TeamWorx SECURITY
INTELLIGENT WORKFORCE TECHNOLOGY

Malware Analysis Intermediate Course Syllabus (MAI)

This 40-hour, five (5) day course builds on foundational knowledge by delving deeper into cyber threats to better understand the inner workings of sophisticated malware variants and the advanced persistent threats (APTs) that use them. MAI begins to hone tradecraft of the individual analyst by focusing on hands on practical exercise in memory forensics, sandbox evasion, and polymorphic malware detection.

Through hands-on real-world examples and team collaboration, MAI students will explore use-cases from around the world to practice effective tradecraft and be prepared to operate immediately.

Contact Information

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

Course Description and Course Goals

- Introduction to history of malware and malware analysis
- Ability to explore environments, recognize methodologies, and create reporting
- Introduction to executable files
- Ability to apply analysis to executable files
- Ability to recognize malicious PDF and Microsoft Office documents
- Ability to reverse engineer malicious materials and create reporting

Module 1

- Introduction to the history of malware and malware analysis
- Ability to recognize malware definitions and types
- Exposer to supply chain attacks
- Exposure to relevant threat actors
- Understanding how to defend against malware
- Understanding MITRE ATT&CK and malware tactic, techniques, and procedures (TTPs)

Module 2

- Introduction to entropy
- Understanding file packing
- Exposure to file encoding and hashing
- Understanding common persistence tactics
- Understanding of living of the land techniques
- Exposure to industry standard tools
- Understanding of “why” we conduct analysis

Module 3

- Exposure to common malicious file types
- Understanding of file headers data
- Deep dive exposure of executable files
- Practical application of executable analysis

Module 4

- Deep dive exposure of PDF files
- Deep dive exposure of Microsoft Office files
- Practical application of PDF and Microsoft Office file analysis

Module 5

- Practical application of exploitation development
- Understanding of analysis and production
- Show positive knowledge transference through capstone exercise

Students will Need

A computer with internet access. Students are also welcome to bring any other note taking materials they wish. (some handouts will be provided)

Grading

This course is based on participation within daily discussions and group activities. Students **MUST** be present to do so.

Course Schedule

Course schedules can vary based on customer needs.

Five (5) Day Course Schedule Expectations:

- Daily start time will be 0900 (9 a.m.)
- Daily end time will be between 1600 (4 p.m.) and 1730 (5:30 p.m.)
- Daily lunch break time will be between 1130 to 1300 (1:00 p.m.)
- Daily schedule may flex based on how quickly students are understanding concepts and questions