ИСКУССТВО ЦИФРОВОЙ САМОЗАЩИТЫ

Дмитрий Артимович

Annotation

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.

Дмитрий Александрович Артимович
Искусство цифровой самозащиты

© Артимович Д.А., 2023
© ООО «Издательство АСТ», 2023

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.

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.

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 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.

• **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 ВВС 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.

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.

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 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.

• **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.

• **Трояны-прокси**

Программа, предназначенная для анонимного доступа злоумышленника в интернет через компьютер жертвы. Т. е. злоумышленник попросту использует IP-адрес[19] жертвы для выхода в интернет. Прокси обычно используются для рассылки спама, перебора паролей, взлома сайтов или же в схемах обналичивания денег с похищенных карт (когда кардер делает покупку чужой картой в интернет-магазине).

Итак, троянская программа – это такая вредоносная программа, которая проникает на ваш компьютер под видом абсолютно легитимного программного обеспечения, но при этом дает злоумышленнику возможность использовать ресурсы вашего компьютера без вашего ведома (прокси, DDoS-атаки, рассылка спам-сообщений), красть ваши пароли или платежные данные (кейлоггер),

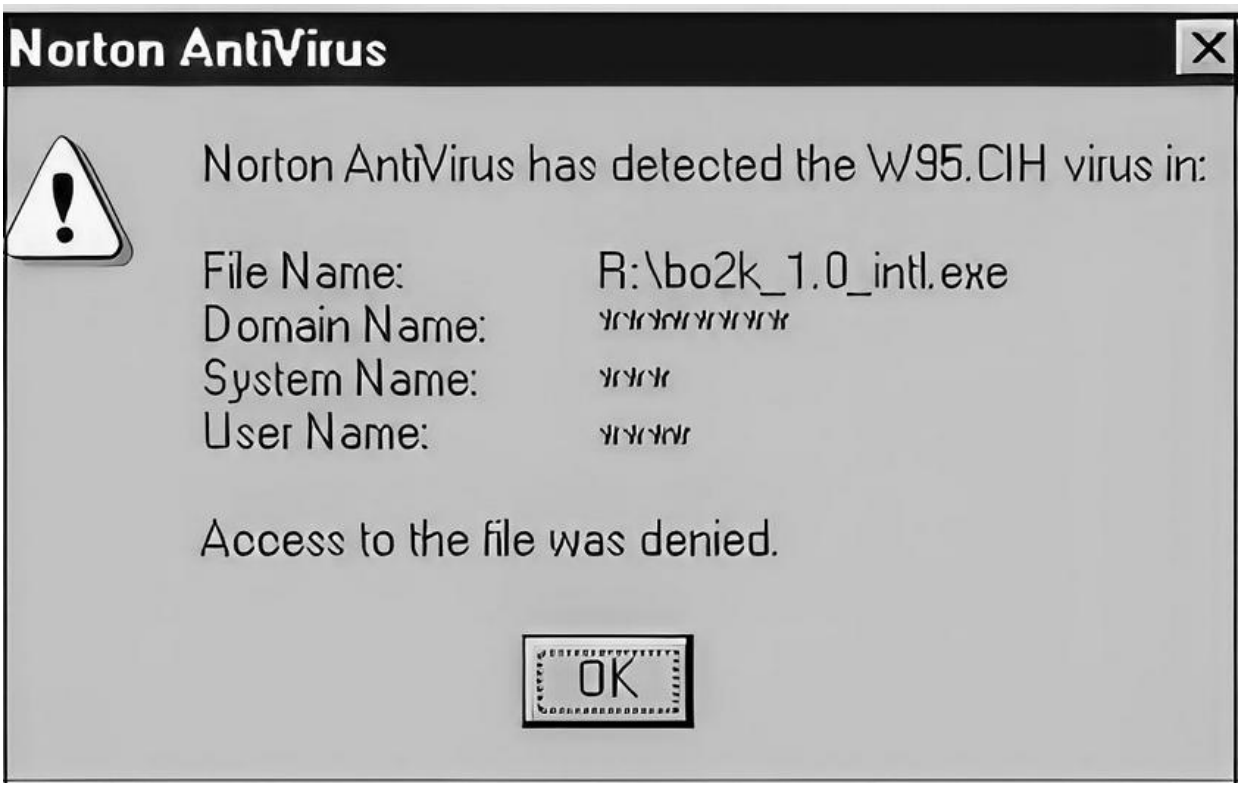
вымогать у вас деньги (шифровальщики) или обманом заставлять купить антивирус-пустышку.

Вирусы

В 2000 году широкой общественности представили новую операционную систему Windows 2000. И мы с братом решили ее попробовать на своем домашнем компьютере скромной конфигурации Intel Celeron 266, 64 Мб памяти, 4 гигабайта hdd. Достали пиратский компакт-диск и запустили инсталлятор прямо из-под Windows 98; система что-то скопировала и ушла в перезагрузку. Windows 2000 установила свой загрузчик, который позволял выбрать либо старую ОС Win98, либо новую Win2000.

Уже на новую Win2000 мы тут же установили свеженький AVP[20]. AVP при старте запустил сканирование и весело захрюкал (при обнаружение вируса антивирус издавал хрюкающий звук), когда нашел множество файлов, зараженных вирусом Virus.Win9x.CIH.

26 апреля 1999 года, в годовщину Чернобыльской аварии, вирус активизировался и уничтожал данные на жестких дисках инфицированных компьютеров. На некоторых компьютерах было испорчено содержимое микросхем BIOS[21]. Именно совпадение даты активации вируса и даты аварии на ЧАЭС дало вирусу второе название – «Чернобыль», которое в народе даже более известно, чем CIH.



По различным оценкам, от вируса пострадало около полумиллиона персональных компьютеров по всему миру. На этих компьютерах сработала «логическая бомба» – была уничтожена информация на жестких дисках и повреждены данные на микросхемах BIOS. По данным The Register, 20 сентября 2000 года власти Тайваня арестовали создателя этого знаменитого компьютерного вируса.

При запуске зараженного файла CIH помещает свой код в память Windows, перехватывая запуск EXE-файлов и записывая в них свою копию. В зависимости от текущей даты вирус способен повреждать данные на Flash BIOS и жестких дисках компьютера.

Компьютерные вирусы – это вредоносное программное обеспечение, часто исполняемые файлы, которые могут копироваться и передаваться с одного компьютера на другой с помощью устройств передачи файлов. Они могут присоединяться к другому исполняемому файлу и передаваться через него. Вирусы подразделяются на два типа: резидентные и нерезидентные.

Нерезидентные вирусы предназначены для распространения путем прикрепления к исполняемому файлу. В нерезидентных вирусах есть два компонента, которые работают следующим образом:

• Модуль поиска, который ищет исполняемые файлы в системе.

• Модуль репликатора, который копирует и прикрепляет копии к найденным исполняемым файлам.

Резидентный вирус работает иначе: у него отсутствует модуль поиска, но он постоянно находится в системной памяти. Каждый раз, когда исполняемый файл запускается на компьютере, он становится целью для модуля репликатора, и копия вируса прикрепляется к исполняемому файлу.

Так и мы с братом подцепили вирус Win9x.CIH, как и многие другие пользователи ПК, которым посчастливилось купить тот самый злополучный диск с новой операционной системой Microsoft Windows 2000. Спасло нас, видимо, то, что CIH работал на старом семействе операционных систем Win9x[22], а мы обнаружили и удалили его уже под системой семейства WinNT[23]. У вируса попросту не было возможности активироваться.

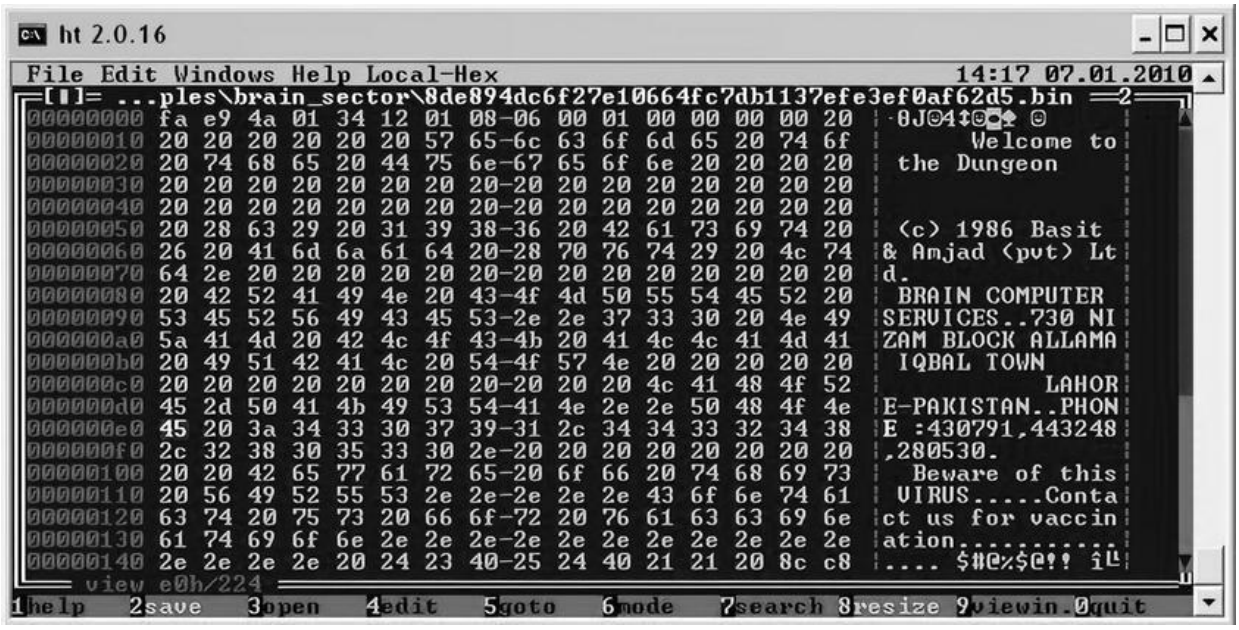
Если уйти в историю, то первым компьютерным вирусом для персонального компьютера под управлением операционной системы MS-DOS и первым вирусом, вызвавшим глобальную эпидемию в 1986 году, был Brain (с *англ.* – мозг). Brain написали два брата из Пакистана, Базит и Амжад Фарук Альви, в целях отслеживания пиратских копий их медицинского программного обеспечения, и он не был нацелен на причинение вреда. Братьям тогда было 17 и 24 года.

Заражение компьютера происходило путем записи копии вируса в загрузочный сектор дискеты[24]. Старая информация переносилась в другой сектор и помечалась как «поврежденная». Метка тома изменялась на ©Brain.

У братьев была компьютерная фирма Brain Computer Services, и вирус они написали, чтобы отслеживать пиратские копии их медицинского софта. Пиратская программа отжирала оперативку, замедляла работу диска и иногда мешала сохранить данные. По заверениям братьев, она не уничтожала данные.

Brain «не умел» работать с разделами жестких дисков, поэтому в него была встроена проверка, не позволявшая ему заражать жесткий диск. Это отличает его от многих вирусов того времени, которые не обращали внимания на разделы, что приводило к уничтожению данных.

Благодаря относительной «миролюбивости» вирус часто оставался незамеченным, особенно когда пользователь не обращал внимания на замедление работы дискет.



Программа содержала следующее сообщение:

Welcome to the Dungeon 1986 Basit & Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES 730 NIZAB BLOCK ALLAMA IQBAL TOWN LAHORE-PAKISTAN PHONE: 430791,443248,280530. Beware of this VIRUS… Contact us for vaccination… $#@%$@!!

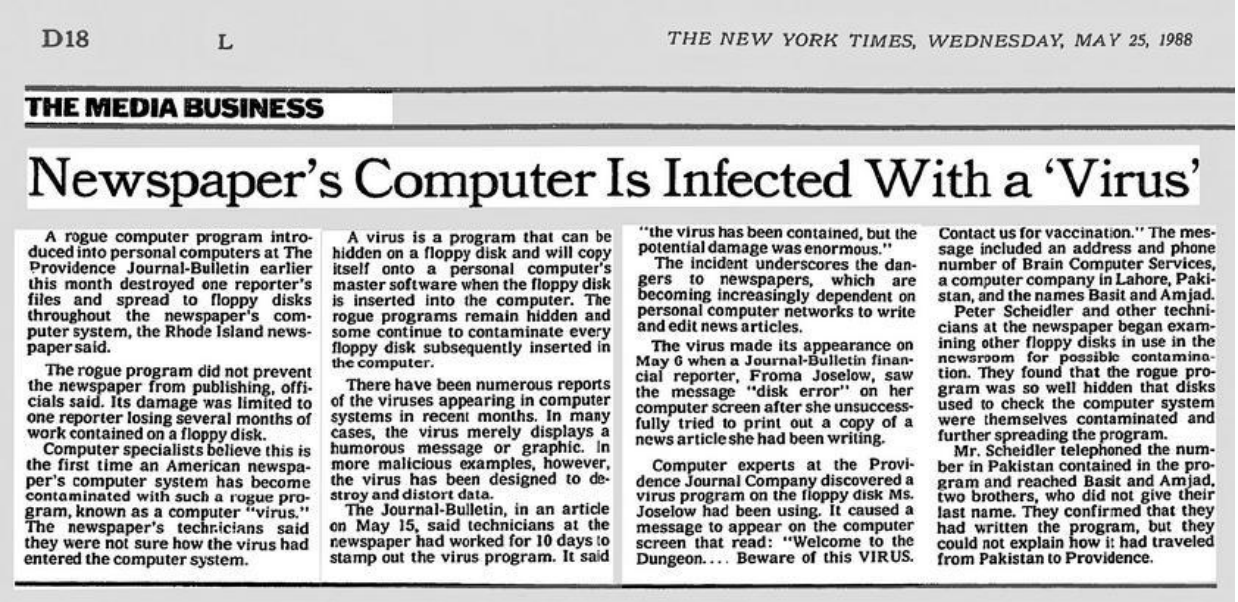
«Добро пожаловать в подземелье… Берегитесь этого вируса… Свяжитесь с нами для лечения…»

В заголовке были указаны реальные контакты. Когда кто-либо звонил им за помощью, они могли идентифицировать пиратскую копию. Также вирус подсчитывал количество сделанных копий.

Братья обнаружили, что пиратство было широко распространено, и копии их программ распространялись очень далеко. Амжад говорит, что первый звонок к ним поступил из США, Майами.

Это был первый из множества звонков из США. Проблема оказалась в том, что Brain распространялся и по другим дискетам, а не только по копиям их программы. В Университете Делавера в 1986 году даже случилась эпидемия этого вируса, а затем он появлялся и во многих других местах. Исков подано не было, но в газетах про это

писали много. Создателей даже упоминали в журнале Time Magazine в 1988 году.



D18 L THE NEW YORK TIMES, WEDNESDAY, MAY 25, 1988

THE MEDIA BUSINESS

Newspaper's Computer Is Infected With a 'Virus'

A rogue computer program introduced into personal computers at The Providence Journal-Bulletin earlier this month destroyed one reporter's files and spread to floppy disks throughout the newspaper's computer system, the Rhode Island newspaper said.

The rogue program did not prevent the newspaper from publishing, officials said. Its damage was limited to one reporter losing several months of work contained on a floppy disk.

Computer specialists believe this is the first time an American newspaper's computer system has become contaminated with such a rogue program, known as a computer "virus." The newspaper's technicians said they were not sure how the virus had entered the computer system.

A virus is a program that can be hidden on a floppy disk and will copy itself onto a personal computer's master software when the floppy disk is inserted into the computer. The rogue programs remain hidden and some continue to contaminate every floppy disk subsequently inserted in the computer.

There have been numerous reports of the viruses appearing in computer systems in recent months. In many cases, the virus merely displays a humorous message or graphic. In more malicious examples, however, the virus has been designed to destroy and distort data.

The Journal-Bulletin, in an article on May 15, said technicians at the newspaper had worked for 10 days to stamp out the virus program. It said "the virus has been contained, but the potential damage was enormous."

The incident underscores the dangers to newspapers, which are becoming increasingly dependent on personal computer networks to write and edit news articles.

The virus made its appearance on May 6 when a Journal-Bulletin financial reporter, Froma Joselow, saw the message "disk error" on her computer screen after she unsuccessfully tried to print out a copy of a news article she had been writing.

Computer experts at the Providence Journal Company discovered a virus program on the floppy disk Ms. Joselow had been using. It caused a message to appear on the computer screen that read: "Welcome to the Dungeon.... Beware of this VIRUS. Contact us for vaccination." The message included an address and phone number of Brain Computer Services, a computer company in Lahore, Pakistan, and the names Basit and Amjad.

Peter Scheidler and other technicians at the newspaper began examining other floppy disks in use in the newsroom for possible contamination. They found that the rogue program was so well hidden that disks used to check the computer system were themselves contaminated and further spreading the program.

Mr. Scheidler telephoned the number in Pakistan contained in the program and reached Basit and Amjad, two brothers, who did not give their last name. They confirmed that they had written the program, but they could not explain how it had traveled from Pakistan to Providence.

New York Times писала в мае 1988-го: «Дерзкая компьютерная программа, которая в этом месяце появилась на компьютерах “Бюллетеня Провиденса”, уничтожила файлы одного корреспондента и распространилась через дискеты по всей сети газеты. Компьютерщики считают, что это первый случай заражения компьютерной системы американской газеты такой дерзкой программой, которую называют компьютерным вирусом».

Братьям Альви пришлось сменить телефоны и убрать контакты из поздних версий вируса. Продажи программы они прекратили в 1987 году. Их компания выросла в телекоммуникационного провайдера, и сейчас это крупнейший провайдер в Пакистане. Расположена она всё по тому же адресу.

Итак, компьютерный вирус – это такая вредоносная программа, которая может распространять сама себя путем внедрения своего кода в другие программы, загрузочные сектора дисков, системные области памяти. Главное отличие вируса от троянской программы – в его способности к самораспространению через заражение. Кроме того, часто его сопутствующей функцией является

нарушение работы программно-аппаратных комплексов – удаление файлов, удаление операционной системы, приведение в негодность структур размещения данных, нарушение работоспособности сетевых структур, кража личных данных, вымогательство, блокирование работы пользователей и т. п. Т. е. вирус может распространяться через заражение файлов, но нести в себе функционал троянской программы. А вот троянская программа представляет из себя отдельный исполняемый файл, который сам по себе распространяться не может.

Хотя вирусы и остаются ощутимой угрозой, время их массового создания и распространения уже прошло. Интернет стал доступен практически каждому, а программы теперь просто скачиваются, а не продаются на дисках. Злоумышленникам стало дешевле и проще заражать пользователей в сети, используя эксплойты, вместо того чтобы писать саморазмножающиеся вирусы.

Один из последних случаев массового заражения компьютерным вирусом произошел в далеком 2004 году. Началось всё с того, что вирус ILoveYou был разослан на почтовые ящики с Филиппин в ночь с 4 на 5 мая 2000 года. В теме письма содержалась строка ILoveYou, отсюда и его название, а к письму был приложен скрипт LOVE-LETTER-FOR-YOU.TXT.vbs[25]. В большинстве случаев пользователь открывал вложение. При открытии вирус рассылал копию самого себя всем контактам в адресной книге Microsoft Outlook. Он также перезаписывал файлы определенных типов и распространялся через IRC-каналы, создавая файл LOVE-LETTER-FOR-YOU.HTM в системном каталоге Windows. В общей сложности вирус поразил более 5 миллионов компьютеров по всему миру. Предполагаемый ущерб, который червь нанес мировой экономике, оценивается в размере до 15 миллиардов долларов, за что вирус вошел в Книгу рекордов Гиннесса как самый разрушительный в мире.

Со временем вирусописателям пришлось выдумывать различные способы противостоять антивирусам, поэтому появились полиморфные и метаморфные вирусы.

Полиморфные вирусы

Полиморфный вирус – сложный компьютерный вирус, он зашифрован с помощью переменного ключа шифрования. У такого вируса есть небольшая часть – декриптор (дешифратор), он получает управление при запуске вируса и расшифровывает основное тело. Поэтому каждая копия отличается от других. Другими словами, это зашифрованный вирус, разработанный для предотвращения обнаружения антивирусным программным обеспечением или сканером.

Предположим, что один пользователь зашел на сайт и скачал исполняемый файл. Затем другой пользователь переходит по той же ссылке и загружает тот же исполняемый файл. Оба пользователя получают два разных файла. Несмотря на то что код самого вируса одинаков, он каждый раз шифруется разными ключами. Поэтому полиморфный вирус трудно обнаружить с помощью сканеров и антивирусного программного обеспечения. В таких случаях антивирусу нужно расшифровать код вируса и уже потом проверить его по базе сигнатур. Для этого в антивирусах существует эвристический анализатор.

Метаморфные вирусы

Метаморфный вирус – вирус, который изменяет свой собственный код. Он переводит свой собственный код и создает временное представление. Затем он редактирует это временное представление и записывает себя обратно в обычный код. Другими словами, он переводит и переписывает свой собственный код, чтобы каждый раз копии вируса выглядели по-разному.

Метаморфный вирус не использует метод шифрования ключей, как в полиморфном вирусе. Когда вирус создает новую собственную копию, он преобразует существующие инструкции в функциональные эквиваленты. Поэтому ни одна секция вируса не остается постоянной, и вирус не вернется к своей первоначальной форме во время выполнения. Следовательно, антивирусное программное обеспечение не сможет его обнаружить по базе сигнатур.

Черви

Сетевой червь – разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные (интернет) компьютерные сети.

Червь в некоторой степени считается подклассом вирусов. Черви распространяются от компьютера к компьютеру, но, в отличие от вирусов, они имеют возможность путешествовать без любого человеческого действия. Самой большой опасностью червя является его способность копировать себя на вашей системе – тем самым он может посылать сотни и тысячи копий самого себя.

Ранние эксперименты по использованию компьютерных червей в распределенных вычислениях провели в исследовательском центре Xerox в Пало-Альто Джон Шоч (John Shoch) и Йон Хупп (Jon Hupp) в 1978 году. Термин «червь» возник под влиянием научно-фантастических романов «Когда ХАРЛИ исполнился год» Дэвида

Герролда (1972), в котором были описаны червеподобные программы, и «На ударной волне» (*англ.*) Джона Браннера (1975), где вводится сам термин.

Червь Морриса

Одним из наиболее известных компьютерных червей является червь Морриса, написанный в 1988 году Робертом Моррисом-младшим, который был в то время студентом Корнеллского Университета.

Роберт родился в 1965 году, его отец был специалистом в области криптографии, работал в Bell Labs и помогал в разработке Multics и Unix. То есть будущему программисту было у кого поучиться.

Роберт хорошо учился в школе, поэтому постигать азы науки парня отправили в Гарвард, после чего он продолжил получать образование в Корнеллском университете. Будучи студентом первого курса, Моррис-младший и натворил дел. «Всё в познавательных целях», – уверял позже Роберт.

Дополнительной драмы добавляло то, что его отец в то время уже являлся сотрудником Агентства национальной безопасности. Он занимал руководящий пост в подразделении, ответственном за IT-безопасность систем федерального правительства.

Червь Морриса нередко называют первым сетевым червем, однако он может считаться таковым лишь потому, что это первая подобная программа, расползшаяся чуть ли не по всему интернету. Интернет, напомним, тогда был совсем небольшим и имел мало общего с тем, что позже придумал Тим Бернерс-Ли[26].


The Morris Internet Worm source code
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.
The worm was the first of many intrusive programs that use the Internet to spread.
Computer History Museum
Internet Worm - Source code
X1204.96 A-D

Роберт задумывал свое детище якобы как экспериментальный проект. Он должен был измерить тот самый интернет – об этом программист заявил позже. Оригинальный мотив в 1988 году мог быть иным. На это указывает и то, что парень тщательно пытался замести следы, отправляя червя в свободное плавание из кампуса MIT.

Код писался для запуска на компьютерах VAX компании Digital Equipment Corporation и SUN под управлением BSD UNIX[27]. Роберт использовал несколько уязвимостей, в том числе в программах sendmail (отвечает за работу с электронной почтой) и fingerd (получение некоторых данных о пользователе). Также эксплуатировались иные дыры, позволявшие узнать пароли локального пользователя.

В sendmail, например, после ряда исправлений имелся баг: в определенных условиях можно было запустить дебаг (внезапно:

отправив команду debug). Тогда sendmail позволяла вместо адресов указывать дополнительные инструкции. На деле, конечно, всё не так просто, но и особых изысков Роберту придумывать не пришлось.

Парень посчитал, что админы очень скоро заметят вторжение и предпримут шаги для защиты. Например, заставят червя думать, что его копия уже установлена. 23-летний программист учел и это. Его код действительно проверял наличие копии себя на чужом компьютере, однако в 14 % случаев устанавливался, невзирая на полученный отклик. Есть фейк? Всё равно установлюсь. Есть другая копия? Да кто ж поймет, всё равно установлюсь.

Оказавшись на удаленном компьютере (первыми под удар попали знакомые ему скрытые университетские и исследовательские сети), червь сканировал окружение на наличие других компьютеров и копировался на них. Роберт не ожидал прыти, которую продемонстрировал его код. Ведь условие 14 %, как несложно догадаться, хоть и выполнялось, но было бессмысленным: программа наматывала «круги» по сети.

Серверы тем временем раз за разом выполняли бесконечные команды, подаваемые червем, полностью парализующим работу систем: программа Морриса работала исключительно в оперативной памяти. Данный факт также не позволял изучить файлы червя, которые удалялись в случае отключения.

Заново включенный в сеть компьютер опять становился жертвой, и самым эффективным способом справиться с напастью в тот момент было полное отключение компьютера от сети. Только после этого администраторы могли убрать нагрузку и «вылечить» машину. Если знали, что и где искать.

Роберт Моррис испугался того, что натворил. Как следует из отчета по итогам расследования инцидента, он предпринял попытки остановить эпидемию («рубильник», само собой, предусмотрен не был), но не слишком активные. Студент не стал во всеуслышание рассказывать о черве и информировать ответственных, однако позвонил приятелю с просьбой опубликовать анонимные извинения и руководство по «лечению».

Инженеры из Беркли активно работали над поиском и препарированием компонентов программы. Через 12 часов им удалось продумать все необходимые алгоритмы и подготовить заплатки, однако

их распространению мешал… да, червь Морриса, из-за которого целые сети либо «лежали», либо были отключены от внешнего мира. Потребовалось несколько дней, чтобы успокоить бурю, поднятую начинающим программистом.

Для понимания масштабов «шухера», который натворил червь, перечислим агентства, организации и ведомства, привлеченные к решению проблемы. Это Центр национальной компьютерной безопасности, Национальный институт науки и технологий, Агентство военной связи, DARPA, Министерство энергетики США, Лаборатория баллистических исследований, Ливерморская национальная лаборатория имени Лоуренса, ЦРУ, Калифорнийский университет в Беркли, Массачусетский технологический институт, институт SRI International и ФБР.

Считается, что червь Морриса заразил около 6 тыс. компьютеров – примерно 10 % от всех, что были подключены в то время к интернету. Ущерб в зависимости от важности владельцев компьютеров оценивали в диапазоне от $200 до $53 тыс. за систему (традиционно речь идет о «предполагаемом», то есть гипотетическом ущербе). Власти называли общую сумму ущерба в диапазоне от $100 тыс. до $10 млн, которая с годами превратилась в $95–100 млн и 60 тыс. зараженных компьютеров. Более вероятными представляются всё же первоначально озвученные цифры.

На определение авторства ушло время. Есть версия, согласно которой отец 23-летнего парня рекомендовал ему самому рассказать о себе властям. Походит на правду, учитывая пост Морриса-старшего и его непосредственную связь с правительством и нацбезопасностью.

Механизмы распространения

Все механизмы («векторы атаки») распространения червей делятся на две большие группы:

• Использование уязвимостей и ошибок администрирования в программном обеспечении, установленном на компьютере. Червь Морриса использовал известные на тот момент уязвимости в программном обеспечении – а именно в почтовом сервере sendmail, сервисе finger – и подбирал пароль по словарю. Такие черви способны

распространяться автономно, выбирая и атакуя компьютеры в полностью автоматическом режиме.

• Средства так называемой социальной инженерии провоцируют запуск вредоносной программы самим пользователем. Чтобы убедить пользователя в том, что файл безопасен, могут подключаться недостатки пользовательского интерфейса программы – например, червь VBS.LoveLetter (рассмотренный выше вирус ILOVEYOU) использовал тот факт, что Outlook Express скрывает расширения файлов. Данный метод широко применяется в спам-рассылках, социальных сетях и т. д.

Иногда встречаются черви с целым набором различных векторов распространения, стратегий выбора жертвы, и даже эксплойтов под различные операционные системы.

Структура

Черви могут состоять из различных частей.

Часто выделяют так называемые резидентные черви, которые могут инфицировать работающую программу и находиться в ОЗУ, при этом не затрагивая жесткие диски. От них можно избавиться перезапуском компьютера (и, соответственно, сбросом ОЗУ). Такие черви состоят в основном из «инфекционной» части: эксплойта (шелл-кода) и небольшой полезной нагрузки (самого тела червя), которая размещается целиком в ОЗУ. Специфика заключается в том, что они не загружаются через загрузчик, как все обычные исполняемые файлы, а значит, могут рассчитывать только на те динамические библиотеки, которые уже были загружены в память другими программами.

Также существуют черви, которые после успешного инфицирования памяти сохраняют код на жестком диске и принимают меры для последующего запуска этого кода (например, путем прописывания соответствующих ключей в реестре Windows). От таких червей можно избавиться только при помощи антивирусного программного обеспечения или подобных инструментов. Зачастую инфекционная часть таких червей (эксплойт, шелл-код) содержит небольшую полезную нагрузку, которая загружается в ОЗУ и может «догрузить» по сети непосредственно само тело червя в виде отдельного файла. Загружаемое таким способом тело червя (обычно

отдельный исполняемый файл) теперь отвечает за дальнейшее сканирование и распространение уже с инфицированной системы по локальной сети, а также может содержать более серьезную, полноценную полезную нагрузку, целью которой может быть, например, нанесение какого-либо вреда (к примеру, DoS-атаки).

Большинство почтовых червей распространяются как один файл. Им не нужна отдельная «инфекционная» часть, так как обычно пользователь-жертва при помощи почтового клиента или интернет-браузера добровольно скачивает и запускает червя целиком.

> ***Дам определение еще раз: сетевой червь – это вредоносная программа, самостоятельно распространяющаяся через локальные и глобальные компьютерные сети. Ключевое отличие от вируса – именно в распространении через сети, а не через заражение других исполняемых файлов.***

Сетевой червь

Эксплойты

Программы, будь то игры, вебсайты или приложения под смартфоны, пишут программисты. А программист, насколько бы хорошим он ни был, прежде всего человек. Как сказал Цицерон, каждому человеку свойственно ошибаться… Вот и программисты при разработке делают ошибки в коде. Иногда из-за таких ошибок программа некорректно себя ведет или просто падает, а иногда ошибка (далее будем называть ее уязвимостью) позволяет выполнить некий привилегированный набор команд.

Например, червь Морриса эксплуатировал переполнение буфера утилиты finger, изначально предназначенной для удаленного определения времени подключения пользователя к рабочей станции, а написан он был аж в 1988-м. 34 года спустя переполнение буфера – до сих пор одна из самых распространенных уязвимостей. Хотя описание работы этой атаки выходит за рамки данной книги и скорее относится уже к специализированной технической литературе, попробую объяснить кратко и понятно для человека, далекого от программирования.

Программы работают с разными порциями данных, под которые в оперативной памяти выделяются участки, называемые буферами. Эти данные могут приходить из сети, от ввода пользователя с клавиатуры, с диска и т. д. Уязвимость появляется тогда, когда разработчик забывает проверить размер полученных данных, т. е. если данных получено больше, чем размер буфера. При грамотном использовании атаки переполнение позволяет вставить в программу вредоносный код, который, например, может скачать с удаленного компьютера вирус и запустить на вашей машине.

Как всё это использовать злоумышленнику в реальности? В первую очередь нас интересуют уязвимости в браузерах. Да, браузеры пишут тоже люди, и ошибок в них хватает. А для использования этих ошибок и появляются эксплойты.

