Malware Detection Report

File: ExecuteShellcodeWD.exe

Overview

This report provides a detailed assessment of the executable file **ExecuteShellcodeWD.exe**, submitted on **June 13, 2025**. The file exhibits multiple indicators consistent with malicious behavior, including detection by YARA rules and PE structure anomalies.

File Metadata

MD5	80cde44d8c0aa53cd8f5edf4d26b363a
SHA-256	4b4331dd18caa432a0f755422f32d663af3f8bf5f33a40ef2303783c304451c2
File Type	PE32+ (64-bit executable for Windows)
File Size	63.49 KB
Compilation Date	2025-06-13 18:27:06

Threat Classification

Initial threat label: **Trojan:Win32/Meterpreter.O**.
YARA Rules matched: **Windows.Trojan.Metasploit** with high severity.
Signature matched against shellcode patterns used in known post-exploitation frameworks.

Suspicious Characteristics

- Invalid PE checksum – frequently associated with packed or obfuscated malware.
- Suspicious API: `GetProcAddress` – commonly used in dynamic API resolution to bypass static analysis.
- Non-standard PE sections (e.g., .textbss, .msvcjmc, .00cfg) – may evade signature-based detection.

Dynamic Behavior (RedEDR)

The executable launched `calc.exe` as a child process, indicating shellcode execution leading to a separate process launch. While advanced EDR scanning tools like PE-Sieve, Moneta, and Patriot failed to initialize or returned no findings, behavioral evidence supports exploitation activities.

Static Analysis

- Entropy: 3.61 (Low – suggesting unencrypted or unpacked code)
- YARA scan hits with shellcode patterns.
- ThreatCheck located malicious code chunks through binary dissection at increasing offsets.

Conclusion

> **Conclusion:** The file `ExecuteShellcodeWD.exe` is likely a loader for post-exploitation frameworks (e.g., Meterpreter) and should be classified as **malicious**. It demonstrates advanced static and dynamic evasion mechanisms. Immediate containment and forensic review are advised.

Analyst: Automated report via internal sandbox
Date: June 13, 2025