Recorded Future®
Triage

General

Target
8cc84c910910535990b7ec98b521f7bb84774a78fa...

Size
207KB

Sample
221213-dbm5bagb9t

MD5
a57745a30d63f511d28aa43e4b710e1c

SHA1
5985e7d1831784fd15de2cc62451deb16b65b046

SHA256
8cc84c910910535990b7ec98b521f7bb84774a78fa...

SHA512
d7297bc3945f14b820379989b32d9476be5c3da04...

Score

10/10

cerber

gozi

banker

evasion

persistence

ransomware

spyware

stealer

trojan

Malware Config

Extracted

Path C:\Users\Admin\Music\# DECRYPT MY FILES #.html

Ransom Note

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>&#067;erber &#082;ansomware</title>
    <style>
    a {
      color: #47c;
      text-decoration: none;
    }
    a:hover {
      text-decoration: underline;
    }
    body {
      background-color: #e7e7e7;
      color: #333;
      font-family: "Helvetica Neue", Helvetica, "Segoe UI", Arial, freesans, sans-serif, "Apple Color Emoji", "Segoe UI Emoji", "Segoe UI Symbol";
      font-size: 16px;
      line-height: 1.6;
      margin: 0;
      padding: 0;
    }
    hr {
      background-color: #e7e7e7;
      border: 0 none;
      border-bottom: 1px solid #c7c7c7;
      height: 5px;
      margin: 30px 0;
    }
    li {
      padding: 0 0 7px 7px;
    }
    ol {
      padding-left: 3em;
    }
    .container {
      background-color: #fff;
      border: 1px solid #c7c7c7;
      margin: 40px;
      padding: 40px 40px 20px 40px;
    }
    .info, .tor {
      background-color: #efe;
      border: 1px solid #bda;
      display: block;
      padding: 0px 20px;
    }
    .logo {
      font-size: 12px;
      font-weight: bold;
      line-height: 1;
      margin: 0;
    }
    .upd_on {
      color: red;
      display: block;
    }
    .upd_off {
      display: none;
      float: left;
    }
    .tor {
      padding: 10px 0;
      text-align: center;
    }
    .url {
      margin-right: 5px;
    }
    .warning {
      background-color: #f5e7e7;
      border: 1px solid #ebccd1;
      color: #a44;
      display: block;
      padding: 15px 10px;
      text-align: center;
    }
    </style>
  </head>
  <body>
    <div class="container">
      <h3>C E R B E R&nbsp;&nbsp;&nbsp;R A N S O M W A R E</h3>
      <hr>
      <p>Cannot you find the files you need?<br>Is the content of the files that you looked fo
not readable?</p>
      <p>It is normal because the files' names, as well as the data in your files have been
encrypted.</p>
      <p>Great!<br>You have turned to be a part of a big community "#C3rber Ransomware".
</p>
      <hr>
      <p><span class="warning">If you are reading this message it means the software
"Cerber" has been removed from your computer.</span></p>
      <hr>
      <h3>What is encryption?</h3>
      <p>Encryption is a reversible modification of information for security reasons but
providing full access to it for authorized users.</p>
      <p>To become an authorized user and keep the modification absolutely reversible (in
other words to have a possibility to decrypt your files) you should have an individual private
key.</p>
      <p>But not only it.</p>
      <p>It is required also to have the special decryption software (in your case "Cerber
Decryptor" software) for safe and complete decryption of all your files and data.</p>
      <hr>
      <h3>Everything is clear for me but what should I do?</h3>
      <p>The first step is reading these instructions to the end.</p>
      <p>Your files have been encrypted with the "Cerber Ransomware" software; the
instructions ("# DECRYPT MY FILES #.html" and "# DECRYPT MY FILES #.txt") in the folders
with your encrypted files are not viruses, they will help you.</p>
      <p>After reading this text the most part of people start searching in the Internet the
words the "Cerber Ransomware" where they find a lot of ideas, recommendations and
instructions.</p>
      <p>It is necessary to realize that we are the ones who closed the lock on your files and
we are the only ones who have this secret key to open them.</p>
```

```
        <p><span class="warning">!Any attempts to get back your files with the third-party too
can be fatal for your encrypted files!</span></p>
        <p>The most part of the third-party software change data within the encrypted file to
restore it but this causes damage to the files.</p>
        <p>Finally it will be impossible to decrypt your files!</p>
        <p>When you make a puzzle, but some items are lost, broken or not put in its place - the
puzzle items will never match, the same way the third-party software will ruin your files
completely and irreversibly.</p>
        <p>You should realize that any intervention of the third-party software to restore files
encrypted with the "Cerber Ransomware" software may be fatal for your files.</p>
        <hr>
        <p><span class="warning">There are several plain steps to restore your files but if you
do not follow them we will not be able to help you, and we will not try since you have read this
warning already.</span></p>
        <hr>
        <p>For your information the software to decrypt your files (as well as the private key
provided together) are paid products.</p>
        <p>After purchase of the software package you will be able to:</p>
        <ol>
        <li>decrypt all your files;</li>
        <li>work with your documents;</li>
        <li>view your photos and other media;</li>
        <li>continue your usual and comfortable work at the computer.</li>
        </ol>
        <p>If you understand all importance of the situation then we propose to you to go direct
to your personal page where you will receive the complete instructions and guarantees to
restore your files.</p>
        <hr>
        <div class="info">
        <p>There is a list of temporary addresses to go on your personal page below:</p>
        <ol>
        <li><span class="upd_off" id="upd_1">Please wait...</span><a class="url"
href="http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C" id="url_1"
target="_blank">http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C</a>(<a
href="#updateUrl" onClick="return updateUrl();" style="color: red;">Get a NEW address!</a>)
</li>
        <li><a href="http://bqyjebfh25oellur.onion.cab/AA79-9F05-B08B-0046-168C"
target="_blank">http://bqyjebfh25oellur.onion.cab/AA79-9F05-B08B-0046-168C</a></li>
        <li><a href="http://bqyjebfh25oellur.onion.nu/AA79-9F05-B08B-0046-168C"
target="_blank">http://bqyjebfh25oellur.onion.nu/AA79-9F05-B08B-0046-168C</a></li>
        <li><a href="http://bqyjebfh25oellur.onion.link/AA79-9F05-B08B-0046-168C"
target="_blank">http://bqyjebfh25oellur.onion.link/AA79-9F05-B08B-0046-168C</a></li>
        <li><a href="http://bqyjebfh25oellur.tor2web.org/AA79-9F05-B08B-0046-168C"
target="_blank">http://bqyjebfh25oellur.tor2web.org/AA79-9F05-B08B-0046-168C</a></li>
        </ol>
        </div>
        <hr>
        <h3>What should you do with these addresses?</h3>
        <p>If you read the instructions in TXT format (if you have instruction in HTML (the file
with an icon of your Internet browser) then the easiest way is to run it):</p>
        <ol>
        <li>take a look at the first address (in this case it is <span class="upd_off"
id="upd_2">Please wait...</span><a class="url" href="http://bqyjebfh25oellur.onion.to/AA79-
9F05-B08B-0046-168C" id="url_2" target="_blank">http://bqyjebfh25oellur.onion.to/AA79-
9F05-B08B-0046-168C</a>);</li>
        <li>select it with the mouse cursor holding the left mouse button and moving the cursor
to the right;</li>
        <li>release the left mouse button and press the right one;</li>
        <li>select "Copy" in the appeared menu;</li>
        <li>run your Internet browser (if you do not know what it is run the Internet Explorer);</li
        <li>move the mouse cursor to the address bar of the browser (this is the place where th
site address is written);</li>
        <li>click the right mouse button in the field where the site address is written;</li>
        <li>select the button "Insert" in the appeared menu;</li>
        <li>then you will see the address <span class="upd_off" id="upd_3">Please wait...
</span><a class="url" href="http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C"
id="url_3" target="_blank">http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C</a
appeared there;</li>
        <li>press ENTER;</li>
        <li>the site should be loaded; if it is not loaded repeat the same instructions with the
second address and continue until the last address if falling.</li>
        </ol>
        <p>If for some reason the site cannot be opened check the connection to the Internet; i
the site still cannot be opened take a look at the instructions on omitting the point about
working with the addresses in the HTML instructions.</p>
        <p>If you browse the instructions in HTML format:</p>
        <ol>
        <li>click the left mouse button on the first address (in this case it is <span
class="upd_off" id="upd_4">Please wait...</span><a class="url"
href="http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C" id="url_4"
target="_blank">http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C</a>);</li>
        <li>in a new tab or window of your web browser the site should be loaded; if it is not
loaded repeat the same instructions with the second address and continue until the last
address.</li>
        </ol>
        <p>If for some reason the site cannot be opened check the connection to the Internet.
</p>
        <hr>
        <p>Unfortunately these sites are short-term since the antivirus companies are intereste
in you do not have a chance to restore your files but continue to buy their products.</p>
        <p>Unlike them we are ready to help you always.</p>
        <p>If you need our help but the temporary sites are not available:</p>
        <ol>
        <li>run your Internet browser (if you do not know what it is run the Internet Explorer);</li
        <li>enter or copy the address <a href="https://www.torproject.org/download/download-
easy.html.en" target="_blank">https://www.torproject.org/download/download-
easy.html.en</a> into the address bar of your browser and press ENTER;</li>
        <li>wait for the site loading;</li>
        <li>on the site you will be offered to download Tor Browser; download and run it, follow
the installation instructions, wait until the installation is completed;</li>
        <li>run Tor Browser;</li>
        <li>connect with the button "Connect" (if you use the English version);</li>
        <li>a normal Internet browser window will be opened after the initialization;</li>
        <li>type or copy the address <span class="tor">http://bqyjebfh25oellur.onion/AA79-
9F05-B08B-0046-168C</span> in this browser address bar;</li>
        <li>press ENTER;</li>
        <li>the site should be loaded; if for some reason the site is not loading wait for a momen
and try again.</li>
        </ol>
        <p>If you have any problems during installation or operation of Tor Browser, please, visit
<a href="https://www.youtube.com/results?search_query=install+tor+browser+windows"
target="_blank">https://www.youtube.com/</a> and type request in the search bar "install to
browser windows" and you will find a lot of training videos about Tor Browser installation and
operation.</p>
        <p>If TOR address is not available for a long period (2-3 days) it means you are late;
usualy you have about 2-3 weeks after reading the instructions to restore your files.</p>
        <hr>
        <h3>Additional information:</h3>
        <p>You will find the instructions for restoring your files in those folders where you have
your encrypted files only.</p>
        <p>The instructions are made in two file formats - HTML and TXT for your convenience.
</p>
```