Эксплойты (exploits) – подвид вредоносных программ. Термин связан с английским глаголом to exploit, означающим «эксплуатировать, применять в своих интересах».

Для пользователя основную опасность, как я уже писал выше, представляют эксплойты под различные браузеры. Такой набор эксплойтов называют связкой.

Как работает заражение компьютеров при просмотре сайтов в интернете? Злоумышленник взламывает чужие сайты (в основном также из-за наличия уязвимостей) и устанавливает на них свой вредоносный код – связку эксплойтов. При каждом посещении сайта вредоносный код активируется, подбирает к конкретному браузеру и операционной системе нужный эксплойт – код, который использует конкретную уязвимость конкретного браузера под конкретную операционную систему. В случае успешного срабатывания эксплойта в ваш браузер или набор команд выполняется внедренный злоумышленникам код. Обычно это команда скачать и запустить трояна-загрузчика. Троян-загрузчик позже может загружать к вам на систему произвольные исполняемые файлы. На черном рынке такая успешная загрузка и запуск файла называется установкой (от английского install).

На практике всё чуточку сложнее. Конечно же, на каждый взломанный сайт не копируют связку эксплойтов. Обычно сама связка располагается на отдельном хостинге[28]. А на взломанных сайтах просто ставят фреймы со ссылками на связку. Такой вариант куда проще и элегантнее. Отсюда вытекает и другое следствие: злоумышленники могут просто покупать фреймовый трафик[29]. Т. е. внутри основного HTML[30] сайта вставляется очень-очень маленькое окно фрейма размером 1 на 1 пиксель, в котором загружается вредоносный URL[31] на связку эксплойтов. Очень часто такой трафик продают сайты «для взрослых» – учтите это, если захотите посетить подобные ресурсы.

Тут мы плавно перешли к разделению труда на черном рынке киберкриминала. Есть некий образ хакера, навязанный нам массмедиа и Голливудом. Некий криминальный гений, способный сломать любую защиту и украсть что угодно у кого угодно. Обычно же люди, которые пишут связки эксплойтов, банковские трояны, продают загрузки или трафик, – это разные персонажи.

Пишут эксплойты и трояны, безусловно, хакеры. Для создания такого вредоносного кода нужно хорошо разбираться в программировании и конкретно врубаться в то, как функционирует компьютер на низком уровне. Слово Hacker как раз и произошло от английского глагола to hack – врубаться.

Используют связки эксплойтов люди, обычно далекие от программирования, – загрузчики (так их называют на теневых форумах). И пытаются они выжать из вашего ПК максимум. Поэтому я и написал, что эксплойт устанавливает у вас на машине трояна-загрузчика. После чего загрузки (установки другого вредоносного ПО) продаются во много рук. Так что не удивляйтесь, что ваш компьютер

начал слать спам, ддосить, да еще и вымогать у вас деньги одновременно. Скорее всего, это три разных трояна.

Эксплойты бывают не только для браузеров, а еще для:

• операционных систем (например, для обхода UAC в Windows);

• прикладного программного обеспечения (например, вирус ILoveYou эксплуатировал ошибки безопасности в почтовом клиенте Microsoft Outlook);

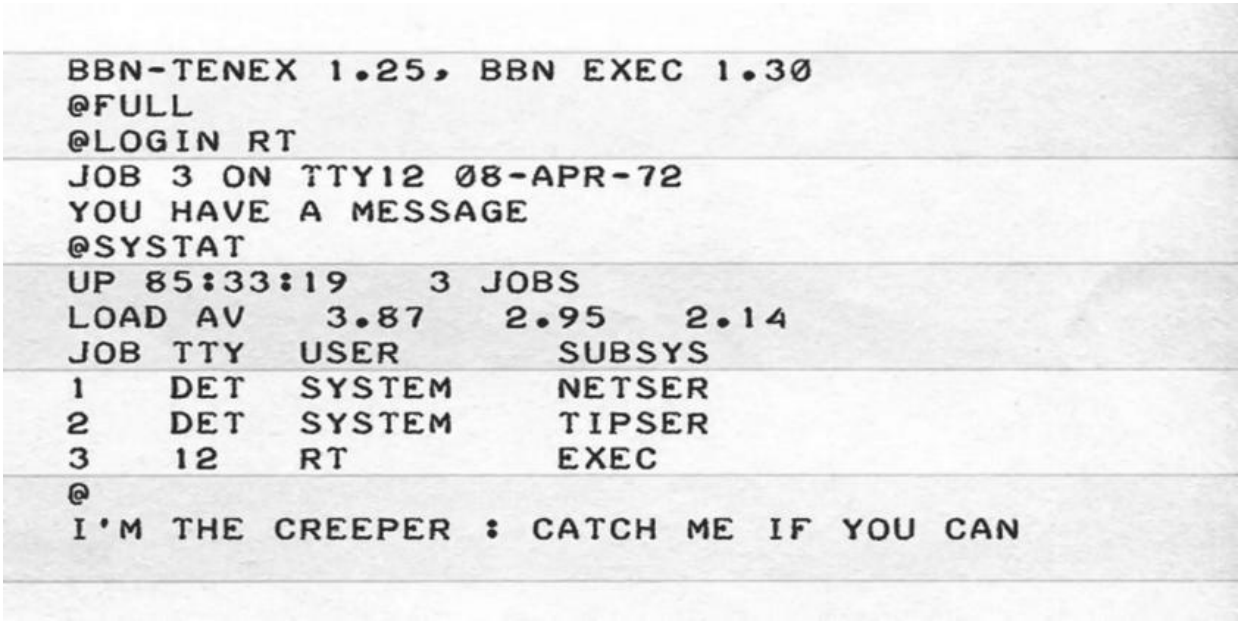
• веб-сервисов (например, уязвимости в популярном движке создания блогов WordPress);

• аппаратных компонентов.

Антивирусы

I’m the Creeper: catch me if you can.

«Я Creeper: поймай меня, если сможешь». 1971 год, эта фраза стала появляться перед глазами изумленных пользователей компьютеров, входящих в сеть ARPANET[32]. Что же означает эта фраза?



Это была визитная карточка Creeper – первого компьютерного вируса в истории, разработанного Бобом Томасом, программистом из BBN Technologies. Хотя сообщение и смущало, но намерения Томаса были безвредными. Его цель состояла в том, чтобы создать программу, которая могла бы сама перемещаться между компьютерами. И он этого добился.

После заражения компьютера Creeper выводил свое сообщение на экране или печатал на принтере. Не успев закончить печать, переходил к следующему компьютеру в сети, исчезая с предыдущего.

Впервые было создано программное обеспечение, способное автоматически передаваться с одного компьютера на другой. Это также привело к созданию его заклятого врага – первого в истории антивируса Reaper.

Reaper явно был ответом Creeper’у. Просто обратите внимание на игру слов: Creeper означает «ползун», Reaper – «жнец». Достоверных сведений о том, кто разработал Reaper, нет. Одни версии утверждают, что это был сам Боб Томас, другие – что это дело рук Рэя Томлинсона, известного создателя электронной почты. Правда в том, что Reaper был очень эффективен в своем назначении: как только он обнаруживал атаку Creeper, он удалял вирус из системы, предотвращая распространение на другие компьютеры.

Некоторые усомнились бы в «вирусном» характере Creeper’а, поскольку он не размножался, а путешествовал с одного компьютера на другой. На самом деле ни понятия вируса, ни понятия антивируса в то время не существовало. Однако если вы не уверены, что Creeper действительно был первым вирусом, мы можем поговорить о первом вирусе в истории, который также был вредоносным, – Rabbit.

Rabbit появился вскоре после Creeper’а, в 1972 году. Основное отличие состоит в том, что Rabbit воспроизводил себя на зараженном компьютере до тех пор, пока не вторгался в систему и не вызывал ее сбой. Спустя годы появились некоторые из его преемников, такие как Elk Cloner в 1981 году, поразивший Apple II и передававшийся через загрузочные дискеты операционной системы, или Brain, первый компьютерный вирус, разработанный в 1986 году.

История Brain интересна и заслуживает внимания. Brain был одним из первых вирусов массового распространения (в то время он заразил около 20 000 компьютеров, что немаловажно) и передавался через нелегальные копии MS-DOS, чтобы контролировать их и предотвращать их распространение. Оказавшись внутри системы, он отправлял сообщение пользователю, предупреждая его о заражении и предоставляя контактные данные для решения проблемы. Правда в том, что эта небольшая история вирусов и антивирусов подчеркивает тот факт, что в мире компьютеров нелегко понять, какое небольшое событие может в конечном итоге привести к глобальным изменениям. Концепция, разработанная в анекдотическом и безобидном эксперименте, таком как Creeper, в конечном итоге извратилась до такой степени, что породила проблему, затрагивающую всех, и даже привела к созданию компаний-миллионеров, таких как производители антивирусов, основная деятельность которых состоит именно в том, чтобы покончить с потомками мелкой лианы.

РОЖДЕНИЕ КОММЕРЧЕСКОГО АНТИВИРУСА

1987 – McAfee

В 1987 году на рынок впервые были выпущены антивирусные продукты. До сих пор неясно, кто разработал первый продукт, и существует несколько версий. Наиболее значительной из них является VirusScan – продукт, созданный молодым программистом британского происхождения Джоном Макафи.

Это было началом антивирусного взрыва, и к концу десятилетия на рынке появилось множество антивирусных решений. Эти ранние программы состояли из простых сканеров, которые выполняли контекстный поиск для обнаружения уникальных последовательностей кода вируса. Сканеры включали «иммунизаторы», которые модифицировали программы, чтобы вирусы считали, что компьютер уже заражен и поэтому не атаковали его. Это работало только в течение короткого промежутка времени, поскольку иммунизаторы становились неэффективными, когда количество вирусов увеличивалось и они становилось всё более изощренными.

Хотя Джон Макафи покинул компанию еще в 1994 году, а сама компания несколько раз перепродавалась, выпускаемый антивирус до сих пор носит название McAfee Antivirus.

1987 – G DATA

G Data была основана в Германии в 1985 году, ее создали Кай Фигге и Андреас Лунинг. Они выпустили свой первый антивирус под названием Anti-Virus Kit (AVK) в 1987 году.

1987 – ESET

Компания ESET была основана Петером Пасько, Мирославом Трнкой и Рудольфом Хруби в 1992 году, но антивирус они сделали раньше. Первый антивирус ESET под названием NOD был создан в 1987 году.

1988 – Avira

Компания Avira была основана как H+BEDV Тьярком Ауэрбахом в 1986 году в Германии. В 2006 году H+BEDV и AntiVir стали называться Avira. H+BEDV выпустила свой AntiVir в 1988 году.

1988 – Avast

Avast Software была основана как ALWIL Software Павлом Баудишем и Эдуардом Кучерой в Чешской Республике в 1988 году. В 2010 году ALWIL Software стала Avast Software. Они выпустили свой Avast antivirus в 1988 году.

1988 – AhnLab

Ан Чеол-Су запустил свой антивирус под названием V1 в 1988 году. Позднее, в 1995 году, он основал компанию AhnLab в Южной Корее.

1988 – Антивирусный инструментарий доктора Соломона

В 1988 году Алан Соломон основал S&S International в Великобритании. Он создал свой антивирус под названием Dr. Solomon’s Anti-Virus Toolkit в 1988 году.

1988 – Sophos

Компания Sophos была основана Яном Хруска и Питером Ламмером в 1985 году в Англии. Они продемонстрировали свой антивирус под названием Vaccine в 1988 году.

1989 – Kaspersky

Kaspersky был основан Евгением Касперским, его женой Натальей Касперской и их коллегами Алексеем Де-Мондериком и Вадимом Богдановым в 1997 году. Ранее, в 1989 году, Евгений Касперский написал свой первый инструмент для удаления вирусов Cascade.1704. С 1991 по 1997 год Касперский разрабатывал антивирусную программу AVP (AntiViral Toolkit Pro) для Центра информационных технологий КАМИ. После основания своей компании он переименовал AVP (AntiViral Toolkit Pro) в Антивирус Касперского. Нынешний Антивирус Касперского существует с 1989 года.

1989 – F-PROT

В 1989 году Фриорик Скуласон создал антивирус F-PROT. Позже, в 1993 году, он основал в Исландии компанию FRISK Software. В 1991

году F-PROT выпустила свой антивирус с первым в мире эвристическим сканером поведения.

1989 – Symantec

Symantec была основана Гэри Хендриксом в 1982 году в Соединенных Штатах Америки. Компания выпустила свой первый антивирусный продукт для Macintosh под названием Symantec Antivirus for the Macintosh (SAM) в 1989 году.

1990 – Panda

В 1990 году Микель Уризарбаррена основал Panda Software и создал свой первый антивирусный продукт под названием Panda AntiVirus. Panda Software стала Panda Security в 2007 году.

1990 – Trend Micro

Компания Trend Micro была основана Стивом Чангом, его женой Дженни Чанг и ее сестрой Евой Чен в США в 1988 году. В 1990 году Trend Micro представила свой антивирусный продукт под названием PC-cillin.

1991 – VirIT eXplorer

В 1991 году Джанфранко Тонелло создал в Италии свое антивирусное программное обеспечение под названием VirIT eXplorer. В 1992 году он основал свою компанию под названием TG Soft.

1991 – Norton

В 1990 году Symantec приобрела компанию Peter Norton Computing, основанную Питером Нортоном в 1982 году. На момент приобретения Peter Norton Computing не разрабатывала никаких антивирусных продуктов. В 1991 году Symantec выпустила Norton AntiVirus 1.0 (NAV).

1992 – AVG

AVG Technologies была основана как Grisoft Software Яном Грицбахом и Томасом Хофером в 1991 году в Чехии. В 2008 году Grisoft стала называться AVG Technologies. В 2016 году Avast Software

приобрела AVG Technologies. Компания Grisoft запустила свой AntiVirus Guard (AVG) в 1992 году.

1993 – Dr.Web

В 1992 году Игорь Данилов выпустил пакет SpiderWeb, который состоял из трех программ – Spider, Dr.Web и программа проверки диска Scorpion. Автономный антивирус Dr.Web был выпущен в 1993 году. В 2003 году Игорь Данилов основал в России компанию Dr.Web.

1994 – F-Secure

F-Secure была основана как Data Fellows в 1988 году в Финляндии. В 1999 году Data Fellows стала F-Secure. Антивирус Data Fellows был выпущен в 1994 году. F-Secure была первой компанией, разработавшей технологию Anti-Rootkit[33]. В 2005 году они выпустили свою антируткит-программу под названием BlackLight.

1996 – Bitdefender

Компания Softwin, материнская компания антивируса Bitdefender, была основана в Румынии в 1990 году Флорином Таплесом и его женой Мариукой Таплес. Softwin выпустила свой первый антивирусный продукт под названием Antivirus eXpert (AVX) в 1996 году. Позже, в 2001 году, Флорин Таплес основал Bitdefender. Антивирус Antivirus eXpert (AVX) был заменен линейкой Bitdefender.

2001 – ClamAV

В 2001 году Томаш Койм выпустил антивирус для GNU/Linux под названием ClamAV.

Это была небольшая история первых компьютерных антивирусных программ и антивирусных компаний.

КАК РАБОТАЮТ АНТИВИРУСЫ

Антивирус – это компьютерная программа или программное обеспечение, которое предотвращает заражение системы компьютерными вирусами.

Антивирусное программное обеспечение необходимо для любой машины с операционной системой. Без него система становится очень уязвимой. Злоумышленник может получить доступ к вашим данным, контроль над системой, чтобы использовать ее не по назначению. Антивирусное программное обеспечение защищает систему от опасных компьютерных вирусов, программ-шпионов, троянов, червей, ботов и программ-вымогателей. Это может снизить вероятность дальнейшего распространения вредоносного программного обеспечения или файлов. Кроме того, антивирус может блокировать ненужные электронные письма со спамом.

В операционные системы Windows 10 и 11 встроен бесплатный антивирус Windows Defender. Сможет ли он защитить ваш компьютер? Учитывая, что в разработку антивирусов Microsoft пришла с опозданием, Defender неплохой продукт, но он всё же не дотягивает до лидеров отрасли. Поэтому я настоятельно рекомендую устанавливать что-то из антивирусов с историей: Avira, ESET, Kaspersky, Norton и другие.

Большая часть антивирусного программного обеспечения работает в фоновом режиме и постоянно или периодически сканирует систему. В случае обнаружения любого подозрительного файла или приложения анивирус либо удаляет файл, либо информирует пользователя о необходимости немедленной обработки файла. Теперь давайте поговорим о методах, которые антивирусное программное обеспечение использует для обнаружения вредоносных программ или файлов. Существует три основных подхода: методы обнаружения на основе сигнатур, эвристики и песочницы.

Обнаружение на основе сигнатур

Сигнатура – это формализованное описание некоторых признаков, по которым можно определить, что сканируемый файл – это вирус, и вирус вполне определенный. Тут возможны разные методики. Например, использовать сигнатуру, составленную из N байт вредоносного объекта. При этом можно сделать не просто сравнение, а сравнение по некоторой маске (например, искать байты AC???? FF 26). Или задавать дополнительные условия вроде «такие-то байты должны находиться у точки входа в программу» и так далее.

Это один из основных и широко используемых методов обнаружения вирусов. Компании-разработчики антивирусного программного обеспечения поддерживают обширную базу данных сигнатур различных вирусов и вредоносных программ. При установке любого антивируса вся база сигнатур идет вместе с ним и периодически обновляется из интернета. Поэтому, когда мы устанавливаем какое-либо программное обеспечение или загружаем файлы, антивирусное программное обеспечение, работающее в фоновом режиме, сканирует этот файл и сопоставляет его с базой данных сигнатур.

Преимущество метода обнаружения на основе сигнатур заключается в том, что одна сигнатура вируса определенного типа может совпасть с набором вредоносных файлов, имеющих некоторые общие черты. Таким образом, с помощью одной сигнатуры мы можем обнаружить несколько вредоносных файлов. Если сигнатура вновь загруженного файла совпадает с какой-либо вредоносной из существующей базы данных, антивирус уведомляет и предупреждает пользователя. Хотя антивирусное программное обеспечение постоянно обновляет базу данных сигнатур, могут быть файлы, для которых нет совпадений в базе. В таком случае антивирус не сможет определить, безопасен ли только что загруженный файл.

Эвристический анализ

Эвристический анализ – это метод обнаружения компьютерных вирусов и вредоносных программ, которых нет в базах (вирусных сигнатурах), путем изучения фрагментов кода и сравнения их с известными вирусными угрозами.

Термин «эвристика» – греческого происхождения, означает «отыскивать» или «находить». Технология основывается на гипотетическом предположении, что новые вирусы частично схожи со знакомыми изученными образцами. В большинстве случаев эта догадка правдива. Положительная сторона эвристического анализа – практическая способность нахождения новых, неизученных вредоносных приложений. Несовершенство этой гипотезы – в ошибочном определении вирусного кода в безопасных файлах (ложные срабатывания).

Современные антивирусы оснащены эвристическими анализаторами, в первую очередь для выявления полиморфных

вирусов, изменяющих свой программный код после каждого заражения. При нахождении зараженных объектов пользователь информируется об этом. А вот вылечить зараженные файлы станет возможно только после изучения, внесения информации в сигнатурные базы и разработки способа лечения. До этого опасные файлы изолируются в карантине, откуда, в случае ложной тревоги, их можно будет восстановить на прежнее место. Лечение не применяется из опасения потери информации или нанесения большего вреда, чем само заражение.

На практике эвристический анализ оказывается не столь эффективным, как утверждают разработчики антивирусных программ в рекламных проспектах. Авторы вирусов перед распространением тестируют их на популярных антивирусах, чтобы найти способы обмануть эвристику и сигнатурное сканирование.

Как уже было сказано выше, главный недостаток эвристического анализа – ложные срабатывания, когда безопасные программы по ошибке определяются как зараженные, потому что их части машинного кода аналогичны вредоносному программному обеспечению.

Даже если вредоносная программа будет успешно обнаружена, лечение зараженных файлов невозможно. Только люди могут создать алгоритм изъятия вредоносного кода без нанесения вреда остальной информации. Остается лишь изолировать небезопасные объекты в защищенной карантинной зоне и ждать, пока вирус изучат и появится безопасный способ лечения.

Эвристическое сканирование бессильно против передовых новаторских вирусных программ, написанных с чистого листа и не похожих на другие компьютерные вирусы (угрозы нулевого дня).

Песочница (sandbox)

Этот метод основан на том, что антивирусное программное обеспечение запускает программу или файл в виртуальной среде. Основная цель – записывать поведение файлов и автоматически анализировать их с помощью системы весов в песочнице. Цель анализа – проверить назначение файла и выявить какие-либо вредоносные действия. Антивирус разрешит выполнение файла в реальной среде только в том случае, если он безопасен.

Метод песочницы не только определяет вредоносный характер файла, но и предоставляет подробную информацию о файле. Это

медленный процесс, потому что после установки антивирус должен запустить программу в виртуальной среде. Кроме того, необходимо дождаться результатов поведенческого анализа. Поэтому метод обнаружения требует времени и не идеален для небольших систем, таких как ноутбуки или настольные компьютеры. Крупные организации, где безопасность важнее времени, в основном используют антивирус с песочницей.

Существенным преимуществом метода песочницы является то, что он предсказывает действия, которые файл может выполнять в реальной системе. Основным ограничением является время, необходимое для анализа файла. Кроме того, для выполнения и сбора отчета о поведении требуется отдельная виртуальная среда.

Проактивная защита

Проактивные технологии – совокупность технологий и методов, используемых в антивирусном программном обеспечении, основной целью которых, в отличие от реактивных (сигнатурных) технологий, является предотвращение заражения системы пользователя, а не поиск уже известного вредоносного программного обеспечения в системе. При этом проактивная защита старается блокировать потенциально опасную активность программы только в том случае, если эта активность представляет реальную угрозу. Серьезный недостаток проактивной защиты – блокирование легитимных программ (ложные срабатывания).

Проактивные технологии начали развиваться практически одновременно с классическими (сигнатурными) технологиями. Однако первые реализации проактивных технологий антивирусной защиты требовали высокого уровня квалификации пользователя, то есть не были рассчитаны на массовое использование простыми пользователями персональных компьютеров. Спустя десятилетие антивирусной индустрии стало очевидно, что сигнатурные методы обнаружения уже не могут обеспечить эффективную защиту пользователей. Этот факт и подтолкнул к возрождению проактивных технологий.

Технологии проактивной защиты:

- **Эвристический анализ**

Технология эвристического анализа позволяет на основе анализа кода выполняемого приложения, скрипта или макроса обнаружить участки кода, отвечающие за вредоносную активность. Эффективность данной технологии не является высокой, что обусловлено большим количеством ложных срабатываний при повышении чувствительности анализатора, а также большим набором техник, используемых авторами вредоносного ПО для обхода эвристического компонента антивирусного ПО.

• **Эмуляция кода**

Технология эмуляции позволяет запускать приложение в среде эмуляции, эмулируя поведение ОС или центрального процессора. При выполнении приложения в режиме эмуляции приложение не сможет нанести вреда системе пользователя, а вредоносное действие будет детектировано эмулятором. Несмотря на кажущуюся эффективность данного подхода, он также не лишен недостатков: эмуляция занимает слишком много времени и ресурсов компьютера пользователя, что негативно сказывается на быстродействии при выполнении повседневных операций. Также современные вредоносные программы способны обнаруживать выполнение в эмулированной среде и прекращать свое выполнение в ней.

• **Анализ поведения**

Технология анализа поведения основывается на перехвате всех важных системных функций или установке т. н. мини-фильтров, что позволяет отслеживать всю активность в системе пользователя. Технология поведенческого анализа позволяет оценивать не только единичное действие, но и цепочку действий, что многократно повышает эффективность противодействия вирусным угрозам. Также поведенческий анализ является технологической основой для целого класса программ – поведенческих блокираторов (HIPS – Host-based Intrusion Systems).

• **Sandbox (Песочница) – ограничение привилегий выполнения**

Технология песочницы работает по принципу ограничения активности потенциально вредоносных приложений таким образом, чтобы они не могли нанести вреда системе пользователя. Ограничение активности достигается за счет выполнения неизвестных приложений в ограниченной среде – собственно песочнице, откуда приложение не имеет прав доступа к критическим системным файлам, веткам реестра

и другой важной информации. Технология ограничения привилегий выполнения эффективно противостоит современным угрозам, но следует понимать, что пользователь должен обладать знаниями, необходимыми для правильной оценки неизвестного приложения.

• **Виртуализация рабочего окружения**

Технология виртуализации рабочего окружения работает с помощью системного драйвера, который перехватывает все запросы на запись на жесткий диск и вместо выполнения записи на реальный жесткий диск выполняет запись в специальную дисковую область – буфер. Таким образом, даже в том случае, если пользователь запустит вредоносное программное обеспечение, оно проживет не дольше чем до очистки буфера, которая по умолчанию выполняется при выключении компьютера. Однако следует понимать, что технология виртуализации рабочего окружения не сможет защитить от вредоносных программ, основной целью которых является кража конфиденциальной информации, так как доступ на чтение файлов на жестком диске не запрещен.

Применение проактивных технологий в настоящее время

Сегодня проактивные технологии являются важным и неотъемлемым компонентом антивирусного программного обеспечения. Более того, как правило, в антивирусных продуктах используется сочетание сразу нескольких технологий проактивной защиты – например, эвристический анализ и эмуляция кода успешно сочетаются с поведенческим анализом, что позволяет многократно повысить эффективность современных антивирусных продуктов против новых, всё более изощренных вредоносных программ. Проактивная защита в некоторых антивирусах самостоятельно анализирует поведение программ, используя поведенческие сигнатуры (шаблоны опасного поведения).

Современный антивирус немыслим без проактивной защиты. Также современный антивирус должен сканировать сайты на наличие эксплойтов, электронную почту – на наличие вредоносных вложений и ссылок. Только комплексная защита обеспечит безопасность вашего компьютера.

Из чего состоит антивирусное ПО?

Принцип работы современных антивирусов заключается в комплексном подходе к вопросам кибербезопасности. У всех компаний разный состав модулей антивирусного ПО. Вот несколько основных:

• **Сканер**

Ищет вредоносное ПО в оперативной памяти, загрузочных секторах при включении, на локальных и внешних дисках, а также в системных файлах операционной системы. Может выполняться по расписанию, по запросу пользователя или при обращении к данным. Монитор Отслеживает все манипуляции с файлами в режиме реального времени. Находит и обезвреживает вредоносное ПО до того, как оно успевает инфицировать систему.

• **Проактивная защита**

Анализирует в реальном времени поведение всех запущенных программ и файлов в системе. Выявляет нежелательную активность и вредоносные программы, включая эксплойты.

• **Файервол**

Контролирует входящий трафик для защиты устройства от несанкционированного вторжения из локальной сети или интернета. Фильтрует подозрительный исходящий трафик. Этот модуль может выпускаться как отдельное ПО.

• **Интернет-монитор**

Мониторит весь веб-трафик пользователя, блокирует опасные и фишинговые страницы. Фильтрует спам, а также проверяет вложения и ссылки в электронной почте на наличие вредоносных программ и фишинга. Использует отдельный зашифрованный браузер с защитой от клавиатурных шпионов для безопасных онлайн-платежей. Позволяет настроить ограничения доступа к нежелательным категориям сайтов.

Creeper и Reaper

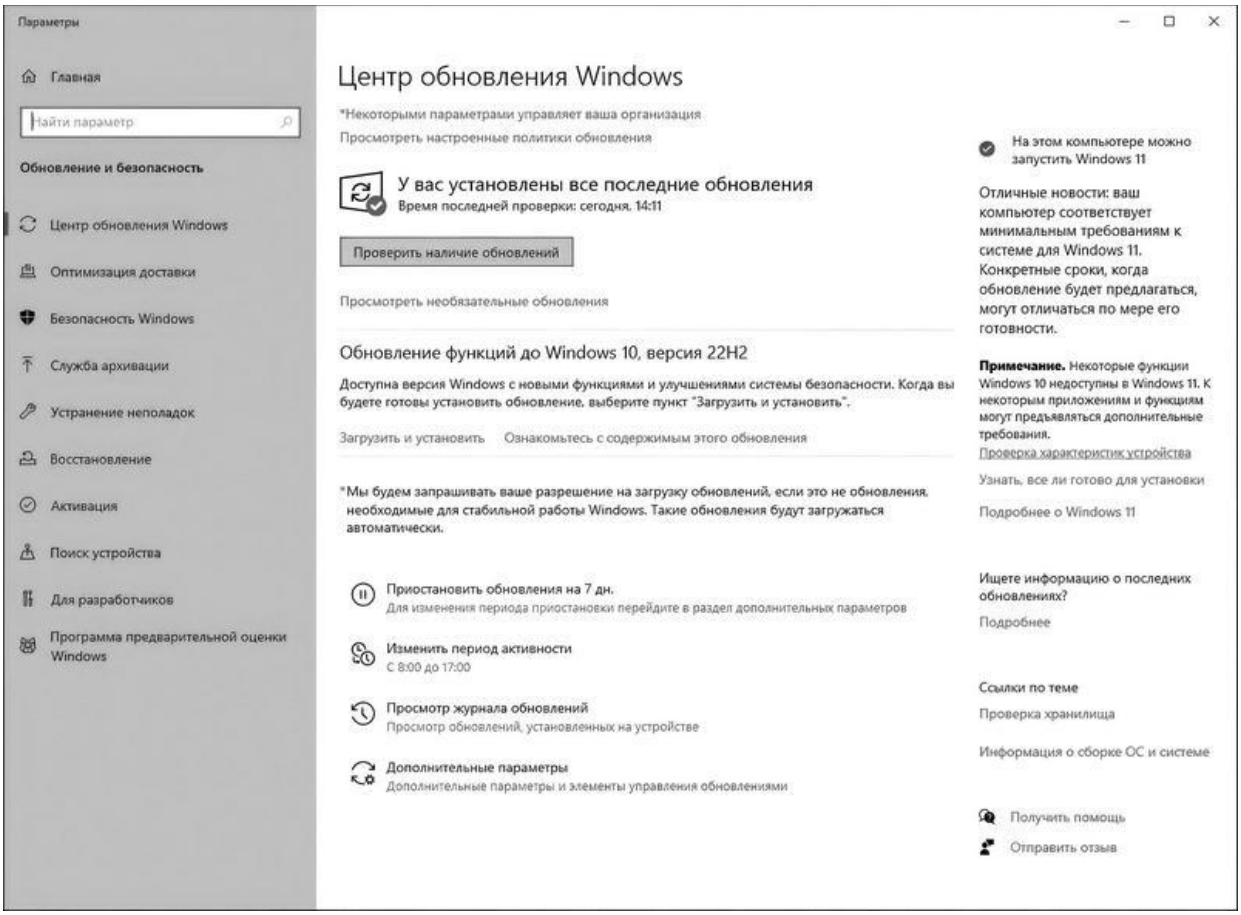
Правила

Мы с вами кратко изучили существующее вредоносное программное обеспечение (вирусы, трояны, черви) и пути его попадания на компьютеры (эксплойты, рассылки по электронной почте или передача через съемные накопители). В современном мире распространение вирусов через съемные накопители практически сошло на нет. Зато возникли новые угрозы: заражение компьютеров троянами-кейлоггерами, шифровальщиками и т. д. через зараженные связками эксплойтов сайты. Если двадцать лет назад вирусы писали больше из интереса, то сейчас отрасль киберпреступности ориентируется на извлечение прибыли – кражу персональных данных, денег со счетов и карт, вымогательство, обман.

Как защитить свой компьютер от всей этой заразы?

1. Своевременно устанавливайте обновления для операционной системы, обновляйте браузеры.

Пуск – > Проверить наличие обновлений.



Настройте систему на автоматическую ежедневную проверку обновлений.

