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

14th Conference on

DATA ANALYSIS METHODS
for Software Systems

November 30 – December 2, 2023

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

VILNIUS UNIVERSITY PRESS
Vilnius, 2023

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. Robertas Damaševičius (Lithuania)
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)
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 2109315

https://doi.org/10.15388/DAMSS.14.2023
ISBN 978-609-07-0985-6 (digital PDF)

Obfuscation and Evasion Techniques for Red Team Assessments

Juozas Dautartas, Arnoldas Budžys, Viktor Medvedev

Institute of Data Science and Digital Technologies
Vilnius University

juozas.dautartas@mif.stud.vu.lt

In today's increasingly complex digital environment, businesses, governmental institutions, and ordinary citizens can become a target of cyber criminals. Therefore, measures like advanced Anti-viruses, Endpoint Detection and Response systems, and Extended Detection and Response systems are becoming more and more critical in everyday life as successful cyber-attacks can cause severe damage (e.g., Not-Petya attack in 2017). That's why large organizations have their cyber defense specialists working around the clock in what as part of so-called Blue teams. In many cases, these specialists protect critical infrastructure such as banking sectors, power plants, governmental infrastructure, or businesses in general. Moreover, these Blue teams usually rely heavily on previously mentioned security tools and the telemetry that these tools gather. Therefore, it became a common practice to hire ethical hackers who try to breach and test Blue team's effectiveness. Additionally, report these weak points to security teams before any cyber criminals exploit these holes.

To simulate real-world attacks, Red teams usually use open-source or custom tools to achieve their goals. Since modern defense tools commonly use advanced machine learning algorithms to detect malicious activity, strong malware obfuscation and evasion techniques are particularly important for realistic adversary emulation. In this work, a concept of „ethical malware" obfuscation will be introduced to validate and strengthen existing security defences. Using machine learning techniques, our approach combines generative adversarial networks (GANs) and Siamese neural network capabilities to create, validate, and identify obfuscated malware. The essence of this ethical malware is that it evades detection by traditional defenses. It also intends to work on specialized

malware feature extraction and methods for transforming non-image data into visual form (e.g., GAFMAT method) for training convolutional neural networks and generating malware using GANs.

The effectiveness of these methods could be tested in national and NATO cyber security exercises such as Amber Mist and Locked Shields. Overall, this research is intended to contribute to more resilient and adaptable cyber security as well as train high-level professionals to seek out emerging cyber threats.