```
      <p>Unfortunately antivirus companies cannot protect or restore your files but they can
make the situation worse removing the instructions how to restore your encrypted files.</p>
      <p>The instructions are not viruses; they have informative nature only, so any claims on
the absence of any instruction files you can send to your antivirus company.</p>
      <hr>
      <p>Cerber Ransomware Project is not malicious and is not intended to harm a person ar
his/her information data.</p>
      <p>The project is created for the sole purpose of instruction regarding information
security, as well as certification of antivirus software for their suitability for data protection.
</p>
      <p>Together we make the Internet a better and safer place.</p>
      <hr>
      <p>If you look through this text in the Internet and realize that something is wrong with
your files but you do not have any instructions to restore your files, please, contact your
antivirus support.</p>
      <hr>
      <p>Remember that the worst situation already happened and now it depends on your
determination and speed of your actions the further life of your files.</p>
    </div>
    <script>
    function getXMLHttpRequest() {
      if (window.XMLHttpRequest) {
        return new window.XMLHttpRequest;
      }
      else {
        try {
          return new ActiveXObject("MSXML2.XMLHTTP.3.0");
        }
        catch(error) {
          return null;
        }
      }
    }
    function getUrlContent(url, callback) {
      var xhttp = getXMLHttpRequest();
      if (xhttp) {
        xhttp.onreadystatechange = function() {
          if (xhttp.readyState == 4) {
            if (xhttp.status == 200) {
              return callback(xhttp.responseText.replace(/[\s ]+/gm, ""), null);
            }
            else {
              return callback(null, true);
            }
          }
        };
        xhttp.open("GET", url + '?_=' + new Date().getTime(), true);
        xhttp.send();
      }
      else {
        return callback(null, true);
      }
    }
    function server1(address, callback) {
      getUrlContent("http://btc.blockr.io/api/v1/address/txs/" + address, function(result, error)
        if (!error) {
          var tx = /"tx":"([\w]+)","time_utc":"[\w-:]+","confirmations":
[\d]+,"amount":-/.exec(result);
          if (tx) {
            getUrlContent("http://btc.blockr.io/api/v1/tx/info/" + tx[1], function(result, error) {
              if (!error) {
                var address = /"vouts":\[{"address":"([\w]+)"/.exec(result);
                if (address) {
                  return callback(address[1], null);
                }
                else {
                  return callback(null, true);
                }
              }
              else {
                return callback(null, true);
              }
            });
          }
          else {
            return callback(null, true);
          }
        }
        else {
          return callback(null, true);
        }
      });
    }
    function server2(address, callback) {
      getUrlContent("http://api.blockcypher.com/v1/btc/main/addrs/" + address, function(resu
error) {
        if (!error) {
          var tx = /"tx_hash":"([\w]+)","block_height":[\d]+,"tx_input_n":
[\d-]+,"tx_output_n":-/.exec(result);
          if (tx) {
            getUrlContent("http://api.blockcypher.com/v1/btc/main/txs/" + tx[1], function(result
error) {
              if (!error) {
                var address = /"outputs":\[{"value":[\d]+,"script":"[\w]+","spent_by":"
[\w]+","addresses":\["([\w]+)"/.exec(result);
                if (address) {
                  return callback(address[1], null);
                }
                else {
                  return callback(null, true);
                }
              }
              else {
                return callback(null, true);
              }
            });
          }
          else {
            return callback(null, true);
          }
        }
        else {
          return callback(null, true);
        }
```

Extracted

Path	C:\Users\Admin\Music\# DECRYPT MY FILES #.txt
Ransom Note	

C_E_R_B_E_R   R_A_N_S_O_M_W_A_R_E

##

Cannot you find the files you need?
Is the content of the files that you looked for not readable???

It is normal because the files' names, as well as the data in your files
have been encrypted.

Great!
You have turned to be a part of a big community "#Cerb3r Ransomware".

##

!!! If you are reading this message it means the software "Cerber" has
!!! been removed from your computer.

!!! HTML instruction ("# DECRYPT MY FILES #.html") always contains a
!!! working domain of your personal page!

##

What is encryption?

Encryption is a reversible modification of information for security
reasons but providing full access to it for authorized users.

To become an authorized user and keep the modification absolutely
reversible (in other words to have a possibility to decrypt your files)
you should have an individual private key.

But not only it.

It is required also to have the special decryption software
(in your case "Cerber Decryptor" software) for safe and complete
decryption of all your files and data.

##

Everything is clear for me but what should I do?

The first step is reading these instructions to the end.

Your files have been encrypted with the "Cerber Ransomware" software; the
instructions ("# DECRYPT MY FILES #.html" and "# DECRYPT MY FILES #.txt")
in the folders with your encrypted files are not viruses, they will
help you.

```
After reading this text the most part of people start searching in the
Internet the words the "Cerber Ransomware" where they find a lot of
ideas, recommendations and instructions.

It is necessary to realize that we are the ones who closed the lock on
your files and we are the only ones who have this secret key to
open them.

!!!  Any attempts to return your files with the third-party tools can
!!!  be fatal for your encrypted files.

The most part of the third-party software change data within the
encrypted file to restore it but this causes damage to the files.

Finally it will be impossible to decrypt your files.

When you make a puzzle, but some items are lost, broken or not put in its
place - the puzzle items will never match, the same way the third-party
software will ruin your files completely and irreversibly.

You should realize that any intervention of the third-party software to
restore files encrypted with the "Cerber Ransomware" software may be
fatal for your files.


################################################################################


!!!  There are several plain steps to restore your files but if you do
!!!  not follow them we will not be able to help you, and we will not try
!!!  since you have read this warning already.


################################################################################


For your information the software to decrypt your files (as well as the
private key provided together) are paid products.

After purchase of the software package you will be able to:

1.  decrypt all your files;

2.  work with your documents;

3.  view your photos and other media;

4.  continue your usual and comfortable work at the computer.

If you understand all importance of the situation then we propose to you
to go directly to your personal page where you will receive the complete
instructions and guarantees to restore your files.


