# Sandcastle: Analysis Summary >>

**File:** ThisIsNormalDocument.pdf

**SHA-256:** 391cfcd153881743556f76de7bbca5b19857f8b69a6f6f6dfde6fd9b06c17f5e

---

>> Analysis Results:

**Designation:** MALWARE

**Threat level:** 4/5

Analysed 07 Feb, 2022, 11:10:28

**Sandbox OS:** Windows 10

>> In Summary:

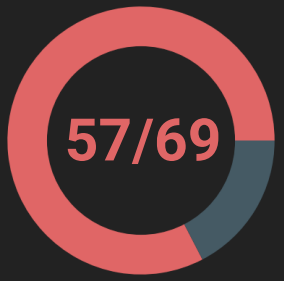
Overall,the sample was found to be:

MALICIOUS

Sandcastle Analysis scores this sample:

EXTREME

VirusTotal: Flagged as malicious by:




Security Vendors

## Insights //>>

*<// Confused by a technical term? Check out our website for explanations!*

» Threat Intel: Sample is most likely a ransomware.

» Threat Intel: Sample is likely an instance of the babuk threat.

» Threat Intel: Triggered a majority of Anti-virus engines.

» Threat Intel: References blacklisted strings and imports blacklisted libraries.

» Threat Intel: Triggered one or more YARA Rules or Rulesets.

» Behaviour: Triggered one or more Sigma Rules or Rulesets.

» Stealth Technique: Packed to avoid malicious code detection.

» Sandbox Intel: 3 out of 3 Third-Party Dynamic Sandboxes find this sample malicious.

## Report Contents //>>

**-\\ Clickable Chapters** **Pg.**

## File Details //>>

| | |
|---|---|
| **File:** | ThisIsNormalDocument.pdf |
| **MD5:** | 98b04a1cfdf18674315ec137733553a8 |
| **SHA-1:** | dd1cdb8782b5e08695b006393d1e8ab4e447556e |
| **SHA-256:** | 391cfcd153881743556f76de7bbca5b19857f8b69a6f6f6dfde6fd9b06c17f5e |
| **SS-DEEP:** | 1536:Bb6MM2qw/ZhutMC1u2srQLOJgY8ZZP8LHD4XWaNH71dLdG1iiFM2iG2Lr:VM2qaZ2i2srQLOJgY8Zp8LHD4XWaNH7j |

>> File Packing:

**Is File Packed?** Packed

**Entropy** 7.35

**Packer:**
Exe Packer 2.300

>> More Details:

**Size** 121212 kB (121.21 kB)

**Compiler** C++ Compiler

**Compile Timestamp** 2022-01-11 13:06:32

**Type** Portable Executable (PE32 GUI)

## Report Engine Data //>>


Breakdown of Sigma rules triggered.

6

YARA rules were triggered.

Blacklisted Strings found:

0

Blacklisted Imported Libraries found:

0

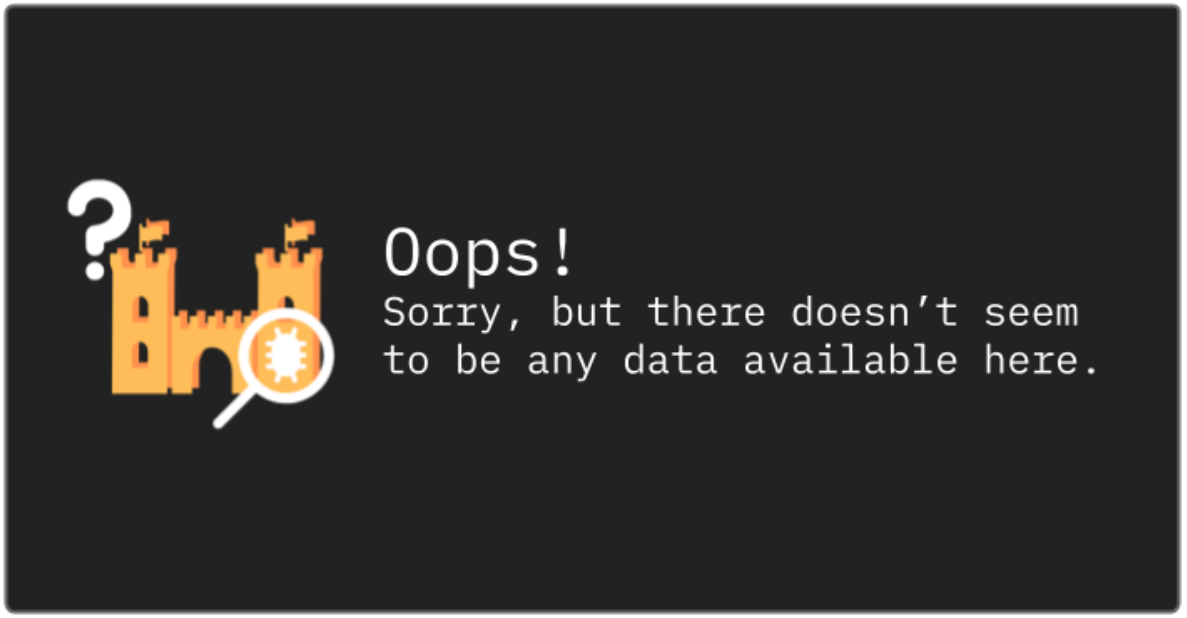
0

Malicious URL connections found.

