ИСКУССТВО ЦИФРОВОЙ САМОЗАЩИТЫ

Дмитрий Артимович

Звезда YouTube

Дмитрий Артимович

Искусство цифровой самозащиты

«Издательство АСТ»
2023

УДК 004.056
ББК 32.973.26

Артимович Д. А.

Искусство цифровой самозащиты / Д. А. Артимович — «Издательство АСТ», 2023 — (Звезда YouTube)

ISBN 978-5-17-156580-0

Дмитрий Артимович - русский хакер, специалист по платежным системам и информационной безопасности, автор книг «Электронные платежи в интернете» и «Я - хакер! Хроника потерянного поколения». Его новая книга - настольный путеводитель для тех, кто заинтересован понять искусство цифровой безопасности. В ней он расскажет о многих видах и способах мошенничества в цифровом поле, научит, как правильно защитить от них себя и свои данные, чем именно обезопасить свою технику и какие правила необходимо соблюдать. В современном мире люди хранят свою информацию в цифровом пространстве: банковские реквизиты, паспортные данные и многое другое. Вместе с этим, растет количество способов эту информацию украсть. Именно поэтому сегодня людям необходимо знать, как защититься от любых возможных атак, будь то компьютерный вирус или же фальшивый звонок из банка. В формате PDF A4 сохранен издательский макет книги.

УДК 004.056
ББК 32.973.26

ISBN 978-5-17-156580-0

Содержание

Вступление 6
Часть 1. Вредоносное ПО (Malware) 7
Кейлоггер (Keylogger) 10
Троян (Trojan) 14
Конец ознакомительного фрагмента. 20

Дмитрий Александрович Артимович
Искусство цифровой самозащиты

Вступление

В современный цифровой век безопасность платежных данных, да и вообще конфиденциальной информации, стала очень актуальной. Все мы периодически слышим о телефонных мошенниках, краже денег с банковских карт и счетов, а также о нескончаемых утечках персональных данных.

Издательство хотело от меня правила – как защитить себя от этих угроз – в подробностях. На самом деле правил очень мало, и они очень краткие:

- Установите антивирус на свой персональный компьютер.
- Своевременно обновляйте программное обеспечение (ПО).
- Устанавливайте ПО только из проверенных источников.
- Никому не сообщайте свои платежные данные, особенно по телефону (номера карт, СМС-коды и подобное).

Как бы я ни старался, я не смог бы растянуть эти правила на сотню страниц. Поэтому, если вам нужны только правила, – они выше, на этом вы можете закрыть книгу. Если же вам интересен мир вирусов, история их появления, самые громкие примеры, если вы хотите понять, как вирусы и другое вредоносное программное обеспечение попадает на компьютеры и телефоны, как работает киберкриминальный подпольный рынок, что делают с украденными данными, – эта книга для вас. Я постарался объяснить всё это предельно простым языком. Не расстраивайтесь, если чего-то не поняли. Самые важные определения выделены курсивом. И, естественно, после каждой главы я буду приводить те самые правила безопасности с примерами.

Первая часть книги – «Вредоносное ПО (Malware)» – будет полностью посвящена вредоносному программному обеспечению, созданному под персональные компьютеры. В этой главе будет практически одна занудная – а для кого-то интересная – теория. Если вы не хотите читать ее полностью, просмотрите только определения.

Вторая часть описывает вредоносы под смартфоны и умные устройства.

Третья часть расскажет о техниках социальной инженерии: фишинге, «нигерийских письмах», телефонных звонках и мошенничестве с технической поддержкой.

Четвертая часть коснется еще одной важной темы – кардинга.

Заключительная, пятая часть – «Паранойя» – рассчитана на продвинутых пользователей, которые хотят защитить свои данные не только в интернете, но и при утере или хищении личного компьютера – например, коррумпированными сотрудниками правоохранительных органов.

Начинаем…

Часть 1. Вредоносное ПО (Malware)

2010 год, октябрь, утро… 2 часа дня. Да, у многих айтишников утро начинается поздно. Я встаю с кровати и подхожу к своему старенькому ноутбуку Aser. Странно, моя ICQ[1] перестала подключаться, пароль больше не подходит.

