

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1439770-0

Total Deleted Page(s) = 1
Page 8 ~ b3; b6; b7C; b7E;

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

In Reply, Please Refer to

File No.

b3
b7E

FBI CASE STATUS FORM

Date: 01/22/1999

To: Honorable Richard H. Deane, Jr., 75 Spring Street, Atlanta, GA. 30335
(Name and Address of USA)

From: SAC Jack A. Daulton
(Name of Official in Charge and Field Division) (Signature of Official in Charge)

RE: UNSUB. - BELLSOUTH.NET-VICTIM:
(Name of Subject) Age Sex

You are hereby advised of action authorized by AUSA
(Name of USA or AUSA)

b6
b7C

on information submitted by Special Agent SA on 1/25/99
(Name) (Date)

(Check One)

- Request further investigation
- Immediate declination
- Filing of complaint
- Presentation to Federal Grand Jury
- Filing of information
- Other

For violation of Title 18, USC, Section(s) 1030 (a) (5)

Synopsis of case: BellSouth.net has reported a denial of service attack affecting one of their clients, AmSouth Bank causing as yet a undetermined amount of money. The attacks came through UUNET and Cable Wireless and both ISP's are aware of the attack.

AUSA was advised and he stated, if proven, this would be a violation if Title 18, Section 1030, for which he would prosecute.

2-US ATTORNEY'S OFFICE
2-
1-SA

Sup
b3
b6
b7C
b7E
sp

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/20/1999

To: Atlanta

From: Atlanta

Squad 11

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: UNSUB;
BellSouth.net - Victim,
AmSouth Bank - Victim;
Denial of Service Attack,

*Refer -
Out new
as filled to
SA [redacted]
1/21/99
1/21/99
[signature]*

b3
b6
b7C
b7E

Synopsis: To Open Case.

Details: BellSouth.net contacted writer and advised that they have been having a string of denial of service attacks affecting them as well as one of their clients, AmSouth Bank. The attack is coming in the form of a rapid mail spamming (approximately 40 to 70 messages a minute for several days without stop.

One of the ISP's used in this attack was UUNET. UUNET has been contacted by BellSouth and they have advised they have the identity of the subscriber through his IP address. However, UUNET will not release any information to BellSouth, but, they will cooperate with the FBI via subpoena. UUNET has been contacted and they have advised they will accept a faxed subpoena and they will also fax the information back. UUNET advised to make reference to tracking number UU1148498.

AUSA [redacted] has been contacted and advised he will obtain a subpoena to get this information and thereafter appropriate investigation will be conducted.

b6
b7C

◆◆

[redacted]

SEARCHED _____	INDEXED _____
SERIALIZED _____	FILED _____
JAN 21 1999	
FBI - ATLANTA	

b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 02/09/1999

To: Washington Field

Attn: Squad C-17

SA [redacted]

✓ From: Atlanta

Squad 11

Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Pending)

b3
b7E

Title: UNSUB;
BellSouth.net - Victim,
AmSouth Bank - Victim;
Denial of Service Attack
(OO:AT)

Synopsis: [redacted]

b3

Enclosures: [redacted]

Details: Unsub. attacked the victims with a denial of service
attack that lasted at least 51 hours causing financial and
service damage. [redacted]

[redacted]

[redacted]

b3
b7E

To: Washington Field From: Atlanta
Re: [redacted] 02/09/1999

b3
b7E

LEAD (s):

Set Lead 1:

WASHINGTON FIELD OFFICE

[redacted]

b3

◆◆

*

~~Close C-4
9409
5-10-00~~
SD
5-10-00

SEARCHED		INDEXED	
SERIALIZED		FILED	
		1999	
FBI - ATLANTA			

05/10/00
15:01:00

View Document Attributes

ECFVA0M0

Orig. Office : WF
Document Type :
Document Date :
To :
From : WASHINGTON FIELD
Case ID :
Topic : DOCUMENTS REQUESTED
Author :
Approver :
Ref. Case ID :

Responses :
Text . . . :
FIF :

b3

Serial :

b3
b7E

Serial :