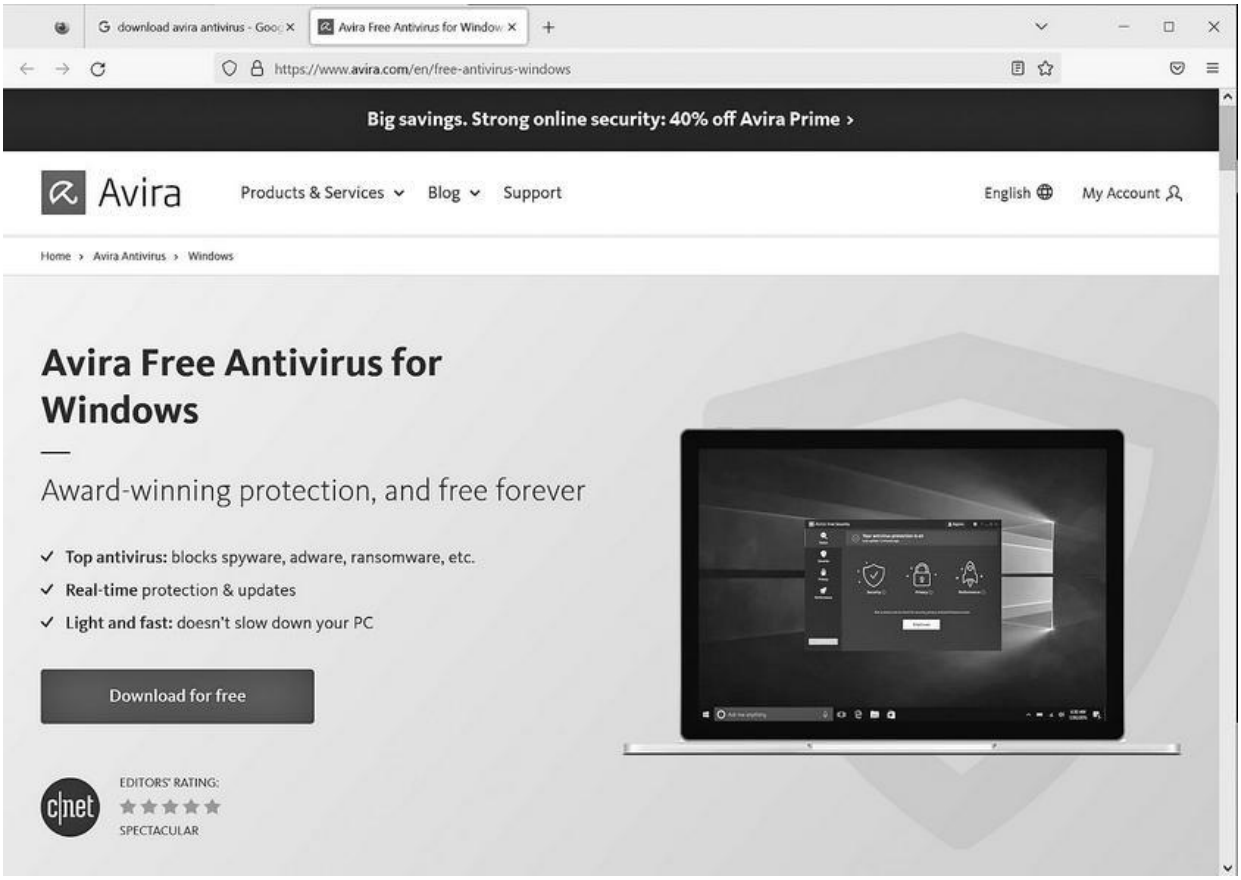
2. Используйте только поддерживаемые операционные системы, потому что к ним периодически выходят обновления, которые закрывают найденные бреши в безопасности.

3. Установите антивирус. Как я уже писал выше, антивирусные компании уже давно выпускают комплексные защиты, включающие в себя антивирус с проактивной защитой и файервол. Вы можете выбрать любой из этих продуктов: Norton 360, Avira Antivirus Pro, Kaspersky Internet Security, ESET NOD32, AVG, 360 Total Security, Bitdefender Total Security, McAfee Total Protection. Помните, хороший продукт стоит денег. Так что не экономьте и купите платную подписку.

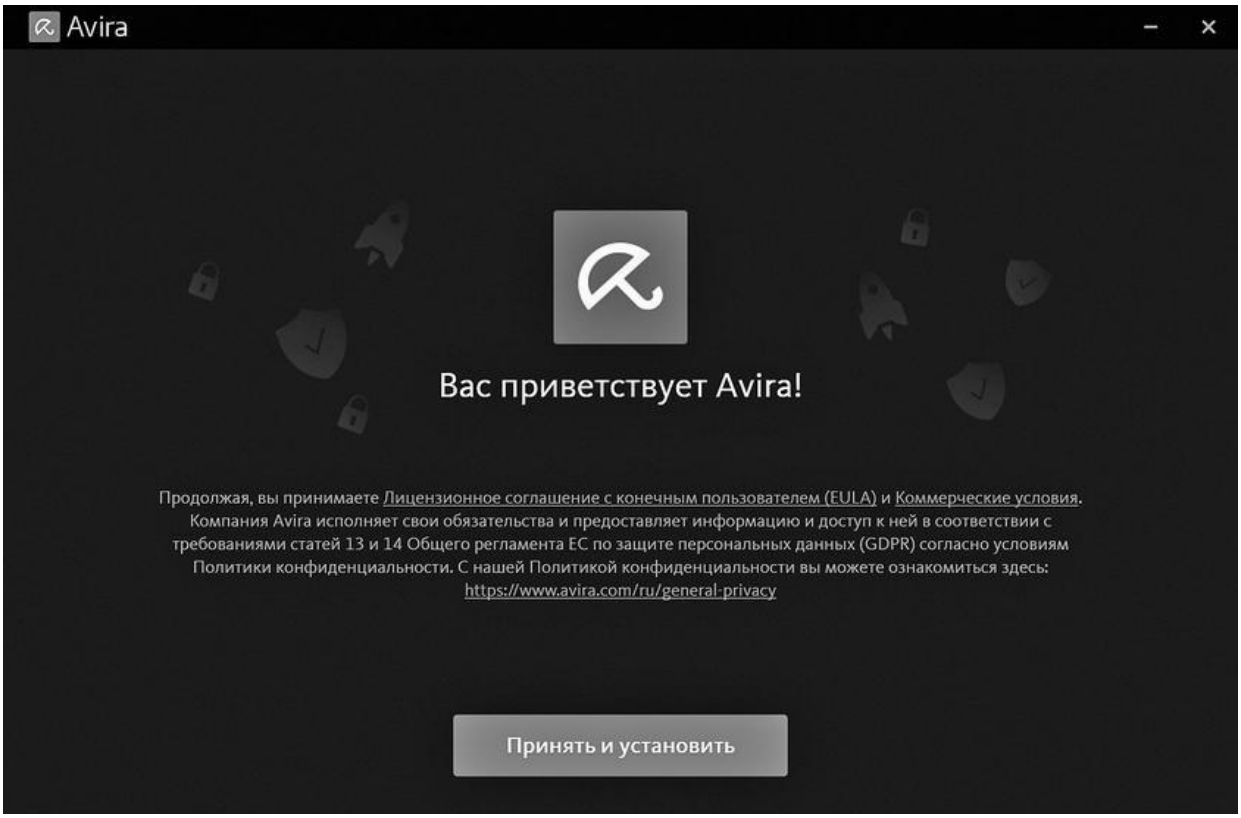
4. Я не буду агитировать за какой-то конкретный антивирус. Но я бы не рекомендовал Avast, так как тот был уличен в продаже данных пользователей третьим лицам. А также я не доверяю Касперскому, так как сталкивался уже с их экспертами в ходе судебного процесса, о

котором подробно рассказывал в своей предыдущей книге «Я – хакер! Хроника потерянного поколения». Так что я просто покажу ход установки антивируса на примере Avira Antivirus.

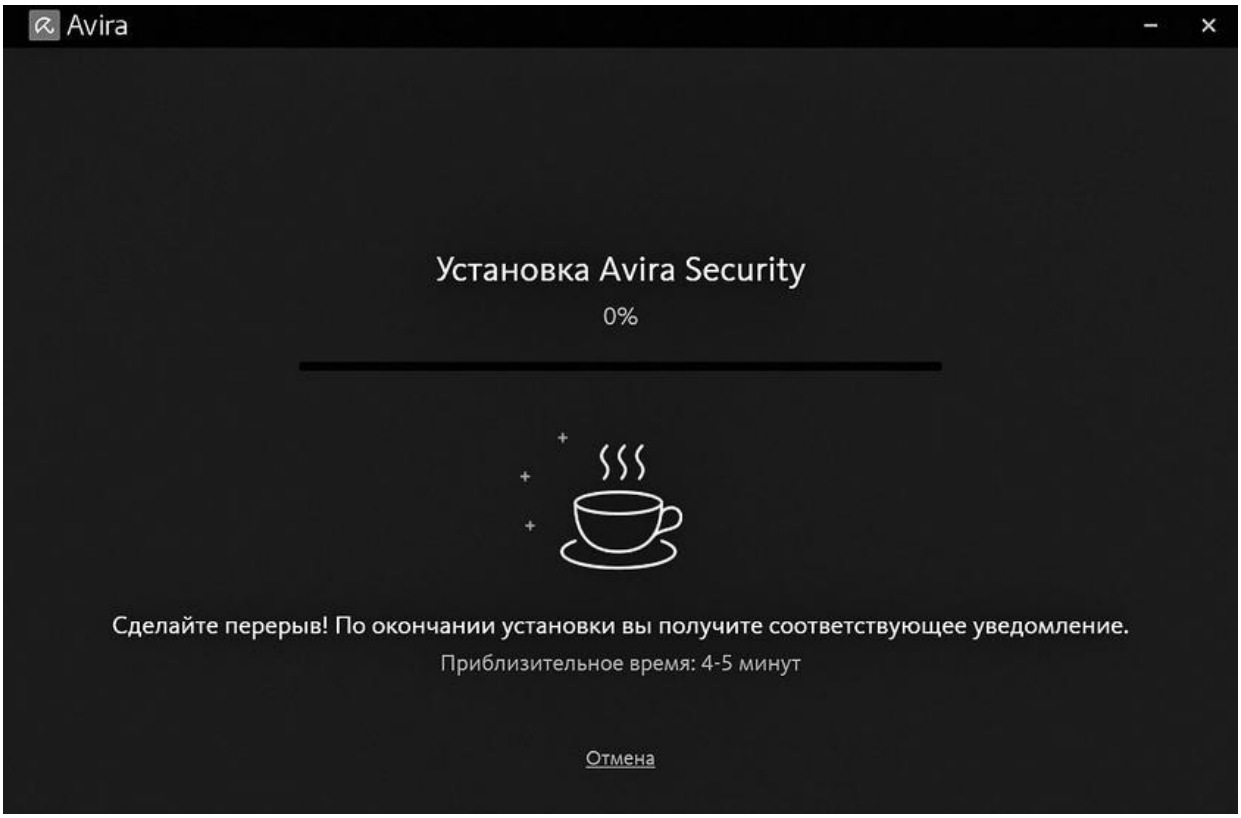
Скачиваем Avira из интернета:



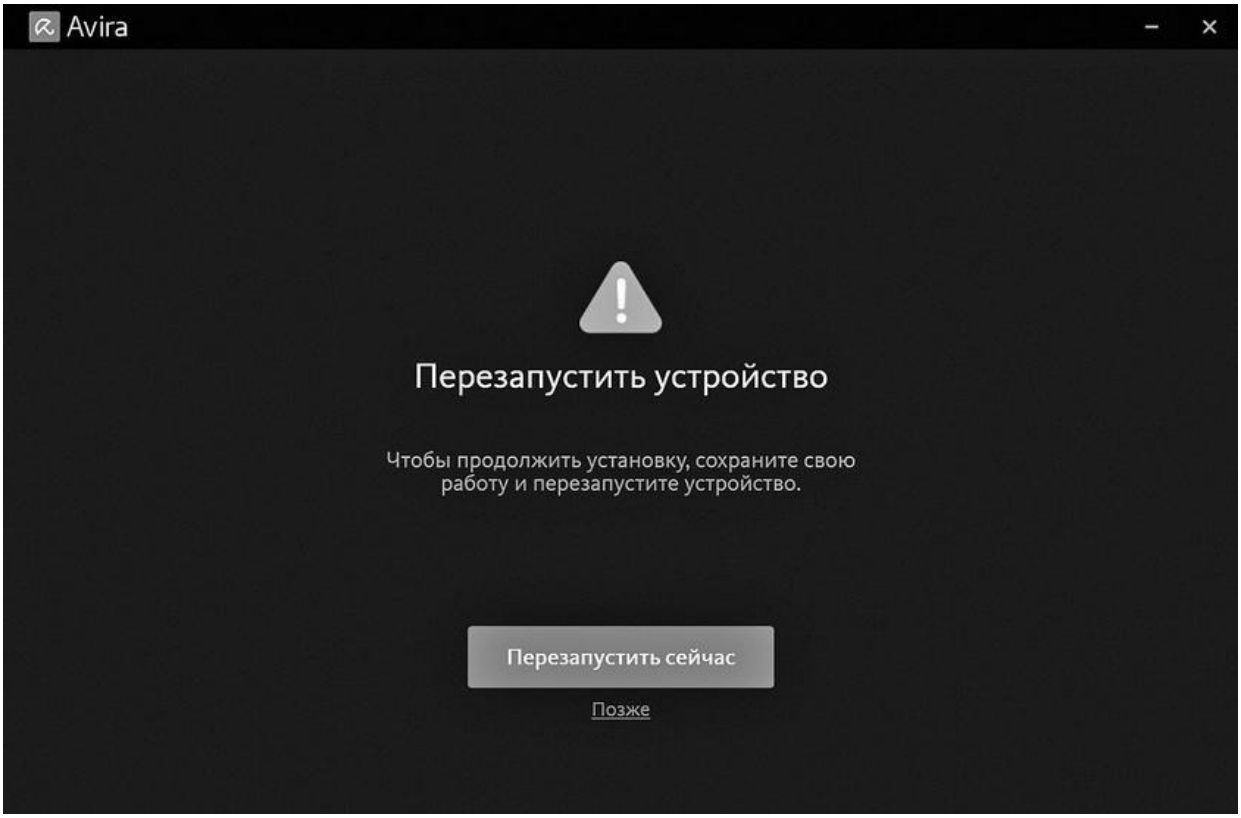
Запускаем установщик:



Устанавливаем:



Перезагружаемся:



Проходим первое сканирование:

Вот и всё. Современные антивирусы достаточно просты в обращении.

Часть 2. Смартфоны и умные устройства

Смартфоны

Теперь вы знаете, что такое вирусы. И на самом деле компьютерных вирусов сейчас практически не осталось.

Лет десять назад мобильные операционные системы, такие как Symbian, были подвержены вирусным атакам. Правда, вирусов было всего от силы штук двадцать. Победоносного шествия зловредов, как на ранних персональных компьютерах, не получилось.

Первой вредоносной программой для Symbian был червь Cabir. Его обнаружили 14 июня 2004 году. Червь распространялся под видом SIS-приложения Caribe Security Manager (которое должно было, по идее, защищать смартфон). Запустившись на инфицированном телефоне, он первым делом выводил на экран текстовую строчку Caribe, по созвучию с которой и получил свое название. Затем вредонос пытался передать свою копию по Bluetooth на все доступные поблизости устройства, поддерживающие режим Object Push Profile. Эта технология

разработана для передачи между различными девайсами фотографий, музыкальных клипов и других файлов, причем поддерживали ее не только телефоны, но и некоторые Bluetooth-принтеры. Cabir отправлял свою копию в виде файла с расширением. sis, и для успешного заражения владелец атакуемого телефона должен был, во-первых, согласиться принять файл, а во-вторых, запустить его. Тогда Cabir сохранялся в директорию приложений Apps и начинал рассылать себя уже с нового устройства.

В современных операционных системах Android и iOS безопасности уделено достаточно много внимания. Производители учли опыт настольных операционных систем, который формировался десятилетиями. Каждое приложение запускается изолированно и на определенные действия запрашивает разрешение пользователя.

Подавляющее большинство вредоносного программного обеспечения под Android и iOS маскируется под легитимное ПО и требует прямого участия пользователя: он сам должен скачать и установить такое ПО. Мошенники скрывают вирусы под видом безобидных приложений и файлов: браузеры, плееры, игры, навигаторы, книги, антивирусы. Затем они распространяют их:

• на сайтах для взрослых, сайтах со взломанными приложениями и пиратскими фильмами, торрент-трекерах и т. п. Например, вы ищете в

интернете какую-нибудь игру или программу и попадаете на форум. Кто-то оставил нужную ссылку или файл, и все дружно его благодарят. На самом деле форум и комментаторы ненастоящие;

• по СМС, MMS и электронной почте. Как правило, это СМС от «девушек с сайтов знакомств», с сайтов бесплатных объявлений, письма от «нотариусов из Германии», сообщения о выигрыше в лотерею. Будьте осторожны, в большинстве случаев это мошенники.

Эксплойты под Android и iOS никто не отменял, и уязвимостей под эти операционные системы ничуть не меньше, чем под Windows или MacOS. Подхватить вредоноса, посещая зараженный веб-сайт, тоже можно, но таких случаев единицы, и они скорее используются спецслужбами, о чем я напишу ниже. Куда чаще ошибки в операционных системах используются вредоносным ПО, чтобы обойти ограничения операционных систем и спрятать себя из списка установленных программ, перехватить ввод или прочитать ваши СМС, получить пароли из браузеров или перенаправить вас на фишинговые сайты.

Вот несколько примеров самых опасных зловредов под Android:

Triada

Данный вирус обнаружили в марте 2017 года. Уникален он своей близостью к классическим вирусам, а не к троянам-вымогателям, как это обычно бывает на Android.

Попав в устройство, эти троянцы первым делом собирают данные о системе: модель устройства, версия ОС, объем SD-карты, список установленных приложений и т. п. Затем отправляют собранную информацию на командный сервер.

Получив сообщение от троянца, командный сервер в ответ посылает ему файл с конфигурациями, содержащий персональный ID зараженного устройства и набор настроек: через какие временные промежутки вирус должен связываться с сервером, какие модули ему нужно установить и тому подобное. После установки модулей они стираются из памяти устройства и остаются только в оперативной памяти.

Особенность «Триады» заключается в том, что это модульный вирус, к нему можно подключить самый разный функционал.

Marcher

Так называемый «банковский зловред» был разработан еще в 2013 году, но его «звездный час» настал летом 2016 года. Знаменит хорошей маскировкой и «интернационализмом».

Marcher представляет собой простой троян, который не проворачивает ничего сверхъестественного, а просто подменяет собой служебные страницы огромного количества банков с помощью всплывающих окон. Механизм следующий:

• Троян проникает в систему вместе с зараженным приложением.

• Ищет на смартфоне банковские приложения и приложения интернет-магазинов, выбирает «заготовки» в соответствии с тем, каким банком вы пользуетесь.

• Отправляет на смартфон «приманку» – сообщение в шторке уведомлений со значком банка/магазина и сообщением в стиле «на ваш счет поступило N рублей»/«купон на скидку 75 % для любого товара только сегодня!».

• Владелец смартфона кликает на уведомление, после чего троян открывает точнейшую копию – страницу, один в один похожую на ту, что вы привыкли видеть в официальном приложении. И говорит что-то в стиле «соединение с сетью прервано, повторите ввод данных банковской карты».

• Владелец смартфона вводит данные банковской карты – и деньги с карты уходят злоумышленнику.

Godless

Троян Godless впечатляет своей маскировкой – длительное время его наличие в приложениях не распознавала даже хваленая система антивирусной проверки в Google Play. Результат предсказуем: зловред заразил свыше 850 тысяч смартфонов по всему миру, причем почти половина из них принадлежит жителям Индии.

Для начала Godless добывает на смартфоне root-права. После этого троян отправляет себя в папку /system (откуда его уже не удалить без перепрошивки) и шифрует себя при помощи AES-ключа.

С полным комплектом прав доступа Godless начинает понемногу воровать личные данные пользователя со смартфона и устанавливать

сторонние приложения.

Pegasus

Эксплойтами пользуются не только киберпреступники, но и спецслужбы. Спецслужбы даже скупают всевозможные уязвимости для целей взлома систем и слежения.

Одной из разработок для слежения за людьми является шпионское ПО Pegasus. Следы этой шпионской программы были найдены в телефонах множества журналистов и активистов по всему миру.

Pegasus – это основной продукт израильской компании «киберразведки» NSO Group, вероятно, наиболее известной из новых компаний, производящих шпионское программное обеспечение. Технологии NSO Group позволяют клиентам (по утверждению компании, исключительно правительствам и никогда – частным лицам или компаниям) выбирать в качестве целей конкретные телефонные номера и заражать связанные с ними устройства трояном Pegasus.

Но вместо того чтобы пытаться перехватить зашифрованные данные, передаваемые одним устройством другому, Pegasus позволяет оператору управлять самим устройством и получить доступ ко всему, что на нем хранится.

Pegasus отслеживает нажатие клавиш на зараженном устройстве – все письменные коммуникации и поисковые запросы, даже пароли – и передает данные клиенту, а также дает доступ к микрофону и камере телефона, превращая его в мобильное шпионское устройство, которое «мишень», не задумываясь, носит с собой.

Раньше для хакерских атак Pegasus требовалось активное участие самой «мишени». Операторы программы посылали текстовое сообщение с вредоносной ссылкой на телефон объекта слежки. Если человек переходил по ссылке, в браузере открывалась страница, скачивающая и запускающая вредоносный код на устройстве. NSO Group использовала разные тактики, чтобы увеличить вероятность перехода по ссылке.

Клиенты посылали спам-сообщения для того, чтобы разозлить «мишень», а затем посылали еще одно сообщение со ссылкой, по которой нужно перейти, чтобы перестать получать спам. Социотехнические приемы использовались для того, чтобы увеличить вероятность клика: вредоносные ссылки вставлялись в сообщения,

которые должны были заинтересовать или напугать объектов шпионского ПО.

Со временем пользователям стало известно о таких тактиках и они научились лучше определять вредоносный спам. Требовалось что-то более изощренное.

Решением стало использование так называемых «эксплойтов без клика». Эти уязвимости не требуют никакого участия пользователя для того, чтобы Pegasus смог заразить устройство. В последние годы правительства, использующие Pegasus, предпочитают именно эту тактику.

Эксплойты без клика полагаются на уязвимости таких популярных приложений, как iMessage, WhatsApp и Facetime. Все они получают и обрабатывают данные – иногда из неизвестных источников.

Как только уязвимость обнаружена, Pegasus проникает в устройство, используя протокол приложения. Пользователю для этого не нужно переходить по ссылке, читать сообщение или отвечать на звонок.

«Эксплойты без клика составляют большинство случаев, которые мы видели с 2019 года», – говорит Клаудио Гуарнери из Лаборатории безопасности Amnesty International. Его команда опубликовала технический отчет по методологии проекта Pegasus.

«Эта скверная программа – особо скверная, – сказал репортерам Тимоти Саммерс, бывший компьютерный инженер разведывательной службы США. – Она проникает в большинство систем обмена сообщениями, включая Gmail, Facebook, WhatsApp, Facetime, Viber, WeChat, Telegram, встроенные мессенджеры и почту Apple и другие. С таким арсеналом можно шпионить за населением всего мира. Очевидно, что NSO предлагает разведывательное агентство как услугу».

Говоря проще, используя уязвимости в популярных мессенджерах, можно отправить определенную команду через протокол мессенджера, чтобы заставить ваш телефон скачать и запустить трояна Pegasus. Радует одно: стоит эта услуга у NSO достаточно дорого, так что вряд ли мы с вами станем их целями.

КАК ЗАЩИТИТЬСЯ ОТ ВИРУСОВ НА СМАРТФОНЕ?

Источников заражения огромное количество, но в 99 % случаев это приложения, которые устанавливаются в обход Google Play или App Store. Поэтому я хочу дать несколько советов, которые должны помочь обезопасить ваше устройство:

1. Устанавливайте приложение только из официальных магазинов Google Play и App Store. Еще лучше ставить приложения, которые выложены туда несколько недель назад и имеют отзывы.

2. Проверяйте разрешения, которые запрашивает устанавливаемое приложение. Если вы, например, запускаете игру, а она требует доступ к звонкам и СМС – это очень подозрительно.

3. Не переходите по ссылкам с неизвестных номеров и почтовых ящиков.

4. Отключите услугу MMS.

5. Не подключайте услугу «Автоплатеж».

Нужен ли антивирус

Зачем антивирус на Android

Самые опасные вирусы на Android

Умные устройства

Mirai

В конце 2016 года французская телекоммуникационная компания OVH подверглась распределенной атаке типа «отказ в обслуживании» (DDoS). Экспертов поразило то, что атака была в 100 раз масштабнее аналогичных. В следующем месяце пострадало более 175 000 веб-сайтов, поскольку Dyn, провайдер DNS (система доменных имен), подвергся еще одной мощной DDoS-атаке. На большей части востока США и в некоторых странах Европы качество интернета значительно ухудшилось.

Эксперты сходятся во мнении, что за атакой на OVH и DYN стоял ботнет Mirai.

Трое молодых людей – Paras Jha, Dalton Norman и Josiah White – создали Mirai. Их первоначальная цель состояла в том, чтобы отключить серверы Minecraft в OVH и вымогать деньги за восстановление работы. После того как интернет-пользователь Anna-senpai, который, по мнению следователей, является псевдонимом Paras Jha, опубликовал исходный код Mirai в интернете, ботнет мутировал.

Mirai ищет интернет-устройства IOT с открытыми портами telnet (порт 23, который является незашифрованным каналом связи). После поиска открытых портов telnet он пытается войти на устройства, используя список/комбо из 61 имени пользователя и пароля, которые используются на этих устройствах по умолчанию и никогда не меняются. После доступа к устройству Mirai скачивает и запускает себя, после этого берет под контроль устройство и удаляет любое другое вредоносное ПО, если оно присутствует на этом устройстве. Mirai использовал достаточно простой недостаток – пароли по умолчанию, а не какой-то сложный механизм заражения.

Последующие его производные (код же был опубликован) уже использовали ряд эксплойтов, позволяющих загрузить и запустить свой вредоносный код. Вообще меня всегда поражала история Mirai. Например, то, что его создатели инициировали совершенно бесполезную и бессмысленную DDoS атаку на блог американского ЦРУшного журналиста Брайна Кребса, после чего выложили исходный код Mirai в открытый доступ. И получили всего 6 месяцев тюремного

заключения за то, что парализовали работу крупного сервиса, целого дата-центра и тысяч сайтов.

Вы уже поняли, что умные устройства (роутеры[34], умные камеры, принтеры) также подвержены заражению вредоносным ПО. Например, Mirai распространялся из-за того, что на многих роутерах был включен административный доступ по telnet извне (доступен к подключению из интернета), а логин/пароль на вход устанавливались многими производителями крайне простые – например, root/root или admin/admin. То же касается и веб-камер.

Вредоносное ПО под умные устройства может делать следующее:

• Использовать устройство для проведения DDoS атак.

• Использовать устройство для майнинга криптовалюты.

• Изменить настройки DNS[35] с легитимных серверов на сервера злоумышленников. И всем, кто подключается в интернет через этот маршрутизатор, подменять IP-адреса сайтов. Представьте, пользователь вводит в строке sber.ru, а вместо реально IP-адреса сайта Сбера его отправляют на фишинговый сайт. Там пользователь вводит свой логин и пароль, которые тут же попадают к злоумышленникам. Кроме фишинга (мы рассмотрим его ниже), пользователя можно перенаправлять также на зараженные сайты с целью инфицировать домашний ПК или на сайты с рекламой.

• Рассылать через устройство спам или сделать из него прокси-сервер.

КАК ЗАЩИТИТЬ УМНЫЕ УСТРОЙСТВА

1. Поменяйте все пароли по умолчанию: для доступа к устройству, пароль от wi-fi и т. д.

2. Отключите удаленный доступ к устройству из интернета, если он вам реально не нужен. Если нужен, то используйте сложные пароли.

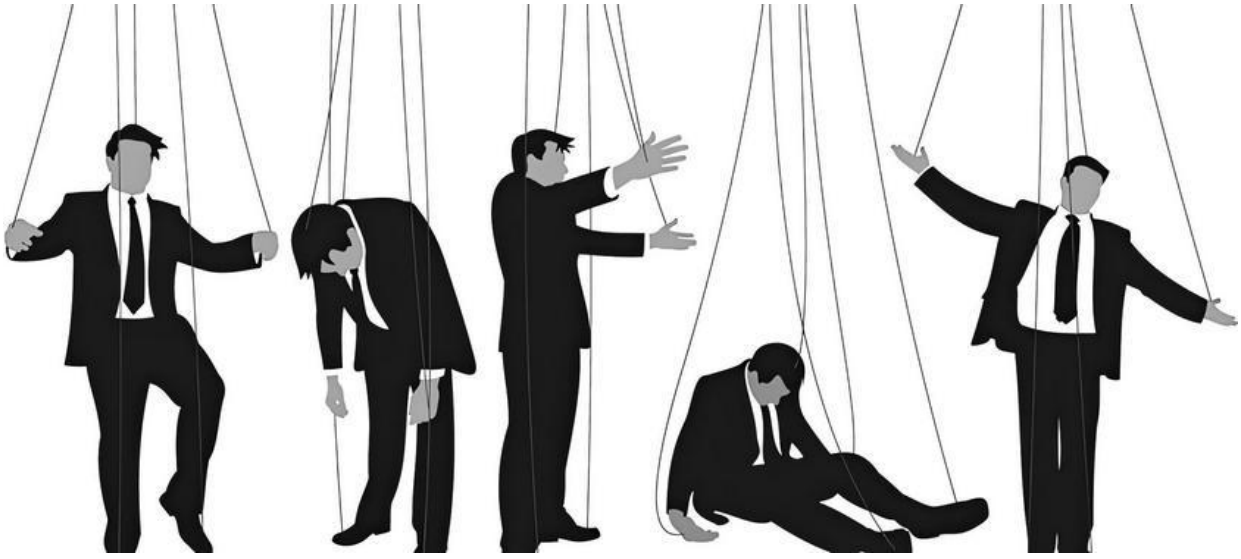
3. Всегда своевременно обновляйте прошивку устройства до самой последней.

Вредоносное ПО, стоящее за крупнейшей DDOS-атакой

Часть 3. Социальная инженерия

Социальная инженерия – в контексте информационной безопасности – психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации. Совокупность уловок с целью сбора информации, подделки или несанкционированного доступа от традиционного «мошенничества» отличается тем, что часто является одним из многих шагов в более сложной схеме мошенничества.

Также может быть определено как «любое побуждение человека к действию, которое может или не может быть в его интересах».



Сегодня благодаря разнообразию социальных сетей собрать сведения о человеке очень легко. А опытные мошенники хорошо разбираются в психологии и могут использовать в своих целях даже минимальные знания о пользователе.

Многие специалисты по информационной безопасности говорят, что как ни защищай программы и системы, есть одно слабое звено – это сам пользователь. Люди зачастую оказываются очень доверчивыми и сами предоставляют мошенникам конфиденциальную информацию.

Сейчас социальная инженерия приобрела прочную связь с киберпреступностью, но на самом деле это понятие появилось давно и

изначально не имело выраженного негативного оттенка.

Люди использовали социальную инженерию с древних времен. Например, в Древнем Риме и Древней Греции очень уважали специально подготовленных ораторов, способных убедить собеседника в его «неправоте». Эти люди участвовали в дипломатических переговорах и работали на благо своего государства.

Спустя много лет, к началу 1970-х годов, стали появляться телефонные хулиганы, нарушавшие покой граждан просто ради шутки. Но кто-то сообразил, что так можно достаточно легко получать важную информацию. И уже к концу 70-х бывшие телефонные хулиганы превратились в профессиональных социальных инженеров (их стали называть синжерами), способных мастерски манипулировать людьми, по одной лишь интонации определяя их комплексы и страхи.

Когда же появились компьютеры, большинство инженеров сменило профиль, став социальными хакерами, а понятия «социальные инженеры» и «социальные хакеры» стали синонимами.

