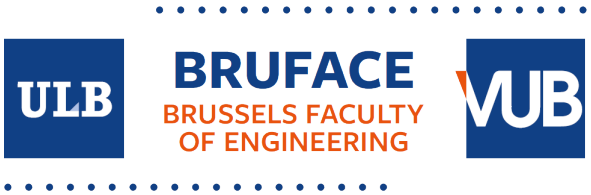

ELEC-H404

Advanced Security Evasion in Windows

Andranik Voskanyan
Cédric Sipakam
Zinar Mutu

Professor
.....

Academic Year
2024 - 2025

Faculty
Electrical Engineering

Contents

List of Figures

Abstract

This project investigates the efficacy of Windows security solutions, primarily focusing on Windows Defender, in detecting and responding to advanced stealthy attack techniques. The study evaluates a range of common attacker methodologies including the deployment of keyloggers, creation of backdoors for remote access, non-visual command execution leveraging built-in system tools, process injection for memory manipulation, and various persistence mechanisms designed to maintain unauthorized access. The evaluation involved executing these attack scenarios in a controlled environment while meticulously logging system behavior, network activity, and Windows event logs to analyze the detection capabilities and response of the security software.

1 Introduction

1.1 Problem Statement and Motivation

The Landscape of cyber threats is constantly evolving, with attackers developing increasingly sophisticated techniques to evade detection by security systems. Detecting these stealthy attacks is a significant challenge for individuals and organization alike. Understanding the methods attackers use to bypass security measures is crucial for defenders to improve their strategies, tools, and overall security posture. This project aims to shed light on these evasion techniques within the Windows operating System, a prevalent target for cyber-attacks.

1.2 Project Aims and Objectives

The Primary aims of this project are:

- To evaluate the detection capabilities of Windows Defender, [...], and [....] against a set of specific attacker techniques
- The attacker techniques investigated include:
  - Keylogger deployment
  - Backdoor creation and remote access
  - Non-visual command execution and process hiding
  - Process injection and memory manipulation
  - Persistence techniques
- To analyze system behavior, network activity, and event logs during these simulated attacks to understand how security solutions respond and what artifacts are generated
- To asses the effectiveness of various evasion methods employed by attackers

1.3 Scope of the project

This project focuses on:

- **Operating System:** Windows 11 Home
- Primary Security Silution: Windows Defender, [...], [....]

2 Background

2.1 Fundamentals of Security Evasion

2.2 Overview of Windows Security Architecture

2.3 Theoretical Overview of Attacker Techniques Investigated