УДК 004.056.55

Учащ. А. М. Фурс
Науч. рук. Б. П. Батурчик, учитель информатики
(ГУО «Запольская средняя школа Червенского района»)

НАЧАЛО КАРЬЕРЫ ШПИОНА ИЛИ КАК СТАТЬ АВТОРОМ ПРОГРАММЫ ШИФРОВАНИЯ ЗАШИФРОВАННОГО

Программы-майнеры, сокрытие файлов, блокировка рабочего стола лечатся достаточно быстро стандартным набором антивирусных программ с актуальными сигнатурами. Но что делать, если злоумышленник получит доступ к вашим паролям в сети Интернет?

А между тем, это не такая уж сложная задача! Одной из причин этого стала повальная синхронизация аккаунтов. Согласитесь, удобно установить на мобильном телефоне браузер Chrome и, зайдя в свою учетную запись, «подхватить» из облака Google закладки и пароли.

Но любое удобное решение приносит в жертву безопасность. **Цель исследования: с**оздать программный продукт, который позволит повысить безопасность хранения паролей и работу в браузере.

Оборудование и ПО: Язык программирования Delphi7 Lite Full v7.4, популярные браузеры (состояние на 01.03.2020), NirSoft 1.20.

Мы пришли к выводу, что повлиять на использование актуального прикладного и антивирусного ПО в силу разных причин проблематично, но обезопасить себя от чрезмерного внимания знакомых и одноклассников вполне возможно.

Решением стало создание portable-программы для создания, хранения и поиска в базе паролей для сайтов и электронной почте. В программе должны быть реализованы следующие функции: генерирование паролей; шифрование и дешифрование записей; просмотр записей; создание бэкапа паролей; поиск в базе паролей.

Анализ источников в сети наиболее популярный и простой способ шифрования – шифрование методом XOR.

К каждому символу мы применяем побитно XOR с заранее известным ключом-словом. Для дешифровки используется обратная операция. Чтобы подобрать пароль надо знать слово-шифр.

Мы рассмотрели три способа шифрования посредством XOR с учетом того факта, что программа будет создана с помощью Delphi:

- Шифрование через пароль, равный длине шифруемого файла
- Шифрование через заданный пароль (6 символов, вводятся заранее в объекте edit на форме программы)
- Шифрование с обращением к файлу с паролем (585 символов)

Так как операции по шифрованию файлов очень быстротечны, то мы воспользовались мультимедийным таймером, который считает такты микропроцессора. Задержка этого таймера по отношению к программе, которая с ним работает, определяется лишь скоростью чтения данных из его регистра. Каждая программа из нашего списка шифровала файл с одинаковыми логинами и паролями. Минимальное количество записей – 20, максимальное – 200, шаг – 20 записей. При каждом запуске программа делала 100 шифрований файла и выводила средневзвешенное значение времени обработки файла с паролями и логинами.

Функцией QueryPerformanceFrequency(Fr) определили тактовую частоту процессора (количество тактов в секунду). Провели считывание счётчика тактов с помощью данной функции.

Таблица значений (в секундах):

	20	40	60	80	100	120	140	160	180	200
1.Шифрование через пароль, равный длине файла	0,0001	0,0002	0,0002	0,0002	0,0002	0,0002	0,0002	0,0003	0,0002	0,0002
2.Шифрование через заданный пароль (6 символов)	0,0590	0,0987	0,1031	0,1527	0,2026	0,2583	0,3036	0,4037	0,4551	0,5051
3.Шифрование с обращением к файлу с паролем (585)	0,0026	0,0023	0,0023	0,0033	0,0024	0,0031	0,0023	0,0023	0,0028	0,0024

Как видно из таблицы, первый и третий вариант стабильны и перепады вызваны особенностями работы ноутбука. Время шифрования файлов во втором случае было большим и возрастало в зависимости от количества шифруемых записей. Также большое время было связано с тем, что программа непрерывно обращалась к форме и считывала пароль.

Для своей программы мы выбрали шифрование через первый вариант. Интерфейс программы мы реализовывали с помощью языка программирования Delphi 7 lite. В меню реализован режим скрытия паролей («звездочками»), которые отражаются в полях генерации пароля и его поиска. Также есть следующие функции: бэкап базы паролей; восстановление из бэкапа; просмотр базы паролей; удаление расшифрованной базы паролей (без удаления основной); перешифрование отредактированной вручную базы паролей (с удалением «старой» базы. Также реализован поиск в базе паролей с выводом на основную форму.

Основное окно программы состоит из 2 частей. В левой части происходит генерирование паролей (по заданной маске) и сохранение

их в базу. В правой части (первоначально скрытой) происходит поиск паролей в базе [3, 4, 5].

Файл с паролями шифруется с помощью функции-криптора [2].

Удаление записи из файла происходит через создание компонента StringList, в который помещаются все строки из декодируемого файла. При переборе строк. При совпадении начала записи с содержимым соответствующего edit'а происходит удалении всей строки.

Программа изначально открывается в «свёрнутом» виде. Через команду «Поиск в базе» или кнопку с символом «>» можно «развернуть» окно, открыв возможность поиска и удаления в базе.

Для дополнительной безопасности можно создать пароль доступа к программе. Либо ввести поле для ввода пароля на объекте Panel, при вводе которого можно будет скрыть базу, либо ввести дополнительное окно, блокирующее основную форму. Мы воспользовались первым способом.

Для скрытия меню мы в свойстве memo основной формы удалили (в нашем случае) надпись MainMenu1 [1]

Наша программа уменьшила угрозы от людей, имеющих непосредственный доступ к вашему устройству.

Функции шифрования паролей и блокирование меню программы позволяет повысить безопасность пользования вашим устройством.

В нашей программе реализовано создание, поиск и удаление паролей из базы.

Программа имеет довольно простой интерфйс и код, что позволяет практически любому человеку, заинтересовавшемуся шифрованием не только получить начальные знания по методике шифрования, но и улучшить уже имеющуюся программу.

ЛИТЕРАТУРА

1. cyberforum.ru [Электронный ресурс] – Режим доступа: http://www.cyberforum.ru/delphi-beginners/thread635949.html

2. interface.ru [Электронный ресурс] – Режим доступа: http://www.interface.ru/home.asp?artId=23099

3. xakep.ru [Электронный ресурс] – Режим доступа: https://xakep.ru/2019/03/15/winrar-exploits/

4. habr.com [Электронный ресурс] – Режим доступа: https://habr.com/ru/post/183462/

5. Архангельский А.Я. Программирование в Delphi. Учебник по классическим версиям Delphi + CD, 2008 - 816 с.