LITHUANIAN COMPUTER SOCIETY
VILNIUS UNIVERSITY, INSTITUTE OF DATA SCIENCE AND DIGITAL TECHNOLOGIES
LITHUANIAN ACADEMY OF SCIENCES

16th Conference on

DATA ANALYSIS METHODS for Software Systems

November 27–29, 2025

Druskininkai, Lithuania, Hotel "Europa Royale"
https://www.mii.lt/DAMSS

VILNIUS UNIVERSITY PRESS
Vilnius, 2025

Co-Chairs:

Dr. **Saulius Maskeliūnas** (Lithuanian Computer Society)
Prof. **Gintautas Dzemyda** (Vilnius University, Lithuanian Academy of Sciences)

Programme Committee:

Dr. **Jolita Bernatavičienė** (Lithuania)
Prof. **Juris Borzovs** (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.bernataviciene@mif.vu.lt
Prof. Olga Kurasova
olga.kurasova@mif.vu.lt
Tel. (+370 5) 2109 315

https://doi.org/10.15388/DAMSS.16.2025

ISBN 978-609-07-1200-9 (digital PDF)

Feature Level Deception or When Malware Wears a Mask

Juozas Dautartas, Juozapas Rokas Čypas, Viktor Medvedev, Olga Kurasova

Institute of Data Science and Digital Technologies
Vilnius University

juozas.dautartas@mif.stud.vu.lt

Today's digital landscape shows an unsettling race between cyber defense and offense fields. The rise in popularity of machine learning (ML) has made this race even more intense as these technologies have become an integral part of our everyday security tools and products. These tools integrate various ML algorithms that have been trained on large datasets of static and dynamic malware features or patterns of malicious network traffic.

Therefore, it comes as no surprise that adversaries are implementing various attacks against these classifiers used by security products. That's why testing and validating current defenses is a critical part of a cybersecurity professional's job. In this research, we will analyze a targeted adversarial attack against classical ML malware classifiers. We will focus on Windows API calls from various benign classes as well as malware. These data will be used to impersonate a specific benign class using feature injection techniques. The adversarial samples will be applied to test trained ML classifiers as well as real products.

This research is conducted for ethical and research purposes with an aim to make cybersecurity defenses more robust and reliable. As these realistic and malicious functionality preserving samples can be used to train more accurate malware classifiers in the future.

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