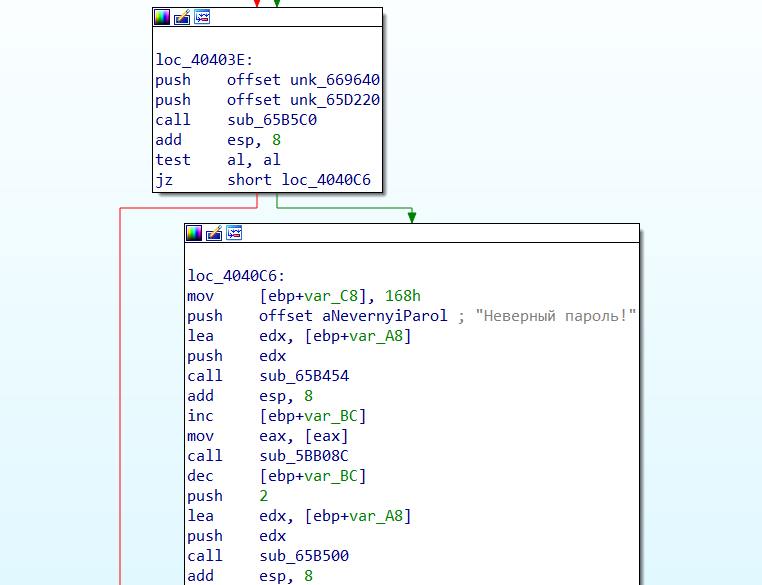
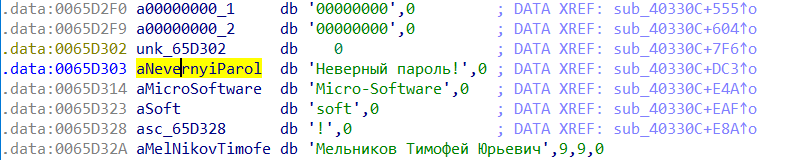
Поскольку в случае ввода неверного пароля выводится строка “Неверный пароль!”, логично проверить, где именно выводится эта строка в программе.

Откроем список всех строк и найдем, где в памяти лежит эта строка:  
Там же можно видеть, где именно и в какой процедуре она вызывается:



Можно видеть, что перед этим на стек кладутся два адреса и затем вызывается некая процедура, после которой и есть опция перехода на неверный пароль

Логично предположить, что именно в этой процедуре проверяется правильность пароля

В данной функции доходим до момента, когда в регистра EAX и EDX оказываются два адреса памяти.  
 По этим адресам в памяти лежат по восемь шестнадцатеричных значений (начиная с выделенной части):



В адресе в EDX лежат значения, соответствующие правильному паролю

Тогда переведем секретное значение в шестнадцатеричные коды и сделаем посимвольно операцию XOR с каждым из значений пароля

Если в результате получается код маленькой латинской буквы или цифры, то этот символ правильный, если нет – сдвигаем код так, чтобы символ был подходящим.

С помощью этих операций и получаем нужный пароль:

