

Article ID: 891716 - Last Review: February 10, 2009 - Revision: 51.0

Deployment of the Microsoft Windows Malicious Software Removal Tool in an enterprise environment

The Microsoft Windows Malicious Software Removal Tool is intended for use with the operating systems that are listed in the "Applies to" section. Operating systems that are not included in the list were not tested and therefore are not supported. These unsupported operating systems include all versions and editions of embedded operating systems.

INTRODUCTION

Microsoft has released the Microsoft Windows Malicious Software Removal Tool to help you remove specific, prevalent malicious software from a computer.

The information that is contained in this article is specific to the enterprise deployment of the tool. We highly recommend that you review the following Microsoft Knowledge Base article. It contains general information about the tool and about the download locations.

For more information, click the following article number to view the article in the Microsoft Knowledge Base:

[890830](http://support.microsoft.com/kb/890830/) (<http://support.microsoft.com/kb/890830/>) The Microsoft Windows Malicious Software Removal Tool helps remove specific, prevalent malicious software from computers that are running Windows Vista, Windows Server 2003, Windows XP, or Windows 2000

The tool is primarily intended for noncorporate users who do not have an existing, up-to-date antivirus product installed on their computers. However, the tool can also be deployed in an enterprise environment to enhance existing protection and as part of a defense-in-depth strategy. To deploy the tool in an enterprise environment, you can use one or more of the following methods:

- Windows Server Update Services
- Microsoft Systems Management Software (SMS) software package
- Group Policy-based computer startup script
- Group Policy-based user logon script

For more information about how to deploy the tool through Windows Update and Automatic Updates, click the following article number to view the article in the Microsoft Knowledge Base:

[890830](http://support.microsoft.com/kb/890830/) (<http://support.microsoft.com/kb/890830/>) The Microsoft Windows Malicious Software Removal Tool helps remove specific, prevalent malicious software from computers that are running Windows Vista, Windows Server 2003, Windows Server 2008, Windows XP, or Windows 2000

The current version of this tool does not support the following deployment technologies and techniques:

- Windows Update Catalog
- Execution of the tool against a remote computer
- Software Update Services (SUS)

Additionally, the Microsoft Baseline Security Analyzer (MBSA) does not detect execution of the tool. This article includes information about how you can verify execution of the tool as part of deployment.

Code sample

The script and the steps that are provided here are meant to be only samples and examples. Customers must test these sample scripts and example scenarios and modify them appropriately to work in their environment. You must change the *ServerName* and the *ShareName* according to the setup in your environment.

The following code sample does the following things:

- Runs the tool in silent mode
- Copies the log file to a preconfigured network share
- Prefixes the log file name with the name of the computer from which the tool is executed and with the user name of the current user. You must set appropriate permissions on the share according to the instructions in the [Initial setup and configuration](#) section.

```

REM In this example, the script is named RunMRT.cmd.
REM The Sleep.exe utility is used to delay the execution of the tool when used as a
REM startup script. See the "Known issues" section for details.
@echo off
call \\ServerName\ShareName\Sleep.exe 5
Start /wait \\ServerName\ShareName\Windows-KB890830-V2.7.exe /q

copy %windir%\debug\mrt.log \\ServerName\ShareName\Logs%\computername%_username%
_mrt.log

```

Note In this code sample, *ServerName* is a placeholder for the name of your server, and *ShareName* is a placeholder for the name of your share.

Initial setup and configuration

This section is intended for administrators who are using a startup script or a logon script to deploy this tool. If you are using SMS, you can continue to the "Deployment methods" section.

To configure the server and the share, follow these steps:

1. Set up a share on a member server. Then name the share **ShareName**.
2. Copy the tool and the sample script, RunMRT.cmd, to the share. See the [Code sample](#) section for details.
3. Configure the following share permissions and NTFS file system permissions:
 - Share permissions:
 - a. Add the domain user account for the user who is managing this share, and then click **Full Control**.
 - b. Remove the Everyone group.
 - c. If you use the computer startup script method, add the Domain Computers group together with Change and Read permissions.
 - d. If you use the logon script method, add the Authenticated Users group together with Change and Read permissions.
 - NTFS permissions:
 - a. Add the domain user account for the user who is managing this share, and then click **Full Control**.
 - b. Remove the Everyone group if it is in the list.

