Global Information Assurance Certification Paper

The SQL Slammer Worm: Challenging Computer Security on a Global Scale

Greg Vanden-Eykel
SANS Security Essentials
GIAC Certification Version 1.4b
May 23, 2003

Table of Contents

List of Figures

Abstract

The SQL Slammer worm attacked computer systems worldwide in January 2003. This malicious attack, while not causing any long-term damage, served as a wake up call to the computer technology industry. Software producers can no longer take system security lightly, and will need to enhance their support capabilities as well as begin an education process for users. The Slammer worm affected users both at home and in business. Malicious attacks remain a constant threat so long as computer technology influences more and more aspects of life.

While industry partners must take the lead in providing better security procedures, the public, in general, must take the initiative to demand the most secure products and systems. Passive approaches will not deter hackers from intruding systems; therefore, everyone must prepare and educate themselves on all possible vulnerabilities. The lessons learned from this attack must be taken seriously, and industry and the public must apply all new ideas and processes accordingly to increase protection.

1 Introduction

In today's world of advancing technologies and faster pace, more and more people develop a reliance on automated and computerized equipment and services. Virtually every aspect of a person's life can be managed or affected by computers. This ability has facilitated the lives of the majority of the population and increased the fortunes of so many. However, with this reliance comes never before seen dangers and threats. For every beneficial use of computer technology, there is always someone trying to exploit the system for his own benefit, often at the expense of innocent bystanders.

More than ever, computer hackers are attempting to infiltrate common programs, systems, and applications in order to locate personal information of others. Intruding into another user's system allows the hacker to steal any type of data, specifically information that will provide them with financial gain or often highly sensitive/classified materials. The common user rarely protects his data well enough to thwart any intruder, and more likely, the user seldom possesses the basic knowledge of how to protect himself.

Therefore, intruders continually develop new intrusion devices, such as viruses, worms, or Trojan horses. These devices, often in the form of emails or small programs, possess the capability to destroy networks and systems across the globe, and allow the intruder to ascertain all the information he could want without being traced. One such intrusion occurred earlier this year in January, and virtually shut down an entire continent's network systems. The SQL Slammer Worm not only proved how susceptible computers can be, but also served as an example of how defense technologies must continually be updated and improved to defeat evolving attacks.

2 Background

One example of a malicious attack is a computer worm. A worm is a program that makes copies of itself, i.e. from one disk drive to another, or by copying itself using email or any other communication method ("Computer Worm Grounds Flights, Blocks ATMs." 26 January 2003. URL: www.cnn.com/2003/TECH/internet/01/25/internet.attack. 15 March 2003). The SQL Slammer proved to be a potentially ruinous attack, and symbolized how much work still needs to be completed in order to fully protect systems.

In the early morning of January 25, 2003, the SQL Slammer worm attacked many global corporations by slipping through their firewalls that had left open Ports 1433 and 1434, or it was spread through the infected

correspondences from e-commerce partners. The Slammer worm was a self-propagating worm that exhausted network bandwidths. Fortunately, this worm infected only computers running MS SQL Server 2000 or MSDE 2000, and it never wrote itself to the user's hard drive ("F-Secure Virus Descriptions." 27 January 2003. URL: www.f-secure.com/v-descs/mssqlm.shtml 15 March 2003).

Corporations affected by this attack were forced to shut down internal operations for a day, if not more, in order to free their networks of the worm, which was flooding their intranets with a denial of service attack (Messmer, Ellen. "Next `Slammer' Could Be Worse." Network World. February 2003: 57).

In its basic form, Slammer randomly scanned, at high speeds, unpatched SQL Servers and any unpatched application using the licensed Microsoft Data Engine code. The worm exploited a flaw in Microsoft systems and also clearly proved that more attention must be paid to conducting fixes and providing them to users across the globe. As a result of its attacks against the unpatched SQL Servers, Slammer generated an enormous amount of User Datagram Protocol (UDP) traffic, which resulted in an almost 50% decline in Web site availability across the globe in a matter of hours. Slammer's denial of service attack was so severe in it early stages that even latency sensitive applications, such as voice over IP were severely affected (Messmer, Ellen. "Next `Slammer' Could Be Worse." Network World February 2003: 57).

The Slammer worm wreaked havoc on more than just corporations in one region; rather it had effects on a global scale, thus proving how devastating these attacks can be. For example, several financial institutions, including Bank of America Corp, who lost 13,000 automated teller machines alone, watched as the worm forced their automated teller machines to shut down as a result of the in-house servers that manage the machines succumbing to its intrusion ("Computer Worm Grounds Flights, Blocks ATMs." 26 January 2003. URL: www.cnn.com/2003/TECH/internet/01/25/internet.attack. 15 March 2003).

