

Operating Systems and Security

Advanced Security Evasion in Windows with Hidden Commands

Authors :

Zinar MUTLU

Andranik VOSKANYAN

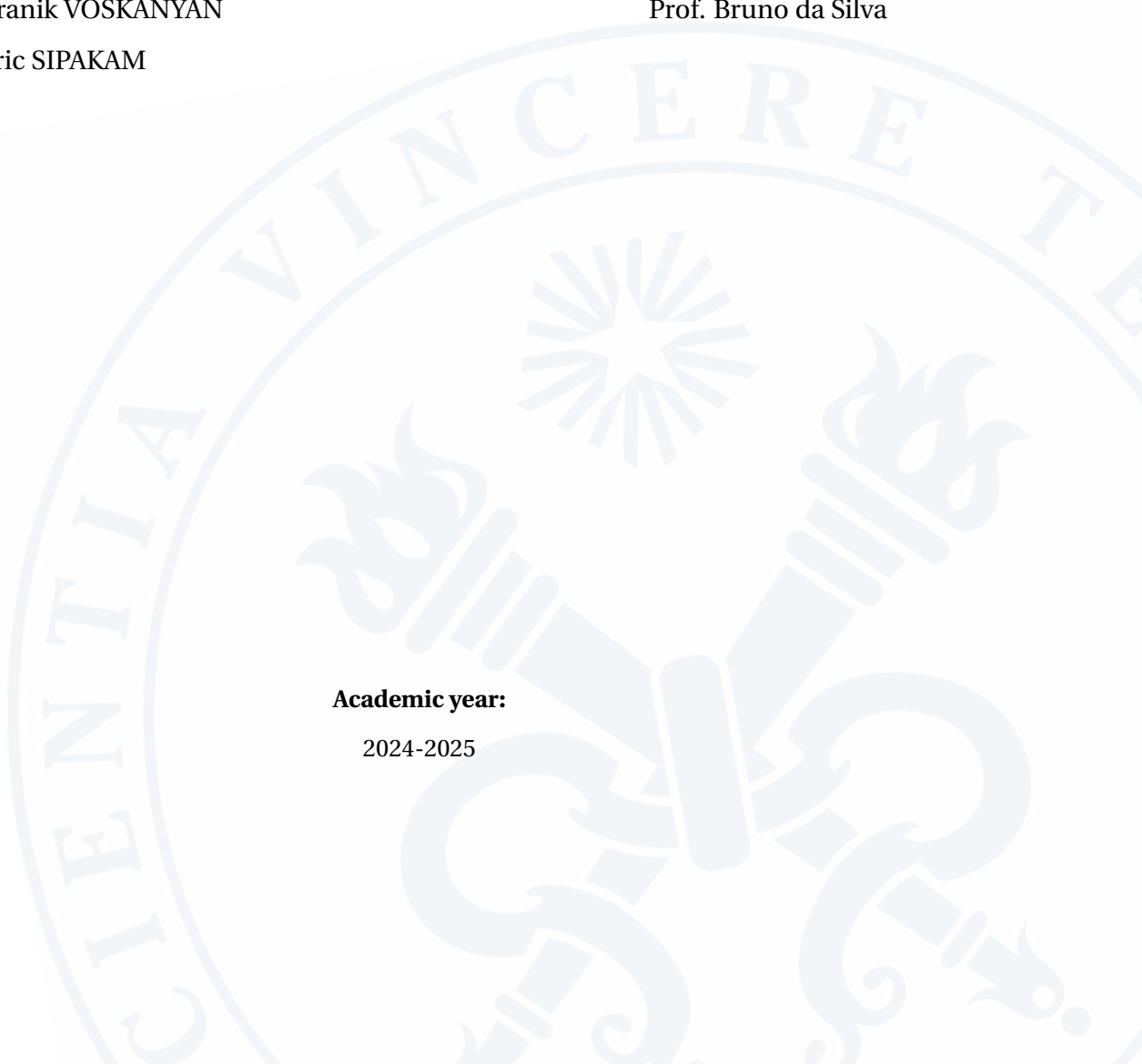
Cedric SIPAKAM

Professor :

Prof. Bruno da Silva

Academic year:

2024-2025



Contents

Introduction	1
Background	2
Description	3
Experimental Results	4
Discussion and Conclusion	5
References	6

In operating systems, particularly Windows, are equipped with built-in security solutions such as Windows Defender and advanced Endpoint Detection and Response (EDR) tools to protect against malicious activities. However, cyber attackers continuously develop techniques to evade these defenses, using stealthy methods to hide malicious processes, inject code into legitimate applications, and maintain persistence within compromised systems. This project focuses on evaluating the effectiveness of Windows Defender and third-party EDR solutions in detecting and responding to such advanced evasion techniques.

The primary goal of this project is to simulate real-world attack scenarios involving hidden command execution, keyloggers, backdoor deployment, and process injection, while analyzing how well the security tools detect and respond to these threats. By monitoring system behavior, network traffic, and event logs, the project aims to compare the detection capabilities, response times, and overall effectiveness of these security solutions.

Through this work, the project highlights key vulnerabilities in Windows security mechanisms and identifies potential areas for improvement. The outcomes of the experiments not only contribute to understanding modern evasion tactics but also help propose enhanced defensive measures to strengthen Windows systems against future attacks.

Description

Experimental Results

Discussion and Conclusion

