*MALWARE ANALYSIS ENVIRONMENT: Testing laboratory built as an integrated component of ISEAGE.*

Malware is currently one of the biggest threats to the highly connected computing world. Malware takes on many different forms and its level of sophistication and malicious intent continues to grow. A great deal of research has been (and continues to be) done on techniques used to detect and defend against malware. This research has shown that using a single test machine for analyzing the complete functionality of a piece of malware is simply not sufficient. For a thorough analysis of the complete functionality of a piece of malware, a full analysis environment that emulates a network environment, as well as the World Wide Web is needed. A malware analysis environment of this type has been designed and created. This new environment is introduced, and the details and specifications of its design are discussed in this paper.

The malware analysis environment created in this project was built specifically as an integrated component of the ISEAGE system. The environment takes advantage of the many security and network traffic flow features already built in to ISEAGE. Its primary purpose is to provide a safe and secure environment for students to learn and practice malware analysis. It will be used for future classes at Iowa State University that teach malware analysis techniques.