Trend Micro

SEARCH

GO

PRODUCTS | DOWNLOADS | TECH SUPPORT | BUY NOW | PARTNERWEB | SECURITY INFO | FREE TOOLS | ABOUT TREND

Virus Information Center

- Virus Advisories
- Virus Encyclopedia
- Weekly Virus Report
- Virus Primer
- Safe Computing Guide
- Glossary of Terms
- Risk Rating Evaluation
- Virus Info Feed

TrendLabs ›

Real-time Virus Tracking ›

Hoaxes ›

Test Files ›

Virus alerts by email

your email

GO

Virus Encyclopedia

Overview | Tech details | Risk statistics

WORM_CRAZYBOX.A

(see also: description and solution)

In the wild:	No
Discovered:	Jul. 2, 2002
Detection available:	Jul. 2, 2002
Detected by pattern file #:	306 (still using 900-series pattern files?)
Detected by scan engine #:	5.200
Language:	English
Place of origin:	Philippines
Platform:	Windows
Encrypted:	No

Size of virus:	UPX-compressed=75,264 Bytes
	Uncompressed=92,160 Bytes

Details:

This UPX-compressed, executable file, written in Microsoft Visual Basic 6.0, requires the MSVBVM60.DLL file to execute. Upon execution, it drops a PISS.EXE (63,488 Bytes) file in the root directory, which is usually C:\. Similar to this worm, the PISS.EXE file is UPX-compressed and is a ZIP utility DOS program.

This worm uses PISS.EXE to add itself to all ZIP files found in the current user’s Disk Drive/s. Its copy that it attaches to the ZIP file is named LOLITA.EXE. When extracted, LOLITA.EXE drops in the Windows System directory.

The worm also drops another executable program file, UPDATE.EXE in the root directory. It is also detected as WORM_CRAZYBOX.A. The worm uses the UPDATE.EXE file to flash the user screen with this text string displayed:

```
BRIGADA
```

The background color of the text is random. It is not a destructive program but very annoying because there is no way to stop the program except to terminate it from memory forcefully (PRESS CTRL+ALT+DELETE on Win9X and select the process named CRAZYBOX).

The worm also copies itself to the root drive and floppy drives, usually using the following filenames:

- LOLITA.EXE
- MS0701i32.EXE
- XXXiew.EXE

It modifies the registry so that it executes upon system startup:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\RunServices
“b8=<ROOT DRIVE or SYSTEM
DIRECTORY>\MS0701i32.EXE –PETIKB8”
```

This worm propagates itself as the file attachments in emails with details as follows:

```
Subject: check us out
Message Body: we exist to give everyone a
smiley face... :)
Attachment: c:\brigada8.zip
```

The worm takes its list of email recipients from the Microsoft Outlook addressbook. It also accepts three different types of command line arguments as follows:

- -peikb8
- -alcopaulb8
- -trojanmode

When executed with –petikb8 argument, this worm ‘infects’ all zip files. When executed with –alcopaulb8, it creates the file BRIGADA8.ZIP in the root drive with itself as the zip content that default to the target directory \WINDOWS\DESKTOP when extracted. When executed with –trojanmode, the worm shuts down the host computer immediately.

The worm has the capability to infect the NORMAL.DOT template of Microsoft Word also but this was not observed or reproduced in the test environment. When uncompressed, the following text strings can be found in the body of the worm:

```
brigada.worm by petik and alcopaul
```

Description created: Jul. 2, 2002

Email this page **Rate** this page **Contact** us