Malware Analysis SIG

Agenda

- About Us
- SIG Mission
- Current Publications
- Goals
- Meeting Time

ABOUT US

Andreas Muehlemann - Co-Chair

James Potter - Co-Chair

Raja Jasper - Co-Chair

Malware Analysis SIG Mission

This SIG will have as goal to develop best practices for the CSIRT community around malware detection, mitigation and remediation. It will aim to build a framework which organizations can readily adopt for malware response, including both baseline and state of the art elements at varying levels of organizational maturity, and develop an index of tools available to fill specific needs.

Current Publications

- Malware Analysis Framework
- Malware Analysis Tools

2023-2024 Goals

- Publish Version 2 of Malware Analysis Framework
- Malware Analysis Lab framework
  - Demo's of existing malware analysis labs from members
- Malware groups and how to analysis
  - Commonly used tool list to perform malware analysis
- Training documentation on malware analysis
  - Beginner to advanced
- General Malware Slack group chat
  - Questions on malware analysis and/or news

Meeting time

9:15-10:15 Thursday, June 8th SIG Room 1 (Notre Dame)

Current Bi-weekly meetings

11am-12pm EST

Slack group: MA-SIG

https://portal.first.org/g/Malware%20Analysis%20SIG