Stock exchanges in Asia, as well as some European governments reported disturbances. Closer to home, the United State's cyber attack first guard, the National Infrastructure Protection Center, failed to locate and quell the worm during its first hours. In the U.S., Federal agencies such as the Department of Defense, the State Department, and the Department of Agriculture exemplified how quickly the worm had spread. The lack of awareness proved to be the first fatal flaw in preventing Slammer from infiltrating thousands of systems.

The lack of awareness and failure to patch affected systems quickly resulted in the SQL Slammer Worm being dubbed as the most damaging Internet attack in 18 months, if not longer. A simple look at where the

worm's presence was felt: Asia, Europe, and North and South America, clearly shows that this attack could have been catastrophic.

3 Technical Aspects of the SQL Slammer

The SQL Slammer worm targeted specific programs and ports on Microsoft systems. For the most part it attacked systems running MS SQL Server 2000, along with systems using Microsoft Desktop Engine 2000, which is included in applications like Visual Studio, .Net, and Office XP Developer Edition (Vamosi, Robert. "SQL Slammer Slows Internet Traffic." 27 January 2003. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2909611,00.html 22 May 2003).

Microsoft's SQL Server 2000 contains two inherent buffer overrun vulnerabilities that allowed the Slammer worm to exploit the systems. These vulnerabilities allow an unauthorized user to hack into the system without ever having to verify his identification with the server, thus giving the hacker an unimpeded route to whatever information he might want. Success is realized when the targeted server becomes totally compromised (http://www.nextgenss.com/adisories/mssql-udp.txt15 March 2003). While Microsoft has offered fixes to these vulnerabilities, few users have incorporated them, thus leaving themselves open and vulnerable to any malicious attack.

To gain an understanding of how quickly the SQL Slammer worm spread across the world, Figure 1 below depicts the traffic patterns during its first three days. The peaks and valleys during the most devastating period of attack can be directly attributed to the opening of business on different continents. The Slammer worm clearly inflicted inconveniences on a worldwide scale.

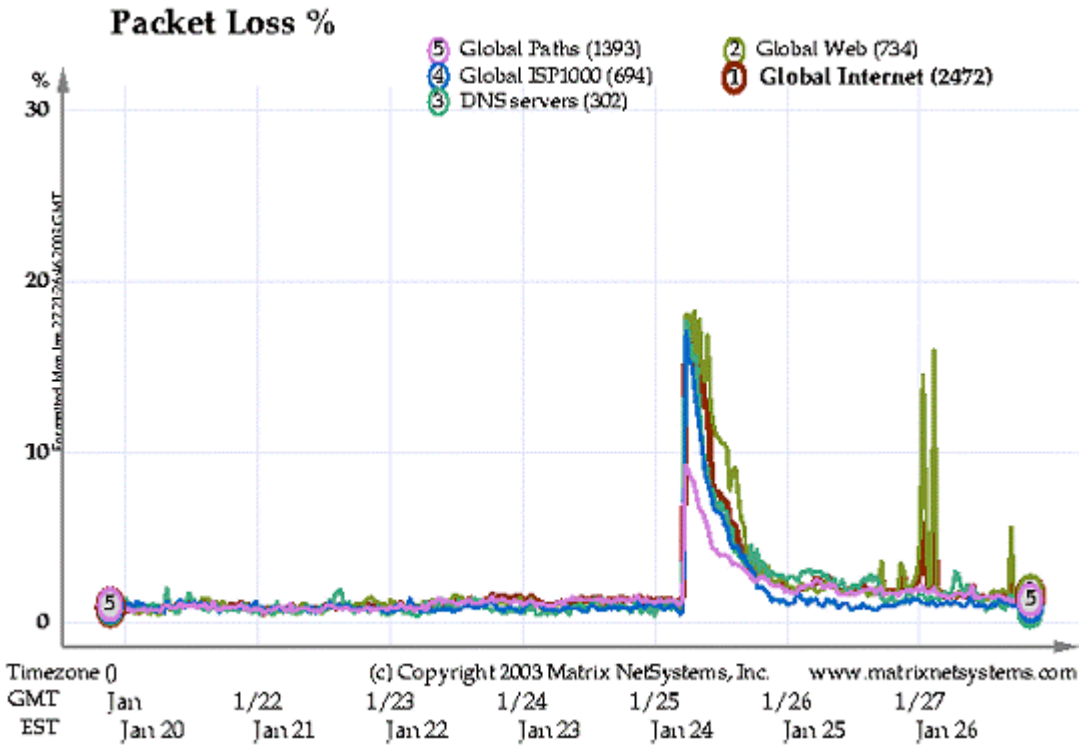

Figure 1: SQL Slammer Path
(Reference: "F-Secure Virus Descriptions." 27 January 2003.
URL: www.f-secure.com/v-descs/mssqlm.shtml 15 March 2003).

