FAQ по взлому клиентских приложений и безопасности сетевых протоколов

крис касперски ака мыщъх, no-email

Q: традиционный вопрос: можно ли взломать Интернет?
A: долгое время на это давался безапелляционный ответ: нет, невозможно. Интернет — это совокупность огромного количества разнородных узлов, работающих под управлением различных операционных систем, каждая из которых содержит "свои" уязвимости, затыкаемые очередной заплаткой, и потому написать универсальный кракер Интернета практически нереально, к тому же, он будет очень недолговечным, ведь однажды найденные дыры быстро устаревают. Но на стыке веков все изменилось. Альтернативные операционные системы неуклонно вымирают и Интернет стремительно вырождается в сеть Windows-машин, обслуживаемых различными "орангутангами", не устанавливающих заплатки годами. Они работают как на клиентских станциях, так и на серверах. Так что взлом Интернета из сказки превратился в реальность.

Q: опасно ли выходить в Интернет?
A: очень опасно! клиентское программное обеспечение дыряво до чрезвычайности, а в сети бродят злобные хакеры и водятся агрессивно настроенные черви, которые атакуют все, что находится у них на пути. И хотя большинство из них не делает ничего, только транжирит сетевой трафик и периодически роняет Винду, нередки случаи уничтожения или утечки данных. В особенности это относится к Интернет-паролям, электронным кошелькам, конфиденциальной информации и т. д. Еще воруют ICQ-номера, идентификаторы сетевых игр, содержимое адресной книги (представляющее огромный интерес для спамеров), да и вообще все, что угодно. Иногда, руками захваченного компьютера осуществляют удаленную атаку, например, направляют шторм SYN-пакетов на правительственный сервер, вот и попробуй доказать, что это не ты козел и тебя подставили!

Q: а как защититься от всех этих угроз?
A: регулярно, не реже одного раза в неделю скачивать заплатки для всех установленных приложений (а не только Windows Update). Ведь ошибки обнаруживаются не только в продукции Microsoft, встречаются они и в Лисе, и в Осле, и в ICQ, и многих других клиентах. Так же, ни в коем случае нельзя открывать вложения, не убедившись в "честности" их расширения. Лучше предварительно сохранить вложения на диск и оттуда действовать уже FAR'ом, он не подведет, а вот стандартного "Проводника" очень легко обмануть

Q: а что же насчет антивирусов?
A: при регулярной установке свежих заплаток, вероятность подцепить сетевого червя — практически нулевая, но зато легко можно запустить инфицированный exe-файл, поэтому, скачивать файлы с подозрительных источников недопустимо. Теоретически, полученный файл можно пропустить через антивирус, но здесь есть одно "но". Крупные компании, "стерилизуют" все программное обеспечение и самостоятельно, поэтому за его чистоту можно не опасаться, а всякие отстойники с кракнутым варезом вполне могут подложить "свинью", заразив файл слегка модифицированным вирусом и никакой AV его не возьмет! К тому же антивирусы отнимают довольно много системных ресурсов, а постоянные обновления баз жрут трафик, так что выгода от их использования довольно сомнительна.

Q: а что на счет брандмауэров?
A: брандмауэр сам по себе еще ни от чего не защищает, и на ПК он, в общем-то, не слишком-то и нужен. Да, он может закрыть уязвимые порты, но более эффективной мерой будет регулярная установка заплаток. Персональный брандмауэр — это удобное средство для наблюдения за легальными приложениями — какое из них ломиться в сеть, что пытается передать и куда, но специальным образом спроектированная программа, может пробить брандмауэр как снаружи, так и изнутри. Он даже хрюкнуть не успеет! Брандмауэр — это инструмент для профессионалов, разбирающихся в TCP/IP протоколах и умеющих читать "сыре" двоичные логи. С настойками по умолчанию — это просто красивая игрушка, которая опять-таки жрет ресурсы, иногда обрушивает Винду, конфликтует с некоторыми приложениями и уменьшает

трафик. Брандмауэры и антивирусы приносят чувство ложного успокоения, жертва расслабляется, забывает об обновлениях и вот тут-то хакер и наносит свой удар!

