GIAC Incident Handling and Hacker Exploit Practical
Version: 3

Using Windows Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) Vulnerability, Exploited by MS Blaster worm to generate an attack via unauthorized Wireless network access.

Yehia Mohamed Mohamed Fathi
CCNA, NCSA, MCP, CCSA
April 5, 2004

Table of contents:

Introduction

MSblaster worm is considered the most famous exploit that exploited the Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) buffer overflow windows vulnerability since August 2003. That exploit will be discussed in this practical paper, showing how unauthorized wireless network access is used as a backdoor for the propagation of such a worm.

1. Statement of Purpose:

The purpose of this paper is to describe how Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) buffer overflow windows vulnerability is used to be exploited by the Blaster worm using backdoor wireless network access. This attack did not happen in the real life, but still possible to happen in any large organization.
This paper will describe the details of the exploit, the platforms and environments used, also will describe stages of the attack and incident handling process in response to this incident.

The attacker is a fictitious person, who is planning to attack a large bank causing a great harm to that bank; he is not going to steal money but will cause the bank to loose a large amount of money via business paralysis and gaining bad reputation in the market.
We shall name the attacker “Mr. Bad Guy” and the Bank will be “Victim Bank “.
Mr. Bad Guy who is the owner of a network security consultant company; he requested to take a loan from that bank for expanding his small company, the loan was taken but he failed to pay back the money to the bank in the required date due to bad market conditions and the bank refused to give him an additional allowance period. The bank took the decision to take over Mr. BadGuy Company causing him to loose all his money.

Mr. Bad Guy was involved in a project to the bank three months ago; he knew a lot of the bank network environment, so he started to think how to take his revenge by causing that bank to loose money and reputation.

During that time W32.Blaster.worm was spreading widely on the internet causing great harm to organizations, so Mr. Bad Guy decided to use such worm to take his revenge.

2. The Exploit

What is a worm?

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place via network connections or email attachments. [1]

Name:

W32.Blaster.Worm is a worm that caused a great damage to most organizations; it has more that one alias by Antivirus vendors, it is known as: [2], [3], [4]

a. Win32.Lovesan (KAV)
b. W32/Lovsan.worm (McAfee)
c. W32/Blaster-A (Sophos)
d. W32.Blaster.Worm (Panda – Symantec)
e. Win32.Poza (Computer Associate)
f. Worm/Lovsan.A (F-Secure)
g. WORM_MSBLAST.H (Trend Micro)

For this paper we shall refer to that exploit by W32.Blaster.Worm
W32.Blaster.Worm is a worm that exploits the DCOM RPC vulnerability - (will be described later in details in Protocols/Services/Applications section)-(described in Microsoft Security Bulletin MS03-026) using ports TCP 135, TCP 4444, UDP 69. The worm also attempts to perform a Denial-of-Service attack on Windows Update internet site .This is an attempt to prevent users from applying a patch on their systems against the DCOM RPC vulnerability. [5]

CVE References: CAN-2003-0352

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0352

Operating System:

W32.Blaster.Worm can affect un patched windows operating systems not installing Microsoft security Patch **KB823980** [5], these operating systems are:

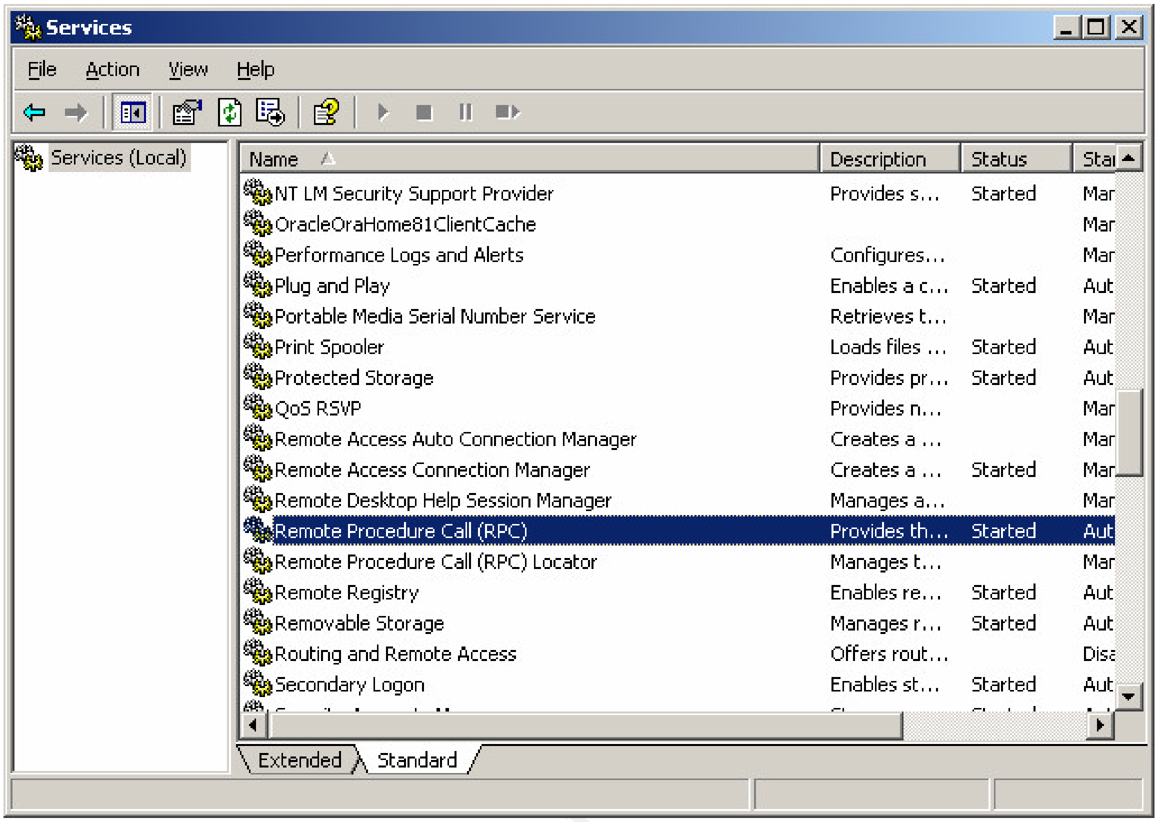
- Windows NT 4.0
- Windows NT 4.0 Terminal Services Edition
- Windows 2000
- Windows XP
- Windows Server 2003

Protocols /services/Applications:

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

What is DCOM RPC Vulnerability?
Before talking about the vulnerability let us first know what **RPC** is, (RPC) stands for Remote Procedure Call which is a protocol used by the Windows operating systems. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The protocol itself is derived from the Open Software Foundation (OSF) RPC protocol, but with the addition of some Microsoft specific extensions.
Also we need to understand what **DCOM** is, (DCOM) stands for Distributed Component Object Model which is a protocol that enables software components to communicate directly over a network in a reliable, secure, and efficient manner. Previously called "Network OLE," DCOM is designed for use across multiple network transports, including Internet protocols such as HTTP. DCOM is based on the Open Software Foundation's DCE-RPC spec and will work with both Java applets and ActiveX® components through its use of the Component Object Model (COM).

After describing what are DCOM and RPC, let us highlight the vulnerability found, There is vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed Component Object interface with RPC, which listens on RPC enabled ports. This interface handles DCOM object activation requests that are sent by client machines to the server. By default, the RPCSS service is enabled. A remote attacker could establish a connection and send a malformed RPC message to overflow a buffer and execute arbitrary code on the system with Local System privileges.
The attacker would be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges. [5]



Name	Description	Status	Sta
NT LM Security Support Provider	Provides s...	Started	Mar
OracleOraHome81ClientCache			Mar
Performance Logs and Alerts	Configures...		Mar
Plug and Play	Enables a c...	Started	Aut
Portable Media Serial Number Service	Retrieves t...		Mar
Print Spooler	Loads files ...	Started	Aut
Protected Storage	Provides pr...	Started	Aut
QoS RSVP	Provides n...		Mar
Remote Access Auto Connection Manager	Creates a ...		Mar
Remote Access Connection Manager	Creates a ...	Started	Mar
Remote Desktop Help Session Manager	Manages a...		Mar
Remote Procedure Call (RPC)	Provides th...	Started	Aut
Remote Procedure Call (RPC) Locator	Manages t...		Mar
Remote Registry	Enables re...	Started	Aut
Removable Storage	Manages r...	Started	Aut
Routing and Remote Access	Offers rout...		Disa
Secondary Logon	Enables st...	Started	Aut

Fig .1 shows the RPC service running on a Windows XP machine.

Variants:

W32/Blaster-B: is functionally equivalent to W32.Blaster.Worm, except that this variant uses the filename teekids.exe and the registry entry: [6]

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Inet Xp

The worm contains an internal message which does not get displayed. The message is different from the one contained in W32.Blaster.Worm and says the following:
”Microsoft can s*** my left testi!”
”Bill Gates can s*** my right testi!”
”And All Antivirus Makers Can S*** My Big Fat C***”
W32/Blaster-C: conducts the same behaviour as W32/Blaster.A and W32.Blaster.B, but uses the filename p****32.exe. [7]

W32/Blaster-D: Conducts the same behaviour as W32/Blaster.A, but uses the filename mspatch.exe instead of msblast.exe, and adds the registry entry: [8]

HKLM\Software\Microsoft\Windows\CurrentVersion\Runon\Nonton Antivirus

W32/Blaster-E: It conducts the same function as W32/Blaster-A, except for the following changes: [9]

- The registry entry used has been changed to HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WindowsAutomation
- The target for the Distributed Denial-of-Service attack has been changed to kimble.org
- The internal message has been changed to "I dedicate this particular strain to me ANG3L -hope yer enjoying yerself and dont forget the promise for me B/DAY!!!!."

W32/Blaster-F: It also conducts the same function as W32/Blaster-A, except for the following changes: [10]

- The worm filename used is enbiei.exe
- The registry entry used has been changed to HKLM\Software\Microsoft\Windows\CurrentVersion\Run\www.hidro.4t.com
- The target for the distributed denial-of-service attack has been changed to tuiasi.ro
- The internal message has been changed to the following text in Romanian:
  "Nu datzi la fuckultatea de Hidrotehnica!!! Pierdetzi timp ul degeaba...Birsan te cheama pensia!!!Ma pis pe diploma!!!!!!" In English this translates to: "Don't go to the Hydrotechnics faculty!!! You are wasting your time... Birsan, your pension awaits!!! I urinate on the diploma!!!!!!"

Description:

As mentioned before W32.Blaster.Worm exploits unpatched windows operating systems that are vulnerable to DCOM RPC vulnerability. When W32.Blaster.Worm is executed the following actions take place:

A. The exploit auto starts and check the Infected PC memory if it is present or not.
B. The exploit starts a distributed denial of service attack (DDoS).
C. It starts to exploit the RPC DCOM Buffer Overflow vulnerability**.**
D. The exploit starts to spread widely among the Network.

A. The exploit auto starts and checks the Infected PC memory to see whether a computer is already infected and whether the worm is running. If so, the worm will not infect the computer a second time. Otherwise it creates the following autorun registry entry so that it executes every time Windows starts:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\
CurrentVersion\Run
"windows auto update" = MSBLAST.EXE
```

B. Then W32.Blaster.Worm starts a DDoS attack by trying to check for Internet connection, until it is able to establish this connection. Once it secures an Internet connection, launches a thread that performs a Distributed Denial of Service attack against windowsupdate.com web site, this behavior will not allow infected users to visit windowsupdate.com website to download and install the required security patch (KB823980).This action will succeed under certain conditions:

- 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.
- The worm runs on a Windows XP computer that was either infected or restarted during the payload period.
- The worm runs on a Windows 2000 computer that was infected during the payload period and has not been restarted since it was infected.
- 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.

This DoS traffic will have the following characteristics:

- Is a SYN flood on port 80 of windowsupdate.com.
- Tries to send 50 HTTP packets every second.
- Each packet is 40 bytes in length.
- If the worm cannot find a DNS entry for windowsupdate.com, it uses a destination address of 255.255.255.255.

Some fixed characteristics of the TCP and IP headers are:

- IP identification = 256
- Time to Live = 128
- 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.
- Destination IP address = dns resolution of "windowsupdate.com"
- TCP Source port is between 1000 and 1999
- TCP Destination port = 80
- TCP Sequence number always has the two low bytes set to 0; the 2 high bytes are random.
- TCP Window size = 16384

C. The third action is that the W32.Blaster. Worm is trying to exploit the RPC DCOM Buffer Overflow windows vulnerability, this takes place as follows:

1. The worm sends one of two types of data, either to exploit Windows XP or Windows 2000 on TCP port 135 that may exploit the DCOM RPC vulnerability, On doing this action you will recognise that Procedure Call (RPC) service stops on Windows XP ,windows 2003 server ,windows 2000 professional and windows 2000 server causing two different actions :

   - A restart action to Windows XP and Windows 2003 Server, this is because the Remote Procedure Call (RPC) service caused NTAUTHORITY\SYSTEM to reboot the machine in 60 seconds.
   - No automatic reboot on other windows operating systems, but since many services depend on RPC, it is given that some services might not work properly causing system paralysis.
2. The Worm uses Cmd.exe to create a hidden remote shell process that will listen on TCP port 4444, allowing an attacker to issue remote commands on an infected system.

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

D. W32.Blaster.Worm spreads widely among the network causing network congestion (saturated with port 135 requests); this is because the worm starts to generate a random IP addresses and starts to infect the hosts with these IP addresses , this process is done according to the following algorithm:

> The generated IP address is of the form of 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. [2], [3]

Signatures of the Attack:

W32.Blaster.Worm can be detected by various means; it can be detected by vendor's intrusion detection systems (host-based and Network Based), vendor's antivirus software, firewalls logs and even can be detected by the well educated user looking in the local services status and tasks on his personal computer. Let us first see how a user can detect W32.Blaster.Worm on his PC.

- By taking a look on the process in the task manager on a malfunction Windows 2000 workstations or servers he can recognize that there is a process called msblast.exe running. This is a significant that the worm exists.

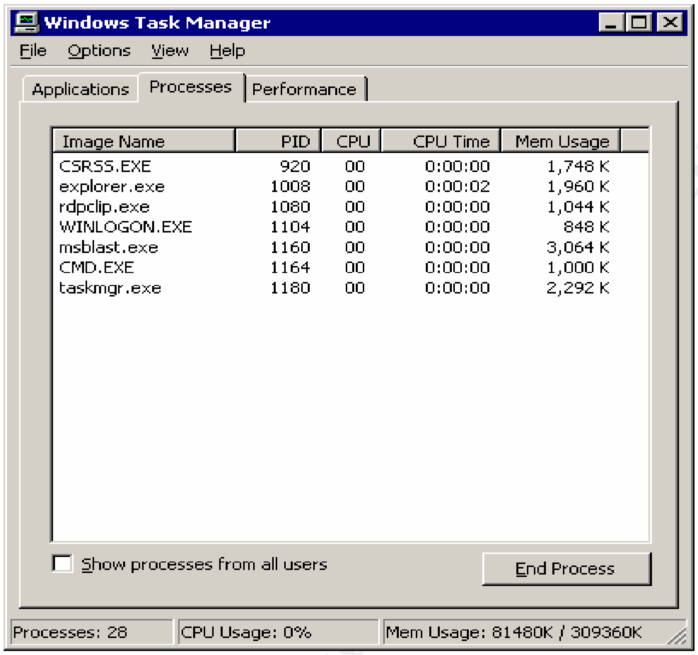
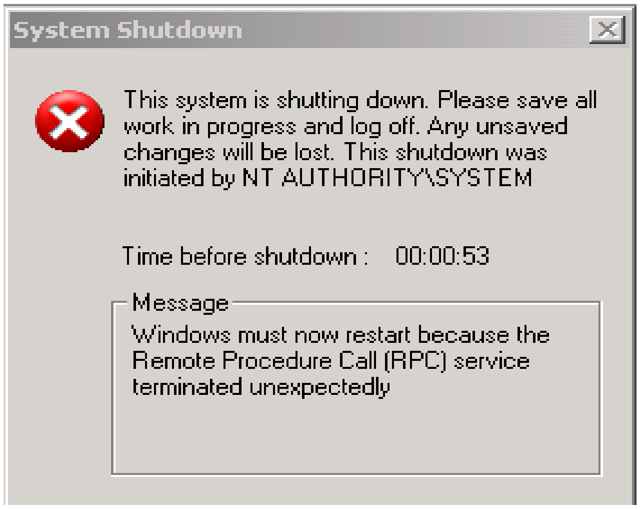


Image Name	PID	CPU	CPU Time	Mem Usage
CSRSS.EXE	920	00	0:00:00	1,748 K
explorer.exe	1008	00	0:00:02	1,960 K
rdpclip.exe	1080	00	0:00:00	1,044 K
WINLOGON.EXE	1104	00	0:00:00	848 K
msblast.exe	1160	00	0:00:00	3,064 K
CMD.EXE	1164	00	0:00:00	1,000 K
taskmgr.exe	1180	00	0:00:00	2,292 K

Processes: 28 CPU Usage: 0% Mem Usage: 81480K / 309360K

Fig .2 shows the how we can investigate the presence of the msblast.exe file using windows task manager.

On a windows XP or windows 2003 the exploit can accidentally cause the remote RPC service to terminate displaying a message entitled "System Shutdown". The Windows XP machine then reboots.



System Shutdown

This 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

Time before shutdown : 00:00:53

Message

Windows must now restart because the Remote Procedure Call (RPC) service terminated unexpectedly

Fig .3 shows how msblast.exe is recognized on a Window XP machine.

All the above can be done besides the manual check for the file by searching the local drives after the file name msblast.exe or looking to the value:
"windows auto update"="msblast.exe"
in the registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

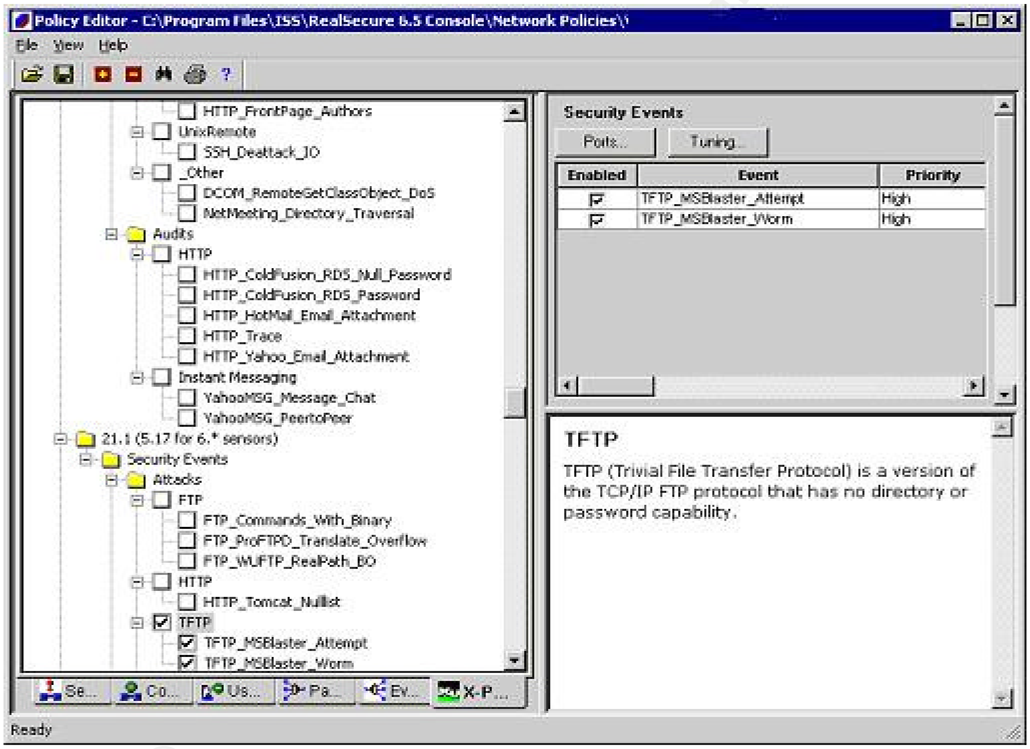
- W32.Blaster.Worm can be detected by virus definition files form any major anti-virus software vendor dated August 11, 2003 or later, (e.g. Symantec antivirus – Sophos)
- W32.Blaster.Worm existence can be detected by investigating Firewall or routers logs; it can be easily detected by investigating the repeated traffic originating from any infected machine using port 135/TCP, 4444/TCP and 69/UDP. (See below logs)