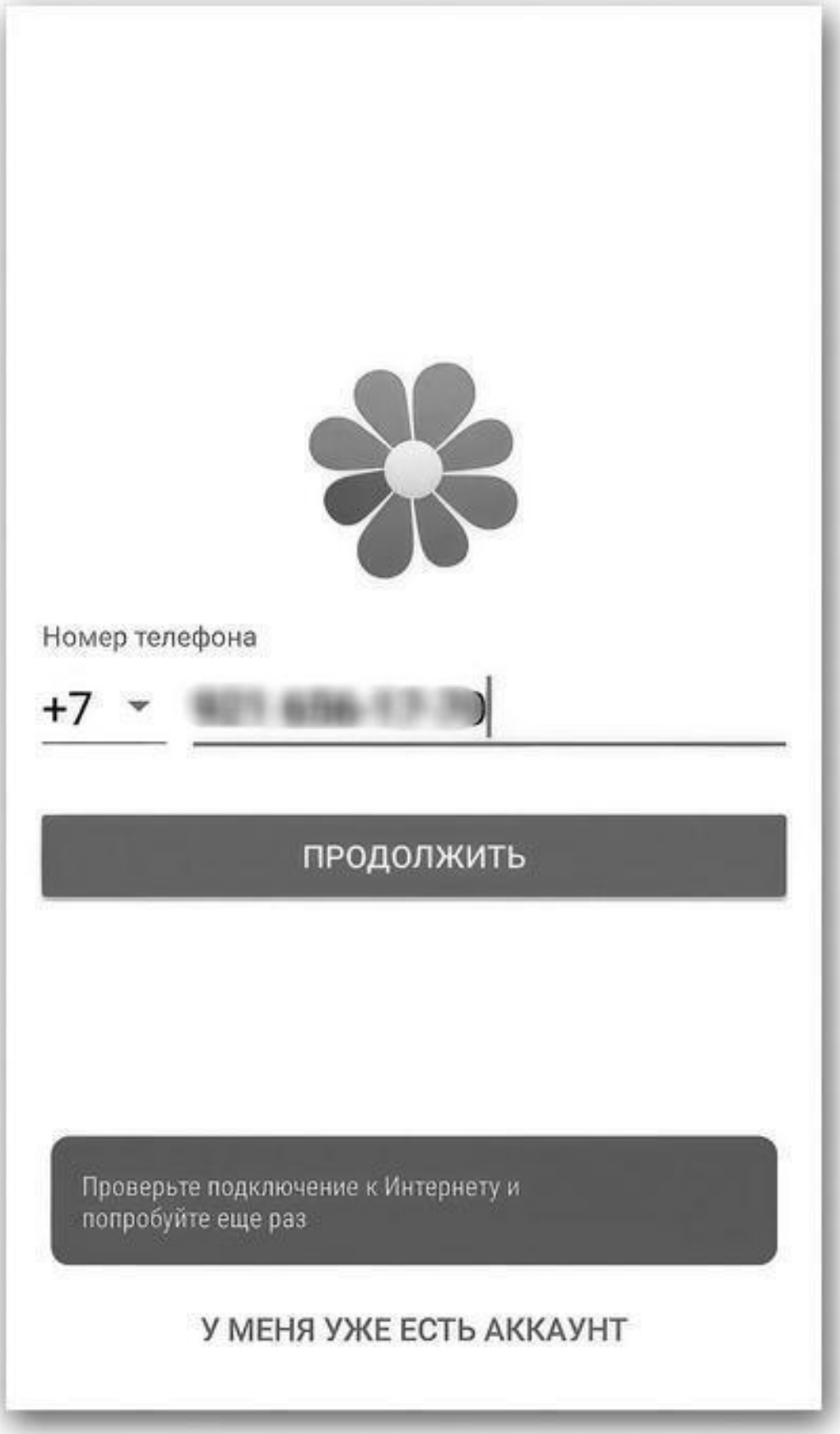
В jabber[2] написал AciD:
– Твоя аська у меня денег в долг просит. Это ты?
– Нет, похоже, украли.

Как это могло случиться? На своем персональном ноутбуке я уже давно пользовался антивирусом, который сканировал интернет-трафик и файлы. Так что этот вариант отпадал.

А вот в «Адамант Мультимедии», где я проработал с 2005 по 2007 год, к безопасности относились наплевательски. Компания разрабатывала компьютерные игры, и работа, безусловно, нравилась мне до определенного момента. У каждого разработчика был довольно мощный компьютер, по два жидкокристаллических монитора. А вот никакой политики обновления ОС, антивирусов там не было и подавно. Судя по всему, на этот рабочий комп я и подхватил кейлоггера. К слову сказать, потеря моей ICQ – единственный случай, когда у меня кто-то что-то украл.

[1] **ICQ** (созвучно фразе *англ.* I seek you – «я ищу тебя») – бесплатная система мгновенного обмена сообщениями. Была популярна в 2000-х годах.

[2] **Jabber** – старое название XMPP-протокола для мгновенного обмена сообщениями, которое до сих пор популярно у пользователей.


Номер телефона
+7
ПРОДОЛЖИТЬ
Проверьте подключение к Интернету и попробуйте еще раз
У МЕНЯ УЖЕ ЕСТЬ АККАУНТ

Тогда основными моими контактами в аське были ребята с форума spamdot[3]. Зарегистрировав новую аську, я создал топик «Угнали ICQ 332084545» на спамдоте в разделе «Кидалы».

Для того чтобы красть деньги с вашей карты или с вашего счета, даже не обязательно быть хакером. Очень часто подобные персонажи покупают существующий вредоносный софт на специализированных форумах. Поднимают сервер[4] для сбора логов, покупают загрузки и собирают чужие пароли, данные карт, доступы к онлайн-банкам, пароли от разных сервисов и т. д. А дальше уже могут продавать эти логи на тех же форумах, где кто-то другой будет их монетизировать. Ничего лучше, как выпрашивать в долг у моих контактов, тот горе-хакер не придумал.

Давайте рассмотрим основные категории, на которые делятся вредоносные программы:

- трояны;
- кейлоггеры (на самом деле кейлоггеры – это подраздел троянов, но я вынес их в отдельную главу);
- вирусы;
- черви.

