Implementation Guide

PestPatrol™

In a Networked Environment

TABLE OF CONTENTS

INTRODUCTION

The biggest threats to your network security may not even be visible to your current security tools. Spyware, hacker tools, and trojans can all sneak on to the network, bypassing existing security measures, and lurk silently until something - or someone - sets them off. When that happens, you could lose passwords, customer data, intellectual property - even your web site or entire network.

PestPatrol: a brief overview

PestPatrol is a powerful security tool that detects and eliminates:

- Spyware/adware: Rogue applications that "phone home" user and system information without permission.
- Hacker tools: Password crackers, key loggers, port scanners, and more
- Trojan horses: Denial-of-service attack agents, remote access trojans (RATs), and more

These pests create back doors into your networks, compromising security and exposing the company to litigation. PestPatrol detects and removes tens of thousands of pests quickly and safely by:

- Check and clean files, registry and start-up areas
- Download and install component and scan string updates automatically
- Log all activities to a central database
- Scan all or selected file types, including archives
- Scan memory as well as local and remote drives
- Block spyware cookies from entering systems
- Configure scheduled scans to meet individual organizations' needs
- Quarantine or remove any identified pest
- Exclude any file used as an internal security tool

PestPatrol in a networked environment

This document is a basic guide to configuring and using PestPatrol in a networked environment.

The key program components covered here are:

- CookiePatrol.exe, the automated real-time spyware cookie remover
- PPMemCheck.exe, the real-time active memory scanner
- PestPatrolCL.exe, the command line hard-drive scanner
- PPUpdater.exe, the automated update program

PestPatrolCL (PPCL) is at the heart of the PestPatrol solution. It provides flexibility in deploying PestPatrol throughout an organization, enabling you to install, configure, run and maintain PestPatrol protection in the way that works best for you. It can be invoked by a login script, from a batch file, from a scheduler, or when you right-click on a file or folder.

NOTE: If you plan to run PestPatrol with Check Point™ SecureClient™, please call +1 866 235 7163, extension 223, or go to www.pestpatrol.com/ProductDocs/ to obtain a guide for this environment.

System Requirements

The above PestPatrol components may be installed on any system running Windows 98/ME/NT/2000/XP, with 96 MB RAM and 7MB free hard disk space.

NOTE: Because of the way in which 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.

USING PESTPATROL WITH LOGIN SCRIPTS (NT4 AND WIN2K)

This section provides the information required to install PestPatrol in a NT4/Win2K server environment, and to invoke PestPatrol from a login script. Running PestPatrol from a login script will ensure that, if a user attempts to log in to the network from a pest-infected machine, the administrator will be notified immediately.

If you wish to run PestPatrol from a NetWare server, please refer to the section later in this document entitled Using PestPatrol in a NetWare Environment.

Syntax

All switches (see below) may be entered in any case (/Append, /APPEND, /append, /aPPEND, etc.) Switches may be entered in any order.

Any amount of space may separate switches on a command line.

To ensure that a full description of each event is written to the log file, the /info switch should be included in all command line scripts.

The example login script below is the recommended starting point for system administrators deploying PestPatrol for the first time. This script is designed to:

- Load the real-time components of the software first
- Minimize impact on users at initial login (/wait and /idle switches)
- Require no user action if a pest is detected (/nopause, /nosound, /nologafter, /auto switches)
- Send session logs to a single e-mail address if a pest is detected (/emailto switch)

Procedure

To install the latest version of PestPatrol, use the installation CD provided, or download the latest version of PestPatrol from the web site. Install PestPatrol to the C:\Program Files\PestPatrol Folder. Create a share name for the folder called pplogon.

Setting permissions for PestPatrol

PestPatrol and the login script must be installed on all login servers (PDCs and BDCs) using the appropriate following method:

NT environment

1. After installing the software, go to the PestPatrol program folder and right click.
2. Select Sharing
3. Under the Sharing tab, click “shared as” and enter the name pplogon. The login script assumes that a share named \pplogon has been created that equates to the PestPatrol program folder.
4. Click the Permissions button and ensure that everyone has Full Control over the folder.
5. Repeat this process for the Logs file, with the exception of leaving the name Logs.

