Course Welcome

Malware authors are constantly trying to hide the true intention of their malware. A malware analyst is required to understand and identify how to defeat common malware obfuscation techniques, as well as how to adapt to and counter the new techniques that are constantly emerging. Malware analysis requires the application of a wide range of skills common to information technology in general and specialized skills rarely used outside of malware analysis.

This course will teach you how to effectively identify and work with files at a low level, and not rely on factors such as its file name or extension. The course primarily focuses on Windows Portable Executable (PE) files, which make up the vast majority of malware in-the-wild. You will understand and learn how to perform static malware analysis as well as dynamic, run-time malware analysis. You’ll examine and work hands-on with malware samples using industry standard static and dynamic analysis tools in a safe environment. You will reverse engineer malware samples, use debuggers to perform dynamic run-time analysis and write small scripts to aid in analysis.

You will also be introduced to advanced malware topics, such as malware packers, common elevation of privilege techniques, propagation techniques, and malware command and control. Malware detection techniques will be taught, as well as common malware detection evasion techniques and advanced malware detection techniques. You will write malware detection signatures using a malware detection engine. Finally, you will learn about advanced topics, such as malware rootkits and boot-kits.

Upon completion of the course, you will be prepared to analyze and report on malware samples and you will be able to perform effective malware detection based on analysis. In addition, you will gain the knowledge to effectively deal with the changing landscape of malware, as malware authors adapt their techniques to avoid analysis and detection.