Image not found or type unknown

www.juventudrebelde.cu

Image not found or type unknown

La bomba zip, aunque no clasifica como malware, es un tipo de archivo capaz de bloquear o dañar ordenadores.Autor: Tomado de Internet Publicado: 17/07/2019 | 08:43 pm

Que no te agarre el zip de la muerte

Un archivo comprimido puede destrozar tu ordenador en segundos. Te explicamos el porqué

Publicado: Miércoles 17 julio 2019 | 09:01:19 pm.

Publicado por: Yurisander Guevara

Circula generalmente por la vía del correo electrónico. Su peso es de 46 megabytes, y se presenta en formato .zip. Pero si este archivo comprimido es abierto por quien lo reciba, probablemente tenga que despedirse de su ordenador, o de todos sus archivos.

Hablo de lo que se conoce como el zip de la muerte, un archivo comprimido capaz de alcanzar hasta 4,5 petabytes de datos. Y no es el único.

Un ordenador estándar actual generalmente emplea un disco duro de un terabyte. Traducido a la unidad más conocida para «medir» la capacidad de estos dispositivos, son 1 024 gigabytes.

Si subimos la parada, un petabyte equivale a 1 048 576 gigabytes, y 4,5 petabytes —el espeluznante número que alcanza el citado zip de la muerte—, significan 4 718 592 gigabytes. Por mucho, el disco duro estándar se queda corto.

Para que se tenga una idea, Facebook, con más de 2 000 millones de usuarios, genera a diario cuatro petabytes de datos, según ha declarado la misma compañía. Que un solo archivo comprimido sea capaz de alcanzar una dimensión superior a la actividad de más de 2 000 millones de personas, es, cuando menos, preocupante.

Un protocolo para más comodidad

Creado por Phillip Walter Katz en enero de 1989, el formato .zip rápidamente se convirtió en un cómodo estándar de la industria computacional, pues permite comprimir archivos para reducir su tamaño.

Luego surgieron otros métodos de compresión, como los archivos .rar (aparecidos en 1993) o .7zip (nacidos en 1999 de la mano del ruso Igor Pavlov), aunque lo cierto es que el más popular durante décadas fue el .zip.

La especificación del protocolo de compresión zip indica que cada archivo puede ser almacenado, bien sin comprimir o mediante una amplia variedad de algoritmos de compresión. Sin embargo, en la práctica, zip se suele utilizar casi siempre con el algoritmo de Phil Katz, explica el sitio especializado incubaweb.com.

Hoy los archivos que emplean la extensión .zip son capaces de contener uno o más ficheros que están comprimidos o almacenados. Entre las aplicaciones que nos podemos encontrar para trabajar con este tipo de extensiones se destacan WinZip, PicoZip, Info-ZIP, WinRAR y 7-Zip.

Además de esos archivos, los principales sistemas operativos del mercado ofrecen funciones nativas para trabajar con archivos .zip, por lo que en la mayoría de los casos no sería necesario realizar la instalación de ningún software adicional, aunque los diseñados para ello generalmente contienen más funcionalidades.

De la compresión a la muerte

Esta gran capacidad de compresión ha sido empleada por hackers para crear la llamada «bomba zip», también conocida como el zip de la muerte, un fichero diseñado para inutilizar sistemas operativos u ordenadores.

El más conocido de estos es 42.zip, un archivo de solo 42 kilobytes que tiene seis capas de compresión y se expande hasta 4.3 gigabytes, lo que provoca un fallo en la lectura de memoria, paso que ocupa al antivirus de tal forma que otro software dañino pasa inadvertido.

Sin embargo, en los últimos tiempos han aparecido otros, como un zip infinito que se replica a sí mismo una y otra vez.

La idea detrás del zip de la muerte es similar al de otros ataques. Se trata de hacer colapsar el sistema u ordenador en base a una gran cantidad de datos que no puede procesar. Algunos ejemplos de este tipo de ataques serían los DDoS (Distributed Denial of Service). Uno muy conocido y similar en concepto sería el de Mil millones de risas, basado en XML, en el que se repite exponencialmente el uso de la sigla LOL —que significa laughing out loud o reírse en voz alta— al cargar el código.

Explica Xataka que, sin tratarse de ningún gusano o virus, otro ataque similar es la bomba fork o wabbit. En este caso, es un archivo que crea copias de sí mismo. Una técnica de la que los usuarios de Linux tampoco se libran, ya que también funciona con archivos TAR.

Afortunadamente la mayoría de los programas antivirus detectan si un archivo es una bomba zip y así evitan descomprimirlo. Muchos lo hacen porque solo permiten unas pocas capas de recursividad para prevenir ataques que podrían causar un desbordamiento de búfer, una condición de falta de memoria o un exceso de tiempo de ejecución del programa, de espacio en disco o memoria.

Sin embargo, el analista de vulnerabilidades de Google, Tavis Ormando, tuiteó recientemente acerca de un zip que solo era detectado por unos pocos antivirus.

AegisLab, Anti-AVL, Comido, Eset NOD32, Kaspersky, ZoneAlarmb y Checkpoint detectaron el virus del zip infinito, que llega bajo el nombre de zblg.zip, según recoge el sitio virustotal.com.

En otro grupo de antivirus esta bomba zip pasó inadvertida, para unos terceros provocó falla en el sistema, y otros dieron como resultado ser «incapaces» de procesar el archivo.

En cualquier caso, se debe evitar abrir los archivos comprimidos si no se conoce con fidelidad su origen. Activar una bomba zip puede ser cuestión de unos pocos clics, pero con esa estarían en riesgo todos nuestros archivos.

http://www.juventudrebelde.cu/suplementos/informatica/2019-07-17/que-no-te-agarre-el-zip-de-la-muerte