**Synoptic – Securing Applications**

Thread 1:

|  |  |
| --- | --- |
| Id | TR1 |
| Name | Adversary tries hiding encrypted malicious JavaScript code |
| Description | Adversary tries to hide malicious data in image which can. |
| Stride | Tampering, Spoofing |
| Entry Points | (E1.1) Main Application |
| Assets | (A1.2) JavaScript Application |
| Mitigation Strategy | Inserting the hidden JavaScript code inside the image |

Thread 2:

|  |  |
| --- | --- |
| Id | TR2 |
| Name | Adversary tries appending data at the end of the bmp file |
| Description | Adversary tries to append the extension of the image and when it is downloaded the image will have hiding configuration data thus the image can run as example: executable. |
| Stride | Spoofing |
| Entry Points | (E2.1) Main Application |
| Assets | (A2.1) Executable Program |
| Mitigation Strategy | Appending the extension of an image |