FAQ в SPY
интервью с разработчиком компьютерных шпионов

на вопросы хакера (X) отвечает молодой человек в темных очках, представившийся x-dragon'ом (D), с которым мы встретились на безлюдном берегу безымянной реки, где поговорили на темы кибернетического шпионажа

X: значит, ты пишешь шпионское ПО, так? это хобби или способ заработка?
D: сначала это было хобби, я с упоением ковырялся в операционных системах, изучал ассемблер, исследовал способы обхода фаеров, механизмы внедрения, ну вирусами баловался естественно и у меня это получалось, скажем так, лучше чем у других. в определенный момент времени я понял, что на этом можно зарабатывать нехилые деньги и… понеслось.

X: кто твои заказчики? кому нужны шпионы и вирусы?
D: мои заказчики себя не раскрывают, но судя по самим заказам это: спаммеры, рассылающие рекламу чужими "руками", мошенники, крадущие номера кредитных карт и WebMoney, различные "темные ребята", интересующиеся базами данных государственных учреждений и корпораций. всем им нужны программы, умеющие внедряться в атакуемый компьютер и тайком выносить оттуда информацию.

X: как ты находишь клиентов? используешь ли объявления с форумов или это палево?
D: действительно, на форумах до фига таких объявлений, но связываться с ними нет мазы. ты никогда не знаешь кто сидит на другой стороне: стукач или кидала. риск загреметь за решетку за хакерские дела в общем-то минимален, гораздо опаснее, что могут сесть на хвост бандитские группировки и заставить работать на себя, причем за смешные деньги и с вероятностью быть убитым в чужих разборках. ну кому это нужно? лучше находить клиентов ~~среди~~ через хорошо проверенных знакомых.

X: давай поговорим о технической части. на чем ты пишешь шпионов? на ассемблере?
D: боюсь разочаровать, но писать шпионов на ассемблере можно только из большой любви к ассемблеру или от нечего делать. современные компиляторы позволяют сделать практически все, что угодно и с минимальными затратами времени (человеческого). конечно, совсем без ассемблерных вставок не обходится, но основная часть кода пишется на си.

X: почему именно си? а не си++? ведь все сейчас сидят именно на нем!
D: …и создают себе проблемы, мужественно их преодолевая. возможно, си++ хороший язык, но его достоинства уравновешиваются недостатками и в первую очередь — ограничением свободы программиста, запретом многих форм трюкачества. сама идеология си++ провоцирует ~~программиста~~ на решение задачи в общем виде, в то время как в частном она решается в десять раз быстрее и в сто раз эффективнее. впрочем, это уже тема для священных войн ну их на хрен!

X: сколько времени у тебя занимает разработка нового шпиона?
D: зависит от самого шпиона, только "нового" в нем будет немного. основную сложность представляет реализация модулей, ответственных за внедрение, сокрытие процессов и файлов, установку back-door'a и т.д., но все это уже реализовано в моей собственной библиотеке, так что фактически шпион конструируется из готовых блоков, на что уходит несколько дней. гораздо больше времени отнимает тестирование и проверка на совместимость с новыми версиями Windows. шпионы со "знаком качества" обкатываются до недели. конечно, библиотека нуждается в развитии — совершенствовании механизмов сокрытия/внедрения, поддержке новых технологий и платформ (например, x86-64), но это происходит в "фоне", так сказать в свободное время.

X: пользуешься ли ты упаковщиками и протекторами для противодействия аверам?
D: когда-то пользовался, но потом признал эту практику порочной и послал все протекторы на три икса. ты спрашиваешь почему? я сейчас скажу. во-первых, аверисты не спят и оперативно учатся распаковывать новые протекторы, так что такая мера ни от чего не спасет. во-вторых, все мои шпионы пишутся индивидуально и хотя они содержат некоторые постоянные фрагменты

(ту же упомянутую библиотеку), при перекомпиляции другим компилятором с другими ключами, они преображаются до неузнаваемости. в-третьих, гораздо выгоднее использовать свой встроенный мини-шифратор на основе SSE-команд с эмуляцией которых у аверов большие проблемы, да что там SSE! многие команды 8086 процессора (такие, например, как AAA) большинством аверо~~мв~~ эмулируются неправильно, а, значит, они не смогут расшифровать код, даже если расшифровщик будет состоять всего из нескольких машинных команд. во всяком случае, это мой код, за который я отвечаю и прилагаю все усилия, чтобы он работал правильно. популярные протекторы содержат массу ошибок и доверить им защиту своих шпионов я не могу, просто не имею морального права перед своими клиентами.

X: а какие гарантии ты даешь своим клиентам? возможно ли засечь твоих шпионов?
D: гарантии обычные — то есть никаких гарантий. по другому просто не получится. никто не застрахован от ошибок и я в том числе. естественно, опытный хакер, умеющий держать отладчик в руках, сможет обнаружить шпиона, ~~если сильно озаботиться этой целью,~~ но для этого ему придется проделать большую и кропотливую работу, которой никто не будет заниматься просто так, если нет подозрения, а подозрений не~~т~~ будет потому, что мои шпионы ведут себя максимально корректно, обходят защитные системы, не замедляют работу компьютера и ни с чем не конфликтуют, хотя проколы и со мной тоже случаются.

