigation strategies

- Systematic methods and simulation tools to analyze cascade effects of attacks, accidents, and failures across interdependent systems
- New technologies for resisting attacks and for recognizing and recovering from attacks, accidents, and failures

**Acquire and foster 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. The current levels of support, however, are far short of what is required to produce the technical specialists we need to secure our systems and networks. These programs should be expanded over the next five years to build the university infrastructure we will need for the long-term development of trained security professionals.

**Provide more awareness and training for Internet users.** The combination of easy access and user-friendly interfaces has 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. Because the survivability of systems is dependent on the security of systems at other sites, fixing one’s own systems is not sufficient to ensure those systems will survive attacks. Home users and business users alike need to be educated on how to operate their computers most securely, and consumers need to be educated on how to select the products they buy. Market pressure, in turn, will encourage vendors to release products that are less vulnerable to compromise.
- Support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing. Children should learn early about acceptable and unacceptable behavior when they begin using computers just as they are taught about acceptable and unacceptable behavior when they begin using libraries.<sup>1</sup> Although this recommendation is aimed at elementary and secondary school teachers, they themselves need to be educated by security experts and professional organizations. Parents need be educated as well and should reinforce lessons in security and behavior on computer networks.

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.

---

<sup>1</sup>National Research Council, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, 1991, recommendation 3c, p. 37.

**Conclusion**

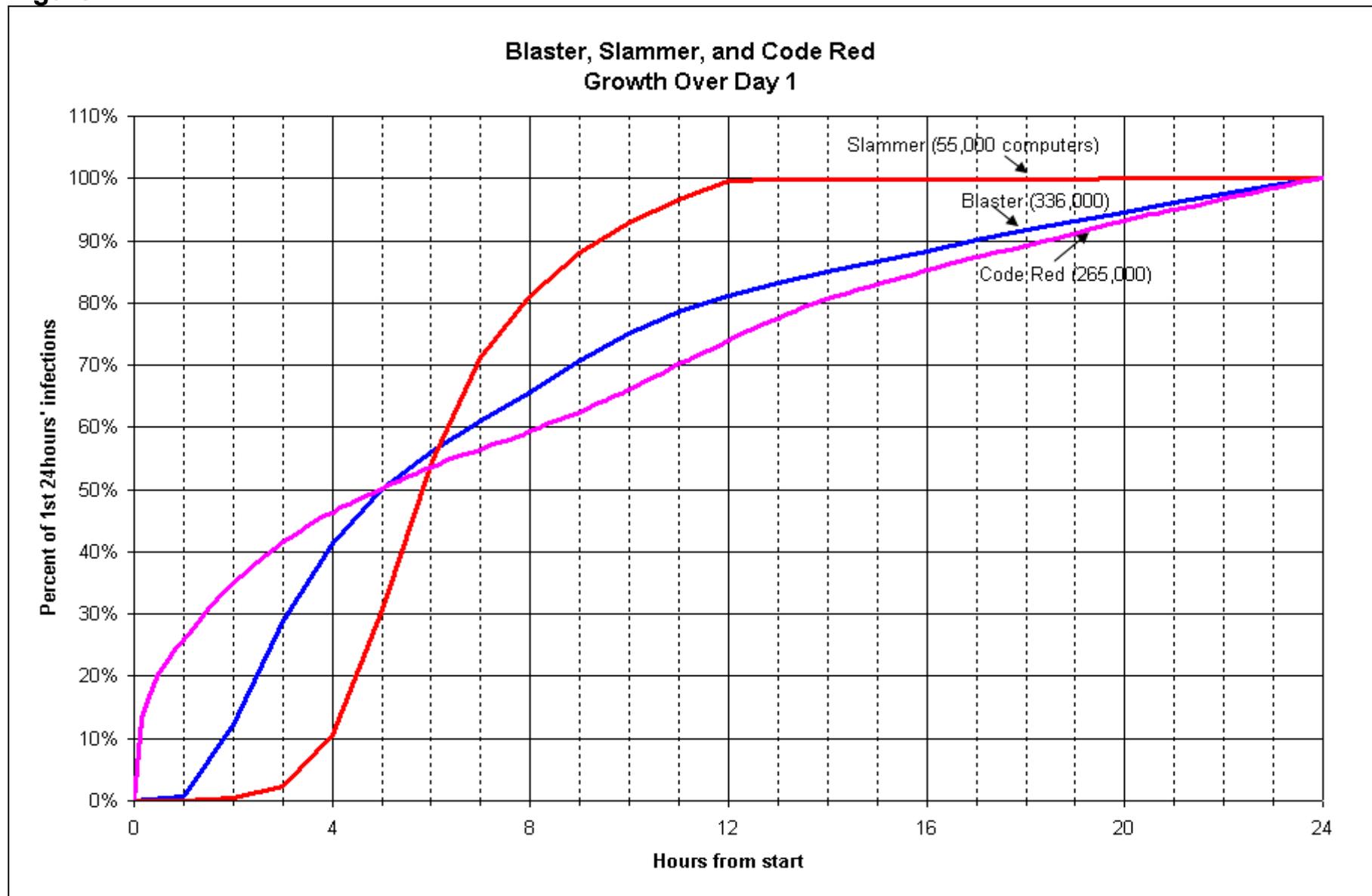
Our dependence on interconnected computing systems is rapidly increasing, and even short-term disruptions from viruses and worms can have major consequences. Our current solutions are not keeping pace with the increased strength and speed of attacks, and our information infrastructures are at risk. Solutions are not simple but must be pursued aggressively to allow us to keep our information infrastructures operating at acceptable levels of 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.



