Malware Analysis Report

Comprehensive Security Assessment

⚠️ MEDIUM RISK DETECTED

File Information

FILENAME

APCProcessInjection.exe

FILE SIZE

65,024 bytes (63.5 KB)

MD5 HASH

aa931669b33e83d6eb8aaddc601474c2

SHA256 HASH

43af4ca8d3a32e25792dbe7fd74d21dd491133d4e9aeb64b108a19acac18b24d

FILE TYPE

PE32+ executable (AMD64)

COMPILE TIME

2025-05-27 18:43:54 UTC

ENTROPY LEVEL

3.61 (Low Detection Risk)

36.1%

Security Analysis Results

2

SUSPICIOUS APIS

3

NON-STANDARD SECTIONS

0

MALWARE SIGNATURES

0

RUNTIME THREATS

Suspicious Indicators Detected

Invalid PE Checksum: Common in modified/packed files (~83% correlation with malware)

Process Memory Manipulation: WriteProcessMemory API detected - potential code injection capability

Dynamic API Resolution: GetProcAddress function found - possible evasion technique

Non-standard PE Sections: Unusual section names (.textbss, .msvcjmc, .00cfg) may trigger static analysis

✓ Clean Analysis Results

✓ No YARA Signature Matches

✓ Windows Defender Clean

✓ ThreatCheck Clean

✓ No Runtime Malicious Behavior

✓ No Memory Injection Detected

PE Structure Analysis

ENTRY POINT

`0x11285`

SUBSYSTEM

`WINDOWS_CUI (Console Application)`

MACHINE TYPE

AMD64 (x64)

TOTAL SECTIONS

10 sections

📋 PE Sections Breakdown

.text

Size: 33,792 bytes
Entropy: 3.6
Status: ✅ Standard

.rdata

Size: 11,776 bytes
Entropy: 2.26
Status: ✅ Standard

.data

Size: 1,024 bytes
Entropy: 2.71
Status: ✅ Standard

.textbss

Size: 0 bytes
Entropy: 0
Status: ⚠️ Non-standard

.msvcjmc

Size: 1,024 bytes
Entropy: 0.8
Status: ⚠️ Non-standard

.00cfg

Size: 512 bytes
Entropy: 0.46
Status: ⚠️ Non-standard

📚 Import Analysis

Standard DLL Imports

ucrtbased.dll VCRUNTIME140D.dll MSVCP140D.dll KERNEL32.dll

⚠ Suspicious API Functions

WriteProcessMemory

DLL: kernel32.dll
Risk: Process memory manipulation detected
Usage: Potential code injection capability

GetProcAddress

DLL: kernel32.dll
Risk: Dynamic API resolution
Usage: Possible evasion technique

⚡ Runtime Behavior Analysis

✓ No Malicious Runtime Behavior Detected

✅ **HSB Scanner:** No behavioral detections (0 findings)

✅ **Moneta Memory Scanner:** No memory anomalies detected

✅ **RedEdr Process Monitor:** No suspicious process activity

✅ **PE-Sieve:** No code injection or modification detected

📊 Risk Assessment & Recommendations

🎯 OVERALL RISK LEVEL: MEDIUM

This file exhibits characteristics commonly associated with process injection tools but shows no active malicious behavior.

⚠️ Risk Factors

- Process injection capabilities
- Invalid PE checksum
- Non-standard PE sections
- API evasion techniques

✅ Positive Indicators

- No malware signatures
- Clean runtime behavior
- No memory injection detected
- Low entropy (3.61)

🔍 Security Recommendations

- **Sandboxed Testing:** Execute only in isolated environments for security research
- **Network Monitoring:** Monitor for unusual network connections if deployed
- **Process Monitoring:** Watch for suspicious child processes or injection attempts
- **Regular Scanning:** Perform periodic scans with updated antivirus definitions
- **Access Control:** Restrict execution to authorized security personnel only

Analysis Report Generated: *May 27, 2025 at 18:47:23 UTC*
Scan Duration: *~22 seconds (Static: 2.0s, Dynamic: 19.8s)*
This automated analysis provides technical indicators and should be reviewed by security professionals for final assessment.