New Worm Targets Portable Memory Drives

May 5 2007

Sophos researchers say worm is an example of hackers targeting removable devices in an effort to get around security.

Researchers from security vendor Sophos say a new worm targeting removable drives is an example of a potential security threat for businesses.

The SillyFD-AA worm searches for removable drives such as floppy disks and USB memory sticks and creates a hidden file called autorun.inf so that a copy of the worm runs the next time the device is connected to a computer running Windows. In addition, it changes the title of Internet Explorer windows to say that the computer has been "Hacked by 1BYTE."

In an interview with eWEEK, Graham Cluley, senior technology consultant at Sophos, said the worm has not been widely distributed, and that researchers were warning the public because of the potential danger. It would be easy, he continued, to add to the worm the ability to transmit through other routes, such as e-mail and instant messaging.

"It is interesting to see hackers using different techniques in their attempt to break into peoples' computers," said Cluley, in Abingdon, United Kingdom. "This type of attack is perhaps understandable as so many businesses these days do have e-mail gateway protection in place…they can scan files coming into their company via e-mail attachments, but can't check the files coming in attached to the keychain in peoples' pockets."

Sophos researchers said hackers are increasingly looking for ways to attack businesses that will meet less resistance than more traditional e-mail-borne viruses and malware. The company's security experts advise users to disable the autorun facility of Windows so removable devices do not automatically launch when they are attached to a computer. Any storage device that is attached to a computer should be checked for virus and other malware before use, Sophos officials said.

"Companies may also consider installing software which locks down and controls access to external drives such as USB sticks," Cluley said. "In some firms this may make sense not just because of the malware threat, but also the problem of employees stealing sensitive or confidential information out of a company on their USB drive."

Sophos officials recommend companies automatically update their corporate virus protection, and defend their users with a consolidated solution to defend against the threats of viruses, spyware, hackers and spam.

However, the threat of this particular worm is limited, partly because up-to-date desktop anti-virus software should be capable of intercepting the virus when it tries to run after a user has plugged in the USB memory stick, Cluley said.