

ALL FBI INFORMATION CONTAINED

HEREIN IS UNCLASSIFIED

DATE 09-18-2012 BY 60324/UC/baw/sab/as

~~Secret~~

FBI IORC Representatives' Log

Updated 02/12/98 3:13 AM

11 February 1998

12:00a Received a faxed copy of requested Internet searches on ISP data from [redacted] @ the CITAC Watch desk.

b6
b7C

There was no material available on current FBI operations, plans, programs, or courses of action. There was no information available on FBI liaison activities with other Federal agencies.

2:00a [redacted]

3:00a [redacted]

Referral/Consult

3:45a MSH delivered site summary and LEA update slides to [redacted] for inclusion into the morning briefing.

4:00a MSH faxed the 10 FEB 98 FBI IORC Rep's log to the CITAC Watch desk.

4:30a [redacted]

5:30a [redacted]

288-HQ-1242560

to: citac
from: IORCb6
b7CRecord # 40
logged 2/12/98
[redacted]

288 HQ-1242560-601

~~Secret~~2/12/98
Am

~~Secret~~

FBI IORC Representatives' Log

Updated 02/12/98 3:13 AM

6:30 CFS assumes watch duty. MSH briefs CFS to action items.

6:31

Info from 0811 standup.

Referral/Consult

- Waiting on CITAC Watch daily summary.

8:30

Passed hot list to [REDACTED] Items included: b6 b7C

(1) Conduct ACS search on [REDACTED]

b6
b7C

(2) Conduct Newgroup search on [REDACTED]

(3) Status of the UNC site. Was it served? What did we get?

Updated items:

Referral/Consult

9:00

Spoke with [REDACTED] CIU, CITAC-working with CERT to confirm any similar (IMAP, PHF, RPC) exploits on civilian side.

b6
b7C

9:30

Referral/Consult

10:00

10:45

CITAC Watch search of ACS: No hits on [REDACTED]

b6
b7C

Referral/Consult

~~Secret~~

~~Secret~~

FBI IORC Representatives' Log

Updated 02/12/98 3:13 AM

- 2703D served at [redacted] b3
- UNC subpoena has NOT been served. b7E
- [redacted]

11:30

Referral/Consult

- 2703D have been served on all previously identified sites including [redacted] b3

- FBI will serve warrants on all .edu sites.
By approximately 14:00 today warrant will be served on Maxoon.com b7E

12:00

Prepare bullets for FBI presentation to DEFS/ECDEF at 1530.

1:00

CFS departs IORC, Pentagon for FBIHQ

5:00

CFS returns to IORC

6:45p

CFS briefs MSH on current situation. Three issues are outstanding:

- There are problems with sharing law-enforcement sensitive information with the entire J39 cell and interagency liaison community. (At the last minute, the LEA briefing slide for the 3:30p briefing was pulled as a result of these sensitivities.) b6
- Ken Geide and [redacted] attended the 3:30p briefing with [redacted] b7C
[redacted] reporting that LEA activities were underway, but that details of investigations could not be divulged. Referral/Consult
- Shift changes may be imminent as a result of manpower stresses at FBI HQ and a reduced need for a person at the IORC based on changes in FBI - IORC information exchange procedures. Decisions on this will be taken at CITAC HQ.

7:00p

MSH assumes station, and listens in on the latter part of the change-of-station briefing.

7:30p

MSH has an off-line conversation with [redacted]

- The FBI liaison schedule will be reconsidered. Referral/Consult

7:50p

MSH calls CITAC HQ and speaks with Ken Geide. MSH authorizes the individual briefing to [redacted]. The issue of support to this briefing and to other briefings is also discussed. Mr. Geide said that [redacted] should feel free to call him with any outstanding questions.

~~Secret~~

~~Secret~~

FBI IORC Representatives' Log

Updated 02/12/98 3:13 AM

Mr. Geide suggests that two regularly scheduled updates can be sent to the FBI IORC rep to be included in this briefing, though this may not occur tonight.

