Zip Bomb - what it is, classic signs, and how to avoid decompression traps

Gridinsoft Help Center

What it is

A zip bomb (decompression bomb) is a tiny-looking archive that explodes into an enormous amount of data when you try to open or scan it. The goal is to freeze or crash your app (or even your antivirus) by using up CPU, RAM, or disk space. Examples and details: https://gridinsoft.com/zip-bomb

Why it matters

One small .zip can stall your PC, lock up your file manager, or blind your security tools so other malware can slip by.

How it works

- Extreme compression: repeats the same data so it expands to gigabytes/terabytes.
- Nesting: zips inside zips inside zips to multiply the expansion.
- Scan trap: makes AV and unpackers chew through endless data and time out.

Red flags

- A very small .zip from an unknown sender or random website.
- Archives that contain many nested folders or more .zip/.rar files inside.
- Your unzip tool shows an enormous uncompressed size or freezes on open.
- Antivirus logs mention a "decompression bomb" warning.

Do it right

- Don’t open unexpected archives. If you must, scan first and use a sandbox or cloud viewer.
- Set your unzip tool/AV to limit max file size and recursion depth.
- Keep your antivirus and OS updated so they detect these traps.
- Delete suspicious zips and empty the recycle bin to free space if you started extracting one.