Provisional Patent Application

Secure Payload Delivery System Using Self-Unregistering Service Workers

Inventor: [Your Name or Alias]

Date of Filing: [Today's Date]

Abstract

This invention provides a novel method for delivering secure, self-destructing payloads via web-based service workers and steganographic encoding. The method ensures controlled execution of payloads while preventing unauthorized persistence, making it useful for cybersecurity training, red team penetration testing, and cryptographic challenges.

Background of the Invention

Current cybersecurity persistence methods lack controlled execution mechanisms that prevent unauthorized reuse. This invention introduces a one-time-use payload delivery system that leverages service workers and steganography for secure execution.

Summary of the Invention

The system encodes a payload within an image file using steganographic techniques. A service worker is registered to intercept requests for the payload. Upon retrieval, the service worker unregisters itself, ensuring the payload cannot be reused. This provides a secure, one-time execution model for ethical cybersecurity use.

Detailed Description

Step 1: Encode the payload in an image file using steganography.

Step 2: Register a Service Worker to intercept and retrieve the payload.

Step 3: Extract and execute the payload, then unregister the Service Worker.

Step 4: Ensure payloads are delivered securely and self-destruct after retrieval.

Claims

1. A method for one-time secure payload execution using service workers.

2. A cybersecurity system that ensures controlled payload retrieval and execution.

3. A self-destructing execution model that prevents unauthorized persistence.

Conclusion

This invention introduces a unique approach to controlled payload execution, offering a secure and ethical framework for cybersecurity applications. By patenting this method, it ensures recognition while allowing public benefit.