Win2K environment

1. After installing the software, go to the PestPatrol program folder and right click.
2. Select Sharing to display the PestPatrol Properties window.
3. Click on Permissions, ensure that Domain Users appears on the Permissions for pplogon tab, and select Full Control.
4. Now go to the Security Tab and add Domain Users, then click Full Control.

Example login script

Under NT, the login script must be placed in the folder C:\winnt\system32\repl\import\scripts.
Under Win2K, the script must be placed in the folder C:\winnt\sysvol\sysvol\domainname\scripts.

This script provides an example for Win9x and NT/Win2K/XP-based clients. The login workload will be distributed among available login servers for NT clients; all Win9x clients will run PestPatrol from a single fixed server as specified in the net use command.

If you need additional assistance in writing a script to meet your needs, please post your request to our online help desk at http://helpdesk.pestpatrol.com

```
@echo off

if "%OS%" == "Windows_NT" goto NT_OS

:W9x_OS

net use x: \\yourserver\pplogon

start x:\cookiepatrol.exe  /NoLog  /NoSound
```

(Note: In some Win9x environments, CookiePatrol is not able to be run silently. If this is the case in your environment, omit the CookiePatrol command line from this portion of the script.)

```
start x:\ppmemcheck.exe /auto /ignore
/emailto=youremailaddress@yourcompany.com

start x:\pestpatrolcl.exe c:\ /wait=300 /info /idle /nologafter /ignore
/emailto=youremailaddress@yourcompany.com
cls

EXIT

:NT_OS (Win2K, NT, XP clients go here)

start %logonserver%\pplogon\cookiepatrol.exe  /NoLog  /NoSound

start %logonserver%\pplogon\ppmemcheck.exe /auto /ignore
/emailto=youremailaddress@yourcompany.com

start %logonserver%\pplogon\pestpatrolcl.exe c:\ /wait=300 /info /idle
/nologafter /ignore /emailto=youremailaddress@yourcompany.com

EXIT
```

SCANNING WITH PPCL

Where to scan

"Drive or Drive+Directory" specifies a location to automatically scan. The default is to scan all local (non-network) fixed disks. At least one such location must be specified for PPCL to operate. The second and third characters must be ":\" or / and up to two locations may be specified. Areas will be scanned in the order specified. Subdirectories will always be scanned. If the path contains a space, enclose it in "double quotes", for example:

```
d:\ "c:\Program Files\ "
```

/hard causes a scan of all local hard drives.
/extensions=ALL causes the program to scan all files. (Warning: this can greatly extend the scan time and increases the risk of false positives). This switch is not recommended for ongoing deployment.
/extensions=*nnn causes the program to scan only those files specified by extension. Below is an example of scanning only files with the .EXE , .COM and .DLL extensions:

```
/extensions=*.EXE;*.COM;*.DLL
```

If no **/extensions=** command is used, the default extensions scanned are: *.ADE; *.ADP; *.ASC; *.AMM; *.BAS; *.BAT; *.CHM; *.CMD; *.COM; *.CPL; *.CRT; *.DO; *.DOC; *.EXE; *.HLP; *.HTA; *.INF; *.INS; *.ISP; *.JS; *.JSE; *.LNK; *.MDB; *.MDE; *.MSC; *.MSI; *.MSP; *.MST; *.PCD; *.PIF; *.PL; *.REG; *.SCR; *.SCT; *.SHB; *.SHS; *.URL; *.VB; *.VBE; *.VBS; *.WSC; *.WSF; *.WSH; *.XL; and *.XLS.

Note: Multiple extensions must be separated by a semicolon.

Logs

/log=fullyqualifiedfilename saves scan results to this file and location, providing the location exists. If the path contains a space, enclose it in " ", for example:

```
"/log=c:\Our Results\Our Log.txt"
```

If no log filename is specified, the log will be named UserID.txt, where UserID is the login id for the system being scanned.
/Append appends the scan results to an existing session log, if it exists. The default is to overwrite a prior session log of the same name.
/NoLogAfter prevents the log from being displayed on completion of a scan. Whatever program is associated with the provided extension will be used to display the log; Notepad will typically be used when the log ends with .txt. The default setting is that a log will be automatically displayed upon completion, provided that a pest was detected and one or more directories were scanned.

