Virus Encyclopedia

Overview | Tech details | Risk statistics

WORM_CRAZYBOX.A

Description:
This worm sends copies of itself as a file attachment in email messages. It does not have a destructive payload.

Risk rating: low risk
Virus type: Worm
Destructive: No

Solution:

Terminating the Malware Program

You need to terminate the malware process from memory before the malware file can be deleted.

1. Open Windows Task Manager.
   On Windows 9x/ME systems, press CTRL+ALT+DELETE
   On Windows NT/2000/XP systems, press CTRL+SHIFT+ESC
2. In the list of running programs, locate the process name:
   <!—B8-->
3. Select the program, then press either the End Task or the End Process button, depending on your version of Windows. Note that for Windows NT/2000/XP, the list of running processes is located under the Processes tab.
4. To verify if the malware process has been terminated, press F5 to refresh Task Manager then review the process list.
5. Close Task Manager.

Removing Autostart Entries from the Registry

Removing autostart entries from registry prevents the malware from executing during startup. This is also an effective malware process termination procedure.

1. Open Registry Editor. Click Start>Run, type REGEDIT then hit the enter key.
2. In the left panel, double click the following:
   HKEY_LOCAL_MACHINE>Software>Microsoft>
   Windows>CurrentVersion>RunServices
3. In the right panel, locate and delete the entry or entries whose data value is the malware path and filename :
   <!-- b8=<ROOT DRIVE or SYSTEM DIRECTORY>\MS0701i32.EXE -PETIKB8-->

Cleaning infected ZIP files

Delete the file LOLITA.EXE from all your zip files in the disk drive(s). Open each of the zip files by double-clicking the file. Select the filename LOLITA.EXE from the ZIP program window and press the DELETE command.

Cleaning infected floppy disks

Check for the copy of the worm in the inserted floppy disk if present. Delete the file(s) with the LOLITA.EXE and/or MS0701i32.EXE filenames.

Deleting drop file (OPTIONAL)

The worm drops a file named, PISS.EXE, into the root directory. This file is a DOS ZIP progam utility, and is not a malware. You can delete or keep

this file.

Removing the Malware Program

To completely remove this malware from your system, scan your system with Trend Micro antivirus and delete all files detected as WORM_CRAZYBOX.A. To do this Trend Micro customers must download the latest pattern file and scan their system. Other email users may use HouseCall, Trend Micro's free online virus scanner.

Trend Micro offers best-of-breed antivirus and content-security solutions for your corporate network or home PC.