

White Paper:
Using User Manager Pro to Detect and
Defeat the Virus Known as:
W32/Mydoom@MM, Novarg,
W32.Novarg.A@mm, Win32/Shimg, or
WORM_MIMAIL.R

Rev 0 - January 27 2004

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

Abstract

This white paper gives step-by-step instructions on how to detect and defeat the W32/Mydoom@MM Virus, using Lieberman Software's User Manager Pro

Contents

1. Introduction	3
2. Background	3
3. Finding Infected Machines	4
4. Producing an Infection Report	5
5. Save List of Infected Machines	7
6. Pushing and Executing a Virus Removal Tool on Infected Systems– Automated Fix Process	8
7. Locking Out (Cratering) Infected Files – Manual Fix Process	9
8. Rebooting Infected Machines	10
9. Deleting Registry Entries Added by Virus – Removing DoS Component	11
10. Deleting Registry Entries Added by Virus – Removing Extraneous Registry Keys	12
11. Fixing the Registry Entry that Modifies the Shell	13
12. Final Notes	14

1. Introduction

The recent outbreak of the W32/Mydoom@MM virus has been causing havoc due to its clever social engineering as well as the slight delay in time before virus protection was available. Using User Manager Pro[®] from Lieberman Software you can quickly discover and remove this threat.

The virus also is known under the following names:
Novarg (F-Secure), W32.Novarg.A@mm (Symantec), Win32.Mydoom.A (CA), Win32/Shimg (CA), WORM_MIMAIL.R (Trend).

Click [here](#) and [here](#) for a description of the virus.

2. Background

User Manager Pro has many features used in the day-to-day mass management of Windows NT, 2000, XP and Server 2003 systems. We will be using a small subset of User Manager Pro's functionality to perform the following tasks (manual virus removal):

- Find infected machines by looking for an entry created by the virus.
- Use the Cratering function within User Manager Pro to disable the executable components of the virus by modifying their ACLs (Access Control Lists). This serves to disable the virus and inhibit further infection. More details on this technique can be found [here](#).
- Removal of Registry keys/values associated with the virus.
- Reboot infected systems.

User Manager Pro also has the ability to push a prepackaged virus removal executable via this "Push/Run" feature. In that case you would:

- Find infected machines by looking for an entry created by the virus.
- Push/Run a fix program provided by one of many anti-virus vendors to all of the systems.
- Reboot all systems later if necessary.
- Prepare a post fix report after the fixes have run.

There are advantages and disadvantages of using the "Push/Run". There is less work for you to do, but the fix program does not attempt to correct damage done to the registry by the virus, only remove bad entries. There is also the potential problem that the Scheduler Service in your remote systems may not be running or configured correctly to take remote jobs (not likely, but possible).

On the other hand, the fix program does remove the requirement of a reboot and can potentially take less time. The fix program also scans all files and removes infected files on your system. You can also mix the techniques so that the fix program is run and the User Manager Program can be used to verify the repair has taken place and the appropriate registry areas can be fixed via the REGEDIT file push feature in User Manager Pro.

3. Finding Infected Machines

All infected machines will have an entry in the keys:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

For the value:

TaskMon = %SysDir%\taskmon.exe

User Manager Pro can prepare a report of all machines that have this value indicating that they are infected. This information can be distributed to your team as an HTML report and the information can be used to create a list for repair (steps covered in this paper).

We assume that you have used User Manager Pro previously and have created a list of machines to scan for the virus. If you have never used the product before, please [click](#) here for information that will assist you in getting started:

- 1) Start User Manager Pro.
- 2) Activate an existing group of systems or create a new group and populate it with systems. Details are in the previously mentioned [link](#) or contact us for assistance at sales@lanicu.com.
- 3) Highlight all the machines to test for the virus infection:

