

REVIEWED FOR RETENTION CRITERIA *DA review*
UP AR 391-10
REVIEWER *Thoma* DATE *30 June 93*

REVIEWED FOR RETENTION CRITERIA
UP AR 391-10
REVIEWER *J. Hoffel* DATE *10/25/93*
10/25/93

DOSSIER NO. **AE548807W**

As of 30 June 93 (Date) all material included
in this file conforms with DA policies currently
in effect.

Ladonna M. Thomas 30 June 93
(Signature) (Date Signed)
Ladonna M. Thomas 7
(Printed Name) (Grade)

REVIEWED FOR RETENTION CRITERIA
UP AR 391-10
REVIEWER *U. Kempf* DATE *6 Dec 00*

10 secret pages

THIS MUST REMAIN TOP DOCUMENT



DEPARTMENT OF THE ARMY
MILITARY INTELLIGENCE BATTALION
(COUNTERINTELLIGENCE) TECHNICAL
FORT GEORGE G. MEADE, MARYLAND 20755-8955



REPLY TO
ATTENTION OF:

IAGPA-A-OP-O (381-45c)

6 May 1993

MEMORANDUM FOR Record

SUBJECT: Missing Original Signature Investigative Memorandum
For Record (IMFR).

1. Original signature IMFRs numbered 1, 13, 17, 18, 19, 21, 22, 23, and 25 are missing from the Report of Investigation for ACCO CCN: due to inadvertent destruction.

2. The POC for this memorandum is SA
DSN

GS-13, DAC
Chief, SCO CONUS

SECRET



DEPARTMENT OF THE ARMY
MILITARY INTELLIGENCE BATTALION
(COUNTERINTELLIGENCE) TECHNICAL
FORT GEORGE G. MEADE, MARYLAND 20755-5955



REPLY TO
ATTENTION OF:

IAGPA-A-OP (381-45c)

6 May 1993

REPORT OF INVESTIGATION

1. ^(U)~~(S)~~ ADMINISTRATIVE DATA:

TITLE: Redstone Arsenal, AL
SAEDA (AUTO)
13 July 1990

ACCO CCN:

b2

INVESTIGATING UNIT: 902d MI Group

CONTROL OFFICE: SCO CONUS

DATE INITIATED: 20 July 1990

DATE CLOSED: 15 June 1993

REASON FOR INVESTIGATION:

To determine if a Foreign Intelligence Service was involved in an attempted penetration of a Department of Army computer system.

CASE STATUS: Terminated.

2. (U) SYNOPSIS:

INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED FROM ANOTHER FEDERAL AGENCY, WHO RESERVES THE RIGHT TO RESTRICT ITS RELEASE, AND WILL NOT BE RELEASED OUTSIDE OF ARMY INTELLIGENCE CHANNELS WITHOUT THEIR APPROVAL.

Referred

CLASSIFIED BY: Appendix E, INSCOM GUIDE 90-01
DECLASSIFY ON: OADR

SECRET

b2 b6

CONFIDENTIAL

IAGPA-A-OP

TITLE: ACCO CCN: b2 (U)

Referred

c. (U) On 21 and 23 August 1990, b6 ADP Security Specialist, Headquarters, Army Material Command, Rock Island, IL provided information that examination of the Rock Island computer system revealed no compromise of the system. However, it was discovered that computer files from the Picatinny Arsenal, Dover, NJ were accessed and transferred to the University of Chicago computer system. (3-4)

d. (U) On 21 August 1990, b6 Automated Data Processing Systems Security Office, U.S. Military Academy, NY provided information that an analysis of the logon files from 25 June to 13 July 1990 indicated no apparent penetration of the computer system or transfer of files from the system to the computer at the University of Chicago. However, the audit trail only listed unsuccessful logons and did not keep a record of successful logons and work processed on the system. (5, Exhibit III).

e. (U) On 23 August 1990, b6 MICOM, Redstone Arsenal, provided a copy of the "Cracker Program" (a computer program used to break encrypted passwords) used to penetrate the MICOM computer system. He also revealed that he could not determine the specific systems penetrated at Redstone Arsenal. (6, Exhibit IV)

Referred

CONFIDENTIAL

CONFIDENTIAL

IAGPA-A-OP

TITLE: ACCO CCN: [b2] (U)

Referred

g. (U) On 17 August and 5 September 1990, [b6] [b6] Assistant Security Manager and Automated Data Processing Special Security Officer, Letterkenny Army Depot, Chambersburg, PA, provided the following information. On 19 June 1990, she was informed of the penetration of the computer system at Letterkenny Army Depot. The system was accessed by an unauthorized user through the computer system at the University of Chicago. Of the seven systems accessed, one contained sensitive information on supply transactions and transportation of ammunition and weapons from depot to depot. Her analysis of the system records did not prove or refute the penetration and loss of data. [b6] is involved in the PATRIOT missile project and processes data on the shipment of the missiles. (8)

h. (U) On 7 September 1990, neither [b6] [b6] nor [b6] [b6] Picatinny Arsenal, Dover, NJ provided any relevant information concerning the unauthorized accessing and transfer of data from the system at Picatinny Arsenal. (9 - 12)

i. (C) On 8 November 1990, analysis of the computer tape from the University of Chicago revealed the presence of a classified message, dated March 1990, marked confidential, and concerned with the results of a Patriot missile counterlaunch experiment. The analysis also revealed that SUSPECT(s) transferred files from accessed computers to the University of Chicago and created a repository file on the University's computer system. These files contained PATRIOT weapons system data; information on key personnel; and project status, costs and vulnerabilities. (13, Exhibits VI-XC)

Referred

CONFIDENTIAL

~~SECRET~~

①

IAGPA-A-OP

TITLE: ACCO CCN: b2 (U)

k. (U) On 26 November 1990, b6 MICOM, Redstone Arsenal, AL alleged that it was determined that the penetration of MICOM's computer system and subsequent loss of data did not involve any classified information. He provided two messages sent to headquarters, U.S. Army INSCOM. One of the messages provided a cursory analysis of the University of Chicago computer tape, which revealed a listing of computer gateways (main entry points from a network to a computer system), computer network and system computer addresses, password files from MICOM, Rock Island Arsenal and Letterkenny Army Depot, data files from the US Army Military Academy and the MICOM PATRIOT Project Office. (15, Exhibits XCI-XCIII)

l. (U) On 27 November 1990, b6 Chief, Program Evaluation Branch, Patriot Project Office, Space Defense Command, Huntsville, AL, revealed the document "Results of Patriot Counterlaunch Experiment," was two years old and determined to be unclassified but sensitive. The document was processed on a system accredited for unclassified only. (16)

m. (U) On 27 November 1990, further analysis of the University of Chicago computer tape found no additional classified information. (17)

n. ~~(S)~~

b1

b1

Referred

4

~~SECRET~~

UNCLASSIFIED

IAGPA-A-OP

TITLE: ACCO CCN: b2 (U)

Referred

p. (U) b6 Computer Systems Analyst and b6 Computer System Analyst, Letterkenny Army Depot, Chambersburg, PA, reported on 16 August 1991 an unauthorized user (SUSPECT) attempted to access the A2 computer system at Letterkenny Army Depot. SUSPECT attempted to logon the system by using a User ID and password that was compromised a year ago. They were notified by b6 Systems Administrator, Columbia University, New York, NY that on 16 August 1991, a computer file identified as belonging to Letterkenny Army Depot was discovered on the Columbia University computer system. (20, Exhibits XCVI-XCVII)

q. (U) A determination was made that the data discovered in ACCO CCN: b2 and ACCO CCN: b2 was part of the data transferred by SUSPECT in this investigation. SUSPECT indicated in a computer talk session that HE used multiple satorage sites when HE transferred data. Based on this information, the above mentioned investigations were terminated and transferred to this investigation ACCO CCN: b2 (21)

r. (U) On 23 August 1991, b6 Computer Security Manager, US Army Information Command, Redstone Arsenal, AL, opined that the Test Measurement and Dianostic Equipment (TMDE) Support Group computer files discovered on the Columbia University computer system were penetrated and transferred during the same time frame as the data found on the University of Chicago computer system (July 1990). The password file used by SUSPECT to access the TMDE files was created prior to July 1990 and the passwords were changed during a shut down of Redstone's computer system in July 1990. (22)

s. (U) On 28 August 1991, b6 Security Specialist, MICOM, Redstone Arsenal, AL revealed the computer files discovered on the Columbia University computer system were from the TMDE computers at Redstone. The data is unclassified and nonsensitive. b6 determined that the password file discovered at Columbia University contained user IDs of personnel who had departed Redstone prior to 1 November 1990. It was determined that there was no recent penetration of the TMDE system and the penetration probably occurred in July 1990. (23)

