

Net-Sec mini letter  
Issue 10 - 04.05.2000  
<http://net-security.org>

This time mini letter will provide you all of information on new virus that is cruising around the Web.

There is no much information on it, but few resources and submissions could describe you possible problems with it.

>From The Register ([www.theregister.co.uk](http://www.theregister.co.uk))  
by Tim Richardson

A virus that panders to people's vanity is doing the rounds and it's got more bite than genital herpes. Called ILOVEYOU, it has an attachment called LOVE-LETTER-FOR-YOU.TXT.vbs. If you receive it, don't open it. The virus appears to have originated from the Philippines and has been described by one expert as the "the most beautifully written virus" he's ever seen. It converts .mp3, .jpg and other files to .vbs files which contain the virus. Unconfirmed reports claim that the City of London has been brought to its knees because of the affectionate virus.

>From AVP.ch mailing list ([www.avp.ch](http://www.avp.ch))

We are getting numerous infection reports about VBS.LoveLetter from Switzerland and other countries. It is spreading rapidly via Email. If you receive an Email with the subject "ILOVEYOU" containing an attachment "LOVE-LETTER-FOR-YOU.TXT.vbs", do not open the message and certainly do NOT open the attachment. Delete this message right away. Detection records for VBS.LoveLetter have been added to AVP's daily update stream. So, please update your AVP using the integrated online updater. More information will be posted to [www.avp.ch](http://www.avp.ch) as soon as it becomes available!

>From Trend Micro web site ([www.antivirus.com](http://www.antivirus.com))

VBS\_LOVELETTER  
Risk rating: HIGH RISK  
Destructive: YES  
Aliases: LOVELETTER

Description:

Note: This virus is currently in the wild and is spreading rapidly.

Once executed this computer worm modifies registry and drops files for it to spread. It replicates via Microsoft Outlook by sending an email with an attachment file "LOVE-LETTER-FOR-YOU.TXT.vbs" to all email addresses listed in the address list. It also propagates using mIRC by modifying the "script.ini." After connecting to a chat server using mIRC, the virus initiates a DCC send to all the users in the current channel and sends a copy of itself. It is also capable of infecting files with specific extensions.

We received unconfirmed report that VBS\_LOVELETTER virus hit government computers.

Thanks to Lady Sharrow and acopalypse for contributing about this virus.

This information is also available on line on the following URL:

"<http://www.net-security.org/cgi-bin/reports/fullnews.cgi?newsid957448436,24131>,"

HNS Staff  
staff@net-security.org  
<http://net-security.org>