

FORMS, TEXT HAS 1 DOCUMENT

#749

TEXT, AX0001 0071642Z

AN 87

IA [REDACTED] (P)

TO DIRECTOR IMMEDIATE

SAN FRANCISCO IMMEDIATE

LEGAT BONN IMMEDIATE

BT

~~SECRET~~

ATTENTION: FBIHQ, INTD, CI-2E, UNIT CHIEF [REDACTED] SAN

FRANCISCO SSA [REDACTED]

"CHANGED": UNSUBS: UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM

IN LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA;

[REDACTED] (OO:AX)

THIS COMMUNICATION IS CLASSIFIED ~~"SECRET"~~ IN ITS ENTIRETY.

TITLE MARKED CHANGED TO SHOW CHANGE IN CHARACTER FROM FBW TO [REDACTED]

RE ALEXANDRIA TTY TO THE DIRECTOR AND LEGAT BONN DATED
DECEMBER 22, 1986. NR

FOR THE INFORMATION OF THE BUREAU, ALEXANDRIA INVESTIGATION
ORIGINATED FROM DR. CLIFFORD STOHL, LAWRENCE BERKELEY

Exec AD-Adm.	
Exec AD-LES	
Asst. Dir.:	
Adm. Servs.	
Crim. Inv.	
Ident.	
Insp.	
Intell.	
Laboratory	
Legal Coun.	
Off. of Cong. & Public Affs.	
Rec. Mgmt.	
Tech. Servs.	
Training	
Telephone Rm.	
Director's Sec'y	

b3
b6
b7C
b7E

196 - 17755-2

b3
b6
b7C
b7E

MAR 17 1987

60 SEP 21 1987

RELAYED TO

b6
b7C

PAGE FIVE AX 196A-999 UNCLAS

THE SUBJECT SHOULD NOT BE CONTACTED UNTIL FBI IS NOTIFIED
HERE. THIS WILL TAKE PLACE WHEN LEAD INFORMATION IS EXHAUSTED AND
NO OTHER ALTERNATIVES EXIST, SUCH AS EXECUTION OF A SEARCH WARRANT.

BT

5633

PAGE THREE

~~SECRET~~

b3
b7E

DISCOVERED NUMEROUS LONG DISTANCE CALLS FROM MODEMS INSIDE THE MCLEAN FACILITY AND TOOK STEPS TO LOCK OUT THE INTRUDER. THE INTRUDER WAS ENTERING A MITRE LOCAL AREA NETWORK THROUGH TYMNET ALSO. MITRE HAS ADVISED THAT THE INTRUDER IS ACCESSING THE SYSTEM AS FOLLOWS: STEP ONE: THE INTRUDER CALLS TYMNET, ASKS FOR MITRE, AND TELLS A MODEM IN MITRE TO DIAL A CALIFORNIA TYMNET NUMBER. THE LONG DISTANCE CALL IS CHARGED TO MITRE. STEP TWO: ASK TYMNET TO CONNECT TO THE LBL COMPUTERS. STEP THREE: USE LBL COMPUTERS TO ACCESS OTHER NETWORKS LIKE ARPANET, OR MFENET AND GAIN ACCESS TO YET OTHER COMPUTER SYSTEMS.

IN LATE NOVEMBER, MITRE LOCKED OUT THE INTRUDER BY ADDING EXTRA PASSWORDS TO THEIR MODEMS IN THE MCLEAN FACILITY. THE LBL INTRUSIONS STOPPED FOR ABOUT THREE WEEKS. DURING THIS TIME A REVIEW OF THE LONG DISTANCE TOLL RECORDS OF MITRE CORPORATION, MADE BY THE OUTGOING MODEMS, REVEALS MANY OTHER COMPUTER SITES DIALED BY THE SAME INTRUDER. SOME OF THE COMPUTERS WERE MILITARY, AND OTHERS WERE DEFENSE CONTRACTORS. IT IS NOT POSSIBLE TO DISCERN ALL OF THE CALLS PLACED BY LEGITIMATE MITRE EMPLOYEES AND THOSE PLACED BY THE INTRUDER. TOLL RECORDS DO SHOW THE INTRUDERS CALLS WHICH MATCH THE LBL INTRUSION TIMES.

PAGE FOUR

~~SECRET~~

b3
b7E

AFTER MITRE SUCCESSFULLY LOCKED OUT THE INTRUDER, HE REAPPEARED BY CALLING THROUGH TYMNET AGAIN. THESE CALLS WERE TRACED AND LBL ADVISES THAT THE SOURCE WAS TRACED TO THE HAMBERG, WEST GERMANY AREA. THE GERMAN PUBLIC TELEPHONE COMPANY HAS COOPERATED WITH TYMNET, AND TRACED THE INTRUDER TO A UNIVERSITY COMPUTER SYSTEM IN BREMEN, WEST GERMANY, AND ULTIMATELY TO A LOCAL ACCESS NUMBER IN BREMEN.

IT IS IN THIS WAY THAT THE INTRUDER STARTS HIS CONNECTION, WHICH IS MOST LIKELY A LOCAL PHONE CALL FOR HIM. THE LOCAL ACCESS PORT ALSO REQUIRES A USER NAME AND PASSWORD, AND IS UNKNOWN WHETHER OR NOT THE INTRUDER IS USING HIS OWN VALID ID OR A STOLEN ID AND PASSWORD.

