SPECIAL ОПРОС

АЛЕКСЕЙ ПЕТРОВ

В IT 20 лет. Эксперт в области защиты данных, эксперт по компьютерным преступлениям, эксперт по сетевым коммуникациям и телефонии. Сертификаты от *Novell/3com/Bay/Siemens/Cisco/ISACA*. Консультант по вопросам ИТ-безопасности в Secproof Oy (*www.secproof.com*). Свободный консультант *Arhont.com*, *iPRO.lv*.

АЛЕКСЕЙ ЛУКАЦКИЙ

Бизнес-консультант по безопасности Cisco Systems. В Cisco отвечает за развитие направления безопасности в России и странах СНГ.

ВЛАДИМИР КОМИССАРОВ

Начальник IT-отдела одной из компаний.

АНТОН КАРПОВ

Специалист в области информационной безопасности. В «Х» пишет с переменной периодичностью вот уже несколько лет. Круг профессиональных интересов: сетевые атаки, безопасность UNIX-систем, безопасность беспроводных сетей...

КРИС КАСПЕРСКИ

Известен еще как мыщъх. Компьютеры грызет еще с тех времен, когда Правец-8Д считался крутой машиной, а дисковод с монитором были верхом мечтаний. Освоил кучу языков и операционных систем, из которых реально использует W2K, а любит FreeBSD 4.5. Живет в норе, окруженной по периметру компьютерами и стеллажами с литературой.

ШПИОНЫ — РЕАЛЬНАЯ УГРОЗА ИЛИ ШУМИХА, КАК И ПРОБЛЕМА Y2K?

КРИС КАСПЕРСКИ: Проблема дырявого ПО — вполне осязаема и реальна, особенно в отношении продуктов Microsoft, в которых регулярно выявляются свежие баги. Поэтому проникнуть в любой компьютер, подключенный к Сети, может даже неквалифицированный программист или в просторечии «пионер». Что, собственно говоря, регулярно и происходит.

В основном, конечно, атакам подвергаются web-серверы и корпоративные сети, содержащие закрытую информацию. Домашние пользователи находятся в меньшей опасности в силу своего большинства, хотя степень защищенности их компьютеров гораздо слабее. Можно провести аналогию с заказными убийствами бизнесменов и бандитизмом, царящим на улицах. Среднестатистический прохожий абсолютно не защищен, но шансы быть убитым у него намного ниже, чем у любого бизнесмена с целой свитой охраны. Ежедневно совершается множество убийств и вторжений в компьютеры (как домашние, так и корпоративные), никто не может чувствовать себя в абсолютной безопасности. Но всегда следует помнить, что паническая истерия перед неизвестной угрозой намного опаснее самой этой угрозы.

АНТОН КАРПОВ: Если говорить о проблеме с точки зрения менеджера или маркетолога, то можно найти сотни отчетов исследовательских компаний о

том, как spyware приносят ежегодные убытки различным компаниям. Однако пока ты (твоя компания) сам не столкнешься с этой проблемой, все эти отчеты, возможно, будешь считать «сферическим конем в вакууме». Это можно понять.

Поэтому отвечу на вопрос с чисто технической точки зрения. А правда здесь состоит в том, что современные пользовательские программы (например, веб-браузер), через которые большинство шпионского ПО и проникает на компьютеры пользователей, стали невероятно сложны и потому подвержены различным уязвимостям. Если посмотреть на историю уязвимостей веб-сервера (Apache) и веб-браузера (IE) за этот год, то у последнего она в разы больше! Это говорит о том, что клиент, потребитель трафика, сегодня подвержен множеству рисков, эксплуатация которых, при отсутствии защиты, становится тривиальной задачей. И как уже мы воспользуемся возможностью «поиметь» клиента — зашлем ему шпиона или еще как — уже второй вопрос.

ВЛАДИМИР КОМИССАРОВ: Надо подразделять понятие шпионских мотивов, а так же программ. Если мы говорим о физическом лице и его личной информации — это дело каждого. И, думаю, мало кто страдает паранойей насчет сохранности неких данных. И совсем другое дело — шпионство в масштабах предприятий, компаний и какого-либо бизнеса. Шумихой это могут называть только дилетанты или самоуверенные личности. Любая угроза, даже мнимо-потенциальная, должна рассматриваться, как реальная и должны быть приняты все меры по предотвращению любых вторжений, как извне, так и внутри информационной среды. Этому моменту необходимо уделять внимание. Лучше быть подготовленным, чем обескураженным.

