Malware/Trojan: TROJ_BANLOAD.BBE

Malware Overview: This Trojan may arrive on a system as a file attached to a spammed email message, or downloaded by an unsuspecting user when visiting malicious Web sites.

It downloads a file detected by Trend Micro as TSPY_BANKER.FGG from a certain URL. As a result, the routines of the related spyware are exhibited on the affected machine.

Details: This Trojan may arrive on a system as a file attached to a spammed email message, or downloaded by an unsuspecting user when visiting malicious Web sites.

Upon execution, it downloads a file from the following URL:

http://www.{BLOCKED}porterx.xpg.com.br/servicos/documento.doc

It then saves the downloaded file, which is detected by Trend Micro as TSPY_BANKER.FGG, as %System%\ICPLDRV.EXE. As a result, the routines of the related spyware are exhibited on the affected machine.

(Note: %System% is the Windows system folder, which is usually C:\Windows\System on Windows 98 and ME, C:\WINNT\System32 on Windows NT and 2000, or C:\Windows\System32 on Windows XP and Server 2003.)

This Trojan runs on Windows 98, ME, NT, 2000, XP, and Server 2003.

Important Windows ME/XP Cleaning Instructions

Users running Windows ME and XP must disable System Restore to allow full scanning of infected computers.

Users running other Windows versions can proceed with the succeeding solution set(s).

Running Trend Micro Antivirus

If you are currently running in safe mode, please restart your computer normally before performing the following solution.

Scan your computer with Trend Micro antivirus and delete files detected as TROJ_BANLOAD.BBE and TSPY_BANKER.FGG. To do this, Trend Micro customers must download the latest virus pattern file and scan their computer. Other Internet users can use HouseCall, the Trend Micro online virus scanner.