New email virus potentially more damaging than "Love Bug"

Mike Ingram
20 May 2000

A new computer virus was reported May 18 which is said to be potentially more damaging than the so-called "Love Bug" which caused up to $10 billion worth of damage to world-wide computer networks earlier this month.

Early reports and a press release by anti-virus company Symantec indicated that the new virus was a variant of the Love Bug. This is not actually the case, according to Symantec's Vincent Weafer. He told CNET News that while the viruses share key characteristics, such as the reliance on Microsoft's Outlook address book and VBS scripting language, they do not share source code.

Like the Love Bug, the new virus takes advantage of features in Microsoft's Outlook email program to send itself to all contacts in the victim's address book. The virus is written as a VisualBasic attachment, which can be recognised by the suffix ".vbs".

While the Love Bug only affects image and sound files, the new virus destroys everything on the computer—data, programs and crucial operating software. It targets files on both the computer's local hard disk as well as any network drives to which it may be connected.

The new virus is said to be far more sophisticated than its predecessor. It does not overwrite files, but shrinks them down to nothing. Moreover, the new virus imitates those in the biological world by making subtle alterations as it spreads.

First the virus changes the subject header of the email by selecting at random from various document files found on the victim's computer and adopting that file's name, preceded by "FW:". The virus then renames itself with the same file name followed ".vbs". Finally, the virus inserts random text into the VBS script itself. This does not alter the behaviour of the virus in any way, but serves to throw virus scanners off track.

The change to the subject line of the message and the name of the file containing the virus is particularly dangerous. While many people would be naturally suspicious of file attachments with unusual names, particularly in the aftermath of the Love Bug, a forwarded file from a business associate or friend with an attachment named in this manner may be less obvious. For example, someone expecting a file named accounts.xls from a business associate could receive the virus in the disguise of accounts.vbs. While the .vbs suffix would put a more knowledgeable user on guard, it could easily be opened without the victim noticing the .vbs extension.

The virus has not been reported in anything like the volume of the Love Bug, though virus experts have classified it as high risk. The outbreak has also been confined largely to the US with the exception of two reports from the UK. So far no reports have been received from Asia or the Pacific, according to anti-virus experts.

Antivirus firm Trend Micro said one corporate customer had reported that all 5,000 of its desktop computers received the virus, but the company did not know how many users had actually opened it. The company is said to have received the virus from its office in Israel, but Trend Micro has cautioned against assuming that the virus originated there. Most experts believe it originated in the US.

It is not unusual for a spate of new viruses to emerge in the aftermath of the type of publicity received by the Love Bug. The attention focused on the inherent weaknesses of Microsoft's email package, moreover, may have encouraged other cyber vandals.

After two weeks of sharp criticism from security experts, Microsoft has finally announced that it is working on a fix for the program. This won't be available until May 22. However, the spread of the latest virus may be slowed as a result of increased awareness of the dangers of email attachments brought home by the Love Bug attack.

Meanwhile, the source of the May 5 Love Bug virus is

© World Socialist Web Site

not yet clear, with investigations still under way in the Philippines. Latest reports indicate that it may have been part of an organised campaign of a computer programming group calling itself Grammersoft.

A computer disk found in a Manila apartment raided by the National Bureau of Investigations (NBI) contained a program with the same characteristics as the Love Bug virus. The disk credits 40 people with creating the program. Elfren Meneses, director of the NBI's anti-fraud and computer crimes division, said, "The virus found in the document files was supposedly authored by Michael Buen, an [Amable Mendoza Aguiluz Computer College] student, with acknowledgement to Onel de Guzman and a certain group called Grammersoft."

The apartment raided by the NBI is the home of 22-year-old Onel de Guzman and his sister Irene. Buen and de Guzman were both students at AMACC and the school says they were both members of Grammersoft. The lawyer of Onel de Guzman last week said it was possible that de Guzman may have accidentally transmitted the virus.

Buen denies any involvement with the design or dissemination of the Love Bug, but came under investigation as a result of a thesis he submitted to AMACC dealing with multiple saving functions, a key component of the Love Bug virus. Meneses said the diskette found in the apartment raid carried Buen's resume, together with a message saying, "If I don't get a stable job by the end of the month, I will release a third virus that will remove all folders in the primary hard disk." Meneses said that of the 40 named on the disk, 30 were also students at AMACC.

Notwithstanding the statements of Meneses, too little is known at present and reports emerging from the Philippines remain too contradictory to say with any degree of certainty that Buen or de Guzman were responsible for the Love Bug virus.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact

© World Socialist Web Site