ВикипедиЯ

Троянская программа

Материал из Википедии — свободной энциклопедии

Троя́нская ви́русная программа (также — **троя́н**, **троя́нец**) — разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации о банковских картах, передача этой информации злоумышленнику, а также использование, удаление или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в целях майнинга, использование IP для нелегальной торговли.

Примеры троянских программ: HookDump, Back Orifice, Pinch, TDL-4, Trojan.Winlock...

Содержание

Происхождение термина

Свое общее название троянские программы получили за сходство механизма проникновения в компьютер пользователя с описанным в эпизоды Илиады, рассказывающем о «Троянском коне» — дарёном деревянном коне, использованном для проникновения в Трою, что и стало причиной падения Трои. В Коне, подаренном в знак лже-перемирия, прятались воины Одиссея, ночью выбравшиеся из Коня и открывшие ворота основным силам объединённой греческой армии. Больша́я часть троянских программ действуют подобным образом — маскируется под безвредные или полезные программы, чтобы пользователь запустил их на своем компьютере. Считается, что первым этот термин в контексте компьютерной безопасности употребил в своём отчёте «Computer Security Technology Planning Study» Дэниэл Эдвардс, сотрудник АНБ.[1]

Цели

Целью троянской программы может быть:

- закачивание и скачивание файлов;
- копирование и подача пользователю ПК ложных ссылок, ведущих на поддельные веб-сайты, чаты или другие сайты с регистрацией;
- создание помех работе пользователя;
- кража данных, представляющих ценность или тайну, в том числе информации для аутентификации, для несанкционированного доступа к ресурсам, выуживание деталей касательно банковских счетов, которые могут быть использованы в преступных целях;
- распространение других вредоносных программ, чаще всего таких, как вирусы или черви;
- уничтожение данных (стирание или переписывание данных на диске, труднозамечаемые повреждения файлов) и оборудования, выведения из строя или отказа обслуживания компьютерных систем, сетей;
- сбор адресов электронной почты и использование их для рассылки спама;
- слежка за пользователем и тайное сообщение злоумышленникам, таких как, например, привычка посещать конкретные сайты;
- регистрация нажатий клавиш с целью кражи информации такого рода как пароли и номера кредитных карточек;
- дезактивация или создание помех работе антивирусных программ и файервола;
- для самоутверждения вирусодела, из мести или просто «повеселиться».

Распространения

Троянские программы распространяются как и людьми — непосредственно загружаются в компьютерные системы злоумышленниками-инсайдерами, так и побуждают пользователей загружать или запускать их на своих системах.

Для достижения последнего троянские программы помещаются злоумышленниками на открытые или индексируемые ресурсы (файл-серверы и системы файлообмена), носители информации, присылаются с помощью служб обмена сообщениями (например, электронной почтой), попадают на компьютер через бреши безопасности или загружаются самим пользователем с адресов, полученных одним из перечисленных способов.

Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определённые компьютеры, сети или ресурсы (в том числе, третьи).

Расширения троянских программ

Троянские программы обычно имеют следующие расширения:

- .exe, .com (под видом игр, офисных приложений и других легальных программ, расширение может быть не видно, если в Windows отключено отображение расширений, возможны файлы с «двойным» расширением, например, image.jpg.exe. Программы после запуска могут работать скрытно);
- .js, .vbs, .jse, .vbe, .bat, .cmd, .sh (скрипты; расширение может быть не видно, иногда файлы этих форматов можно прочитать в редакторе кода);
- .html, .htm, .shtml, .shtm, .xhtml, .xht, .hta (HTML документы; могут скачивать вирусы и другие вредоносные программы из Интернета, перенаправлять на вирусные и ложные сайты; файлы .hta работают вне браузера и могут выполнять опасные действия непосредственно на компьютере);
- .pif (ярлык с возможностью выполнения вредоносных действий);

- .docm, .xlsm и т. п. (в электронных документах могут быть опасные макросы, обычно расширение заканчивается на «m»);
- .xml, .xsl, .svg, .xaml (XML-документы, аналогично HTML);
- .scr (программа, работающая зачастую скрытно);
- некоторые другие.

Маскировка

Троянская программа может имитировать имя и иконку существующей, несуществующей, или просто привлекательной программы, компонента, или файла данных (например, картинки), как для запуска пользователем, так и для маскировки в системе своего присутствия.

Троянская программа может в той или иной мере имитировать или даже полноценно выполнять задачу, под которую она маскируется (в последнем случае вредоносный код встраивается злоумышленником в существующую программу).

Методы удаления

В целом, троянские программы обнаруживаются и удаляются антивирусным и антишпионским ПО точно так же, как и остальные вредоносные программы.

Троянские программы хуже обнаруживаются контекстными методами основанных на поиске известных программ антивирусов, потому что их распространение лучше контролируется, и экземпляры программ попадают к специалистам антивирусной индустрии с бóльшей задержкой, нежели самопроизвольно распространяемые вредоносные программы. Однако эвристические (поиск алгоритмов) и проактивные (слежение) методы для них столь же эффективны.

См. также

- Вредоносная программа
- VirusTotal
- Лаборатория Касперского

Примечания

1. Rick Lehtinen, Deborah Russell, G. T. Gantemi Sr. Computer Security Basics (https://books.google.com/books?id=fqCFfuAJ4uEC&lpg=PA87&ots=PKgBSMxK0H&dq=Daniel%20Edwards%20NSA&pg=PA87#v=onepage&q&f=false) O'Reilly, 2006. ISBN 0-596-00669-1

Ссылки