В этой главе мы рассмотрим, что побуждает плохих парней взламывать компьютеры и что происходит у них в голове. Раньше считалось, что люди создают вирусы и червей по глупым причинам: возможно, просто для того, чтобы доказать себе или своим друзьям, что они умные, или, возможно, потому, что хотят причинить вред. Таких людей в мире не так уж много.

Нет, большинство людей на темной стороне силы находятся там по одной причине: легкие деньги!

Допустим, вы плохой парень и устанавливаете на чей-то компьютер некачественное программное обеспечение. Какие действия вы могли бы предпринять, чтобы заработать деньги? Вот краткий список, который ни в коем случае не является исчерпывающим:

• Вы могли бы собирать номера кредитных карт и связанные с ними данные (например, код подтверждения CVV). Вы могли бы собирать данные по мере того, как пользователи вводят их на сайтах электронной коммерции, а затем продавать их другим злоумышленникам. В конце концов, кто-то может использовать информацию о кредитной карте в течение дня или, возможно, просто для совершения разовой транзакции в надежде, что владелец кредитной карты никогда не заметит мошенничества.

• Вы можете подождать, пока люди воспользуются сайтами онлайн-банкинга, а затем узнать важную информацию об учетной записи (например, имя пользователя, пароль, номер счета и т.д.) или даже перехватить подключение, когда машина будет бездействовать, чтобы вы могли перемещать деньги.

• Вы можете собирать любую информацию об учетной записи. Например, если вы собираете действительные учетные данные для доступа к крупным корпоративным сетям, вы можете заподозрить, что существует черный рынок для подобных вещей. Даже на обычных старых компьютерах вы могли бы продать информацию об учетной записи людям, которые захотят заняться другими видами мошенничества.

• Вы могли бы подождать, пока люди купят товар у онлайн-продавца, например Amazon.com, и обмануть онлайн-продавца, заставив его думать, что вы направили пользователя на Amazon для покупки определенного товара, хотя на самом деле пользователь пришел туда сам. Эта атака вообще не наносит вреда пользователю, а только продавцу, поскольку в конечном итоге она приводит к выплате комиссионных тому, кто их не заслуживает.

• Вы можете рассылать спам с зараженного компьютера. Вы можете удивиться, зачем кому-то понадобилось это делать. Если злоумышленники рассылают спам только из нескольких мест, найти и пресечь источники легко, но если спам рассылается через миллионы компьютеров, многие из которых занимаются в основном законными делами, это гораздо более крепкий орешек.

• Вы можете показывать пользователям рекламу, которую они в противном случае не получили бы. Это модель многих рекламных компаний. Они часто продают дешевую рекламу законным компаниям. Законные компании не знают, как компании заставляют пользователей нажимать на рекламу, они просто заботятся о том, чтобы клики происходили.

• Вы можете обманным путем генерировать “клики” по объявлениям, чтобы получать доход для своего собственного сайта, который ничего не делает, кроме показа тонны рекламы. Вы размещаете свою большую веб-страницу с рекламой, на зараженных компьютерах нажимаете на объявления на этих страницах (зараженному пользователю даже не нужно просматривать страницы), и рекламная сеть выплачивает вам реферальное вознаграждение за клик. Или, если

у вашего бизнеса есть конкурент, вы можете перейти по ссылкам всех своих конкурентов, чтобы израсходовать их рекламный бюджет и лишить их “реального” трафика (большинство рекламных кампаний прекращаются, когда бюджет исчерпан).

• Аналогичным образом вы могли бы заменить всю рекламу, которая должна была показываться пользователю, рекламой, показываемой с вашей домашней страницы. Это полностью имитирует “реальный” трафик, что еще больше затрудняет обнаружение мошенничества рекламными сетями, такими как Google.

• Если компьютер пользователя подключен к активному модему, вы можете набрать номер премиум-класса 1-900 (например, горячую линию экстрасенса) и заставить модем набрать его. В этом случае вы сможете воспользоваться временем телефонного разговора, но счет за звонок будет выставлен пользователю. Или, если у вас есть номер 1-900, вы получите все деньги. Как правило, вы бы хотели, чтобы звонки были короткими и немногочисленными, чтобы люди ничего не заметили или не жаловались, если заметят.