On detection

/[Action] specifies what to do if a pest is found. If no action is provided, PPCL will default to /Ignore.
/Ignore (default) - take no action. This approach is recommended for the first few scans to see what is on the network; Once this is done, we suggest you build the exclusion tables and run the scan once more for confirmation, then change to the delete switch.
/Delete - remove the pest.
/Quarantine - move the pest to a quarantine directory. This approach is n recommended in a login script environment.
/NoSound - disable any sounds that otherwise occur when a pest is found or the scan has completed. The default setting is On.)

/NoPause - disable any popup warnings that otherwise occur when a pest is found. The default setting is On.)

Notification

/EMailTo=<address> specifies the email address to notify if a pest is detected. The message is sent with a log attached. MAPI must be supported by sending machine.

Example: `/EMailTo=Support@PestPatrol.com`

The next 3 switches are optional and should be used if you wish to use a mail server inside your firewall.

/Host=<mail server name>
/UserID=<UserID with permission to send to this mail server>
/Password=<Password for UserID with permission to send to this mail server>

/ICQ=<icqnumber> specifies the icq address to notify if a pest is detected.

Example: `/ICQ=142772065`

Additional switches

/Idle causes PPCL to run only when CPU utilization is idle, minimizing consumption of system resources.
/Info causes a detailed description of each event to be written to the log file, including an indication of the threat level of each pest and advice on appropriate action. If this parameter is not included, the only information written to the log file will be pest name, location, and Pest Verification Token (PVT). Not using the /info switch will decrease the amount of computing resources required during the scan, thus provide faster scan times.

Error levels

The log created when PPCL finishes and exits will show the following error levels:

0: no problem encountered in operation, and no pest detected.
1: trouble reading specified device or file or other error.
2: one or more pests found.

Excluding Pests in the Login Environment:

PestPatrol currently has three exclusion levels; in the network environment, these are global by nature.

1. The first is by category under the "Options" and "What to search for" tabs in the GUI. This is a very general exclusion rule. By unchecking a category, ALL pests in that category will be excluded from detection.

2. The second is by Files and Directories under the "Options" and "What to Exclude" tabs on the left hand side of that screen. Here, you can specify exactly which files and directories are to be excluded from the scan. This method can be implemented before or after a scan and will be honored for all following scans. Simply select "Add" and choose the directory and files to exclude. You must select all the way down to the file level. Selecting just the directory does not mean all the subdirectories and sub files are excluded. You must check every file to exclude. Optionally, files and directories can be removed from the list as well. In a server environment, the client and server paths must be the same for this feature to work. If the file or directory does not exist, the command is simply ignored.

3. The third method of exclusion is by pests that have been detected. This is under the "Options" and "What to Exclude" tabs on the right hand side of that screen. Here you can specifically select which pests to ignore from further detection. Following a scan, by clicking on the "Add" button a list of detected pests will be displayed. Simply select the pests you want to be excluded from further detection and click "OK". This exclusion is pest-specific and will be honored on any client scan regardless of the location the pest is detected.

To exclude pests in a login script environment, methods two and three are suggested. Install the pest program on the server, detect it and exclude it using the GUI, as described in methods two or three above.

Remember; PestPatrol's job is to inform you of the potential backdoors and threats to the computer. You need to determine whether or not some of these threats are acceptable. Using the Exclusions feature will assist you in excluding the pre-determined and acceptable threats.

Examples
The following example script scans the entire hard drive (/hard) but only examines .EXE, .COM, or .DLL files. There will be no pause, even if a pest is found (/nopause), but a warning will be sounded if a pest is found (no /nosound switch). Any pest found will be ignored. Regardless of the outcome, a log will be displayed on completion of the scan.

```
start %logonserver%\pplogon\pestpatrolcl.exe /info /hard
/extensions=*.EXE;*.COM;*.DLL /nopause
```

A note on restoring files from quarantine

When the command line of the start-up script includes /quarantine, the following occurs:

1. An entry is written to the Master Log of the server through which the user logged in.
2. When a pest is identified, the pest file is removed from the user machine, and placed in the /quarantine folder on the appropriate login server. The name of the quarantined file is a sequential number that corresponds to the Master Log entry above.
3. If you run the PestPatrol GUI on that login server, you will see all pests quarantined on that server from the Quarantine tab of the PestPatrol GUI. Note that it is not possible to use the GUI to restore the file from the server. To do this, you need to manually move it by copying the appropriate numerically-named file from the server back to the correct location on the user machine and rename it to the original filename.
4. It is also possible to sit at the user machine, run the PestPatrol GUI remotely from the server, and use the GUI's restore feature to return the file to its original location on that user's machine.

