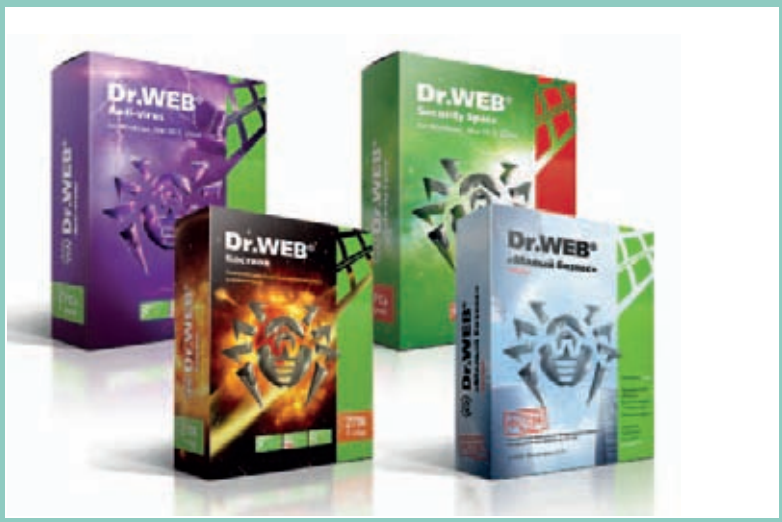
Борис Шаров
Генеральный директор ООО «Доктор Веб»

Банковская сфера давно находится под пристальным вниманием киберпреступников. Не стал исключением и 2015 год, принесший новые банковские трояны, нацеленные на клиентов банков — как на корпоративных, так и на физических лиц. Были и таргетированные атаки непосредственно на банки, но о них, разумеется, мы не можем говорить подробно. Новые трояны создаются постоянно, как и модифицируются старые — с целью обойти традиционную антивирусную защиту хотя бы на отрезок времени между появлением нового образца вредоносной программы и добавлением его в вирусные базы.

Сейчас речь идет уже не о технологиях выявления вредоносных программ на основе базы вирусных сигнатур, а об обезвреживании любой вредоносной активности по моделям ее поведения. Причем нужны новейшие технологии для всех защищаемых нами операционных систем, ведь у каждой — свои особенности. В 2016 г. мы не собираемся расслабляться, да преступники и не дадут.

Мы постоянно развиваем наши технологии превентивной защиты, позволяющие предотвращать заражение новыми, еще не попавшими в сигнатурные базы угрозами. В 2015 г. мы выпустили 11-ю версию нашего антивируса, в которой дополнили и улучшили технологии борьбы с новейшими угрозами. Для тех пользователей, которые предпочитают антивирусы других производителей, мы создали дополнительный несигнатурный антивирус Dr.Web Katana, который собрал в себе самые современные технологии превентивной защиты рабочих станций. Мы ощущаем потребность в этом продукте не только в России, но и в других странах, ведь он позволяет справляться с теми троянами, которые могут быть неизвестны сигнатурному антивирусу, работая с антивирусами других производителей без конфликтов в системе.

Вредоносные программы давно представляют опасность не только для рабочих станций и серверов. Так, POS-терминалы все чаще становятся целью киберпреступников: в 2015 г. наша лаборатория неоднократно сообщала об обнаружении вредоносных программ, заражающих подобные устройства. Определенных успехов добилась наши специалисты и в раскрытии всей инфраструктуры преступников, использовавших троянские программы для кражи и последующей перепродажи данных банковских карт, побывавших в зараженных POS-терминалах.



Также в этом году в геометрической прогрессии росло число банковских троянов для мобильных устройств под управлением ОС Android, из-за чего серьезно вырос спрос на защиту планшетов и смартфонов. Вирусописатели все чаще стали применять в своих атаках более «продвинутые» трояны, используя при этом, например, механизмы таргетированных смс-рассылок по специально сформированным базам реально существующих объявлений, или внедряя вредоносный код в легитимные приложения, например, Банк—Клиенты, с последующим размещением результата на различных сайтах. Некоторые из банковских троянов пытаются нарушить работу ряда антивирусных приложений, когда те производят попытку удаления вредоносной программы с зараженного устройства, с чем наш антивирус, разумеется, успешно борется.

