INBOX.6 (#4671)

RECEIVED [redacted] OF INVESTIGATION

[redacted]

Exec AD Adm
Exec AD Inv
Exec AD
Asst. D
Adm. S
Crim.
Ident.
Inspt.
Intell.
Legal Coun.
Off. Cong. &
Public Affs.
Rec. Mgnt.
Tech. Servs.
Training
Telephone Rm.
Director's Sec'y

[redacted]

b6
b7C

[redacted]

TEXT: AX0002 1801308Z
OO HQ LEGAT BONN
DE AX
O 301255Z JUN 87

FM ALEXANDRIA (196A-999) (P)

TO ACTING DIRECTOR, FBI IMMEDIATE

LEGAT BONN

[redacted]

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)

ON JUNE 26, 1987, DR. CLIFF STOLL, LAWRENCE BERKELEY LABORATORY (LBL) PROVIDED THE MOST CURRENT LIST OF INTRUSION TIMES BY THE WEST GERMAN HACKER. THE TIMES ARE IN GREENWICH MEAN TIME AND WILL HAVE TO BE TRANSLATED INTO FRG TIME.

[redacted]

THE FOLLOWING IS A DIRECT TRANSCRIPTION OF AN ELECTRONIC MAIL MESSAGE FROM DR. CLIFF STOLL:

SUB: TIMES & ADDRESSES FROM LBL

JUNE 26, 1987

TO: EVERYONE ON BOTH SIDES OF THE ATLANTIC

196-7755-1482

b6
b7C

10 JUL 23 1987

[redacted]

RELAY TO Bonn

18 NOV 1 1988

[redacted]

On or about 1/21/87 instant investigation was reclassified back to a 196 matter, and the title was changed to reflect the characterization as an FBW matter. b3 b7E

The case was closed on 2/23/88. On 9/20/88, it was reopened under instant caption as a [redacted] in WMFO. The purpose of this was primarily to make a positive determination whether or not any classified information was accessed by the intruder. WMFO intended to make this determination through examination of records of the hacking sessions which have been maintained at Lawrence Berkeley Laboratories. To date, these records have not been received.

For information, SA [redacted] has advised that the printout of all the intruder's hacking sessions is maintained by DAVE STEVENS at the Lawrence Berkeley Laboratory (LBL). SA [redacted] advised further that STEVENS will not release this material without the consent of LBL's Legal Counsel. He recommended that PHIL SIEBERT, US Department of Energy (DOE), Rockville, Maryland, be contacted as SIEBERT has stated that he can expedite this process. b6 b7C

MON	MAY 18	13:54 - 13:56	SVENTEK	2624 DNIC 5421 0421
MON	MAY 18	14:12 - 14:19	SVENTEK	*
WED	MAY 20	12:48 - 13:01	SVENTEK	2624 DNIC 5421 0421
WED	MAY 20	12:58 - 13:01	SVENTEK	*
WED	MAY 20	16:49 - 16:52	GMJUNG	*
FRI	MAY 29	18:48 - 19:24	SVENTEK	2624 DNIC 4511 0391 38
SAT	MAY 30	13:23 - 14:14	SVENTEK	2624 DNIC 4511 0199 36
SAT	MAY 30	14:15 - 14:16		*
SAT	MAY 30	15:40 - 16:10	SVENTEK	*
TUE	JUNE 2	22:30 - 22:32	SVENTEK	*
THUR	JUN 11	22:38 - 23:13	SVENTEK	2624 DNIC 4511 0198 38
THUR	JUN 11	23:14 - 23:17	SVENTEK	2624 DNIC 4511 0198 38
THUR	JUN 11	23:18 - 23:19	SVENTEK	2624 DNIC 4511 0198 38
FRI	JUN 12	17:55 - 18:15	SVENTEK	2624 DNIC 4511 0391 39
FRI	JUN 12	20:46 - 21:50	SVENTEK	2624 DNIC 4511 0392 37
FRI	JUN 12	21:50 - 21:59		*
SUN	JUN 14	16:32 - 18:03	SVENTEK	2624 DNIC 4511 0199 36
TUE	JUN 16	00:51 - 01:00	SVENTEK	2624 DNIC 4511 0392 36
TUE	JUN 16	01:10 - 02:25	SVENTEK	2624 DNIC 4511 0392 36
TUE	JUN 16	02:25 - 02:45	SVENTEK	2624 DNIC 4511 0392 36

TUE	JUN 16	2:44 - 02:58	SVENTEK	2624 DNIC 4511 0392 36
TUE	JUN 16	04:15 - 04:49	SVENTEK	2624 DNIC 4511 0391 36
TUE	JUN 16	19:47 - 19:52	SVENTEK	*
TUE	JUN 16	20:59 - 21:10	SVENTEK	*
TUE	JUN 16	22:29 - 22:31	SVENTEK	*
FRI	JUN 19	23:01 - 23:27	SVENTEK	*
SUN	JUN 21	19:37 - 19:42	SVENTEK	*

AN ASTERICK (*) MEANS WE (LBL) WILL GET THE CALLING ADDRESS FROM HISTORIC ACCOUNTING RECORDS. THESE ADDRESSES WILL BE AVAILABLE IN ABOUT A WEEK (I HOPE<).

EXCEPT FOR THE SESSION ON JUNE 21, WE (LBL) HAVE COMPLETE PRINTOUTS OF EVERY SESSION. WE PRINTED EVERY CHARACTER ENTERED, AND EVERY CHARACTER FROM THE COMPUTER.