```
1:10:40.395032 192.168.10.1.1294 > 192.168.10.3.135: tcp 0
1:10:40.395323 192.168.10.3.135 > 192.168.10.1.1294: tcp 0
1:10:40.395436 192.168.10.1.1294 > 192.168.10.3.135: tcp 0
1:11:41.508095 192.168.10.1.1294 > 192.168.10.3.135: tcp 72
1:11:41.508310 192.168.10.1.1294 > 192.168.10.3.135: tcp 1460
1:11:41.508346 192.168.10.1.1294 > 192.168.10.3.135: tcp 244
1:11:41.508362 192.168.10.3.135 > 192.168.10.1.1294: tcp 0
1:11:41.508541 192.168.10.3.135 > 192.168.10.1.1294: tcp 60
1:11:41.508681 192.168.10.1.1294 > 192.168.10.3.135: tcp 0
1:11:41.508720 192.168.10.3.135 > 192.168.10.1.1294: tcp 0
1:11:41.512201 192.168.10.3.135 > 192.168.10.1.1294: tcp 0
1:11:41.512346 192.168.10.1.1294 > 192.168.10.3.135: tcp 0
1:11:41.904949 192.168.10.1.1314 > 192.168.10.3.4444: tcp 0
1:11:41.905031 192.168.10.3.4444 > 192.168.10.1.1314: tcp 0
1:11:41.905160 192.168.10.1.1314 > 192.168.10.3.4444: tcp 0
1:11:41.952874 192.168.10.3.4444 > 192.168.10.1.1314: tcp 42
1:11:41.984939 192.168.10.1.1314 > 192.168.10.3.4444: tcp 36
1:11:41.985029 192.168.10.3.4444 > 192.168.10.1.1314: tcp 63
```

```
1:11:42.083469 192.168.10.3.1049 > 192.168.10.1.69: udp 20
1:11:42.118800 192.168.10.1.69 > 192.168.10.3.1049: udp 516
```

In the above case, machine 192.168.10.1 is clearly infecting machine 192.1681.0.3.

- W32.Blaster.Worm can be detected also by vendor Intrusion Detection systems (e.g. ISS Real secure Network sensor, ISS Real Secure server sensor – Snort IDS). Let us start by investigating ISS Real Secure (Network – Server) Sensors signatures, W32.Blaster.Worm activity can be detected when the following signatures are detected on the IDS main console "TFTP_MSBlaster_Worm" and "TFTP_MSBlaster_Attempt" when these events are present, you should apply the "Block" action on the Server sensor, and the "RSKILL" action on the Network sensor, by applying those actions your systems will be virtually patched against the worm even if it is not patched with Microsoft patch.



Policy Editor - C:\Program Files\ISS\RealSecure 6.5 Console\Network Policies\\
File
View
Help
Se...
Co...
Us...
Pa...
Ev...
X-P...
Ready
Ports...
Tuning...

```
□ HTTP_FrontPage_Authors
⊟ □ UnixRemote
    □ SSH_Deattack_IO
⊟ □ _Other
    □ DCOM_RemoteGetClassObject_DoS
    □ NetMeeting_Directory_Traversal
⊟ Audits
  ⊟ □ HTTP
      □ HTTP_ColdFusion_RDS_Null_Password
      □ HTTP_ColdFusion_RDS_Password
      □ HTTP_HotMail_Email_Attachment
      □ HTTP_Trace
      □ HTTP_Yahoo_Email_Attachment
  ⊟ □ Instant Messaging
      □ YahooMSG_Message_Chat
      □ YahooMSG_PeertoPeer
⊟ 21.1 (5.17 for 6.* sensors)
  ⊟ Security Events
    ⊟ Attacks
      ⊟ □ FTP
          □ FTP_Commands_With_Binary
          □ FTP_ProFTPD_Translate_Overflow
          □ FTP_WUFTP_RealPath_BO
      ⊟ □ HTTP
          □ HTTP_Tomcat_Nullist
      ⊟ ☑ TFTP
          ☑ TFTP_MSBlaster_Attempt
          ☑ TFTP_MSBlaster_Worm
```

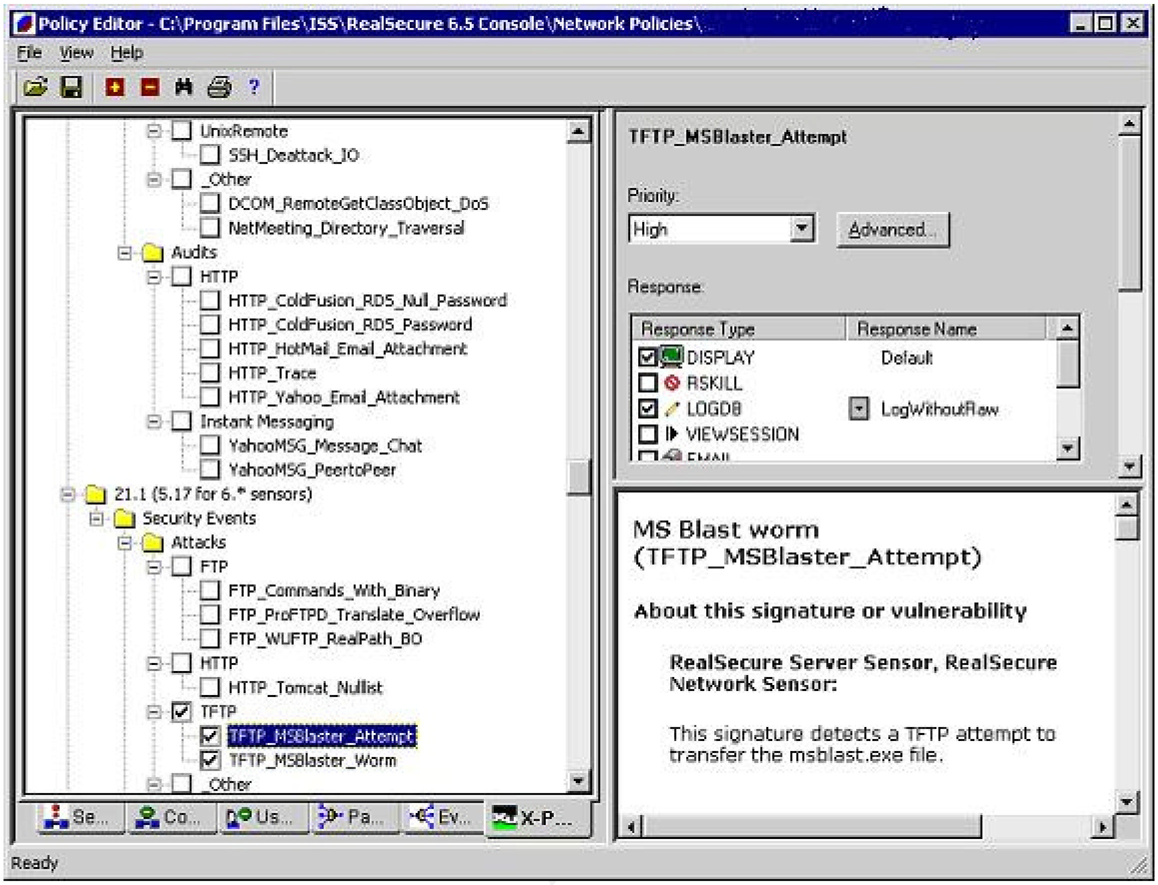
Security Events

Enabled	Event	Priority
☑	TFTP_MSBlaster_Attempt	High
☑	TFTP_MSBlaster_Worm	High

TFTP

TFTP (Trivial File Transfer Protocol) is a version of the TCP/IP FTP protocol that has no directory or password capability.

Fig .4 shows ISS – Real secure (Network – Server) sensor W32.MSblaster.Worm signature.



Policy Editor - C:\Program Files\ISS\RealSecure 6.5 Console\Network Policies\