Q: насколько опасно бродить по порно- и варезным сайтам?
A: underground-сайты (к которым относится и порнуха и врез) делятся на две категории. Первая — это честные сайты, ведущие свой маленький бизнес, и посещать их неопасно, даже если там выложено извращенное садо-мазо в стиле Кенга верхом на Пухе с кактусом под хвостом. Другие же используют порно/варез как приманку и при заходе на сайт забрасывают на клиентский компьютер зловредный код, превращающий ее в дрона, или просто накручивающий рекламу. Это дело поставлено на широкий поток, сюда вкладываются реальные деньги и привлекаются весьма нехилые программисты, оперативно разрабатывающую свежую "мохнатость", зачастую опережающую выход заплаток, поэтому, своевременное обновление уже не помогает. Чаще всего объектом атаки служит браузер (который, как правило, IE, Лис или Опера). Так что ставьте себе что-то совсем необычное (например, links) и не парьтесь.

Q: и что, links спасет от инфицированного вареза?
A: конечно же нет! links спасает только от атак на сам браузер. Порнуху в нем можно смотреть безбоязненно, но вот с варезом сплошной напряг. Лучше качать его с официальных сайтов, а в "дикой" сети искать серийные номера или ключи регистрации. Генераторы регистрационных номеров, будучи исполняемыми файлами, несут в себе большую опасность, поэтому лучше всего запускать их на виртуальной машине (VMWare, Virtual PC) или не запускать вообще. К сожалению, не все программное обеспечение можно скачать с официальных сайтов. Тогда, скачайте взломанные версии с нескольких независимых источников и сравните их утилитой fc из штатного комплекта поставки Windows или любой другой. Инфицированные версии распознаются сразу же! А вот доверять антивирусам резона нет!

Q: где найти варез?
A: вот три основных источника: файлообменные сети, IRC и приватные ftp-сервера. Из файлобменных сетей лидируют Осел (eMule), Shareaza и BitTorrent. В Осле много секретной документации, музыки и софта, через BitTorrent в основном передают видофильмы, Shareaza пока что находится в стадии роста, ну а порнуха есть везде. Чтобы пользоваться файлообменными сетями желательно иметь постоянное подключение, поскольку скорость скачки оставляет желать лучшего и приходится долго простаивать в очередях, иногда передача файла (неважно какого объема) занимает до двух-трех месяцев! IRC – это разновидность чата, но в отличии от WEB-чатов, на IRC можно вешать специальные скрпты, отдающие файлы по запросу. Многие IRC'шники так и поступают. В отличии от файлообменных сетей на IRC вывешивают преимущественно свежий софт, поэтому возможности поиска здесь очень ограничены. Так же, на том же самом IRC и разных web-форумах (например, ru-board.com), частенько пробегают ссылки на стихийно поднятые ftp-серверы, которые через некоторого время бесследно исчезают, но перед этим успевают раздать кучу вареза.

Q: какие клиентские приложения относятся к группе риска?
A: чем сложнее приложение, тем выше вероятность присутствия ошибок в его коде. Браузеры — это очень сложные приложения, фактически операционная система в миниатюре и ошибок не избежал ни один из них ("кастрированные" браузеры типа links'a не в счет). Так же большую опасность представляет Осел, поскольку он "засвечивает" ваш IP и если на компьютере не установлены заплатки он может быть легко атакован. Через файлообменные сети черви очень быстро распространяются!

Q: является ли использование поддельных кредиток нарушением закона или нет?
A: является. однозначно. при покупке "железа" или иных материальных товаров вы серьезно рискуете и прецеденты арестов таких кардеров уже есть. Срок обычно дают условно, однако, перед этим будет суд плюс конфискация компьютера, что не есть хорошо. Даже если компьютер отдадут, то уже в "изнасилованном" состоянии, после чего он будет как не родной. Плюс пятно на репутации, проблемы с трудоустройством и весь прочий мясокомбинат. С нематериальными услугами (порно, медиа, ебуксы) все обстоит иначе. Доказать факт совершения покупки практически невозможно, поскольку никакие бумажные документы не фигурируют и всегда можно сослаться, что это кто-то влез на ваш в компьютер и чего-то там нахимичил. Только не надо воспринимать это как призыв к действию, ОК? Последствия могут быть весьма

удручающими. Например, на одном порно-сайте обещали выслать кастрационную команду быстрого реагирования.

