# Sandcastle: Analysis Summary >>

**File:** Creative Cloud.exe

**SHA-256:** 7092455b4306de907780015a49b1a20dd2ef170a024e80dee7f5e997d28b5bbf

---

>> Analysis Results:

**Designation:** SUS

**Threat level:** 2/5

Analysed 07 Feb, 2022, 11:10:28

**Sandbox OS:** Windows 7

>> In Summary:

Overall,the sample was found to be:

SUSPICIOUS

Sandcastle Analysis scores this sample:

LOW

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 trojan.

» Threat Intel: Sample is likely an instance of the gen2 threat.

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

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

## Report Contents //>>

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

## File Details //>>

| | |
|---|---|
| **File:** | Creative Cloud.exe |
| **MD5:** | 7695e2dc39975320f70ed1fe5b4bba12 |
| **SHA-1:** | 468fa2967b62f47152b70ffdc8ffba7af7dfc8c4 |
| **SHA-256:** | 7092455b4306de907780015a49b1a20dd2ef170a024e80dee7f5e997d28b5bbf |
| **SS-DEEP:** | 768:f6YAcD8LljAqJgQlyaycjI24BXxH5VKLZd7pxUF2Q282hZMIb5PoGvw9AS5VebKu:N8+qJgQlz8HkUcziIp9v2 7mKWCk4UOIL |

>> File Packing:

**Is File Packed?** Packed

**Entropy** 2.3

**Packer:**
UPX->www.upx.sourceforge.net

>> More Details:

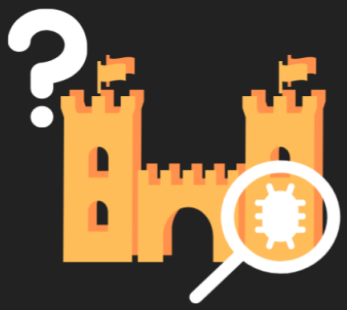
**Size** 150232 kB (150.23 kB)

**Compiler** Intel C++ Compiler Classic

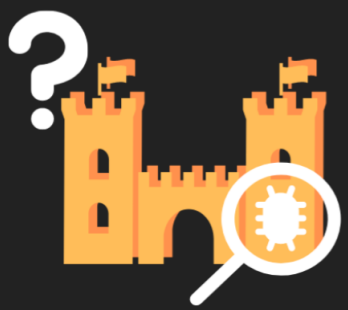
**Compile Timestamp** 2021-08-21 14:06:32

**Type** Portable Executable (PE32 GUI)

## Report Engine Data //>>



No data on Sigma rules triggered.



No data on YARA rules triggered.

Blacklisted Strings found:

0

Blacklisted Imported Libraries found:

0

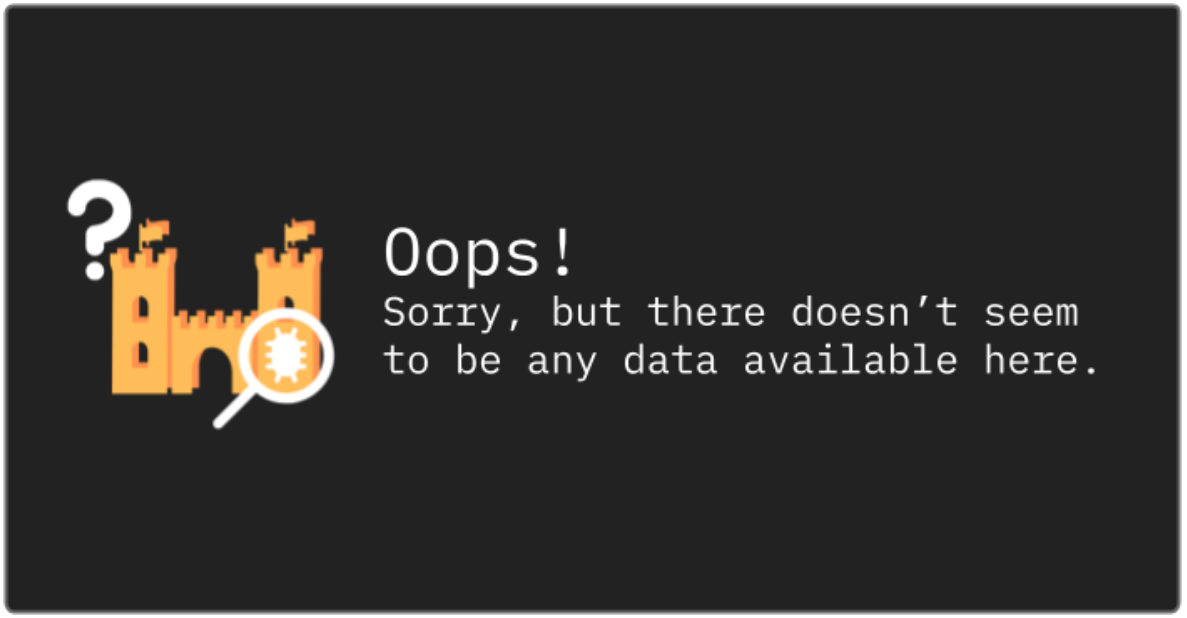
0

Malicious URL connections found.