```
⊟ □ UnixRemote
    □ SSH_Deattack_IO
⊟ □ _Other
    □ DCOM_RemoteGetClassObject_DoS
    □ NetMeeting_Directory_Traversal
⊟ Audits
  ⊟ □ HTTP
      □ HTTP_ColdFusion_RDS_Null_Password
      □ HTTP_ColdFusion_RDS_Password
      □ HTTP_HotMail_Email_Attachment
      □ HTTP_Trace
      □ HTTP_Yahoo_Email_Attachment
  ⊟ □ Instant Messaging
      □ YahooMSG_Message_Chat
      □ YahooMSG_PeertoPeer
⊟ 21.1 (5.17 for 6.* sensors)
  ⊟ Security Events
    ⊟ Attacks
      ⊟ □ FTP
          □ FTP_Commands_With_Binary
          □ FTP_ProFTPD_Translate_Overflow
          □ FTP_WUFTP_RealPath_BO
      ⊟ □ HTTP
          □ HTTP_Tomcat_Nullist
      ⊟ ☑ TFTP
          ☑ TFTP_MSBlaster_Attempt
          ☑ TFTP_MSBlaster_Worm
      ⊟ □ _Other
```

TFTP_MSBlaster_Attempt

Priority: High

Response:

Response Type	Response Name
☑ DISPLAY	Default
□ RSKILL	
☑ LOGDB	LogWithoutRaw
□ VIEWSESSION	
□ EMAIL	

MS Blast worm
(TFTP_MSBlaster_Attempt)

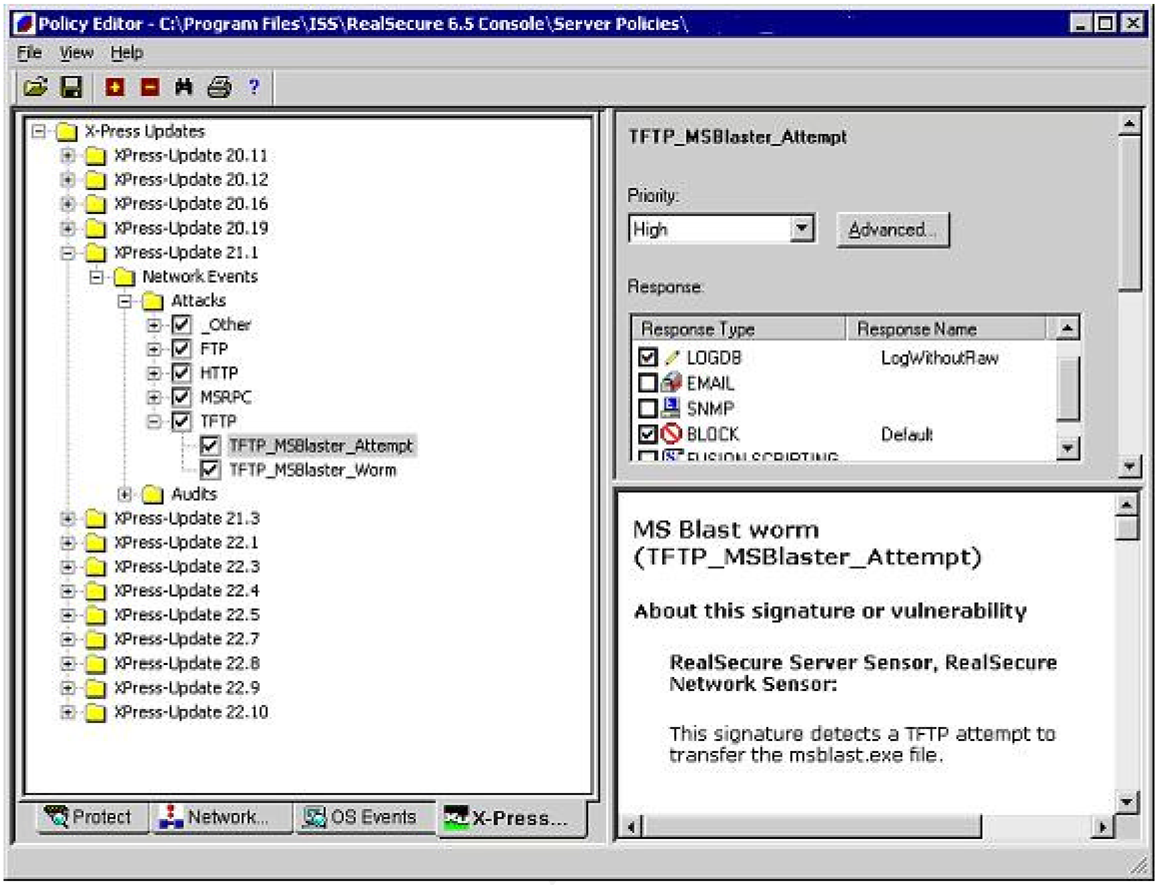
About this signature or vulnerability

RealSecure Server Sensor, RealSecure Network Sensor:

This signature detects a TFTP attempt to transfer the msblast.exe file.

Ready

Fig .5 shows ISS – Real secure Network sensor W32.MSblaster.Worm signature and the responses towards the attack.



TFTP_MSBlaster_Attempt

Priority: High

Response:

Response Type	Response Name
☑ LOGDB	LogWithoutRaw
□ EMAIL	
□ SNMP	
☑ BLOCK	Default
□ FUSION SCRIPTING	

MS Blast worm
(TFTP_MSBlaster_Attempt)

About this signature or vulnerability

RealSecure Server Sensor, RealSecure Network Sensor:

This signature detects a TFTP attempt to transfer the msblast.exe file.

Fig .6 shows ISS – Real secure server sensor W32.MSblaster.Worm signature and the responses towards the attack.

On the other hand , Snort IDS apply this signature as follows:
“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.asp; sid:2251; rev:4;)” . [11], [12], [13]

3. The Platforms/Environments:

Victims Platform:

The victim's platform consists of users 100 PCs, 50 terminal screens, 30 windows 2000 based ATM (automatic teller machine), 20 Windows 2000 server's service pack 3, and 2 IBM AS/400 back-office system.

- The users PCs is a Pentium 4 Intel based processor, 512 MB RAM and 30 GB HDD which is used to run windows based banking applications such as:
    - *Cashier Software*: which is an application used by front desk tellers, to check signature verification, account entries; it is considered to be the back- bone of all banking teller activities.
    - *Stock exchange communications software:* It is the back –bone of the Bank dealing room, it is responsible for communicating deals between the bank and the stock exchange.
    - *Archiving System Clients:* It is used to retrieve the archived banking documents and customers balance statements.
- Terminal screens are dummy terminals TCP/IP based, used by data entry employees.
- The Bank servers are windows 2000 server SP3, 2 GB RAM, 80 GB HDD, and duel Intel based Pentium 4 processor, these servers are used as a Domain controller servers, Mail servers and Cashier application Servers.
- The Banks' ATM machines are Intel processor, windows 2000 based machines that use TCP/IP protocol to communicate with the back end AS/400.
- Finally the IBM AS/400 machine that acts as the Back office for all Banking applications, all the bank branches are connected to that machine using the WAN fiber links.

Note that the entire systems platform are scattered among thirty branch offices.

Source Network:

The source network consists of 2 Laptops with the following configuration:

- The first Laptop, is the administrating and scanning console, It has the following configuration :
    - Pentium 4 Intel based processor, 1 GB RAM and 30 GB HDD, windows XP professional with SP1 installed.
    - Toshiba Wireless LAN mini PCI (built in)
    - Intel (R) Pro /100 VE Network Connection (built in)

- Applications installed are :

  - Internet explorer
  - Tiny personal Firewall (all incoming traffic are denied unless permitted by the administrator)
  - ISS internet scanner
  - Symantec Antivirus with latest virus definition updates, later than 11 august 2003.
  - Wireless Ethernet signal detector software.

- The Second Laptop is the infecting machine, it is a windows 2000 professional unpatched machine, with no antivirus software installed, and it is infected with W32.Msblast.Worm. Also it has the same network connectivity :
  - Toshiba Wireless LAN mini PCI (built in)
  - Intel (R) Pro /100 VE Network Connection (built in)

The connectivity will take place between the 2 laptops using a cross –over cable, but the wireless network adapters will be used as a back door for internal scanning and exploit injection.

<u>Target Network:</u>

"Victim Bank "is a leading bank, it has large network all over the country ,30 branches with an ATM machine placed in each branch , by taking a look at the network diagram in the next section, we can see that the bank is connected to the internet by means of 2 leased line links 128 Kbps and 512 Kbps, the internet router acts as a first line of defense by applying access control lists on it , behind the router is a PIX 525 firewall with a Failover ,that allows only http ,https , ftp , SMTP , and DNS traffic. Behind the firewall is a DMZ network " **10.10.0.0** " ,in that network we can find the front end Lotus Domino mail server ,the bank Web server "www.VictimBank.com" and an E-pay server . The bank is using also an ISS Real Secure Network Sensor which is placed in that DMZ to detect malicious activity that may enter from the internet. As per the bank policy neither internet web browsing nor internet mail is allowed for the employees, only executives are allowed to browse the internet, by applying a policy on the internal checkpoint Firewall.

The Internal Victim's Bank network is a mess, they were afraid of external users that can attack from the internet ,but the administrators did not pay attention to internal intruders, the internal network consists of a class C network **192.168.0.0,** the main branch in which the attack will originate subnet is **192.168.10.0**, the branch offices are connected to the main branch by a frame relay network in a star topology behavior , the branch offices subnets are 192.168.11.0, 192.168.12.0,…….192.168.30.0

The internal network has 2 IBM AS/400 machines it acts as a back-office for all the branches in a centralized Database manner, with the AS/400 machine we find the Windows 2000 Domain controller server, the client PCs, the backend Domino mail server, the DNS and the DHCP server .Also we can find the application servers (Stock exchange communication server, Cashier Server and the document Archiving server), dummy terminals and ATM branch machine. More and above we find **wireless access points** spread among the main branch which will play the main role in our paper.