LBL HAS IN PLACE AN ALARM TO IDENTIFY WHEN THE INTRUDER ACCESSES THEIR SYSTEM. THEY CAN CONTACT THE TYMNET SECURITY OFFICER, [REDACTED] DIRECTLY AT THE TIME OF INTRUSION. [REDACTED] HAS CONTACTS IN WEST GERMANY WHICH HE CAN ALSO QUICKLY CONTACT.

b6
b7C

INITIAL ASSESSMENT SHOWS OVER 20 COMPUTER SYSTEMS HAVE BEEN COMPROMISED. THE AMOUNT AND TYPES OF DATA ARE TO BE REVIEWED BY INVESTIGATORS IN THE ALEXANDRIA FIELD DIVISION. THE MAJORITY,

PAGE FIVE [REDACTED] ~~SECRET~~

b3
b7E

OF THE INTRUSION ATTEMPTS HAVE BEEN TARGETED AT U.S. GOVERNMENT AND MILITARY SYSTEMS. IT IS NOT BELIEVED THAT THE INTRUSIONS COME FROM MULTIPLE PEOPLE PER DR. STOHL AT LBL.

FBI ALEXANDRIA WILL FOLLOW UP WITH DETAILS OF WHAT COMPUTER SYSTEMS HAVE BEEN PENETRATED AND WHAT DATA HAS BEEN OBTAINED.

LEADS: SAN FRANCISCO: AT BERKELEY, CALIFORNIA: CONTACT DR. CLIFFORD STOHL, LAWRENCE BERKELEY LABORATORY, HOME [REDACTED]

b6 per DOE

[REDACTED] WORK [REDACTED] AND OBTAIN PRINTOUTS OF INTRUSIONS INTO AND THROUGH LBL FOR RETURN TO THE ALEXANDRIA FIELD DIVISION. THE DOCUMENTS NUMBER ABOUT 2,000 PAGES. ALSO OBTAIN THE LATEST COPY OF STOHL'S NOTES CONCERNING JANUARY, 1987, INTRUSIONS. ALL DOCUMENTS SHOULD BE TREATED AS EVIDENCE IF ORIGINALS. INQUIRE AS TO WHETHER ANY DOCUMENTS ARE MORE IMPORTANT FOR REVIEW THAN OTHERS.

BONN: LEGAT: AT BREMEN, WEST GERMANY: RELATE CONTACT FROM PREVIOUS AX LEAD WITH [REDACTED] BREMEN PUBLIC PROSECUTOR, [REDACTED] NOTE CHANGED CHARACTER AND TREAT CASE [REDACTED] RELATED RATHER THAN FRAUD BY WIRE. MAINTAIN LIAISON TO AX THROUGH FBIHQ UNIT CHIEF [REDACTED] AND SSA [REDACTED] ADVISE AX AS TO WHAT IS

b3
b6
b7C
b7E

PAGE SIX [] ~~SECRET~~

NECESSARY TO CONTINUE WITH TRAP/TRACE OF SUBJECT(S). ADVISE

b3
b7D
b7E

[] OF IMPORTANCE

~~OF IDENTIFYING ORIGINATOR OF COMPUTER INTRUSIONS~~

~~CLASSIFIED BY G-2; DECLASSIFY ON OADR~~

BT

4242

FORMS.TEXT HAS 1 DOCUMENT

INBOX.20 (#2195)

TEXT: AX0009 0212300Z

PP HQ LEGAT BONN

DE AX

P 21 2300Z JAN 87

FI [REDACTED] (196A-999)

T [REDACTED] FBI PRIORITY

LEGAT BONN PRIORITY

BT

UNCLAS

ATTENTION: [REDACTED] WHITE COLLAR CRIME SECTION, CRIMINAL

INVESTIGATIVE DIVISION; UNT CHIEF, [REDACTED]

UNSUBS; UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN LAWRENCE

BERKELEY LABORATORY, BERKELEY, CALIFORNIA; FBW (OO:AX)

TITLE MARKED CHANGED TO SHOW CHANGE IN CHARACTER FROM [REDACTED]

TO FBW.

RE AX TELETYPES TO BUREAU AND LEGAT BONN, DECEMBER 22, 1986, NR
AND JANUARY 7, 1987; AND BONN TELETYPE TO BUREAU, JANUARY 21, 1987. NR

ON JANUARY 17, 1987, LAWRENCE BERKELEY LABS (LBL) INITIATED
A SUCCESSFUL TRACE OF INTRUDER INTO LBL COMPUTERS. THIS INTRUDER
USED A PASSWORD AND USER IDENTIFICATION WHICH IS ATTRIBUTABLE TO
NUMEROUS UNAUTHORIZED LONG DISTANCE PHONE CHARGES INSIDE OF MITRE

60 JAN 25 1987

RELAYED TO

BON

Exec. AD-Adm. _____
Exec. AD-Inv. _____
Exec. AD- _____
Asst. Dir. _____
Adm. _____
Crim. _____
Ident. _____
Insp. _____
Intell. _____
Lab. _____
Legal Coun. _____
Off. of Cong. & Public Affs. _____
Rec. Mgnt. _____
Tech. Servs. _____
Training _____

b3
b6
b7C
b7E

b6
b7C

PAGE TWO AX 196A-999 UNCLAS

CORPORATION IN MCLEAN, VIRGINIA. THIS INTRUDER HAS BEEN ACCESSING AND ATTEMPTING TO BREAK INTO NUMEROUS U.S. GOVERNMENT COMPUTER SYSTEMS.

