**----------------------------------------------------------------**

**Malware Analysis Report**

**----------------------------------------------------------------**

|  |
| --- |
| **Sample Information** |

|  |  |
| --- | --- |
| **Sample Name:** | Sample.exe |
| **MD5 Hash:** |  |
| **SHA1 Hash:** |  |
| **Fuzzy Hash:** |  |
| **Imphash:** |  |

|  |
| --- |
| **Executive Summary** |

This will contain the TLDR of the analysis. Less technical descriptions of the sample will be here. Used to provide a basic explanation of what the sample does. IOCs will be included here for quick reference.

|  |
| --- |
| **Technical Analysis** |

This section will contain the reverse engineering. The report should be written in a way that the steps taken can be repeated by another analyst. Screenshots and captions should be included.

|  |
| --- |
| MITRE ATT&CK Techniques |

Here a list of all MITRE ATT&CK classifications of the malware sample will be included.

|  |  |  |
| --- | --- | --- |
| **ATT&CK ID** | **Tactic Name** | **Description of use** |
| T1071.001 | Command and Control over web protocols | Sample.exe connects to C2 server over using the HTTP protocol over port 8008. |