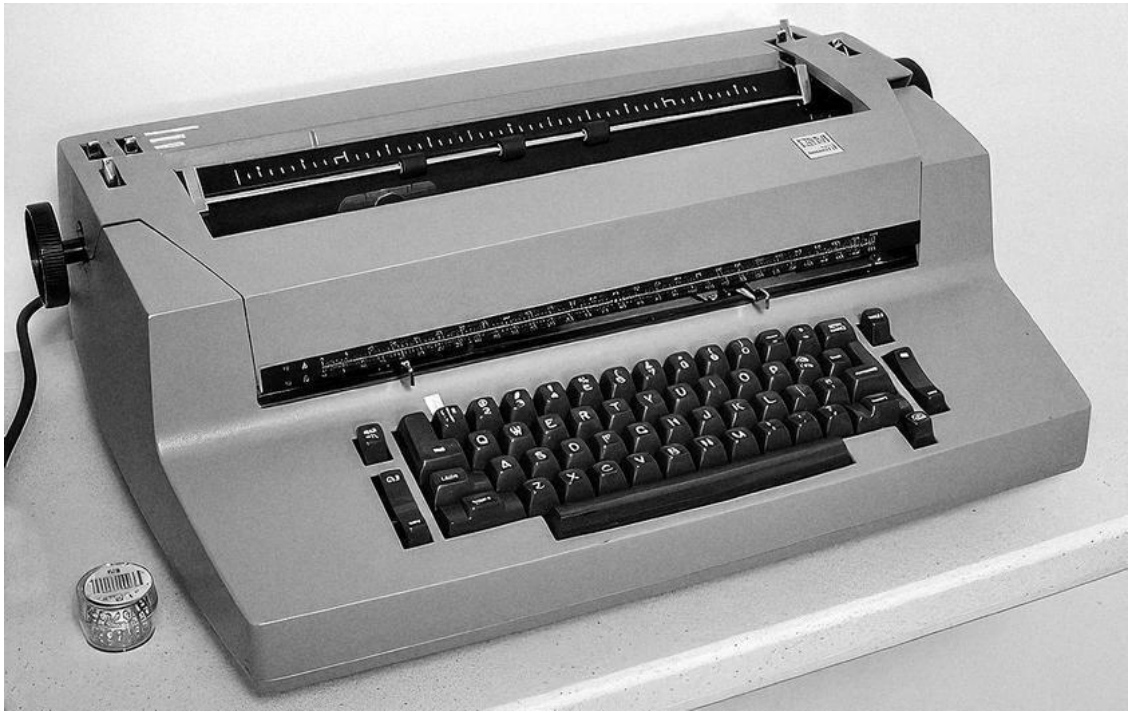
Это разделение довольно условно, потому что троян может распространять себя как вирус или червь, или же это будут разные компоненты: вирус-загрузчик и троян-кейлоггер. Но давайте разберем всё по порядку.

[3] **Spamdot** – форум общения спамеров (людей, кто рассылал почтовый спам). Более подробно о спаме я рассказывал в своей книге “Я – хакер! Хроника потерянного поколения”.

[4] **Сервер** (от *английского*: serve – «обслуживать», корректнее, server – «обслуживатель») – это выделенная физическая машина для выполнения сервисного ПО, простыми словами – это физический компьютер для хранения данных и обеспечения к ним прямого доступа.

Кейлоггер (Keylogger)

Кейлоггером является любой компонент программного обеспечения или оборудования, который умеет перехватывать и записывать все манипуляции с клавиатурой компьютера. Нередко кейлоггер находится между клавиатурой и операционной системой и перехватывает все действия пользователя. Это скрытое вредоносное программное обеспечение обычно передает данные на удаленный компьютер в интернете, где позже злоумышленник просматривает логи[5] на предмет «чем бы поживиться».



Кейлоггеры бывают как аппаратные, так и программные. Интересно, что первый кейлоггер был именно аппаратным, а история его создания и применения поражает.

Во время холодной войны разведка СССР пристально следила за дипломатами США, находившимися на территории нашей страны. Незаменимым помощником в этой слежке и получении важной информации оказались специальные жучки, которые можно считать первыми кейлоггерами.

Жучки устанавливались на печатные машинки, однако американцы в течение нескольких лет не догадывались о существовании подобных устройств.

О способе слежки советских спецслужб рассказали в АНБ еще в 2012 году, но тогда СМИ не обратили на историю внимания. В 2015-м о ней вспомнил специалист по шифрованию и безопасности Брюс Шнайер (Bruce Schneier).

С 1976 по 1984 год жучки устанавливались на печатные машинки IBM Selectric, использовавшиеся в посольстве США в Москве и консульстве в Ленинграде. Всего было обнаружено 16 «зараженных» машинок, в которых применялось несколько «поколений» кейлоггеров.

Принцип работы жучка основывался на движениях пишущей головки IBM Selectric: для набора текста ей нужно было поворачиваться в определенном направлении, уникальном для

[5] **Файл журнала** (протокол, журнал; *англ.* log) – файл с записями о событиях в хронологическом порядке, простейшее средство обеспечения журналирования.

каждого символа на клавиатуре. Кейлоггер улавливал магнитную энергию от движения каретки и преобразовывал ее в цифровой сигнал.

Каждый из полученных и обработанных сигналов хранился на жучке в виде четырехбитного символа. Устройство позволяло хранить до восьми таких символов, после чего отправляло их по радиочастотам на расположенную поблизости станцию прослушки.

Специалисты АНБ заявили, что жучок был «очень изощренным» для своих времен: например, у него был один бит встроенной памяти, что не встречалось ни у каких других подобных устройств того периода. Кейлоггер не был заметен снаружи, работал бесшумно, а при разборке машинки выглядел как одна из ее запчастей.

Обнаружить жучок было нетривиальной задачей даже для американских спецслужб. Его можно было увидеть при просвете рентгеновским излучением, однако он не обладал выдающимся радиофоном, так как зачастую вещал на частотах, используемых американским ТВ. Кроме того, отследить некоторые продвинутые версии жучка по радиосигналу можно было только в том случае, если была включена сама машинка, активирован кейлоггер, а анализатор шпионских устройств настроен на правильную частоту. Обученный советский техник мог установить такой жучок в IBM Selectric за полчаса[6].