MOST OF THE INTRUSIONS HAVE BEEN USING THE TYMNET DATA NETWORK LOCATED IN THE UNITED STATES. TYMNET SECURITY OFFICER [REDACTED] WAS ASKED TO INITIATE A TRACE THROUGH TYMNET TO LOCATE THE INTRUDER. [REDACTED] TELEPHONICALLY ADVISED THE ALEXANDRIA DIVISION THAT THE WEST GERMAN DATEX-P NETWORK WAS ACCESSED IN WEST GERMANY TO CALL THE TYMNET NETWORK IN THE UNITED STATES.

[REDACTED] ADVISED HE WAS TOLD BY DATEX-P AUTHORITIES THAT THE ORIGINATOR OF THE INTRUSIONS WAS TRACED TO A TELEPHONE NUMBER IN WEST GERMANY. THE INTRUDER IS APPARENTLY USING A VALID ACCESS NUMBER TO THE DATEX-P NETWORK AND IT IS BELIEVED THE CALLS ARE ORIGINATED BY AN ADULT.

LEADS:

LEGAT BONN: THROUGH APPROPRIATE [REDACTED] CONTACT [REDACTED] AT DATEX-P NETWORK, TELEPHONE [REDACTED] TO ASSIST ALEXANDRIA IN IDENTIFYING SOURCE OF INTRUSIONS FOR POSSIBLE INDICTMENT IN THE UNITED STATES.

ADVISE [REDACTED] THAT ALEXANDRIA WILL ALSO

b6
b7C

b6
b7C
b7D

PAGE THREE AX 196A-999 UNCLAS

[REDACTED] IN PROSECUTION OF WEST GERMAN

STATUTES BY PROVIDING PHONE TOLL RECORDS AND TIMES OF INTRUSIONS.

ALEXANDRIA REQUESTS ANY PHONE RECORDS OF SUBJECT BE PROVIDED IF POSSIBLE, AS WELL AS SUBJECT'S IDENTIFYING DATA.

ADMINISTRATIVE:

b7D

FOR INFORMATION OF LEGAT, BONN, THIS CASE IS BEING RECLASSIFIED AS A FBW MATTER AND WILL BE HANDLED UNCLASSIFIED AS A CRIMINAL MATTER. IT IS HOPED THAT THIS WILL AID BONN IN ITS LIAISON EFFORTS WITH [REDACTED] TO OBTAIN THEIR COOPERATION IN IDENTIFYING THE SUBJECT AND PROSECUTING UNDER U.S. LAWS.

BT

4354

VZCZCBON 506 035 1224

P 040734Z FEB 87

FM BOMN (196A-221) (P)

TO DIRECTOR PRIORITY

FBI, ALEXANDRIA (196A-999) PRIORITY

BT

UNCLAS

ATTN: [REDACTED] WHITE COLLAR CRIME SECTION

UNSUBS; UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN

LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA; FBW

OO:AX

REBONCAB DATED JANUARY 30, 1987.

ON FEBRUARY 3, 1987 ASSISTANT LEGAT [REDACTED] MET

WITH US AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS (AFOSI)

REPRESENTATIVE [REDACTED] TO DISCUSS CAPTIONED MATTER.

[REDACTED] HE ADVISED THAT HIS HEADQUARTERS DIRECTED HIM TO
CONTACT LEGAT AND PROVIDE WHAT TECHNICAL ADVICE AND ASSISTANCE
MAY BE NEEDED IN THIS INVESTIGATION.

LEGAT WILL ARRANGE ALONG WITH [REDACTED] TO MEET WITH

60 SEP 21 1987

RECEIVED
TELETYPE

4 FEB 87 12 30
FEDERAL BUREAU
OF INVESTIGATION

b6
b7C

b6 per FBI, AFOSI
b7C per FBI, AFOSI

MAR 30 1987

R AK [REDACTED]

PAGE TWO BON 19 6A-221 UNCLAS

b6 per AFOSI
b7C per AFOSI
b7D

[REDACTED] IN ORDER TO OFFER THE
TECHNICAL ASSISTANCE WHICH [REDACTED] MAY BE ABLE TO PROVIDE AND
TO OBTAIN INFORMATION ABOUT DEVELOPMENTS IN THIS CASE TO DATE.

LEAD - ALEXANDRIA AT ALEXANDRIA :

WLL ADVISE OF INFORMATION REQUESTED IN REFERENCED COMMUNICATION.

BT

FBI

TRANSMIT VIA:

☐ Teletype
☐ Facsimile
☒ X AIRTEL

PRECEDENCE:

☐ Immediate
☐ Priority
☐ Routine

CLASSIFICATION:

☐ TOP SECRET
☐ SECRET
☐ CONFIDENTIAL
☐ UNCLAS E F T O
☐ UNCLAS

Date 3/16/87

TO: DIRECTOR, FBI
 ATTN: CCA [redacted] WHITE COLLAR CRIME SECTION

FROM: ACTING [redacted] A (196A-999) (P)

UNSUBS; UNAUTHORIZED USE OF GOVERNMENT
COMPUTER SYSTEM IN LAWRENCE BERKELEY
LABORATORY, BERKELEY, CALIFORNIA;

FBW

OO:AX

Lawrence Berkeley Laboratory

Re Bonn teletypes, 2/4/87 and 1/30/87; Bonn telcall to Alexandria, 2/20/87.

Per telcall to WCCS, FBIHQ the enclosures are sent with cover airtel directly to Legat Bonn via DHL courier.