UNCLASSIFIED

UNCLASSIFIED

IAGPA-A-OP

TITLE: ACCO CCN: b2 (U)

t. (U) On 18 September 1991, b6 Letterkenny Army Depot revealed that the computer file discovered on the Columbia University system was a decrypted version of an encrypted login password file from the A2 computer system at Letterkenny Army Depot and was probably electronically removed as early as August 1990. b6 opined that SUSPECT could have accessed the file and system at Letterkenny from anywhere and only the results of the decryption of the file were found at Columbia University. (24, Exhibit XCVIII)

u. (U) On 21 October 1991, b6 Systems Programmer, Columbia University, New York, NY provided information concerning the unauthorized accessing and use of computers by SUSPECT and the subsequent discovery of computer files belonging to the U.S. Army. b6 was initially made aware of the incident by b6 Director of Molecular Modeling Facility, Columbia University. It was determined the files placed in the university's computer system had been there for over one year. SUSPECT exploited a security hole in the system and gained root privileges (the ability to control the computer with access to all files), created a file storage area on the system and installed a "Cracker" program (a computer program that can decrypt encrypted passwords and user IDs). SUSPECT normally came into the system via a telnet connection from a computer located at Delf University, Netherlands. The files belonging to the U.S. Army were from Letterkenny Army Depot, PA; Redstone Arsenal, AL; and SIMA, Army Material Command Systems, ST Louis, MO. (25, Exhibits IC-CI)

v. (U) On 21 October 1991, b6 Director of Molecular Modeling Facility for Molecular Biology, Columbia University, New York, NY, revealed his computer system was penetrated approximately one year ago. At that time he installed an audit trail and the unauthorized penetrations stopped. On 13 August 1991, he noticed the unauthorized user was back and his audit trail program was tampered with. The SUSPECT was active from 13 through 15 August 1991. b6 confirmed b6 description of the penetration. (26)

w. (U) On 18 November 1991, b6 Systems Programmer, Columbia University, revealed the communications pathway for the penetration of Columbia University's computers was traced through a computer system in Finland and originated from a computer at Delf University, Netherlands. b6 Finnish citizen, computer system administrator, Finland, traced the connection from his computer system in Finland to the system at Delf University. (27)

UNCLASSIFIED

UNCLASSIFIED

IAGPA-A-OP

TITLE: ACCO CCN: [b2] (U)

x. (U) On 17 December 1991, [b6] and [b6] [b6] computer security experts, CIAC, U.S. Army Ballistic Research Laboratory, Aberdeen Proving Ground, MD provided an analysis of the data found on the University of Chicago system. They discovered a subdirectory that was encrypted and the key to the encryption appears to be the Unit Identification Code (UIC) for MICOM HQ. Also, they discovered that on 12 May, SUSPECT attempted to create an account named "rgb" (rgb is one of the hacker aliases used by the SUSPECT

[b6] (28, Exhibit CE)

3. (U) Case Terminated. Investigation revealed that U.S. Army computer systems were penetrated and computer files were transferred to computer systems at the University of Chicago and Columbia University to include one document marked confidential. The origin of the penetrations are from the Netherlands. Foreign Intelligence Service activity or collusion was neither proved nor refuted.

4. (U) ROI prepared by Special Agent [b6] MI BN (CI)(T), 902d MI Group, Fort Meade, MD 20755-5955.

[b6]

Encl
28 IMFRS
102 Exhibits

GS-13, DAC
Chief, SCO CONUS

UNCLASSIFIED



DEPARTMENT OF THE ARMY
 MILITARY INTELLIGENCE BATTALION
 (COUNTERINTELLIGENCE) TECHNICAL
 FORT GEORGE G. MEADE, MARYLAND 20755-5958



REPLY TO
 ATTENTION OF:

IAGPA-A-OP

6 May 1993

MEMORANDUM FOR RECORD

SUBJECT: Unlisted Attachment to Report of Investigation:

b2

1. The following item is appended to the Report of Investigation as unlisted attachment:

U.S. Department of Justice Letter

2. The POC for this action is Mr. b6 DSN
 b6 or (com) b6

b6

1 Encl

GS-13, DAC
 Chief, SCO CONUS



DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
FORT BELVOIR, VIRGINIA 22060-5370

REPLY TO
ATTENTION OF

03 FEB 1992

IAOPS-CI-OI (381-45c)

MEMORANDUM FOR COMMANDER, 902D MILITARY INTELLIGENCE GROUP, FORT
GEORGE G. MEADE, MD 20755-5910

SUBJECT: Dutch Hacker Related Cases

1. The enclosed Department of Justice letter is forwarded for your action. DOJ is requesting that the 902d keep their investigative files open on any Netherland related incidents until further notice. HQ INSCOM should be kept informed of the status of these investigations.

2. HQ INSCOM POC is Ms. b6 AV b6

Encl

b6
Colonel, GS
DCSOPS

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

Information has been withheld in its entirety in accordance with the following exemption(s):

It is not reasonable to segregate meaningful portions of the record for release.

Information pertains solely to another individual with no reference to you and/or the subject of your request.

Information originated with another government agency. It has been referred to them for review and direct response to you.

Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S) NO DUPLICATION FEE FOR THIS PAGE.

Page(s) 12-13

PRIORITY

CONFIDENTIAL

BT 43156 201/1256Z

[Redacted]

PAGE 01

SSSSSSSS	SSSSSSSS	00000000	ROUTER.....	CHECKER.....
SS	SS	00 00	FFFFFF	GGGGGGGG MMM MMM
SSSSSSSS	SSSSSSSS	00 00	FF	GG MMM MMM
SSSSSSSS	SSSSSSSS	00 00	XXX FFFFFF	GG MM MM MM MM
SS	SS	00 00	XXX FFFFFF	GG GGGG MM MMM MM
SSSSSSSS	SSSSSSSS	00000000	FF	GG GGG MM M MM
				GGGGGGGG MM MM

AN

POTMZYUW YEWRT 2561 2011645-MVSH--YEKHOV.
 ZNY MNSH
 ZKZK PP 504 05
 P 181400Z JUL 90
 FM SSO REDSTONE//IAGPA-R-03//
 TO SSO MEADE//IAGPA-02-1//
 SSO MEADE//IAGPA-1-0P/DAMI-CIC-000//
 ZEM

902d ce div
MIBNS
FCA 1/2

~~CONFIDENTIAL~~ [Redacted] SECTION 01 OF 02
 HANDLING INSTRUCTIONS DELIVER DURING FIRST DUTY HOURS. PLS PASS
 TO MI AN-SECURITY, 902D MI GROUP, ATTN: IAGPA-R-02, AND TO DA CO,
 ATTN: DAMI-CIC-000.
 SUBJECT: REDSTONE ARSENAL, ALABAMA

- 9 JULY 1990 (U)
1. (U) AR 381-12 DTD 1 JUL 89, S4E0A
 2. (U) MEMO, DAMI-CIC-000, 19 APR 1990, SUBJECT: COMPUTER SYSTEMS PENETRATIONS/ATTEMPTS
 3. (U) 902ND MI GP REG 381-9, DTD 8 AUG 89, CE OPNS
 4. (U) THE FOLLOWING IS KEYED TO FORMAT PROVIDED IN APP C, REF A, AND IS A CAT VI (AUTO) INCIDENT IAW REF B AND C.
 1. (U) UNKNOWN
 2. (U) REDSTONE ARSENAL, AL.
 3. (U) PERSONS INVOLVED:
 4. (U) SOURCE: [Redacted] b6, SS12, DEPARTMENT OF THE ARMY CIVILIAN (DAC), [Redacted] b6, [Redacted] b6, ASSIGNED TO THE AUTOMATIC DATA PROCESSING (ADP) SECURITY SECTION, SECURITY OPERATIONS BRANCH, COUNTERINTELLIGENCE DIVISION, SECURITY AND INTELLIGENCE DIRECTORATE (IRS), US ARMY MISSILE COMMAND (INCOM), BUILDING 3421, REDSTONE ARSENAL (R94), ALABAMA. TELEPHONE NUMBER: COM: (205) 642-7512.
 5. (U) WITNESSES: NONE
 6. (U) OTHER KNOWLEDGEABLE:

