The Center for Cyber Defenders
Expanding Computer Security Knowledge

SAND2015-5794D

ICS-CERT: Visualization Panel

Kelly Luk Bounsawat, Texas A&M University; Allison Campbell, Southern Illinois University; Andrew Chu, Albuquerque Academy High School

Project Mentors: Samuel Mulder, 5631; Michael King, 5624; Susan Wade, 5628

Problem Statement:

Network attacks are ever present, and ill-prepared entities risk serious damage to critical infrastructure. Often times, network administrators/monitors are not prepared to handle attacks or malicious activity on complex control or monitoring systems.

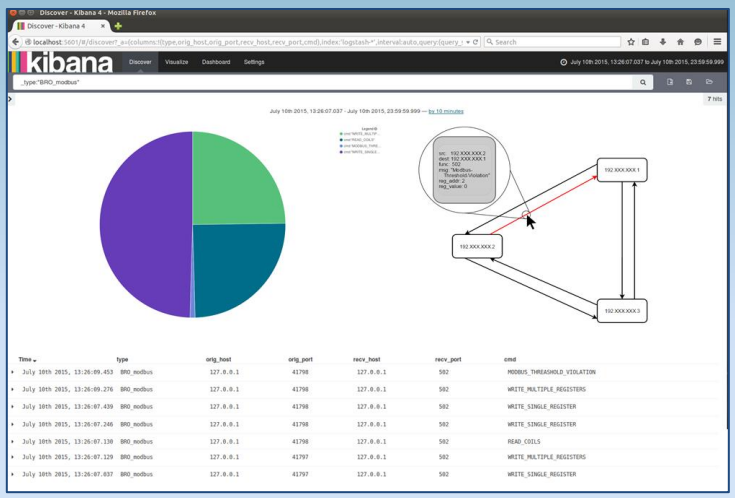
DHS (**D**epartment of **H**omeland **S**ecurity) ICS-CERT's (**I**ndustrial **C**ontrol **S**ystems **C**yber **E**mergency **R**esponse **T**eam) SCADA (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition) system currently lacks an approachable and appropriate software system to monitor modern threats to their systems.

Objective and Approach:

- Design a user-friendly, approachable system to aid network administrators in successfully monitoring and responding to potentially malicious activity on their network
- Track anomalies to determine potential threats
- Utilize Bro Scripts to filter packet information (primarily Modbus)
- Employ Logstash and Elasticsearch to organize and store information obtained from Bro/Bro-Bounds
- Modify Kibana source code to create a dynamic visualization of network traffic

Impact and Benefits:

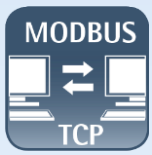
- Improvement of DHS ICS-CERT's SCADA system
- Simplification of network analysis for complex control systems



Screenshot of Kibana User Interface with a custom visualization panel

Results:

- Bro Scripts that filter Modbus network traffic, focusing on statistical anomalies
- Customize Kibana visualization panels to display network traffic anomalies dynamically and relationally



Flow from network monitoring to visualization utilizing Bro and the ELK Stack