White Paper:
Using Lieberman Software's Tools to Quickly Detect and Remove Worms from all of your Systems

Rev 1– August 15, 2003

Written by Philip Lieberman (phil@lanicu.com)
Lieberman Software Corporation
http://www.lanicu.com

Abstract

This white paper gives step-by-step instructions to find and delete worms such as MS Blaster from all infected systems. The process consists of four steps that must be followed in order:

1) Identify which machines need the patch for the virus
2) Apply the patch to the machines that need it
3) Find all infected machines
4) Delete the virus from all infected machines.

Contents

1. Introduction

Welcome to the section of **Lieberman Software's** site demonstrating how to use our products to deal with the threat posed by the MSBlast worm.

The steps required to rid your systems of the virus and to protect them from further attack can be performed manually if you only have a few machines. The manual procedure can take up to half an hour for each machine, so if you have more than five machines you may wish to use an automated solution, such as Lieberman Software's **User Manager Pro** and **Task Scheduler Pro**. Not only are these powerful tools able to handle this virus, these products provide "heavy lifting" capabilities for doing mass management of your systems, including the management of local accounts/passwords, groups, registry and more. Please contact our Sales Department for more information on how our tools might help you with your network administration needs.

If you already have licenses for User Manager Pro and Task Scheduler Pro, you will be able to follow the steps in the following sections and stop the spread of the virus at no additional cost. If you are missing either of these products, you can download a demo version now. Without a license key, you can use the products for 30 days to manage up to 10 systems. If you wish to purchase these products you can contact our Sales Department.

2. Overview

Securing your systems involves three steps.

- Reporting to discover the extent of your vulnerability and infection
- Applying a Microsoft patch to remove the vulnerability
- Disabling the virus on machines that are already infected

NOTE: It is VERY important to carry out these steps in order, so that your machines do not become re-infected immediately before they can be patched. HOWEVER, if the machine is constantly rebooting, it may be a challenge to apply the patch. You may be forced to disable Internet access first, and then proceed with the steps below.

Step 1: Reporting on Infected Machines

Before applying any fixes, most organizations are interested in finding out which machines have already been compromised and which machines have received appropriate patches. You can use the reporting functions of Lieberman Software's User Manager Pro to determine which machines are infected as well as which have received the hotfix.

Step 2: Adding the Microsoft Hotfix

Removing the vulnerability requires the installation of a hotfix on each of your systems. This can be done very quickly using the "unattended installation mode" of service packs/hotfixes from Microsoft in concert with Lieberman Software's Task Scheduler Pro. With Task Scheduler Pro you can deploy the hotfix to thousands of machines in just a few minutes.

Step 3: Disabling the Worm

To disable the worm you can modify the registry of each infected machine so that the worm is no longer launched at boot time. User Manager Pro can be used to identify those machines that are infected by analyzing the registry of all of your machines. Once the infected machines are found, User Manager Pro can delete the problematic registry entry that causes the worm to start up every time your machines boot up, and can then reboot the infected machines to permanently shut down the worm.

3. MSBlast Worm Background

As you have probably heard there is a fast moving new virus known as the RPC/DCOM worm or MSBlast. According to Robert Lemost of CNET News.com, the virus had infected over 330,000 machines by 12:51 p.m. on August 14th. It appears to be spreading at the rate of 2,500 systems per hour. According to Lemost, this virus could infect a million computers in less than two weeks.

If you have used other vendors' mass management tools, you will be pleasantly surprised by the very low hardware and software requirements of Lieberman Software's products (standard Windows 2000 workstation with no other software required), and how they can handle very large sites at extremely high speeds. All of our products are highly optimized (MFC, C++, native-mode, multithreaded and UNICODE throughout) and tested for use in large environments. Contact us for more details and for a free evaluation and demo.

Historically, most viruses required the user to download a hostile program or open an email attachment to infect a machine. The latest worm can enter a user's machine at will if the machine is constantly connected to the Internet and lacks an appropriate firewall. Even with a firewall, a machine may still be infected by another machine on the LAN if the appropriate patches are not installed.

The virus is known by different names: MSBlast, W32/Lovsan (McAfee), WORM_MSBLAST.A (Trend Micro), Win32.Posa.Worm (Computer Associates), and W32.Blaster.worm. It was discovered on August 11, 2003 and its origins are currently unknown. The virus affects systems running any of the following Microsoft operating systems:

- Microsoft Windows Server™ 2003
- Microsoft Windows XP
- Microsoft Windows 2000
- Microsoft Windows NT 4.0
- Microsoft Windows NT 4.0 Terminal Services Edition

Machines running Windows 9x/ME are unaffected. An infected machine will have the file "msblast.exe" or one of its variants in the Windows SYSTEM32 directory. Infected machines may appear to be running very slowly and may reboot every minute or so. You may also receive errors about RPC services failing and see a message indicating the system must reboot.

If you want to investigate further you may notice the presence of unusual TFTP files and the opening of 20 sequential TCP ports (run command: NETSTAT -a) in the range 2500-2522. These are believed to be ports opened to allow remote control of your system by others.

You should be aware that Microsoft has rated this vulnerability as "Critical", meaning you must take immediate action to assure that your systems are protected and infected machines are brought under control.

Mitigating Factors

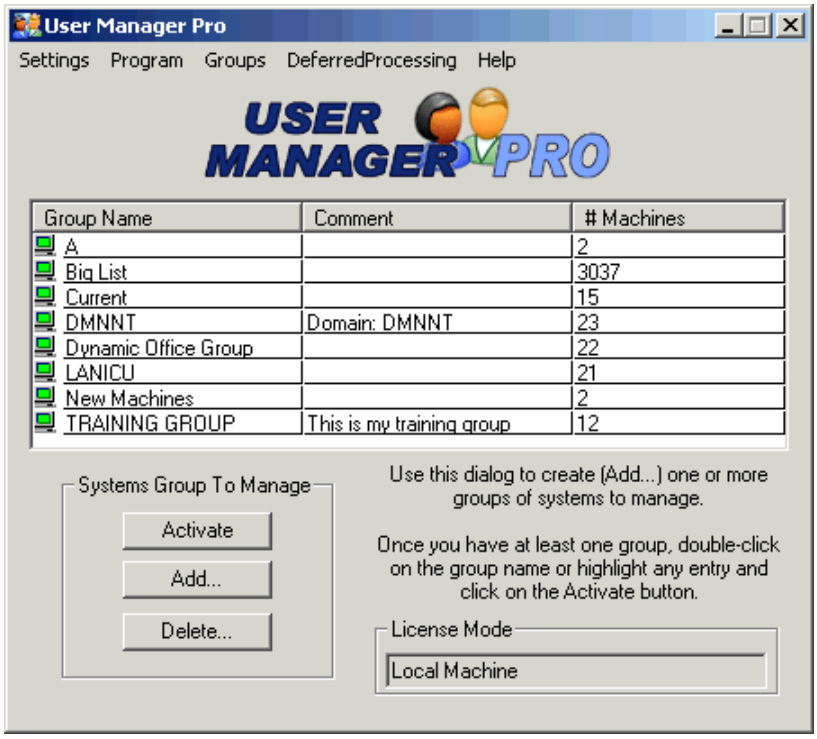
A secure firewall would minimize a vulnerable system's exposure to attacks from Internet-based hosts. In general, a firewall should block access to all RPC services except those that are specifically intended for use by untrusted users.

4. Determining Which Machines Have Hotfix for RPC/DCOM (MSBlast) Virus

Start User Manager Pro.

If you do not own **User Manager Pro** you can download a free demo that alows you to manage 10 systems for 30 days. If you need additional time or systems for your evaluation, please contact our Sales Department. You can also purchase the product on-line for the appropriate number of systems for your organization.

