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 при-

меры, 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

[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.

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.

---

[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.

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 кей-

логгер 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 злоумыш-

ленник 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.

---

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

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 на-

строен 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 дей-

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

ствия 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