Я знаю много высокомерных гиков. Они думают, что их никогда не поразят вредоносные программы, потому что они очень технически подкованы, и они никогда не позволят себе подвергнуться опасности. Они ошибаются.

Точно так же я знаю множество высокомерных пользователей компьютеров, будь то гики или нет. К ним относятся легионы пользователей Apple, которые считают, что операционная система OS X компании волшебным образом лучше, чем основная альтернатива. Среди них есть люди, которые купились на аналогичный маркетинг Microsoft о том, что Vista является самой безопасной операционной системой из когда-либо существовавших.

Такие люди верят в то, во что их заставляют верить плохие парни!

Давайте рассмотрим распространенные способы “обвести вокруг пальца”, и мы увидим, что в некоторых случаях это намного проще, чем может ожидать большинство людей.

Во-первых, получение “0wned”, как правило, может означать одно из нескольких. Это может означать, что на вашем компьютере установлено вредоносное программное обеспечение (malware — сокращение от “вредоносного программного обеспечения”). Или же это может означать, что ваши банковские реквизиты в режиме онлайн передаются постороннему человеку, независимо от того, окажется ли вредоносное ПО на вашем компьютере или нет.

Давайте начнем с заражения (установки вредоносного программного обеспечения). Одним из наиболее распространенных способов заражения вредоносным ПО является его самостоятельная установка. Вы можете перейти по ссылке в сообщении электронной почты, думая, что это законный URL, хотя это не так. Или же вы можете загрузить из Интернета приложение, которое считаете законным, хотя на самом деле это вредоносное ПО.

Существует множество методов обмана, с помощью которых можно заставить людей скачивать плохие материалы. Вы можете попытаться заставить людей думать, что они скачивают то, что на самом деле хотят скачать. Например, представьте, что 18-летние юноши ищут в Интернете видеозапись секса знаменитостей того времени. Они находят в Google сайт, который утверждает, что предоставляет его бесплатно, но для этого требуется подключаемый модуль для Windows Media Player, которого у них нет. Когда они “нажимают здесь”, чтобы получить подключаемый модуль (рис. 3.1), они в конечном итоге устанавливают вредоносное ПО. Это еще более эффективно, если при загрузке устанавливается как вредоносное ПО, так и легальный подключаемый модуль, а затем воспроизводится видео!

Существует множество популярных категорий загрузок, которые, как правило, содержат вредоносное ПО, например, скринсейверы. На всех крупных сайтах с скринсейверами есть заставки, содержащие рекламное или шпионское ПО. И если вы ищете самую крутую новую икону поп-культуры того времени, любой исполняемый файл, который вы можете скачать (например, игру), сразу же вызывает подозрения. Хорошо, если вы юзергик, вы можете подумать, что вы выше этого. Вы не скачиваете материалы, если они не от уважаемого поставщика и вы не можете ясно видеть, что их скачало множество других людей. Оцените это сами.

Тем не менее, существует множество ситуаций, когда вам может показаться, что вы загружаете одно приложение, но на самом деле вы загружаете другое, например, когда в вашей локальной сети есть злоумышленник, который запускает атаку man-in-themiddle или атакует вас с целью отравления DNS-кэша (не волнуйтесь, если вы не знаете что это за вещи; для данного обсуждения это не важно). К счастью, это редкие случаи.

Еще один способ, с помощью которого люди регулярно попадают в “безвыходное положение”, - это когда злоумышленник использует проблемы с безопасностью в их системах, особенно в программном обеспечении, поддерживающем работу в Интернете, таком как веб-браузеры. Веб-браузеры - это массивные фрагменты кода, и у них обязательно будут проблемы с безопасностью, независимо от того, насколько тщательно пользователи их просматривают (эту тему я подробно рассмотрю позже в этой книге). Но существуют веб-сайты, которые могут попытаться взломать ваш компьютер, используя проблему с безопасностью в браузере. Если вы перейдете на неправильный веб-сайт с уязвимым браузером и конфигурацией операционной системы, то, скорее всего, у вас будет установлено вредоносное ПО (“загрузка с диска”).

