FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1449881-000

Total Deleted Page(s) = 51
Page 6 ~ Duplicate;
Page 8 ~ Duplicate;
Page 9 ~ Duplicate;
Page 27 ~ Duplicate;
Page 28 ~ Duplicate;
Page 29 ~ Duplicate;
Page 30 ~ Duplicate;
Page 31 ~ Duplicate;
Page 32 ~ Duplicate;
Page 37 ~ b6; b7C; b7E;
Page 38 ~ b6; b7C; b7E;
Page 40 ~ b6; b7C; b7E;
Page 41 ~ b6; b7C; b7E;
Page 42 ~ b6; b7C; b7E;
Page 43 ~ b6; b7C; b7E;
Page 44 ~ b6; b7C; b7E;
Page 45 ~ b6; b7C; b7E;
Page 46 ~ b6; b7C; b7E;
Page 47 ~ b6; b7C; b7E;
Page 48 ~ b6; b7C; b7E;
Page 49 ~ b6; b7C; b7E;
Page 50 ~ b6; b7C; b7E;
Page 51 ~ b6; b7C; b7E;
Page 52 ~ b6; b7C; b7E;
Page 53 ~ b6; b7C; b7E;
Page 54 ~ b6; b7C; b7E;
Page 56 ~ b6; b7C; b7E;
Page 57 ~ b6; b7C; b7E;
Page 58 ~ b6; b7C; b7E;
Page 59 ~ b6; b7C; b7E;
Page 60 ~ b6; b7C; b7E;
Page 61 ~ b6; b7C; b7E;
Page 62 ~ b6; b7C; b7E;
Page 63 ~ b6; b7C; b7E;
Page 64 ~ b6; b7C; b7E;
Page 65 ~ b6; b7C; b7E;
Page 66 ~ b6; b7C; b7E;
Page 67 ~ b6; b7C; b7E;
Page 68 ~ b6; b7C; b7E;
Page 69 ~ b6; b7C; b7E;
Page 70 ~ b6; b7C; b7E;
Page 71 ~ b6; b7C; b7E;
Page 73 ~ b6; b7C; b7E;
Page 74 ~ b6; b7C; b7E;
Page 75 ~ b3; b6; b7C; b7D; b7E;
Page 79 ~ b1; b3; b6; b7C; b7D; b7E;
Page 80 ~ b1; b3; b6; b7C; b7D; b7E;
Page 86 ~ b6; b7C; b7D; b7E;
Page 87 ~ b6; b7C; b7D; b7E;
Page 88 ~ b6; b7C; b7D; b7E;
Page 94 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

To: [redacted] ATTN: Legat [redacted] International Operations From: Seattle
Re: [redacted] 04/20/2004

b3
b6
b7C
b7D
b7E

LEAD(s):

Set Lead 1: (Action)

INTERNATIONAL OPERATIONS

AT WASHINGTON, DC

Read and clear.

Set Lead 2: (Info)

[redacted]

AT [redacted]

For information.

b6
b7C
b7D
b7E

Set Lead 3: (Info)

CYBER

AT [redacted] WASHINGTON DC

For information.

♦♦

11[redacted]02.ec

To: Cyber From: Seattle
Re: [redacted] xx/xx/2002

b3
b7E

System Data:

Hardware/configuration (CPU): Varies
Operating System: Varies
Software: Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000

Security Features:

Security Software Installed: ☐ yes (if yes, type) ☐ no
-Unknown, but likely in some cases

Logon Warning Banner: ☐ yes ☐ no
-Unknown, but likely in some cases

INTRUSION INFORMATION

Access for intrusion: X Internet connection ☐ dial-up number ☐ LAN (insider)
If Internet: Varies
Network name: Unknown

Method:
Path of intrusion: UDP Port 1434

Path of intrusion: Varies
addresses: 1._____ 2._____ 3._____ 4._____ 5._____
country: 1_____ 2._____ 3._____ 4._____ 5._____
facility: 1._____ 2._____ 3._____ 4._____ 5._____

Subject:
Age: _____ Race: _____
Sex: _____ Education: _____
Alias(s): _____ Motive: _____
Group Affiliation: _____
Employer: _____
Known Accomplices: _____
Equipment used:
Hardware/configuration _____
Operating System: _____
Software: _____

Impact:
Compromise of classified information: ☐ yes ☐ no
-Unknown, but possible
Estimated number of computers affected: 75,000 approx.

To: Cyber From: Seattle
Re: [redacted] xx/xx/2002

b3
b7E

Estimated dollar loss to date: Unknown

Category of Crime:

Impairment:
X Malicious code inserted
☐ Denial of service
☐ Destruction of information/software
☐ Modification of information/software

Theft of Information:
☐ Classified information compromised
☐ Unclassified information compromised
☐ Passwords obtained
X Computer processing time obtained
☐ Telephone services obtained
☐ Application software obtained
☐ Operating software obtained