################################################################################
```

There is a list of temporary addresses to go on your personal page below:

1. http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C
2. http://bqyjebfh25oellur.onion.cab/AA79-9F05-B08B-0046-168C
3. http://bqyjebfh25oellur.onion.nu/AA79-9F05-B08B-0046-168C
4. http://bqyjebfh25oellur.onion.link/AA79-9F05-B08B-0046-168C
5. http://bqyjebfh25oellur.tor2web.org/AA79-9F05-B08B-0046-168C

###

What should you do with these addresses?

If you read the instructions in TXT format (if you have instruction in HTML (the file with an icon of your Internet browser) then the easiest way is to run it):

1. take a look at the first address (in this case it is http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C);

2. select it with the mouse cursor holding the left mouse button and moving the cursor to the right;

3. release the left mouse button and press the right one;

4. select "Copy" in the appeared menu;

5. run your Internet browser (if you do not know what it is run the Internet Explorer);

6. move the mouse cursor to the address bar of the browser (this is the place where the site address is written);

7. click the right mouse button in the field where the site address is written;

8. select the button "Insert" in the appeared menu;

9. then you will see the address http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C appeared there;

10. press ENTER;

11. the site should be loaded; if it is not loaded repeat the same instructions with the second address and continue until the last address if falling.

If for some reason the site cannot be opened check the connection to the Internet; if the site still cannot be opened take a look at the instructions on omitting the point about working with the addresses in the HTML instructions.

If you browse the instructions in HTML format:

1. click the left mouse button on the first address (in this case it is
   http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C);

2. in a new tab or window of your web browser the site should be loaded;
   if it is not loaded repeat the same instructions with the second
   address and continue until the last address.

If for some reason the site cannot be opened check the connection to
the Internet.

```
###############################################################################
```

Unfortunately these sites are short-term since the antivirus companies
are interested in you do not have a chance to restore your files but
continue to buy their products.

Unlike them we are ready to help you always.

If you need our help but the temporary sites are not available:

1. run your Internet browser (if you do not know what it is run the
   Internet Explorer);

2. enter or copy the address
   https://www.torproject.org/download/download-easy.html.en into the
   address bar of your browser and press ENTER;

3. wait for the site loading;

4. on the site you will be offered to download Tor Browser; download and
   run it, follow the installation instructions, wait until the
   installation is completed;

5. run Tor Browser;

6. connect with the button "Connect" (if you use the English version);

7. a normal Internet browser window will be opened after
   the initialization;

8. type or copy the address

```
 ────────────────────────────────────────────
|                                      |
| http://bqyjebfh25oellur.onion/AA79-9F05-B08B-0046-168C |
|────────────────────────────────────────────|
```

   in this browser address bar;

9. press ENTER;

10. the site should be loaded; if for some reason the site is not loading
    wait for a moment and try again.

If you have any problems during installation or operation of Tor Browser,
please, visit https://www.youtube.com/ and type request in the search bar

"install tor browser windows" and you will find a lot of training videos about Tor Browser installation and operation.

If TOR address is not available for a long period (2-3 days) it means you are late; usually you have about 2-3 weeks after reading the instructions to restore your files.

###

Additional information:

You will find the instructions for restoring your files in those folders where you have your encrypted files only.

The instructions are made in two file formats - HTML and TXT for your convenience.

Unfortunately antivirus companies cannot protect or restore your files but they can make the situation worse removing the instructions how to restore your encrypted files.

The instructions are not viruses; they have informative nature only, so any claims on the absence of any instruction files you can send to your antivirus company.

###

Cerber Ransomware Project is not malicious and is not intended to harm a person and his/her information data.

The project is created for the sole purpose of instruction regarding information security, as well as certification of antivirus software for their suitability for data protection.

Together we make the Internet a better and safer place.

###

If you look through this text in the Internet and realize that something is wrong with your files but you do not have any instructions to restore your files, please, contact your antivirus support.

###

Remember that the worst situation already happened and now it depends on your determination and speed of your actions the further life of your files.

URLs

http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.onion.cab/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.onion.nu/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.onion.link/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.tor2web.org/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.onion/AA79-9F05-B08B-0046-168C

Extracted

Path C:\Users\Admin\Desktop\# DECRYPT MY FILES #.html

Ransom Note

CERBERRANSOMWARE
Cannot you find the files you need?
Is the content of the files that you looked for not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.
Great!
You have turned to be a part of a big community "#C3rber Ransomware".
If you are reading this message it means the software "Cerber" has been removed from your computer.
What is encryption?
Encryption is a reversible modification of information for security reasons but providing full access to it for authorized users.
To become an authorized user and keep the modification absolutely reversible (in other words to have a possibility to decrypt your files) you should have an individual private key.
But not only it.
It is required also to have the special decryption software (in your case "Cerber Decryptor" software) for safe and complete decryption of all your files and data.
Everything is clear for me but what should I do?
The first step is reading these instructions to the end.
Your files have been encrypted with the "Cerber Ransomware" software; the instructions ("# DECRYPT MY FILES #.html" and "# DECRYPT MY FILES #.txt") in the folders with your encrypted files are not viruses, they will help you.
After reading this text the most part of people start searching in the Internet the words the "Cerber Ransomware" where they find a lot of ideas, recommendations and instructions.
It is necessary to realize that we are the ones who closed the lock on your files and we are th only ones who have this secret key to open them.
!Any attempts to get back your files with the third-party tools can be fatal for your encrypted files!
The most part of the third-party software change data within the encrypted file to restore it but this causes damage to the files.
Finally it will be impossible to decrypt your files!
When you make a puzzle, but some items are lost, broken or not put in its place - the puzzle items will never match, the same way the third-party software will ruin your files completely and irreversibly.
You should realize that any intervention of the third-party software to restore files encrypted with the "Cerber Ransomware" software may be fatal for your files.
There are several plain steps to restore your files but if you do not follow them we will not be able to help you, and we will not try since you have read this warning already.
For your information the software to decrypt your files (as well as the private key provided together) are paid products.
After purchase of the software package you will be able to:
decrypt all your files;
work with your documents;
view your photos and other media;
continue your usual and comfortable work at the computer.
If you understand all importance of the situation then we propose to you to go directly to your

personal page where you will receive the complete instructions and guarantees to restore you
files.
There is a list of temporary addresses to go on your personal page below:
Please wait... http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C(Get a NEW address!)
http://bqyjebfh25oellur.onion.cab/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.onion.nu/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.onion.link/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.tor2web.org/AA79-9F05-B08B-0046-168C
What should you do with these addresses?
If you read the instructions in TXT format (if you have instruction in HTML (the file with an icon of your Internet browser) then the easiest way is to run it):
take a look at the first address (in this case it is Please wait... http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C);
select it with the mouse cursor holding the left mouse button and moving the cursor to the right;
release the left mouse button and press the right one;
select "Copy" in the appeared menu;
run your Internet browser (if you do not know what it is run the Internet Explorer);
move the mouse cursor to the address bar of the browser (this is the place where the site address is written);
click the right mouse button in the field where the site address is written;
select the button "Insert" in the appeared menu;
then you will see the address Please wait... http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B
0046-168C appeared there;
press ENTER;
the site should be loaded; if it is not loaded repeat the same instructions with the second address and continue until the last address if falling.
If for some reason the site cannot be opened check the connection to the Internet; if the site still cannot be opened take a look at the instructions on omitting the point about working with the addresses in the HTML instructions.
If you browse the instructions in HTML format:
click the left mouse button on the first address (in this case it is Please wait... http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C);
in a new tab or window of your web browser the site should be loaded; if it is not loaded repe
the same instructions with the second address and continue until the last address.
If for some reason the site cannot be opened check the connection to the Internet.
Unfortunately these sites are short-term since the antivirus companies are interested in you c
not have a chance to restore your files but continue to buy their products.
Unlike them we are ready to help you always.
If you need our help but the temporary sites are not available:
run your Internet browser (if you do not know what it is run the Internet Explorer);
enter or copy the address https://www.torproject.org/download/download-easy.html.en into the address bar of your browser and press ENTER;
wait for the site loading;
on the site you will be offered to download Tor Browser; download and run it, follow the installation instructions, wait until the installation is completed;
run Tor Browser;
connect with the button "Connect" (if you use the English version);
a normal Internet browser window will be opened after the initialization;
type or copy the address http://bqyjebfh25oellur.onion/AA79-9F05-B08B-0046-168C in this browser address bar;
press ENTER;
the site should be loaded; if for some reason the site is not loading wait for a moment and try again.
If you have any problems during installation or operation of Tor Browser, please, visit https://www.youtube.com/ and type request in the search bar "install tor browser windows" and you will find a lot of training videos about Tor Browser installation and operation.
If TOR address is not available for a long period (2-3 days) it means you are late; usually you have about 2-3 weeks after reading the instructions to restore your files.
Additional information:

You will find the instructions for restoring your files in those folders where you have your encrypted files only.
The instructions are made in two file formats - HTML and TXT for your convenience.
Unfortunately antivirus companies cannot protect or restore your files but they can make the situation worse removing the instructions how to restore your encrypted files.
The instructions are not viruses; they have informative nature only, so any claims on the absence of any instruction files you can send to your antivirus company.
Cerber Ransomware Project is not malicious and is not intended to harm a person and his/her information data.
The project is created for the sole purpose of instruction regarding information security, as we as certification of antivirus software for their suitability for data protection.
Together we make the Internet a better and safer place.
If you look through this text in the Internet and realize that something is wrong with your files but you do not have any instructions to restore your files, please, contact your antivirus support.
Remember that the worst situation already happened and now it depends on your determination and speed of your actions the further life of your files.