Referred

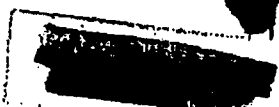
CONFIDENTIAL

[Redacted]

JUL 23 1990

PRIORITY

~~CONFIDENTIAL~~



b2

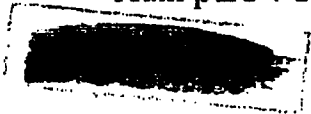
7.(U) SUSPECT: NONE

SOURCE HAD NO OBJECTION TO HIS IDENTITY BEING RELEASED
 A. (U) (C) ON 17 JULY 1990, b6 CONTACTED REPRESENTATIVES OF
 THE REDSTONE MI DETACHMENT TO REPORT THE PENETRATION OF A COMPUTER
 SYSTEM BELONGING TO MICON. ON 13 JULY 1990, b6 WAS
 CONTACTED BY MAJOR b6 (NFI) OF THE DEFENSE COMMUNICATIONS AGENCY
 (AUTOVON b6 WHO INFORMED HIM THAT A COMPUTER FOLDER,
 IDENTIFIED AS BELONGING TO THE PATRIOT PROJECT OFFICE, WAS LOCATED
 ON 9 JULY 1990 IN A COMPUTER SYSTEM BELONGING TO THE UNIVERSITY OF
 CHICAGO. THE FOLDER WAS FOUND BY A PROFESSOR AT THE UNIVERSITY
 (NFI) WHO HAD PURGED HIS FILES ON 25 JUNE 1990, PRIOR TO GOING ON
 LEAVE. THE FOLDER WAS NOT IN HIS FILES ON 25 JUNE 1990, BUT WAS
 FOUND THERE ON 9 JULY 1990 UPON HIS RETURN FROM LEAVE. THE FOLDER
 WAS TITLED b6 AND CONTAINED TRIP REPORTS, MEETING NOTES,
 INTRA-OFFICE MEMOS AND OTHER ROUTINE CORRESPONDENCE. SOMEONE
 ATTEMPTED TO RETRIEVE THE INFORMATION FROM THE UNIVERSITY OF
 CHICAGO COMPUTER ON 13 JULY 1990, BETWEEN 1500 AND 1600 HOURS BUT
 WAS UNABLE (NFI). THERE WAS NO CLASSIFIED INFORMATION STORED IN
 THE PATRIOT PROJECT OFFICE SYSTEM. THIS SYSTEM IS LINKED TO THE
 #2561

NNNN

Regraded UNCLASSIFIED on
 12 JAN 2011
 by USAINSCOM FOI/PA
 Auth para 4-102, DOD 5200-1R

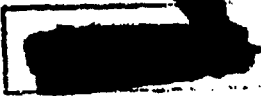
~~CONFIDENTIAL~~



PRIORITY

PRIORITY

~~CONFIDENTIAL~~



2

PT 43157 201/1R51Z

PAGE 01

				ROUTER.....	CHECKER.....			
SSSSSSSS	SSSSSSSS	00000000		FFFFFFF	GGGGGGGG	MM	MM	MM
SS	SS	00	00	FF	GG	MM	MM	MM
SSSSSSSS	SSSSSSSS	00	00	XXX FFFFF	GG	MM	MM	MM
SSSSSSSS	SSSSSSSS	00	00	XXX FFFFF	GG	GGGG	MM	MM
SS	SS	00	00	FF	GG	GG	MM	MM
SSSSSSSS	SSSSSSSS	00000000		FF	GGGGGGGG	MM	MM	MM

0CTMZYUW YEDAZT 2576 2011645--MNSH--YEKH9V.

ZNY MNSH

ZKZK OP SDA OF

0 181600Z JUL 90

FM SSO REDSTONE//JAGPA-H-PS// by USAINSCOM FOI/PA

TO SSO HEAD//LAGPA-OR-I//

SSO HEAD//JAGPA-3-OP/DAMI-CIC-CC//

ZEM

Regraded UNCLASSIFIED on

12 JAN 2011

Auth para 4-102, DOD 5200-1R

2/3
902d
FCP
MIBW

~~CONFIDENTIAL~~

0000 SECTION 02 OF 02

UNITED STATES ARMY INFORMATION SYSTEMS COMMAND-MICOM (USAISC-MICOM) CAMPUS AREA/WIDE AREA NETWORK THROUGH THE USE OF MODEMS. THE USAISC-MICOM AREA/WIDE AREA NETWORK LINKS MOST OF THE MICOM PROJECT OFFICES, PROGRAM EXECUTIVE OFFICES, BUDGET OFFICES, FINANCE AND ACCOUNTING OFFICES, MICOM SECURITY AND CLEARANCE FILES, AS WELL AS OTHER RFA SUPPORT AGENCIES. THE NETWORK ALSO ACCESSES THE DEFENSE DATA NETWORK (DDN). THE USAISC-MICOM CAMPUS AREA/WIDE AREA NETWORK DOES NOT CONTAIN CLASSIFIED OR SPECIAL ACCESS INFORMATION. SUBSEQUENT TO THE INITIAL INTERVIEW OF THE SOURCE, HE WAS RECONTACTED BY MR. b6 OF THE CERT WHO INFORMED HIM THAT FURTHER FOLDERS BELONGING TO MICOM WERE FOUND IN OTHER COMPUTER SYSTEMS AT THE UNIVERSITY OF CHICAGO. APPROXIMATELY 15 MEGABITES OF INFORMATION HAVE BEEN FOUND THAT INDICATES 58 PASSWORDS ON THE USAISC-MICOM CAMPUS AREA/WIDE AREA NETWORK WERE COMPROMISED. ALL INFORMATION BELONGING TO MICOM THAT IS FOUND IN THE UNIVERSITY OF CHICAGO COMPUTER SYSTEMS WILL BE RETURNED TO MICOM FOR PRINTING AND ANALYSIS BY MICOM AOP SECURITY PERSONNEL. THIS ANALYSIS WILL DETERMINE THE EXTENT OF THE PENETRATION AS WELL AS IF ANY INFORMATION BECOMES CLASSIFIED THROUGH COMPILATION.

5. (U) ACTIONS TAKEN:

A. (U) A SCHEMATIC DIAGRAM TO THE USAISC-MICOM CAMPUS AREA/WIDE AREA NETWORK WAS OBTAINED FROM THE SOURCE AND MAY BE FORWARDED UNDER SEPARATE COVER IF NECESSARY.

6. (U) COMMENTS:

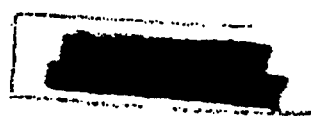
A. (U) THIS PENETRATION WILL CLOSE THE USAISC-MICOM CAMPUS AREA/WIDE AREA NETWORK DOWN FOR A MONTH IN ORDER TO REESTABLISH SECURITY IN THE NETWORK.

9. (U) RECOMMENDATIONS:

(1) (U) PSMD MONITOR THE ANALYSIS OF THE INFORMATION BY MICOM AOP SECURITY SPECIALISTS TO DETERMINE IF THERE IS ANY

Referred

~~CONFIDENTIAL~~



PRIORITY

REF ID: A3157

UNCLASSIFIED

Referred

7. (U) THIS MESSAGE IS MANUALLY RETYPED IN MESSAGE HANDLING CHANNELS PRIOR TO TRANSMISSION AND IS SUBJECT TO TRANSCRIPTION AND TYPOGRAPHICAL ERRORS. ALL IDENTIFYING DATA SHOULD BE INDEPENDENTLY VERIFIED BEFORE USE OR FILING FOR CROSS REFERENCE.