Браузеры - не единственные программы, которые могут быть уязвимы. Были проблемы с настольными приложениями, такими как Microsoft Word, в которых открытие вредоносного файла данных также приводит к установке вредоносного ПО. Также были обнаружены заметные бреши в системе безопасности служб Microsoft (программ, которые запускаются, даже когда пользователь не находится за компьютером; обычно они позволяют программам на других компьютерах подключаться и взаимодействовать с машиной, на которой они выполняются) и другим важным программным обеспечением сторонних производителей, когда служба находится на вашем компьютере и ожидает, пока к ней подключатся другие пользователи. Злоумышленники просто должны быть в состоянии связаться с этой службой, тогда они смогут взломать ваш компьютер без какого-либо вмешательства с вашей стороны.

Несколько технологий (таких как брандмауэры) не позволяют случайным пользователям Интернета видеть уязвимые сервисы, но есть множество других случаев, когда существует риск. Например, если ваш компьютер подключен к корпоративной сети, часто все компьютеры в корпоративной сети могут без проблем взаимодействовать друг с другом. Если злоумышленник контролирует любую из машин в этой сети, которые могут вас видеть, и на вашем компьютере запущена уязвимая служба, вы подвергаетесь риску. Однако в наши дни по умолчанию доступно лишь несколько служб, за исключением общих сетевых служб (а в Windows в прошлом с ними, безусловно, были большие проблемы).

Даже если у вас не запущен уязвимый браузер или вы не находитесь в ситуации, когда какое-либо другое программное обеспечение может быть уязвимо, вас легко обмануть с помощью вещей, которые выглядят законными, но таковыми не являются. Например, если вы случайно введете неверное доменное имя или иным образом перейдете по неправильной ссылке, вы можете получить ложное сообщение об ошибке, утверждающее, что вредоносное ПО мешает вам загрузить ссылку, и в диалоговом окне, которое выглядит так, как будто оно исходит из Windows, будет предпринята попытка установить антивирусное программное обеспечение, которое на самом деле является вредоносным ПО. это не так.

Или же вы можете получить другое поддельное всплывающее окно, которое выглядит так, будто оно исходит из Windows, и побуждает вас установить что-то, что вы можете установить, потому что, по вашему мнению, Microsoft предлагает это.

Иногда эти фальшивые сообщения от Microsoft предлагают вам различные варианты, чтобы выглядеть более респектабельно. Большинство высокомерных гиков, которых я знаю, все равно не стали бы возражать против существующего положения вещей. Они будут утверждать, что не посещают какие-либо опасные сайты, им либо не нужно программное обеспечение для обеспечения безопасности, либо они используют программное обеспечение только от проверенных поставщиков, и они используют “персональные брандмауэры”, которые предназначены для того, чтобы их компьютеры не принимали нежелательный трафик, даже если программные службы, которые они используют, заражены. Они также не ожидают, что попадутся на удочку фишинговых мошенников.

Такие люди приучили себя игнорировать электронные сообщения от eBay, если в них явно не указан их идентификатор пользователя (когда злоумышленники рассылают множеству людей поддельные сообщения с eBay, они обычно не называют индивидуальные имена пользователей eBay, потому что они их не знают). Точно так же они не загружают “открытки от друга!”, если имя друга не указано четко. Но я все еще знаю нескольких ранее высокомерных гиков, которые попались на удочку фишинговых мошенников.

Фишеры, как правило, используют эффективные методы, но иногда они меняют тактику. Например, за несколько недель до того, как я написал это, фишеры начали рассылать сообщения, в которых утверждалось, что получатель получил посылку UPS, которую невозможно доставить. Сообщение, судя по всему, пришло от UPS и содержало просьбу к получателю предоставить правильные личные данные, чтобы посылка могла быть доставлена. Поскольку это был новый метод, несколько довольно сообразительных людей стали его жертвами. Но у плохих парней в запасе есть еще несколько трюков.

Один из методов называется подводный фишинг, который, по сути, настраивает попытки фишинга на отдельные компании или даже отдельных людей. Вы можете получить электронное сообщение, которое, по-видимому, пришло от ИТ-специалистов вашей компании, с просьбой войти на веб-портал и сменить пароль, поскольку срок его действия подходит к концу. Конечно, если письмо приходит от злоумышленника, сайт будет поддельным, и целью будет захват вашего текущего пароля, а не его смена. Подводную охоту можно легко использовать для поиска отдельных лиц и сетей друзей.

