Excel@FIT

Generic Unpacker of Executable Files

Marek Milkovič 30

Revealing the true behavior of executable files

1. Introduction

The software may use packing as a protection against its analysis. This can be often seen in malware. If such file needs to ba analyzed, it has to be unpacked with a tool called unpacker. The generic means that unpacker is able to unpack more than one packer and it is able to adapt to the variety of used techniques.

There are already few generic unpackers. However, they focus mostly on the one aspect of the unpacking and that is whether the file remains executable. There is also another point of view, which look at how well was the structure of the file reconstructed, compared to the original file. Because this new generic unpacker is used in AVG Retargetable Decompiler[1], the structure of the file needs to remain the same as much as possible.

2. Packing

Packing is a process of compression of the code or even data of an executable file, while the output is a new packed executable file. More importantly, the new packed file still remains executable and performs the same action as the original file. Every packer works differently, but the most of them work on similar basis. They insert a routine called unpacking stub into the packed program, which unpacks the original file content on the program start. The general structure of the original and the packed file can be seen in Figure 1.

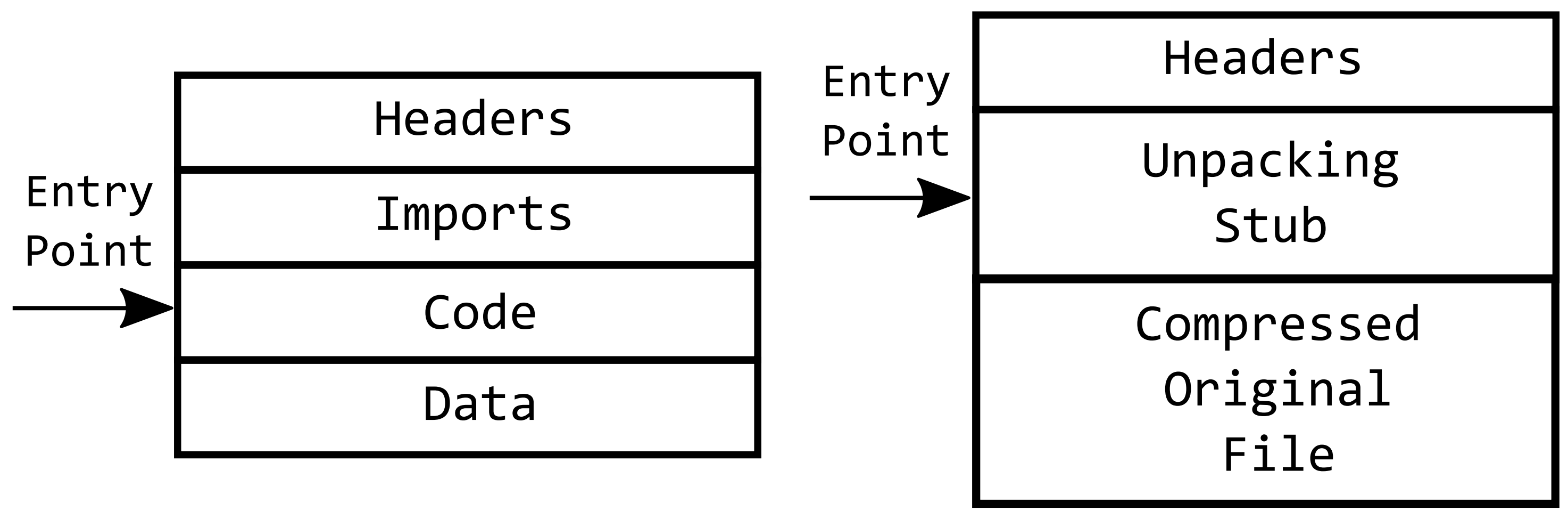


Figure 1. The structure of the original (on the left) file and the packed (on the right) file.

3. Unpacking

There are more possible approaches to the unpacking, however the most notable are dynamic and static unpacking. The often chosen approach is dynamic, which runs the packed program and let it unpack itself. After that, the content of memory is copied into the file. However, running the application if we do not know the origin is not secure. On the other hand, static approach does not run the program at all. It simulates the actions of the unpacking stub. Our generic unpacker uses the static unpacking techniques to achieve the security, and the platform and architecture independent unpacking.

