



Fernando de la Cuadra
Editor Técnico Internacional
Panda Software (www.pandasoftware.es)
E-mail: Fdelacuadra@pandasoftware.es



Bugbear.B, polymorphic viruses and detection

In order to escape antivirus activity, Bugbear.B uses polymorphism, and as a result only antivirus programs with the highest capacity of virus detection can detect it. Through this technique, it changes every time it is run or replicates, making it difficult for antivirus programs to recognize it.

Malicious code use many techniques to hide from antivirus activity, such as stealth (hiding visible signs of infection), tunneling (in order to 'dodge' resident antivirus protection) or encryption to prevent the antivirus from doing its job.

With the appearance of Windows operating systems, many of these techniques fell into disuse, whereas polymorphism has survived as a system for preventing antivirus programs from finding malicious code.

The most widely used technique for detecting malicious code is algorithmic, which consists of looking for a sequence of bytes that identify a certain virus. This method has been used since antivirus programs were invented. However, for this method to be effective, the virus must not change, so that the sequence of bytes stored in the virus signature file in an antivirus program always matches that in the virus code.

A classic polymorphism system is encryption. In order to encrypt content, an encryption routine is essential. If a different encryption routine is used each time, the virus will change every time.

Panda Software uses a special technology that allows its antivirus engine to effectively detect polymorphic viruses. This system, called Generic Decryption Engine or GDE, decrypts polymorphic viruses making it possible to detect them.

Before a polymorphic virus can be decrypted, it must first be run, and running a virus on a computer results in infection. For this reason, Panda Software has opted to develop an emulator, which simulates the virus being run, in a special secure zone in the memory of the computer. As soon as the virus has been decrypted, the antivirus engine will be able to find the sequence of bytes that identifies the virus, or in other words, detect it. Logically, this process must be completed in record time without the user being aware of the extremely complex task that the antivirus is carrying out in order to detect the virus.

Users of products like Panda Software's antivirus solutions, which are capable of detecting any kind of virus, can test the technology used to fight viruses, regardless of the system they use to hide.

More information about the Bugbear.B worm is available in Panda Software's Virus Encyclopedia at:

http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?idvirus=39823