Яркие примеры социальной инженерии

Кража у компании The Ubiquiti Networks 40 миллионов долларов в 2015 году. Никто не взламывал операционные системы и не крал данные – правила безопасности нарушили сами сотрудники. Мошенники прислали электронное письмо от имени топ-менеджера компании и попросили, чтобы финансисты перевели большую сумму денег на указанный банковский счет. И те перевели.

В 2007 году одна из самых дорогих систем безопасности в мире была взломана – без насилия, без оружия, без электронных устройств. Злоумышленник просто забрал из бельгийского банка ABN AMRO алмазы на 28 миллионов долларов благодаря своему обаянию. Мошенник Карлос Гектор Фломенбаум, человек с аргентинским паспортом, украденным в Израиле, завоевал доверие сотрудников банка еще за год до инцидента. Он выдавал себя за бизнесмена, делал подарки, короче говоря – налаживал коммуникацию. Однажды сотрудники предоставили ему доступ к секретному хранилищу драгоценных камней, оцененных в 120 000 каратов.

А слышали, как Виктор Люстиг продал достояние Парижа – Эйфелеву башню – на металлолом? Всё это стало возможным с помощью социальной инженерии.

Эти реальные примеры социальной инженерии говорят о том, что она легко адаптируется к любым условиям и к любой обстановке. Играя на личных качествах человека или отсутствии профессиональных (недостаток знаний, игнорирование инструкций и так далее), киберпреступники буквально «взламывают» человека.

Самые популярные методы социальной инженерии:

• **Фишинг** – это вид мошенничества, суть которого – завладение логинами и паролями от важных сайтов, аккаунтов, счетов в банке и другой конфиденциальной информацией путем рассылки писем со ссылками на мошеннический сайт, внешне очень похожий на настоящий. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить его ввести на поддельной странице свои логин и пароль, что позволяет им получить доступ к аккаунтам и банковским счетам.

• **Фарминг** – при фарминге на персональный компьютер жертвы устанавливается вредоносная программа, которая меняет информацию по IP-адресам, в результате чего обманутый пользователь перенаправляется на поддельные сайты без его ведома и согласия. Это более продвинутая версия фишинга, тут уже не нужно слать письма.

• **Вишинг** – метод, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карточки конфиденциальную информацию или стимулируют его к совершению каких-то действий со своим счетом или банковской платежной карточкой.

• **Взлом социальных сетей** – взламывается страница пользователя, и от его имени идут сообщения его друзьям, чаще всего с просьбой «скинь денег на карточку». Тот, кого взломали, может понять это, когда не сможет войти в свой аккаунт, ведь пароль уже изменен.

• **СМС-атаки** – мошенник создает фейковый аккаунт в социальных сетях либо регистрируется, к примеру, в Viber, с сим-карты, которая оформлена не на него. Далее высылает объявление «Помогите на лечение ребенку», размещая фото и реквизиты. Если это

действительно реальный человек, то реквизиты легко проверяются. Но, к сожалению, люди не часто проверяют такую информацию.

• **Претекстинг** – набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон, электронная почта и т. п. Для использования этой техники злоумышленнику необходимо изначально иметь некоторые данные о жертве (имя сотрудника, должность, название проектов, с которыми он работает, дату рождения). Используя такую информацию, он входит в доверие и получает необходимые ему данные.

• **Кви про кво** (в английском языке это выражение обычно используется в значении «услуга за услугу») – злоумышленник представляется, например, сотрудником технической поддержки и информирует о возникновении каких-то проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» такой проблемы злоумышленник подталкивает жертву к совершению действий, позволяющих атакующему выполнить определенные команды или установить необходимое вредоносное программное обеспечение на компьютере жертвы. Эта техника предполагает обращение злоумышленника к пользователю – как правило, по электронной почте или корпоративному телефону.

• **Обратная социальная инженерия** – создается такая ситуация, при которой жертва вынуждена сама обратиться к злоумышленнику за «помощью». Например, мошенник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте со злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

Методов мошенничества, которые используют социальную инженерию, множество. Перечисленные – это всего лишь их часть. Самые распространенные для нашей страны – фишинг, взлом социальных сетей и вишинг.

Рассмотрим некоторые виды социальной инженерии более подробно.

Что такое социальная инженерия

«Нигерийские письма»

«Нигерийские письма» (также скам[36] – от *англ.* Advance-fee scam, буквально «Мошенничество с предоплатой») – распространенный вид мошенничества типа «писем счастья», получивший наибольшее развитие с появлением массовых рассылок по электронной почте (спама). Письма названы так потому, что особое распространение этот вид мошенничества получил в Нигерии, причем еще до распространения интернета, когда такие письма распространялись по обычной почте. Однако «нигерийские письма» приходят и из других африканских стран, а также из городов с большой нигерийской диаспорой (Лондон, Амстердам, Мадрид, Дубай). Рассылка писем началась в середине 1980-х годов.

Как правило, мошенники просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются всё более крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам и т. п.

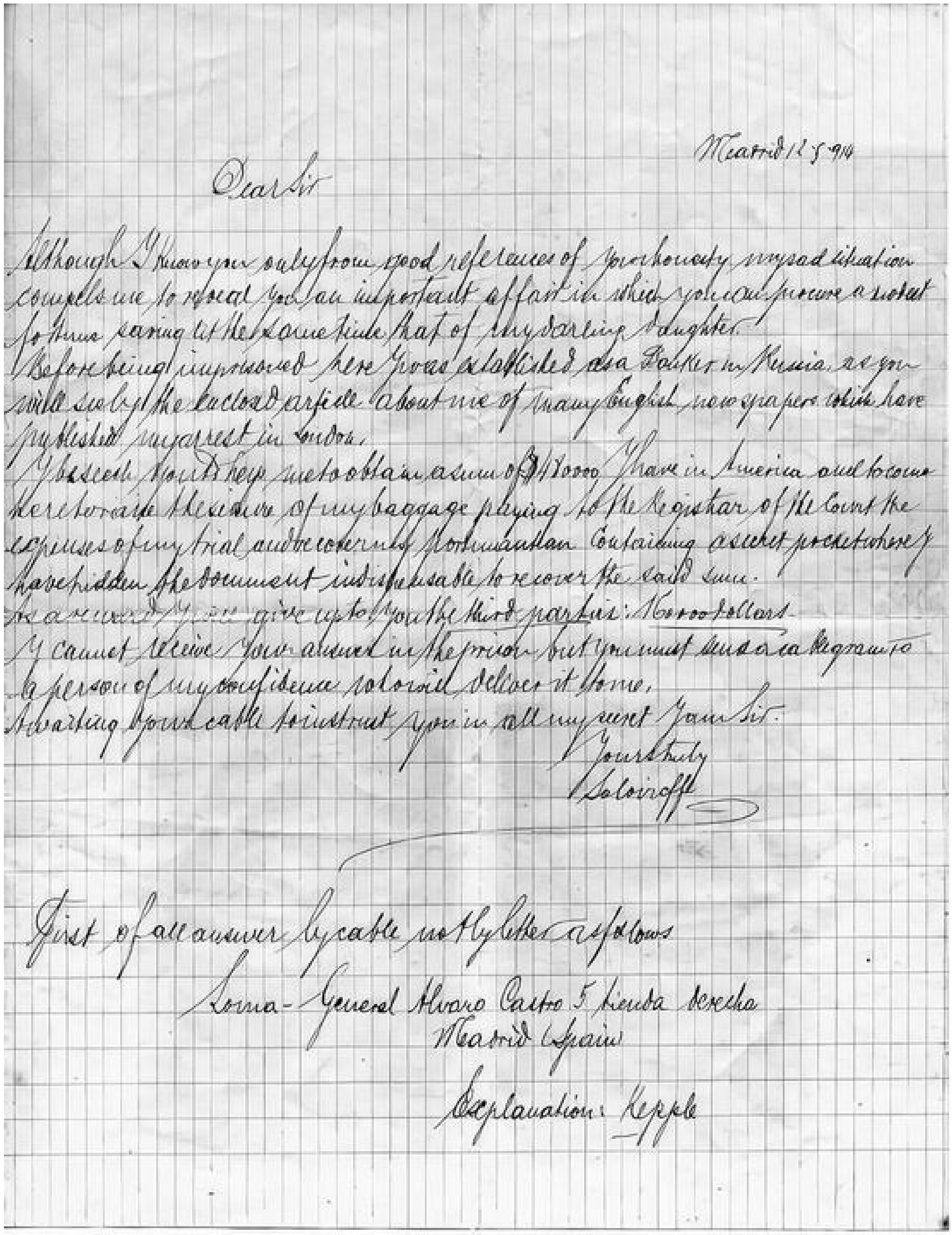
«Нигерийские письма» – один из самых распространенных видов мошенничества в интернете. Нигерийские спамеры даже получили в 2005 году так называемую анти-Нобелевскую премию в области литературы. Еще одно название, используемое в англоязычных документах, – scam 419. Оно также связано с Нигерией: 419 – это номер статьи нигерийского закона, запрещающей, в частности, этот вид мошенничества.

Письмо испанского заключенного

В 1898 году один из выпусков New York Times подробно описал получившую в те годы широкое распространение технику надувательства через письма и окрестил ее «Испанский заключенный» (Spanish Prisoner). Выжимка из статьи «Новая волна мошенничества» (An Old Swindle Revived) и сегодня кажется актуальной:

«Человек получает письмо из-за границы. <…> Незнакомец изъясняется на довольно хорошем английском языке, с некоторыми грамматическими ошибками и характерным для иностранцев слогом. Автор послания, обыкновенно, находится в тюрьме по обвинению в

политическом преступлении. У него всегда есть большая сумма денег, спрятанная в определенном месте, что и является причиной его беспокойства. <…> Заключенный каким-либо образом знает о получателе и уверен, что ему можно доверять. Как правило, у них якобы есть общий знакомый, имя которого не может быть раскрыто по соображениям безопасности. В качестве вознаграждения за оказанную услугу он обязуется выплатить 1/3 от вызволенных средств».


Madrid 12-5-914

Dear Sir

Although I know you only from good references of your honesty my sad situation compels me to reveal you an important affair in which you can procure a robust fortune saving at the same time that of my darling daughter.
Before being imprisoned here I was established as a Banker in Russia as you will see by the enclosed article about me of many English newspapers which have published my arrest in London.
I beseech you to help me to obtain a sum of $ 470000 I have in America and to come here to raise the seizure of my baggage paying to the Registrar of the Court the expenses of my trial and recover my portmanteau containing a secret pocket where I have hidden the document indispensable to recover the said sum.
As a reward I will give up to you the third part i.e. [illegible] dollars.
I cannot receive your answer in the prison but you must send a cablegram to a person of my confidence who will deliver it to me.
Awaiting your cable to instruct you in all my secret I am Sir.

Yours truly
Solovieff

First of all answer by cable not by letter as follows
Lorna - General Alvaro Castro 5 tienda derecha
Madrid Spain
Explanation: Reply

Письмо на фотографии выше датировано началом прошлого века и вполне могло принадлежать к волне, описанной в Times. Витиеватый, причудливый почерк владельца послания сложен для восприятия, но его основная мысль заключается в следующем: некий русский банкир по имени Сергей Соловьёв (Serge Solovieff) был заключен под стражу и

обращается к получателю, чтобы тот помог ему вернуть его деньги, спрятанные где-то в Америке. К письму прилагается вырезка из газеты, упоминающая об реальном аресте г-на Соловьева.

Копия этого письма была опубликована в сети в 2000-х годах Ричардом Зельтцером (Richard Seltzer). Тем самым он дал возможность множеству людей, получивших практически идентичные послания, распознать мошенников. В результате была составлена целая коллекция писем: хотя они написаны разным почерком, естественно, ни одно из них не принадлежит г-ну Соловьёву.

«Сотни, если не тысячи таких писем, – пишет Зельтцер, – были разосланы адресатам в совершенно случайном порядке, наподобие современного спама, но тем не менее многие приняли их за чистую монету: старый трюк сработал вновь».

На момент публикации статьи в Times (1898) злоумышленники действовали по этой схеме уже более 30 лет, и местные власти, всерьез обеспокоенные ситуацией, решили осветить вопрос в СМИ, чтобы хоть как-то предостеречь доверчивых граждан. Однако оказалось, что во Франции подобные спамерские атаки начались задолго до этого.

В 1832 году в своих мемуарах бывший французский преступник, впоследствии ставший главой национальной безопасности и первым в истории частным детективом, Эжен Франсуа Видок (Eugène François Vidocq), так описал процесс одурачивания: «[Мошенник] узнавал адрес некой богатой провинциальной особы у какого-нибудь вновь прибывшего заключенного. После этого он составлял послание, содержащее приблизительно следующие слова:

«Сэр,

Вы, без сомнения, удивитесь, получив письмо от незнакомого вам человека, который к тому же просит Вас об услуге. Однако мое положение настолько плачевно, что я нахожусь на грани отчаяния. Именно поэтому я обращаюсь к Вам, так как я много слышал о Вашей доброте и знаю, что Вам можно доверять. Будучи слугой маркиза N, я сопровождал своего господина на пути эмиграции, но, чтобы избежать подозрений, мы шли пешком. В багаже, который я нес, находилась шкатулка, содержащая 16 000 франков золотом и алмазы покойной маркизы».

Вероятно, вы уже догадались, что следовало дальше. Для того чтобы избежать разоблачения, автор письма со своим «маркизом»

вынуждены были спрятать шкатулку с драгоценностями в укромном месте. Но по возвращении за ней «слуга» был схвачен и заключен под стражу ввиду отсутствия паспорта.

«Оказавшись в этой ужасной ситуации, я сразу подумал о Вас: Ваше доброе имя не раз упоминала в своих рассказах знакомая моего маркиза. <…> Я умоляю вас, если это только возможно, помочь мне вернуть спрятанную шкатулку, и в качестве награды вы сможете взять себе часть драгоценностей. Если вы сделаете это для меня, вы значительно облегчите мое освобождение, так как я смогу выплатить компенсацию моему адвокату. Это он диктует мне это письмо и убежден, что при наличии достаточных средств вытащить меня отсюда не составит труда.

С глубочайшим уважением,

N.»

Согласно Франсуа Видоку, коэффициент ответа на эти письма составил примерно 20 %.

Почему это до сих пор работает

Что делает этот, казалось бы, очевидный обман настолько эффективным и почему, как и 200 лет назад, люди до сих пор ему верят? Вот что сообщает уже знакомая нам колонка в The New York Times:

«Как известно, выявление и раскрытие преступлений, когда в деле замешаны разные государства, представляет определенную сложность, особенно если жертвы редко заявляют о случившемся. Никто не знает, как много людей пострадало от рук этих мошенников и скольких тысяч долларов им стоило так называемое вознаграждение».

Так как на удочку шарлатанов попадаются, в основном, наивные и простодушные люди, они часто стесняются рассказать о произошедшем. Нельзя с уверенностью утверждать, но по приблизительным оценкам ущерб от «авансового мошенничества» в 2007 году составил $198 400 000 в США, а в 2013-м – $12 300 000 000 во всем мире (согласно данным международной научно-исследовательской организации Ultrascan). В связи с тем, что деньги переводились за границу, в страны с бедной банковской

инфраструктурой, отследить передвижение средств и найти виновных оказывается крайне трудно.

В современном мире мало что изменилось: с одной стороны, благодаря интернету большинство людей прекрасно осведомлены о различных махинациях, но и мошенники тоже не стоят на месте. Проявляя недюжинную изобретательность, они выдумывают всё новые истории, отличные по содержанию, но такие же трогательные и душераздирающие. Помимо этого, современные технологии значительно облегчили процесс: теперь массовая рассылка писем практически ничего не стоит, особенно когда одна жертва может принести тысячи, если не миллионы долларов.

Кормак Херли (Cormac Herley), один из исследователей Microsoft Research, считает, что невысокий показатель конверсии (большое количество разосланных электронных писем к ответам) играет даже на руку вымогателям. Так как в эту хорошо известную ловушку попадают только очень легковерные люди, преступники тратят меньше времени на непродуктивную переписку с теми, кто в итоге раскусит их замысел или переведет лишь небольшую сумму.

Еще одна особенность современного общества заключается в том, что с появлением интернета и повсеместным использованием e-mail-технологий увеличилось не только число жертв, но и количество преступников. Схема, описанная сыщиком Видоком в начале XIX века, действовала до тех пор, пока слухи о ней не распространились слишком широко, предостерегая от обмана состоятельных особ.

Люди в странах Запада прекрасно осведомлены о различных видах интернет-мошенничества, но в более отдаленных уголках планеты еще остались те, куда технический прогресс пришел совсем недавно. Один из репортеров Mother Jones сообщает, что сегодня жертвами «нигерийских писем» нередко становятся сами жители Нигерии, а их авторы иногда маскируются под уроженцев Ганы.

Кроме того, с развитием технологий злоумышленники осваивают новые инструменты воздействия через социальные сети, а для своих махинаций используют более анонимные электронные кошельки. Вы никогда не задумывались о том, почему незнакомые люди регулярно пытаются добавить вас в друзья?

Если эта история может чему-либо научить нас – так это тому, что как бы мы ни старались защититься от спама различными фильтрами,

необходимо проявлять осторожность по отношению ко всем необычным сообщениям. Технологии развиваются, а вместе с ними изобретаются и новые методы обмана. Пока люди взаимодействуют друг с другом, полностью искоренить мошенничество не удастся, и даже старые техники, приняв современное обличье, продолжают действовать по сей день.

Примеры

Подавляющее большинство «нигерийского» спама идет на английском языке, но в 2004–2005 гг. спамеры взялись активно осваивать Рунет. Появился «нигерийский» спам на русском языке, эксплуатирующий горячие события российской политической жизни. Внимание спамеров привлекло нашумевшее дело ЮКОСа, и пользователям Рунета было предложено обналичить миллионы Ходорковского.

«Меня зовут Бакаре Тунде, я брат первого нигерийского астронавта, майора ВВС Нигерии Абака Тунде. Мой брат стал первым африканским астронавтом, который отправился с секретной миссией на советскую станцию “Салют-6” в далеком 1979 году. Позднее он принял участие в полете советского “Союза Т-163” к секретной советской космической станции “Салют-8Т”. В 1990 году, когда СССР пал, он как раз находился на станции. Все русские члены команды сумели вернуться на Землю, однако моему брату не хватило в корабле места. С тех пор и до сегодняшнего дня он вынужден находиться на орбите, и лишь редкие грузовые корабли “Прогресс” снабжают его необходимым. Несмотря ни на что, мой брат не теряет присутствия духа, однако жаждет вернуться домой, в родную Нигерию. За те долгие годы, что он провел в космосе, его постепенно накапливающаяся заработная плата составила 15 000 000 американских долларов. В настоящий момент данная сумма хранится в банке в Лагосе. Если нам удастся получить доступ к деньгам, мы сможем выплатить Роскосмосу требуемую сумму и организовать для моего брата рейс на Землю. Запрашиваемая Роскосмосом сумма равняется 3 000 000 американских долларов. Однако для получения суммы нам необходима ваша помощь, поскольку нам, нигерийским госслужащим, запрещены все операции с иностранными счетами.

Вечно ваш, доктор Бакаре Тунде, ведущий специалист по астронавтике», – нетленная классика «нигерийского письма», в свое время очень популярная в интернете.

Для убедительности в письмах обязательно наличествуют красивые цветистые печати и скрины официальных бланков документов, адреса и номера телефонов, имена нотариусов, занимающихся наследством, и прочие уловки, заставляющие жертву поверить в серьезность происходящего.


YUKO\'S OIL. - Western European (ISO)

File Edit View Tools Message Help

From: vkchambers
Date: 18 октября 2004 г. 14:10
To:
Subject: YUKO\'S OIL.

Good day ,

I Barrister Miroslav Vlado Khodo, representing Mr.Mikhail Khodorkovsky
(m.k.) of Russia. He is one time the richest man in Russia and the head of
YUKO'S OIL till that unfaithful day that they got him arrested and since
then all his accounts and known businesses have been confiscate. I would
like to ask for your partnership in re-profiling funds over US$42 million.
I will give the details, but in summary, the funds are coming via bank transfer.
Please note that as an attorney I want a very straight forward and God fearing
person as this is a legitimate transaction and not a Child play. You will
be paid 10% for your "management fees". You can log into this web site to

Как несложно догадаться, мошенничество, как и всегда, начинается в ту минуту, когда собеседник впервые просит перевести ему деньги. Обычно речь идет о небольших тратах: оформление документов, заверение документов нотариусом, перевод документов на другой язык. Ослепленная манящими миллионами и открывшимися

перспективами жертва начинает переводить эти небольшие суммы, которые в будущем могут вырасти в довольно солидный денежный куш для аферистов. Известны случаи, когда с одной жертвы мошенники таким образом «стрясали» несколько тысяч долларов.

Расходы на оформление документов преподносятся как сущие копейки по сравнению с обещанным наследством. При этом мошенники постоянно подбрасывают всё новые факты и очень торопят: нужно срочно заплатить за оформление документов, открыть счет в банке или дать взятку чиновнику. Это необходимо, чтобы жертва не опомнилась и свято верила липовым адвокатам.

«Нигерийское письмо» – это вид мошенничества по электронной почте, когда у вас просят помощи в проведении многомиллионных операциях. А в качестве вознаграждения обещают процент от переведенных денег.

Правила

Никогда не верьте подобным письма. Помните, что собеседник на том конце – изощренный психолог, и он будет тянуть за ниточку жажды наживы.

Многовековая история мошенничества с почтой

Нигерийские письма

Техническая поддержка

Это тип мошенничества, при котором мошенник утверждает, что предлагает настоящую службу технической поддержки. Жертвы связываются с мошенниками различными способами: часто через поддельные всплывающие окна, напоминающие сообщения об ошибках, или через поддельные «линии помощи», рекламируемые на веб-сайтах, принадлежащих мошенникам. «Липовые» службы технической поддержки используют социальную инженерию и различные уловки, чтобы убедить свою жертву в наличии проблем на их компьютере или мобильном устройстве, таких как заражение вредоносным ПО, хотя с устройством жертвы проблем нет. Затем мошенник старается убедить жертву заплатить за устранение фиктивных «проблем», которые, как он утверждает, он обнаружил.

О мошенничестве с технической поддержкой стало известно еще в 2008 году. Исследования показывают, что миллениалы[37] и представители поколения Z[38] больше ему подвержены, однако

пожилые люди с большей вероятностью отдадут деньги мошенникам. Мошенничество с технической поддержкой было названо компанией Norton главной фишинговой угрозой для потребителей в октябре 2021 года. Также компания Microsoft обнаружила, что 60 % потребителей, принявших участие в их опросе, подвергались мошенничеству с технической поддержкой в течение предыдущих двенадцати месяцев.

Происхождение и распространение

Первые случаи мошенничества с техподдержкой, как уже сказано выше, были зафиксированы в 2008 году. Такое мошенничество было замечено в различных странах, включая США, Канаду, Великобританию, Ирландию, Австралию, Новую Зеландию, Индию и Южную Африку. Исследование, опубликованное в 2017 году на симпозиуме NDSS, показало, что по задействованным IP-адресам мошенников можно определить, из каких стран совершаются эти действия: 85 % IP-адресов оказалось в Индии, 7 % – в США и 3 % – в Коста-Рике.

В Индии миллионы людей, говорящих по-английски, борются за относительно небольшое количество рабочих мест. Например, в одном муниципалитете было 114 рабочих мест – и 19 000 претендентов на них. Такой высокий уровень безработицы служит стимулом для работы в сфере мошенничества с техподдержкой, которое часто хорошо оплачивается. Люди часто даже не осознают, что подают заявки и проходят обучение для вакансий в сфере мошенничества с технической поддержкой, но многие решают остаться, после того как узнают характер деятельности, поскольку считают, что уже слишком поздно отказываться. Претенденты вынуждены выбирать между сохранением работы или безработицей. Некоторые мошенники убеждают себя, что нацелены на богатых людей, у которых есть лишние деньги, что оправдывает их кражи, в то время как других привлекает получение «легких денег».

Как это начинается

Мошенничество с технической поддержкой может начинаться по-разному:

• С всплывающих окон на зараженных веб-сайтах. Жертве показываются всплывающие окна, которые напоминают стандартные сообщения об ошибках, такие как синий «экран смерти» (BSOD), и блокируют веб-браузер жертвы. Всплывающее окно предлагает позвонить мошенникам по номеру телефона, чтобы исправить «ошибку».

• С холодных звонков. Обычно это автоматические звонки, которые утверждают, что они – официальный представитель третьей стороны, например, Microsoft или Apple.

• Мошенники могут также покупать рекламу по ключевым словам в основных поисковых системах для таких фраз, как «поддержка Microsoft». Жертвы, которые нажимают на эти объявления, попадают на веб-страницы, содержащие номера телефонов мошенников.

Как мошенник убеждает

Как только жертва связывается с мошенником, он обычно дает указание загрузить и установить программу удаленного доступа, такую как TeamViewer, AnyDesk, LogMeIn или GoToAssist. Дальше мошенник убеждает жертву предоставить учетные данные, необходимые для удаленного доступа, что дает полный контроль над рабочим столом жертвы.

Получив доступ, мошенник пытается убедить жертву, что компьютер страдает от проблем, которые необходимо устранить, чаще всего – от злонамеренной хакерской деятельности. Мошенники используют несколько методов, чтобы предоставить содержимое и значение общих инструментов Windows и системных каталогов в ложном свете как свидетельство вредоносной деятельности, такой как вирусы и другие опасные программы. Эти уловки предназначены для неопытных пользователей и пожилых людей, которые не знакомы с реальным использованием инструментов ОС Windows. Затем мошенник уговаривает жертву заплатить за услуги или программное обеспечение, которое, как он утверждает, предназначено для «ремонта» или «очистки» компьютера, но на самом деле представляет собой вредоносное ПО, заражающее компьютер, или просто пустышку.

Уловки бывают следующие:

Мошенник может продемонстрировать пользователю средство просмотра событий Windows (Event Viewer), отображающее журнал различных событий, который системные администраторы используют для устранения неполадок. Хотя многие записи журнала представляют собой относительно безобидные уведомления, мошенник может заявить, что записи журнала, помеченные как предупреждения и ошибки, являются свидетельством активности вредоносного ПО или того, что компьютер поврежден и должен быть незамедлительно «вылечен».

• Мошенник может показать жертве системные папки, содержащие файлы с необычными именами – например, папки Windows Prefetch и Temp – и заявить, что эти файлы являются свидетельством наличия вредоносного ПО на компьютере жертвы. Мошенник может открыть некоторые из этих файлов в «Блокноте», где содержимое файла отображается как беспорядочный набор служебных символов. Мошенник утверждает, что вредоносное ПО повредило эти файлы, что привело к абракадабре. На самом деле файлы в Prefetch обычно представляют собой безвредные, неповрежденные двоичные файлы, используемые для ускорения определенных операций.

• Мошенник может заявить, что некоторые отключенные службы не должны быть отключены.

• Мошенник может неправильно использовать инструменты командной строки для создания подозрительного вывода – например, с помощью команды tree или dir /s, которая отображает расширенный список файлов и каталогов. Мошенник может заявить, что утилита является сканером вредоносных программ, и во время работы команды ввести текст, якобы являющийся сообщением об ошибке (например, «нарушение безопасности… обнаружены трояны»), который появится после завершения выполнения команды.

• Мошенник может представить значения и ключи, хранящиеся в реестре Windows, как вредоносные.

• Мошенник может заявить, что предполагаемые «проблемы» являются результатом истекших лицензий на оборудование или программное обеспечение, например ключей ОС Windows, и уговорить жертву заплатить за «продление».

• Мошенник может заблокировать экран на компьютере жертвы, утверждая, что это результат действий вредоносного ПО или

запущенного сканирования, и использовать время для поиска конфиденциальной информации на компьютере жертвы.

• Мошенник может запустить команду netstat в терминале/ командном окне, которая показывает локальные и внешние IP-адреса соединений. Затем мошенник сообщает жертве, что эти адреса принадлежат хакерам, получившим доступ к его компьютеру.

• Мошенник может заявить, что нормальный процесс Windows, такой как rundll32.exe, является вирусом. Часто мошенник ищет в интернете статью о процессе Windows и переходит к разделу, в котором говорится, что имя процесса также может быть частью вредоносного ПО, даже если компьютер жертвы не содержит этого вредоносного ПО.

Согласно веб-сайту Microsoft, если кто-то свяжется с вами, представившись Microsoft:

1. Не покупайте никакое программное обеспечение или услуги.
2. Спросите, есть ли оплата или подписка, связанные с этой «услугой», – если есть, повесьте трубку.
3. Никогда не давайте контроль над своим компьютером третьему лицу, если вы не можете подтвердить, что это законный представитель компьютерной поддержки компании, клиентом которой вы уже являетесь.
4. Никогда не предоставляйте информацию о своей кредитной карте или финансовую информацию кому-либо, выдающему себя за сотрудника службы технической поддержки Microsoft.

Мошенничество с техподдержкой

Фишинг

Фишинг (*англ.* Phishing, от fishing – «рыбная ловля, выуживание») – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Это достигается путем проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приемами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определенному сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Для защиты от фишинга производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая, соответственно, именуется «антифишинг».

История

Техника фишинга была подробно описана в 1987 году, а сам термин появился 2 января 1996 года в новостной группе alt.online-service.America-Online сети Usenet[39], хотя возможно его более раннее упоминание в хакерском журнале 2600.

Ранний фишинг на AOL

Фишинг на AOL тесно связан с варез-сообществом, занимавшимся распространением программного обеспечения с нарушением авторского права, мошенничеством с кредитными картами и другими сетевыми преступлениями. После того как в 1995 году AOL приняла меры по предотвращению использования поддельных номеров кредитных карт, злоумышленники занялись фишингом для получения доступа к чужим аккаунтам.

Фишеры представлялись сотрудниками AOL и через программы мгновенного обмена сообщениями обращались к потенциальной жертве, пытаясь узнать ее пароль. Для того чтобы убедить жертву, использовались такие фразы, как «подтверждение аккаунта», «подтверждение платежной информации». Когда жертва называла пароль, злоумышленник получал доступ к данным жертвы и использовал ее аккаунт в мошеннических целях и при рассылке спама. Фишинг достиг таких масштабов, что AOL добавила ко всем своим сообщениям фразу: «Никто из работников AOL не спросит Ваш пароль или платежную информацию».

После 1997 года AOL ужесточила свою политику в отношении фишинга и вареза и разработала систему оперативного отключения мошеннических аккаунтов. В то же время многие фишеры, по большей части подростки, уже переросли свою привычку, и фишинг на серверах AOL постепенно сошел на нет.

Переход к финансовым учреждениям

Захват учетных записей AOL, позволявший получить доступ к данным кредитной карты, показал, что платежные системы и их пользователи также уязвимы. Первой известной попыткой стала атака на платежную систему e-gold в июне 2001 года, второй – атака, прошедшая вскоре после теракта 11 сентября. Эти первые попытки были лишь экспериментом, проверкой возможностей. А уже в 2004 году

фишинг стал наибольшей опасностью для компаний, и с тех пор он постоянно развивается и наращивает потенциал.

Фишинг сегодня

Целью фишеров сегодня являются клиенты банков и электронных платежных систем. В США, маскируясь под Службу внутренних доходов, фишеры собрали значительные данные о налогоплательщиках. И если первые письма отправлялись случайно, в надежде на то, что они дойдут до клиентов нужного банка или сервиса, то сейчас фишеры могут определить, какими услугами пользуется жертва, и применять целенаправленную рассылку. Часть последних фишинговых атак была направлена непосредственно на руководителей и иных людей, занимающих высокие посты в компаниях.

Социальные сети также представляют большой интерес для фишеров, позволяя собирать личные данные пользователей. В 2006 году компьютерный червь разместил на MySpace[40] множество ссылок на фишинговые сайты, нацеленные на кражу регистрационных данных. В мае 2008 года первый подобный червь распространился и в популярной российской социальной сети «ВКонтакте». По оценкам специалистов, более 70 % фишинговых атак в соцсетях успешны.

Фишинг стремительно набирает обороты, но оценки ущерба сильно разнятся: по данным компании Gartner, в 2004 году жертвы фишеров потеряли 2,4 млрд долларов США, в 2006 году ущерб составил 2,8 млрд долларов, в 2007-м – 3,2 миллиарда.