Referral/Consult

8:00p

8:20p

Both

9:29p

Received taxed copy of day's FBI case activity from

b6
b7C

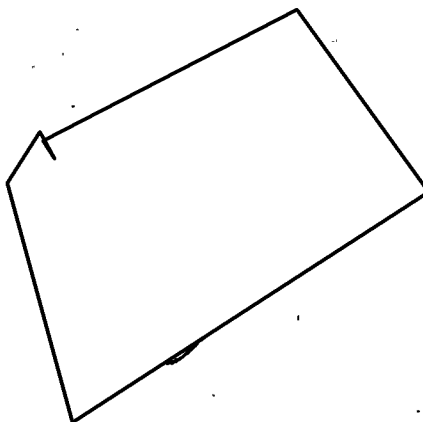
9:45p

JSAN user id and password given to FBI reps.

11:55p

Referral/Consult

~~Secret~~



b6
b7C

429

Daily Report of Leads Completed

2/13/98 3:57:10 PM

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Lead Received From: IOS b6
b7C

Lead Assigned To:

Lead Due On: Referral/Consult

Details:

288-HQ-1242560
from:
to:

b6
b7C

288-HQ-1242560-65

Received On: 2/2/98

Source Document: Other

Detail Date: 2/2/98

Detail Time: 1:35:00 PM

Subject: [redacted] b7E

Lead Received From: SSA [redacted] b6

Lead Assigned To: [redacted] b7C

Lead Due On:

Details: Floppy disc received from [redacted] with a listing of [redacted]
[redacted] can be reached
on Ext. [redacted]

b6
b7C
b7E

Received On: 2/9/98

Source Document: EC

Detail Date: 2/9/98

Detail Time:

Subject: Unsub(s); Multiple Intrusions into DOD Facilities

Lead Received From: SSA [redacted]

Lead Assigned To: [redacted]

Lead Due On: 2/9/98

b6
b7C

Details: The above-EC was drafted by [redacted] requesting the opening of a Headquarters case.

On this same date, IOS [redacted] contacted [redacted] Division 4, who established the following file number for this case: 288-HQ-1242560

Received On: 2/10/98

Source Document: Phone Message

Detail Date: 2/10/98

Detail Time:

Subject: CERT

Lead Received From: SSA [redacted]

Lead Assigned To: IOS [redacted]

Lead Due On: b6
b7C

Details: [redacted] is to send her information

Received On: 2/10/98

Source Document: EC

Detail Date: 2/10/98

Detail Time:

Subject: Unsubs; Multiple Intrusions into DOD Facilities

Lead Received From: SSA [REDACTED]

Lead Assigned To: Laboratory/WFO

Lead Due On: 2/11/98

Details: COORDINATED BY SSA [REDACTED]

CART at HQ and WFO is requested to determine the proper location & procedure to conduct the CART duplication & examinations on an expedited basis, & advise CITAC of its decision by COB 2/11/98. It is also requested that approximate CART processing time be provided.

b6
b7c

A copy of this lead was facsimiled to WFO. A copy of this lead was also hand carried to CART.

SSA [REDACTED] advised that , per SSA [REDACTED] CART, WFO should handle the matter. This matter was resolved on 2/11/98

Received On: 2/12/98

Source Document: E-Mail

Detail Date: 2/12/98

Detail Time: 10:29:00 AM

Subject: Computer Viruses

Lead Received From: IOS [redacted] b6
b7C

Lead Assigned To: Watch

Lead Due On:

Details: Report any significant history of computer viruses for the month of February.

As of 2/12/98 - IOS [redacted] this lead was covered by the watch and a copy of the information that was sent to [redacted] will be given to [redacted]

b6
b7C
Referral/Consult

4/39

Daily Report of Pending Leads

2/13/98 3:57:05 PM

Lead Assigned To:

Lead Received From: IOS

b6
b7C

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details:

b6
b7C

288-HQ-1242560

from
to:

288-HQ-1342560-66

Lead Assigned To:

Lead Received From:

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details:

--

Lead Assigned To:

Lead Received From: IOS

b6
b7C

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details:

Lead Assigned To:

Lead Received From: IOS

b6
b7C

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details:

Lead Assigned To: All Entities

Lead Received From: SSA

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Indices Checks

Details: Conduct appropriate indices checks - statd, etc.