FINALLY, I HAVE KEPT A LOG-BOOK OF "RECORD INTRUSIONS INTO THE LBL COMPUTER SYSTEM". THIS IS ABOUT 100 PAGES, DESCRIBING THE EVENTS BEGINNING IN AUGUST, 1986.

CLIFF STOLL

--- --- --- END OF MESSAGE FROM LBL --- --- ---

BT

6029

INBOX.29 (#6563)

TEXT: AX0012 1662157Z
OO HQ PG SF LEGAT BONN
DE AX
O 152100Z JUN 87

16 JUN 87 03 58 FBI/DOJ

FM ALEXANDRIA (196A-999) (P)

TO ACTING DIRECTOR, FBI IMMEDIATE

LEGAT BONN IMMEDIATE

PITTSBURGH PRIORITY

SAN FRANCISCO PRIORITY

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)

ON JUNE 13, 1987, DR. CLIFF STOLL, LAWRENCE BERKELEY LABORATORY (LBL) PROVIDED THE MOST CURRENT LIST OF INTRUSION TIMES BY THE WEST GERMAN HACKER. THE TIMES ARE IN PACIFIC DAYLIGHT TIME (PDT) AND WILL HAVE TO BE TRANSLATED INTO FRG TIME.

STOLL ADVISED THAT THE CONFIDENCE OF THE INTRUDER IS HIGH AND HE IS STAYING ON FOR EXTENDED PERIODS OF TIME. IT IS ANTICIPATED THAT THE HACKER WILL ACCESS THE COMPUTERS THE WEEKEND OF THE 19TH

196-7755-14X4

9 JUL 21 1987

RELAY TO BOA

18 DEC 07 1988

THROUGH 21ST. IT IS NECESSARY THAT PROPER PERSONNEL BE STANDING BY, IN THE FRG. TO TRACE THE PHONE CALLS AND ALSO TO EXECUTE SEARCH WARRANTS.

FOLLOWING ARE THE MOST RECENT TIMES OF ACCESS BY THE INTRUDER:

THURS JUN 11 3:38 P.M. TO 4:13 P.M. PDT (22:30 TO 23:13 GMT).

THURS JUN 11 4:14 P.M. TO 4:17 P.M. PDT (23:14 TO 23:17 GMT).

THURS JUN 11 4:18 P.M. TO 4:20 P.M. PDT (23:18 TO 23:20 GMT).

THESE CALLS ORIGINATED FROM DNIC 2624 4511 0198 38. TELEPHONE REGISTRATION UNITS MAY SHOW ONLY ONE CALL FROM 22:38 TO 23:20 GMT.

FRI. JUN 12. 10:55 A.M. TO 11:15 A.M. PDT (17:55 TO 18:15 GMT). THE CALL WAS TRACED TO DNIC 2624 4511 0391 39.

SUN. JUN 14. 09:32 A.M. TO 11:03 A.M. (16:32 TO 18:03 GMT).

SUN. JUN 14. 11:04 TO 11:04 A.M. PDT (18:04 TO 18:04). THESE CALLS WERE TRACED TO DNIC 2624 4511 0199 36.

DURING THESE INTRUSIONS THE HACKER SUCCESSFULLY STOLE A COMPUTER PASSWORD FILE, BROKE INTO U.S. GOVERNMENT COMPUTERS, AND FAR EXCEEDED A NORMAL USER'S AUTHORIZATION BY BECOMING A SUPER USER ON THE LBL COMPUTER SYSTEM.

IT IS IMPORTANT TO NOTE THAT THE INTRUDER IS VERY FAMILIAR WITH

THE UNIX OPERATING SYSTEM. HE IS PERSISTENT, PATIENT AND KEEPS A RECORD OF HIS ACTIVITIES GOING BACK AT LEAST EIGHT MONTHS. DURING THESE MOST RECENT INTRUSIONS, HE CHECKED ON ACCOUNTS HE ALTERED ABOUT EIGHT MONTHS AGO. THIS INFORMATION WOULD HAVE BEEN NEARLY IMPOSSIBLE TO HAVE RECALLED FROM MEMORY AND NOTES OR RECORDS MUST HAVE BEEN USED.

LEADS. LEGAT BONN AT BREMEN, FRG: EXPEDITIOUSLY PROVIDE THE ABOVE INFORMATION TO [redacted]

ESTABLISH IF [redacted] b7D

IN PLACE CURRENTLY IS A SYSTEM TO PROVIDE INFORMATION TO THE [redacted] STOLLE, AT LBL, CALLS TYMNET b6 b7C b7D WHEN THE INTRUDER IS ACCESSING THE LBL SYSTEM. WITHIN FIVE MINUTES OF THE INTRUSTION, IT IS KNOWN TO TYMNET WHAT DNIC PORT AT HONNOVER (FRG) IS BEING USED BY THE INTRUDER. AT THE NEXT STEP, YOU NEED A TRAP/TRACE BY [redacted] TO EXECUTE THE TRAP AND TRACE.

LEGAT IS REQUESTED TO ADVISE [redacted] TO THE RECENT SURGE OF ACTIVITY. WITH A THREE DAY WINDOW [redacted] IT IS THOUGH THAT THIS WILL SOLVE ALL PROBLEMS OF TIME AND TRACING. PLEASE ADVISE ALEXANDRIA IMMEDIATELY IF [redacted] WILL ALLOCATE THE RESOURCES NECESSARY TO CATCH THIS INTRUDER.

