SAND2022-9459D

The Center for Cyber Defenders
Expanding computer security knowledge

Project Tantrum

Hannah Stroble, Auburn University
Jonathan Hernandez, University of Texas at San Antonio

Mentors: Amanda Gonzales, Org. 5621; Susan Wade, Org. 5628

What is Tantrum?

Project Tantrum focuses on the following:

- Creating behavioral analytics to detect abnormal activity
- Assist in collection and analysis of protocol traffic

Current Work

Tantrum gathers data from cyber-physical sites and provides analysis on this vast amount of data. Tantrum focuses on network anomaly and threat detection without the use of signature detection.

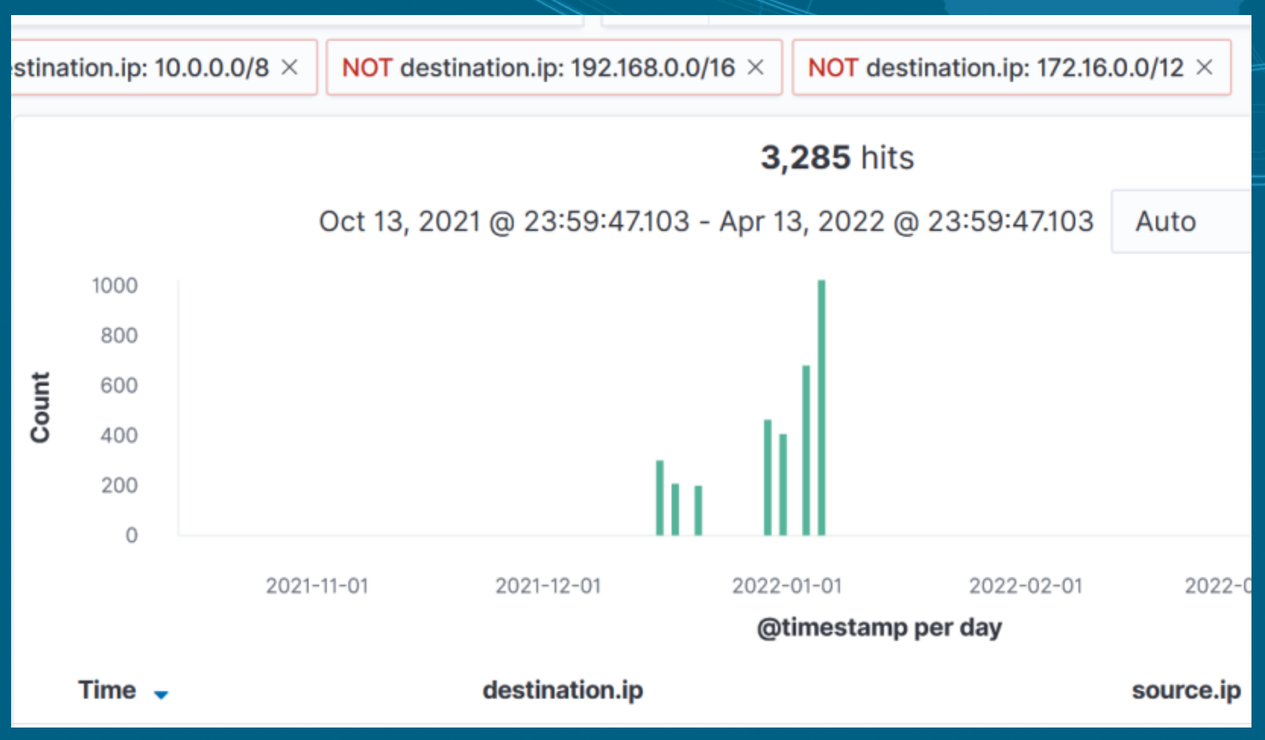
Current features:

- Construct detailed analytics that are used to detect malicious oddities using threat intelligence
- Develop red team attacks to test current analytics

Impact

Tantrum combats zero-day VxWorks vulnerabilities, where more than two billion devices within SCADA, infrastructure, and industrial controllers are effected. Cyber-physical systems produce vast amounts of data that are difficult to protect and analyze. Tantrum enables tackling this problem by:

- Analyzing data using threat intelligence and machine learning
- Automatically sorting through massive amounts of data to find patterns and their risk scores
- Enabling repeatable and controllable analytics for further applications

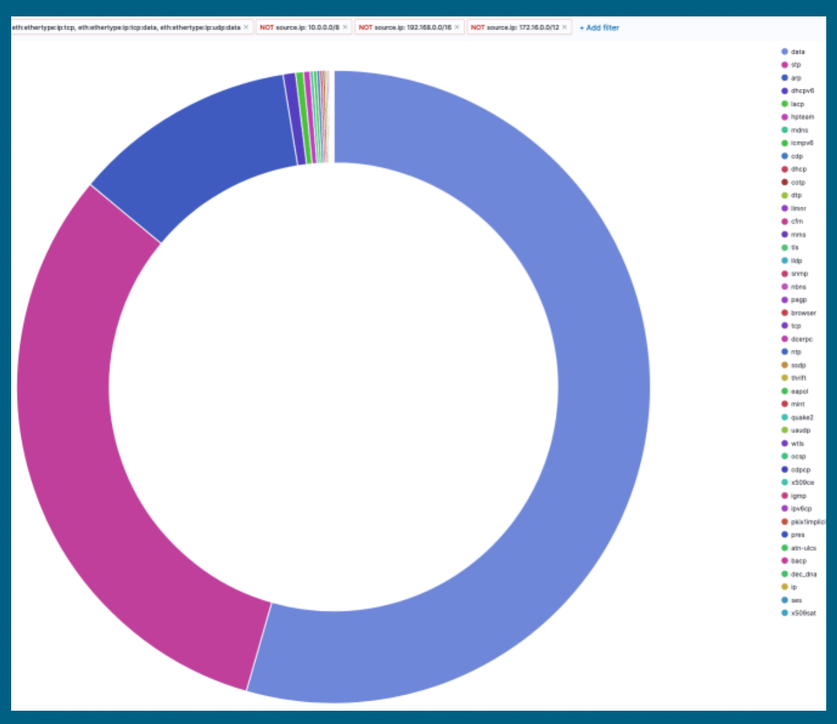


Routable IP Anomalies:
The network range appears legitimate, however these OT protocols traveling to public facing Ips without encryption or tunneling is unexpected and unusual

Project Design

The Tantrum project is divided into **three** main components. Tantrum is very flexible with introducing more tools into the structure.

- ***Archimedes:*** software focused in discovering anomalies in OT traffic using machine learning
- ***ElasticUtils:*** software configured to parse PCAPs for fields of interest and visualize behavior with Kibana
- ***Tamizar:*** system of network analytics used to ingest and view data for other anomalies, sister project



External Sources by Protocol:
Several OT protocols were found speaking to external Ips. These protocols included COTP and MMS which is unusual

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2019-8014 D.

U.S. DEPARTMENT OF ENERGY
National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.