

Identify/React Chart: MyDoom/Zincite.A

MyDoom variants are mass-mailing worms that use their own SMTP engine to spread. MyDoom plants and opens a back door (Backdoor.Zincite.A) on TCP port 1034. In addition to stealing any e-mail addresses found locally, recent MyDoom variants also use major search engines to locate more addresses. Other versions plant back doors but use different port numbers.

How to identify

MyDoom infects a system when a malicious attachment to an e-mail is opened. The attachment will carry one of these extensions: EXE, COM, SCR, PIF, BAT, CMD, or ZIP, but it may also use double extensions. The From address will likely appear to come from a known individual. While subject lines vary, a common one is some form of an e-mail delivery failure message.

The body of MyDoom messages warns that your system has been hijacked and invites you to open an attachment and run the "cleanup" file, which is actually MyDoom. It adds a mutual exclusion object that prevents multiple copies of the worm from starting.

This version immediately copies itself to the Windows directory %Windows% (such as C:\Winnt) as Java.exe. (There is no such file on uninfected systems.) It also plants Services.exe in the same directory and creates registry entries that cause the worm and Trojan to run at startup:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  JavaVM = "%Windows%\java.exe"
```

and

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
  Services = "%Windows%\services.exe" (this is the
  Zincite.A Trojan)
```

MyDoom also creates these registry keys:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Daemon
```

and

```
HKEY_CURRENT_USER\Software\Microsoft\Daemon
```

MyDoom will often also create "%Temp%\zincite.log".

How to react

Removal is different for different versions of MyDoom. Previous versions, such as MyDoom.A and Novarg.A, used various registry values and different filenames, making them more difficult to remove. The most recent version of MyDoom (variants Q/S, also known as Backdoor.Nemog) is relatively easy to get rid of because the files always have the same name.

Warning: This requires editing the registry.

1. On XP and Me, disable System Restore.
(Antivirus tools can't delete infected files in the Restore folder.)
2. Reboot W95, 98, Me, 2000, and XP in Safe Mode. Reboot NT4 in VGA mode. (Repeatedly press or press/hold [F8] during reboot or startup, or use the System Configuration Utility by clicking Start | Run and entering *msconfig*.)
3. Back up the registry.
4. Select Start | Run and enter *regedit*.
5. Move to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run.
6. Delete "winpsd"="%System%\winpsd.exe".
7. Move to HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer and remove "InstaledFlashhMx"="1".
8. Delete HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version.
9. Exit Regedit and reboot in Normal mode.