First of all let us highlight some known risks resulting from implementing misconfigured wireless access points and connecting them to the network, these risks are: [14]

- <u>Insertion attacks:</u>
  These attacks are based on connecting unauthorized devices or creating new wireless networks without going through security process and review. For example connecting a wireless client to an access point without authentication, or implementing wireless capabilities on the network without taking the organization approvals. These actions could lead to unauthorized clients gaining access to corporate resources through an unauthorized connected access point.
- <u>Interception and monitoring of wireless traffic:</u>
  In this attack the attacker is intercepting and monitoring network traffic across the wireless LAN. The attacker needs only to be 300 feet from the wireless access point to be able to monitor traffic.
- <u>Jamming:</u>
  In this attack the attacker can perform a denial of service attack on the wireless access point using certain tools causing it to stop functioning. Simply what is done is flooding the network frequency range using attack tools causing the network signal to corrupt and the wireless access point stop functioning.
- <u>Client to Client Attacks:</u>
  Clients can talk directly to each other, bypassing the access point, so clients need to be defended against each other.
- <u>Brute Force Attacks Against Access point passwords:</u>
  Access points uses shared passwords with all wireless clients. Brute force attack is done against this shared password, if this password is known to the attacker, he can easily gain access to the wireless access point and to the corporate network resources.
- <u>Misconfiguration:</u>
  Many access points are installed to production environments with default factory setting, these setting ignores security configuration for the ease of use. Examples of default setting are default shared password and unrestricted access point access.

<u>Network Diagram:</u>

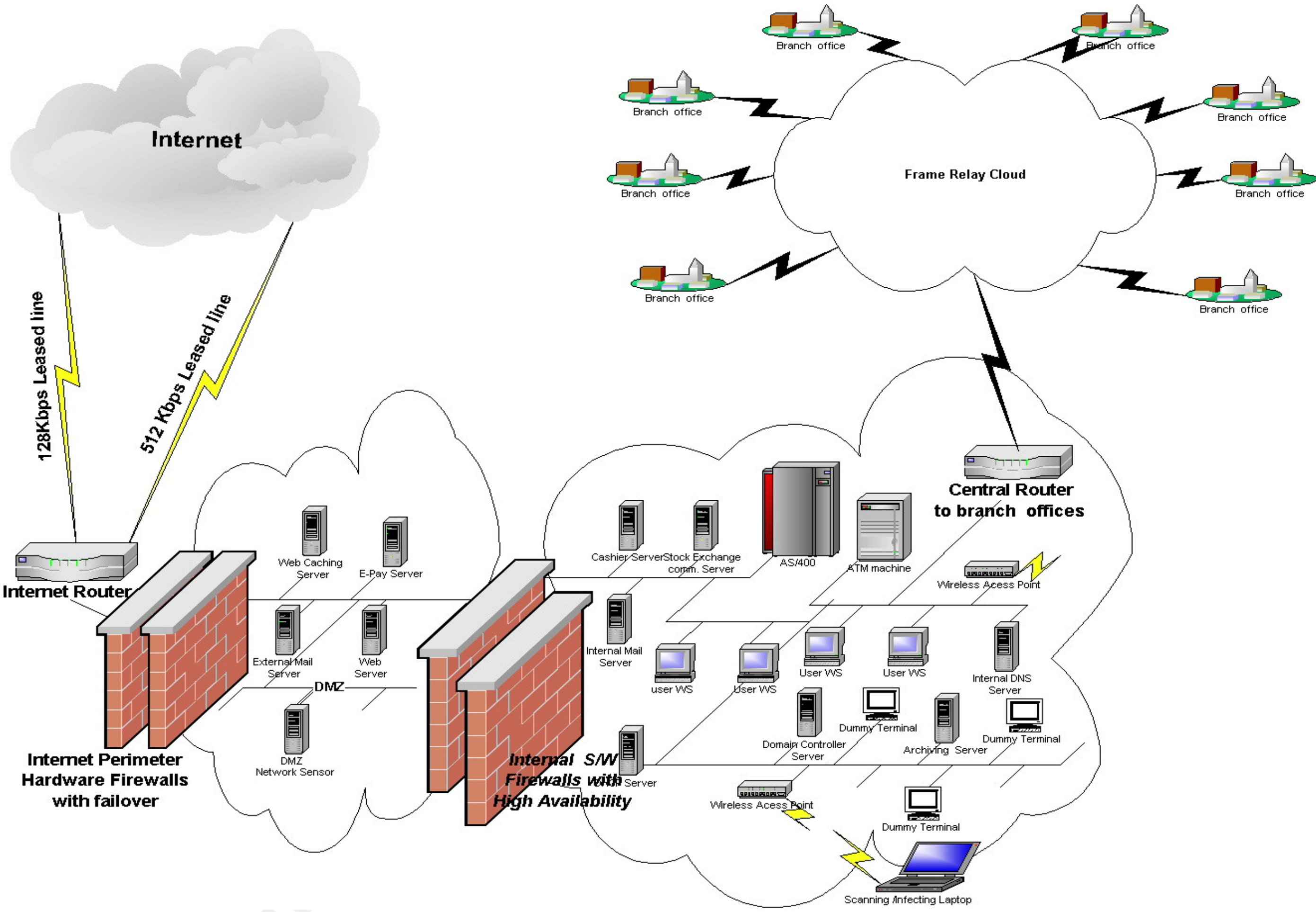


Fig .7 Shows the Victim's Bank network diagram.

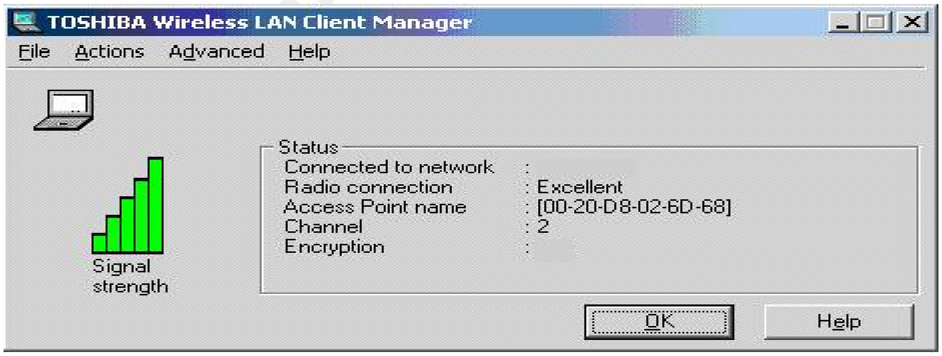
Note that the Victim's Bank network topology is star connectivity, this is due to the nature of centralized database located in the main headquarter.

4. Stages of the attack:

Reconnaissance:

Reconnaissance is gathering of information as much as possible from open sources. This information can be gained easily from web sites, domain name registration information and social engineering.

In this paper, social engineering method is used. As mentioned before Mr. Bad Guy was the owner of a security consultant company who did some projects for the Victim Bank three months ago, these projects were implementing physical access control solution for the Victims Bank's employees. During that time in the bank he made a lot of relations with the Victim Bank‘s network administrators. These administrators were doing network administration plus network security, he knew from several unofficial talks with them that there are several operating systems running on network, such as IBM OS/400, Windows 2000 server and professional, he also knew that there is neither corporate Anti-virus system nor windows update patching server is running on that network. This is because the bank's IT management main concern is about the IBM AS/400 database security that holds the customer accounts, also the bank IT management had a restrictive user policy that restricts the internet and mail access on all employees except for the executives, also the PC‘s 1.4 M diskette drive and CD ROMs are disabled, all software are found on a shared drive to be installed only by the technical support engineers. Mr. Bad Guy knew a valuable information regarding the new wireless network that is taking place in the head quarters main office, he knew that there is two development network access points connected directly to the corporate network with their default configurations, these access points were done for the executives attending meetings in the banks meeting rooms located in the second floor above the customer service and tellers main area. Mr. Bad Guy had a Laptop with a wireless network card; he noticed that there is a signal detected by the wireless network software (see below fig.)



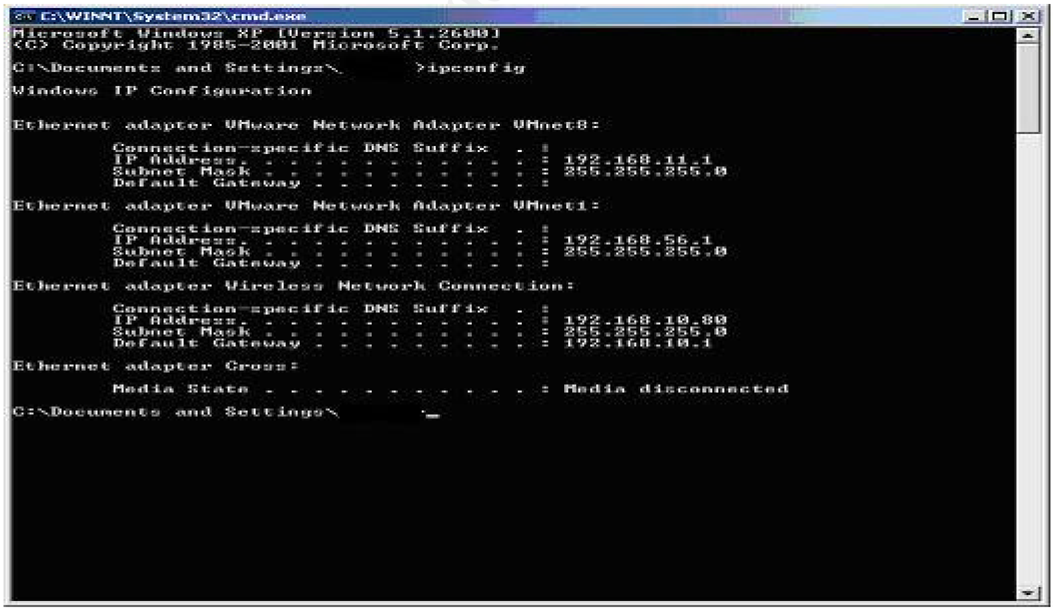
Status
Connected to network : [redacted]
Radio connection : Excellent
Access Point name : [00-20-D8-02-6D-68]
Channel : 2
Encryption : [redacted]

Fig .8 Shows the wireless network signal indicator software.

Mr. Bad Guy, collected large amount of information during his time working with the Victim‘s Bank technical staff. Although he knew a lot of security weaknesses and mal configuration in the current setup - (we shall talk about these security weaknesses in the following sections) -he was not planning to generate any attacks against the bank, but due to his failure to pay back the loan - (as mentioned in the statement of purpose section) -and the bank refused to extend his allowance period causing him bankruptcy, he decided to begin the attack and cause the bank a great harm.

During that time , W32.Blaster.worm was hitting most international and local companies networks from the internet , but as the Victim’s Bank internet policy is so restrictive, no infections took place during the first week of the W32.Blaster.worm discovery .No one paid attention that the wireless access points represent security weakness in the bank ‘s corporate network . Mr. Bad Guy recognized that, he knew that the wireless access points were operating using the default configuration, and the signal coverage was detected 20 metes away from the bank’s premises. With a simple test, Mr. Bad Guy opened the Laptop from his car parking next to the bank; he noticed the signal detector to have the same signal strength as if he is staying inside the bank, and finally he obtained an IP address from the bank‘s DHCP server connecting to the corporate network . This can be easily checked by typing “ipconfig “command from the command prompt. (See fig. 9), we can notice that the Laptop has the IP address 192.168.10.80 which is from the corporate Bank internal IP range.

Now Mr. Bad Guy is ready to start the next step of his attack.

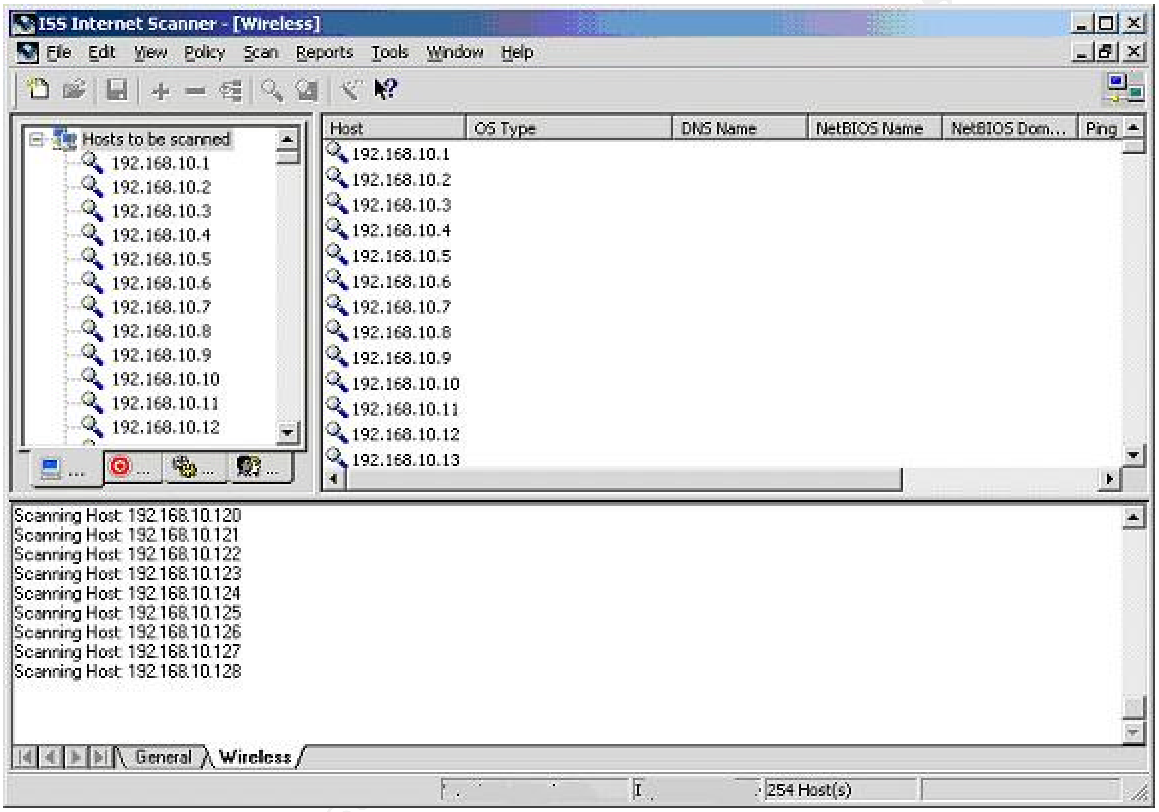