Например, предположим, что вы хотите отправить мне сообщение о целенаправленной попытке фишинга. Во-первых, вы можете легко получить несколько моих адресов электронной почты, просто введя мое имя. Точно так же, если вы окажетесь плохим парнем, у которого есть мой адрес электронной почты, потому что вы купили его в каком-то списке, вы можете легко найти мое имя с помощью небольшого поиска в Интернете (который может быть автоматизирован).

Допустим, вы хотите обманом заставить меня загрузить какую-нибудь вредоносную программу и считаете, что было бы неплохо замаскировать ее под открытку от одного из моих друзей. Для этого мы можем легко использовать Facebook. Сначала давайте введем в поиск мое имя.

Это здорово, результат только один. Давайте посмотрим на моих друзей. Для этого я создал временную учетную запись без друзей, которую удалил после этого эксперимента.

Отлично, теперь у вас есть пара сотен имен, от которых вы могли бы получить открытку. Если вы утверждаете, что живете в Бостоне, штат Массачусетс, то теперь вы можете просмотреть весь мой профиль и найти всевозможные личные данные, чтобы понять, как на меня ориентироваться, - от сообщений о моем статусе до моей трудовой биографии.

Все это настройки Facebook по умолчанию. Вы можете скрыть свой список друзей от посторонних, но для этого вам придется приложить немало усилий, а это делают немногие. Злоумышленники могут легко удалить такую информацию автоматически. В то время как легальные сайты, такие как Facebook, пытаются обнаружить людей, которые выкладывают слишком много информации, злоумышленники могут получать информацию по крупицам за раз, оставаясь при этом незамеченными, и затем отправлять гораздо меньше целевых электронных сообщений, что будет иметь гораздо больше шансов на успех, чем массовая кампания по электронной почте.

Возможно, некоторые из моих наиболее высокомерных знакомых-ботаников сказали бы мне,

что они не открыли бы открытку, даже если бы она была от их матерей или подруг (те, с кем вы встречаетесь, обычно приходят к людям из того же города). Они могут чувствовать себя невосприимчивыми ко всему, что они прочитали до сих пор. Никакая социальная инженерия их не одурачит! И, как мы уже говорили, они никогда бы не зашли на рискованные сайты. Но стали бы они заходить на MLB.com (сайт Высшей бейсбольной лиги), The Economist или сайты для гиков, такие как Slashdot?

Все эти сайты хорошо зарекомендовали себя и пользуются большим уважением, однако именно они могут стать местом, где вы в конечном итоге можете заразиться. Злоумышленники покупают законную рекламу на крупных сайтах, а затем время от времени размещают какие-нибудь вредоносные материалы, например рекламу поддельного видео-продукта, который оказывается шпионским ПО. Или это может быть реклама, которая выглядит законной, но пытается использовать ваш браузер. И это может произойти на любом сайте, который размещает рекламу в крупной сети, например CNN.com. Конечно, рекламные сети стараются не допускать такого рода материалов, но это часто бывает непросто, особенно если учесть, что реклама часто состоит из кода, а не просто статичных картинок. Многие рекламные объявления разрабатываются на ActionScript, языке программирования Adobe.

Если вы не считаете, что уязвимы для рекламы на вашем любимом веб-сайте, использующем эксплойт браузера, то вы очень самонадеянный компьютерщик. Я подозреваю, что вы относитесь к одной из этих двух категорий:

• Вы думаете, что вас никогда не обманут, и изо всех сил стараетесь использовать самые последние версии своего браузера.

• Вы думаете, что находитесь в безопасности, потому что пользуетесь системой Apple или Linux, или, может быть, таким необычным браузером, как Opera, или вы думаете, что делаете что-то еще достаточно необычное, чтобы обезопасить себя. Если вы относитесь к первой категории и действительно старательно относитесь к этому, то единственное, что вас по-настоящему беспокоит, - это когда злоумышленник начинает использовать эксплойт “нулевого дня” против вашего браузера, что означает (более или менее), что поставщик браузера не устранил проблему до того, как эксплойт начал выходить из-под контроля. К счастью, такое случается не так уж часто.

Если вы относитесь ко второй категории, просто осознайте, что вы становитесь экономически непривлекательной мишенью для злоумышленников, а это означает, что им гораздо дешевле найти жертв в другом месте. Это не всегда может быть правдой. Пользователям Apple, в частности, следует беспокоиться, о чем я вскоре расскажу.