Техника фишинга

Социальная инженерия

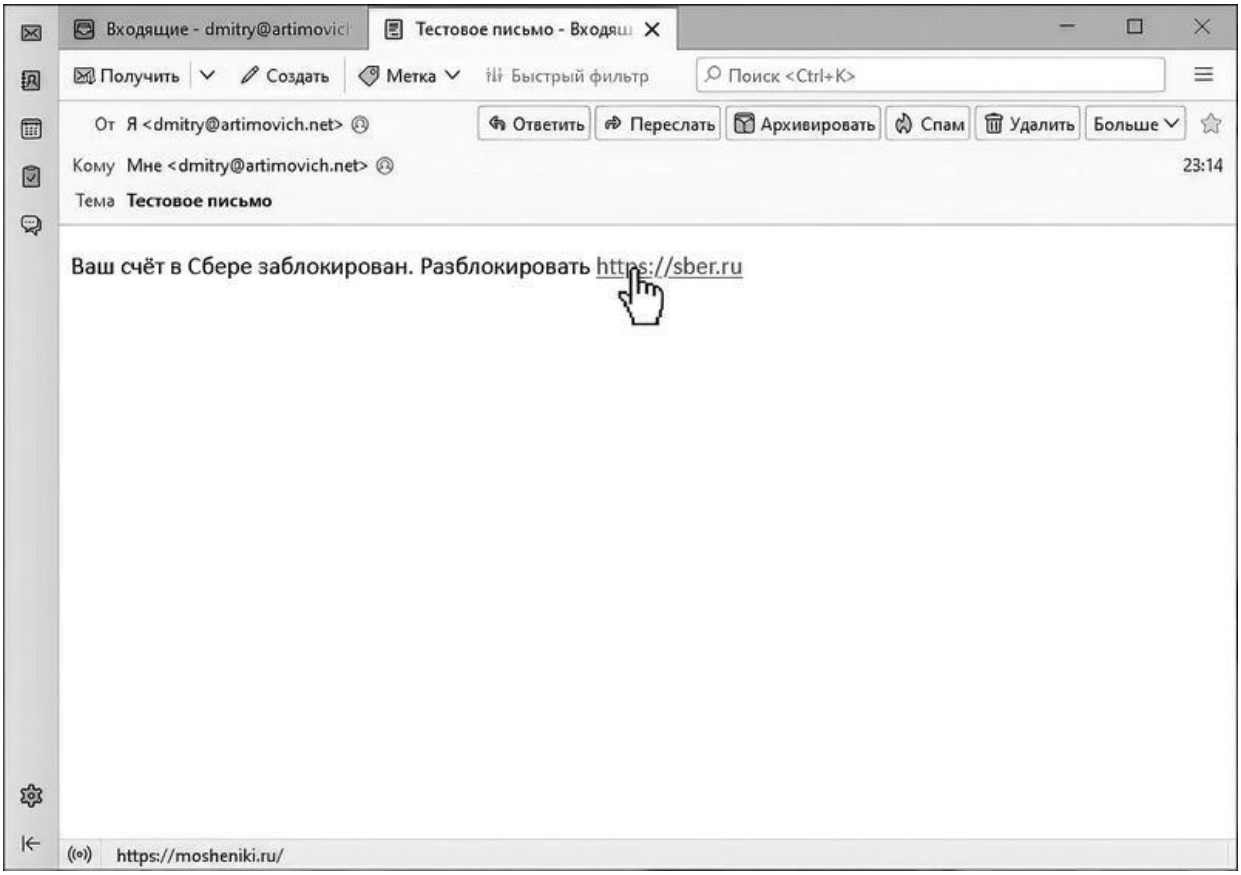
Человек всегда реагирует на значимые для него события. Поэтому фишеры стараются своими действиями встревожить пользователя и вызвать его немедленную реакцию. К примеру, электронное письмо с заголовком «чтобы восстановить доступ к своему банковскому счету…», как правило, привлекает внимание и заставляет человека пройти по веб-ссылке для получения более подробной информации.

Веб-ссылки

Большинство методов фишинга сводится к тому, чтобы замаскировать поддельные ссылки на фишинговые сайты под ссылки

настоящих организаций. Адреса с опечатками или субдомены часто используются мошенниками.

Например, https://www.yourbank.example.com похож на адрес банка Yourbank, а на самом деле он ссылается на фишинговую составляющую сайта example.com. Другая распространенная уловка заключается в использовании внешне правильных ссылок, в реальности ведущих на фишинговый сайт. Дело в том, что HTML позволяет указывать разными реальную ссылку и видимую часть, чем и пользуются мошенники. Кстати, любой браузер и многие почтовые клиенты показывают реальную ссылку внизу окна при наведении.



Один из старых методов обмана заключается в использовании ссылок, содержащих символ @, который применяется для включения в ссылку имени пользователя и пароля. Например, ссылка http://www.google.com@members.tripod.com приведет не на www.google.com, а на members.tripod.com от имени пользователя www.google.com. Эта функциональность была отключена в Internet

Explorer, а Mozilla Firefox и Opera выдают предупреждение и предлагают подтвердить переход на сайт.

Еще одна проблема была обнаружена при обработке браузерами интернациональных доменных имен: адреса, визуально идентичные официальным, могли вести на сайты мошенников. Например, в домен sber.ru можно вставить русскую букву E вместо английской.

Обход фильтров

Фишеры часто вместо текста используют изображения, что затрудняет обнаружение мошеннических электронных писем антифишинговыми фильтрами. Но специалисты научились бороться и с этим видом фишинга. Так, фильтры почтовых программ могут автоматически блокировать изображения, присланные с адресов, не входящих в адресную книгу. К тому же появились технологии, способные обрабатывать и сравнивать изображения с сигнатурами однотипных картинок, используемых для спама и фишинга.

Новые угрозы

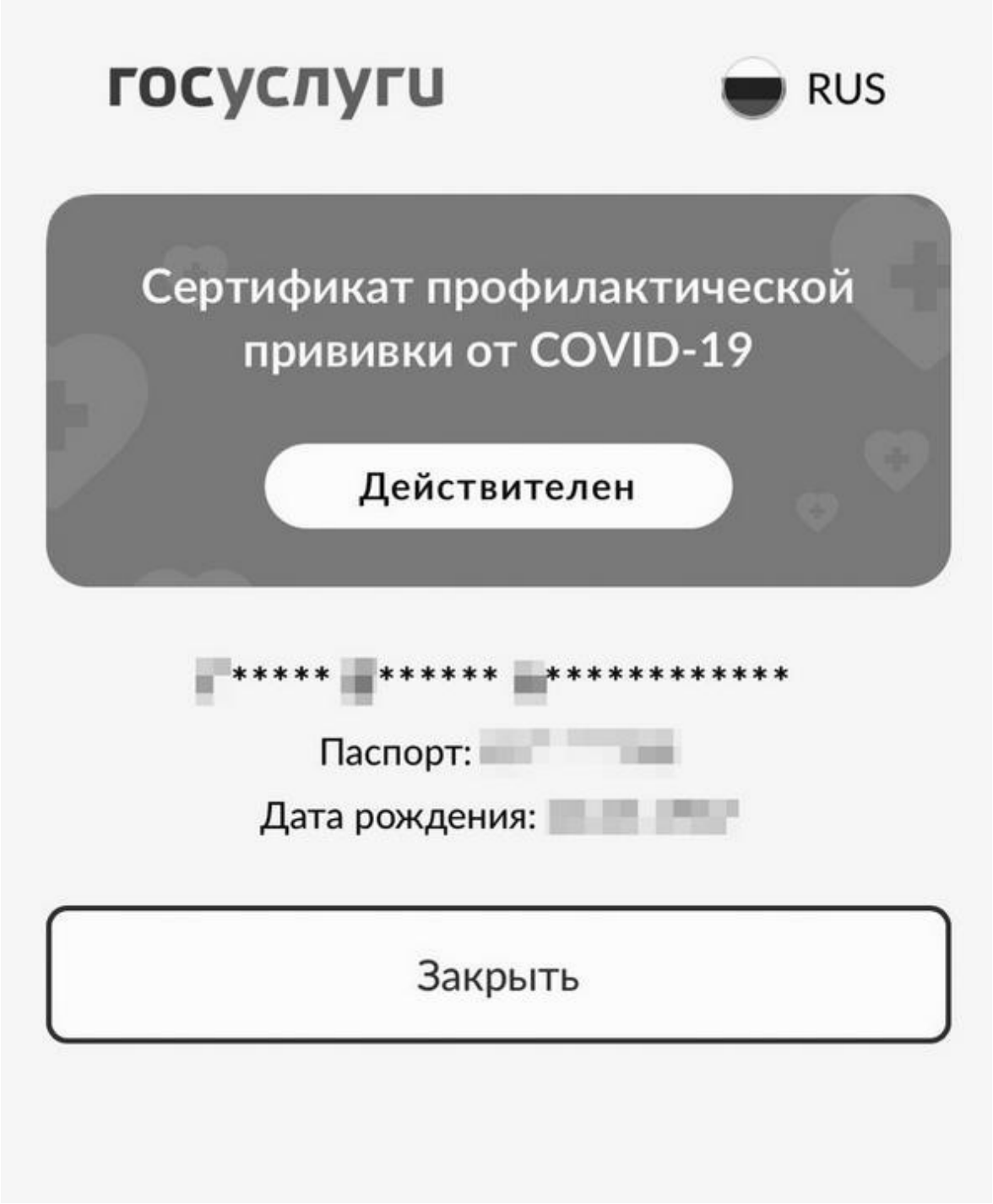
Сегодня фишинг выходит за пределы интернет-мошенничества, а поддельные веб-сайты стали лишь одним из множества его направлений. Письма, которые якобы отправлены из банка, могут сообщать пользователям о необходимости позвонить по определенному номеру для решения проблем с их банковскими счетами. Эта техника называется вишинг (голосовой фишинг). Позвонив на указанный номер, пользователь заслушивает инструкции автоответчика, которые указывают на необходимость ввести номер своего счета и PIN-код. К тому же вишеры, используя фальшивые номера, могут сами звонить жертвам, убеждая их, что они общаются с представителями официальных организаций. Чаще всего злоумышленники выдают себя за сотрудников службы безопасности банка и сообщают жертве о зафиксированной попытке незаконного списания средств с его счета. В итоге человека также попросят сообщить его учетные данные.

Набирает свои обороты и СМС-фишинг, также известный как смишинг (англ. SMiShing – от SMS и «фишинг»). Мошенники рассылают сообщения, содержащие ссылку на фишинговый сайт. Входя на него и вводя свои личные данные, жертва таким образом передает их злоумышленникам. В сообщении также может говориться о

необходимости позвонить мошенникам по определенному номеру для решения «возникших проблем».

QR-коды

Помните, как в 2021 году мэрия Москвы при поддержке Минцифры решила в очередной раз блеснуть своей глупостью и ввела QR-коды для посещения заведений общепита?



Технология QR-кода достаточно проста: в нем закодирована ссылка на внешний сайт. В примере с сертификатами вакцинации ссылка вела на портал Госуслуг, где была простенькая страничка, отображавшая, что сертификат действителен.

Почему я вдруг поднял эту тему? А всё просто: если взять технику фишинга, т. е. скопировать страничку, вставить туда нужные данные и разместить на каком-нибудь сайте типа gosuslugi.app – ни один проверяющий не заметит, что сайт ненастоящий. Честно признаться, в 2001-м я несколько раз проходил в кафе и рестораны по такому коду.

Я продемонстрировал, как легко подделать QR-код вакцинации газете «Коммерсантъ» и они написали статью «Неподменимых у нас нет». Тема была настолько больная, что поднялась настоящая буря в СМИ, да такая, что вызвала озабоченность даже в Кремле.

КАК НЕ ПОПАСТЬСЯ НА УДОЧКУ МОШЕННИКОВ?

1. Самое главное правило – компании и сервисы не запрашивают вашу конфиденциальную информацию по электронной почте. Если вы видите призыв зайти и что-то ввести – на 99 % это фишинг.

2. Настоящие компании и сервисы обычно называют вас по имени. Мошенники же опускают обращение и пишут просто что-то вроде «Дорогой пользователь».

3. Настоящие компании и сервисы присылают письма со своих доменов. Обращайте внимание, от кого пришло письмо, если в доменном имени есть лишние буквы и опечатки.

4. Проверяйте ссылки, по которым вас просят перейти. Наведите мышкой на ссылку и проверьте, совпадает ли отображаемое имя с тем, куда реально ведет ссылка, и написана ли сама ссылка верно, без ошибок (смотри выше техники фишинга).

5. При любом малейшем подозрении в том, что вы получили фишинговое письмо, просто свяжитесь с компанией напрямую. Например, настоящий URL-адрес компании можно найти в поисковой системе, банки часто пишут свои телефоны и адреса сайтов на обратной стороне карт.

Фишинг

Телефонное мошенничество

«Телефонные мошенники похищают со счетов россиян 3,5–5 миллиардов рублей ежемесячно. Средний чек по успешной мошеннической операции находится на уровне 8 тысяч рублей» (Станислав Кузнецов, зампред правления Сбербанка).

Ниже приведены некоторые из методов телефонного мошенничества.

Потенциальный покупатель

Человек размещает объявление в интернете, например, о продаже недвижимости на Авито. Так телефон из объявления немедленно попадает в поле зрения мошенников. И владельцу звонит некий «потенциальный покупатель», готовый платить, не торгуясь, но только на карту или «Сбербанк онлайн».

Для этого он просит сообщить номер карты, срок действия, CVV-код с обратной стороны карты. И СМС-код из сообщения банка о проведенной операции. Или же доступы от «Сбер-онлайн» и код подтверждения. Неопытный пользователь вполне может назвать все реквизиты, вот только после этого счет не пополняется, а опустошается мошенниками.

Звонки от «службы безопасности» банка

Не менее распространены звонки из «службы безопасности банка-эмитента платежной карты» о совершенной подозрительной операции или сбое в программном обеспечении, который привел к потере средств. Для восстановления счета и возврата денег якобы необходимо подтвердить, что вы – это вы, а для этого нужны данные вашей карты и СМС-код подтверждения. Или же другой сценарий: ваши деньги срочно нужно перевести на другой защищенный счет, данные от которого вам даже могут прислать в СМС с короткого номера банка.

Большинство банков имеют специальные номера, которые используются только для сообщений клиентам. Сбербанк, например, рассылает свои уведомления только с номеров 900 или 9000. Технология VoIP[41] позволяет менять номер звонящего, а некоторые провайдеры не блокируют эту возможность. Есть даже специальные

VoIP сервисы под такие вот мошеннические колл-центры, которые оставляют возможность смены номера. Так, при звонке мошенников вы можете видеть номер Сбера и на вопрос «А вы действительно Сбер?» вам нахально ответят: «Вы видите номер, с которого я звоню!»

Проблема настолько обострилась, что 02.07.2021 президент России подписал поправки в Федеральный закон «О связи», позволяющие блокировать СМС-сообщения и голосовые звонки с подменных номеров. Операторы лишаются права менять истинный телефонный номер звонящего и обязаны подключиться к специальной службе Роскомнадзора. Частично закон вступил в силу 01.12.2021, а полностью – с 01.05.2022 года. Нет сомнений, что эта мера резко осложнит жизнь телефонным мошенникам.

Звонки от «сотрудников» правоохранительных органов и государственных служб

Особенно циничны звонки из правоохранительных органов, якобы расследующих случаи мошенничества по телефону. Цель та же самая – усыпить бдительность и выманить нужную информацию. На фоне пандемии активизировались мошенники, которые представляются работниками Роспотребнадзора или Пенсионного фонда с сообщениями о новых социальных выплатах. Но для их получения необходимы все те же данные платежных карт.

Махинации со счетами мобильных телефонов

Самый распространенный вариант такого мошенничества – сообщение или звонок об ошибочном переводе денег на счет мобильного телефона и просьба вернуть их владельцу. Могут быть даже угрозы обращения в полицию или оператору с требованием блокировки телефона.

Сообщения о попавшем в беду родственнике и просьбы о помощи

Панический звонок о попавшем в беду родственнике обычно случается среди ночи, полусонной жертве сообщают об автомобильной аварии, наезде на пешехода, крушении поезда или любых других происшествиях, случившихся с детьми, внуками или просто друзьями.

Далее следует просьба о срочной помощи в виде перевода немалой суммы на электронный кошелек или счет мобильника.

Сообщения о выигрыше в лотерею

Отличная новость сопровождается требованием перевода на покрытие технических издержек самой лотереи. Здесь расчет на незнание законодательства РФ, согласно которому все расходы организаторов ложатся на них самих.

Сообщения-«грабители»

Жертве приходит СМС с просьбой перезвонить по мобильному номеру, где ему якобы должны сообщить важную новость (о выигрыше в лотерею, проблемах с банковской картой, получении наследства). На звонок долго нет ответа, а после отключения обнаруживается, что со счета списана большая сумма. Мошенники используют возможность зарегистрировать сервис с платным звонком. Обычно подобные сервисы развлекательные и обязательно сообщают о платности в рекламе. Но мошенники этого не делают, и за любой звонок по этому телефону взимается немалая плата.

Махинации с короткими номерами

В этом случае мошенники тоже используют мобильный сервис. При заказе некой услуги абонент получает сообщение, что для ее подключения нужно отправить сообщение на короткий номер такой-то. После отправки со счета списываются деньги. Механизм тот же, короткий номер тоже можно зарегистрировать как платный и не сообщать об этом абоненту.

КАК НЕ ПОПАСТЬСЯ НА УДОЧКУ ТЕЛЕФОННЫХ МОШЕННИКОВ?

Чаще всего мошенники представляются сотрудниками службы безопасности банков или правоохранительных органов. Звонящий сообщает о попытке взлома или блокировки банковской карты, подозрительных действиях в интернет-банке, пропущенном платеже по кредиту или угрозе штрафа по надуманному обвинению. На самом деле сотрудники служб безопасности банков никогда не звонят клиентам, а о подозрительной деятельности или других проблемах сообщают

другими способами. Правоохранительные органы тем более вызывают на допрос к себе в отделение повесткой, а не проводят допросы по телефону.

Данные карты, которые можно называть, – это только ее номер. Более того, сотрудники банка никогда не просят вас назвать номер полностью – обычно только последние четыре цифры.

Код безопасности CVV, ПИН-код карты сообщать никому по телефону нельзя. А СМС, которая приходит вам (код подтверждения), – тем более. Эта СМС по закону является аналогом вашей собственноручной подписи. Если вы сообщите мошеннику код из СМС, а тот подтвердит операцию перевода, вы снимете любую ответственность с банка за украденные деньги. Но об этом мы поговорим чуточку позже.

Если у вас возникли какие-то сомнения по поводу звонящего, сбросьте звонок и перезвоните по номеру поддержки вашего банка сами – обычно он есть на карте, в мобильном приложении или на сайте банка.

Мошенничество по телефону

Мошенничество в социальных сетях

Практически каждый современный человек пользуется социальными сетями. Они играют всё более важную роль в нашей повседневной жизни. А этим, в свою очередь, пользуются мошенники. По мнению экспертов, это происходит из-за того, что люди размещают в своих профилях слишком много личной информации. Так преступники могут больше узнать о потенциальной жертве, втереться к ней в доверие и обмануть.

Копии страниц

Схема проста – мошенники создают копию вашей страницы. Обычно профили пользователей открыты, и ничто не составит труда скопировать оттуда ваши фотографии, данные о работе, учебе, ваших друзьях. Если же ваша страница закрыта, то вы можете получить запрос на добавление в друзья от незнакомого человека. После создания копии вашей страницы с нее направляются сообщения вашим знакомым с просьбой перевести деньги или со ссылкой на вредоносный сайт.

То же самое, если вашу страницу удалось взломать. Хотя это уже не социальная инженерия. Например, вы подхватили трояна-кейлоггера, а он угнал у вас файлы cookies[42] и настройки браузера. Тем самым злоумышленник сможет зайти в социальную сеть вместо вас, даже без логина и пароля.

Кстати, Facebook старается бороться с копиями профилей. Если кто-то выложит уже размещенную ранее вами фотографию профиля, то алгоритмы Facebook могут заподозрить неладное и запросить проверку созданного аккаунта-копии.

Как распознать мошенника:

Случаи, когда хорошо знакомые друг другу люди просят деньги взаймы через социальные сети, редки. Просто позвоните знакомому и спросите его обо всем по телефону.

Онлайн-знакомства

С развитием социальных сетей они постепенно превратились в платформу для поиска второй половины. По данным журнала

Psychology Today, каждое пятое знакомство в Сети перерастает в романтические отношения. По прогнозам специалистов, к 2040 году около 70 % семей будут начинаться с онлайн-дейтинга.

Открытые для знакомств пользователи становятся целевой аудиторией мошенников, специализирующихся на кэт-фишинге. Это такой тип обмана, когда преступник создает в социальной сети фейковый аккаунт, наполняет его ненастоящими фотографиями и ложной информацией, которая, по его мнению, привлечет внимание потенциальных жертв. Глубоко увязнув в виртуальных отношениях, вы с большой долей вероятности согласитесь выслать мошеннику небольшую сумму денег для решения его срочных проблем – как и сотня других жертв.

Как распознать мошенника:

• Ваш собеседник отказывается от личной встречи, но просит вас выслать деньги.

• В странице собеседника есть нестыковки: мало фотографий, страница ведется недавно.

• Мое правило – никогда не давать деньги тем людям, которых ты не знаешь лично продолжительное время.

Онлайн-покупки

В соцсетях мошенники часто используют группы для торговли, продавая или покупая различные товары. Мошенники обычно размещают товар по низкой цене, получают за него деньги, но не отправляют товар. Также честные продавцы часто сталкиваются с фиктивными покупателями, которые предлагают приобрести у них товар с помощью поддельных услуг курьерских служб (DHL, Omniva и т. д.). Мошенники предлагают продавцам открыть ссылки с символикой данных компаний и ввести свои данные, после чего со счета продавца выманиваются деньги.

Одна из самых популярных схем мошенничества в Instagram также связана с торговлей. Мошенники зачастую создают фиктивные магазины в Instagram: выставляют несколько красивых фотографий товаров, покупают фальшивых подписчиков и размещают предложение о «суперакции», которое заставляет жертв попасться на крючок и

перечислить деньги или ввести и передать свои данные мошенникам, которые затем могут получить доступ к банковским счетам жертв и снять деньги.

Как распознать мошенника:

• Товар подозрительно дешевый.

• Реклама требует от вас незамедлительных действий (купи сейчас).

Отдавайте предпочтение крупным авторитетным маркетплейсам[43] (OZON, Яндекс. Маркет, eBay и т. д.), а не небольшим незнакомым магазинам. В больших маркетплейсах есть все товары, и маркетплейс несет ответственность за ваши платежи. В случае недобросовестного продавца вам вернут деньги.

Сообщения о выигрышах

Еще одна широко распространенная схема мошенничества как в Instagram, так и в Facebook связана с публикациями о различных конкурсах или выигрышах. Мошенники пользуются этим для имитации профилей организаторов конкурса и отправляют поддельные уведомления о выигрыше, которые обычно содержат ссылки, где требуется ввести личные данные якобы для получения выигрыша. Как только пользователь вводит свои данные, у него выманиваются деньги.

• Для получения выигрыша достаточно только номера карты. Если страница запрашивает больше – что-то тут нечисто.

• Бесплатный сыр бывает только в мышеловке. Я в принципе не верю в такие выигрыши.

Сообщения со ссылками

Такие сообщения хотя бы раз в жизни получал каждый из нас. Это текст, в котором содержатся ссылка и вопрос, стимулирующий переход по ней, например, «Ты видел свою фотографию?» или «Тут про тебя кое-что написали. Это правда?».

Кликнув по ссылке, вы попадаете на зараженный сайт или сайт-копию (фишинг). Например, на копию социальной сети. Далее мошенник получает ваши логин и пароль. Но сейчас это становится всё

менее актуально, так как социальные сети видят вход с другого компьютера и запрашивают подтверждение – например, по СМС.

Как распознать мошенника

1. Проверяйте отправителя сообщения. Это может быть пользователь, чье имя очень похоже на имя вашего друга, но в нем изменены одна-две буквы.

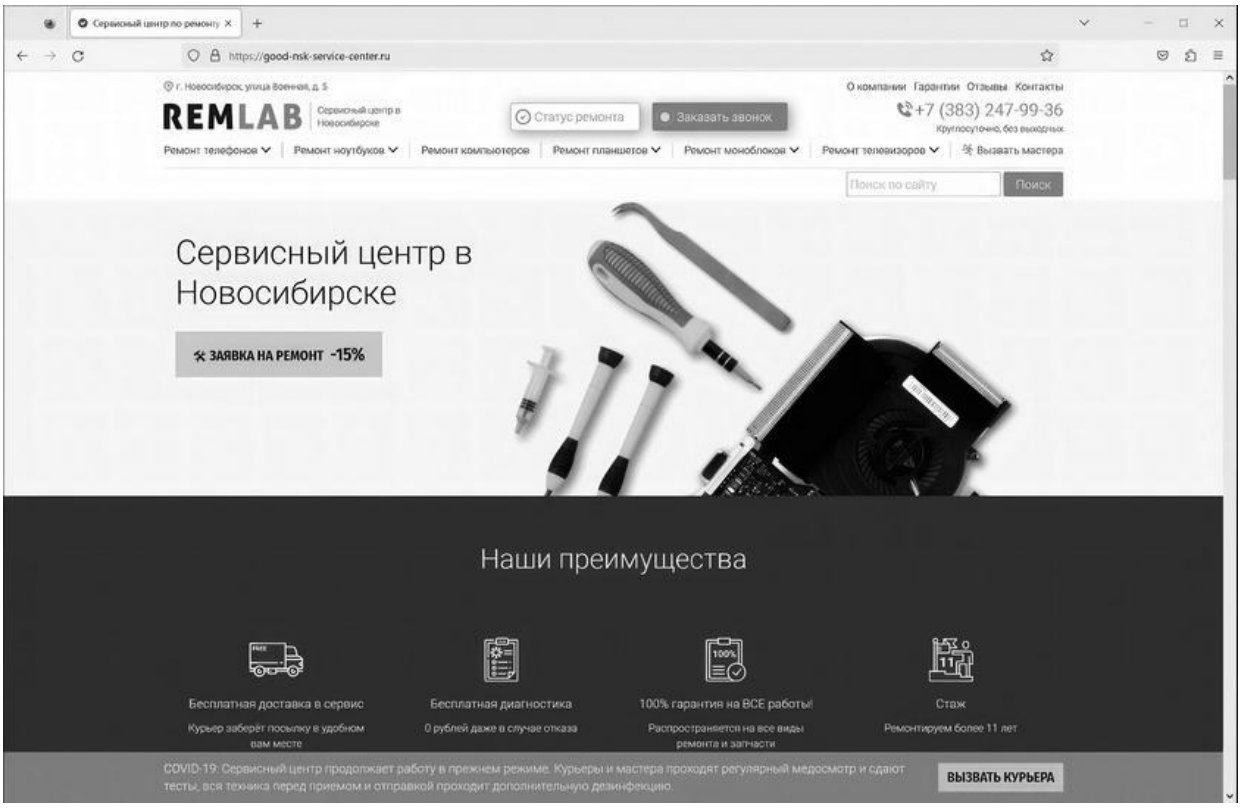
2. Никогда не переходите по незнакомым ссылкам.

3. Всегда проверяйте ссылку – это может быть домен, в котором также изменена пара букв.

Как мошенники обманывают в соцсетях

Сервисные центры

Не так давно у меня стал глючить ноутбук Asus VivoBook s14. Покупал я его еще в офис для своего сотрудника, сотрудник в итоге уволился. А ко мне в гости пришли «блюстители закона» из СД МВД России и незаконно изъяли всю мою технику (три ноутбука HP EliteBook разных поколений). Раз я вдруг неожиданно стал свидетелем, а эти «блюстители» могли заявиться и второй раз, как к другому такому же свидетелю, я решил попользоваться офисным недорогим ноутбуком.



Год он отработал и стал периодически подвисать, выводя в журнале Windows ошибку доступа к диску. Нашел я ближайший сервисный центр в Новосибирске, позвонил. Мне вежливо объяснили, что сейчас их офис не работает, но они могут прислать ко мне курьера. «Отлично, – сказал я, – это еще лучше».

Курьер забрал ноутбук, а на следующий день мне позвонил «мастер»:

– У вас компьютер подвисает, я даже тест запустить не могу.

– Да? – удивился я. – И что делать?

– У вас, скорее всего, на плате короткое замыкание. Я могу попробовать восстановить всё по заводскому трафарету.

– Ну давайте.

Прошло еще полдня. Звонит «мастер» еще раз:

– Все-таки не понравилась мне эта история с замыканием. Стал я разбираться, у вас пайка процессора с заводским браком, там искра проскакивает.

– Так у меня вроде только с диском проблемы были?

– Ну вот оно коротит и бьет по контроллерам. Я могу восстановить пайку. Это будет еще 10 тысяч, или поменять процессор – это 17 тыс. Лучше новый поставить, у него кеша больше будет.

– Хорошо, давайте новый.

В итоге, когда мне привезли ноутбук, то насчитали за ремонт 31 тыс. руб.: замена процессора, восстановление обвязки процессора и т. п. Признаюсь, я очень спешил и ноутбук нужен был срочно, поэтому, не особо разбираясь, я скинул 31 тыс. на карту по номеру телефона.

Хотя и насторожило меня следующее: старый выпаянный процессор мне не привезли. На следующий день при включении никакого увеличения кеша я не нашел, и подвисал ноутбук так же, с той же ошибкой.

После моего объяснения «сотрудникам» данного сервисного центра, что это 159-я статья чистой воды и что мне достаточно отвезти ноутбук на экспертизу и написать заявление в полицию, деньги мне вернули. Видимо, я очень убедительно объяснял.

Схема обмана здесь проста: вам начинают рассказывать много технических, часто бредовых, деталей и выписывают большие счета.

РЕКОМЕНДАЦИИ:

1. Выбирайте только официальные сервисные центры, обязательно с офисом.

2. Читайте отзывы в интернете.

3. Платите картой. В случае обмана перевод можно будет отследить.

Часть 4. Кардинг

Термином «кардинг» (carding) называют мошеннические операции с платежными картами (реквизитами карт), не одобренные держателем карты. Кардинг включает в себя различные способы обмана законных владельцев материальных средств.

В первой главе мы обсуждали трояны-кейлоггеры, которые воруют банковские данные и данные карточек. В этой главе мы подошли к цели кражи данных – их монетизации.

Скимминг

Кстати, данные карт можно красть не только с компьютеров и телефонов. Еще карты можно копировать в банкоматах или, например, ресторанах, когда вы даете карту в руки официанту. Ведь на всех картах до сих пор есть магнитная полоса, которую и можно скопировать. И до сих пор есть старые банкоматы, которые читают магнитную полосу. Также есть терминалы в некоторых магазинах, которые настроены на чтение магнитной полосы при ошибке (в нашем случае – отсутствии) чипа на карте.

Скиммер – специальное устройство, которое используется для считывания данных магнитной полосы пластиковых банковских карт. В большинстве случаев скиммеры крепятся непосредственно к банкомату, а именно к слоту картоприемника. При этом заметить наличие скиммера сможет лишь хорошо обученный и наблюдательный человек, у большей части граждан не возникнет никаких опасений.

Смиммер состоит из следующих элементов:

• считывающая магнитная головка – она считывает информацию с магнитной полосы, когда вы вставляете карту;

• преобразователь – преобразовывает считанную информацию в цифровой код;

• накопитель – записывает цифровой код на носитель данных.

Скиммеры для считывания данных с магнитной полосы карты бывают двух видов:

• одни накапливают информацию и требуют обслуживания, т. е. преступник должен физически снять данные;

• другие, более продвинутые, сразу передают информацию о картах мошенникам при помощи радиоканала на принимающее устройство, установленное поблизости. Может использоваться вариант устройства со встроенной сим-картой и передачей данных по сетям сотовой связи.