Intrusion:
X Unauthorized access
☐ Exceeding authorized access

REMARKS

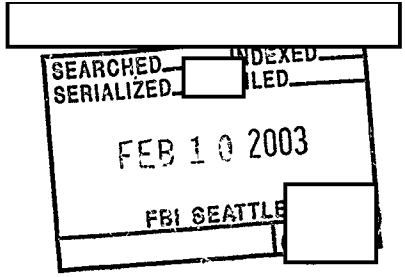
On January 25, 2003, the Sapphire worm was discovered. Within one minute after it's introduction, it is estimated the worm infected approximately 75,000 systems. The Sapphire worm targets vulnerabilities in the Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000 applications. Microsoft Corporation is located in Seattle, Washington and, as a result, contacted the Seattle Division of the Federal Bureau of Investigation (FBI) to initiate investigation.

b4
b7E

When the Sapphire worm attacks a system, it sends itself to the SQL Server Resolution Service which uses User Datagram Protocol (UDP) port 1434 for incoming and outgoing traffic. [redacted] network traffic becomes slow, and the effects of the attack resemble a Denial of Service attack.

♦♦
41[redacted]03.801

b6
b7C



b3
b6
b7C
b7E

b6
b7C

Title and Character of Case:

SAPPHIRE WORM
SLAMMER WORM

Date Property Acquired: 01/18/2005

Source from which Property Acquired:
SA [redacted] - FBI SEATTLE

b6
b7C

Anticipated Disposition: DESTROY

Acquired By: [redacted] Case Agent:

Description of Property: Date Entered
1C 1

SIX(6) DOCUMENTS RELATING TO ANALYSIS CONDUCTED ON SLAMMER WORM

Barcode: Location: 01/25/2005

(1) [redacted]

b6
b7C

(2) FILE

Case Number: [redacted] (X) (U) 1C1
Owning Office: SEATTLE

~~SECRET~~

b3
b6
b7C
b7E

[redacted]

JAN 26 2005

[redacted]

FILE

1A Envelope

Case ID: [redacted] (S)

b3
b6
b7C
b7D
b7E

SE	1	DOCUMENTS PROVIDED BY [redacted] TO FBI REGARDING [redacted]
SE	2	EMAILS REGARDING IMPACT OF SLAMMER ON BELLEVUE [redacted]
SE	3	[redacted]
SE	4	[redacted]
SE	5	MICROSOFT REPORT ON [redacted]
SE	6	PRELIMINARY SEARCH CD PROVIDED TO [redacted] PRELIMINARY REPORT CD PROVIDED TO
SE	7	ORIGINAL NOTES RE: CONFERENCE CALL WITH [redacted] AND MICROSOFT
SE	8	FINAL TECHNICAL ANALYSIS REPORT PROVIDED TO [redacted] (CD VERSION)
SE	9	2 CDS - FINAL TECHNICAL REPORT AND PRELIMINARY SEARCHES
SE	10	FD-192A FOR 1C1 - DESTROYED 6/29/05 PER EC SERIAL 46

SEARCHED [redacted] EXED
SERIALIZE ED
JUN 29 2005
FBI SEATTLE

FD-340 (Rev. 4-11-03)

File Number [redacted]

Field Office Acquiring Evidence SE

Serial # of Originating Document _____

Date Received 6/29/05

From SA [redacted]
(Name of Contributor/Interviewee)

_____
(Address)

_____

By ET [redacted]

To Be Returned ☐ Yes ☐ No

Receipt Given ☐ Yes ☐ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e) Federal Rules of Criminal Procedure

☐ Yes ☐ No

Federal Taxpayer Information (FTI)

☐ Yes ☐ No

Title:

Reference: _____
(Communication Enclosing Material)

Description: ☐ Original notes re interview of

FD-192a for 1C1 - destroyed 6/29/05 per ser. 46

b3
b6
b7C
b7E

b6
b7C

Title and Character of Case:

SAPPHIRE WORM
SLAMMER WORM

Date Property Acquired: Source from which Property Acquired:
SA [redacted] - FBI SEATTLE
01/18/2005

b6
b7C

Anticipated Disposition: Acquired By: Case Agent:
DESTROY [redacted]

Description of Property: Date Entered
1C 1

SIX(6) DOCUMENTS RELATING TO ANALYSIS CONDUCTED ON
SLAMMER WORM

Barcode: Location: 01/25/2005

Destroyed
6/29/05
per ltr. [redacted]

b3
b6
b7C
b7E

Case Number: [redacted]
Owning Office: SEATTLE

(S) (U) - 1C1
~~SECRET~~

MARKED

Inventory of Bulky Nonevidentiary Property
FD-192a (Rev. 2-12-02)

Date 1/25/05

Title and Character of Case
Slammer Worm, UNSUB(s); Victim - Microsoft Corp

File No.: [redacted]

OO: Seattle, WA

b3
b6
b7C
b7E

Date Acquired	Acquired F		
1/18/05	SA [redacted]		
To Be Returned ☐ Yes ☑ No	**See Serial**	**Acquiring Agent** SA [redacted]	**Case Agent** SA [redacted]

☐ Yes ☐ No Grand Jury Material - Disseminate Only Pursuant to Rule 6(e), Federal Rules of Criminal Procedure

☐ Yes ☑ No Property To Be Forfeited To The U.S. Government

Description of Property (Be Specific)

- 6 documents relating to ~~exploit~~ analysis conducted on Slammer Worm

For Administrative Use:

Location of Property: _____

Control Number: _____

BLOCKSTAMP

1c1

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/09/2003

To: Seattle

From: Seattle
Squad 11
Contact: SA [redacted] b3 b6 b7C b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SAPPHIRE WORM
SAPPHIRE WORM, AKA; DDOS_SQLP1434.A,AKA
W32.SQLEXP.WORM, AKA; WORM.SQL.HELKERN;
[redacted]

Synopsis: To close captioned investigation.

