CYBERSECURITY LECTURE SERIES

GHOST IN THE KERNEL: USING MEMORY FORENSICS AND REVERSE ENGINEERING TO DEFEAT AN OBFUSCATED ROOTKIT

May 15th, 2023 at 3:30 P.M.

DMC Theater, LSU Digital Media Center

Andrew Case

ABSTRACT

As reported by Kaspersky, the Ghost Emperor APT group targeted high-profile victims across Southeast Asia, including government entities and private corporations. As part of these attacks, a potent rootkit was deployed to maintain privileged access to compromised systems in a stealthy manner. This rootkit not only hid all attacker activity on a compromised system, but also included numerous anti-forensics techniques to frustrate analysis. These techniques include memory-only (reflective) loading of kernel drivers, strings-obfuscation, wiping of driver metadata, altering of in-memory file contents, and more. In this presentation, the internals of this rootkit will be presented along with a deep technical analysis of one of the rootkit's most notable features – the ability to hide running services on Windows 10 systems. This feature stands out as Microsoft added several security technologies aimed at preventing such anti-forensics techniques. The analysis of the rootkit's service hiding will include a live demonstration of memory forensics against the rootkit followed by a showcase of advanced reverse engineering techniques to reconstruct its obfuscated module. Attendees of the presentation will learn the extent to which adversaries work to remain hidden along with a live demonstration of how trained analysts can quickly waste the adversaries' efforts.

SPEAKER BIO

Andrew Case is the Director of Research at Volexity, a core developer of the Volatility memory analysis framework, and Senior Cybersecurity Consultant at LSU. His professional experience includes digital forensic investigations, incident response handling, malware analysis, penetration tests, and source code audits. Andrew is a co-author of the award-winning book "The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory". Andrew's primary research focus is physical memory analysis, and he has presented his research at conferences including Black Hat, RSA, SecTor, SOURCE, BSides, OMFW, GFirst, and DFRWS.

LSU | Center for Computation & Technology