4. Results

We support MPRESS[2] and partially UPX[3] packers currently. The MPRESS unpacking plugin was tested on 91 in-the-wild samples downloaded from VirusTotal[4]. The results were compared with the results from the internal AVG unpacker used in the antivirus core and PackerBreaker[5]. Three criteria are observed:

- **Sucessful unpacking ratio** - Number of successfully unpacked executable files to the number of all executable files
- **Executability ratio** - Number of executable files that remained executable to the number of sucessfully unpacked files
- **Successful decompilation ratio** - Number of successfully decompiled files to the number of successfully unpacked files

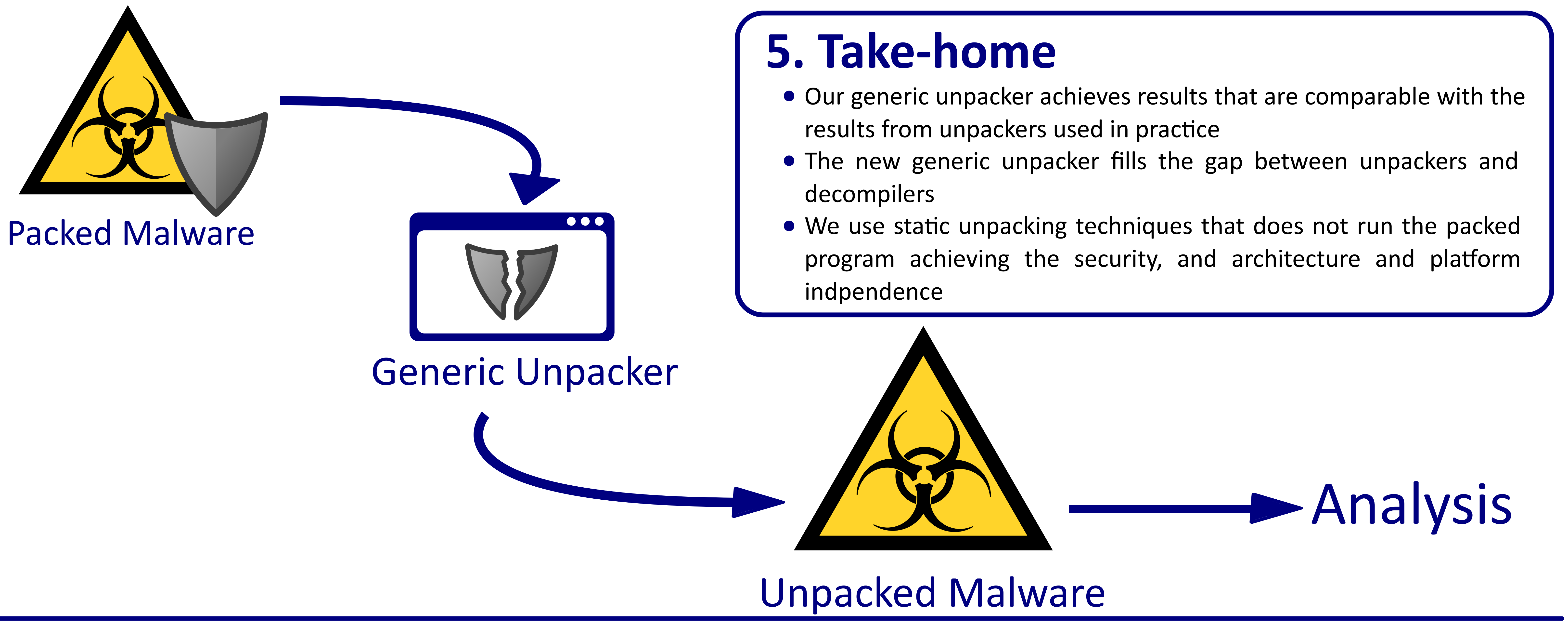
The results of the test can be seen on Table 1.

Unpacker	Successful unpacking ratio	Executability ratio	Successful decompilation ratio
Generic Unpacker	**93.41 %**	**100 %**	**100 %**
Internal AVG unpacker	93.41 %	100 %	0 %
PackerBreaker	93.41 %	95.29 %	0 %

Table 1. The results of unpacking

5. Take-home

- Our generic unpacker achieves results that are comparable with the results from unpackers used in practice
- The new generic unpacker fills the gap between unpackers and decompilers
- We use static unpacking techniques that does not run the packed program achieving the security, and architecture and platform indpendence



[1] http://www.retdec.com/

[2] http://www.matcode.com/mpress.htm

[3] http://upx.sourceforge.net/

[4] https://www.virustotal.com/

[5] http://www.sysreveal.com/tag/packerbreaker/