Format inspired by NWO reviewer guidelines and templates.

Identification

Proposal title: DeVM: Automated De-Virtualization of Virtual Machine-Obfuscated Malware

Overall assessment

Explain in one sentence or short paragraph how you see the entire project.

The project is an interesting and promising approach to deobfuscating virtualized malware. The proposal proposes a systematic approach using techniques that can inspire new directions of research.

Final score. How do you assess the entire application? Please give the final score for this proposal. Consider doing this after completing the rest of the application.

The final grade for this proposal is, in your view:

seven (7) Format: "ten (10)" or "six (6)", but not "ten" or "6".

Use the following scores in your grading:

Score	Meaning
10	Outstanding, must fund
9	Excellent, must fund
8	Very good, should fund
7	Good overall with one aspect very good, fund if room
6	Good, fund if room
5	Sufficient, fund if room
4	Insufficient, do not fund
3	Bad, do not fund
2	Very bad, do not fund
1	Does not meet academic level, do not fund

Please explain your answers. Try to exceed the length of 50-100 words per answer only when absolutely necessary.

Question 1. What is the scholarly, scientific or technological relevance of the problem? Is the problem original, timely, challenging? Is this a new line of research?

Answer:
Malware reverse engineering is of all time. The problem is not original [1,2] but it is still an open problem. The problem is very challenging because of the sheer amount of possibilities for an adversary to obfuscate his code using virtualization, generalizing over these possibilities is hard.

Question 2. What are the innovative and original aspects of the proposal? Are the project objectives challenging and scientifically ground-breaking? Is the methodology credible?

Answer:
The innovative and original aspects of the proposal are the usage of concolic execution to capture side effects on instruction blocks and the usage of machine learning to classify side effect traces according to machine instructions. The methodology is open enough to be challenging. If proven successful, both original aspects could inspire new lines of malware research.

Question 3. Is the approach effective, including the practical work programme? How do you assess the program of work described in the proposal (realistic, feasible, ...)? Are the most important risks identified and effectively mitigated?

Answer:
The program of work is realistic by following a systematic approach. The methodology is visualized using a clear diagram. Some risks are missing. For example, it could be difficult to collect enough traces to accurately train the neural network. Another risk that is not mentioned is the possibility of state explosion using concolic execution if not enough concrete values can be provided.

Question 4. Is the proposal well-written and are the project's objectives clearly worded? Do you expect this project will lead to significant advancement of scholarship, science, or technology (academic impact)?

Answer:
The proposal is very well-written and the project's objectives are clearly worded.

Question 5. What is your opinion on the societal impact of the proposed research? Are the expected results of the research relevant for solving a popular/economic/cultural/ technical or policy-related challenge?

Answer:
The proposed research has the potential to decrease the reverse engineering effort of malware. This can consequently decrease the response time on a malware outbreak and

improve the ability to mitigate damages caused by such an outbreak. The proposed research can have a positive economical and technical impact.

Question 6. Are the main stakeholders of the problem clearly identified and addressed in the proposal? If any, what are the most important stakeholders the proposal does not address?

Answer:
Both companies and malware researchers are named as stakeholders. No important stakeholder is omitted.

Question 7. Is the release of data and software artifacts clearly identified and addressed in the proposal?

Answer:
The proposal does not address the release of data and software artifacts.

Question 8. Are the main ethical concerns clearly identified and addressed in the proposal? If any, what are the most important ethical concerns the proposal does not address?

Answer:
The main ethical concern is breaking VM based DRM solutions, which is addressed in the proposal.

Please identify at least 3 of the main strengths of the proposal:

Answer:
S1. Systematic approach.
S2. Inspires new directions of research.
S3. Potential for societal impact.

Please identify at least 3 of the main weaknesses of the proposal:

Answer:
W1. The proposal does not try to reuse and build upon existing compiler and lifting frameworks such as LLVM.
W2. The proposal does not address the release of data and software artifacts.
W3. Some potential risks are not addressed.

[1] Salwan, J., Bardin, S., & Potet, M. L. (2018, June). Symbolic deobfuscation: From virtualized code back to the original. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 372-392). Cham: Springer International Publishing.

[2] Coogan, K., Lu, G., & Debray, S. (2011, October). Deobfuscation of virtualization-obfuscated software: a semantics-based approach. In Proceedings of the 18th ACM conference on Computer and communications security (pp. 275-284).