# Quasar Chaos

Published: 2023-04-13 · Archived: 2026-04-05 23:08:11 UTC

```
import base64
import malduck
from Crypto.Protocol.KDF import PBKDF2




string_data = 'muoBJw7vz107HYcI4tyRBz0XVW2kCA367J52yCDjuHUkVGWPKkpXUgV5Q1/s4HNhSAMJDhTJwYIa3MxqdMkg7/

string_data_b64 = base64.b64decode(string_data)
string_data_b64 = string_data_b64[32:]
iv = string_data_b64[:16]
enc_data = string_data_b64[16:]

key_data = "SM73jcn259KtoJ4uPciZ"

iterations = 50000
salt = bytes([191,235,30,86,251,205,151,59,178,25,2,36,48,165,120,67,0,61,86,68,210,30,98,185,212,24

key = PBKDF2(key_data, salt, count=iterations)


strings = [
"3DaXS6MYqYL9Q/3WF/cPdbdoy2NggCqoSmasPYwzkPD389j4IoSZZVQHHz196cPEy2h4VSsjy7se22/++XH89w==",
"U2MkYAPUljFBQRO9iIkRZVGmxS2mOB+3klWr1xcKn3OqiosSod4C8iKk+GmogWRVZ6xUFktvHtwFnyOxg+ZSLPjbO+3+OdrVI8o
"1WvgEMPjdwfqIMeM9MclyQ==",
"NcFtjbDOcsw7Evd3coMC0y4koy/SRZGydhNmno81ZOWOvdfg7sv0Cj5ad2ROUfX4QMscAIjYJdjrrs41+qcQwg==",
"NX2L76Nud+1o8CF2fRs8qiHu4v2wb0E701jiqZNY+WP0X+oOZUuIpza8zsipPF550Uz4XlYTbeon9njxoQ2MBA==",
"DQSIoMapurAvRyZWC74v/c0E7zcV+8LgDPpOmChR453N+Cj+6Fwipe5tbYPbhkpNhwf9hEy/78hh8qB6c1B3nw==",
"p56HD6/EQvRGDzCuDAjko6aJqVPRc/Mug3q2bslOWAZN8H2n4vy8m3x0RtwAUXh5C6kG15y+qrvsfs2s4qJHQBdKg5BmNrg62Yn
"xf05S4o+UGg6gPS2slPSroORS4DLfYXnHiWz6VyhTQOpNKzIHxhEvDSTlPMFUIek3Wi3lCxroWOHJr9WeGvvHe6fxXcVPTWnPs4
"muoBJw7vz107HYcI4tyRBz0XVW2kCA367J52yCDjuHUkVGWPKkpXUgV5Q1/s4HNhSAMJDhTJwYIa3MxqdMkg7A==",
"B0T3cryizrl4VOcnw40TDxor8c5ycs9chw7RjsLxM2h+rS/BlcPa2ZW4po/PpJXob3byyEj4GOuWUPn+M4Shcg=="]


for s in strings:
    try:
        string_data_b64 = base64.b64decode(s)
        string_data_b64 = string_data_b64[32:]
```

```
        iv = string_data_b64[:16]
        enc_data = string_data_b64[16:]
        out = malduck.aes.cbc.decrypt(key, iv, enc_data)
        print(out)
    except:
        pass
```

---

Source: https://research.openanalysis.net/quasar/chaos/rat/ransomware/2023/04/13/quasar-chaos.html