Symantec United States

global sites

products

purchase

service and support

security updates

downloads

about symantec

search

feedback

Legal Notices
Privacy Policy

security updates

VBS.Copy@mm

Discovered on: June 18, 2001

Last Updated on: June 20, 2001 at 09:59:09 PM PDT

Printe Printer-friendly version

VBS.Copy@mm is a simple mass-mailing worm. The worm contains several payloads that are executed only on certain days of the month. The worm emails itself to all contacts in the Microsoft Outlook Address Book.

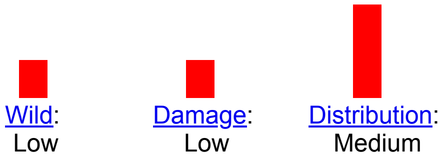
NOTE: Definitions dated prior to the June 18, 2001, detect this worm (using heuristics detection) as Bloodhound.VBS.Worm.

Category: Worm

Infection Length: 3626 Bytes

Virus Definitions: June 18, 2001

Threat Assessment:



Wild:

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

Damage:

- Payload Trigger: On the 1st, 12th, 14th, 15th, 28th and 30th of every month
- Payload: There are several different ones. Please see description below
  - Large scale e-mailing: Attempts to email everyone in the Microsoft Outlook addressbook
  - Modifies files: Attempts to modify all .VBS files on the system

Distribution:

- Subject of email: What is the seven sins??
- Name of attachment: seven.vbs
- Size of attachment: Approx. 3Kb

Technical description:

VBS.Copy@mm is a simple worm. When executed, the worm does the following:

1. It copies itself as
   - C:\Windows\Seven.vbs
   - C:\Windows\System\Envy.vbs

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

- C:\<tempfolder>\Lust.vbs (by default, <tempfolder> is C:\Windows\Temp)

2. It adds the value

```
Envy
```

to the registry key

```
HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows\CurrentVersion\Run
```

and the value

```
Lust
```

to the registry key

```
HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows\CurrentVersion\RunServices
```

3. Next, the worm determines the current day of the month. There are several payloads in the worm, which are executed depending on which day it is:

- On the 1st, 15th, and 30th of the month, the worm adds the value

  ```
  Anger
  ```

  to the registry key

  ```
  HKEY_CURRENT_USER\Software\Microsoft\
  Windows\CurrentVersion\Run
  ```

  This causes the mouse to be disabled after restarting the computer.
- On the 12th and the 28th of the month, the worm displays a message and attempts to shut down Windows.
- On the 14th of the month, the worm attempts to disable the keyboard and display a message.
- On the 5th and 17th of the month, the worm creates a new .vbs file that displays a message the next time that the computer is restarted.

4. After the payload routine has been triggered, the worm performs a recursive search on all drives for .vbs files. When a .vbs file is found, the worm adds three lines of code to the beginning of the file. These three lines cause C:\Windows\Seven.vbs to be executed whenever an infected .vbs file is executed.
5. Finally, the worm sends the following email message to all contacts in the Microsoft Outlook Address Book:

Subject: "What is the seven sins??"
Body: "Look at this file and learn them"
Attachment: Seven.vbs

Removal instructions:

To remove this worm, delete files detected as VBS.Copy@mm, and remove the values that it added to the registry.

To remove this 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 VBS.Copy@mm.

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 key

```
HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows\CurrentVersion\Run
```

4. In the right pane, delete the following values if they exist:

```
Envy
Anger
```

5. Navigate to the key

```
HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows\CurrentVersion\RunServices
```

6. In the right pane, delete the value

```
Lust
```

7. Exit the Registry Editor.

Write-up by: Neal Hindocha

Tell a Friend about this Write-Up