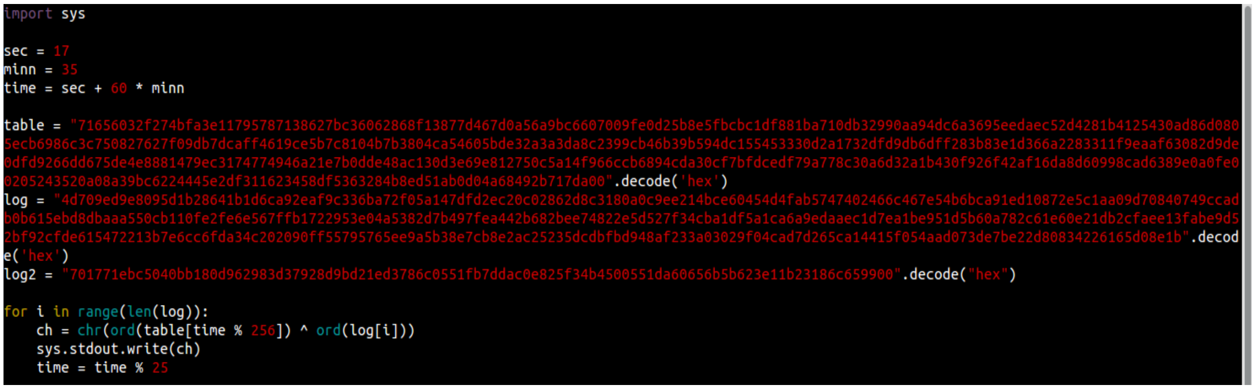
Keylogger (Operation M.E.M.)

I used the volatility framework [1] to extract the keylogger executable from the provided memory dump.

Following a static analysis of the executable with IDA, I managed to deduce the way it encoded the characters it captured, and decode the log file with the following script:



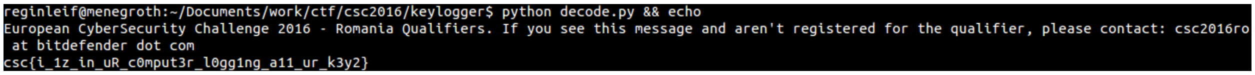
```
import sys

sec = 17
minn = 35
time = sec + 60 * minn

table = "71656032f274bfa3e11795787138627bc36062868f13877d467d0a56a9bc6607009fe0d25b8e5fbcbc1df881ba710db32990aa94dc6a3695eedaec52d4281b4125430ad86d080
5ecb6986c3c750827627f09db7dcaff4619ce5b7c8104b7b3804ca54605bde32a3a3da8c2399cb46b39b594dc155453330d2a1732dfd9db6dff283b83e1d366a2283311f9eaaf63082d9de
0dfd9266dd675de4e8881479ec3174774946a21e7b0dde48ac130d3e69e812750c5a14f966ccb6894cda30cf7bfdcedf79a778c30a6d32a1b430f926f42af16da8d60998cad6389e0a0fe0
0205243520a08a39bc6224445e2df311623458df5363284b8ed51ab0d04a68492b717da00".decode('hex')
log = "4d709ed9e8095d1b28641b1d6ca92eaf9c336ba72f05a147dfd2ec20c02862d8c3180a0c9ee214bce60454d4fab5747402466c467e54b6bca91ed10872e5c1aa09d70840749ccad
b0b615ebd8dbaaa550cb110fe2fe6e567ffb1722953e04a5382d7b497fea442b682bee74822e5d527f34cba1df5a1ca6a9edaaec1d7ea1be951d5b60a782c61e60e21db2cfaee13fabe9d5
2bf92cfde615472213b7e6cc6fda34c202090ff55795765ee9a5b38e7cb8e2ac25235dcdbfbd948af233a03029f04cad7d265ca14415f054aad073de7be22d80834226165d08e1b".decod
e('hex')
log2 = "701771ebc5040bb180d962983d37928d9bd21ed3786c0551fb7ddac0e825f34b4500551da60656b5b623e11b23186c659900".decode("hex")

for i in range(len(log)):
    ch = chr(ord(table[time % 256]) ^ ord(log[i]))
    sys.stdout.write(ch)
    time = time % 25
```

The parameters sec & min, that the executable used, I deduced from the file name of the log.



```
reginleif@menegroth:~/Documents/work/ctf/csc2016/keylogger$ python decode.py && echo
European CyberSecurity Challenge 2016 - Romania Qualifiers. If you see this message and aren't registered for the qualifier, please contact: csc2016ro
 at bitdefender dot com
csc{i_1z_in_uR_c0mput3r_l0gg1ng_a11_ur_k3y2}
```

[1] https://github.com/volatilityfoundation/volatility