symantec. security updates

VBS.Ketip.A@mm

Discovered on: April 25, 2001
Last Updated on: May 2, 2001 at 04:51:44 PM PDT

Printer-friendly version

VBS.Ketip.A@mm is a Visual Basic Script (VBS) worm. It arrives as an HTML email message. Like many other worms, it uses Microsoft Outlook and IRC clients to spread. The script attempts to send information that is stolen from infected computers to some email addresses.

Also Known As: VBS.Ketip.B@mm

Category: Worm

Virus Definitions: April 25, 2001

Threat Assessment:

Wild:

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

Damage:

- Payload:
  - Large scale e-mailing: Sends an HTML message to all addresses in the Microsoft Word Address Book.
  - Modifies files: Overwrites .exe, .ini, .gif, .jpg, .htm, .vbs, .vbe, .js and .jse files. Sets attribute of .mp3, .doc, .xls, .ppt and .hlp files to hidden.
  - Causes system instability: If the worm runs, Windows will no longer operate.

Distribution:

- Subject of email: Important Message From Microsoft Corporation

Technical description:

When the worm is executed, it does the following:

1. It copies itself to C:\Windows\Petik.txt.vbs.

2. It adds the value

```
Petik       <Windows System
Folder>\Petik.txt.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

to the registry key

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

to enable itself to run at startup.

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

Subject: `Important Message From Microsoft Corporation`
Message: `"This message has permanent errors. <br>Sorry<br>"`

The HTML message contains Visual Basic Script, and it attempts to drop the file C:\Windows\Worm.vbs, but it fails to do so because of bugs in the worm's code.

4. The worm then attempts to send the following information from the infected computer to petik@caramail.com and ppetik@hotmail.com:

Infected Date
Infected Time
Computer Name
Organization
Language
OS Version
OS Version Number
Product ID
Product Key
Internet Explorer Start Page
Internet Explorer Download directory path
Windows directory path
System directory path
Temporary directory path
Program Files directory path

5. It next drops two .ini files for IRC clients:

C:\Mirc\Mirc.ini
C:\Program Files\Pirch\Script.ini

These do not work properly due to bugs in the worm's code.

6. It modifies or overwrites following files:
   - Files with the extensions .vbs, .vbe, .js, and .jse are overwritten by the worm.
   - Files with the extensions .exe, .ini, .gif, .jpg, and .htm have the .vbs extension appended to them and are overwritten by the worm.
   - Files with the extensions .mp3, .doc, .xls, .ppt, and .hlp have their attribute set to hidden.

If this process is executed, you will have to reinstall Windows and most programs because .exe files have been overwritten.

Removal instructions:

To remove this worm, delete files detected as VBS.Ketip.A@mm, VBS.Ketip.A@mm (2), or VBS.Ketip.A@mm.ini, and undo the change the worm made to the registry.

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.A@mm, VBS.Ketip.A@mm (2), or VBS.Ketip.A@mm.ini.

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 value

```
Petik       <Windows System
Folder>\Petik.txt.vbs
```

5. Exit Registry Editor.

Write-up by: Kaoru Hayashi

Tell a Friend about this Write-Up