Lab - Unpacking

The goal of this lab is to develop effective techniques for unpacking malware while focusing on manual analysis. This will provide a more comprehensive view and allow for you to later identify more effective (dynamic) approaches for unpacking.

I will provide sample information from video demonstrations. You do NOT need to unpack sample 1 or 2, but can for practice

**[OPTIONAL] Demo 1 - TeslaCrypt from Alexu-edu-eg   
MD5: 9ce01dfbf25dfea778e57d8274675d6f**

The first sample demonstrates how monitoring memory allocations may lead to discovery of the unpacked malware. This is a simple technique that does not always yield results, but is often the first technique that I try.

**[OPTIONAL] Demo 2 – Simda  
MD5: 69f27b07404cf9c51dd2d2e40fca4d65**

This sample employs a custom packer and highlights how you can use both dynamic and manual analysis to unpack it. Follow the code as I did in the video to understand the KEY transition points, such as jumping to shellcode and jumping from shellcode, to help determine exactly when the unpacking process is done.

This is a sample of Simda, some background information (not the actual sample):

<https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/simda>

Please note how to use Scylla to help with import reconstruction and how the malware used shellcode to assist with the unpacking process.

Source: <http://www.malware-traffic-analysis.net/2015/02/13/index.html>

**[REQUIRED] sample 1   
MD5: 9c1b18161e0310d6c42c1a2c168d5a78**

1. This sample uses a well-known packer, identify what that packer is and provide evidence through program analysis to support your conclusion.

**[REQUIRED] sample 2  
MD5: 66f33597cbf097345c51891ab951b641**

This is a modern trojan, your task is to completely unpack it. You will encounter several rounds of unpacking before it is completely done.

1. Identify the first layer of packing and describe how you unpacked it.
2. The second layer of unpacking involves shellcode, describe how you identified this code and provide analysis of its behavior (but stay focused on unpacking)
3. Once you’ve identified the unpacked malware, you will need to provide some “fixes”. Describe how you obtained the unpacked malware and what fixes were required.

**[REQUIRED] sample 3   
MD5: 6c8e800f14f927de051a3788083635e5**

This is another recent trojan that employs some unique tricks during the unpacking process before it leverages several anti-analysis techniques.

1. Unpack this malware, noting the general flow of unpacking and any anti-analysis techniques you encountered along the way. This malware will be unpacked once you see it checking the process list against a list of hard-coded values.

**Deliverable**

Your lab report in a Word document or PDF.