Breaking Virus News:
MyDoom Hobbles Internet E-mail

By Jay Munro
January 27, 2004
Last Updated: January 28, 2004
Total posts: 3

Click here to subscribe to our Security Watch newsletter.

Print Email Save Discuss Subscribe

A powerful worm virus known variously as W32/Novarg.A, W32/Shimg, W32/Mydoom, or W32/Mimail.R is devastating personal and corporate e-mail systems across the globe. This fast-moving mass mailer internet worm apparently started spreading on the popular peer-to-peer file-sharing application, Kazaa, and has now moved to e-mail. The virus will overwrite certain system files, e-mail itself to every e-mail address it finds on a victim's machine, and opens a back door to malicious attack. It affects Windows 9x/Me/2000/2003/XP systems. As of Tuesday morning, it was the top virus/worm in North America, and most Antivirus companies had escalated the threat to a high or dangerous level.

The message spoofs both the To: and From: address fields, and can have a random subject line. The virus is contained in an attachment that typically has a double extension, such as .jpg.exe, or .txt.scr. The second extension however, like the Dumaru.Y virus that broke over the weekend, has a number of spaces, which may mask the second, dangerous executable extension.

The subject may be one of the following:

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

the document will typically be:

document
readme

news
MyDoom.F-mm Starting Slow, But Has Scary Potential
This Worm Only Wants to Heal
A Front Row Seat to a Major Attack
MyDoom.A:Fastest Spreading Virus in History
Dumaru.Y—Very New and Very Dangerous
View All >

new white papers
Want to Let Customers Know Your Website is Safe?
Looking for mission-critical server security?
Protect Your Network from Corporate E-mail Threats
All White Papers >

doc
text
file
data
test
message
body

and have one of these as the first (visible) extension

.htm
.txt
.doc

However, the worm will always have one of the following executable extensions.

.pif
.scr
.exe
.cmd
.bat
.zip

The actual message will be one of the following:

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

When a user executes the extension, the virus creates three files, a copy of itself in a file named %system%/shimgapi.dll, %temp%/Message (this is a text file), and %system%/taskmon.exe. The last file, Taskmon.exe is a legitimate Windows file and should not be deleted while cleaning the virus. Note that %system% is normally C:\windows\system, C:\windows\system32 or C:\winnt\system32, depending on operating system. The %temp% file is the Windows default temporary folder, and is usually located in the main windows folder. The virus also adds keys and values to the Windows registry folder so it runs when the victim's machine is started.

The virus will search the victim's hard drive for files with the extensions htm, .sht, .php, .asp, .dbx, .tbb, .adb, .pl, .wab and .txt, and harvests e-mail addresses. The addresses are used to send out copies of the virus using its own SMTP engine. Between February 1, 2004 and February 12, 2004, the virus will use the victim's machine to launch a DOS (Denial of Service) attack against www.sco.com. The attack will launch 63 threads on the users machine through port 80 (normal web browser port), making it difficult to use a local firewall unless you're set to allow only specific applications.

If the victim's machine has Kazaa installed, the virus will add Copies itself to the Kazaa download folder using one of the following file names.

winamp5
icq2004-final
activation_crack
strip-girl-2.0bdcom_patches
rootkitXP
office_crack

nuke2004

And uses the extensions:

.pif
.scr
.bat
.exe

The virus will also open a backdoor on TCP ports 3127 thru 3198 to allow an attacker access to the system.

next >

- **2/03 - Special Edition Sun Net Talk Secure and Affordable: Sun's Java™ Desktop System in Action** with Michael Krieger. *Sponsored by Sun Microsystems, Inc.*
- **2/05 - Beyond Voice Mail: Reducing Business Costs With Latest Generation of Unified Communications Applications** with Frank Derfler. *Sponsored by AVST.*
- **2/18 - Instant Messaging: The Gateway to the Real-Time Enterprise** with Jim Louderback. *Sponsored by Yahoo.*

FREE Online Seminars presented by Intel

- PC Refresh: Your Strategy for Success!
- Server Consolidation-Expand Your Options
- Wireless LAN: One Size Doesn't Fit All
- PC Fleet Management: Tools & Strategies

view more eSeminars >>

SHAREWARE.PCMAG.COM - HOT FILES

Download the best in free trial software from the PCMag.com Shareware Library. Recent hot files:

- **SeeknClean** Cleans junk off your hard disk super fast!
- **Girder** Great tool for automating Windows.
- **DiskSpace Explorer Home Edition** Manage your hard disk space, find and delete useless items.
- **My Stuff** Home and personal inventory manager.
- **CyberScrub** CyberScrub removes all traces of online activity.

