Риски ИБ и инструменты Dr. Web для борьбы с ними

Вячеслав Медведев
Начальник сектора продукт-менеджмента компании «Доктор Веб»

Известно — точный диагноз дает только патологоанатом. К области информационной безопасности данное утверждение подходит как нельзя более.

Почему так? Причин несколько. Помните анекдот про Ходжу Насреддина? Как-то его спросила женщина «Чего мне бояться?». Ходжа ответил «Черного орла, залетевшего в твой дом». Вопрошавшая была так впечатлена ответом, что не обратила внимания на добавленное скороговоркой «...и серых мышей, шуршащих под полом». Безжалостная статистика показывает, что компании не того боятся и не тем защищаются. Производители средств защиты публикуют обзоры, проводят обучения и презентации, информация об угрозах никоим образом не скрывается (скрывать ее совершенно не выгодно, так как отсутствие спроса на средства защиты от современных угроз тормозит развитие этих самых средств защиты). И что же?

Какое представление об источниках и средствах угроз системам сложилось у пользователей? Исходя из каких соображений и какие именно требования предъявляются к способам защиты систем от проникновения вредоносных программ? Насколько они адекватны и достигает ли желанных целей выполнение этих требований? Попробуем выяснить это.

Опросы показывают, что если спросить IT-специалистов о том, какой наиболее опасный путь проникновения вредоносных программ на сегодняшний день, то называют (в разной последовательности) сменные носители, почту, порнографические сайты. Но сменные носители можно запретить офисным контролем, почту можно фильтровать на вирусы, спам и фишинг, а порнографические сайты можно заблокировать, разрешив доступ только к определенным ресурсам сети. Кстати, порнографические сайты не лидер зараженности — им выгодно распространять иные услуги.

Настоящая и истинная опасность исходит от сайтов, которые сотрудники посещают, выполняя служебные обязанности — новостные, финансовые и прочие ресурсы сети нельзя запретить в компании. Но они не менее уязвимы, чем все другие, и, учитывая ограничения бюджета, накладываемые на обслуживание сайтов, можно только посочувствовать тем, кто посещает эти сайты на постоянной основе.

Итак, пусть сайт взломан, туда запущен троян — но трафик же проверяется, значит, троян при наличии антивируса не должен попасть в систему. Но это тоже заблуждение, еще более опасное! Наиболее совершенные вредоносные программы давно выпускают не хакеры-любители, а профессионалы, объединенные в своеобразные подобия фирм — разработчиков компьютерных программ. Вредоносные программы тестируются и не выпускаются «в свет», пока остается возможность, что они будут обнаружены хотя бы одним антивирусом, использующимся у атакуемой группы пользователей.

Соответственно распространенным мифам формулируются и требования к организации защиты: выбранный антивирус (желательно использующий облачные технологии) должен ловить все вредоносные программы, пытающиеся проникнуть в защищаемую сеть, антивирус должен интегрироваться в корпоративную сеть управления, антивирус должен поддерживать возможность подключения к компьютеру только разрешенных сменных устройств... Список требований далеко не полный, но типичный. Только все не так просто.

Антивирус не способен перехватить все, что проникает в систему. При этом активная и неизвестная антивирусу вредоносная программа может использовать интеграцию с корпоративной системой управления для деинсталляции системы защиты — ведь она не защищена системой самозащиты!

Со сменными носителями иная проблема: партии флешек идут с одним идентификатором. Скажем, банкоматы и терминалы, как правило, заражаются со сменных носителей. Казалось бы, достаточно составить список сменных носителей, разрешенных для подключения к банкомату, и

злоумышленник не сможет внедрить свою программу. Да вот только первое же подключение разрешенной флешки будет сфотографировано, а подобрать такую же флешку — дело техники.

Итак, оказывается, что источники и способы заражения не всегда правильно оцениваются пользователем, тем более не очевидны пути решения проблемы. Решения Dr. Web, основанные как на многолетнем опыте, так и на постоянном отслеживании современных тенденций, призваны обеспечить надежную защиту вычислительных систем.

В решениях Dr.Web сознательно не используется ряд технологий, которые могли бы позволить злоумышленникам нейтрализовать систему безопасности. Одновременно постоянное развитие новых технологий детектирования и лечения уже активных вредоносных программ обеспечивает бОльшую эффективность защиты при меньших затратах ресурсов компьютеров и устройств. Стало возможным периодически уменьшать количество записей ядра, что обеспечивает возможность работы на слабых рабочих станциях, банкоматах и терминалах

Решения Dr.Web содержат в себе проактивную технологию, анализирующую запускаемые программы. Данная технология не требует обучения со стороны пользователей — она построена на знании характерных признаков поведения такого, например, опасного класса вредоносных программ, как шифровальщики. Кроме того, данная подсистема связана с системой резервного копирования и позволяет восстанавливать зашифрованные или утерянные файлы.

Решения Dr.Web проверяют любой трафик до его попадания в клиентскую программу — вредоносный файл не сможет использовать ее еще не устраненную уязвимость. Технология ScriptHeuristic (работающая со всеми браузерами) предотвращает исполнение любых вредоносных скриптов в браузере, html- и pdf-документах, не нарушая при этом функциональности легитимных скриптов.

Благодаря функции защиты трафика вредоносная программа не имеет возможности перехвата обновлений, а функция фонового сканирования и нейтрализации активных угроз в критических областях Windows и системной BIOS компьютера позволит уничтожить ранее неизвестные вредоносные программы, как бы глубоко они не проникли в систему

Возможность установки на любые операционные системы, использование практически всех баз данных, выполнение всех требований регулирующих органов — все это обеспечивается только при использовании решений Dr.Web.