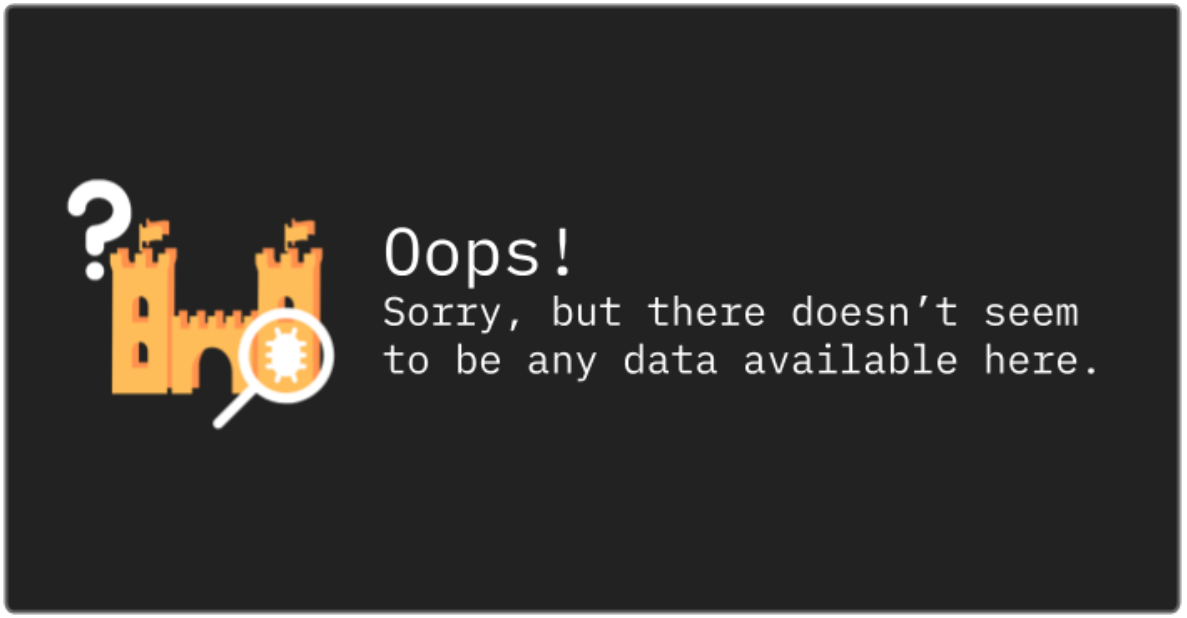
0

Malicious IP connections found.

## Network Connections - IP Addresses //>>



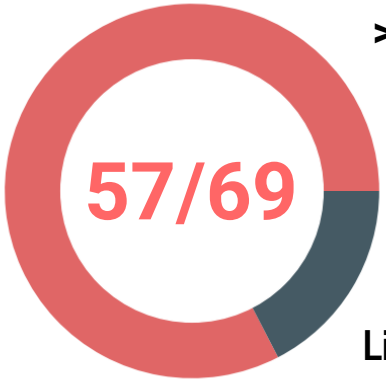
## Network Connections - URLs //>>



## VirusTotal Analysis //>>

*<// Click here to view the full VirusTotal report //--*

| | |
|---|---|
| **Most Commonly Known As** | 391cfcd153881743556f76de7bbca5b19857f8b69a6f6f6dfde6fd9b06c17f5e_unpacked |
| **Last Analysed** | 2022-01-20 11:38:04 |
| **Number of Submissions** | Submitted 8 times on VirusTotal.com |




### >> Security Vendor Data

**Detection Stats:** 57 Detect as MALICIOUS, 12 UNDETECTED.

**Catagorised as:** ransomware (Flagged by 24 vendors)

**Likely Threat Name:** babuk (Flagged by 10 vendors)

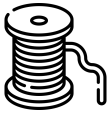
### >> Top 3 Dynamic Sandbox Analysis Results

| | |
|---|---|
| **Dr.Web vxCube** | **Malicious?** YES /// **Verdict:** \| MALWARE \| |
| **Yomi Hunter** | **Malicious?** YES /// **Verdict:** \| MALWARE \| |
| **Lastline** | **Malicious?** YES /// **Verdict:** \| MALWARE \| \| TROJAN \| \| RANSOM \| |

*You can view all sandbox results on the full VirusTotal report.*

## Imports //>>


Oops!
Sorry, but there doesn't seem
to be any data available here.



## Strings //>>

»

Copyright1998-2009byJoergenIbsenAllRightsReserved.,PoweredbySmartAssembly6.8.0.121,!PoweredbySmartAssembly6.6.1.44,!PoweredbySmartAssembly6.6.4.95,$Info:ThisfileispackedwiththeUPXexecutablepackerhttp://upx.sf.net$,$Id:UPX3.91Copyright1996-2013theUPXTeam.AllRightsReserved.$,ScreenCapture,WebcamCapture,PacketSniffer,\.mailslot\%s,ProxyServer