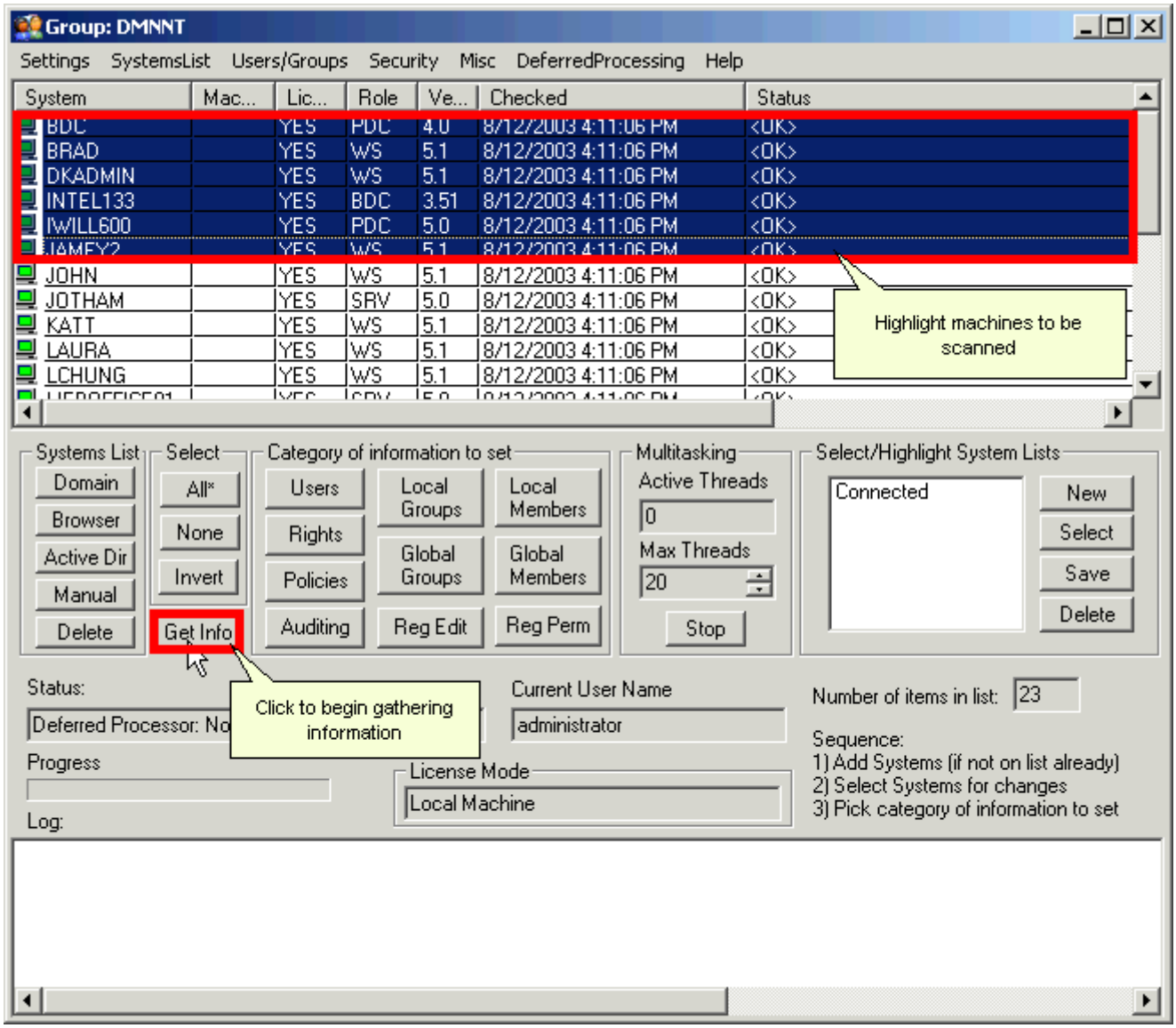
Once User Manager Pro is started, you should see the initial machine group screen. If you do not have any machine groups, you can create a new group to hold the list of machines to manage by clicking on the "Add..." button. Otherwise, just double-click on the group you want to examine.



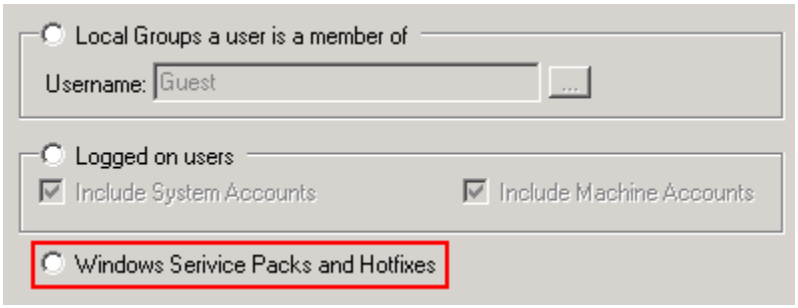
The hotfix that corrects the MSBLAST virus is known under the designation: KB823980. To determine which of your machines have the hotfix, highlight the list of machines to check and click on the "Get Info" button.

Highlight the list of machines to scan for the virus, or click on the "Select" | "All" button.

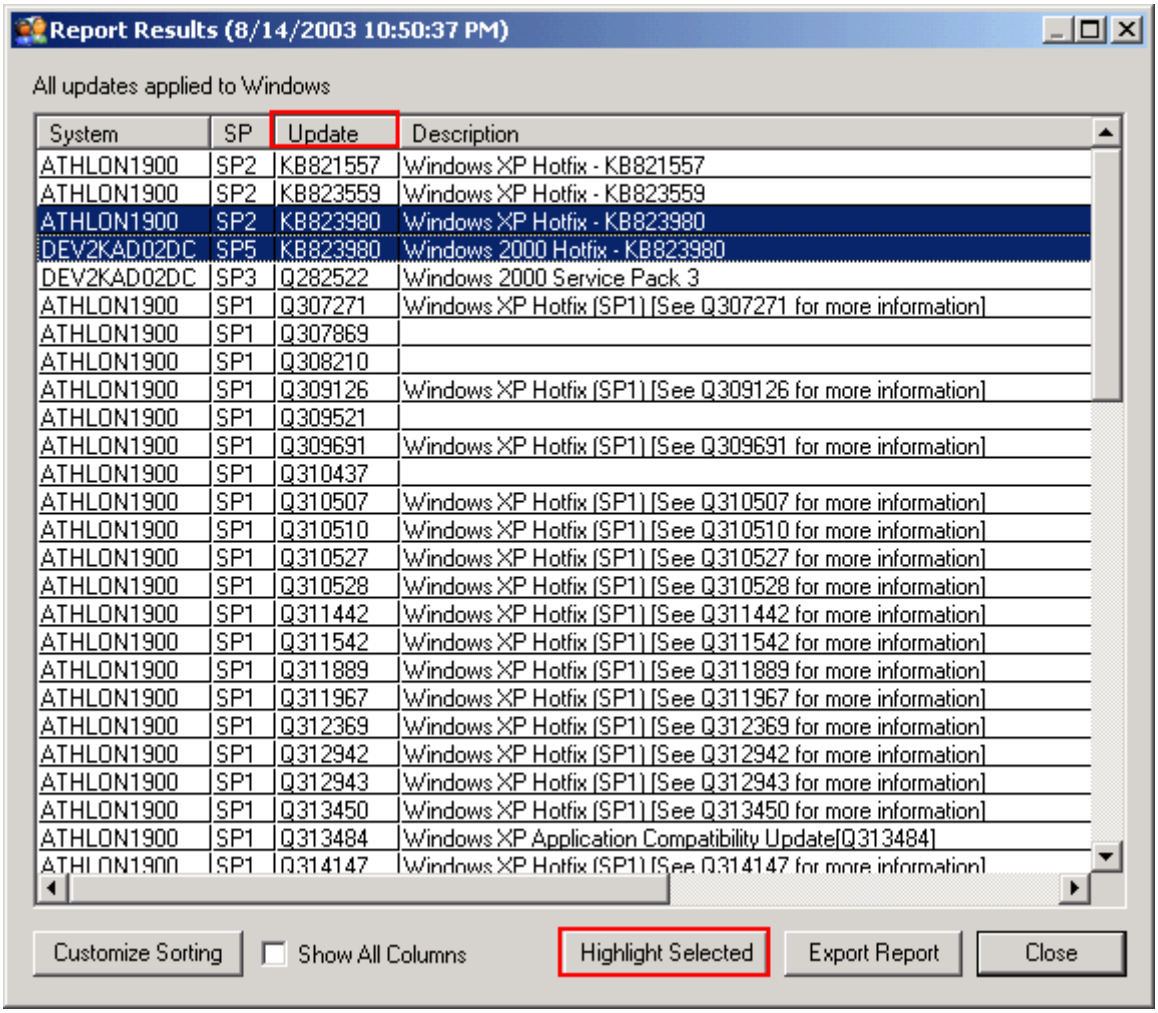
If you do not have any machines in your group, you can add them by going to the menu "SystemsList" and selecting one or more of the "Add..." menu options. You can also import a list of machines from a text file. More details are available via the on-line help.



