Malware Analysis WG

Olivier Caleff (Liaison @FR)
Andreas Muehlemann (SWITCH @CH)

Wednesday, May 6th, 2021 – 15:10 CET

Context

- Many chair rotations over the last years
  - Maarten Van Horenbeeck, then Michael Mitama + Susan Ballestero
  - Michael Mitama + Olivier Caleff , then Olivier Caleff + Kyle O'Meara
  - **Olivier Caleff + Andreas Muehlemann**
    - **COVID: everyone is very busy, not a lot of time unfortunately**

- Meetings
  - Regular meetings, every other Fridays 6pm CET / noon EDT
  - Malware Analysis Framework, every other Fridays 1pm CET / 7am EDT
- Attendance
  - 3 to 4 participants for meetings
- Tools
  - Mailing-list, Amnesia portal, Slack channel

Projects

- IOC Types v2 → nothing validated
- Updates of the FIRST Web page on tools → soon
- Malware Tools Overview → soon to be published

soon

- Malware Analysis Framework → started working on it

NEW

Malware Tools Overview

- Re-use what's already available, don't re-invent the wheel
  - Analysis VMs: too much work to compete with existing projects
  - Trainings: much is available for free, don't create new training courses

- **Present a starting point to anyone willing to start in the field**
- **Present guidelines to support the learning process**
- **Try to initiate discussions within the FIRST community about malware related topics**

Malware Analysis Framework

- Reasons for tracking some malware
  - Activity sector-based / constituencies need / input from feeds / potential impacts / …
- Best practices on malware analysis and response
  - Phase 1 – Preparation
    - Triage process, prioritization, which strategy/playbook to analyze the sample
  - Phase 2 – Analysis Process
    - the actual analysis
  - Phase 3 – Post analysis
    - Good practices to share hashes (at minimum) and files (when appropriate)

Plans for 2021 – 2022

- Increase the number of active participants
- Publish deliverables and updates
- Work on the Malware Analysis Framework
  - This is a brand new initiative, join