Writing Analysis Reports

File Analysis Reports

- **CONTENTS DEPEND ON PURPOSE**
  There are many different ways reports can look like
- **WE ARE USING ONLY EXAMPLES**
  no exhaustive list, no definite rules
  purpose: give you some idea on report writing
- **WE LOOK AT MALWARE REPORTS FOR BLOGS**
  probably most useful for you

Example 1: Antivirus file submission

1. FILE HASH(ES)
2. SUBMITTER
3. DATE
4. REASON FOR SUBMISSION
5. ADDITIONAL INFORMATION
6. DESCRIPTION OF SAMPLE
7. ANTIVIRUS DETECTIONS BEFORE & AFTER
8. VERDICT & REASON FOR VERDICT

Example 1: Antivirus File Submission

- **FILE HASH**
  e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
- **SUBMITTER**
  Jane Doe
- **DATE**
  28. Mai 2023
- **REASON FOR SUBMISSION**
  The file is malicious, your scanner fails to detect it --> False negative
- **ADDITIONAL INFORMATION**
  This file made my system sluggish! See benchmark.

Example 1: Antivirus File Submission

- **DESCRIPTION OF SAMPLE**

  The submitted file has a size of 0 bytes

- **VERDICT + REASON**

  Junk, because it is an empty file.

  It is likely that the sample upload failed, support should check the customer's Firewall settings.

- **ANTIVIRUS DETECTION BEFORE AND AFTER**

  No antivirus detection, this did not change

Why blog articles?

- Helps your work to be be seen
- Can point to it at job application
- Contribution to the greater good
- Learn systematic, goal oriented analysis
- Improves writing skills

Example 2: Blog article about malware

1. **STORY**
   - common thread of the article
2. **TECHNICAL DETAILS**
   - infection vector
   - persistence
   - evasion techniques
   - idiosyncracies
   - communication
   - potential danger
3. **MALWARE CLASSIFICATION**
   - minimum: family and type
4. **PROTECTION OPPORTUNITIES**
   - e.g. detection signatures, security advisory
5. **INDICATORS OF COMPROMISE**
   - must have: file hashes
   - optional: file names, C2, download URLs, ...