Вот еще несколько примеров аппаратных кейлоггеров:

• **Аппаратный кейлоггер клавиатуры,** который подключается где-то между клавиатурой компьютера и самим компьютером, обычно встроенный в разъем кабеля клавиатуры. Более скрытые реализации могут быть установлены или встроены в стандартные клавиатуры, чтобы на внешнем кабеле не было видно никаких устройств. Оба типа регистрируют все действия с клавиатурой в своей внутренней памяти, к которой впоследствии можно получить доступ. Аппаратные кейлоггеры не требуют установки какого-либо программного обеспечения на компьютер целевого пользователя, поэтому они не мешают работе компьютера и с меньшей вероятностью будут обнаружены работающим на нем программным обеспечением. Однако физическое присутствие кейлоггера может быть обнаружено, если, например, установить его вне корпуса в качестве внешнего устройства между компьютером и клавиатурой. Некоторыми из этих реализаций можно управлять и контролировать их удаленно с помощью стандарта беспроводной связи.

[6] Источник https://masterok.livejournal.com/8284214.html

• **Анализаторы беспроводной клавиатуры и мыши.** Такие анализаторы собирают пакеты данных, передаваемые с беспроводной клавиатуры и ее приемника. Поскольку для защиты данных, передаваемых по беспроводной связи, между двумя устройствами может использоваться шифрование, то требуется доступ к ключам шифрования производителя.

• **Электромагнитное излучение:** можно зафиксировать электромагнитное излучение проводной клавиатуры на расстоянии до 20 метров (66 футов) без физического подключения к ней. В 2009 году швейцарские исследователи протестировали 11 различных клавиатур USB, PS/2 и ноутбуков в полубезэховой камере и обнаружили, что все они уязвимы – прежде всего, из-за непомерно высокой стоимости добавления экранирования во время производства. Исследователи использовали широкополосный приемник, чтобы настроиться на определенную частоту излучения клавиатуры.

Рассказывать про аппаратные кейлоггеры можно и дальше. Но в основном такие штуки используются спецслужбами. Например, в 2000 году ФБР хитроумно заманило двух подозреваемых российских хакеров в США. ФБР перехватило их имена пользователей и пароли с помощью кейлоггера, который был тайно установлен на машине, которую хакеры использовали для доступа к своим компьютерам в России. Затем ФБР с помощью этих учетных данных взломали компьютеры подозреваемых в России, после чего воспользовались полученными доказательствами для судебного преследования. Только не стоит забывать, что некоторые сотрудники спецслужб могут переступать грань закона и злоупотреблять служебным положением в целях личной наживы, промышленного шпионажа или заказного уголовного дела. Более подробно об аппаратных кейлоггерах мы поговорим в разделе «Паранойя». Сейчас же наибольший интерес для нас представляют программные кейлоггеры, которые входят в семейство троянских программ.

Кстати, существуют и легальные виды кейлоггеров, записывающие действия пользователей. Например, часть DLP-системы внутри организации.

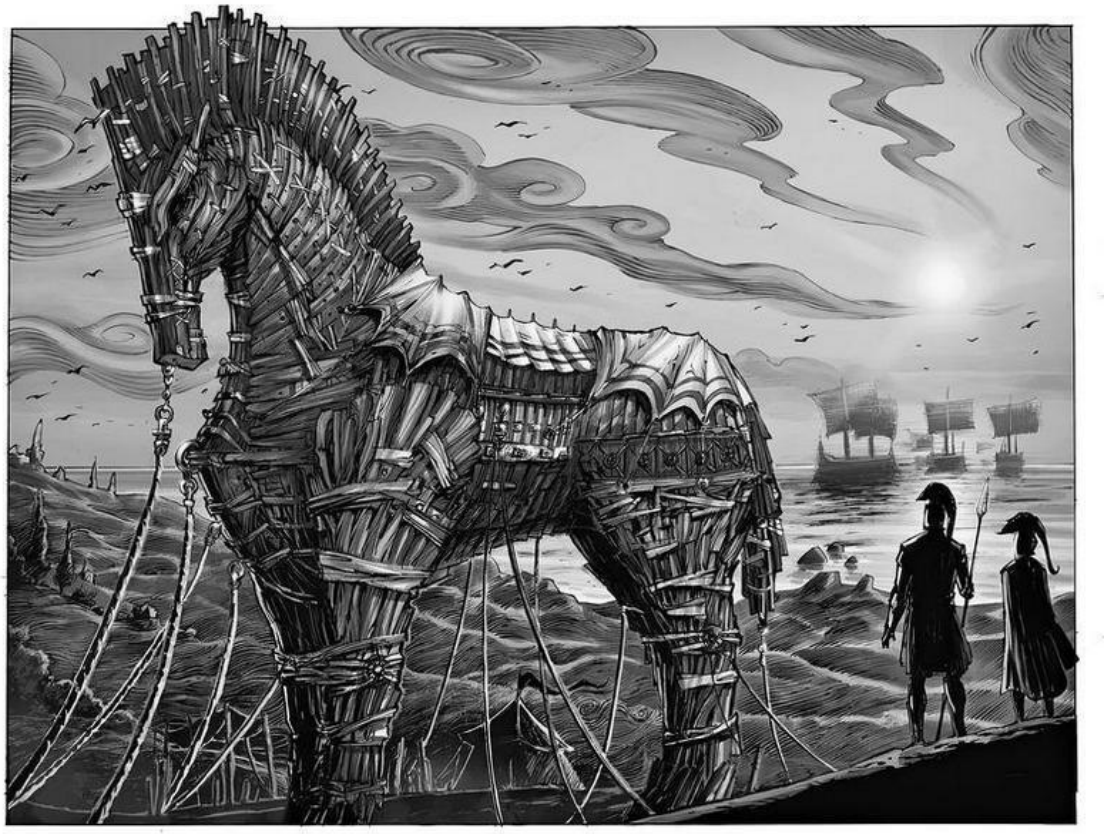
DLP-система – специализированное программное обеспечение, предназначенное для защиты компании от утечек информации. Эта аббревиатура расшифровывается как Data Loss Prevention (предотвращение потери данных) или Data Leakage Prevention (предотвращение утечки данных).

