(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 04/03/1998

To: Criminal Investigative **Attn:** NIPC/CIU
Chicago **Attn:** 288 Supervisor
San Francisco **Attn:** 288 Supervisor

From: [redacted]
Squad 4
Contact: SA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted] :tjm

Case ID #: 288-HQ-1242560 -211 (Pending)
288-KC-0 -68

Title: SOLAR SUNRISE;
CITA/NIPC

Synopsis: Information is being forwarded to receiving offices regarding captioned matter.

Details: On 4/3/98, SA [redacted] Kansas City Division (KCD), telephonically contacted [redacted] MOREnet Network and Security Services (MNSS), 1805 E. Walnut Street, Columbia, Missouri 65201, telephone number [redacted] fax number (573) 884-6673, regarding a fax received from [redacted] on 3/6/98. The fax described an intrusion into a computer at the Central Methodist College, cmc2.cmc.edu, which is a downstream connection from MNSS. b6 b7C

[redacted] advised that someone named [redacted] sent an E-mail message to MNSS with a password file attached. The password file was later verified as an old password file from cmc2.cmc.edu. [redacted] claimed he received the password file from an "east coast" hacker who claimed to be involved with the compromises of the Pentagon servers via the Internet. The hacker sent the password file to [redacted] as proof of his hacking ability. b6 b7C

[redacted] later learned that [redacted] was a [redacted] for the publication AntiOnline, web address: www.antionline.com. [redacted] advised [redacted] chatted with [redacted] using Internet Relay Chat (IRC), and that [redacted] was the one who sent [redacted] the password file. b6 b7C

11881 b6 b7C

b6
b7C

A copy of the aforementioned fax is attached.

This information is being forwarded to receiving offices for whatever action deemed appropriate.

♦♦

MOREnet
The Missouri Research and Education Network ✦ 1805 East Walnut Street ✦ Columbia, Missouri 65201
(573) 884-7200 ✦ FAX - (573) 884-6673 ✦ World Wide Web - http://www.more.net ✦ E-mail - info@more.net

March 6, 1998

TO: SA [redacted]

COMPANY: Federal Bureau of Investigation, Kansas City Field Office

ADDRESS:

PHONE:

FAX: [redacted]

FROM: [redacted]

Missouri Research and Education Network
1805 E. Walnut St.
Columbia, MO 65201

b6
b7C

PHONE: [redacted]

FAX: (573) 884-6673

MESSAGE: Following is a summary of the current incident we are working on. Feel free to contact me with anything you need further on this. I look forward to meeting and working with you!

Best regards;

[redacted]

MOREnet Security Services
Incident Summary: MN#12696

Tuesday, 3 Mar 98 approx 2241 CST MOREnet received a page from [redacted] at ISCA regarding a security incident with one of our downstream connections. [redacted] the MOREnet Security Coordinator responded to [redacted]'s call and learned that he was in possession of a password file, reportedly from a computer designated cmc2.cmc.edu

The computer designated is located at Central Methodist College, connected via MOREnet to the Internet. The Internic Whois table lists MOREnet as the technical contact, which precipitated [redacted] call to us.

[redacted] reported that he received the file from an 'east coast' hacker who was claiming to be involved with the recent compromises of the Pentagon and other servers via the Internet. He was sent the file as verification of the hacker's abilities.

After exchanging PGP keys, [redacted] forwarded the file to us on 4 Mar 98 via electronic mail from an account [redacted] We forwarded the file to [redacted] the system administrator at Central Methodist College who confirmed file was indeed the password file from the cmc2.cmc.edu computer as it appeared in late 1996 or early 1997. Related note; we had an incident in November of 1996 wherein the same server was compromised and the password file was suspected to have been cracked at that time.

b6
b7C

On 5 Mar 98 at approx 1445 CST, [redacted] at Central Methodist reported that he observed a userID logged into the cmc2.cmc.edu system at IP Address [redacted] that was attempting to install COPS, a commonly used UNIX system cracking tool [redacted] terminated the user session, and within a few minutes noticed that another userID logged into the system and attempted the same installation. [redacted] noted and reported to us that the sessions were connecting via telnet from a system identified as dyn4.kaskad.ru at IP Address [redacted] terminated the second session, and as of 1630 CST had not had further login attempts from outside of the College's network.

At approx 1500 CST, MOREnet reported the incident to CERT. CERT's suggestion was to send email to the network provider for kaskom.ru with the incident information. CERT requested to be cc'd on the email note. [redacted] from MOREnet sent this note at approx 1700 CST. MOREnet recommended to Central Methodist that the server be taken off line, have the operating system installed from known media and patched to the current levels before bringing the system back online. MOREnet further blocked the IP address [redacted] at the site router, preventing further network traffic to and from the system.

Nothing Further.
[redacted] MOREnet Network and Security Services
5 Mar 98 1730CST