Note If you receive an error message when you remove the Everyone group, click **Advanced** on the **Security** tab, and then click to clear the **Allow inheritable permissions from parent to propagate to this object** check box.

- c. If you use the computer startup script method, grant the Domain Computers group Read & Execute permissions, List Folder Contents permissions, and Read permissions.
 - d. If you use the logon script method, grant the Authenticated Users group Read & Execute permissions, List Folder Contents permissions, and Read permissions.
4. Under the ShareName folder, create a folder that is named "Logs."

This folder is where the final log files will be collected after the tool runs on the client computers.

5. To configure the NTFS permissions on the Logs folder, follow these steps.

Note Do not change the Share permissions in this step.

- a. Add the domain user account for the user who is managing this share, and then click **Full Control**.
- b. If you use the computer startup script method, give the Domain Computers group Modify permissions, "Read & Execute" permissions, List Folder Contents permissions, Read permissions, and Write permissions.
- c. If you use the logon script method, give the Authenticated Users group Modify permissions, "Read & Execute" permissions, List Folder Contents permissions, Read permissions, and Write permissions.

Deployment methods

Note To run this tool, you must have Administrator permissions or System permissions,

regardless of the deployment option that you choose.

How to use the SMS software package

The following example provides step-by-step instructions for using SMS 2003. The steps for using SMS 2.0 resemble these steps.

1. Extract the Mrt.exe file from the package that is named Windows-KB890830-V1.34-ENU.exe /x.
2. Create a .bat file to start Mrt.exe and to capture the return code by using ISMIF32.exe.

The following is an example.

```
@echo off
Mrt.exe /q
If errorlevel 13 goto error13
If errorlevel 12 goto error12
Goto end

:error13
Ismif32.exe -f MIFFILE -p MIFNAME -d "text about error 13"
Goto end

:error12
Ismif32.exe -f MIFFILE -p MIFNAME -d "text about error 12"
Goto end

:end
```

For more information about Ismif32.exe, click the following article numbers to view the articles in the Microsoft Knowledge Base:

- [268791](http://support.microsoft.com/kb/268791/) (http://support.microsoft.com/kb/268791/) How a status Management Information Format (MIF) file produced by the ISMIF32.exe file is processed in SMS 2.0
- [186415](http://support.microsoft.com/kb/186415/) (http://support.microsoft.com/kb/186415/) Status MIF creator, Ismif32.exe is available

3. To create a package in the SMS 2003 console, follow these steps:
 - a. Open the SMS Administrator Console.
 - b. Right-click the **Packages** node, click **New**, and then click **Package**.

The **Package Properties** dialog box is displayed.
 - c. On the **General** tab, name the package.
 - d. On the **Data Source** tab, click to select the **This package contains source files** check box.
 - e. Click **Set**, and then choose a source directory that contains the tool.
 - f. On the **Distribution Settings** tab, set the **Sending priority** to **High**.
 - g. On the **Reporting** tab, click **Use these fields for status MIF matching**, and then specify a name for the **MIF file name** field and for the **Name** field.

Version and **Publisher** are optional.
 - h. Click **OK** to create the package.
4. To specify a Distribution Point (DP) to the package, follow these steps:
 - a. In the SMS 2003 console, locate the new package under the **Packages** node.
 - b. Expand the package. Right-click **Distribution Points**, point to **New**, and then click **Distribution Points**.
 - c. Start the New Distribution Points Wizard. Select an existing Distribution Point.
 - d. Click **Finish** to close the wizard.
5. To add the batch file that was previously created to the new package, follow these steps:
 - a. Under the new package node, click the **Programs** node.
 - b. Right-click **Programs**, point to **New**, and then click **Program**.
 - c. Click the **General** tab, and then enter a valid name.
 - d. At the **Command line**, click **Browse** to select the batch file that you created to start Mrt.exe.
 - e. Change **Run** to **Hidden**. Change **After** to **No action required**.
 - f. Click the **Requirements** tab, and then click **This program can run only on specified client operating systems**.