Другими словами, ваш босс или даже специальный отдел в вашей компании может следить за вашими действиями без вашего ведома, но абсолютно законно. Конечно, до тех пор, пока он не захочет где-то ввести номер вашей кредитной карты… Но будем надеяться на его благоразумие, и на ваше тоже.

> ***Итак, кейлоггеры – это такие вредоносные программы, которые, попав на ваш компьютер, будут отслеживать нажатие клавиш без вашего ведома и разрешения. Соответственно, всё, что вы вводите на клавиатуре, – пароли, номера ваших банковских карт, личная переписка – попадет в руки злоумышленнику.***

Троян (Trojan)

Троянская вирусная программа (также – троян) – разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно. Современные трояны могут записывать не только нажатие клавиш, но и перехватывать данные форм интернет-браузеров (вводимые пароли от почты, номера карт, пароли от онлайн-банков), извлекать сохраненные пароли из других программ (например, как у меня пароли от ICQ), делать скриншоты рабочего стола, следить за перемещением пользователя, записывать изображения или видео с камеры.



В эпической поэме Вергилия «Энеида» греческий стратег Одиссей придумал коварный план, чтобы проникнуть за неприступные крепостные стены осажденной Трои. Вместо того чтобы проламывать стены или взбираться на них, Одиссей предложил другой способ: прибегнуть к хитрости. Троянцы увидели, как греческие корабли уплыли прочь, оставив после себя гигантского деревянного коня в знак признания поражения. Ликуя и празднуя победу, троянцы втащили коня в город, не подозревая, что внутри спрятались Одиссей и его солдаты, которые дождались глубокой ночи и захватили город.

Есть несколько элементов этой истории, которые делают термин «троянский конь» подходящим названием для этих типов кибератак:

• **Троянский конь** был уникальным решением для преодоления защиты цели. В оригинальной истории нападавшие осаждали город 10 лет и так и не смогли его победить. Троянский

конь дал им доступ, о котором они мечтали столько лет. Точно так же троянский вирус может быть хорошим способом обойти сложную систему защиты.

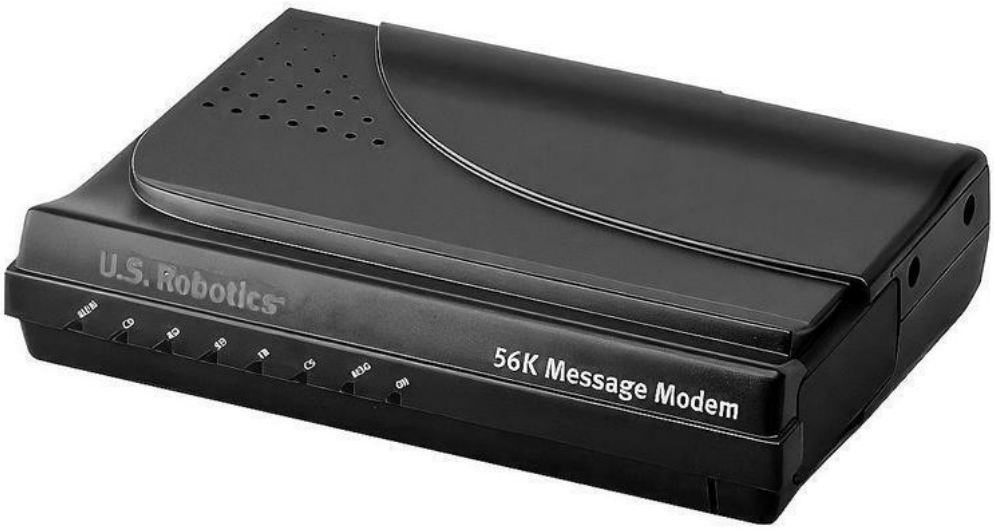
• **Троянский конь** казался обычным подарком. В том же духе троянский вирус выглядит как легальное программное обеспечение.

• **Солдаты из троянского коня** захватили и взяли под контроль систему обороны города. С помощью троянского вируса вредоносное ПО получает контроль над вашим компьютером, потенциально делая его уязвимым для других «захватчиков».

Впервые термин «троян» был использован в ссылке на вредоносный код в отчете BBC США 1974 года, посвященном анализу уязвимостей компьютерных систем. Термин стал популярным в 1980-х, особенно после лекции Кена Томпсона на награждении ACM Turing Awards 1983 года.

Одним из основоположников известных троянов стал PC-Write Trojan (1986). Текстовый редактор PC-Write был одной из первых свободно распространяемых shareware[7] программ. PC-Write Trojan маскировался как версия 2.72 текстового редактора PC-Write, хотя сами создатели никогда не выпускали такую версию. Пользователь думал, что запускает новую версию условно-бесплатной программы, а по факту запускал троян на своем компьютере. После запуска троян уничтожал все файлы на диске.

