техника промышленного шпионажа

крис касперски aka мыщъх, aka elraton, aka nezumi, aka souriz aka жирный нутряк, no-email

промышленный шпионаж существует — это факт. и занимаются им не только (и не столько) красавчики вроде Джеймса Бонда, но и простые хакеры, практически никогда не выходящие из дома и все действия осуществляющие через Сеть. иногда — из любопытства, иногда — из необходимости или желания подзаработать. стать шпионом может каждый, причем совершенно на законных основаниях!

К иномаркам запчасти найти труднее, чем к нашим машинам. К "МАЗу" за бутылку водки любую деталь через забор перекинут.

Александр Лукашенко о преимуществах отечественной продукции

форум - это забор. на котором все пишут что хотят. у некоторых заборов собираются интересные люди, у других - не очень. уборщицы периодически стирают самые похабные надписи. можно любить писать на зоборе, можно любить читать, что другие написали, но ДОВЕРЯТЬ самому забору???

(с) неизвестный

введение

Мир очень сильно изменился за последний десяток лет, а вместе с ним изменились цели и задачи промышленного шпионажа. Уже никто не делает секрета из сроков выхода новых продуктов или их потребительских характеристик, как это было во времена ранней молодости MS-DOS, разработчикам которой так и не позволили увидеть прототип IBM PC, разрабатывающийся в обстановке полной секретности, однако, во многом это было излишним.

Допустим, шпионы смогли выкрасть весь комплект документации или на худой конец сам образец, но… что с ним делать? Без соответствующей инфраструктуры и "носителей знаний" — инженеров, держащих в голове все детали проекта, это просто кипы бумаги и груда металла, на разор которого уйдет практически столько же времени, сколько на независимую разработку. Шпионаж и переход на копирование западных технологий в конечном счете привел к развалу отечественной вычислительной техники, ведь даже если выкрасть самый передовой образец, то за время "проектирования наоборот" чужая инженерная мысль уйдет далеко вперед, а мы окажемся сзади. К тому же, в СССР все украденное у запада считалось общенародным достоянием и на патенты никто не обращал внимания.

Рисунок 1 хакеры работают в темноте, на ощупь находя клавиши и продвигаясь наугад

о патентах, корпорациях и NDA

Сейчас же, влияние американских корпораций на весь прилагающий к ним мир таково, что выпускать продукцию, уклонясь от лицензирования патентованных технологий, можно только в китайском подвале, да и то лишь до того момента, пока правообладатель не составит исковое заявление в суд, что полностью обессмысливает промышленный шпионаж, поскольку суть патентования заключается в раскрытии технологии в обмен на монопольное право владения. То есть, если технология не запатентована и удерживается в секрете, всякий кому удастся ее раздобыть (например, путем шпионажа или обратного проектирования) может беспрепятственно пользоваться ею. Напротив, если технология запатентована, она доступна для ознакомления всем желающим (для этого даже не придется ничего платить, тексты патентов свободно выложены в сети), но… любая форма практического применения (не важно коммерческая или нет), требует наличия лицензии от владельца патента, который в праве запросить за нее любые деньги или просто отказать в лицензировании по "политическим" или маркетинговым соображениям.

Все, что не патентуется (например, исходные тексты программ) может быть получено под NDA (аналог нашей "подписки о неразглашении"), легкость получения которой просто поражает и по сути представляет чисто формальную процедуру. Было бы большим заблуждением считать, что исходные тексты Windows представляют огромную тайну, тщательно охраняемую Microsoft. Если Microsoft что-то и охраняет, так это распространение, а

отнюдь не разглашение. Получить доступ к исходным текстам через NDA — вполне реально. Достаточно вспоминать компанию VM Ware, которой они были необходимы для реализации виртуальной машины и через дырявый сервер которой произошла утечка, благодаря которой код Windows 2000 стал доступен всем желающим (как говорится, что в осла попало...), но как бы там ни было, прибегать к помощи Джеймса Бонда для этого совершенно необязательно. Легальные пути — быстрее, эффективнее и надежнее, во всяком случае в теории дела обстоят именно так. А вот что нам преподносит реальность…