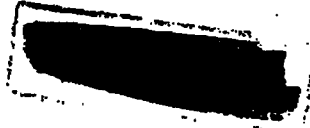
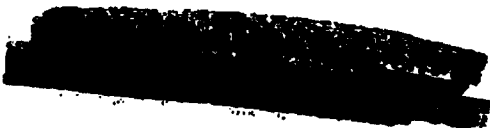
8. (U) POINT OF CONTACT IS [b6] OF [b6] AV

[b6] (S) (SECURE) [b6]
CLASSIFIED BY: MULTIPLE SOURCES; DECLASSIFY ON: OADR.
#2576

UNCL

Exhibit:

(I) Electronic Message, Subject: Penetration of MICOM Microcomputer



UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~CONFIDENTIAL~~

U.S. ARMY INTELLIGENCE

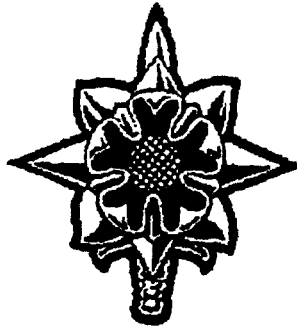


EXHIBIT COVER SHEET

SUBJECT: (u) REDSTONE ARSENAL, AL
SAEDA (AUTO)
13 July 1990

DACCO CCN: (U)

SCO CONUS CCN: (U)

PREPARING UNIT: (U) Redstone MI Det, 902d MI Group

REPORT DATED: (U) 18 July 1990

DESCRIPTION: (U) Confidential Electronic Message
From Commander MICOM
Dated 171620Z JUL 90
Subj: Penetration of MICOM Minicomputer (U)

b2



EXHIBIT 1

Regraded UNCLASSIFIED on
12 JAN 2011
by USAINSCOM FOIPA
Auth para 4-102, DOD 5200-1R

~~CONFIDENTIAL~~

CLASSIFICATION

*Regraded UNCLASSIFIED
when requested from
classified in all use*

CONFIDENTIAL

② CI
Tech

ZCZCOPD5997PEA461 LGG LN 077 1982244 JRNL TAPE 077
PCTCZYUW RUCDGRA2611 1982236-CCCC--RUDHAAA.
ZNY CCCCC
ZKZK PP GHI DE
P 171602Z JUL 90
FM CDR MICOM REDSTONE ARSENAL//AMSMI-SI//
TO RUDHAAA/CDR INSCOM FT BELVOIR VA//IAOPS-CI-TO//
INFO RUKLDAR/CDR AMC ALEX VA//AMCMI-CS//
RUKGNBA/CDR USAISS FT BELVOIR VA//ASBI-SDS//
RUEAQWD/HQDA WASH DC//DAMI-CIC-AS/SAIS-AOS//
RUCDGDA/CDR MICOM REDSTONE ARSENAL AL//AMSMI-SI//
RUCDGDA/PEO AIR DEFENSE REDSTONE ARSENAL AL//SFAE-AD/SFAE-AD-PA//
BT
CONFIDENTIAL
SUBJECT: PENETRATION OF MICOM MINICOMPUTER (U)

Referred

BT
02311

CONFIDENTIAL

JUL 20 1990
BAH

CONFIDENTIAL
20

SECRET --- 3

JOINT MESSAGEFORM						SECURITY CLASSIFICATION				
						SECRET				
PAGE	DTG/RELEASE TIME			PRECEDENCE		CLASS	SPECAT	LMF	CIC	ORIG. MSG IDENT
	DATE-TIME	MONTH	YR	ACT	INFO					
01 of 04	201900Z	AUG	90	PP	PP	SSSS				2321900Z
MODE	MESSAGE HANDLING INSTRUCTIONS									
<p>FROM: SAIC RO 902D MIGP FT SHERIDAN IL//IAGPA-C-SH//</p> <p>TO: CDR902DMIGP FT GEORGE G MEADE MD//IAGPA-OP-I//</p> <p>INFO: CDR MID 902D MIGP FT SAM HOUSTON TX//IAGPA-C-SA//</p> <p>CDR MIBN(CI)(CE) 902D MIGP PSF SFRAN CA//IAGPA-C-OP//</p> <p>ZEN/CDR MIBN(CI)(S) 902D MIGP FT GEORGE G MEADE MD</p> <p>//IAGPA-B-OP//</p> <p>ZEN/CDR DSD 902D MIGP FT GEORGE G MEADE MD</p> <p>//IAGPA-B-DS//</p> <p>ZEN/CDR MIBN(CI)(T) 902D MIGP FT GEORGE G MEADE MD</p> <p>//IAGPA-A-OP//</p> <p>ZEN/DIR DACCO FT GEORGE G MEADE MD//DAMI-CIC-CCO//</p> <p>CDRINSCOM FT BELVOIR VA//IAOPS-CI-OI/IAOPS-CI-TO//</p>										
SECRET [REDACTED]										
SUBJECT: INVESTIGATIVE MEMORANDUM FOR RECORD (U)										
1. (U) [REDACTED] TITLE: REDSTONE ARSENAL, AL										
SAEDA (AUTO)										
13 JUL 90 [REDACTED] (U)										
2. (U) DATE OF REPORT: 17 AUGUST 1990										
3. (U) CCN: SCO b2										
Regraded UNCLASSIFIED on 12 JAN 2011 by USAINSCOM FOLPA Auth para 4-102, DOD 5200-1R										
DISTR:										
2										
OL PHONE SAIC, IAGPA-C-SH AV: 459-2275						SPECIAL INSTRUCTIONS CLASSIFIED BY: INSCOM PAM 380-6 DECLASSIFY ON: OADR				
RELEASE b6 SAIC, IAGPA-C-SH						SECRET SECURITY CLASSIFICATION SECRET DATE TIME GROUP				

6
5
4
3
2
1
0

~~SECRET~~ (4)

JOINT MESSAGEFORM						SECURITY CLASSIFICATION SECRET				
PAGE	DTG/RELEASE TIME			PRECEDENCE		CLASS	SPECAT	LMP	CIC	ORIG/MSG IDENT
	DATE-TIME	MONTH	YR	ACT	INFO					
02 of 04	201900Z	AUG	90	PP	PP	SSSS				2321900Z
BOOK	MESSAGE HANDLING INSTRUCTIONS									
<p>4. (U) FORM INVESTIGATIVE RESULTS:</p> <p>INFORMATION CONTAINED IN THIS REPORT WAS OBTAINED FROM ANOTHER FEDERAL AGENCY WHO RESERVES THE RIGHT TO RESTRICT ITS RELEASE, AND WILL NOT BE BE RELEASED OUTSIDE OF ARMY INTELLIGENCE CHANNELS WITHOUT THEIR APPROVAL.</p> <p>A. (U) ████ ON 15 AUGUST 1990, SPECIAL AGENT Referred SQUAD 5B, CHICAGO FIELD OFFICE (CFO), Referred CHICAGO, IL, MET WITH MEMBERS OF THE CHICAGO RESIDENT OFFICE (CRO), 902D MILITARY INTELLIGENCE (MI) GROUP, FORT SHERDIAN, IL, AND PROVIDED THE FOLLOWING INFORMATION:</p> <p>(U) B. TST ON 9 JULY 1990, b6 DEPARTMENT OF ASTRONOMY AND ASTROPHYSICS (A&A), UNIVERSITY OF CHICAGO (U OF C), CHICAGO, IL, DISCOVERED COMPUTER FILES ON THE U OF C'S COMPUTER SYSTEM BELONGING TO COLONEL b6 REDSTONE ARSENAL, HUNTSVILLE, AL. THESE FILES WERE PLACED ON b6 FILES WHILE b6 WAS ON A TWO WEEK VACATION. b6 VACATION WAS POSTED ON THE COMPUTER BULLETIN BOARD AND ANYONE COULD HAVE OBTAINED THIS INFORMATION ONCE THEY HAD SIGNED ON TO THE SYSTEM.</p> <p>(U) C. TST b6 FOUND APPROXIMATELY TEN MILLION BYTES OF ADDITIONAL INFORMATION IN HIS COMPUTER FILES WHICH HE DID NOT PLACE THERE. REALIZING THIS INFORMATION WAS NATIONAL DEFENSE INFORMATION,</p>										
DISTR:										
DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE						SPECIAL INSTRUCTIONS				
TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE						SECRET				
b6						SECURITY CLASSIFICATION SECRET		DAYS TIME GROUP		

