Отчет по лабораторной работе №4

В ходе “батлевания” с визави (Максимом Прищепом) использовалось программное средство IDA для дизассемблирования исполняемого модуля с целью реверс-инжиниринг.

В папке с отчетом можно найти следующие файлы, пронумерованы в соответствии с очередью получения:

1. **ilya\_source.cpp** — файл с исходным кодом на языке записи алгоритмов С++
2. **ilya\_source\_22092019.exe** — отправленный Максиму мой исходный исполняемый модуль
3. **maksim\_source\_22092019.exe** — полученный от Максима его исходный исполняемый модуль
4. **maksim\_hacked\_24092019.exe** — исправленный исполняемый модуль Максима с измененным паролем
5. **ilya\_hacked\_24092019.exe** — исправленный исполняемый модуль мой с измененным паролем
6. **ilya\_hacked\_fixed\_24092019.exe** —исправленный исполняемый модуль мой с измененным обратно паролем

**Изучение исполняемого модуля соперника**

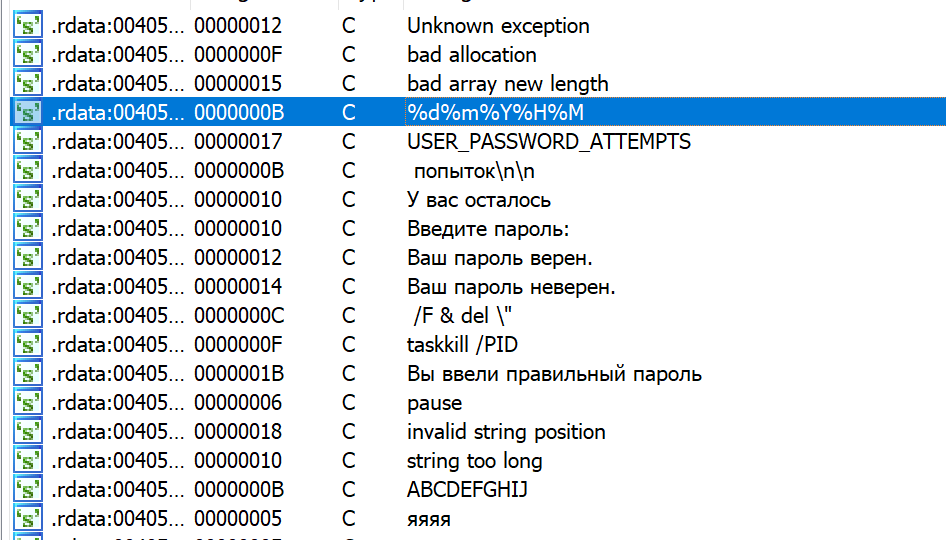
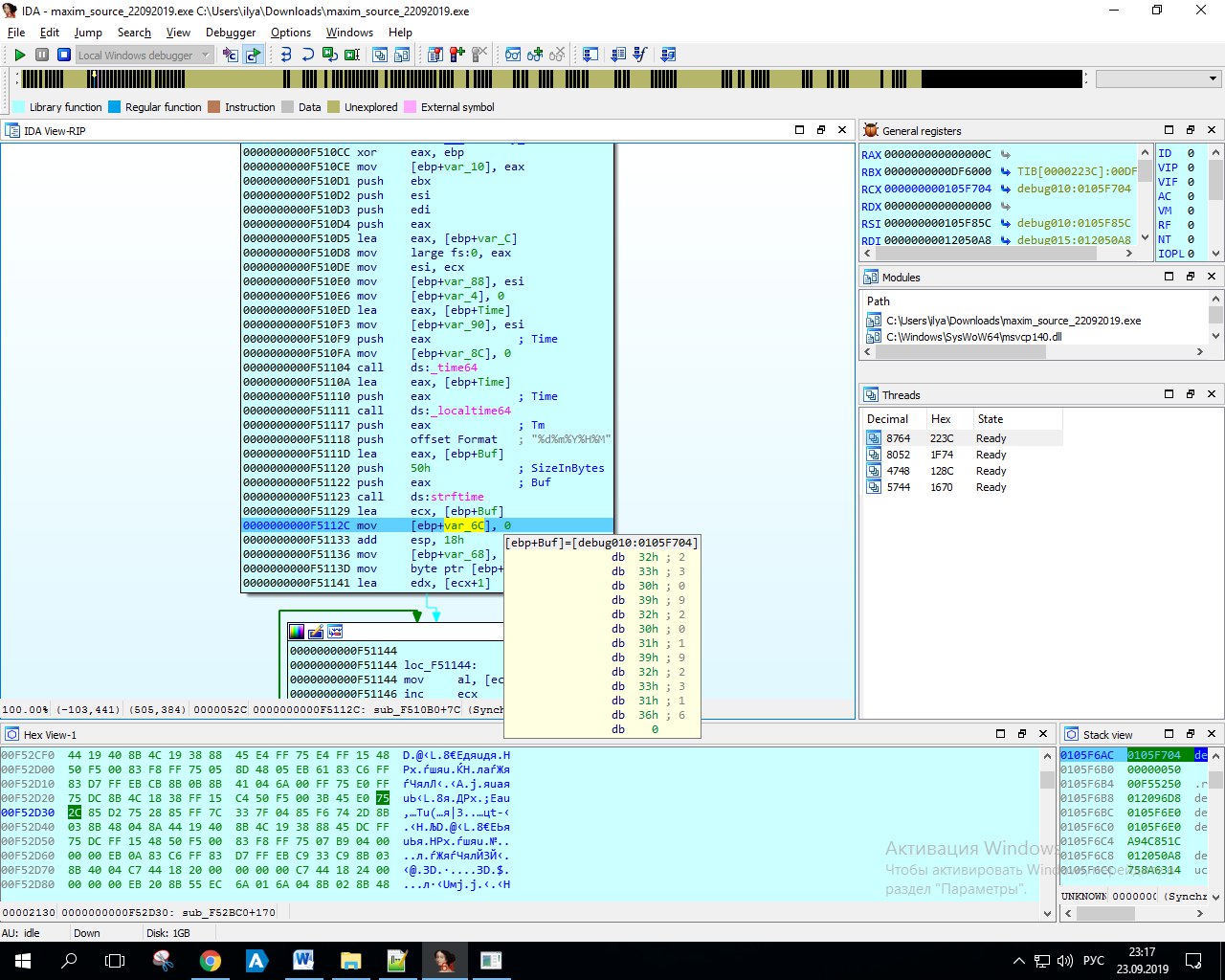
Исполняемый модуль (**maksim\_source\_22092019.exe**) был получен вечером 22.09.2019, а уже вечером 23.09.2019 стал целью моего изучения. После дизассемблирования исполняемого модуля, мной были обнаружены строки: **%d%m%Y%H%M** и **ABCDEFGHIJ**, которые вызвали у меня интерес (рисунок 1).

