Analysis Report for: 460B27B546A1279E551EC80A104DD23E.exe

Overall Functionality

This code is a batch script (`.bat` file disguised as a `.c` file) designed to activate Microsoft Office 2016 Professional Plus and Standard editions. It attempts to do this by installing product keys from files located in a `Licenses16` directory, then tries to activate the software using a KMS (Key Management Service) server hosted by `MSGuides.com`. The script is highly suspicious and likely malware.

Function Summaries

The code doesn't contain C functions in the traditional sense. It's a batch script that uses commands built into the Windows command interpreter (cmd.exe). The "functions" are essentially commands and command blocks. Let's break down some key "functions":

* **`cd /d "%ProgramFiles%\..."`:** Changes the current directory to the location of the `ospp.vbs` file, which is used for Office product key management. It tries both Program Files and Program Files (x86) locations.
* **`for /f %%x in ('dir /b ...') do ...`:** This loops through all files matching specific patterns (`proplusvl_kms*.xrm-ms` and `proplusvl_mak*.xrm-ms`) in the `Licenses16` directory. For each file, it uses `cscript ospp.vbs /inslic:"..."` to install the product key from that file.
* **`cscript ospp.vbs /unpkey:...`:** Removes existing product keys from Office. This is done for several keys.
* **`cscript ospp.vbs /inpkey:...`:** Installs a specific product key.
* **`cscript ospp.vbs /sethst:...`:** Sets the KMS server hostname.
* **`cscript ospp.vbs /act`:** Activates Office using the KMS server.
* **`find /i "successful"`:** Checks the output of the activation command for the word "successful".

Control Flow

The script follows a fairly straightforward control flow:

1. **Initialization:** Sets up the environment, finding the `ospp.vbs` script and installing product keys.
2. **KMS Server Selection:** Attempts activation using three different KMS servers (`kms7.MSGuides.com`, `kms8.MSGuides.com`, `kms9.MSGuides.com`) sequentially.
3. **Activation Attempt:** Calls `cscript ospp.vbs /act` to activate Office.
4. **Success/Failure Handling:** If activation is successful (indicated by "successful" in the output), the script displays a success message and prompts the user to visit the author's website. If it fails, it tries the next KMS server or displays an error message.
5. **Unsupported Version:** If none of the KMS servers work after the third attempt it states that the Office version is not supported and provides a link.

Data Structures

The script uses minimal data structures. It primarily relies on variables (like `%i%` and `%KMS_Sev%`) to store the current KMS server index and the hostname. File paths are also managed as string variables.

Malware Family Suggestion

Given its functionality, this code strongly suggests a **Keygen/Crack** type of malware. It attempts to illegally activate Microsoft Office by using potentially stolen keys and connecting to unofficial KMS servers. The inclusion of the author's website and donation links further hints at malicious intent, likely to track users and/or monetize the illegal activation process. The script's obfuscation, attempting to hide its true nature by presenting itself as a `.c` file, is another red flag. It is likely part of a wider malware operation potentially including keyloggers or other exploits. Running this script is highly discouraged as it poses security risks to your system and violates Microsoft's End User License Agreement.