264A-KX-61179

The USSS investigation has revealed that numerous Government and private sector computer systems have been subject to attack over the past years. Rather than the "hackers" keeping stolen computer files on their own personal computers, the "hacker" group uses the computer systems they invade to store programs and files they steal. Several systems have been used in this manner before. It has been determined that the LEGION OF DOOM organization also uses a Turkish government computer system called ARMA in Ankara, Turkey, to store computer files, specifically, a copy of the November 1989 Phrack Journal.

The LEGION OF DOOM involves a tightly knit core group of about 15 individuals who are from 21 to 22 years of age and whose primary reason for affiliation is to gather information for and then publish a "hackers" magazine called "PHRACK 2600". The LEGION OF DOOM is loosely affiliated with other "hackers" from both the United States and overseas, contacts noted as being primarily in England, Germany and Australia.

The Knoxville Offi	ce has a listing of the members of
the LEGION OF DOOM which lis	ts 60 known members of this
the <u>LEGION OF DOOM which lis</u> organization. Also listed i	n this organization were
Laka and	aka
dba	has five telephone lines,
	ockport, Illinois, which is used in
	the E911 file involved in the
February 1990. USSS case. I	t should also be noted that this same
<u>individual</u> , ak	is the same individual
identified as one of the "ha	ckers" in the Knoxville COLONIAL
FREIGHT case, still using th	e same handle of
the same of the sa	The state of the s

b6 b7C

Memorandum



6/30/92 SAC, KNOXVILLE (264A-KX-61179) (P)

From: SA b6 b7C

Subject:

UNSUB(S);

COLONIAL FREIGHT SYSTEMS, KNOXVILLE, TENNESSEE -

VICTIM;

JANUARY 1990 - DECEMBER 1991;

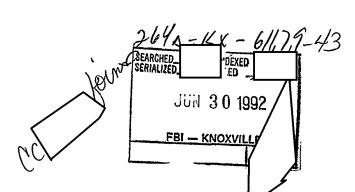
COMPUTER FRAUD AND ABUSE -

IMPAIRMENT: KNOXVILLE 00:

The purpose of this memo is to give background information on captioned case and to give an update into this ongoing investigation. On 1/13/92, captioned investigation was opened after the Knoxville Office received a telephone call from COLONIAL FREIGHT TRUCKING COMPANY (victim company) that someone had entered their computer system and had access to their telephone lines without authorization. The Knoxville FBI Office checked into the matter and immediately realized that Unknown Subject(s) (UNSUB(s)) intentionally modified the COLONIAL FREIGHT SYSTEMS network by gaining "super-user" access to the operating system, placing copyright software on the computer, unlawfully using the telephone circuits, and otherwise effecting the normal operations of the computer.

COLONIAL's computers are located in five states: Texas, North Carolina, New Jersey, Georgia, Ohio, and Tennessee. Therefore, COLONIAL's network qualifies as a "Federal Interstate Computer", under Title 18, United States Code, Section 1030(e)(2)(B) since it is one of two or more computers used in committing the offense, not all of which are located in the same state.

The intruder(s) exceeded authorized access since he/she accessed COLONIAL's computer without authorization to obtain an alter information that the accessor is not entitled to obtain or alter (Title 18, United States Code, Section 1030(e)(6).



b6 b7C