Enclosed for Legat Bonn is a 73 page document created by Dr. CLIFFORD STOLL, U.S. Department of Energy, Lawrence Berkely Laboratory.

For the information of Legat Bonn, the enclosed document is an explanation of the computer intruders into Lawrence Berkely Laboratory since late 1985. Pages 1 through 4 contain a synopsis of all the events leading to present. 4 through 10 are a chronological listing of the times the intruder accessed the computers. At the end of the document is a flow chart showing the path of the intruder's phone call.

It should be understood that the nature of this investigation is technical to understand, but not impossible. The Alexandria case agent has retained a copy of the STOLL document enclosed and if any questions arise the Legat is directed to telephonically contact the case agent.

2 - Bureau
 2 - Bonn (Enc. 1) (Attn: Asst. Legat [redacted])
 2 - Alexandria

(6)

2 MAR 20 1987

Approved:

58 NOV 16 1987

Transmitted

(Number)

(Time)

Per

b6
b7Cb6
b7Cb6
b7C

APR 14 1954

The document has been marked in red and blue pen by the case agent with the following directions:

1. Blue markings show the government computer intrusions for police authorities and the main pertinent investigative data.
2. Red markings for more sensitive information which should not be generally released to non-police or non-phone company officials.

The Legat is directed to use absolute discretion in the dissemination of the documents. They contain in some cases, active passwords, and actual network addresses in the U.S. Military Data Network. These network addresses are not classified nor is any part of the enclosed document.

The document is a perfect case study of international computer intrusions, and should not be disseminated so as to allow individuals to use it as a guide to network intrusion and possible sabotage.

Ongoing investigation has determined that other computer networks other than TYMNET are also being used by persons in West Germany to access U.S. Government computers in violation of United States Federal statutes. During the month of February persons using Datex-P dial-in pads in Hamburg, West Germany, accessed illegally a computer maintained by the Department of Agriculture in Washington, D.C.. The intruders used the TELENET Network, headquartered in Reston, Virginia, which is an alternative service to TYMNET. The Department of Agriculture maintains that no authorized users access their computers from West Germany and the international connections have been rerouted so as to not allow any international connections to their computers.

This is a solution not available to the other networks involved in this matter as it is necessary that our Military sites utilize worldwide connectivity.

Leads: Legat Bonn,

1. Assistant Legat is directed to find out what federal and state prosecutive agencies are involved in the investigation of captioned matter. The names of these agencies should be sent by teletype to Alexandria for the use of Department of Justice attorneys.

2. Due to the inter-governmental agency attention this matter has drawn it is necessary to quickly discover the identities of the intruders and whether or not the FRG intends their prosecution if US authorities can provide necessary evidence.

3. The Assistant United States Attorney for the Eastern District of Virginia believes that prosecution is in order given most circumstances; either by United States courts, FRG courts, or both.

4. The times and dates of access by the intruder as listed in the enclosed document should be referenced to any times and dates that the West German officials have. It should be possible to show times and dates a person was using his phone or Datex-P account and reference them to the enclosed documents.

Administrative:

Alexandria Field Division is ready to provide assistance to Legat Bonn if necessary. The case agent is ready to explain the activities of the intruders to the Legat and other necessary officials.

Department of Justice Attorneys have high interest in the matter and are also bringing it to the attention of the State Department. It should not be unexpected that the Legat will be contacted by State Department personnel.

8
FORMS.TEXT HAS 1 DOCUMENT

INBOX:19 (#3496)

TEXT: AX0001 0282215Z

OO HQ LEGAT BONN SF

DE AX

0 28 2215Z JAN 87

ALEXANDRIA (196A-999) (P)

TO DIRECTOR IMMEDIATE

LEGAT BONN IMMEDIATE

SAN FRANCISCO [REDACTED] RRIORITY

BT

UNCLAS

ATTENTION: [REDACTED] WHITE COLLAR CRIME SECTION, CRIMINAL

INVESTIGATIVE DIVISION.

UNSUBS: UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN

LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA; FBW (OO:AX)

RE ALEXANDRIA TELETYPES TO BUREAU AND LEGAT BONN, DECEMBER 22, 1986, JANUARY 7, 1987, JANUARY 21, 1987; AND BONNTEL TO BUREAU, 196-7755-2

FOR THE INFORMATION OF SAN FRANCISCO, TITLE WAS CHANGED PREVIOUS TELETYPE TO SHOW CHANGE IN CHARACTER FROM FCI - GO TO FBW.

ON JANUARY 28, 1987, ROBERT GREEVES, DIRECTOR OF AUTOMATED DATA PROCESSING FOR THE DEPARTMENT OF ENERGY, ADVISED THE

Exec AD-Adm.
Exec AD-Inv.
Exec AD-LES
Asst. Dir.:
Adm. Serv.
Crim. Inv.
Ident.
Intell.
Lab.
Legal Coun.
Off. Cong. & Public Affs.
Rec. Mgmt.
Tech. Serv.
Training
Telephone Rm.
Director's Sec'y

b3
b6
b7C
b7E

V-158

DE-134

196-7755-8

JAN 28 1987

b6
b7C

RELAYED TO: BON

RECEIVED
FBI

JAN 28 11 10 PM '87

CRIMINAL INVESTIGATION
DIVISION / FBI CITY OFFICE

JAN 29 7 26 AM '87

WHITE-COLLAR
CRIMES SECTION
U.S. DEPT. OF JUSTICE

8

8

0

PAGE TWO AX 196A-999 UNCLAS

ALEXANDRIA DIVISION THAT ON FEBRUARY 10, 1987, HE INTENDED TO STOP MONITORING PENETRATIONS INTO LAWRENCE BERKELEY LAB (LBL) COMPUTERS. INVESTIGATION TO DATE HAS STEMMED FROM LBL ALLOWING UNSUBS TO ACCESS LBL COMPUTERS AND MONITOR THEIR ACTIVITIES AS THE INTRUDER(S) THEN ATTEMPTED TO PENETRATE VARIOUS U.S. GOVERNMENT COMPUTER SYSTEMS.