АЛЕКСЕЙ ПЕТРОВ: Угроза реальна, но не смертельна. Как и с Y2K, общество IT в целом переживет эту проблему. Также как и с Y2K, много денег будет неразумно потрачено не на те проблемы. Надо бороться с причинами, а antivirusi/firewall'ы — это борьба с последствиями. В целом, проблема «шпионского ПО» будет помасштабнее и более комплексной, а риски — более серьезными. Все-таки просто безвозвратная «потеря» данных (Y2K — отказ в обслуживании) и попадание в чужие руки (шпионаж) — вещи несопоставимые. Целенаправленные шпионы представляют большую угрозу для корпоративных клиентов и целевых групп, на которые они ориентированны, — они обходят средства защиты и крадут конкретную информацию. Индивидуально написанный шпион не будет распознан по сигнатуре и, скорее всего, при талантливом подходе, сможет обойти и средства защиты proxy/firewall's.

Проблема будет актуальной до тех пор, пока «дырки» в системе залатываются медленно, а комплексность и сложность системы растет с куда большей скоростью. Без изменения механизмов защиты в самой OS, даже при наличии активных «навесных» средств защиты, срабатывать они будут значительно чаще — и даже опытный пользователь не всегда правильно сможет распознать и ответить, как реагировать в каждой ситуации, когда стоит разрешить, а когда запретить исполнение.

НУЖНЫ ЛИ ОТДЕЛЬНЫЕ СРЕДСТВА ЗАЩИТЫ ИЛИ ДОСТАТОЧНО ГРАМОТНОГО АНТИВИРУСА, В КОТОРОМ ВСЕ, ЧТО НАЗЫВАЕТСЯ, ВКЛЮЧЕНО?

КРИС КАСПЕРСКИ: Антивирус — всего лишь одно из защитных средств (точнее, подкласс защитных средств и довольно обширный: сканеры, ревизоры и т. д.), который нацелен на решение определенного круга задач. Кстати говоря, в последнее время становящихся все менее актуальными. Вирусы (то есть программы, внедряющиеся в другие программы) практически полностью перевелись, и сейчас приходится бороться в основном с червями и удаленными атаками. Антивирус может обнаружить известного ему червя и даже может убить его, но что толку? Ведь дыру, через которую приходит червь, антивирус закрыть не может. Тут нужна заплатка от производителя ПО. Откуда она у антивируса? А с удаленными атаками антивирус не может справиться в принципе, особенно если shell-код пишется под конкретную атаку и существует в единственном экземпляре. Для отражения атак применяют системы обнаружения вторжений, honeypot'ы (образно говоря, «капканы для хакеров»), и много чего еще. Конечно, коробка с диском, на котором написано «антивирус», может содержать в себе все, что угодно, но это уже скорее вопрос терминологии, чем, собственно, самой защиты.

АНТОН КАРПОВ: Если коротко, то да, нужны. Незащищенный пользователь выходит в интернет, с уязвимым веб-браузером и уязвимым почтовым клиентом и сталкивается с большим количеством угроз. Решить его проблемы призваны те самые «грамотные антивирусы «all-in-one». Однако есть и другие способы. Как вариант — идея очистки «грязного» интернет-трафика. Согласно этой идее, контент фильтруется на наличие вирусов, троянов, шпионских программ и даже спама еще на стороне провайдера, на специальных шлюзах. И до клиента доходит уже «очищенный» трафик. Подобная услуга только ищет свое применение в России, однако в некоторых странах провайдеры уже предлагают подобный «чистый интернет», который стоит, разумеется, дороже. Техническое исполнение такого решения, которое бы обладало эффективной пропускной способностью и в то же время уверенно фильтровало трафик, возможно, и подобные продукты есть. Такой подход кажется более разумным и в перспективе — правильным.