Преступникам, помимо того, что нужно считать информацию с карты, также нужно узнать и ПИН-код. Для этого применяются специальные накладные клавиатуры и миниатюрные камеры, заметить которые практически невозможно. Часто их маскируют под рекламные материалы или же непосредственно под козырек банкомата. Микрокамеры могут быть установлены где угодно, не обязательно на самом банкомате – всё зависит от сообразительности преступников.

В последнее время для уменьшения жертв скимминга многие банки стали устанавливать терминалы и банкоматы с сенсорными экранами, однако мошенников это абсолютно не смутило. Для получения ПИН-кода они начали использовать специальные накладки, которые крепятся прямо на экран.

Производители банкоматов выпускают также антискимминговые накладки, которые призваны не допустить установки скиммеров, а последние модификации подавляют работу мошеннических накладок с помощью электромагнитных волн, препятствуя считыванию информации с карты.

Правила

Пользуйтесь банкоматами в отделениях банков. Там банкоматы находятся под круглосуточным видеонаблюдением и риск нарваться на скиммер в разы меньше, чем, например, при использовании банкомата в торговом центре.

Кардинг

Возвращаемся к нашим троянам-кейлоггерам и фишинговым сайтам. Когда-то вирусы писали из чистого интереса. Со временем же сформировалась целая отрасль киберпреступности, в который разные люди обычно занимаются разными задачами:

• Есть хакеры, которые пишут трояны, кейлоггеры, шифровальщики, скайвары, связки эксплойтов.

• Есть люди, которые продают трафик под эксплойты.

• Есть люди, которые покупают эксплойты и трафик и продают уже загрузки.

• Есть люди, которые покупают трояны-кейлоггеры, эксплойты и трафик или же напрямую загрузки, а на выходе продают так называемы дампы (логины, пароли от сайтов, карточные данные, данные от онлайн-банков).

• Есть люди, которые разводят дропов (об этом чуть ниже).

• Есть люди, которые непосредственно покупают дампы карт, услуги дроповодов и обналичивают деньги с карт через покупку товаров.

Конечно, существуют целые команды, в которых есть все вышеуказанные «профессии». Кто-то пишет свои кейлоггеры, сам добывает загрузки и сам обналичивает деньги с украденных карт. Но это, наверное, частные случаи. В основном в подпольном кардерском рынке есть четкие разделения на «профессии». Общаются же эти люди на закрытых кардерских форумах в интернете или даркнете.

Очень часто СМИ смешивают понятия «хакер» и «кардер». Наверное, вы не раз читали отчеты о задержании хакерских группировок? Так вот, изначально хакерами называли программистов, которые исправляли ошибки в программном обеспечении каким-либо быстрым или элегантным способом. Слово hack пришло из лексикона хиппи, в русском языке есть идентичное жаргонное слово «врубаться» или «рубить в чем-либо». СМИ и Голливуд исказили слово «хакер», пропагандируя версию, что это именно компьютерный взломщик. Нет, ребята, которые пишут ядра операционных систем, антивирусы,

драйверы устройств, – это тоже хакеры. Да, Линус Торвальдс[44] – тоже хакер, хотя он ничего и не взламывал.

СМИ любят сообщать о задержании «группы хакеров», хотя в большинстве случаев задерживают только верхушку айсберга – людей, которые непосредственно заняты обналичкой денег.

Как работает обналичивание денег с краденых карт? Через покупку товаров или услуг.

Вещевой кардинг

Например, по краденым картам покупается техника в интернет-магазинах, ее нужно куда-то доставить. Вот тут и вступают в игру дропы и дроповоды. Дроп – это подставной человек, которому потом высылается товар, купленный по краденой карте. Очень часто дроп даже не подозревает, что его используют в незаконных целях. Обычно с дропом заключается договор (разумеется, липовый) о приеме на работу и оказании содействия в пересылке поставляемого товара. После получения товара дроп его либо пересылает дальше, либо продает на месте в комиссионке и переводит часть прибыли кардерам. Когда полиция начинает расследовать дело (если вообще начинает), то конечным получателем выступает подставной человек, который, скорее

всего, даже не догадывается о мошеннической схеме. Если же интернет-магазин, дроп и банк, выпустивший украденную карту, находятся в разных странах, это намного усложняет поиск реальных злоумышленников.

Кстати, в истории со скиммерами из украденного дампа печатается пластик. С ним злоумышленник идет в магазин затариваться техникой, которую потом продаст. Или попросту идет в банкомат и снимает деньги.

Кардинг услуг

Для обналичивания денег с украденных карт можно использовать схему по покупке хостинга, например, выделенных серверов. Такие серверы продаются на тех же подпольных форумах и обычно стоят в 2 раза дешевле. Такая схема более безопасна и проста: тут не нужны дропы, не нужно пересылать товар. Хотя в последнее время серверы и так сильно подешевели в цене.

Заливы

«Заливом» на сленге называют отмывание украденных денежных средств. В основном для этого используют всё тех же дропов. Работает это так: неизвестный человек предлагает очень выгодную операцию.

По его словам, на банковский счет получателя поступит некая, обычно довольно крупная, сумма денег, которую надо снять в банкомате и разделить на две части. Первую часть отправить на другой счет или электронный кошелек, а вторую – оставить себе в качестве вознаграждения. Удержаться от того, чтобы за несколько минут «подзаработать» приличную сумму, крайне сложно, даже если человек понимает, что операция, скорее всего, незаконная.

Трояны-кейлоггеры часто собирают доступы от онлайн-банков. Поэтому деньги могут украсть не только с карт, но и напрямую со счета. Особенно если ваш банк не требует подтверждения операций по СМС или каким-то другим способом.

Раньше среди кардеров эта была целая отмывочная отрасль. Когда деньги со счетов – в основном, граждан западных стран – переводились на счета дропов, а те их снимали и при помощи Western Union уже отправляли дальше мошенникам.

Правила

Пользуйтесь только теми банками, которые уделяют достаточно внимания безопасности: каждый вход или каждый перевод требует дополнительного подтверждения СМС-кодом или кодом со специального устройства, называемого цифровым ключом (digipass). В таком случае, даже получив ваши логин и пароль, злоумышленник всё равно ничего не сможет сделать.

Банковские карты

Я хочу немного рассказать об истории появления банковских карт, чтобы вы поняли, какая разница в защите прав держателя карт между США и Россией. Эту историю я описывал в своей первой книге – «Электронные платежи в интернете».

В США изначально кредитные (именно кредитные) карты распространяли по обычной почте – рассылали в конвертах. В погоне за раздачей как можно большего количества карт банки рассылали карты по телефонным книгам. Иногда доходило до абсурда – кредитную карту мог получить малолетний ребенок или домашний питомец. Естественно, карты крали из почтовых ящиков, иногда даже сами сотрудники почты. Банки несли убытки.

Продолжалось это до 1970 года, пока Конгресс США не издал закон, запрещающий рассылать карты по почте без разрешения держателя. При этом большинство случаев мошенничества включало в себя кражи карт из кошельков и карманов.

В 1970 году был издан закон Title 15 U.S. Code § 1644 – Fraudulent use of credit cards. Закон использовался для обвинения подсудимых в использовании поддельных, переделанных, утерянных, украденных или полученных обманным путем кредитных карт. Но это не уменьшило число случаев мошенничества с картами.

Наконец, в 1974 году Конгресс принимает Fair Credit Billing Act, который впервые узаконил следующее:

• 60-дневный срок, в течение которого держатель карты может оспорить ошибку в платежной выписке;

• если держатель карты обнаружил ошибку, он должен отправить запрос на оспаривание в письменной форме своему эмитенту;

• держатель карты не несет ответственности при использовании потерянной, украденной карты или использовании карты без его разрешения, достаточно просто позвонить в банк. Хотя закон и устанавливает минимальный размер транзакции 50$ при использовании карты (Face-to-Face), Visa и MasterCard это ограничение не используют. А при использовании карты мошенником в онлайне или по телефону держатель карты полностью освобождается от ответственности.

Fair Credit Billing Act считается прародителем chargeback'а[45]. Дальше закон трансформировался в правила Международных платежных систем (МПС), а правила обросли поправками. Сам же законодатель поступил достаточно мудро: раз банки создали МПС и зарабатывают на каждой транзакции и на кредитовании, то и за несовершенства в их системе должны отвечать они сами.

На сайте американской Visa вы можете увидеть Visa Zero Liability, которая гласит, что «вы не будете нести ответственность за неавторизованное использование вашей карты. Вы защищены, если ваша карта потеряна, украдена или используется мошеннически».

В Россию карты (эмиссия) пришли только в 90-е годы, у банков хватало других забот: торговля ценными бумагами, банковский кризис и т. д. Так что продвижением карт как «безопасного способа оплаты» никто не занимался.

27 июня 2011 г. вышел Закон № 161-ФЗ «О национальной платежной системе», который в пункте 11 статьи 9 «Порядок использования электронных средств платежа» дал аж целый 1 день (!) на уведомление банка-эмитента о мошеннической операции.

По правилам МПС вы можете заявить о мошеннической операции в течении 120 дней. По факту российские банки впаривают вам «страховку от мошенничества». Это, по сути, деньги из воздуха, то, что и так заложено в правилах платежных систем. В случае возврата украденных средств деньги возвращаются за счет интернет-магазина – а нам преподносят это как некую платную услугу.

Нередки случаи, когда банки отказываются вернуть украденные деньги. Например, если у вас скопировали карту и сняли деньги в банкомате вашего банка-эмитента. Тут риск и компенсация полностью ложатся на банк-эмитент. А если сумму украли приличную, эмитент может и не захотеть ее возвращать. И пожаловаться-то вам некому – вы не участник платежной системы (участники – только банки), жалобу от вас не примут. ЦБ также защищает интересы банков.

В своей книге One from Many: VISA and the Rise of Chaordic Organization создатель Visa Ди Хок сожалеет, что так и не смог сделать держателей карт участниками организации Visa наравне с банками.

То, что в США десятилетиями формировалось с помощью законов и правил, развивая карточную отрасль, у нас аккуратно замалчивается и

не афишируется.

Наряду с нежеланием заниматься лишней работой банки также практикуют подмену понятий. Например, практически все банки рекламируют держателям карт технологию 3D-Secure, которая, вообще-то, защищает в первую очередь сами банки, а не кардхолдеров. Исторически ведь риски за мошенничество лежат на банке-эквайере, и уже потом банк-эквайер[46] перекладывает chargeback на торговые точки. При оспаривании таких платежей МПС в большинстве случае становятся на сторону держателя карты. Отсюда родился новый тип мошенничества – Friendly Fraud, когда держатель карты сначала покупает, а потом сам же и оспаривает платеж. И именно 3D-Secure защищает эквайера/торговую точку от chargeback'ов: «держатель карты не авторизовал транзакцию». Прошел подтверждение эсэмэской – значит, сам и платил. А дело всё в том, что СМС по закону приравнивается к собственноручной подписи: подписал – значит, тебе никто не должен. Рядовому держателю карты от 3D-Secure ни тепло, ни холодно, а кардер уж точно не станет покупать iPhone там, где нужно вводить код из СМС.

Еще очень важный момент: в платежных системах предусмотрены возвраты (чарджбеки, от *англ*. chargeback) не только за мошенническую транзакцию, но еще и в случае неоказанной услуги или недоставленного товара. Вы об этом знали? Если вы купили товар, но он вам не пришел, а магазин отказывается вернуть деньги, вы можете смело писать заявление в свой банк-эмитент на возврат денег.

При этом механизм чарджбеков не распространяется на перевод с карты на карту (p2p[47]), так как этот механизм был сделан для перевода от физического лица физическому лицу, а не для оплаты товаров и услуг. В случае, если вы платили за товары переводом на карту, правила МПС по возвратам работать не будут.

Здесь тот же случай, что и с телефонными мошенниками, которые стараются получить данные вашей карты и сделать перевод с карты на карту. Если им получается выудить смс-подтверждение, т. е. если вы его назвали (по факту вы подписали перевод) – тем самым вы снимаете любую ответственность за такую операцию с банков и платежной системы.

Что же все-таки делать, если никаких СМС-кодов вы никому не сообщали, деньги с карты все-таки украли, а банк отказывается их вам

вернуть? В российском Гражданском кодексе есть одна лазейка: каждая банковская карта у нас привязана к счету, а оплата любого товара или услуги – это, по сути, списание денег с вашего счета. Так вот, ст. 854 ГК РФ «Основания списания денежных средств со счета» гласит: «Списание денежных средств со счета осуществляется банком на основании распоряжения клиента». Т. е. если вы не давали распоряжения и не подтверждали операцию, такое списание можно оспорить в гражданском суде.

Правила еще раз

1. Пользуйтесь банкоматами в отделениях банков. Там банкоматы находятся под круглосуточным видеонаблюдением и риск нарваться на скиммер в разы меньше, чем, например, при использовании банкомата в торговом центре.

2. Помните, что у вас есть право оспорить мошеннический платеж в течение 120 дней в своем банке-эмитенте, если вы не подтверждали такую операцию СМС-кодом.

3. Если же банк отказывается вернуть деньги, украденные с карты без вашего ведома, есть статья 854 ГК РФ, которой можно воспользоваться при подаче гражданского иска к банку-эмитенту.

Кардинг

Часть 5. Паранойя

Защита информации в современном мире становится всё более актуальной темой. Ведь, кроме «злых хакеров», которые пытаются подсадить вам очередного трояна-кейлоггера и похить ваши банковские данные, есть угроза физического доступа к вашему компьютеру, угроза перехвата вашего интернет-трафика. Если, например, вы пользуетесь криптовалютой или у вас хранится конфиденциальная информация, ее, безусловно, нужно защищать. Ваш компьютер (ноутбук тем более) могут украсть, вы можете его забыть, или же его могут изъять «оборотни в погонах», когда будут отрабатывать очередной заказ на вашего шефа.

К сожалению, проблема заказных уголовных дел и незаконных обысков в России стоит очень остро. Например, в марте 2022 года ко мне вломились сотрудники Следственного департамента МВД (того, что находится на Газетном, 4). Заказное уголовное дело было возбуждено против моего старого работодателя, господина Врублевского. Для наведения шума были устроены обыски у 20 «свидетелей». При этом в свидетели записывали по следующему признаку: работал там 10 лет назад – значит, свидетель. В итоге у меня были незаконно изъяты денежные средства и техника.

Печально то, что наша правоохранительная система абсолютно не работает. Судьи-подстилки ложатся под продажное следствие. Например, судья Мещанского суда Бельченко 4 раза отказывалась принимать жалобу на отказ следователя вернуть изъятые денежные средства, а после максимально тянула время до передачи дела в апелляцию.

К чему я всё это рассказываю? Для того, чтобы показать вам важность защиты и резервного копирования данных. Иначе вы можете лишиться всего в один миг. Нужно быть готовым к этому.

Когда я в день обыска попал на допрос, следователь Евгений Морозов изо всех сил пытался меня убедить назвать пароли от зашифрованного диска. И заверял, что моя криптовалюта будет скопирована и будет содержаться в сохранности. Что-то мне подсказывает, что она пропала бы в неизвестном направлении. А такие

судьи, как Бельченко или Оганова, разводили бы руками и говорили, что абсолютно не понимают, о чем речь.

Вернуть свои наличные и технику я не могу уже год. Полагаю, что это месть за отказ предоставить доступ к зашифрованным дискам. Ведь рано или поздно деньги и вещи придется отдать, а вот криптовалюта могла бы и пропасть… Вот имена этих «героев»: следователь по особо важным делам 3-го отдела Управления по расследованию организованной преступной деятельности майор юстиции Евгений Морозов, Дмитрий Бабушкин, Иван Клевцов, Д.С. Карсаев. Господин Карсаев так вообще заявил, что он не определился еще, что делать с моими деньгами, сумма которых в десятки раз превышает вменяемую сумму хищения.

Случаи хищения криптовалюты правоохранительными органами нередки: например, всё в том же 2022 году сотрудник УФСБ по Самарской области Дмитрий Дёмин признал вину в краже биткоинов на 187,4 миллиона рублей у подследственного хакера из Сызрани[48].

Так что я очень серьезно отношусь к защите свои данных. И в этой главе я расскажу о ней. Некоторые правила могут вызвать у вас ассоциацию с паранойей – отсюда и название. Но эти правила мне уже не раз помогали. Тем более что это не первое мое столкновение с так называемыми защитниками правопорядка. О первом, когда сотрудник ФСБ хотел, чтобы я зарабатывал ему деньги, я писал в книге «Я – хакер! Хроника потерянного поколения».

Глава рассчитана на продвинутых пользователей. Пользователей, у которых есть данные, которые не должны попасть в руки злоумышленников или коррумпированных сотрудников правоохранительных органов.

Шифрование дисков

Отстраивать безопасность своих данных нужно с шифрования дисков – в первую очередь дисков вашего рабочего компьютера. Тогда в случае изъятия, кражи или потери (бывает такое: забыл где-то ноутбук) никто не сможет получить доступ к вашей конфиденциальной переписке, платежным данным, криптокошелькам, паролям и всему, что вы храните на своем компьютере. При этом шифровать нужно как системный диск (диск, на котором стоит операционная система), так и любой другой диск с данными.

В любом вопросе защиты (шифрования) данных или переписки ни в коем случае нельзя доверять коммерческому программному обеспечению. Хотя, например, все криптографические[49] продукты в России должны проходить обязательную сертификацию в ФСБ, это абсолютно ничего не значит.

Нужно исходить из того, что ко всем криптографическим коммерческим или сертифицированным продуктам есть запасные лазейки у спецслужб – будь то российские продукты или западные.

В коммерческую операционную систему Microsoft Windows встроена система шифрования дисков BitLocker, которая даже умеет хранить криптографические ключи (т. е., по сути, ключи, которыми можно расшифровать весь ваш диск) в модулях TPM[50]. Неужели вы действительно считаете, что у Microsoft или производителя вашего дорого ноутбука с указанным выше криптографическим чипом нет возможности извлечь ваши ключи шифрования? Или правда верите в сказки, что ФБР судится с Apple из-за того, что Apple отказывается передать ФБР средства дешифровки айфонов?

Столкновение Apple и правительства США связано с делом террориста Сайеда Фарука. Сайед Ризван Фарук вместе со своей женой Ташфин Малик 2 декабря 2015 года ворвались в центр для людей с ограниченными возможностями в Сан-Бернардино, где открыли беспорядочную стрельбу, убили 14 человек и ранили 22. Оба террориста были застрелены. В ходе расследования обнаружилось, что преступники предварительно уничтожили все средства связи и стерли информацию о себе. Но спустя некоторое время был найден смартфон Фарука.

ФБР обратилось к Apple с просьбой оказать помощь в получении доступа к данным террориста на заблокированном iPhone 5c. Apple согласилась оказать посильную помощь в расследовании дела, в частности, выкачав для ФБР все данные Фарука из облачного хранилища iCloud. Но компания отказалась предоставить физические данные, содержащиеся на самом смартфоне, поскольку система безопасности Apple устроена так, что даже работники компании не могут получить доступ к ним. Схема защиты стирает все данные при десятикратном вводе неверного пароля для разблокировки экрана.

Как бы вам ни понравилась эта история, но я в нее не верю. Для меня это просто цинично срежиссированная реклама. У спецслужб

очень много возможностей и ниточек, за которые они могли бы потянуть и получить желаемое.

Чего стоит раскрытая Эдвардом Сноуденом программа глобальной слежки США PRISM. PRISM – комплекс мероприятий, осуществляемых с целью массового негласного сбора информации, передаваемой по сетям электросвязи, принятая американским Агентством национальной безопасности (АНБ) в 2007 году в качестве замены Terrorist Surveillance Program, формально классифицированная как совершенно секретная.

Широкой общественности о существовании программы стало известно 6 июня 2013 года, когда отрывки из секретной презентации о PRISM были опубликованы в газетах Washington Post и Gardian.

По оценкам Washington Post от 2010 года, ежедневно системы сбора информации АНБ (в том числе PRISM) перехватывали и записывали около 1,7 миллиарда телефонных разговоров и

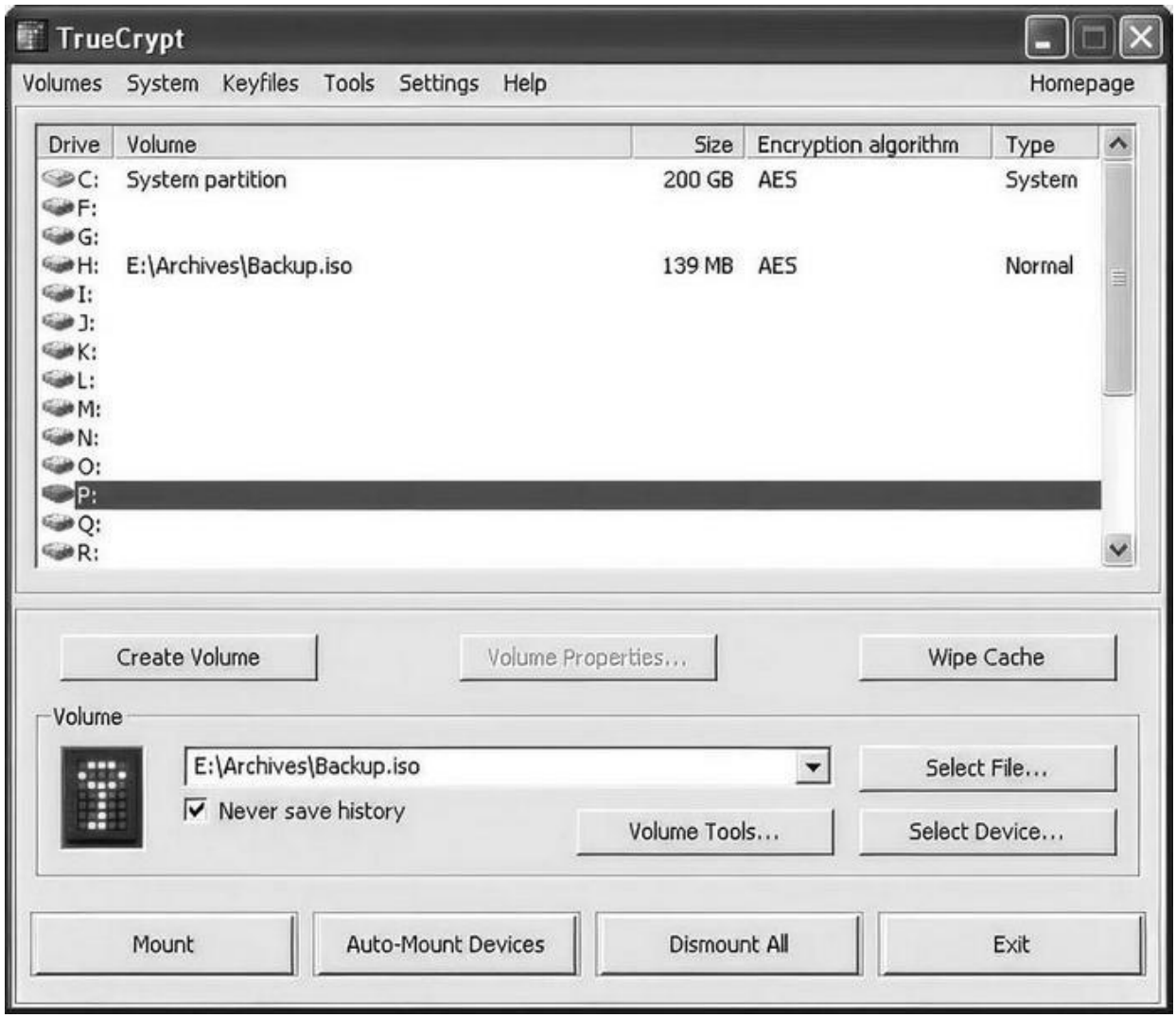
электронных сообщений и около 5 миллиардов записей о местонахождении и передвижениях владельцев мобильных телефонов по всему миру.

Директор Национальной разведки США Джеймс Клеппер подтвердил существование PRISM и заявил, что программа работает в соответствии с Законом об иностранной разведке, недавно пересмотренным Конгрессом США. Отчеты, основанные на утечках документов, описывают PRISM как комплекс административных мер, предоставляющих возможность углубленного наблюдения за интернет-трафиком пользователей некоторых интернет-ресурсов. Потенциальной целью наблюдения могут быть любые пользователи определенных сервисов, не являющиеся гражданами США, либо граждане США, чьи контакты включают в себя иностранцев. Особо отмечается, что наибольший интерес представляют люди, живущие вне Соединенных Штатов. PRISM дает право Агентству получать самую разнообразную информацию: просматривать электронную почту, прослушивать голосовые и видеочаты, просматривать фотографии, видео, отслеживать пересылаемые файлы, узнавать другие подробности из социальных сетей.

По заявлениям спецслужб, по решению суда на активное сотрудничество вынуждены были пойти многие крупные компании, предоставив спецслужбам доступ к серверам Microsoft (Hotmail), Google (Google Mail), Yahoo! Facebook, YouTube, Skype, AOL, Apple и Paltalk.

Какими бы благими ни были провозглашаемые намерения, но никто не гарантирует, что люди, управляющие такими инструментами, не будут злоупотреблять своей властью. Ведь ничто не помешало американцам (в том числе и лично директору АНБ) обвинить Россию во вмешательстве в выборы президента США в 2016 году.

Когда у вас в руках есть власть, почему бы не воспользоваться ею для своих личных интересов? Как, например, сделал Следственный департамент МВД, проведя незаконный обыск в моей квартире и незаконно изъяв деньги и технику в марте 2022 года.



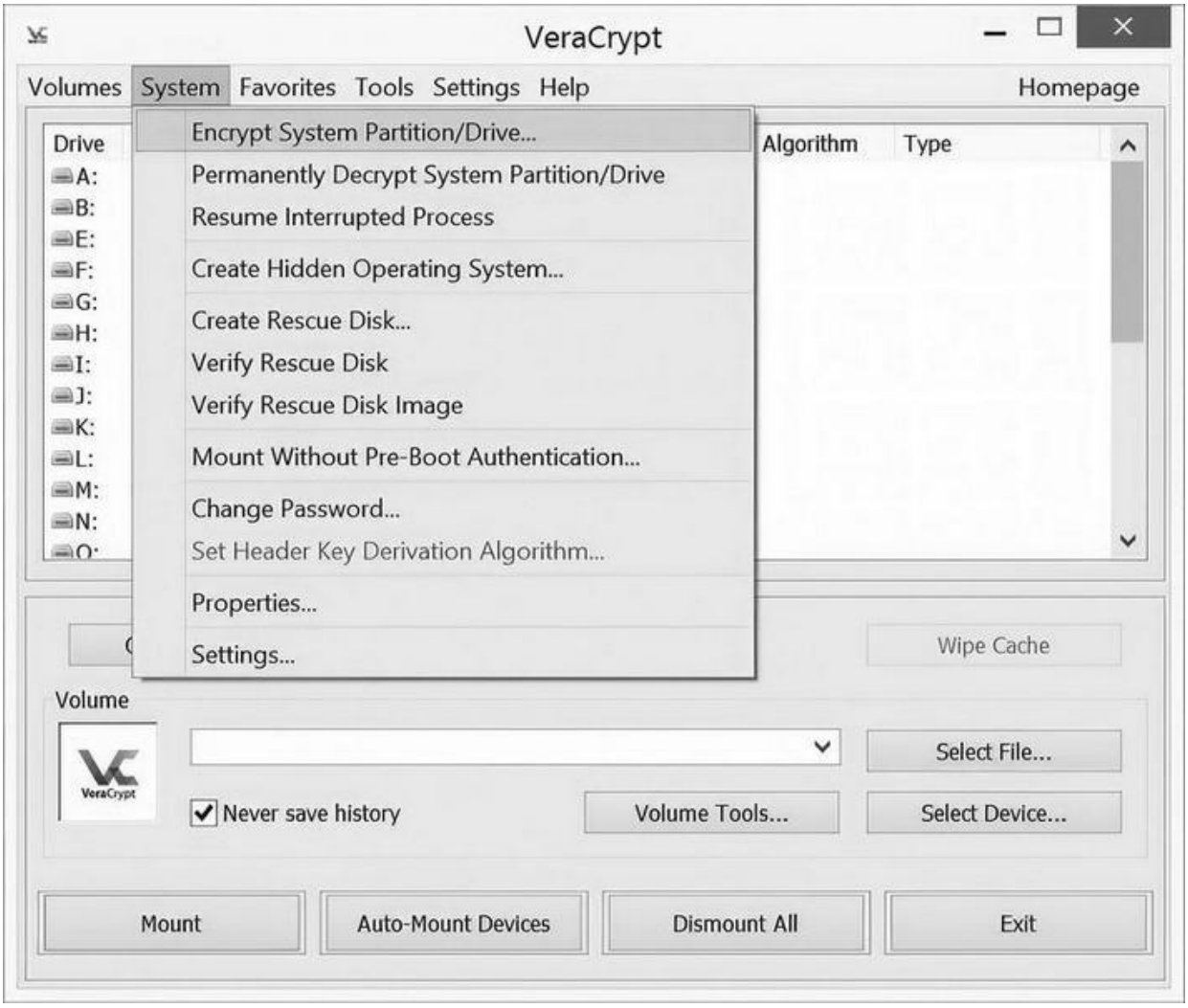
Итак, отдавайте предпочтение криптографическому программному обеспечению с открытым исходным кодом. Это, конечно, не гарантирует на 100 %, что в таком коде не будет скрытых лазеек, но как минимум уменьшит шанс, что такие лазейки будут, на порядки.

Лучшим выбором для шифрования диска раньше был TrueCrypt, пока его не купила и не свернула разработку Microsoft в 2014 году. Верно, зачем нужен бесплатный инструмент шифрования, да еще и с открытым исходным кодом, без лазеек для спецслужб…

Но энтузиасты взяли код TrueCrypt и сделали несколько ответвлений от него, также с открытым исходным кодом. Я, к примеру, пользуюсь VeraCrypt.

Инструкция по шифрованию системного раздела

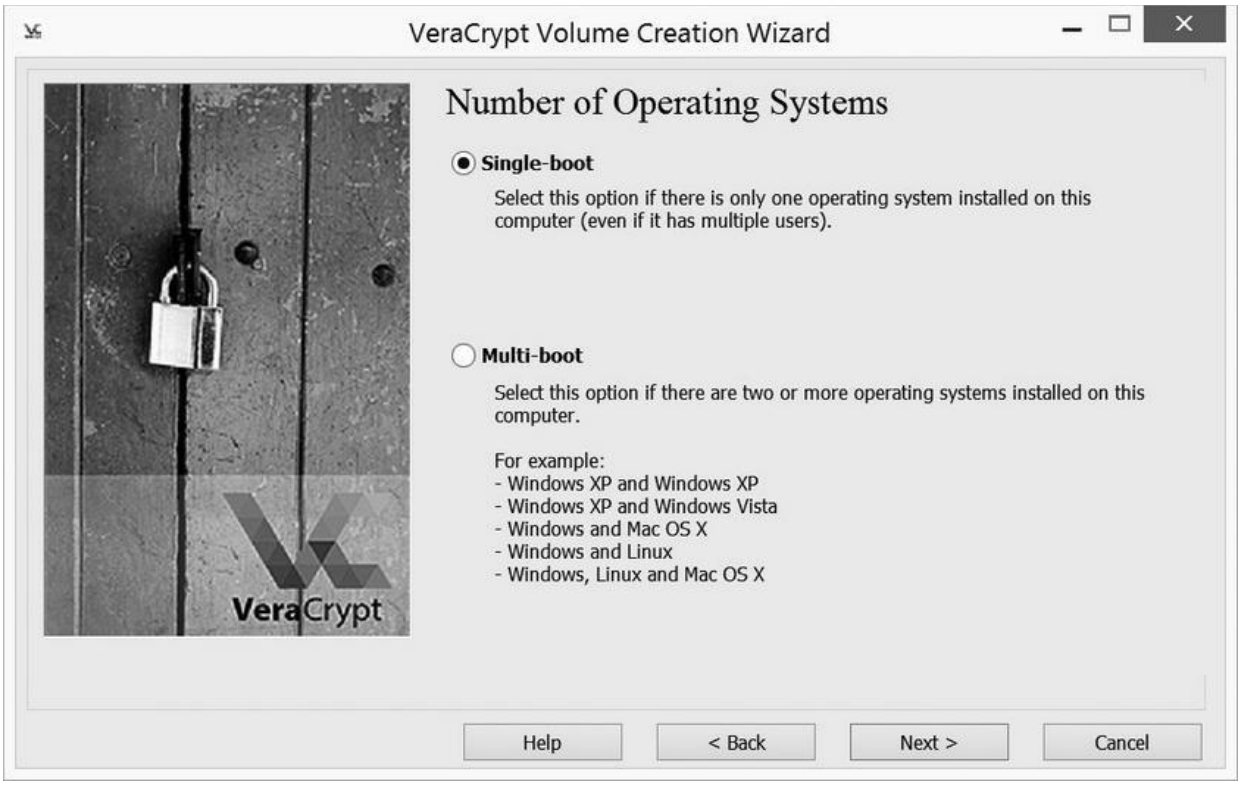
1. Запускаем VeraCrypt, выбираем Encrypt system partition/drive.



