УДК 004.491

ПРОГРАММНЫЕ И АППАРАТНЫЕ КЛАВИАТУРНЫЕ ШПИОНЫ

Блохина Е.Е., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В., к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова: *клавиатурные шпионы, кейлоггеры, электронное мошенничество.*

В данной статье рассматривается сущность клавиатурных шпионов, их основные виды, а также способы защиты от вредоносных кейлоггеров.

Желая завладеть информацией, которая хранится на наших устройствах, злоумышленники прибегают к различным методам. Одним из основных методов электронного мошенничества является кейлоггер.

Клавиатурный шпион или кейлоггер - программное обеспечение или аппаратное устройство, принцип работы которого заключается в собирании действий, которые выполняет пользователь (нажатие клавиш клавиатуры и мыши), и перевода его в текстовый файл.[3]

В настоящее время такого рода мошенничество принимает все большее развитие. Кейлоггерам теперь не составляет труда привязать собранную информацию к окну, запущенной в тот момент, программы, отследить список приложений, которые были запущены, а также сделать скриншоты экрана в определенный период времени. [1]

Существует два основных вида кейлоггеров: программные и аппаратные. (Таблица 1)

Кейлоггер может быть довольно опасен для пользователя ПК, т.к. с помощью кейлоггера злоумышленник может узнать пароли, коды и номера счетов в электронных платежных системах, адреса, логины и другую конфиденциальную информацию, вводимую пользователем с помощью клавиатуры.

Наличие такой информации у злоумышленников может привести к серьезным последствиям: осуществление экономического и политического шпионажа, получение доступа к сведениям, составляющим не только коммерческую, но и государственную тайну и т.д.

Чтобы защититься от вредоносных программ, установленных без нашего ведома, нужно придерживаться следующих правил:

Таблица 1 - Виды кейлоггеров:

Программные	Аппаратные
Кейлоггеры, относящиеся к данной группе реализуют надзор за работой пользователя ПК. Изначально программные продукты этого типа были созданы только для записи информации о нажатиях клавиш клавиатуры в специальный журнал регистрации, который далее изучался человеком, установившем эту программу.В настоящее время выполняются также и недавно открытые функции программных продуктов, такие как: перехват информации из окон, перехват кликов мыши, перехват буфера обмена, запись заданий, которые были отправления на принтер, перехват звука с микрофона и изображения с веб-камер, подключенных к компьютеру.[2]	Представляют собой миниатюрные приспособления, прикрепляющиеся между клавиатурой и компьютером или встроенные в саму клавиатуру. Они фиксируют все нажатия клавиш, сделанные на клавиатуре. Пользователю, который будет впоследствии пользоваться информацией, процесс регистрации будет неизвестен. Аппаратные кейлоггеры не требуют установки какой-либо программы на компьютере, чтобы успешно перехватывать все нажатия клавиш. Когда аппаратный кейлоггер прикрепляется, то, включенный компьютер или выключенный, не имеет никакого значения. Время его работы не ограничено, так как он не требует для своей работы дополнительного источника питания.[2]

Использовать проверенные или рекомендованные вам антивирусные или антишпионские программы, которые используют поведенческие анализаторы для противодействия мошенническим программным продуктам.

Пользоваться программами, шифрующими информацию, вводимую с клавиатуры.

Регулярно проверять внутренние и внешние компьютерные системы.

Использовать виртуальные клавиатуры.[1]

Таким образом, можно сделать вывод о том, кейлоггеры могут как помочь нам, так и нанести вред нашей конфиденциальной, если попадут в руки мошенников. Но при этом данный метод до сих пор актуален для рассмотрения в некоторых сферах защиты информации.

Библиографический список:

1. Обзор клавиатурных шпионов и методы борьбы с ними [Электронный ресурс]. - Режим доступа: https://ru.neospy.net/functions/keylogger/Vidy-klaviaturnyh-shpionov/
2. Аппаратные и программные клавиатурные шпионы [Электронный ресурс]. Режим доступа: https://sibac.info/archive/technic/6(42).pdf
3. Что такое кейлоггер? [Электронный ресурс]. - Режим доступа: https://blog.kaspersky.ru/chto-takoe-keylogger/700

SOFTWARE AND HARDWARE KEYLOGGERS

Blokhina E.E.

Keywords: *keyloggers, keyloggers, electronic fraud.*

This article discusses the essence of keyloggers, their main types, as well as ways to protect against malicious keyloggers.