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

[Finish the Abstract at the end of the report] Description: 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.

Results:[ANALYZE WHAT WE DID EXACTLY BEFORE] The experimental findings indicate varying levels of detection success by Windows Defender. While some less sophisticated or signature-based attacks, such as basic keylogger file drops or known backdoor patterns, were often identified, more advanced evasion tactics presented significant challenges. Techniques employing fileless malware, Living Off The Land Binaries and Scripts (LOLBAS) for command execution, obfuscated PowerShell commands, and certain process injection methods frequently bypassed default detection mechanisms. Analysis of logs revealed that enhanced logging, such as PowerShell Script Block Logging and Sysmon, provided crucial telemetry for manual threat hunting where automated alerts were absent. Windows Defender's resource utilization showed moderate increases during active attack simulations.[2]

Discussion and Conclusion: The results underscore that while Windows Defender offers a crucial baseline of protection, sophisticated attackers can employ various evasion techniques to circumvent its defenses. The study highlights the limitations of relying solely on default security configurations and emphasizes the importance of a defense-in-depth strategy. Effective defense against advanced threats necessitates comprehensive logging, proactive threat hunting, and the integration of advanced endpoint detection and response (EDR) capabilities. The findings conclude that continuous adaptation and understanding of evolving attacker tradecraft are paramount for maintaining robust security postures in Windows environments.

1 Introduction

2 Background

2.1 Fundamentals of Security Evasion

2.2 Overview of Windows Security Architecture

2.3 Theoretical Overview of Attacker Techniques Investigated

2.3.1 Keyloggers

2.3.2 Backdoors and Remote Access

2.3.3 Non-Visual Command Execution and Process Hiding

2.3.4 Process Injection and Memory Manipulation

2.3.5 Persistence Techniques

2.4 Relevant Frameworks and Tools

3 Description

3.1 Test Environment Setup

3.1.1 Victim Machine

3.1.2 Attacker Machine

3.1.3 Network Configuration

3.2 Security Solution Configuration

3.2.1 Windows Defender

3.3 Implementation of Attacker Techniques

3.3.1 Objective of the specific test

3.3.2 Tools and Scripts Used

3.3.3 Step-by-step Execution Procedure

3.3.4 Specific Evasion Methods Employed

3.4 Monitoring and Data Collection Strategy

3.4.1 Security Solution Logs

3.4.2 System-Level Logs

3.4.3 Network Traffic Analysis

3.4.4 Performance Logging

3.5 Evaluation Criteria

4 Experimental Results

5 Discussion and Conclusion

6 References