Subject: Warning: Spy Virus Spreading
Posted by Matt2405 on Fri, 30 Jan 2004 07:03:20 GMT
View Forum Message <> Reply to Message

If you have not read the papers or listened to the radio, a very dangorous virus
is spreading. It is coming in through in emails. If you don't have Norton Antivirus you better get it. Be very careful becuase it comes in from other people you know e.g. takavar2@yahoo.com sent me an email that had the virus in an attachment, I don't even know this person. You also recieve it from any of your friends. You could get it from anyone who has you in their address book.

What the virus does is basically spy on you. It allows the idiots who made the virus be able to see what your typing! So if your purchasing something and you give your credit card details, thats all your money blown!

This is just a very quick warning!

http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.html

Subject: Warning: Spy Virus Spreading
Posted by Xtrm2Matt on Fri, 30 Jan 2004 07:42:25 GMT
View Forum Message <> Reply to Message

This virus is also known as "MyDoom".

Quote:Why We Are Issuing This Alert
At 9:00 A.M. Pacific Time on Wednesday, January 28, 2004, Microsoft began investigating reports of a variant of a new worm named "Mydoom" or "Novarg," known as Mydoom.B. This variant reportedly blocks access to some websites, including some Microsoft.com websites. The worm attempts to entice e-mail recipients into opening a message that has a file attachment. If the attached file is opened, the worm installs malicious code on the computer user's system and sends itself to all contacts in the user's address book.

http://www.microsoft.com/security/antivirus/mydoom.asp

Also, Symantec have made a tool to quickly remove this virus from your PC. They call it the "W32.Novarg.A@mm Removal Tool".

Quote:The W32.Novarg.A@mm Removal Tool does the following:

Terminates the W32.Novarg.A@mm viral processes.
Terminates the viral thread running under Explorer.exe.
Deletes the W32.Novarg.A@mm files.
Deletes the registry values added by the worm.

http://securityresponse.symantec.com/avcenter/venc/data/w32.novarg.a@mm.removal.tool.html

And if your not sure if you have the virus, then do this:

Quote:If you use Windows XP

To find out if a computer is infected, do the following:

Click Start, and then click Search.
In the What do you want to search for? box, click All files and folders.
In the All or part of the file name box, type ctfmon.dll. If that file exists on the computer, the computer is infected with Mydoom.B, and you need to follow the steps below. Otherwise, the computer is not infected with that variant of the virus.

If you use Windows 2000 or Windows NT 4.0

To check for the worm yourself, do the following:

Click Start, and then click Run.
In the Open box, type cmd
Click OK. The black Command Prompt window will open, displaying C:\...> followed by a cursor.
Click the cursor, type dir ctfmon.dll /a /s and then press ENTER.
Wait a few moments:
If the results show File Not Found, the computer is not infected with Mydoom.B.

If you use Windows 98 or Windows 95

Click Start, and then click Run.
In the Open box, type command
Click OK. The black Command Prompt window will open, displaying C:\...> followed by a cursor.
Click the cursor, type dir ctfmon.dll /a /s and then press ENTER.
Wait a few moments:
If the results show File Not Found, the computer is not infected with Mydoom.B.

If any of the above actions actually find this .DLL file, i strongly advise you use the "W32.Novarg.A@mm Removal Tool" OR the steps below:

What to Do If Your Computer Is Infected

If your computer is infected, first try going to the website of your antivirus-software vendor to get the latest updates and information. If you are unable to access your antivirus-software vendor's site and need to fix the infection yourself, follow these steps:

Quote:Click Start, and then click Run.

In the Open box, type cmd.

Click OK. The black Command Prompt window will open, displaying C:\...> followed by a cursor.

Click the cursor and:
Type del /F %systemroot%\system32\drivers\etc\hosts
Press ENTER.

Type echo # Temporary HOSTS file >%systemroot%\system32\drivers\etc\hosts
Press ENTER.

Type attrib +R %systemroot%\system32\drivers\etc\hosts
Press ENTER.

After typing these commands, do one of the following:
If you use Windows NT 4.0, restart your computer.
If you use Windows XP or Windows 2000, do not restart your computer.

Instead, do the following:
Type ipconfig /flushdns
Press ENTER.

