RPC/DCOM EXPLOITS DETECTION AND NOTIFICATION

HALIM BIN AYUB

A report submitted in partial fulfilment
of the requirements for the award
of the degree of
Bachelor of Computer Science (Computer Systems and Network)

Faculty of Computer Systems & Software Engineering
University College of Engineering & Technology Malaysia

NOVEMBER, 2005

ABSTRACT

Nowadays, the usages of the internet have grown rapidly. But internet also is exposed to any kind threat that can cause to many kind of damage. One (1) example of the internet threat is the network worm. The famous example of network worm is Msblaster worm. Msblaster attack the Microsoft windows operating system especially Windows XP and Windows 2000. Msblaster used the vulnerabilities in RPC DCOM architecture to exploits to the operating system. The main problem of the Msblaster is it can craft the victim's IP addresses and try to exploits the computer with that IP addresses. This has made the network traffic become high and make the internet become unreachable in certain organization's network. Although the attack of Msblaster worm have decreased, but there is a potential of the worm to attack again in the future if the worm is not fully remove in the network. The purpose of this project is to detect the computer that have been infected by this worm and ask the user to remove the worm. The research and analysis of current type of attacks was done to get better understanding of the system. The SDLC methodology was used as the project development methodology. This project was developed using Microsoft Visual Basic 6.0 and using the design of client server model as the project architecture. As the result of the successful of this project, we can ensure that the worm is totally removed from our network.

ABSTRAK

Pada masa kini, kegunaan internet telah berkembang dengan pesat sekali. Tetapi internet juga terdedah kepada ancaman yang boleh menyebabkan bermacam jenis kerugian. Salah satu contoh daripada ancaman internet ialah cecacing rangkaian. Contoh cecacing rangkaian yang terkenal ialah cecacing Msblaster. Msblaster menyerang sistem operasi Microsoft Windows terutama Windows XP dan Windows 2000. Msblaster menggunakan kelemahan daripada rekabentuk RPC DCOM untuk memecah masuk ke dalam sistem operasi. Masalah utama Msblaster ialah ia boleh menjana alamat protokol internet dan cuba untuk memecah masuk ke dalam komputer dengan menggunakan alamat protokol yang telah dijana sebelum ini. Ini boleh menyebabkan trafik rangkaian menjadi sesak dan menyebabkan internet tidak boleh dicapai oleh sesetengah rangkaian organisasi. Walaupun serangan cecacing Msblaster telah berkurang, tetapi terdapat potensi untuk cecacing berkenaan menyerang kembali jika cecacing berkenaan tidak dibuang sepenuhnya dari dalam rangkaian. Tujuan projek ini adalah untuk mengesan komputer yang dijangkiti cecacing ini dan mengarahkan pengguna membuang cecacing berkenaan. Kajian dan analisis daripada jenis-jenis serangan pada masa kini adalah dilakukan untuk mendapatkan penjelasan yang lebih jelas mengenai system yang akan dibina. Metodologi SDLC digunakan sebagai kaedah pembangunan sistem. Projek ini dibangunkan dengan menggunakan Microsoft Visual Basic 6.0 dan rekaan model 'client server'. Hasil daripada kejayaan projek ini ialah kita dapat memastikan yang cecacing ini telah dibersihkan sepenuhnya dari rangkaian kita.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATION

R2DN	-	RPC/DCOM Exploits Detection and Notification
RPC	-	Remote Procedure Call.
DCOM	-	Distributed Component Object Model.
Msblaster	-	Network worm.
LAN	-	Local Area Network
IP	-	Internet Protocol
DoS	-	Denial of Service
DDoS	-	Distributed Denial of Service

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Microsoft has officially released the Windows XP operating system at October 25, 2001. The high reputation on Microsoft products have made Windows XP used by most computer in this world. The vendor of notebook like Acer and Hp-Compaq also recommended the use of this operating system to user and implemented this operating system to most of their notebook.

Windows XP have offering the user to the new friendly interface with the multimedia features set. This is a total different to be compared with the other previous version of windows. All this new features have made the user very interest to change their operating system to Windows XP and make this giant software company have won to dominate the operating system market.