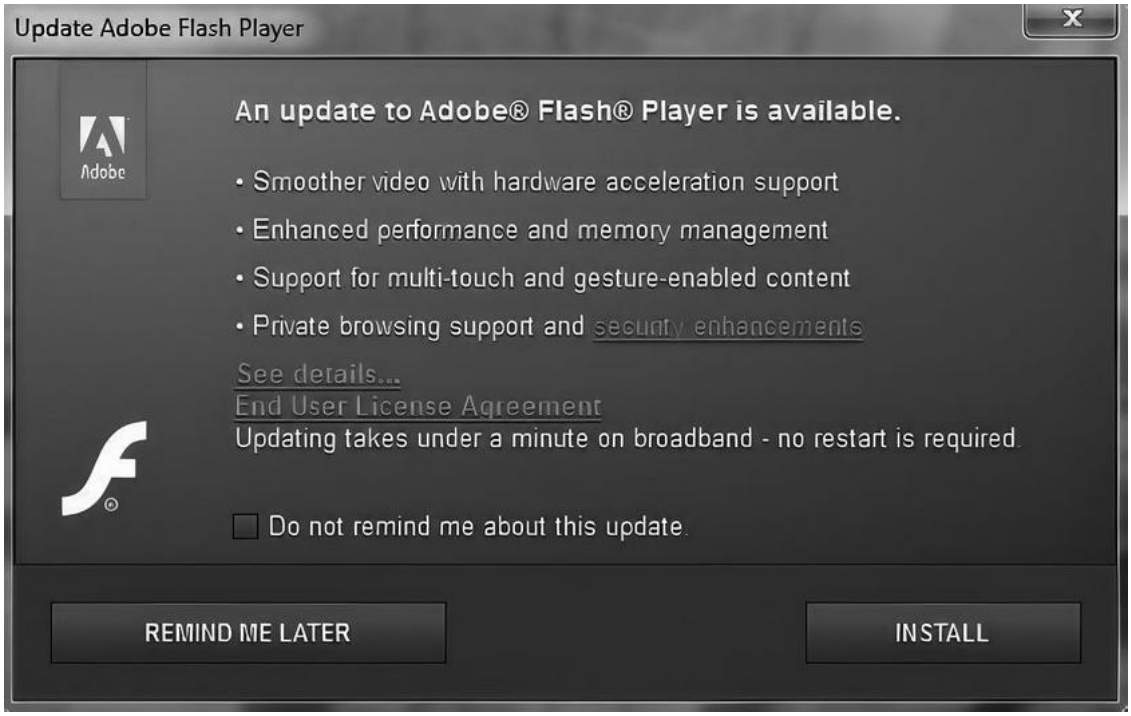
Своего первого трояна я написал еще в 1998 году. Интернет тогда у нас был через обычные телефонные модемы по проводным телефонным линиям. Скорость по такому интернет-соединению достигала максимум 56 кбит/с, т. е. вы могли скачивать всего 7 килобайт в секунду, и то в лучшем случае.



[7] **Shareware** (или условно-бесплатные программы) – это коммерческое ПО с безвозмездным использованием. Однако, как правило, либо функциональность таких программ ограничена, либо они предоставляются бесплатно на испытательный период, который заканчивается по истечении определенного количества дней.

У нас в Кингисеппе[8] интернет был только по модему и достаточно дорогой для того времени. Звонишь по определенному номеру и потом платишь по несколько рублей за минуту на линии. Поэтому для электронной почты некоторые умельцы подняли выделенный сервер, расположили его на местном заводе «Фосфорит»[9]. Специальная программа Minihost дозванивалась до сервера и принимала/отправляла почту по протоколу UUCP[10]. Вот под этот почтовый клиент я и написал трояна на Pascal'е[11]: он должен был стащить пароли от почты и отправить тем же Minihost'ом мне на специальный адрес электронной почты. Закинул этого трояна я в местную почтовую конференцию под видом «крутого скринсейвера».

Следующий мой троян использовался как загрузчик для спам-бота[12] Festi. Задача трояна была скрытно установить бота на компьютер пользователя. Вот только одна проблема: начиная с Windows Vista Microsoft встроила в операционную систему UAC[13], который блокировал установку драйверов-руткитов.



[8] **Кингисепп** (до 1922 года – Ямбург[7]) – город (с 1784 года) в России, административный центр Кингисеппского района Ленинградской области и муниципального образования Кингисеппское городское поселение. Основан новгородским боярином Иваном Фёдоровичем как крепость Ям в 1384 году.

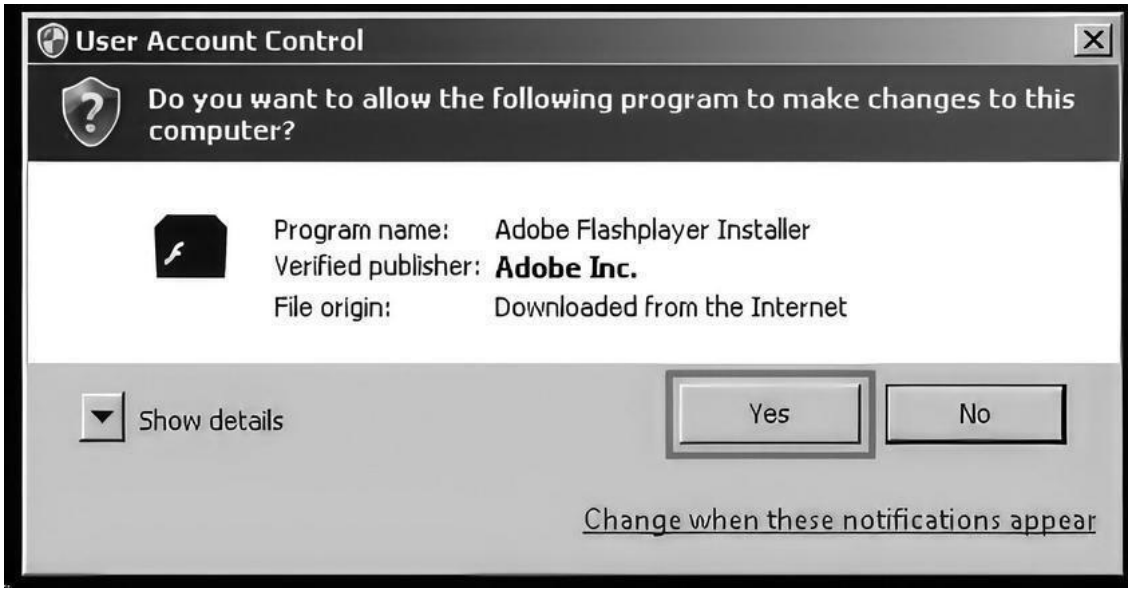
[9] **ООО «Промышленная Группа «Фосфорит»** – один из ведущих производителей фосфорных удобрений и кормовых фосфатов на Северо-Западе России, а также фосфоритной муки, серной и фосфорной кислот для нужд собственного производства. Его доля в российском производстве фосфорных удобрений составляет более 10 %.