THIS INTRUDER MUST BE IDENTIFIED AND PROSECUTED IF POSSIBLE. b7D HIS METHODOLOGY HAS PROVEN THAT EVEN IF HE IS LOCKED OUT OF LBL, HIS PENETRATIONS WILL CONTINUE VIA ANOTHER ROUTE OF INTRUSION.

LEGAT IS REQUESTED TO ADVISE ALEXANDRIA AS SOON AS LIAISON IS SET UP [redacted] IT WILL BE IMPOSSIBLE TO COORDINATE ALL THE NECESSARY PERSONNEL INVOLVED IN CATCHING THIS HACKER. OTHER GOVERNMENT AGENCY ATTENTION REMAINS HIGH IN THIS MATTER AND IS NOT LESSENING.

BT

5885

INBOX.33 (#4772)

RECEIVED
TELETYPE UNIT
9 JUN 87 05 27 Z
FBI/DOJ

TEXT: AX0014 1592314Z
RR HQ PG SF LEGAT BONN
DE AX
P 08 2220Z JUN 87

FM ALEXANDRIA (196A-999) (P)

TO DIRECTOR PRIORITY

PITTSBURGH PRIORITY

SAN FRANCISCO PRIORITY

LEGAT, BONN PRIORITY

BT

UNCLAS E F T O

ATTENTION: SSA [redacted] WHITE COLLAR CRIME SECTION, CID

UNSUBS; UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA; FBW; 00:AX

ON JUNE 6, 1987, DR. CLIFF STOLL, LAWRENCE BERKELEY LABORATORY (LBL), PROVIDED THE MOST CURRENT LIST OF INTRUSION TIMES BY THE WEST GERMAN HACKER. THE TIMES ARE IN PACIFIC DAYLIGHT TIME (PDT) AND WILL HAVE TO BE TRANSLATED INTO FRG TIME. THEY ARE IDENTIFIED AS FOLLOWS:

APRIL 6, 1987 - 07:54 AM TO 09:08 AM. DURING THIS LOG IN, THE INTRUDER LOGGED OUT AND BACK IN UNDER DIFFERENT USER NAMES,

Exec AD Adm
Exec AD Inv.
Exec AD LES
Asst. Dir.:
Adm. Ser
Crim. Inv
Ident.
Insp.
Intell.
Lab.
Legal Co
Off. Cong
Public Af
Rec. Mgmt.
Tech. Servs
Training
Telephone Rm.
Director's Sec'y

b6
b7C

196-7755-145

JUL 9 1987

RELAY TO Bonn

6-

18 DEC 07 1988

BUT PROBABLY DID NOT DISCONNECT IN THE FRG. IT SHOULD BE UNDERSTOOD THAT IF THE HACKER DISCONNECTS FROM THE LBL COMPUTER, HE MIGHT STILL BE CONNECTED TO THE FRG DATEX-P SYSTEM.

APRIL 14, 1987 - 05:40 AM TO 05:42 AM, 06:36 AM TO 06:38 AM, 06:40 AM TO 06:45 AM. ON THIS DATE, THE HACKER PRINTED OUT A PASSWORD FILE WHICH IS A CLEAR VIOLATION OF UNITED STATES STATUTES.

APRIL 19, 1987 - 09:03 AM TO 09:04 AM, 12:39 PM TO 12:40 PM, 12:41 PM TO 12:44 PM. THE INTRUDER ATTEMPTED TO LOG IN AS THE USER "ATCHLEY" WITH AN OLD VERSION OF THE PASSWORD. ATCHLEY HAD CHANGED HIS PASSWORD AND THE ATTEMPTED LOGIN FAILED. THE SIGNIFICANCE OF THIS IS THAT THE INTRUDER HAD DOWNLOADED THE ENCRYPTED PASSWORD FILE PREVIOUSLY, AND HE MUST BE USING A SOPHISTICATED PASSWORD CRACKING, OR DECODING PROGRAM IN THE FRG.

MAY 5, 1987 - 5:39 PM TO 5:43 PM. THE INTRUDER CHANGED HIS PASSWORD ON ONE OF HIS STOLEN ACCOUNTS.

MAY 29, 1987 - 11:48 AM TO 12:24 PM. THE INTRUDER FAR EXCEEDED A NORMAL USER'S AUTHORITY, BECAME A SUPER USER AND ATTEMPTED TO BREAK INTO OTHER U. S. GOVERNMENT COMPUTER SITES.

MAY 30, 1987 - 06:23 AM TO 07:14 AM, 07:15 AM TO 07:16 AM, 08:40 AM TO 09:10 AM. AGAIN THE INTRUDER BECAME A SUPER USER AND

ATTEMPTED TO BREAK INTO OVER 30 DIFFERENT U. S. GOVERNMENT COMPUTER SYSTEMS.

ON MAY 29, 1987, THE INTRUDER WAS TRACED BY TYMNET TO A HANOVER DATEX-P PAD DNIC 4511 0391 38. ON MAY 30, 1987, THE INTRUDER WAS AGAIN TRACED TO DNIC 4511 0391 38.

ON JUNE 2, 1987, THE INTRUDER WAS ON LINE FROM 3:30 PM TO 3:32 PM PDT. IT IS NOT YET KNOWN WHAT TOOK PLACE AT THIS TIME.

IN A COMMUNICATION FROM [redacted] OF DATEX-P TO [redacted] OF TYMNET, AND CLIFF STOLL OF LBL, HE ADVISED THE FOLLOWING:

b6
b7C
b7E

THE PHONE COMPANY HAS INSTALLED PEN REGISTERS ON SUSPECTED PHONE NUMBERS OF THE INTRUDER.