b
5
4
3
2
1
0

SECRET

JOINT MESSAGEFORM						SECURITY CLASSIFICATION SECRET				
PAGE	DTG/RELEASE TIME			PRECEDENCE		CLASS	SPICAT	LMP	CIC	ORIG. MSG IDENT
	DATE TIME	MONTH	YR	ACT	MMO					
03 of 04	201900Z	AUG	90	PP	PP	SSSS				2321900Z
BOOK	MESSAGE HANDLING INSTRUCTIONS									
<p>b6 ERASED THE INFORMATION TO THE COMPUTER EMERGENCY RESPONSE TEAM (CERT) TO CARNEGIE-MELLON, PITTSBURGH, PA, AND THEN ERASED THE INFORMATION FROM HIS FILES AS PER STANDARD OPERATING PROCEDURE.</p> <p>D. ^(u) (S) THE U OF C TRACED AN ILLEGAL ACCESS ATTEMPT THROUGH A REQUESTED TELEPHONE TRACE BACK TO GTE TELENET, 303 E. WACKER DRIVE, CHICAGO, IL. b6 ADVISED THAT GTE TELENET IS A "HUB," AND IT WILL BE VIRTUALLY IMPOSSIBLE TO TRACE THE CALL BACK ANY FURTHER.</p> <p>E. ^(u) (S) U OF C'S ON CAMPUS COMPUTER SYSTEM IS CONNECTED TO A REGIONAL SYSTEM WHICH IS CONNECTED TO THE NATIONAL SCIENCE FOUNDATION (NSF) SYSTEM. THROUGH THE NSF A "CRACKER" (NEW TERM FOR HACKER) WOULD HAVE ACCESS TO OTHER SYSTEMS THROUGHOUT THE U.S. AND OVERSEAS. ADDITIONALLY, IF AN UNAUTHORIZED USER ENTERED THE U OF C COMPUTER THROUGH A TELEPHONE NETWORK, IT IS VERY DIFFICULT TO TRACE OR TRACK THE USER. THIS APPEARS TO BE THE CASE IN THIS INCIDENT IN THAT THE ENTRY WAS THROUGH GTE TELENET.</p> <p>F. ^(u) (S) IT IS BELIEVED THIS CRACKER MAY BE ON A "LEARNING CURVE," MEANING ONE COULD SEE THE PROGRESS AND LEVEL OF COMPETENCE THAT WAS GAINED THE LONGER THE CRACKER WAS ON THE SYSTEM. DUE TO THE GRAMMER AND PUNCTUATION USED, IT IS BELIEVED THE CRACKER MAY BE EUROPEAN</p>										
DISTR:										
DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE						SPECIAL INSTRUCTIONS				
TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE						SECRET				
b6						23		SECRET		DATE TIME GROUP

6
5
4
3
2
1
0

SECRET

JOINT MESSAGEFORM						SECURITY CLASSIFICATION SECRET	
-------------------	--	--	--	--	--	-----------------------------------	--

PAGE	DTG/RELEASE TIME			PRECEDENCE		CLASS	SPECAT	IMP	CIC	ORIG/MSG IDENT
	DATE-TIME	MONTH	YR	ACT	INFO					
04 of 04	201900Z	AUG	90	PP	PP	SSSS				2321900Z

BOOK MESSAGE HANDLING INSTRUCTIONS

AND WORKING ALONE. THE CRACKER SIGNED ON AT ABOUT 0300 to 0400 HOURS AND REMAINED ON FOR TWELVE TO SIXTEEN HOURS EACH DAY, WITH AN OCCASIONAL BREAK BETWEEN 0800 AND 1000 HOURS. THIS PATTERN LASTED FOR ABOUT TWO WEEKS, DATES NOT PROVIDED, WITH ONLY ONE DAY OFF. G. [8] ON 28 JULY 1990, [b6] NOTICED A CRACKER ON THE U OF C COMPUTER SYSTEM WHEN HE THOUGHT A FRIEND OF HIS, [b6] NOT FURTHER IDENTIFIED, WAS ON THE SYSTEM. [b6] ASKED [b6] WHEN HE HAD RETURNED FROM HIS TRIP. THE CRACKER RESPONDED BY ASKING ABOUT GAINING ACCESS TO ANOTHER COMPUTER SYSTEM. THE CRACKER THEN IDENTIFIED HIMSELF AS A HACKER AND SIGNED OFF.

Referred

6
5
4
3
2
1
0

DECLASS OADR

DISTR.

DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE		SPECIAL INSTRUCTIONS	

RELEASE	TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE		SECURITY CLASSIFICATION	DATE TIME GROUP
	[b6]		SECRET	

SECRET
U.S. ARMY INTELLIGENCE

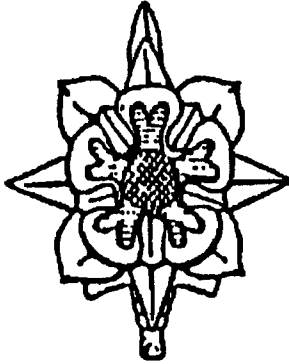



EXHIBIT COVER SHEET

SUBJECT:

(u)  REDSTONE ARSENAL, AL
SAEDA (AUTO)
13 July 90

DACCO CCN:

(U) SCO  b2

PREPARING UNIT:

(U) Chicago Resident Office
902d Military Intelligence Group

REPORT DATED:

(U) 17 August 1990

DESCRIPTION:

(u) Sanitized copy of  report (S)



EXHIBIT **SECRET**

II
*Regraded UNCLASSIFIED
when separated from
classified enclosure*

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

Information has been withheld in its entirety in accordance with the following exemption(s):

It is not reasonable to segregate meaningful portions of the record for release.

Information pertains solely to another individual with no reference to you and/or the subject of your request.

Information originated with another government agency. It has been referred to them for review and direct response to you.

Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S) NO DUPLICATION FEE FOR THIS PAGE.

Page(s) 26-27

~~CONFIDENTIAL~~

(S)

JOINT MESSAGEFORM						SECURITY CLASSIFICATION			
						CONFIDENTIAL			

PAGE	DTG/RELEASE TIME			PRECEDENCE		CLASS	SPECAT	LMF	CIC	ORIG/MSG IDENT
	DATE-TIME	MONTH	YR	ACT	INFO					
01 of 03	212100Z	AUG	90	PP	PP	CCCC-				2332100Z

BOOK	MESSAGE HANDLING INSTRUCTIONS
------	-------------------------------

FROM: SAIC RO 902D MIGP FT SHERIDAN IL//IAGPA-C-SH//
 TO: CDR902DMIGP FT GEORGE G MEADE MD//IAGPA-OP-I//
 INFO: CDR MID 902D MIGP FT SAM HOUSTON TX//IAGPA-C-SA//
 CDR MIBN(CI){CE} 902D MIGP PSF SFRAN CA//IAGPA-C-OP//
 ZEN/CDR MIBN(CI){S} 902D MIGP FT GEORGE G MEADE MD
 //IAGPA-B-OP//
 CDR MID 902D MI GP FT MEADE MD//IAGPA-C-FM//
 ZEN/CDR DSD 902D MIGP FT GEORGE G MEADE MD
 //IAGPA-B-DS//
 ZEN/CDR MIBN(CI){T} 902D MIGP FT GEORGE G MEADE MD
 //IAGPA-A-OP//
 ZEN/DIR DACCO FT GEORGE G MEADE MD//DAMI-CIC-CCO//
 CDRINSCOM FT BELVOIR VA//IAOPS-CI-OI/IAOPS-CI-TO//

~~CONFIDENTIAL~~ [REDACTED]

SUBJECT: INVESTIGATIVE MEMORANDUM FOR RECORD (U)

1. (U) [REDACTED] TITLE: REDSTONE ARSENAL, AL

SAEDA (AUTO)

13 JUL 90 [REDACTED] (U)

2. (U) DATE OF REPORT: 21 AUGUST 1990

Regraded UNCLASSIFIED on

DISTR: 12 JAN 2011
 by USAINSCOM FOI/PA
 Auth para 4-102, DOD 5200-1R

DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE	SPECIAL INSTRUCTIONS
b6 SAIC	CLASSIFIED BY: INSCOM PAM 380-b
IAGPA-C-SH	DECLASSIFY ON: OADR
AV: b6	

TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE	SECURITY CLASSIFICATION	DATE TIME GROUP
b6 SAIC, IAGPA-C-SH	CONFIDENTIAL	
SIGNATURE	3	
b6	CONFIDENTIAL	

6
5
4
3
2
1
0

~~CONFIDENTIAL~~

5

JOINT MESSAGEFORM				SECURITY CLASSIFICATION CONFIDENTIAL						
PAGE 02 of 03	DTG/RELEASER TIME			PRECEDENCE		CLASS	RECAT	LMT	CIC	ORIG MSG IDEN1
	DATE TIME	MONTH	YR	ACT	INFO					
	212100Z	AUG	90	PP	PP	CCCC				2332100Z
BOOK	MESSAGE HANDLING INSTRUCTIONS									