Lead Assigned To:

Lead Received From: SSA

b6
b7C

Received On:

2/11/98

Source Document:

Write-Up

Detail Date:

2/11/98

Detail Time:

Subject:

2703 (d)

Details:

Obtain 2703(d) response.

Lead Assigned To:

Lead Received From: SSA

b6
b7c

Received On:

2/12/98

Source Document:

Write-Up

Detail Date:

2/12/98

Detail Time:

10:00:00 AM

Subject:

Navy Case

Details:

Get update on Navy case in Florida.

Lead Assigned To: IOS []

Lead Received From: SSA []

Received On: 2/10/98

Source Document: Voice Message

Detail Date: 2/10/98

Detail Time:

b6
b7C

Subject: CERT

Details: [] is to set up a meeting between himself and [] to discuss information passed on to CERT.

Lead Assigned To: Legat Israel

Lead Received From: SSA

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Parliment Website

Details: Lead to Legat Israel Re: Penetration of Parliment Web-Site

Lead Assigned To: San Franc

Lead Received From: SSA

b6
b7C

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

Subject: University of Maryland

Details: Tagging of hacker tools at the University of Maryland

Lead Assigned To: WFO

Lead Received From: SSA

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Trap and Trace Order

Details:

b3

Lead Assigned To: SSA

Lead Received From: SSA

b6
b7C

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

Subject: Profile Requests

Details: Draft response to profile requests.

Lead Assigned To: SSA

Lead Received From: SSA

b6
b7C

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

Subject: Gospelcom.net

Details: Gospelcom.net

Lead Assigned To: SSA

Lead Received From: SSA

b6
b7C

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

Subject: Lead to all field offices

Details: Lead to all field offices: check all logical sources

Lead Assigned To: SSA

Lead Received From: SSA

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Gospelcom.Net

Details: Coordinate Gospelcom.net investigation.

Lead Assigned To: SSA

Lead Received From: SSA

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

b6
b7C

Subject:

Details: Pursue case.

Lead Assigned To: SSA

Lead Received From: SSA

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Request for Information

Details:

Referral/Consult

Lead Assigned To: SSA

Lead Received From: SSA

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject:

Details: EC to WFO: Open separate Navy case

Referral/Consult

~~X~~

Lead Assigned To: SSA

Lead Received From: SSA

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time: 2:55:00 PM

b6
b7C

Subject: Facsimile

Details: Fax All Field Office EC and list of sites hit to Cleveland Attn:

Lead Assigned To: SSA

Lead Received From: SSA

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Hacker Case

Details: Get details about Cleveland hacker case.

~~20~~

Lead Assigned To: SSA

Lead Received From: b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: TR #

Details: Obtain TR #

~~30~~

Lead Assigned To: WFO

Lead Received From: SSA

b6
b7C

Received On: 2/12/98

Source Document: Write-Up

Detail Date: 2/12/98

Detail Time: 10:00:00 AM

Subject: Interviews

Details: Interview sys-admin at University of Maryland re: hacker tool files

~~21~~

Lead Assigned To: WFO at Falls Church,

Lead Received From: SSA [REDACTED]

b6
b7c

Received On: 2/12/98

Source Document: EC

Detail Date: 2/12/98

Detail Time: 2:12:00 PM

Subject: Unknown Subjects;
Multiple Intrusions into DOD Facilities (288-HQ-
1242560-18)

Details: Prepare for evidence storing and CART processing. Upon receipt of materials
prepare two copies of each, [REDACTED]

Referral/Consult

~~32~~

Leads: 2/16/98 5:00PM

from: [redacted] 439
to: [redacted]

b6
b7C

SF:

- ✓ Will obtain [redacted]
- ✓ Will begin surveillance of [redacted]
- ✓ Will obtain revised trap and trace for [redacted]
- ✓ Will continue T-III monitoring of [redacted]
- ✓ Will continue Pen register on [redacted]
- ✓ Will execute trap and trace for subject #2.
- ✓ Will conduct logical investigation of [redacted]
- ✓ Will amend T-III order to obtain [redacted]

288-HQ-1242560
b3
b7E

Hoston:

WFO:

- ✓ Will contact and interview [redacted] Obtain all relevant b3 records.

