External Technical Root Cause Analysis   Malware Sample Execution

File: ddfc9420dd7d61ff16c24433bb7bc678301f8fae7842fd1298e3851fd04a912e.exe

Date: July 8, 2025

INTRODUCTION

This report details the behavioral analysis of a malware sample executed in an air gapped virtual environment. Procmon and Sysmon were used to capture the operational telemetry across 4,194 system events. This analysis outlines the observed behaviors, key indicators and technical root cause of actions from the malicious binary.

WHAT HAPPENED

At 7:21 PM on July 8, 2025, the malware sample was executed by the user: (Malwaretest) on a Windows 11 VM.

The Binary:
ddfc9420dd7d61ff16c24433bb7bc678301f8fae7842fd1298e3851fd04a912e.exe
spawned with a PID: 4980 and initiated system level operation consistent with execution registry, probing, image loading, and environmental discovery.

Noted red flags:

- Registry probing under HKLM\System\CurrentControlSet\Control\AppID
- Access to .NET framework assemblies
- Repeated read and write operations using CreateFile and ReadFile
- Minimal thread spawning and no observed network operations

FINDINGS AND MITIGATIONS

1. Excessive Registry Access in AppLocker Context

Findings:

The malware made over 1,400 registry operations, Primarily targeting:

- HKLM\System\CurrentControlSet\Control\AppID\Configuration\SMARTLOCKER (396 reads)
- HKLM base key (202 reads)

This suggests a reconnaissance or evasion check against AppLocker configs.

Mitigations:

Enforce AppLocker audit and deny rules with alerts for programmatic access to SMARTLOCKER keys.

2. Reflection of .NET Assembly Loading

Findings:

The Binary loaded several native images of .NET framework DLLs including:

- Mscorlib.ni.dll (176 times)
- System.ni.dll (173 times)
- Clr.dll (94 times)

This may imply execution through .NET runtime wrapper or obfuscation technique.

Mitigations:

Apply Defender ASR rules and log all managed runtime execution with Command Line and parent-child tracking.

3. Thread and Process Control

Findings:

- Only 1 process start and 14 thread creation events observed.
- Limited threading activity implies possible payload staging or sandbox detection.

Mitigation:
Increase Sysmon granularity on thread injection, shellcode triggers, and map thread call stacks to detect unusual loading.

4. Prefetch and AppCompat Directory Access

Findings:

Access attempts to:

- \Windows\Prefetch\
- AppCompat\programs\recentFileCache.bcf

These are indicative of ant analysis checks or execution tracking circumvention.

Mitigation:

Implement prefetch file integrity monitoring and block unauthorized access to AppCompat files from controlled folder access.

OPERATIONAL BREAKDOWN

Event type	**Count**
Registry Reads	**782**
Registry Value Queries	**766**
File Reads	**669**
DLL Loads	**61**
Thread Creation	**14**
Process Start/Exit	**1**

The malware operated using standard Win32 APIs and did not exhibit code injection or network behavior during runtime. It likely functions as a loader or sandbox-aware stub that delays or hides true payload activity.