ВЛАДИМИР КОМИССАРОВ: Это дело совести и профессионализма каждого, скажем так, отвечающего за «security», в широком смысле этого слова. Чтобы рассмотреть необходимость чего-либо, надо иметь представление о информационной среде, которую собираешься охранять. В каждом отдельном случае, конечно же, нужна дополнительная защита, причем желательно индивидуально предусмотренная. Не говорю о том, что нужно садиться и писать какой-либо софт своими руками. Надо просто

предусмотреть все возможные как реальные, так и фантастические пути проникновения в среду, и уже это будет немаловажным этапом по защите. Главное — не забывать следить за соответствующими рассылками, уязвимостями и так далее. А то, как обычно бывает, поставят и забудут — вот основная причина уязвимости.

АЛЕКСЕЙ ЛУКАЦКИЙ: Мой опыт показывает, что большинство антивирусов и даже персональных систем предотвращения атак не способны эффективно бороться с spyware, а посему необходимо использование других защитных мер. Далеко не всегда это должен быть платный или вообще какой-то специализированный продукт. Многие проблемы решают бесплатные утилиты, коих в интернете можно найти в избытке. Одной из таких утилит является BHODemon, которая отслеживает появление spyware, инсталлируемого через механизм Browser Helper Objects. Еще одним эффективным защитным маневром является регулярное обновление своего компьютера путем установки патчей, service pack'ов и т.д. Это позволит прикрыть те дыры, которые используются spyware для проникновения. Но главное — бдительность и здравомыслие. Не надо ставить «левый» софт, скачанный с «левых» сайтов. Не надо на каждое окошко, всплывающее в браузере, сразу жать «Да» или «Согласен». Это позволит существенно снизить проблему заражения своего компьютера с помощью spyware.

АЛЕКСЕЙ ПЕТРОВ: Spyware/mailware/virus — все эти «зловреды» для антивируса выглядят примерно одинаково. Они могут распознаваться по их уникальным «сигнатурам» (то есть по некоторой уникальной последовательности байтов), по их злобным действиям и следам, оставляемым в системе, эвристикой (эвристический анализ), эмуляцией исполнения кода или активного слежения (tracing). Но вот способностей к «врачеванию» у некоторых антивирусов не хватает. Конечно, они могут быть дополнены, но чаще всего они много распознают и кричат, но не очень лечат. Разница в работе антивирусов (anti-spyware/anti-trojans) базируется на следующих принципах: объем базы (количество записей) «зловредов», скорость обновления и пополнения этой базы, стабильность распознавания, классификация и реакция. Типичная проблема антивирусов — в распознавании «подозрительного» или несмертельного зверя «mailware/adware». «Криков» со стороны антивируса может быть чересчур много, что мешает работе пользователя.

Комплекс средств всегда будет эффективнее. Чем больше ступеней защиты, тем выше ее надежность и меньше риски. Но и тут все не так просто, ведь чем больше ступеней — тем сложнее и неудобнее пользоваться. Это как качели. На одной стороне безопасность, на другой — удобство пользователя, а решение — в балансе между ними.

СМОЖЕТ ЛИ MICROSOFT ПОТЕСНИТЬ КОНКУРЕНТОВ НА РЫНКЕ ЗАЩИТЫ ОТ ШПИОНСКОГО ПО?

КРИС КАСПЕРСКИ: MS создает рынок шпионского ПО. Во-первых, потому, что пишет небрежный, дырявый и излишне сложный код, который выбрасывает на рынок прежде, чем успеет протестировать. Во-вторых, она продвигает идею, что компьютер — это что-то вроде тостера: включил и работаешь. Читать инструкцию и сопутствующую литературу необязательно. Этим она оболванивает рядовых пользователей и отнимает хлеб у профессиональных администраторов, в результате чего заботу о сервере поручают случайным людям. Рынок защиты MS, похоже, совсем не интересует. Да, она интегрировала какую-то пародию на брандмауэр в последние версии XP и создала несколько утилит для поимки малвари. Но чтение блогов их разработчиков создает стойкое впечатление, что эти люди увидели живую малврь уже после написания своего чуда техники, которое, к тому же, очень легко обойти. И малварь будет его обходить, как только получит распространение. На данный момент достоверно известно лишь одно — у MS есть деньги. Много денег. И если она захочет прибрать к рукам этот сегмент рынка...

