Threat Description: The YARA rule PE_File_Detection detects Portable Executable files based on the presence of the "MZ" magic bytes at the file's start. This is a fundamental rule for recognizing Windows executable binaries.

Indicators of Compromise (IoCs):

"MZ" signature at file offset 0

Detection Mechanism:

Matches Windows PE file headers in both malicious and legitimate binaries.

Possible Attribution & Use Cases:

Used in basic file classification and malware analysis pipelines.