Интересный троян был обнаружен нашими вирусными аналитиками в декабре 2015 г. — он похищал конфиденциальную информацию, создавая поверх приложений мошеннические формы ввода, которые «привязывались» к атакуемым программам и были оформлены в стиле приложений мобильного банкинга популярных российских банков.

К сожалению, даже задержание киберпреступников, создающих или использующих вредоносные программы для кражи денежных средств с помощью систем ДБО, не ограничивают атаки на клиентов банков. Например, в апреле 2015 г. управлением «К» МВД России были задержаны участники группы,

«Доктор Веб»:
новые задачи, новые технологии

создававшие определенный вид банковских троянов для устройств, работающих под Android, однако в том же месяце нашими специалистами были обнаружены новые модификации. Киберпреступность уже давно стала бизнесом, где крутятся большие деньги, а вредоносное программное обеспечение создается, сдается в аренду, перепродается и пишется на заказ.

Непосредственно в области защиты мобильных устройств под Android запланирован ряд интересных инноваций. В феврале 2016 г. выйдет 11-я версия защиты с очень важной и оригинальной особенностью, которой пока что нет ни у кого. Не буду много говорить о ней заранее, но появилась эта возможность благодаря выходу Android 6.0. Новая версия должна дополнительно утвердить нас в качестве производителя самого популярного мобильного антивируса под Android — только через Google Play его скачало уже почти 100 млн пользователей.

Если говорить о том, что стало символом угроз 2015 г., то это, безусловно, трояны-вымогатели, шифрующие данные на зараженном компьютере. Их число росло лавинообразно, большая часть запросов в нашу техподдержку приходила именно от пострадавших от этих вредоносных программ. Важно отметить, что обращаются к нам в подавляющем большинстве пользователи других антивирусов. Именно это и подтолкнуло нас к выделению блока новейших превентивных технологий, реализованных в нашем основном продукте для Microsoft Windows, в отдельный продукт — Dr.Web Katana, который мы адресуем тем, кто по тем или иным причинам не выбрал антивирус Dr.Web в качестве средства защиты.

Наша компания старается оперативно отвечать на появление подобных угроз. Вирусные аналитики тщательно изучают каждый новый экземпляр попадающих в лабораторию «шифровальщиков» и в некоторых случаях предоставляют пользователям возможность расшифровки поврежденных данных. Так, недавно мы сообщили о первом трояне-вымогателе для Linux-серверов, и буквально на следующий день после обнаружения его удалось расколоть. И хотя помочь мы можем далеко не всем обратившимся, услуга расшифровки данных силами специалистов «Доктор Веб» становится популярной во все большем числе стран.

Мы будем и дальше держать на высоком уровне норму нашей прибыли, оставаясь одной из 50 самых прибыльных IT-компаний России (http://www.tadviser.ru/index.php). Наша компания просто не имеет права допустить нестабильность нашего бизнеса, ведь под защитой наших технологий так много корпоративных клиентов, органов законодательной, исполнительной и судебной власти, силовых структур и ведомств нашей страны. Мы вносим свой вклад в обороноспособность России, защищая ее от негативных внешних воздействий, в том числе хакерских атак силами спецслужб недружественных государств и террористических организаций. С января 2016 г. наши корпоративные заказчики смогут начать использовать новейшие технологии Dr.Web Enterprise Security Suite версии 10, прошедшие сертификацию ФСТЭК России.

В уходящем году активно обсуждалась тема импортозамещения. Принято важное постановление правительства на эту тему, намечены конкретные меры по поддержке отечественных разработчиков, по предотвращению ухода бюджетных денег, выделяемых на IT-решения, за рубеж. Но для компании «Доктор Веб» с этим ничего не поменялось. С самого начала своего существования мы как раз и занимались импортозамещением, создавая продукты, превосходящие по своим качествам и надежности зарубежные аналоги. Мы понимаем, что это единственный способ завоевать отечественный рынок, рынок страны, которая является для нас главной во всех отношениях.