* **Троянские вирусы — Trojan.**

- это тип вредоносных программ, маскирующихся под легитимное ПО. Он часто используется киберпреступниками для кражи личных данных, слежения за пользователями и получения несанкционированного доступа к системам.

**Последствия:**

* Удаление данных
* Блокировка данных
* Изменение данных
* Копирование данных
* Нарушение работы компьютеров и компьютерных сетей

**Метод ликвидации:**

* найти и скачать антивирусную программу
* установить ее, обновить базу и версию, если они неактуальны
* произвести сканирование системы
* принять правильные решения относительно действий с каждым зараженным файлом
* убедиться в полной очистке компьютера, если лечение вируса-**трояна** прошло успешно

Задания:

1. Что такое Троян?

2. Вы обнаружили на своей машине файл dawdTrojanSkypee.exe и у вас отсутствует доступ к интернету, какие действия вам необходимо предпринять для остановки возможного вируса?

* **Вирусы-маскировщики — Rootkit.**

- утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

**Последствия:**

* скрытие файлов на устройствах хранения информации (жестких дисках), разделов и значений реестра Windows, процессов в системе, загруженных модулей, участков памяти (в случае бесфайлового вредоносного ПО), сетевой активности, секторов диска и других объектов и артефактов;
* противодействие изменению и (или) удалению руткита антивирусом в случае обнаружения, в том числе путем восстановления измененных компонентов;
* обеспечение вредоносному коду или приложениям доступа к ядру ОС - для остановки процессов антивируса, внедрения вредоносного кода в легитимные процессы, перехвата сетевого трафика (прослушивание сети), перехвата ввода данных с клавиатуры (клавиатурный шпион) и т. д.

**Метод ликвидации:**

* Поиск активного заражения в системной памяти операционной системы;
* Сканирование всех возможных мест автозапуска;
* Устранение обнаруженного активного заражения, восстановление на ранней стадии загрузки операционной системы
* Нейтрализация активного заражения во время установки продукта на зараженную систему.

Вирус шпион KeyLogger - программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя — нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т. д.

Последствия:

- Кража личных данных

- Кража страниц в социальных сетях

-Размещение личных данных в интернете

-Копирование данных из буфера обмена

-Создание и отправка скриншотов

-Сохранение и отправка всех данных на почту либо сервер хакера

**Методы защиты**

* использование антишпионских программных продуктов и/или антивирусных программных продуктов известных производителей с автоматическим обновлением сигнатурных баз.

Защита от «неизвестных» несанкционированно установленных программных кейлоггеров:

* использование антишпионских программных продуктов и/или антивирусных программных продуктов известных производителей, которые для противодействия шпионским программным продуктам используют так называемые эвристические (поведенческие) анализаторы, то есть не требующие наличия сигнатурной базы.
* использование программ, шифрующих вводимые с клавиатуры данные, а также применение клавиатур, осуществляющих такое шифрование на аппаратном уровне;

Защита от «известных» и «неизвестных» несанкционированно установленных программных кейлоггеров включает в себя использование антишпионских программных продуктов и/или антивирусных программных продуктов известных производителей, которые для противодействия шпионским программным продуктам используют:

* постоянно обновляемые сигнатурные базы шпионских программных продуктов;
* эвристические (поведенческие) анализаторы, не требующие наличия сигнатурной базы.

Защита от несанкционированно установленных аппаратных кейлоггеров:

* тщательные внешний и внутренний осмотры компьютерных систем;
* использование виртуальных клавиатур.

Adware — тип лицензирования программного обеспечения. Само программное обеспечение распространяется бесплатно, однако автор или распространитель приложения получает доход за счет показа рекламы. Также, термином «adware» называют тип зловредной программы, которая навязчивым образом отображает нежелательные объявления.

Чем опасен Adware?

Основным назначением деятельности по показу рекламы является **получение прибыли и покрытие расходов на разработку программного обеспечения** (например, конвертера видео или клиента системы мгновенных сообщений), таким образом, adware — это неявная форма оплаты за использование программного обеспечения

Adware-программы, которые собирают данные с вашего согласия, не следует путать с троянскими программами-шпионами, которые собирают информацию без вашего разрешения и ведома. **Если Adware-программа не уведомляет о сборе информации, она считается вредоносной**, например, вредоносная программа троянец-шпион (Trojan-Spy).