[redacted] / Gospelnet.com investigation.

b6
b7C

[redacted] investigation : EAPNET/CLARKNET.

- ✓ Followup with University of Maryland.

[redacted]

Boston:

Referral/Consult

288-HQ-1242560-67

[redacted]

- ✓ Will Seek consent search from Sys Admin and all users.

FBIHQ:

✓ Followup on efforts at Utah State, Notre Dame, University of Conn.

✓ Will conduct checks of indices and public records for all entities.

✓

Referral/Consult

✓ Check significant of "II" and 3/26/97.

✓ Check UNC logs for other victim sites. Run indices checks on all listed sites.

✓ Obtain orders for tagging of University of Maryland tools.

✓ Open FCI case (297 to be opened)

Draft response to profile requests

b6
b7C

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 02/17/98 Time: 12:48

Case ID: 288-HQ-1242560 Serial: 68

Description of Document:

Type : FAX

Date : 02/10/98

To : CITAC

From :

Topic: UPDATE ON ACTIVITIES

Reason for Permanent Charge-Out:

b6
b7c

SHOULD NOT HAVE SERIALIZED

Employee:

(12/31/1995)

DECLASSIFIED BY 60324/UC/baw/sab/as
ON 09-19-2012

429

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 02/17/1998

To: Houston

Attn: [REDACTED]

(CITA Supervisor)

San Francisco

Attn: [REDACTED]

(CITA Supervisor)

b6
b7C

Washington Field Office

Attn: [REDACTED]

(CITA Supervisor)

From: NSD/CID

OCCIP/CITAC/Room 11887

Contact: IOS [REDACTED]

Approved By: Geide Kenneth M *WJ*

[REDACTED] *SKS*

b6
b7C

Drafted By: [REDACTED]:apm

Case ID #: (U) ~~(S)~~ 288-HQ-1242560-69 (Pending)

Title: (U) ~~(S)~~ SOLAR SUNRISE;
CITAC MATTERS;
OO: HQ;

Synopsis: (U) ~~(S)~~ Request for status report on DOD intrusions.

(U) ~~(S)~~

~~Classified By: 4511, CITAC/NSD~~

~~Reason: 1.5(c)~~

~~Declassify On: 02/12/2008~~

Details: (U) ~~(S)~~ Due to the increasing demand for updates and briefings to DOD, the AG, and other government agencies regarding the intrusions into Department of Defense's (DOD) computer systems, each CITA team is to report a daily status to CITAC on this investigation by 7:00p.m.(EST). This status report can be faxed to the attention, Kenneth Geide, or [REDACTED] CITAC, fax number [REDACTED] (unsecure), [REDACTED] (secure).

b6
b7C

~~SECRET~~

01 100-10-11-10

~~SECRET~~

To: Houston From: NSD/CID
Re: (U) ~~(S)~~ 288-HQ-1242560, 02/17/1998

LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

All offices are to report case status daily to CITAC,
attention Kenneth Geide.

CC: 1 - Mr. Geide

1 -
1 -
1 -
1 -
1 -



b6
b7C

♦♦

~~SECRET~~

2/10/98

To:

[Redacted]

b6
b7C

From:

[Redacted]

IT-Middle East Unit -

NS-3B, Ext.