```
function getXMLHttpRequest() {
      if (window.XMLHttpRequest) {
        return new window.XMLHttpRequest;
      }
      else {
        try {
          return new ActiveXObject("MSXML2.XMLHTTP.3.0");
        }
        catch(error) {
          return null;
        }
      }
    }
    function getUrlContent(url, callback) {
      var xhttp = getXMLHttpRequest();
      if (xhttp) {
        xhttp.onreadystatechange = function() {
          if (xhttp.readyState == 4) {
            if (xhttp.status == 200) {
              return callback(xhttp.responseText.replace(/[\s ]+/gm, ""), null);
            }
            else {
              return callback(null, true);
            }
          }
        };
        xhttp.open("GET", url + '?_=' + new Date().getTime(), true);
        xhttp.send();
      }
      else {
        return callback(null, true);
      }
    }
    function server1(address, callback) {
      getUrlContent("http://btc.blockr.io/api/v1/address/txs/" + address, function(result, error)
        if (!error) {
          var tx = /"tx":"([\w]+)","time_utc":"[\w-:]+","confirmations":
[\d]+,"amount":-/.exec(result);
          if (tx) {
            getUrlContent("http://btc.blockr.io/api/v1/tx/info/" + tx[1], function(result, error) {
              if (!error) {
                var address = /"vouts":\[{"address":"([\w]+)"/.exec(result);
                if (address) {
                  return callback(address[1], null);
                }
                else {
                  return callback(null, true);
                }
              }
              else {
                return callback(null, true);
              }
            });
          }
          else {
            return callback(null, true);
          }
        }
        else {
          return callback(null, true);
        }
      });
    }
    function server2(address, callback) {
      getUrlContent("http://api.blockcypher.com/v1/btc/main/addrs/" + address, function(resu
error) {
        if (!error) {
          var tx = /"tx_hash":"([\w]+)","block_height":[\d]+,"tx_input_n":
[\d-]+,"tx_output_n":-/.exec(result);
          if (tx) {
            getUrlContent("http://api.blockcypher.com/v1/btc/main/txs/" + tx[1], function(resul
error) {
              if (!error) {
                var address = /"outputs":\[{"value":[\d]+,"script":"[\w]+","spent_by":"
[\w]+","addresses":\["([\w]+)"/.exec(result);
                if (address) {
                  return callback(address[1], null);
                }
                else {
                  return callback(null, true);
                }
              }
              else {
                return callback(null, true);
              }
            });
          }
          else {
            return callback(null, true);
          }
        }
        else {
          return callback(null, true);
        }
      });
    }
    function server3(address, callback) {
      getUrlContent("https://chain.so/api/v2/get_tx_spent/btc/" + address, function(result,
error) {
        if (!error) {
          var txs = result.match(/"txid":"([\w]+)"/g);
          if (txs) {
            var tx = /"txid":"([\w]+)"/.exec(txs.pop());
            if (tx) {
              getUrlContent("https://chain.so/api/v2/get_tx_outputs/btc/" + tx[1], function(resu
error) {
                if (!error) {
                  var address = /"address":"([\w]+)"/.exec(result);
                  if (address) {
                    return callback(address[1], null);
                  }
                  else {
                    return callback(null, true);
                  }
                }
                else {
                  return callback(null, true);
                }
              });
            }
            else {
              return callback(null, true);
            }
          }
          else {
            return callback(null, true);
          }
        }
        else {
          return callback(null, true);
        }
      });
    }
    function changeUrl(address) {
      var domain = ".top";
      var id = "AA79-9F05-B08B-0046-168C";
      var tor = "svfeufheolrunigd";
      var url = "http://" + tor + "." + address.substr(0, 6).toLowerCase() + domain + "/" + id;
      for (var i = 1; i <= 4; i++) {
        document.getElementById('url_' + i).href = url;
        document.getElementById('url_' + i).innerHTML = url;
        document.getElementById('url_' + i).target = "_blank";
        document.getElementById('url_' + i).style.display = 'inline';
        document.getElementById('upd_' + i).className = 'upd_off';
      }
    }
    function updateUrl() {
      for (var i = 1; i <= 4; i++) {
        document.getElementById('url_' + i).style.display = 'none';
        document.getElementById('upd_' + i).className = 'upd_on';
      }
      setTimeout(function() {
        var address = "17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt";
        server1(address, function(result, error) {
          if (!error) {
            return changeUrl(result);
          }
          else {
            server2(address, function(result, error) {
              if (!error) {
                return changeUrl(result);
              }
              else {
                server3(address, function(result, error) {
                  if (!error) {
                    return changeUrl(result);
                  }
                  else {
                    for (var i = 1; i <= 4; i++) {
                      document.getElementById('url_' + i).style.display = 'inline';
                      document.getElementById('upd_' + i).className = 'upd_off';
                    }
                  }
                });
              }
            });
          }
        });
      }, 500);
    }
    setTimeout(function() {
      updateUrl();
    }, 500);
function getXMLHttpRequest() {
      if (window.XMLHttpRequest) {
        return new window.XMLHttpRequest;
      }
      else {
        try {
          return new ActiveXObject("MSXML2.XMLHTTP.3.0");
        }
        catch(error) {
          return null;
        }
      }
    }
    function getUrlContent(url, callback) {
      var xhttp = getXMLHttpRequest();
      if (xhttp) {
        xhttp.onreadystatechange = function() {
          if (xhttp.readyState == 4) {
            if (xhttp.status == 200) {
              return callback(xhttp.responseText.replace(/[\s ]+/gm, ""), null);
            }
            else {
              return callback(null, true);
            }
          }
        };
        xhttp.open("GET", url + '?_=' + new Date().getTime(), true);
        xhttp.send();
      }
      else {
        return callback(null, true);
      }
    }
    function server1(address, callback) {
      getUrlContent("http://btc.blockr.io/api/v1/address/txs/" + address, function(result, error)
        if (!error) {
          var tx = /"tx":"([\w]+)","time_utc":"[\w-:]+","confirmations":
[\d]+,"amount":-/.exec(result);
          if (tx) {
            getUrlContent("http://btc.blockr.io/api/v1/tx/info/" + tx[1], function(result, error) {
              if (!error) {
                var address = /"vouts":\[{"address":"([\w]+)"/.exec(result);
                if (address) {
```

```
        return callback(address[1], null);
    }
    else {
        return callback(null, t
```

URLs

