



OFFICE OF THE CHIEF INFORMATION OFFICER

STANDARD OPERATING PROCEDURE

July 22, 1999

Virus Pattern Update for ScanMail



Effective:

This standard operating procedure is effective immediately and will remain in effect until cancelled or superseded.

Approval Date:

July 22, 1999

Introduction:

This standard operating procedure outlines the steps required to update the ScanMail virus pattern.

Requirements:

Risk Identification:

The ScanMail virus pattern must be updated regularly to prevent new virus files from entering the network system. If the ScanMail virus pattern is not regularly updated, the network will become susceptible to new virus files. Virus infection can cause file corruption, registry corruption, and data loss.

Validation:

Not required.

Approval:

Procedural Steps:

1. Create the directory C:\Trend\Updates\Patterns on your hard drive using the following steps: (**NOTE**: If this directory already exists, delete all files in the directory and proceed to Step 2.)
  - a. Right-click on **Start** and choose **Explore** to open the **Windows Explorer** dialog box. In the **All Folders** list, select C. From the **File** menu, go to **New** and choose **Folder**. Name the new folder Trend and press ENTER.
  - b. From the **All Folders** list, select the Trend folder. From the **File** menu, go to **New** and choose **Folder**. Name the new subfolder Updates.
  - c. From the **All Folders** list, select the Updates folder. From the **File** menu, go to **New** and choose **Folder**. Name the new subfolder Patterns.
2. Download the new pattern file LPTxxx.zip using the following steps:
  - a. Open your Web browser and log on to <http://www.antivirus.com>.
  - b. On the Trend Micro homepage, click the **Corporate Users** link to open the News and Information page.
  - c. On the News and Information page, click the **Downloads** link to open the Downloads page. (**NOTE**: You do not need a serial number.)
  - d. On the Downloads page, click the **Pattern Files** link to open the Pattern Files page.
  - e. You will be given the option to download two files, LPTxxx.zip or PTNxxx.tar. Click on LPTxxx.zip to download the ScanMail Pattern Update for Intel. (**NOTE**: You can download the file using either HTTP or FTP.)

- f. If the **Unknown File Type** dialog box opens, click the **Save File...** button. The **Save As** dialog box will then open. Browse to the C:\Trend\Updates\Patterns directory and click the **Save** button. (**NOTE**: This is the same directory you created in Step 1.)
  - g. After the file is downloaded, the **Save As** dialog box will automatically close. Close your Web browser.
3. Extract LPT\$vpn.xxx and Whatsnew.txt by running LPTxxx.zip using the following steps:
- a. Click the **Start** button and choose **Run**.
  - b. Click the **Browse** button to open the **Browse** dialog box.
  - c. Browse to the location where you saved LPTxxx.zip.
  - d. Select LPTxxx.zip and click **Open** to open the **Run** dialog box. Click **OK** to extract the files. (**NOTE**: Double-clicking on LPTxxx.zip will automatically open the **Run** dialog box.)
  - e. After you click **OK**, Winzip will automatically open. From the **Actions** menu, choose **Extract** to open the **Extract** dialog box. Make sure that the **All Files** option button is selected and click the **Extract** button. The following files will be extracted:  
  
LPT\$vpn.xxx  
Whatsnew.txt
  - f. These files will automatically be extracted into the C:\Trend\Updates\Patterns directory. Once the extraction is completed, delete LPTxxx.zip.
4. Copy LPT\$vpn.xxx to all IS Servers (test-is-100 to test-is-110 and PF-01) using the following steps:
- a. Double-click on **Network Neighborhood**. From the **Network** dialog box, double-click on Test-ns-01 to open the Test-ns-01 property sheet.
  - b. In the Test-ns-01 property sheet, double-click on NOD-Tools. In the NOD-Tools property sheet, double-click on Virusup. In the Virusup property sheet, double-click on Scanmail.bat to automatically update the ScanMail Virus Pattern on test-is-100 – 110 and PF-01.