Hope this helps

---

Subject: Re: Warning: Spy Virus Spreading
Posted by msgtpain on Fri, 30 Jan 2004 08:57:32 GMT
View Forum Message <> Reply to Message

Matt2405
Be very careful becuase it comes in from other people you know

e.g. takavar2@yahoo.com sent me an email that had the virus in an attachment,

I don't even know this person.

---

Subject: Warning: Spy Virus Spreading
Posted by Aircraftkiller on Fri, 30 Jan 2004 09:06:25 GMT
View Forum Message <> Reply to Message

Funny thing is I get this shit all the time...

http://www.aspenth.com/ACK/WTF.jpg
http://www.aspenth.com/ACK/WTF1.jpg

I've had over 2,000 in the past two months... My solution is just to delete everything from people I don't know or if their e-mail\name is obviously fucked up.

Subject: Warning: Spy Virus Spreading
Posted by Sk8rRIMuk on Fri, 30 Jan 2004 09:50:26 GMT
View Forum Message <> Reply to Message

Nobody really opens a .bat, .scr, .exe or any other executable application from a e-mail unless it's was expected to be sent by a good friend.

I get these e-mails a lot, even at my e-mail address that is not on any mailing list.

Best thing to do is why ACK does:

AircraftkillerIve had over 2,000 in the past two months... My solution is just to delete everything from people I don't know or if their e-mail\name is obviously fucked up.

Subject: Warning: Spy Virus Spreading
Posted by England on Fri, 30 Jan 2004 10:30:34 GMT
View Forum Message <> Reply to Message

Keep this in mind

If you didnt ask for it, dont open it.

I have about 100+ emails containing this bullshit virus.

Subject: Warning: Spy Virus Spreading
Posted by Majiin Vegeta on Fri, 30 Jan 2004 11:30:20 GMT
View Forum Message <> Reply to Message

if your stupid enuff to open it.. oh well..

Subject: Warning: Spy Virus Spreading
Posted by NHJ BV on Fri, 30 Jan 2004 12:47:41 GMT
View Forum Message <> Reply to Message

Haven't seen it yet...I feel left out

Subject: Warning: Spy Virus Spreading

Posted by snipesimo on Fri, 30 Jan 2004 12:58:58 GMT
View Forum Message <> Reply to Message

Don't get norton. If you should run any AV run AVG. And also, the best way to prevent getting a virus is to not open email attachments.

Subject: Warning: Spy Virus Spreading
Posted by Deactivated on Fri, 30 Jan 2004 13:01:19 GMT
View Forum Message <> Reply to Message

And turn off HTML in Outlook

Subject: Warning: Spy Virus Spreading
Posted by Yano on Fri, 30 Jan 2004 13:35:29 GMT
View Forum Message <> Reply to Message

Lets see, I have gotten about 25 since Wensday

Subject: Misconceptions
Posted by HeXetic on Fri, 30 Jan 2004 13:59:04 GMT
View Forum Message <> Reply to Message

A couple of misconceptions to clear up.

- MyDoom "works" because it looks like a ZIP file - not the more recognizeable EXE or BAT or VBS or COM or SCR etc. files - to the unfortunate shmuck who gets it in the mail. My own dad double-clicked on it even though I've told him in the past not to do stuff like that (happily, he doesn't have administrative privileges on the computer, so the virus couldn't actually do anything).

- The "from" address in pretty much all virus and spam e-mails is forged. If the mail says it's "FROM: hexetic@planetcnc.com" it was probably sent from a 286 in the mountains of Tibet. Various schemes are used to come up with the fake return address; sometimes it's random, sometimes the viruses use previously harvested e-mail addresses. It's all just to make the virus look a little more real and *also* create more havoc by generating throusands of "bounce" messages (sent by the mailserver when a mesage can't be delivered) or "returned mail" messages (sent by the mailserver when it thinks the e-mail has a virus - of course the guy to whom the mailserver returns the mail is almost certainly not the guy who's infected).

- The #1 best way to improve your safety if you use Outlook Express is to get a virus scanner. All of them are good, provided you get the updates and configure the virus scanner to either clean or delete infected attachments; unfortunately the default action is often "try to clean" (which fails if there's nothing to clean i.e. the file is 100% virus) then pass. I prefer Trend PC-Cillin (comes free with a lot of motherboards) myself. The #2 best way to improve your safety is to turn off the Preview Pane, which is The Root Of All Evil - View->Layout->Preview Pane.