[Redacted]

[Redacted]

b7E

has bulky
ENCLOSURE

2008-HQ-1242560-72
2008-HQ-1242560

434

Daily Report of Leads Completed

2/18/98 8:13:37 AM

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Lead Received From: IOS b6
b7C

Lead Assigned To:

Lead Due On:
Referral/Consult

Details:

from:
to

b6
b7C

208-HQ-104560-78

Received On: 2/10/98

Source Document: EC

Detail Date: 2/10/98

Detail Time:

Subject: Unsubs; Multiple Intrusions into DOD Facilities

Lead Received From: SSA [REDACTED]

Lead Assigned To: Laboratory/WFO

Lead Due On: 2/11/98

b6
b7C

Details: COORDINATED BY SSA [REDACTED]

CART at HQ and WFO is requested to determine the proper location & procedure to conduct the CART duplication & examinations on an expedited basis, & advise CITAC of its decision by COB 2/11/98. It is also requested that approximate CART processing time be provided.

A copy of this lead was facsimiled to WFO. A copy of this lead was also hand carried to CART.

SSA [REDACTED] advised that , per SSA [REDACTED] CART, WFO should handle the matter. This matter was resolved on 2/11/98.

b6
b7C

On 2/17/98 the [REDACTED]
[REDACTED]

b7E

439

Daily Report of Pending Leads

2/18/98 8:13:32 AM

Lead Assigned To:

Lead Received From: IOS

b6
b7C

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details:

[Redacted]

from:
to:

[Redacted]

b6
b7C

285-44-1246-20-79

Lead Assigned To:

Lead Received From: IOS

b6
b7C

Received On: 2/11/98

Source Document: E-Mail

Detail Date: 2/11/98

Detail Time:

Subject: IRC Monitoring

Referral/Consult

Details:

Lead Assigned To: Boston

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Seek consent search from Sys Admin and all users.

Lead Assigned To: Boston

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Referral/Consult

Details:

Lead Assigned To: FBIHQ

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Will conduct checks of indices and public records for all entities.

Lead Assigned To: FBIHQ

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Follow-up on efforts at Utah State, Notre Dame, University of Conn.

Lead Assigned To: FBIHQ

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details:

Referral/Consult

Lead Assigned To: FBIHQ

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details:

Referral/Consult

Lead Assigned To: FBIHQ

Lead Received From: SSA b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Check UNC logs for other victim sites. Run indices checks on all listed sites.

Lead Assigned To: FBIHQ

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Obtain orders for tagging of University of Maryland tools.

Lead Assigned To: FBIHQ

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Open FCI case (297 to be opened)

Lead Assigned To: San Francisco

Lead Received From: SSA [REDACTED]

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Continue Pen Register on [REDACTED]

b3

Lead Assigned To: San Francisco

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject: 288-HQ-1242560

Details:

Obtain

b3

Lead Assigned To: San Francisco

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Begin surveillance of

b3

Lead Assigned To: San Francisco

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Continue T-III monitoring of [redacted]

b3

Lead Assigned To: San Francisco

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Execute Trap and Trace for subject #2

Lead Assigned To: San Francisco

Lead Received From: SSA [REDACTED]

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Conduct logical investigation of [REDACTED]

b7E

Lead Assigned To: San Francisco

Lead Received From: SSA [REDACTED]

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Amend T-III order to obtain [REDACTED]

b3

Lead Assigned To: San Francisco

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Obtain revised trap and trace for

b3

Lead Assigned To: SSA

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Draft response to profile requests.

Lead Assigned To: SSA

Lead Received From: SSA

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject:

Details: Open FCI Case

Lead Assigned To: SSA [redacted]

Lead Received From: SSA [redacted]

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Harvard

Details:- Follow up with Boston on service to Harvard

Lead Assigned To: SSA

Lead Received From: SSA

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: Hacker Case

Details: Get details about Cleveland hacker case.