Set the radio button on the "Windows Service Packs and Hotfixes" option.



Click on the "Report" button to generate a report of which service packs are installed.



Click on the "Update" header to sort the service packs by their designation. Find all of the entries designated as: "KB823980" and select/highlight them.

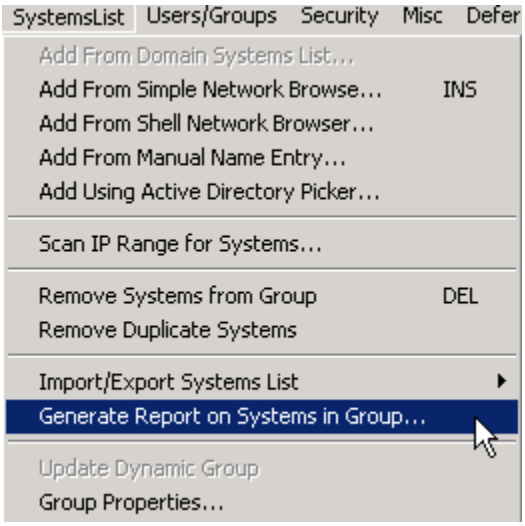
Click on the "Highlight Selected" button. This step will highlight all machines on the manage systems list that have the hotfix.

Click on the "Close" button.

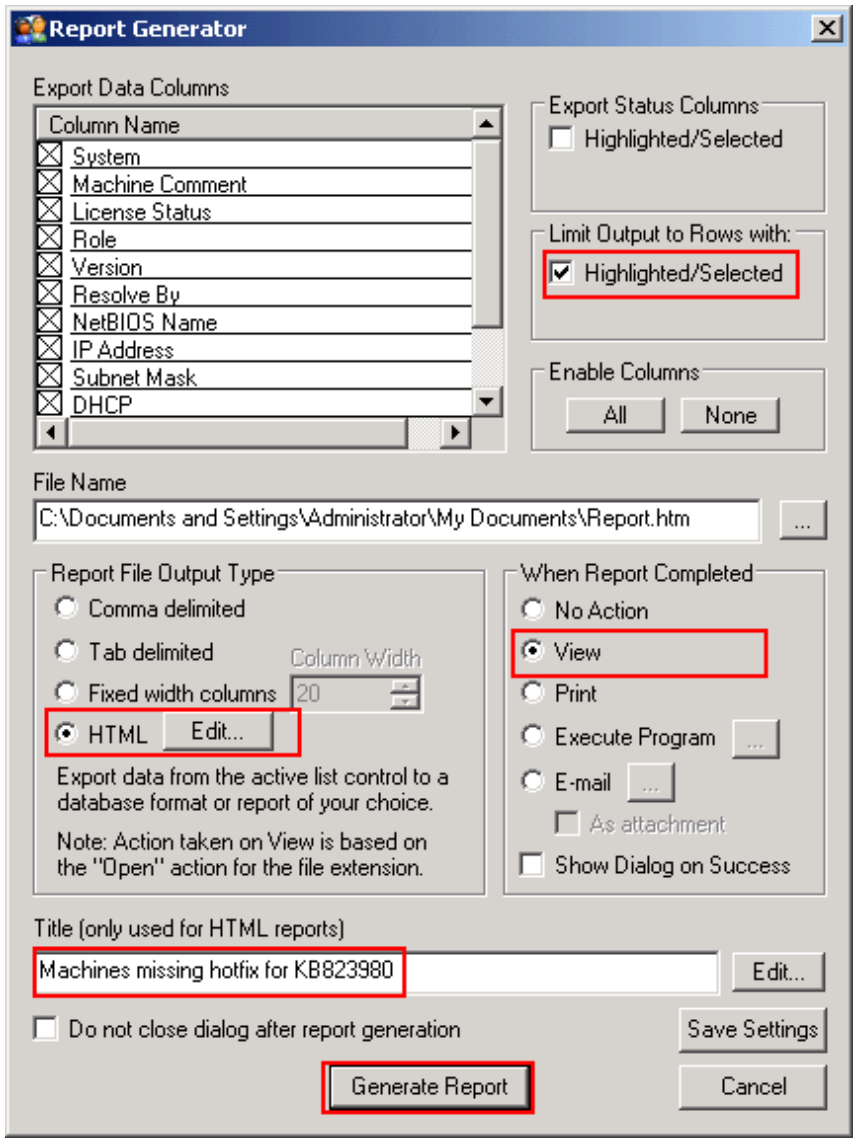
To see the machines that do not have the hotfix, click on the "Invert" button.

Note that all of the now highlighted machines are those that are lacking the hotfix, or were not tested, or were off-line.

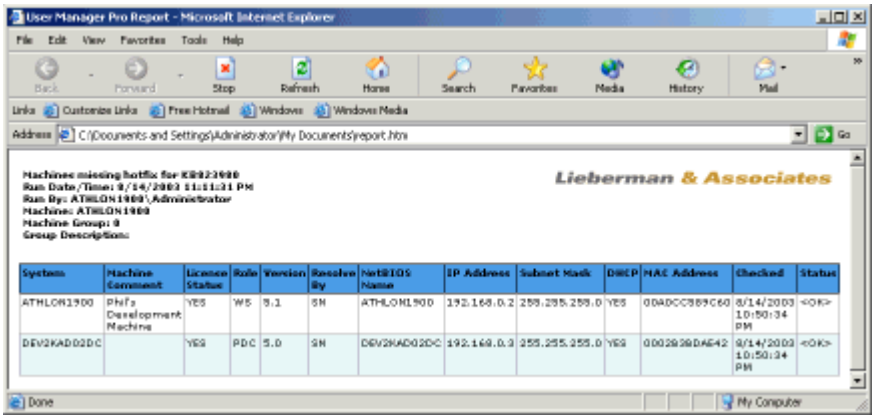
You can generate a report of the resulting machines by going to the menu option: "SystemsList" | "Generate Report on Systems in Group..."



The program will pop up a dialog that allows you to export this information. To limit the output to only those machines that are highlighted, set the checkbox: "Limit Output to Rows with" | "Highlighted/Selected". To generate a nice HTML report, set the "Report File Output Type" to "HTML". Set the "When Report Completed" to "View" to cause your web browser to launch with the data. You can customize the HTML report by editing the text in the "Title" field.



Click on the "Generate Report" button. In a few moments you will see a web page with the data.



5. Applying Microsoft Patches with Task Scheduler Pro

The MSBlast worm, also called the RPC/DCOM vulnerability, requires that you install a specific version of the patch for each platform you are patching. **Task Scheduler Pro** allows enables you to copy the appropriate platform specific patch to each of your systems, execute the patch in an unattended manner, and reboot the systems remotely without any further action on your part.

Task Scheduler Pro allows administrators to deploy patches across their enterprise much faster than distribution systems like Microsoft SMS. Patch tasks can be created on all of your systems simultaneously, and they begin executing on your systems almost immediately. In a virus outbreak situation, speed is essential.

Preparation - Download Patches

First download the patches you will need from the Microsoft web site and store them in a common and convenient location on your local machine. Task Scheduler Pro will copy these files to your systems. The following section provides lists of file names and specific links to the Microsoft web site to download each patch. For the sake of easy installation, these should be all stored in a common location on your local workstation.

When this guide was written the current files were named as follows:

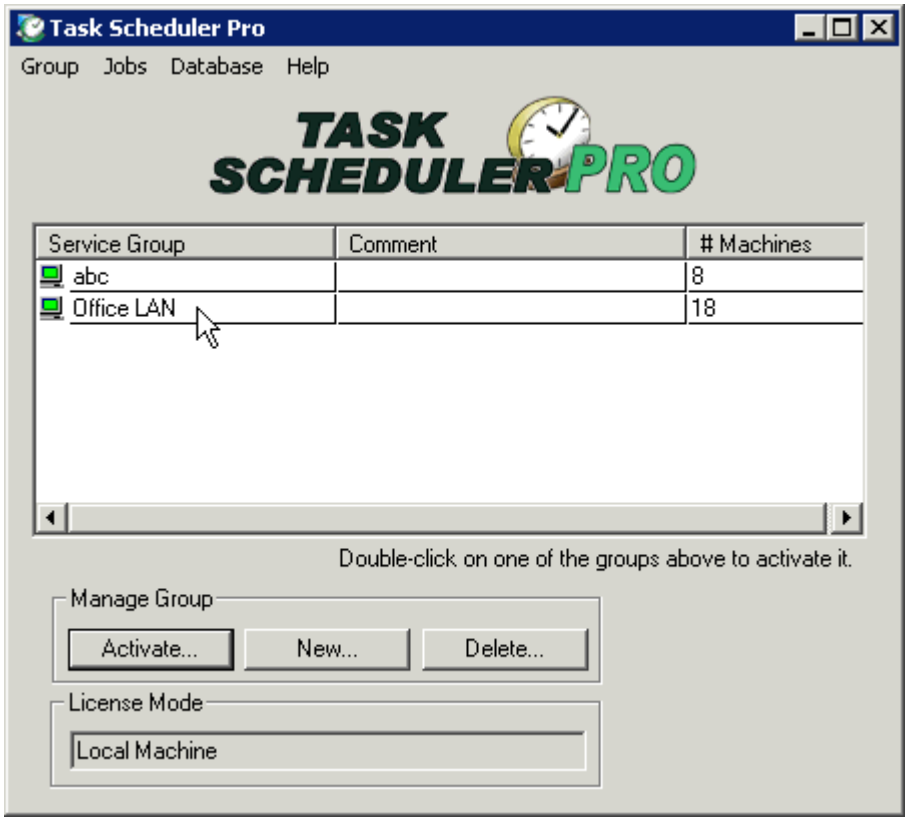
Windows NT 4.0 Server File Name: Q823980i.EXE
Windows NT 4.0 Terminal Server Edition File Name: Q823980i.EXE
Windows 2000 File Name: Windows2000-KB823980-x86-ENU.exe
Windows XP 32 bit Edition File Name: WindowsXP-KB823980-x86-ENU.exe
Windows XP 64 bit Edition File Name: WindowsXP-KB823980-ia64-ENU.exe
Windows Server 2003 32 bit Edition File Name: WindowsServer2003-KB823980-x86-ENU.exe
Windows Server 2003 64 bit Edition File Name: WindowsServer2003-KB823980-ia64-ENU.exe

Patching Your Systems with Task Scheduler Pro

Start Task Scheduler Pro.

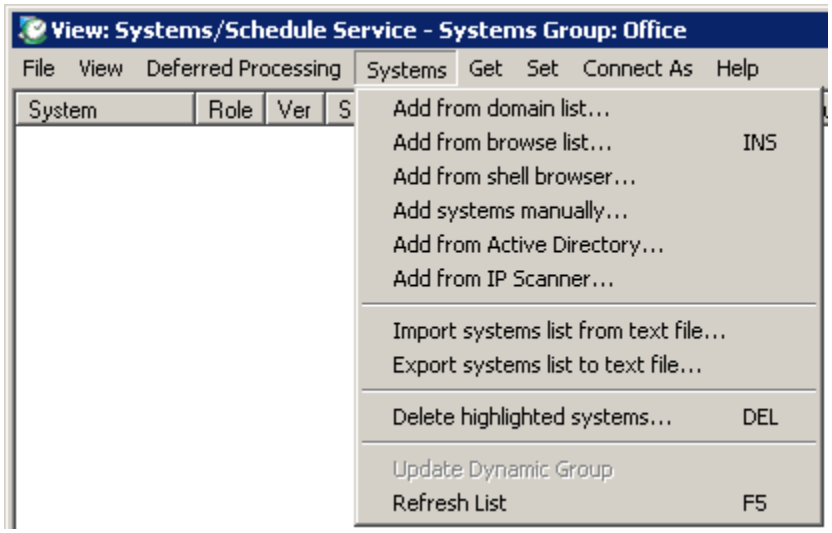
If you do not own Task Scheduler Pro you can download a free demo that alows you to manage 10 systems for 30 days. If you need additional time or systems for your evaluation, please contact our Sales Department. You can also purchase the product on-line for the appropriate number of systems for your organization.

When the program starts running you will see the group management window. This window allows you to create a named group of systems to manage. If you already have systems in a group, just double-click on the group name. If you are just starting, click on the "New..." button and give your group of systems a name.

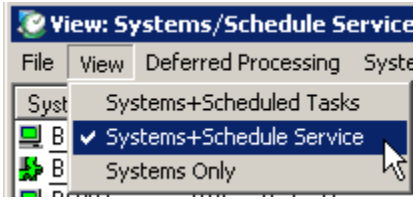


Add Systems to Your Machine List and Confirm that the Scheduler is Running on All Targets

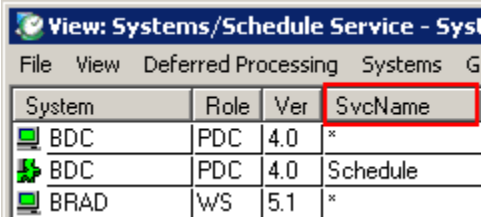
You will need to tell Task Scheduler Pro the names of the machines you want to patch. You can create a list of machines by going to the "Systems" menu and using one of the different "Add" options. You can also import a list of machines previously exported by User Manager Pro.



In order to install remote tasks, the Task Scheduler service must be running on all of your target machines. To verify the running state of the services as well as your administrative rights to these machines, go to the "View" menu and select the "Systems+Schedule Service" menu option.



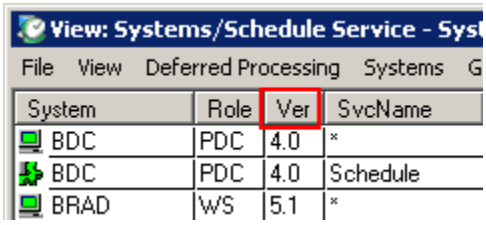
Perform a refresh on the service status on all of the systems by highlighting them and pressing the F5 key. The program will then refresh the state of each machine as well as the service status. To separate the different information (services and machine status), click on the "SvcName" column.



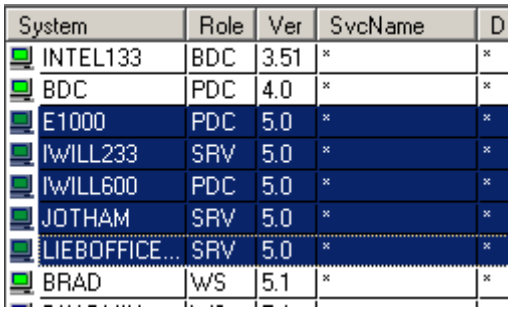
Make sure that the scheduler service is running (scroll down where the SvcName is not an asterisk (*) on all systems. If it is disabled, you can highlight the disabled services and use the right-click context menu to enable/start the services.

Organize Machines By Operating System Version

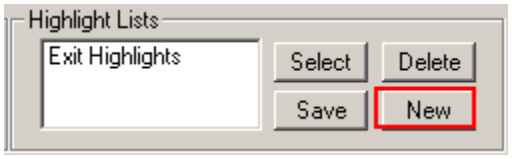
Sort the list of systems by operating system version. Click on the "Ver" column to perform the sort operation.



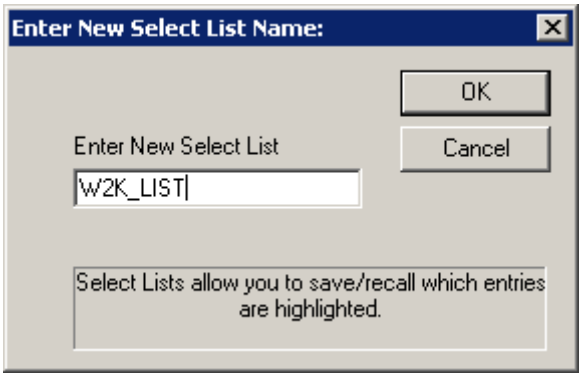
Version 4.0 is NT 4.0, 5.0 is Windows 2000, 5.1 is Windows XP, and 5.2 is Server 2003. Note that you will be creating different tasks for different versions of the operating system and then running them remotely.



We will be using the "Highlight Lists" feature of Task Scheduler Pro. This feature allows us to memorize highlighted groups of entries. Make sure you highlight all of the systems (systems have asterisks in the service field for machines) of each operating system version as a set and use the "New" button to save the set under an appropriate name (i.e. NT_LIST for 4.0 systems, W2K_LIST for 5.0 systems, and so on).



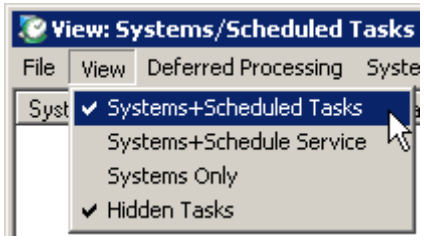
In this example you will save the list of Windows 2000 systems by entering the new name and clicking on the "OK" button.



For the sake of convenience you should select the highlight "None" button and then create different Highlight Lists for all of the different operating system versions in your environment. Below is the highlighted entries for the XP_LIST.

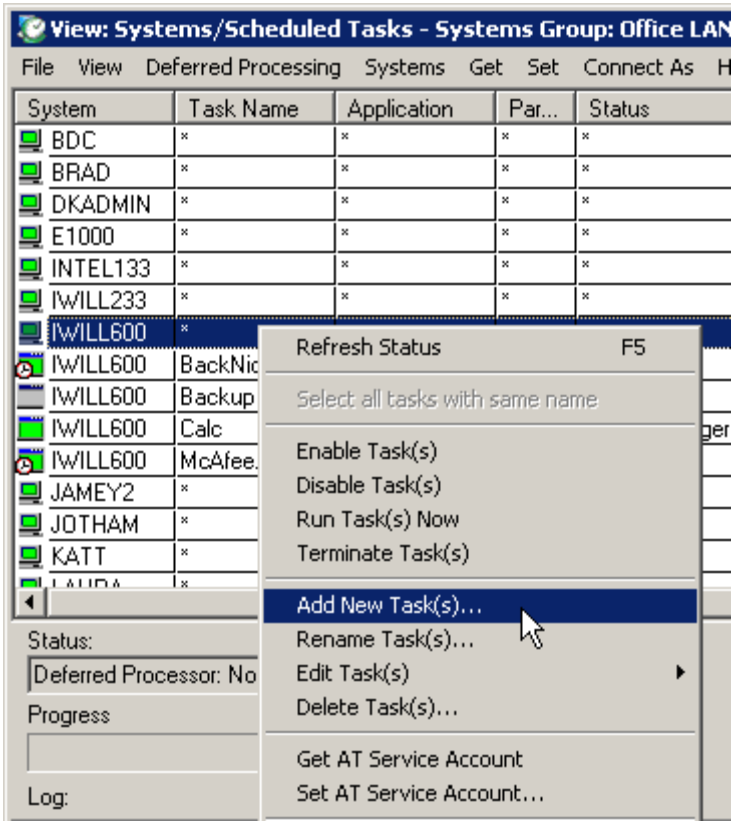
Create & Distribute Patch Task to a Group of Systems

Switch to the Tasks view by clicking on the menu option: "View" | "Systems+Scheduled Tasks".

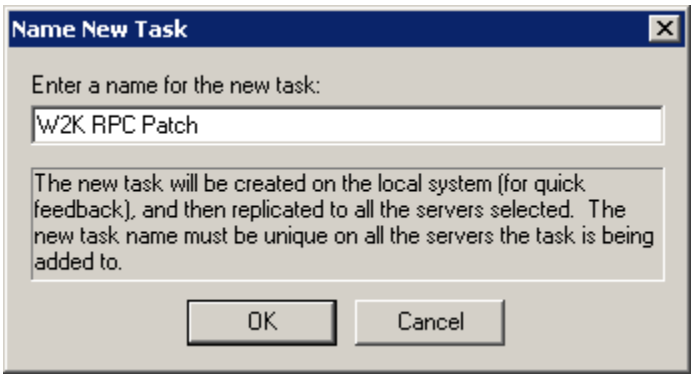


Decide which patch you want to do first. In this example we will do Windows 2000 systems. Double-click on the "W2K_LIST" highlight list to highlight all of the Windows 2000 systems.

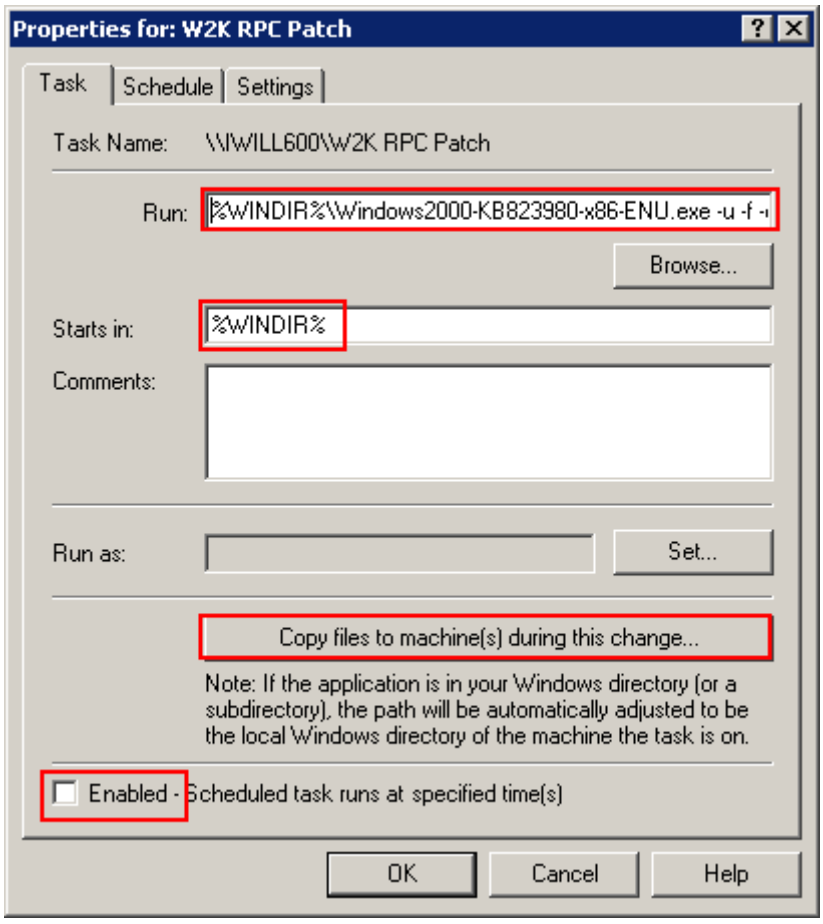
Right-click on one of the highlighted entries and select the "Add New Task(s)..." option.



Enter the name of the patch being distributed to all of the machines. We are using the "W2K RPC Patch".



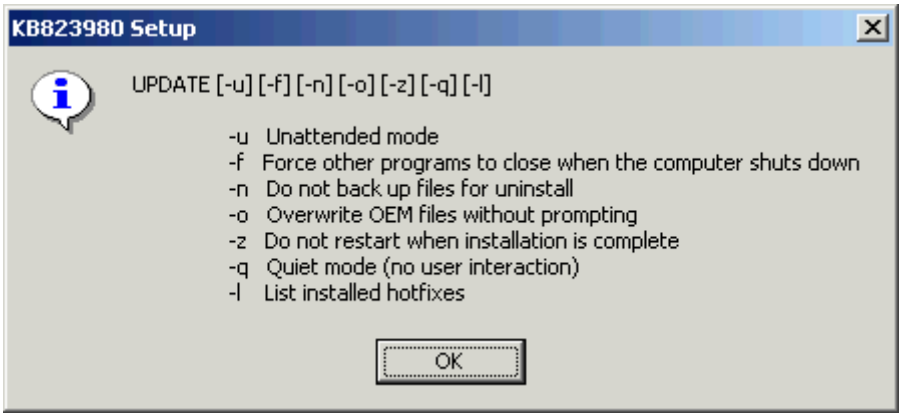
Set the "Run" field with the program name with path and command lines.



We set the "Run" string to:

```
"%WINDIR%\Windows2000-KB823980-x86-ENU.exe -u -f -o -q -n"
```

The command line arguments are based on the options available for updates. Depending on your circumstances you may want to select different command line options.

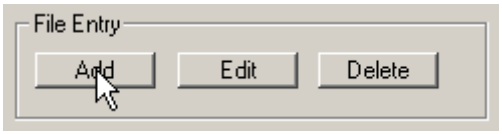


Set the "Starts in" field to "%WINDIR%.

Set the "Enabled" checkbox (at the bottom of the dialog) to unchecked. You will be starting the task manually a little bit later.

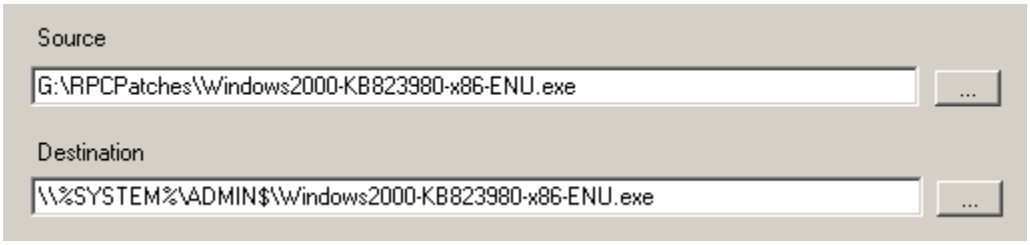
Click on the "Copy files to machine(s) during this change" button. We can copy the patch file(s) to the remote machine as part of the task creation process.

Click on the "Add" button to specify the file transfer parameters.

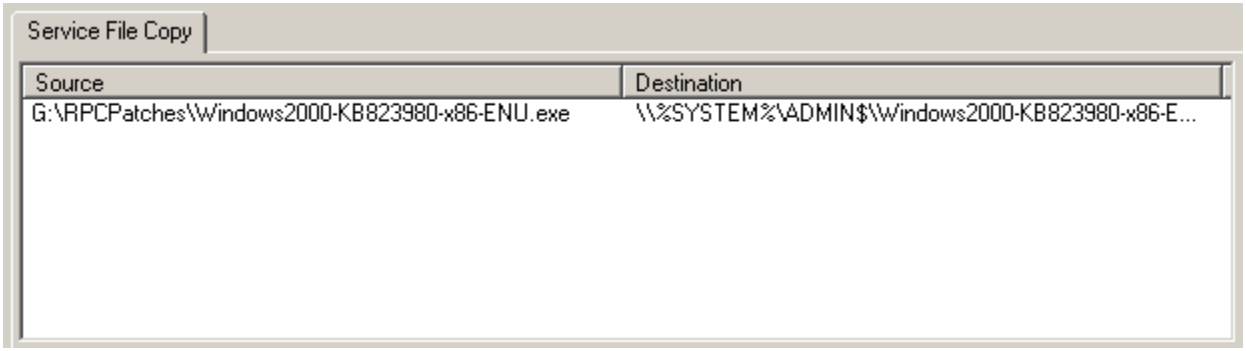


Use the top ellipse ("...") button to set the path to the patch file on your local machine. For the destination, use:

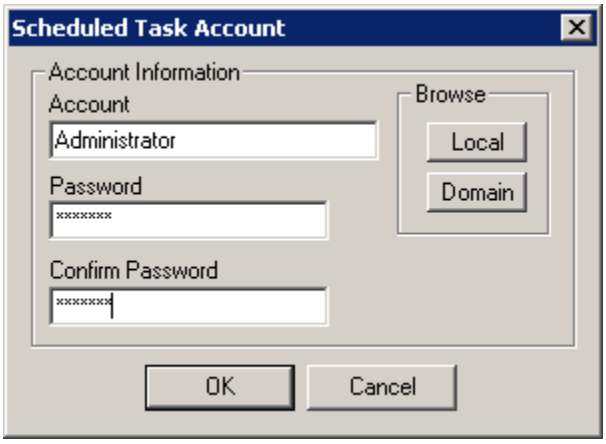
\\%SYSTEM%\ADMIN$\YourPatchFileName



When you view the file list you should see the fixed source path and the variable destination path. Note that the file name at the end of both paths (source and destination) must be identical.



Click on the "OK" button to launch the creation process. As part of the task creation, you will be asked to provide credentials for the new tasks. The credentials provided must be seen as an administrator on each local machine.



Running Remote Patch Tasks

Double-click on the highlight list name for your group of systems. Right-click and select the "Run Tasks Now".

After a few moments, you should get a confirmation in the Status that the task is running on all of your machines. Your patches are now running. You should give them about 10 minutes to complete.

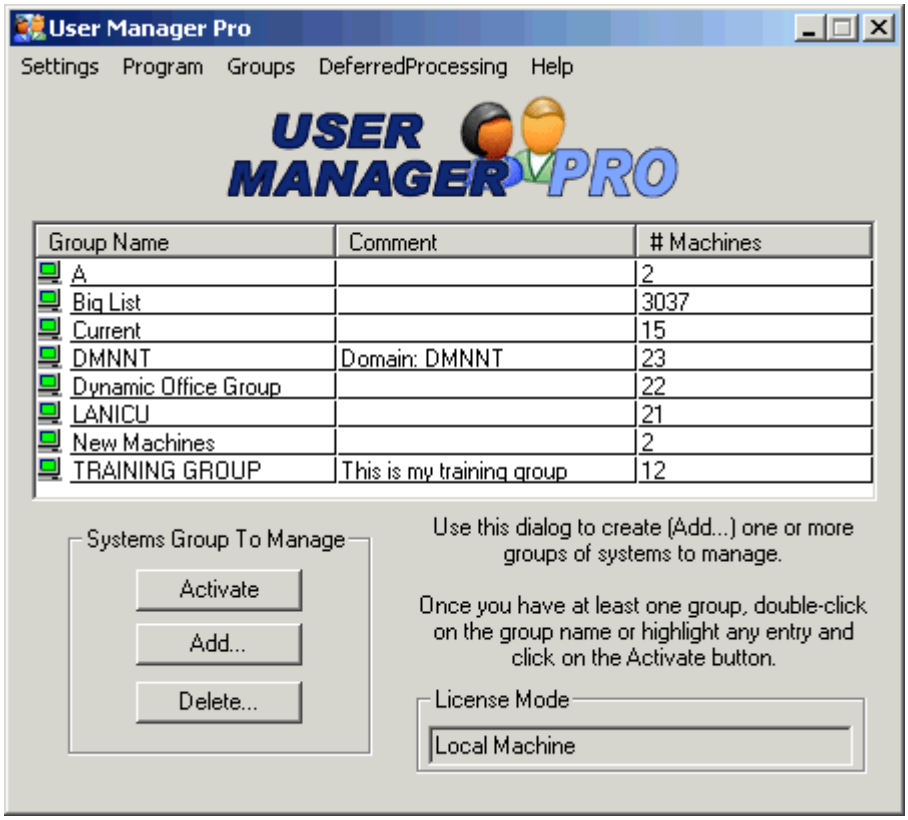
6. Finding and Disabling a Virus Launched by the Registry Run Key

After your systems have been patched, you must find and cleanse systems that have been infected. Lieberman Software's **User Manager Pro** allows you to quickly find and dinsinfect all of your compromised systems.

Start User Manager Pro.

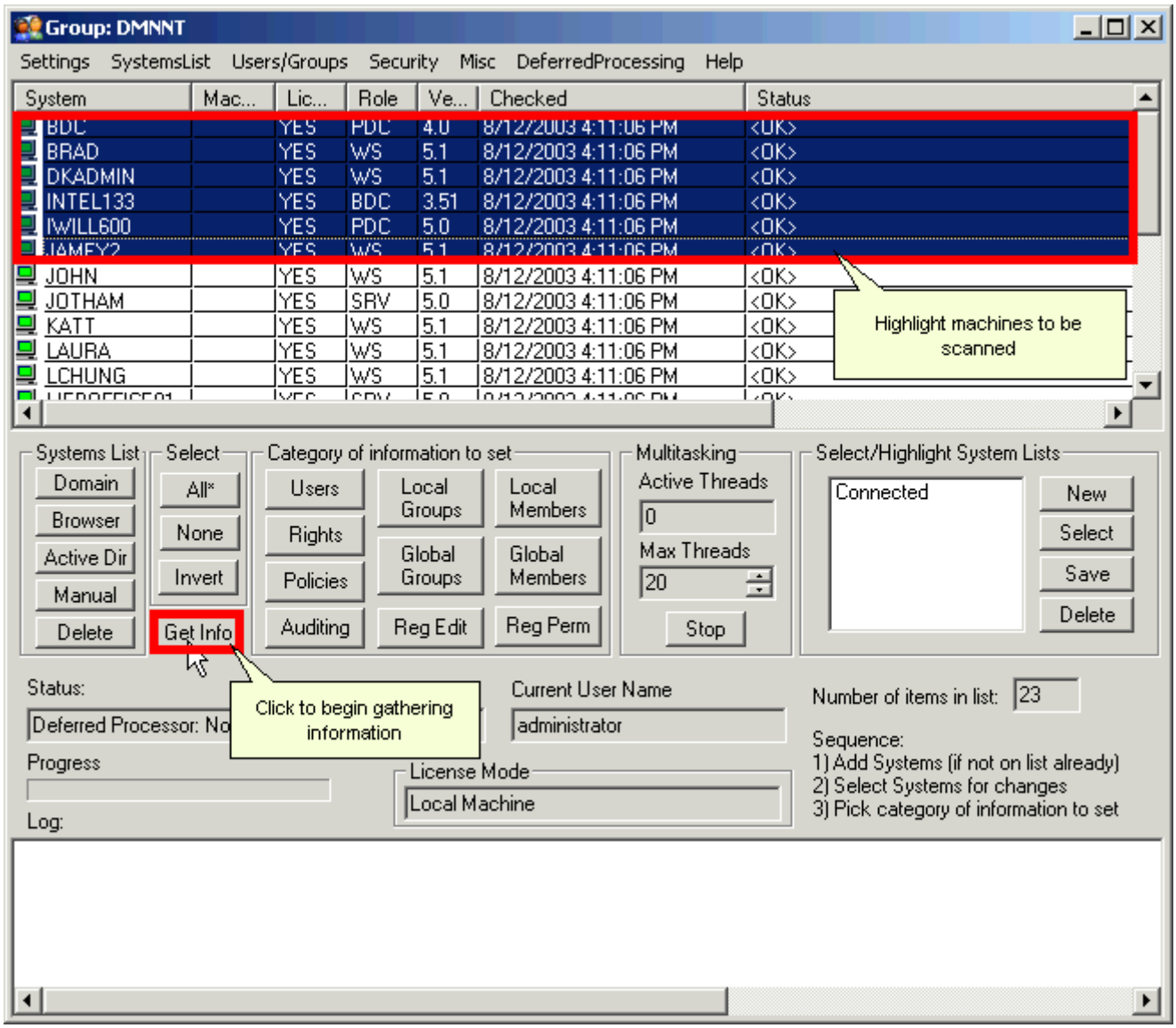
If you do not own User Manager Pro you can download a free demo that alows you to manage 10 systems for 30 days. If you need additional time or systems for your evaluation, please contact our Sales Department. You can also purchase the product on-line for the appropriate number of systems for your organization.

Once User Manager Pro is started, you should see the initial machine group screen. If you do not have any machine groups, you can create a new group to hold the list of machines to manage by clicking on the "Add..." button. Otherwise, just double-click on the group you want to work with.



Highlight the list of machines to scan for the virus, or click on the "Select" | "All" button.

If you do not have any machines in your group, you can add them by going to the menu "SystemsList" and selecting one or more of the "Add..." menu options. You can also import a list of machines from a text file. More details are also available via the on-line help.



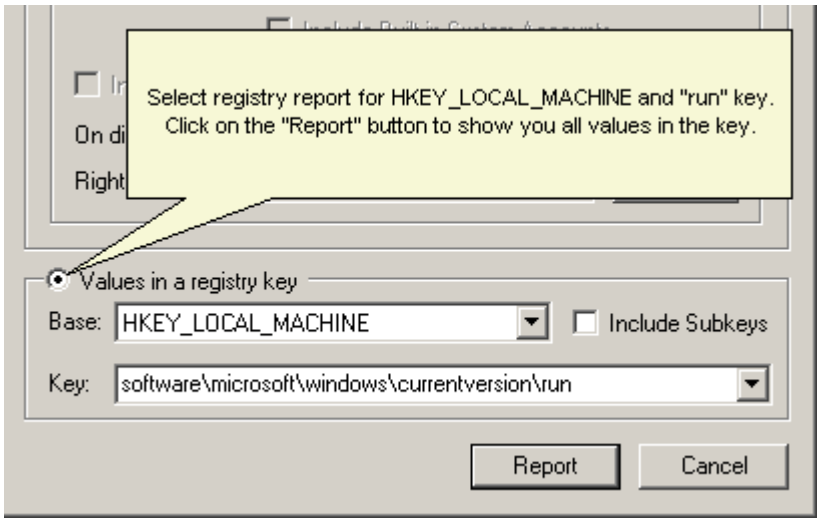
Next, click on the "Get Info" button to begin reporting on your infected machines.

In the "Report On..." screen, click on the radio button in the lower right of the dialog to select reporting on the registry of your highlighted machines. Make sure that the "Base" key is set to the

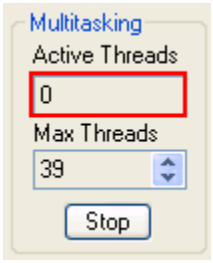
"HKEY_LOCAL_MACHINE". Next, use the drop down list to find the key (this is preloaded for you), SOFTWARE\Microsoft\Windows\CurrentVersion\Run. Note that capitalization is not important.

Tip! Highlight the "Key" string and capture it to the keyboard for later use (Control + C).

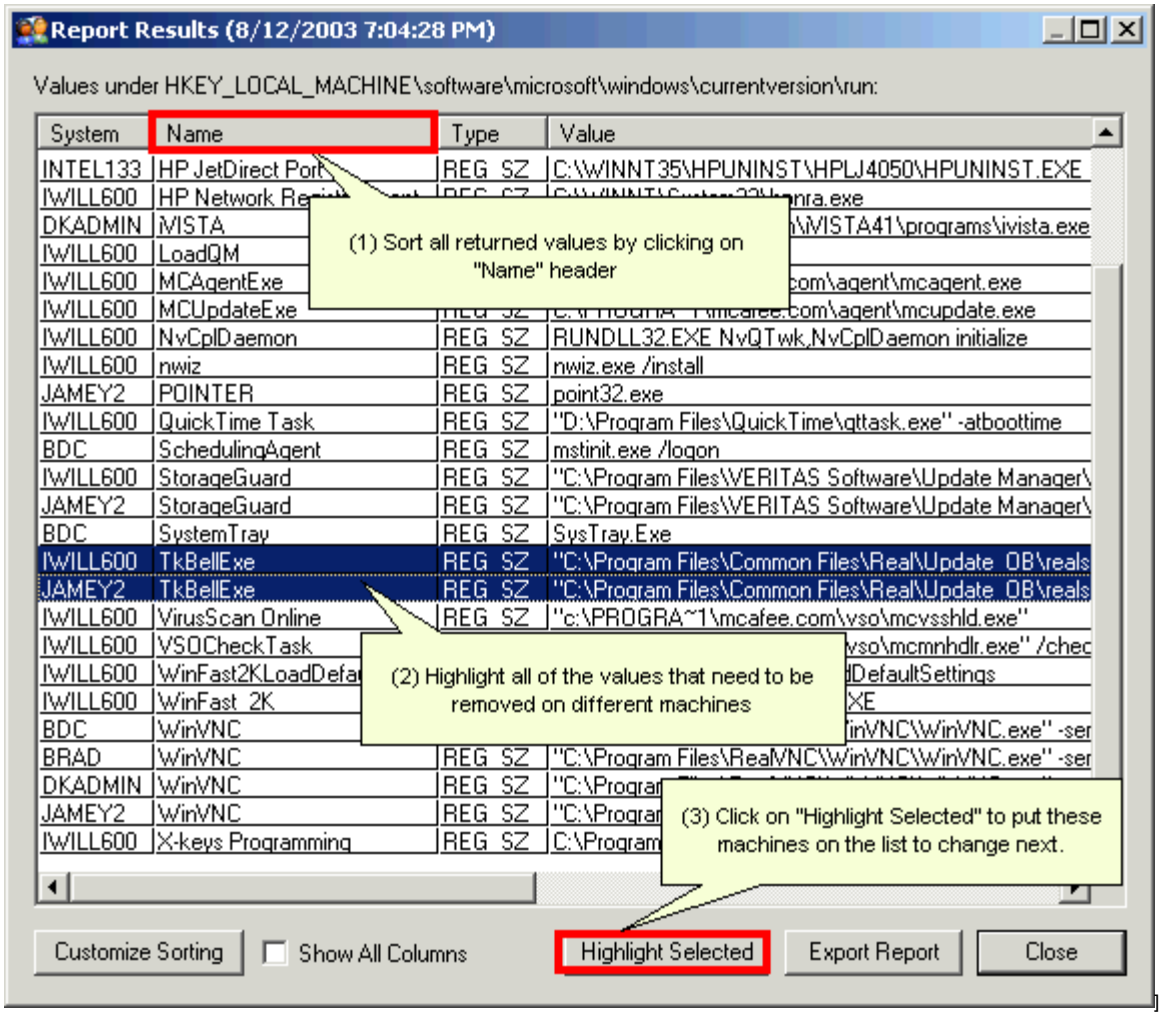
Click on the "Report" button to scan all of your machines. This will take a little bit of time to complete.



Tip! Keep an eye on the "Active Threads" counter on the main screen. When it gets down to zero, the next window will appear.



When the scan has completed you will see a window similar to the screen below. All of the values are grouped by machine. This report can be used to find autostarting programs on all machines.



To find the virus, click on the "Name" header to sort the values.

Any machine that has an entry in the "Name" column that says "windows auto update" is infected. The value can be "msblast.exe", "msblast.exe I just want to say LOVE YOU SAN!! bill" or "teekids.exe" or other entries. **You can delete the "windows auto update" value/name on all machines that contain it.**

Highlight all of the name entries that contain "windows auto update" then click the "Highlight Selected" button. This step highlights all machines that have the values you highlighted.

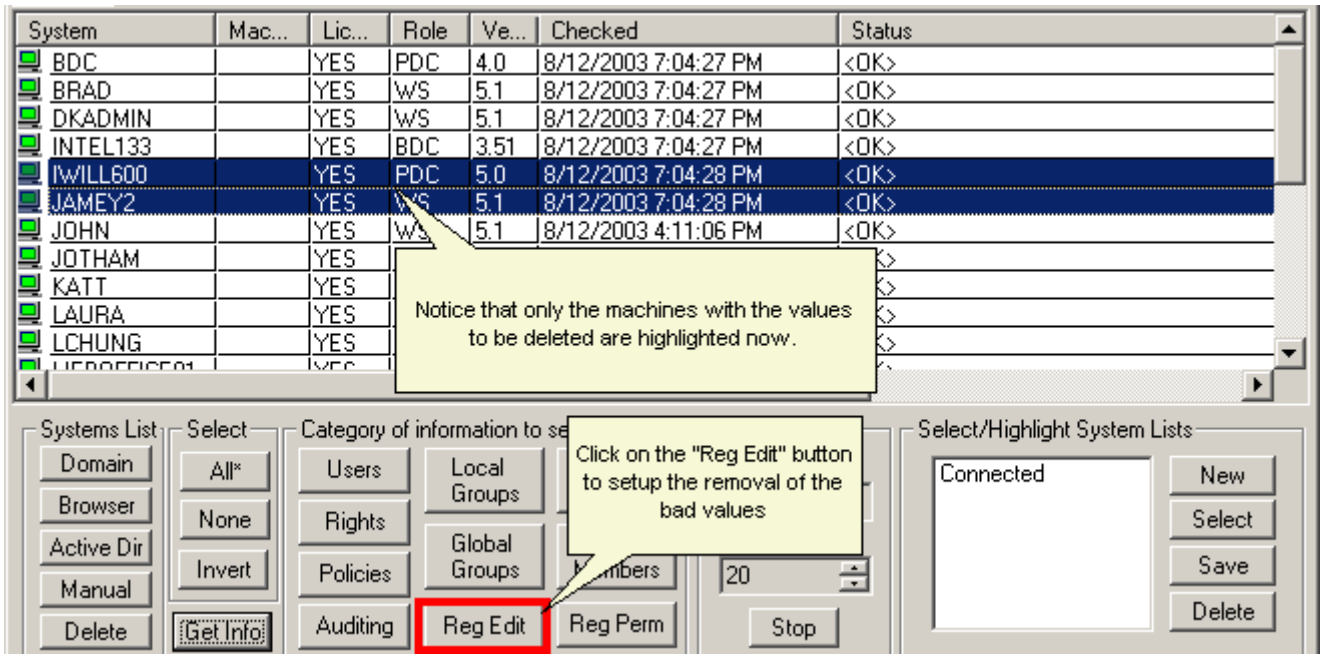
Disinfecting Machines

NOTE: To secure systems from the MSBlast virus, you must apply hotfix MS03-026 to insulate machines from further infection BEFORE attempting to disinfect your systems as described on this page. If you have not yet done so, follow the procedure described in **Using Task Scheduler Pro to deploy this hotfix**

Click on the "Close" button to begin the process of deleting the value that launches the virus.

After the dialog closes, notice that some of your machines are now highlighted. These are the machines that will receive the registry change.

Click on the "Reg Edit" button.



Set the radio button marked, "Single Key/Value". This dialog allows you to make registry changes.

Set the "Key" to **"HKEY_LOCAL_MACHINE"**.

Set the Key "Action" to "No Change to Key". **DO NOT SET THE KEY ACTION TO DELETE. ONLY THE BASE VALUE NEEDS DELETION.**

Place the mouse in the "Subkey" field and paste in the path that was previously copied. You can enter the path manually:

software\microsoft\windows\currentversion\run

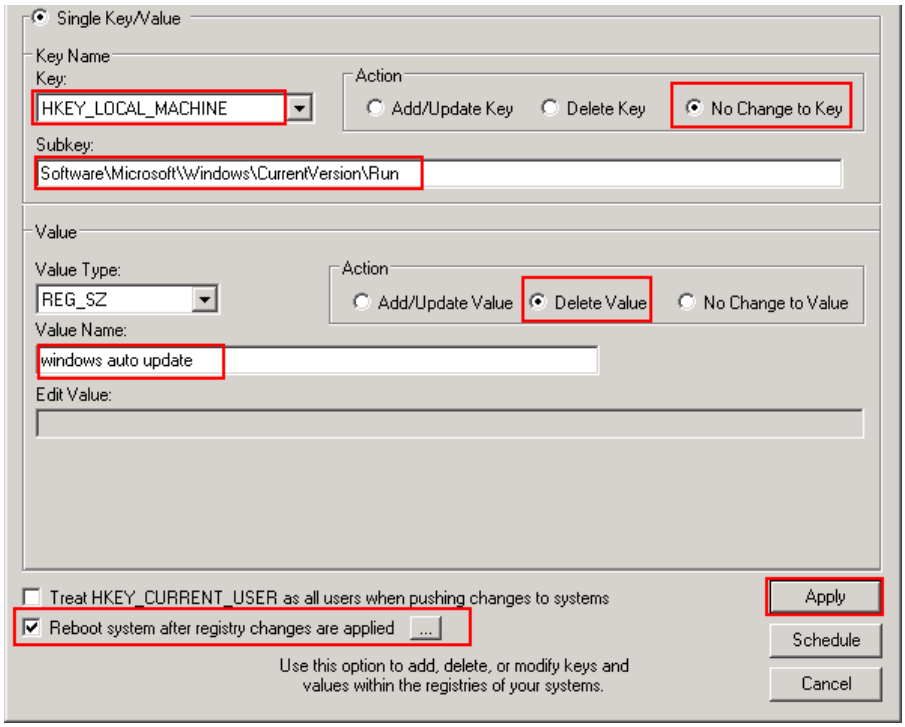
Set the "Action" field for the Value to "Delete Value".

Set the "Value Name" to **`"windows auto update".`**

Set the checkbox on the "Reboot system after registry changes are applied". Set the ellipse ("...") to the right of the checkbox to set the countdown time to an acceptable reboot delay time after the registry change has been made.

Note: The "reboot after change" function is available on ***User Manager Pro*** Version 4.63 and later. If you have an earlier version, perform the registry change as described, then highlight the same machines and select the reboot option on the program's context menu (right-click).

Click on the "Apply" button to zap the value and reboot the machine.



When the operation is completed on all of the machines you will get the following pop-up dialog.

Congratulations, your systems have now been secured!

Our support staff is available to answer your technical questions whether you are a customer or not.

Voice: 800.829.6263 (USA/Canada) Voice: (01) 310.550.8575 (Worldwide) Fax: (01) 310.550.1152 (Worldwide)
Web: www.lanicu.com Email: support@lanicu.com

Microsoft GOLD CERTIFIED Partner

