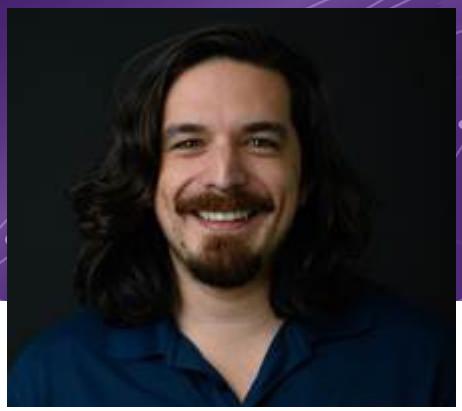
CYBERSECURITY LECTURE SERIES

REVERSING ROCKWELL: PREPARING FOR THE NEXT TRISIS BY JOURNEYING THROUGH COMPILER HELL



November 14th at 4:30 P.M.

DMC Theater, LSU Digital Media Center

Jimmy Wylie

Technical Lead Malware Analyst @ Dragos, Inc.

ABSTRACT

In 2017, when we discovered TRISIS, we were lucky. Triconex program downloads were in a native assembly language, PowerPC, which matched the CPU we found in the Triconex. This meant that we could use standard reverse engineering tools to examine the underlying code and firmware and understand the malicious code's effects on the system. But, this situation is only sometimes the case across vendors. Rockwell is a major ICS vendor in the United States. While working on separate research, we realized that their program downloads were not in a native assembly, and we didn't have a way to understand the contents of program downloads to a Rockwell controller. In Rockwell's case, they appeared to be using an interpreted bytecode. So, what if a threat group like conducted a TRISIS-style attack against a Rockwell controller? At best, we could detect that an unauthorized download occurred and deduce the effects based on what happens to the process, but we'd have no ground-truth way of confirming based on the code. We decided to explore this problem attempting to answer two questions: How much effort and time is required to understand a custom assembly language? Once we understand the language, can we identify general "suspicious" techniques and then build follow-on tools to detect those techniques? This talk will cover how we selected Rockwell and the process of reversing their compiler thus far. The reverse engineering discussion will pay particular attention to overcoming problems when reverse engineering large binaries, and static reverse engineering of C++ classes, their respective hierarchies, as well as C++ templates.

SPEAKER BIO

Jimmy Wylie is a Technical Lead Malware Analyst at Dragos, Inc. who spends his days (and nights) searching for and analyzing threats to critical infrastructure. He was the lead analyst on PIPEDREAM, the first ICS attack "utility belt", TRISIS, the first malware to target a safety instrumented system, and analysis of historical artifacts of the CRASHOVERRIDE attack, the first attack featuring malware specifically tailored to disrupt breakers and switchgear in an electric transmission substation.

Starting as a hobbyist in 2009, Jimmy has over 10 years experience with reverse engineering and malware analysis. He has worked for various DoD contractors, leveraging a variety of skills against national level adversaries, including network analysis, dead disk and memory forensics, and software development for detection and analysis of malware. After leaving the DoD contracting world, he joined Focal Point Academy, where he developed and taught malware analysis courses to civilian and military professionals across the country. In his off-time, Jimmy enjoys learning about operating systems internals, playing board games, and failing at crossword puzzles. He can be found on Mastodon: @mayahustle@infosec.exchange

---

LSU | Center for Computation & Technology