Details: Due to a lack of prosecutorial merit and the ability of the victim to provide any further information or logs regarding the origins of the Sapphire Worm, the ongoing captioned investigation will be closed. Any and all leads produced during the investigation will be researched as deemed necessary and appropriate.

♦♦

129[redacted]01.ec b6 b7C

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/09/2003

To: Seattle

From: Seattle
Squad 11
Contact: SA [redacted] b3 b6 b7C b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SAPPHIRE WORM
SAPPHIRE WORM, AKA; DDOS_SQLP1434.A,AKA
W32.SQLEXP.WORM, AKA; WORM.SQL.HELKERN;
[redacted]

Synopsis: To close captioned investigation.

Details: Due to a lack of prosecutorial merit and the ability of the victim to provide any further information or logs regarding the origins of the Sapphire Worm, the ongoing captioned investigation will be closed. Any and all leads produced during the investigation will be researched as deemed necessary and appropriate.

♦♦

12[redacted]01.ec b6 b7C

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/09/2003

To: Cyber **Attn:** Computer Investigations Unit, Room 5965

From: Seattle
Squad 11
Contact: [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SAPPHIRE WORM, aka
DDOS_SQLP1434.A, aka
W32.SQLExp.Worm, aka
Worm.SQL.Helkern,
UNSUB(s);
MICROSOFT CORP. - Victim;
OO:Seattle
February 10, 2003

[redacted]

SUBMISSION: ☐ Initial ☐ Supplemental X Closed

CASE OPENED:

CASE CLOSED: May 9, 2003

☐ No action due to state/local prosecution (Name/Number_____)
☐ USA declination
☐ Referred to Another Federal Agency (Name/Number:_____)
☐ Placed in unaddressed work
X Closed administratively
☐ Conviction

COORDINATION: FBI Field Office Seattle
Government Agency Federal Bureau of Investigation
Private Corporation Microsoft

VICTIM

Company name/Government agency: Microsoft Corporation and others unknown.

Purpose of System: Varies

Highest classification of information stored in system: Varies

To: Cyber From: Seattle
Re: [redacted] 05/09/2003

b3
b7E

System Data:

Hardware/configuration (CPU): Varies
Operating System: Varies
Software: Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000

Security Features:

Security Software Installed: ☐ yes (if yes, type) ☐ no
-Unknown, but likely in some cases

Logon Warning Banner: ☐ yes ☐ no
-Unknown, but likely in some cases

INTRUSION INFORMATION

Access for intrusion: X Internet connection ☐ dial-up number ☐ LAN (insider)
If Internet: Varies
Network name: Unknown

Method:

Path of intrusion: UDP Port 1434

Path of intrusion: Varies
addresses: 1._____ 2._____ 3._____ 4._____ 5._____
country: 1._____ 2._____ 3._____ 4._____ 5._____
facility: 1._____ 2._____ 3._____ 4._____ 5._____

Subject:

Age: _____ Race: _____
Sex: _____ Education: _____
Alias(s): _____ Motive: _____
Group Affiliation: _____
Employer: _____
Known Accomplices: _____
Equipment used:
Hardware/configuration _____
Operating System: _____
Software: _____

Impact:

Compromise of classified information: ☐ yes ☐ no
-Unknown, but possible
Estimated number of computers affected: 75,000 approx.

To: Cyber From: Seattle
Re: [redacted] 05/09/2003

b3
b7E

Estimated dollar loss to date: Unknown

Category of Crime:

Impairment:
X Malicious code inserted
☐ Denial of service
☐ Destruction of information/software
☐ Modification of information/software

Theft of Information:
☐ Classified information compromised
☐ Unclassified information compromised
☐ Passwords obtained
X Computer processing time obtained
☐ Telephone services obtained
☐ Application software obtained
☐ Operating software obtained

Intrusion:
X Unauthorized access
☐ Exceeding authorized access

REMARKS

Due to a lack of prosecutorial merit and the ability of the victim to provide any further information or logs regarding the origins of the Sapphire Worm, the ongoing captioned investigation will be closed. Any and all leads produced during the investigation will be researched as deemed necessary and appropriate.