[redacted] HAS INSTALLED HARDWARE MONITORS TO RECORD CONNECTIONS OF ALL INGOING AND OUTGOING TRAFFIC. IF THE HACKER USES [redacted] AS TRANSIT POINT, THIS INFORMATION WILL BE AVAILABLE [redacted]

b6
b7C
b7D

THE PHONE COMPANY WILL HAVE A MORE DIFFICULT TIME OF TRACING THE PHONE CALLS TO THE DATEX-P PAD, DUE TO A STANDARDIZATION OF THE PAD NUMBERS THROUGHOUT THE FRG.

[redacted] WAS SUPPOSED TO HAVE A CONFERENCE ON JUNE 2, 1987, TO DISCUSS THE NEXT STEPS IN THE FRG IN CATCHING THE INTRUDER.

LEGAT BONN HAS PREVIOUSLY REQUESTED THE RECORDS OF INTRUSIONS LOCATED AT LBL. THE RECORDS ARE SENSITIVE IN NATURE AND SHOULD BE GUARDED AGAINST LOSS OF IMPROPER DISSEMINATION. DUE TO THE VOLUME OF INFORMATION, IT IS DIFFICULT TO SEND (TO THE FRG) THOUSANDS OF PAGES OF DOCUMENTS THAT THE INTRUDER'S SESSIONS HAVE GENERATED. THE PRINTOUTS ARE TECHNICAL IN NATURE AND IT WOULD BE NECESSARY FOR SOMEONE FROM THE U. S., FAMILIAR WITH THEM, TO EXPLAIN THEM [redacted] IT IS NOT A SIMPLE MATTER TO MATCH SEIZED RECORDS TO WHAT WOULD BE SENT TO THE FRG. THE MERE VIEWING OF THE THOUSANDS OF PAGES OF THE LBL PRINTOUTS IS A TIME CONSUMING TASK, NOT INCLUDING THE COMPREHENSION OF THE OPERATING SYSTEM COMMANDS THE INTRUDER IS USING.

LEADS. LEGAT BONN. AT BREMEN, [redacted] b7D

ADVISE ALEXANDRIA AS TO WHETHER OR NOT [redacted]

ESTABLISH [redacted]

[redacted]

ADVISE ALEXANDRIA AS TO WHETHER OR NOT [redacted]

[redacted]

[redacted] IT IS THOUGHT THAT

[redacted] BUT IT IS VERY UNCLEAR

TO ALEXANDRIA [redacted] ALEXANDRIA

WOULD LIKE TO BRING CASE TO TIMELY CONCLUSION DUE TO OTHER

GOVERNMENT AGENCIES' INTERESTS IN THE METHODOLOGY USED BY THE

INTRUDER. b7D

LEGAT IS REQUESTED TO ESTABLISH WHETHER OR NOT [redacted]

[redacted] AND TO

DISSEMINATE THIS INFORMATION TO ALEXANDRIA.

LEGAT IS REQUESTED TO ADVISE FBIHQ AND ALEXANDRIA PRIOR TO

ANY INTERVIEWS BEING CONDUCTED OF THE FRG SUBJECT DUE TO

NECESSITY OF TIMELY INTERVIEW OF SUBJECT IN THE UNITED STATES.

BT

5812

NNNN

FORMS.TEXT HAS 1 DOCUMENT

INBOX.14 (#10402)

TEXT: AX0006 3151852Z

PP HQ LEGAT BONN BS PH CG SF PG

DE AX

[redacted] 1850Z NOV 87

[redacted] EXANDRIA (196A-999) (P)

TO DIRECTOR PRIORITY

LEGAT, BONN PRIORITY

BOSTON (264A-1) PRIORITY

PHILADELPHIA PRIORITY

CHICAGO (264B-2) PRIORITY

SAN FRANCISCO (196A-2587) [redacted] PRIORITY

PITTSBURGH (196A-1638) PRIORITY

BT

UNCLAS

SECTION 1 OF 2

ATTENTION: CID, WHITE COLLAR CRIME SECTION

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

UNSUBS, AKA COMPUTER CHAOS CLUB, HAMBURG, FEDERAL REPUBLIC OF GERMANY (FRG); FBW

DE-139 196-7755-110

UNSUBS, AKA CARL HAGBARD, HAGGIE, HAGBARD C., HAGGIE KARL; NET

11 NOV 24 1987

[redacted]

2 WT XEROX

JUN 15 1988

53 SEP 01 1988

RELAYED TO: BON

b3
b6
b7C
b7E

b6
b7C

196-8035-
264-13-

Unrecorded Copy Filed In

RANGERS; CHAOS COMPUTER CLUB (CCC); HANNOVER, WEST GERMANY;
COMPUTER FRAUD AND ABUSE

REFERENCE BONN TELETYPE DATED OCTOBER 14, 1987; AND CHICAGO AIRTEL TO BUREAU DATED SEPTEMBER 24, 1987.

THIS TELETYPE WILL PROVIDE LIMITED INFORMATION ABOUT THE CHAOS COMPUTER CLUB, ANSWER LEAD QUESTIONS SET FORTH BY BONN LEGAT, AND ESTABLISH THE EXISTENCE OF A LINK BETWEEN THE CERN INTRUSIONS AND THE LAWRENCE BERKELEY LABORATORY (LBL) INTRUSIONS. NASA SPACENET INTRUSIONS ARE NOT ADDRESSED IN THIS COMMUNICATION AND ARE NOT BEING INVESTIGATED BY ALEXANDRIA.