The success of Windows XP was not long because the hackers have identified the weakness of this operating system. The hackers seem does not take too much time to find the vulnerabilities that lay inside Windows XP architectures.

The first worm that released to exploits the vulnerabilities in Windows XP was the *W32.NIMDA.A* that also known as nimda. At this time, the credibility of Microsoft Corporation in develop the operating system have been questioned again by the most user. The promise of the stability and reliability in Windows XP does not mean anything without the high security in that operating system. The hackers seem to give a warning directly to the Bill Gates especially about the domination of the Microsoft product in the IT markets. They think that Microsoft is likely just aim to make money by dummying the user with the operating system that have rich multimedia feature instead of tighten the security and reliability of their operating system.

There is another alternative operating system instead of using Microsoft product. The open sources operating system like Red Hat, Suse, Mandrake and many more were very popular operating system nowadays. Although open sources operating offering the more reliable and lower price operating system compared to Microsoft product but it does not have attracted too many user to use this products. Maybe the user does not have much exposure and knowledge about this operating system.

We do not have the right to force user to change to other operating system. We just can give an opinion about the operating system and it is up to the user what they like to use. Even though we have facing too many problem that have arise with Microsoft product, but only the user can make a choice what is the best operating system for them to use. What we can do now is just take an action that needed to minimize the damage to our network if this operating system is being attacked again.

1.2 Problem Statements

The attack of the network worm especially at University College of Engineering and Technology Malaysia (KUKTEM) network environment have give a great impact to the flow of internet and intranet performance in KUKTEM. Instead of affecting the personal computer, the worm also has made the network traffic in intranet KUKTEM become unstable. After affecting a computer, the worm will try to exploits other computer by broadcast the packet to the IP addresses that have been generate by its algorithm. The more computers infected, more computers will broadcast the packet and this will create a high network traffic that will make the internet become unreachable.

Not many the ICT staff can do to prevent this worm from spreading and make network unstable if most of the computer are still infected with the worm. The attacked of the worm have made our wireless network become unreliable. The only thing that can be done to revive the network to their optimal performance is to clean the entire worm in the personal computer.

The users know about this worm, but the only problem is there is a certain user that does not know whether their computer is being infected by the worm or not. Although the ICT centre have provide the removal tools and security patch for Windows XP, but without having a good knowledge about this worm, the problem will still arrive.

The user should be notified if their system is infected by worm. The user also should be asked to clean the worm and patch their system to avoid infection again. By this reason, a scanner is used to detect which computer is being infected by the worm especially Msblaster worm.

1.3 Objectives

The system that being developed is named RPC DCOM exploits detection and notification (R2DN). There are several objectives that going to be archived when developing the system. Stated below are the project objectives:

(i) Listen to the computer port for any attempt of attack.

(ii) Find information about the computer that trying to initiate a connection and save the information in a log file.

(iii) Send message to the computer that try to make a connection to the port.

1.4 Scopes

The system can listen to the port 135 and 445 that is commonly known to be attacked by most of the worm. The user also can set a port to be listening by the system. The system can detect the computer that trying to initiate a connection to the computer and save the information about the computer into a log file. After that, it will notify the user that their computer is possibly having a worm ask them to remove the worm from their computer.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter reviewed about three (3) things that were the types of attack, RPC/DCOM vulnerabilities and Msblaster worm. All this things was related to the network worm that is very popular nowadays.

The types of attack discussed about two (2) most common attack that were viruses/worms and DoS attack. The combination between these two (2) types of attack has the result of the creation of the network worm.

RPC/DCOM vulnerabilities were the weakness of the windows XP. In the year 2001 to 2004, almost all the network worm uses this vulnerability to exploit to the computer to spread the worm.

Msblaster worm is one (1) of the examples of network worm. This worm is very popular worm that use the vulnerabilities in the windows XP architecture. Msblaster also have the ability to make the infected computer to launch the DDoS attack to Microsoft Windows update website.

2.2 Types of Attack

There are many types of attack that have been invented today to exploit and make damage to the network or to the computer itself. The styles of the attacks are different and it depends on the purpose of attack. Computer users actually should be ready for any types of attack that can occur in the network.

