Analysis Report for: F0D3E5890A887B93271462ACC0949913.exe

Overall Functionality

The provided code snippet is not a complete C program; it's a single line containing a PowerShell command encoded using Base64. The code does not perform any C-related actions. Instead, it aims to execute a malicious PowerShell script on the system. The Base64-encoded string needs to be decoded to understand the true nature of the malicious script.

Function Summaries

There are no functions defined in the provided C code. The entire code is a single statement that attempts to execute an external program (PowerShell).

Control Flow

There's no control flow within the C code itself. The control flow resides entirely within the yet-to-be-decoded PowerShell script. The C code simply provides a mechanism to execute this external script.

Data Structures

There are no data structures used within the C code itself. Data structures might exist within the decoded PowerShell script, but those are not visible in the provided Base64 encoded string.

Malware Family Suggestion

Decoding the Base64 string reveals a PowerShell command that uses `-exec bypass` and `-enc`, indicating a likely attempt to execute malicious code surreptitiously. The presence of these parameters strongly suggests that this code is part of a **downloader/dropper** or an **implant** malware family. It's unlikely to be a standalone malware; its purpose seems to be downloading and executing further malicious payloads. The specific malware family can't be definitively determined without decoding the Base64 payload and analyzing the resulting PowerShell script, which would require further reverse engineering. However, based on this initial examination, this snippet exhibits traits commonly seen in several malware families that rely on PowerShell for execution, such as:

* **PowerShell-based malware:** The direct use of PowerShell points towards this category.
* **Downloaders/Droppers:** The encoded script likely contains the actual malicious code downloaded from a remote location or embedded in the base64 encoded string.

The highly obfuscated nature of the code (Base64 encoding) is also consistent with the techniques employed by malware authors to hinder analysis and detection. Without decoding and analyzing the payload, a definitive classification is impossible. It’s crucial to note that attempting to decode and execute this code can be extremely risky. You should only perform this in a carefully controlled and isolated environment (virtual machine with no network connectivity) using dedicated security analysis tools.