УДК 004.056.57

МЕТОДЫ ОБНАРУЖЕНИЯ И БОРЬБЫ С ВРЕДОНОСНЫМИ ПРОГРАММАМИ ТИПА «ТРОЯНСКИЙ КОНЬ»

Омельницкая Екатерина Викторовна, Масальская Елена Александровна
Государственный ВУЗ «Национальный горный университет», nmu.org.ua,
Omelnyckaya18katya@mail.ru

«Троянский конь» – это программа, которая имеет привлекательный внешний вид, но выполняет вредные, очень часто – разрушительные функции. Примером типичного "троянского коня" является программа, которая выглядит, как простая игра для рабочей станции пользователя. Однако пока пользователь играет в игру, программа отправляет свою копию по электронной почте каждому абоненту, занесенному в адресную книгу этого пользователя. Все абоненты получают по почте игру, вызывая ее дальнейшее распространение.

Ключевые слова **–** ***«***Троянский конь***», «***Spy Sheriff***», «***Trojan Hunter***»***

ВСТУПЛЕНИЕ

Работа посвящена изучению вредоносной программы вида «Троянский конь». Эти вредоносные программы являются, на сегодняшний день, одними из самых популярных. Они постоянно усовершенствуются и пользователи должны суметь защитить свои информацию и данные от такого типа вредоносных программ. Классический «Троянский конь» не имеет функции доставки программы на компьютер-жертву, однако его задание – обратить на себя внимание пользователя и заставить его запустить эту программу. Какие бы меры для защиты ни принимались, никакую сеть невозможно оградить от одной серьезной опасности — человеческой доверчивости. Ведь если программа была установлена по доброй воле, она может преодолеть любые брандмауэры, системы аутентификации и сканеры вирусов.

ВИДЫ ТРОЯНСКИХ ВИРУСОВ И ВАРИАНТЫ ИХ РАСПРОСТРАНЕНИЯ

Программы вида «Троянский конь» отличаются друг от друга вредоносными действиями, которые они выполняют, оказавшись в компьютере. Но самой большой проблемой является то, что данный вид программ может привести к уничтожению данных на диске и порче оборудования. Некоторые виды «троянских коней», объединившись с вирусами, распространяются между системами по электронной почте.

Варианты распространения данных программ:

- «троянский конь» представляется как обновление, отдельно поставляемое программное средство, используемое для устранения проблем в программном обеспечении или изменения его функционала. Исправление может применяться к уже установленной программе, либо к её исходным кодам. Сюда входит исправление ошибок, изменение внешнего вида, улучшение эргономичности или производительности программ, а также любые другие изменения, которые разработчик пожелал сделать.
- «троянский конь» представляют собой самостоятельный архив и т.д.

«Троянских коней» обычно классифицируют, исходя из действий, которые они осуществляют:

- шпионские программы;
- троянские прокси-серверы;
- интернет-кликеры;
- «бомбы» в архивах;
- инсталляция вредоносных программ;
- доставка вредоносных программ;
- оповещение об атаке;
- троянские утилиты отдаленного администрирования;
- почтовые «Троянские кони»;
- программы – шутки.

Исходя из последних исследований, выделяют такой тип «Троянских коней», как Spy Sheriff.

Этот троянский вирус классифицируется как «malware» (зловредное программное обеспечение). Как только Spy Sheriff попадает на компьютер пользователя, его очень трудно удалить. Если попробовать удалить его обычным способом, то он просто заново установиться с помощью скрытых файлов, которыми он заразил систему. Большинство антивирусных и «antispyware» программ не смогут обнаружить этот вирус. Также его невозможно удалить, с помощью функции восстановления системы, поскольку он контролирует компоненты, которые управляют этой особенностью в ОС Windows.

Помимо хакерства «троянские кони» могут использоваться для шпионажа за людьми и действовать как настоящие преступники, хотя и виртуальные. Однако есть несколько способов минимизировать риск: регулярное резервное копирование является необходимой процедурой для восстановления информации после воздействия тех «троянских коней», вмешательство которых ограничивается уничтожением данных. Использование полного набора программных средств защиты, таких, как брандмауэры и сканеры вирусов, может помочь выявить некоторые наиболее известные виды нарушителей. При заражении компьютера вирусом важно его быстро обнаружить. Для этого следует знать об основных признаках

проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;

СПОСОБЫ ЗАЩИТЫ КОМПЬЮТЕРА ОТ ТРОЯНСКИХ ВИРУСОВ

Почти все троянские программы попадают в компьютер через Интернет, вместе с картинками и информацией, которую загружает браузер в кэш. Многие программы известных разработчиков содержат в себе множество ошибок и недоработок, злоумышленники, тем самым, могут использовать их в своих целях, а именно: обмануть (просьба оплатить программу), украсть какие-либо важные данные с компьютера, или заразить его «Троянским конем». В данной ситуации можно снизить риск. Достаточно своевременное обновление операционной системы через встроенную утилиту Windows Update.

Для защиты компьютера через Интернет, на компьютере должен быть установлен антивирус с защитой от ненадежных сайтов. Антивирус будет проверять все файлы и диски, а также следить за файлами, которые попадают в компьютер из Интернета или съемных носителей. Антивирусная база должна постоянно обновляться, необходимо это для того, чтобы антивирус мог обновлять виды вирусов. В случае не своевременного обновления.

Существуют вирусы, которые внедрены в исполняемый файл, и антивирус не сможет его распознать. Поэтому наличие антивирусной базы, количество зараженных файлов программой «Троянских коней» будет выше, тем самым пользование сетью Интернет будет рискованней.

На сегодняшний день существуют программы, нацеленные специально на лечение от троянских вирусов, например программа Trojan Hunter.

ВЫВОДЫ

Таким образом, следует контролировать запуск задач и сервисов в системе. Почти во всех случаях заражения троянским вирусом, его запуск происходит вместе с запуском системы и прячется в запущенных процессах. Таким образом, можно вычислить вирус и удалить его. Для правильного и эффективного удаления нужно сначала удалить соответствующую запись в реестре, затем после перезагрузки компьютера удалить файл «Троянского коня».

Для сохранения важной информации или паролей, необходимо их содержать на дисках и других носителях информации. В случае заражения компьютера, вирусу не будут доступны эти данные.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. Способы защиты компьютера от троянских программ(Электрон. ресурс) / Способ доступа: URL: http://www.compport.ru/dir/file/sposoby_zashhity_kompyutera_ot_troyanskix_virusov.html.– Загол. с экрана.

2. Замаскированные вредоносные программы (Электрон. ресурс) / Способ доступа: URL: http://www.zahist.narod.ru/tojan.htm.– Загол. с экрана.