Actually anyone can launch an attack to our network. Nowadays, there are many attack tools available in the internet and can be easily download by anyone. Someone who does not like our organization can easily download the attack tool and used it to attack our computer network. There is also someone who called as a script kiddie that we should be aware. "Script kiddie is someone who attempts to disrupt computer systems by running available tool that designed to crack computer systems (Liska, 2003)." Actually script kiddie does not necessarily understand the program or script that they being used. Their goal is just to make as much damage as possible. "It is reported that in February 2000, a script kiddie manage to knock down eight of the largest website offline for several hours by using a tools for launching the Distributed Denial of Services (DDOS) attack (Vamosi, 2004)."

The network administrator should know all information about any types of attack. They should learn as deep as possible about the different types of attack and what the attack is designed to do. The better attack types are understood, the easier it will be to defend against the incursion.

Two (2) most common types of attack are the viruses/worm and the DoS attack. These two (2) types of attack were related to the network worm such as Msblaster, Sasser and many more.

2.2.1 Viruses and Worm

2.2.1.1 Viruses

There are many definitions about the computer virus. The general definition about the virus is a program or programming code that being used to infect a computer.

"Definition of the virus is a parasitic program written intentionally to enter a computer without the user's permission or knowledge. The word parasitic is used because a virus attaches to files or boot sectors and replicates itself, thus continuing to spread. Though some viruses do little but replicate, others can cause serious damage or affect program and system performance (Cohen, 1994)."

The Chernobyl virus is the first virus known to have the power to damage computer hardware. Chernobyl virus is known as CIH. "CIH has been written by Chen Ing Hau, computer engineering student from Taiwan. Different from the ELK Cloner that spread via diskette, CIH virus is spread via CD. CIH has many variant. The most common version is *CIH 1.2* that activate it payload on April, 26 1998. April, 26 is the birthday of the author and also the thirteen (13) anniversary of the disaster at the Chernobyl nuclear reactor in Ukraine. CIH is a space filler virus referring to its ability to clandestinely take up file space on computers. The activated viral strain attempts to erase the hard drive and overwrite the system's BIOS as well (Yamamura, 2004)." CIH is very dangerous because it has ability to wipes out the hard disk, and then tries to overwrite the computer's BIOS chip. Once the BIOS are overwritten, user will be unable to use the computer at all. Repair involves physically removing the BIOS chip and replacing it with a fresh one (1). On some computers, the BIOS chip is not removable, so it can only be replaced by swapping the entire motherboard.

A virus program has to be run before it can infect the computer. Viruses have a ways to make sure that this happens. They can attach themselves to other programs or

hide in code that is run automatically when users open certain types of file. Sometimes virus can exploit security flaws in the computer operating system to run and to spread itself. User might receive an infected file in an email attachment, in a download from the internet, or on a disk. As soon as the file is launched, the virus code runs. Then the virus can copy itself to other files or disks and make changes to the computer system.

2.2.1.2 Worm

Worm is often being confused with viruses. Worm and viruses have a very different style of attack. The only similarity about this two (2) treats is both them can cause lost a million and even billion dollars. Do not confuse with worm and WORM. WORM that writing in capital letter is an acronym for Write Once Read Many that is an optical disk technology that allows you to write data onto a disk just once. After that, the data is permanent and can be read any number of times.

Worm that being discuss here is a program or code that can replicate itself from system to system. Worm do not require assistance to spread, instead it can automatically email itself to other user, copy itself through network or even scan host for vulnerabilities and attack them.

"The first worm code is written by two Xerox Palo Alto Research Center (PARC) researchers at the year 1978. The worm that been created by that researchers can search out other computer hosts, then copies itself and self destructs after a programmed interval (Palke, 2000)."