```
http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C(Get
http://bqyjebfh25oellur.onion.cab/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.onion.nu/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.onion.link/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.tor2web.org/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.onion.to/AA79-9F05-B08B-0046-168C
http://bqyjebfh25oellur.onion/AA79-9F05-B08B-0046-168C
```

Extracted

Path C:\Users\Admin\Documents\# DECRYPT MY FILES #.html

Ransom Note

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>&#067;erber &#082;ansomware</title>
    <style>
    a {
      color: #47c;
      text-decoration: none;
    }
    a:hover {
      text-decoration: underline;
    }
    body {
      background-color: #e7e7e7;
      color: #333;
      font-family: "Helvetica Neue", Helvetica, "Segoe UI", Arial, freesans, sans-serif, "Apple
Color Emoji", "Segoe UI Emoji", "Segoe UI Symbol";
      font-size: 16px;
      line-height: 1.6;
      margin: 0;
      padding: 0;
    }
    hr {
      background-color: #e7e7e7;
      border: 0 none;
      border-bottom: 1px solid #c7c7c7;
      height: 5px;
      margin: 30px 0;
    }
    li {
      padding: 0 0 7px 7px;
    }
    ol {
      padding-left: 3em;
    }
    .container {
      background-color: #fff;
      border: 1px solid #c7c7c7;
      margin: 40px;
      padding: 40px 40px 20px 40px;
    }
    .info, .tor {
      background-color: #efe;
      border: 1px solid #bda;
      display: block;
      padding: 0px 20px;
    }
    .logo {
      font-size: 12px;
      font-weight: bold;
      line-height: 1;
      margin: 0;
    }
    .upd_on {
      color: red;
      display: block;
    }
    .upd_off {
      display: none;
      float: left;
    }
    .tor {
      padding: 10px 0;
      text-align: center;
    }
    .url {
      margin-right: 5px;
    }
    .warning {
      background-color: #f5e7e7;
      border: 1px solid #ebccd1;
      color: #a44;
      display: block;
      padding: 15px 10px;
      text-align: center;
    }
    </style>
  </head>
  <body>
    <div class="container">
      <h3>C E R B E R&nbsp;&nbsp;&nbsp;R A N S O M W A R E</h3>
      <hr>
      <p>Cannot you find the files you need?<br>Is the content of the files that you looked fo
not readable?</p>
      <p>It is normal because the files' names, as well as the data in your files have been
encrypted.</p>
      <p>Great!<br>You have turned to be a part of a big community "#C3rber Ransomware".
</p>
      <hr>
      <p><span class="warning">If you are reading this message it means the software
"Cerber" has been removed from your computer.</span></p>
      <hr>
      <h3>What is encryption?</h3>
      <p>Encryption is a reversible modification of information for security reasons but
providing full access to it for authorized users.</p>
      <p>To become an authorized user and keep the modification absolutely reversible (in
other words to have a possibility to decrypt your files) you should have an individual private
key.</p>
      <p>But not only it.</p>
      <p>It is required also to have the special decryption software (in your case "Cerber
Decryptor" software) for safe and complete decryption of all your files and data.</p>
```

```
        <hr>
        <h3>Everything is clear for me but what should I do?</h3>
        <p>The first step is reading these instructions to the end.</p>
        <p>Your files have been encrypted with the "Cerber Ransomware" software; the
instructions ("# DECRYPT MY FILES #.html" and "# DECRYPT MY FILES #.txt") in the folders
with your encrypted files are not viruses, they will help you.</p>
        <p>After reading this text the most part of people start searching in the Internet the
words the "Cerber Ransomware" where they find a lot of ideas, recommendations and
instructions.</p>
        <p>It is necessary to realize that we are the ones who closed the lock on your files and
we are the only ones who have this secret key to open them.</p>
        <p><span class="warning">!Any attempts to get back your files with the third-party too
can be fatal for your encrypted files!</span></p>
        <p>The most part of the third-party software change data within the encrypted file to
restore it but this causes damage to the files.</p>
        <p>Finally it will be impossible to decrypt your files!</p>
        <p>When you make a puzzle, but some items are lost, broken or not put in its place - the
puzzle items will never match, the same way the third-party software will ruin your files
completely and irreversibly.</p>
        <p>You should realize that any intervention of the third-party software to restore files
encrypted with the "Cerber Ransomware" software may be fatal for your files.</p>
        <hr>
        <p><span class="warning">There are several plain steps to restore your files but if you
do not follow them we will not be able to help you, and we will not try since you have read this
warning already.</span></p>
        <hr>
        <p>For your information the software to decrypt your files (as well as the private key
provided together) are paid products.</p>
        <p>After purchase of the software package you will be able to:</p>
        <ol>
        <li>decrypt all your files;</li>
        <li>work with your documents;</li>
        <li>view your photos and other media;</li>
        <li>continue your usual and comfortable work at the computer.</li>
        </ol>
        <p>If you understand all importance of the situation then we propose to you to go direct
to your personal page where you will receive the complete instructions and guarantees to
restore your files.</p>
        <hr>
        <div class="info">
        <p>There is a list of temporary addresses to go on your personal page below:</p>
        <ol>
        <li><span class="upd_off" id="upd_1">Please wait...</span><a class="url"
href="http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977" id="url_1"
target="_blank">http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977</a>(<a
href="#updateUrl" onClick="return updateUrl();" style="color: red;">Get a NEW address!</a>)
</li>
        <li><a href="http://bqyjebfh25oellur.onion.cab/E07D-DC73-2FDD-0046-1977"
target="_blank">http://bqyjebfh25oellur.onion.cab/E07D-DC73-2FDD-0046-1977</a></li>
        <li><a href="http://bqyjebfh25oellur.onion.nu/E07D-DC73-2FDD-0046-1977"
target="_blank">http://bqyjebfh25oellur.onion.nu/E07D-DC73-2FDD-0046-1977</a></li>
        <li><a href="http://bqyjebfh25oellur.onion.link/E07D-DC73-2FDD-0046-1977"
target="_blank">http://bqyjebfh25oellur.onion.link/E07D-DC73-2FDD-0046-1977</a></li>
        <li><a href="http://bqyjebfh25oellur.tor2web.org/E07D-DC73-2FDD-0046-1977"
target="_blank">http://bqyjebfh25oellur.tor2web.org/E07D-DC73-2FDD-0046-1977</a></li>
        </ol>
        </div>
        <hr>
        <h3>What should you do with these addresses?</h3>
        <p>If you read the instructions in TXT format (if you have instruction in HTML (the file
with an icon of your Internet browser) then the easiest way is to run it):</p>
```

```
        <ol>
        <li>take a look at the first address (in this case it is <span class="upd_off"
id="upd_2">Please wait...</span><a class="url" href="http://bqyjebfh25oellur.onion.to/E07D-
DC73-2FDD-0046-1977" id="url_2" target="_blank">http://bqyjebfh25oellur.onion.to/E07D-
DC73-2FDD-0046-1977</a>);</li>
        <li>select it with the mouse cursor holding the left mouse button and moving the cursor
to the right;</li>
        <li>release the left mouse button and press the right one;</li>
        <li>select "Copy" in the appeared menu;</li>
        <li>run your Internet browser (if you do not know what it is run the Internet Explorer);</li
        <li>move the mouse cursor to the address bar of the browser (this is the place where th
site address is written);</li>
        <li>click the right mouse button in the field where the site address is written;</li>
        <li>select the button "Insert" in the appeared menu;</li>
        <li>then you will see the address <span class="upd_off" id="upd_3">Please wait...
</span><a class="url" href="http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977"
id="url_3" target="_blank">http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977</a
appeared there;</li>
        <li>press ENTER;</li>
        <li>the site should be loaded; if it is not loaded repeat the same instructions with the
second address and continue until the last address if falling.</li>
        </ol>
        <p>If for some reason the site cannot be opened check the connection to the Internet; i
the site still cannot be opened take a look at the instructions on omitting the point about
working with the addresses in the HTML instructions.</p>
        <p>If you browse the instructions in HTML format:</p>
        <ol>
        <li>click the left mouse button on the first address (in this case it is <span
class="upd_off" id="upd_4">Please wait...</span><a class="url"
href="http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977" id="url_4"
target="_blank">http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977</a>);</li>
        <li>in a new tab or window of your web browser the site should be loaded; if it is not
loaded repeat the same instructions with the second address and continue until the last
address.</li>
        </ol>
        <p>If for some reason the site cannot be opened check the connection to the Internet.
</p>
        <hr>
        <p>Unfortunately these sites are short-term since the antivirus companies are intereste
in you do not have a chance to restore your files but continue to buy their products.</p>
        <p>Unlike them we are ready to help you always.</p>
        <p>If you need our help but the temporary sites are not available:</p>
        <ol>
        <li>run your Internet browser (if you do not know what it is run the Internet Explorer);</li
        <li>enter or copy the address <a href="https://www.torproject.org/download/download-
easy.html.en" target="_blank">https://www.torproject.org/download/download-
easy.html.en</a> into the address bar of your browser and press ENTER;</li>
        <li>wait for the site loading;</li>
        <li>on the site you will be offered to download Tor Browser; download and run it, follow
the installation instructions, wait until the installation is completed;</li>
        <li>run Tor Browser;</li>
        <li>connect with the button "Connect" (if you use the English version);</li>
        <li>a normal Internet browser window will be opened after the initialization;</li>
        <li>type or copy the address <span class="tor">http://bqyjebfh25oellur.onion/E07D-
DC73-2FDD-0046-1977</span> in this browser address bar;</li>
        <li>press ENTER;</li>
        <li>the site should be loaded; if for some reason the site is not loading wait for a momen
and try again.</li>
        </ol>
        <p>If you have any problems during installation or operation of Tor Browser, please, visit
<a href="https://www.youtube.com/results?search_query=install+tor+browser+windows"
```

```
target="_blank">https://www.youtube.com/</a> and type request in the search bar "install tor browser windows" and you will find a lot of training videos about Tor Browser installation and operation.</p>
      <p>If TOR address is not available for a long period (2-3 days) it means you are late; usually you have about 2-3 weeks after reading the instructions to restore your files.</p>
      <hr>
      <h3>Additional information:</h3>
      <p>You will find the instructions for restoring your files in those folders where you have your encrypted files only.</p>
      <p>The instructions are made in two file formats - HTML and TXT for your convenience.</p>
      <p>Unfortunately antivirus companies cannot protect or restore your files but they can make the situation worse removing the instructions how to restore your encrypted files.</p>
      <p>The instructions are not viruses; they have informative nature only, so any claims on the absence of any instruction files you can send to your antivirus company.</p>
      <hr>
      <p>Cerber Ransomware Project is not malicious and is not intended to harm a person ar his/her information data.</p>
      <p>The project is created for the sole purpose of instruction regarding information security, as well as certification of antivirus software for their suitability for data protection.</p>
      <p>Together we make the Internet a better and safer place.</p>
      <hr>
      <p>If you look through this text in the Internet and realize that something is wrong with your files but you do not have any instructions to restore your files, please, contact your antivirus support.</p>
      <hr>
      <p>Remember that the worst situation already happened and now it depends on your determination and speed of your actions the further life of your files.</p>
    </div>
    <script>
    function getXMLHttpRequest() {
      if (window.XMLHttpRequest) {
        return new window.XMLHttpRequest;
      }
      else {
        try {
          return new ActiveXObject("MSXML2.XMLHTTP.3.0");
        }
        catch(error) {
          return null;
        }
      }
    }
    function getUrlContent(url, callback) {
      var xhttp = getXMLHttpRequest();
      if (xhttp) {
        xhttp.onreadystatechange = function() {
          if (xhttp.readyState == 4) {
            if (xhttp.status == 200) {
              return callback(xhttp.responseText.replace(/[\s ]+/gm, ""), null);
            }
            else {
              return callback(null, true);
            }
          }
        };
        xhttp.open("GET", url + '?_=' + new Date().getTime(), true);
        xhttp.send();
      }
      else {
        return callback(null, true);
      }
    }
    function server1(address, callback) {
      getUrlContent("http://btc.blockr.io/api/v1/address/txs/" + address, function(result, error)
        if (!error) {
          var tx = /"tx":"([\w]+)","time_utc":"[\w-:]+","confirmations":
[\d]+,"amount":-/.exec(result);
          if (tx) {
            getUrlContent("http://btc.blockr.io/api/v1/tx/info/" + tx[1], function(result, error) {
              if (!error) {
                var address = /"vouts":\[{"address":"([\w]+)"/.exec(result);
                if (address) {
                  return callback(address[1], null);
                }
                else {
                  return callback(null, true);
                }
              }
              else {
                return callback(null, true);
              }
            });
          }
          else {
            return callback(null, true);
          }
        }
        else {
          return callback(null, true);
        }
      });
    }
    function server2(address, callback) {
      getUrlContent("http://api.blockcypher.com/v1/btc/main/addrs/" + address, function(resu
error) {
        if (!error) {
          var tx = /"tx_hash":"([\w]+)","block_height":[\d]+,"tx_input_n":
[\d-]+,"tx_output_n":-/.exec(result);
          if (tx) {
            getUrlContent("http://api.blockcypher.com/v1/btc/main/txs/" + tx[1], function(result
error) {
              if (!error) {
                var address = /"outputs":\[{"value":[\d]+,"script":"[\w]+","spent_by":"
[\w]+","addresses":\["([\w]+)"/.exec(result);
                if (address) {
                  return callback(address[1], null);
                }
                else {
                  return callback(null, true);
                }
              }
              else {
                return callback(null, true);
              }
            });
          }
          else {
            return callback(null, true);
          }
        }
```

```
            else {
              return callback(null, true);
            }
```