Q: является ли сканирование портов нарушением закона или нет?
A: с юридической точки зрения понятия "сканирования" просто нет. Уголовный кодекс оперируют такими понятиями как несанкционированный доступ к охраняемой информации, нарушение работоспособности вычислительной машины, искажение или уничтожение данных и т.д. Если сканирование не уронило сервер, то ничего криминального с точки зрения УК не произошло. А как же несанкционированный доступ к данным? Да не было никакого несанкционированного доступа! Сканирование выявляет перечень услуг легально предоставленных сервером, это вроде как чтение табличек у дверей "открыто" или "закрыто". Тем не менее, сканирование портов обычно является первой фазой хакерской атаки, так сказать, своеобразным сигналом к вторжению, поэтому все его боятся и при первой же возможности пресекают. До суда дело еще ни разу не доходило (ведь состава преступления нет), но вот нажаловаться провайдеру обиженная сторона очень даже может. В худшем случае последует отключение от сети, но обычно все дело сводится к "выговору" по телефону. Правда, отмечены неоднократные случаи физических разборок с тяжелыми телесными повреждениями.

Q: я забыл пароль на свой ящик на mail.ru, помогите мне его взломать пожалуйста!
A: будем надеяться, что это действительно ваш пароль, а не пароль вашей подружки или партнера по бизнесу, как и случается чаще всего. Значит так, чтобы добыть пароль с сервера, необходимо хакнуть весь его целиком. Теоретически, это возможно, но практически труднореализуемо и к тому же наказуемо, поэтому приходится идти другим путем. Как правило, на многих серверах, есть служба забытых паролей, требующая ответа на такой-то вопрос. Зачастую ответ тривиален или может быть угадан с нескольких попыток. Если же это все-таки не ваш ящик, можно забросить на компьютер жертвы любую из систем удаленного администрирования или, выражаясь, хакерским языком, открыть на ней shell, для чего подойдет любой shell-exploit. А если жертва находится в одной локальной сети, пароль можно выудить сниффером.

Q: я вот хакнул нечто очень крутое и вот сейчас сижу, типа боюсь, что менты нагрянут
A: не нагрянут, не бойся. С первого раза еще никого не повязали. Тут ведь доказательная база нужна, плюс заявление от потерпевшего. Даже если потерпевший напишет заявление, будет отслежен ваш маршрут и определен домашний адрес —в квартиру никто не вламывается, а за человеком устанавливается более или менее плотная слежка. Если лечь на дно и не предпринимать никаких незаконных действий (на хакерские форумы, впрочем, лазить можно), то никакой угрозы нет. Во всяком случае в России дела обстоят именно так. На западе все сложнее. Да и что с него, дикого возьмешь? Уродами были, уродами и остались. Только индейцев покоцали. В Америку после этого вам можно будет въехать только чучелом или тушкой. Арестовать могут прямо в аэропорту без предупреждений!

Q: какая операционная система самая защищенная?
A: такой системы нет, во всех ныне существующих осях обнаруживаются дыры. Чем популярнее операционная система, тем интенсивнее ее ковыряют и, соответственно, наоборот. До недавнего времени считалось, что в Линухе дыр нет, но на самом деле его просто никто не исследовал как следует, а теперь дыры сыплются как из рога изобилия. На FreeBSD дыр намного меньше, разработчики вылизывают релизы до зеркального блеска, предпочитая семь раз подумать и один раз накодить. Поэтому, FreeBSD очень медленно развивается и неизбежно отстает от прогресса. QNX, которая как известно, работает в атомных реакторах и реактивных истребителей, никаких дыр похоже вообще не содержит, но и софта под нее выпущено очень немного, да и тот большей частью ориентирован на разработчиков. В мире Windows, наиболее непрошибаемой оказалась… Windows 98. Линейка NT (2000, XP и т.д.) просто скопище багов, поэтому, если есть такая возможность от ее использования лучшего всего отказаться. Лично я сижу под W2K, но постепенно перехожу на Debian.

