

Asunto: Mail server report

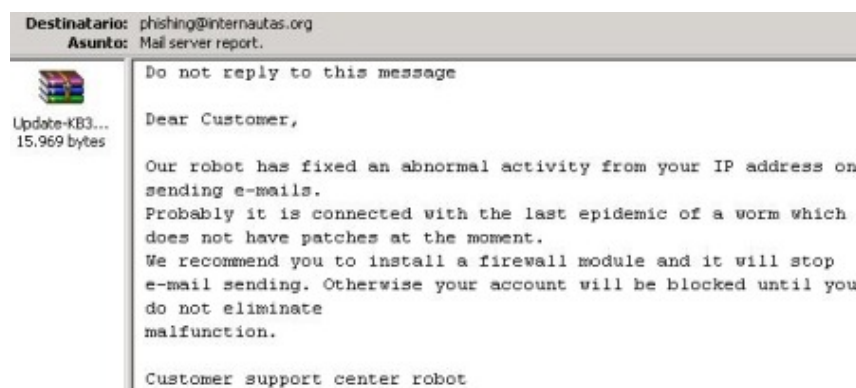
Cuidado, recepción de correos electrónicos que contienen virus / gusano.

En las ultimas horas se están detectando a gran escala la recepción de miles de correos electrónicos que contienen un falso aviso-reporte de nuestro proveedor de correo, estos fraudulentos correos incorporan una supuesta actualización, pero en realidad es un gusano.

Si usted recibe un mail con el asunto: **Mail server report**

Y además contiene un fichero adjunto con el nombre Update-KB7571-x86.zip o similar sepa que es un gusano para infectar a su maquina, este fichero no lo ejecute, puede poner en peligro su equipo.

El correo electrónico que se esta recibiendo es el siguiente:



El correo trata de convencernos de que nuestra IP es usada para infectar a otras maquinas en internet, por ello debemos de actualizar nuestro cortafuego con un nuevo modulo y de esta manera evitar una posible epidemia, si no lo hacemos nos amenaza con cerrar nuestra cuenta de correo electrónico, esta claro que el modulo que nos envía es el anzuelo para infectar nuestra maquina.

Con un fichero adjunto:



El nombre puede variar con los siguientes nombre aleatorios; **Update-KB7328-x86.zip, Update-KB3531-x86.zip, Update-KB7571-x86.zip, etc.**

La mayoría de los antivirus no detectan esta nueva amenaza por lo que se recomienda que no ejecuten ficheros de personas desconocidas, aunque como norma de seguridad si el correo electrónico es de nuestro circulo de conocidos pero no esperaba recibir un fichero es recomendable preguntarle antes por el mismo.

4d 5a 4b 45 52 4e 45 4c 33 32 2e 44 4c 4c 00 00	MZKERNEL32.DLL..
4c 6f 61 64 4c 69 62 72 61 72 79 41 00 00 00 00	LoadLibraryA...
47 65 74 50 72 6f 63 41 64 64 72 65 73 73 00 00	GetProcAddress...
e9 34 ef 00 00 42 79 44 77 69 6e 67 40 00 00 00	e4i..ByDwing@...
50 45 00 00 4c 01 02 00 00 00 00 00 00 00 00	PE..L.....
00 00 00 00 e0 00 0f 01 0b 01 00 29 00 60 00 00à.....)
00 40 00 00 00 00 00 00 30 10 00 00 00 10 00 00	..@.....0.....
00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00	..p.....@.....
04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00
00 80 01 00 00 02 00 00 00 00 00 00 02 00 00 00
00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00
00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00
be 01 01 00 28 00 00 00 00 c0 00 00 5c 09 00 00	%... (... À ... \ ...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 2e 55 70 61 63 6b 00 00 Upack ..
00 b0 00 00 00 10 00 00 2f 01 00 00 ab 00 00 00 / « ..
00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 e0 à
2e 72 73 72 63 00 00 00 c0 00 00 00 c0 00 00 00	..rsrc... À... À..
e6 41 00 00 00 02 00 00 00 00 00 00 00 00 00 00	eÀ.....
00 00 00 00 60 00 00 e0 e8 01 41 00 07 00 00 00 àè À ..
5c c9 40 00 00 00 00 ff ff ff ff 01 00 00 00 00	\E@..... yyyy ..

Otro peligro del nuevo gusano es una mutación (modificación) del mismo en las ultimas horas para esquivar los cortafuegos y antivirus que añadan las nuevas firmas (código) del nuevo gusano.

Fecha artículo: 2007-03-03 14:10:00 - url artículo: <http://www.internautas.org/html/4115.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