Представим себе сотрудника ремонтной мастерской, озабоченного поиском принципиальной схемы нового телевизора фирмы Sony или программиста, разрабатывающего драйвер для видео-карт производства ATI под LINUX. И хотя ни сервисная документация на телевизор, ни техническая спецификация на видео-карту сами по себе секретом не являются, получение их через официальные каналы упирается в бюрократические проволочки, зачастую отнимая гораздо больше времени и усилий, чем обратное проектирование. Логически, Sony заинтересована в том, чтобы продать как можно больше телевизоров (а для этого нужно, чтобы их умели ремонтировать, иначе от них откажутся как покупатели, так и продавцы). ATI заинтересована в том, чтобы продать как можно больше видео-карт и хотя она упорно игнорирует существование LINUX, не желая вкладывать деньги в разработку драйверов, глупо упускать возможность, мешая создавать драйвера другим. Люди, стоящие у руля, это прекрасно понимают, но… раздачей спецификаций занимаются не они, а добиться чего-то от клерков на местах — практически безнадежное дело. То есть, через NDA получить спецификации вполне возможно, только зачем они нам нужны с NDA?

Потребность в промышленном шпионаже, существенно снижавшись на "высоком корпоративном уровне", осталась актуальной для отдельных лиц и небольших компаний. И вот о ней-то мы и будем говорить!

Существует не так уж много способов промышленного шпионажа, реализуемых через Сеть и они далеко не так эффективны как разведчики типа Штирлица, но с вышеописанными задачами вполне справляются, не вызывая никаких конфликтов с законом, что делает их вдвойне опаснее!

Рисунок 2 рабочее место типичного хакера, занимающегося промышленным шпионажем

крепость берут изнутри

Корпоративная политика — это лишь видимая часть огромной машины, приводимой в движение обыкновенными людьми, которые общаются друг с другом, обсуждают технические проблемы или просто болтают на разные темы, посылая куда подальше секретность и прочие

правила, диктуемые уставом компании. Многие задачи решаются совместными усилиями инженеров, работающих в соседних или даже конкурирующих (!) компаниях. Практика показывает, что конкуренция внутри компании зачастую намного сильнее, чем вне ее. Типичная ситуация — инженеру поручили задачу, с которой он справиться оказался не в состоянии. Признаться в этом — означает признать собственную некомпетентность. Обратиться за помощью к коллегам — так ведь один хрен они помогут, а если и помогут то только ценой продвижения своей карьеры за счет других. Как говориться, не имей сто рублей, а имей сто друзей, пускай даже работающих на другом континенте и знакомых заочно по сети. Все равно, любой инженер, так или иначе, со временем обрастает сетевыми знакомствами, даже если он не сжигает время на форумах, то по крайней мере читает техническую литературу — книги и статьи, а там как правило стоит e-mail…

Конечно, люди встречаются самые разные. Есть среди них и щедрые, и скупые, и просто козлы из которых ни грамма полезной информации не выдавишь. Как говориться, в одних живет Аллах, в других — дьявол, а в некоторых водятся только глисты. Но найти демократично настроенного человека, увлеченного своим делом и ставящего дружбу превыше интересов компании — нетрудно, такие сами идут навстречу, а с другими и общаться не стоит! Конечно, наивно надеяться, что кто-то за просто так может передать полный комплект исходных текстов (документации, принципиальных схем), хотя бы уже потому, что существует такое понятие как разграничение доступа и каждый работает только с теми частями проекта, в которые его "посвятили", иначе наступит полный бардак и любой обиженный сотрудник сможет завались всю компанию.

