Защита в реальном мире

текст Вячеслав Медведев, ведущий аналитик отдела развития компании «Доктор Веб»

Конфликт вокруг Украины стал лакмусовой бумажкой для понимания реальной защищенности многих компаний и организаций и оценкой реального отношения руководства компаний и чиновников самого высокого уровня к обеспечению безопасности, в том числе собственной. Взломы переписки чиновников по всему миру показали: несмотря на то что властные структуры России и Украины делают громкие заявления о создании собственных операционных систем, о запрете на общение через зарубежные почтовые сервисы и т.д., в реальной жизни они не следуют своим во многом правильным и своевременным планам.

Отношение к безопасности денежных операций ничуть не лучше. Особенно в сфере малого и среднего бизнеса. С одной стороны, модные тенденции BUOD и привлечение фрилансеров приводят к тому, что компании с удовольствием разрешают сотрудникам работать с личных устройств и домашних компьютеров. С другой стороны, налицо общее заблуждение, что малый бизнес не интересен хакерам, так как потраченное на взлом время никогда не окупится.

Вот только все совсем не так. Вредоносные программы, в том числе и банковские троянцы, распространяются через взломанные сайты, как правило, посещаемые сотрудниками компаний по служебной необходимости. Откроет ли сайт бухгалтер небольшой компании или финансовый директор корпорации – программе нет разницы, кого заражать. Более того, поскольку уровень защиты (в том числе в связи с меньшими бюджетами) в малом и среднем бизнесе куда ниже, то заражать такие компании выгоднее.

Еще хуже обстоят дела с личными компьютерами и устройствами. Если офисный компьютер отделен от сети Интернет шлюзом, на компьютере работает, как правило, один человек, а за безопасность отвечает специалист, то при использовании личной машины все обстоит иначе. Прямой доступ в Интернет – значит прямой доступ хакеров к компьютеру, наличие большого количества пользователей, не имеющих никаких знаний в области безопасности (а то и старательно в силу возраста их игнорирующих), постоянное посещение ресурсов, сомнительных с точки зрения наличия угроз... Для безопасности компьютеров локальной сети нормальным считается применение межсетевых экранов, средств аутентификации и контроля доступа и т.д. – конечно, все они не обязательно должны стоять именно на компьютере бухгалтера. Уровень угроз для домашней машины куда выше: ее защита ограничивается, как правило, одним антивирусом, а как минимум в трети случаев не устанавливается даже он, так как считается, что любое заражение будет сразу заметно, а по сомнительным ресурсам никто не ходит.

Получается, что злоумышленникам куда выгоднее и проще атаковать личные компьютеры сотрудников, работающих из дома, тем более что и из дома, и с работы они посещают по служебной необходимости одни и те же ресурсы сети Интернет.

По данным Digital Security хотя бы одну уязвимость содержат все изученные приложения мобильного банкинга для iOS и Android.

Злоумышленники не выпускают в мир вредоносные программы (в том

УЯЗВИМО ВСЕ: ПРАКТИЧЕСКИ ВСЕ АКТИВНО ИСПОЛЬЗУЕМЫЕ ПРОГРАММЫ ИМЕЮТ УЯЗВИМОСТИ (ИСТОЧНИК: SECUNIA TOP 50 VULNERABILITY REVIEW 2012)

GOOGLE CHROME	291
MOZILLA FIREFOX	257
APPLE ITUNES	243
ADOBE FLASH PLAYER	67
ORACLE JAVA JRE SE	66
ADOBE AIR	56
MICROSOFT WINDOWS 7	50
ADOBE READER	43
MICROSOFT INTERNET EXPLORER	41

**РЕАГИРУЮТ ЛИ НА УГРОЗЫ ПОЛЬЗОВАТЕЛИ?
(ИСТОЧНИК: MICROSOFT SECURITY INTELLIGENCE REPORT, ВЫПУСК 13)**

Статус обновления безопасности	MICROSOFT WINDOWS	MICROSOFT WORD	ADOBE READER	ORACLE JAVA	ADOBE FLASH PLAYER
Нет последнего обновления	34%	39%	60%	94%	70%

числе и банковские троянцы), если они обнаруживаются актуальными версиями антивирусов. Банковские троянцы стремятся работать максимально незаметно: закрывают за собой уязвимости, через которые проникли, удаляют конкурирующие вредоносные программы и т.д.