- MyDoom doesn't automagically infect you if you open the e-mail, thank goodness. You have to actually double-click on the attachment to get whacked.

- If you run with User or Power User privileges only (Win2K and WinXP), then you can't get infected as you don't have the ability to install programs - including viruses like MyDoom.

---

Subject: Warning: Spy Virus Spreading
Posted by MrBob on Fri, 30 Jan 2004 23:09:42 GMT
View Forum Message <> Reply to Message

I haven't gotten any with my Cox account. Maybe I should check my theoriginalmrbob.com account, I already get 40+ crap emails a day.

I was once stupid and opened a PIF file (thinking it was an image). I was still able to use the computer until I got Norton a few months later.

---

Subject: Re: Misconceptions
Posted by gibberish on Fri, 30 Jan 2004 23:59:16 GMT
View Forum Message <> Reply to Message

HeXeticA couple of misconceptions to clear up.

- If you run with User or Power User privileges only (Win2K and WinXP), then you can't get infected as you don't have the ability to install programs - including viruses like MyDoom.

Although I would recommend only running with the priviledges you need to do your every day stuff.

The worst thing you can do is to become complacent about viruses.

You should never run suspicious files even as an ordinary user.
Unfortunately MS have too many privilege escalation bugs in their OS'es, for me to believe that "I am safe as long as I am not logged on as an administrator".

Just by 2 cents,
Gib

---

Subject: Warning: Spy Virus Spreading
Posted by Ferhago on Sat, 31 Jan 2004 14:10:46 GMT
View Forum Message <> Reply to Message

I have gotten two of these such emails. One was from "The _Cozzy@something" and the other I dont remember. I usually delete any email I dont expect

Edit: Just got a third one from "cncgenocide@aol.com" Must be pulling them from te forums

Subject: Warning: Spy Virus Spreading
Posted by Scythar on Sat, 31 Jan 2004 15:51:37 GMT
View Forum Message <> Reply to Message

Let's see....I've got none at all, and I use Hotmail.

Subject: Warning: Spy Virus Spreading
Posted by Matt2405 on Sat, 31 Jan 2004 16:41:51 GMT
View Forum Message <> Reply to Message

I got 2, one from "SomeRhino@renevo.com" and one from "takavar2@yahoo.com" at first. And I recieved a load more after, I would say I have recieved about 8 all from different people.

Subject: Warning: Spy Virus Spreading
Posted by Jaspah on Sat, 31 Jan 2004 20:38:39 GMT
View Forum Message <> Reply to Message

So far so good... Does the virus effect the Hotmail.com servers? Or the fact I use their service, not Microsoft Outlook?

EDIT: It doesn't effect Hotmail servers! Yay!

(I checked the Symantec databases.)

Subject: Warning: Spy Virus Spreading
Posted by IRON FART on Sat, 31 Jan 2004 21:02:57 GMT
View Forum Message <> Reply to Message

Most web services have filters...Use them.

Also if you use Outlook Express, turn off the prieview pane.

Subject: WRF????
Posted by TAKAVAR on Sun, 01 Feb 2004 03:28:44 GMT
View Forum Message <> Reply to Message

WTF . i didn't open shit , how did i get it ? i'm TAKAVAR2@yahoo.com
meeh ...
well . i'm going to remove it now . but this is ....

---

Subject: Warning: Spy Virus Spreading
Posted by TAKAVAR on Sun, 01 Feb 2004 04:17:46 GMT
View Forum Message <> Reply to Message

ok this is wierd now
northon's anti virus or even the special removal tool for my doom virus didn't detect ANY thing ...
donnu whats going on ...

---

Subject: Warning: Spy Virus Spreading
Posted by sniper12345 on Sun, 01 Feb 2004 04:24:51 GMT
View Forum Message <> Reply to Message

I think they harvested your email, you didn't "submit" it.

---

Subject: Warning: Spy Virus Spreading
Posted by exnyte on Sun, 01 Feb 2004 06:42:10 GMT
View Forum Message <> Reply to Message

The reason it was recieved from you is it pulls email addresses from:

symantec.comSearches for the email addresses in the files with the following extensions:

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

It uses the email addresses it pulls off of these files to send email to and use as the "from" on those emails.

---