More than 20 countries affected

"Love-Bug" virus damage estimated at $10 billion

Mike Ingram
10 May 2000

It is estimated that the so-called "Love-Bug" email virus has caused some $10 billion in losses in as many as 20 countries.

The virus was originally distributed in an email with the subject line "I love you". The message contains the text "kindly check the attached LOVELETTER from me" and an attached file called LOVE-LETTER-FOR-YOU.TXT.VBS. If this attachment is opened it will replicate itself and be transferred to all addresses within a user's email address book. The virus also deletes graphic files ending with the letters jpg or jpeg, and alters music files ending in mp3 to make them inaccessible.

The victim's Internet browser is directed by the virus to visit four web sites in the Philippines, where another malicious program called WIN-BUGSFIX.EXE is downloaded. This program searches the victim's hard drive for password files and sends them to an Internet account in the Philippines, managed by Access Net Inc., an Internet service provider.

Since the original attack last week, the virus has continued to circulate in new and particularly dangerous variants calculated to cause the maximum damage. One such new message has the subject heading "Virus warning" and another is marked "Mother's Day Order Confirmation." The latter tells the recipient that $326.92 is being charged to his credit card for a "diamond special" and urges him to review the attached invoice, which contains the virus.

It is estimated that there are at least 10 new variants of the virus in circulation. A new virus with the title "Friend Message" and containing the file FRIEND_MESSAGE.TXT.vbs is also in circulation. The results of this are the same as the LoveLetter virus but the code has been completely rewritten. Virus detection software upgraded to detect the original "Love-Bug" will not detect this new and no less destructive version.

Security experts and systems administrators warn that all email attachments from unknown sources should be regarded with suspicion and that files with the VBS extension should never be opened.

The search for the author of the virus, which shut down the email service of the British parliament and attacked the computers of the Pentagon and CIA in the US, focused on the Philippines, after security experts scrutinised the code of the virus.

Initial reports that the author had used the name "spider" proved to be misleading. The references to "spider" in the software code were, in fact, references to the author of the password collection software used in the file "WIN-BUGSFIX.EXE", which infected computers were directed to download. Stolen passwords were emailed to accounts at Access Net in the Philippines with the message, "Barok... e.mail.passwords.sender.Trojan-by spyder."

Barok is the name of popular password-stealing software and "spyder" is the name used by the hacker who created it. Barok is currently at version 2.1 and was released on underground Internet sites about a month ago. An earlier version of the software included a reference to Amable Mendoza Aguiluz Computer College (AMACC) in the Philippines. The words "Manila, Philippines" were also found elsewhere in the virus code.

As the details of the computer code were revealed, experts feared that the clues were so numerous that they could have been left deliberately as false tips, to throw

investigators off track. "This may be somebody putting us on, and the reality is, he might be sitting in his boxer shorts in New Jersey having a good laugh a us," warned Elias Levy, chief technology officer at SecurityFocus.Com of San Mateo, California.

A computer expert in Sweden said Saturday that he believed the attack was the responsibility of an 18-year-old German exchange student in Australia who had hacked into computers in the Philippines, but Australian Federal Police say they have been given no firm evidence to back up the allegation.

Despite conflicting opinions as to the validity of the details left in the computer code, a full-scale hunt for the authors of the virus has focused on the Phillipines.

Over the weekend of May 6-7, the Philippines National Bureau of Investigations (NBI), accompanied by officers of the US Federal Bureau of Investigations (FBI), arrested 27-year-old Reomal Ramones following a surveillance operation outside his home in the Bagong Barangay suburb of Manila. Irene de Guzman, said to be Ramones' live-in girlfriend, is also sought by police.

It is by no means certain that Ramones or de Guzman, both bank workers, were involved in the attacks. Security experts say that even if the attacks were traced to a computer in the house, this could also have been the work of hackers who used the computer to launch the attacks without the knowledge of the owners. Attorneys for both Ramones and Guzman say they deny any involvement in the virus attacks.

Ramones was released Tuesday after Philippine prosecutors ruled that police did not have enough evidence to hold him.

Investigators were led to the Bagong Barangay house after Access Net examined chat room logs containing incriminating references to hacking and the creation of viruses. These were traced back to an email account said to belong to either Ramones or de Guzman.

It was revealed that Ramones and Guzman both attended courses at AMACC and the college has now become the focus for further investigations. NBI officer Elfren Meneses said some eight other people with links to the school could be involved in the spread of the virus. He told reporters there were 10 coded names found embedded in the virus. "There were reports from the FBI that the names are somewhat from an organisation called AMACC," he said.

Whoever turns out to be behind the virus attacks and whatever their motives, acts of vandalism such as these serve no positive political or social purpose. The justifiable and widespread concerns that these attacks generate are used by governments to instigate new police powers and more intrusive forms of control over the Internet. This is already illustrated by the massive police operation under way in the Philippines and the sensationalised media coverage it is receiving.