Lead Assigned To: SSA

Lead Received From:

b6
b7C

Received On: 2/11/98

Source Document: Write-Up

Detail Date: 2/11/98

Detail Time:

Subject: TR #

Details: Obtain TR #

Lead Assigned To: WFO

Lead Received From: SSA [REDACTED]

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Contact and interview [REDACTED] Obtain all relevant records.

b3

Lead Assigned To: WFO

Lead Received From: SSA

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

b6
b7C

Subject:

Details: Gospelnet.com investigation

Lead Assigned To: WFO

Lead Received From: SSA

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

b6
b7C

Subject:

Details: investigation:EAPNET/CLARKNET

Lead Assigned To: WFO

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Details: Follow-up with University of Maryland

Lead Assigned To: WFO

Lead Received From: SSA

b6
b7C

Received On: 2/17/98

Source Document: Write-Up

Detail Date: 2/16/98

Detail Time: 5:00:00 PM

Subject:

Referral/Consult

Details:

Contact

From: [REDACTED]
To: [REDACTED]
Date: February 18, 1998 (Wednesday) 8:05 am
Subject: LEADS 288-WF-1242560 -Reply

b6
b7C

[REDACTED]

b7E

288- HQ- 1242560

288- HQ- 1242560-80

(12/31/1995)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-19-2012 BY 60324/UC/baw/sab/as

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 02/18/1998

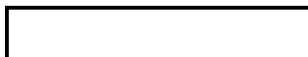
To: Boston
Houston
San Francisco
WMFO

Attn: SSA
Attn: SSA
Attn: SSA
Attn: SSA



From: NSD/CID/CITAC

Contact: SSA



b6
b7C

Approved By: Geide Ken M *ky*

Drafted By:



hg

Case ID #: 288-HQ-1242560-81 (Pending)

Title: OPERATION SOLAR SUNRISE

CITA MATTERS

OO:HQ

Synopsis: This communication sets forth additional investigative leads to be addressed regarding captioned subject.

(U) ~~(S)~~

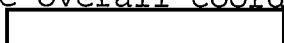
~~Classified By: 4511, CITAC/D5~~

~~Reason: 1.5(c)~~

~~Declassify On: x-1~~

Administrative: Receiving field offices should reference Bureau EC to All Field Offices, dated 2/9/98; Bureau EC to All Field Offices dated 2/12/98.

Referral/Consult

Details: (S) Referenced matter continues to receive the highest level of attention and scrutiny from the Department of Defense and the National Security Council. The Attorney General has ordered all necessary DOJ resources be afforded to this matter, and all avenues of investigation be pursued. FBIHQ will continue to provide overall coordination, analytical support and liaison with DOD,  under umbrella case 288-HQ-1242560. The following leads delineate specific areas of investigative responsibility for receiving field offices, under which field office of origin (OO) cases may be opened. Investigation and leads should be expeditiously addressed and telephonically provided to

~~SECRET~~

~~SECRET~~

To: Boston From: NSD/CID/CITAC
Re: 288-NQ-1242560, 02/18/1998

SSA [redacted] or Acting Unit Chief [redacted]
[redacted] These telephonic contacts should be
followed up with appropriate paper communications.

b6
b7C

~~SECRET~~

~~SECRET~~

To: Boston From: NSD/CID/CITAC
Re: 288-NQ-1242560, 02/18/1998

LEAD (s):

Set Lead 1:

BOSTON

AT BOSTON, MA

Referral/Consult

Set Lead 2:

HOUSTON

AT HOUSTON, TX

Referral/Consult

(U) ~~(S)~~

Set Lead 3:

SAN FRANCISCO

AT SAN FRANCISCO, CA

(U) ~~(S)~~ Will open an OO case into intrusions in to
department of defense domain name servers and [redacted]

b7E

(U) ~~(S)~~ Will continue T-III monitoring of [redacted]
perform analysis of content and provide results to CITAC. Will
obtain [redacted]

b3

[redacted] and conduct appropriate analysis.

~~SECRET~~

~~SECRET~~

To: Boston From: NSD/CID/CITAC
Re: 288-NQ-1242560, 02/18/1998

(U) ~~(S)~~ Will initiate surveillance of subjects, as deemed appropriate.

