

DE CADENAS Y ALGO MÁS

Diseminados entre los ya muchos correos basura que recibimos a diario, hay mensajes tenebrosos que alertan la aparición de nuevos virus y programas maliciosos que pueden destruir el corazón mismo del sistema, mensajes informando que se ha ganado un premio (¡!), chicos que necesitan dinero para trasplantes, gente que ofrecen cuantiosas sumas de dinero, poesías por el día del amigo y otros parecidos, diseñados sólo para atraparnos y hacernos reenviar ese mensaje a todos los que conozcamos. Mucho de esos mensajes son "hoaxes" ("engaño" en inglés) o cadenas de correos.

Las cadenas de correos son ese sistema a través del cual pasamos a ser un eslabón al recibir mensajes masivos y reenviarlos también de forma masiva, por compasión, por solidaridad, o por cualquier razón que nos ha parecido buena.

Los mensajes en cadenas de correos raramente están infectados con virus o troyanos (una forma de virus que no destruye pero espía e informa acerca de nuestro sistema), pero sus objetivos primordiales son:

- conseguir direcciones de mail: si señores; la gran lista de direcciones de correos que aparecen por cada mensaje que usted recibe y que le ha sido reenviado en cadena servirá en un futuro inmediato para hacer SPAMS (envío de correo no solicitado). Esto implica que, cuanto más usted se involucre en estas cadenas, más correo basura recibirá porque su dirección está siendo publicada de forma intempestiva y sin control.
- congestionar los servidores de correo
- Pérdida de tiempo: lo que implica pérdida de dinero y abuso de un medio para provocar molestias indeseadas.
- deshonrar marcas y personas
- aumentar el ego del creador

Retomando, las cadenas de correos son mensajes escritos con un solo propósito: que usted lo reenvíe masivamente.

RIESGOS Y COSTOS

Los riesgos y costos de las cadenas de correos no parecen ser tan altos, menos aún si consideramos el costo relacionado a uno solo de esos mensajes en una sola computadora. Pero si consideramos todos los que reciben un correo de estos, ese pequeño costo aumenta de forma exponencial, tanto si consideramos el costo de nuestro tiempo, como si consideramos el de manipulación por parte de los servidores de correo o de nuestras propias computadoras.

Si todos en Internet estuviésemos por recibir, leer y descartar un mensaje de cadena, y si esta operación nos llevara un minuto de nuestro tiempo, el costo sería algo como:

50 millones personas bajando una cadena x 1 minuto x \$0,05/minuto = \$ 2,5 millones

Y \$0,05 es lo que gana por minuto alguien con un sueldo de \$480.

Probablemente, el riesgo más alto de estas cadenas, es su propiedad de multiplicarse. La mayoría de las personas reenvían estos mensajes a todos los que están en su libreta de direcciones. Pero pensemos qué sucede si alguien envía una cadena a sólo 10 personas. La primera persona (1ra generación) envía la cadena a 10 contactos. Cada contacto envía esa cadena a otros 10 contactos (2da generación) y así sucesivamente.

| Generación: | 1 | 2 | 3 | 4 | 5 | 6 |
|----------------|----|-----|-------|--------|---------|-----------|
| Nº de mensajes | 10 | 100 | 1,000 | 10,000 | 100,000 | 1,000,000 |

Para la sexta generación, se habrán enviado UN MILLÓN de mensajes. Imagine, sólo 6 personas en la cadena equivalen a un millón de correos. Esta capacidad debe poder ser administrada por los servidores de correo a través de la red de redes camino al destinatario, sino, los servidores pueden verse con demoras y hasta caerse.

Recuerde esto: las cadenas son para los aquellos que envían correo basura la forma de cosechar millones de direcciones de correos válidas y en funcionamiento.

