Пытаемся найти вхождение строк в гидре, но их нет

Выходит, они зашифрованы, а значит, должны содержаться в некоторых разделах файла. Находим интересные строки в .rdata

```
                        s_65=34`z_140004440
140004440 36 35 3d          ds          "65=34`z"
          33 34 60
          7a 00
```

Идем в xref и ищем какая функция с ними взаимодействует. Находим xor 0x5a

```
  do {
    puVar1 = param_1;
    if (0xf < (ulonglong)param_1[3]) {
      puVar1 = (undefined8 *)*param_1;
    }
    *(byte *)((longlong)puVar1 + uVar2) = *(byte *)(uVar2 + param_2) ^ 0x5a;
    uVar2 = uVar2 + 1;
  } while (uVar2 < param_3);
}
```

Можно посимвольно расшифровать каждую строку и получить правильные имя пользователя и пароль

А так как программа в процессе работы их расшифровывает сама, то можно запустить её в x64dbg, поставить брейкпоинт по адресу 19e0 и посмотреть регистры

ПОСТФАКТУМ

Да, возникли сложности

Сначала я не мог найти вхождения строк, и только потом понял, что они скорее всего зашифрованы. Получилось найти, где записаны зашифрованные строки и где они используются, но все никак не мог найти функцию, где они расшифровываются. Посмотрел райтапы, понял, что искать. Но все равно не нашел. Смог вытащить логин и пароль через отладчик, но стало интересно, где же это всё находится в гидре, наверняка такую задачу можно решить с помощью только статического анализа

И правда – я в упор не замечал вызовы функций в начале main, который дешифруют строки, откуда можно было вытащить ключ 0x5a

Резюмирую – надо быть внимательнее