• Если у вас под контролем большое количество зараженных компьютеров, вы можете брать деньги у других людей, чтобы попытаться “отключить” популярные веб-сайты, используя так называемую распределенную атаку типа "отказ в обслуживании" (DDOS). Вероятно, рынок сбыта для этого невелик, но такого рода атаки типа "отказ в обслуживании" (DOS) случаются время от времени. Вероятно, чаще всего их совершают плохие парни с политическими целями или просто люди, желающие навредить.

• Вы можете использовать зараженный компьютер для атаки на другой компьютер. Вы можете взломать другие компьютеры в своей сети и использовать любой из вышеупомянутых методов, чтобы заработать деньги на этих новых зараженных компьютерах.

• У вас могут храниться важные данные для получения выкупа (например, личные фотографии, локально сохраненные сообщения электронной почты, музыкальные файлы и видео). Обычно это делается путем шифрования файлов на компьютере, чтобы жертва не могла получить к ним доступ, пока не получит ключ для расшифровки.

Чем больше компьютеров у злоумышленника, тем лучше он зарабатывает. Чем больше компьютеров, тем легче рассылать спам и продолжать генерировать мошеннические клики, если распределить работу по максимальному количеству компьютеров, чтобы ни одна машина не выполняла слишком много работы.

Многие плохие парни в конечном итоге устанавливают программное обеспечение общего назначения, которым они могут управлять удаленно и делать все, что захотят. Индустрия называет такое программное обеспечение ботнетическим программным обеспечением (бот - это сокращенная форма слова “робот”, указывающая на то, что зараженный компьютер, вероятно, запустит автоматизированное программное обеспечение для выполнения гнусных приказов злоумышленника).

Очевидно, что в экономических интересах злоумышленника, чтобы жертва не знала о том, что его компьютер захвачен. Злоумышленник может многое сделать, чтобы использовать компьютер жертвы для зарабатывания денег, при этом жертва не должна знать, что на нем находится злоумышленник. Чем менее назойлив плохой парень, тем лучше для него. Итак, в наше время, когда компьютер заражен, скорее всего, злоумышленник просто хочет медленно и незаметно забрать деньги у владельца машины, потому что он не хочет, чтобы его выгнали из машины! Если злоумышленник предпримет что-то экстремальное, например, захватит файлы в заложники (так называемое программное обеспечение-вымогатель), он может никогда не

получить деньги, а если и вернет файлы, то после этого компьютер, вероятно, будет очищен, что затруднит дальнейшую монетизацию машины. Поэтому программы-вымогатели не слишком популярны.

Я бы предположил, что злоумышленники будут прибегать к таким мерам в качестве последнего средства — если их основная вредоносная программа обнаружена и удалена, некоторые вторичные программы-вымогатели могут в качестве последнего средства захватить данные компьютера.

В общем, быть плохим парнем в Интернете выгодно! Это намного проще, чем совершать традиционные преступления, по нескольким основным причинам:

• Плохим парням не обязательно находиться физически рядом со своими жертвами, чтобы совершать преступления против них. На самом деле, многие компьютерные преступления совершаются в таких странах, как Россия и Китай, где законы о компьютерных преступлениях и их правоприменение слабы. Если преступление выходит за рамки юрисдикции, найти и наказать плохих парней становится намного сложнее.

• Гораздо проще не оставлять никаких реальных улик. Хотя у компьютеров есть адреса, по которым их можно в определенной степени отследить, есть много способов, которыми злоумышленник может замести следы. Например, некоторые системы позволяют людям делать что-либо через Интернет анонимно.

В конечном счете, компьютерная преступность обходится злоумышленнику намного дешевле, чем другие виды преступлений, если у него есть технические навыки для ее совершения. И есть множество способов заработать много денег, не воруя их напрямую у конечных пользователей (например, мошенничество с кликами, когда вы в конечном итоге крадете у корпораций небольшие суммы). К тому же, не так уж много людей попадается на этом. Неудивительно, что это достаточно популярная и привлекательная профессия в странах, экономика которых не предлагает много высокооплачиваемых карьерных возможностей.