CYBERSECURITY LECTURE SERIES

DEFEATING EDR EVADING MALWARE WITH MEMORY FORENSICS

September 24th at 4:30 P.M.

DMC Theater, LSU Digital Media Center

Andrew Case

Director of Research at Volexity

ABSTRACT

Andrew Case is the Director of Research at Volexity and has significant experience in incident response handling and malware analysis. He has conducted numerous large-scale investigations that span enterprises and industries. Case is a core developer of the Volatility memory analysis framework, and a co-author of the highly popular and technical forensics analysis book “The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory.”

SPEAKER BIO

Endpoint detection and response (EDR) software has gained significant market share due to its ability to examine system state for signs of malware and attacker activity well beyond what traditional anti-virus software is capable of detecting. This deep inspection capability of EDRs has led to an arms race with malware developers who want to evade EDRs while still achieving desired goals, such as code injection, lateral movement, and credential theft. This monitoring and evasion occurs in the lowest levels of hardware and software, including call stack frames, exception handlers, system calls, and manipulation of native instructions. Given this reality, EDRs are limited in how much lower they can operate to maintain an advantage. The success of EDR bypasses has led to their use in many high-profile attacks and by prolific ransomware groups.

In this talk, we discuss our research effort that led to the development of new memory forensics techniques for the detection of the bypasses that malware uses to evade EDRs. This includes bypass techniques, such as direct and indirect system calls, module overwriting, malicious exceptions handlers, and abuse of debug registers. Our developed capabilities were created as new plugins to the Volatility memory analysis framework, version 3, and will be released after the talk.