ALEXANDRIA HAS BEEN INVESTIGATING SINCE DECEMBER, 1986, INTRUSIONS INTO NUMEROUS GOVERNMENT COMPUTER SYSTEMS WITH THE SOURCE OF THE INTRUSIONS ORIGINATING IN THE FEDERAL REPUBLIC OF GERMANY (FRG). THE INVESTIGATION RESULTED IN TELEPHONE TRACES TO A RESIDENCE IN HANNOVER, FRG AND THE EXECUTION OF A SEARCH WARRANT ON JUNE 25, 1987. THE FRG WARRANT WAS EXECUTED AT THE APARTMENT OF [redacted] COMPUTERS AND DISKS WERE SEIZED AT THE LOCATION AND IT SHOULD BE NOTED THAT [redacted]

b6
b7C
b7D

[redacted]

ALEXANDRIA [redacted]

[redacted] b7D

ON NOVEMBER 5, 1987, A SPECIAL AGENT OF THE AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS (OSI) PROVIDED INFORMATION THAT THE INTRUDER IN THE LBL COMPUTER SYSTEMS HAD ACCESSED CLASSIFIED INFORMATION LOCATED ON THE AIR FORCE SPACE SYSTEMS COMMAND COMPUTER LOCATED IN CALIFORNIA. AN ONGOING DAMAGE ASSESSMENT BY OSI AGENTS WILL YIELD SPECIFIC INFORMATION RETRIEVED BY THE INTRUDER. LOGS RETAINED AT LBL BY DR. CLIFF STOLL REFLECT THE INTRUSIONS, AND SOME OF THE ORIGINAL PRINTOUTS REFLECTING INTRUSIONS AT SPACE SYSTEMS COMMAND ARE RETAINED IN EVIDENCE CONTROL AT ALEXANDRIA FBI.

ALEXANDRIA DOES NOT HAVE A LOT OF INFORMATION REGARDING THE CHAOS COMPUTER CLUB (CCC). DR. STOLL AT LBL HAS EXCHANGED ELECTRONIC MAIL WITH OTHER COMPUTER SYSTEMS MANAGERS REGARDING THIS GROUP AND ADVISED THAT THE CCC HAS OPERATED IN FRG SINCE 1985. THEY ARE A SEMI-UNDERGROUND ORGANIZATION THAT DOES NOT HOLD PUBLIC MEETINGS, AND SEVERAL VMS AND UNIX COMPUTER SYSTEM MANAGERS PARTICIPATE IN THE ORGANIZATION. A MAIN PURPOSE OF THE

GROUP IS TO ENTER COMPUTER SYSTEMS TO WHICH THEY HAVE NO LEGITIMATE ACCESS. THEY HAVE CAUSED PROBLEMS AT CERN (SWISS PHYSICS LAB), DESY (GERMAN PHYSICS LAB), UNIVERSITY OF TORONTO IN CANADA, UNIVERSITY OF KARLSRUHE, FRG, EUROPEAN MOLECULAR BIOLOGY LABS, SPACE PHYSICS ANALYSIS NETWORK (SPAN), AND FERMI NATIONAL ACCELERATOR LABORATORY (FNAL), BATAVIA, ILLINOIS. SYSTEMS MANAGERS AT THESE COMPUTER SITES HAVE ATTRIBUTED DAMAGE TO COMPUTER SYSTEMS AND THEFT OF COMPUTING SERVICES AND TIME TO MEMBERS OF THIS GROUP.

LEGAT BONN REQUESTED INFORMATION REGARDING A NUMBER OF COMPUTER PROGRAMS AND CODE WORDS USED BY THE SUBJECTS OF THE CERN INTRUSIONS. IN A NUMBER OF CASES THE CODE WORDS REFER TO COMPUTER PROGRAMS THAT COULD BE USED FOR BREAKING INTO A COMPUTER. IF COPIES OF THESE PROGRAMS AND OR THEIR SOURCE CODE IS PROVIDED TO THE ALEXANDRIA EBI FIELD DIVISION, THE EXACT MEANING OF THE PROGRAM CAN BE DETERMINED.

IT IS OF CONCERN TO THE ALEXANDRIA DIVISION THAT THE CERN INTRUDER KNEW ABOUT SDINET. THE USE OF SDINET BY THE CERN INTRUDER SHOWS THAT EITHER THE LBL HACKER EXCHANGED INFORMATION WITH THE CERN HACKER(S), AND/OR THEY ARE ONE AND THE SAME. IT IS HIGHLY

IMPROBABLE TO IMPOSSIBLE, THAT THE CERN HACKER WOULD SEARCH FOR SDINET ON THE CERN COMPUTER WITHOUT HAVING HAD SOME CONTACT WITH THE LBL HACKER. SDINET IS PURELY FICTITIOUS AND WAS PLACED ON THE LBL COMPUTER BY DR. STOLL (SUPRA) AS A DEVICE TO KEEP THE HACKER ONLINE FOR A LONGER PERIOD OF TIME, ENABLING THE TRAP AND TRACES TO TAKE PLACE. THIS SHOULD BE OF GREAT INTEREST TO [redacted] IT IS HIGHLY SUSPECT THAT THE CERN INTRUDER USED LBL AND SDINET AT CERN, AND AS THIS COMBINATION IS UNIQUE, IT SHOWS SOME CONTACT BETWEEN [redacted] AND THE CERN HACKERS(S).

b6
b7C
b7D

SVENTEK IS A USER NAME EMPLOYED BY THE HACKER ON THE LBL COMPUTER AND IT IS UNUSUAL THAT THIS NAME WOULD BE USED AT BOTH SITES, BUT NOT IMPOSSIBLE SINCE IT BELONGS TO A FAMOUS UNIX PROGRAMMER.