Class Level : SN Authority : Duration : SCI :
Rule 6(e) . . : Caveats . . : FD-501 . . :
Secure Doc. :

Command . . . > +
F1=Help F3=Exit F4=Prompt F12=Cancel F14=List F15=PrevDoc F16=NextDoc

Sup

b3
b7E

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 02/15/1999

To: Atlanta

Attn: Squad 11

SA [redacted]

b6
b7C

From: WFO

Squad C-17, Northern Virginia Resident Agency (NVRA)

Contact: SA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

b3
b7E

Title: UNSUB;
BellSouth.net - Victim,
AmSouth Bank - Victim;
Denial-of-Service Attack;
OO:AT

Synopsis: [redacted]

b3
b6
b7C

Enclosures: Subpoena and FD-302 copies for case file.

Details: RE: Telcal between SA [redacted] and SA [redacted] (2/9/99)
SA [redacted]

[redacted] WFO considers lead set by EC from AT dated 2/9/1999 to be covered.

◆◆

Handwritten initials

[redacted]

b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/28/1999

To: Atlanta

From: Atlanta

Squad 17

Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

b3
b7E

Title: UNSUB;
BellSouth.net - Victim,
AmSouth Bank - Victim,
Denial of Service Attack

Synopsis: To report contact with AUSA [redacted]

b6
b7C

Details: On 6/22/99 AUSA [redacted] advised that at this time he is considering prosecuting captioned case. He was previously advised by SA [redacted] that in order to attempt a successful prosecution, a Title III would probably be necessary in order for a ISP, who is cooperating, [redacted]. At that time [redacted] took this under advisement about whether or not the effort would be effective. On 6/22/99 [redacted] advised that captioned case should remain open and he wanted to explore the possibilities of a Title III as well as any other types of investigation.

b3

◆◆

HUP

179 hwp01.ec

b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/20/2003

To: Cyber Division

Attn: Criminal Computer
Intrusion Unit

From: Atlanta

Approved By:

[Redacted]

b6
b7C

Drafted By:

Case ID #:

[Redacted]

b3
b7E

Title: UNSUB(S);
BELLSOUTH.NET - VICTIM;
AMSOUTH BANK - VICTIM;
COMPUTER INTRUSION - CRIMINAL

SUBMISSION: Initial Supplemental Closed

CASE OPENED: 01/22/1999

CASE CLOSED: 05/10/2000

- 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 _____
 Government Agency _____
 Private Corporation _____

VICTIM

Company name/Government agency: BellSouth.net
 Address/location: Atlanta, GA
 Purpose of System: ISP
 Highest classification of information stored in system: Unclassified

DAR

To: Cyber Division From: Atlanta
Re: [redacted] Date: 06/20/2003

b3
b7E

System Data:

Hardware/configuration (CPU):
Operating System:
Software:

Security Features:

Security Software Installed: yes (identify _____) no
Logon Warning Banner: yes no

INTRUSION INFORMATION

Access for intrusion: Internet connection dial-up number LAN (insider)

If Internet: Internet address:

Network name:

Method:

Technique(s) used in intrusion: (list provided)

Path of intrusion:

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 (CPU):

Operating System:

Software:

Impact:

Compromise of classified information: yes no

Estimated number of computers affected: Undetermined

Estimated dollar loss to date: Undetermined

To: Cyber Division From: Atlanta
Re: Date: 06/20/2003

b3
b7E

Category of Crime:

Impairment:

- Malicious code inserted
- Denial of service
- Destruction of information/software
- Modification of information/software
- Telephone services obtained
- Application software obtained
- Operating software obtained

Theft of Information:

- Classified information compromised
- Unclassified information compromised
- Passwords obtained
- Computer processing time obtained

Intrusion:

- Unauthorized access
- Exceeding authorized access

REMARKS

BellSouth.net contacted FBI Atlanta and advised that the company has been having a string of denial of service attacks affecting them as well as one of their clients, AmSouth Bank. The attack is coming in the form of a rapid mail spamming, approximately 40 to 70 messages a minute for several days without stop.

Investigation failed to develop significant information regarding the identity of UNSUB(S). Case was closed administratively.

◆◆