SECTALKS
CTF 0x04 Solution

swarley, kronicd

May 22, 2014

0.1 START

We have a 128 byte file named 'key' and a 4 MB file named 'mail'. After messing around thinking the key was the actual AES encryption key kronicd realised it was the password.

From there it was a matter of stripping the mail headers from the mail file, and decrypting it with the keyfile.

```
swarley@Pro: openssl enc -d -aes-128-cbc -kfile key -in mail -out
    decrypt
```

Open decrypt in texteditor and strip the header and footer to leave a nice block of base64'd data (which is likely an mp4 given the name of the "attachment")

```
Content-Type: application/octet-stream
Content-Disposition: attachment; filename="W1EBFwEcSaQ.mp4"
Content-Transfer-Encoding: base64
```

Then it was a case of decoding the base64'd data into our mp4 file thusly:

```
swarley@Pro: base64 -D -i decrypt2 -o fuckyou.mp4
```

0.2 FIN

```
<flag>
flag: the radio is playing some sort of.. rick roll
</flag>
```

0.3 EDIT!

Seems the flag we got was only the beginning (I guess you can't assume "flag" means flag...)

So with our mp4 in hand the next step is to determine what information this guy had!

```
swarley@Pro: strings fuckyou.mp4
```

Figure 1: A mad wicked sick image of the man himself.

```
<output redacted>
...
verax/ops/02/01/statusPK
verax/ops/02/timelinePK
verax/ops/02/goalPK
```

```
verax/ops/02/02/PK
verax/ops/02/02/goalPK
verax/ops/02/02/statusPK
verax/ops/02/idPK
verax/ops/02/statusPK
verax/ops/03/PK
verax/ops/03/goalPK
verax/ops/03/idPK
verax/ops/03/statusPK
verax/contact.txtPK
verax/photo.jpgPK
```

Hmmm ok theres embedded files in this mp4. Whip out everyone's favourite tool (read: Nobody's favourite tool) FOREMOST (MADDD SICCKKKKK!!!)

```
swarley@Pro: foremost -i fuckyou.mp4 -o output/
```

Oh shit some pics and contact deets!

```
n: Edward Joseph Snowden
b: 1983-06-21
a: unknown
p: unknown
e: snowedin@sqweek.net
```

Some GOALS appeared (files were titled "goal"):

```
swarley@Pro: cat ops/*/goal

"Verax" has been communicating with media figures Glenn Greenwald
and Laura Poitras, if not others.

The goal of this operation is to discover who he is and what he
    knows
before it becomes a problem.
Capture Edward Snowden and return him to US soil.
Discredit Edward Snowden.
Locate Edward Snowden's Russian address.
```

There was loads of other cool stuff indicting the traitor Snowdenz for what he is (a traitor scumbag treason committing piece of socialist shit). mugshot.jpg had exif data including some sweet GPS locational coordination.

Figure 2: A guy who got himself snoweden (GET IT!?).

```
swarley@Pro: exiftool mugshot.jpg
<REDACTED STUPID SHIT>
...
Y Cb Cr Sub Sampling          : YCbCr4:2:0 (2 2)
GPS Latitude                 : 55 deg 50' 55.79" N
```

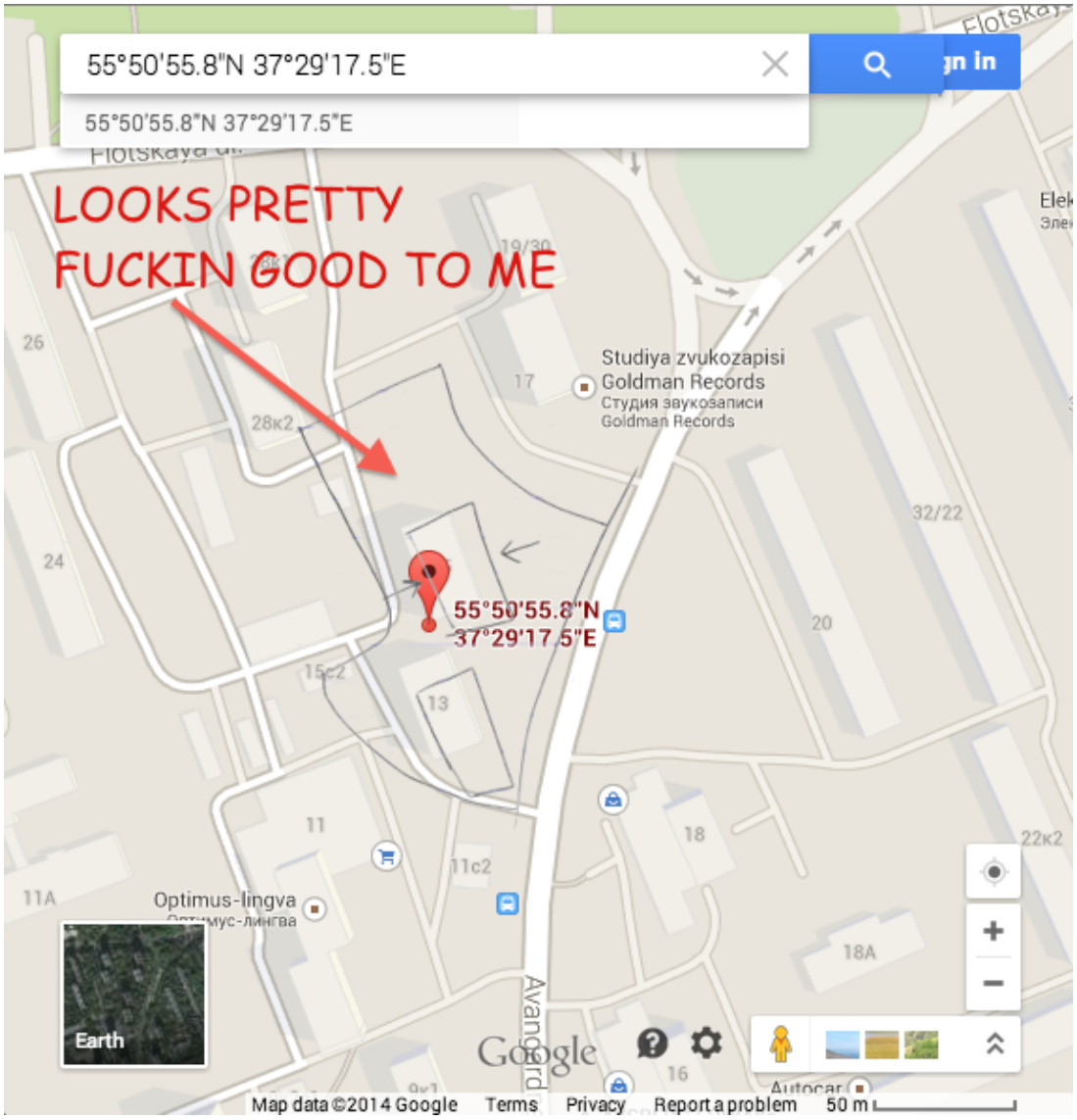

Figure 3: MAPPP MOTHERFUCKER

```
GPS Longitude                   : 37 deg 29' 17.46" E
GPS Position                    : 55 deg 50' 55.79" N, 37 deg 29'
    17.46" E
Image Size                      : 220x265
```

Chuck those coords into wolfram alpha and it takes you straight to the motherland. The coords seemed to align with the dodgy mudmap included in the same directory (map.jpg) - see Figure whatever it is.

I think the address is:

Room 2.11 STEP Mebel', IP Latunov s. B.
Avangardnaya ulitsa, 15
Moscow
Russia