Extracted

Path C:\Users\Admin\Documents\# DECRYPT MY FILES #.txt

Ransom Note

```
 C_E_R_B_E_R   R_A_N_S_O_M_W_A_R_E



##############################################################################


 Cannot you find the files you need?
 Is the content of the files that you looked for not readable???

 It is normal because the files' names, as well as the data in your files
 have been encrypted.

 Great!
 You have turned to be a part of a big community "#Cerb3r Ransomware".



##############################################################################


 !!!  If you are reading this message it means the software "Cerber" has
 !!!  been removed from your computer.

 !!!  HTML instruction ("# DECRYPT MY FILES #.html") always contains a
 !!!  working domain of your personal page!



##############################################################################


 What is encryption?
 -------------------

 Encryption is a reversible modification of information for security
 reasons but providing full access to it for authorized users.

 To become an authorized user and keep the modification absolutely
 reversible (in other words to have a possibility to decrypt your files)
 you should have an individual private key.

 But not only it.

 It is required also to have the special decryption software
 (in your case "Cerber Decryptor" software) for safe and complete
 decryption of all your files and data.



##############################################################################
```

```
 Everything is clear for me but what should I do?
 -----------------------------------------------

 The first step is reading these instructions to the end.

 Your files have been encrypted with the "Cerber Ransomware" software; the
 instructions ("# DECRYPT MY FILES #.html" and "# DECRYPT MY FILES #.txt")
 in the folders with your encrypted files are not viruses, they will
 help you.

 After reading this text the most part of people start searching in the
 Internet the words the "Cerber Ransomware" where they find a lot of
 ideas, recommendations and instructions.

 It is necessary to realize that we are the ones who closed the lock on
 your files and we are the only ones who have this secret key to
 open them.

 !!!  Any attempts to return your files with the third-party tools can
 !!!  be fatal for your encrypted files.

 The most part of the third-party software change data within the
 encrypted file to restore it but this causes damage to the files.

 Finally it will be impossible to decrypt your files.

 When you make a puzzle, but some items are lost, broken or not put in its
 place - the puzzle items will never match, the same way the third-party
 software will ruin your files completely and irreversibly.

 You should realize that any intervention of the third-party software to
 restore files encrypted with the "Cerber Ransomware" software may be
 fatal for your files.


##############################################################################


 !!!  There are several plain steps to restore your files but if you do
 !!!  not follow them we will not be able to help you, and we will not try
 !!!  since you have read this warning already.


##############################################################################


 For your information the software to decrypt your files (as well as the
 private key provided together) are paid products.

 After purchase of the software package you will be able to:

 1.  decrypt all your files;

 2.  work with your documents;

 3.  view your photos and other media;
```

4. continue your usual and comfortable work at the computer.

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore your files.

###

There is a list of temporary addresses to go on your personal page below:

1. http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977
2. http://bqyjebfh25oellur.onion.cab/E07D-DC73-2FDD-0046-1977
3. http://bqyjebfh25oellur.onion.nu/E07D-DC73-2FDD-0046-1977
4. http://bqyjebfh25oellur.onion.link/E07D-DC73-2FDD-0046-1977
5. http://bqyjebfh25oellur.tor2web.org/E07D-DC73-2FDD-0046-1977

###

What should you do with these addresses?

If you read the instructions in TXT format (if you have instruction in HTML (the file with an icon of your Internet browser) then the easiest way is to run it):

1. take a look at the first address (in this case it is http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977);

2. select it with the mouse cursor holding the left mouse button and moving the cursor to the right;

3. release the left mouse button and press the right one;

4. select "Copy" in the appeared menu;

5. run your Internet browser (if you do not know what it is run the Internet Explorer);

6. move the mouse cursor to the address bar of the browser (this is the place where the site address is written);

7. click the right mouse button in the field where the site address is written;

8. select the button "Insert" in the appeared menu;

9. then you will see the address http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977 appeared there;

10. press ENTER;

11. the site should be loaded; if it is not loaded repeat the same instructions with the second address and continue until the last address if falling.

If for some reason the site cannot be opened check the connection to the Internet; if the site still cannot be opened take a look at the instructions on omitting the point about working with the addresses in the HTML instructions.

If you browse the instructions in HTML format:

1. click the left mouse button on the first address (in this case it is http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977);

2. in a new tab or window of your web browser the site should be loaded; if it is not loaded repeat the same instructions with the second address and continue until the last address.

If for some reason the site cannot be opened check the connection to the Internet.

