Analysis Report for: FCE5DBFE992EDC2198D76956E9BD93D951865B78

Overall Functionality

This C code is heavily obfuscated using a combination of techniques including variable renaming (using seemingly random hexadecimal numbers), string encoding, and function packing. After deobfuscation, it reveals itself to be a large JavaScript library designed for a web application, likely an e-commerce platform, incorporating various functionalities such as:

* **AJAX interactions:** Extensive use of jQuery's AJAX methods for server communication.
* **DOM manipulation:** Heavy usage of jQuery for dynamic modification of the HTML Document Object Model.
* **Animations:** Implements animations using jQuery's `animate` function.
* **Event handling:** Handles numerous events using jQuery's `on` and `off` methods.
* **Cookie management:** Includes functions for setting, getting, and removing cookies.
* **Form serialization:** Serializes forms into a query string format.
* **Custom UI elements:** It appears to manage custom UI components, possibly dialog boxes.
* **Countdown timer:** Includes a countdown timer functionality.

The code demonstrates a sophisticated understanding of JavaScript programming. However, the obfuscation makes reverse engineering and precise function determination challenging without automated deobfuscation tools.

Function Summaries

Due to the obfuscation, providing precise summaries for every function is extremely difficult. Many function names are replaced with hexadecimal numbers. However, we can categorize and describe some of the major functions based on their deobfuscated (or inferred) functionality:

* **`_0x375b` (Deobfuscated to a function that returns an array of strings):** This function acts as a lookup table for the obfuscated code.
* **`_0x2993` (Deobfuscated to a function that acts as a custom encoding/decoding function):** This function is crucial for decoding obfuscated strings and hexadecimal variable names within the code.
* **`_0x41ea3f` (Deobfuscated to the main jQuery object):** This represents the core jQuery library, providing the foundation for most of the application's functionality.
* **`_0x41ea3f.fn.init` (jQuery initializer):** The standard jQuery constructor.
* **`_0x41ea3f.fn.extend` (jQuery extensions):** Functions added to jQuery's prototype. This includes various functionalities like AJAX, DOM manipulation, event handling and more.
* **`_0x3dcc21` (Deobfuscated to jQuery Animation Function):** This likely handles animation logic.
* **`_0xc678b1` (Deobfuscation infers an animation function):** This appears to manage animations and their queues.
* **`_0x1ac0d2` (Deobfuscation infers a jQuery selector engine):** A custom implementation or extension of jQuery's selector engine, possibly with custom selectors.
* **`_0x38dfe3.fn.countdown` (Countdown timer):** Manages the countdown timer's initialization, updates and other aspects.
* **`_0x38dfe3.countdown` (Countdown timer object):** Contains countdown timer's settings and methods.
* **`ajax_form`, `ajax_form_catename`, `collect_goods`, `collect_store`, `DoSearch.price`, `DoSearch.keyword`, `DoSearch.region`:** Functions dealing with various form submissions and AJAX calls that appear to manage interactions with an e-commerce back-end.
* **`drop_confirm`, `go`, `goUrl`, `change_captcha`, `price_format`, `number_format`, `getFullPath`, `sendmail`, `imTalk`, `show_district`, `fLen`, `TrunTo`, `get_current_page_url`, `replaceParam`, `Base64`, `loadUi`, `singleton`, `loadScript`, `owa_ad_clicks`, `check_important`, `check_browser`, `changeLazy`, `lazy_load`, `li_hover`, `_hover_wx`, `hover_sub`, `get_apple_icon`, `changTab`, `showTab`, `show_district`, `isKeyTrigger`, `in_array`, `in_array_id`, `addBookmark`, `set_domain`, `has_sensitive_code`, `str_len`:** Helper functions for various tasks in the web application.

Control Flow

Analyzing the control flow of every function is impractical due to the obfuscation. However, common patterns include:

* **While loops:** The main obfuscated section uses a `while` loop to decrypt its code, iterating until a specific condition is met.
* **Conditional statements:** Extensive use of `if` and `else` statements to control the flow based on conditions like button clicks, event types, AJAX response status, or data validation.
* **Callbacks:** jQuery's AJAX functions and event handlers rely on callback functions executed asynchronously.

Data Structures

The code heavily uses:

* **Arrays:** Used extensively to store data such as event handlers, animation queues, and arrays of elements obtained through jQuery selectors.
* **Objects:** Used for storing configuration settings, AJAX options, and event handler data (jQuery event objects).
* **jQuery objects:** jQuery wraps HTML elements and DOM nodes into its own object structure, enabling chaining of methods for manipulating elements.

The `_0x375b` function returns an array of strings serving as a lookup table for obfuscated hexadecimal numbers representing variable and function names, highlighting the strength of obfuscation.

Malware Family Suggestion

While the code itself is not malicious, the *extensive obfuscation* is a hallmark of malware. Malicious actors frequently obfuscate their code to hinder analysis and detection. The sheer size and complexity of the obfuscation in this code, combined with its lack of a clear, legitimate purpose (without deep contextual analysis of the surrounding application), raises suspicions. The functions and structures present could very easily be adapted for malicious purposes.

It is **not possible** to definitively label this code as belonging to a specific malware family without further analysis and knowledge of its deployment context. However, the obfuscation techniques strongly suggest it *could* be part of a larger malicious program or be a tool used by malware developers to create more complex malware components. The functionality of interacting with the DOM, handling events, manipulating cookies, and making AJAX requests are common capabilities used in various types of malware, making reverse engineering critical to determine the true intentions behind its usage.