- g. Click **All x86 Windows 2000, All x86 Windows Server 2003, and All x86 Windows XP**.
 - h. Click the **Environment** tab, click **Whether a user is logged in** in the **Program can run** list. Set the **Run** mode to **Run with administrative rights**.
 - i. Click **OK** to close the dialog box.
6. To create an advertisement to advertise the program to clients, follow these steps:
 - a. Right-click the **Advertisement** node, click **New**, and then click **Advertisement**.
 - b. On the **General** tab, enter a name for the advertisement. In the **Package** field, select the package that you previously created. In the **Program** field, select the program that you previously created. Click **Browse**, and then click the **All System** collection or select a collection of computers that only includes Microsoft Windows 2000 and later versions.
 - c. On the **Schedule** tab, leave the default options if you want the program to only run one time. To run the program on a schedule, assign a schedule interval.
 - d. Set the **Priority** to **High**.
 - e. Click **OK** to create the advertisement.

How to use a Group Policy-based computer startup script

This method requires you to restart the client computer after you set up the script and after you apply the Group Policy setting.

1. Set up the shares. To do this, follow the steps in the [Initial setup and configuration](#) section.
2. Set up the startup script. To do this, follow these steps:
 - a. In the **Active Directory Users and Computers** MMC snap-in, right-click the domain name, and then click **Properties**.
 - b. Click the **Group Policy** tab.
 - c. Click **New** to create a new Group Policy object (GPO), and type **MRT Deployment** for the name of the policy.
 - d. Click the new policy, and then click **Edit**.
 - e. Expand **Windows Settings for Computer Configuration**, and then click **Scripts**.
 - f. Double-click **Logon**, and then click **Add**.

The **Add a Script** dialog box is displayed.

- g. In the **Script Name** box, type `\\ServerName\ShareName\RunMRT.cmd`.
 - h. Click **OK**, and then click **Apply**.
3. Restart the client computers that are members of this domain.

How to use a Group Policy-based user logon script

This method requires that the logon user account is a domain account and is a member of the local administrator's group on the client computer.

1. Set up the shares. To do this, follow the steps in the [Initial setup and configuration](#) section.
2. Set up the logon script. To do this, follow these steps:
 - a. In the **Active Directory Users and Computers** MMC snap-in, right-click the domain name, and then click **Properties**.
 - b. Click the **Group Policy** tab.
 - c. Click **New** to create a new GPO, and then type **MRT Deployment** for the name.
 - d. Click the new policy, and then click **Edit**.
 - e. Expand **Windows Settings for User Configuration**, and then click **Scripts**.
 - f. Double-click **Logon**, and then click **Add**. The **Add a Script** dialog box is displayed.
 - g. In the **Script Name** box, type `\\ServerName\ShareName\RunMRT.cmd`.
 - h. Click **OK**, and then click **Apply**.
3. Log off and then log on to the client computers.

In this scenario, the script and the tool will run under the context of the logged-on user. If this user does not belong to the local administrators group or does not have sufficient permissions, the tool will not run and will not return the appropriate return code. For more information about how to use startup scripts and logon scripts, click the following article numbers to view the articles in the Microsoft Knowledge Base:

[198642](http://support.microsoft.com/kb/198642/) (<http://support.microsoft.com/kb/198642/>) Overview of logon, logoff, startup, and shutdown scripts in Windows 2000

[322241](http://support.microsoft.com/kb/322241/) (<http://support.microsoft.com/kb/322241/>) How to assign scripts in Windows 2000

Additional information that is relevant to enterprise deployment

How to examine return codes

You can examine the return code of the tool in your deployment logon script or in your deployment startup script to verify the results of execution. See the [Code sample](#) section for an example of how to do this.

