

# MYDOOM WORM SYMPTOMS & REMOVAL INSTRUCTIONS

**Source:** <http://linux.derkeiler.com/Mailing-Lists/RedHat/2004-01/1138.html>

---

**From:** SR Khaleeq ([m\\_shoaib\\_rehman\\_at\\_yahoo.com](mailto:m_shoaib_rehman_at_yahoo.com))

**Date:** 01/30/04

To: [prestongrads@yahoogroups.com](mailto:prestongrads@yahoogroups.com)

Date: Fri, 30 Jan 2004 00:59:58 -0800 (PST)

This is a mass-mailing and peer-to-peer file-sharing worm that bears the following characteristics:

- contains its own SMTP engine to construct outgoing messages
- contains a backdoor component (see below)
- contains a Denial of Service payload

The virus arrives in an email message as follows:

From: (Spoofed email sender)

Subject: (Varies, such as)

Error ,Status ,Server Report ,Mail Transaction Failed ,Mail Delivery System ,hello ,hi

Body: (Varies, such as)

The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.  
The message contains Unicode characters and has been sent as a binary attachment.  
Mail transaction failed. Partial message is available.

Attachment: (varies [.bat, .exe, .pif, .cmd, .scr] – often arrives in a ZIP archive) (22,528 bytes)

examples (common names, but can be random) ,doc.bat ,document.zip ,message.zip ,readme.zip ,text.pif  
hello.cmd ,body.scr ,test.htm.pif ,data.txt.exe ,file.scr

In the case of two file extensions, multiple spaces may be inserted as well, for example:

document.htm (many spaces) .pif

## Symptoms

Upon executing the virus, Notepad is opened, filled with nonsense characters.  
Existence of the files and registry entry listed above

## Method Of Infection

This worm tries to spread via email and by copying itself to the shared directory for Kazaa clients if they are

## RedHat: MYDOOM WORM SYMPTOMS & REMOVAL INSTRUCTIONS

present.

The mailing component harvests address from the local system. Files with the following extensions are targeted:

wab ,adb ,tbb ,dbx ,asp ,php ,sht ,htm ,txt ,pl

The worm avoids certain address, those using the following strings:

.gov ,mil ,abuse ,acketst ,arin. ,avp ,berkeley ,borlan ,bsd  
example ,fido ,foo. ,fsf. ,gnu ,google ,gov. ,hotmail ,iana ibm.com  
icrosof ,ietf ,inpris ,isc.o ,isi.e ,kernel ,linux ,math ,mit.e ,mozilla  
msn. ,mydomai ,nodomai ,panda ,pgp ,,rfc-ed ,ripe. ,ruslis ,secur  
sendmail ,sopho ,syma ,tanford.e ,unix ,usenet ,utgers.ed

Removal Instructions:

If you think that you may be infected with Mydoom, and are unsure how to check your system, you may <http://vil.nai.com/vil/stinger> to scan your system and remove the virus if present

Details can be viewed at [http://vil.nai.com/vil/content/v\\_100983.htm](http://vil.nai.com/vil/content/v_100983.htm)

Regards,

Shoaib Rehman Khaleeq

Systems Consultant  
Ants Consulting Pakistan  
shoaib.rehman@ants.com.pk  
+92-300-2202802

---

Do you Yahoo!?

Yahoo! SiteBuilder – Free web site building tool. Try it!

--

redhat-list mailing list  
unsubscribe <mailto:redhat-list-request@redhat.com?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>