System	Ma...	Lic...	Role	V...	Checked	Status
BDC		YES	PDC	N...	1/27/2004 4:23:24 PM	<OK>
BRAD		YES	WS	XP	1/27/2004 4:23:24 PM	<OK>
CHANNON		YES	WS	XP	1/27/2004 4:23:24 PM	<OK>
DELL		YES	WS	XP	1/27/2004 4:23:24 PM	<OK>
DEVNT4wKST		YES	WS	N...	1/27/2004 4:23:24 PM	<OK>
DKADMIN		YES	WS	XP	1/27/2004 4:23:24 PM	<OK>
E1000		YES	PDC	w...	1/27/2004 4:23:24 PM	<OK>
INTEL133		YES	BDC	3...	1/27/2004 4:23:24 PM	<OK>
IWILL233		YES	SRV	w...	1/27/2004 4:23:24 PM	<OK>
IWILL600		YES	PDC	w...	1/27/2004 4:23:24 PM	<OK>
JAMEY2		YES	WS	XP	1/27/2004 4:23:24 PM	<OK>
JOHNN		YES	WS	XP	1/27/2004 4:23:24 PM	Basic Connect Failed: 53 - The network path...

- 4) Click the "Get Info" button. 
- 5) Select the Registry Reporting area and the Run key.

Values in a registry key

Base: Include Subkeys

Key:

- 6) Click on the “Report” button. Wait for the information to be retrieved (this will take a little time).
- 7) After the report appears, click on the “Name” header to sort by value name.

System	Name	Type	Value
--------	------	------	-------

- 8) Scroll through the list looking for any entries in the “Name” field with the name: “TaskMon”. Highlight only these entries (if any) using CTRL+Left Mouse Click or any other selection method you like.

If you have no entries with the “TaskMon” value, none of the scanned machines have the virus and you can close the program.

System	Name	Type	Value
SLIM	Roulette Tray Monitor	REG_SZ	C:\PROGRAM FILES\ROULETTE\ROULETTE TRAY
BDC	SchedulingAgent	REG_SZ	mstinit.exe /logon
DEVNT4WKST	SchedulingAgent	REG_SZ	mstinit.exe /logon
IWILL600	StorageGuard	REG_SZ	"C:\Program Files\VERITAS Software\
JAMEY2	StorageGuard	REG_SZ	"C:\Program Files\VERITAS Software\
LORI	StorageGuard	REG_SZ	"C:\Program Files\VERITAS Software\
SCROSS	StorageGuard	REG_SZ	"C:\Program Files\VERITAS Software\
SLIM	StorageGuard	REG_SZ	"C:\Program Files\VERITAS Software\
STEVE	StorageGuard	REG_SZ	"C:\Program Files\VERITAS Software\
LAURA	SunJavaUpdateSched	REG_SZ	C:\Program Files\Java\j2re1.4.2_03\bin
SLIM	SunJavaUpdateSched	REG_SZ	C:\Program Files\Java\j2re1.4.2_03\bin
BDC	SystemTray	REG_SZ	SvsTray.Exe
DEVNT4WKST	SystemTray	REG_SZ	SvsTray.Exe
SALES01	SystemTray	REG_SZ	systray.exe
LINDA	TaskMon	REG_SZ	C:\WINDOWS\System32\taskmon.exe
IWILL600	TCRemoteAgent	REG_SZ	"c:\Program Files\Automated QA\Test
JOTHAM	TCRemoteAgent	REG_SZ	"C:\Program Files\Automated QA\Test
IWILL600	TkBellExe	REG_SZ	"C:\Program Files\Common Files\Real
JAMEY2	TkBellExe	REG_SZ	"C:\Program Files\Common Files\Real
LORI	TkBellExe	REG_SZ	"C:\Program Files\Common Files\Real
NICK	TkBellExe	REG_SZ	"C:\Program Files\Common Files\Real
PAT	TkBellExe	REG_SZ	"C:\Program Files\Common Files\Real
RANDY	TkBellExe	REG_SZ	"C:\Program Files\Common Files\Real
BRAD	VirusScan Online	REG_SZ	"c:\PROGRAM FILES\mcafee.com\vsos\mc
CHANNON	VirusScan Online	REG_SZ	"c:\PROGRAM FILES\mcafee.com\vsos\mc
IWILL600	VirusScan Online	REG_SZ	"c:\PROGRAM FILES\mcafee.com\vsos\mc
JAMEY2	VirusScan Online	REG_SZ	"c:\PROGRAM FILES\mcafee.com\vsos\mc

- 9) Click on the “Highlight Selected” button on the bottom of the dialog to record the list of infected machines.