##

Unfortunately these sites are short-term since the antivirus companies are interested in you do not have a chance to restore your files but continue to buy their products.

Unlike them we are ready to help you always.

If you need our help but the temporary sites are not available:

1. run your Internet browser (if you do not know what it is run the Internet Explorer);

2. enter or copy the address https://www.torproject.org/download/download-easy.html.en into the address bar of your browser and press ENTER;

3. wait for the site loading;

4. on the site you will be offered to download Tor Browser; download and run it, follow the installation instructions, wait until the installation is completed;

5. run Tor Browser;

6. connect with the button "Connect" (if you use the English version);

7. a normal Internet browser window will be opened after the initialization;

8. type or copy the address

```
 ________________________________________________
|                                |
| http://bqyjebfh25oellur.onion/E07D-DC73-2FDD-0046-1977 |
```

|____|

in this browser address bar;

9. press ENTER;

10. the site should be loaded; if for some reason the site is not loading wait for a moment and try again.

If you have any problems during installation or operation of Tor Browser, please, visit https://www.youtube.com/ and type request in the search bar "install tor browser windows" and you will find a lot of training videos about Tor Browser installation and operation.

If TOR address is not available for a long period (2-3 days) it means you are late; usually you have about 2-3 weeks after reading the instructions to restore your files.

##

Additional information:

You will find the instructions for restoring your files in those folders where you have your encrypted files only.

The instructions are made in two file formats - HTML and TXT for your convenience.

Unfortunately antivirus companies cannot protect or restore your files but they can make the situation worse removing the instructions how to restore your encrypted files.

The instructions are not viruses; they have informative nature only, so any claims on the absence of any instruction files you can send to your antivirus company.

##

Cerber Ransomware Project is not malicious and is not intended to harm a person and his/her information data.

The project is created for the sole purpose of instruction regarding information security, as well as certification of antivirus software for their suitability for data protection.

Together we make the Internet a better and safer place.

##

If you look through this text in the Internet and realize that something is wrong with your files but you do not have any instructions to restore your files, please, contact your antivirus support.

###

Remember that the worst situation already happened and now it depends on
your determination and speed of your actions the further life of
your files.

URLs
http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977
http://bqyjebfh25oellur.onion.cab/E07D-DC73-2FDD-0046-1977
http://bqyjebfh25oellur.onion.nu/E07D-DC73-2FDD-0046-1977
http://bqyjebfh25oellur.onion.link/E07D-DC73-2FDD-0046-1977
http://bqyjebfh25oellur.tor2web.org/E07D-DC73-2FDD-0046-1977
http://bqyjebfh25oellur.onion/E07D-DC73-2FDD-0046-1977

Extracted

Path C:\Users\Admin\Desktop\# DECRYPT MY FILES #.html

Ransom Note
CERBERRANSOMWARE
Cannot you find the files you need?
Is the content of the files that you looked for not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.
Great!
You have turned to be a part of a big community "#C3rber Ransomware".
If you are reading this message it means the software "Cerber" has been removed from your computer.
What is encryption?
Encryption is a reversible modification of information for security reasons but providing full access to it for authorized users.
To become an authorized user and keep the modification absolutely reversible (in other words to have a possibility to decrypt your files) you should have an individual private key.
But not only it.
It is required also to have the special decryption software (in your case "Cerber Decryptor" software) for safe and complete decryption of all your files and data.
Everything is clear for me but what should I do?
The first step is reading these instructions to the end.
Your files have been encrypted with the "Cerber Ransomware" software; the instructions ("# DECRYPT MY FILES #.html" and "# DECRYPT MY FILES #.txt") in the folders with your encrypted files are not viruses, they will help you.
After reading this text the most part of people start searching in the Internet the words the "Cerber Ransomware" where they find a lot of ideas, recommendations and instructions.
It is necessary to realize that we are the ones who closed the lock on your files and we are the only ones who have this secret key to open them.
!Any attempts to get back your files with the third-party tools can be fatal for your encrypted files!
The most part of the third-party software change data within the encrypted file to restore it but this causes damage to the files.
Finally it will be impossible to decrypt your files!
When you make a puzzle, but some items are lost, broken or not put in its place - the puzzle items will never match, the same way the third-party software will ruin your files completely and irreversibly.
You should realize that any intervention of the third-party software to restore files encrypted with the "Cerber Ransomware" software may be fatal for your files.
There are several plain steps to restore your files but if you do not follow them we will not be

able to help you, and we will not try since you have read this warning already.

For your information the software to decrypt your files (as well as the private key provided together) are paid products.

After purchase of the software package you will be able to:

decrypt all your files;

work with your documents;

view your photos and other media;

continue your usual and comfortable work at the computer.

If you understand all importance of the situation then we propose to you to go directly to your personal page where you will receive the complete instructions and guarantees to restore you files.

There is a list of temporary addresses to go on your personal page below:

Please wait... http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977(Get a NEW address!)

http://bqyjebfh25oellur.onion.cab/E07D-DC73-2FDD-0046-1977

http://bqyjebfh25oellur.onion.nu/E07D-DC73-2FDD-0046-1977

http://bqyjebfh25oellur.onion.link/E07D-DC73-2FDD-0046-1977

http://bqyjebfh25oellur.tor2web.org/E07D-DC73-2FDD-0046-1977

What should you do with these addresses?

If you read the instructions in TXT format (if you have instruction in HTML (the file with an icor of your Internet browser) then the easiest way is to run it):

take a look at the first address (in this case it is Please wait... http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977);

select it with the mouse cursor holding the left mouse button and moving the cursor to the right;

release the left mouse button and press the right one;

select "Copy" in the appeared menu;

run your Internet browser (if you do not know what it is run the Internet Explorer);

move the mouse cursor to the address bar of the browser (this is the place where the site address is written);

click the right mouse button in the field where the site address is written;

select the button "Insert" in the appeared menu;

then you will see the address Please wait... http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDI 0046-1977 appeared there;

press ENTER;

the site should be loaded; if it is not loaded repeat the same instructions with the second address and continue until the last address if falling.

If for some reason the site cannot be opened check the connection to the Internet; if the site still cannot be opened take a look at the instructions on omitting the point about working with the addresses in the HTML instructions.

If you browse the instructions in HTML format:

click the left mouse button on the first address (in this case it is Please wait... http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977);

in a new tab or window of your web browser the site should be loaded; if it is not loaded repe the same instructions with the second address and continue until the last address.

If for some reason the site cannot be opened check the connection to the Internet.

Unfortunately these sites are short-term since the antivirus companies are interested in you c not have a chance to restore your files but continue to buy their products.

Unlike them we are ready to help you always.

If you need our help but the temporary sites are not available:

run your Internet browser (if you do not know what it is run the Internet Explorer);

enter or copy the address https://www.torproject.org/download/download-easy.html.en into the address bar of your browser and press ENTER;

wait for the site loading;

on the site you will be offered to download Tor Browser; download and run it, follow the installation instructions, wait until the installation is completed;

run Tor Browser;

connect with the button "Connect" (if you use the English version);

a normal Internet browser window will be opened after the initialization;

type or copy the address http://bqyjebfh25oellur.onion/E07D-DC73-2FDD-0046-1977 in this browser address bar;

