тема номера

# с чем входим в новый год в сфере ИБ?

## форум в Магнитогорске — это своеобразный рубеж, на котором принято подводить итоги и давать прогнозы. Не будем делать исключения из этого правила и на этот раз

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

**Если говорить об информационной безопасности, то прошедший год и развитие его тенденций в нынешнем году были достаточно интересны. На 2015 год прогнозировались рост угроз для мобильных платформ и (не всеми экспертами, но мы предупреждали!) рост интереса злоумышленников к Linux. Прогнозы оправдались: количество угроз для этих платформ выросло, вредоносные программы для них были оснащены новыми возможностями.**

Впрочем, гораздо важнее то, что прошедший год был ознаменован выходом в массы «умных» устройств среди пользователей и интересом злоумышленников и к ним, и к проникновению в системы управления технологическими процессами. Нельзя сказать, что и того, и другого ранее не было, – было, вспомним тот же Stuxnet. Но, в отличие от проникновений прошлых лет, произошел переход от единичных таргетированных атак к исследованию устройств и систем, используемых большинством компаний. И смело можно сказать, что к противостоянию на этом фронте не готовы ни поставщики средств защиты, ни большинство клиентов.

Но вернемся к итогам года. Фактически застопорилось исполнение требований регуляторов в области защиты банками своих клиентов. Это действительно требует массы усилий при неочевидной выгоде для банка. Прошлый год был отмечен увеличением доли вредоносных файлов для мобильных устройств, направленных на кражу денежных средств клиентов банков, а также на модификацию СМС-подтверждений систем ДБО. Появились и новые вредоносные файлы для кражи денежных средств через банкоматы.

Естественно, у вендоров есть продукты, позволяющие защитить и банкоматы, и мобильные устройства. Существуют решения и для антифрод-систем. В последнем случае можно передавать в антифрод-систему сведения сервиса Dr.Web AV-Desk, который банк использует для защиты своих клиентов, или, используя специальное API, получать данные о наличии антивирусной системы защиты на рабочих станциях и серверах, с которых осуществляется платеж. Антифрод-система может проверять, установлена ли антивирусная защита, насколько давно производилось обновление и какие настройки используются пользователем. Последнее особенно важно, так как в интересах злоумышленников обеспечить незаметную работу вредоносного ПО в течение длительного времени.

Для противодействия специально разработанному ПО, еще не попавшему в руки аналитиков антивирусных компаний, недостаточно использовать только возможности антивирусного ядра или превентивной защиты, основанной на сигнатурах – признаках конкретных угроз. Необходим контроль на основе соответствия поведения запущенных программ моделям поведения программ вредоносных. При этом важно отслеживать не только взаимодействие вредоносного процесса с ресурсами зараженной системы, но и работу вредоносного объекта-эксплойта внутри зараженного процесса. Для кражи денежных средств достаточно изменить лишь вид страницы браузера – при этом внешне для контролирующих систем зараженный процесс будет вести себя вполне легитимно.

Особую проблему составляет защита мобильных устройств. Многие пользователи пренебрегают защитой своих девайсов, что не дает устранить угрозу даже в случае обнаружения подозрительного поведения зараженного устройства. Появившиеся в прошлом году троянские программы (такие как Android.BackDoor.240.origin и Android.DownLoader.155.origin, попавшие, кстати, в десятку наиболее распространенных) могут получать root-привилегии на атакуемых устройствах. Архитектура Android подразумевает, что антивирус работает с правами обычных приложений и не может удалять вредоносные устройства из системных областей. Решение, естественно, есть – например, лечение таких заражений поддерживается в Dr.Web Security Space для Android. Но даже в этом случае к подобной угрозе нужно быть готовыми, поскольку во многих случаях устранение угрозы происходит при участии владельца устройства.

Еще больше проблем возникает при защите устройств и систем, установка антивирусов на которые невозможна, – например, по причине ограниченности ресурсов. Для защиты таких устройств приходится контролировать поступающие на эти устройства файлы – это возможно, но владельцы устройств должны понимать, что полной защиты это не дает. Риск заражения неизвестным троянцем есть всегда, и нужно быть во всеоружии, когда об этом станет известно.