

II CAMPAÑA CONTRA EL FRAUDE ONLINE Y POR LA SEGURIDAD EN LA RED.

## **Aumenta el uso combinado del spam y de las técnicas de ingeniería social como método para distribuir malware**

**- En los últimos días se han producido varios envíos de correos con malware incorporado como el gusano Nurech.Z o Grum.A**

**- Los ciber- delincuentes utilizan técnicas combinadas de spam e ingeniería social como reclamo para que el propio usuario descargue el archivo infectado**

PandaLabs ha detectado un aumento en el uso combinado del spam y de técnicas de ingeniería social para distribuir malware. En los últimos días ha habido varios ejemplos como es el caso del envío de correos con una alerta de malware con asuntos como: Worm alert! (alerta gusano) o spyware alert! (alerta software espía) que llevaban incorporados el gusano Nurech.Z. Para hacer más creíble el mensaje, los ciber-delincuentes utilizaron como remitente el nombre de fuentes confiables, como Customer Support.

Otro caso reciente utilizaba como reclamo fotos de la cantante Britney Spears. El correo electrónico tenía asuntos como Britney spears naked pussy & paris Hilton o Hot pictures of Britiney Speers . Al abrir el correo, los usuarios se encontraban con diversas fotos eróticas de esta cantante. Cuando pinchaban sobre esa foto para acceder a más fotografías, automáticamente se descargaban en su ordenador un código malicioso que aprovechaba la vulnerabilidad en los ficheros ANI de Microsoft para propagarse. Este código, a continuación, descargaba otro u otros ejemplares de malware en esos ordenadores.

El tercer ejemplo se ha producido unos días más tarde, aunque con las mismas características del anterior, pero cambiando la protagonista. En este caso se han utilizado fotos de la actriz porno Jenna Jameson como reclamo para hacer pinchar a los usuarios sobre el link oculto en las fotografías. El resultado era el mismo: un código infectaba el ordenador aprovechando la vulnerabilidad de ficheros ANI y procedía a descargar más malware.

También se han recibido correos en los que el asunto era Hot pictures of paris hilton nude u otros similares. El objetivo siempre es el mismo: tentar a los usuarios con un tema de su interés para que pinchen el vínculo y caigan en la trampa. Esto es lo que se conoce como ingeniería social , explica Luis Corrons, Director Técnico de PandaLabs.

Un último ejemplo fue el utilizado para difundir el gusano Grum.A. Este malware se propagaba en correos que ofrecían una beta de Internet Explorer 7. Como en el caso anterior, en el interior el usuario encontraba una gran fotografía que, supuestamente, permitía el acceso a esa versión beta.

¿Por qué usar el spam para difundir malware? Por un lado, con el correo basura se consigue llegar a un gran número de personas, lo que aumenta las posibilidades de éxito. Por otro, lo que intentan los ciber-delincuentes es que sea el propio usuario el que se descargue el archivo infectado, en lugar de adjuntar ficheros que puedan ser detectados y eliminados por los antivirus antes de que llegue al cliente de correo.

[PandaLabs](#)

**Fecha artículo: 2007-04-17 10:59:57 - url artículo: <http://www.internautas.org/html/4172.html>**

**Logos y marcas propiedad de sus respectivos autores.**

**Los comentarios son propiedad y responsabilidad de cada autor.**

**© 1998-2009 Asociación de Internautas - <http://www.internautas.org>**

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: [asociacion@internautas.org](mailto:asociacion@internautas.org)