(U) ~~(S)~~ Will seek amended T-III order or letter from [redacted]

b3

(U) ~~(S)~~ Will consider use of [redacted]

b6
b7C
b7E

Set Lead 4:

WMFO

AT WASHINGTON, DC

(U) ~~(S)~~ Will contact and interview [redacted]
[redacted] regarding trace of Internet session accessed through [redacted] Obtain all relevant records.

Referral/Consult

(U) ~~(S)~~ Will continue investigation into [redacted] and coordinate with NCIS.

b6
b7C

(U) ~~(S)~~ Will obtain and serve 2703 D order on University of Maryland systems administrator to determine source of hacker tool files. Conduct appropriate investigation to determine user account holding and accessing files, date files were accessed and locations to which they were transferred. Will obtain trap and trace order for [redacted]

b3

Referral/Consult

CC: 1 - Mr. Geide



1 - [redacted]

b6
b7C

~~SECRET~~

~~SECRET~~

To: Boston From: NSD/CID/CITAC
Re: 288-NQ-1242560, 02/18/1998

1 - Mr. 
1 - Mr. 

b6
b7c

♦♦

~~SECRET~~

(12/31/1995)

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: **PRIORITY**

Date: 02/16/1998

To: FBI Headquarters

Attn: CITAC
Unit Chief

From: Houston
WC-4

Contact: SA

b6
b7C

Approved By:

Drafted By: : sfr

Case ID #: 288-HQ-A1220460 (Pending)

Title: COMPUTER INTRUSIONS

Synopsis: Measures taken to date, measures to be taken and request of CITAC.

Reference: 288-HQ-A1220460 Serial

Details: MEASURES TAKEN TO DATE:

On February 9, 1998, an immediate teletype from FBIHQ was received by the Houston Division, via secure fax explaining the details of an extensive hacker investigation that linked back to a company in College Station, Texas, known as Maroon.com. [REDACTED]

b3
b7E

provided Agents of

Referral/Consult

In reviewing the [redacted] Agents found that the [redacted] contained information that was beyond the scope of the 2703(d) court order. Due to this fact, the [redacted] [redacted] pending the issuance of a search warrant.

b3
b7E

288-HQ-1242560

entered
2/19/98

log# 65

b6
b7C

To: FBI Headquarters From: Houston
Re: 288-HQ-A1220460, 02/16/1998

On February 14, 1998, a search warrant application was filed and a search warrant allowing the FBI total access to all data backed up from [] system was signed by Judge Stacy. The back up tapes were then recovered from [] by Agents of the FBI and a chain of custody was started.

On February 15, 1998, CART agent [] took possession of the above referenced back up tapes and started an analysis of the data. Currently, these back up tapes are being reviewed for leads by Houston's CART trained Agents.

b6
b7C

Questions regarding this matter should be addressed to
SA []

MEASURES TO BE TAKEN:

On February 15, 1998, a meeting of the Houston CITAC team, consisting of the following persons:

ASAC []
ASAC []
SSA []
SSA []
SSA []
ASSA []
SA []
SA []
SA []
SA []
SA []
SA []
SA [] (Answer Coordinator)
Mr. []

b6
b7C

The purpose of the meeting was to formulate a logical process in which to cover all leads generated during this case. As a result of the meeting, the following measures will be taken:

1. Houston will immediately start Rapid Start.
2. Effective February 17, 1998, information obtained from the analysis by Special Agent [] will be loaded into a rapid start.
3. Copies of the back up tapes obtained from Maroon.com will be forwarded to CITAC and the FBIHQ laboratory for analysis.
4. Houston Division will obtain GROUPWISE E-mail with direct access to CITAC, Strategic Information Operation Center(SIOC) and the San Francisco Division.

b6
b7C

To: FBI Headquarters From: Houston
Re: 288-HQ-A1220460, 02/16/1998

REQUESTS OF CITAC:

The Houston Division requests authority to obtain a STU-III (secure telephone) and a secure fax to disseminate and receive secure information generated throughout this investigation.

♦♦