Threat Name: ZIP_File_Detection

Threat Category: Archive File Identification

Threat Description: The YARA rule ZIP_File detects ZIP archive files based on their file signature (magic number).

Indicators of Compromise (IoCs):

File header: { 50 4B 03 04 } (ZIP signature)

Detection Mechanism:

Matches ZIP file headers at the start of a file.

Possible Attribution & Use Cases:

Used in identifying compressed files that could contain malware.

Recommended Actions:

Inspect archive contents for suspicious files.