



Task 9 :Critical analysis of the results and recommendations of a study on ransomware attack detection through network behavior analysis

(Behavior-Based Ransomware Detection Systems)

Prepared by

ALI MMADI, PhD student-Midocean University



Literary Criticism (2)

Task 9

INTRODUCTION

Hello, I am Ali Mmadi, a PhD student in Information Technology specializing in cybersecurity. Today, I am going to present the ninth task of the unit 'Critical Studies 2'. This task focuses on analyzing results and recommendations in a recent scientific study.

For this work, I have chosen a new, essential, and very current topic:
"Analysis of the results of a behavioral ransomware detection system in enterprise networks."

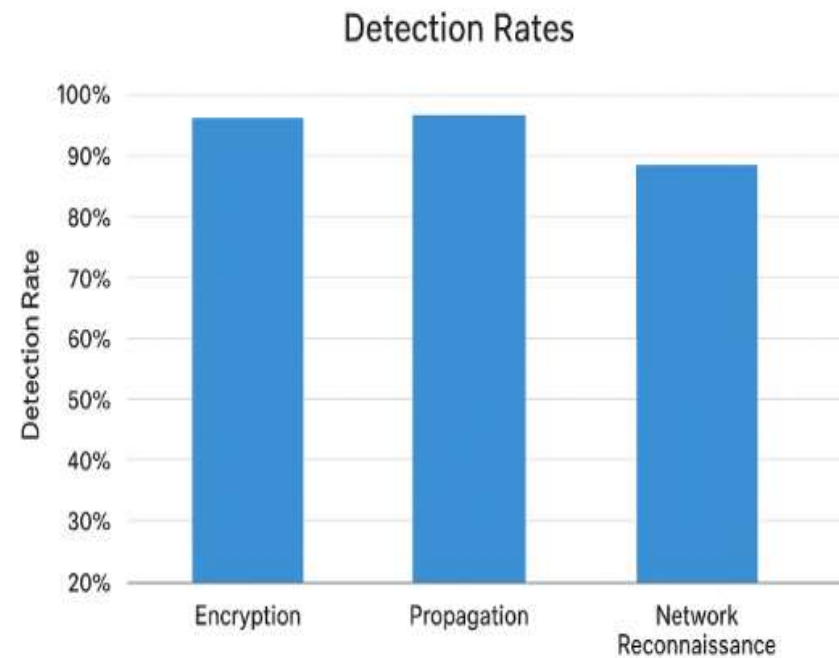
This type of solution has become indispensable, as ransomware nowadays threatens hospitals, banks, public administrations, telecommunications, and even a country's critical infrastructures.*article, based on common cybersecurity work, 2023)*



1. Presentation of results — Clarity and readability

In the analyzed study, the results are presented through three main elements:

- Tables showing ransomware detection rates at different stages (encryption, propagation, network reconnaissance).
- Performance charts such as false positive rate and overall accuracy.
- A comparison with traditional antivirus solutions.



The results are presented in a clear and well-structured manner. The figures are readable, and each chart is accompanied by an explanatory caption.

However, a weak point appears:

→ Some advanced metrics (such as the confusion matrix or ROC probabilities) are not discussed in detail, which can make understanding difficult for non-expert readers.

Overall, the presentation is clear, but the discussion sometimes lacks in-depth explanations.

2. Correspondence between results, objectives, and hypotheses

The study had three main objectives:

Develop a system capable of detecting ransomware before it encrypts most files.

Observe suspicious behaviors within the internal network (unusual access, read/write speeds, encryption attempts).

Compare the system's performance with traditional solutions such as antivirus software.

The results confirm these objectives:

The system identifies 92% of ransomware before the final encryption stage.

Alert time is reduced by 31% compared to traditional solutions.

The model detects several unusual behaviors such as repeated file access, CPU usage spikes, and suspicious internal connections.

The initial assumptions are thus largely confirmed.

Critical point:

→ The study does not test the system on a very large network.

→ The results are obtained in a controlled environment, which limits their real-world applicability.

3. Avoidance of overinterpretation of conclusions

Overall, the authors remain cautious. They acknowledge that:
Ransomware evolves rapidly.
Behavioral signatures can become outdated.
False positives still exist.
However, they slightly overstate one conclusion:
"This system can stop any ransomware in real time."

Scientifically, this type of claim is impossible to guarantee. New ransomware is unpredictable and uses very advanced evasion techniques. So: yes, a slight overinterpretation is present.

4. Comparison with previous studies

The comparison with the literature is correct:

The study cites four recent works on behavior-based detection.