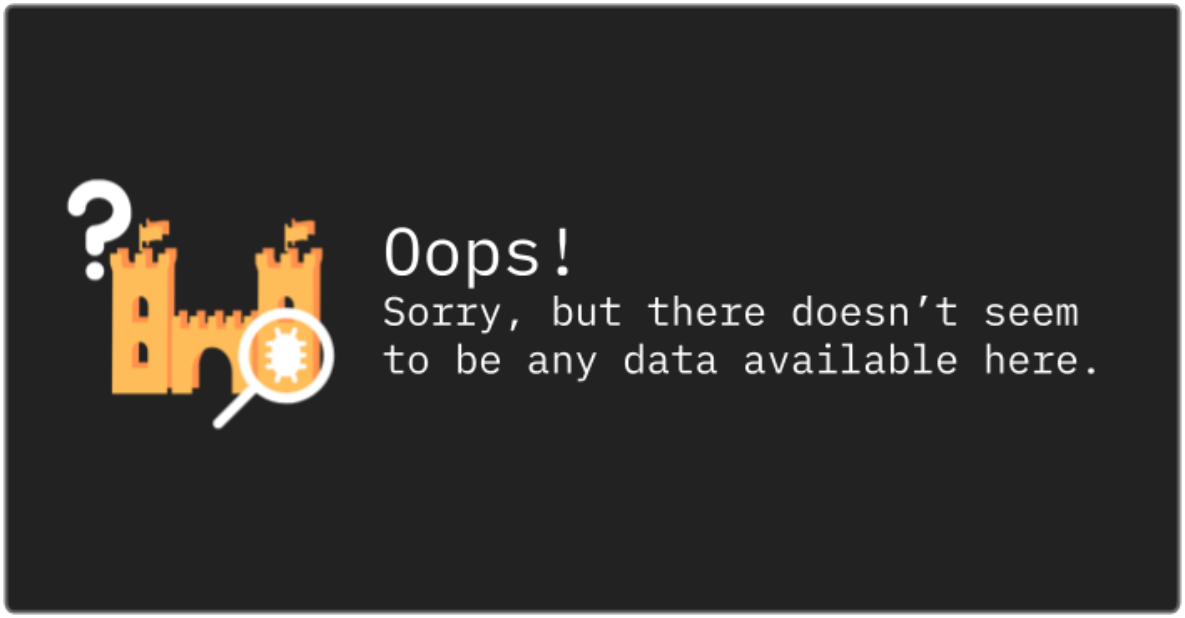
0

Malicious IP connections found.

## Network Connections - IP Addresses //>>



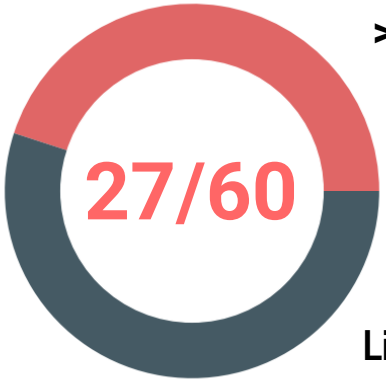
## Network Connections - URLs //>>



## VirusTotal Analysis //>>

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

| | |
|---|---|
| **Most Commonly Known As** | traveldoc4.xlsx |
| **Last Analysed** | 2020-06-04 21:10:58 |
| **Number of Submissions** | Submitted 1 times on VirusTotal.com |




### >> Security Vendor Data

**Detection Stats:** 27 Detect as MALICIOUS, 33 UNDETECTED.

**Catagorised as:** trojan (Flagged by 9 vendors)

**Likely Threat Name:** gen2 (Flagged by 6 vendors)

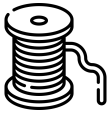
### >> Top 3 Dynamic Sandbox Analysis Results

*Sorry, looks like there isn't any data from our 3rd party analysis Sandboxes.*

***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 //>>

» R6002

-floatingpointsupportnotloaded

,R6002

-floatingpointnotloaded

,R6008

-notenoughspaceforarguments

,R6009

-notenoughspaceforenvironment

,programnameunknown,abnormalprogramtermination

,R6010

-aborthasbeencalled

,R6016

-notenoughspaceforthreaddata

,R6017

-unexpectedmultithreadlockerror

,R6018

-unexpectedheaperror

,R6019

-unabletoopenconsoledevice

,R6024

-notenoughspacefor_onexit/atexittable

,R6025

-purevirtualfunctioncall

,R6026

-notenoughspaceforstdioinitialization

,R6027

-notenoughspaceforlowioinitialization