♦♦
129[redacted]03.801

b6
b7C

CASE reopened 7-8-03

[redacted]

[redacted]
SEARCHED [redacted] INDEXED
SERIALIZED [redacted] FILED
JUL 0 7 2003
FBI SEATTLE
[redacted]

b3
b6
b7C
b7E

Remove From Closed Files.
CASE Reopened 7-8-03

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/07/2003

To: Cyber **Attn:** Computer Investigations Unit, Room 5965

From: Seattle
Squad 11
Contact: [redacted]

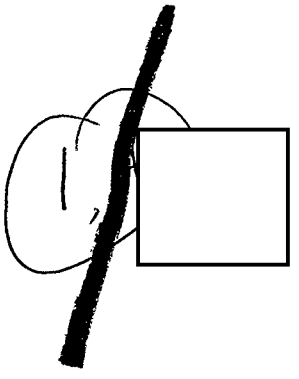
b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SAPPHIRE WORM, aka
SLAMMER WORM, aka
DDOS_SQLP1434.A, aka
W32.SQLExp.Worm, aka
Worm.SQL.Helkern,
UNSUB(s);
MICROSOFT CORP. - Victim;
OO:Seattle
February 10, 2003



SUBMISSION: ☐ Initial X Supplemental ☐ Closed

CASE OPENED: Case to be re-opened due to identification of possible subject.

CASE CLOSED:

☐ No action due to state/local prosecution (Name/Number_____)
☐ USA declination
☐ Referred to Another Federal Agency (Name/Number:_____)
☐ Placed in unaddressed work
☐ Closed administratively
☐ Conviction

COORDINATION: FBI Field Office Seattle
Government Agency Federal Bureau of Investigation
Private Corporation Microsoft

VICTIM

Company name/Government agency: Microsoft Corporation and others unknown.

Purpose of System: Varies

To: Cyber From: Seattle
Re: [redacted] 07/07/2003

b3
b7E

Highest classification of information stored in system: Varies

System Data:

Hardware/configuration (CPU): Varies
Operating System: Varies
Software: Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000

Security Features:

Security Software Installed: ☐ yes (if yes, type) ☐ no
-Unknown, but likely in some cases

Logon Warning Banner: ☐ yes ☐ no
-Unknown, but likely in some cases

INTRUSION INFORMATION

Access for intrusion: X Internet connection ☐ dial-up number ☐ LAN (insider)
If Internet: Varies
Network name: Unknown

Method:
Path of intrusion: UDP Port 1434

Path of intrusion: Varies
addresses: 1._____ 2._____ 3._____ 4._____ 5._____
country: 1._____ 2._____ 3._____ 4._____ 5._____
facility: 1._____ 2._____ 3._____ 4._____ 5._____

Subject:
Age: _____ Race: _____
Sex: _____ Education: _____
Alias(s): _____ Motive: _____
Group Affiliation: _____
Employer: _____
Known Accomplices: _____
Equipment used:
Hardware/configuration _____
Operating System: _____
Software:_____

Impact:
Compromise of classified information: ☐ yes ☐ no

b3
b7E

-Unknown, but possible
Estimated number of computers affected: 75,000 approx.
Estimated dollar loss to date: Unknown

Category of Crime:

Impairment:
X Malicious code inserted
☐ Denial of service
☐ Destruction of information/software
☐ Modification of information/software

Theft of Information:
☐ Classified information compromised
☐ Unclassified information compromised
☐ Passwords obtained
X Computer processing time obtained
☐ Telephone services obtained
☐ Application software obtained
☐ Operating software obtained

Intrusion:
X Unauthorized access
☐ Exceeding authorized access

b4
b7E

REMARKS

On January 25, 2003, the Sapphire worm was discovered. Within one minute after it's introduction, it is estimated the worm infected approximately 75,000 systems. The Sapphire worm targets vulnerabilities in the Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000 applications. Microsoft Corporation is located in Seattle, Washington and, as a result, contacted the Seattle Division of the Federal Bureau of Investigation (FBI) to initiate investigation. When the Sapphire worm attacks a system, it sends itself to the SQL Server Resolution Service which uses User Datagram Protocol (UDP) port 1434 for incoming and outgoing traffic. [redacted] network traffic becomes slow, and the effects of the attack resemble a Denial of Service attack.

On June 13, 2003, Special Agents with the FBI met with Security professionals from Microsoft Corporation. Microsoft provided new information regarding the origins of the malicious code including a possible

To: Cyber From: Seattle
Re: [redacted] 07/07/2003

b3
b6
b7C
b7E

subject: [redacted]

[redacted] Seattle will take additional steps to further identify this individual and his role in the development of the Slammer worm.

♦♦

88[redacted]01.801

b6
b7C

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/07/2003

To: Cyber **Attn:** Computer Investigations Unit, Room 5965

From: Seattle
Squad 11
Contact: [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SAPPHIRE WORM, aka
SLAMMER WORM, aka
DDOS_SQLP1434.A, aka
W32.SQLExp.Worm, aka
Worm.SQL.Helkern,
UNSUB(s);
MICROSOFT CORP. - Victim;
OO:Seattle
February 10, 2003

SUBMISSION: ☐ Initial X Supplemental ☐ Closed

CASE OPENED: Case to be re-opened due to identification of possible subject.

CASE CLOSED:

☐ No action due to state/local prosecution (Name/Number_____)
☐ USA declination
☐ Referred to Another Federal Agency (Name/Number:_____)
☐ Placed in unaddressed work
☐ Closed administratively
☐ Conviction

COORDINATION: FBI Field Office Seattle
Government Agency Federal Bureau of Investigation
Private Corporation Microsoft

VICTIM

Company name/Government agency: Microsoft Corporation and others unknown.

