TeamWorx SECURITY
INTELLIGENT WORKFORCE TECHNOLOGY

## Malware Intermediate Analysis Couse Syllabus

This 40-hour, five (5) day course focuses on building from the Malware Fundamentals Course allowing analysts to dive deeper into understanding malware and conduct basic static and dynamic malware analysis.

Our courses are primarily designed for the Department of Defense malware analysts but also meet the training and mission needs of any sector malware analyst. Our goal is to promote a more efficient integration between mission operations and analysis.

## Contact Information

**Contact:** 443-620-TEAM (8326) Option #2 **or** training@teamworxsecurity.com

## Course Description and Course Goals

- Navigate initial access vectors of malware (users, vulnerabilities and supply chain compromise) and their most common behaviors
- Explore File Headers and Magic Numbers to help further identify different file types and understand why these techniques are beneficial
- Identify resources to assist in conducting open-source research (OSR) in support of malware analysis
- Clearly identify the different stages of conducting malware analysis (Static, Dynamic, Reverse Engineering)
- Understand different system environment requirements and corresponding tools utilized to conduct malware analysis
- Conduct basic static and dynamic analysis on previously discussed file types
- Identify indicators of compromise after conducting analysis and compiling all data to generate a final report
- Students will be able to properly identify, recognize and conduct malware analysis
- Students will come away will a repeatable process for report generation that easily digestible to defenders and decision makers
- Overall students will understand the “what” of malware analysis

## Students will Need

- Note taking materials (notepad, pen, pencil, etc.)
- Access to computer with internet access and video conferencing capabilities. Teamworx Security will utilize a conferencing platform that meets the students’ needs.

## Grading

This course is based on participation within daily discussions and lab submissions. With the requirement for grading based on participation and lab completion, the student **MUST** be present to do so.

## Assignments and Homework

- Review recent news or topics relating to malware in preparation for daily discussion
- Homework assignments will require students to apply skills learned throughout the course to reports in MATRIX through provided accounts.
- On the last day students will complete a lab to conduct analysis and generate a malware analysis report that will be submitted for review

## Course Schedule

Courses schedules can vary based on customer needs.

- Daily start time will be 0800 (8 a.m.)
- Daily end time will be between 16000/1700 (4/5 p.m.)
- Daily lunch break will be between 1130 and 1300 (1 p.m.)
- Daily schedule may ebb and flow based on how quickly students are understanding concepts and questions