Sandcastle: Analysis Summary >>

File: Creative Cloud.exe

SHA-256: 49a9eb601f18e882db732475bf69c09f5efb94124a20f1e13c5e65f20d9411f7

>> Analysis Results:

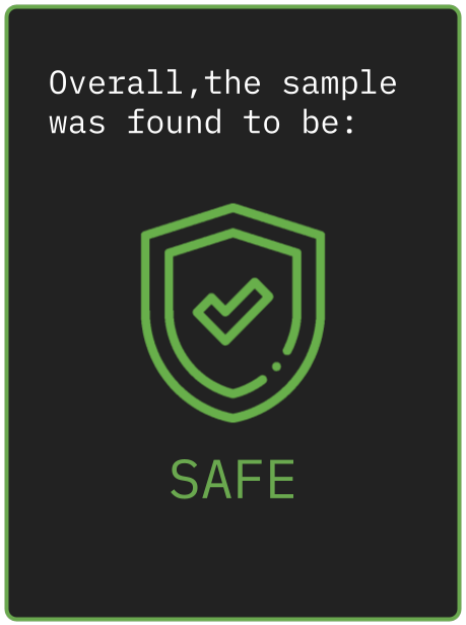
Designation: SAFE

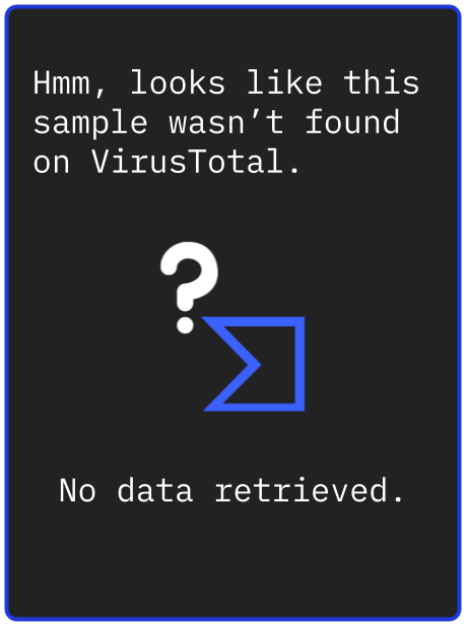
Threat level: 1/5

Analysed 07 Feb, 2022, 11:10:28

Sandbox OS: Windows 10

>> In Summary:





Insights //>>

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

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

Report Contents //>>

-\\ Clickable Chapters **Pg.**

File Details //>>

File:	Creative Cloud.exe
MD5:	fcb789n179dcdas3867q3cvfwq
SHA-1:	12347890vn234v7890n2347v890n1234789v35789b
SHA-256:	49a9eb601f18e882db732475bf69c09f5efb94124a20f1e13c5e65f20d9411f7
SS-DEEP:	V20N658347:VT0B23458Q190VDSB23645T

>> File Packing:

Is File Packed? Not Packed

Entropy 3.9

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

>> More Details:

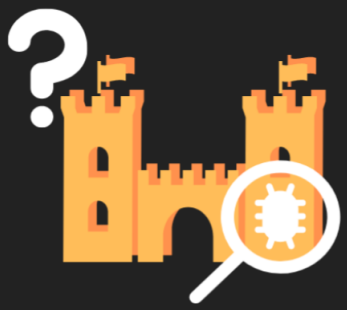
Size 123456 kB (123.46 kB)

Compiler Assembler

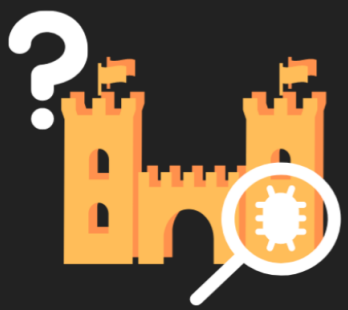
Compile Timestamp 2022-01-12 14:49:28

Type Executable

Report Engine Data //>>



No data on Sigma rules triggered.



No data on YARA rules triggered.