Purpose of System: Varies

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/09/2003

To:

From: Seattle
Squad 11
Contact: SA

Approved By:

Drafted By:

Case ID #: (Pending)

Title: SAPPHIRE WORM
SLAMMER WORM, AKA;
DDOS_SQLP1434.A, AKA
W32.SQLEXP.WORM, AKA;
WORM.SQL.HELKERN;
UNSUB(S);
MICROSOFT CORP - VICTIM

Synopsis: To set lead requesting further investigation.

Enclosure(s): Copies of documentation relating to Copy of Copy of original post on Google newsgroup; Copy of

Details: On January 25, 2003, the SLAMMER worm was discovered. Within one minute after it's introduction, it is estimated the worm infected approximately 75,000 systems. The SLAMMER worm targets vulnerabilities in Microsoft SQL Server 2000. Microsoft Corporation is located in Seattle, Washington and, as a result, contacted the Seattle Division of the Federal Bureau of Investigation (FBI) to initiate investigation.

When the SLAMMER worm attacks a system, it sends itself to the Server Resolution Service which uses User Datagram Protocol (UDP) port 1434 for incoming and outgoing traffic.

b3
b6
b7C
b7D
b7E

b6
b7C
b7E

b4
b6
b7C
b7E

SEARCHED INDEXED
SERIALIZED FILED
JUL 1 3 2003
FBI SEATTLE

b3
b6
b7C
b7D
b7E

[redacted] network traffic becomes slow, and the effects of the attack resemble a Denial of Service attack.

On January 3, 2003, [redacted] b6
posted on the newsgroup: microsoft.public.sqlserver.security. [redacted] stated he had recently installed Norton Internet Security and found that his SQL Server was trying to access external Internet sites or was trying to be accessed by external Internet sites. [redacted] b7C b7E

As a result of the impact on SQL, Microsoft hired Internet Crimes Group (ICG), an independent Internet security company to investigate the origins of the SLAMMER worm. The ICG investigators came across the website, [redacted] b6 b7C which is a site "dedicated to providing information about computer viruses." The site contained [redacted] b7E

[redacted]

To: [redacted] From: Seattle
Re: [redacted] 07/09/2003

b3
b6
b7C
b7D
b7E

LEAD(s):

Set Lead 1: (Action)

[redacted]

b6
b7C
b7D
b7E

AT [redacted]

Contact appropriate law enforcement liaison to:
Conduct logical investigation and record checks for, [redacted]

[redacted]

♦♦

190[redacted]01.ec

Evidence that [redacted]

Evidence [redacted]

b6
b7C
b7E

Evidence that [redacted]

b6
b7C
b7E

Evidence that [redacted]

Evidence that [redacted]

[redacted]

b6
b7C
b7E

Evidence of [redacted]

b6
b7C
b7E

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 10/08/2003

To: International Operations **Attn:** A/UC [redacted]
IOU1, R-7458
Attn: SSA [redacted]
IOU1, R-7458

Seattle **Attn:** SA [redacted]
Squad 11

b3 b6 b7C b7D b7E

From: [redacted]
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SAPPHIRE WORM
SLAMMER WORM, AKA;
DDOS_SQLP1434.A, AKA
W32.SQLEXP.WORM, AKA;
WORM.SQL.HELKERN;
USUB(S);
MICROSOFT CORP - VICTIM

Synopsis: To report investigative results. Lead covered.

Reference: [redacted]

b3 b6 b7C b7D b7E

Administrative: Unofficial translation. Seattle may consider requesting Language Services Translation Center to translate verbatim [redacted]

Enclosure(s): [redacted]

Details: On 10/3/2003, [redacted] provided the following information to Legat [redacted] via fax:

b3 b6 b7C b7D b7E

[redacted]

[redacted]

Searched
Indexed
Serialized
Filed

[redacted]

[redacted]

281 [redacted] EC-3

To: International Operations From: [redacted]
Re: [redacted] 10/08/2003

b3
b6
b7C
b7D
b7E

[redacted]

There is no information on file re [redacted]

[redacted] In the event additional information will become available, Legat [redacted] will be advised."

To: International Operations From: [redacted]
Re: [redacted] 10/08/2003

b3
b7D
b7E

LEAD(s):

Set Lead 1: (Action)

INTERNATIONAL OPERATIONS

AT WASHINGTON, DC

Read and clear.

Set Lead 2: (Action)

SEATTLE

AT SSEATTLE, WASHINGTON

Read and clear.

♦♦

(Rev. 01-31-2003)

~~SECRET~~

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/09/2004

To: Seattle **Attn:** SA [redacted] Squad 11
International Operations **Attn:** UC [redacted] IOU1

b3
b6
b7C
b7D
b7E

From: [redacted]
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (U) [redacted]

Title: (U) SAPPPHIRE WORM
SLAMMER WORM, AKA;
DDOS_SQLP1434.A, AKA
W32.SQLEXP.WORM, AKA;
WORM.SQL.HELKERN;
USUB(S);
MICROSOFT CORP - VICTIM

b1
b3
b6
b7C
b7D
b7E

Synopsis: (U) To provide information.

~~(S)~~ (U) ~~Classified By: [redacted] FBI/PR~~
~~Reason : 1.5(b)~~
~~Declassify On: X5~~

Reference: (U) [redacted]

(U) **Enclosure(s):** ~~(S)~~ Enclosed for Seattle is the original document [redacted] (U)

[redacted] ~~(S)~~ (U)

[redacted] For details, see enclosure.

