



# Detecting Packers and Code Obfuscation

Length	Micromodule
Collection	NSA NCCP
Updated	March 9, 2019
Contributors	Josh Stroschein
Academic Levels	Undergraduate
Topics	Malware, Software Security And Secure Programming, Programming
Link	<a href="https://clark.center/details/jstroschein/876f39db-43db-422c-8058-b7048e3823f8">https://clark.center/details/jstroschein/876f39db-43db-422c-8058-b7048e3823f8</a>

## Description

Code obfuscation is a technique heavily employed by malware authors to hide the true intent of their programs, as well as utilized to help avoid detection by security products. In this module, you will learn to identify when code is packed, to detect indications of obfuscation, differentiate between obfuscation and packing, understand common obfuscation techniques and learn tools to help you perform this analysis.

## Notes

Please note that the lab files contain malicious software - please handle in a safe manner and only analyze in a proper environment. This work was made possible by NSA Grant for the development of cyber security curriculum.

## Outcomes

- Identify when code has been packed
- Examine common obfuscation techniques
- Differentiate between different packing and code obfuscation methods
- Identify when code has been obfuscated

## Files Not Included in Bundle

Download links of files associated with this object but not included in bundle

- [05 - Packers and Obfuscation.mp4](#)

## Links

External links that are associated with this learning object

- [YouTube - Packers and Obfuscation](#)