LEGAT BONN REQUESTED OTHER INTERPRETATIONS OF WORDS AND PROGRAMS USED BY THE CERN HACKER. THE FOLLOWING IS AS CLOSE AN ESTIMATE AS IS POSSIBLE WITHOUT THE ACTUAL PROGRAMS:

NETDCL.COM IS A TOOL TO BREAK INTO VAX/VMS COMPUTERS. A USER FROM A DISTANT COMPUTER CAN CONNECT INTO A VAX/VMS COMPUTER OVER THE DECNET NETWORK. THIS CONNECTION PROVIDES ALMOST NO

PRIVILEGES TO THE USER; FOR EXAMPLE, THE FOREIGN USER MAY BE ALLOWED TO PRINT A FILE, OR TO GET THE STATUS OF THE COMPUTER, BUT CANNOT EXECUTE "SHELL-SCRIPT" COMMANDS (KNOWN AS DCL COMMANDS). NETDCL.COM IS A PROGRAM THAT GIVES PRIVILEGES TO A NON-PRIVILEGED NETWORK USER. IT IS A TOOL TO INCREASE PRIVILEGES BEYOND WHAT IS AUTHORIZED.

A.MAR AND A.LIS ETC. ARE ASSEMBLY LANGUAGE PROGRAMS FOR VAX/VMS COMPUTERS. A LISTING OF THE PROGRAM WILL TELL EXACTLY WHAT IT DOES.

CTERM.MAR IS AN ASSEMBLY LANGUAGE PROGRAM THAT MIGHT BE A TERMINAL-EMULATER. IT IS UNKNOWN WHAT IT DOES WITHOUT A LISTING OF THE PROGRAM.

PWDCH.FOR IS A FORTRAN PROGRAM FOR VAX/VMS WHICH MIGHT DO A NUMBER OF THINGS, A LISTING IS NECESSARY TO ADVISE PROPERLY.

WHOS IS A SYSTEM COMMAND TO LIST USERS ON A FOREIGN SYSTEM.

SYS$ANNOUNCE IS THE VAX/VMS MESSAGE AREA. IT HAS BEEN USED BY HACKERS AS A PLACE WHERE THEY CAN PLANT TROJAN HORSES OR LOGIC BOMBS.

BT

7346

FORMS.TEXT HAS 1 DOCUMENT

INBOX.15 (#10403)

TEXT: AX0009 3151856Z
PP HQ LEGAT BONN BS PH CG SF PG
DE AX
P 111858Z NOV 87

FM ALEXANDRIA (196A-999) (P)

TO DIRECTOR PRIORITY

LEGAT, BONN PRIORITY

BOSTON (264A-1) PRIORITY

PHILADELPHIA PRIORITY

CHICAGO (264B-2) PRIORITY

SAN FRANCISCO (196A-2587) [redacted] PRIORITY

b3
b7E

PITTSBURGH (196A-1638) PRIORITY

BT

UNCLAS

SECTION 2 OF 2

ATTENTION: CID, WHITE COLLAR CRIME SECTION

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

UNSUBS, AKA COMPUTER CHAOS CLUB; HAMBURG, FEDERAL REPUBLIC OF GERMANY (FRG); FBW

UNSUBS, AKA CARL HAGBARD, HAGGIE, HAGBARD C., HAGGIE KARL; NET RANGERS; CHAOS COMPUTER CLUB (CCC); HANNOVER, WEST GERMANY; COMPUTER FRAUD AND ABUSE

PWDCHANGE ALMOST CERTAINLY CHANGES PASSWORDS. THIS IS AN EXTREMELY DANGEROUS PROGRAM TO THE SYSTEM SINCE IT CAN BE USED TO ALLOW A HACKER TO OBTAIN ACCESS WITHOUT PERMISSION. THE LBL HACKER USED SOPHISTICATED PASSWORD CRACKING TECHNIQUES TO DECRYPT PASSWORDS COPIED FROM OTHER COMPUTERS AND THE ABOVE PROGRAM WOULD BE A PART OF THAT PROCESS.

GNU-EMACS IS THE FILE EDITOR ON THE VAX/VMS AND UNIX SYSTEMS. IT CONTAINS A FLAW THAT ALLOWS AN ORDINARY USER TO BECOME A SYSTEM MANAGER OR SUPER-USER. THE LBL HACKER USED THIS PROGRAM TO BECOME SYSTEM MANAGER ON THE LBL AND THE ANNISTON ARMY DEPOT COMPUTERS IN THE UNITED STATES.

OTHER ACCOUNT NAMES THE LBL HACKER STOLE INCLUDE: SVENTEK, MARK, WHITBERG, GORAN, BEDPAT, EADES, ABREN AND RITA. HE CREATED NEW LOGIN NAMES OF HUNT AND LANGMAN.

ANY OTHER PROGRAMS ON THE TELETYPE ARE NOT ABLE TO BE DECIPHERED WITHOUT AN ORIGINAL COPY PROVIDED TO ALEXANDRIA. THE ABOVE PROGRAM DEFINITIONS ARE ATTRIBUTED TO DR. CLIFF STOLL AT

LBL AND THE ALEXANDRIA CASE AGENT.