```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\[redacted]>ipconfig

Windows IP Configuration


Ethernet adapter VMware Network Adapter VMnet8:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.11.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet1:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.56.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

Ethernet adapter Wireless Network Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.10.80
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.10.1

Ethernet adapter Cross:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\[redacted]>_
```

Fig .9   Shows how Mr. Bad Guy detected that he is a part of Victim‘s Bank Corporate network.

<u>Scanning:</u>

Mr. Bad Guy started to scan the target corporate Victim's Bank network from his car parking outside the bank premises, he is scanning the bank internal network using ISS internet scanner tool. This tool in addition to port scans the network it also undergo a vulnerability scan, and operating system detection. After applying the vulnerability scanner signature updates to include the W32.Balster.Worm windows vulnerability, he started scanning the network.


ISS Internet Scanner - [Wireless]
File Edit View Policy Scan Reports Tools Window Help
Hosts to be scanned
General
Wireless
254 Host(s)

Hosts to be scanned
- 192.168.10.1
- 192.168.10.2
- 192.168.10.3
- 192.168.10.4
- 192.168.10.5
- 192.168.10.6
- 192.168.10.7
- 192.168.10.8
- 192.168.10.9
- 192.168.10.10
- 192.168.10.11
- 192.168.10.12

Host	OS Type	DNS Name	NetBIOS Name	NetBIOS Dom...	Ping
192.168.10.1					
192.168.10.2					
192.168.10.3					
192.168.10.4					
192.168.10.5					
192.168.10.6					
192.168.10.7					
192.168.10.8					
192.168.10.9					
192.168.10.10					
192.168.10.11					
192.168.10.12					
192.168.10.13					

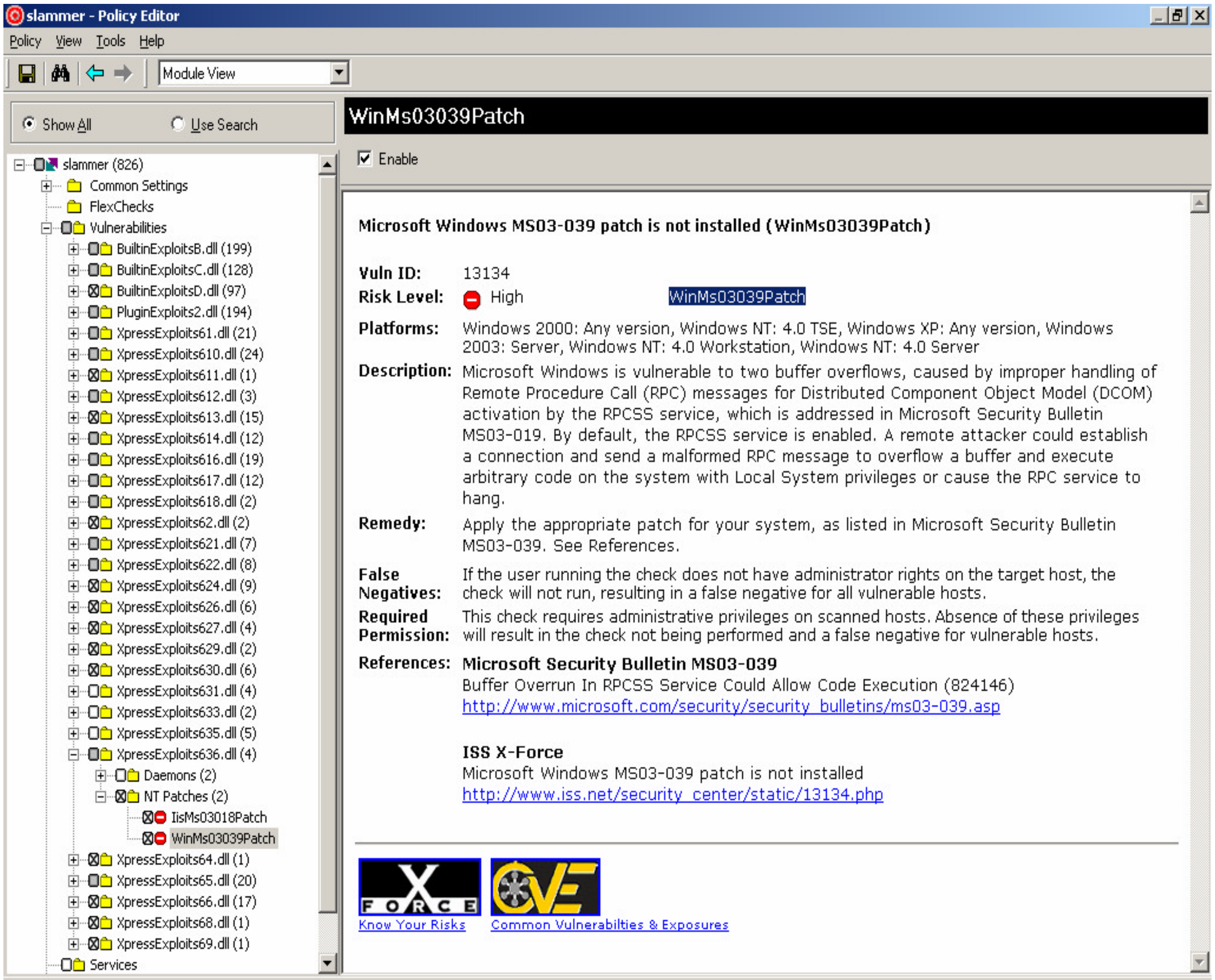
```
Scanning Host: 192.168.10.120
Scanning Host: 192.168.10.121
Scanning Host: 192.168.10.122
Scanning Host: 192.168.10.123
Scanning Host: 192.168.10.124
Scanning Host: 192.168.10.125
Scanning Host: 192.168.10.126
Scanning Host: 192.168.10.127
Scanning Host: 192.168.10.128
```

Fig .10 Shows ISS internet Scanner software console.

After scanning some of the machines on the network he discovered that the W32.Blaster.worm windows vulnerability is found on most PC, this was expected as the Bank did have neither corporate antivirus system nor windows patching update policy.

By taking a look on the below figure, we can see that how ISS internet scanner recognize the vulnerable systems by using its own vulnerability database.

The vulnerability name is **WinMs03039Patch** which is categorized as a high critical.


slammer - Policy Editor
Policy View Tools Help
Module View
● Show All ○ Use Search
slammer (826)
Common Settings
FlexChecks
Vulnerabilities
BuiltinExploitsB.dll (199)
BuiltinExploitsC.dll (128)
BuiltinExploitsD.dll (97)
PluginExploits2.dll (194)
XpressExploits61.dll (21)
XpressExploits610.dll (24)
XpressExploits611.dll (1)
XpressExploits612.dll (3)
XpressExploits613.dll (15)
XpressExploits614.dll (12)
XpressExploits616.dll (19)
XpressExploits617.dll (12)
XpressExploits618.dll (2)
XpressExploits62.dll (2)
XpressExploits621.dll (7)
XpressExploits622.dll (8)
XpressExploits624.dll (9)
XpressExploits626.dll (6)
XpressExploits627.dll (4)
XpressExploits629.dll (2)
XpressExploits630.dll (6)
XpressExploits631.dll (4)
XpressExploits633.dll (2)
XpressExploits635.dll (5)
XpressExploits636.dll (4)
Daemons (2)
NT Patches (2)
IisMs03018Patch
WinMs03039Patch
XpressExploits64.dll (1)
XpressExploits65.dll (20)
XpressExploits66.dll (17)
XpressExploits68.dll (1)
XpressExploits69.dll (1)
Services
WinMs03039Patch
☑ Enable
FORCE
Know Your Risks
Common Vulnerabilties & Exposures

Microsoft Windows MS03-039 patch is not installed (WinMs03039Patch)

Vuln ID: 13134

Risk Level: High WinMs03039Patch

Platforms: Windows 2000: Any version, Windows NT: 4.0 TSE, Windows XP: Any version, Windows 2003: Server, Windows NT: 4.0 Workstation, Windows NT: 4.0 Server

Description: Microsoft Windows is vulnerable to two buffer overflows, caused by improper handling of Remote Procedure Call (RPC) messages for Distributed Component Object Model (DCOM) activation by the RPCSS service, which is addressed in Microsoft Security Bulletin MS03-019. By default, the RPCSS service is enabled. A remote attacker could establish a connection and send a malformed RPC message to overflow a buffer and execute arbitrary code on the system with Local System privileges or cause the RPC service to hang.

Remedy: Apply the appropriate patch for your system, as listed in Microsoft Security Bulletin MS03-039. See References.

False Negatives: If the user running the check does not have administrator rights on the target host, the check will not run, resulting in a false negative for all vulnerable hosts.

Required Permission: This check requires administrative privileges on scanned hosts. Absence of these privileges will result in the check not being performed and a false negative for vulnerable hosts.

References: **Microsoft Security Bulletin MS03-039**
Buffer Overrun In RPCSS Service Could Allow Code Execution (824146)
http://www.microsoft.com/security/security_bulletins/ms03-039.asp

ISS X-Force
Microsoft Windows MS03-039 patch is not installed
http://www.iss.net/security_center/static/13134.php

Fig.11 shows how ISS internet scanner defines W32.Blaster.worm windows vulnerability.

Exploiting the system:

In this section, Mr. Bad Guy will start exploiting the target network with W32.Blaster.worm; this will take place also from his own car parking outside the bank premises. As mentioned previously in the source network section, Mr. Bad Guy had two Laptops, one is used for scanning the target network and the other one is used for exploiting the network. Simply Mr. Bad Guy connected the second (infecting) Laptop on the network; the machine joined the bank network as stated before and started infecting the whole network with W32.Blaster.worm. Mr. Bad Guy left the machine for a while connecting on the car battery for ensuring that the Laptop will be connected for long time on the Victim's Bank network .Mr. Bad Guy left his car and started going inside the bank to observe what is going on inside the customer service and tellers area.

Due to the W32.Blaseter.worm nature and behavior, it started to propagate across a network causing a Denial of Service attack on all network resources.

Keeping Access and Covering Tracks:

After Mr. Bad Guy entered the Bank reception, he took a number from the receptionist, and sat down waiting for his turn to make a deposit. He waited for about two hours because the bank was crowded on that day. He noticed that the technical support engineers were arriving one after the other, investigating some strange activities , after that he noticed that the counter workstations were out of order, then the windows based ATM machine located in the bank entrance were displaying "out of service "notice on its screen.

He was quit sure that he reached his aim; he took his car and visited another branch office connected via the bank intranet, he noticed that the ATM machines are displaying the same massage, and the bank counter is closed due to technical problems.

The next day he visited the bank to ask for extending the loan allowance again, he met his old network administrators friends, they told him that the bank was parallelized yesterday and most customers complained about bad service, the bank lost a great amount of money due to loosing communications with the stock exchange, and overall the bank shares prices went low in the stock exchange due to bad reputation. Mr. Bad Guy although is going to loose his money, but he is so happy that he reached his own target.

No one discovered who did the attack, as there is no internal IDS network sensor to detect and log the attack origin, time, and event of that incident so as to take it as evidence.

5. The Incident Handling Process:

Preparation:

Existing Countermeasures

Victim 's Bank has existing counter measures that helps in handling internet intrusion incidents or breach , in addition the bank has a well trained incident handling team that takes place if internal or external fraud incidents occur by employees or by external theft.

- Victim's Bank is applying a security in depth policy to prevent the internal network from being breached by a hacker sitting on the internet, this is achieved as follows:

  - The internet router has an access list that denies all traffic except those defined on the Cisco PIX firewall
  - Two Cisco PIX firewalls placed on the internet, these firewalls acts in a failover manner to achieve a high available solution. The firewalls policy is as follows :

    - Denying all outbound traffic except internet mail (25 TCP), DNS query (53 UDP) and web browsing (80,443 TCP) traffic.
    - Denying all inbound traffic except website and e-commerce traffic (80,443 TCP).

  - In the DMZ also we can find an ISS network sensor appliance that can detect malicious traffic entering the network from the internet, sending RS-KILL responses to terminate that traffic.
  - Two checkpoint internal firewalls in a high available manner, this firewalls separate the corporate network from the DMZ network, the firewalls are configured on a deny-all basis unless required as per the business needs.
  - Vendor penetration testing takes place each month on the Victim's bank internet range, this testing is done periodically to check for network vulnerabilities and to ensure that the perimeter network is secure.

- The Victim's Bank is applying a restrictive user policy in a way that neither internet browsing access nor internet mail is permitted to normal employees, only executives have this facility. Moreover all CD –ROMs and Diskette drives are disabled from all workstations using windows 2000 group policy object, this is to prevent any employee from installing infected or illegal software on his machine ,only technical support and windows domain administrators are allowed to install operating system and business related applications.

- On an employee login on the Victim's Bank network ,a warning banner is displayed , this banner advises the user that :

  - Access to the system is limited to the bank authorized activity.
  - Any unauthorized access is prohibited.
  - Unauthorized users may face criminal penalties.
  - If system logging shows possible evidence of criminal activity, the bank can provide the documents to law enforcement.

- Each employee in the Victim's Bank is required to sign on the employee's policy that is written in the employee handbook issued by the HR (human resources department) .It states that any employee abuses computer usage will be terminated immediately.
- The Victim's Bank has a well trained IT technical staff who is responsible for maintaining all the bank's services 24 hours all over the week. The teams are divided as follows :
  - The Help Desk Team, that team acts as a 1st line of support for all banking applications .This team is responsible to provide over the phone support to users.
  - The Technical support Team, that team who has a direct contact with all users, and is responsible to install new software on the users' workstations, provide remote support to all ATM machines.
  - The Network support Team, that team is responsible for supporting all the LAN and WAN environment .Also that team is responsible for administrating network security all over the bank.
  - An AS/400 system and Windows 2000 administrator, who is responsible for adjusting user system privileges to all employees, the user privilege is given according to the employee job description. The system administrator is responsible also for setting up shared drives, print and application servers.
  - The AS/400 system operators, who is responsible for taking a periodic system and database backup, printing daily reports for all the departments. Moreover they are responsible for monitoring the AS/400 system activities and issue a daily report describing the overall system performance.
  - AS/400 system security analyst, who is responsible for reading and investigating AS/400 system logs, so as to know if any unauthorized access attempt occurred.
- The Victim's Bank help desk team takes all calls issued from all departments; the team investigates each call, and then issues for each call a case number either to the technical support or network team. In case of suspecting any security problem, the Incident handling team will be issued a case number, the case contains the issuer contacts and a brief description of that incident.

- Victim ‘s Bank has a well trained financial auditing team that takes care of any fraud or theft incident , this team is responsible of investigating the AS/400 database reports containing customers accounts and comparing it to the accounts activity movements .
- The Victim’s Bank password policy states that all user accounts must have a minimum password length of eight characters including numbers, alphanumeric and special characters, all passwords must be changed every three month, all accounts are disabled after three unsuccessful login attempts.
- The Victim’s Bank data integrity policy states that incremental backup is to run daily at end of day run process .Full backups are to be taken over the weekends, and at the end of each month. There is a complete offline AS/400 system located in another premise to be used as a backup system in case of full running current system failure. All backups are kept in a safe protected from theft and damage.

Incident handling Process

Victim’s bank has an incident handling team, this team was responsible for both computer and financial crimes, but this team as well as the bank‘s IT management did not pay attention to network threats originating from inside the network. By taking a look on the network architecture we notice that they paid attention to internet threats and ignored any internal network threats. They invested their money in buying perimeter and internal firewalls, even the intrusion detection sensor is placed in the DMZ network .They did not invest their money in installing a corporate anti-virus system, they thought that virus will propagate only by installing programs from either CD-ROMs, diskettes or from downloading content from the internet, so they restricted their access by all the employees except some executives.

The Victim’s bank incident handling team members are as follows:

- Senior level manager, who acts as a team leader, he is responsible for the communications between the team and the Board of directors and senior management, he prepares a high level report for senior management so as to help them taking clear decisions.

- Computer system security analyst, he is responsible for reading and investigating the IBM AS/400 system logs, moreover he translates what is found in logs to the financial analyst to help in comparing computer logs with real investigations.

- Helpdesk member representative, he is responsible for summarizing all incidents and builds a case of calls origin, i.e. he can determine who is reporting an incident and in which location it took place, he can also calculate the total amount of received calls as a result of an incident.

- Technical support member, he is responsible for investigating all client side related issues as well as all windows based servers log investigations.

- Financial analyst, he is responsible for investigating financial reports and comparing it to computer reports, then issue findings to the senior level manager.

- An outsourced financial auditor ,he has the same responsibility as the financial analyst , but his presence is a must so as to compare his findings with the financial analyst ,then both of them work together to complete the fraud report ,and gives it to the senior level manager.

- Network analyst, who is a member of the network support team as stated he is responsible for the local area network (LAN), and wide area network (WAN) connectivity and security. When an incident takes place, the network analyst starts to investigate the perimeter router logs in addition to firewalls and intrusion detection logs. Then he reports his finding to the senior level manager. Note that Victim's Bank has no team specialized in network security, all security activities are done by a network administrator.

- A member from the legal department, he is responsible to revise the case from the legal point of view before communicating it to the legal authorities.

- An administration assistant or a secretary, he is responsible to collect data from network and financial analyst reports, and construct the executive report with the assistance of the senior level manager.

- A member from the human resources department, he is responsible for applying the bank's employee's termination policy in case of an employee abusing computer usage.

When an incident is reported by the help desk team member to the incident handling team leader (senior manger level) he starts to communicate the team members -according to the type of incident- to start investigations. The incident can be either computer crime incident, or monetary fraud or both. Each incident is given a case number, the case number format is as follows "dd_mm_yy_ dept "for example if a case is opened on 19th march 2004 by the financial department the case will be given the number "19_03_04_finance".The team starts to work in the incident according to its severity. Any department can report a problem to the help desk team if they suspect in an incident, a case is issued immediately to the incident handling team leader. Old solved cases are kept in a safe in the computer room.

If the incident is monetary fraud, the team members will be:

- Team Leader
- Computer system analyst
- Financial analyst
- Outsourced financial auditor
- Human resources member
- Legal department member
- Secretary

If the incident is Computer crime, the entire Incident handling team must be present to collect evidence.

Identification:

In this section we shall describe how W32.Blaster.worm was identified by the incident handling team and what were the events confirming this was really a worm.

The incident took place last year; it was Monday, 18 August 2003. The Victim's bank headquarter opened its doors for customers at 8:30 am as usual and all banking activity was running normally. Mr. Bad Guy planned to exploit the bank network from his car using the bank wireless network (as stated before).

- Monday, 18 August 2004. 10:00 am Cairo local Time (CLT)

Mr. Bad Guy was sitting in his car connecting the infected Laptop containing the W32.Blaster.worm on the Victim's Bank wireless network, his laptop easily obtained an IP address from the bank's corporate network and the worm started propagating infecting the overall network.

- Monday, 18 August 2004. 1:00 pm CLT

The bank's front counter containing all the tellers' windows based workstations were facing a great crowd, and the tellers were complaining that they have some delay in the cashier banking applications. After a while the windows based ATM machines were displaying the "out of service" notice on its front screen.

- Monday, 18 August 2004. 1:05 pm CLT

The Helpdesk team received several calls from the tellers and customer service employees located in the ground floor; they reported that severe delay is facing all their banking applications. Immediately the helpdesk opened a case number for the responsible technical support engineer for handling the problem.

- Monday, 18 August 2004. 1:10 pm CLT

The technical support engineer went to the tellers and customer service area; he investigated some machines and reported back to the helpdesk that all the machines were facing network problems.

- Monday, 18 August 2004. 1:15 pm CLT

After some time the ATM control room reported to the helpdesk that they lost communications with all the ATM machines. The helpdesk opened another case number for the responsible network support engineer. After 15 minutes the help desk received a call from all remote sites reporting that the communications between headquarter and remote sites are extremely slow. The helpdesk opened another case number for the network support engineer. And finally the helpdesk representative in the incident handling team suspected that they might facing an incident, so he issued a case number to the incident handling team with a high severity to start investigating.

- Monday, 18 August 2004. 1:30 pm CLT

The incident handling team started making their own investigations, all the team were directed to the tellers and customer service area. At first the technical support engineer took a further look on one of the machines facing delay, he noticed that the machine processor is busy, after taking a look on the windows task manager he realized that there is a task named msblast.exe which is allocating a lot of the memory usage (see fig 2).The technical support engineer reported what he found to be used for further investigations. The network support engineer started to update the signature of the network sensor located in the DMZ from the vendor web site, he managed to change the location of the DMZ network sensor to the infected network, and he connected the network sensor to a spanning port on the infected network Ethernet switch to start monitoring all the traffic passing through that switch. He managed also to install a network sniffer on his Linux based laptop for monitoring packet behavior .He noticed a high activity traffic containing some IP addresses not belonging to the network range, also the increased activity were of TCP ports 135, 4444 and UDP 69 (see the following logs)