SCHEDULING SCANS WITH PPCL

You can combine PestPatrolCL.exe with a task scheduler to set schedules for regular scanning to meet your organization's requirements:

Scheduling scans under Windows 9x

First, make sure that the system date and time on your computer are accurate. The Windows Task Scheduler relies on this to know when to run scheduled tasks. To check and/or change the date and time, double-click on the time on the taskbar. Below are two examples of scheduling a scan using the Windows Task Scheduler - the first very simple, the second invoking several different scanning parameters. The results of any scheduled scan are added to the Master Log in the normal way.

Scheduling a simple scan

1. Double-click **Add Scheduled Task** on the **Scheduled Tasks** list to invoke the wizard.
2. Use the **Browse** button to locate PestPatrolCL.exe (normally in c:\Program Files\PestPatrol)
3. Enter a name for the task, for example PPScan.
4. Select the frequency for the task to take place.
5. Set the start date and time for the first instance of the task. The wizard presents a summary of your scheduled activity.
6. Click **Finish** to accept the scheduled task, or **Back** to go back and edit your choices.

Scheduling a complex scan

Follow the steps outlined above for the simple scan but, when you get to the Finish stage, open Advanced Options to enter the required command line switches. Make sure that the path for the program to be run (PestPatrolCL.exe) is enclosed in double quotation marks and that you leave a space before adding the command line switches. Do not use quotation marks around the switches.

Scheduling scans under Windows NT/2000

Windows NT has a built-in scheduler, which you can control by using the AT command. Use it to automatically run PPCL in the background (invisible mode) or in the foreground (interactive mode).

Make sure that the **Schedule** service is turned on:

1. Go to the **Control Panel**
2. Double click on the Services icon
3. Select **Task Scheduler.** If the Task Scheduler service's startup is not set to **Automatic**, do so by clicking on the **Startup**... button If the Task Scheduler service does not start, do so by clicking on **Start**.
4. Run **Command Prompt**
5. Add programs to the scheduler using the following command syntax:
   AT <time> /INTERACTIVE /EVERY:<dates> "<command>"

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

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

SCANNING MEMORY WITH MEMCHECK

MemCheck is designed to provide real-time protection. If a user executes a pest inadvertently between scans, or if a keylogger runs automatically, MemCheck will see the process and handle it according to the parameters assigned (terminate process, quarantine, delete, etc.). MemCheck may be installed on individual PCs and run locally or installed on a server and invoked from a login script. For ease of deployment and maximum protection, it is recommended that MemCheck be invoked from a login script in conjunction with PPCL. PPCL provides a complete sweep of a client PC at the time the user logs in, while MemCheck provides protection against the execution of a pest downloaded sometime after the initial login and prior to the next login.

MemCheck can be set up to run with or without user intervention. Command line switches are provided to control the actions to be taken when a hands off mode is selected. For example:

```
Start %logonserver%\pplogon\ppmemcheck.exe /info /auto /quarantine
/emailto=Sysadmin@yoursite.com
```

On detection of a pest in memory, this command automatically quarantines the pest and sends an e-mail (with logfile attached) to notify the administrator that a pest has been detected. No user action is required. When used in a login script on a Win9x system, simply substitute `x:` for `%logonserver%`.

Parameters

MemCheck accepts the following parameters directly at the command line:

/Info causes a detailed description of each event to be written to the log file, including an indication of the threat level of each pest and advice on appropriate action. If this parameter is not included, the only information written to the log file will be pest name, location, and Pest Verification Token (PVT).
/Auto - If a pest is detected in memory, MemCheck's Pest Detected dialog is not displayed and PPCL is invoked immediately. This switch implies the PPCL parameters **/NoLogAfter** and **/NoPause**.
/Delete - If a pest is detected in memory and the user chooses to terminate it, or if the **/Auto** parameter is given, PPCL deletes it. The pest is removed from memory before PPCL is invoked.
/Quarantine - If a pest is detected and the user chooses to terminate it or the **/Auto** parameter is given, PPCL quarantines it. The pest is removed from memory before PPCL is invoked.
/Ignore - If a pest is detected, PPCL will ignore it. The pest will not be removed from memory before PPCL is invoked when the **/Auto** parameter is given. Otherwise, the pest will be removed in accordance with the user's response to the Pest Detected dialog.

