How to write Malware Analysis Reports

Description and details of the malware

- Name, date, format, file size, brief description and acquisition of the malware
- MD5/SHA hash
- Virustotal, VirSCAN, Metascan Online results

Results from analysis

- Excerpts from Cutter, IDA and such
- Any form of communication with the outside.
- Similarities/Dissimilarity with other specimens.
- How does it achieve execution/persistence.
- Dependencies
- What does it do
- How does it spread
- How was it produced

General Tips

- Use mindmaps like this one
- Maintain notes during analysis, take screenshots, save logs

Malware Report Template

Dependencies
- Supported OS
- Required libraries
- Configuration files
- Scripts and executables
- URLs

Observations
- Behavioral analysis
- Static code analysis
- Dynamic code analysis
- Memory analysis

Supporting Figures
- Logs
- Strings
- Function listings
- Screenshots

Summary of the analysis
- Key observations
- Recommendations
- Limitations
- Report date and authors

Sample's Identification
- File name, type, size
- File hashes
- Anti-malware identifiers

Sample's Characteristics
- Infection capabilities
- Self-defensive measures
- Spreading mechanics
- Data leakage abilities
- Remote attacker interactions