```
1:10:40.395032 192.168.10.1.1294 > 192.168.10.3.135: tcp 0
1:10:40.395323 192.168.10.3.135 > 192.168.10.1.1294: tcp 0
1:10:40.395436 192.168.10.1.1294 > 192.168.10.3.135: tcp 0
1:11:41.508095 192.168.10.1.1294 > 192.168.10.3.135: tcp 72
1:11:41.508310 192.168.10.1.1294 > 192.168.10.3.135: tcp 1460
1:11:41.508346 192.168.10.1.1294 > 192.168.10.3.135: tcp 244
1:11:41.508362 192.168.10.3.135 > 192.168.10.1.1294: tcp 0
1:11:41.508541 192.168.10.3.135 > 192.168.10.1.1294: tcp 60
1:11:41.508681 192.168.10.1.1294 > 192.168.10.3.135: tcp 0
1:11:41.508720 192.168.10.3.135 > 192.168.10.1.1294: tcp 0
1:11:41.512201 192.168.10.3.135 > 192.168.10.1.1294: tcp 0
1:11:41.512346 192.168.10.1.1294 > 192.168.10.3.135: tcp 0
```

```
1:11:41.904949 192.168.10.1.1314 > 192.168.10.3.4444: tcp 0
1:11:41.905031 192.168.10.3.4444 > 192.168.10.1.1314: tcp 0
1:11:41.905160 192.168.10.1.1314 > 192.168.10.3.4444: tcp 0
1:11:41.952874 192.168.10.3.4444 > 192.168.10.1.1314: tcp 42
1:11:41.984939 192.168.10.1.1314 > 192.168.10.3.4444: tcp 36
1:11:41.985029 192.168.10.3.4444 > 192.168.10.1.1314: tcp 63
1:11:42.083469 192.168.10.3.1049 > 192.168.10.1.69: udp 20
1:11:42.118800 192.168.10.1.69 > 192.168.10.3.1049: udp 516
```

And finally the network support engineer took a look on the IDS signatures; he noticed that the following signatures were reported “TFTP_MSBlaster_Worm” and “TFTP_MSBlaster_Attempt”; these were the signatures of the W32.Blaster.worm.

The network support engineer visited the IDS vendor web site (http://www.iss.net/db_data/xpu/RSNSNS_21.1.php)for calculating more information regarding his findings; he also visited one of the anti-virus websites (http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html)to start comparing the worm activity with his findings.

- ❑ Monday, 18 August 2004. 2:00 pm CLT

The technical support engineer and the network support engineer, concluded in their report that the bank is facing a virus outbreak, they confirmed their investigations by placing the antivirus and ids vendors website links in their draft technical report. But still the network support engineer is wondering how the worm reached the internal network? By taking a look on the network diagram, he is quite sure that the virus did not reach the internal corporate network from the internet due to restrictive firewall rule-base policy; it must be originated from the internal network itself. He is wondering also, why the propagation originated from the ground floor, and not from any other location? Finally the network support engineer started to examine the development wireless access points located near the tellers’ area in the ground floor. He noticed that the signal is detected outside the bank premise; more over it is detected in the parking area .Now he is sure that the attack is originated from outside the bank premise directly to the internal network by an infected windows machine. The final technical report highlighted the Virus outbreak incident and how it reached the internal network.

Containment

In this section we shall see how Victim's Bank managed to keep the problem from getting worse. The Victim 's Bank daily working hours are from 8:30 am till 5:00 pm ,for five days a week .The week end vacation is every Friday and Saturday .The customer visiting period is from 9:00 am to 2:00 pm . All ATM and mobile banking applications are always available. The problem was identified to be a virus outbreak at 2:00 pm, i.e. at the end of the customer visiting period. The bank faced almost one hour of down time at the first day, so a broadcast massage was sent on the internal voice system apologizing to the customers on that downtime and explaining to them that they are managing to correct a technical problem.

❑ Monday, 18 August 2004. 2:30 pm CLT

The Bank's network gradually got congested and all banking applications and activities got parallelized. By that time the incident handling team leader managed to arrange a containment plan, and communicated it to the senior directors for approvals .The plan consists of the following steps:

- All banking activities will be resumed manually, no computer intervention is required.
- All non IT employees are requested to come two hours early the next day than their usual arrival time for manual data entry, and application testing.
- The network support team must disable all wireless access points located in all sites.
- All technical support, windows administrators and helpdesk staff must work together to contain the virus outbreak incident, this team will be called the virus defending team.
- The leading person will be the network support engineer.
- The Technical support team is to construct a CD containing a virus removal tool, antivirus software for 30 days evaluation license as well as the required Microsoft patch.
- The virus removal instructions will be printed and distributed on all the support staff to start removing the virus from all the machines.
- Network support engineers will detect infected area, and isolate the head quarter site from all remote sites so as to limit the virus propagation.
- The team will start removing the virus from all the infected windows application servers and ATM machines then from all the client workstations.
- Last clean database backup is to be restored on all the database systems after the incident is cleared.

The virus defending team was fifteen engineers consisting of ten technical support engineers and five windows 2000 administrators; while the networks support team was five engineers.

The incident handling team “jump Kit” consists of some simple tools, these tools will help in investigating and identifying the attack origin. These tools are:

- Windows resource Kit
- Latest anti-virus software
- Blank IDE drive
- Two direct cat5 cables and one crossover
- Dual boot laptop (Windows and Linux)
- Flashlight
- Wireless Ethernet card
- Notebook and pencils
- Cellular phone and one extra battery

Now the team is ready to start removing the virus from all windows servers and workstations.

Eradication

In this section we shall describe the detailed steps for removing the W32.Blaster.worm from all systems .As described before the incident handling team recognized the attack to be a virus attack. By surfing the vendor’s antivirus web sites, the incident handling team knew exactly how to remove completely the worm. The worm removal can be done by one of two methods either manual removal or by using an antivirus removal tool:

- Manual Removal :

  - Restoring internet connectivity: This can be done on both Windows 2000 and Windows XP; restoring internet connectivity can be done by applying the following steps :
    - Click Start > Run. - The Run dialog box appears
    - Type: “SERVICES.MSC /S” in the open line, and then click OK. The Services window opens.
    - In the right pane, locate the Remote Procedure Call (RPC) service.
    - Right-click the Remote Procedure Call (RPC) service, and then click Properties.
    - Click the Recovery tab.
    - Using the drop-down lists, change First failure, Second failure, and Subsequent failures to "Restart the Service."
    - Click Apply, and then OK.

- Ending the Worm process: This can be achieved by :
    - Press Ctrl+Alt+Delete once.
    - Click Task Manager.
    - Click the Processes tab.
    - Double-click the Image Name column header to alphabetically sort the processes.
    - Scroll through the list and look for Msblast.exe
    - If you find the file, click it, and then click End Process.
    - Exit the Task Manager.
- Obtaining the latest virus definitions: This can be done by visiting one of the vendor antivirus websites and download the latest virus definition update. In the Victim's Bank case the incident handling team managed to download a 30 days evaluation version of Symantec antivirus, and then remove it after the case is closed.
- Reversing the changes made to the registry : In this step we shall reverse the changes which was done by the worm , this can be achieved by applying the following steps :
    - Click Start, and then click Run. (The Run dialog box appears.)
    - Type regedit, and then click OK. (The Registry Editor opens.)
    - Navigate to the Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run
    - In the right pane, delete the value: windows auto update
    - Exit the Registry Editor.
- Scanning for and deleting the infected files: this can be done by Starting Symantec antivirus program, configure it to scan all files, and then delete infected files.

- Antivirus Removal Tool: This removal Tool undergo the following activities: [15]

    - Terminates the W32.Blaster.Worm viral processes.
    - Deletes the W32.Blaster.Worm files.
    - Deletes the dropped files.
    - Deletes the registry values that have been added.

    This tool can be easily downloaded from Symantec web site: http://securityresponse.symantec.com/avcenter/FixBlast.exe

For more information regarding the W32.Blaster.worm removal instructions refer to the following links:

http://securityresponse.symantec.com/avcenter/FixBlast.exe http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html

Back to our case, the virus defending team began his job, the job was so hard, and they had to spend hours and hours removing the worm from all the systems, the detailed scenario was as follows:

- Monday, 18 August 2004. 3:00 pm CLT

As stated in the incident handling plan, the first thing is to complete the daily business work manually with no computer intervention, all employees rather than the IT staff completed their work ,this procedure is done to overcome any lost of data , moreover all manual data will be submitted to the database after the incident clears. All non IT employees were requested to come the next day two hours early so as to start the manual data entry, moreover to test the banking applications after last day infection.

During that time the development wireless access points were disabled from the network, this was done to prevent any unauthorized access from reaching the AS/400 database. Moreover all the bank's remote offices were isolated from the main infected headquarter, this preventive action was done to limit the worm from infecting remote sites .Site to site communications were stopped also to prevent infected branch office from infecting clean ones (due to a star topology network).

- Monday, 18 August 2004. 3:10 pm CLT

