Analysis Report for: 022C531033E7D1768BBC319A782B82E9.exe

Overall Functionality

This code is a batch script (indicated by the `@echo off` and the use of `for`, `if`, `ren`, `del`, and `powershell` commands) designed to update a shortcut on the desktop and rename associated executable files. It appears to be related to updating a software application, specifically one named "S O S Assistec". The script deletes old shortcut links, renames the application executable and its configuration file, creates a new desktop shortcut pointing to the renamed executable, and refreshes the desktop to show the changes. The self-deletion at the end (`del %0`) is typical of malicious scripts to remove traces of their execution.

Function Summaries (Note: This code does not contain functions in the traditional C sense; it's a batch script.)

The code consists of a sequence of commands, not functions. Each command performs a specific action.

Control Flow

1. **Delay:** `timeout /t 2 /nobreak > NUL` pauses execution for 2 seconds. This is likely to avoid detection or to allow for other processes to finish.

2. **Shortcut Deletion:** `for %%A in (...) do if exist %%A del %%A` iterates through a list of three shortcut files (.lnk) on the desktop. If any of these files exist, it deletes them.

3. **File Renaming:** Two `ren` commands rename the executable file and its configuration file. The new names include timestamps, suggesting an update process. The old names are very similar, implying a version upgrade.

4. **Shortcut Creation:** A PowerShell command creates a new shortcut on the desktop (`C:\\Users\\Samsung\\Desktop\\S O S Assistec.lnk`). This shortcut points to the newly renamed executable. It also sets the window style, description, and icon.

5. **Desktop Refresh:** Another PowerShell command refreshes the desktop to make the new shortcut immediately visible.

6. **Self-Deletion:** `del %0` deletes the script itself.

The control flow is primarily sequential, with conditional execution only in the shortcut deletion step.

Data Structures

There are no complex data structures used. The script primarily manipulates file paths as strings.

Malware Family Suggestion

While this script doesn't contain any directly malicious code like network connections or data exfiltration, its behavior strongly suggests it might be part of a larger malicious campaign or used by malware for self-propagation and persistence. The self-deletion, the renaming of files to obfuscate their nature, and the update of an application all align with common malware techniques. Without further analysis of the `Abre o sistema20250728180047_75b910e7-b5ff-4bff-81d3-1434d53ead80.VB.exe` file, a definitive malware classification is impossible, but it is highly suspicious and warrants further investigation. The behavior aligns with a **self-updating malware or dropper** that could potentially download or install further harmful components.

Security Concerns

* **Self-Deletion:** Makes forensic analysis significantly harder.
* **File Renaming:** Attempts to hide the original executable and its config files, potentially to avoid detection by security software.
* **Unclear Origin:** The source and purpose of the `Abre o sistema` application are unknown and need scrutiny.
* **Potential for Further Actions:** The updated executable could contain malware.

In summary, this script, while seemingly performing a simple application update, exhibits characteristics consistent with malware behavior. It's crucial to investigate the targeted executable file to determine its true nature. Simply observing the script raises serious security concerns.