OBFUSCATION AND EVASION TECHNIQUES FOR RED TEAM ASSESSMENTS

ID I-9

Juozas Dautartas, Arnoldas Budžys, Viktor Medvedev
Institute of Dada Science and Digital Technologies, Vilnius University
juozas.dautartas@mif.stud.vu.lt

INTRODUCTION

Cyber realm has evolved significantly over the past two decades and has become essential part of our lives. Cyber actors target governments, businesses and in some cases ordinary people. Therefore, advanced antivirus, EDR, and XDR systems are crucial for protecting businesses, governments, and individuals from cyber threats in today's digital world.

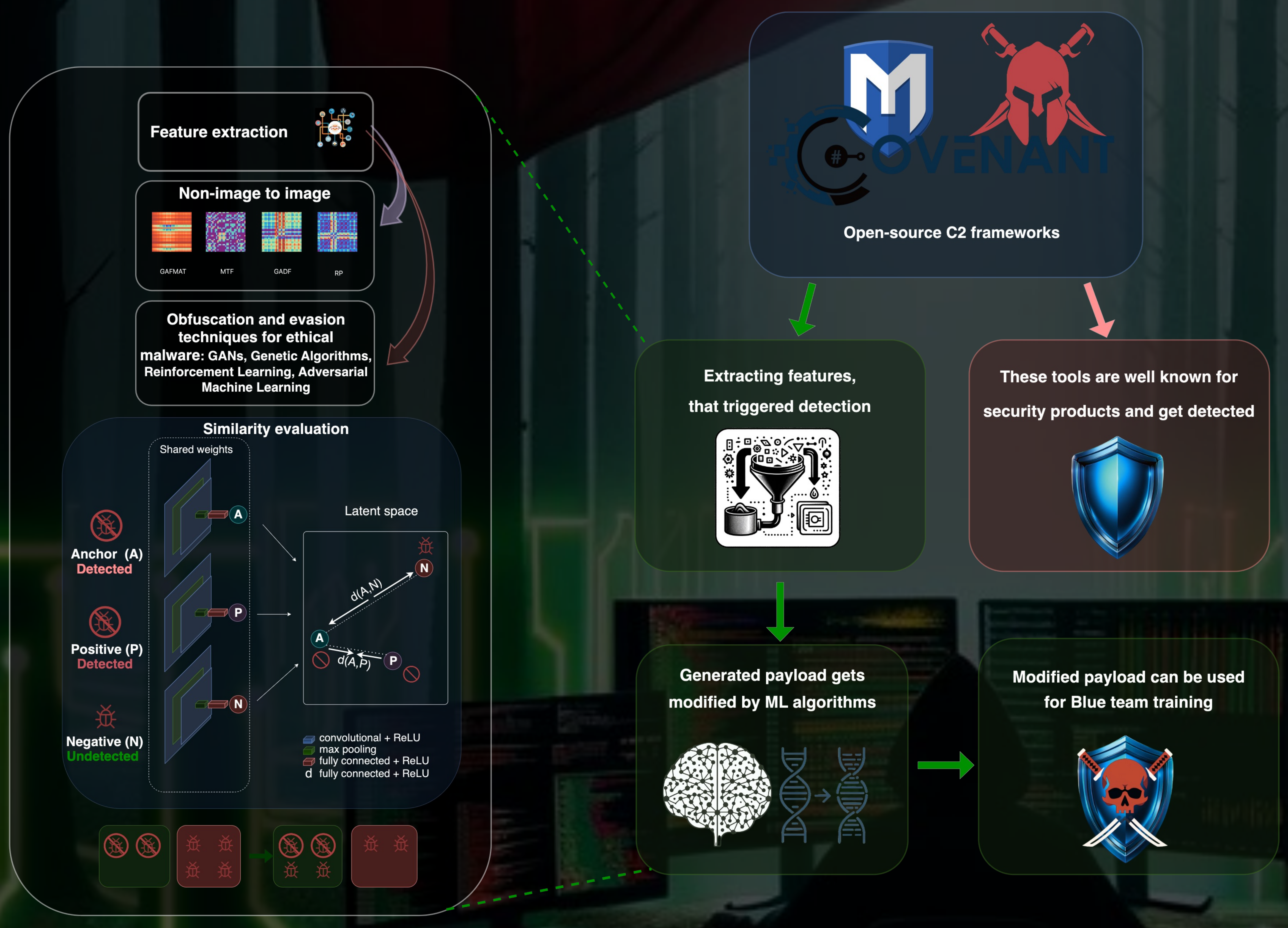
At the end of the day cyber security essentially relies on the weakest and also the strongest link – people. Blue teams protect critical infrastructure need to learn how to hunt attackers and test their tools in a safe environment. To achieve this, we must simulate realistic attacks without causing actual damage. Red teaming is a crucial part of security. And for this proper evasion and obfuscation tools are needed for what is called `Ethical Malware`. Relationship between Red and Blue leads us to safer tomorrow!

BLUE AND RED TEAMS

Blue team specialists protect critical infrastructure such as banking sectors, power plants, governmental infrastructure, or businesses in general. These specialist are first responders when it comes to attack prevention and mitigation if it occurred. However, blue teams usually rely heavily on previously mentioned security tools and telemetry that these tools gather. Realistic training and constant "cyber perimeter" check is very important to ensure readiness of blue teams.

Red teams help train and prepare blue teams by simulating cyber-attacks without actual damage to organization. Red teams usually use open source or custom tools to achieve their goals. These simulations and reports help train blue teams and test security tools that they use.

