La Bomba Zip (Zip of Death)

Una bomba zip es un archivo comprimido malicioso diseñado no para infectar un sistema con *malware*, sino para **deshabilitarlo o colapsarlo** al saturar sus recursos. Su peligrosidad radica en su pequeño tamaño inicial, lo que permite pasar desapercibido en correos electrónicos o escaneos básicos de seguridad.

El principio central es la **desproporción extrema entre el tamaño comprimido y el tamaño descomprimido (relación de compresión).**

1. ¿Cómo Funciona Exactamente?

El ataque se basa en dos técnicas principales, que se ejemplifican perfectamente en el famoso archivo **42.zip**:

A. Relleno de Datos (Data Inflation)

La mayoría de las bombas zip están llenas de archivos que contienen grandes secuencias de datos idénticos (por ejemplo, millones de caracteres 'A', o archivos binarios llenos de ceros).

- **Compresión Eficaz:** Los algoritmos de compresión modernos (como LZ77 utilizado en el formato ZIP) son increíblemente eficientes para codificar datos repetitivos. En lugar de almacenar 10,000 ceros, el algoritmo solo almacena la instrucción: **"Repetir el cero 10,000 veces."** Esto permite reducir gigabytes de datos repetitivos a solo unos pocos kilobytes.
- **Ataque:** Cuando el *software* de descompresión intenta ejecutar esta instrucción, necesita asignar inmediatamente la memoria o el espacio en disco para el archivo de salida de gigabytes, lo que provoca la saturación de los recursos del sistema.

B. Anidamiento Recursivo (Layering)

El 42.zip utiliza una técnica más sofisticada conocida como anidamiento o "capas" recursivas:

1. El archivo raíz de **42 KB** contiene 16 archivos ZIP.
2. Cada uno de esos 16 archivos ZIP contiene, a su vez, otros 16 archivos ZIP.

3. Este proceso se repite en **cinco capas** de profundidad.
4. El archivo real de "relleno" solo se encuentra en la capa más profunda.

Efecto: Un *software* antivirus o un descompresor que solo analiza una capa de profundidad (para ahorrar tiempo y recursos) solo ve el archivo de 42 KB y lo declara seguro. Un descompresor completo debe procesar miles de archivos, lo que no solo satura el disco duro, sino que consume vastas cantidades de memoria RAM y tiempo de CPU, paralizando el sistema.

2. El Caso de 42.zip

El archivo 42.zip es el ejemplo más famoso de esta técnica debido a su increíble relación de compresión:

Parámetro	**Valor**
Tamaño Comprimido Inicial	42 KB
Tamaño Real Descomprimido	4.5 Petabytes (PB)
Relación de Compresión	106 mil millones a 1
Capas de Anidamiento	5
Número total de Archivos	$16^5 = 1,048,576$ (más de un millón de archivos)

3. ¿Todavía Funciona?

La eficacia de las bombas zip, incluido el 42.zip, ha disminuido significativamente con el tiempo debido a las defensas implementadas en el *software* moderno.

Aspecto	Antes (Eficacia Alta)	Ahora (Eficacia Baja)
Defensas de Antivirus	Muchos escaneaban solo la primera capa, fallando en detectar el contenido real.	Los *scanners* modernos limitan la descompresión recursiva (ej: solo revisan las primeras 5-10 capas) o imponen un **límite de tamaño máximo** para el archivo descomprimido.
Gestores de Archivos	Colapsaban por la necesidad de asignar espacio en disco.	Los gestores populares (como 7-Zip o WinRAR) ahora suelen implementar **medidas preventivas** que detectan archivos con relaciones de compresión sospechosamente altas y emiten advertencias o detienen la descompresión.
Memoria (RAM)	Los ordenadores tenían poca RAM, lo que llevaba a una rápida saturación de la memoria.	La memoria RAM moderna es mucho más abundante (8 GB, 16 GB, etc.), lo que reduce la posibilidad de un colapso instantáneo solo por la sobrecarga de la CPU o la memoria caché.