Blacklisted Strings found:

0

Blacklisted Imported Libraries found:

0

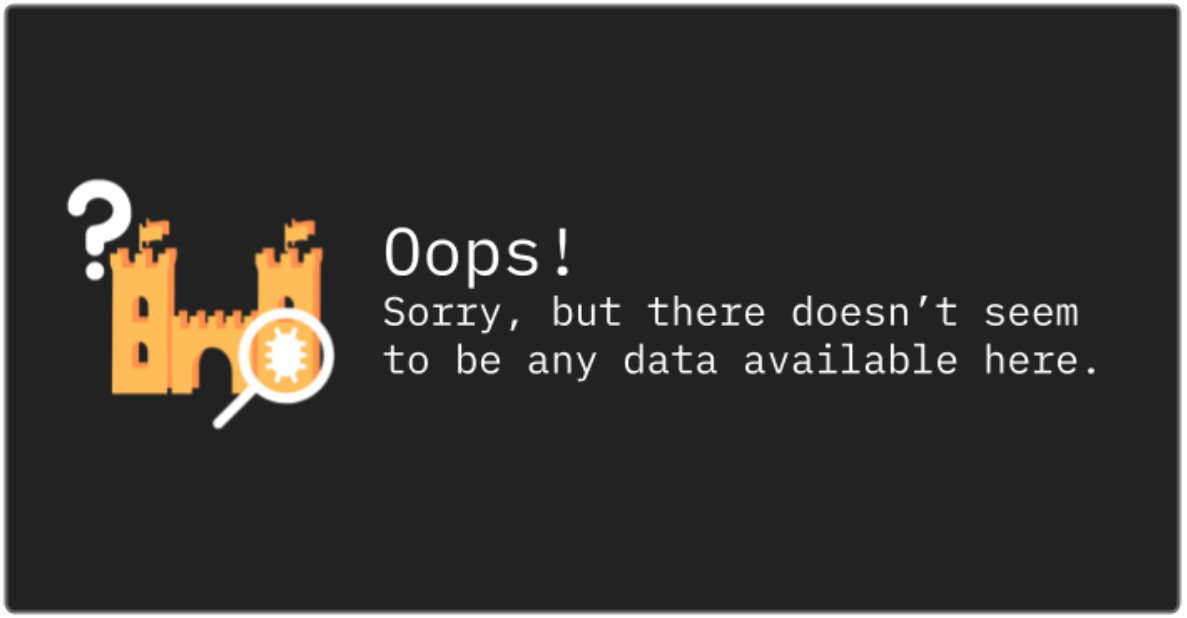
0

Malicious URL connections found.