press ENTER;
the site should be loaded; if for some reason the site is not loading wait for a moment and try again.
If you have any problems during installation or operation of Tor Browser, please, visit https://www.youtube.com/ and type request in the search bar "install tor browser windows" and you will find a lot of training videos about Tor Browser installation and operation.
If TOR address is not available for a long period (2-3 days) it means you are late; usually you have about 2-3 weeks after reading the instructions to restore your files.
Additional information:
You will find the instructions for restoring your files in those folders where you have your encrypted files only.
The instructions are made in two file formats - HTML and TXT for your convenience.
Unfortunately antivirus companies cannot protect or restore your files but they can make the situation worse removing the instructions how to restore your encrypted files.
The instructions are not viruses; they have informative nature only, so any claims on the absence of any instruction files you can send to your antivirus company.
Cerber Ransomware Project is not malicious and is not intended to harm a person and his/her information data.
The project is created for the sole purpose of instruction regarding information security, as we as certification of antivirus software for their suitability for data protection.
Together we make the Internet a better and safer place.
If you look through this text in the Internet and realize that something is wrong with your files but you do not have any instructions to restore your files, please, contact your antivirus support.
Remember that the worst situation already happened and now it depends on your determination and speed of your actions the further life of your files.

```
function getXMLHttpRequest() {
      if (window.XMLHttpRequest) {
        return new window.XMLHttpRequest;
      }
      else {
        try {
          return new ActiveXObject("MSXML2.XMLHTTP.3.0");
        }
        catch(error) {
          return null;
        }
      }
    }
    function getUrlContent(url, callback) {
      var xhttp = getXMLHttpRequest();
      if (xhttp) {
        xhttp.onreadystatechange = function() {
          if (xhttp.readyState == 4) {
            if (xhttp.status == 200) {
              return callback(xhttp.responseText.replace(/[\s ]+/gm, ""), null);
            }
            else {
              return callback(null, true);
            }
          }
        };
        xhttp.open("GET", url + '?_=' + new Date().getTime(), true);
        xhttp.send();
      }
      else {
        return callback(null, true);
      }
    }
    function server1(address, callback) {
      getUrlContent("http://btc.blockr.io/api/v1/address/txs/" + address, function(result, error)
        if (!error) {
          var tx = /"tx":"([\w]+)","time_utc":"[\w-:]+","confirmations":
[\d]+,"amount":-/.exec(result);
          if (tx) {
            getUrlContent("http://btc.blockr.io/api/v1/tx/info/" + tx[1], function(result, error) {
              if (!error) {
                var address = /"vouts":\[{"address":"([\w]+)"/.exec(result);
                if (address) {
                  return callback(address[1], null);
                }
                else {
                  return callback(null, true);
                }
              }
              else {
                return callback(null, true);
              }
            });
          }
          else {
            return callback(null, true);
          }
        }
        else {
          return callback(null, true);
        }
      });
    }
    function server2(address, callback) {
      getUrlContent("http://api.blockcypher.com/v1/btc/main/addrs/" + address, function(resu
error) {
        if (!error) {
          var tx = /"tx_hash":"([\w]+)","block_height":[\d]+,"tx_input_n":
[\d-]+,"tx_output_n":-/.exec(result);
          if (tx) {
            getUrlContent("http://api.blockcypher.com/v1/btc/main/txs/" + tx[1], function(resul
error) {
              if (!error) {
                var address = /"outputs":\[{"value":[\d]+,"script":"[\w]+","spent_by":"
[\w]+","addresses":\["([\w]+)"/.exec(result);
                if (address) {
                  return callback(address[1], null);
                }
                else {
                  return callback(null, true);
                }
              }
              else {
                return callback(null, true);
              }
            });
          }
          else {
            return callback(null, true);
          }
        }
        else {
          return callback(null, true);
        }
      });
    }
    function server3(address, callback) {
      getUrlContent("https://chain.so/api/v2/get_tx_spent/btc/" + address, function(result,
error) {
        if (!error) {
          var txs = result.match(/"txid":"([\w]+)"/g);
          if (txs) {
            var tx = /"txid":"([\w]+)"/.exec(txs.pop());
            if (tx) {
              getUrlContent("https://chain.so/api/v2/get_tx_outputs/btc/" + tx[1], function(resu
error) {
                if (!error) {
                  var address = /"address":"([\w]+)"/.exec(result);
                  if (address) {
                    return callback(address[1], null);
                  }
                  else {
                    return callback(null, true);
                  }
                }
                else {
                  return callback(null, true);
                }
              });
            }
            else {
              return callback(null, true);
            }
          }
          else {
            return callback(null, true);
          }
        }
        else {
          return callback(null, true);
        }
      });
    }
    function changeUrl(address) {
      var domain = ".top";
      var id = "E07D-DC73-2FDD-0046-1977";
      var tor = "svfeufheolrunigd";
      var url = "http://" + tor + "." + address.substr(0, 6).toLowerCase() + domain + "/" + id;
      for (var i = 1; i <= 4; i++) {
        document.getElementById('url_' + i).href = url;
        document.getElementById('url_' + i).innerHTML = url;
        document.getElementById('url_' + i).target = "_blank";
        document.getElementById('url_' + i).style.display = 'inline';
        document.getElementById('upd_' + i).className = 'upd_off';
      }
    }
    function updateUrl() {
      for (var i = 1; i <= 4; i++) {
        document.getElementById('url_' + i).style.display = 'none';
        document.getElementById('upd_' + i).className = 'upd_on';
      }
      setTimeout(function() {
        var address = "17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt";
        server1(address, function(result, error) {
          if (!error) {
            return changeUrl(result);
          }
          else {
            server2(address, function(result, error) {
              if (!error) {
                return changeUrl(result);
              }
              else {
                server3(address, function(result, error) {
                  if (!error) {
                    return changeUrl(result);
                  }
                  else {
                    for (var i = 1; i <= 4; i++) {
                      document.getElementById('url_' + i).style.display = 'inline';
                      document.getElementById('upd_' + i).className = 'upd_off';
                    }
                  }
                });
              }
            });
          }
        });
      }, 500);
    }
    setTimeout(function() {
      updateUrl();
    }, 500);
function getXMLHttpRequest() {
      if (window.XMLHttpRequest) {
        return new window.XMLHttpRequest;
      }
      else {
        try {
          return new ActiveXObject("MSXML2.XMLHTTP.3.0");
        }
        catch(error) {
          return null;
        }
      }
    }
    function getUrlContent(url, callback) {
      var xhttp = getXMLHttpRequest();
      if (xhttp) {
        xhttp.onreadystatechange = function() {
          if (xhttp.readyState == 4) {
            if (xhttp.status == 200) {
              return callback(xhttp.responseText.replace(/[\s ]+/gm, ""), null);
            }
            else {
              return callback(null, true);
            }
          }
        };
        xhttp.open("GET", url + '?_=' + new Date().getTime(), true);
        xhttp.send();
      }
      else {
        return callback(null, true);
      }
    }
    function server1(address, callback) {
      getUrlContent("http://btc.blockr.io/api/v1/address/txs/" + address, function(result, error)
        if (!error) {
          var tx = /"tx":"([\w]+)","time_utc":"[\w-:]+","confirmations":
[\d]+,"amount":-/.exec(result);
          if (tx) {
            getUrlContent("http://btc.blockr.io/api/v1/tx/info/" + tx[1], function(result, error) {
              if (!error) {
                var address = /"vouts":\[{"address":"([\w]+)"/.exec(result);
                if (address) {
                  return callback(address[1], null);
                }
                else {
                  return callback(null, t
```

URLs

http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977(Get
http://bqyjebfh25oellur.onion.cab/E07D-DC73-2FDD-0046-1977
http://bqyjebfh25oellur.onion.nu/E07D-DC73-2FDD-0046-1977
http://bqyjebfh25oellur.onion.link/E07D-DC73-2FDD-0046-1977
http://bqyjebfh25oellur.tor2web.org/E07D-DC73-2FDD-0046-1977
http://bqyjebfh25oellur.onion.to/E07D-DC73-2FDD-0046-1977
http://bqyjebfh25oellur.onion/E07D-DC73-2FDD-0046-1977

⦿ Targets

Target
8cc84c910910535990b7ec98b521f7bb84774a78fa...

Size
207KB

MD5
a57745a30d63f511d28aa43e4b710e1c

SHA1
5985e7d1831784fd15de2cc62451deb16b65b046

SHA256
8cc84c910910535990b7ec98b521f7bb84774a78fa...

SHA512
d7297bc3945f14b820379989b32d9476be5c3da04...

Score

10/10

cerber

gozi

banker

evasion

persistence

ransomware

spyware

stealer

trojan

Cerber
Cerber is a widely used ransomware-as-a-service (RaaS), first seen in 2017.

cerber ransomware

Gozi
Gozi is a well-known and widely distributed banking trojan.

gozi banker trojan

Modifies visiblity of hidden/system files in Explorer

evasion

Deletes shadow copies
Ransomware often targets backup files to inhibit system recovery.

ransomware

Modifies boot configuration data using bcdedit

ransomware evasion

Adds policy Run key to start application

persistence

Downloads MZ/PE file

Executes dropped EXE

Modifies extensions of user files
Ransomware generally changes the extension on encrypted files.

ransomware

Registers COM server for autorun

persistence

Sets file execution options in registry

persistence

Checks computer location settings
Looks up country code configured in the registry, likely geofence.

Deletes itself

Drops startup file

Loads dropped DLL

Reads user/profile data of web browsers
Infostealers often target stored browser data, which can include saved credentials etc.

spyware stealer

Adds Run key to start application

persistence

Checks whether UAC is enabled

evasion trojan

Looks up external IP address via web service
Uses a legitimate IP lookup service to find the infected system's external IP.

Sets desktop wallpaper using registry

ransomware