

 Symantec United States

 global sites


 products

 purchase

 service and

 security updates

 downloads

 about symantec

 search

 feedback

©1995-2001 Symantec Corporation.  
All rights reserved.

[Legal Notices](#)  
[Privacy Policy](#)

 security updates

## W32.Fiend.Worm

*Discovered on: May 17, 2001*

*Last Updated on: May 21, 2001 at 10:38:11 PM PDT*



[Printer-friendly version](#)

W32.Fiend.Worm is an IRC worm and is an intended Microsoft Outlook mass mailer.

**Category:** [Worm](#)

**Infection Length:** 6656,

**Infection Length:** 662,

**Infection Length:** 141

**Virus Definitions:** May 17, 2001

**[Threat Assessment:](#)**



### [Security Updates](#)

Symantec AntiVirus Research Center and SWAT

### [Download Virus Definitions](#)

Keep your protection up to date

### [Virus Encyclopedia](#)

Search for Information on Viruses, Worms and Trojan Horses

### [Virus Hoaxes](#)

Information on Virus Hoaxes

### [Jokes](#)

Information on Jokes

### [Newsletter](#)

Email Sent from the Symantec AntiVirus Research Center

### [Virus Calendar](#)

Monthly Calendar Listing Trigger Dates for Viruses

### [Reference Area](#)

Learn About Virus Detection Technologies

### [Submit Virus Samples](#)

Send Suspected Threats for Review



**[Wild:](#)**  
Low



**[Damage:](#)**  
Low



**[Distribution:](#)**  
Low

### **[Wild:](#)**

- [Number of infections:](#) 0 - 49
- [Number of sites:](#) 0 - 2
- [Geographical distribution:](#) Low
- [Threat containment:](#) Easy
- [Removal:](#) Easy

### **[Damage:](#)**

- [Payload Trigger:](#) 5th of any month
- [Payload:](#) Displays message

### **[Technical description:](#)**

When the worm is first executed, it will drop the Petik file in the \Windows folder, and then copy it to:

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

When you use mIRC, this will send the isetup.exe file to others who connect to the same channel that you are using.

NEXT, it will create C:\Friends\Maya.vbs and execute it. This file is supposed to send Windows\Netfriends.exe to every address in your Microsoft Outlook Address Book; however, the worm's code contains bugs and does not work.

After the failed attempt to send email, the worm will copy itself as Windows\iesetup.exe.

Then, so that the worm executes when Windows starts, depending on your operating system, it does one of the following:

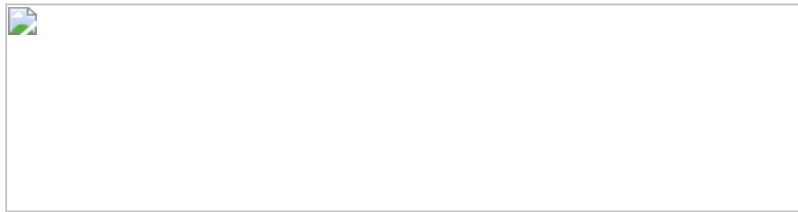
- Windows 95/98. It alters the run= line in the Win.ini file to:  
run=c:\windows\iesetup.exe
- Windows NT/2000. It adds the value

run <path>\Iesetup.exe

to the registry key

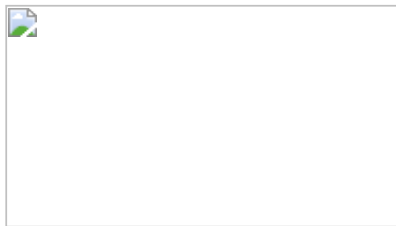
```
HKEY_CURRENT_USER\Software\Microsoft\
Windows NT\CurrentVersion\Windows\run
```

Next, the following message is displayed:



The worm alters the Window's owner and company name settings in the registry, but because of a bug, the text is not set to the intended values.

On the 5th of any month, the following message is displayed:



### Removal instructions:

Because W32.Fiend.Worm affects different operating systems in different ways, how you remove this worm depends on your operating system. Follow the instructions in the order given.

#### **To remove the worm:**

1. Run LiveUpdate to make sure that you have the most recent virus definitions.
2. Start Norton AntiVirus (NAV), and then run a full system scan, making sure that NAV is set to scan all files.
3. Delete any files detected as W32.Fiend.Worm.
4. Do one of the following:
  - If you are using Windows 95/98/Me, skip to the section **To edit the Win.ini file**.
  - If you are using Windows NT/2000, skip to the section **To edit the registry**.

#### **To edit the registry:**

**CAUTION:** We strongly recommend that you back up the system registry before making any changes. Incorrect changes to the registry could result in permanent data loss or corrupted files. Please make sure you modify only the keys specified. Please see the document [How to back up the Windows registry](#) before proceeding. This document is available from the Symantec Fax-on-Demand system. In the U.S. and Canada, call (541) 984-2490, select option 2, and then request document 927002.

1. Click Start, and click Run. The Run dialog box appears.
2. Type `regedit` and then click OK. The Registry Editor opens.
3. Navigate to the following key:

```
HKEY_CURRENT_USER\Software\Microsoft\
Windows NT\CurrentVersion\Windows
```

4. In the right pane, delete the following value:

```
run    <path>\iesetup.exe
```

5. Exit the Registry editor.
6. Restart the computer.

#### **To edit the Win.ini file:**

1. Click Start, and then click Run.
2. Type the following and then click OK:

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

**NOTE:** If you have installed Windows to a different location, make the appropriate substitution.

3. In the [windows] section, locate the run= line. It will look similar to the following:

```
run=c:\windows\iesetup.exe
```

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

```
run=
```

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

---

*Write-up by: Peter Ferrie*



*Tell a Friend about this Write-Up*