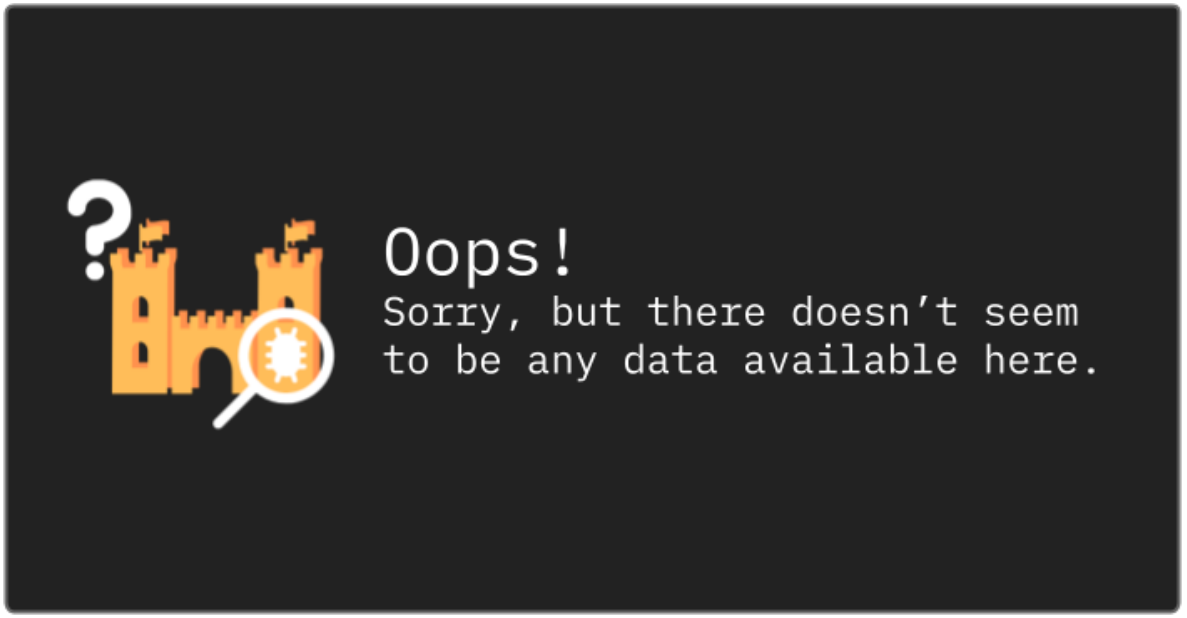
0

Malicious IP connections found.

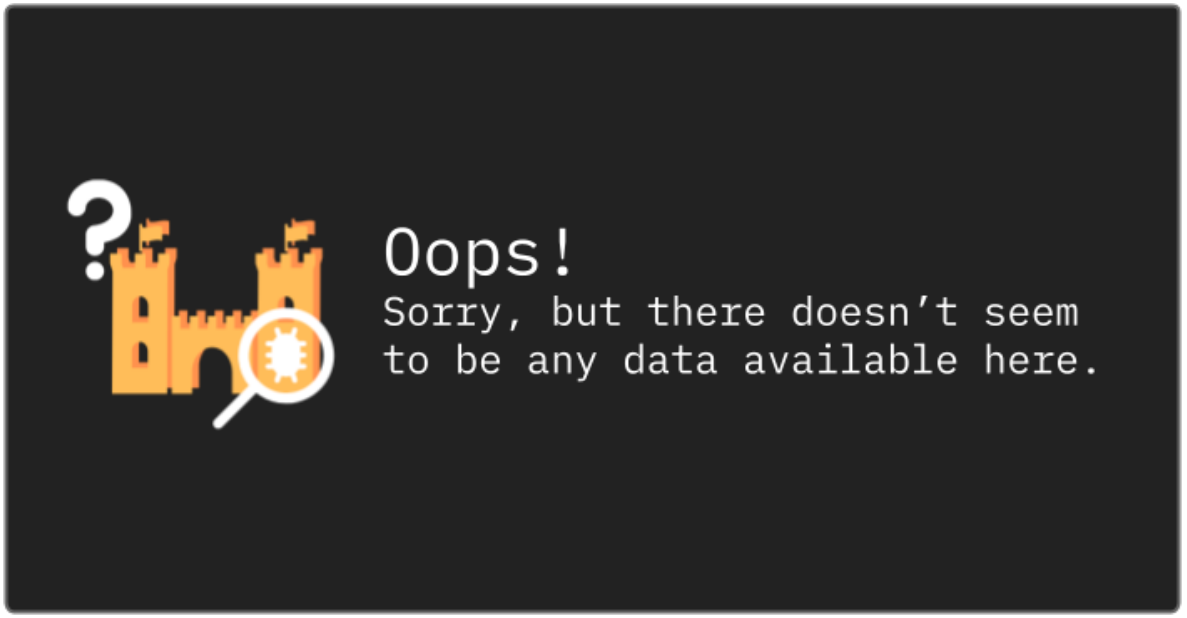
Network Connections - IP Addresses //>>



Network Connections - URLs //>>



VirusTotal Analysis //>>

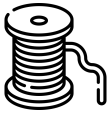


Imports //>>

»

SslFreeCertificate,SslGenerateRandomBits,SslGetServerIdentity,LZRead,LZCopy,LZInit,LZSeek,LZStart,LZClose,CACloseCert

Type



Strings //>>

» %WINDIR%system32cmd.exe /c pause

» c.._.,

» RPC ControlConsoleLPC-0x0000000000004B8--2011455480-27866242770034225105549481312593917963633305251386256528-1650549854

» Sessions1WindowsApiPort

» Sessions1WindowsApiPort

» _C:Win32.DarkTequila.exeConsoleLPC-0x0000000000004B8--2011455480--1650549854

» Sessions1WindowsApiPort