[10] **UUCP** (сокр. от *англ.* Unix-to-Unix CoPy) – команда копирования файлов между двумя компьютерами под управлением операционной системы UNIX, использующая одноименный протокол. Позже появились реализации этого протокола под другие операционные системы, в том числе DOS, Windows, OS/2.

[11] **Паскаль** (*англ.* Pascal) – один из наиболее известных языков программирования, используется для обучения программированию в старших классах и на первых курсах вузов, является основой для ряда других языков.

[12] **Спам-бот** – это компьютерная программа или группа (пакет) компьютерных программ основной или единственной целью которой является автоматизированная рассылка рекламных сообщений – спама.

[13] **Контроль учетных записей пользователей** (*англ.* User Account Control, UAC) – компонент операционных систем Microsoft Windows, впервые появившийся в Windows Vista. Этот компонент запрашивает.



Нужно было получить права администратора. И один из таких способов – социальная инженерия. Троян-загрузчик притворялся обновлением Adobe Flash Player[14] и при нажатии на Install запрашивал те самые права администратора, что уже не вызывало подозрений у пользователя. Далее троян имитировал процесс обновления и закрывался, выполнив свою задачу.

Этот пример хорошо иллюстрирует природу троянской программы: замаскироваться под видом чего-то вполне легального и выполнить некоторые действия без ведома и разрешения пользователя. Такие программы в подавляющем большинстве случаев служат для вредоносных целей.

Виды троянских программ:

• Удаленный доступ (Backdoors)

Бэкдоры открывают злоумышленникам доступ к управлению зараженным компьютером. Злоумышленник может делать что угодно на захваченном ПК – например, копировать файлы, делать снимки экрана. Так очень часто начинается взлом целой сети предприятия. На зараженной машине находят доступы от других компьютеров в сети – рабочих станций, баз данных, почтовых серверов – и устанавливают на них, например, шифровальщика.

• Дроппер (Dropper)

Название происходит от английского слова drop – сбрасывать. Дроппер несет внутри себя другой вредоносный код, который он запускает (сбрасывает) на зараженном компьютере. Например, дроппер может содержать трояна-кейлоггера, который после запуска маскируется внутри системы и перехватывает весь ввод с клавиатуры.

• Загрузчик (Loader)

Так же, как и дроппер, может запускать на инфицированном компьютере произвольный код без ведома и согласия пользователя. Но, в отличие от дроппера, загрузчик остается резидентным в памяти и может загрузить произвольный файл с удаленного сервера злоумышленника и выполнить его на целевой машине. Обычно загрузчиками пользуются поставщики

[14] **Adobe Flash** (ранее – Macromedia Flash или просто Flash) – мультимедийная платформа компании Adobe Systems для создания веб-приложений или мультимедийных презентаций. Использовалась для создания рекламных баннеров, анимации, игр, а также воспроизведения на веб-страницах видео- и аудиозаписей.Поддержка Adobe Flash была прекращена 31 декабря 2020 года. С 12 января 2021 года при попытке запуска swf-файла через Adobe Flash Player вместо него будет загружена лишь кнопка, ведущая на страницу Adobe с информацией об окончании жизненного цикла платформы.

загрузок (installs), которые продают эти загрузки на теневых форумах. Но об этом мы поговорим позже.

• Банковские трояны

Банковские трояны встречаются наиболее часто. Их используют злоумышленники для кражи доступов в онлайн-банки, платежные системы, а также для кражи номеров кредитных карт. Вообще такие трояны обычно крадут доступы от любых сайтов, будь то ваш личный счет в PayPal или ваш аккаунт на mail.ru. Периодически полученные данные отправляются на удаленный сервер, контролируемый злоумышленником. На языке кардеров [15] подобные данные называются логами[16].

• Трояны, выполняющие DDoS-атаки

Распределенные атаки типа «отказ в обслуживании» (DDoS) продолжают будоражить интернет. В этих атаках к серверу или сети обращается огромное количество запросов, как правило, это делается с использованием ботнетов[17]. В июне 2022 года произошла рекордная DDoS-атака[18]. Источником стал ботнет Mantis, состоящий из зараженных серверов и виртуальных машин. Атака достигала 26 млн запросов в секунду. Представьте, тысячи машин по всему миру слали одновременно 26 млн запросов в секунду! Такую атаку выдержит не каждая DDoS-защита, не то что сайт. Для достижения такой вычислительной мощности необходимо огромное количество ботов. Ботнеты состоят из так называемых компьютеров-зомби. На первый взгляд эти компьютеры работают нормально, однако они также используются при совершении атак. Причиной является троянская программа с бэкдором, незаметно присутствующая на компьютере и при необходимости активируемая оператором. Результатом успешных DDoS-атак является недоступность веб-сайтов или даже целых сетей.

