🛡️ MALWARE ANALYSIS REPORT

Comprehensive Security Assessment

⚠️ HIGH THREAT LEVEL

🚨 Executive Summary

Sample Name: DLLInjection.exe
Classification: Trojan.Dropper
Analysis Status: Complete

ℹ️ File Information

Property	Value
File Name	DLLInjection.exe
File Type	Windows Executable
Target OS	Windows
Compilation Date	Fri Mar 14 16:13:21 2025 UTC

File Hashes:
MD5: 61c16b7ee1c80b1ae5890ac61f372d2d
SHA1: 4a400b5df6b880ebfd4165c48a6e8e4b42054b3d
SHA256: 49b0f1939848c1c1f8716b83bbf0ba9bc8aba84e8d02b6942c82050d38e7f3f6
IMPHASH: 0cbaf2efd96e34f55370a925cf0aa749

🔬 Technical Analysis

🎯 Malicious Indicators

Suspicious Strings Found:
- `notepad.exe` - Target process for injection
- `C:\evil.dll` - Malicious payload location
- Debug path reveals development environment

📊 Function Categories

269	164	10
Total Functions	Imports/Exports	PE Sections

🔍 Capability Analysis

The malware demonstrates the following capabilities:

Process Manipulation (20) · Memory Management (24) · Evasion/Bypassing (20) · Information Gathering (20) · DLL/Resource Handling (13) · File Operations (5) · Registry Access (4)

⚡ Critical Functions Detected

Function	Category	Risk Level	Purpose
CreateRemoteThread	Process	HIGH	Code injection into remote process
WriteProcessMemory	Memory	HIGH	Writing malicious code to target process
VirtualAllocEx	Memory	HIGH	Allocating memory in remote process
IsDebuggerPresent	Evasion	MEDIUM	Anti-debugging detection
OpenProcess	Process	HIGH	Obtaining handle to target process

🎯 YARA Rule Matches

⚠️ CRITICAL MATCHES DETECTED

🔴 Rule: anti_dbg

Description: Anti-debugging techniques detected

Offset	Matched String
0x175ce	KERNEL32.dll
0x17abc	IsDebuggerPresent

🔴 Rule: inject_thread

Description: Thread injection capabilities detected

Offset	Matched String
0x17524	OpenProcess
0xff21	VirtualAllocEx
0xff49	WriteProcessMemory
0xff71	CreateRemoteThread

⚙️ PE Section Analysis

Section	Virtual Size	Virtual Address	Raw Data Size	Entropy	Analysis

🛡️ Security Recommendations

🚨 Immediate Actions

- **Quarantine:** Immediately isolate any systems where this file was detected
- **Block Hashes:** Add file hashes to security tools and firewalls
- **Network Monitoring:** Monitor for suspicious outbound connections
- **Process Monitoring:** Watch for notepad.exe process anomalies

🔍 Detection Signatures

IOCs (Indicators of Compromise):
- File: DLLInjection.exe
- Suspicious file: C:\evil.dll
- Process injection into notepad.exe
- Anti-debugging behavior
- Memory allocation in remote processes

🛠️ Mitigation Strategies

- Deploy endpoint detection and response (EDR) solutions
- Implement application whitelisting
- Monitor process creation and injection attempts
- Regular security awareness training
- Keep systems and security tools updated

Note: This analysis was performed in a controlled environment. The malware poses significant risks to production systems and should be handled only by trained security professionals.

Report Generated: 5/23/2025, 8:08:06 PM
Analysis Tool: Qu1cksc0pe Security Scanner
Analyst: Blue Team Security Operations