(U) ~~(S)~~ Information provided in the document is classified ~~"SECRET"~~, for LEAD INFORMATION ONLY and is not to be discussed outside of Intelligence channels.

~~SECRET~~

Please place in
case file. Thanks!

To: Seattle From: [redacted]
Re: (U) [redacted] 02/09/2004

b3
b7D
b7E

(U) ~~(S)~~ Seattle is requested to review document and analyze information. Any further investigation is left to the discresion of Seattle.

To: Seattle From: [redacted]
Re: (U) [redacted] 02/09/2004

b3
b7D
b7E

LEAD(s):

Set Lead 1: (Action)

SEATTLE

AT SEATTLE, WA

(U) ~~(S)~~ Seattle is requested to review document and analyze information. Any further investigation is left to the discresion of Seattle.

Set Lead 2: (Info)

INTERNATIONAL OPERATIONS

AT IO1, DC

(U) Read and clear.

♦♦

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/22/2004

To: Cyber **Attn:** [redacted] SSA [redacted]
Cyber **Attn:** STAS, SSA
International Operations **Attn:** IUO-I, LA
Investigative Technology **Attn:** [redacted] Unit, UC [redacted]
[redacted] **Attn:** Legat [redacted]
Seattle **Attn:** SSA [redacted] and SA [redacted]

b3
b6
b7C
b7D
b7E

From: Cyber
International Investigative Support Unit
Contact: SSA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 66F-HQ-A1407434-IF (Pending)
[redacted]

Title: INTERNATIONAL INVESTIGATIVE SUPPORT UNIT
INVESTIGATIVE SUPPORT -FIELD/FBIHQ
INVESTIGATIONS

SAPPHIRE WORM
SLAMMER WORM, AKA;
DDOS_SQLP1434.A, AKA
W32.SQLEXP.WORM, AKA;
WORM.SQL.HELKERN;
UNSUB(S);
MICROSOFT CORP - VICTIM

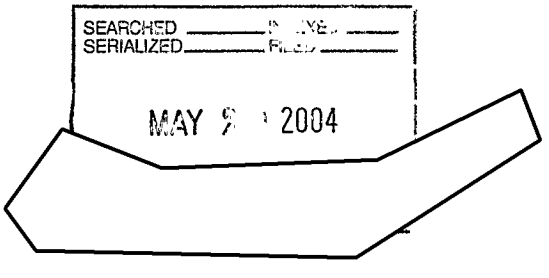
Synopsis: To document information obtained from [redacted] related to the above captioned computer intrusion case, and to set leads regarding assistance [redacted] have requested.

b6
b7C
b7D

Administrative: Meeting between [redacted] Legat [redacted] and SSA [redacted] IISU, on 03/16/2004.

Enclosure(s): For Seattle documents provided by [redacted] during the referenced (administrative) meeting.

Details:



LEAD(s):

Set Lead 1: (Action)

CYBER

AT [redacted] WASHINGTON DC

b7D
b7E

Gather victim statements documenting clear financial loss resulting from viruses and/or worms associated with this subject. Provide these statements [redacted] via IISU and the Legat.

Set Lead 2: (Action)

CYBER

AT CODU, DC

Advise IISU of any requirements and/or limitations associated with the CODU's ability to provide the requested analysis.

Set Lead 3: (Info)

INTERNATIONAL OPERATIONS

AT WASHINGTON, DC

For information.

Set Lead 4: (Discretionary)

INVESTIGATIVE TECHNOLOGY

AT QUANTICO, VA

Be advised that Cyber Division will request that [redacted]

b7D
b7E

[redacted]

Set Lead 5: (Info)

[redacted]

AT [redacted]

For information.

Set Lead 6: (Action)

SEATTLE

AT SEATTLE, WA

Obtain victim statements documenting clear financial loss and/or a threat to public safety resulting from the Slammer worm. Provide these statements [redacted] via IISU. b7D

♦♦

FD-542 (Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/24/2004

To: Seattle

From: Seattle
Squad 11
Contact: [redacted] b3 b6 b7C b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SAPPHIRE WORM
SLAMMER WORM, AKA;
DDOS_SQLP1434.A, AKA
W32.SQLEXP.WORM, AKA;
WORM.SQL.HELKERN;
UNSUB(S);
MICROSOFT CORP - VICTIM

Synopsis: To report statistical accomplishments for investigation.

Details: [redacted] has been identified as [redacted] b6 b7C b7D b7E Based on information from Microsoft and the FBI, [redacted] have initiated an investigation on [redacted] and Cyber have asked for assistance from the Seattle Division in helping to determine the extent of damages caused by the release of the SLAMMER worm. Seattle will concur and provide assistance as necessary.