The SQL Slammer worm had been recognized, and security fixes had been released back in July 2002, which helps to explain why the activity prior to January 25th was rather stable, however, the worm still infiltrated enough unprotected systems, and once it did, it spread from system to system at a rate of doubling the number of computers it infected every 8.5 seconds in the first few minutes of its appearance, a rate of more than 55 million scans per second after about 3 minutes. This fantastic rate categorizes Slammer as a "Warhol" worm because it could infect the entire Internet within 15 minutes (Broersma, Matthew. "Slammer—The First `Warhol' Worm?" 3 February 2003. URL: http://news.com.com/2100-1001-983197.html 15 March 2003).

The concept of a "Warhol" worm has been debated for many years, and while still a theory, it receives more credence when attacks like the Slammer infiltrate vulnerabilities at such a rapid speed. The frightening dimension of this attack lies in the fact that users and computers affected by Slammer were fortunate because Slammer did not carry any malicious payload.

More specifically, the Slammer worm did not write itself to any disks, rather, it existed only in network packets and in running processes in infected computers, which is similar to some prior worm attacks. This

similarity to prior malicious attacks creates a greater frustration as to how something like this could happen twice.

After the worm entered the vulnerable system, its first objective was to ascertain addresses to certain system functions and then beginning an infinite loop to scan for other vulnerable hosts. The worm would employ random number generations to find IP addresses searching for vulnerable hosts, and to make detection more complicated, it would attempt new IP addresses in random sequence. This means that just one computer, with the proper Internet connection, could scan the entire Internet in 12 hours ("Advisory: SQL Slammer." http://robertgraham.com/journal/030126-sqlslammer.html 15 March 2003). A planned side effect of this attack involved the generation of a large amount of network traffic, leading to the buffer overflow (("F-Secure Virus Descriptions." 27 January 2003. URL: www.f-secure.com/v-descs/mssqlm.shtml 15 March 2003).

For those who failed to install the security patch released the prior year, the only ways to control Slammer were to block various SQL ports, or f for an infected system, the user could reboot the system. However, rebooting would not guard against any Slammer infection at a later time. Slammer's effects could have been more widespread had the random number generator designed into the worm not been flawed. Unable to all possible internet addresses, the worm possessed limits that spared many computers. And perhaps most fortunately, Slammer's own tremendous speed and aggressiveness caused its demise. Because the worm shut down so many networks so quickly, it was unable to operate at its highest potential.

4 Case Study: The Federal Government

While the SQL Slammer caused the majority of its damage in Asia, agencies across the United States felt its effects. While they all avoided receiving extremely significant damage, the worm left its mark and reminded officials of the need to bolster network and computer defenses, particularly in this era of global insecurity. Within various agencies, the worm caused high central processing unit usages on Microsoft Servers, either by slowing down or, in some cases, completely collapsing servers through the exploitation of known vulnerabilities (Yasin, Rutrell. "Agencies Thwart SQL Worm." Federal Computer Week. 27 January 2003. URL: www.fcw.com/fcw/articles/2003/0127/web-worm-01-27-03.asp 15 March 2003) Because the worm spread and caused the majority of its damage within five to eight hours of being launched, it served as a sign that the need for preventive procedure and plan must be drafted in each agency. Each agency must recognize that attacks will continue, and stopping them from causing any harm once will not protect them in the future. The best defense consists of constant updates and education.

An example of successful defense and preventive measures can be found by looking at the Department of Veterans Affairs. Running a 24 X 7 security operations center (SOC), the Department actively surveyed the situation and its defense capability reached its highest level at the most critical moments (Yasin, Rutrell. "Agencies Thwart SQL Worm." Federal Computer Week. 27 January 2003. URL: www.fcw.com/fcw/articles/2003/0127/web-worm-01-27-03.asp 15 March 2003). Having this pre-attack system potentially saved the Department not only millions of dollars, but also preserved the integrity, confidentiality, and availability of sensitive information.

