HARVINDER DHAMI

STUDENT, MASTER OF INFORMATION SYSTEMS SECURITY AND ASSURANCE

A TECHNICAL INCIDENT DETECTION AND RESPONSE FOR THE MEMORY INJECTABLE MALWARE

Malwares are one of the biggest threat to information systems. Malware is not limited to operating systems but it affects regardless hardware platforms including firmware. Microsoft Operating system is most common target for adversaries. Highly sophisticated malware uses memory injection techniques to stay undetected. Currently, Incident detection and response is performed by very highly skilled malware analysts but security professional who are not malware experts faces problem as they have very less experience in performing malware analysis. Here, I will propose a technical incident response framework which will help security professionals to detect and response to malware incidents for malware that uses memory injection techniques to evade the detection.

Research Advisors: Dr. Dale Lindskog, Dr. Pavol Zavarsky