### **These are the List of Packer’s used in Malware.**

### **UPX**

UPX is short for the “Ultimate Packer for Executables.” It uses an open-source algorithm that does not require any additional system memory for decompression.

### **The Enigma Protector**

Like most packers, The Enigma Protector is marketed for individuals and businesses who want to protect their files from hacking. Nonetheless, The Enigma Protector is commonly used to obfuscate malware.

### **MPRESS**

MPRESS was originally designed to compress files and decrease application start times. While this free software is extremely useful for regular file compression, it is also easily accessible to hackers and other malware writers.

### **Exe Packer 2.300**

Exe Packer 2.300 is a standard, free software for file compression and decompression. Since it has been around for years, Exe Packer 2.300 is one of the most popular packers for malicious file obfuscation.

### **ExeStealth**

ExeStealth is a tool that encrypts files to avoid detection and hacking. Designed by WebToolMaster, this free software is simple to implement and one of the best anti-hacking tools on the market, which also makes it effective at hiding malware code in your system.

### **Morphine**

Unlike most other packers, Morphine includes its own PE loader, allowing users to encrypt the output of compressed data. The polymorphic engine is also used to create completely unique decryptors for malware.

### **Themida**

Themida was developed by Oreans to protect Windows applications from hackers. Unfortunately, it can also be used to encrypt malicious files and complicate attempts to reverse-engineer malware.

### **MEW**

MEW is primarily used for smaller malware file compression using the LZMA algorithm. Even though it was designed for small files, it has been updated over time so that it can also obfuscate larger malware files.

### **FSG**

The free, simple FSG software compresses both small and large files. While it is popular and commonly used to hide malware code, it is also relatively simple to unpack through a decompression loop that writes the data to the final destination.

### **PESpin**

PESpin compresses Windows code using MASM. It protects files against patching and disassembling, making it a popular resource for malware authors.

### **Andromeda**

While Andromeda refers to a botnet that has been around since 2011, it is also a custom packer. Custom packers are especially dangerous because they are not as simple to reverse-engineer.

### **VMProtect**

VMProtect is very popular, as it can encrypt a wide range of files, including executable files, drivers and dynamic-link libraries. When an application encrypted by VMProtect is opened, the packer does not decrypt anything; instead, it runs on a virtualized code.

### **Obsidium**

Obsidium works for both 32-bit and 64-bit Windows applications. This software is capable of encrypting, compressing, and obfuscating malware.

## **How to detect malware packers**

Since most malware packers make it difficult to find and analyze malicious code, it may be necessary to use a script specifically designed for packer detection. Thankfully, there are a number of packer-detecting tools available. Here are some of the best tools for identifying malware packers:

* [Windows Executable Packer Detection](https://www.guidancesoftware.com/app/Windows-Executable-Packer-Detection)
* [PackerID](https://github.com/sooshie/packerid)
* [PEiD](https://www.softpedia.com/get/Programming/Packers-Crypters-Protectors/PEiD-updated.shtml)
* [RDG Packer Detector](http://www.rdgsoft.net/)