The Center for Cyber Defenders

Expanding computer security knowledge

SAND2020-7291D

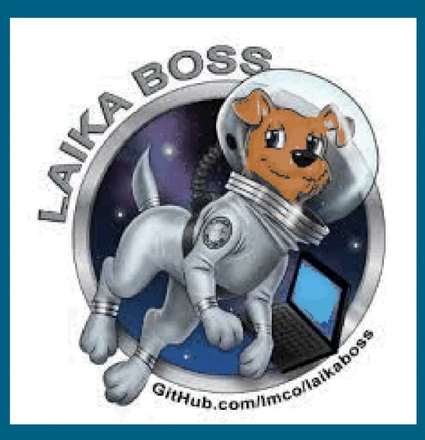
Windows Error Reporting Analysis

Max Triano, University of Michigan; Jared Wilson, Purdue University;
Phil Dawson, Santa Clara University

Project Mentors: Kaitlyn Gurule and Brian Healy, Org. 9317

Problem Statement

- Thousands of crash events from computers across the Lab are sent to WERA every day. We want to extract the signal from the noise by filtering out duplicate and uninteresting events. We also seek to extend the functionality of WERA by parsing memory dumps and automatically alerting if WERA goes down.



Objectives and Approach

- One of the main tools which we have used for this project is Splunk. It has allowed us to analyze crash metadata. This analysis will allow us to help determine which crashes are normal and which crashes could be signs of malicious behavior.
- We also used LaikaBOSS as a tool to gain more information from crash reports

Results

- Identified and filtered out the most common events using Splunk, allowing us to reduce the number of files we process significantly
- Used Splunk to extract least common files for further analysis

Impact and Benefits

- Analyzing and processing crash reports will help provide useful knowledge on how the Sandia networks and Sandia devices operate. The ability to process, analyze, and parse this data properly will allow us to separate the noise (uninteresting crashes) from the potential "needle in haystack" which is a crash which provides information about malicious activity. It is commonplace that applications and files which adversaries use can cause crashes as part of their malicious activity. WERA will be able to detect when these crashes occur and help the Incident Response team pinpoint malicious actions.

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. SAND2020-XXXX X.