All other parameters (eg **/EmailTo**) are passed verbatim to PPCL in all cases where it is launched. For example, if MemCheck is run with the switch

```
/delete /info /emailto=sysadmin@yourcompany.com
```

MemCheck calls PPCL with the appropriate switch settings. PPCL does the actual deletion of the pest, writing to the log file(s), and e-mailing the log to the administrator.

CONTROLLING SPYWARE COOKIES WITH COOKIEPATROL

CookiePatrol provides real-time protection against spyware cookies. It may be installed on individual machines and run locally or installed on a server and invoked from a login script. For ease of deployment and maximum protection, it is recommended CookiePatrol be invoked from a login script in conjunction with PPCL and MemCheck. CookiePatrol will automatically detect and eliminate spyware cookies as soon as they arrive on a user machine.

To invoke CookiePatrol in a login script, add the following command line to the script:

```
Start %logonserver%\pplogon\CookiePatrol.exe /NoLog /NoSound
```

On detection of a spyware cookie, this command automatically deletes the spyware cookie without writing the spyware cookie deletion event to the log or generating any sound effects when a spyware cookie is detected – use of both these switches are strongly recommended in a corporate environment, given the large number of spyware cookie detection events that will be experienced on every system every day. No user intervention is required. Using Cookie Patrol in a login script on a Win9x system is not recommended; on these systems, it is preferable to leave the job of cleaning up spyware cookies to PPCL.

PPUPDATER

PPUpdater.exe ensures that PestPatrol components and scan strings are always up-to-date. Install PPUpdater.exe in the server event scheduler and schedule it to run it as frequently as you feel is appropriate. This must be done on the PDC and each BDC where PestPatrol might be invoked during a user login.

How PPUpdater works

PPUpdater retrieves a file called version.txt from PestPatrol's web site and compares the MD5 information for files in its directory with the MD5 information for this file. Any difference means the local copy needs updating. PPUpdater backs up any files that need updating, retrieves each file that it needs, and runs a test to ensure the update is good. It may be run in unattended or attended mode. PPUpdater always creates a log of actions taken at `\PestPatrol\Logs\PPUpdaterLog.txt`

Unattended use

In its unattended mode, invoked by PestPatrol.exe or a scheduler, PPUpdater will exit after completing its work, provided that you have invoked it with **/autoexit**. If this switch is not used, you will need to exit the process manually.

No notification of update

In certain installations, it might be desirable for the user not to be notified that PPUpdater has been run. To enable PPUpdater to run in the background, include the /silent switch.

Forcing a delayed start

You can invoke PPUpdater but ask it to wait a specified number of seconds before beginning. Do this with /wait=nnn where nnn is the number of seconds you wish it to wait.

Execute on close

You might want to run some process automatically when PPUpdater exits, such as distributing new files to other locations in your organization. Do this with **/RunAfter=xxx** where xxx is the name of the application you wish to run when PPUpdater exits.

Scheduling Updates

You can schedule updates using the Windows Task Scheduler under Windows 9x, or the AT command under Windows NT/2000:

Scheduling updates under Windows 9x

1. Double-click on **Add Scheduled Task** on the **Scheduled Tasks** list to invoke the wizard.
2. Locate PPUpdater.exe (normally in c:\Program Files\PestPatrol)
3. Enter a name for the task, for example PPUpdate.
4. Select the frequency for the task to take place.
5. Set the start date and time for the first instance of the task. The wizard presents a summary of your scheduled activity.
6. Click Finish to accept the scheduled task, or Back to go back and edit your choices.

Scheduling updates under Windows NT/2000

Windows NT has a built-in scheduler, which you can control by using the AT command to run PPUpdater automatically in the background (invisible mode) or in the foreground (interactive mode).