Рисунок 1 — найденные строки

Далее я стал изучать дизассемблированный модуль на языке ассемблер на предмет обнаружения этих строк, и была обнаружена строка с использованием формата даты (рисунок 2 и 3) и найден цикл (рисунок 4), в котором берется число из даты и далее получается символ для 0 - A, а для 9 - J. Это было выяснено с помощью отладчика. Продолжая дальше отладку, был и найден сам пароль (рисунок 5).

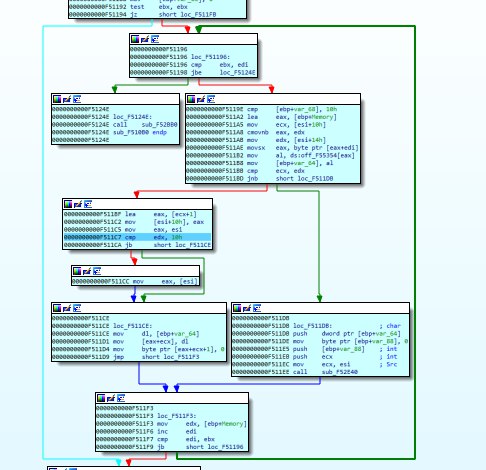
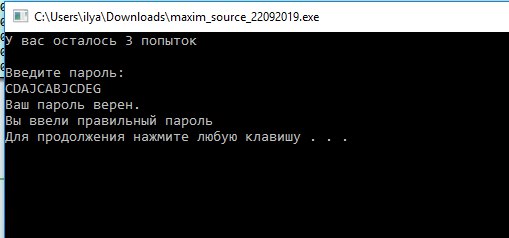
Рисунок 2 и 3 — Использование формата для даты

