JASON DION
TRAINING THE CYBER SECURITY WORKFORCE


# Reverse Engineering

## THREAT MANAGEMENT

# Reverse Engineering

- Malware authors do not explain how their software works
- Reverse engineering is a technique to take a finished product and understand its inner workings through decomposition
- Conducted through dynamic or static analysis



# Dynamic Analysis

- Malware is placed in a sandbox and its behavior observed on the system and the virtual network

- Automated solutions can do this in near real-time, where email attachments are launched and automatically analyzed for malicious activity



# Static Analysis: Software

- Analysis of the code of the malware
  - For Ruby and Python, the code is readable because they are interpreted languages
  - For C/C++ and Java, code is compiled into binary
- Static analysis of compiled code requires a decompiler or analysis in binary format



# Reverse Engineering Hardware

- Very difficult to perform due to embedded software in firmware
- Most often, dynamic analysis is conducted on hardware
- *Hardware should be purchased from a trusted supplier to minimize the risk of malware being inserted into the firmware of hardware devices during procurement and shipment to your company*