W95.Buggy.Worm@mm

Discovered on: May 22, 2001
Updated on: May 25, 2001 at 12:40:28 PM PDT

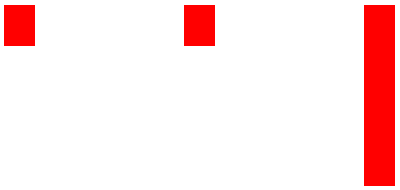
This worm consists of a Microsoft Outlook mass mailer and an IRC worm.

Category: Worm

Infection Length: 8192 (ie042601.exe), 928 (email.vbs), 351 (script.ini), 71 (win.drv), 445 (wsock32.bat)

Virus Definitions: May 23, 2001

Threat Assessment:



Wild:	Damage:	Distribution:
Low	Low	High

Wild:

- Number of infections: 0 - 49
- Number of sites: 0 - 2
- Geographical distribution: Low
- Threat containment: Easy
- Removal: Easy

Damage:

- Payload: Mails itself every time that it is executed
  - Large scale e-mailing: Sends itself to all recipients in Windows Address Book

Distribution:

- Subject of email: The last patch for Internet Explorer
- Name of attachment: ie042601.exe
- Size of attachment: 8192

Technical description:

When this worm is executed, it does the following:

1. It hides itself from the Windows Task List by calling RegisterServiceProcess. Under Windows NT and 2000, this simply fails.
2. It copies itself as \Windows\System\ie042601.exe.
3. So that the worm executes when Windows starts, it changes the `run=` line in the Win.ini file to `run=c:\windows\system\ie042601.exe`
4. The worm drops the following files:

- C:\Script.ini
- \Windows\Email.vbs
- C:\Win.drv
- \Windows\Wsock32.bat.

5. The Script.ini file is copied to

- C:\Mirc\Script.ini
- C:\Mirc32\Script.ini

6. When you use mIRC, the ie042601.exe file is sent to others who connect to the same channel that you are using.
7. The Wsock32.bat file contains code to run each of the dropped files. The worm waits for an active Internet connection and tries to establish one by attempting to connect to www.yahoo.fr. When the connection is successful, Wsock32.bat is executed.
8. The Email.vbs file contains Microsoft Outlook mass-mailing code, which has been copied from VBS.Newlove.A. It sends ie042601.exe to every entry in every address list in the Windows Address Book. The mail appears as follows:

Subject: `The last patch for Internet Explorer`
Message: `Date : <current date> A lot of virus and worms use a bug in Internet Explorer This patch allows you to correct this problem`
Attachment: ie042601.exe

9. Win.drv is an FTP script that is supposed to download the Petik.bmp file; however, the script contains a bug and no file is downloaded. Despite this, the worm attempts to change the Windows wallpaper to use this file; this code also contains a bug, and the values are set incorrectly.
10. After altering the wallpaper setting, the worm hides every .bmp file in the \Windows folder. This may be an attempt to hide the Petik.bmp file, but that file is not stored in the \Windows folder.

Removal instructions:

To remove this worm, delete any files detected as W95.Buggy.Worm@mm and undo the change that it made to the Win.ini file.

To remove the worm:
1. Run LiveUpdate to make sure that you have the most recent virus definitions.
2. Start Norton AntiVirus (NAV), and run a full system scan, making sure that NAV is set to scan all files.
3. Delete any files detected as W95.Buggy.Worm@mm.

To edit the Win.ini file:
1. Click Start, and click Run.
2. Type the following, and then click OK:

NOTE: If Windows is installed in a different location, make the appropriate substitution.

```
edit c:\windows\win.ini
```

3. In the [windows] section, locate the `run=` line. It will look similar to the following:
```
run=c:\windows\system\ie042601.exe
```

4. Remove the text to the right of the equal (=) sign, so that the line now reads

```
run=
```

5. Click File, click Save, and then exit the MS-DOS Editor.