Highlight Selected

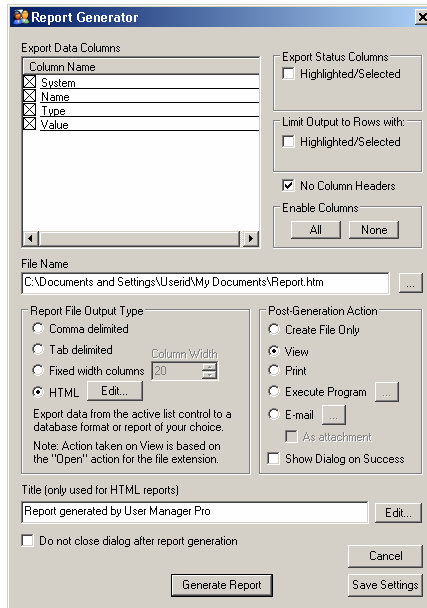
This step will highlight only the infected machines on the initial machine list for the group (they were all initially highlighted when you began).

4. Producing an Infection Report

- 1) To produce a report on the infected machines, click on the “Export Report” button located at the bottom of the dialog.

Export Report

2) You will then see a dialog similar to the following:



3) Set the “Output Type” to “HTML”, set the “Post Generation Action” to “View” or “Email” depending on where you want the output to go. If you will be using the EMAIL option, you will need to configure the recipients list as well as the SMTP output settings. You can send the page via the browser also.

4) If you only want to export the highlighted entries (machines with the infection), check the box: “Limit Output to Rows with Highlight”. Click on the “Generate Report” button.

Generate Report

5) After a few moments you will either generate the report (picture on next page is to demonstrate the output format, not actual data):

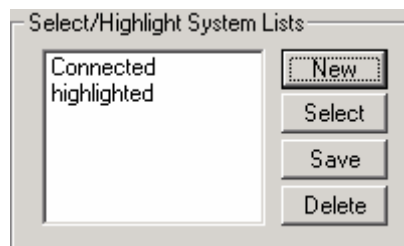
Report generated by User Manager Pro
 Run Date/Time: 1/28/2004 12:27:46 PM
 Run By: INTEL3000\Administrator
 Machine: INTEL3000
 Machine Group: 0
 Group Description:

Lieberman & Associates

INTEL3000	NvCplDaemon	REG_SZ	RUNDLL32.EXE C:\WINDOWS\System32\NvCpl.dll,NvStartup
INTEL3000	nwiz	REG_SZ	nwiz.exe /install
INTEL3000	Cmaudio	REG_SZ	RunDll32 cmicnfg.cpl,CMICtrlWnd
INTEL3000	PRONMgr.exe	REG_SZ	C:\Program Files\Intel\NCS\PROSet\PRONMgr.exe
INTEL3000	X-keys Programming	REG_SZ	C:\Program Files\PIEngineering\X-keys\XKWdkApp.exe
INTEL3000	VSOCheckTask	REG_SZ	"c:\PROGRAM~1\mcafee.com\vso\mcmnhldr.exe" /checktask
INTEL3000	VirusScan Online	REG_SZ	"c:\PROGRAM~1\mcafee.com\vso\mcvsshld.exe"
INTEL3000	MCAGENTEXE	REG_SZ	c:\PROGRAM~1\mcafee.com\agent\mcagent.exe
INTEL3000	MCUPDATEEXE	REG_SZ	C:\PROGRAM~1\McAfee.com\Agent\mcupdate.exe
INTEL3000	type32	REG_SZ	"C:\Program Files\Microsoft IntelliType Pro\type32.exe"
INTEL3000	QuickTime Task	REG_SZ	"C:\Program Files\QuickTime\qttask.exe" -atboottime

5. Save List of Infected Machines

- 1) After the report has been generated (optional activity) and control has been returned to the dialog that lists all of the highlighted (infected) systems, click on the "New" button within the "Select/Highlight Systems List" area.



- 2) Enter the name "Infected Mydoom" and click the "OK" button. We can now highlight the list of infected machines by double-clicking on this name in the list box.

6. Pushing and Executing a Virus Removal Tool on Infected Systems – Automated Fix Process

Click [here](#) for a manual fix program that is available from Symantec.