The Department of Defense faced similar circumstances, and ultimately avoided any real damage. As a result of possessing the proper configure management tools and protocols, such as firewalls and virtual private networks, the Department of Defense efficiently protected one of its larger networks deployed throughout North America and Asia. These tools, properly managed and configured, serve as an effective means for protecting critical systems, and they serve as an example for those unfamiliar with malignant attacks as how to protect oneself.

5 Lessons Learned

Malicious attacks come in a variety of forms, some of which security providers and designers are prepared for. However, preparation does not always lead to proper prevention. As Microsoft learned during the Slammer Worm, attempts at moderate upgrades in protection will not subdue the most vicious attacks.

In 2002, Microsoft laid the groundwork for their security program after several malicious attacks diminished the corporations' systems. Microsoft chief Bill Gates challenged his employees to make privacy and security their chief concerned, and the company as a whole reduced its product development so that resources could be allocated to security training and prevention (Lemos, Robert. "Decoding the Lessons of Slammer." 04 march 2003. URL: http://news.com.com/2008-1082-990757.html 15 March 2003). However, all of this focus could not prevent Slammer from not only infecting Microsoft users, but Microsoft itself.

The question remains, what can Microsoft and other software development organizations do to ensure that their systems will combat and deter malicious attacks? For one thing, these corporations can begin to divert some of their security focus from their operating systems, and pay closer attention to various software products that consumers will place on their computer, such as SQL Server in the Slammer case. Software developers must begin to pay less attention to production and marketing and begin to focus on maximizing reliability and personnel training (Tolly, Kevin. "SQL Slammer Attack Reveals Reliability Reality." Network World. February 2003: 20). Simply put: the key principle for technology producers should be no

major crashes! This attack could have been prevented had managers of Microsoft systems applied the latest security fixes.

Apathy should never play a role when securing computer systems. There is no excuse as to why a fix was not implemented when received. System operators' unwillingness to apply such fixes served as one reason why Slammer infiltrated so many systems. This unwillingness can be attributed to several factors, including distaste for installing the frequent number of required updates; assumptions that updates could cause more bugs than they fix; and desire to avoid the inevitable system disruption caused by implementing an update (Brander, Scott. "Familiar Welcome to the New Year." Network World. February 2003: 24). These reasons do not adequately support reasons why Slammer was able to affect so many systems. Questions and assumptions like the ones above should not enter into administrators' minds; rather, protecting the systems to the best of their ability should be a duty not a chore.

Perhaps one thing that producers like Microsoft could do to ensure consumers and global corporations alike protect their systems at the highest level, is to focus more attention on educating the public. Sending users patches and security service packs will solve the problem for a small number of people; however, most users simply do not understand the harm that a virus can cause and/or the need for proper patch management. And often, the service packs can cause more difficulties and make a system more vulnerable if not properly administered. If Microsoft, for example, offered personal security management courses or easy to read documentation or books to the general public, and some corporations for that matter, the first step in preventative maintenance would be complete. Like many other aspects of life, education in security management can go a long way toward alleviating a serious problem.

The Slammer worm affected corporations more than personal computers during its peak periods. Therefore, a priority for software development companies should be to work with companies and assist in the development of proper security plans (Lemos, Robert. "Decoding the Lessons of Slammer." 04 march 2003. URL: http://news.com.com/2008-1082-990757.html 15 March 2003). System security plans, if maintained and updated frequently, can serve as the first line of defense versus an intrusion. Much like the value of educating the common user, assistance with corporations for proper security plan development would ensure proper training and give employees the chance to ask any questions for issues that they do not understand. If companies developed system security plans that employees were required to read and sign, familiarity of the system by the company as a whole would increase, and the chance of security weaknesses being opened would decrease.

The Slammer worm also clearly exploited the deficiency in software management and security assessment tools available on the market. Despite the daily possibility of malicious attacks and system intrusions, software developers have failed to create vulnerability tools that allow the customer to protect his system fully and easily (Messmer, Ellen. "Next `Slammer' Could Be Worse." Network World. February 2003: 57). Customers often do not have the capacity to assess their system and determine which vulnerabilities have been patched or what equipment needs restored. Producers often ignore this fact, or when they do release a tool, there is little instruction on how to utilize it effectively.

Most importantly, perhaps more so than educating customers, both individuals and corporations, and building tools, software producers must listen to their users because in all practicality, the users have the most hands-on experience. If the producers listen to the security needs their users, they can address the most problematic issues proposed by users, thus alleviating customer dissatisfaction, and at the same time, improving the quality of their product. For example, Microsoft knows that it must improve its capacity to address security issues before delivering a product; must continue to review security issues of a product after delivery; must continue to release *high quality and effective* patches; and it must ensure that patch deployment continues to become easier (Lemos, Robert. "Decoding the Lessons of Slammer." 04 march 2003. URL: http://news.com.com/2008-1082-990757.html 15 March 2003).

