ZIP BOMB

ABHISHEK BHAWARE(IIT2019037)
RANVEER SINGH(IIT2019080)
SONAL (IIT2019122)
SAKSHAM SOOD(IIT2019164)
AAMINKUMAR CHAUDHARI(IIT2019206)

Indian Institute of Information Technology

Allahabad

Abstract:- Zip bomb is also called decompressed bomb which is a malicious file that is designed in such ways that it is used to crash or hang the system. It is often designed to disable the antivirus software which cannot be detected by using any kind of antivirus software. If you wanna detect, you need some special kind of software to detect it. This document deals with the Insertion, mitigation and prevention of zip bombs.

Introduction:- Zip bomb we can say that it is going to use an enormous amount of data once it is unpacked. Let's take the example of the 42.zip. It has a size of 42kB. It contains recursively nested zip files. On the lowest level, there is a single file that decompressed to a size of 4.3 GB. If I increase the nested zipping in the zip it can increase more than 4.3PB This is I think pretty much a big size for any storage system.

Literature Survey:- Zip bomb attack is an attack meant to fill the ram and hard disk of the pc by extracting a large file. Due to extraction the resources of the pc got full and unable to take any action. These are generally single layered but as the time changes the zip bomb got also various type.

1. 42.zip
2. A better zip
3. Self replicating zip

Their base are same but better they have large chunk of data in side that but have multi layer and self replicating feature that makes the more dangerous. In this paper we try to send the zip file through tcp connection and key to detect that zip through reference of compression ratio and depth size evaluation if can able to detect that and find out by which ip it is coming we have to block that ip so that no further chunk will come through that file.

Compression Ratio:-

Zip (Windows 8.1)	**86.4% of the original size**
Zip (WinZip)	**76.3% of the original size**
RAR (WinRAR)	**86.4% of the original size**
7z (7-Zip)	**85% of the original size**

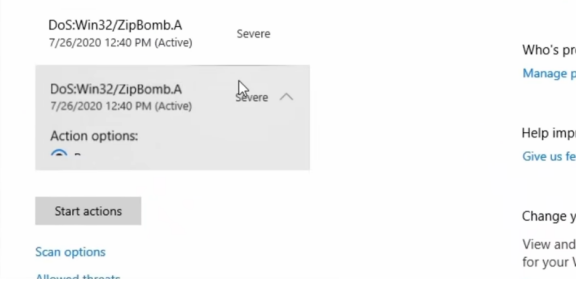
How Zip Bomb Works:-

Working of the Zip Bomb is not based on the hijacking, it allows the program to work as it is but archived is carefully crafted so that unpacking it required a big amount of memory and space.

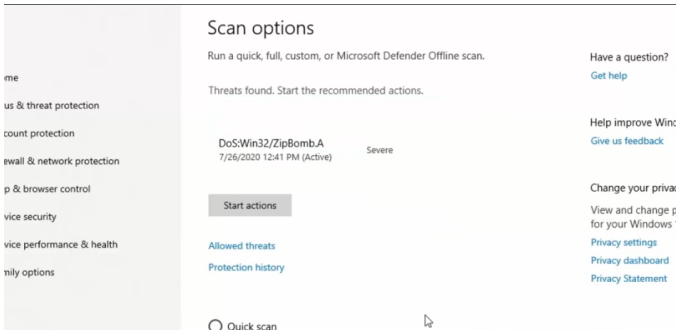
A zip bomb is usually a small file for ease of transport and to avoid suspicion. However, when the file is unpacked, its contents are more than the system can handle. The technique was used on dial-up bulletin board systems in the past.

Test Run of 42.zip

Tested On Windows OS.So when you try to extract the zip file the window defender will surely warn you about the zip bomb.

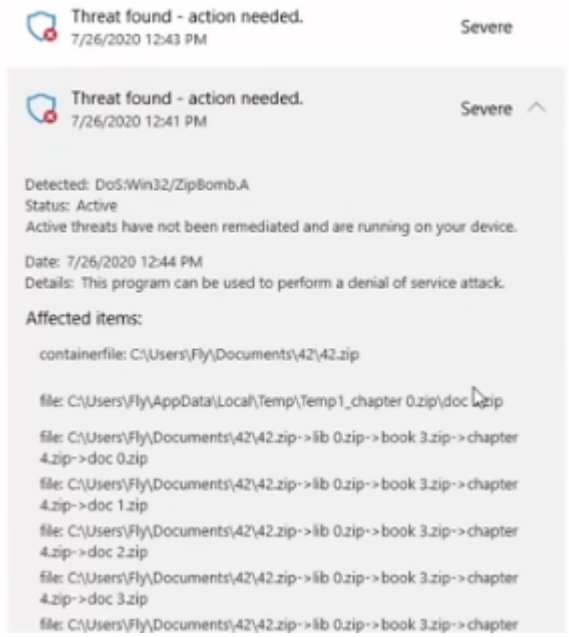


Then you surely click on the start action button to get rid of this zip bomb but the defender will not be able to remove it. It takes a lot of time but the result is not positive.

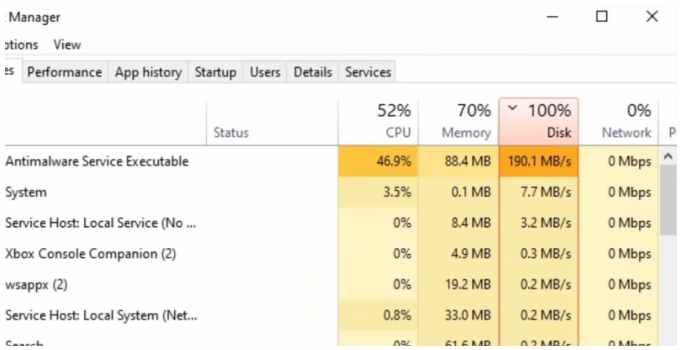


It stuck in this process.