X: что за проколы?
D: да всякие. о многих даже стыдно говорить. например, однажды мой шпион случайно отобрал фокус у окна winlogon'a и не возвратил, некоторые пользователи обратили на это внимание (~~т.к~~. раньше они просто набирали пароль при входе в систему, а теперь на ~~него~~ окно приходилось кликать мышем), вот мой шпион и погорел. несколько раз напарывался на сюрпризы недокументированных возможностей, неожиданно менявшихся в очередном service pack'e без всякого предупреждения и лишающего шпиона работоспособности, а меня репутации и заработка. сейчас я полностью отказался от использования недокументированных возможностей и наменян придерживаться той же стратегии и в дальнейшем.

X: как же так?! шпион - и без недокументированных особенностей?
D: представь себе, написать шпиона, использующего только документированные возможности вполне возможно и он от этого только выиграет. да, в использовании недокументированных возможностей есть какой-то романтизм, но в серьезных разработках использовать его недопустимо! это могут делать либо _очень_ опытные гуру, либо пионеры. я же не отношусь ни к тем, ни к другим. кстати, MS в последнее время "рассекретила" множество функций, бывших ранее недокументированными, чем серьезно облегчила мне и моим коллегам жизнь.

X: какие алгоритмы сокрытия файлов и процессов ты используешь?
D: это как раз проще всего. достаточно перехватить ряд низкоуровневых функций, например, внедрив за концом их пролога jump на свой обработчик. почему после пролога, как поступает большинство шпионов? да потому что уже существуют утилиты, сканирующие первые байты функций на предмет наличия jump'ов к тому же необходимо отслеживать открытие файла NTOSKRNL.EXE, чтобы никакая защита не могла сравнить образ памяти ядра с оригиналом. вообще же, лучший способ маскировки — не создавать никаких дополнительных потоков/процессов, внедряясь в уже существующие, и не дрыгать диско~~в~~м, держа все данные в памяти. _любую_ активную маскировку достаточно легко обнаружить. защите достаточно, например, прочитать диск на сектором уровне и сравнить эти данные с данными, возвращенными операционной системой. если обнаружатся различия — значит, кто-то маскируется.

X: а разве нельзя перехватить посекторное чтение диска?
D: почему нельзя? можно. но это усложняет шпиона, да и к тому же всего не предусмотришь. с этим, кстати, связан еще один мой прокол. я не учел существование USB-носителей и некоторых других типов дисков, вот их и не перехватывал. а следовало бы… (тяжелый вздох). но всего же не учтешь, ведь правда? к тому же некоторые ревизоры сканируют диск еще до загрузки операционной системы, а потому в принципе не могут быть перехвачены шпионом. то есть могут, конечно, но для этого шпион должен внедряться в первичный загрузчик. хорошо, когда он расположен на IDE-диске, а если это RAID или SCSI? сокрытие своего присутствия (то есть стелсирование) — изначально плохая и порочная идея, поскольку ~~она~~ порождает проблемы, решение которых порождает новые проблемы и мы падаем в пропасть в ~~получаем~~

бесконечномый рекурсивномый спуске. ~~в пропасть.~~ впрочем, это только мое личное мнение и если заказчик хочет получить стелисирование — он его получает~~, но я сразу же предупреждаю его чем это чревато~~.

X: мы и не подозревали, что в создании шпионов столько тонкостей!
D: на самом деле их гораздо больше! хороший шпион — большая редкость и его конструкция отрабатывается годами, просто так сесть и написать ни у кого не получится, особенно если ты ~~ничего~~ круче домашнего ПК с IDE-винчестеров~~в~~м и Windows XP Professional ничего другого в глаза не видел! необходимо иметь опыт работы с различным оборудованием, исследовать сотни защитных механизмов (типа брандмауэров, систем обнаружения вторжения и т. д.), причем знать не только теорию, но и практический расклад и расстановку сил, то есть _реальное_ положение дел, определяемое пресловутым человеческим фактором. и много чего еще…

X: вот мы все про Windows говорим, а как на счет шпионажа в никсах?
D: технически это весьма просто (если только это не OpenBSD и админ не латает систему с параноической усердностью). у меня есть несколько готовых шпионов, но спрос на них порядка на два ~~меньше~~ниже, чем на Windows, но, возможно, в будущем ситуация изменится, поэтому шпион~~ов~~ы ~~необходимо подготовить~~ готовятся заранее. ~~заблаговременно.~~

X: что ты хочешь сказать в заключении интервью?
D: то, что разработка шпионов – это удел тех, кто не смог (или не захотел) реализовать себя как-нибудь иначе. сверхбольших денег она не приносит, а риск все-таки есть. он давит на тебя как танк, нависает словно осеннее небо, но… ничего другого кроме шпионов ты программировать ты не умеешь, а клепать аплеухи — тебе не позволяет гордость. вот и…

мы расстались с x-dragon'ом, вечерний туман растворил его силуэт, но сказанные им слова — остались! [он так и не согласился сфотографироваться, поэтому, мы прилагаем лишь панораму реки на берегу которой происходила эта беседа]