(/)

**Dashboard (/dashboard/)**

☰ **Recent (/analysis/)**

⚙ **Pending (/analysis/pending/)**

🔍 **Search (/analysis/search/)**

Subm
⬆
(/subm

# Summary

📄 ransomware_c2.exe

## 📄 File *ransomware_c2.exe*

### Summary

⬇ Download (/file/sample/685550271c665b16dac234c4/)

🔄 Resubmit sample (/submit/re/6570319/)

| | |
|---|---|
| **Size** | 3.2MB |
| **Type** | PE32+ executable (console) x86-64, for MS Windows |
| **MD5** | d45ba3248cbdc0952d2a691f6727a97f |
| **SHA1** | ae46fc37b831f60b3670ddfa8ba77dec31843872 |
| **SHA256** | dc40d6f0cb069d6b89ba4742d4601fbb8186330168fb53111797932df5488972 |
| **SHA512** | Show SHA512 |
| **CRC32** | B863B743 |
| **ssdeep** | None |
| **Yara** | • spyeye - SpyEye X.Y memory<br>• ThreadControl__Context - (no description)<br>• SEH__vectored - (no description)<br>• Check_OutputDebugStringA_iat - (no description)<br>• anti_dbg - Checks if being debugged<br>• network_http - Communications over HTTP |

## 🔥 Score

This file appears fairly benign with a score of **0.1 out of 10.**

**Please notice**: The scoring system is currently still in development and should be considered an *alpha* feature.

## ✈ Feedback

Expecting different results? Send us this analysis and we will inspect it. Click here

## ⏻ Information on Execution