`ETHICAL MALWARE` OBFUSCATION METHODOLOGY



Feature extraction

Non-image to image

Obfuscation and evasion techniques for ethical malware: GANs, Genetic Algorithms, Reinforcement Learning, Adversarial Machine Learning

Similarity evaluation

Open-source C2 frameworks

Extracting features, that triggered detection

These tools are well known for security products and get detected

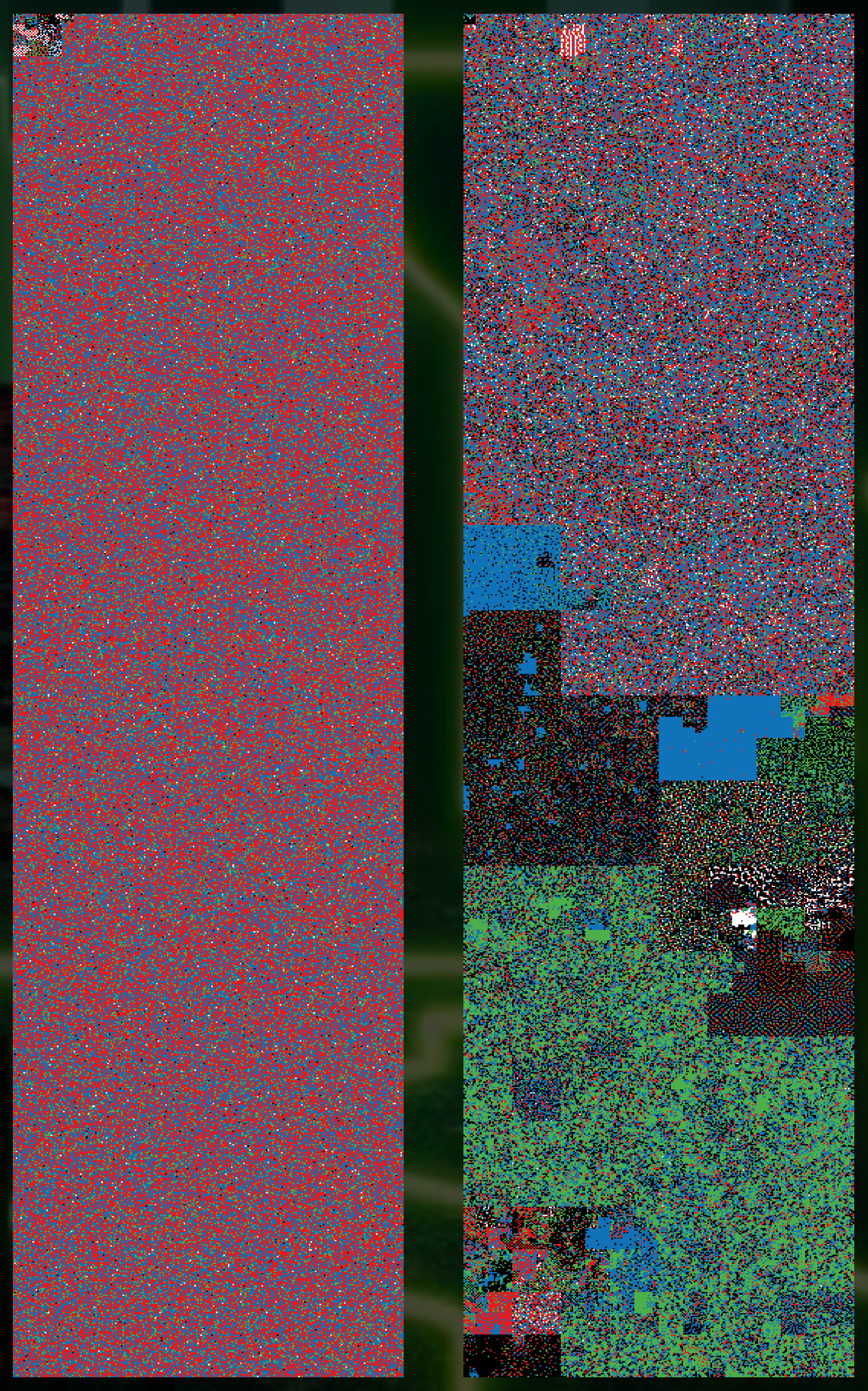
Generated payload gets modified by ML algorithms

Modified payload can be used for Blue team training

FEATURES FOR MALWARE DETECTION

Example of Win32 API functions used for Process injection	Example of Win32 API functions used by Spyware
VirtualAllocEx	GetRawInputData
VirtualProtectEx	GetClipboardData
CreateThread	SetWindowsHookExA
OpenProcess	GetKeynameTextA
OpenProcessToken	GetKeyState
SuspendThread	GetForegroundWindow
…	…

Win32 API calls and their combinations can be used as features for malware classification.



Difference in file entropy. Left benign file and right is malware. This is an important feature regarding malware detection.

DISCUSSION AND FUTURE WORKS

- Identify various machine learning based malware detection methods.
- Empirically test what malware features are most likely to trigger certain security products.
- Based on the extracted features, propose ML-based algorithm for `Ethical Malware` obfuscation to evade detection systems.
- Cyber security exercises such as "Amber Mist" or "Locked Shields" are essential and very valuable training ground for blue teams. And results of this research can be tested and used in these trainings.

"All warfare is based on deception." – Sun Tzu "The art of war"

`Ethical Malware`