3. {U} ~~FROM:~~ SCO b2

4. {U} INVESTIGATIVE RESULTS:

A. (u) ~~████~~ ON 21 AUGUST 1990, b6 ADP SECURITY SPECIALIST, INSTALLATION SECURITY OFFICE, HEADQUARTERS, AMCCOM, ROCK ISLAND ARSENAL, ROCK ISLAND, ILLINOIS, WAS TELEPHONICALLY CONTACTED BY THE CHICAGO RESIDENT OFFICE {CRO}, 902D MILITARY INTELLIGENCE GROUP, FT. SHERIDAN, IL, AND PROVIDED THE FOLLOWING INFORMATION:

B. (u) ~~██~~ AFTER LEARNING OF THE FILES BEING DISCOVERED ON THE UNIVERSITY OF CHICAGO'S COMPUTER SYSTEM, b6 CHIEF OF SECURITY AND INTELLIGENCE, HQ, AMCCOM, ROCK ISLAND ARSENAL, CHECKED ALL THE COMPUTER LOGS FOR THE MONTH OF JULY 1990. AFTER CAREFUL EXAMINATION BY b6 AND THE INFORMATION SYSTEMS COMMAND, IT WAS DETERMINED THAT NONE OF THE FILES AT ROCK ISLAND ARENSAL HAD BEEN COMPROMISED. IT WAS LEARNED HOWEVER, FILES FROM ONE OF THE SUBORDINATE UNITS AT DOVER, OFFICE SYMBOL AMSMC-MGM, WERE STOLEN. HEADQUARTERS AMCCOM IS THE HEADQUARTERS FOR THE UNIT AT DOVER, WHICH MAY INDICATE WHY IT WAS BELIEVED THE FILES CAME FROM ROCK ISLAND ARSENAL. b6 DID NOT HAVE ANY INFORMATION ON THE TYPE OF INFORMATION WHICH WAS STOLEN FROM DOVER.

6
5
4
3
2
1
0

Regraded UNCLASSIFIED on

DISTR: 12 JAN 2011
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE		SPECIAL INSTRUCTIONS	
TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE		CONFIDENTIAL	
RELEASER SI	b6	SECURITY CLASSIFICATION CONFIDENTIAL	DATE TIME GROUP

~~CONFIDENTIAL~~

JOINT MESSAGEFORM							SECURITY CLASSIFICATION CONFIDENTIAL			
PAGE	DTG/RELEASER TIME			PRECEDENCE		CLASS	SPECAT	LMI	CIC	ORIG-MSG IDENT
	DATE-TIME	MONTH	YR	ACT	INFO					
03 of 03	212100Z	AUG	90	PP	PP	EEEE				2332100Z
BOOK	MESSAGE HANDLING INSTRUCTIONS									
<p>C. (U) EE b6 EXPLAINED THERE IS A PASSWORD PROTECTION SYSTEM IN PLACE AT ROTOR ISLAND ARSENAL. THIS SYSTEM LIMITS THE AMOUNT OF LOGONS ALLOWED, MAKES USE OF A SIX CHARACTER PASSWORD, AND HAS NEUTRALIZED ANY "BACKDOORS" WHICH MAY HAVE BEEN IN PLACE.</p> <p>5. (U) REPORT SUBMITTED BY: S/A b6 CR0, 902D MI GROUP, AV: b6</p> <p>DECLASS OADR</p>										
<p>Regraded UNCLASSIFIED on 12 JAN 2011 by USAINSCOM FOI/PA Auth para 4-102, DOD 5200-1R</p>										
DISTR:										
DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE							SPECIAL INSTRUCTIONS			
RELEASER	TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE						CONFIDENTIAL			
	SIGNATURE b6									

6
5
4
3
2
1
0

CONFIDENTIAL

5

JOINT MESSAGEFORM						SECURITY CLASSIFICATION CONFIDENTIAL				
PAGE	DTG/RELEASER TIME			PRECEDENCE		CLASS	SPECAT	LMF	CIC	ORIG MSG IDENT
	DATE TIME	MONTH	YR	ACT	INFO					
01 of 02	231500Z	AUG	90	PP	PP	CCCC				2351500Z

BOOK _____ MESSAGE HANDLING INSTRUCTIONS _____

FROM: SAIC RO 902D MIGP FT SHERIDAN IL//IAGPA-C-SH//
 TO: CDR902DMIGP FT GEORGE G MEADE MD//IAGPA-OP-I//
 INFO: CDR MID 902D MIGP FT SAM HOUSTON TX//IAGPA-C-SA//
 CDR MIBN(CI){CE} 902D MIGP PSF SFRAN CA//IAGPA-C-OP//
 ZEN/CDR MIBN(CI){S} 902D MIGP FT GEORGE G MEADE MD
 //IAGPA-B-OP//
 CDR MID 902D MI GP FT MEADE MD//IAGPA-C-FM//
 ZEN/CDR DSD 902D MIGP FT GEORGE G MEADE MD
 //IAGPA-B-DS//
 ZEN/CDR MIBN(CI){T} 902D MIGP FT GEORGE G MEADE MD
 //IAGPA-A-OP//
 ZEN/DIR DACCO FT GEORGE G MEADE MD//DAMI-CIC-CCO//
 CDRINSCOM FT BELVOIR VA//IAOPS-CI-OI/IAOPS-CI-TO//

~~CONFIDENTIAL~~ [REDACTED]

SUBJECT: INVESTIGATIVE MEMORANDUM FOR RECORD (U)

A. EIMFR, IAGPA-C-SH, DTG 212100Z AUG 90, SAB

1. (U) [REDACTED] TITLE: REDSTONE ARSENAL, AL

SAEDA (AUTO)

Regraded UNCLASSIFIED on

13 JUL 90 [REDACTED] (U)

12 JAN 2011

by USAINSCOM FOI/PA

Auth para 4-102, DOD 5200-1R

6
5
4
3
2
1
0

DISTR: _____

DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE b6 SAIC IAGPA-C-SH AV: b2	SPECIAL INSTRUCTIONS CLASSIFIED BY: INSCOM PAM 380-B DECLASSIFY ON: OADR
--	--

RELEASER b6	DRIVER NAME, TITLE, OFFICE SYMBOL AND PHONE SAIC, IAGPA-C-SH	SECURITY CLASSIFICATION CONFIDENTIAL	DATE TIME GROUP
----------------	---	--	-----------------

~~CONFIDENTIAL~~

6

JOINT MESSAGEFORM						SECURITY CLASSIFICATION				
						CONFIDENTIAL				
PAGE	DTG/RELEASER TIME			PRECEDENCE		CLASS	SPECAT	LMF	CIC	ORIG/MSO IDENT
	DATE TIME	MONTH	YR	ACT	INFO					
02 of 02	231500Z	AUG	90	PP	PP	CCCC				2351500Z
MESSAGE HANDLING INSTRUCTIONS										
<p>2. {U} FROM OF REPORT: 23 AUGUST 1990</p> <p>3. {U} CCRD: SCO b2</p> <p>4. {U} INVESTIGATIVE RESULTS:</p> <p>A. {U} ON 23 AUGUST 1990, b6 ADP SECURITY SPECIALIST, INSTALLATION SECURITY OFFICE, HEADQUARTERS, AMCCOM, ROCK ISLAND ARSENAL, ROCK ISLAND, ILLINOIS, WAS TELEPHONICALLY CONTACTED BY THE CHICAGO RESIDENT OFFICE (CRO), 902D MILITARY INTELLIGENCE GROUP, FT. SHERIDAN, IL, AND PROVIDED THE FOLLOWING INFORMATION:</p> <p>B (U) (S) AFTER LEARNING OF THE FILES BEING DISCOVERED ON THE UNIVERSITY OF CHICAGO'S COMPUTER SYSTEM, A CHECK OF ALL COMPUTER LOGS AT ROCK ISLAND ARSENAL, ROCK ISLAND, ILLINOIS, SHOWED THAT FILES FROM ONE OF THEIR SUBORDINATE UNITS, PICATINNY ARSENAL, DOVER, NEW JERSEY, OFFICE SYMBOL AMSMC-MGM, HAD BEEN STOLEN. THE POINT OF CONTACT AT PICATENNY ARESENAL IS b6</p> <p>5. {U} REPORT SUBMITTED BY: S/A b6 CRO, 902D MI GROUP, AV: b6</p>										
<p>DECLASS OADR</p> <p style="text-align: right;">Regraded UNCLASSIFIED on 12 JAN 2011 by USAINSCOM FOI/PA Auth para 4-102, DOD 5200-1R</p>										
DISTR:										
DRAFTER TYPED NAME, TITLE, OFFICE SYMBOL, PHONE						SPECIAL INSTRUCTIONS				
						CONFIDENTIAL				
TYPED NAME, TITLE, OFFICE SYMBOL AND PHONE						SECURITY CLASSIFICATION		DATE TIME GROUP		
b6						CONFIDENTIAL				

