

Table of Contents

[Navigate through the document](#)

01 Introduction

Overview of Frankenstein APC Injection and ethical guidelines

02 Theory: What's the Frankenstein Process Injection?

Explanation of the technique's core mechanics and steps

03 Theory: How we find opened handles

Methods for enumerating and filtering system handles

04 Theory: Current Situation

Analysis of current detection and evasion landscape

05 1. Evading the use of VirtualAllocEx

Techniques for avoiding monitored memory allocation

06 2. Evading the use of WriteProcessMemory

Alternatives for remote memory writing

07 3. Don't abuse the main thread

Improving stability through proper thread selection

08 4. Unique Build Each Compilation

Ensuring binary uniqueness for better evasion

09 Exercise

Practical challenge to extend the technique

10 Conclusions

Key takeaways and next steps
