SAND2020-7372C

The Center for Cyber Defenders

Expanding computer security knowledge

Laika BOSS

File Analysis and Metadata Collection

Callie Aboaf, Cornell University

Hannah Reinbolt, Missouri University of Science and Technology

Project Mentor: Greg Walkup, Org. 9312

Problem Statement

Given the increasing variety and number of files on corporate networks, there is a need for a mechanism that detects and mitigates the threats of malicious file objects.

An object scanner:

- examines potentially harmful objects
- determines what security risks they may present
- gathers metadata

To this end, Laika BOSS, developed by Lockheed Martin, was introduced as a scalable and flexible object scanning framework.

Objectives and Approach

Laika BOSS is one of the first lines of defense against malicious file objects. To scan objects, the framework recursively applies a combination of:

- Analysis
- Data Extraction
- Metadata Extraction

Laika BOSS can also apply file-based signature detections to identify malicious files through static analysis. The scan results can then be used to react to a file in real time or afterwards by incident responders.

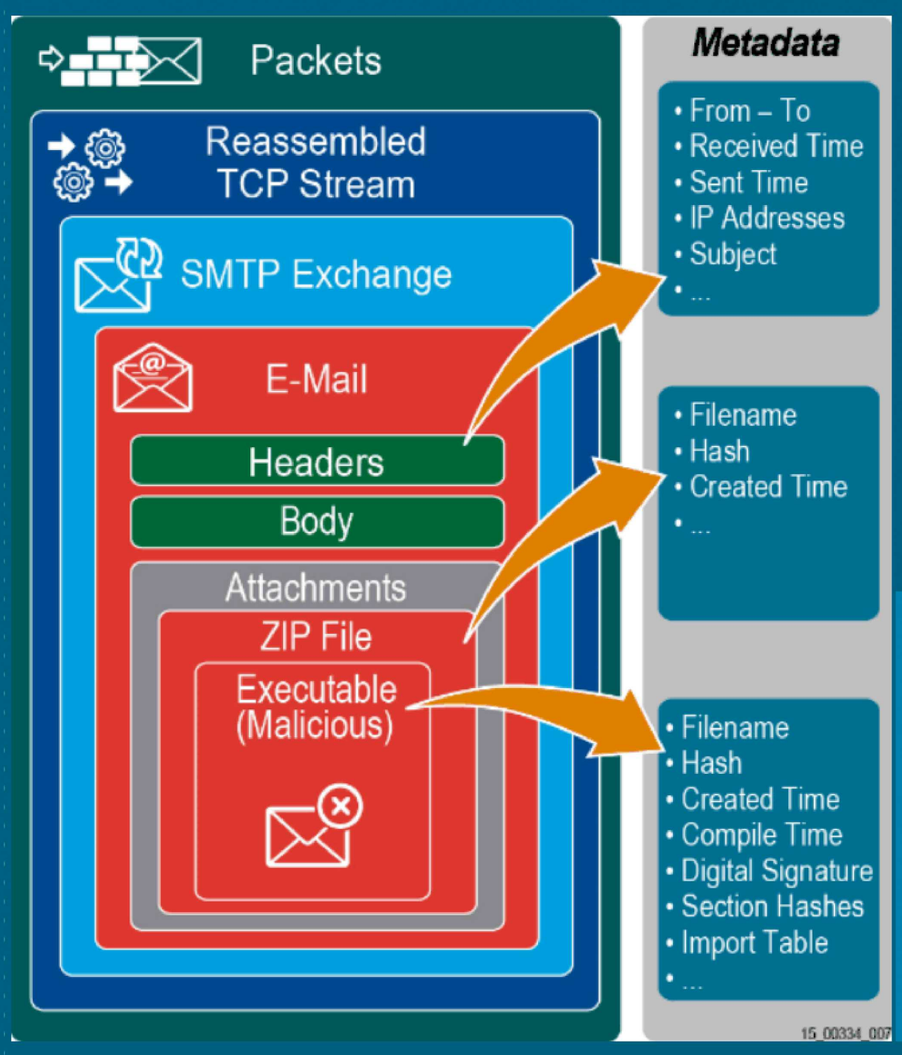

Figure 1:

Laika view of an exploded email, showing a malicious executable contained within a ZIP file and extracted metadata.

Results

Over the summer, we extended the Laika BOSS framework to extract embedded information, do further analysis, and discover metadata for new data sources, including:

- **Har files:** short for HTTP Archive, which serve as a log of a web browsing session
- **Hachoir utility:** ability to browse and edit binary streams like files and folders
- **DMARC reports:** which detail information about malicious emails sent to a corporate network

Impact and Benefits

With our improvements, Laika BOSS has visibility into a wider variety of files that are found in a workplace environment. This increased visibility enables incident response teams to better identify and react to incoming threats, from phishing attacks to malicious documents and applications.

Furthermore, the data gathered by scanning these objects can be used to develop strategies to protect the network from future attacks.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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. SAND2017-XXXXC.