TIPOS DE CADENAS

Mostramos aquí diferentes tipos de cadenas con ejemplos:

- Advertencias de códigos maliciosos (virus o troyanos)
- Mitos urbanos y leyendas: mensajes que describen algo malo que le ha ocurrido a una persona o animal con advertencias. Por ejemplo, en la época de los sobres con ántrax una famosa cadena decía que si recibe por correo convencional un sobre azul de la "Fundación Kligerman 8" que decía "Un regalo para usted", que no lo abra. Luego describía lo que contenía el sobre, cuánta gente se encontraba hospitalizada por ello y cuánta gente había muerto por la misma causa.
- Dinero de regalo: mensajes prometiendo dinero a cambio de reenvíos. Hasta hace poco circulaba un mensaje diciendo que la empresa Microsoft estaba dando cierta cantidad de dinero al que reenviaba ese mensaje, destinado a la prueba de nuevos programas a ser lanzados.
- Mensajes con información "interesante", sin consecuencias: mensajes con información sin consecuencias, que provoca en nosotros la necesidad de que todos lo sepan. Por ejemplo, circulaban mensajes acerca de "cómo actuar ante ataques cardíacos si se está solo"...
- Mensajes de simpatía y de pedidos de ayuda: mensajes con poesías por el día del amigo, o con pedidos de solidaridad a través de reenvíos para gente que necesita transplantes, que ha quedado huérfano, etc.
- Cadenas tradicionales: cadenas como las que se hacían con correo convencional, generalmente predicen mala suerte si no se reenvía a cierta cantidad de personas y hasta pedido de envío de dinero a las personas que se encuentran por encima nuestro en la cadena.
- Bromas: bromas sobre imágenes que aparecen en el monitor o sonidos graciosos.

Y existen muchas más variedades.

Pero además, recuerde esto: incluso si la información que se está publicando es verdadera, el chiste es gracioso o el poema es conmovedor, reenviar mensajes de forma masiva, publicando incluso correos de otras personas que se encuentran en nuestra libreta de direcciones ES generar una cadena de correos.

CÓMO DETECTARLAS

En casos de mensajes que advierten presencia de virus nuevos y poseen directivas de cómo proceder, debemos asegurarnos que la fuente del mensaje es realmente de la empresa que dice ser. Las empresas serias y conocidas de productos antivirus siempre facilitan direcciones de Internet a las que se pueden acceder para buscar más información acerca de ese acontecimiento.

Nuestra sugerencia es NO entrar nunca a sitios cuyos enlaces no muestran de qué empresas provienen, o sea, enlaces del estilo: <http://hgd.ert.net/rtsf.htm>

Esa es una pauta muy fuerte de que la información no es verdadera. Incluso es recomendable que abramos nosotros una ventana del navegador y escribamos la dirección de la página principal de los sitios conocidos de antivirus, y en ella seguramente encontraremos información actualizada. Ejemplo de empresas reconocidas son: Symantec Norton Antivirus (www.symantec.com); Panda Software (www.pandasoftware.com); McAfee (www.mcafee.com).

Recuerde que si el sitio está en inglés, en algún lugar de la parte superior de la página principal debería aparecer una opción para ver la versión en castellano.

En casos de otros estilos de mensajes, el sólo hecho de ver que es un mensaje que ha sido reenviado dentro de un grupo de personas, o de la solicitud de que sea enviado a todas las direcciones de nuestra lista de direcciones, es más que suficiente.

Reitero, por más que la información sea verdadera, no deberíamos entrar en la cadena.

CÓMO ACTUAR

Muchas personas conscientes de este tipo de cadenas reaccionan mal ante la presencia de uno y responden al remitente de mala forma. Lo correcto sería explicar en pocas palabras qué son las cadenas y pedir que no entren en ellas, o al menos, que no nos envíen a nosotros ese tipo de mensajes.

De la misma forma, no deberíamos reenviar estos mensajes ni publicar las direcciones de correo de las personas en nuestra lista de contactos, mucho menos cuando no sabemos de dónde proviene originalmente el mensaje y... adónde quiere llegar.

Hay sitios dedicados a publicar las más recientes cadenas y de esa forma "denunciarlas" públicamente. Incluso hay buscadores de cadenas, con descripciones, historias y demás.

Lo más importante de reconocer es que el mayor porcentaje de las veces, las cadenas pretenden engañarnos con información falsa para robar direcciones de correo. Y el porcentaje restante, envía información verdadera, pero el objetivo principal sigue siendo el convertirnos en futuros blancos de correos basuras.