NIPC ADVISORY 99-030

"W97 m/Caligula Virus"

December 23, 1999

Various sources of known reliability are reporting a reemergence of the W97m/Caligula virus. The currently-released virus contains the same payload found in the original W97m/Caligula virus, and should be recognized by up-to-date anti-virus software.

Military, federal, state and local governmental and commercial/educational systems have all been affected by the W97m/Caligula virus recently; the potential for further infection is significant due to increased ongoing release activity.

The characteristics of the W97m/Caligula include:

- W97m.Cali.a is a macro virus. This Microsoft Word 97 macro virus will add a VBA module called Caligula into infected documents or templates.
- While infecting a document or global template, this macro virus uses a temporary text file c:\io.vxd.
- While closing an infected document on the thirty first day of any month, it displays a message box entitled W97m/Caligula (c) opic [codebreakers 1998].
- The currently-released W97m/Caligula virus propagates in the same manner as the original W97m/Caligula virus. The virus is propagated via infected document exchange. This exchange may take place via diskette, local drive, network drive, or e-mail attachment.
- The payload of W97m/Caligula virus is not currently destructive. The virus searches for PGP secret key ring files (secring.skr) and attempts to transmit any located files to a remote host machine. Due to this attempt to obtain keys to encryption software, it can be reasonably deduced that the primary danger is loss of information.

Inasmuch as this virus has been in widespread circulation for nearly a year, all modern and updated commercial anti-virus packages should detect and disable this virus. Additional information about this virus is available at the web sites of Symantec (www.symantec.com), Network Associates (www.nai.com), and Trend Micro (www.antivirus.com).

The NIPC recommends system administrators to update installed anti-virus software immediately and take other appropriate measures to prevent infection by and spread of W97m/Caligula virus. NIPC recommends widest possible dissemination of this advisory throughout federal, state and local government, military, and private organizations. Please report any information on and damage from infections by this virus to your local FBI office, the NIPC, or incident response group, as appropriate. The NIPC Watch and Warning Unit can be reached 24 hours a day at (202) 323-3204/3205/3206 or (202) 323-2204/2206 (STU-III) or by e-mail at nipc.watch@fbi.gov.