THE DEPARTMENT OF ENERGY IS WILLING TO COOPERATE IN ANY WAY NECESSARY TO AID ONGOING INVESTIGATION. ALEXANDRIA RECEIVED INFORMATION FROM TYMNET SECURITY OFFICER, [REDACTED] ON JANUARY 27, 1987, THAT [REDACTED]

b6
b7C
b7D

IT IS IMPORTANT THAT LIAISON BE MAINTAINED SO THAT THE POSSIBILITY OF RETAINING THE LBL MONITORING CAPABILITY CAN BE ESTABLISHED. AFTER THE FEBRUARY 10, 1987, CUTOFF DATE, THE INTRUDERS WILL NOT HAVE ACCESS TO THE LBL COMPUTERS, BUT IT HAS ALREADY BEEN SHOWN THAT THIS WILL NOT PRECLUDE THE UNSUB FROM ACCESSING OTHER GOVERNMENT COMPUTER SYSTEMS.

FOR THE INFORMATION OF LEGAT BONN, AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS (AFOSI) IS ALSO INVESTIGATING CAPTIONED MATTER, AS A NUMBER OF AIR FORCE COMPUTERS HAVE BEEN PENETRATED

8

PAGE THREE AX 196A-999 UNCLAS

BY THE LBL INTRUDER. IT IS NOT UNEXPECTED THAT LEGAT MAY DISCOVER
PARALLEL EFFORTS BY AFOSI PERSONNEL IN WEST GERMANY.

ALEXANDRIA DESIRES TO IDENTIFY [REDACTED]

[REDACTED] TO ASSIST LEGAT IN LIAISON EFFORTS. [REDACTED]
[REDACTED]

b7D

LEGAT BONN: CONTINUE EFFORTS AS SET FORT IN JANUARY 21, 1987
TELETYPE. WHEN [REDACTED] IS IDENTIFIED,

ADVISE [REDACTED]

ADVISE [REDACTED]

[REDACTED] SUTEL RESULTS AS SOON AS
POSSIBLE.

BT

4409

~~SECRET~~

TRANSMIT VIA:

- ☐ Teletype
- ☐ Facsimile
- ☒ X Airtel

PRECEDENCE

- ☐ Immediate
- ☐ Priority
- ☐ Routine

CLASSIFICATION:

- ☐ TOP SECRET
- ☐ SECRET
- ☐ CONFIDENTIAL
- ☐ UNCLAS E F T O
- ☐ UNCLAS

Date 5/4/87

TO: DIRECTOR, FBI
ATTN: FBIHQ, SSA [redacted] WHITE COLLAR CRIME
SECTION
FBIHQ, SSA [redacted] DIV 5, CI2C

b6
b7C

FROM: ACTING SAC, ALEXANDRIA (196A-999) (P)

UNSUBS; UNAUTHORIZED USE OF GOVERNMENT
COMPUTER SYSTEM IN LAWRENCE-BERKELEY
LABORATORY, BERKELEY, CALIFORNIA;
FBW
OO:AX

This document is unclassified unless otherwise noted.

For the information of Pittsburgh, the Alexandria investigation is predicated upon information received from DR. CLIFFORD STOLL, Lawrence Berkeley Laboratory (LBL). Since 1985, LBL has had unauthorized persons using their computers, and this was discovered in August 1986. After unsuccessful attempts to lock out the intruders, LBL started monitoring the actions of the intruders. STOLL discovered that the intruders were using LBL as a gateway to the DEFENSE DATA NETWORK (DDN), and they were attempting to penetrate numerous government computer systems.

b6
b7C

Investigation by local police agencies traced calls to McLean, Virginia, inside of MITRE corporation. Alexandria Field Division was brought into the matter when it was believed that the intruders were originating from this Northern Virginia company. It was later determined that the calls were originating from the Federal Republic of Germany, specifically the Datex-P data network. The intruders were entering LBL from the American based Tymnet Network, after placing the call from West Germany.

- ④ - Bureau 2-FCU
2 - Pittsburgh
2 - San Francisco
2 - Cincinnati
2 - Alexandria

(12)

196-7735-11

10 MAY 6 1987

Approved: [redacted]

Transmitted

(Number) (Time)

Per [redacted]

CLASSIFIED BY G-3
DECLASSIFY ON OADR

60 JAN 12 1988

~~SECRET~~

b6
b7C

JUN 23 1987



~~SECRET~~

DR. STOLL kept Alexandria informed on the matter and on January 1, 1987, a sensitive data base inside the Pentagon was accessed by the same West German intruder. No classified data to date has been compromised, but very sensitive data, such as an indices and abstracts of classified documents have been searched. //

In early January, 1987, DR. STOLL placed documents on his LBL computer that he thought would be of interest to the intruder. This was an attempt to keep the hacker interested and online long enough to complete an international trap and trace. STOLL placed convincing documents on his computer concerning a fictitious new network named SDINET. On January 16th the intruder at LBL far exceeded normal user capabilities, and read about the new network in a private area of the computer. STOLL advised that this intruder was the only person other than himself to have read this document on the LBL computer.

