Analysis Report for: au3.txt

Overall Functionality

This AutoIt script acts as a malicious installer. It reads configuration settings from a `setup.ini` file, then performs several actions based on those settings. These actions include:

1. **Modifying Internet Explorer settings:** It forcefully sets the homepage and start page in various registry locations, including locations protected by Group Policy, to a URL fetched from `setup.ini`. It uses `gpupdate /force` to apply the changes immediately. This is a classic symptom of browser hijacking.

2. **Creating Desktop shortcuts:** It creates a shortcut on the desktop linking to an executable downloaded from a URL specified in `setup.ini`.

3. **Downloading and executing files:** It downloads executables from URLs specified in `setup.ini` and executes them. This is a clear indicator of potential malware installation.

4. **Self-deletion and process termination:** After completing its malicious activities, the script deletes its own files (`setup.ini`, `data.bin`) and attempts to terminate itself using a convoluted command involving `taskkill`. This is a common technique to hinder analysis and cleanup.

Function Summaries

* **_SETUP($dl, $exe):** This function downloads a file from a URL ($dl) and saves it as $exe in the temporary directory. Then it executes the downloaded file.
* **Parameters:** $dl (URL string), $exe (filename string).
* **Return Value:** None.

* **Main Script:** The main part of the script reads configurations from `setup.ini`, and based on these settings, calls functions to modify the system, download and run files.

Control Flow

The main script's control flow is primarily driven by conditional statements (`If IniRead(...) = 0x1 Then`). Each `If` block checks a flag from `setup.ini` (check1, check2, check4, check5). If the flag is set to 1 (0x1), the corresponding action is performed:

1. **`If IniRead($ini, "Plugin", "check1", "0") = 0x1 Then`:** This block forcefully changes the Internet Explorer homepage and start page and performs system updates to apply changes.

2. **`If IniRead($ini, "Plugin", "check2", "0") = 0x1 Then`:** This block creates a desktop shortcut to an executable.

3. **`If IniRead($ini, "Plugin", "check4", "0") = 0x1 Then` and `If IniRead($ini, "Plugin", "check5", "0") = 0x1 Then`:** These blocks download and execute files from specified URLs using the `_SETUP` function.

The `_SETUP` function's control flow is simple: it downloads a file using `InetGet`, waits for the download to complete, and then executes the downloaded file. The loop `Do ... Until InetGetInfo($hdownload, 0x2)` ensures that the download is finished before proceeding.

Data Structures

The primary data structure is the configuration file `setup.ini`, which uses an INI format. It stores key-value pairs to control the script's behavior. The script also uses strings, integers, and file handles.

Malware Family Suggestion

Based on its functionality, this script strongly resembles a **downloader/installer** often used as part of a broader malware infection chain. It's not a specific, well-known malware family, but its actions clearly indicate malicious intent. The features of browser hijacking, arbitrary file download and execution, self-deletion, and administrative privilege requirement (indicated by `#RequireAdmin`) are common characteristics of malware installers that install other components after initial deployment. It could potentially be part of a larger malware campaign, dropping additional malware payloads from the URLs in the `setup.ini` file.