IN AN INTERVIEW WITH DR. STOLL, HE EXPRESSED DOUBTS THAT THE RECENT SPAN INTRUSIONS WERE ACCOMPLISHED BY THE LBL HACKER. HE ALSO EXPRESSED A CONCLUSION THAT THE CERN HACKING WAS CLOSELY RELATED TO THE LBL HACKING. STOLL ALSO ADVISED HE COULD INTERPRET ANY COMPUTER PROGRAMS PROVIDED TO HIM AND THAT HE WOULD ACT AS AN EXPERT WITNESS REGARDING SYSTEMS SOFTWARE.

IT IS AGAIN REQUESTED THAT THE ALEXANDRIA CASE AGENT BE ALLOWED TO REVIEW THE COMPUTER EVIDENCE SEIZED AT HANNOVER, AS HE HAS PERSONAL EXPERIENCE IN THE COMPUTERS THAT WERE SEIZED AND IN THE METHODS OF RECOVERY OF ERASED DATA.

BT

7347

DE-175

INBOX.124 (#6125)

TEXT:

VZCZCWM0010

RR HQ SF

DE WM #0010 3440125

ZNY SSSSS

R 080201Z DEC 88

FM FBI WASHINGTON METROPOLITAN FIELD OFFICE [redacted] (P)(CI-7)

TO DIRECTOR, FBI/ROUTINE/

FBI SAN FRANCISCO [redacted] /ROUTINE/

BT

~~S E C R E T~~

CITE: ~~//3920//~~

PASS: HQ FOR DIVISION 5.

SUBJECT: UNSUBS, UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA; [redacted]

OO:WMFO.

196-7755-21

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

PRELIMINARY INQUIRY INITIATED 9/26/88; TO EXPIRE 1/17/89.

DE-175 196-7755-18

REFERENCE WMFO TELETYPE TO FBIHQ AND SF, 9/27/88, AND SF TELETYPE TO FBIHQ AND WMFO, 10/11/88.

DEC 19 1988

MR 8/22/8 [redacted]

REFERENCED WMFO TELETYPE REQUESTED THAT SAN FRANCISCO

[redacted]

14

1-4117

CONTACT ROY KERTH, ASSOCIATE DIRECTOR FOR GENERAL SCIENCES, LAWRENECE BERKELEY LABORATORY (LBL), TO RETRIEVE ALL ORIGINAL PRINTOUTS FROM ALL HACKING SESSIONS OF THE LBL INTRUDER. REFERENCED SF TELETYPE ADVISED THAT CONTACT HAD BEEN MADE WITH KERTH, THAT KERTH WOULD BE OUT OF TOWN FOR APPROXIMATELY ONE WEEK, AND THAT KERTH WOULD THEN REVIEW MATERIAL IN LBL'S CUSTODY. SF TELETYPE FURTHER STATED THAT KERTH BELIEVED ALL ORIGINAL PRINTOUTS HAVE ALREADY BEEN PROVIDED TO THE FBI BY CLIFFORD STOHL.

FORMER WMFO CASE AGENT HAS BEEN IN CONTACT WITH STOHL RECENTLY AND ADVISED THAT HE WAS TOLD BY STOHL THAT, AS OF TWO WEEKS AGO, VIRTUALLY ALL ORIGINAL PRINTOUTS REMAIN AT LBL. THE SOLE EXCEPTION, PER STOHL, IS A PRINTOUT OF APPROXIMATELY 200-300 PAGES, CONCERNING THE SPACE SYSTEMS COMMAND, EL SEGUNDO, CALIFORNIA.

WMFO IS UNABLE TO PROCEED IN THIS MATTER UNTIL IT IS ABLE TO EXAMINE THE ORIGINAL PRINTOUTS AND TO MAKE A DETERMINATION OF WHETHER CLASSIFIED MATERIALS WERE OBTAINED. WMFO IS RECEIVING INQUIRIES FROM OTHER AGENCIES IN THIS MATTER, AND IS ANXIOUS TO RESOLVE THE MATTER. IF SAN FRANCISCO IS UNABLE TO RECONTACT

PAGE THREE DE WM 0010 ~~S E C R E T~~

KERTH AND ASCERTAIN THE WHEREABOUTS OF THE PRINTOUTS, FORMER CASE AGENT IS FAMILIAR WITH THE MATTER AND IS WILLING TO TRAVEL TO LBL.

LEAD. SAN FRANCISCO. AT LAWRENCE BERKELEY LABORATORY.

RECONTACT ROY KERTH. ASCERTAIN IF SUCH A PRINTOUT EXISTS. IF SO, OBTAIN PRINTOUT AND EXPEDITIOUSLY FORWARD SAME TO WMFO.

~~S E C R E T~~

~~C BY: 8796; DECL ON: OADR~~

BT

#0010

NNNN

INBOX.73 (#2528)

TEXT: [redacted]

VZCZCSF0001

RR HQ WF

DE SF #0001 2860052

ZNY SSSSS

R 110000Z OCT 88

FM FBI SAN FRANCISCO [redacted] (P)(ORA 3)

TO DIRECTOR FBI /ROUTINE/

FBI WMFO [redacted] (CI-7)/ROUTINE/

BT

~~S E C R E T~~

~~CITE: //3790//~~

SUBJECT: UNSUBS; UNAUTHORIZED USE OF GOVERNMENT COMPUTER [redacted]
IN LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA;

194-T155-22

OO: WMFO

ALL MARKINGS, NOTATIONS AND ITEMS OF INFORMATION CONTAINED IN THIS COMMUNICATION ARE CLASSIFIED ~~"SECRET"~~ UNLESS OTHERWISE NOTED.