**Методы защиты**

* Удаление навязчивых баннеров из Google Chrome путем переустановки браузера. Способ простой и понятный, однако при его использовании навсегда теряются ранее выполненные настройки.
* Не заходить на веб-сайты подозрительной тематики
* Обновлять базы своего антивирусника
* Сканировать на предмет заражения жесткие диски и флеш-накопители, которые вставляются в USB-порт
* Не скачивать веб-продукты с непроверенных страничек.

**Trojan.Winlock (Винлокер)** — семейство вредоносных программ, блокирующих или затрудняющих работу с операционной системой, и требующих перечисление денег злоумышленникам за восстановление работоспособности компьютера, частный случай Ransomware (программ-вымогателей).

-Ни в коем случае нельзя выполнять требования злоумышленников. Следует помнить, что стоимость SMS может доходить до нескольких десятков долларов независимо от указанной в «интерфейсе» вируса. Практически во всех случаях после отправки SMS обещанный код разблокировки не приходит.

-В случае предлагаемой оплаты по SMS можно позвонить в службу поддержки контент-аггрегатора, которому принадлежит номер. Часто они могут сообщить код разблокировки.

-При возможности воспользоваться онлайн-сервисами подбора кода разблокировки на сайтах производителей антивирусного ПО.

-Произвести полное сканирование компьютера антивирусной утилитой со свежими обновлениями антивирусной базы (например, «одноразовым» антивирусом Dr.Web CureIt или Kaspersky Virus Removal Tool, скачать его желательно со «здорового» компьютера, даже в случае успешной разблокировки системы подбором кода).

-Если вирус блокирует доступ к определённым ресурсам Интернет (обычно к популярным социальным сетям и сайтам с антивирусным ПО), необходимо удалить лишние записи (кроме строки «127.0.0.1 localhost») из файла C:\WINDOWS\System32\drivers\etc\hosts и очистить кэш DNS (командой ipconfig /flushdns от имени администратора), а также очистить cookies и кэш в браузере.

-В некоторых случаях помогает перестановка даты в BIOS на пару лет назад.

-При полной блокировке можно загрузиться в систему с помощью LiveCD и попытаться удалить трояна при помощи антивирусов.

-Открыть диспетчер задач (если это возможно). Посмотреть процессы на предмет подозрительных. Попробовать завершить процесс. Скорее всего, процесс перезапустится. Перезагрузиться в безопасном режиме и удалить программу вручную.

-Если троян блокирует обычный безопасный режим, то при нажатии клавиши F8 необходимо выбрать безопасный режим с поддержкой командной строки. На данный момент времени большинство Винлокеров не способны его заблокировать. После загрузки надо запустить редактор реестра при помощи команды regedit и искать там подозрительные записи. В первую очередь, необходимо проверить ветку HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon, в частности в параметре Shell должно быть написано explorer.exe, а в параметре Userinit - C:\WINDOWS\System32\userinit.exe, (обязательно с запятой). Если там всё в порядке, необходимо проверить этот же путь, но в ветке HKEY\_CURRENT\_USER. Также желательно проверить ветки, в которых прописаны автозагружаемые программы, например, HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. В случае обнаружения подозрительных записей их необходимо заменить на стандартные значения (в случае с автозагрузкой удалить). После перезагрузки и входа в систему троян можно удалить вручную по уже известному пути. Этот способ хоть и эффективен, но подходит только для опытных пользователей.

-Кроме того, некоторые трояны заменяют собой один из файлов userinit.exe, winlogon.exe и explorer.exe в соответствующих каталогах. Рекомендуется восстановить их из дистрибутива или каталога C:\WINDOWS\System32\DLLCACHE.

-Троян может создавать раздел HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\userinit.exe, где прописывает вызов своего исполняемого файла (чаще всего debug.exe), а для возобновления работы системы необходимо удалить данный раздел[1].

-Одна из последних версий трояна не делает ничего из вышеперечисленного, а создает файл с именем по типу 0.5887702400506266.exe в корневой папке профиля пользователя и прописывает в реестре по адресу любой ветки, откуда может производиться автозапуск (например, HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options) раздел с непонятным именем. Если на компьютере есть второй профиль администратора, то его легко вычистить, зайдя из под другого профиля, просто удалив файл и ветку реестра. Однако было замечено, что бесплатные и платные антивирусы не реагируют на файл. Также можно найти и удалить этот файл, войдя в Windows через безопасный режим.