The first attack of the worm over internet is Morris Worm. "The worm has been written by Robert Tappan Morris Jr at the Massachusetts Institute of Technology (MIT) Artificial intelligence Laboratory. It was released on November 2, 1988 and quickly infected a great many computers on the Internet at the time. Morris then convicted

DDoS (Distributed Denial-of-Service) attack is an enhance version of DoS attack. DDoS uses combination of the technique in DoS attack. It is very effective to make a target website offline. "DDoS attack begins by exploiting vulnerability in one (1) computer system and making it the DDoS master. It is from the master system that the intruder identifies and communicates with other systems that can be compromised (Patrikakis *et al.*, 2004)." The intruder loads cracking tools available on the Internet on thousands of compromised systems. With a single command, the intruder instructs the controlled machines to launch one (1) of many flood attacks against a specified target.

Refer back to the DoS attack at pizza delivery services that have been describe before. Imagine the hacker secretly plants his program onto many computers on the Internet. This would have a bigger impact because there would be more computers calling the same pizza store. It would also be more difficult to locate the attacker, since the program is not running from the attacker's computer. The attacker is only controlling the computer that secretly had the program installed. This is an analogy for a Distributed DoS (DDoS) attack.

There are a large number of known vulnerabilities in network software and protocols existed. DoS can be achieved in a number of ways.

(i) Sending enough data to consume all available network bandwidth (Bandwidth Consumption).

(ii) Sending data in such a way as to consume a resource needed by the service (Resource Starvation).

(iii) Exercising a software bug that causing the software running the service to fail (Programming Flaws).

(iv) Malicious use of the Domain Name Service (DNS) and Internet routing Protocols.

2.2.2.1 Bandwidth Consumption

Attackers consume all the available bandwidth on a remote or local network. The victim's network connection is saturated by the large volume of traffic generated by the attacker. There are two (2) ways in which this can be achieved.

Firstly is larger pipe. The attacker has a high speed or much faster network connection than the victim. Secondly is amplification. Attackers amplify their DoS attack by engaging multiple sites to flood the victim's network. Using this process, attackers with a slow twenty eight (28) kbps connection can completely saturate a five hundred and twelve (512) kbps connection.

2.2.2.2 Resource Starvation

This type of attack targets system resources on the victim's computer rather than network resources. In doing this the target system is no longer able to operate normally and provide a service across the network.

"On entering a system the attacker will abuse their allocated quota of system resources to crash the machine. The target system may crash or be forced to reset due to the file system becoming full, processes hanging or CPU utilization at hundred (100) percent (Kabay, 2001)." Alternatively, if the attacker has managed to gain unauthorized access, they may choose to simply disable the running service by executing a kill command.

2.2.2.3 Programming Flaws

Operating systems, applications or even embedded software have the potential to fail while handling exceptional conditions. These conditions usually result when a user

sends unintended data to the program. "Attackers can abuse this vulnerability to send non-compliant packets of data, in an attempt to create a buffer overflow condition and crash the application. For specific applications that reply on user input, attackers can send large data strings thousands of lines long. A service that provides the application such as web or ftp running a service with a known flaw could be exploited and cause that service unavailable (Smithline, 2005)."

2.2.2.4 DNS Attacks

"DNS attacks involve compromising a Domain Name Server (DNS) and convincing it to cache bad, or incorrect address information. The DNS protocol is inherently vulnerable to this style of attack, due to the weakness of its sixteen (16) bit transaction IDs, used during communication with remote systems. When the DNS performs a lookup, it will return the wrong IP address for the domain name, redirecting it to a black hole, or the attacker's site (Stewart, 2003)." The attacker's site can then pose as the victim's site.

The end-user has no knowledge that they are connected to the wrong website. Since the victim is completely uninvolved in the attack, they have no knowledge traffic intended for their site is being sent elsewhere. This is known as DNS cache poisoning as outline in Figure 2.1.