АНТОН КАРПОВ: Microsoft стоит задуматься о том, где находится корень зла ;). Вместо того, чтобы выпускать защиту от проблем, появляющихся вследствие, в том числе и качества программного кода уязвимых систем, им следует следить за этим самым качеством кода.

ВЛАДИМИР КОМИССАРОВ: Не думаю. В конкуренции рождается истина, и благодаря ей продолжается развитие. Если конкуренции не будет, то используемый софт будет слабоват и уязвим. И потом, Microsoft'а на всех не хватит. И это радует.

АЛЕКСЕЙ ЛУКАЦКИЙ: Ее конкуренты сами вынудили компанию пойти этим путем. Когда MS выпустила бесплатный MS AntiSpyware, большинство антивирусных производителей стали забрасывать ее исками о нарушении монопольного законодательства и т.д. Однако MS сама всегда признавала, что ее решения обеспечивают базовый уровень защиты, расширить который можно с помощью решений других вендоров. Теперь же компанию вынудили вплотную заняться выпуском полноценного программного продукта (или сервиса, такого как OneCare), который, учитывая возможности и ресурсы MS, потеснит многих игроков с этого рынка. Можно долго говорить о том, что серьезные покупатели не выберут MS в качестве поставщика средств защиты, но рядовой пользователь почему-то этого «не слышит» и по-прежнему делает выбор в пользу продукции Microsoft. Также он поступит и с ее решениями по защите компьютеров — это привычнее и гораздо выгоднее.

АЛЕКСЕЙ ПЕТРОВ: Судя по уровню и тем продуктам MS, которые сейчас доступны, вряд ли MS сможет завоевать этот рынок. Разве что компания в очередной раз скупит какую-нибудь успешную разработку и введет ее в состав MS :). Другой аспект проблемы заключается в том, что изначально неудачная конструкция и механизмы безопасности MS-продуктов как раз таки и являются корнем всей проблемы —

конструкция «никак» не противодействует активности вирусов и троянов. А множественные ошибки в ПО прикладного (IE/Outlook) и основного уровней (data-objects parsing/handling) представляют прекрасную платформу для активизации вирусов-троянов. Излишне сложный механизм обновлений только способствует этому.

/ ПО СЛОВАМ ИГОРЯ ДАНИЛОВА, РЫНОК АНТИВИРУСОВ — ЭТО ОГРОМНЫЙ МЫЛЬНЫЙ ПУЗЫРЬ, КОТОРЫЙ ДЕРЖИТСЯ НА СТРАХЕ ПОЛЬЗОВАТЕЛЕЙ. ТАК ЛИ ЭТО?

ВЛАДИМИР КОМИССАРОВ: Абсолютно не согласен. Не сказать, что в корне, но я так не думаю и правильно делаю. Страх проходит: благо, компьютер в домах граждан — уже не диковинка. И сами они уже умеют давить на клавиши и осознают, что им надо, а что нет. Если же взять масштабы предприятия и ценности информации, то тут я в корне с господином Даниловым не согласен. Потому как не уследишь, какой сотрудник какой диск принесет, на какой сайт залезет... И последствия инфицирования могут серьезно отразиться на бюджете компании. Поэтому ГРАМОТНЫЙ IT-специалист никогда не пренебрежет защитой, пусть даже от дурака. Работа такая.

АЛЕКСЕЙ ЛУКАЦКИЙ: Интересно слышать такое высказывание от разработчика Dr.Web. Но отчасти он прав. Проблемы излишне преувеличены. Число «диких» вирусов несопоставимо с числом вирусов, выращенных в пробирке и хранящихся только в исследовательских центрах антивирусных компаний. Большинство антивирусных компаний паразитируют на данной проблеме, пугая неискушенного пользователя всякими страшилками. Ведь решить проблему вирусов можно гораздо эффективнее и не прибегая к большим финансовым затратам на приобретение антивирусов. Достаточно вспомнить, что для того, чтобы не заразиться дизентерией, в абсолютном большинстве случаев достаточно мыть перед едой руки и фрукты. Для этого не надо колоть себе антибиотики и пропускать фрукты через многоступенчатую систему химической очистки. Аналогичная ситуация и с антивирусными продуктами.

