Events

Current Events
Lectures▼
Events Archive▼

Cybersecurity Lecture Series

Dissecting Industrial Control System Malware

Jimmy Wylie, Dragos

Digital Media Center 1034
September 16, 2019 - 04:00 pm

Abstract:

Discovery of TRISIS/TRITON was a landmark event in the Industrial Control Systems (ICS) security community. It is the fifth known ICS-specific malware (following STUXNET, HAVEX, BLACKENERGY2, and CRASHOVERRIDE), and the first such malware to specifically target safety instrumented systems. Since identification and public disclosure in early December 2017, much has been written on TRISIS and its implications, but technical deep-dives of TRISIS, specifically the binary payloads, are scarce.

TRISIS is a complex piece of malware and analyzing the attack requires a blend of both hardware and software reverse engineering. In this talk, we will explain our approach to analyzing this sample and at the same time, provide a detailed walkthrough of TRISIS with a focus on the PowerPC payloads and relevant portions of the Triconex firmware. Further, we will discuss the impact of TRISIS for the reverse engineering community as a whole.

Speaker's Bio:

Jimmy Wylie is a Senior Adversary Hunter at Dragos who spends his days (and nights) searching for and tearing apart threats to critical infrastructure. Starting as a hobbyist in 2009, he has over 9 years of experience with reverse engineering and malware analysis. As a professional in the U.S. Intelligence Community, he utilized a wide range of skills against national level adversaries, including network analysis, dead disk and memory forensics, in-depth malware analysis, and software development supporting the detection, analysis and classification of malware in a variety of programming languages. Before joining Dragos, he was a course developer and instructor at Focal Point Data Risk, teaching a wide range of malware analysis techniques starting with beginner behavioral analysis and ending with kernel driver analysis. He can be found on Twitter @mayahustle.