Email virus wreaks havoc on corporate networks throughout Europe and America

Mike Ingram
6 May 2000

A computer virus, which has become known as the "love bug," has spread rapidly across corporate networks connected to the Internet.

The virus, embedded in an email with the subject line "I love you," first appeared May 4 in Asia and rapidly spread throughout Europe, causing the British House of Commons to shut down its email system for two hours.

By the time offices opened for work in the US, system administrators were aware of the virus but many networks had already been infected and others took the decision to shut down while inoculation software was upgraded. Companies affected included Ford Motor Co., Microsoft Corp. and Estee Lauder. The US Army and Navy also shut down their electronic mail systems.

If the "love bug" email is opened, a line of text tells users to "kindly check the attached LOVELETTER from me" and an attached file called LOVE-LETTER-FOR-YOU.TXT.VBS. If the file is ignored it will cause no harm, but if the 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 and jpeg and alters music files ending in mp3 to make them inaccessible.

Indicating that the virus may be part of a more sustained attack, it directs the victim's Internet browser 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.

Though password files are usually encrypted, decoding tools are readily available, making it relatively easy for hackers to use the passwords to breach the security systems of corporate computer networks and gain access to material or carry out further actions, such as the “denial of service” attacks that brought down a number of prominent commercial web sites earlier this year.

The chief operator of Access Net, Jose O Carlotta, said he was taking steps "to identify the parties responsible."

Within the software code sent with the email, the author left the name "spyder" and a message, "I hate [to] go to school." The words "Manila, Philippines" were also found in the code, prompting initial investigations to focus on the Philippines as a possible source of origin. Also embedded in the code was a reference to an account at a New York email service, Mail.com Inc. A spokeswomen for the company told the *Wall Street Journal* that they found "no evidence that the owner of that account or of any other Mail.com account has any connection to the virus."

The embedded references and the simple character of the software code indicate that the virus may have been the work of a child. US government investigators said the code "doesn't look like the work of someone real mature." Security experts warn that the messages may have been left deliberately in order to throw investigators off track.

As system administrators fought to counter the effects of the initial virus, within 24 hours a new strain emerged. In what are thought to be copy-cat attacks, the virus began to reappear in email messages with the subject line of "FWD: joke," and including the file "VERY FUNNY."

Security experts fear that the impact of the virus could be even greater than the "Melissa" virus of March 1999, which caused at least $80 million in damages. A 31-year-old programmer in New Jersey, David L. Smith, pleaded guilty in December 1999 to having created that virus.

The virus could prove embarrassing for Microsoft as it only affects users of the company's Outlook email program. The specific features of the program that helped replicate the virus are not needed by the majority of users, drawing attention to one aspect of the government case against Microsoft—the bundling of features that are not really needed. The rapid spread of the virus also draws attention to the unrivalled monopoly exercised by Microsoft, which controls 90 percent of the market for business applications.

As with the Melissa virus, the problem lies with Outlook's use of Microsoft's Visual Basic programming language, known as VBScript or VBS. VBScript is widely used in business software to allow different applications to work together. VBS allows the automation of certain electronic events. For example, an employee can download sales report forms from a corporate web site and automatically send the completed form to the sales manager over the Internet. Hackers can use these automatic events and manipulate VBScript to gain access to address books and automatically send thousands of email messages. This is exactly what happened with both the so-called "love bug" and the Melissa virus.

Microsoft responds to criticism by pointing out that code such as VBScript helps run many business-critical applications, and is asked for by users. Some experts believe there is a necessary trade-off between functionality and security, but this is rejected by Joe Chung, the chief technology officer at Art Technology Group Inc, which makes e-commerce software. "These types of viruses have been really well-known for years. It's kind of like if someone went around building houses, and made it so that anyone could get in through the basement," he said.

The source of these attacks is not yet known. It could be the work of a disgruntled individual or even a school boy, as indicated by the code of the virus. It may just as easily be part of an increasing wave of misguided cyber protests against big business.

Whatever their source or motivation, attacks such as these serve no positive political or social purpose. They do nothing to lessen the dominance of capitalist corporations upon society and are ultimately used by governments to instigate new police powers and more intrusive forms of control over the Internet.

The immediate outcome of recent acts of cyber vandalism against Yahoo.com and other web sites was the raiding of an Internet Service Provider in Canada, forcing it to hand over personal details of users. As the hunt for the author of the "love-bug" virus gets under way, one can expect to see new legal precedents for enhancing the powers of electronic surveillance and the strengthening of anti-democratic encroachments on freedom of access and expression on the Internet.