

## Cómo se clasifican los códigos maliciosos (II). Los nuevos virus

**Madrid, 25 de junio de 2003.** - Cada vez con más frecuencia aparecen nuevos virus con características muy particulares. Esto hace que la actual clasificación de los virus en tres subgrupos denominados virus, gusanos y troyanos ya no sea todo lo satisfactoria que debiera.

Existen virus que podríamos describir como "código puro", ya que no necesitan estar empaquetados en un archivo para llevar a cabo sus acciones. Así, son capaces de transmitirse directamente a través de Internet. Tal es el caso de uno de los gusanos más famosos de los últimos tiempos: **CodeRed** ([http://www.pandasoftware.es/virus\\_info/enciclopedia/verficha.aspx?idvirus=39131](http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=39131)). Sin embargo, esto sólo es un cambio de forma ya que se multiplica y realiza acciones similares al del resto de gusanos conocidos. Por ello, en este caso no habría ningún problema para ubicarlo dentro de la clasificación antes mencionada.

El problema surge cuando se trata de códigos maliciosos "**híbridos**", es decir, que combinan características propias de dos o más tipos de virus. Un caso muy claro de un código malicioso de este tipo sería **Nimda** ([http://www.pandasoftware.es/virus\\_info/enciclopedia/verficha.aspx?idvirus=33307](http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=33307)), capaz de propagarse como un gusano, de infectar archivos ejecutables tal y como lo hace un virus y, además, de explotar una vulnerabilidad de Internet Information Server para infectar páginas web que, a su vez, serán capaces de infectar los equipos de los usuarios que las visiten.

Más ejemplos de este tipo de virus "inclasificables" serían **Lovgate** ([http://www.pandasoftware.es/virus\\_info/enciclopedia/verficha.aspx?idvirus=39620](http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=39620)), que combina características de virus, gusano y troyano, o **Bride** ([http://www.pandasoftware.es/virus\\_info/enciclopedia/verficha.aspx?idvirus=37563](http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=37563)), un gusano que incorpora una modificación del peligroso **Funlove** ([http://www.pandasoftware.es/virus\\_info/enciclopedia/verficha.aspx?idvirus=25844](http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=25844)).

Un tipo de virus muy abundante en los últimos tiempos es el llamado **gusano/troyano**. Sin embargo, en este caso no puede hablarse de un solo código malicioso que tenga características comunes a ambos tipos de virus, ya que normalmente suelen tener dos componentes: uno que actúa como gusano y otro que hace las funciones de troyano. Este último puede que ni siquiera vaya acompañando al gusano en un primer momento, sino ser descargado posteriormente desde alguna página web .

Existen también los virus denominados "autoactualizables", es decir, capaces de mejorar sus funcionalidades mediante descargas desde páginas web. Sin embargo, y gracias a la colaboración de los proveedores de servicios de Internet, las páginas donde se almacenan dichas actualizaciones suelen cerrarse de manera casi inmediata. Debido a ello, no se trata de una técnica muy empleada. Como ejemplo, podríamos citar al gusano **Opaserv**

[http://www.pandasoftware.es/virus\\_info/enciclopedia/verficha.aspx?idvirus=37403](http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=37403)).

Pueden mencionarse también casos curiosos, como el de gusano **Sobig.B** ([http://www.pandasoftware.es/virus\\_info/enciclopedia/verficha.aspx?idvirus=39628&sind=0](http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=39628&sind=0)) (o **Palyh**) que, además de otras acciones, trata de aumentar el número de visitas a una determinada página web, o los virus que son creados como respuesta a un conflicto político. Aquí podría citarse al gusano **Lentin** ([http://www.pandasoftware.es/virus\\_info/enciclopedia/verficha.aspx?idvirus=36830](http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=36830)), desarrollado y puesto en circulación por un grupo Indio con la intención de lanzar ataques de denegación de servicio (DoS) sobre páginas web de Pakistán, su enemigo tradicional. Otro caso similar sería el de **CodeRed.F** ([http://www.pandasoftware.es/virus\\_info/enciclopedia/verficha.aspx?idvirus=39131](http://www.pandasoftware.es/virus_info/enciclopedia/verficha.aspx?idvirus=39131)), que estaba diseñado para llevar a cabo un ataque DoS sobre la web de la Casa Blanca.

Con todo esto, puede observarse como los creadores de virus siempre intentan ir un paso más allá, por lo que, para mantener un sistema protegido, no queda otra alternativa que contar con la presencia en el equipo de un software antivirus de reconocido prestigio que disponga de actualizaciones diarias. Es el caso de Panda Antivirus Platinum 7.0 que, para evitar los ataques de hackers y de virus que se propagan directamente a través de Internet, incorpora un firewall personal de última generación.

### Información adicional

- **DoS / Denegación de servicios:** es un ataque, causado en ocasiones por los virus, que evita al usuario la utilización de ciertos servicios (del sistema operativo, de servidores Web, etc).

- **Firewall / Cortafuegos:** su traducción literal es *muro de fuego*, también conocido a nivel técnico como *cortafuegos*. Es una *barrera* o protección que permite a un sistema salvaguardar la información al acceder a otras redes, como por ejemplo Internet.

Más definiciones técnicas relacionadas con los virus y los antivirus en:

<[http://www.pandasoftware.es/virus\\_info/glosario/default.aspx](http://www.pandasoftware.es/virus_info/glosario/default.aspx)>