Cybersecurity Lecture Series

Analyzing PIPEDREAM: Challenges in testing an ICS attack toolkit

Jimmy Wylie, Dragos, Inc.

Principal Malware Analyst II

Hybrid: Digital Media Center/Zoom Theatre/Zoom
October 10, 2022 - 03:30 pm

Abstract:

ZOOM INFO:

Zoom link: https://lsu.zoom.us/i/98612180731
Meeting ID: 98612180731
Passcode: cyber

Identified early in 2022, PIPEDREAM is the seventh-known ICS-specific malware and the fifth malware specifically developed to disrupt industrial processes. PIPEDREAM demonstrates significant adversary research and development focused on the disruption, degradation, and potentially, the destruction of industrial environments and physical processes. PIPEDREAM can impact a wide variety of PLCs including Omron and Schneider Electric controllers. PIPEDREAM can also execute attacks that take advantage of ubiquitous industrial protocols, including
CODESYS, Modbus, FINS, and OPC-UA.

This presentation will summarize the malware, and detail the difficulties encountered during the reverse engineering and analysis of the malware to include acquiring equipment and setting up our lab. This talk will also release the latest results from Drago's lab including an assessment of the breadth of impact of PIPEDREAM's CODESYS modules on equipment beyond Schneider Electric's PLCs, testing Omron servo manipulation, as well as OPC-UA server manipulation. While a background in ICS is helpful to understand this talk, it is not required. The audience will learn about what challenges they can expect to encounter when testing ICS malware and how to overcome them.

Speaker's Bio:

Jimmy Wylie is a Principal 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.

Jimmy 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 pool, cheap beer, and good whiskey. He can be found on Twitter @mayahustle.

Center for Computation & Technology
2003 Digital Media Center • Telephone: +1 225/578-5890 • Fax: +1 225/578-8957