**NIPC ADVISORY 00-056**

# "SubSeven DEFCON8 2.1 Backdoor" Trojan

October 17, 2000

A new variant of the SubSeven Trojan Horse has been discovered in the wild. This malicious computer code could constitute a new threat of distributed denial of service (DDoS) attacks. DDoS attacks were responsible for serious disruptions of several major e-commerce web sites in February 2000. The NIPC and industry partners believe that this new variant may be used to conduct further DDoS attacks which may be more difficult to detect.

Internet Security Systems Inc. (ISS) indicates that the new variant of SubSeven, named DEFCON8 2.1, has been distributed on Usenet news groups with an executable filename of "SexxxyMovie.mpeg.exe." ISS believes that individuals are using this Trojan to test new distributed denial of service methods. More information can be obtained from the ISS web site at http://xforce.iss.net/alerts/advise65.php

The NIPC has independently determined that this variant of SubSeven works on Windows 95, Windows 98 and Windows ME. Previously released variants of SubSeven have allowed remote attackers to obtain all cached information including, for example, passwords, play audio files, access a webcam, and capture screenshots. Upon execution of the "SexxxyMovie.mpeg.exe," a copy of the executable is renamed using a random name/number scheme and placed in the c:\windows directory. After the Trojan copies itself, an entry is placed within the registry and system.ini to start the Trojan process with every boot of Windows. Subsequently the Trojan deletes itself, thus leaving only the newly created Trojan filename within Windows. This variant of SubSeven joins an IRC (Internet Relay Chat) channel on irc.icq.com to notify intruders via IRC or ICQ when new computers are infected. This variant of SubSeven listens on port 16959 or the default port 27374.

The NIPC and others are currently in the process of analyzing the Trojan's code to identify its purpose.

ISS provided a copy of the binary code to the NIPC for further distribution to CERT/CC and the greater anti-virus community. The anti-virus software industry has been notified of the new variant and will test the new variant against their existing SubSeven Dat files which they believe will pick up this malicious code. Full descriptions and removal instructions of a number of variants can be found at various anti-virus software firms web sites, including the following:

http://www.symantec.com
http://www.nai.com (McAfee)
http://www.antivirus.com (Trend Micro)
http://www.fsecure.com
http://www.sophos.com

As always, users are advised to keep their anti-virus software current by checking their vendors' web sites frequently for new updates, and to stay apprised of alerts from NIPC, CERT/CC, and other cognizant organizations.

**Please report any illegal or malicious activities to your local FBI office or the NIPC, and to your military or civilian computer incident response group, as appropriate. Incidents may be reported online at** http://www.nipc.gov/incident/cirr.htm **.**