More files at the Shareware Library >>

NEW FROM ZIFF DAVIS E-LEARNING

Gain new IT and programming skills, prepare for accreditation, and more with online courses from Ziff Davis eLearning.

- **New! Microsoft® Office® Skill Builders**: Office XP, Access, Powerpoint, Excel, Word
- **Development and IT**: Java, Adobe, E-Business, Linux, Macromedia, Macromedia Web Professional, Oracle 8i, Project Management, SQL Server, Visual Basic
- **Certification Prep**: A+, Certified Novell Engineer, iNET+, MCSA, MCSE, Network+, Security, Server+

See all courses at Ziff Davis eLearning >>

Breaking Virus News: MyDoom Hobbles Internet E-mail

Print Email Save Discuss Subscribe

Removing/Blocking MyDoom

The easiest way to remove MyDoom and Novarg is to update your antivirus program. As of 1/27, most antivirus vendors have added at least beta detection and deletion to their pattern definition updates. If you don't have an antivirus, we have confirmation that TrendMicro's freely available Housecall http://housecall.trendmicro.com, has been updated to detect the virus, but you'll have to manually remove the registry entries as outlined below. Panda Software also has a free removal utility (registry required) for MyDoom, http://www.pandasoftware.com/ virus_info/encyclopedia/overview.aspx?idvirus=44140. McAfee's stinger http://vil.nai.com/vil/stinger/ has also been updated to detect and remove MyDoom. Note that you need to reboot after running Stinger to completely repair your system.

Update: On Wednesday, Symantec released two new removal tools, available at: http://securityresponse. symantec.com/avcenter/venc/data/w32.novarg.a@mm.remo val.tool.html and F-Secure also posted one at http://www.f-secure.com/tools/f-mydoom.zip

Manually removing W32/MyDoom/ W32.Novarg.A-mm

Manually removing MyDoom requires editing the registry as outlined in the following steps.

Step 1. Disable System Restore if you're using Windows Me/XP. When you make changes to your system, Windows does a restoration checkpoint. If it does this while the system is infected, it may come back to re-infect later. For Windows XP (http://support.microsoft.com/default.aspx?kbid=283073) or ME (http://support.microsoft.com/default.aspx?kbid=264887)

Step 2. Restart the computer in Safe Mode (or VGA mode on Windows NT). Since MyDoom creates running processes, and Windows doesn't allow you to delete files connected with running processes, restarting is necessary. Using Safe mode prevents Windows from loading drivers and autorun entries so your system boots relatively clean.

Step 3. Run a full system scan with an updated Antivirus scanner. If your

news
MyDoom.F-mm Starting Slow, But Has Scary Potential
This Worm Only Wants to Heal
A Front Row Seat to a Major Attack
MyDoom.A:Fastest Spreading Virus in History
Dumaru.Y—Very New and Very Dangerous
View All >

scanner does not remove everything, follow the next few steps.

Step 4. Your antivirus software should, during detection, produce a list of files associated with the MyDoom virus. Delete all these files. The files will typically be the ones mentioned in the description above.

Step 5. Make a backup of the registry before you edit. (Windows 95/98/ME go to http://support.microsoft.com/default.aspx?scid=kb;en-us;322754, Windows XP/2000/2003 go to http://support.microsoft.com/default.aspx?scid=kb;en-us;322756). Delete the entries associated with MyDoom from the registry as listed above. Delete any entries flagged by your antivirus program.

a. The following instructions from the Symantec site outline the exact keys that are modified and need to be edited: Click Start, and then click Run. (The Run dialog box appears.)

b. Type regedit Then click OK. (The Registry Editor opens.)

c. Navigate to the keys:
•HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
•HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

d. In the right pane, delete the value:
"Taskmon"="%System%\taskmon.exe"

e. Delete the key HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersionExplorer\ComDlg32\Version

f. Delete the key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersionExplorer\ComDlg32\Version

g. Navigate to the key HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32

h. In the right pane, modify the value as follows:
"(Default)"="%System%\webcheck.dll"

i. Exit the Registry Editor.

Step 6. Re-enable System Restore (Windows ME, XP), reboot machine.

Click here for more virus news and security news.

< back