The virus defending team started their hard job; they had to get the total system hardware inventory record to calculate the total number of windows machines, the number of machines were thirty windows based ATM machines, one hundred windows 2000 professional machines and twenty windows 2000 servers, this make a total number of one hundred fifty machines that must be cleaned before the bank's next day opening.

At first the windows 2000 servers and the windows based ATM machines must be cleaned , so as to allow employees using clean workstations to connect and start their work ,moreover to allow external customers use the ATM machines as the ATM machines reflects the bank's image to all customers .

The virus removal CDs and instructions were printed and distributed among the virus defending team, the CDs were labeled "W32.Blaster.Worm" removal tool these instructions were as follows:

- Insert the CD in the CD-ROM drive
- Double Click on "Blaster CD"
- Choose your operating System folder.
- Choose the "Patch Folder" &run the file
- Choose the "removal tool" & run the file

- Install the Evaluation Copy Symantec Antivirus Software.
- Install the latest "AV Update "& run the file.

The Defending team tasks were divided as follows:

- Each window 2000 server administrator will remove the virus from four servers and restore last day clean database backup.
- Each technical support will remove the virus from ten workstations and three ATM machines.

By calculating the over all tasks we find that five administrators having the first task will remove the virus from the twenty servers, while ten technical support engineers will remove the virus from hundred workstations and thirty ATM machines. The estimated time for completing the task is twelve hours; these twelve hours are calculated as follows:

- Four hours are taken by each windows administrator for total servers' recovery.
- Simultaneously, eight hours by each technical support for complete ATM and workstations recovery.

Let's take an example of what a technical support or a Windows administrator will do to remove the infecting worm from the machines. The removal steps are illustrated in the following screen-shots:

1. The CDs contents are shown as follows in the infected machines:

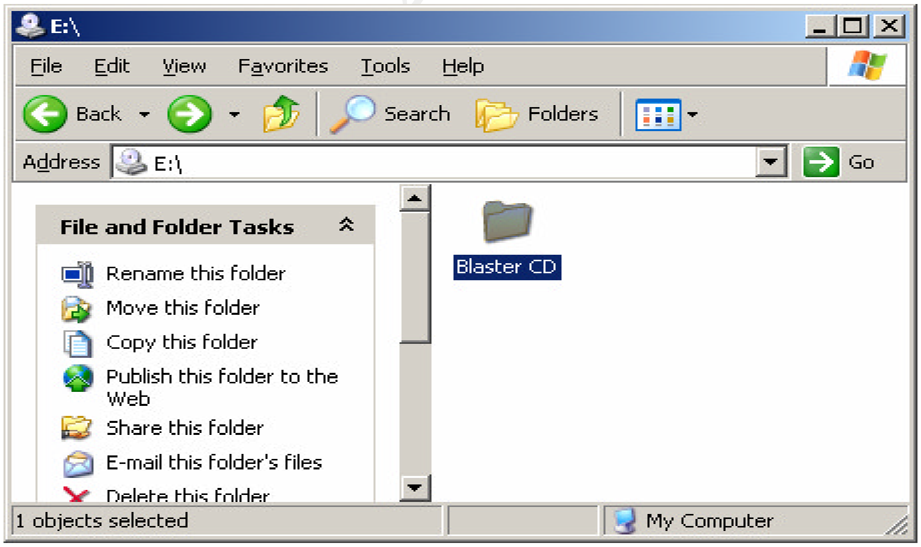


Fig.12 Shows the contents of the "W32.Blaster.Worm" removal tool CD.

2. The Blaster Folder contains three folders representing the infected windows operating systems.

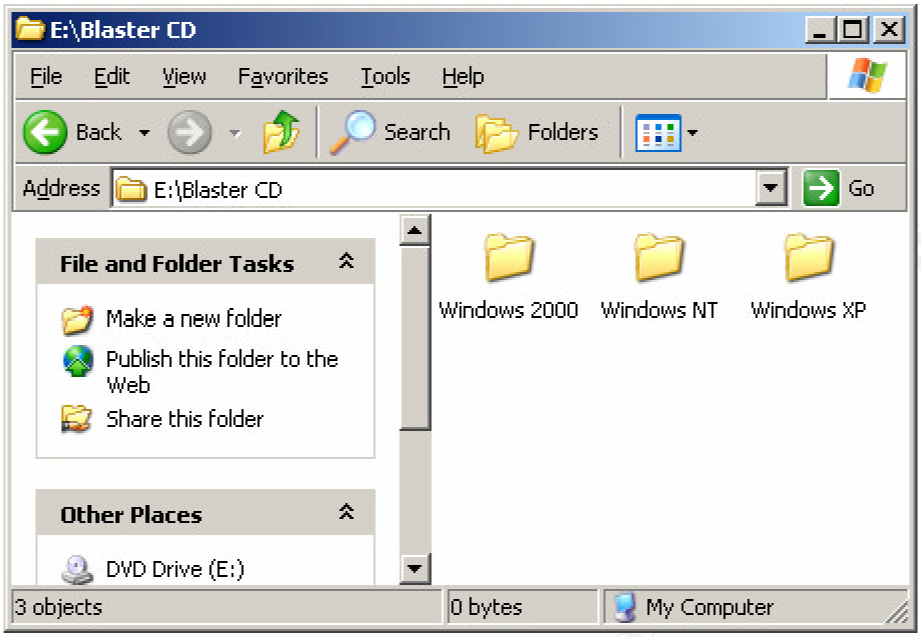


Fig.13 Shows the how this CD can be used for various operating systems.

3. Each folder of the three folders contains the required Microsoft patch, Symantec removal tool and the latest Antivirus update file.

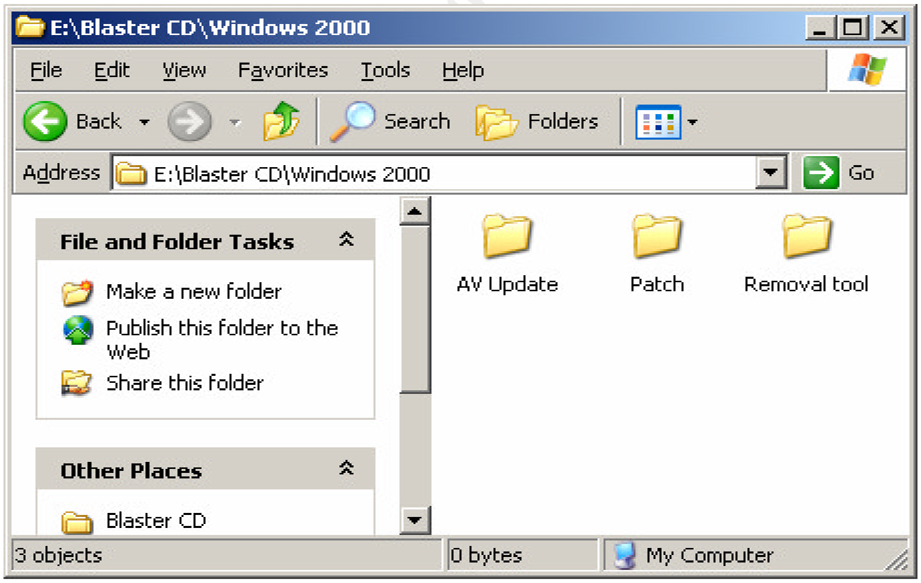


Fig.14 Shows the recovery tools per operating system.

4. The first step of recovery is done by installing the required Microsoft patch; the installation is a straight forward procedure.

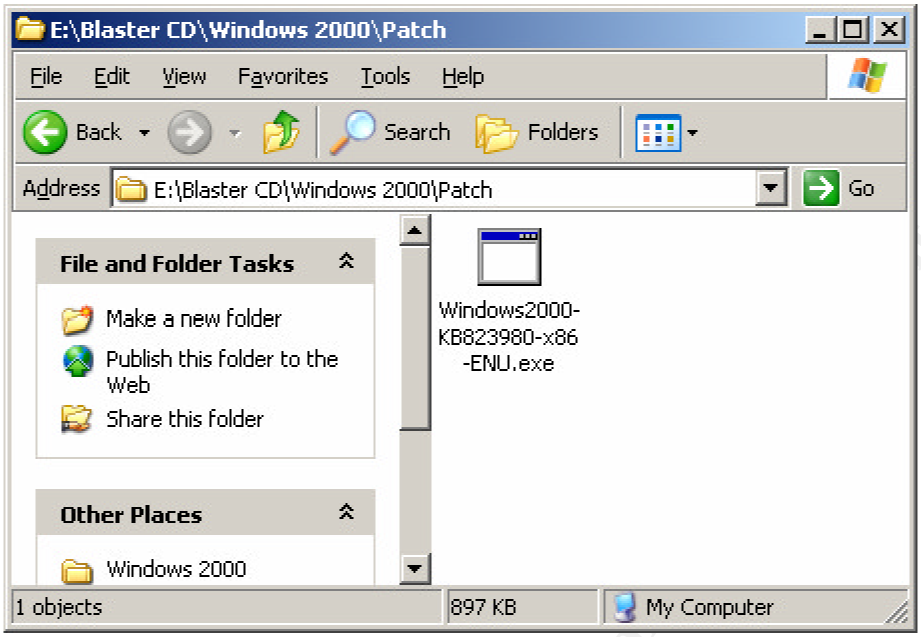
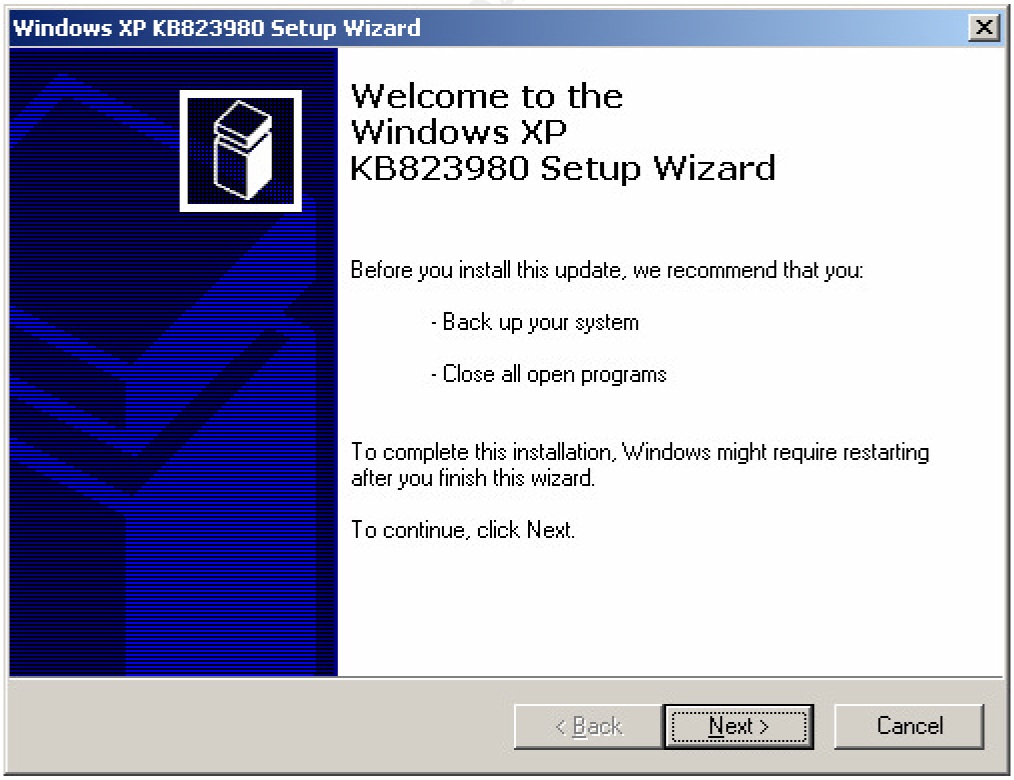

E:\Blaster CD\Windows 2000\Patch
File Edit View Favorites Tools Help
Back Search Folders
Address E:\Blaster CD\Windows 2000\Patch Go
File and Folder Tasks
Make a new folder
Publish this folder to the Web
Share this folder
Other Places
Windows 2000
Windows2000-KB823980-x86-ENU.exe
1 objects
897 KB
My Computer

Fig.15 Shows the Microsoft patch file name.

5. The installation starts by double clicking the required patch file "windows2000KB823980-X86-ENU.exe"


Windows XP KB823980 Setup Wizard

Welcome to the Windows XP KB823980 Setup Wizard

Before you install this update, we recommend that you:

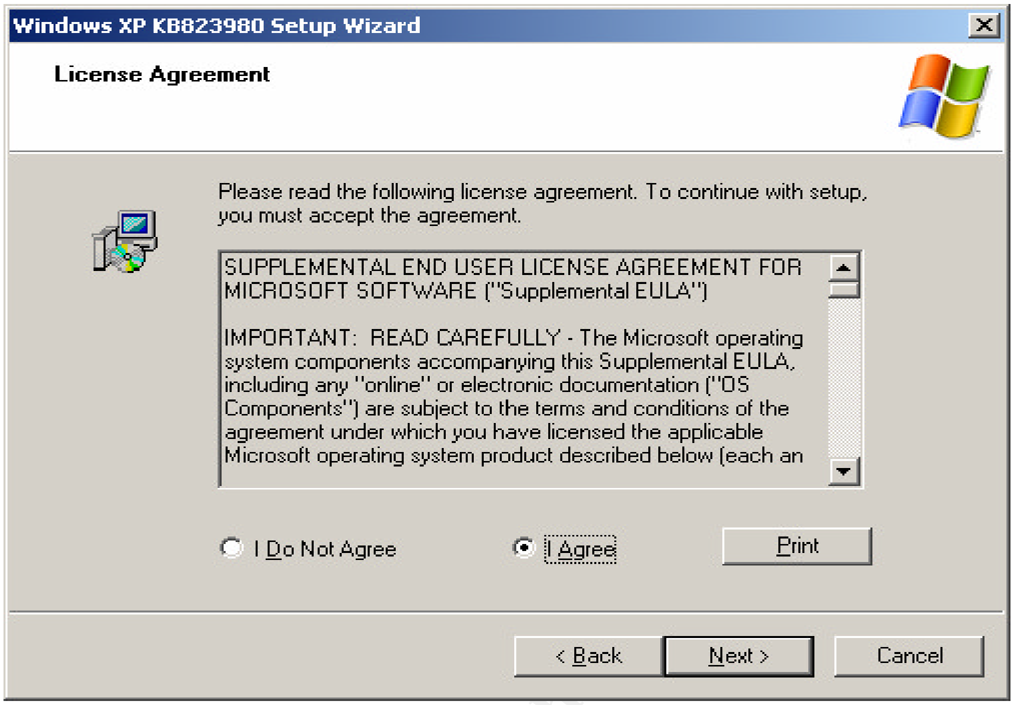
- Back up your system

- Close all open programs

To complete this installation, Windows might require restarting after you finish this wizard.

To continue, click Next.

6. By pressing next the installation will continue straight forward, see below.



Windows XP KB823980 Setup Wizard

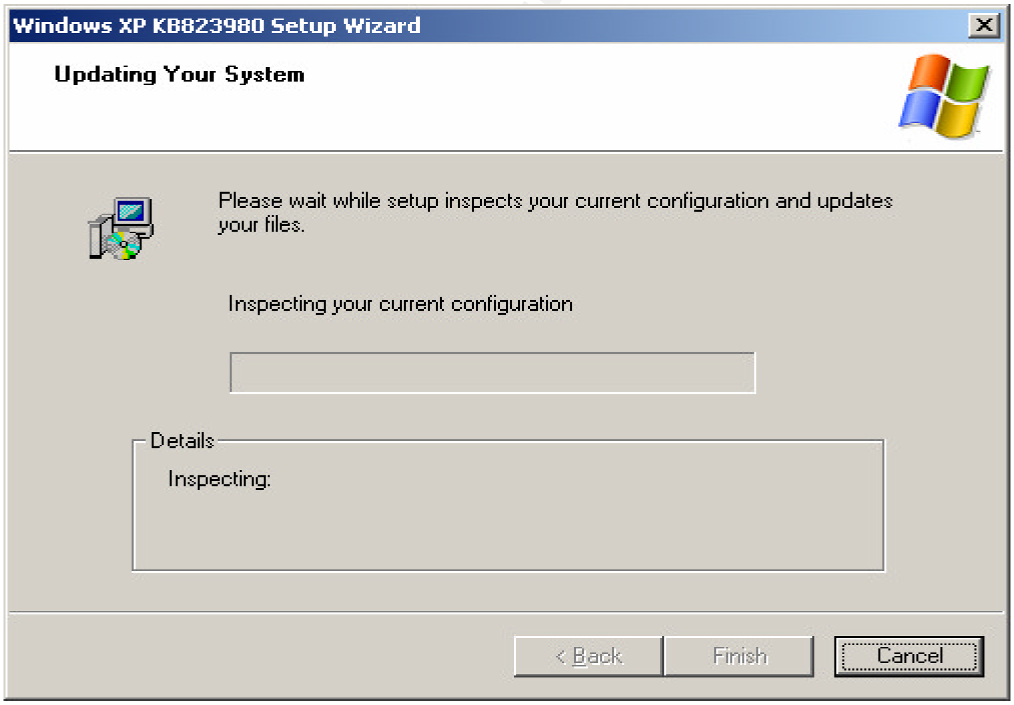
License Agreement

Please read the following license agreement. To continue with setup, you must accept the agreement.

SUPPLEMENTAL END USER LICENSE AGREEMENT FOR MICROSOFT SOFTWARE ("Supplemental EULA")

IMPORTANT: READ CAREFULLY - The Microsoft operating system components accompanying this Supplemental EULA, including any "online" or electronic documentation ("OS Components") are subject to the terms and conditions of the agreement under which you have licensed the applicable Microsoft operating system product described below (each an

○ I Do Not Agree ● I Agree



Windows XP KB823980 Setup Wizard

Updating Your System

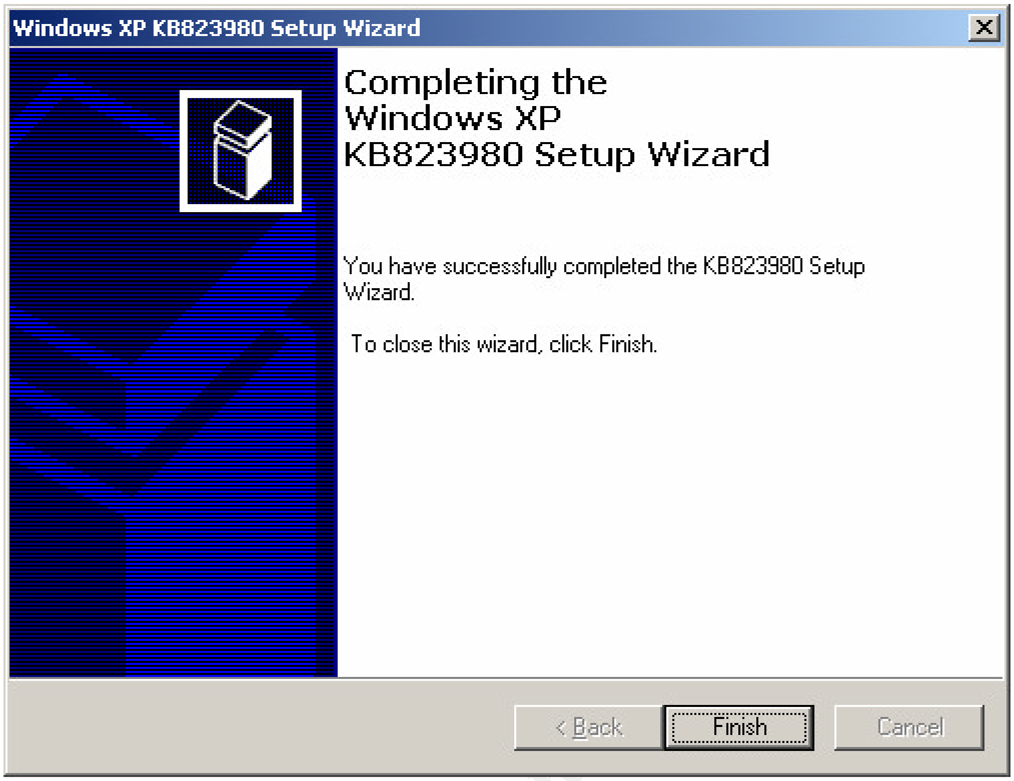
Please wait while setup inspects your current configuration and updates your files.

Inspecting your current configuration

Details

Inspecting:

7. By clicking "Finish "the required patch is now installed successfully.



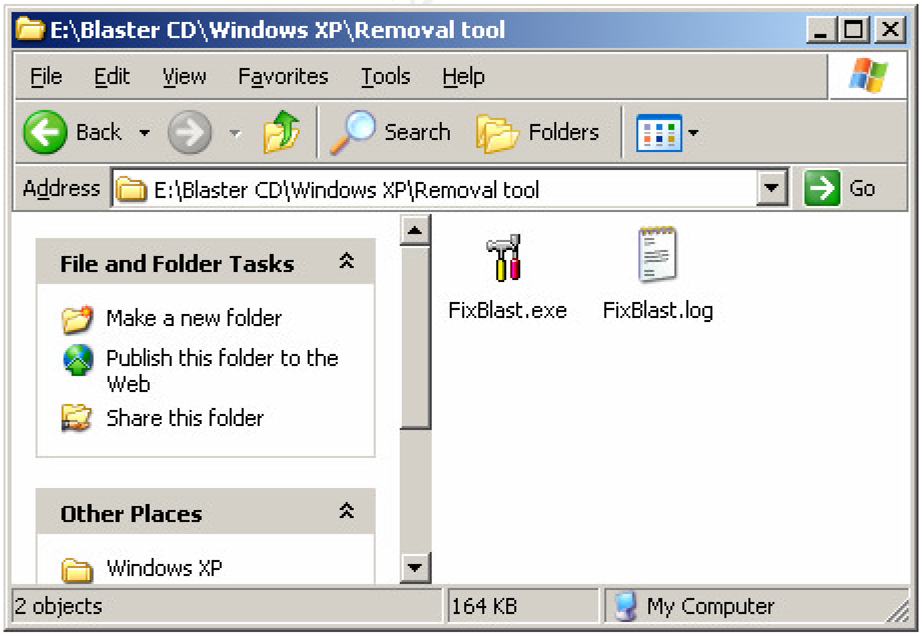
Completing the Windows XP KB823980 Setup Wizard

You have successfully completed the KB823980 Setup Wizard.

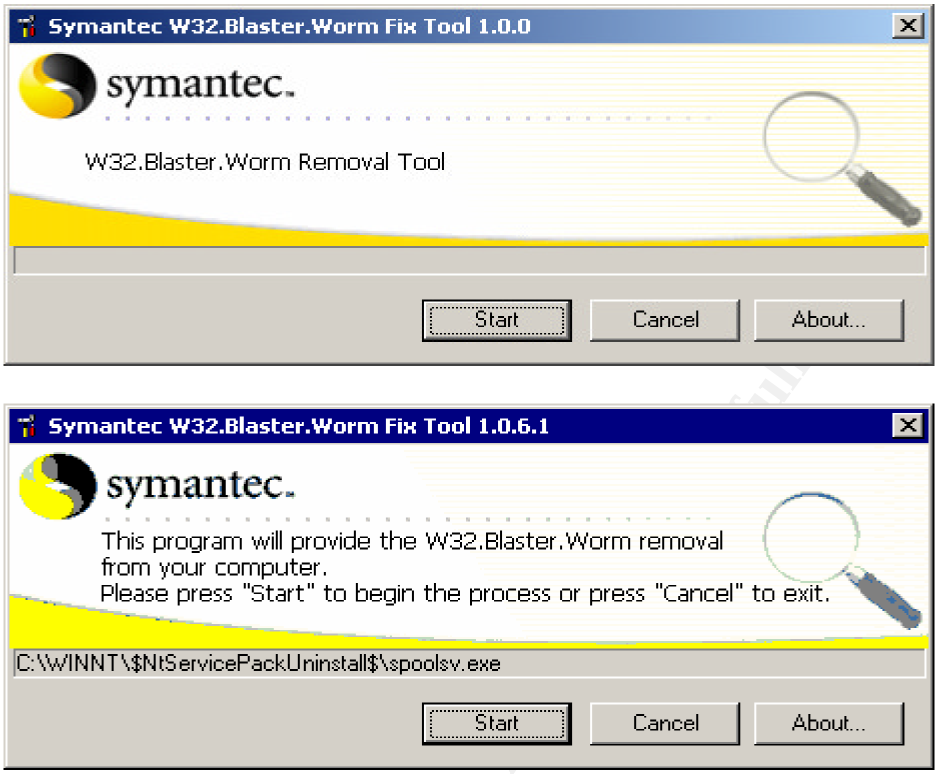
To close this wizard, click Finish.

Fig.16, 17, 18, 19 Shows the Microsoft patch installation steps.

8. The next step to complete the virus removal is to run the antivirus removal tool. This is achieved by double clicking the file "FixBlast.exe"



9. The Removal tool will directly launch, and by clicking start button the tool will start to scan and remove the infecting worm.



Symantec W32.Blaster.Worm Fix Tool 1.0.0

W32.Blaster.Worm Removal Tool

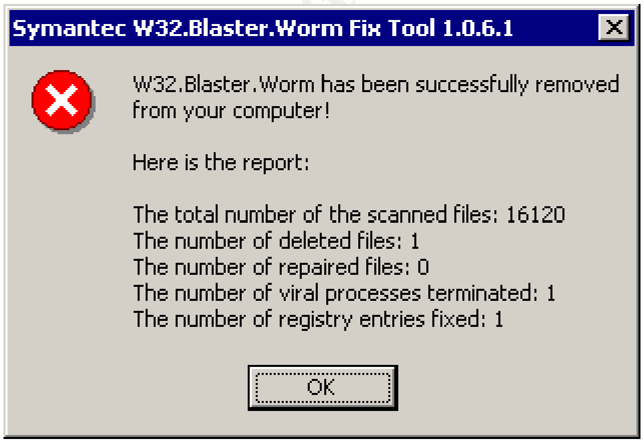
Symantec W32.Blaster.Worm Fix Tool 1.0.6.1

This program will provide the W32.Blaster.Worm removal from your computer.
Please press "Start" to begin the process or press "Cancel" to exit.

C:\WINNT\$NtServicePackUninstall$\spoolsv.exe

Fig.20, 21, 22 Shows how Symantec W32.Blaster.worm removal tool works.

10. After the tool finishes scanning it displays the resulting report screen, also the report can be viewed in the log file "FixBlast.log"



Symantec W32.Blaster.Worm Fix Tool 1.0.6.1

W32.Blaster.Worm has been successfully removed from your computer!

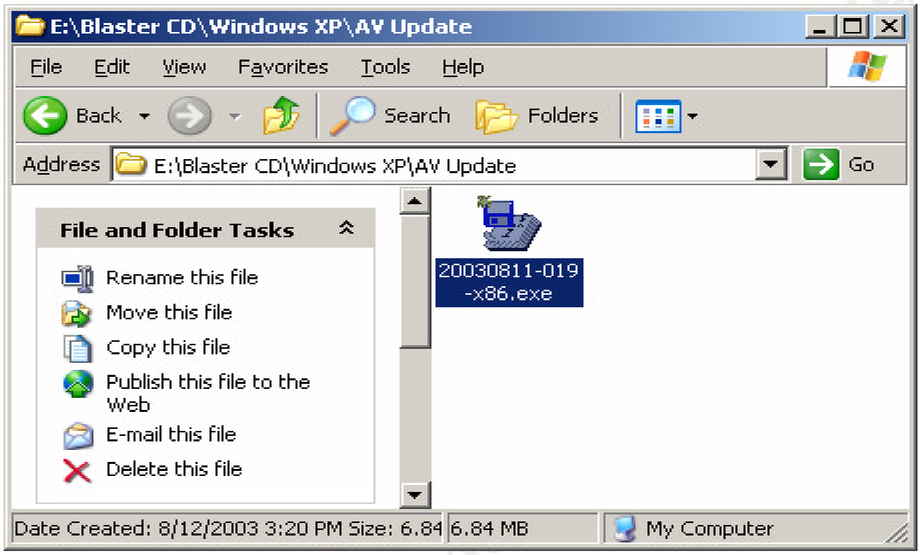
Here is the report:

The total number of the scanned files: 16120
The number of deleted files: 1
The number of repaired files: 0
The number of viral processes terminated: 1
The number of registry entries fixed: 1

Fig. 23 Shows Symantec removal tool report.

Note that the report contains the total number of scanned files, the number of deleted files, and number of repaired files, number of registry entries fixed and the number of vital processes terminated.

The final step of keeping the machines away from the being exploited again is to install the antivirus software and its latest updates. In our case we shall use Symantec anti virus evaluation license as mentioned before , this will be used as a temporary solution till the bank buy a licensed Corporate Symantec antivirus license. Below we shall see how Antivirus updates are to be installed manually by the technical support.



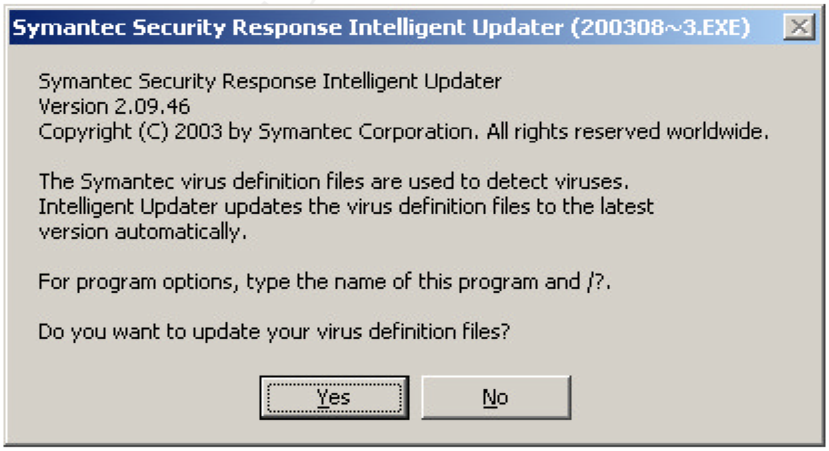
Address: E:\Blaster CD\Windows XP\AV Update

20030811-019-x86.exe

Date Created: 8/12/2003 3:20 PM Size: 6.84 | 6.84 MB

Fig. 24 Shows Symantec antivirus updates Filename.

The Technical Support just double click on the update executable fie “20030811-019-X86.exe”, then the file self extract it self and the virus definition updates are added to the antivirus software, the figures below illustrate the operation.



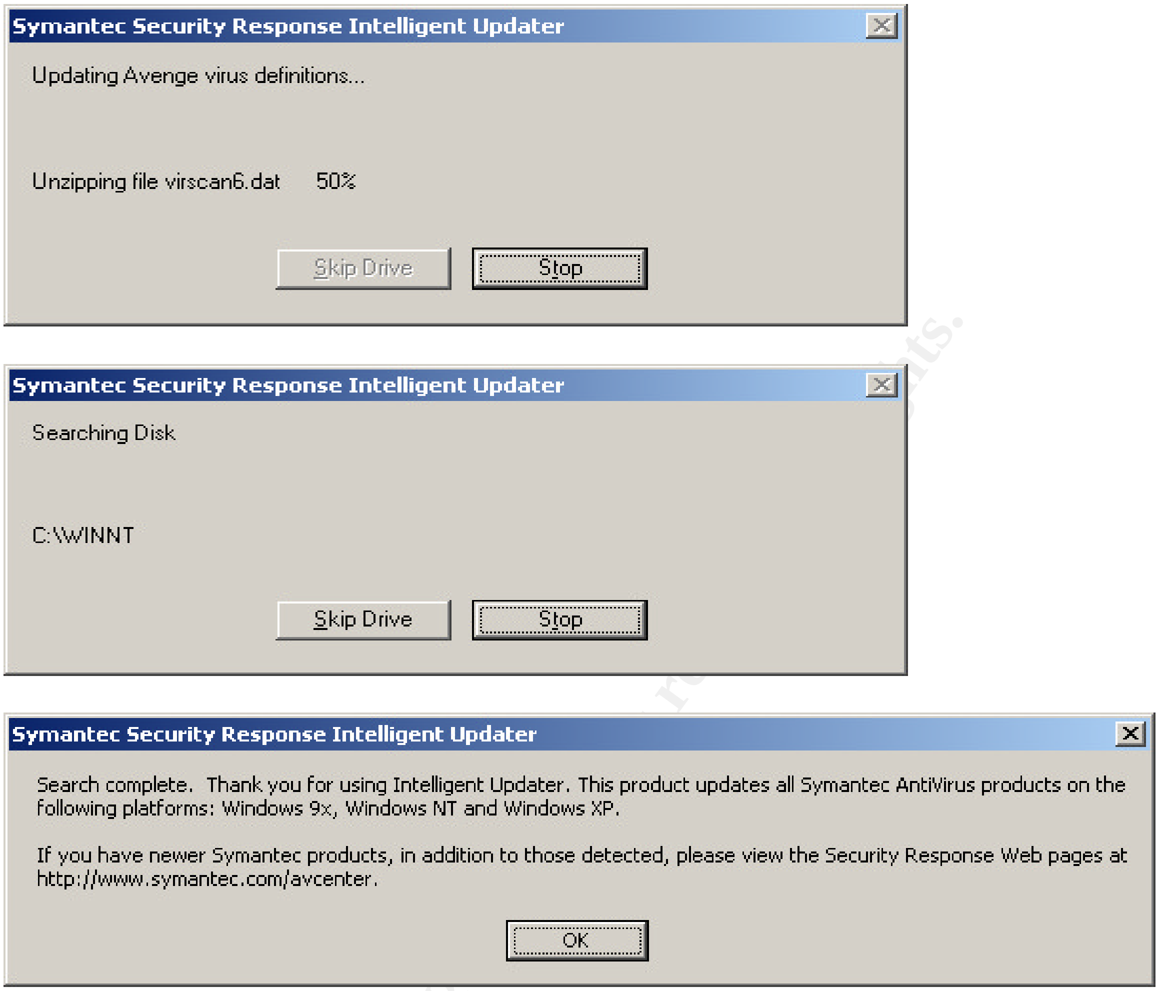
Symantec Security Response Intelligent Updater (200308~3.EXE)

Symantec Security Response Intelligent Updater
Version 2.09.46
Copyright (C) 2003 by Symantec Corporation. All rights reserved worldwide.

The Symantec virus definition files are used to detect viruses.
Intelligent Updater updates the virus definition files to the latest version automatically.

For program options, type the name of this program and /?.

Do you want to update your virus definition files?



Symantec Security Response Intelligent Updater

Updating Avenge virus definitions...

Unzipping file virscan6.dat   50%

Skip Drive
Stop
Symantec Security Response Intelligent Updater

Searching Disk

C:\WINNT

Skip Drive
Stop
Symantec Security Response Intelligent Updater

Search complete. Thank you for using Intelligent Updater. This product updates all Symantec AntiVirus products on the following platforms: Windows 9x, Windows NT and Windows XP.

If you have newer Symantec products, in addition to those detected, please view the Security Response Web pages at http://www.symantec.com/avcenter.

Fig. 25, 26.27.28 Shows Symantec antivirus updates file operates.

- Tuesday, 19 August 2004. 3:00 am CLT

The Windows administrators and the technical support engineers finished their tasks in the due expected time, mean while the network support engineers where monitoring traffic on the banks network using their network sensor. By that time the network congestion is limited and the ATM machines started communicating again with its main switch, and were back to service. The technical support team tested the banking client-server applications and ensured that the communication was normal.

Recovery

In this section we shall describe how the bank was back to business, and how the incident handling team was quit sure that the network is virus free.

- Tuesday, 19 August 2004. 6:30 am CLT

As mentioned before all non IT employees were asked to come two hours early the next day of infection , this was for two reasons ,the first one was to test the overall banking applications after being cleaned from virus infections ,while the second reason was to complete the data entry of the day before.

The entire virus defending team slept in the bank that day so as to be ready for the employees the early morning .When the employees started their data entry, every thing seemed to be normal, moreover the intrusion detection network sensor did not detect the W32.Blaster.worm signatures again "TFTP_MSBlaster_Worm" and "TFTP_MSBlaster_Attempt". Also windows 2000 administrators restored last clean database backup, ATM machines were operational since today at 3:30 am. The technical support team started a random manual scan on some windows 2000 professional machines. They scanned the machines' hard drives but no virus was found, also they viewed windows task manager for the MSblast.exe process, and was not found (see fig.2).