Then you surely go to reboot OS but after that, it shows that there are various attempts to remove the file



After that when you check the disk space it keeps on changing that means some deleting and replicating work is going on behind the scene and your defender's antivirus will get exhausted on memory and OS will surely go to end the process and this is the gateway for hackers to attack the system.



Create Zip Bomb Manually:-

In order to create a Zip first create a new text file and save them in an extension as .txt open the text file and type the null character(alt+255) in it, and then press ctrl+A then Simultaneously click ctrl+V, for a couple of times make few zero bytes, and then make several copies of the text in the same directory and name them accordingly.

Open the Command Prompt and navigate the text Folder that contains the text file, by navigating the text folder that a super copy can be created, then repeat all the steps from beginning to make really a big text file, once a big file is created then Zip them using WinRAR or WinZip

Zip Compression Ratio:-

Well this is a bit controversial Topic It depends on many factors if you are thinking about zip bomb data generally the data in the zip bomb file is repetitive and it is easy to compress to a very further extent but data that is heterogeneous will not be compressed to that level as compared to zip bomb compression and generally, we have the

heterogeneous data so the talking about the numbers you can compress the size by 1/10th after that you have to face lossy compression but it also depends on the type of the file also.

How to detect Zip Bomb:-

In many anti-virus scanners, only a few layers of recursion are performed on archives to help prevent attacks that would cause a buffer overflow, an out-of-memory condition, or exceed an acceptable amount of program execution time. Zip bombs often (if not always) rely on the repetition of identical files to achieve their extreme compression ratios. Dynamic programming methods can be employed to limit the traversal of such files, so that only one file is followed recursively at each level, effectively converting their exponential growth to linear.

One another method is also possible in python to get the size of the ZIP file without extracting data by using the following code:

```
def get_extracted_size(filepath: str)
-> int:

    zp = ZipFile(filepath)
    name = zp.infolist()
    if zp.infolist()[0].file_size*0.23
> zp.infolist()[0].compress_size:
        return -1
    pathname =
zp.infolist()[0].filename
    return sum([zinfo.file_size for
zinfo in zp.filelist])

def unzip (path, total_count,depth):
    if depth>5:
        return -1
    time.sleep(1)

    for root, dirs, files in
os.walk(path):
        for file in files:
            file_name =
os.path.join(root, file)
            if (not
file_name.endswith('.zip')):
                total_count += 1
            else:
                num =
get_extracted_size(root+"/"+ file)
                if num == -1:
                    return -1
                currentdir =
file_name[:-4]
                if not
os.path.exists(currentdir):

os.makedirs(currentdir)
                with ZipFile(file_name)
as zipObj:

zipObj.extractall(currentdir)
                os.remove(file_name)

                total_count =
unzip(currentdir, total_count,depth+1)

                if total_count== -1:
```

```
                    return -1
    return total_count
```

But then you have one problem with this. The problem is that you can nest ZIP files. So the extracted files could again contain zipped files. If you apply recursion, you might want to have a maximum recursion depth and keep track of the used memory/disk space. You can improve this by applying recursion to this but that's not an easy task because you also have to apply Dynamic Programming to keep track of the repeating data so that extraction will not end up in the exponential time

Prevention:-

One method is that you can limit the resources, this can easily be done by limiting the number of resources your decomposition script uses and terminating it once it reaches a certain level.
You could use the resource module in python to limit resources available to your process and its children but this is beyond our scope.
If you need to decompress in memory then you could set resources.RLIMIT_AS (or RLIMIT_DATA, RLIMIT_STACK) .If the limit is reached; MemoryError is raised.

Conclusion:-

In this paper, we introduce the structures of the nonrecursive zip bomb and design an algorithm for detecting such a zip bomb. At the same time, we list some details that should be noticed in the detection and the algorithm efficiency about non-recursive zip bombs and info-zip is given.
In real-life situations, an attacker may not use a standard structure bomb. The attacker can make a non-recursive bomb whose structure is different from the previously mentioned structures. However, as long as the bombs use overlapping structures, they will most probably be detected by given algorithms.

Reference:-

1. python - How to protect myself from a gzip or bzip2 bomb? - Stack Overflow
2. https://stackoverflow.com/questions/13622706/how-to-protect-myself-from-a-gzip-or-bzip2-bomb
3. https://www.reddit.com/r/learnpython/comments/1wazaw/how_to_protect_against_a_possible/
4. https://www.quora.com/Computer-Security-What-exactly-does-a-zip-bomb-do-How-does-it-work
5. https://www.bamsoftware.com/hacks/zipbomb/
6. https://help.eset.com/eis/14/en-US/idh_config_threat_sense.html
7. https://infosecwriteups.com/zip-bombs-30337a1b0112
8. LIVEcommunity - How to detect zip bomb file? - LIVEcommunity - 276983
9. iis - Is there any way to detect an incoming ZipBomb? - Server Fault
10. The Most Clever 'Zip Bomb' Ever Made Explodes a 46MB File to 4.5 Petabytes
11. Information about size limits with WinZip – WinZip - Knowledgebase