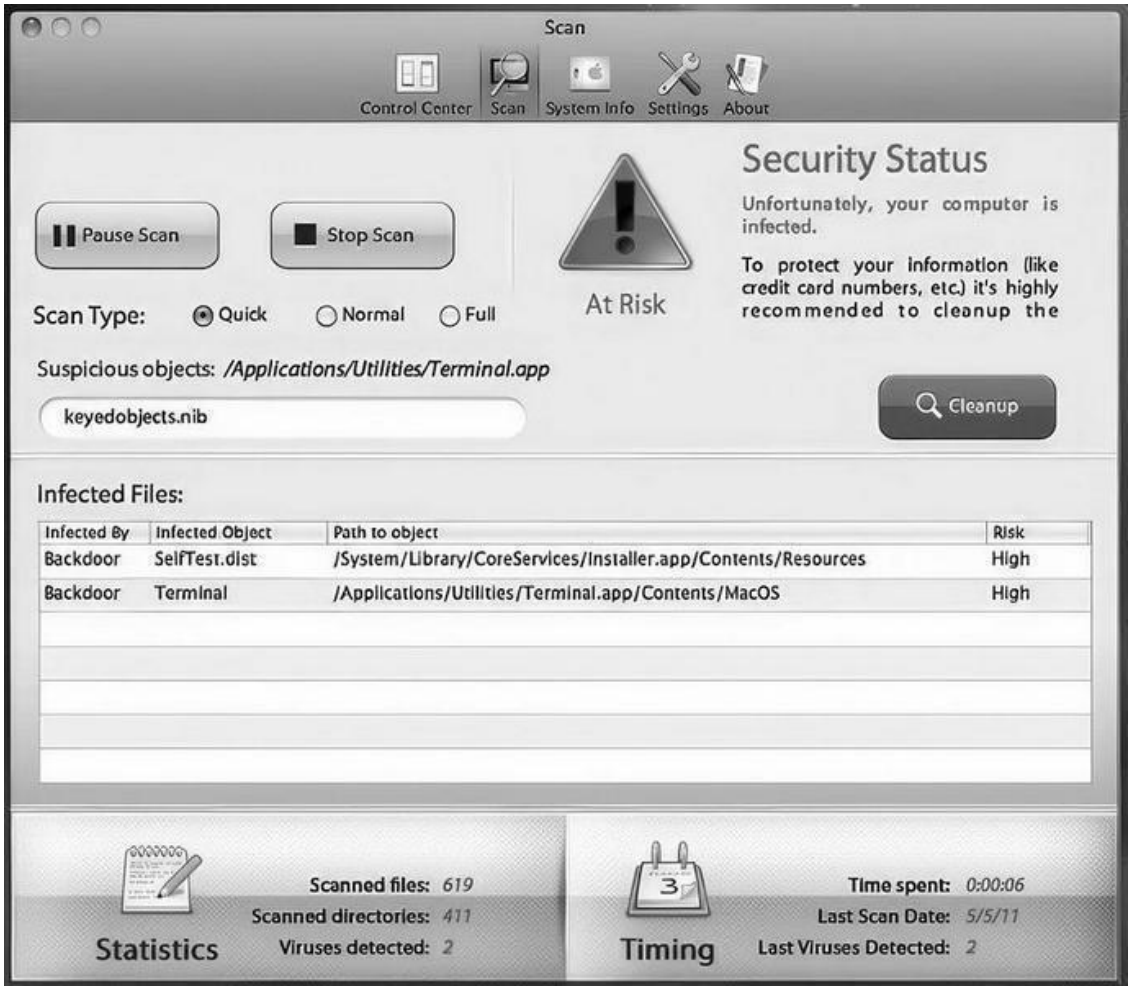
---

[15] **Кардер** (*англ.* Carder) – человек, который ворует деньги с банковских карт.

[16] **Файл журнала** (протокол, журнал; *англ.* log) – файл с записями о событиях в хронологическом порядке, простейшее средство обеспечения журналирования.

[17] **Ботнет** (*англ.* botnet; произошло от слов robot и network) – сеть, состоящая из некоторого количества компьютеров с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на устройство жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов зараженного компьютера.

[18] Источник: https://safe.cnews.ru/news/top/2022-07-20_proizoshla _krupnejshaya_v_istorii



• Трояны, имитирующие антивирусы (Fake AV)

Трояны, имитирующие антивирусы, относятся к классу программ-страшилок (Scareware). Такие лжеантивирусы особенно коварны. Вместо защиты устройства они являются источником серьезных проблем. Эти троянские программы имитируют обнаружение вирусов, тем самым вызывая панику у ничего не подозревающих пользователей и убеждая их приобрести эффективную защиту за определенную плату. Однако вместо полезного инструмента антивирусной проверки вы получаете пустышку, либо, что еще хуже, данные вашей карты попадают к злоумышленникам – кардерам.

• Трояны-вымогатели

Этот тип троянских программ может изменять данные на компьютере, вызывая сбои в его работе, или блокировать доступ к определенным данным. Злоумышленники обещают восстановить работоспособность компьютера или разблокировать данные только после получения требуемого выкупа. Примером такого трояна является шифровальщик. Один из самых резонансных инцидентов с вымогателями-шифровальщиками за последнее время – атака на Colonial Pipeline, компанию, снабжающую топливом часть Восточного побережья США. Шифровальщик уведомляет жертву, что ее компьютер или серверы зашифрованы, а также отправляет личный URL-адрес утечки: украденная информация загружена в интернет и ждет автоматической публикации, если организация не заплатит до определенного срока. Также хакеры сообщают, что удалят все данные жертвы из сети в случае оплаты. Режим ЧП был введен в 18 штатах США. Позже стало известно, что оператор трубопроводов Colonial Pipeline выплатил взломавшей его системы группировке хакеров DarkSide около $5 миллионов в качестве выкупа в криптовалюте сразу через несколько часов после атаки.

Конец ознакомительного фрагмента.