Арабы в таких случаях говорят, хочешь пробраться к сановнику — сдружись с привратником. За неимением привратника сойдет и системный администратор. Случай из личной жизни. Потребовалось мне как-то раздобыть документацию на одно оборудование, которая отдавалась только под NDA и только компаниям-членам. Ну быть членом в мои мыщъхиные планы не входило, поэтому, пришлось ограничиться перепиской с системным администратором, на которого мыщъх вышел через других сотрудников компании, с которыми познакомился через публичные адреса, висящие на сайте. Администратор (как и положено) был неразговорчив и мрачен как облака, предвещающие шквал (см. "предсказание погоды по местным признакам", выложенную на моем ftp). Дело было совсем не в неразделенной любви, а регулярно падающей NT. Как известно, в последних Service Pack был ужесточен контроль за ошибками и освобождение уже освобожденной памяти ранее сходившее драйверам с рук, теперь стало вызывать выпадения в BSOD. И ведь для нашего же с вами блага! Microsoft посчитала, что лучше остановить систему, чем позволить драйверу химичить с памятью! Вся проблема в том, что этот драйвер управлял сложным аппаратным комплексом, срок технической поддержки на который уже давно истек и все, что мог предложить его поставщик — это купить новый аппаратный комплекс вместе с новой версией драйвера, стоимость которого была весьма немалой, к тому же он был несовместим с некоторым используемым оборудованием.

Отказ от установки Service Pack'a решал проблему BSOD, но оставлял не заткнутыми многие дыры, для которых "индивидуальных" заплаток не существовало, точнее, эти заплатки влекли за собой зависимости, приводящие к смене ядра ОС и установке обновленной версии с ужесточенным контролем. Служба поддержки Microsoft только пожимала плечами, мол кого @=> чужие проблемы, и перекладывала всю ответственность на разработчиков драйвера, вина которых была очевидной и неоспоримой, но… это не было ответом на вопрос: как дальше жить и что делать? Голубые экраны смерти продолжались, компания терпела убытки, администратор получал шишки и… тут на сцене появился мыщъх.

Для меня, как для хакера, решение было очевидным. Дизассемблировать ядро, найти то место, где производится проверка освобождения уже освобожденной памяти (а найти его очень просто — по перекрестным ссылкам к функции KeBugChekEx, вызываемой с соответствующим STOP-кодом) и слегка пропатчить ядро, предварительно отключив защиту от записи путем сброса бита WriteProtect в регистр CR0. Мыщъх просто предложил несчастному администратору переслать по почте его NTKRNLOS.EXE, и буквально через несколько минут выслал "исправленный" вариант. И… нет! Никакой заразы, никакого малваре, похищающего пароли, мыщъх туда не вписал. Вместо этого просто попросил свести с людьми, которые могли бы помочь (ну типа походатайствовать там) с документацией. Вот и все!

Рисунок 3 правка KTOSKRNL.EXE в soft-ice

Вы думаете, что коррупция существует только в нашей стране и что, например, в Азии не крадут и не берут взяток? Напротив, там это делают все, нисколько не стесняясь. Вот только одна история, рассказанная сотрудником той же компании: при постройке нового цеха, проектировщики запросили у метеорологов среднегодовую температуру по Таиланду. На основании полученных данных была спроектирована, изготовлена и установлена система кондиционирования и вентиляции. И все бы ничего, но… в "среднегодовой" и "среднетиповой" температуре обнаружился значительный разрыв, особенно хорошо заметный в летнюю жару. Стали искать виновных. Метеорологи отмазались сразу: мол, что нас спросили, то мы и ответили, а проектировщики упирали на то, что ни хрена не разбираются в метеорологических терминах и просто не знают как "по науке" называется, то, что они имели ввиду. Дело кончилось тем, что проектировщиков уволили, а систему кондиционирования демонтировали, перепроектировали и смонтировали заново. Вся соль в том, что первая система существовала только на бумаге, а стоимость фиктивных работ по изготовлению/монтажу/демонтажу вы себе представляете? Там многим поживиться хватило! Но мы отвлеклись. Вернемся к нашим баранам.