6
5
4
3
2
1
0

01 05 221500Z AUG 90 PP PP ~~CCCC~~

2341430Z

(C)

SAIC NYRO 902D MI GP FT HAMILTON NY//IAGPA-C-NY//
 CDR 902D MI GP FT MEADE MD//IAGPA-OP-I//
 INFO CDR FMOMID 902D MI GP FT MONMOUTH NJ//IAGPA-C-MO//
 CDR MI BN (CI) (CE) PSF SFRAN CA//IAGPA-C-OP//
 DIR DA CCO FT MEADE MD//DAMI-CIC-CCO//
 CDR INSCOM FT BELVOIR VA//IAOPS-CI-OI//
 CDR INSCOM FT BELVOIR VA//IAOPS-CI-TO//
 ADP DET FT MEADE MD//IAGPA-A-DP//

~~CONFIDENTIAL~~ [REDACTED] NO NIGHT ACTION REQUIRED-DELIVER
 DURING FIRST DUTY HOURS

SUBJECT: INVESTIGATIVE MEMORANDUM FOR RECORD (U)

A. (U) [REDACTED] CONF MSG, CDR, 902D MI GP, IAGPA-OP-I, 082022Z AUG 90, SUB:
 REDSTONE ARSENAL, AL; SAEDA (AUTO); 13 JUL 90

1. (U) [REDACTED] TITLE: REDSTONE ARSENAL, AL
 SAEDA (AUTO)
 13 JUL 90

Regraded UNCLASSIFIED on
 12 JAN 2011
 by USAINSCOM FOI/PA
 Auth para 4-102, DOD 5200-1R

2. (U) DATE OF REPORT: 21 AUG 90

3. (U) CASE CONTROL NUMBER: 902D CCN: b2

4. (U) INVESTIGATIVE RESULTS

-----SOURCE HAD NO OBJECTION TO HER IDENTITY-----

b6

b6

SA, IAGPA-C-NY,

CLASSIFIED BY: AR 381-12

902D MI GROUP, AV b6

DECLASSIFY ON: OADR

b6

SAIC, IAGPA-C-NY 630-4388

b6

~~CONFIDENTIAL~~ [REDACTED]

5

~~CONFIDENTIAL~~

02 05 221500Z AUG 90 PP PP CCCC

2341430Z

2

-----BEING RELEASED IN CONJUNCTION WITH THIS INVESTIGATION-----

A. (u) ~~(S)~~ ON 21 AUG 90, THE REPORTING AGENT MET WITH b6
b6 AUTOMATED DATA PROCESSING SYSTEM SECURITY OFFICER
{ADPSSO}, DIRECTORATE OF INFORMATION MANAGEMENT {DOIM}, UNITED
STATES MILITARY ACADEMY {USMA}, HIGHLAND FALLS, NY. b6
PROVIDED THE FOLLOWING DOCUMENTS AND INFORMATION CONCERNING THE
PENETRATION OF USMA'S STAFF COMPUTER SYSTEM {SCS} BETWEEN 25 JUN 90
AND 13 JUL 90, AS WELL AS THE FOLLOWING SUGGESTIONS ON DEVELOPING AN
AUDIT TRAIL:

B. (u) ~~(S)~~ b6 PROVIDED A COPY OF THE LOGON FILES FOR THIS TIME
PERIOD.

C. (u) (C) BASED ON SOURCE'S ANALYSIS OF THE APPROXIMATELY 7500 LOGON
ATTEMPTS LISTED IN THE ABOVE FILES BETWEEN 22 JUN 90 AND 21 JUL 90,
PENETRATION OF USMA'S SCS WAS NOT APPARENT. THESE LOGON FILES
LISTED ONLY UNSUCCESSFUL LOGON ATTEMPTS, AS USMA'S UNISYS 5000/80
COMPUTER {A UNIX-BASED OPERATING SYSTEM} WAS NOT PROGRAMMED TO
RETAIN SUCCESSFUL LOGONS. PER USMA DOIM'S PROCEDURES, THE SCS
RETAINED ONLY THE PREVIOUS TEN DAYS OF THE SYSTEM FILES NEEDED TO
TRACK THE TRANSFER OF FILES FROM THE SCS TO THE UC HOST.

b6

b6

SA, 902D MI GROUP

b6

Regraded UNCLASSIFIED on

12 JAN 2010

by USAINSCOM FOI/PA

Auth para 4-102, DOD 5200-1R

~~CONFIDENTIAL~~

CONFIDENTIAL [REDACTED] 2

03 05 221500Z AUG 90 PP PP CCCC

2341430Z

D. (U) (C) ANALYSIS REVEALED NONE OF THE FOLLOWING PASSWORDS LISTED IN REFERENCE A., PARA 3.B: "ANONYMOUS", "GUEST", "LISTEN", "SETUP", "FILE", "TRANSFER PROTOCOL", AND "ECT". "FTP" APPEARED FREQUENTLY IN THE LOGON FILES, BUT WAS NOT USED AS A PASSWORD. SOURCE EXPLAINED THAT "FTP" IS A PROCESS THAT FACILITATES FILE TRANSFERS AND IS A STANDARD ENTRY ON MANY LOGON FILES.

E. (U) (C) ANALYSIS REVEALED THE FOLLOWING COMMAND LISTED IN REFERENCE A., PARA 3.C: "ROOT", BUT NONE OF THE OTHERS LISTED: "LIST", "COPY", AND "PASSWD".

F. (U) (C) ANALYSIS REVEALED NO INDICATIONS THAT THE INTRUDER USED A LEGITIMATE ACCOUNT HOLDER'S LOGON IDENTIFICATION, OR ATTEMPTED TO BECOME A "SUPER USER."

G. (C) ANALYSIS OF ALL DIRECTORIES REVEALED NONE OF THE FOLLOWING SIGNS OF ENTRY LISTED IN REFERENCE A., PARA 3.C: "ROOT", "USR", "USR2", "MAIL", "BIN", AND "DOT{.}."

H. (U) (C) IN ORDER TO DEVELOP AN AUDIT TRAIL, SOURCE WOULD NEED THE FILE NAMES AND CONTENTS TAKEN FROM THE SCS; ANY KNOWN PAST SECURITY DEFICIENCIES IN THE UNISYS 5000/80 OPERATING SYSTEM; AND THE INTRUDER'S FULL OR PARTIAL USER IDENTIFICATION AND/OR NETWORK ADDRESS IN ORDER TO MONITOR ANY FUTURE SCS PENETRATION ATTEMPTS.

b6

b6

SA, 902D MI GROUP

b6

Regraded UNCLASSIFIED on
12 JAN 2011
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

CONFIDENTIAL [REDACTED]

04 05 221500Z AUG 90 PP PP ~~CCCC~~

2341430Z

5. (U) AGENT NOTES:

A. (U) REPORTING AGENT WAS ASSISTED BY b6 .TC,
DIRECTOR, COMPUTER SYSTEMS DIVISION, DOIM, USMA; b6
GS12, SECURITY MANAGER, COMPUTER SYSTEMS DIVISION, DOIM, USMA; AND
b6 GS12, COMPUTER SYSTEMS MANAGER, COMPUTER SYSTEMS
DIVISION, DOIM, USMA.

B. (U) b6 APPRECIATED BEING ALERTED TO THIS SCS PENETRATION AND
WILL MONITOR THE SCS DAILY FOR THE ABOVE MENTIONED INDICATORS AFTER
PROGRAMMING THE UNISYS 5000/80 COMPUTER TO RETAIN SUCCESSFUL LOGON
ENTRIES, ALONG WITH THE UNSUCCESSFUL ATTEMPTS. b6 WILL CONTACT
NYRO IF HE SUSPECTS OR DETECTS ANY FUTURE PENETRATIONS.

