

# A Research Protocol

## A.1 Research Questions

- SQ1: What processes and procedures do cybersecurity practitioners follow to attribute an attack to a ransomware group in service of sanction screening?
- SQ2: What techniques and indicators are currently used for ransomware threat actor attribution?
- SQ3: To what extent are high-level indicators reliable in the identification of ransomware groups?
- SQ4: What needs to be improved to further develop ransomware attribution standards?

Table 9 lists our interview questions.

## A.2 Collection of Empirical Data

### Invitation and Explanation

You are being invited to participate in a research study titled “Leveraging High-Level Indicators: Correlating Ransomware Attacks to Threat Actors”. This study is being done by <responsible researcher> from the <institution> and supervised by <company>.

The purpose of this research study is to find out whether high-level indicators can help correlate ransomware attacks to threat actors by the means of audio recording and will take you approximately 90 minutes to complete. Therefore, the participants are experts in identifying cyber-threat actors (Cyber-threat attribution). The data will be used for improving the state of art on the current cyber-threat attribution process and their current limitations. We will be asking you to provide information about the current cyber-threat attribution process and the limitations. In addition, improvement points or ideas to improve the current cyber-threat attribution process are appreciated.

As with any online activity, the risk of a breach is always possible. To the best of our ability, your answers to this study will remain confidential. We will minimize any risks by storing the data in a Project Storage at <institution>, which allows for access restrictions in such a way that only authorized members can access the data. By doing this, the risk of a data leak, which can lead to reputational risk, is minimized. The information will be anonymized and only the function and a small job description will be used. The information you provide will be synthesized in an anonymous summary. The summary will be sent to you for review and will be used for analysis purposes. The summary will be made publicly available with the final report. Should you have any concerns regarding the content of the summary, you will be welcome to oppose its publication.

Your participation in this study is entirely voluntary, and you can withdraw at any time. You are free to omit any ques-

tions. The participant has the right to request access to provided data and can demand to rectify or erase personal data.

If there are any questions before/after the interview, you can contact me with the following contact details: <details>

Table 9: Interview questions

| Segment 1: Overview of Cyber Threat Attribution  |
|--|
| 1. How are cyber threat actors typically categorized based on their characteristics and traits?  |
| 2. Can you describe the techniques or methods that your organization currently employs for cyber threat actor attribution of ransomware groups?  |
| 3. In your experience, which indicators are typically considered when attributing a cyber threat to a ransomware actor or group?   |
| 4. Are there differences in cyber threat attribution techniques when dealing with different types of threat actors, such as state-sponsored groups, cybercriminals, or hacktivists?                      |
| 5. Are there different levels of attribution? If so, do you observe differences in the level of attribution when comparing different organizations, such as law enforcement and cybersecurity companies? |
| 6. At what level is the ransomware attacker identified?  |
| Segment 2: Strengths and Limitations   |
| 7. What do you consider the main strengths of the attribution techniques or methods you use?   |
| 8. What limitations or challenges have you encountered when attempting to attribute cyber threats to specific actors or groups?  |
| 9. Can you provide an example of a recent or notable case of cyber threat attribution you have worked on, and walk through the process of attribution, including the techniques and indicators used?     |
| 10. In your opinion, how important is it to consider the potential risk of false attribution in the field of attributing cyber threat actors, and how do you mitigate this risk?                         |
| 11. Are there specific legal or ethical considerations that impact your approach to attributing cyber threat actors, and if so, how do they influence your work?   |
| 12. Can you share examples of cases where attribution efforts did not lead to a clear identification of the threat actor? What were the main challenges in these cases?                                  |
| Segment 3: Adaptation and Future Developments  |
| 13. How do you stay informed about evolving techniques and indicators in the field of attributing cyber threat actors, and how do you adjust your methods accordingly?                                   |
| 14. In your opinion, what are the most significant areas of improvement or development needed in the field of attributing cyber threat actors?   |