By now all windows machines are installed with updated antivirus software with the required Microsoft patch installed, this will minimize the probability of being infected again with the same worm.

The network support engineers disabled all development wireless access points, for reconfiguring it again with security precautions. They walked around outside the bank premises to detect the wireless signal but no signal detected. All remote sites are connected to the main headquarter and centralized database is accessed by all branch offices.

The incident handling team, contacted the helpdesk team to know exactly the types of calls and how frequently they are , this is know if any one was still infected or not, but the helpdesk reported that every thing is normal.

Lessons Learned

In the next day, the help desk calls and network traffic measures were normal. All banking applications were working fine and the customers did not complain any performance issue.

- Tuesday, 20 August 2004. 10:30 am CLT

The Incident handling team arranged for a meeting to discuss the reasons why the incident took place, and to prepare an executive summary describing the recommendations for not allowing such an incident to occur again.

The technical support and the network support reports described in details how this incident took place, and highlighted on some weak points in the Victims Bank network, the weak points are as follows:

- The lack of a centrally managed Antivirus solution .If a centrally antivirus server is installed on the network, with an automatic virus definition update service enabled, the updates would be automatically pushed on the workstations and servers preventing it from being infected by any virus.
- The lack of a centralized windows-update solution. If a centralized windows update server is installed on the network, the required windows update patches would be automatically installed on the clients and servers correcting the vulnerability exploited by the virus.
- The Lack of internal host-based and network based intrusion detection system. Although the Victim's Bank had a network sensor placed in the DMZ network, the internal network including all mission critical systems is lacking the presence of any sensor. If network sensors were scattered among the bank critical subnets, and these sensors were updated with the W32.Blaster.Worm signature detection, the worm traffic could be easily identified and the originating traffic would be reset by the network sensor placed on that subnet .Moreover the server sensors if installed on critical servers would have protected these servers from being infected even if the patch is not installed by applying its virtual patching feature.
- Locating development devices on the internal network with default factory setting could cause security weakness. As mentioned before the wireless access points were installed with default factory settings these factory settings allows any machine to connect to the wireless access point without any restrictions ,these settings are summarized as follows:[16]

  - <u>Default configured Server Set ID (SSID):</u>
    SSID is a configurable identification that allows clients to communicate with an appropriate wireless access point. SSID acts as a shared password between the wireless access point and the clients, so only clients with correct SSID can communicate with the wireless access point. The Risk in default configured SSID is that these wireless access points can be easily compromised.
  - <u>Disabled Wired Equivalent Privacy (WEP):</u>
    WEP is the method of encrypting wireless traffic; WEP can be configured with 40 bit encryption, 128 bit encryption, or no encryption at all. Most default wireless access points factory setting disables WEP, allowing SSID to be transmitted on the air as a clear text. So if any one is monitoring the network, the SSID can be easily detected.
  - <u>SNMP Community password:</u>
    SNMP is used for remote management. SNMP requires a community word or a password, if the community word is left on the factory default value, an intruder can read and write sensitive data on the wireless access point.
  - <u>Configuration Interfaces:</u>
    Most access points have configuration interfaces enabled by default with a default password .This interface is used for remote management and configuration purposes. Wireless access points can use telnet, web, serial and SNMP services for management interfaces. If an intruder knows the default management interface password, he can easily connect to the wireless access point and modify running configuration.
- Lack of network segmentation. Victim's Bank local area network has a remarkable design weakness; it is constructed of one Cisco 5000 series layer two backbone switch and all edge switches connected to that backbone. By taking a look on the network topology we can realize that all the head quarter network in on one logical subnet. If the network was subnetted, it would be easily for the network support engineer to isolate the infected subnet from the rest of the network leading to minimize the virus propagation impact.

The incident handling team prepared an executive summary describing briefly the incident; and highlighted upon recommendations and action items that must be taken to prevent such an incident to occur again. The recommendations were as follows:

- A security administrator must be hired; he will be responsible for all operational security functions, such as firewall administration and configuration, intrusion detection implementation and log analysis, antivirus daily operation tasks.

- There must be a licensed brand-name central management antivirus server such as Symantec Corporate Edition .The main role of that server is to push automatically latest virus definition updates to all workstations and servers.
- Deploy a central windows update server, example Microsoft Software Update Service (SUS) which is designed to update all client workstations and servers automatically with windows critical security patches.
- Install Intrusion detection server sensors and network sensors on selected mission critical network segments to detected worm syndromes early.
- Subscribe in an online vulnerability alerting services such as Symantec Deepsite Alert, this service is responsible for sending alerts such as mails and SMS for all subscribers in case there is a new virus or vulnerability found in a well known systems or operating system, this can act as an early alerting tool .
- Never connect any development device on a production network, moreover construct a development network for testing any new systems or devices.
- Security awareness sessions should be held for all technical support, network support and helpdesk team. These sessions will highlight upon virus activities and social engineering techniques.
- Wireless security should be taken into consideration ,any wireless access point joining the network should be installed with a customized setup that meet the bank's security requirements, this customized setup should include : [16]
    - Removing default factory configuration and change all default passwords.
    - The wireless access point SSID should consist of a complex combination to be difficult for guessing and WEP must be enabled with a 128 bit encryption.
    - The access point must undergo client authentication, this can be achieved by basic MAC address filtering or by user authentication against radius server or active directory.
    - Wireless access points power should be adjusted. This is essential for controlling the access point coverage and preventing signals to extend outside the bank's premises.
    - Wireless access client configuration inputs should be securely stored. This can be done by storing the SSID in a windows registry key, and the WEP key in the firmware where it is difficult to access.
    - Wireless access points should enable all traffic to be encrypted using PPTP or IPSec as well as dynamic session tokens.

- Construct monthly follow up meetings with all concerned parties to see how these recommendations are developed and solve any problems causing delay.

References:

[1] Trend Micro. (2004) Glossary of Virus Terms .Retrieved March 15, 2004 from:

http://www.trendmicro.com/en/security/general/glossary/overview.htm#Worm

[2] Symantec Security Response (2004) .Win32.Blaster.Worm .Retrieved March 16 2004 from:
http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html

[3] Trend Micro. (2004) Virus Encyclopedia (WORM_MSBLAST.A). Retrieved March 16, 2004 from:
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A

[4] Sophos virus analysis (2004). W32-Blaster-A .Retrieved March 17, 2004 from:

http://www.sophos.com/virusinfo/analyses/w32blastera.html

[5] Microsoft Security Bulletin (MS03-26) 2004. Retrieved March 18 2004 from:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp

[6] Sophos virus analysis W32-Blaster-B.htm (2004) .Retrieved March 18, 2004 from:
http://www.sophos.com/virusinfo/analyses/w32blasterb.html

[7] Blaster worm variants discovered, Sophos Anti-Virus provides protection Retrieved March 18, 2004 from:
http://www.sophos.com/virusinfo/articles/blaster2.html

[8] Sophos virus analysis W32-Blaster-D.htm .Retrieved March 19, 2004 from:
http://www.sophos.com/virusinfo/analyses/w32blasterd.html

[9] Sophos virus analysis W32-Blaster-E.htm.Retreived March 19, 2004 from:
http://www.sophos.com/virusinfo/analyses/w32blastere.html

[10] Sophos virus analysis W32-Blaster-F.htm.Retrieved March 19, 2004 from:
http://www.sophos.com/virusinfo/analyses/w32blasterf.html

[11] Network Sensor, XPU vNS_21_1.htm .Retrieved March 19, 2004 from:
http://www.iss.net/db_data/xpu/RSNSNS_21.1.php

[12] Server Sensor, XPU vSS_21_1.htm. Retrieved March 19, 2004 from:
http://www.iss.net/db_data/xpu/RSSSSS_21.1.php

[13] Snort_org.htm. Retrieved March 19 2004 from:
http://www.snort.org/snort-db/sid.html?sid=2251

[14] Wireless LAN 802_11b Security FAQ.htm. Retrieved March 20, 2004 from:
http://www.iss.net/wireless/WLAN_FAQ.php

[15] Symantec Security Response - W32_Blaster_Worm Removal Tool.htm
Retrieved March 21 2004 from:
http://securityresponse.symantec.com/avcenter/FixBlast.exe

[16] Wireless_LAN_security.pdf. Retrieved March 21, 2004 from:
http://documents.iss.net/whitepapers/wireless_LAN_security.pdf

Appendix A: Figure Reference