Accomplishment Information:

Number: 1
Type: NIPCIP SUBJECT IDENTIFIED
ITU: [redacted] b6 b7C b7E
ITU:
ITU:
ITU:
Claimed By:
SSN: [redacted]
Name:
Squad: 11

To: Seattle From: Seattle
Re: [redacted] 03/24/2004

b3
b6
b7C
b7E

Number: 2
Type: NIPCIP CASE REFERRED TO FOREIGN LAW ENFORCEMENT
ITU:
ITU:
ITU:
Claimed By:
SSN:
Name:
Squad: 11

♦♦

83[redacted]01.542

FD-542 (Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/24/2004

To: Seattle

From: Seattle
Squad 11
Contact: [redacted] b3 b6 b7C b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SAPPHIRE WORM
SLAMMER WORM, AKA;
DDOS_SQLP1434.A, AKA
W32.SQLEXP.WORM, AKA;
WORM.SQL.HELKERN;
UNSUB(S);
MICROSOFT CORP - VICTIM

[redacted]

Synopsis: To report statistical accomplishments for investigation.

Details: [redacted] has been identified as [redacted] Based on information from Microsoft and the FBI, [redacted] have initiated an investigation on [redacted] and Cyber have asked for assistance from the Seattle Division in helping to determine the extent of damages caused by the release of the SLAMMER worm. Seattle will concur and provide assistance as necessary. b6 b7C b7D b7E

Accomplishment Information:

Number: 1
Type: NIPCIP SUBJECT IDENTIFIED
ITU: [redacted] b6 b7C b7E
ITU:
ITU:
ITU:
Claimed By:
SSN: [redacted]
Name:
Squad: 11

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 03/24/2004

To: Charlotte

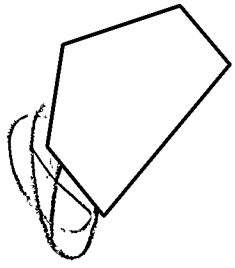
From: Seattle
Squad 11
Contact: [redacted] b3 b6 b7C b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SAPPHIRE WORM
SLAMMER WORM, AKA;
DDOS_SQLP1434.A, AKA
W32.SQLEXP.WORM, AKA;
WORM.SQL.HELKERN;
UNSUB(S);
MICROSOFT CORP - VICTIM



Synopsis: To set lead requesting letter to be delivered to Bank of America regarding damages incurred due to SQL Slammer Worm.

Enclosure(s): Letter to [redacted] Bank of America. b6 b7C b7D b7E

Details: In January 2003, the SLAMMER worm was discovered and unleashed on the Internet. Within one minute after it's introduction, it is estimated the worm infected approximately 75,000 systems. The SLAMMER worm targeted vulnerabilities in Microsoft SQL Server 2000. Based on details provided by Microsoft, [redacted] initiated an investigation of the person [redacted] and is believed to be responsible for the authoring and distributing of the Slammer Worm. [redacted]

[redacted] b6 b7C b7D b7E

To: Charlotte From: Seattle
Re: [redacted] 03/24/2004 b3 b7D b7E

[redacted]

[redacted] have requested our assistance with obtaining victim statements [redacted]

The FBI is aware the SQL Slammer Worm affected the United States-based financial institute, Bank of America, their network and over 13,000 of their ATM machines. As a result, Seattle requests the enclosed letter be hand delivered to [redacted] b6 b7C The letter asks Bank of America to provide detailed information concerning the extent of damages incurred by Bank of America as a result of the Slammer Worm.

To: Charlotte From: Seattle
Re: [redacted] 03/24/2004 b3 b7E

LEAD(s):

Set Lead 1: (Action)

CHARLOTTE

AT CHARLOTTE

Deliver letter request and explain its purpose to [redacted] b6 b7C
[redacted] Bank of America, NC1-014-14-04, 200 South College Street, Charlotte, NC 28255-0001.

If Bank of America is willing, conduct interview regarding the nature and extent of damages incurred.

♦♦

8[redacted]03.ec

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No. [redacted]

1110 Third Avenue
Seattle, Washington 98101

202-622-0460
March 24, 2004

b3
b6
b7C
b7E

RE: SQL Slammer Worm

[redacted]

The Federal Bureau of Investigation (FBI) is currently investigating various computer-related crimes including the release of the SQL Slammer Worm which occurred around January 2003. The FBI is making progress with regards to the investigation and requests assistance from Bank of America. It is our understanding the SQL Slammer Worm affected the Bank of America network and over 13,000 ATM machines. In order to determine prosecutorial strategy, it is imperative that the FBI be able to assess damages caused as a result of the release of this malicious code.

The FBI requests a statement from Bank of America regarding the effects of the SQL Slammer Worm, including, but not limited to:

- Actual amount of downtime to Bank of America systems
- Any physical damages incurred (i.e. lost equipment)
- Any monetary damages incurred (i.e. extra man-hours, new software/equipment purchased, consulting costs, etc.)
- Impact analysis of the outage (i.e. impact on customers)

The FBI understands the sensitive nature of the requested information and will assure that the information provided is used solely for the purpose of progressing the investigation. Please refer any questions to Special Agent [redacted]
Thank you for your cooperation.

