



Monitoring Tools

Length	Micromodule
Collection	NSA NCCP
Updated	March 9, 2019
Contributors	Josh Stroschein
Academic Levels	Undergraduate
Topics	Malware
Link	https://clark.center/details/jstroschein/67092cc6-bb8d-4368-a046-1ddb7e647868

Description

In this course, students will be presented with two activities of identifying malware network activity using a variety of dynamic analysis tools.

Lab Environment: Use of variety of tools is needed for this lab. It is recommended to do this lab in a virtualized environment. The tools we will be using are ProcMon and Wireshark

Outcomes

- Interpret why malware communicates to outside sources
- Examine common techniques of malware communication
- Identify ways malware attempts to communicate to outside sources

Links

External links that are associated with this learning object

- [YouTube - Monitoring Tools](#)