The following list contains the valid return codes.

How to parse the log file

The Malicious Software Removal Tool writes details about the result of its execution in the %windir%\debug\mrt.log log file.

Notes

- This log file is available only in English.
- Starting with version 1.2 of the removal tool (March 2005), this log file uses Unicode text. Before version 1.2, the log file used ANSI text.
- The log file format has changed with version 1.2, and we recommend that you download and use the latest version of the tool.

If this log file already exists, the tool appends to the existing file.

- You can use a command script that resembles the previous example to capture the return code and to collect the files to a network share.
- Because of the switch from ANSI to Unicode, version 1.2 of the removal tool will copy any ANSI versions of the Mrt.log file in the %windir%\debug folder to Mrt.log.old in the same directory. Version 1.2 also creates a new Unicode version of the Mrt.log file in that same directory. Like the ANSI version, this log file will be appended to each month's release.

The following example is an Mrt.log file from a computer that was infected with the Sasser.A worm:

```
Microsoft Windows Malicious Software Removal Tool v1.28, April 2007
Started On Mon Mar 19 13:15:07 2007
```

Quick Scan Results:

```
-----
Found virus: Win32/Sasser.A.worm in file://C:\WINDOWS\avserve.exe
Found virus: Win32/Sasser.A.worm in
regkey://HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\avserve.exe
Found virus: Win32/Sasser.A.worm in
runkey://HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\avserve.exe
Found virus: Win32/Sasser.A.worm in file://C:\WINDOWS\avserve.exe
```

Quick Scan Removal Results

```
-----
Start 'remove' for
regkey://HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\avserve.exe
Operation succeeded !
```

```
Start 'remove' for
runkey://HKLM\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN\avserve.exe
Operation succeeded !
```

```
Start 'remove' for file://\?\C:\WINDOWS\avserve.exe
Operation succeeded !
```

Results Summary:

```
-----
Found Win32/Sasser.A.worm and Removed!
```

```
Return code: 6
Microsoft Windows Malicious Software Removal Tool Finished On Mon Mar 19 13:15:57 2007
```

The following is an example log file where no malicious software is found.

```
Microsoft Windows Malicious Software Removal Tool v1.2, March 2005
Started On Wed May 01 21:19:01 2002
```

Results Summary:

```
-----
No infection found.
```

```
Return code: 0
Microsoft Windows Malicious Software Removal Tool Finished On Wed May 01 21:19:05 2002
```

The following is a sample log file in which errors are found.

For more information about warnings and errors that are caused by the tool, click the following article number to view the article in the Microsoft Knowledge Base:

[891717](http://support.microsoft.com/kb/891717/) (http://support.microsoft.com/kb/891717/) How to troubleshoot an error when you run the Microsoft Windows Malicious Software Removal Tool

Microsoft Windows Malicious Software Removal Tool v1.2, March 2005
Started On Wed May 01 21:27:57 2002

Scanning Results:

Found virus: Win32/HLLW.Gaobot.ZF in process 1880
Found virus: Win32/HLLW.Gaobot.ZF in process 1880
Found virus: Win32/HLLW.Gaobot.ZF in file C:\WINDOWS\System32\winsec16.exe
Found virus: Win32/HLLW.Gaobot.ZF in process 1880
Found virus: Win32/HLLW.Gaobot.ZF in process 1880
Found virus: Win32/HLLW.Gaobot.ZF in file C:\WINDOWS\System32\winsec16.exe
Found virus: Win32/HLLW.Gaobot.ZF in file C:\WINDOWS\System32\winsec16.exe

Removal Results:

Terminating process with pid 1880
->Sysclean ERROR: Failed to kill process with PID: 1880 (Win32 Error Code: 0x00000102
(258):The wait operation timed out.) [697]
Operation failed !

Terminating process with pid 1880
Operation had previously completed.

Terminating process with pid 1880
Operation had previously completed.

Deleting registry value HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices,
entry: WinSec
Operation succeeded !

