Analysis Report for: a.txt

Overall Functionality

This AutoIt script acts as a malicious installer. It reads configuration from `setup.ini`, performs several actions based on flags in that file, and then self-destructs. These actions include:

1. **Modifying Internet Explorer settings:** It forcefully sets the homepage and start page to a URL specified in `setup.ini`, overriding any Group Policy settings that might prevent this. This is a strong indication of malicious intent.

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 additional executables from URLs specified in `setup.ini` and runs them. This is a classic dropper behavior.

4. **Self-deletion:** The script deletes its own files (`setup.ini` and `data.bin`), along with the attempt to kill its own process after running some additional command.

Function Summaries

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

Control Flow

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

1. **`If IniRead($ini, "Plugin", "check1", "0") = 0x1 Then ... EndIf`:** This section aggressively modifies Internet Explorer settings, demonstrating a clear attempt to hijack the user's browser. The use of both `HKCU` and `HKCU64` keys suggests it attempts compatibility across 32-bit and 64-bit systems. The `gpupdate /force` command ensures the changes are applied immediately, even overriding Group Policy settings.

2. **`If IniRead($ini, "Plugin", "check2", "0") = 0x1 Then ... EndIf`:** This section creates a desktop shortcut pointing to an executable downloaded from a URL specified in `setup.ini`. This is a common technique for persistence and user interaction.

3. **`If IniRead($ini, "Plugin", "check4", "0") = 0x1 Then ... EndIf` and `If IniRead($ini, "Plugin", "check5", "0") = 0x1 Then ... EndIf`:** These sections call the `_SETUP` function to download and execute additional files, likely payloads for the malware.

The `_SETUP` function itself has a simple control flow: it downloads a file using `InetGet`, waits for the download to complete, and then executes the downloaded file.

Data Structures

The primary data structure is the `setup.ini` configuration file. It's a simple INI file containing key-value pairs that determine the actions performed by the script. These pairs control URLs to download from and filenames of executables.

Malware Family Suggestion

Based on its functionality, this code strongly suggests a **downloader/dropper** type of malware. The script downloads and executes other files, which could be any kind of malware (ransomware, keylogger, etc.). The forceful modification of browser settings is characteristic of browser hijackers. The self-deleting nature and use of `RequireAdmin` further enhance its malicious capabilities. Its specific payload is unknown without analyzing the downloaded files but its behavior is very consistent with a malware installer, designed to install additional malware components or a malicious payload onto a system.