CYBERSECURITY LECTURE SERIES

HUNTING OF PYTHONS AND GOPHERS: PLAYBOOKS FOR BINARY TRIAGE

November 11 at 4:00 p.m.

DMC Theater, LSU Digital Media Center

Jimmy Wylie

DRAGOS, INC.

ABSTRACT

Python and Go make software development easier, but what helps software developers can also empower attackers. From TRISIS and PIPEDREAM to FrostyGoop, these languages have become the favored tools for ICS/OT malware authors. Yet compiled Python and Go binaries don't yield to traditional reverse engineering approaches, leaving many analysts struggling when they encounter these threats.

This presentation will demonstrate techniques for analyzing Python and Go malware using four real-world ICS-related samples discovered through threat hunting: a multi-exploit PLC/HMI attack tool, Kurtlar_SCADA—a weaponized VNC client used to compromise dozens of HMIs, a Chinese vulnerability scanner targeting industrial protocols, and an obfuscated Go reverse shell targeting Ukrainian defense entities.

For each sample, we'll show you how we found it, what analysis challenges it presented, and how we used tools like PyLingual and Goresolver, as well as manual techniques, to determine its capabilities and assess its reputation. You'll learn why automated tools fail, how to exploit static properties in obfuscated binaries, and workflows for deobfuscating or decompiling these types of samples. Attendees will leave with playbooks for analyzing compiled Python and obfuscated Go binaries, an essential skill in modern IT and ICS malware analysis.

SPEAKER BIO

Jimmy Wylie is a malware analyst at Dragos, Inc., focused on threats to critical infrastructure. He was the lead analyst on several landmark cases, including PIPEDREAM—the first ICS attack utility belt; TRISIS—the first malware to target safety instrumented systems; and the analysis of historical artifacts from CRASHOVERRIDE—the first malware designed to disrupt breakers and switchgear in electric transmission substations. He has over 15 years of experience in reverse engineering and malware analysis, and has presented at SANS ICS Summit, DEF CON, and RECON, sharing insights on ICS malware analysis and threat group capabilities. Find him on LinkedIn, Mastodon (@mayahustle@infosec.exchange) and BlueSky (@mayahustle.com).

LSU Center for Computation & Technology

LSU Cyber Center

LSU Ethics Institute