Terminating process with pid 1880
Operation had previously completed.

Deleting registry value HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, entry:
WinSec
Operation succeeded !

Writing in file C:\WINDOWS\system32\drivers\etc\hosts
Operation succeeded !

Deleting file C:\WINDOWS\System32\winsec16.exe
Operation succeeded !

Deleting file C:\WINDOWS\System32\winsec16.exe
Operation had previously completed.

Deleting file C:\WINDOWS\System32\winsec16.exe
Operation had previously completed.

Results Summary:

For cleaning Win32/HLLW.Gaobot.ZF, the system must be restarted.
Found Win32/HLLW.Gaobot.ZF, partially removed.

Known issues

When you run the tool by using a startup script, error messages that resemble the following error message may be logged in the Mrt.log file:

Error: MemScanGetImagePathFromPid(pid: 552) failed.
0x00000005: Access is denied.

Note The pid number will vary.

This error message occurs when a process is just starting or when a process has been recently stopped. The only effect is that the process that is designated by the pid is not scanned.

To work around this problem, use the Sleep.exe Platform SDK utility to delay five seconds in the startup script before you run the tool. See the previous sample script. This delay lets processes on the computer stabilize after the restart process.

FAQ

Q1. When I test my startup or logon script to deploy the tool, I do not see the log files that are being copied to the network share that I set up. Why?

A1. This is frequently caused by permissions issues. For example, the account that the removal tool was run from does not have Write permission to the share. To troubleshoot this, first make sure that the tool ran by checking the registry key. Alternatively, you can look for the presence of the log file on the client computer. If the tool successfully ran, you can test a simple script and make sure that it can write to the network share when it runs under the same security context in which the removal tool was run.

Q2. How do I verify that the removal tool has run on a client computer?

A2. You can examine the value data for the following registry entry to verify the execution of the tool. You can implement such an examination as part of a startup script or a logon script. This process prevents the tool from running multiple times.

Subkey: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RemovalTools\MRT
Entry name: Version

Every time that the tool is run, the tool records a GUID in the registry to indicate that it has been executed. This occurs regardless of the results of the execution. The following table lists the GUID that corresponds to each release.

Release	Value data
January 2005	E5DD9936-C147-4CD1-86D3-FED80FAADA6C
February 2005	805647C6-E5ED-4F07-9E21-327592D40E83
March 2005	F8327EEF-52AA-439A-9950-CE33CF0D4FDD
April 2005	D89EBFD1-262C-4990-9927-5185FED1F261
May 2005	08112F4F-11BF-4129-A90A-9C8DD0104005
June 2005	63C08887-00BE-4C9B-9EFC-4B9407EF0C4C
July 2005	2EEAB848-93EB-46AE-A3BF-9F1A55F54833
August 2005	3752278B-57D3-4D44-8F30-A98F957EC3C8
August 2005 A	4066DA74-2DDE-4752-8186-101A7C543C5F
September 2005	33B662A4-4514-4581-8DD7-544021441C89
October 2005	08FFB7EB-5453-4563-A016-7DBC4FED4935
November 2005	1F5BA617-240A-42FF-BE3B-14B88D004E43
December 2005	F8FEC144-AA00-48B8-9910-C2AE9CCE014A
January 2006	250985ee-62e6-4560-b141-997fc6377fe2
February 2006	99cb494b-98bf-4814-bff0-cf551ac8e205
March 2006	b5784f56-32ca-4756-a521-ca57816391ca
April 2006	d0f3ea76-76c8-4287-8cdf-bdfee5e446ec
May 2006	ce818d5b-8a25-47c0-a9cd-7169da3f9b99
June 2006	7cf4b321-c0dd-42d9-afdf-edbb85e59767
July 2006	5df61377-4916-440f-b23f-321933b0afd3
August 2006	37949d24-63f1-4fdc-ad24-5dc3eb3ad265
September 2006	ac3fa517-20f0-4a42-95ca-6383f04773c8
October 2006	79e385d0-5d28-4743-aeb3-ed101c828abd
November 2006	1d21fa19-c296-4020-a7c2-c5a9ba4f2356
December 2006	621498ca-889b-48ef-872b-84b519365c76

