Analysis Report for: c3.txt

Overall Functionality

The provided text is not C code; it's the output from `olevba`, a tool used to analyze VBA (Visual Basic for Applications) macros within OLE (Object Linking and Embedding) files, specifically an executable file. The analysis reveals two VBA macros: `Arkusz13.cls` (empty) and `xlm_macro.txt`. The `xlm_macro.txt` macro contains suspicious hex-encoded and Base64-encoded strings, suggesting potential obfuscation of malicious code. There's no actual C code to analyze.

Function Summaries

There are no functions in the provided text. The output describes the contents of VBA macros, not C functions.

Control Flow

There is no control flow to analyze because the provided text doesn't show the implementation of any functions. The `olevba` output only indicates the presence of suspicious strings within the `xlm_macro.txt` macro, not the execution logic.

Data Structures

No specific data structures are described in the output. The analysis only points towards the existence of encoded strings within the VBA macro. These strings might represent data structures within the actual (unseen) VBA code, but their nature is unknown without decoding.

Malware Family Suggestion

Based on the `olevba` output, the file exhibits characteristics consistent with a **macro virus** or a file containing malicious VBA code. The presence of obfuscated strings (hex and Base64 encoded) is a strong indicator of an attempt to hide malicious commands. Without decoding the strings, it's impossible to definitively identify the specific malware family, but the obfuscation technique is a common tactic used by various malware authors. The association with an Excel file (.xls or similar) also points toward a macro virus targeting Microsoft Office applications. Further analysis using tools that can decode the strings and analyze the VBA code itself would be needed to confirm this and determine the exact nature of the malware.