Make sure that the Schedule service is turned on:

1. Go to the Control Panel
2. Double click on the Services icon and select Task Scheduler
   If the Task Scheduler service's startup is not set to Automatic, do so by clicking on the Startup... button
   If the Task Scheduler service is not started, do so by clicking on Start.
3. Run Command Prompt
   Add programs to the scheduler using the following command syntax:

```
AT <time> /INTERACTIVE /EVERY:<dates> "<command>"
```

Example:
To run PPUpdater every Monday at 6:00 AM, enter at the command prompt:

```
AT 6:00 /interactive /every:M "[path to PPCL\]PPUpdater.exe
```

USING PESTPATROL IN A NETWARE ENVIRONMENT

This section provides the information required to install PestPatrol in a Novell NetWare server environment, and to invoke PestPatrol from a login script.

Syntax

All switches (see below) may be entered in any case (/Append, /APPEND, /append, /aPPEND, etc.).
Switches may be entered in any order.
Any amount of space may separate switches on a command line.
To ensure a full description of each event is written to the log file, the /info switch should be added to all command line scripts.

Procedure

Install PestPatrol on the shared Network drive (for example: `s:\`). To install the latest version of PestPatrol, use the installation CD provided, or download the latest version of PestPatrol from the web site.

NOTE: PestPatrol is installed by default to the C:\Program Files\PestPatrol directory. During the install process, use the browse feature to indicate that you wish to install PestPatrol to `s:` You must ensure that this folder (and all subfolders) are accessible by all users for execute, read and write. During a PestPatrol scan, a user must be able to read/write into the root folder, as well as to create/read/write into folders such as quarantine, logs, and any temporary folders used by PestPatrol.

Next, create a login script entry to invoke PestPatrol; the script will need these lines:

```
s:
cd\PestPatrol
start pestpatrolcl /info /wait=60 /noLogAfter /ignore /nosound /nopause
/emailto=SysAdmin@yoursite.com
```

If you also wish to invoke the MemCheck active memory scanner during the login process, add this line prior to the start pestpatrolcl command line:

```
start PPMemCheck /info /auto /delete /emailto=SysAdmin@yoursite.com
```

If you also wish to invoke CookiePatrol, add this line prior to the start pestpatrolcl command line:

```
Start CookiePatrol /NoLog /NoSound
```

Finally, to ensure that updates to PestPatrol are retrieved periodically, PPUpdater should be added to the event scheduler on the server. To run PPUpdater without user intervention, use the autoexit switch:

```
PPUpdater.exe /autoexit
```

The only requirement is that there must be an active Internet connection when PPUpdater runs, so that it can retrieve new components from the PestPatrol website.

Details of all available switches are provided elsewhere in this document.

A NOTE ON LOGS

The Master Log includes columns for Date/Time, the sequence number (the order in which events were added to the log), the MAC Address of the machine scanned, the user's login name, the file path, the name of the pest, its PVT, and the action taken. By clicking on any column header, the log is sorted on that column. A second click on that column header sorts again on that column, but in reverse order. Logs may be exported in CSV, HTML, XML, and text file formats.

SUPPORT

You should post technical support questions directly to our online helpdesk at http://helpdesk.pestpatrol.com, which is monitored 24x7; you should receive a reply within one business day. In an emergency, don't hesitate to call our toll free number 1 866-235-7163 x223 (1 717 243 6588 x223 from outside North America).

Latest information

The most recent information about the major components of PestPatrol can always be found at the following web pages:

For PPCL	http://www.pestpatrol.com/pestpatrolcl/
For PPUpdater	http://www.pestpatrol.com/ppupdater/
For PPMemCheck	http://www.pestpatrol.com/ppmemcheck/
For KeyPatrol.exe	http://www.pestpatrol.com/keypatrol/
For CookiePatrol.exe	http://www.pestpatrol.com/cookiepatrol/

Suspect files

If you have a suspicious file that PestPatrol does not identify as a known pest, please send it to us for analysis and, if appropriate, scan string updates. When you send the pest, please tell us what you know about it -- author, date of origin, how you obtained it, symptoms, etc. This will help us with the analysis. Send all suspicious files by email to our help desk at http://helpdesk.pestpatrol.com.

