DLL Forensic Analysis Report

Generated: 2025-10-20 08:16:14
Memory Image:
C:\Users\Win-11\PycharmProjects\dll\memory.dumps\TAMMAM-20251019-171329.dmp

Analysis Summary

Metric	Value
Total DLLs Analyzed	11319
Unique DLLs	1194
Total Processes	198
Suspicious Findings	3156
Critical Findings	704
High Severity Findings	16
Medium Severity Findings	2436

Suspicious Findings

PID	Process	DLL	Severity	Reason
4884	MpDefenderCore	Windows	HIGH	Suspicious path: \\ProgramData\\
4884	MpDefenderCore	Windows	HIGH	Suspicious path: \\ProgramData\\
4224	MsMpEng.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
4224	MsMpEng.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
4224	MsMpEng.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
4224	MsMpEng.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
4224	MsMpEng.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
4224	MsMpEng.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
4224	MsMpEng.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
5136	svchost.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
7556	RtkAudUService	Windows	HIGH	Suspicious path: \\ProgramData\\
13224	WavesSvc64.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
18036	svchost.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
7188	svchost.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
7744	NisSrv.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
7744	NisSrv.exe	Windows	HIGH	Suspicious path: \\ProgramData\\
620	winlogon.exe	-	CRITICAL	Non-system DLL in critical process
620	winlogon.exe	-	CRITICAL	Non-system DLL in critical process
620	winlogon.exe	-	CRITICAL	Non-system DLL in critical process
620	winlogon.exe	-	CRITICAL	Non-system DLL in critical process