6. (U) EXHIBITS:

A. (U) FOUR LOGON FILES FROM 22 JUN 90 TO 23 JUL 90 LABELED ON THE
TOP "ACADEMY MANAGEMENT SYSTEM COMPUTER OPERATIONS BRANCH"
APPROXIMATELY TWO INCHES THICK.

~~B. (U) NONDISCLOSURE WARNING STATEMENT, EXECUTED BY, b6
b6 DATED 28 AUG 90 b6~~

~~C. (U) DISCLOSURE WARNING STATEMENT, EXECUTED BY, b6
b6 DATED 28 AUG 90 b6~~

~~D. (U) DISCLOSURE WARNING STATEMENT, EXECUTED BY, b6~~

b6

Regraded UNCLASSIFIED on
12 JAN 2011
by USAINSCOM FOL/PA
Auth para 4-102, DOD 5200-1R

b6 SA, 982D MI GROUP
b6

UNCLASSIFIED



LIMDIS

05 05 221500Z AUG 90 PP PP

~~UNCL~~

2341430Z

DATED 20 AUG 90.

(U)

~~EC DISCLOSURE WARNING STATEMENT, EXECUTED BY~~

b6

b6

~~DATED 20 AUG 90~~

b6

7. (U) REPORT SUBMITTED BY

b6

SA, 902D MI GP, DSN (AV)

b6

DECL OADR

Regraded UNCLASSIFIED on

12 JAN 2011

by USAINSCOM FOI/PA

Auth para 4-102, DOD 5200-1R

b6

b6

SA, 902D MI GROUP

b6

UNCLASSIFIED



~~LIMDIS~~

[REDACTED]

US ARMY
INTELLIGENCE AND SECURITY
COMMAND

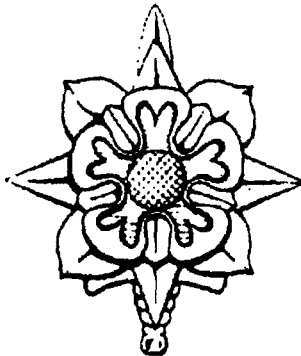


EXHIBIT
COVER SHEET

Regraded UNCLASSIFIED on
12 JAN 2011
by USAINSCOM FOI/PA
Auth para 4-102, DOD 5200-1R

SUBJECT:

[REDACTED] Redstone Arsenal, AL
SAEDA (AUTO)
13 July 1990

FILE NUMBER:

[REDACTED] b2

PREPARING UNIT:

[REDACTED] New York Resident Office
902d MI GP

AGENT REPORT DATED:

[REDACTED] 21 August 1990

DESCRIPTION:

[REDACTED] Staff Computer System Logon Files (2" thick)
Directorate of Information Management
United States Military Academy
22 Jun 90 - 23 Jul 90

[REDACTED]

For **OFFICIAL USE
ONLY**

[REDACTED]

EXHIBIT III

~~FOR OFFICIAL USE ONLY~~

**ACADEMY MANAGEMENT SYSTEM
COMPUTER OPERATIONS BRANCH**

USERID -

ACCOUNT NAME - *UAD*

RUNID - *RSPOOM*

FILENAME -

DATE - *AUG 21, 1990*

TIME - *11:56:17*

PRINTER - *LX1*

FORM - *F600*

ROUTE TO - *ROOT*

~~FOR OFFICIAL USE ONLY~~

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

Information has been withheld in its entirety in accordance with the following exemption(s):

b2

It is not reasonable to segregate meaningful portions of the record for release.

Information pertains solely to another individual with no reference to you and/or the subject of your request.

Information originated with another government agency. It has been referred to them for review and direct response to you.

Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 42-45

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

- Information has been withheld in its entirety in accordance with the following exemption(s):

b2

It is not reasonable to segregate meaningful portions of the record for release.

- Information pertains solely to another individual with no reference to you and/or the subject of your request.
- Information originated with another government agency. It has been referred to them for review and direct response to you.
- Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 46-55

FOR OFFICIAL USE ONLY

**ACADEMY MANAGEMENT SYSTEM
COMPUTER OPERATIONS BRANCH**

USERID - *RSPool*

ACCOUNT NAME - *UAD*

RUNID - *RSPool*

FILENAME -

b2

DATE - *AUG 21, 1990*

TIME - *11:56:24*

PRINTER - *LX1*

FORM - *F600*

ROUTE TO - *ROOT*

FOR OFFICIAL USE ONLY

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

Information has been withheld in its entirety in accordance with the following exemption(s):

b 2

It is not reasonable to segregate meaningful portions of the record for release.

Information pertains solely to another individual with no reference to you and/or the subject of your request.

Information originated with another government agency. It has been referred to them for review and direct response to you.

Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 57-59

214 Jun 90

FOR OFFICIAL USE ONLY

**ACADEMY MANAGEMENT SYSTEM
COMPUTER OPERATIONS BRANCH**

USERID -

ACCOUNT NAME - *UAD*

RUNID - *RSPOOM*

FILENAME -

DATE - *AUG 21, 1990*

TIME - *11:56:28*

PRINTER - *LX1*

FORM - *F600*

ROUTE TO - *ROOT*

FOR OFFICIAL USE ONLY

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

Information has been withheld in its entirety in accordance with the following exemption(s):

b2

It is not reasonable to segregate meaningful portions of the record for release.

Information pertains solely to another individual with no reference to you and/or the subject of your request.

Information originated with another government agency. It has been referred to them for review and direct response to you.

Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 61-62

FOR OFFICIAL USE ONLY

**ACADEMY MANAGEMENT SYSTEM
COMPUTER OPERATIONS BRANCH**

USERID -

ACCOUNT NAME - *UAD*

RUNID -

FILENAME -

DATE - *AUG 21, 1990*

TIME - *11:56:31*

PRINTER - *LX1*

FORM - *F600*

ROUTE TO - *ROOT*

FOR OFFICIAL USE ONLY

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

Information has been withheld in its entirety in accordance with the following exemption(s):

b2

It is not reasonable to segregate meaningful portions of the record for release.

Information pertains solely to another individual with no reference to you and/or the subject of your request.

Information originated with another government agency. It has been referred to them for review and direct response to you.

Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 64-80

FOR OFFICIAL USE ONLY

**ACADEMY MANAGEMENT SYSTEM
COMPUTER OPERATIONS BRANCH**

USERID - b2

ACCOUNT NAME - *UAO*

RUNID - *RSPOOM*

FILENAME - b2

DATE - *AUG 21, 1990*

TIME - *11:56:37*

PRINTER - *LX1*

FORM - *F600*

ROUTE TO - *ROOT*

FOR OFFICIAL USE ONLY

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

Information has been withheld in its entirety in accordance with the following exemption(s):

b2

It is not reasonable to segregate meaningful portions of the record for release.

Information pertains solely to another individual with no reference to you and/or the subject of your request.

Information originated with another government agency. It has been referred to them for review and direct response to you.

Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 82, 89

FOR OFFICIAL USE ONLY

ACADEMY MANAGEMENT SYSTEM

COMPUTER OPERATIONS BRANCH

USERID - b2

ACCOUNT NAME - *UAD*

RUNID - *RSPOOM*

FILENAME - b2

DATE - *AUG 21, 1990*

TIME - *11:56:42*

PRINTER - *LX1*

FORM - *F600*

ROUTE TO - *ROOT*

~~FOR OFFICIAL USE ONLY~~

Freedom of Information Act/Privacy Act
Deleted Page(s) Information Sheet

Indicated below are one or more statements which provide a brief rationale for the deletion of this page.

- Information has been withheld in its entirety in accordance with the following exemption(s):

b2

It is not reasonable to segregate meaningful portions of the record for release.

- Information pertains solely to another individual with no reference to you and/or the subject of your request.
- Information originated with another government agency. It has been referred to them for review and direct response to you.
- Information originated with one or more government agencies. We are coordinating to determine the releasability of the information under their purview. Upon completion of our coordination, we will advise you of their decision.

DELETED PAGE(S)
NO DUPLICATION FEE
FOR THIS PAGE.

Page(s) 91-124

**NATIONAL
SECURITY
ARCHIVE**

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu