Table of Contents

I-Worm.Wargame

This is a virus-worm that spreads via the Internet attached to infected e-mails. The worm itself is a Windows PE EXE file about 77Kb in length (encrypted by ASProtect EXE files protection utility), and written in Borland C++.

The infected messages have one of the three following variants of the Subject/Body/Attached file:

Subject: Mail to %RecipientEmail%
Body: I send you this patch.
It corrects a bug into Internet Explorer and Outlook.
Attachment: patch.exe

or

or

The worm activates from infected e-mail only when a user clicks on an attached file. The worm then installs itself to the system, runs its spreading routine and payload.

Installing

While installing, the worm copies itself to the Windows system directory twice with the "article.doc.exe" name and with a random ".exe" name (like WVUUQ.EXE), and then registers the latter file in:

under Win9x: WIN.INI file, [windows] section, "run=" command
under WinNT: system registry Run= key.

The worm also creates additional registry key:

HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\WarGames Worm
DisplayName = Wargames Uninstall
UninstallString = rundll32 mouse,disable

The worm also looks for several programs and attempts to terminate their processes. In this list there are anti-virus programs, as well as a few wildspread viruses:

AVP32.EXE
AVPCC.EXE
AVPM.EXE
WFINDV32.EXE
F-AGNT95.EXE
NAVAPW32.EXE
NAVW32.EXE
NMAIN.EXE
PAVSCHED.EXE
ZONEALARM.EXE
KERN32.EXE
SETUP.EXE
RUNDLLW32.EXE
GONER.SCR
LOAD.EXE
INETD.EXE
FILES32.VXD
SCAM32.EXE
GDI32.EXE
_SETUP.EXE
EXPLORE.EXE
ZIPPED_FILES.EXE

Spreading

To send infected messages, the worm uses three different ways (and sends messages of three different types - see above).

First, the worm scans *.HT*, *.DOC and *.XLS files in the Windows directory in a user's Personal, Desktop, Favorites and Internet Cache directories, looks for e-mail addresses in there and then sends infected messages to these addresses.

Next, the virus creates the "wargames.vbs" file in the Windows directory, writes a VBS script to there and runs it. The scripts sends infected messages to all addresses from the MS Outlook Address Book.

At the end, the worm, by using Windows MAPI functions, connects to the incoming e-mail box and "answers" all the messages from there.

Page Top

Last update: 02/26/2002
email: viruslist@avp2000.com