To push the fix program use the following steps:

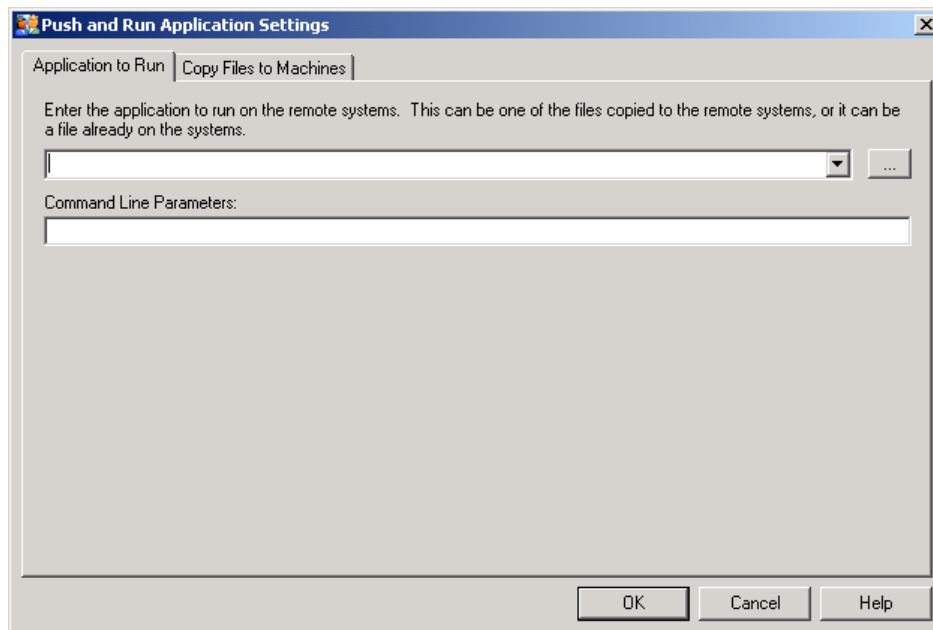
- 1) All machines that are to receive the fix should already be highlighted. If not, use the previously recorded highlight list (i.e. “Infected Mydoom”).
- 2) Use the menu option:
Misc | Push/Run Application...
- 3) You will be on the “Application to Run” tab page.
- 4) Fill out the parameters for the application (assuming the use of the Symantec fix tool to be located on the C: drive of targeted systems):

Application:

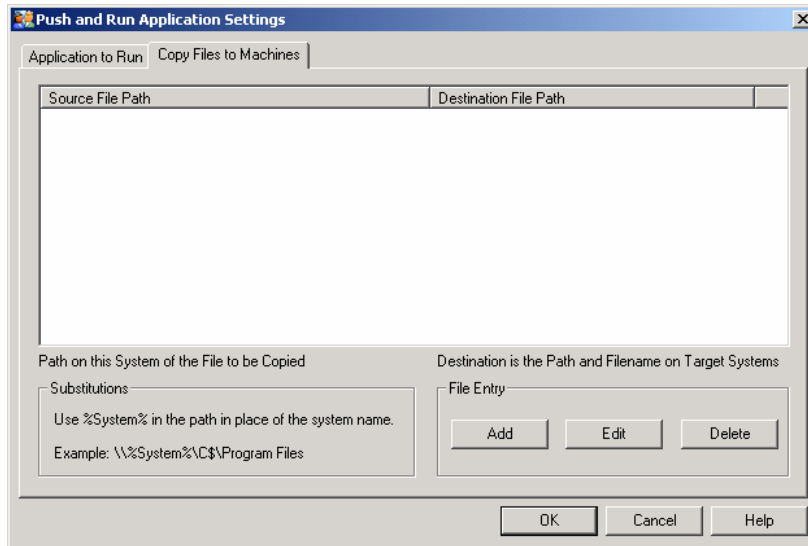
C:\FxFovarg.exe

Command Line Parameters:

/SILENT /EXCLUDE=M:\ /LOG=c:\FxFovarg.txt



- 5) Click on the “Copy File to Machines” tab.



- 6) You will need to provide the list of files to transfer as part of the application. After downloading the fix file from Symantec or your preferred vendor, click on the “Add” button to create a file copy list entry.