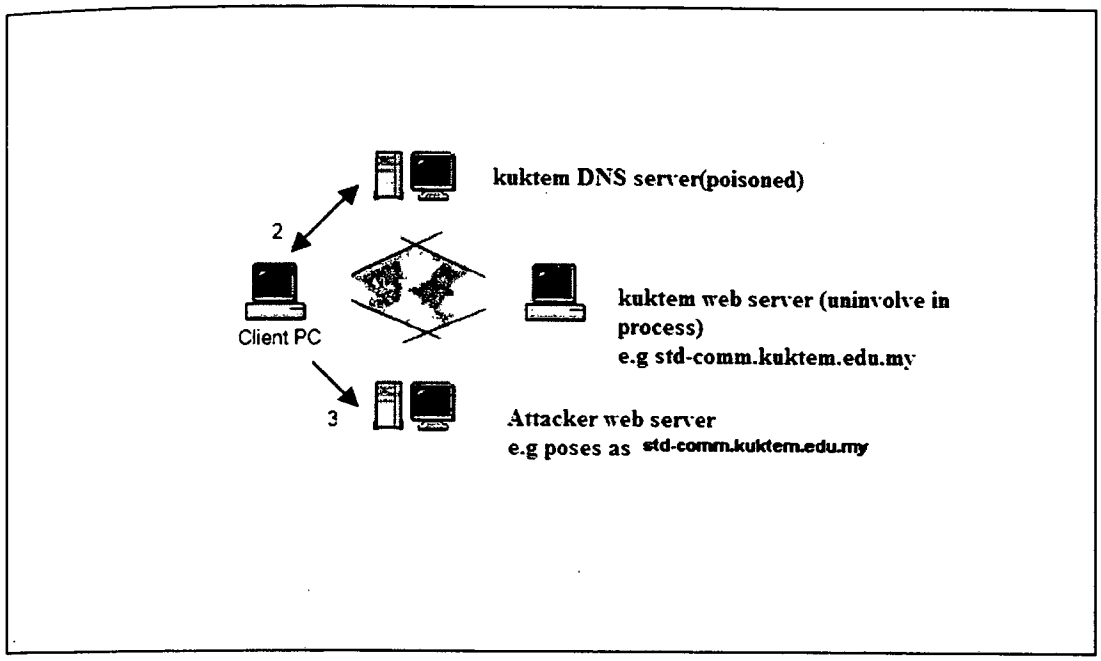

Figure 2.1: DNS cache poisoning.

The attack that illustrated in Figure 2.1 is described as below:

(i) Client PC requests std-comm.kuktem.edu.my. The browser tries to resolve IP from KUKTEM DNS server.

(ii) Cache is poisoned and returns IP for hacker's website.

(iii) User is directed to hacker website that posing as an exact copy of std-comm.kuktem.edu.my.

(iv) Hacker runs background scripts in website to send sensitive information to an inconspicuous email address.

(v) Hacker checks email account and extracts information as needed.

2.2.2.5 Distributed Denial of Service

"A DDoS attack is one (1) technique in which an attacker install daemons on large number of compromised hosts. At a later point, the attacker sends a request to the

daemon asking it to begin flooding a victim with various types of packets. The ensuing massive stream of data overwhelms the victim's hosts or routers, rendering them unable to provide a service (Cisco, 2004)." Thus DDoS attacks create large scale bandwidth consumption conditions. The first step for any DDoS attacker is to target and gain administrative access on as many systems as possible. The process can be divided into the following steps, in which the attackers:

(i) Initiate a scan on a large number of hosts probing for vulnerabilities.
(ii) Compromise the vulnerable hosts to gain access.
(iii) Install the DDoS tool on each host that will act as DoS agent.
(iv) Use the compromised hosts for further scanning and compromising.

After gaining access to a large number of systems, attackers will upload their chosen DDoS program to each zombie. At this point the attacker is poised to launch the attack whenever they wish. The compromised machines have no knowledge they are about to participate in a large scale attack and the attacker is completely removed from any trace attempt. All flood traffic will be generated from these zombie machines. The Figure 2.2 illustrates this process, showing multiple system compromising and the final assault.