Numerous difficulties in communications between West Germany and Alexandria have slowed the investigation. The main problem consisted of two sources of information to Alexandria. Tymnet Data Network Security person, [redacted] advised that West German Datex-P authorities had indeed traced the LBL call on January 16, 1987. The Legat sent a communication to FBI Alexandria asking about access times of the intruder almost 3 weeks after Alexandria sent a document containing them to Bonn. The document sent to the Legat was a 75 page condensed diary of everything that has occurred at LBL. The document included times of access, dates of access and the user name that the intruder used. Legat has determined that [redacted] //

b6
b7C
b7D

[redacted] and have been waiting for the intruder to re-establish a connection with LBL. The intruder has logged on to the LBL computer in April, 1987, but he has not stayed on longer than five minutes at any given time. Also the frequency of calls has diminished to about one logon every three weeks.

On April 27, 1987, STOLL telephonically contacted SA [redacted] in the Alexandria Division. STOLL had received a request in the mail for information concerning SDINET. The information that the person had requested had only been known by the intruder and DR. STOLL. It is assumed that the person requesting the information has some connection to the intruder.

b6
b7C

~~SECRET~~

~~SECRET~~

The letter received by STOLL is a near verbatim copy of what the hacker received while online with the IBL computer. It requests various documents and is signed by [REDACTED]. The letterhead features the name [REDACTED]. The envelope is postmarked April 22, 1987, and bears postage meter number [REDACTED]. Alexandria indices showed a record check for the same person requested by Pittsburgh in 1982. [REDACTED] checks were negative regarding [REDACTED]. The address of the person in the record check is the same as the requestor of information, [REDACTED] PITTSBURGH, PA, 15236. The Pittsburgh file number was [REDACTED] and requestor of the record check was [REDACTED]. Pertinent biographic data is shown as : [REDACTED]

b3
b6
b7C
b7E

[REDACTED] search revealed an entry of another person with the same name, possibly [REDACTED] pertinent information as: [REDACTED]

(S)

Due to the sensitivity of the investigation it is requested that all logical investigation be conducted in a non-alerting manner. No contact is to be made with [REDACTED]. Subjects are considered a flight risk due to their status as [REDACTED]. An online Dunn and Bradstreet request is not to be done due to the possibility of discovering that this check had been requested.

REQUEST OF THE BUREAU

b6
b7C

FBI HQ: Conduct all logical indices and database inquiries to provide biographic and substantive data regarding [REDACTED]

LEADS

Pittsburgh at Pittsburgh: Conduct necessary biographic investigation, including reviews of existing subject file data. If any subpoenas are necessary to obtain information, Alexandria will forward them. All indices checks are requested as well as logical local record checks. It is requested that the postal inspectors be contacted to obtain the location of meter number [REDACTED]. For any necessary subpoenas contact SA [REDACTED] in the Alexandria FBI office, FTS 967-1200.

b6
b7C

Cincinnati at Columbus: Search Records of Defense Industrial Security Clearance Office (DISCO). for any information on [REDACTED] and [REDACTED]

~~SECRET~~

FILE

UNCLASSIFIED

May 7, 1987

JUDGE:

RE: UNAUTHORIZED USE OF GOVERNMENT COMPUTER
SYSTEM IN LAWRENCE BERKELEY LABORATORY,
BERKELEY, CALIFORNIA;
FRAUD BY WIRE;
OO: ALEXANDRIA

b6
b7C

SYNOPSIS: A computer system, housing government information in Berkeley, California, has repeatedly been intruded by a sophisticated user in West Germany. The creation of a fictitious computer file has resulted in the identification of a possible co-conspirator in Pittsburgh, Pennsylvania. Both a criminal investigation and a foreign counterintelligence preliminary inquiry have been initiated in an effort to identify the scope and identities of those responsible for the intrusions.

DETAILS: Since 1985, the Lawrence Berkeley Laboratory (LBL) has experienced numerous occasions wherein unauthorized persons gained access to their computers. This was not discovered until 1986 when unsuccessful attempts to lock out the intruder were discontinued in favor of monitoring the intrusions. The monitoring showed the intruder utilized LBL as a gateway to the Defense Data Network (DDN) which linked numerous computer systems. The LBL was able to determine the calls originated in West Germany and utilized the Tymnet Network which routed the connections through the MITRE Corporation in McLean, Virginia, then into the LBL computer.

In an effort to identify the intruder, Dr. Clifford Stoll established a fictitious file in the LBL computer titled SDI Network Project. That file indicated numerous documents on file and a form letter indicating an individual and an address from whom copies of the documents could be obtained. On January 16, 1987, the intruder gained access to the LBL computer and to the fictitious file. By utilizing advanced computer technology far greater than that normally associated with a computer hacker, the intruder was able to become a master user and review subfiles within the fictitious SDI file. This intrusion was traced back to a specific West German location, and information has been furnished to Legat Bonn in an effort to identify the intruder.

1 - Mr. Revell

1 -
1 -
1 -
1 -
1 -
1 -
1 -
1 -

1 -
1 -
1 -
1 -
1 -
1 -
1 -
1 -
1 -
1 -

(17) 1028

7755

FILE

b6
b7C

UNCLASSIFIED

UNCLASSIFIED

On April 27, 1987, Dr. Stoll received a letter from [redacted] of [redacted] requesting several of the documents from the fictitious SDI file at LBL. The request was a near verbatim rendition of the information accessed by the intruder on January 16, 1987. [redacted]

[redacted] It appears that there is some connection between [redacted] and the West German intruder.

