

## Cómo se clasifican los códigos maliciosos (I)

**Madrid, 18 de junio de 2003.** - Existe una cierta confusión en lo que a la clasificación de los distintos códigos maliciosos se refiere. No es raro ver cómo se utilizan términos tales como "virus" o "gusano" indistintamente. Sin embargo, cada uno de estos nombres responde a un tipo de código malicioso en concreto que posee características propias.

En realidad, todos los códigos maliciosos pueden englobarse dentro de un concepto mucho más amplio denominado *malware*, y que puede definirse como cualquier programa, documento o mensaje susceptible de causar perjuicios a los usuarios de sistemas informáticos.

Así, dentro del *malware* se encuentran los llamados genéricamente **virus**. Se trata del tipo de código malicioso más abundante y que, por lo tanto, suele protagonizar los incidentes más graves. Sin embargo, en realidad, el conjunto de los virus esta compuesto por tres subgrupos: **virus**, **gusanos** y **troyanos**.

Los **virus** son programas informáticos capaces de multiplicarse mediante la infección de otros programas mayores e intentan permanecer ocultos en el sistema hasta darse a conocer. Pueden introducirse en los ordenadores de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.

Por su parte, un **gusano** es un programa similar a un virus que, a diferencia de éste, solamente realiza copias de sí mismo, o de partes de él. Así, no necesita infectar otros archivos para poder multiplicarse.

Finalmente, los **troyanos** son programas que llegan al ordenador por cualquier medio, se introducen en él, se instalan y realizan determinadas acciones para tomar el control del sistema afectado. La historia mitológica "El caballo de Troya" ha inspirado su nombre.

Los programas que conocemos como "antivirus" tienen como misión principal detectar y eliminar los tipos de códigos maliciosos antes mencionados, ya que, en la práctica, son los que pueden causar daños más importantes a los sistemas.

Sin embargo, esta clasificación debería ser revisada en un futuro no muy lejano, debido a la aparición de nuevos tipos de códigos maliciosos que reúnen características de más de un grupo. Un claro ejemplo lo constituyen los gusanos-troyanos que, como su nombre indica, incorporan características de ambos grupos.

Además, los códigos maliciosos son cada vez más sofisticados sobre todo en lo que a formas de propagación se refiere. De hecho, ya existen códigos maliciosos que se distribuyen directamente a través de Internet.

Debido a ello, los programas antivirus deben evolucionar al mismo tiempo que lo hacen las técnicas para la creación de códigos maliciosos. Es fundamental que el antivirus que se tenga instalado tenga actualizaciones diarias del fichero de firmas de virus y del propio motor del antivirus cada vez que las circunstancias lo requieran. Asimismo, deben tenerse en cuenta las nuevas formas de propagación de los virus, o la posibilidad de ataques por parte de hackers destinados a introducir algún tipo de código malicioso en el ordenador. Como ejemplo puede citarse a Panda Antivirus Platinum 7.0, que incorpora un firewall personal de última generación y se actualiza de forma diaria y automática, por lo que está siempre preparado contra cualquier amenaza procedente de Internet.