Click here!

Online Services | **Anti-Virus** | Business Corner | About Us | Shopping | Support | Downloads

Update ActiveShield
DAT Updates
Free Virus Map
Free Virus News
Virus Information Library
Virus Calendar
Virus Hoaxes
Virus Support
Virus Glossary
Anti-Virus Tips
Regional Virus Info
What's On Sale

Site Assistant

SHOPPING SERVICES
• Buy a gift certificate
• Get info on new viruses with McAfee.com Dispatch!

Virus Information Library Search Center

Search for Viruses   Limit search to:

[containing ▼]   [   ]   [GO]

➤ Keyword Search   ➤ Advanced Search

Virus Profile

Virus Name:	Risk Assessment:
W32/PetTick@MM	**Low**

Virus Information:	
Date Discovered:	6/13/01
Date Added:	7/11/01
Origin:	Unknown
Length:	6,656
Type:	Virus
SubType:	E-mail
DAT Required:	4144

Quick Links:

➤ Virus Characteristics
➤ Indications of Infection
➤ Method of Infection
➤ Removal Instructions
➤ Aliases

➤ Update ActiveShield
➤ Perform a Scan

➤ Download the latest DAT files

Virus Characteristics:

This is a simple mass-mailing worm which masquerades as an update to the Windows game Minesweeper.

When run, a message box is displayed.

It then copies itself to the WINDOWS SYSTEM directory as Winmine.exe (note: the valid WINMINE.EXE program usually resides in the WINDOWS directory). A WIN.INI entry is created to load this program at startup.

[windows]
load=C:\WINDOWS\SYSTEM\WINMINE.EXE

Upon reboot, the WINMINE.EXE file is run from the SYSTEM directory which results in the program creating and executing the VBScript file C:\ENVOIE_VBS.vbs (554 bytes, detected as VBS/Generic@MM). This script sends an email to all recipients found in the Microsoft Outlook address book with the following information:

Subject: Is the work so hard ??
Body:

Relax you with the last version of <Winmine>.

Attachment: Winmine.exe

Indications Of Infection:

Presence of C:\ENVOIE_VBS.vbs

On the 15th of the month, a message box is displayed and the mouse is configured for a left-handed user.

5 minutes later, the program shuts down Windows.

Method Of Infection:

This is a mass mailing email worm virus. It arrives as an email attachment. Executing that attachment infects the local system which is then used to propagate the virus further.

Removal Instructions:

Use specified engine and DAT files for detection and removal. Delete any file which contains this detection.

Windows ME Info:
NOTE: Windows ME utilizes a backup utility that backs up selected files automatically to the C:_Restore folder. This means that an infected file could be stored there as a backup file, and VirusScan will be unable to delete these files. These instructions explain how to remove the infected files from the C:_Restore folder.

Disabling the Restore Utility

1. Right click the My Computer icon on the Desktop.
2. Click on the Performance Tab.
3. Click on the File System button.
4. Click on the Troubleshooting Tab.
5. Put a check mark next to "Disable System Restore".
6. Click the Apply button.
7. Click the Close button.
8. Click the Close button again.
9. You will be prompted to restart the computer. Click Yes.
NOTE: The Restore Utility will now be disabled.
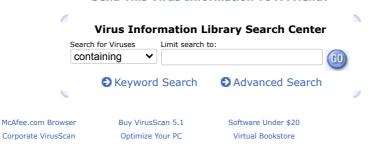10. Restart the computer in Safe Mode.
11. Run a scan with VirusScan to delete all infected files, or browse the file's located in the C:_Restore folder and remove the file's.
12. After removing the desired files, restart the computer normally.
NOTE: To re-enable the Restore Utility, follow steps 1-9 and on step 5 remove the check mark next to "Disable System Restore". The infected file's are removed and the System Restore is once again active.

Aliases:

I-Worm.Winmine, W32.Mineup.Worm (NAV), W32/Petik@MM

Send This Virus Information To A Friend?

Virus Information Library Search Center

Search for Viruses   Limit search to:
containing ▾

GO

➡ Keyword Search   ➡ Advanced Search

McAfee.com Browser   Buy VirusScan 5.1   Software Under $20
Corporate VirusScan   Optimize Your PC   Virtual Bookstore

FAQs | **What's On Sale?** | **Events** | **Investor Relations**
Partners | **Jobs** | **FREE Virus News**