Use the following parameters (change these depending on your specific installation):

Path of File on Local Machine:

D:\Downloads\FxNovarg.exe

Path of File on Remote Machine(s):

\\%System%\C\$\FxNovarg.exe

- 7) Click on the “OK” button to begin the file transfer and run process.

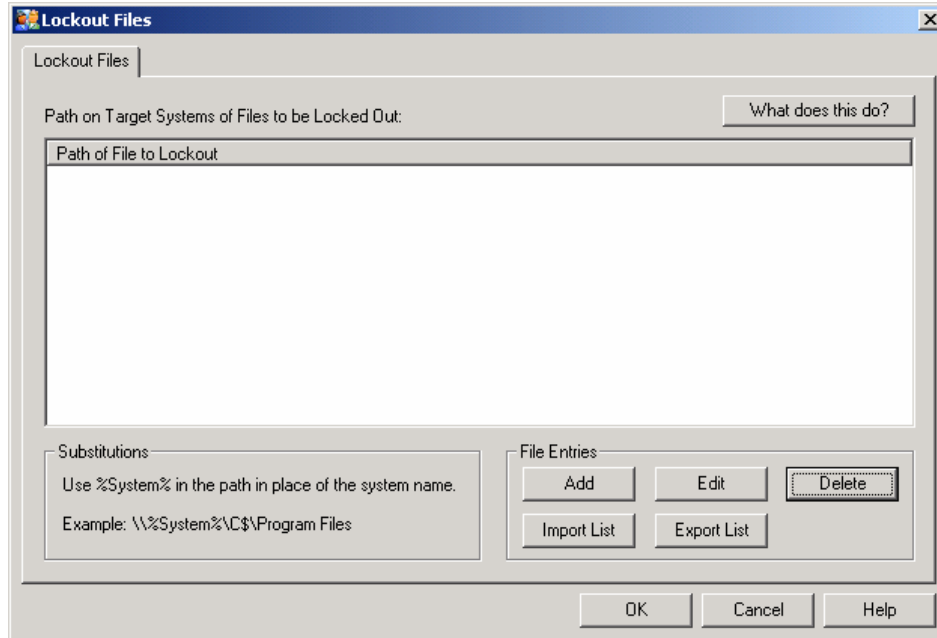
Note: Push and Run creates a one-time AT scheduled task on your remote systems using the default account for the Scheduler Service (usually LocalSystem). If you wish to push and run this type of repair file with more control and monitoring, please take a look at our [Task Scheduler Pro® program](#). With Task Scheduler Pro you can run the fix under any account you wish and periodically check on the job status.

Note: You can check on the success of the repair process on your remote systems by running the registry report previously described after allowing sufficient time for the repair process to run.

7. Locking Out (Cratering) Infected Files – Manual Fix Process

The following will allow you to disable the files that are part of the virus. By disabling the files you will stop all virus activity after rebooting. These steps modify the Access Control Lists (ACLs) on the virus components so that they can no longer run.

- 1) Go to the menu option: “Misc | File Operations | File Lockout.”