В каждой фирме имеется огромная техническая библиотека, содержащая до фига всего интересного — как документацию на свои собственные разработки, так и обширную справочную литературу, ставшую уже библиографической редкостью. Тем не менее, раздобыть ее очень просто — достаточно уломать одного из сотрудников компании пойти туда и чего-то скопировать. Как правило, эта просьба удовлетворяется, и хотя с точки зрения руководства является грубым нарушением, ставить руководство в известность никто не собирается. Как

вариант, можно сдружиться с отделом верстки любого крупного издательства, бесплатно получая электронные копи новых книг, которые ваши друзья вам беспрепятственно вышлют, если будут знать, что дальше вас они никуда не пойдут, иначе дружба врозь.

Как вариант, закрытую техническую документацию можно получить через NDA, только обращаться за этим надо не через официальные каналы, а через знакомых внутри компании, которые посоветуют к кому лучше всего обратиться по данному вопросу. Как уже говорилось выше: в современном мире технологии защищаются не секретами, а патентами и закрытая документация легко отдается под NDA, если конечно, действовать не через адреса менеджеров, вывешенные на сайте — те и так перегружены работой. Лишняя возня им совсем ни к чему. Гораздо проще ответить отказом, чем ввязываться в бюрократическую волокиту. И ведь их можно понять…

к любому замку ключ подобрать можно

Поговорим теперь о незаконных способах. Не для того, чтобы применять, а просто, чтобы знать о них (как говориться, тот кто предупрежден — вооружен). На первом месте, как водится, стоят удаленные атаки. Современные системы — дырявы, администраторы — необразованны и/или ленивы, так почему бы хакерам и не процветать? Опять-таки этот пресловутый человеческий фактор, позволяющий проникнуть в корпоративную сеть и без изощренных методов. Простого письма с вложением, направленного в службу поддержки, обычно оказывается вполне достаточно, особенно если там сидят девочки, набранные по объявлению. Писать от имени big-boss'a совершенно необязательно. Лучше притвориться ничего не понимающим лосем, желающим купить дорогостоящий продукт, если только ему объяснят на хрена он вообще кому-нибудь нужен. Ведь, образно говоря, Windows Server в миску не проложишь. И проблем она создает столько, что не помогает даже вазелин. Ой! О чем это я?

Ах да! Прежде чем войти, подумай, как выйти (с) башкирская сказка. Стоит прислушаться к башковитым обитателям южного урала, тем более, что похожая поговорка есть и у арабов — не открывай дверь, которую ты не в силах закрыть. Короче! Перелезть через брандмауэр намного проще, чем вылезти потом обратно. Если вы не вступите в горшок с медом (он же honey-pot), то разбудите Цербера (в смысле Intruder System Detection — Систему Обнаружения Вторжений), после чего останется только молиться на proxy — чтобы не выдал истинный IP-адрес, а многие "анонимные" proxy его выдают. Кроме того, даже оставшись незамеченным (будешь сиять тихо — узнаешь много, как говорят дружественные нам татары), далеко не всегда можно сориентироваться в корпоративной сети и утащить что-то конкретное. Но, если Аллах закрывает одну дверь, он открывает тысячу других, посылая нам проводника. А еще лучше — проводницу. Такую симпатичную, хорошую проводницу. И совсем не толстую. Или толстую. Как пышку. Это уже кому какие нравятся. Но в практическом плане толстая все же лучше худой — меньше самцов на нее обращают внимание, что приводит к разговорчивости по Яське, быстрой влюбчивости (а сердце девушки, по мнению татаров, — кипящий котел, ни с чем не считается). Триста лет татаро-монгольского ига не прошли для нас даром и теперь мы возвращаем упущенное всеми путями.