АЛЕКСЕЙ ПЕТРОВ: Частично да. И происходит это частично из-за непонимания проблемы в целом. Антивирус — не панацея, а только одна из возможных навесных «ступенек» защиты, частично превентивная и частично пост-фактум мера, но это никогда не 100% гарантия. Антивирус ловит и распознает «знакомые» и «широко распространенные вирусы». Это противоядие, которое еще не факт что спасет, антивирус — это не прививка, у которой гарантии куда выше. «Зловреды» стараниями своих создателей за последнее время сильно мутировали и «поумнели»: приобрели способности обходить firewall'ы и распространенные антивирусы, умеют самообновляться. А распространенные антивирусы — это как раз те, которых в первую очередь и будут обходить. И цены на антивирусы искусственно сильно завышены.

/ КАКИЕ СРЕДСТВА ЗАЩИТЫ ОТ ШПИОНОВ/ТРОЯНОВ/ВИРУСОВ ИСПОЛЬЗУЕШЬ САМ И ЧТО СОВЕТУЕШЬ ДРУГИМ?

КРИС КАСПЕРСКИ: Прежде всего, это разграничение доступа — я вхожу в систему под администратором только тогда, когда это действительно нужно, а в остальное время я — пользователь. Второе — использование максимально недырявого ПО (и в первую очередь отказ от IE в пользу Оперы/Лиса/Рыся). Третье — не запускаю программ, полученных из ненадежных источников на основной машине, только под VM Ware. И на закуску — раз или два раза в год запускаю онлайновый сканер Евгения Касперского, чтобы убедиться, что все спокойно. Или использую какой-нибудь другой антивирус. Поскольку это делается чисто для успокоения (то есть создания иллюзии безопасности и самообмана), — выбор антивируса некритичен.

АНТОН КАРПОВ: Так повелось, что системы и софт, который использую лично я, не подвержены шпионам, троянам и вирусам. Мне трудно вспомнить, когда я последний раз видел вирусы и трояны для FreeBSD (имеется в виду клиентская машина, так как я использую эту ОС в качестве настольной рабочей системы) или эксплоит для почтового клиента Mutt, например.

ВЛАДИМИР КОМИССАРОВ: Использую корпоративный Symantec Antivirus и еще пару сторонних программ. И, конечно, собственные глаза и руки. Анализ логов слежения за трафиком и процессами еще никто не отменял, и никакая программа лучше тебя не заподозрит неладное задним чувством и не направит на путь истинный.

АЛЕКСЕЙ ЛУКАЦКИЙ: Во-первых, у меня установлен антивирус, который обеспечивает мне первую линию обороны. На втором уровне у меня задействуется несигнатурный Cisco Security Agent. Для защиты от BHO-spyware использую BHODemon. Конечно же, регулярная установка патчей, защищенная настройка браузера и ОС. И, наконец, здравомыслие при использовании интернета и различных «посторонних» программ. Кстати, о последних. Я ими практически не пользуюсь. Я либо приобретаю лицензионное ПО, либо использую то, что мне централизованно предоставляет компания (а это очень большой список).

АЛЕКСЕЙ ПЕТРОВ: Для Win применяю комплекс из нескольких антивирусов, нескольких antispyware, активный персональный firewall (мои рекомендации — Outpost Firewall от Agnitum), плюс соответствующая настройка самой системы, как минимум IE/MS win. Активный application layer firewall не просто блокирует какие-то порты, а распознает, кто пытается установить соединение. Agnitum FW был первым на этом пути и по-прежнему полон новаторских идей. Кстати, популярность альтернативных web browser'ов тоже в некоторой степени базируется на снижении рисков инфицирования, по сравнению с IE. В каждом конкретном случае все подбирается, исходя из условий, под задачи, которые надо решать. Хорошая защита — это всегда индивидуальный и уникальный подход, а информация о периметре и средствах безопасности — это часть мер безопасности, и тоже секрет. Стандартная защита и ломается стандартно **C**