APPENDIX A: Running PPCL from the Microsoft Scheduler

The same powerful command line capabilities (PPCL) that allow PestPatrol to be run from a login server can also be used to run PestPatrol in automatic mode on/from the desktop under Windows 2000 and XP. There are several reasons you might wish to use this level deployment of PPCL:

- To demonstrate PestPatrol command line capabilities in a controlled setting
- As the recommended deployment for remote users on slow dialup connections.
- To run PestPatrol during off-peak hours or when it cannot be triggered by the user logging into the network.

1. From the Control Panel, click on Scheduled Tasks and Add a Scheduled Task. This will invoke the Scheduled Tasks Wizard.
2. Click next to continue, and then Browse to the PestPatrolCL.exe file located in the C:\Program Files\PestPatrol folder.
3. Click Open to place the file in the Scheduled Tasks Wizard.
4. Select the frequency with which you want PestPatrolCL to run.
5. User name and logon password are required to successfully run the task, so enter the appropriate user name and password.
6. Click Finish and check the box to Open Advanced Properties.
7. Add the appropriate switches PPCL should run in the RUN: text box. These switches should be entered after the program path text C:\Program Files\PestPatrol\PestPatrolCL.exe that already appears on the RUN: line. Use a space to separate each switch that you choose to deploy. Recommended and optional switches are described below.
8. Once the desired switches have been entered, click Apply or OK and re-confirm the login password, then click OK. The task will then appear in the list of scheduled tasks and PPCL will now run under the established commands. Close the scheduler and you are done!

If you have any questions about this process, please post them directly to our online helpdesk at http://helpdesk.pestpatrol.com,

Recommended switches

C: A drive path designation is required. If you wish to scan all hard drives on the machine, the **/hard** switch may be used. Start the command line with this switch (instead of C:\)
/wait=nnn causes the system to wait nnn seconds before loading CL to allow other processes to finish. This switch is typically used when scanning on boot.
/idle runs the program when the CPU is not busy.
/info provides information on pests detected.
/spycookie enables spyware cookie detection.
/nopause suppresses pop-up notification to the user when a pest is detected.
/nosound suppresses audio notification to the user when a pest is detected.

Optional switches

/extensions= specifies which types of file should be scanned. Each extension must be prefaced with ***.** and be separated by a semi-colon, for example:

```
extensions=*.exe;*.vbs;*.scr;*.doc;*.reg;*.com;*.bat;*.sys
```

If no /extensions= switch is provided, the default files scanned are: *.ADE; *.ADP; *.ASC; *.AMM; *.BAS; *.BAT; *.CHM; *.CMD; *.COM; *.CPL; *.CRT; *.DO; *.DOC; *.EXE; *.HLP; *.HTA; *.INF; *.INS; *.ISP; *.JS; *.JSE; *.LNK; *.MDB; *.MDE; *.MSC; *.MSI; *.MSP; *.MST; *.PCD; *.PIF; *.PL; *.REG; *.SCR; *.SCT; *.SHB; *.SHS; *.URL; *.VB; *.VBE; *.VBS; *.WSC; *.WSF; *.WSH; *.XL; *.XLS

/quarantine sends all pests to the Quarantine folder to allow time to review each detected pest while providing protection. Using the **/delete** switch is permanent and does not allow for pest risk level review.

/log=zzz allows the log to be saved to a named file rather than the default filename. The user must have full control of this file, not just read/write privileges. For example:

```
/log=h:\PestPatrollogs\username.txt
```

Remember quotes must be used to encapsulate a command that includes spaces, for example:

```
“/log=c:\Program Files\PestPatrol\Logs\username.txt”
```

/EMailto=yyy provides e-mail notification of the results from every machine running PPCL and using this switch, provided yyy is a valid e-mail address, for example:

```
/emailto=yourname@yourcompany.com
```

In order for this switch to work, MAPI must be enabled and unfettered access to the Internet available for port 25 (SMTP) traffic.

Example

```
"C:\Program Files\PestPatrol\PestPatrolCL.exe" c:\ /idle /info /SpyCookie
/nopause /nosound /quarantine “/log=c:\Program
Files\PestPatrol\Logs\username.txt”
/emailto=username@yourcompany.com
```