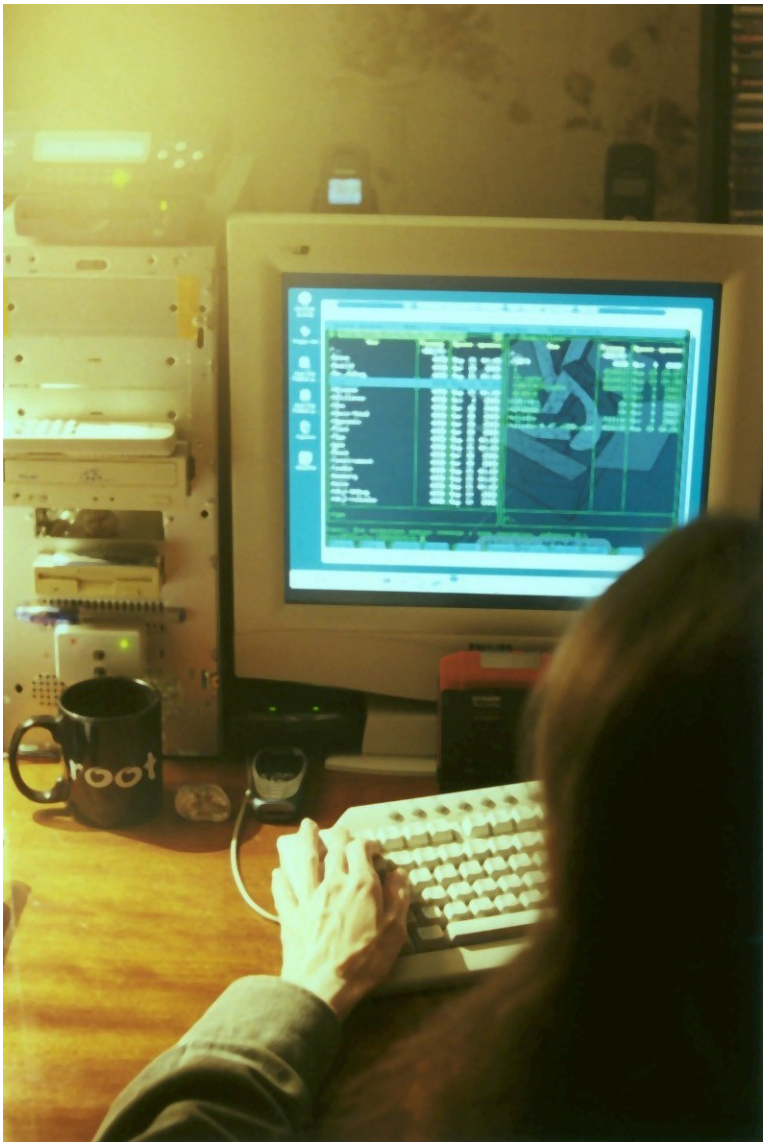

Рисунок 4 промышленный шпионаж в самом разгаре

Обратившись за консультацией к калмыкам мы узнаем, что дурного можно и не спрашивать — он сам все скажет. Соединив это с собственным опытом (все бабы — такие…), нам останется только слушать. Весь вопрос в том, где этих красавиц найти? Если публичные адреса на web-сайте не помогут, тогда начинам рыскать на разных службах знакомств, делая веерные рассылки писем-на-которые-нельзя-не-ответить, и определяя их принадлежность по IP-адресам в заголовках, поскольку большинство барышень пишет со служебного компьютера, в служебное время, что кстати говоря, легко позволяет определить их географическую принадлежность, особенно в свете того факта, что первым делом по приходу на работу проверяется почта, а затем уже все остальное (про часовые пояса не забываем, да? они _очень_ богатую информацию несут! при условии, конечно, что человек не сова, а вполне конкретный жаворонок, но быть секретаршей-совой довольно проблематично, особенно в свете того факта, что большинство фирм на ночь запирается, так что особенно тут не по секретутствуешь...).