2. Далее – Type of system encryption – > Normal.

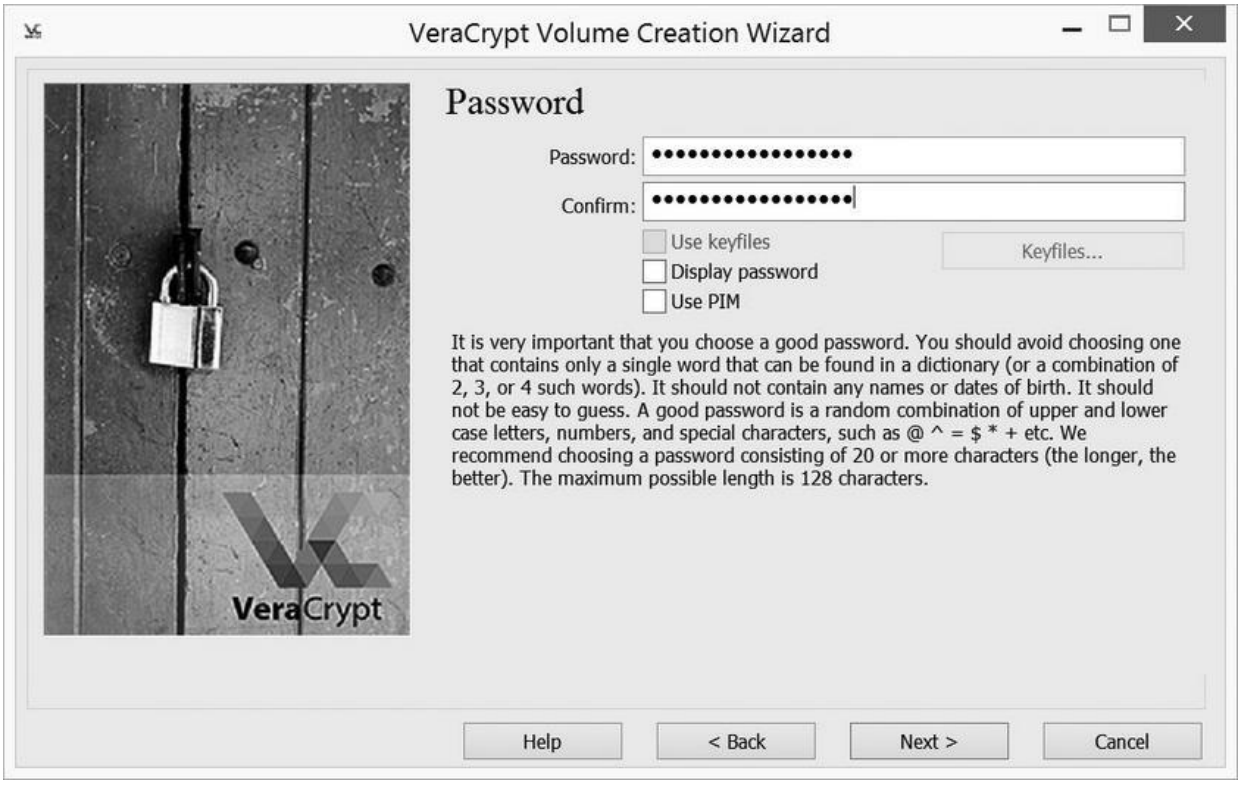
3. Encrypt the Windows system partition.

4. Number of Operation Systems – тут зависит от того, сколько у вас операционных систем стоит. У меня одна – основная.

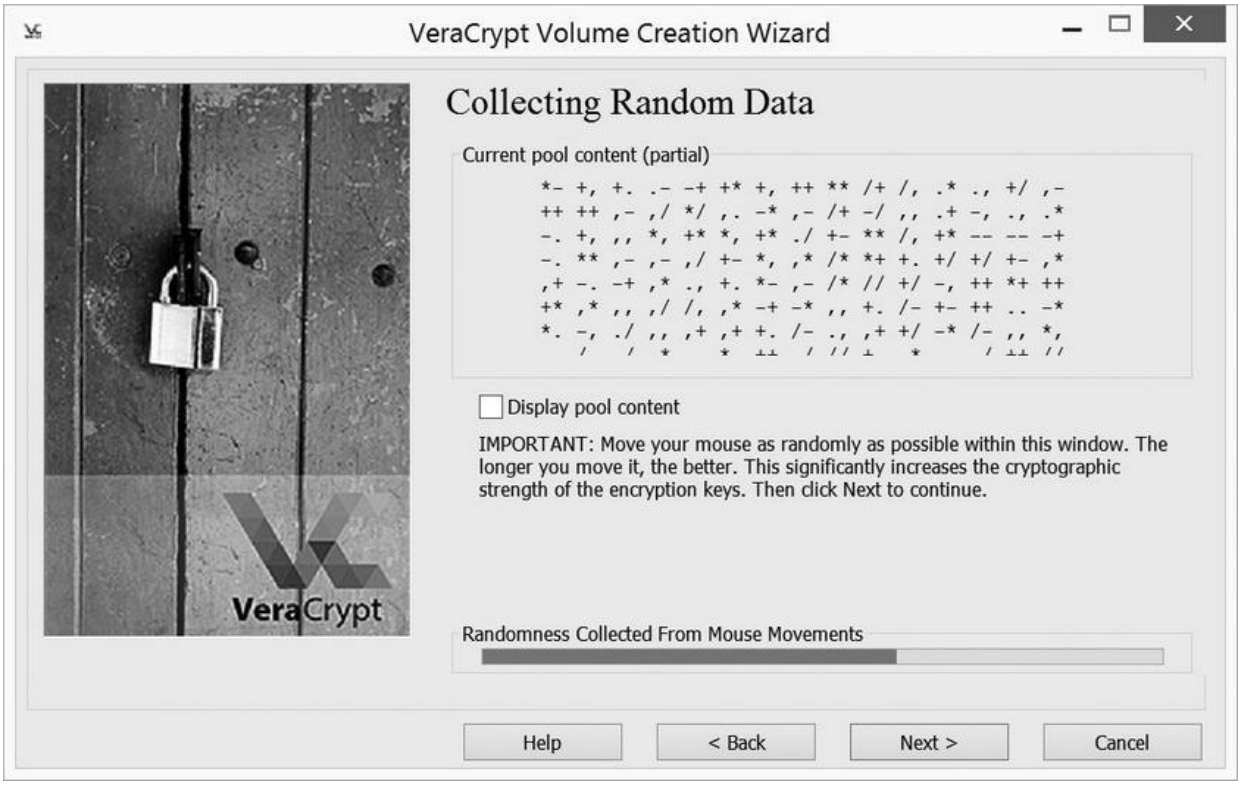


5. Выбираем шифрование AES.

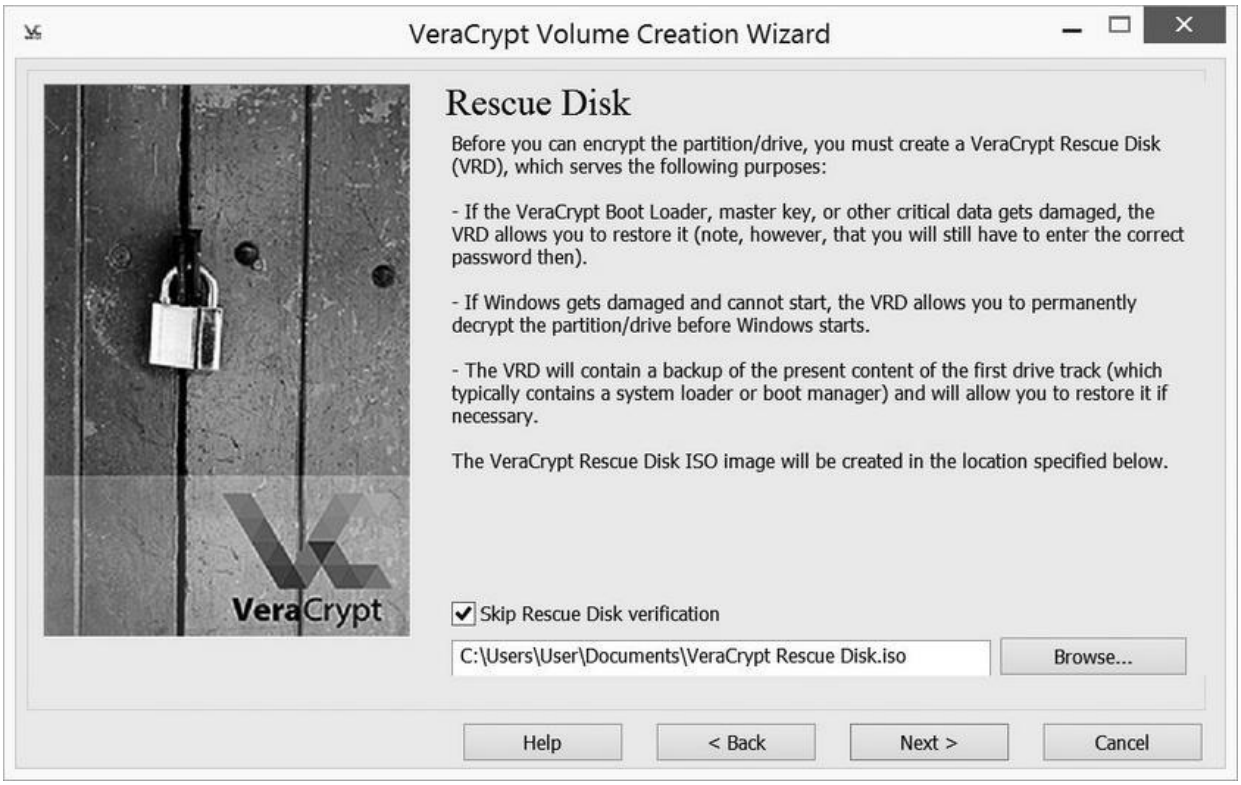
6. Вводим пароль и подтверждение. Пароль обязательно должен состоять из букв разных регистров, цифр, желательно – специальных символов и быть длинным.



7. Дальше энергично водим мышкой, пока VeraCrypt собирает ваши беспорядочные движения – как только линия снизу станет зеленой, можно двигаться дальше.



8. Создаем Rescue Disk. Архив нужно будет распаковать и положить на флешку и в бекап. Если вдруг какой-то кривой апдейт Windows перетрет загрузочную область, вы рискуете потерять все данные. А так вы всегда можете загрузить со спасательной флешки и восстановить загрузчик VeraCrypt’a.



9. Дальше выбираем Wipe Mode – количество перезаписей сектора мусорными данными. Дело в том, что даже после удаления данных с диска их всё еще можно восстановить, но для этого требуется специальное дорогое оборудование. У западных лабораторий такое точно есть. Про наши ничего сказать не могу. Так что ставьте 3 перезаписи – этого будет вполне достаточно.

10. Дальше нажимаем Test. Система перезагрузится и попросит ввести пароль. Диск еще не зашифрован, просто это проверка того, что загрузчик и драйверы VeraCrypt’а встали нормально. Если что-то вдруг пойдет не так, то загрузчик ОС можно будет достаточно легко восстановить.

11. Загружаемся, в появившемся окне нажимаем Encrypt и ждем.

12. После окончания диск зашифрован.

Аналогичным образом можно зашифровать любой другой диск или флешку – например диск, на котором вы храните бекапы (об этом ниже).

Правила

Все компьютеры, диски, флешки с беками шифруются любым софтом, производным от TrueCrypt’a (full disk encryption). Сам TrueCrypt ухреначил Microsoft, он больше не поддерживается. Софт обязательно должен быть с открытым кодом. Всё платное – сразу в топку.

PRISM (программа разведки)

Установите пароли на всё

Представьте такую ситуацию. Вы предприняли все меры к защите данные: зашифровали диск, установили длинный сложный пароль и ушли за кофе, не заблокировав компьютер.

В это время через окно в ваш кабинет проникает «злостный хакер» и копирует всю конфиденциальную информацию на флешку, после чего так же бесшумно исчезает через то же окно.

Мораль такова: нужно установить пароли на всё – на вход в систему, на вход в BIOS. Всегда, когда отходите от компьютера даже на минуту, блокируйте систему.

Пароли должны быть сложнее стандартных qwerty, password, «пароль» или 12345. Желательно, чтобы это были цифры и буквы разных регистров (большие и маленькие). К тому же пароль от VeraCrypt или подобного программного обеспечения должен быть длинным.

Настройте скринсейвер[51] на автоматическое включение через 5 минут, а возврат в систему – только с вводом пароля.

Теперь можно пойти за кружечкой кофе. Если только вас не взяли в разработку американские спецслужбы…

Отключите спящий режим

Пока ваш компьютер включен, ключи шифрования от системного диска находятся в оперативной памяти ОЗУ[52]. Поэтому возникает резонный вопрос: а можно ли эти ключи оттуда достать? Оказывается, можно – для этого нужен физический доступ к вашему компьютеру.

Cold boot attack (platform reset attack, атака методом холодной перезагрузки) – в криптографии это класс атак, при которых злоумышленник, имеющий физический доступ к компьютеру, может извлечь из него ключи шифрования или ценные данные. Атака требует полной перезагрузки компьютера либо выключения и изъятия из него модулей памяти. В атаке используется эффект сохранения данных в ОЗУ типа DRAM и SRAM после выключения питания. Данные частично сохраняются в течение периода от нескольких секунд до нескольких минут. Если же охладить микросхемы памяти жидким азотом, то время сохранения данных возрастает многократно.

Для выполнения атаки производится «холодная перезагрузка» (cold boot) компьютера, то есть выключение питания без использования средств операционной системы и последующее включение (например, при помощи кнопки reset на корпусе или путем выключения блока питания). После включения производится загрузка специальной небольшой операционной системы (например, с USB-диска) и сохранения текущего состояния оперативной памяти в файл. Альтернативный путь выполнения атаки заключается в изъятии модулей памяти из компьютера жертвы и их установка в другой компьютер для считывания данных с них. Полученная информация затем анализируется на предмет наличия в ней ключей шифрования или иной ценной информации. Существуют специальные программы для автоматического поиска.

Специалисты компании F-Secure еще в 2018 году продемонстрировали, как можно получить доступ к ключам шифрования ноутбука, отправленного в спящий режим.

Спящий режим – это энергосберегающий режим, который переводит компьютер в состояние ожидания. На всех без исключения ноутбуках с Windows по умолчанию при закрытии крышки система переходит в спящий режим. В нем вся работа сохранится, а энергия будет использоваться для поддержания компьютера во включенном состоянии. Другими словами, потребление энергии уменьшится за счет отключения периферийных устройств – портов, дисплея, – а вот оперативная память не будет обесточена, и в ней сохранятся все данные.

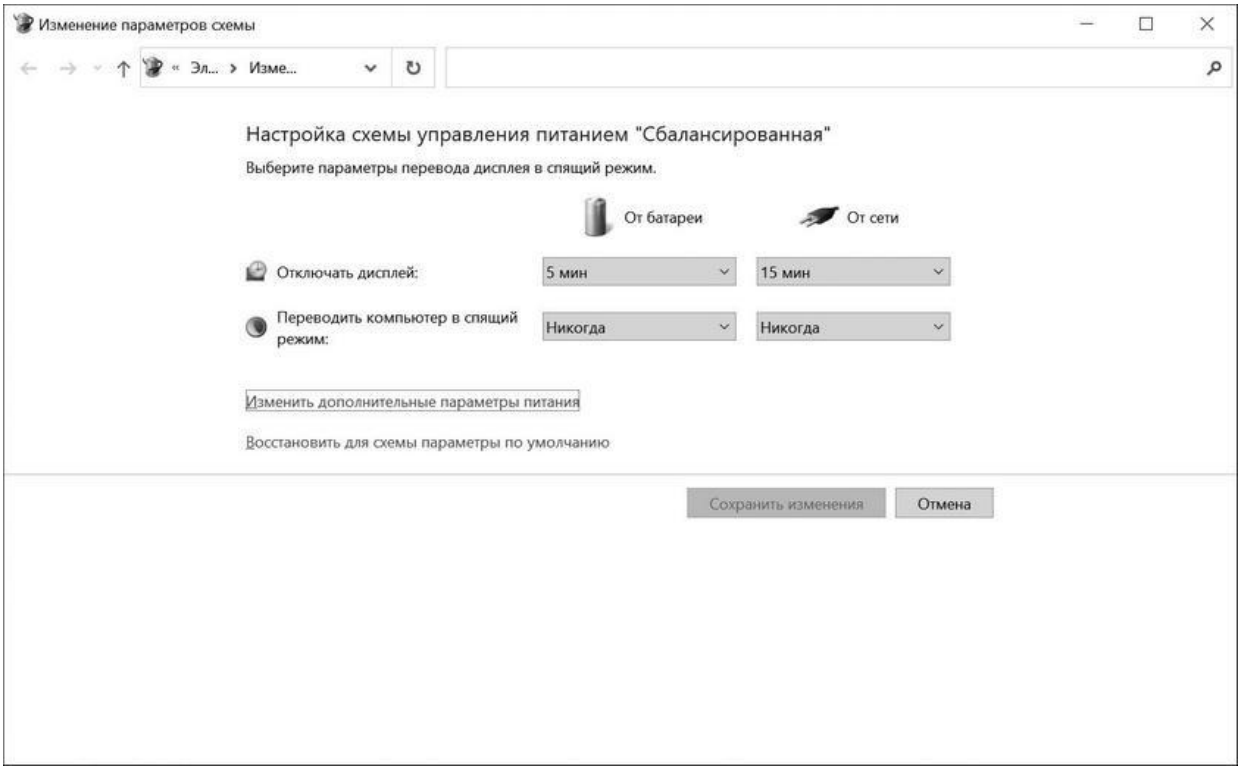
Так вот, специалисты финской компании по кибербезопасности продемонстрировали в видеоролике, как, имея физический доступ к ноутбуку, отправленному в спящий режим, можно получить ключи шифрования. Для этого атакующий:

1. Открывает нижнюю крышку ноутбука и сбрасывает настройки BIOS. Это позволит обойти установленный пароль на BIOS и выбрать источник загрузки – USB-флешку.
2. Вставляет загрузочную USB-флешку с заранее подготовленным программным обеспечением для поиска ключей шифрования в памяти.
3. Замораживает модули памяти баллончиком-фризером (обычный баллончик с охладителем, который вы можете купить на Яндекс. Маркете, способен опустить температуру поверхности, на которую производится распыление, до –45° и ниже).
4. Отправляет компьютер в перезагрузку.
5. Компьютер загружается с USB-флешки. Специальная программа находит ключи шифрования в памяти.

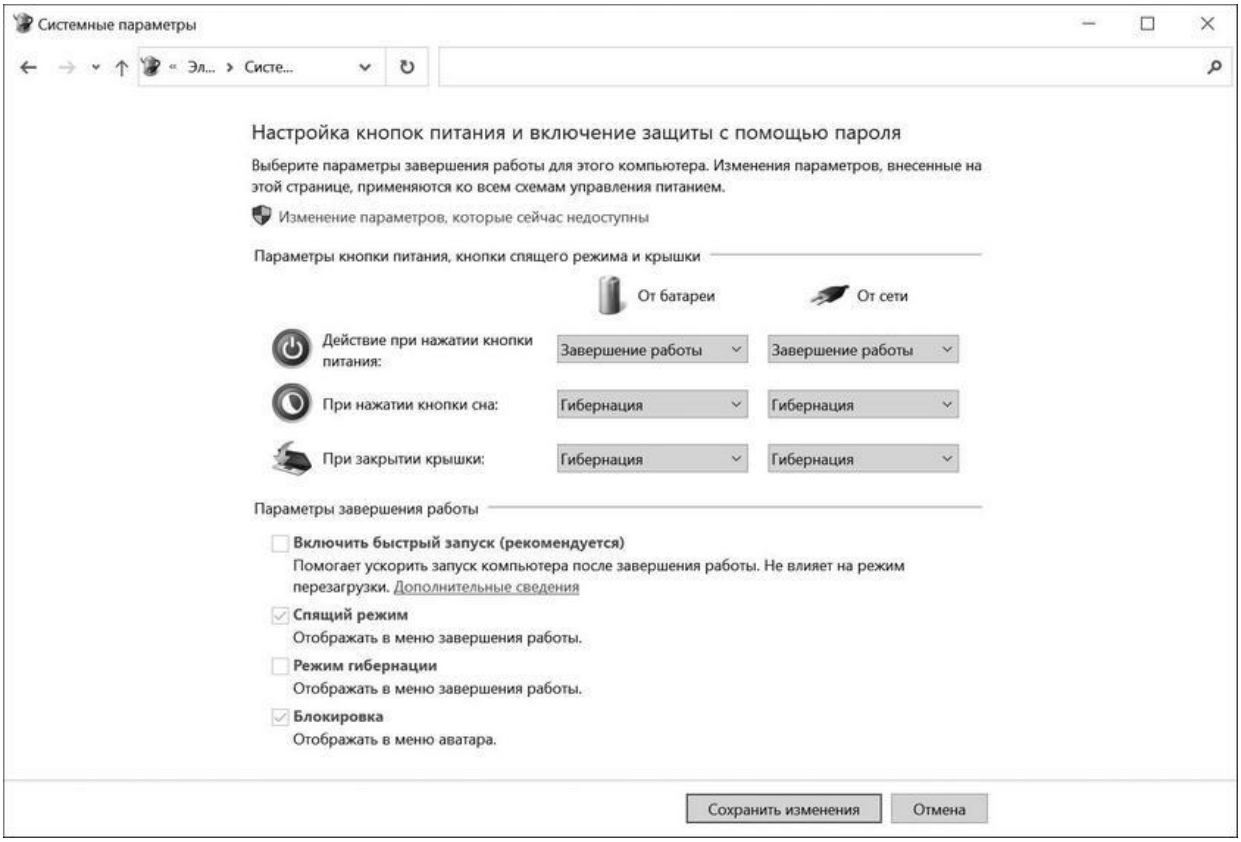
Я, конечно, не слышал, чтобы кто-то из спецслужб применял подобного рода атаку во время задержания преступников. Но исключать то, что западные спецслужбы (в частности, американские) на это способны, нельзя. Насчет наших МВД и ФСБ я сильно сомневаюсь. Наши скорее берут на испуг – и человек сам называет пароли от зашифрованных дисков. От меня, например, следователь очень хотел получить пароль к VeraCrypt. К счастью, я ему не поверил. И правильно сделал.

Если вы шифруете полностью системный диск, то я рекомендую отключить спящий режим вообще и отправлять компьютер в гибернацию[53], когда вы отходите от него более чем на несколько минут. После гибернации достаточно подождать несколько секунд – и данные в оперативной памяти при комнатной температуре уже невозможно будет восстановить.

Откройте «Электропитание»: один из способов – в строке поиска или в меню «Выполнить» (выполнить вызывается клавишами Win+R) введите команду powercfg.cpl и нажмите клавишу Enter. С правой стороны от названия схемы, которую вы хотите изменить, нажмите на «Настройка схемы электропитания». Изменять настройки нужно у активной схемы электропитания.



Если вы пользуетесь ноутбуком, то поменяйте действие на закрытие крышки – гибернация. Для этого нажимаете те же клавиши Win+R на клавиатуре, вводите powercfg.cpl, нажимаете Enter. Слева в меню выбираете «Действие при закрытии крышки».



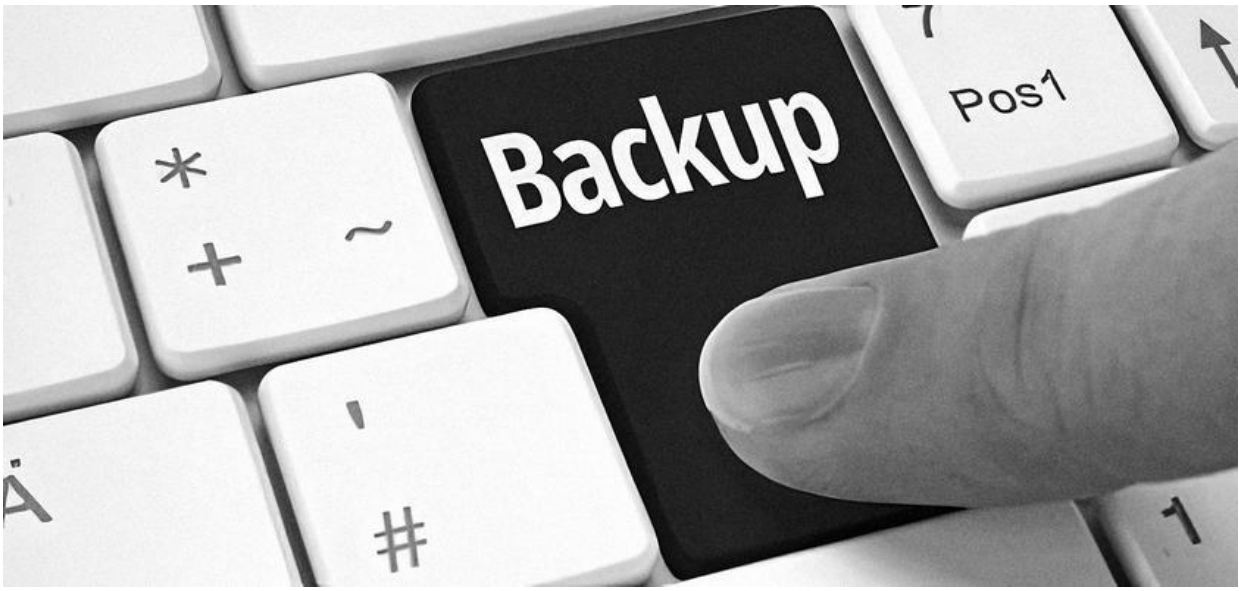
В пунктах «При нажатии кнопки сна», «При закрытии крышки» ставим «Гибернация». В пункте «Действие при нажатии кнопки питания» ставим «Завершение работы».

Настоятельно рекомендую при использовании шифрования всего системного диска закрывать крышку ноутбука или переводить компьютер в режим гибернации вручную, если вы далеко отходите от него, а также делать то же самое на ночь. Если к вам вдруг заявятся «оборотни в погонах», они, скорее всего, придут рано утром, чтобы застать вас врасплох.

Бекапы

Резервное копирование (англ. backup copy) – процесс создания копии данных на носителе (жестком диске, дискете и т. д.), предназначенном для восстановления данных в оригинальном или новом месте их расположения в случае их повреждения или разрушения.

Ситуации бывают разные: у вас может сломаться компьютер, его могут украсть, к вам домой может заявиться спецназ, и у вас изымут не только компьютер, но и все флешки и диски. Во всех этих случаях вы теряете свой компьютер и данные на нем.



Поэтому очень важно периодически делать бекапы. Хранить бекапы я рекомендую в разных местах:

1. Криптованный той же VeraCrypt внешний диск. Учтите, что если вы будете хранить такой диск в своем рабочем кабинете, в случае визита нежданных гостей из МВД или ФСБ такой диск улетит вместе с вашим рабочим компьютером.

2. Заливайте бекапы в виде одного большого зашифрованного архива в облачные хранилища. Выбор хранилищ я оставляю за вами. Достаточно ввести в Google запрос online web storage и подобрать подходящее. Многие имеют подписку Lifetime – когда вы платите один

раз и пользуетесь пожизненно. Я рекомендую два хранилища на всякий случай, вдруг что-то произойдет (бывает же, что сгорают целые дата-центры).

Например, у меня написан CMD-файл[54] для создания архивных копий всех нужных мне директорий. Выглядит он примерно так:

rar a -inul «%1\Desktop.rar» «C: \Users\Dmitry\Desktop»

rar a -inul «%1\Documents.rar» «C: \Users\Dmitry\Documents»

rar a -inul «%1\Downloads.rar» «C: \Users\Dmitry\Downloads»

%1 – это параметр «имя директории, куда складывать архивы», который передается скрипту при запуске (путь до rar должен быть прописан в глобальной переменной Path). Например:

backup 40–09.12.2022

После чего папка отправляется на диск, шифруется WinRar’ом в режиме Store и загружается на два облачных хранилища.

Моя привычка делать бекапы после дела о DDoS-атаке «Аэрофлота» помогла мне при последнем визите «правоохранителей». А привычка всё шифровать спасла мои финансовые активы (в том числе крипто).

VPN

VPN (*англ.* virtual private network – «виртуальная частная сеть») – технология, позволяющая создать безопасное подключение пользователя к сети, организованной между несколькими компьютерами. Используется в том числе для обхода ограничений, а также помогает сохранять конфиденциальность в сети.

Например, VPN может использоваться для доступа к сети вашей компании. Подключившись, вы получаете доступ ко всем внутренним ресурсам, при этом сами данные, которые идут от вас до вашей корпоративной сети по обычным протоколам TCP/IP, будут зашифрованы.

Также очень часто VPN используют для подключения к удаленному серверу, который будет для вашего компьютера точкой выхода в интернет, а весь трафик до этого сервера будет шифроваться. Именно это применение нам и нужно.

Например, в 2010 году мой интернет-канал поставили «на прослушку» (СОРМ[55]) доблестные сотрудники ФСБ. Мы с братом тогда занимались продажей индийских дженериков (аналоги виагры, циалиса и других таблеток) в интернете. Тогда мы работали с партнерской программой RX-Promotion. Партнерские программы в интернете работают по схеме распределения прибыли: вы приводите покупателей в магазины, которые предоставляет спонсор (партнерская программа). И с каждой продажи вы получаете часть прибыли. Приводили мы покупателей через спам-рассылки. Всё это я рассказывал в книге «Я – хакер! Хроника потерянного поколения».

Мы были молодые, неопытные, VPN’ом не пользовались. RX-Promotion работала по протоколу HTTP (данные передаются без шифрования, в отличие от HTTPS). Для того чтобы забрать свои комиссионные, нужно было просто заказать деньги из личного кабинета RX-Promo. Еще раз повторю: пароли на вход в нее передавались открытым текстом.

Вот кто-то после СОРМа за нас и заказал. Я, конечно, подозреваю, кто именно. Но не могу показать пальцем, а то еще расценят как клевету. Но, наверное, это те, кто позже получил по 20 лет за государственную измену.

Так что важность шифровать данные, например, до сервера в Германии есть. Все-таки в Европе, чтобы получить разрешение на съем данных с канала, нужно предоставить веские доказательства в суде. Не как у нас, когда решения суда потом штампуются задним числом. Особенно на фоне всяких «законов Яровой». Напомню, что закон Яровой заставляет всех операторов связи (интернета в том числе) хранить ваши звонки, СМС, исходящий трафик. Хоть закон и пропихивался под громкие антитеррористические лозунги, но я не верю в нашу правоохранительную систему. Оба моих столкновения с ней показывали мне только личную заинтересованность конкретных лиц. И это очень плохо.

Итак, я теперь пользуюсь OpenVPN – проектом некоммерческим, с открытым исходным кодом. Информация о том, как настроить OpenVPN-сервер, выходит за рамки этой книги, да и в интернете много материалов по этой теме. Вы, конечно, можете воспользоваться платными сервисами, но помните:

• Крайне бесполезное ведомство Роскомнадзор периодически любит блокировать IP-адреса таких сервисов.

