УДК 004.056.53

студентка Е.И. Кузнецова
ГВУЗ «Национальный горный университет»

КЛАВИАТУРНЫЕ ШПИОНЫ

В данной работе приводится обзор клавиатурного шпионажа как одного из главных видов электронного мошенничества. Описана его «легальная» сторона и рассмотрены способы распространения. Так же приведены некоторые рекомендации защиты как от программных, так и от аппаратных клавиатурных шпионов.

Клавиатурные шпионы (англ. keyloggers — регистраторы нажатий клавиш) образуют категорию вредоносных программ, представляющую большую угрозу для безопасности пользователя. Они не являются вирусами, поскольку не обладают способностью к размножению. Как правило, современные клавиатурные шпионы не просто записывает коды вводимых клавиш - они "привязывает" клавиатурный ввод к текущему окну и элементу ввода. Кроме того, многие клавиатурные шпионы отслеживают список запущенных приложений, умеют делать "снимки" экрана по заданному расписанию или событию, шпионить за содержимым буфера обмена и решать ряд задач, нацеленных на скрытное слежение за пользователем. Записываемая информация сохраняется на диске и большинство современных клавиатурных шпионов могут формировать различные отчеты, могут передавать их по электронной почте или http/ftp протоколу. [1]

Большинство существующих на данный момент клавиатурных шпионов считаются «легальными» и свободно продаются, так как разработчики декларируют множество причин для их использования, например:

1. Для родителей: отслеживание действий детей в Интернете и оповещение родителей в случае попыток зайти на сайты «для взрослых» (parental control);

2. Для службы безопасности организации: отслеживание фактов нецелевого использования персональных компьютеров, их использования в нерабочее время, набора на клавиатуре критичных слов и словосочетаний, которые составляют коммерческую тайну организации, и разглашение которых может привести к материальному или иному ущербу для организации;

3. Для различных служб безопасности: проведение анализа и расследования инцидентов, связанных с использование персональных компьютеров и др.

В настоящее время клавиатурные шпионы, наряду с fishing и методами социальной инженерии, являются одним из главных видов электронного мошенничества. Они могут быть использованы для кражи персональной информации пользователей и осуществления экономического и политического шпионажа. [2] Однако если в случае fishing бдительный пользователь может сам себя защитить – игнорировать явные fishing- письма, не вводить персональные данные на подозрительных веб-страницах, – то в случае с клавиатурными шпионами никаким другим способом, кроме использования специализированных средств защиты, обнаружить факт шпионажа практически невозможно, поскольку клавиатурные шпионы пользуются RootKit технологиями для маскировки следов своего присутствия в системе.

Все клавиатурные шпионы можно условно разделить на аппаратные и программные. Первые представляют собой небольшие устройства, которые могут быть закреплены на клавиатуре, проводе или в системном блоке компьютера. Вторые – это специально написанные программы, предназначенные для отслеживания нажатий клавиш на клавиатуре и ведения журнала нажатых клавиш.

Способы распространения клавиатурных шпионов в целом не отличаются от способов распространения других вредоносных программ. Можно выделить следующие:

1. При открытии файла, присоединенного к электронному письму;
2. При запуске файла из каталога, находящегося в общем доступе в peer-to-peer сети;
3. С помощью скрипта на веб-страницах, который использует особенности интернет-браузеров, позволяющие программам запускаться автоматически при заходе пользователя на данные страницы;

4. С помощью ранее установленной вредоносной программы, которая умеет скачивать и устанавливать в систему другие вредоносные программы. [3]

Большинство антивирусных компаний добавляют известные клавиатурные шпионы в свои базы, поэтому метод защиты от них довольно прост: установка антивирусного продукта и поддержание его базы в актуальном состоянии. А что же делать в тех случаях, когда клавиатурный шпион не известен антивирусной программе или изготовлен специально для атаки конкретной системы? Разумным будет следование таким правилам:

1. Использовать одноразовые пароли и двухфакторную аутентификацию;
2. Использовать системы проактивной защиты, предназначенные для обнаружения программных шпионов;
3. Использовать виртуальные клавиатуры.

Но что касается последнего из вышеперечисленных способов защиты как от программных, так и от аппаратных клавиатурных шпионов, то следует отметить, что встроенная в Windows экранная клавиатура плохо применима для обмана данной угрозы. Она создавалась не как средство защиты, а для помощи людям с ограниченными возможностями, и передача данных после ввода с помощью данной клавиатуры может быть очень легко перехвачена вредоносной программой. Экранная клавиатура, которая может быть использована для того, чтобы обойти клавиатурные шпионы, должна быть разработана специальным образом, исключающим перехват вводимых данных на любой стадии их ввода и передачи.

Перечень литературы:

1. http://www.staffcop.ru/articles/keylogger-klaviaturniyshpion.php – Keyloggers.
2. http://www.idportal.org/page-id-1310.htm – Клавиатурные шпионы.
3. http://www.compress.ru/article.aspx?id=11114&iid=442 – Обзор keyloggers.