RE: WMFO TELETYPE TO FBIHQ AND SAN FRANCISCO DATED SEPTEMBER 27, 1988.

CONTACT HAS BEEN MADE WITH MR. ROY KERTH, ASSOCIATE [redacted]

1-4117

CONS/RPS [redacted]

b6
b7C

3/6/90

LABORATORY DIRECTOR FOR GENERAL SCIENCES, LAWRENCE BERKELEY LABORATORY (LBL), BERKELEY, CALIFORNIA, TELEPHONE [redacted] b6 per DOE

IN AN EFFORT TO RETRIEVE ALL ORIGINAL PRINT-OUTS FROM HACKING SESSIONS OF THE LBL INTRUDER. KERTH ADVISED THAT HE WAS THE HEAD OF THE COMPUTING DIVISION AT LBL AT THE TIME OF THE HACKING INCIDENT, WHICH WAS HANDLED WITHIN LBL BY DR. CLIFFORD STOHL. STOHL NO LONGER WORKS FOR LBL AND ALL INFORMATION PERTAINING TO THE LBL HACKER HAS BEEN PLACED IN STORAGE. HE WILL REVIEW THIS INFORMATION BUT BELIEVES THAT ALL ORIGINAL PRINT-OUTS HAVE ALREADY BEEN PROVIDED BY STOHL TO THE FBI. FURTHER, KERTH STATED THAT HE WAS NOT AWARE OF ANY OBVIOUSLY CLASSIFIED INFORMATION THAT THE HACKER GAINED ACCESS TO NOR HAD STOHL GIVEN HIM ANY INFORMATION TO THE CONTRARY. KERTH STATED THAT HE WOULD BE OUT OF TOWN FOR APPROXIMATELY ONE WEEK BUT THAT HE WOULD THEN REVIEW ALL MATERIAL STILL IN THE POSSESSION OF LBL PERTAINING TO CAPTIONED MATTER. SAN FRANCISCO WILL ADVISE WMFO OF THE OUTCOME OF THIS REVIEW.

~~C (G-3); D (OADR)~~

BT

#0001

NNNN

~~SECRET~~

AIRTEL

TO: DIRECTOR, FBI 3/3/89
ATTN: SSA [redacted] CI-1E

[redacted]

WASHINGTON METROPOLITAN FIELD OFFICE [redacted] (C) (CI-7)

b3
b6
b7C
b7E

UNSUB;
UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN
LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA;
[redacted]
00:WMFO.

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

Preliminary inquiry initiated 9/26/88; extended to 4/16/89.

Reference conference at FBIHQ, 3/3/89, between SSA [redacted]
[redacted] SSA J. [redacted] SSA [redacted] SSA [redacted]
SA J. [redacted] and SA [redacted]

b3
b6
b7C
b7E

As per referenced discussion, instant investigation is being closed at WMFO in order to facilitate consolidation at FBIHQ.

This investigation had been opened on 12/22/86 in the Alexandria Field Office as a 196-A matter (Fraud by Wire). The original caption was "UNSUBS; UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN LAWRENCE LIVERMORE NATIONAL LABORATORY, BERKELEY, CALIFORNIA; FBW; 00:AX."

It was reclassified 1/9/87 into a [redacted] matter. The title was thereupon changed to "UNSUBS; UNAUTHORIZED USE OF GOVERNMENT COMPUTER SYSTEM IN LAWRENCE BERKELEY LABORATORY, BERKELEY, CALIFORNIA; [redacted] 00:AX."

[redacted]

~~CLASSIFIED BY: 8796~~
~~DECLASSIFY ON: OADR~~

196-7755-23

1cc Rm 4123

3-FBIHQ
(1-CI-2E)
1-WMFO

[redacted]
(4)

65-[redacted]

b6
b7C

4 MAR 10 1989

[redacted]

FIVE

[redacted]

CI[redacted]

1cc CI2E

58

~~SECRET~~

[redacted] to Cons 10-17-89 [redacted]

~~GBEL~~

[redacted] 4-12-90

[redacted]

b6
b7C

~~PFOKEL~~

FROM: CLIFF STOLL

LAWRENCE BERKELEY LABORATORY

BERKELEY, CALIFORNIA 94720 USA

[redacted] b6 per DOE

FOLLOWING IS SHORT LIST OF TIMES WHEN INTRUDER WAS KNOWN TO BE IN THE LBL COMPUTERS. (THE LONG LIST GOES BACK TO AUGUST, 1986)

ALL DATES AND TIMES ARE IN GMT

PDT = GMT - 7 HOURS

DATE	TIME (GMT)	ACCOUNT	CALLING ADDRESS
MON APR 6	14:54 - 14:54	EADES	*
MON APR 6	14:55 - 15:01	SVENTEK	*
MON APR 6	15:03 - 16:08	EADES	"HANNOVER PAD" *
TUE APR 14	12:40 - 12:42	SVENTEK	*
TUE APR 14	13:36 - 13:38	BUCK	*
TUE APR 14	13:40 - 13:45	EADES	"FROM EUROPE" *
SUN APR 19	16:03 - 16:04	EADES	*
SUN APR 19	19:39 - 19:40	ATCHLEY	*
SUN APR 19	19:41 - 19:44		*
WED MAY 6	00:39 - 00:43	EADES	*
MON MAY 18	13:54 - 13:54	EADES	2624 DNIC 5421 0421