Conclusión:

El 42.zip ya no es una amenaza fatal para un ordenador o sistema antivirus moderno. Sin embargo, el **principio de la bomba zip** sigue siendo una consideración importante en la seguridad y es relevante para el análisis de *malware*, donde los atacantes aún utilizan técnicas de compresión con alta entropía o anidamiento para intentar **evadir la detección inicial** en *sandboxes* limitados.

"ATAQUES DE DESCOMPRESIÓN" O **"ATAQUES DE DENEGACIÓN DE SERVICIO LÓGICO" (LDOS)**:

1. Bomba de Archivo Comprimido No-Zip

El principio de la bomba zip se aplica a **cualquier formato de archivo** que tenga una alta relación de compresión, especialmente aquellos que son comúnmente utilizados para la transferencia de datos.

Caso	Explicación	Mecanismo
Bomba de GZIP / TAR	Similar a la bomba zip, pero se usa un solo archivo comprimido con herramientas de Unix/Linux (tar.gz, tar.bz2).	La explosión de datos ocurre con una sola llamada de descompresión. Se usan datos repetitivos para lograr una relación de compresión extrema (ej: 1 MB comprimido a 100 GB descomprimido).
Bomba de Imagen (BMP)	Una imagen **BMP (Bitmap)** puede ser sorprendentemente grande si está llena de una única secuencia de color.	El formato BMP no utiliza compresión. Un archivo BMP de 1x1 píxel es pequeño, pero un archivo de **200.000 x 200.000 píxeles** (un archivo descomprimido de 120 GB) puede ser creado y luego comprimido con ZIP a un tamaño muy pequeño (ya que los datos pueden ser muy repetitivos). Al descomprimirlo o intentar mostrarlo, colapsa el visor o el sistema.
Bomba de PDF	Un archivo PDF puede contener recursos comprimidos internamente o referencias circulares.	Diseñado para **agotar la memoria (RAM)** de los *parsers* (analizadores) de PDF. El atacante usa estructuras de datos recursivas o una cantidad excesiva de archivos o fuentes comprimidas, haciendo que el *parser* consuma toda la memoria disponible.

2. Zip con Múltiples Extensiones (Defensa Contra Antivirus)

Aunque no están diseñados para colapsar el sistema, utilizan la lógica del compresor para evadir la detección en sistemas de seguridad antiguos.

Caso	Explicación	Mecanismo
Zip Políglota	Un archivo que es válido para dos o más formatos de archivo (ej: un archivo que es un ZIP válido *y* también un archivo PNG válido).	Se usa para ocultar el contenido malicioso. Un *scanner* de archivos puede ver la cabecera PNG y no descomprimirlo, mientras que la víctima utiliza un descompresor que solo ve la cabecera ZIP.
Zip con Contraseña Falsa	Un archivo ZIP con contraseña que contiene la verdadera bomba zip.	El atacante proporciona una contraseña falsa en el correo electrónico. El antivirus no puede escanear el contenido cifrado y, al no tener la contraseña correcta, lo marca como "no escaneable" y lo deja pasar. El atacante usa luego el *malware* para obtener la contraseña real e iniciar el ataque.

3. Ataque "Quine" Recursivo

Este es un concepto teórico y forense que demuestra la recursividad sin la necesidad de la compresión binaria.

Caso	Explicación	Mecanismo
Quine de Archivos ZIP	Una bomba zip anidada diseñada para autoreplicarse.	El archivo ZIP más interno contiene una copia del archivo ZIP que lo contiene, creando un ciclo infinito. Al intentar descomprimirlo por completo, el *software* entra en un bucle sin fin hasta que agota los límites de tiempo, memoria o profundidad

Caso	Explicación	Mecanismo
		recursiva impuestos por el sistema.