Guidelines for initial testing of PestPatrol™

This short guide will help you get quick results from your first experience with PestPatrol. After this initial quick test, we encourage you to install the product on a login server and do more extensive testing using the command line approach described in the Network Implementation Guide supplied with the software.

If you plan to evaluate on a client system, scan your files manually and watch the results fly across your screen. If you plan to evaluate on a server, be aware that a manual scan - unlike automated and log-in scans - uses some system resources and may slow the system while it is running. If this is likely to cause a problem, you should run the manual scan during off-peak hours.

1. **Select a system on which to perform the first tests**
   Select a PC that you suspect is infected with one or more pests. Typical symptoms of an affected machine are slow or erratic performance and unexpected or unrequested actions, such as random system reboots. If you don't have a machine you suspect of being infected with a pest, just choose any system that has frequent Internet use or a laptop that is used outside the firewall; we think you'll be surprised by what's on that system that you don't know about.

2. **Install PestPatrol**
   Install PestPatrol on this machine, following the onscreen instructions. During installation you will be asked if you want to load the PestPatrol Control Terminal. Answering yes to this will place a PestPatrol icon in your systray which allows for easy access to different product features. Make sure to print the Network Implementation Guide, which can be found at www.pestpatrol.com/productdocs. This provides all the information you need when you move on to testing the program in a network environment.

3. **Set the suggested test configurations**
   When you open PestPatrol you will be in the **Scan** tab. If you are evaluating on a client, you can check the 'all hard drives' box or you can go through the directory tree on the left and pick specific areas to be scanned. Your selected drives/folders will be shown in the right-hand window.

   Now go to **Options|Automatic Scans** tab:

   - **Scan on Boot** is not checked, by default. Using this option will invoke PPCL at boot instead of running the GUI. You will probably want to experiment with PPCL more after this first test-drive.
   - **Invoke on Boot** is the default setting for the MemCheck memory scanner. Using MemCheck turns PestPatrol into a real-time pest detector. More on MemCheck and its command line switches can be found at www.pestpatrol.com/ppmemcheck
   - **PPControl** places an icon in the systray that enables you to control various program features using right click; this also defaults to Invoke on boot.
   - **KeyPatrol** is a heuristic scanner that detects any keylogger not specifically identified by PestPatrol scan strings. Because of the increased risk of false alarms, KeyPatrol does not default to Invoke on boot. More information on KeyPatrol can be found at www.pestpatrol.com/keypatrol.
   - **CookiePatrol** identifies and deletes all spyware cookies automatically as they enter the PC, and records all events to a separate log - machine-name_CookiePatrolLog.txt. The default is Invoke on boot, but for the purposes of evaluation, we suggest you first scan with this switch turned off. More on CookiePatrol can be found at www.pestpatrol.com/cookiepatrol . Note that CookiePatrol by default makes a sound each time a cookie is deleted. If you want to stop this sound, open the CookiePatrol menu from the system tray and select Disable Sound.

   You may choose to enter some switches under PPMemCheck Memory Scan, following the conventions described in the PestPatrol Network Implementation Guide. For the purposes of this test drive, you could insert the following:

   ```
   /auto /quarantine /emailto=<name>@<company.com>
   ```

   to automatically quarantine any pests detected in memory and send an alert e-mail to a designated individual.

All other options should be left in the default setting for your first scan. You can start your scan from any screen by clicking on the **Start** icon in the top right corner. When you select **Start,** the screen display will automatically change to the **Logs|Detected** tab.

NOTE: Because of the way PestPatrol operates, we do not recommend using it to scan remote drives on a peer-to-peer network. In a peer-to-peer environment, it is advisable to install a full copy of PestPatrol on each system.

4. **Analyze the scan results**
   When scanning is complete, you can decide how to proceed with the pests identified. You should first review the logs for any authorized security tools that PestPatrol identified because they could be used in a malicious manner (such as RemotelyAnywhere). You can permanently exclude such tools from future scans on this system using the **Exclude** command.

   The remaining pest files may be quarantined or deleted. If you are concerned about whether any particular file is a genuine pest, place it in quarantine and send a copy of the log to PestPatrol support by clicking on the **E-mail Support** button. You will be contacted within 24 hours.

5. **Scheduling Automatic Scans**
   We recommend automatic scanning on a daily basis at a time when system usage is at its lowest.

   (a) Open the **Task Scheduler** and click on **Add Scheduled Task**
   (b) Use the **Browse** button to locate PestPatrolCL.exe (normally in c:\Program Files\PestPatrol)
   (c) Enter a name for the task, for example PestScan.
   (d) Select the frequency for the task to take place.
   (e) Set the start date and time for the first instance of the task.
   (f) Click **Finish** to accept the scheduled task, or **Back** to go back and edit your choices.

   Example:
   To run a scan every Monday through Friday at 6:00am enter at the command prompt:

```
AT 6:00 /interactive /every:M,T,W,Th,F "[path to PPCL\]PestPatrolCL.exe [/hard
/nosound /nopause]"
```

   Other settings in PestPatrol will allow you to configure the system to meet your individual needs.

6. **Scheduling Automatic Updates**
   Follow the directions for scheduling scans above. In place of PestPatrolCL.exe, substitute PPUpdater.exe. The only command line switch required is **/autoexit**. As a rough guide, we recommend running PPUpdater on a weekly basis, but the frequency you select should be determined by your own vulnerability estimates.

   Further information on PPUpdater may be found at www.pestpatrol.com/PPUpdater/

7. **Testing MemCheck**
   You can download a test file called Bait from www.pestpatrol.com/support/downloads.asp#testfiles. Don't worry, the file is harmless and is designed solely for testing purposes in the same way as eicar.txt is used to test anti-virus scanners. Save it to your desktop and change the name to Bait.exe. Double click on it and watch closely. Then, check your e-mail for an alert (you will need to be using the /**emailto** switch as described above for an e-mail to be sent.

If you have any questions as you test the product, don't hesitate to call our toll free number +1 866-235-7163 x223 (+1 717 243 6588 x223 from outside North America). Alternatively, you can post technical support questions directly to our online helpdesk.

PESTPATROL
Protecting computers from hidden threats

PestPatrol, Inc
453 Lincoln Street, Carlisle, PA 17013
Phone: 717 243 6588 Fax: 717 243 8545 E-mail: sales@pestpatrol.com