|  |  |
| --- | --- |
| Begriff | Erklärung |
| Decompression bomb / zip bomb | Malicious archive file designed to crash or render useless the program or system reading it. It is often employed to disable antivirus software, so that a more traditional virus sent afterwards could get through undetected.  Rather than hijacking the normal operation of the program, a zip bomb allows the program to work as intended, but the archive is carefully crafted so that unpacking it (e.g. by a virus scanner in order to scan for viruses) requires inordinate amounts of time, disk space or memory.  A zip bomb is usually a small file (up to a few hundred kilobytes) for ease of transport and to avoid suspicion. However, when the file is unpacked its contents are more than the system can handle.  The term was apparently first coined in July 2001, but the same technique has been used on dialup bulletin board systems at least as long as compressing data archive programs have been around.  Today, most antivirus programs can detect whether a file is a zip bomb and so avoid unpacking it. One example of a Zip bomb was the file "42.zip" which was 42 kilobytes of compressed data, containing six layers of nested zip files in sets of 16, each bottom layer archive containing a 4.0 gigabyte file for a total of 4.0 petabytes of uncompressed data. This file is still available for download on various websites across the internet. |
|  |  |
|  |  |
|  |  |