## Attachments

- Figure 1 Blaster, Slammer, and Code Red Growth Over Day 1
- Figure 2 Comparing Blaster and Code Red in the First 18 Hours
- Figure 3 Blaster-Infected Systems Scanning per Hour: Long-Lasting Effects
- Figure 4 Email Messages per Day to cert@cert.org

Figure 1



**Figure 2**

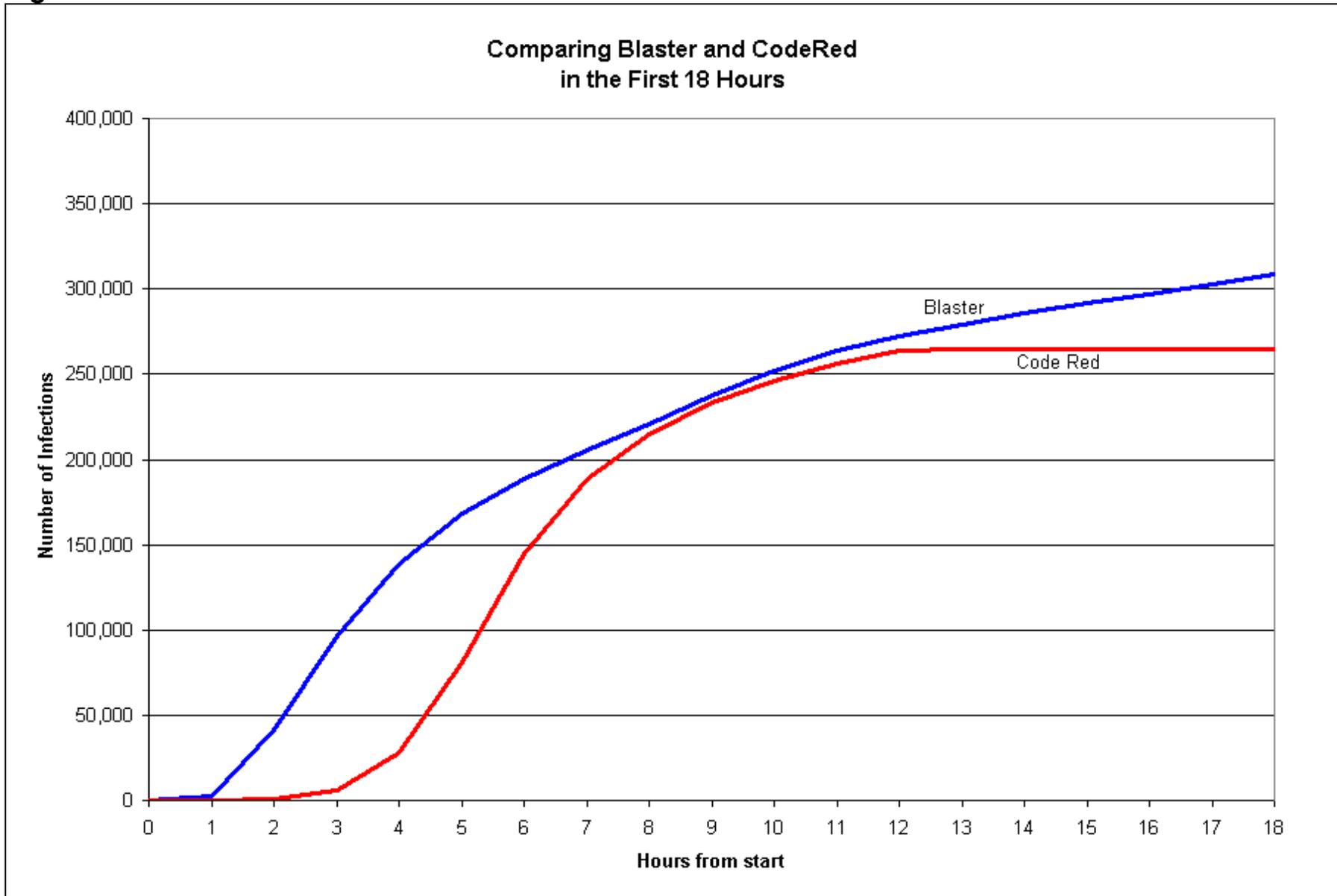


Figure 3

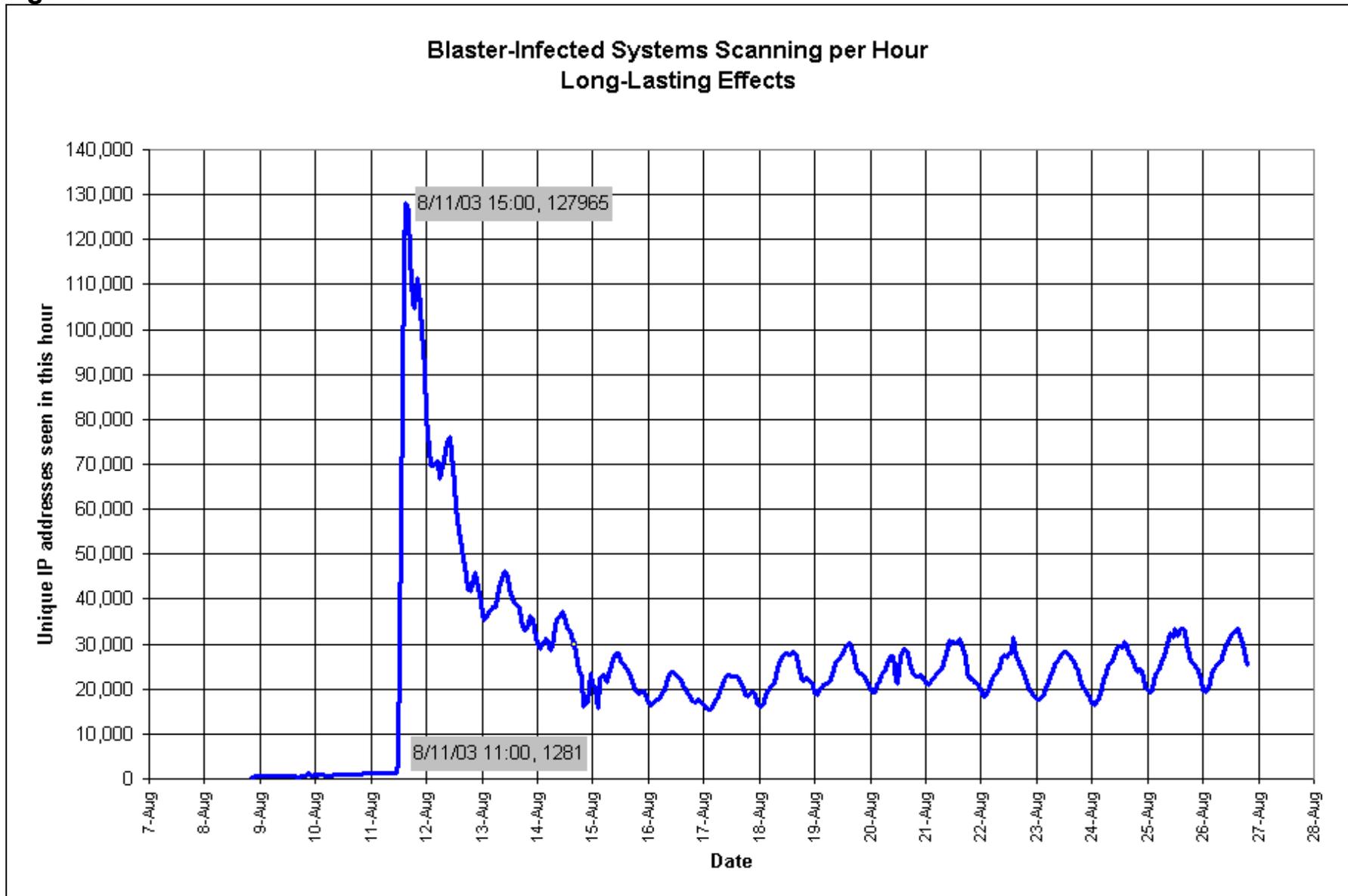


Figure 4

