Analysis Types

Analysis Types

STATIC ANALYSIS

all analysis methods that do not execute the sample

- infection risk very low

DYNAMIC ANALYSIS

all analysis methods that execute the sample

- must be done in safe environment e.g. Virtual Machine

META INSPECTION

analysis methods that only look at meta data or overview information

- also called "basic analysis" but this term is misleading

CODE INSPECTION

all analysis methods that involve reading or modifying the sample's code

- also called "advanced analysis" but this term is misleading

Analysis Types

Meta inspection	File format viewers Strings Hex Editor	Behavior Monitoring Automatic Sandbox Reports
Code inspection	Disassembly Decompilation	Debugging

But when to use which analysis type?

Typical use cases for each analysis type

Meta inspection	Triage	Triage: automatic reports Main analysis: extract, unpack, monitor behavior
Code inspection	Main analysis: reading and understanding the code, static deobfuscation	Main analysis: unpacking, deobfuscation, use as aid to understand functions that are unclear from static inspection