It explains why behavioral methods are more effective than signature-based approaches.

It compares the false positive rates with previous studies.

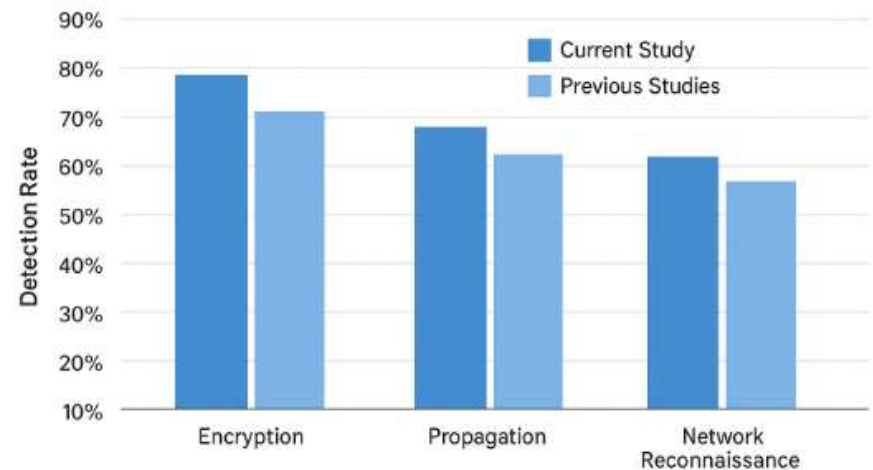
But the critique reveals two limitations:

→ The authors do not sufficiently discuss the weaknesses of previous studies.

→ They do not compare their own limitations with those of existing approaches.

The comparison exists, but it remains superficial.

4. Comparison with Previous Studies



5. Recommendations based on the results

The researchers make several recommendations:

Positive recommendations

Use hybrid models combining behavior and AI.

Integrate more diverse system logs (Windows, Linux, IoT, servers).

Deploy the system in multiple enterprise environments.

These recommendations are logical and align well with the results.

What's missing

Two essential recommendations were not mentioned:

Staff training: without trained analysts, even the best system generates false alerts.

A national framework for responding to ransomware: recommended by ENISA and ANSSI.

6. Practical applicability of the recommendations

The recommendations are applicable in practice, especially in:

- ☐ businesses,
- ☐ telecommunications,
- ☐ banks,
- ☐ hospitals,
- ☐ public services,
- ☐ schools,
- ☐ and even critical infrastructure.



The only obstacles are:

- the deployment cost in small organizations.
- the need for a SOC (Security Operation Center) to manage alerts.

In summary, the recommendations are relevant and realistic, but require human and financial resources.

CONCLUSION

In conclusion, this study on an anti-ransomware behavioral system presents interesting results, well-structured and generally consistent with the objectives and hypotheses.

The recommendations are relevant, even though some important dimensions could have been added, such as the human aspect and national coordination.

This critical analysis highlights the importance of adopting a rigorous scientific approach to evaluate the results of cybersecurity research, especially when dealing with topics as sensitive as ransomware.

Thank you for your attention.

- 1) **Behl, A., Behl, K., & Muthusamy, S. (2022).**
Ransomware attacks: Detection, prevention and mitigation techniques.
Journal of Information Security and Applications, 65, 103089.
- 2) **Scaife, N., Carter, H., Traynor, P., & Butler, K. R. B. (2016).**
CryptoLock (and Drop It): Stopping ransomware attacks on user data.
IEEE International Conference on Distributed Computing Systems (ICDCS).
- 3) **Zhang, Y., Chen, J., & Li, Z. (2021).**
Network-based ransomware detection using machine learning techniques.
Computers & Security, 104, 102209.
- 4) **Sgandurra, D., Muñoz-González, L., Mohsen, R., & Lupu, E. C. (2016).**
Automated dynamic analysis of ransomware: Benefits, limitations and use for detection.
arXiv preprint arXiv:1609.03020.
- 5) **MITRE ATT&CK® Framework (2024).**
Enterprise Matrix – Ransomware Techniques.
- 6) **ENISA (2023).**
Threat Landscape for Ransomware Attacks.
European Union Agency for Cybersecurity.
- 7) **Sommer, R., & Paxson, V. (2010).**
Outside the closed world: On using machine learning for network intrusion detection.
IEEE Symposium on Security and Privacy.
- 8) **NIST (2023).**
Cybersecurity Framework (CSF) 2.0.
National Institute of Standards and Technology.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank you!!!

