Analysis Report for: E9E879F782F0CD2D93902F725EABB881.exe.vbs

Overall Functionality

This code snippet is not C code; it's a batch script (indicated by `@echo off`). It sets a series of environment variables. These variables define paths, system information (OS, processor details, user name), and seemingly some application-specific settings (like JAVA_HOME, OneDrive locations, SQL Server paths, and a cryptic variable `IGCCSVC_DB` which looks like Base64 encoded data). The script prepares the environment for another process or application to run, potentially a C program or other executable. The values assigned are suggestive of a Windows system, potentially a server given the number of processors and presence of SQL Server paths.

Function Summaries

There are no functions in this batch script. It's a sequence of `set` commands, each assigning a value to an environment variable.

Control Flow

The control flow is simple and linear. The script executes each `set` command sequentially, from top to bottom. There are no loops or conditional statements (like `if` or `for`).

Data Structures

There are no explicit data structures in this batch script. The only data involved are simple strings used as environment variable names and values.

Malware Family Suggestion

While this script itself is not malicious, it's highly suspicious and strongly suggestive of potential malicious activity or the precursor to it. The reasons are:

* **Cryptic Variable:** The `IGCCSVC_DB` variable containing Base64 encoded data is a red flag. This is a common technique used to obfuscate sensitive information or commands, which could be used to download and execute malware, or to store configuration information for malicious operations. Further analysis of this decoded data is necessary to determine if it is malicious.

* **Extensive Environment Variable Modification:** The sheer number of environment variables modified is unusual. Malicious code often manipulates environment variables to hide its presence, inject malicious code paths, and change system behavior.

* **System-Level Information:** The collection of system information (processor details, OS version, user name) is typical of reconnaissance performed by malware before deployment of further malicious actions.

* **Batch Script as a Launcher:** Batch scripts are frequently used as a simple and portable method to launch more complex malware.

Conclusion

This batch script is not malware in and of itself, but it displays characteristics strongly suggestive of actions often used as a preliminary step in malware deployment or execution. The Base64 encoded data in `IGCCSVC_DB` is critical for further analysis to determine the true nature and intent of this script. Decoding that variable is essential before drawing any definitive conclusion. It is strongly advised to treat the script and related files with extreme caution and to run a full malware scan on the system. The likely malware family depends on the content of the decoded `IGCCSVC_DB` value; it could be many different kinds (e.g., backdoors, ransomware, or information stealers), or possibly benign if the decoded data reveals a legitimate application configuration.