Q: какой юридической силой обладает EULA (она же End User License Agreement)?
A: Почему-то большинство считает, что лицензия едва ли не равноценна Уголовному Кодексу и все, что там ни написано, следует в обязательном порядке соблюдать иначе придется коротать длинные зимние ночи под небом в клетку вместе с друзьями в полоску. Бред! Чушь собачья! Лицензия – это договор и не более того! Не стоить строить против нее никаких иллюзий,

приписывая ей несуществующее могущество. Скажем, срывать пломбы на телевизоре тоже по идее нельзя (так во всяком случае в паспорте, прилагаемом к телевизору, написано). Но если рискнуть это сделать – наивно ожидать нашествия ОМОНА и длительного тюремного заключения – срыв пломб повлечет за собой всего лишь нарушение договора, заключенного между продавцом и покупателем, с последующей потерей всех гарантий и обязательств, данных продавцом. Ситуация с программным обеспечением в точности аналогична. При заключении сделки вы, покупатель, со своей стороны обязуетесь выполнять все пункты лицензионного соглашения, а разработчик, стало быть, продавец, обещает вам всяческую помощь, как-то: техническую поддержку, скидку на все новые версии, ну и так далее. Если вы нарушите лицензию, все, что сможет предпринять против вас продавец, – отказать в технической поддержке, отменить скидки на новые версии, т.е. забрать все свои обязательства обратно. Но ничего сверх этого! Однако, если помимо лицензии нарушить авторское или патентное право, тут же вступят в силу совсем другие законы. Например, сорвав пломбы с телевизора, вы еще не совершаете никакого преступления, но когда изучите его монтажную схему, изготовите такой же точно агрегат и вынесете его на рынок продавать, – производитель сможет подать в суд за нарушение патентного права, вчинив иск того или иного размера. Аналогию с программным обеспечением, думаю, приводить не надо, – она очевидна и так. В то же время, никто не запрещает ковыряться и вносить конструктивные изменения в свой экземпляр телевизора «для домашнего пользования» (по аналогии – ломать, ой, простите, адоптировать, программы). Что можно вытворять с программным обеспечением перечислять можно бесконечно долго – лучше сказать что с ним делать нельзя. Нельзя его копировать (не путать с "распространять"), нельзя выдавать за свое собственное, наконец его нельзя кушать, вот, пожалуй, и все.

Q: а что мне будет, если я скажу, что никакой лицензии не было или я ее не заметил?
A: Мне часто приходится видеть людей, впадающих в другую крайность и начинающих утверждать, что все электронные лицензии никакой силы не имеют, поскольку не снабжены ничьей подписью. На худой конец можно попробовать прикинуться наивным чукотским юношей, не умеющим читать, а раз человек не читал, то какой с него спрос? (Утверждение «не знание закона не освобождает от ответственности» здесь неприемлемо, ибо речь идет не о законе, а о договоре, незнание которого ото всех обязательств, данных по нему освобождает, поскольку, как гласит Статья 432 Гражданского кодекса РФ, если одна из сторон не сумела или не захотела прочитать договор, то он признается недействительным). На самом деле понятие договора столь широко, что выходит за рамки бумаг и папирусных свитков. Так, опуская жетон (карточку) в метро, с юридической точки зрения вы заключаете договор, – деньги в обмен на услугу доставки вашего тела нужное место и нужное время. Нигде ничьей подписи не стоит, но это еще не означает, что если автомат жетон благополучно проглотит, а вас все равно не пропустит, это сойдет ему с рук ввиду отсутствия на договоре подписи, заверенной печатью. Такая же ситуация складывается и с программам обеспечением. Электронный договор не является препятствием для вынесения иска лицу, нарушавшему его. Техника собора необходимых доказательств – вопрос совсем другой, но не стоит надеется, что у истца такие доказательства отсутствуют. Короче говоря, в жизни действует такая схема: если люди просят за свой продукт нормальные бабки, его покупают, в противном случае — тыбрят (а в Пизе ничего не пропадало?) и пусть они попробуют что-то доказать. Да, это не призыв, а констатация факта.