

Cybersecurity Digest

Bi-Weekly Update by the O/o CISO of Meghalaya Rural Bank

Vol 3 Issue 11

Date: 01.09.2026

Zip Bomb

A zip bomb, also known as a “decompression bomb” or “zip of death,” is a type of malicious archive file designed to overwhelm a system’s resources when decompressed. Unlike most malware, which corrupts or steals data, zip bombs create chaos by exhausting a system’s CPU, RAM, and storage capacity. These files often appear harmless and are

no larger than a few kilobytes. However, once extracted, their content can explode into terabytes or even petabytes of junk data, crashing any system that attempts to unpack them.

Zip bombs serve two main purposes in cyberattacks:

- **Disruption:** Crash systems or antivirus tools to enable attacker entry.
- **Diversion:** Stall



cybersecurity defenses while sneaking in secondary payloads.

How do Zip Bombs work?

Zip bombs take advantage of compression algorithms that can shrink massive amounts of data into tiny packages. The simplicity of their function is what makes them so dangerous.

Recursive compression

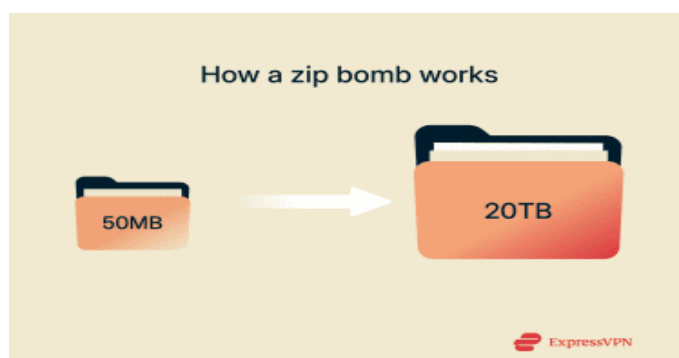
Many zip bombs use multiple layers of nested compression. A single archive file may contain hundreds of compressed folders within, leading to expo-

ponential data inflation once fully extracted.

Example: Take the infamous “42.zip,” a zip bomb that’s only 42 KB in size but decompresses into 4.5 petabytes of data, thanks to recursive layers of 16 zip files per folder.

Non-recursive overlapping compression

More advanced zip bombs use non-recursive methods, where data segments overlap and compress



more efficiently. This results in extreme data inflation with fewer layers, making detection harder.

Infinite decompression loops

These bombs embed structures that trap decompression algorithms in endless cycles, consuming all available memory and processing power.

Types of Zip Bombs

Recursive Zip Bombs

These contain deeply nested zip files, forcing systems to unpack layer after layer until they collapse under the weight of the inflated data.

Non-recursive Zip Bombs

Rely on ingenious compression techniques to reduce large datasets into deceptively small files with minimal layering.

Weaponized Zip Bombs

Some zip bombs aren't just

about resource exhaustion. They serve as payload carriers, delivering malware after the decompression chaos has crippled defenses.

Real-world impact of Zip Bombs

Resource exhaustion: Older antivirus scanners, servers, and endpoint machines are the primary targets, often crashing due to excessive demand on CPU, memory, or disk space.

Denial of service: By incapacitating systems with a swamped decompression process, zip bombs create a denial-of-service scenario, cutting off employees and users from critical opera-

tions.

Security system bypassing:

Paused antivirus engines or delayed logs open gaps for attackers to exploit with more dangerous secondary malware.

Best practices for securing against Zip Bombs

Staying ahead of zip bomb threats involves combining tools, tactics, and training. Here's how you can prevent these attacks effectively:

A) Proactive Detection with Huntress

The Huntress SOC ensures false positives are minimized while validating true risks. This targeted approach allows analysts to stay focused on strategic tasks.

B) Limiting Decompression Parameters

Modern decompression tools (e.g., WinRAR, 7-Zip) allow admins to set limits:

- Restrict recursion depth to avoid infinite unpacking cycles.
- Cap CPU and memory consumption during decompression

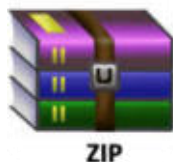
efforts.

- Set extraction size limits for unknown files.

C) Educating Your Team

Human error often enables zip bomb success. Leverage security awareness training so your employees know to:

- Avoid opening zip files from unknown or unverified sources.
- Double-check email links or file origins when in doubt.
- Recognize unusual file patterns, such as tiny file sizes claiming to contain significant data.



D) Creating Collaborative Defense Networks

Participate in information-sharing groups, such as ISACs, to stay informed on emerging zip bomb tactics. Collaborating with an industry-wide defense community increases overall preparedness.

Zip bombs are digital chaos packed in a deceptively tiny file. With tools like endpoint detection and response, and security awareness training, you can safeguard your systems from falling victim to these crafty attacks.



Call this helpline number to report cyber crimes to National Cyber Crime Reporting Portal.

