ОТДЕЛ ПО РАСКРЫТИЮ ПРЕСТУПЛЕНИЙ
В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ
КРИМИНАЛЬНОЙ МИЛИЦИИ
УВД ГОМЕЛЬСКОГО ОБЛИСПОЛКОМА

ОПОРНЫЙ ПЛАН-КОНСПЕКТ

Тема:
«**Банковские троянцы**»

Гомель
2019

Троянская программа (также – троян, троянец, троянский конь) – разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации банковских карт и т.д. и её передачу злоумышленнику, её использование, удаление или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в целях майнинга, использование IP для нелегальной торговли.

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 объединенной греческой армии.*

Большая часть троянских программ действуют подобным образом – маскируется под безвредные или полезные программы, чтобы пользователь запустил их на своем компьютере.

Троянские программы распространяются людьми – как непосредственно загружаются в компьютерные системы злоумышленниками-инсайдерами, так и побуждают пользователей загружать и (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.

Целью троянской программы может быть:

- закачивание и скачивание файлов;
- копирование ложных ссылок, ведущих на поддельные вебсайты, 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, таких как вирусы;
- 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 третьим лицам сведений, 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 создателя вируса.

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);
- .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.

Задачи, которые могут выполнять троянские программы, бесчисленны (как бесчисленны и существующие ныне в мире компьютерные вредоносные программы), но в основном, они идут по следующим направлениям:

- нарушение работы других программ (вплоть до зависания компьютера, решаемого лишь перезагрузкой, и невозможности их запуска);
- настойчивое, независимое от владельца предложение в качестве стартовой страницы спам-ссылок, рекламы или порносайтов;
- распространение по компьютеру пользователя порнографии;
- превращение языка текстовых документов в бинарный код;
- мошенничество (например, при открывании определённого сайта пользователь может увидеть окно, в котором ему предлагают сделать определённое действие, иначе произойдёт что-то трудно-поправимое – бессрочная блокировка пользователя со стороны сайта, потеря банковского счета и т. п., иногда за деньги, получение доступа к управлению компьютером и установки вредоносного ПО).

Банковские троянцы – специализированные программы, созданные для похищения личных данных пользователей. В особенности они заточены на воровство логинов и паролей пользователей интернет-банкинга. Троянцы также могут перехватывать SMS с секретными кодами, которые присылает банк, и перенаправлять их злоумышленникам. Кроме того, они способны также непосредственно воровать деньги со счета – все сразу или постепенно небольшими переводами.

Наиболее вероятные пути заражения. Путь заражения компьютера пользователя троянской программой, как правило, происходит одинаково: она маскируется под безобидные, а часто и очень известные приложения. Самыми распространенными вариантами являются загрузка обновления программы не с официального сайта разработчика, а со стороннего ресурса, который имитирует оригинальный. Пользователь скачивает, казалось бы, известную программу, а внутри нее прикреплен троян, который заражает ПК. Кроме того, троянцев могут загружать на ПК другие трояны и вредоносное ПО, которым заражен компьютер. Не менее актуальным способом распространения банковских троянцев можно назвать СПАМ-рассылку. Этот метод усиливается технологиями социальной инженерии, которые строятся на психологии поведения и заставляют пользователя открыть прикрепленный документ или перейти по ссылке на зараженный сайт.

Банковские троянцы являются причиной 80% случаев кражи денег с банковских счетов. Банковские троянцы – довольно опасный хакерский

инструмент. В «умелых» руках он может нанести ощутимый ущерб финансам жертв.

Так, один из самых известных и опасных вредоносных программ этой категории **Zeus**, по подсчетам экспертов, стал причиной потерь от 50 до 100 млн долларов от непосредственного воровства и более 900 млн на разработку систем защиты. Казалось, что время этого трояна уже прошло, и с ним научились бороться. Однако в 2016 году был выявлен новый мощный банковский троян **Atmos**, который, по мнению экспертов отрасли, способен побить все рекорды, поскольку является намного более технологичным продуктом. Не менее известный троян **SpyEye** нанес ущерб в размере 100 млн долларов и смог собрать данные более 250 тысяч пластиковых карт.

Отдельно стоит сказать про троян **Citadel**, заразивший более 10 тысяч компьютеров и, по данным спецслужб США, ставший инструментом кражи более 500 млн долларов.

К слову, такие технологии стоят довольно дорого. На черном рынке цена на банковский троянец проверенной «марки» может варьироваться от 5 до 50 тысяч долларов (троян Carberp).

Стоит отметить, что создатель **Citadel** получил 5 лет в американской тюрьме, а творец **SpyEye** Александр Панин (Gribodemon) – 9 лет лишения свободы.

Лучшей защитой от троянских программ, является осмотрительность. Зная и используя несколько базовых правил кибербезопасности, можно свести к минимуму вероятность заражения:

1. Не открывайте письма от неизвестных адресатов с вложенными архивами и текстовыми документами.

2. Если открыли такое письмо, не открывайте файлы.

3. Удалите такое письмо.

4. Не используйте установочные файлы известных программ из сторонних источников.

5. Пользуйтесь антивирусом, как на ПК, так и на мобильном устройстве.

6. Регулярно делайте копии важной информации.

7. Реквизиты банковской карты должны запрашиваться при каждой повторной покупке в интернет-магазине. В противном случае, необходимо обратиться к менеджеру банка.

8. Помните: для входа в интернет-банкинг НЕ требуется ввод PIN-кода вашей карты.

Примеры уголовных дел:

Речицким РОСК 18.09.2019 возбуждено уголовное дело № 19124210769 по ч. 4 ст. 212 УК Республики Беларусь в отношении неустановленного лица, которое 15 мая 2019 года в 15 часов 37 минут, в неустановленном месте, из корыстных побуждений, через систему ОАО «АСБ Беларусбанк» - «клиент-банк», при помощи вредоносной программы «банковский троян» осуществило попытку хищения денежных средств в сумме 28 638 рублей, принадлежащих ООО «Вудвокпродакшн» на расчетных счет BY34 AKBB 3014 0003 2062 2521 0000 на имя Trotski Uladzimir, но не довело свой преступный умысел до конца по независящим от него причинам.

Гомельским ГОСК 13.09.2019 возбуждено уголовное дело № 19124353628 по ч. 3 ст. 212 УК Республики Беларусь в отношении неустановленного лица, которое в период времени с 25.06.2019 до 09.00 часов 26.06.2019 (точная дата и время в ходе следствия не установлены), в неустановленном месте, неустановленным способом из корыстной заинтересованности, путем использования компьютерной техники, осуществило несанкционированный доступ к компьютерной информации, путем введения в компьютерную систему ОАО «АСБ Беларусбанка», заведомо ложной информации о владельце расчетного счета, осуществило несанкционированный доступ к информации о банковском карт-счете, принадлежащем «Гомельской областной клинической психиатрической больницы», с которого умышленно пыталось похитить денежные средства в размере 12 344,40 рублей, однако не довело свой преступный умысел до конца по независящим от него обстоятельствам.