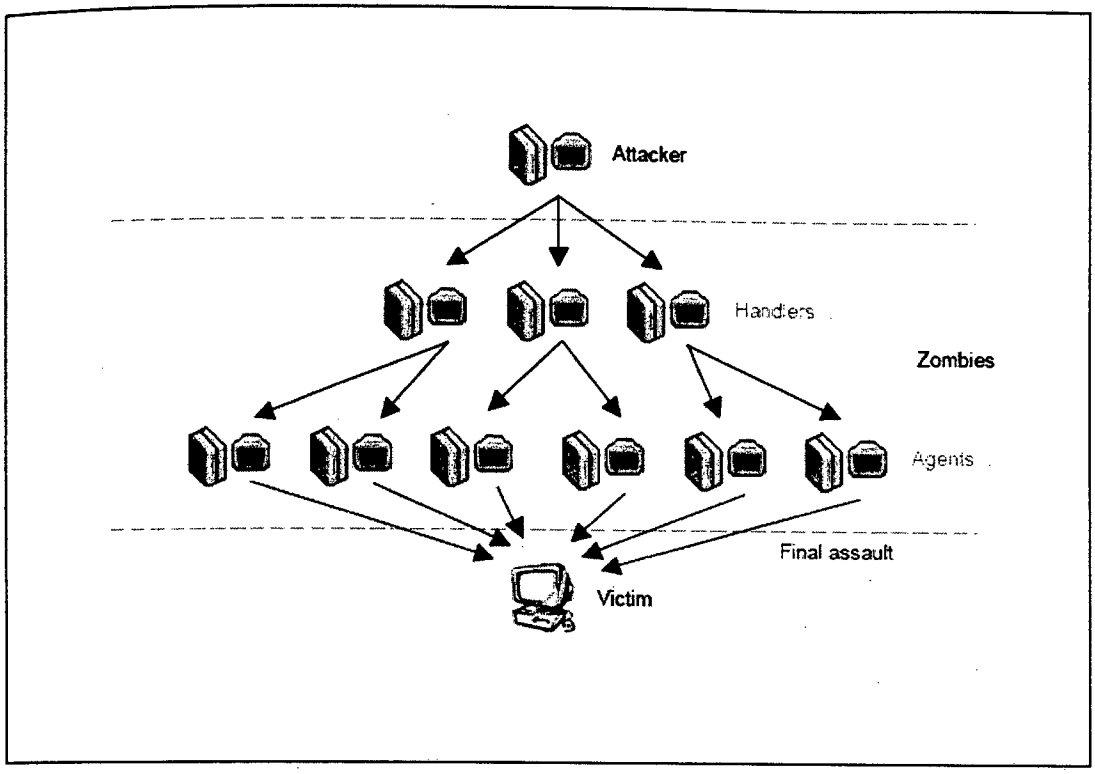

Figure 2.2: The DDoS attack

A handler is a compromised host with a special automated program running on it, scanning for more vulnerable systems. Each handler is also capable of controlling multiple agents. An Agent is a compromised host that has the chosen DDoS tool installed. Each agent will be responsible for generating a stream of packets directed toward the victim. The number of DDoS tools grows almost monthly. "Some popular DDoS tools that available today are Trin00, TFN, TFN2K and Stacheldraht (Dietrich *et al.*, 2000)."

2.2.3 The Worm and DDoS

The term network work is popular nowadays. The network worm has the characteristic of worm and DoS attack. Network worm have two (2) purposes that is

infecting the personal computer and also launching the DoS/DDoS attack. The most popular network worm is Msblaster.

The Msblaster worm infects Windows XP and Windows 2000 machines, taking advantage of a known vulnerability in the DCOM (Distributed Component Object Model) interface, which handles messages sent using the RPC (Remote Procedure Call) protocol. The vulnerable systems are connected to the Internet and can be compromised without any interaction from the user.

Msblaster not only causes problems on the infected personal computer, but attempts to use the machine as a DoS zombie in a distributed attack against Microsoft Windows Update website. The *windowsupdate.microsoft.com* domain is targeted, preventing Microsoft from simply changing the address of the domain to sidestep the problem. So far the site has withstood the attack and users have been able to download Msblaster patch software from it. This recent attack proves that DoS is still a favorites tool in the underground community. Since the DDoS tool was so easily available, the attackers simply choose to bolt on this feature to their virus code. It is theorized that all future network worms will include some form of DoS mechanism.

2.3 RPC/DCOM Vulnerabilities

DCOM or Distributed Component Object module is a new protocol that being implemented in the windows XP operating system. With the recent exploits by the Msblaster worm, there are many security flaw have been discovered and most of the vulnerabilities is related in the way RPC and DCOM being implemented in the most version of windows operating system especially Windows XP .