Case Study # 1

Note: No need for extensive reports, just report what you think you understood. A guideline is given,but you are open to report any interesting findings you happen to find. Do mention that explicitly at the end of the report.

Pre-processing

0.1. What is an APT group?

A. Choosing your poison

1. Choose an APT group.

Fancy Bear, Cozy Bear, Lazarus, Transparent tribe or just any apt group (Why not an APT group of a random country/state).

2. Is APT group state sponsored?

3. Describe their Major attack

- Timeline of events.
- Malware/tools used.
- Target industries or organizations.
- Attack techniques (just a brief of methodologies)

B. Threat Intelligence Analysis

4. What were the impacts of attack (was it done for financial gain, national security, etc)

5. Which threat intelligence feed would you prefer to use?

6. Identify indicators of compromise from this attack.

C. What have you learned??

7. In which category of malware should you classify the malware used by apt (if you think it was a combination of different malware types, mention all of them)

D. Lessons Learned

8. What mistakes did the victims make that enabled the attack?

9. What measures could have reduced impact?