Analysis Report for: au3.txt

Overall Functionality

This AutoIt script acts as a malicious installer. It reads configuration from a `setup.ini` file, which specifies URLs and filenames for various components. Based on flags in the INI file, it performs the following actions:

1. **Modifies Internet Explorer settings:** It forcefully sets the homepage and start page to a URL fetched from the `setup.ini` file, overriding Group Policy settings. This is a strong indication of malicious intent.
2. **Creates a desktop shortcut:** It creates a shortcut to an executable downloaded from a URL specified in `setup.ini`, placing it on the user's desktop.
3. **Downloads and executes files:** It downloads and runs executables from URLs provided in `setup.ini`. These downloaded executables are likely the payload of the malware.
4. **Self-deletion:** It deletes the script itself and associated files (`setup.ini` and `data.bin`) after execution. This is a common technique to hinder analysis and removal.
5. **Process Termination:** It attempts to forcefully terminate its own process.

Function Summaries

* **`_SETUP($dl, $exe)`:** This function downloads a file from a URL ($dl) and saves it to the temporary directory as $exe. It then executes the downloaded file.
* **Parameters:** `$dl` (string: URL of the file to download), `$exe` (string: filename for the downloaded file).
* **Return Value:** None.

Control Flow

The main part of the script consists of a series of `If` statements that check flags ("check1", "check2", "check4", "check5") read from the `setup.ini` file. Each flag controls whether a specific action is performed.

1. **`If IniRead($ini, "Plugin", "check1", "0") = 0x1 Then`**: This block executes if `check1` is set to 1. It aggressively alters the IE homepage settings and uses `gpupdate /force` to apply the changes immediately, overcoming potential Group Policy restrictions. This is a clear sign of malicious activity designed to prevent the user from easily changing the homepage. The use of both HKCU and HKCU64 registry keys indicates an attempt to achieve this on both 32-bit and 64-bit systems.

2. **`If IniRead($ini, "Plugin", "check2", "0") = 0x1 Then`**: This block creates a desktop shortcut to an executable downloaded from a URL and location specified in `setup.ini`.

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

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 used is the `setup.ini` file, which acts as a configuration file. It uses a simple INI format (sections, keys, values) to store URLs and filenames for the various components the script downloads and installs.

Malware Family Suggestion

Based on its functionality, this script is strongly indicative of a **downloader/installer** type of malware. It downloads and executes arbitrary files from remote locations, modifies system settings without user consent (especially critical homepage modification), and has self-deletion capabilities. It acts as a dropper, deploying additional malicious payloads. The aggressive registry manipulation suggests a drive for persistence. The lack of any apparent beneficial functionality seals its classification as malicious software. The specific family would require further analysis of the downloaded payloads. But its overall behavior fits the profile of a downloader that acts as a first stage in a more complex malware installation process.