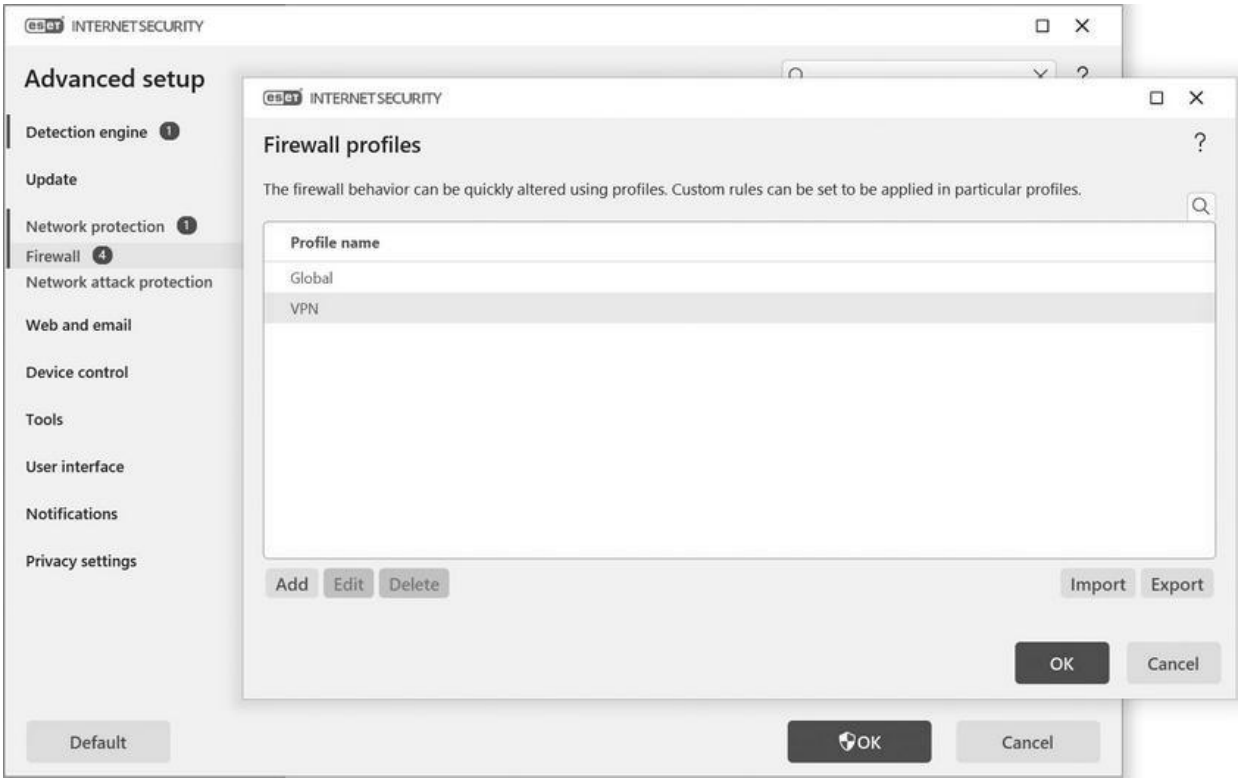
• Нельзя быть на 100 % уверенным, что ваш трафик не будет мониториться в случае чего.

• Исключите использование VPN-сервисов, принадлежащих компаниям с русскими корнями. Особенно в свете предыдущего пункта.

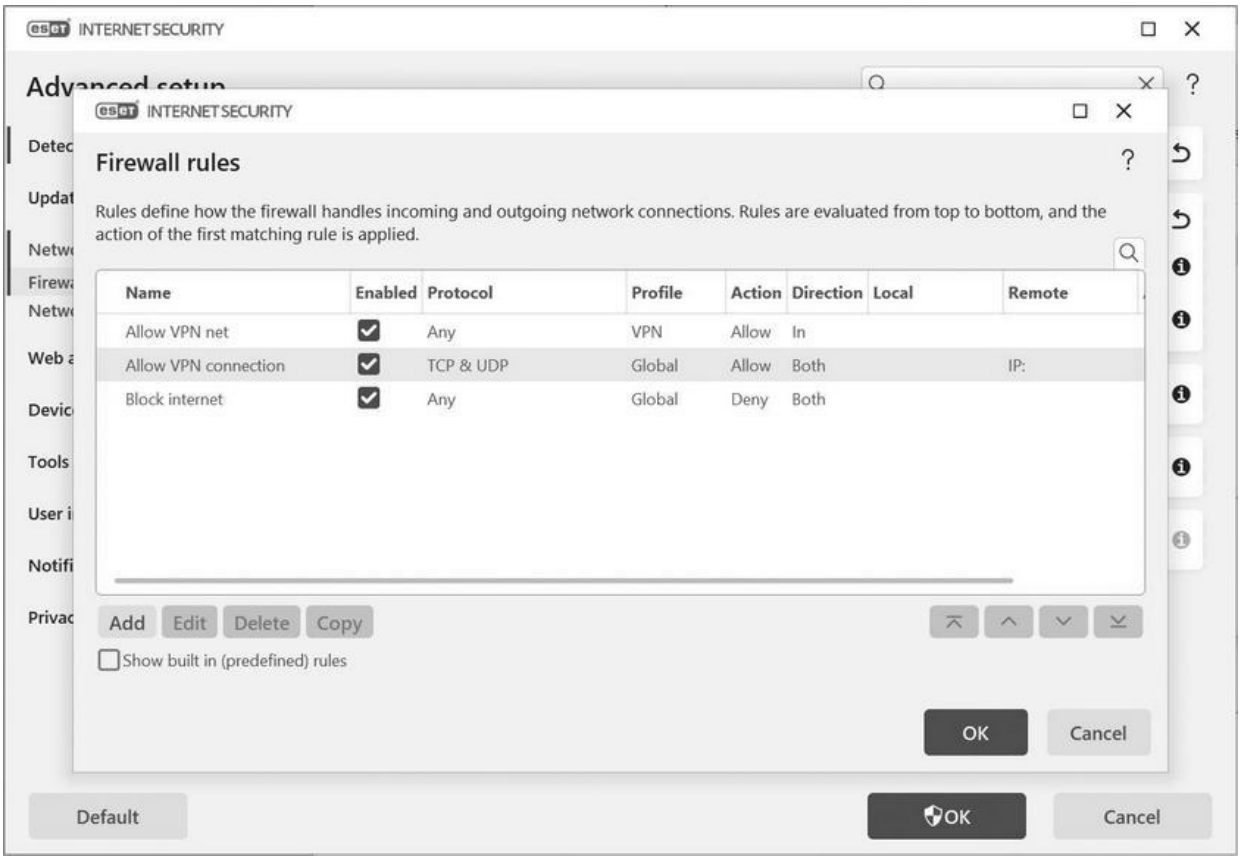
Файервол

Очень полезно настроить файервол на блокирование интернета без VPN: мало ли, у вас разорвется соединение. Правда, не все файерволы это умеют делать. Точно умеет делать ESET. Для этого нужно:

1. В Advanced Settings создать два профайла – Global и VPN. По умолчанию поставить профиль Global, а для TAP адаптеров OpenVPN (там же, в настройках) задать профиль VPN.



2. Дальше создаете 3 правила в разделе Rules. Одна правило для профиля Global – блокировать весь интернет; следующее правило – разрешить подключение (TCP или UDP) к IP-адресу VPN-сервера; и последнее, третье правило – разрешить все протоколы на профиле VPN.



В общем-то, логика простая: как только VPN подключается, весь интернет идет через профиль VPN, отключается через Global, который его блокирует.

На других антивирусах, я, конечно, пробовал не всё, так настроить интернет у меня не получилось. Например, на том же Касперском при таких же настройках VPN-адаптер не работает.

Мессенджеры

Если вы дорожите приватностью вашей деловой переписки, помните: ни один мессенджер не безопасен. WhatsApp, Facetime, Viber читаются американскими спецслужбами, Telegram – российскими.

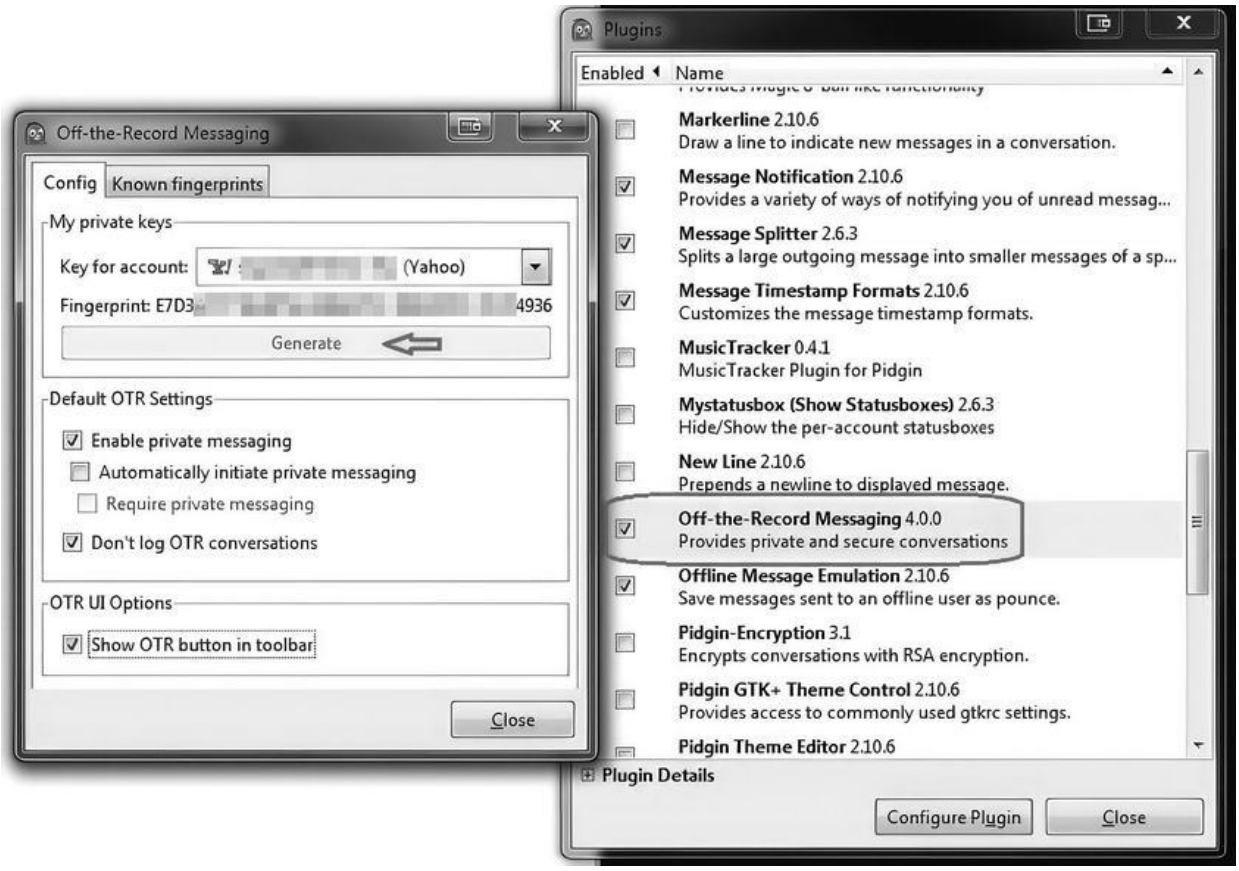
Telegram – это вообще отдельная история и целый спектакль. Напомню, что в марте 2018 года основатель Telegram Павел Дуров заявил, что мессенджер не выдаст ФСБ ключи шифрования даже под угрозой блокировки в России. По его словам, «абсолютная конфиденциальность» пользователей важнее всего. 13 апреля 2018 года Таганский суд Москвы вынес решение в пользу Роскомнадзора, тем самым позволив начать блокировку мессенджера на территории России.

Меня всегда настораживало то, что решением суда, в общем-то, всё и ограничилось. Никто не пошел заставлять Google и Apple удалить приложение Telegram из Google Play и App Store. Зато бесполезное ведомство Роскомнадзор стало рьяно что-то там блокировать, но Telegram оказался круче – он всех победил. Вдумайтесь: ведь бред же! Можете со мной не согласиться, но это был хорошо срежиссированный спектакль.

Вот вам ещё: внутренность работы Telegram описана на сайте Палача[56]. Telegram по умолчанию шифрует данные только до сервера (т. е., по сути, вся ваша переписка доступна), исходный код Telegram не такой уж и открытый – он публикуется только в части клиентских приложений пару раз в год, а часть, отвечающая за шифрование, и вообще закрыта.

Мой совет: не ведите важные переговоры с телефона. По сути, я не знаю ни одного мессенджера для телефона, который бы удовлетворял конфиденциальности переписки на все 100 %.

Мой второй совет: для защищенной переписки на компьютере используйте джаббер (Jabber) с плагином OTR, например Pidgin. И сам клиент, и плагин шифрования к нему OTR – ПО с открытым исходным кодом.



Я не встречал ни одного клиента Jabber с OTR, корректно работающего на смартфоне.

Всё написанное выше так же относится и к общению в социальных сетях. Все они читаются.

Виртуализация

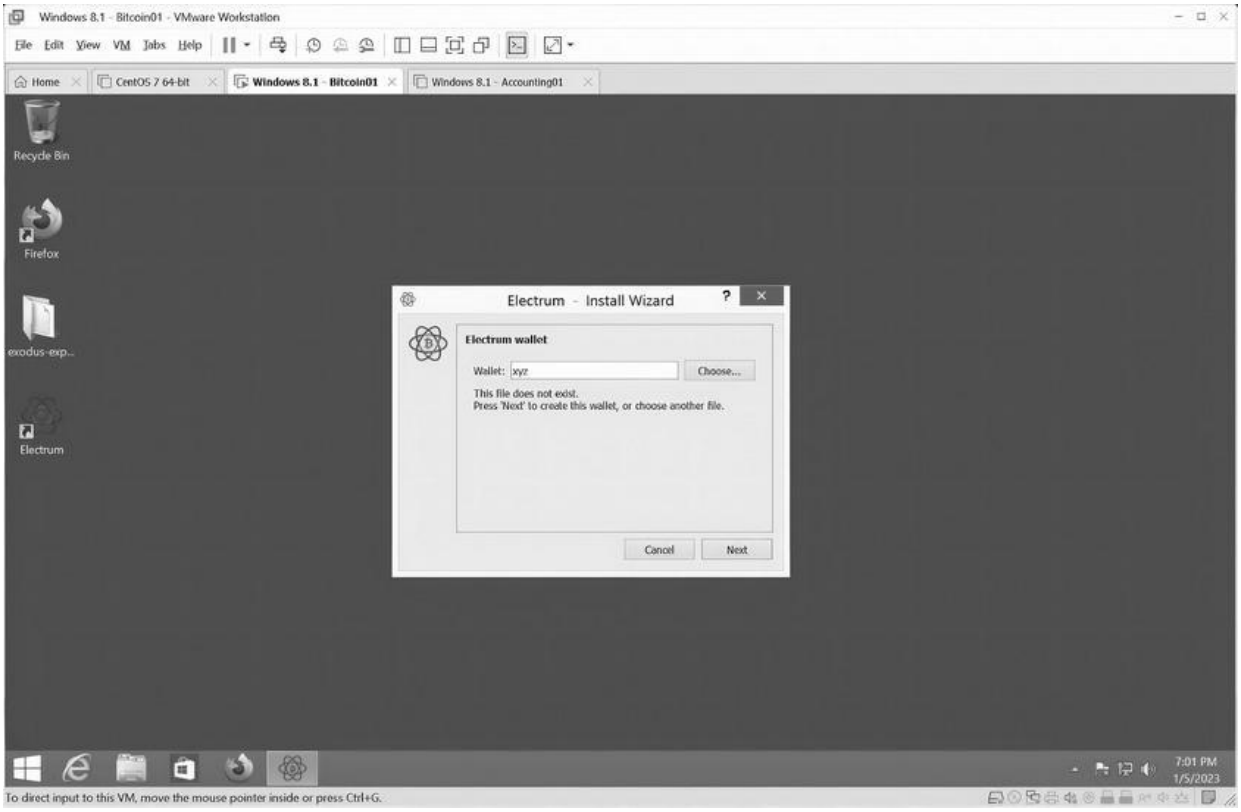
Какой бы хороший антивирус у вас ни стоял, как бы часто вы ни обновляли систему, всё равно риск заражения есть, особенно если вы активно серфите[57] по интернету. Поэтому я использую виртуализацию для изоляции наиболее ценных активов – например, криптокошельков, доступов к онлайн-банкам и т. д. Т. е. если вы подхватите какую-то заразу на основную систему, вряд ли она проникнет на виртуалку. Это еще удобно тем, что виртуалки можно бекапить и в случае чего очень быстро развернуть на другом компе, особенно если онлайн-банки требуют установки каких-либо сертификатов (чего стоит только наша Крипто-ПРО).

Из виртуализации выбирайте то, что нравится: VMWare или Virtual PC.

Смартфоны

По поводу телефонов:

Все андроиды с 6-й версии идут с шифрованием диска тоже. Проверить, закриптован ли телефон, можно через режим отладки утилитой ADB. У Google, скорее всего, есть резервный ключ, но русским его точно не дадут.



В любом случае я не рекомендую хранить на телефонах что-то важное и конфиденциальное. Конечно, вы можете установить на свой смартфон какую-нибудь операционную систему с открытым исходным кодом, найти шифровальщик. И при этом всё равно будете пользоваться всё теми же мессенджерами или вести переписку в соцсетях, так что толку не будет.

Как СССР следил за дипломатами США через печатные машинки

Вирус CIH

Заключение

Вы предприняли все действия для защиты ваших данных от кражи или злоупотребления служебным положением сотрудниками правоохранительных органов. Перечислим их снова:

1. Зашифровали системный диск, флешки, внешние накопители, используя сложные длинные пароли.

2. Установили сложный пароль на вход в операционную систему.

3. Отключили спящий режим, настроили гибернацию.

4. Позаботились о периодическом создании резервных копий.

5. Настроили VPN.

6. Разнесли важные финансовые данные на изолированные виртуальные машины.

Хотите больше?

1. Никогда не оставляйте компьютер включенным без присмотра. Если ваш компьютер изымут включенным, то теоретически можно будет вытащить ключи шифрования из оперативной памяти.

2. При обысках не верьте разводам правоохранительных органов – назвать пароль, и тогда вам якобы быстрее вернут технику. Технику вам всё равно не вернут.

3. Никогда не пользуйтесь удаленным доступом к своему компьютеру с чужих рабочих станций (например, в отеле), так как на них могут стоять кейлоггеры.

4. Не используйте беспроводные клавиатуры. Помните, мы обсуждали это в начале книги. Беспроводные клавиатуры передают данные о нажатии клавиш по радиосвязи. Радиосигнал вашей клавиатуры можно перехватить. Естественно, все современные клавиатуры шифруют канал общения до компьютера, но у производителя железа есть ключи шифрования или же оставлена лазейка для спецслужб. Маловероятно, что наши спецслужбы таким образом смогут перехватить нажатия клавиш, а вот западные – более чем.

5. Не храните данные на серверах в России. За ними всегда могут прийти, доказывать свою правоту вы потом будете в судах годами. А работать вам нужно прямо сейчас.

6. Не храните бекапы, важные документы и деньги дома.

Эти правила мне помогли, учитывая, что ко мне второй раз за последние несколько лет проявили нездоровый интерес правоохранительные органы.

Если вам понравилась книга и мои рассуждения – подписывайтесь на мой Telegram-канал:

https://t.me/labart

---

notes

Примечания

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.

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.

5

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

6

Источник https://masterok.livejournal.com/8284214.html

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.

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.

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.

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

19

IP-адрес (от *англ.* Internet Protocol) – уникальный числовой идентификатор устройства в компьютерной сети, работающей по протоколу IP.

20

AVP (аббревиатура, образованная из букв названия AntiViral Toolkit Pro) – антивирус Евгения Касперского. В 2000 году был переименован в Антивирус Касперского.

21

BIOS (от *англ.* Basic Input/Output System) – это набор микропрограмм, которые позволяют произвести настройку отдельных комплектующих системного блока, а также загрузку операционной системы и прочую настройку важных параметров. Дословно BIOS можно назвать базовой системой ввода-вывода. Сами микропрограммы находятся в энергонезависимой памяти на материнской плате компьютера.

22

Windows 9x – часто используемое общее название для операционных систем Windows версий 4.x: Windows 95, Windows 98/98SE и Windows Me от корпорации Microsoft. Поскольку архитектура этих систем весьма схожа, термин Windows 9x зачастую используется для обозначения их всех (например, при сравнении этих систем с системами линии Windows NT).

23

Windows NT (в просторечии просто NT) – линейка операционных систем (ОС) производства корпорации Microsoft и название первых версий ОС. Windows NT была разработана после прекращения сотрудничества Microsoft и IBM над OS/2, развивалась отдельно от других ОС семейства Windows (Windows 3.x и Windows 9x). В отличие от Windows 3.x и Windows 9x, Windows NT позиционировалась как надёжное решение для рабочих станций (Windows NT Workstation) и серверов (Windows NT Server). Windows NT дала начало семейству операционных систем, в которое входят: собственно Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8, Windows 10.

24

Дискета, гибкий магнитный диск (ГМД; *англ*. floppy disk, англ. diskette) – сменный носитель информации, используемый для многократной записи и хранения данных. Представляет собой гибкий пластиковый диск, покрытый ферромагнитным слоем и помещённый в защитный корпус из пластика. Считывание или запись данных с дискет производится посредством специального устройства – дисковода; в отечественной индустрии также использовался термин «накопитель (на) гибких магнитных дисках» (НГМД).

Дискеты имели массовое распространение с 1970-х и до начала 2000-х годов, придя на смену магнитным лентам и перфокартам. В конце XX века дискеты начали уступать более ёмким оптическим дискам CD-R и CD-RW, а в XXI веке – и более удобным флеш-накопителям.

25

VBScript (VBS, развернуто Microsoft Visual Basic Script Edition, иногда Visual Basic Script) – язык сценариев, созданный компанией Microsoft на основе языка Visual Basic, предназначенный для применения в приложениях, использующих технологию Active Scripting.

26

Сэр Тимоти Джон Бе́рнерс-Ли (*англ.* Sir Timothy John «Tim» Berners-Lee; род. 8 июня 1955 года, Лондон) – создатель URI, URL, HTTP, HTML и Всемирной паутины (совместно с Робертом Кайо) и действующий глава Консорциума Всемирной паутины. Автор концепции семантической паутины, множества других разработок в области информационных технологий.

27

BSD (*англ.* Berkeley Software Distribution) – система распространения программного обеспечения в исходных кодах, созданная для обмена опытом между учебными заведениями. Особенностью пакетов ПО BSD была специальная лицензия BSD, которую кратко можно охарактеризовать так: весь исходный код – собственность BSD, все правки – собственность их авторов.

В данный момент термин BSD чаще всего употребляется как синоним BSD-UNIX – общего названия вариантов UNIX, восходящих к дистрибутивам университета Беркли.

Упрощенное генеалогическое дерево UNIX и его клонов

К семейству BSD относятся: NetBSD, FreeBSD, OpenBSD, ClosedBSD, MirBSD, DragonFly BSD, PC-BSD, GhostBSD, DesktopBSD, SunOS, TrueBSD, Frenzy, Ultrix и частично XNU (ядро macOS, IOS, tvOS, watchOS, CarPlay, Darwin).

28

Хостинг (от *англ.* hosting) – услуга по размещению сайта или иного контента на сервере, обычно имеющем непрерывный доступ к Сети.

29

Фрейм (от *англ.* Frame) – это самостоятельный документ, который отображается в отдельном окне браузера и представляет собой полностью законченную HTML-страницу. Простыми словами, фрейм – разделитель браузерных окон на отдельные области.

30

HTML (от *англ.* HyperText Markup Language – «язык гипертекстовой разметки») – стандартизированный язык гипертекстовой разметки документов для просмотра веб-страниц в браузере. Веб-браузеры получают HTML документ от сервера по протоколам HTTP/HTTPS или открывают с локального диска, далее интерпретируют код в интерфейс, который будет отображаться на экране монитора.

31

URL – это уникальный адрес веб ресурса (сайта), который зарегистрирован в единой схеме адресации известной как «Uniform Resource Locator» или сокращенно – URL. Простыми словами URL – это адрес сайта, включая путь к конкретной странице или контенту на ней. Все браузеры имеют строку для ввода адреса, где отображается просматриваемая в данный момент страница.

32

ARPANET (Advanced Research Projects Agency Network) – компьютерная сеть, созданная в 1969 году в США Агентством Министерства обороны США по перспективным исследованиям (DARPA) и явившаяся прототипом сети Интернет. 1 января 1983 года она стала первой в мире сетью, перешедшей на маршрутизацию пакетов данных. В качестве маршрутизируемого протокола использовался IP, который и по сей день является основным протоколом передачи данных в сети Интернет. ARPANET прекратила своё существование в июне 1990 года.

33

Rootkit – программа, которая скрывает от антивирусов собственные вредоносные действия, либо маскирует работу другого вредоносного ПО – например, трояна. Руткитом скрываются, в частности, системные процессы, файлы, драйверы, записи в реестре и сетевые соединения, не позволяя антивирусам идентифицировать следы присутствия этой зловредной программы.

34

Роутер (маршрутизатор) – это устройство, которое распределяет интернет между подключенными к нему устройствами. По сетевому кабелю (компьютеры, телевизоры и т. д.), или по Wi-Fi (смартфоны, планшеты, ноутбуки).

35

DNS (Domain Name System) – это система, преобразующая человекочитаемые доменные имена в IP-адреса, понимаемые машиной.

36

Скам (от *англ.* scam – «афера, мошенничество») – мошенничество в интернете.

37

Миллениалы, или **Поколение Y** (поколение «игрек»; другие названия: поколение Миллениума, поколение «некст», «сетевое» поколение, милленитs, эхо-бумеры) – поколение людей, родившихся примерно с 1981 по 1996 год (к дате начала поколения в различных источниках причисляют 1980–1987 годы, к дате конца – 1994–2005 годы), встретивших новое тысячелетие в юном возрасте, характеризующееся прежде всего глубокой вовлечённостью в цифровые технологии.

38

Поколение Z (*англ.* Generation Z) (также известное как зумеры, хоумлендеры англ. Homelanders, Homeland Generation, Zoomers или New Silent Generation) – термин, применяемый в мире для поколения людей, родившихся примерно с 1997 по 2012 год.

39

Юзнет (*англ*. usenet – сокр. от англ. user network) – компьютерная сеть, используемая для общения и публикации файлов. Usenet состоит из новостных групп, в которые пользователи могут посылать сообщения. Usenet оказал большое влияние на развитие современной веб-культуры, дав начало таким широко известным понятиям, как «ник», «смайл», «подпись», «модератор», «троллинг», «флуд», «флейм», «бан», «FAQ» и «спам».

40

MySpace (с *англ*. – «моё пространство») – международная социальная сеть, которая начала работать в августе 2003 года. Это сайт сетевых сообществ и блог-платформа, в которой представлена возможность создания сообществ по интересам, персональных профилей, ведения блогов, размещения фото- и видеоконтента, а также возможность прослушивания аудиотреков популярных исполнителей. Штаб-квартира расположена в Беверли-Хиллз (Калифорния, США).

41

VoIP (Voice over Internet Protocol) или IP-телефония – это голосовая связь через интернет (в отличии от традиционной телефонной связи, которая происходит через телефонные линии или мобильную GSM/3G сеть).

На данный момент основным назначением IP-телефонии являются дешевые или бесплатные междугородние и международные звонки. Для совершения этих звонков вам нужно воспользоваться услугами одного из провайдеров IP-телефонии и вы сможете звонить с компьютера, IP-телефона или обычного телефона.

42

Куки (*англ*. cookie, *букв*. – «печенье») – небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя. Веб-клиент (обычно веб-браузер) всякий раз при попытке открыть страницу соответствующего сайта пересылает этот фрагмент данных веб-серверу в составе HTTP-запроса. Применяется для сохранения данных на стороне пользователя, на практике обычно используется для: аутентификации пользователя; хранения персональных предпочтений и настроек пользователя; отслеживания состояния сеанса доступа пользователя; сведения статистики о пользователях.

43

Маркетплейс (торговая площадка) – это онлайн-платформа для продажи и покупки товаров и услуг через интернет, простыми словами продавцы размещают свои товары, покупатели выбирают лучшие варианты по ценам, характеристикам и другим параметрам.

44

Ли́нус Бенедикт То́рвальдс или **Ту́рвальдс** (28 декабря 1969, Хельсинки, Финляндия) – финно-американский программист. Создатель ядра Linux и системы управления версиями Git.

45

Chargeback (возвращённый платеж) – процедура опротестования транзакции банком-эмитентом (в целях защиты прав плательщика), при которой сумма платежа безакцептно списывается с получателя (банка-эквайера) и возвращается плательщику, после чего обязанность доказательства истинности транзакции возлагается на получателя.

46

Банк-эквайер (обслуживающий банк) – кредитная организация, организующая точки приема банковских карт (терминалы, банкоматы) и осуществляющая весь комплекс финансовых операций, связанных с выполнением расчетов и платежей по банковским картам в этих точках.

47

p2p – Person To Person

48

Источник: https://lenta.ru/news/2022/09/12/hkufs/

49

Криптография – это метод защиты информации путем использования закодированных алгоритмов, хэшей и подписей.

50

TPM (Trusted Platform Module) – спецификация, описывающая криптопроцессор, в котором хранятся криптографические ключи для защиты информации, а также обобщенное наименование реализаций указанной спецификации, например, в виде «чипа TPM» или «устройства безопасности TPM».

51

Скринсейвер (*англ.* Screensaver; заставка, хранитель экрана) – функция или отдельная программа гашения экрана при простое компьютера (или иного устройства), призванная снизить непроизводительный износ оборудования и его отдельных частей, а иногда и энергопотребление. Заставки призваны снизить яркость изображения (в том числе погасить экран полностью) и снизить общий износ, и/или устранить статичность рабочего изображения для снижения локального износа – выгорания люминофора на статических элементах, что актуально для устройств на основе электронно-лучевой трубки и плазменных экранов.

52

Оперативная память (*англ*. Random Access Memory, RAM – память с произвольным доступом) – в большинстве случаев энергозависимая часть системы компьютерной памяти, в которой во время работы компьютера хранится выполняемый машинный код (программы), а также входные, выходные и промежуточные данные, обрабатываемые процессором. Оперативное запоминающее устройство (ОЗУ) – техническое устройство, реализующее функции оперативной памяти

53

Гибернация (*англ.* hibernation – «зимняя спячка») – энергосберегающий режим операционной системы компьютера, при котором содержимое оперативной памяти сохраняется на энергонезависимое устройство хранения данных (жесткий диск) перед выключением питания. В отличие от спящего режима, в режиме гибернации после сохранения данных оперативной памяти подача электроэнергии полностью прекращается. После включения питания компьютера содержимое памяти восстанавливается (загружается с диска в память), и пользователь сможет продолжить работу с того же места, на котором он остановился, так как все запущенные ранее программы продолжат выполняться.

54

Пакетный файл (*англ*. batch file) – текстовый файл в Windows, содержащий последовательность команд, предназначенных для исполнения командным интерпретатором. После запуска пакетного файла программа-интерпретатор (как правило, COMMAND.COM или cmd.exe) читает его строка за строкой и последовательно исполняет команды. Пакетный файл – аналог скриптовых файлов командной строки (shell script) в Unix-подобных операционных системах.

55

СОРМ (*сокр*. от Система технических средств для обеспечения функций оперативно-разыскных мероприятий) – комплекс технических средств и мер, предназначенных для проведения оперативно-разыскных мероприятий в сетях телефонной, подвижной и беспроводной связи и радиосвязи (согласно Закону «О связи» и приказу Министерства связи № 2339 от 9 августа 2000 г.).

56

https://click-or-die.ru/

57

Серфинг в интернете – просмотр страниц веб-сайтов.