Rather than placing all of the blame on the technology producers, perhaps some fault lies in the users themselves. While it is true that the majority of users truly do not understand how to protect themselves, like with any product, users should expect and demand the best. Users should make it clear to producers that they want resources spent on developing the highest product standards, and investments made in testing and integration (Gibbs, Mark. "Laying Blame when Things Are Going Wrong." Network World February 2003 58). Users would not buy a car that they knew failed a safety test, so why risk privacy and security on a computer system that did not receive proper testing.

6 Conclusions

In the world of computer and information technology, many perils and questions exist. As technology permeates every aspect of daily and business life, these perils will increase. The SQL Slammer provided a concrete example of how quickly an attack can spread into a variety of different cultures, economies, and businesses. Computers have interconnected the entire world, which makes detecting and preventing these outbreaks all the more difficult.

With the increasing reliance on computer technology, effective computer security is essential. The SQL Slammer worm showed that security is still

not taken as seriously as it needs to be. As mentioned earlier in the paper, users and systems were fortunate that this worm did not carry any malignant code, otherwise, the damage would have been catastrophic. To protect computer systems successfully, both the technology producers and the users must play important roles.

From the production viewpoint, more attention must be placed on creating secure products. They must spend the extra research and development dollars that will ensure vulnerabilities receive proper attention. This aspect could be more important in the long run than large product marketing campaigns, because it would take only one large attack to cost the producer not only millions of dollars, but more importantly, the producer's reputation would be destroyed.

Software producers need to educate their own employees who can provide customer support, but more than that, they need to provide training and guidance to those who purchase their equipment. Educating corporations on proper detection and security plans will ensure that entities systems will receive the most attention possible. For the personal user, software developers must clearly define malicious attacks, such as SQL Slammer, and make the public aware of the dangers. The public generally does not comprehend the danger involved in computer technology, and the only people to educate them are the information technology experts.

From the user standpoint, not having the ability to understand the dangers of the SQL Slammer is not a reason to sit by and let it happen continuously. Even those that do not grasp computer technology must recognize the threat that exists. Therefore, users must implore those that possess the proper knowledge, the computer technology industry, to increase their standards and provide users with the strongest defense mechanisms. Users must treat their computers like any other product, that is to say, they must ensure its security because on that computer is often very private information.

The SQL Slammer worm served as a wake-up call for computer experts across the globe. Malicious attacks will threaten computerized systems for as long as computers exist, therefore, rather than reacting when each attack occurs the attack must be met with a proactive approach that will detect all assaults prior to any serious damage. Security is paramount when handling computer technology, and it should never serve as the second fiddle.

Works Cited

Bradner, Scott. "Familiar Welcome to the New Year." Network World. February 2003: 24.

Broersma, Matthew. "Slammer—The First `Warhol' Worm?" 3 February 2003. URL: http://news.com.com/2100-1001-983197.html 15 March 2003.

Gibbs, Mark. "Laying Blame when Things Are Going Wrong." Network World February 2003 58.

Lemos, Robert. "Decoding the Lessons of Slammer." 04 march 2003. URL: http://news.com.com/2008-1082-990757.html 15 March 2003

Messmer, Ellen. "Next `Slammer' Could Be Worse." Network World. February 2003: 57.

Tolly, Kevin. "SQL Slammer Attack Reveals Reliability Reality." Network World. February 2003: 20.

Vamosi, Robert. "SQL Slammer Slows Internet Traffic." 27 January 2003. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2909611,00.html 22 May 2003.

Yasin, Rutrell. "Agencies Thwart SQL Worm." Federal Computer Week. 27 January 2003. URL: www.fcw.com/fcw/articles/2003/0127/web-worm-01-27-03.asp 15 March 2003.

"Advisory: SQL Slammer." http://robertgraham.com/journal/030126-sqlslammer.html 15 March 2003.

"Computer Worm Grounds Flights, Blocks ATMs." 26 January 2003. URL: www.cnn.com/2003/TECH/internet/01/25/internet.attack. 15 March 2003.

"F-Secure Virus Descriptions." 27 January 2003. URL: www.f-secure.com/v-descs/mssqlm.shtml 15 March 2003.

http://www.nextgenss.com/adisories/mssql-udp.txt15 March 2003.