b6
b7C
b7E

Sincerely,

Patrick J. Adams
Special Agent in Charge

[redacted]
Supervisory Special Agent

FEDERAL BUREAU OF INVESTIGATION

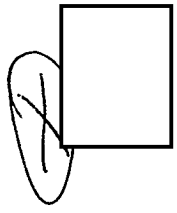
Date of transcription 04/09/2004

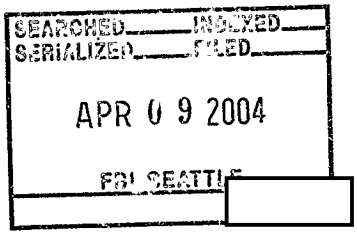
[redacted] for the City of Bellevue, Washington, telephone [redacted] e-mail [redacted] after being contacted by the Seattle Division of the Federal Bureau of Investigation (FBI), concerning an ongoing investigation into the SLAMMER worm, provided the following information via e-mail: b6 b7C b7E

[redacted]

[redacted] did not believe the City of Bellevue incurred any physical or monetary damages. [redacted] stated that after the SLAMMER attack, the City of Bellevue had to access their current procedures and change them to better respond in the future. The assessment of their current procedures resulted in increased operational costs for the City of Bellevue, but [redacted] did not believe they were directly related to the release of the SLAMMER worm. b6 b7C

The e-mail received from [redacted] was printed and placed in a 1A envelope in the associated case file.





Investigation on 03/25/2004 at Seattle, Washington

File # [redacted]

by SA [redacted]

Date dictated

b3 b6 b7C b7E

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/09/2004

[redacted] for the City of Bellevue, Washington, telephone [redacted] e-mail [redacted] after being contacted by the Seattle Division of the Federal Bureau of Investigation (FBI), concerning an ongoing investigation into the SLAMMER worm, provided the following information via e-mail: b6 b7C b7E

[redacted]

[redacted] did not believe the City of Bellevue incurred any physical or monetary damages. [redacted] stated that after the SLAMMER attack, the City of Bellevue had to access their current procedures and change them to better respond in the future. The assessment of their current procedures resulted in increased operational costs for the City of Bellevue, but [redacted] did not believe they were directly related to the release of the SLAMMER worm. b6 b7C

The e-mail received from [redacted] was printed and placed in a 1A envelope in the associated case file.

Investigation on 03/25/2004 at Seattle, Washington

File # [redacted] Date dictated

by SA [redacted] b3 b6 b7C b7E

This docume[redacted] conclusions of the FBI. It is the property of the FBI and is loaned to your agency;

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/20/2004

To: [redacted] **ATTN:** Legat [redacted]
International Operations **ATTN:** SSA [redacted]
Cyber **ATTN:** SSA [redacted]

b3
b6
b7C
b7D
b7E

From: Seattle
Squad 11
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SLAMMER WORM, AKA,
SAPPHIRE WORM,
UNSUB(S);
MICROSOFT CORP. - VICTIM

[redacted]

Synopsis: To report details of ongoing investigation.

Details: On April 9, 2004, [redacted] for the City of Bellevue, Washington, responded via e-mail after being contacted by the Seattle Division regarding the impact of the release of the Slammer worm [redacted] did not believe the city had incurred any direct monetary or physical damages as a result of the Slammer worm. [redacted] did state, however, that the city incurred increased operational costs due to having to go back and reconstruct their systems so that future incidents like this would not take them off-line. This communication was documented in FD-302 format and placed in the associated case file, Serial 21.

b6
b7C
b7E

On March 24, 2004, an Electronic Communication (EC) was sent to the Charlotte Division from the Seattle Division requesting an interview with [redacted] for Bank of America (BofA) also regarding the impact the Slammer worm had on their organization. According to news releases and reports, thousands of BofA ATMs were knocked off-line and unavailable to customers. The lead was assigned to SA [redacted] After contacting SA [redacted] Seattle was informed that [redacted] SA [redacted] believed that [redacted]

b6
b7C
b7E

To: [redacted] ATTN: Legat [redacted] International
Operations From: Seattle
Re: [redacted] 04/20/2004

b3
b6
b7C
b7D
b7E

[redacted]

As a result, SA [redacted] has contacted Microsoft to identify other potential victims and obtain impact statements. SA [redacted] was informed that the Maryland Department of Transportation also fell victim to the release of the Slammer worm. SA [redacted] has contacted their Information Technology department and requested a contact person who the FBI could work with and who could provide a victim impact analysis.

FD-801 (Rev. 7-15-97)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 02/10/2003

To: Cyber **Attn:** Computer Investigations Unit, Room 5965

From: Seattle
Squad 11
Contact: [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: SAPPHIRE WORM, aka
DDOS_SQLP1434.A, aka
W32.SQLExp.Worm, aka
Worm.SQL.Helkern,
UNSUB(s);
MICROSOFT CORP. - Victim;
OO:Seattle
February 10, 2003

SUBMISSION: X Initial ☐ Supplemental ☐ Closed

CASE OPENED:

CASE CLOSED:

☐ No action due to state/local prosecution (Name/Number_____)
☐ USA declination
☐ Referred to Another Federal Agency (Name/Number:_____)
☐ Placed in unaddressed work
☐ Closed administratively
☐ Conviction

COORDINATION: FBI Field Office Seattle
Government Agency Federal Bureau of Investigation
Private Corporation Microsoft

VICTIM

Company name/Government agency: Microsoft Corporation and others unknown.

Purpose of System: Varies

Highest classification of information stored in system: Varies