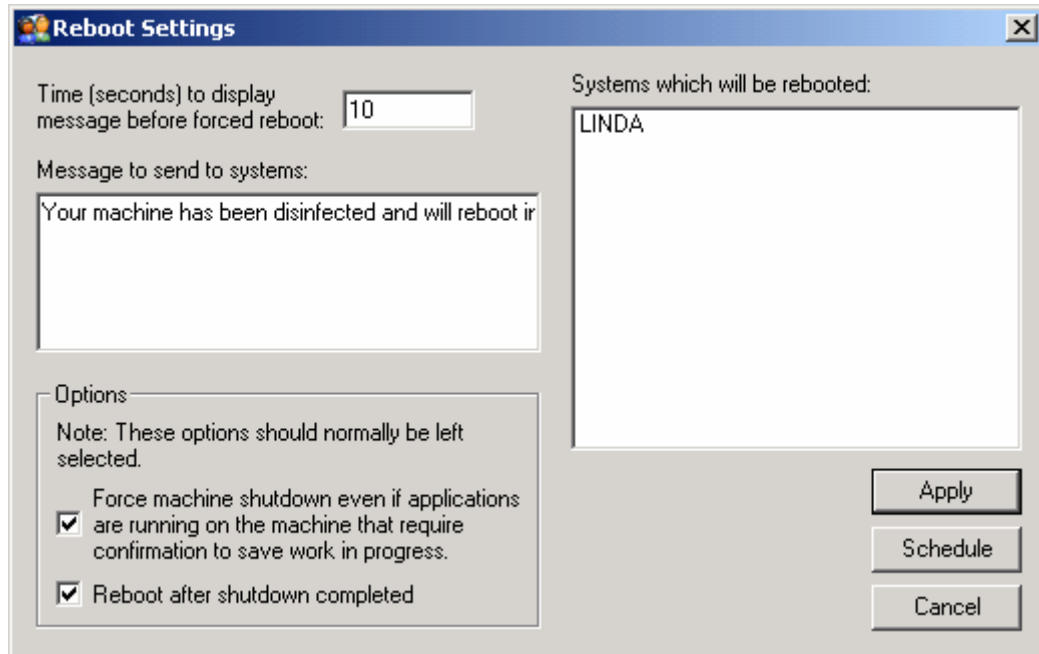
- 2) Click on the “Add” button and add the entries:
%Windir%\System32\shimgapi.dll
%Windir%\System32\taskmon.exe

These entries provide the program with the file names and locations for the virus components. The %Windir% entry allows the program to customize the file lockout path for each system based on the directory used by the operating system.

- 3) Click on the “OK” button.
- 4) Click on “Yes” button to confirm the cratering of the infected file. You will then see entries in the program log confirming the modification of the virus components.
- 5) After completing this process, we recommend a reboot before modifying the registry.

8. Rebooting Infected Machines

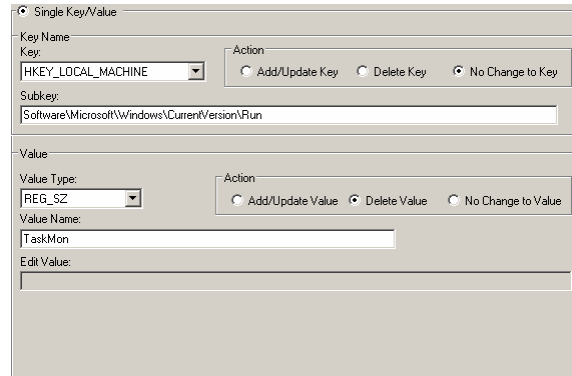
- 1) Make sure that infected machines are still highlighted. If not, double-click on the “Infected Mydoom” entry in the “Select/Highlight System Lists”.
- 2) Select the menu option: “Misc | Reboot.”
- 3) Insert an appropriate message/delay and click on the “Apply” button.
- 4) When the machine reboots, the infection should be removed and further infection should be inhibited.



9. Deleting Registry Entries Added by Virus – Removing DoS Component

After your machines reboot, the registry entries previously placed by the virus will attempt to load the virus components. Because the virus components have been locked out, they will no longer function--clearing the way to removing the registry entries.

- 1) The list of infected machines should still be highlighted.
- 2) Click on the "Reg Edit" button.
- 3) Select the "Single Key/Value" radio button.
In this next section we will be removing the component that runs when you start Windows. This component launches threads to perform a denial of service attack (DoS) against www.sco.com.
- 4) Under Key Name, set:
Action: "No Change to Key"
Key: **HKEY_LOCAL_MACHINE**
Subkey: **Software\Microsoft\Windows\CurrentVersion\Run**
- 5) Under Value, set:
Action: "Delete Value"
Value Type: **REG_SZ**
Value Name: **TaskMon**

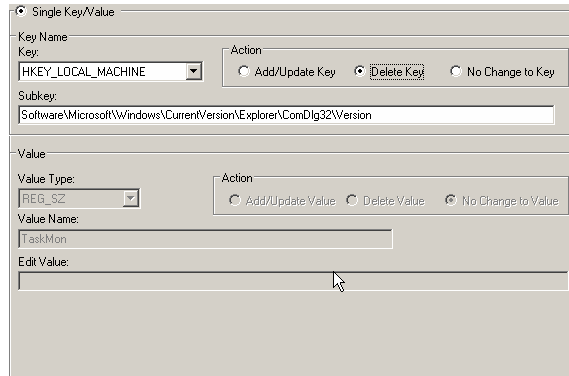


- 6) Click on the “Apply” button.
- 7) You should then see positive confirmation that this first entry has been removed. When the operation has been completed, click on the “Reg Edit” button.
Notice that all of the previous settings are remembered. We are now going to only change one setting for the registry hive.
- 8) Under Key Name, change:
Key: **HKEY_USERS**
- 9) Click on the “Apply” button.

10. Deleting Registry Entries Added by Virus – Removing Extraneous Registry Keys

This next set of steps gets rid of some extraneous registry keys created by the virus. Make absolutely certain that you have entered the key paths for the keys that you are about to delete. If you leave out pieces of the path and delete the root path, not the full path as shown, you will permanently damage your systems requiring the reinstallation of the operating systems. Be careful!

- 10) The list of infected machines should still be highlighted.
- 11) Click on the “Reg Edit” button.
- 12) Select the “Single Key/Value” radio button.
- 13) Under Key Name, set:
Action: **“Delete Key”**
Key: **HKEY_LOCAL_MACHINE**
Subkey (must all be one line exactly as shown):
Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version
- 14) Under Value, set:
Action: **“No Change to Value”**



- 15) Click on the “Apply” button.
- 16) You should then see positive confirmation that this first entry has been removed. When the operation has been completed, click on the “Reg Edit” button. Notice that all of the previous settings are remembered. We are now going to only change one setting for the registry hive.
- 17) Under Key Name, change:
Key: **HKEY_USERS**
- 18) Click on the “Apply” button.

11. Fixing the Registry Entry that Modifies the Shell

This virus changes the load path for a component known as “Webcheck” that is loaded by explorer.exe (operating system shell). You will need to restore the damaged registry area to return your systems to their previously uninfected state.

User Manager Pro has the ability to push out a REGEDIT file containing the replacement area of the registry to all of your systems. You can create the REGEDIT file yourself by:

- 1) Start REGEDIT on an uninfected machine running Windows XP or equivalent for your environment.
- 2) Go to the key:

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32

- 3) Right click on the key and select the “Export” option. Save the file under the name: Webcheck.reg.

The following is a Regedit export file which contains the proper entry for Windows NT/2000/XP/ Server 2003 systems (note that the line starting with “[HKEY...” must not be split between two lines.

REGEDIT4

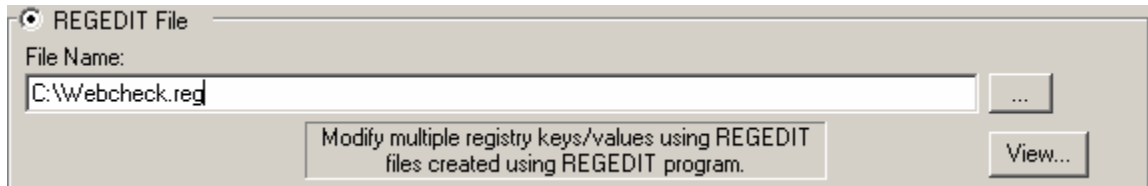
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32]
@=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,00,74,00,25,\
```

00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,77,00,65,00,\
62,00,63,00,68,00,65,00,63,00,6b,00,2e,00,64,00,6c,00,6c,00,00,00

Note: This is the Regedit export for the default key value of: %SystemRoot%\System32\webcheck.dll. The hex(2) is the export format for the registry value type of REG_EXPAND_SZ. If you import this file, you should see that value and value type in the key.

To push the corrected file to your systems:

- 1) Make sure that all of your infected systems are highlighted on the list.
- 2) Click on the "Reg Edit" button.
- 3) Select the "REGEDIT File" option button.
- 4) Enter the path to the file containing the corrected entries.
- 5) Click on the "Apply" button.



12. Final Notes

User Manager Pro provides the administrator of a large group of systems the ability to detect and surgically remove foreign content such as virus and Trojan programs. The program also has a vast wealth of other features that we would be happy to show you.

If you have any problems using the User Manager Pro program to remove the virus, or would like an overview of this or our other products, please feel free to contact us.

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

