



Login

Reports



7906dc47\_by\_Librana...

Overview  
overview

10

Static  
static

7906dc47\_by\_Li...is...  
windows7\_x64

3

7906dc47\_by\_Li...is...  
windows10\_x64

Download Sample

Feedback

Sharing

<https://tria.ge/210521-f7lr19wnc6>

Twitter

E-mail

▼ General

Target  
7906dc47\_by\_Libranalysis

Size  
22KB

Sample  
210521-f7lr19wnc6

Score

10 /10

MD5

7906dc475a8ae55ffb5af7fd3ac8f

SHA1

e7304e2436dc0eddddba229f1ec7

SHA256

1814a6a6749684cdacd792374e0b

SHA512

c087b3107295095e9aca527d02b7

ransomware

▼ Malware Config

Extracted

Path

C:\Users\Admin\Desktop\readme.txt

ALL YOUR DOCUMENTS PHOTOS DATABASES AND OTHER IMPORTANT FILES  
HAVE BEEN ENCRYPTED!

=====



© 2018-2021

**Ransom Note**

To receive the private key and decryption program follow the instructions below:

1. Download "Tor Browser" from <https://www.torproject.org/> and install it.
2. In the "Tor Browser" open your personal page here:

<http://6260bea096ec44d022eltalkfzj.n5fnrf4l7bdjhelx.onion/eltalkfzj>

Note! This page is available via "Tor Browser" only.

=====  
=====

Also you can use temporary addresses on your personal page without using "Tor Browser":

<http://6260bea096ec44d022eltalkfzj.jobbig.cam/eltalkfzj>


<http://6260bea096ec44d022eltalkfzj.boxgas.icu/eltalkfzj>

<http://6260bea096ec44d022eltalkfzj.sixsees.club/eltalkfzj>

<http://6260bea096ec44d022eltalkfzj.nowuser.casa/eltalkfzj>


Note! These are temporary addresses! They will be available for a limited amount of time!


<http://6260bea096ec44d022eltalkfzj.n5fnrf4l7bdjhelx.onion/eltalkfzj>  <http://6260bea096ec44d022eltalkfzj.jobbig.cam/eltalkfzj> 

**MD5**  
7906dc475a8ae55ffb5af7fd3ac8 

**Filesize**  
22KB

**10** /10

**SHA256**  
1814a6a6749684cdacd792374ec 

**SHA512**  
c087b3107295095e9aca527d02t 

## Tags

ransomware

## Signatures

Process spawned unexpected child process 

## Description

This typically indicates the parent process was compromised via an exploit or macro.

Suspicious use of NtCreateProcessExOtherParentProcess

... ..

Suspicious use of SetThreadContext

Related Tasks

behavioral1 behavioral2

▼  MITRE ATT&CK Matrix

Collection	Command and Control	Credential Access	Defense Evasion	Discovery	Execution	Exfiltration	Impact	Initial Access
			Modify	Query				

