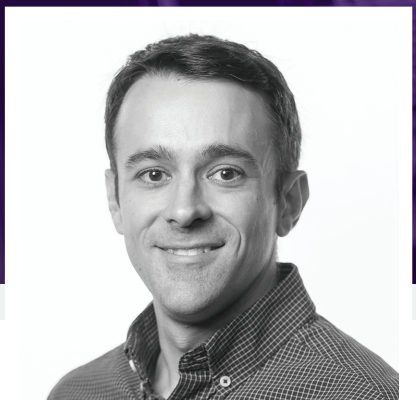
CYBERSECURITY LECTURE SERIES

DETECTING & DEOBFUSCATING MALICIOUS POWERSHELL WITH TREE-SITTER



April 20 at 4:30 - 6 p.m.

DMC Theater, LSU Digital Media Center

David McDonald

VOLEXITY

ABSTRACT

The malicious obfuscation of code from scripting languages, such as PowerShell, Python, and JavaScript, continues to be used as an essential part of threat actors' toolkits. Obfuscation techniques hamper analysts' ability to investigate and respond quickly to compromises by complicating reverse engineering of the original script and pose significant challenges to scanning engines, such as Yara, that rely on byte-based pattern recognition. Windows' built-in defense mechanisms, notably the built-in Antimalware Scanning Interface (AMSI) DLLs, struggle to detect these obfuscations, allowing for trivial bypasses of the AMSI subsystem via relatively simple obfuscations. AMSI bypass tools and techniques are routinely deployed by obfuscated code as part of their infection chain. The tree-sitter parsing library opens new avenues for detection and analysis by providing an API that allows developers to interact programatically with a script's syntax tree. This talk will showcase new techniques for rapidly detecting, analyzing, and preventing infections, culminating with the demonstration of a custom AMSI provider DLL that can deobfuscate, block, and log obfuscated PowerShell payloads.

SPEAKER BIO

David McDonald is a researcher and software engineer with 5 years of digital forensics R&D experience. His passion for this field began with his involvement in the University of New Orleans CTF team, as well as through his time as a Systems Programming teaching assistant. After over two years of digital forensics research and development on Cellebrite's computer forensics team, he joined Volexity's Volcano team, where he now works to develop next-generation memory analysis solutions. He believes deeply in sharing knowledge and helping others discover their abilities and interests through their own journeys in cybersecurity, and strives to pay forward the benefits of the mentorship that has opened so many doors for him.