CURRENT DEVELOPMENTS: In view of the scope and nature of this matter, both a criminal investigation [redacted] [redacted] have been initiated and supported as needed by the Technical Services Division.

b3
b6
b7C
b7D
b7E

This matter is being coordinated by [redacted] [redacted] the Criminal Investigative Division with support by Legal Attache Bonn, Alexandria Field Office, the Pittsburgh Field Office and the San Francisco Field Office. Members of the intelligence gathering community have expressed extreme concern over this matter.

Executive Assistant Director Oliver B. Revell was briefed on this matter on April 30, 1987.

You will be kept advised of developments.



b6
b7C

UNCLASSIFIED

INBOX.40 (#7310)

TEXT: AX0009 141222Z
OO HQ LEGAT BONN
DE AX
O 21 2200Z MAY 87

22 MAY 87 03 11

ANDRIA (196A-999) (P)

CTOR, FBI PRIORITY

BONN IMMEDIATE

BT

UNCLAS

ATTN: SSA [REDACTED] WHITE COLLAR CRIME SECTION, CID

UNSUBS; UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN LAWRENCE
BERKELEY LABORATORY, BERKELEY, CALIFORNIA; FBW; (OO:AX)

RE TELCALL TO BONN, ASST. LEGAT [REDACTED] MAY 20, 1987,
AL TELCALL TO SSA [REDACTED] FBIHQ, MAY 20, 1987.

ALEXANDRIA HAS BEEN CONDUCTING AN INVESTIGATION OF UNAUTHORIZED
ACCESSES OF DEPARTMENT OF ENERGY COMPUTER SYSTEMS AT LAWRENCE
BERKELEY LABORATORY (LBL), BERKELEY, CALIFORNIA. DURING THIS
INVESTIGATION, NUMEROUS ACCESSES HAVE BEEN RECORDED WHICH HAVE BEEN
ATTIBUTABLE TO A SINGLE SOURCE. THE FOLLOWING SET OF CONCLUSIONS
CAN BE DRAWN CONCERNING THIS INVESTIGATION. A. THE SAME STOLEN
USER ACCOUNTS OF THE LBL COMPUTER ARE BEING USED, THE PASSWORDS ON

15 JUL 9 1987

22 SEP 29 1988 450

DECLINE LOT

RELAYED TO:

BON

Exec AD Adm
Exec AD Inv
Exec AD LES
Asst. Dir.:
Adm. Servs.
Crim. Inv.
Ident.
Insp.
Intell.
Lab.
Legal Coun.
Off. Cong. &
Public Affs.
Rec. Mgnt.
Tech. Servs.
Training
Telephone Rm.
Director's Sec'y

b6
b7C

b6
b7C

PAGE TWO AX 196A-999 UNCLAS

THESE ACCOUNTS HAVE BEEN CHANGED FREQUENTLY AND ONLY THE PERSON CHANGING THEM WOULD BE ABLE TO HAVE REPEATED ACCESS. B. THE PERSON MUST KEEP NOTES SINCE SO MANY DIFFERENT ACCOUNTS AND PASSWORDS ARE BEING USED. IT WOULD BE EXTREMELY DIFFICULT TO KEEP TRACK OF THE METHODS BEING USED WITHOUT WRITTEN OR ELECTRONICALLY RECORDED NOTES.

C. THE PERSON HAS DISSEMINATED INFORMATION CONTAINED IN A GOVERNMENT COMPUTER SYSTEM. THIS INFORMATION WAS NEARLY IDENTICAL TO THE INFORMATION THAT WAS READ BY THE INTRUDER ON JANUARY 16, 1987.

D. THE PERSON IS CONTINUING HIS INTRUSIONS FOR VERY LIMITED PERIODS OF TIME, DEFEATING TRAP AND TRACE ATTEMPTS.

ON MAY 19, 1987, THE INTRUDER WAS ON THE LBL COMPUTER AT 06:54 TO 06:56 AND 07:12 TO 07:19 PACIFIC DAYLIGHT TIME (PDT). ON MAY 20, 1987, THE INTRUDER WAS ON THE LBL COMPUTER FROM 05:48 TO 06:01 AND AT 09:49 TO 09:52 PDT. UNSUBS TERMINAL MALFUNCTIONED AT 05:57 A.M., AND HE ACTUALLY CALLED BACK FROM 05:58 TO 06:01. THESE CALLS WERE TRACED BY TYMNET DATA NETWORK TO THE UNIVERSITY OF BREMEN. THE DATEX-P NETWORK ADDRESS OF THE ORIGINATING CALLS WAS 2624-5421-0421. THIS IS IMPORTANT LEAD INFORMATION AND COULD ESTABLISH A CRIME BEING COMMITTED IN THE FRG.

WITH DATEX-P COULD ESTABLISH THE EXACT LOCATION OF

b6
b7c

PAGE THREE AX 196A-999 UNCLAS

THE COMPUTER USED IN THESE ATTEMPTS. THE SYSTEM OPERATORS OF THE COMPUTER AT THE UNIVERSITY OF BREMEN COULD TELL THE INVESTIGATOR WHAT USER ID WAS USED TO AT THESE TIMES AND DATES TO CALL THE DATEX-P NETWORK, OR SIMPLY THE USER ID'S USING THE COMPUTER AT THESE TIMES. THIS COMPUTER IS BEING REGULARLY USED BY THE INTRUDER.