January 2007	2F9BC264-1980-42b6-9EE3-2BE36088BB57
February 2007	FFCBCFA5-4EA1-4d66-A3DC-224C8006ACAE
March 2007	5ABA0A63-8B4C-4197-A6AB-A1035539234D
April 2007	57FA0F48-B94C-49ea-894B-10FDA39A7A64
May 2007	15D8C246-6090-450f-8261-4BA8CA012D3C
June 2007	234C3382-3B87-41ca-98D1-277C2F5161CC
July 2007	4AD02E69-ACFE-475C-9106-8FB3D3695CF8
August 2007	0CEFC17E-9325-4810-A979-159E53529F47
September 2007	A72DDD48-8356-4D06-A8E0-8D9C24A20A9A
October 2007	52168AD3-127E-416C-B7F6-068D1254C3A4
November 2007	EFC91BC1-FD0D-42EE-AA86-62F59254147F
December 2007	73D860EC-4829-44DD-A064-2E36FCC21D40
January 2008	330FCFD4-F1AA-41D3-B2DC-127E699EEF7D
February 2008	0E918EC4-EE5F-4118-866A-93f32EC73ED6
March 2008	24A92A45-15B3-412D-9088-A3226987A476
April 2008	F01687B5-E3A4-4EB6-B4F7-37D8F7E173FA
May 2008	0A1A070A-25AA-4482-85DD-DF69FF53DF37
June 2008	0D9785CC-AEEC-49F7-81A8-07B225E890F1
July 2008	BC308029-4E38-4D89-85C0-8A04FC9AD976
August 2008	F3889559-68D7-4AFB-835E-E7A82E4CE818
September 2008	7974CF06-BE58-43D5-B635-974BD92029E2
October 2008	131437DE-87D3-4801-96F0-A2CB7EB98572
November 2008	F036AE17-CD74-4FA5-81FC-4FA4EC826837
December 2008	9BF57AAA-6CE6-4FC4-AEC7-1B288F067467
December 2008	9BF57AAA-6CE6-4FC4-AEC7-1B288F067467
January 2009	2B730A83-F3A6-44F5-83FF-D9F51AF84EA0
February 2009	C5E3D402-61D9-4DDF-A8F5-0685FA165CE8

Q3. How can I disable the infection-reporting component of the tool so that the report is not sent back to Microsoft?

A3. An administrator can choose to disable the infection-reporting component of the tool by adding the following registry key value to computers. If this registry key value is set, the tool will not report infection information back to Microsoft.

Subkey: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\MRT
 Entry name: \DontReportInfectionInformation
 Type: REG_DWORD
 Value data: 1

This functionality is automatically disabled if the following registry key value exists:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\WUserver

This registry key value indicates that the computer is connected to an SUS server.

Q4. With the March 2005 release, data in the Mrt.log file appears to have been lost. Why was this data removed, and is there a way for me to retrieve it?

A4. Starting with the March 2005 release, the Mrt.log file is being written as a Unicode file. To make sure of compatibility, when the March 2005 version of the tool is run, if an ANSI version of the file is on the system, the tool will copy the contents of that log to Mrt.log.old in %WINDIR%\debug and create a new Unicode version of Mrt.log. Like the ANSI version, this Unicode version will be appended to with each successive execution of the tool.

APPLIES TO

- Microsoft Windows Server 2003, Standard Edition (32-bit x86)
- Microsoft Windows Server 2003, Enterprise Edition (32-bit x86)
- Windows Server 2008 Standard
- Windows Server 2008 Enterprise
- Microsoft Windows XP Professional
- Microsoft Windows XP Home Edition
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Professional Edition

Keywords: kbinfo KB891716



Hai bisogno di aiuto?

[Contatta un tecnico Microsoft.](#)

Aiuto & Supporto

Microsoft
©2009 Microsoft