|  |  |
| --- | --- |
|  |  |
| On-demand malware analysis service | |
| Express analysis | |

|  |  |
| --- | --- |
| Type | Standard |
| Version | 1.0 |
| Date | 28/03/2017 |
| Analyst | <*name\_of\_analyst*> |
| Approved by | C. Harpes |
| Classification | Confidential |

Context

Example: *“itrust consulting was asked to perform an express analysis of a binary file, which is suspected to be malicious. The analysis is supposed to take about 2 hours. If the analysis is inconclusive due to the complexity of the file, itrust consulting will provide a quotation for a full analysis of the initial file and will not charge for the express analysis.”*

General file details

**MD5:**

**SHA1:**

**SHA256:**

**Compilation time:**

**Architecture:**

**File type:**

Analysis

**Malicious:** Yes/No/Unknown.

**Why:** Some evidences (screenshots) of key-logger/ spyware/ etc.

**Command & Control:** URL, server info and how it was determined.

**Targeted to Client:** Yes/No/Unknown.

**Why:** Some evidences...

Conclusion

Example: *“The analysed malware has keylogging and data exfiltration capabilities. We believe that this may not be the only piece of malware present on the machine. However, those files may have been deleted in the meantime. Knowing that the machine has been infected for a long time we recommend a full restaging of the machine.”*