

## **PandaLabs advierte a los usuarios sobre una oleada de correos fantasma .**

- **En las últimas horas un gran número de usuarios de todo el mundo están recibiendo emails que tienen como remitente y destinatario la propia dirección del usuario, si bien no contienen ningún tipo de malware**
- **La recepción de uno de estos mensajes puede implicar que esa dirección de correo forma parte de alguna base de datos empleada por ciberdelincuentes para llevar a cabo acciones como envío de spam, ataques phishing, o distribución de ejemplares de malware.**

En las últimas horas PandaLabs está detectando numerosos casos de usuarios de todo el mundo que han recibido mensajes de correo que tienen como remitente y destinatario la propia dirección del usuario. Dichos correos electrónicos tienen como asunto y cuerpo de texto -que está en formato HTML- cifras escogidas aparentemente al azar.

En realidad, estos emails no son enviados desde la dirección del usuario, sino que utilizan la táctica del falseamiento de direcciones o *spoofing* , es decir, aparentar que la dirección de la que proviene el mensaje es otra distinta a la original.

Hay que señalar que dichos mensajes no contienen ningún tipo de malware, por lo que, en ese sentido, los usuarios pueden estar tranquilos. Sin embargo, lo que sí debe preocupar es que la recepción de uno de estos mensajes implica muy posiblemente que esa dirección de correo forma parte de alguna base de datos empleada por ciberdelincuentes para llevar a cabo acciones maliciosas. Las mismas pueden ser desde el envío de spam publicitario, hasta la realización de ataques phishing, o la distribución de ejemplares de malware conocidos o desconocidos.

Según Luis Corrons, director de PandaLabs: Lo más probable es que un grupo de hackers esté comprobando la validez de su base de datos de direcciones de correo electrónico. Mediante el envío de estos mensajes pueden determinar las que se encuentran en activo y eliminar las que ya no sirven. Por otra parte, lo que más sorprende a los usuarios es que el mensaje proceda de su propia dirección de correo electrónico; esto no tiene nada de misterioso, sino que se debe a que los autores de estos envíos intentan evitar así los sistemas de filtrado de correo electrónico que los usuarios puedan tener instalados, ya que nadie filtra su propia dirección de correo .

En caso de haber recibido uno de estos mensajes, y dado que es imposible determinar que tipo de ataque podría producirse, es muy recomendable contar con soluciones que integren diferentes tecnologías (antispam, antiphishing, antivirus, antispyware, etc.) de manera que puedan hacer frente a todo tipo de malware. Asimismo, y dado que a raíz de la actual dinámica del malware (que tiene como objetivo conseguir beneficio económico) los atacantes tratan de introducir sus creaciones en los sistemas de forma discreta y restringida en lugar de provocar epidemias masivas, es muy conveniente que la solución de seguridad a emplear incorpore tecnologías proactivas capaces de determinar la presencia de malware por sí mismas, sin necesidad de conocerlo con anterioridad.

No podemos saber cuándo se producirá el ataque ni la naturaleza del mismo. De lo que sí podemos estar seguros es de que alguien se está tomando demasiadas molestias como para quedarse ahí, por lo que en este caso lo mejor es prevenir. Desde luego, recibir un mensaje de estas características no

debe dejarnos indiferentes, ya que es un síntoma de que nuestra dirección de correo se encuentra en manos de indeseables , concluye Luis Corrons.

[PandaLabs](#)

**Fecha artículo: 2006-06-07 21:53:05 - url artículo: <http://www.internautas.org/html/784.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)