Рисунок 4 — Цикл с формированием пароля

Рисунок 5 — Найденный пароль в отладчике

Соотнеся найденную строку **ABCDEFGHIJ** c найденным паролем, было найдено, как мой соперник хранит пароль: он берет текущую дату и время, а далее собирает пароль, где каждое число из даты это индекс в строке **ABCDEFGHIJ**. Например, возьмем дату **230920192200**, получится пароль **CDAJCABJCCAA**. Соотношение символа в пароле и числа представлено в таблице 1. Правильность разгадки пароля представлена на рисунке 6.

| Таблица 1 | |
| --- | --- |
| A | 0 |
| B | 1 |
| C | 2 |
| D | 3 |
| E | 4 |
| F | 5 |
| G | 6 |
| H | 7 |
| I | 8 |
| J | 9 |

Рисунок 6 - Правильно разгаданный пароль

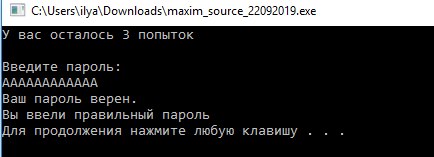
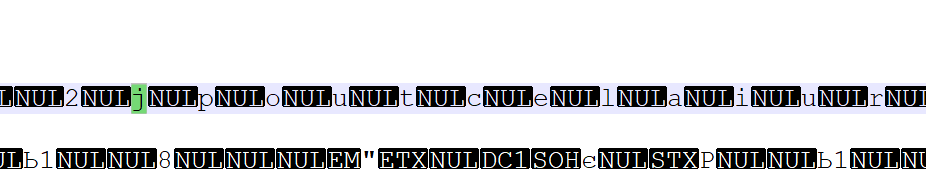
Следующим этапом было изменение пароля в исполняемом модуле. Для этого был открыт исполняемый модуль как текстовый файл в программном средстве Notepad++ с помощью поиска, и была найдена строка **ABCDEFGHIJ** и изменена на **AAAAAAAAAA**, и пароль теперь всегда будет **AAAAAAAAAAAA**, что проверено и отображено на рисунке 7. Ночью 24.09.2019 исполняемый модуль (**maksim\_hacked\_24092019.exe**) был отправлен визави для проверки на то, что исполняемый модуль запускается, и пароль был заменен.

Рисунок 7 - Подмена пароля

**Изучение моего исполняемого модуля, который модифицировал соперник**

Моему сопернику был отправлен 22.09.2019 исполнимый модуль (**ilya\_source\_22092019.exe**) с паролем **qvjbof`wvlsi1**, но это был результат посимвольного применение операции *xor* строки **ruialectuopj2** и константы **3**, которые были объявлены как директивы препроцессора.

Далее был получен модифицированный исполняемый модуль (**ilya\_hacked\_22092019.exe**) от соперника, который функционировал и пароль был заменен.

Открыв его с помощью Notepad++ и просмотрев предыдущую исходную строку для создания пароля, я заметил, что он просто перевернул ee и я заменил обратно, что соответствует **ilya\_hacked\_fixed\_24092019.exe** файлу.

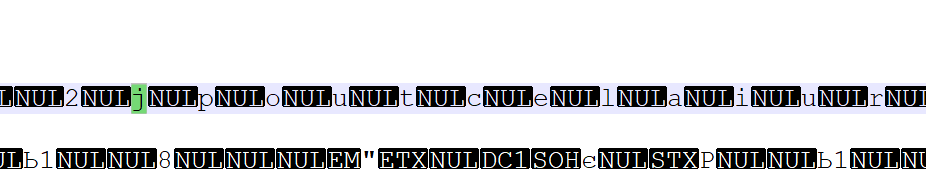


Рисунок 8 - Измененная строка для создания пароля

**Замечание.**

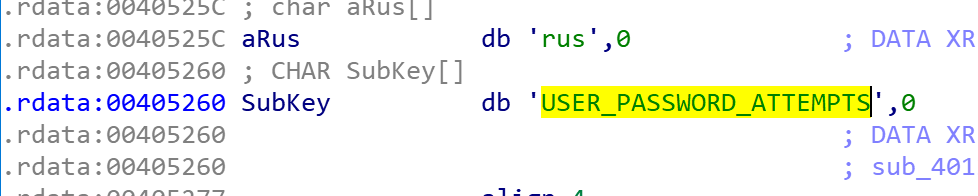
Также я обнаружил, что мой соперник хранит попытки в реестре операционной оболочки Windows, поэтому я мог легко их поменять.

Рисунок 9 — Ключ для записи в реестр