



DAMSS

DATA ANALYSIS
METHODS FOR SOFTWARE
SYSTEMS



15th Conference on

DATA ANALYSIS METHODS for Software Systems

November 28–30, 2024

Druskininkai, Lithuania, Hotel “Europa Royale”

<https://www.mii.lt/DAMSS>

Co-Chairmen:

Prof. **Gintautas Dzemyda** (Vilnius University, Lithuanian Academy of Sciences)

Dr. **Saulius Maskeliūnas** (Lithuanian Computer Society)

Programme Committee:

Dr. **Jolita Bernatavičienė** (Lithuania)

Prof. **Juris Borzovs** (Latvia)

Prof. **Janis Grundspenkis** (Latvia)

Prof. **Janusz Kacprzyk** (Poland)

Prof. **Ignacy Kaliszewski** (Poland)

Prof. **Bożena Kostek** (Poland)

Prof. **Tomas Krilavičius** (Lithuania)

Prof. **Olga Kurasova** (Lithuania)

Assoc. Prof. **Tatiana Tchemisova** (Portugal)

Assoc. Prof. **Gintautas Tamulevičius** (Lithuania)

Prof. **Julius Žilinskas** (Lithuania)

Organizing Committee:

Dr. **Jolita Bernatavičienė**

Prof. **Olga Kurasova**

Assoc. Prof. **Viktor Medvedev**

Laima Paliulionienė

Assoc. Prof. **Martynas Sabaliauskas**

Prof. **Povilas Treigys**

Contacts:

Dr. Jolita Bernatavičienė

jolita.bernatavicienne@mif.vu.lt

Tel. (+370 5) 2109 315

Prof. Olga Kurasova

olga.kurasova@mif.vu.lt

Copyright © 2024 Authors. Published by Vilnius University Press.

This is an Open Access article distributed under the terms of the Creative Commons Attribution Licence, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

<https://doi.org/10.15388/DAMSS.15.2024>

ISBN 978-609-07-1112-5 (digital PDF)

© Vilnius University, 2024

Red Team Tactics Against Malware Detection Using Adversarial Attacks

Juozas Dautartas, Arnoldas Budžys, Haroldas Jomantas,
Olga Kurasova, Viktor Medvedev

Institute of Data Science and Digital Technologies
Vilnius University

juozas.dautartas@mif.stud.vu.lt

Static and dynamic malware analysis has been used for a while among cybersecurity professionals and researchers. While static analysis can be used to gather useful information about file features such as strings, hash values, creation date, import address tables, sections and many more, attackers have adapted to these analysis methods quite easily. Dynamic analysis, on the other hand, offers a much deeper insight into what the program does as it monitors the process itself. However, this analysis method requires an isolated virtual environment and can slow down the workflow of the system as it requires additional resources. By combining these two methods, security researchers and security products started using machine learning and deep learning algorithms to detect and mitigate known and unknown cyber threats. Application of these technologies allows antivirus and EDR (Endpoint Detection and Response) systems make decisions faster regarding a file or process is malicious or not. It helps to save some computational resources as well because deeper inspection and classification can take place in a centralised remote server instead of on local computer resources. It comes with no surprise that threat actors started to investigate and search for weaknesses in these detection algorithms as well. Therefore, a deeper insight regarding weaknesses in these deep learning and machine learning models is necessary. Furthermore, deep learning algorithms such as Generative Adversarial Neural Networks, Variational Autoencoders can be used to generate adversarial malware samples that could evade detection. In our research, we aim to design a Command and Control (C2) framework that would use deep learning algorithms to make it more

evasive than standard C2 frameworks. This will help red team members to better train blue teams and notice anomalies by not being over-reliant on automated tools.

Acknowledgements: This project has received funding from the Research Council of Lithuania (LMTLT), agreement No S-MIP-24-116.