Влюбленная девушка способна на многое. И нужно быть гадом, чтобы толкнуть ее на служебное преступление. Но ведь толкают же, шакалы позорные, после чего растворяются в сети как утренний туман. Не зря турки говорили ,что волк туман любит. Но… с другой стороны: не знать пива - не знать радости, особенно когда отливаешь. Стоп! Мы опять отвлекаемся! Да сохранит нас Аллах от недостатка пищи и от избытка слов! Выбросим пиво (все равно его уже не осталось) и продолжим дальше перебирать способы добычи информации какие только на свете есть! А мир так велик, что нет ничего такого, чего бы не было, и если мужской монастырь напротив женского монастыря - даже если ничего не происходит, то все-таки что-то есть! Так что ты поднимай, а я буду пыхтеть! сейчас кааак дунем!

Рисунок 5 перерыв на обед без отрыва от шпионской деятельности

Что у нас там дальше по списку? Ага, шантаж. Дело это грязное и во всех смыслах сильно уголовное, но ведь находятся такие козлы, что им занимаются, так что приходится быть наготове. Физической расправой угрожают редко, поскольку ее очень трудно осуществить через сеть (на самом деле — очень просто: находим горячих парней на прилегающей территории, переводим им немного денег через сеть и обещаем перевести еще больше, если они слегка поколотят такого-то мужчину или доведут средство его личного транспорта до непотребного передвижения путем изображения известного органа в масштабе 1:50 — читайте Press Enter, там это подробно расписано) и еще потому, что с угрозами такого рода легко справляется полиция.

Гораздо хуже, если шантажист намекнет, что он может сообщить ревнивой жене о имевшей место измене, против чего не попрешь. Ох, и не зря мы называем своих баб лебедушками. Вы видели лебедя, когда он в гневе? "Как ни зол лебедь - и он своих яиц не бьет" (с) калмыки, а по нашим мочит со всего маху! И в полицию ведь с такой угрозой не пойдешь. Да много разных "честных" способов шантажа существует. Например, сообщить ребенку о том что он (яко бы) совсем не родной, а… приемный. В переходном возрасте, когда конфликт отцов и детей (тургенева все проходили?) особенно силен, такой, зароненный в душу червь сомнений, может иметь очень далеко идущие последствия! Но по любому, лучше сразу оказать шантажисту отпор, чем идти у него на поводу, надеясь, что после выполнения всех его требований, он оставит нас в покое!

заключение

Бывают только непорочные невесты, но не бывает непорочных свах (с) дружественные народы китая. Каждому из нас, программистов, приходится грешить, действуя не всегда честным путем. Если для создания жизненно важной, можно даже сказать судьбоносной программы, нужна информация, которую не удается получить официальным путем, то остается руководствоваться лишь жесткостью наказания, помноженным на вероятность быть пойманным и моральным законом внутри себя.

Обычная тактика, которой придерживаются практически все западные компании, например, та же CISCO и Microsoft: если можно купить — покупаем (за разумную цену, естественно), если нет — форсируем реку тибор и один хрен пусть попробуют доказать, что мы не были в Пизе. Кстати говоря, скандал, разгоревшийся вокруг кражи исходных кодов CISCO OS не в последнюю очередь связан с тем, что в состав этой оси входит немало компонентов "позаимствованных" у линуха, которые (по лицензии) не могут использоваться в закрытых продуктах, но, увы, суды очень редко удовлетворяют иски сообщества Open Source, а все

потому, что оно, с точки зрения государственной машины на хрен не нужно, поскольку не платит налогов в отличии от компаний-гигантов. Но что позволено Юпитеру — не дозволено быку. Так что не будем высаживаться, а предоставим жизни идти своим чередом, чтобы и ворам товарищ, и каравану друг.

Рисунок 6 в глубине хакерской норы