CYBERSECURITY LECTURE SERIES

GROWING PAINS: DRAGOS INTEL'S EVOLVING DEFINITION OF ICS MALWARE

November 12th at 4:30 P.M.

DMC Theater, LSU Digital Media Center

Jimmy Wylie

Distinguished Malware Technical Lead @ Dragos, Inc.

ABSTRACT

In 2016, CrashOverride was discovered, and it was the only malware that year that could be reasonably called ICS Malware. 8 years later, we now have ICS Aware ransomware, as well as other ICS-capable threats, like FuxNet, FrostyGoop, COSMICENERGY, and more. Throughout that timeframe, Dragos Intel has had to think about what constitutes an ICS threat and when to apply the moniker of ICS Malware to a sample. Do we count ransomware as ICS Malware? Do we count malware that targets an ICS Vendor's IT network? What about malware with no related event? Or weirder, malware where we don't even have source code?

In this talk, I'll recount a small history of the Dragos Intel team and how our understanding of ICS Malware has grown over the years. I'll cover the samples Dragos considers ICS Malware, what they have in common, and how these commonalities led us to our current definitions of ICS Malware and ICS Threats. I'll then show how we apply that process to known ICS malware, as well as malware that doesn't quite make the cut.

SPEAKER BIO

Jimmy Wylie is a Distinguished Malware Technical Lead at Dragos, Inc. who spends his days 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 13 years experience with reverse engineering and malware analysis. In his off-time, Jimmy enjoys learning about operating systems internals, playing board games, and solving crossword puzzles.