Проникшие банковские троянцы могут похищать файлы cookies, записывать нажатия пользователем клавиш (с целью хищения паролей), перехватывать и анализировать сетевой трафик (в том числе защищенный), создавать скриншоты в процессе ввода каких-либо данных в экранные формы с использованием виртуальной клавиатуры, перехватывать и передавать злоумышленникам изображения с подключенных к компьютеру веб-камеры и микрофона, красть сохраненные в системе пароли. И кроме всего прочего, перехватывать все электронные письма и содержание мгновенных сообщений – в дальнейшем это используется для шантажа.

ЧТО В ИТОГЕ?

По данным B2B International, 72% российских интернет-пользователей, которые подверглись кибератакам и потеряли в итоге реальные деньги, так и не смогли вернуть свои финансовые сбережения в полном объеме.

Что делать? Поставить (и настроить) необходимое программное обеспечение и продумать, что нужно делать в том случае, если принятых мер будет недостаточно.

Казалось бы, первая часть – выбор мер защиты – не является трудным делом: существуют стандарты PCI-DSS и СТО БР РФ, приказы ФСТЭК России, письма Банка России (включая Письмо № 49-Т). Для работы в системе «Банк-Клиент» должен быть выделен отдельный компьютер, по возможности использующий операционную систему, для которой разработано меньшее количество вредоносных файлов. Устанавливаем антивирус, запрещаем сменные носители и все ресурсы, кроме необходимых для системы «Банк-Клиент» и обновлений безопасности. Все?

Нет. В казалось бы ясном деле есть проблема: для всех документов по безопасности нет глоссария, правильно определяющего термины. Например, все они требуют установки антивируса везде, где может действовать вредоносная программа и где антивирус не мешает технологическому процессу. На первый взгляд, что может быть проще? Но проблема в том, что в большинстве случаев специалисты пролагают: антивирус должен ловить все входящие вредоносные программы. То есть если установлен антивирус, то иные средства предотвращения проникновения вредоносных программ не нужны, а антивирус, пропускающий вирусы, просто плохой, и его нужно заменить хорошим. Но хакеры распространяют свои «произведения», только если они не обнаруживаются антивирусами в момент выпуска.

Антивирус нужен не только для обнаружения проникающих программ (и он это делает успешно), но и для лечения ранее проникших и неизвестных вредоносных программ – кроме него это сделать не в силах ни одна программа. А для противодействия проникновению новейших троянцев используется не традиционное антивирусное ядро, а офисный контроль (ограничение прав доступа к объектам системы, белый список запускаемых программ), превентивная защита, контролирующая запускаемые программы на основе знаний о шаблонах поведения вредоносных программ, и система контроля точек проникновения – основных мест, которые стремятся изменить вредоносные программы. И естественно, не забываем обновлять все установленные приложения и использовать надежные пароли.

Но программы не могут всего – нужны процедуры на случай, когда страшное все же случилось. Что делать, когда обнаружена кража денежных средств или были зашифрованы файлы? Вызвать системного администратора? Написать на форум? Выключить компьютер? Позвонить в полицию? Запустить антивирус?

Вопросов возникает много, а действовать надо мгновенно – перевод денег по стране может пройти за считаные минуты. На этот случай и нужны процедуры: каждый работник должен знать порядок своих действий, список сотрудников, которых он должен оповестить, и т.д.

Знание решает многие проблемы, поэтому не нужно стесняться задавать вопросы вендорам – однажды это может вас спасти. NBJ

СПРАВКА

«Доктор Веб» – российский разработчик средств ИБ. Продукты Dr.Web демонстрируют превосходные результаты детектирования вредоносных программ, соответствуют мировым стандартам безопасности, сертифицированы ФСТЭК, Минобороны и ФСБ России.

Флагманское решение – комплекс корпоративных продуктов Dr.Web Enterprise Security Suite – отвечает всем актуальным требованиям к системе антивирусной безопасности. Интернет-сервис Dr.Web AV-Desk, дающий возможность пользоваться антивирусом в качестве услуги сервис-провайдеров, предлагают своим клиентам более 200 компаний, предоставляющих ИТ-услуги в России и за рубежом. «Доктор Веб» имеет собственную службу вирусного мониторинга и аналитическую лабораторию.