

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 08/14/2002

To: Counterterrorism

Attn: NIPC CIU

Canberra
Ottawa

Legat
Legat

b3
b6
b7C
b7E

From: Chicago

Squad IP/C

Contact: SA

Approved By:

Drafted By:

Case ID #:

Pending) ✓

Title: OPERATION ODAY
COMPUTER INTRUSIONS

Synopsis: To provide information to FBIHQ and to request assistance from Legates Australia and Canada.

Enclosure(s):

For NIPC: One (1) FD-302 of source interview
One (1) document with

b7E

For Legate Canberra: One (1) FD-302 of source interview.
One (1) document of

For Legate Ottawa: One (1) FD-302 of source interview.
One (1) document of

Details: The concurrent version system (CVS) for OpenBSD operating system (OS) has been compromised. As a result,

b7E

An OpenSSH exploit, has also been discovered.

OpenBSD was compromised through the Internet host cvs.openbsd.org or ftp.openbsd.org, both located in Canada. claimed on the IRC channel which he connects to from Internet hosts in Australia, to have committed the hack.

b6
b7C
b7E

226mdhDI.ec

b3
b7E

To: Counterterrorism Room: Chicago
Re: [REDACTED] 08/14/2002

b3
b7E

LEAD(s):

Set Lead 1:

COUNTERTERRORISM

AT WASHINGTON, D.C.

Provide analysis of information and source code for OpenBSD and OpenSSH. Conduct logical follow-up investigation.

Set Lead 2:

CANBERRA

AT MELBOURNE & SYDNEY

Contact Internet service providers to determine identity of individual using the following Internet hosts:

[REDACTED]

b6
b7C

The individual using these Internet hosts may be responsible for the hack and exploit of OpenBSD and OpenSSH. Conduct logical follow-up investigation.

Set Lead 3:

OTTAWA

AT CALGARY & EDMONTON, ALBERTA

[REDACTED]

b6
b7C

To: Counterterrorism Room: Chicago
Re: [REDACTED] 08/14/2002

b3
b7E

regarding unauthorized intrusions resulting in exploits in OpenBSD and OpenSSH. Conduct logical follow-up investigation.

[REDACTED] has administrative control over the Internet host cvs.openbsd.org, and [REDACTED] has administrative control over the Internet host ftp.openbsd.org.

b6
b7C

◆◆