THE INTRUDER IS EITHER USING A UNIVERSITY TERMINAL OR IS CALLING INTO THE UNIVERSITY COMPUTER FROM A COMPUTER IN HIS HOME OR OFFICE. THE USER ID UNSUB IS USING IS EITHER VALID OR STOLEN. IF THE INVESTIGATOR IS ABLE TO DETERMINE FROM THE UNIVERSITY OF BREMEN THE OWNER OF THE ID BEING USED, THEN HE WILL BE ABLE TO FIND OUT IF THE INTRUDER IS USING HIS OWN OR SOMEONE ELSE'S CODE. IF UNSUB IS USING HIS OWN CODE, THEN WE WILL HAVE THE TRUE IDENTITY OF THE INTRUDER. IF HE IS USING A STOLEN CODE, THE UNDOUBTEDLY THE POLICE IN WEST GERMANY HAVE A LOCAL VIOLATION OF THEIR LAWS. THE INTRUDER IS CHARGING NUMEROUS INTERNATIONAL DATA CONNECTIONS TO THE STOLEN PERSON'S ID. ALSO THE DATEX-P MAY BE ABLE TO TELL WHAT USER ID WAS USED AT THAT TIME TO GAIN ACCESS TO THE NETWORK.

SINCE THE INTRUDER IS CALLING A UNIVERSITY OF BREMEN COMPUTER, OR A DATEX-P DIAL-IN PAD NUMBER, THERE ARE ONLY A FEW NUMBERS THE INTRUDER IS CALLING FROM HIS HOME OR PLACE OF BUSINESS. IT IS

PAGE FOUR AX 196A-999 UNCLAS

SUGGESTED THAT A DIALED NUMBER RECORDER, (PEN REGISTER), BE USED TO SEE IF THE KNOWN SUBJECT IS DIALING INTO ANY OF THESE NUMBERS OF ACCESS PORTS, SO THE FBI CAN MATCH THESE TIMES TO TIMES OF ACCESS OF THE LBL COMPUTERS.

IF A DIALED NUMBER RECORDER WAS USED, [REDACTED]

[REDACTED] THIS MATTER COULD ALSO TELL IF THE SUBJECT IS USING A COMPUTER AND AT WHAT TIMES, DUE TO HIS DIALING COMPUTER ACCESS PORT NUMBERS. THE INFORMATION FROM A DIALED NUMBER RECORDER IN THE UNITED STATES HAS PROVEN A STRONG SOURCE OF TIMELY INFORMATION FOR SEARCH WARRANT AFFIDAVITS.

LEAD. LEGAT BONN AT BREMEN, FRG: CONTACT LEGAT BONN AT BREMEN: PROVIDE RECENT INFORMATION CONCERNING ACCESSES OF LBL COMPUTER THROUGH THE UNIVERSITY OF BREMEN COMPUTER TO [REDACTED]

[REDACTED] IDENTIFY THE OWNER OF RECENT NETWORK ID USED TO GAIN ACCESS TO THE TYMNET NETWORKD AND THEN LBL, AT TIMES AND DATES INDICATED ABOVE. [REDACTED] AT DATEX-P IS LOGICAL SOURCE OF INFORMATION. ALSO ESTABLISH [REDACTED]

[REDACTED] IF A STOLEN NETWORK ID NUMBER IS BEING USED THEN THE SUBJECT IS CERTAINLY BREAKING LOCAL LAWS.

b6
b7C
b7D

PAGE TWO ~~SECRET~~

b3
b7E

LABORATORIES (LBL), BERKELEY, CALIFORNIA. INTRUSIONS INTO LBL COMPUTERS HAVE BEEN ONGOING SINCE SEPTEMBER, 1985, AND HAVE BEEN CLOSELY MONITORED. COMPUTERS AT LBL ARE ACCESSED BY A MODEM OR THROUGH ONE OF A NUMBER OF COMPUTER NETWORKS. THE MAJORITY OF THE INTRUSIONS HAVE BEEN FROM TYMNET, WHICH IS A NATIONWIDE NETWORK THAT CAN BE DIALED BY A LOCAL PHONE CALL FROM MOST MAJOR CITIES.

IT IS IMPORTANT TO UNDERSTAND THAT AFTER CONNECTING TO THE LBL COMPUTERS, THE INTRUDER THEN HAS USED THE LBL COMPUTER TO CONNECT TO OTHER NETWORKS AND COMPUTERS. LBL HAS MAINTAINED LOGS WHICH SHOW ALMOST ALL OF THE INTRUDER'S ACTIVITIES WHILE CONNECTING THROUGH THE LBL SYSTEMS. IT IS IN THIS MANNER THAT IT HAS BEEN DETERMINED THAT A NUMBER OF COMPUTER SYSTEMS HAVE BEEN THE TARGETS OF ATTEMPTED AND SOMETIMES SUCCESSFUL PENETRATIONS.

WHEN LBL DISCOVERED THE METHODS THAT THE INTRUDER WAS USING, THEY OBTAINED WARRANTS THROUGH CALIFORNIA COURTS AND TRACED INCOMING PHONE CALLS. THE CONNECTION TO TYMNET WAS DISCOVERED TO ORIGINATE FROM INSIDE OF MITRE CORPORATION IN MCLEAN, VIRGINIA. WHEN MITRE WAS APPRISED OF THE SITUATION, THEY